

(BETA)FIDO2 Configuration in Access (MacOS)

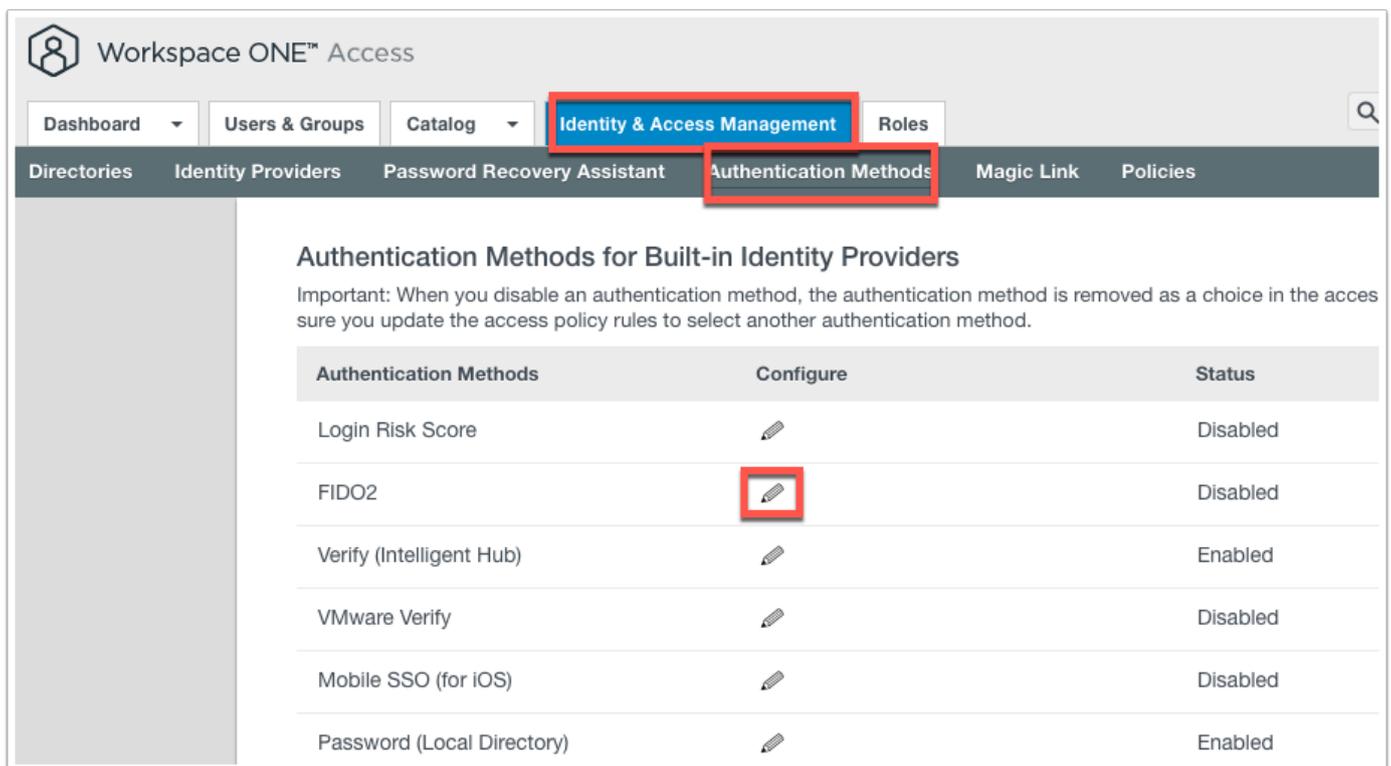
This lab is designed to help you understand how to setup and authenticate using FIDO2 (Fast Identity Online). You will discover the requirements and implement the solution into your existing Workspace ONE Access environment.

Part 1: Setup FIDO2

Part 2: Register Authenticator

Part 3: Administer FIDO2 Keys

Part 1: Setup FIDO2



Workspace ONE™ Access

Dashboard Users & Groups Catalog Identity & Access Management Roles

Directories Identity Providers Password Recovery Assistant Authentication Methods Magic Link Policies

Authentication Methods for Built-in Identity Providers

Important: When you disable an authentication method, the authentication method is removed as a choice in the access policy rules. Make sure you update the access policy rules to select another authentication method.

Authentication Methods	Configure	Status
Login Risk Score		Disabled
FIDO2		Disabled
Verify (Intelligent Hub)		Enabled
VMware Verify		Disabled
Mobile SSO (for iOS)		Disabled
Password (Local Directory)		Enabled

1. 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
System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Enabled
Built-in	Verify (Intelligent Hub) Certificate (cloud deployment) Password (cloud deployment)	LivefireSync	ALL RANGES	ws1-connector.euc-livfire.com	Built-in	Enabled
Workspacel..._3666	Password	LivefireSync	ALL RANGES	ws1-connector.euc-livfire.com	Workspace ONE Access	Enabled
Auth0	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.

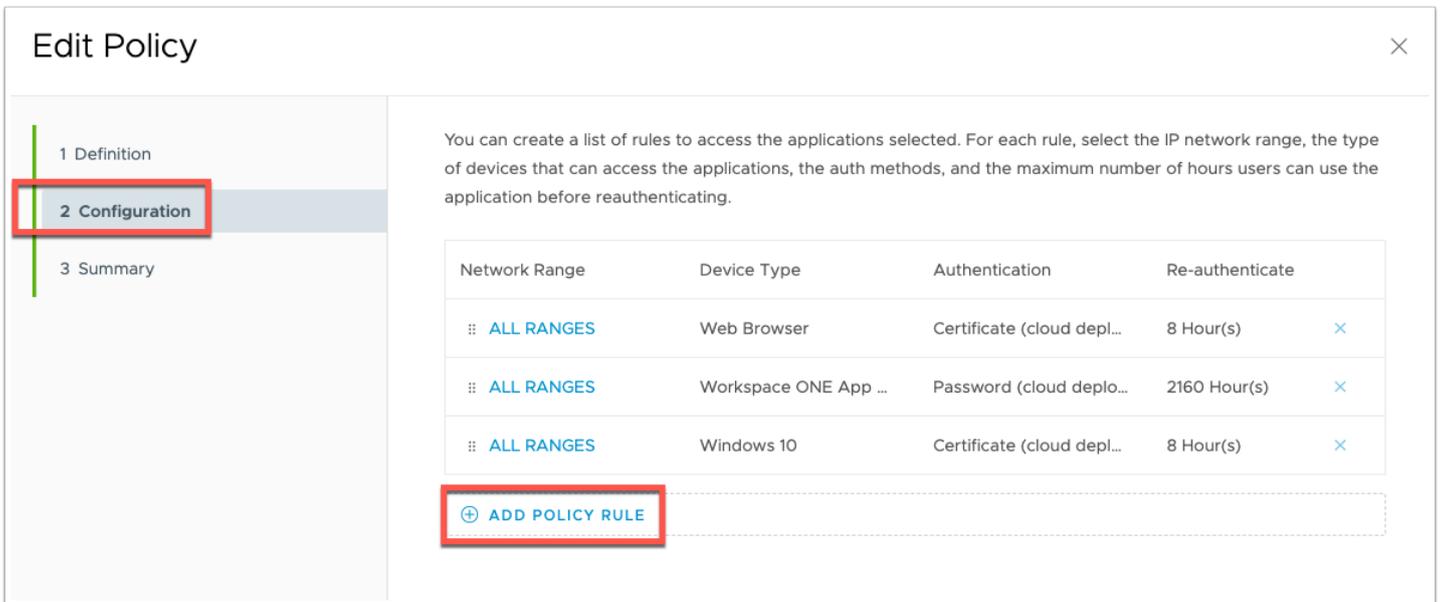
- After the **Authentication Methods** loads on the Built-in IDP screen click to enable the **FIDO2** authentication method.
 - Click **Save** at the bottom of the screen

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

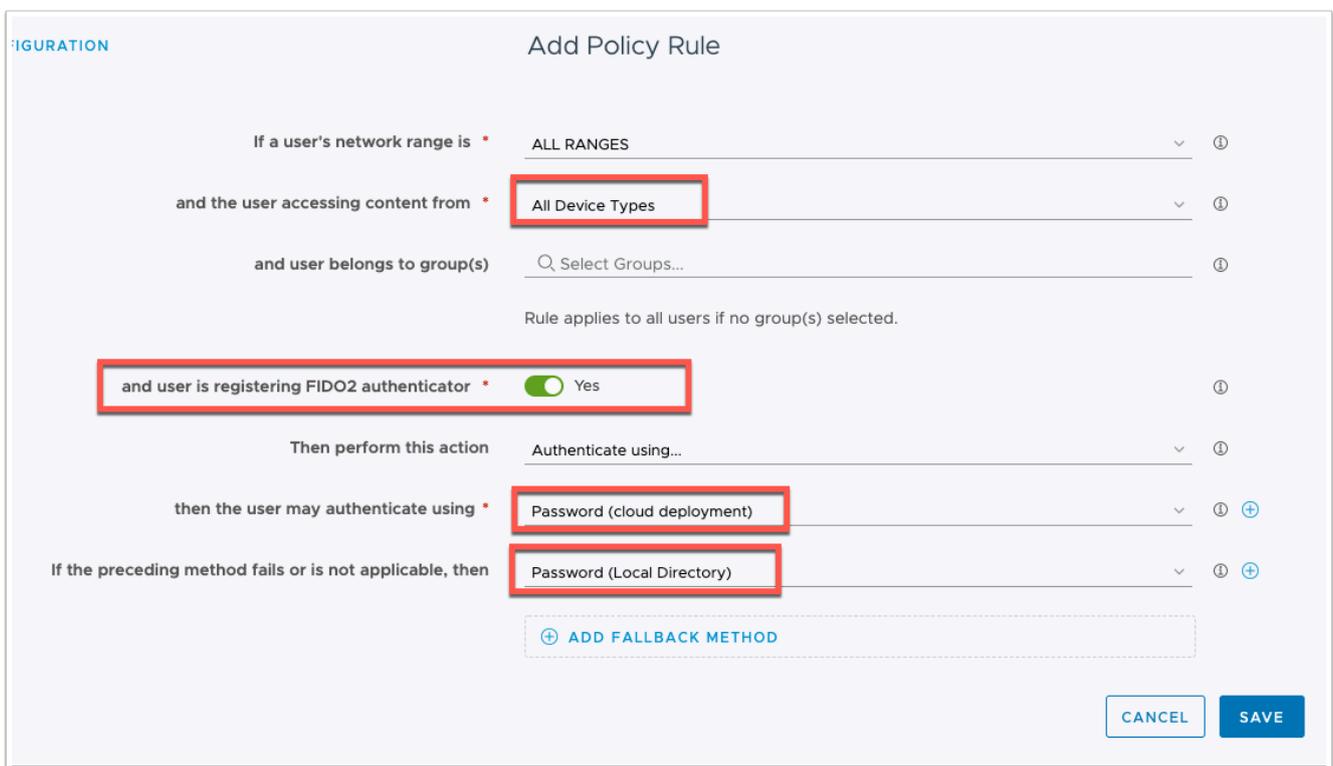
Directories | Identity Providers | Password Recovery Assistant | **Authentication Methods** | Magic Link | Policies

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**



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



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)**

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	Any	Password (cloud depl...	8 Hour(s) ✕
ALL RANGES	Web Browser	Certificate (cloud depl...	8 Hour(s) ✕
ALL RANGES	Workspace ONE App ...	Password (cloud depl...	2160 Hour(s) ✕
ALL RANGES	Windows 10	Certificate (cloud depl...	8 Hour(s) ✕

⊕ ADD POLICY RULE

8. Move the policy you just built from the bottom to the top.

- Now click **ALL RANGES** next to Web Browser. This should be your second policy from the top.

If a user's network range is * ALL RANGES ⌵ ⓘ

and the user accessing content from * Web Browser ⌵ ⓘ

and user belongs to group(s) 🔍 Select Groups... ⓘ

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

and user is registering FIDO2 authenticator * No ⓘ

Then perform this action ⓘ

then the user may authenticate using * ⓘ ⊕

If the preceding method fails or is not applicable, then and ⓘ ⊕ ✕

Select authentication method...

Password (Local Directory)

✓ FIDO2

Certificate (cloud deployment)

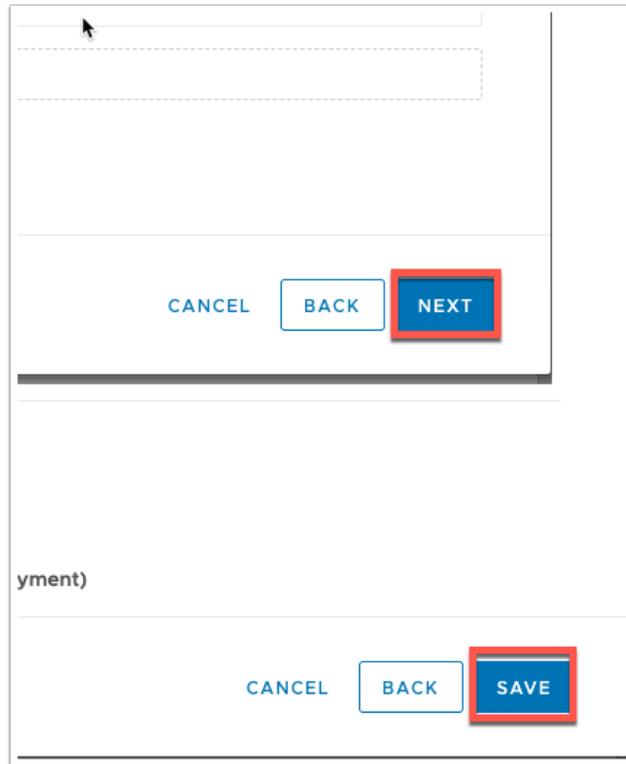
Password (cloud deployment)

Password

Auth0

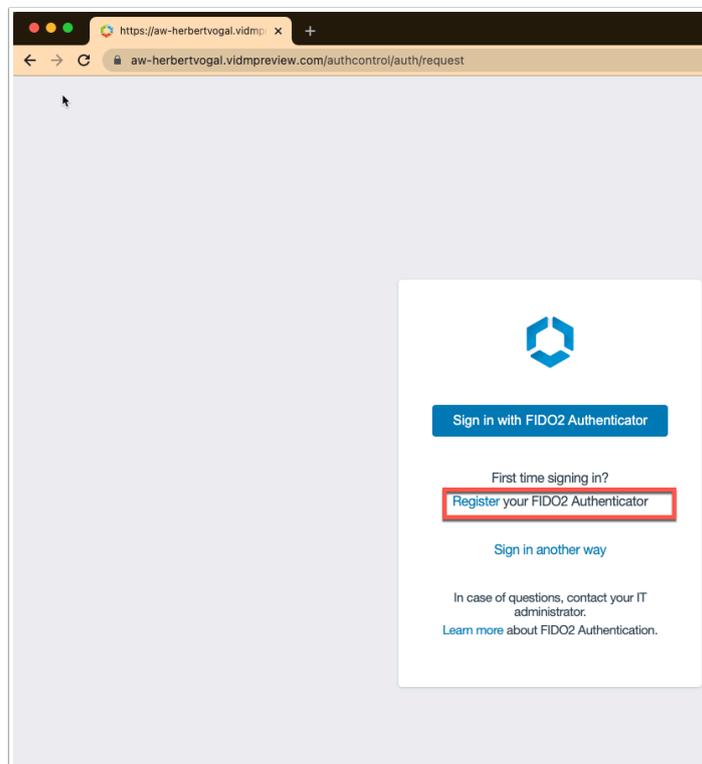
9. Change the first authentication method to **FIDO2**

- Click **Save** at the bottom of the page



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

Part 2: Register Authenticator



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)

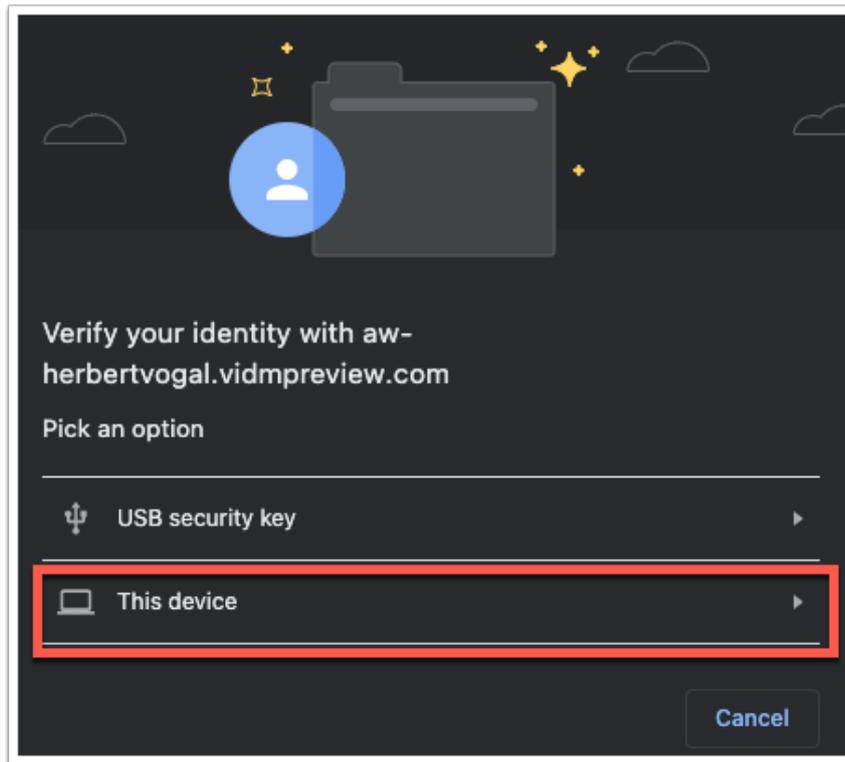
- You should now see Sign in with FIDO2 Authenticator.
- Click **Register** your **FIDO2** Authenticator

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)

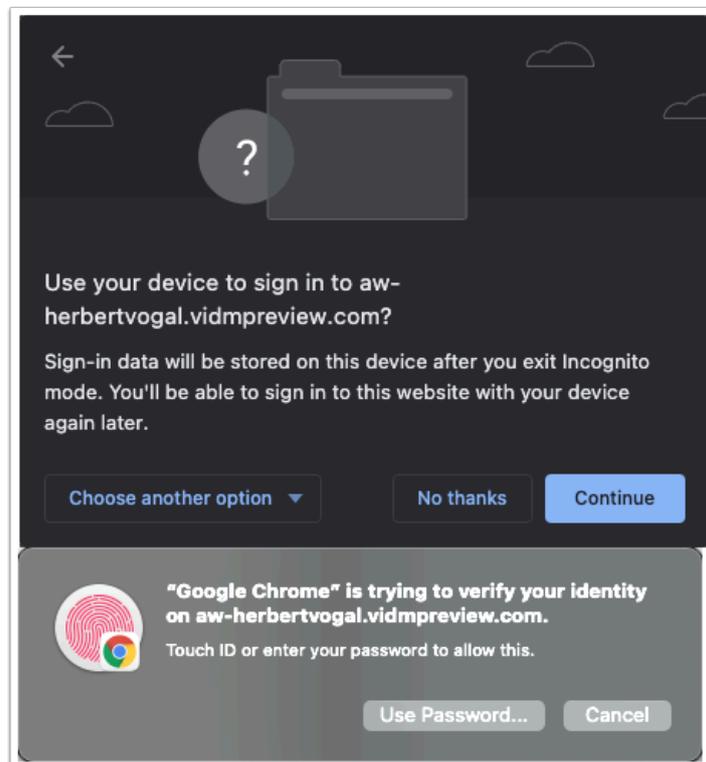
2. Note the authentication form factors on the various different browsers and operating systems. Make sure you are using one of these and not in a virtual lab environment.

The screenshot shows two parts of the Workspace ONE login interface. The top part is a 'Select Your Domain' dropdown menu with options: 'System Domain' (checked), 'euc-livefire.com' (highlighted with a red box), and 'Auth0'. Below the dropdown is a blue 'Next' button. The bottom part is a sign-in form with fields for 'username' (containing 'mark') and 'password' (masked with dots). Below the fields is the domain 'euc-livefire.com', a blue 'Sign in' button, a 'Forgot password?' link, and a 'Change to a different domain' link. The VMware logo is visible at the bottom of both sections.

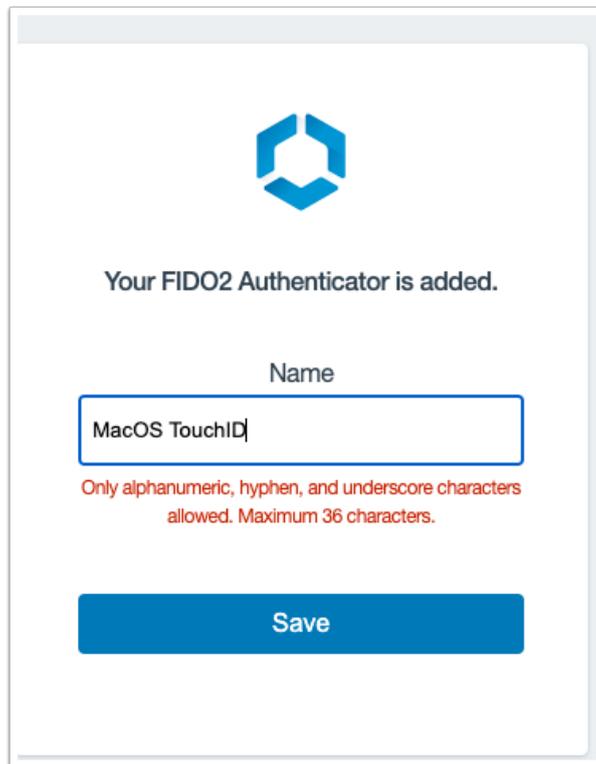
3. Select the euc-livefire.com domain and authenticate using the **Mark VMware1!** account. Click **Sign in**



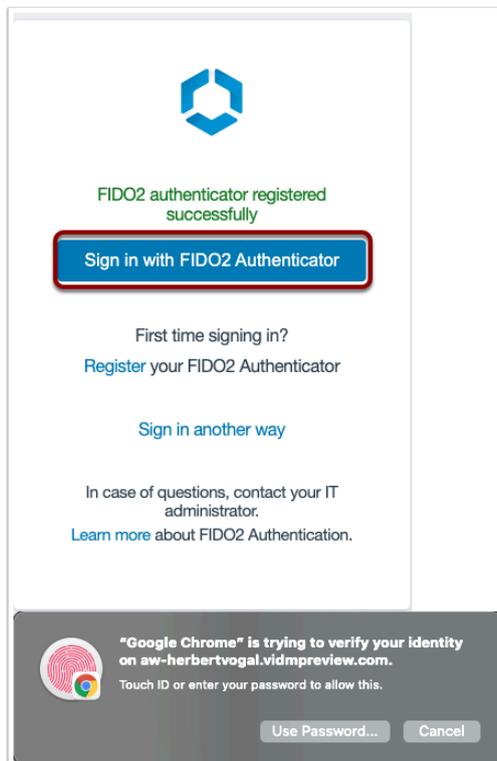
4. At this point the registration for **FIDO2** kicks in and you will be asked in by the browser to select how to verify your identity.
 - click **This device**



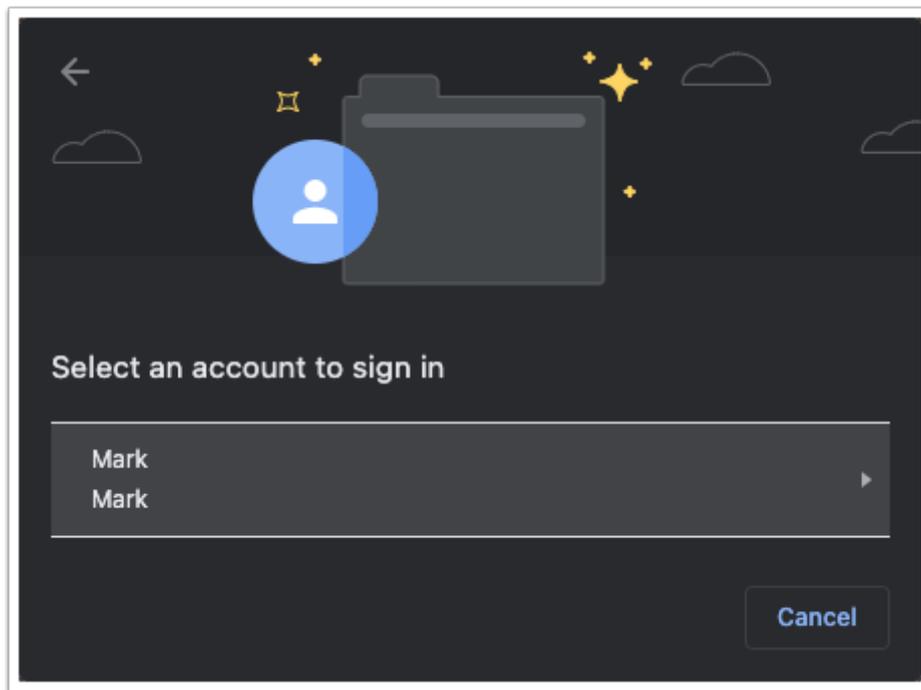
5. Click **Continue** on the next prompt
 - Then use you Password & Windows Hello or Touch ID



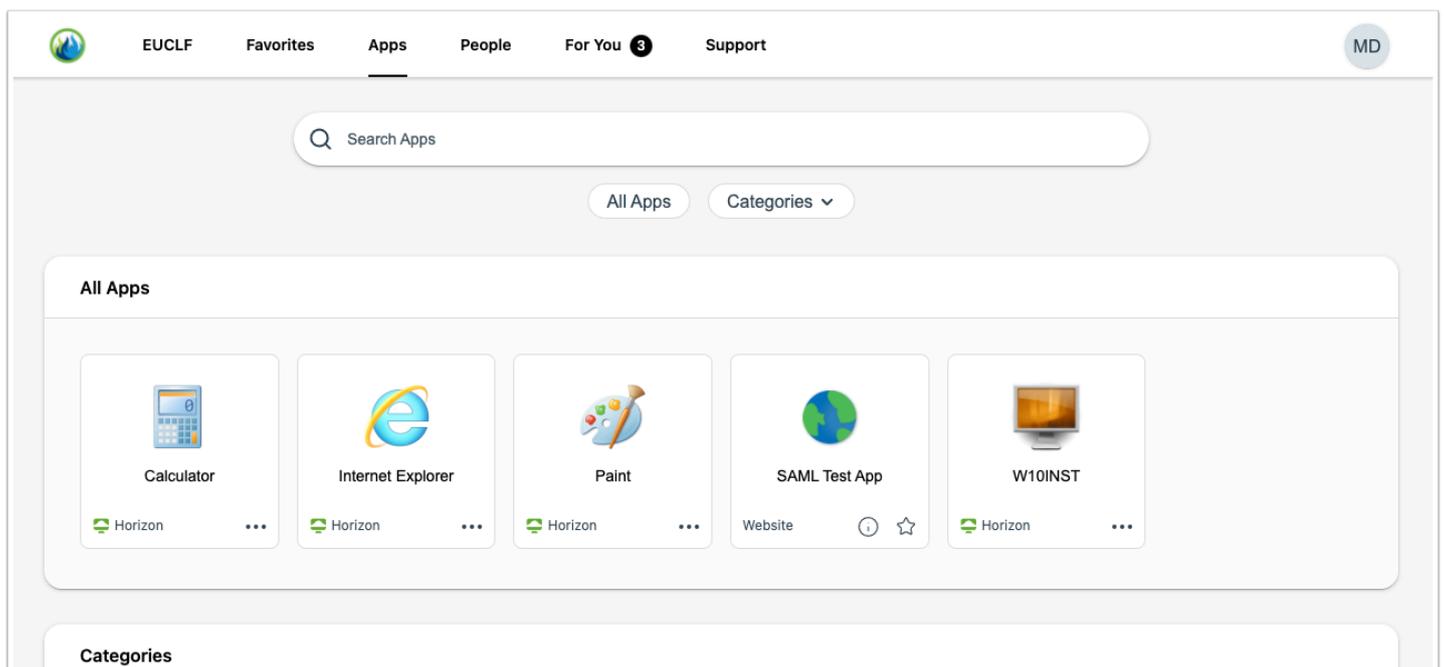
6. Give your authenticator method a name and click **Save**



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**

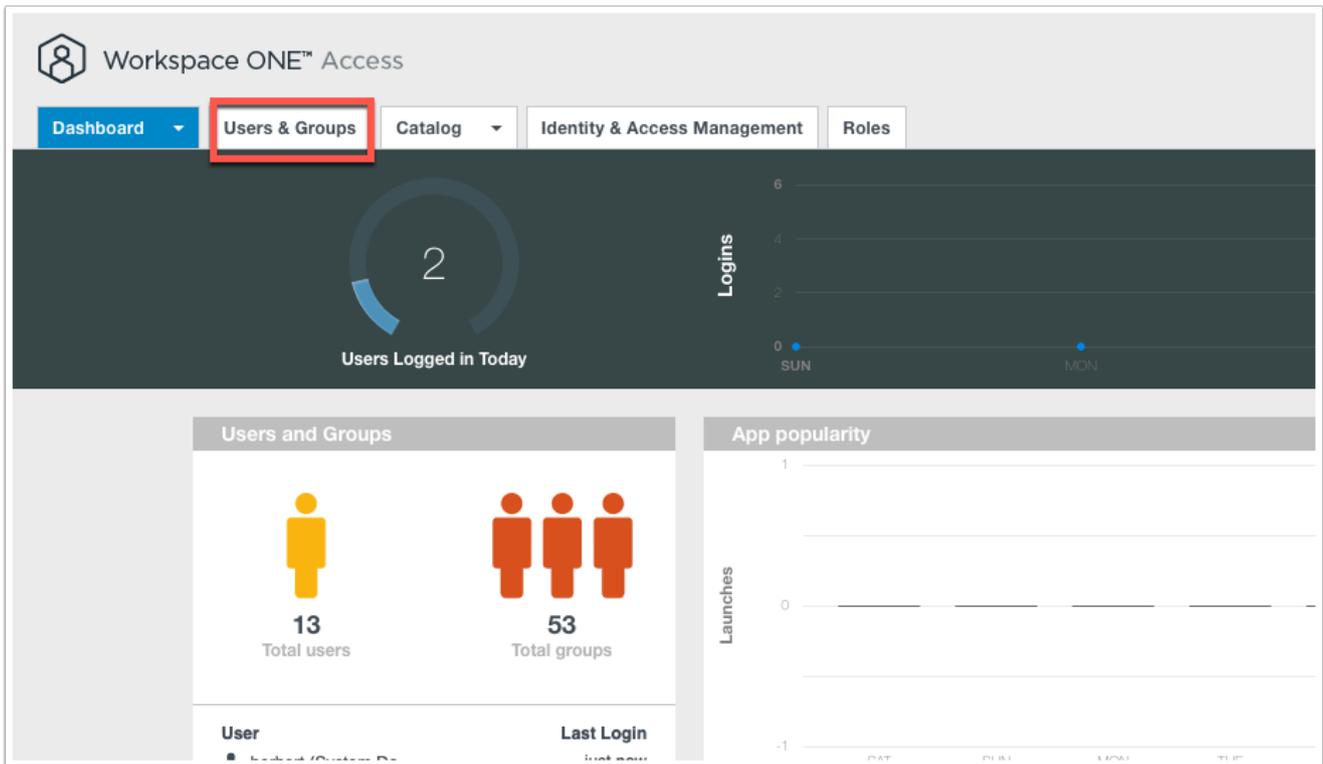


9. You should be authenticated with the user **Mark** to **Intelligent Hub**.

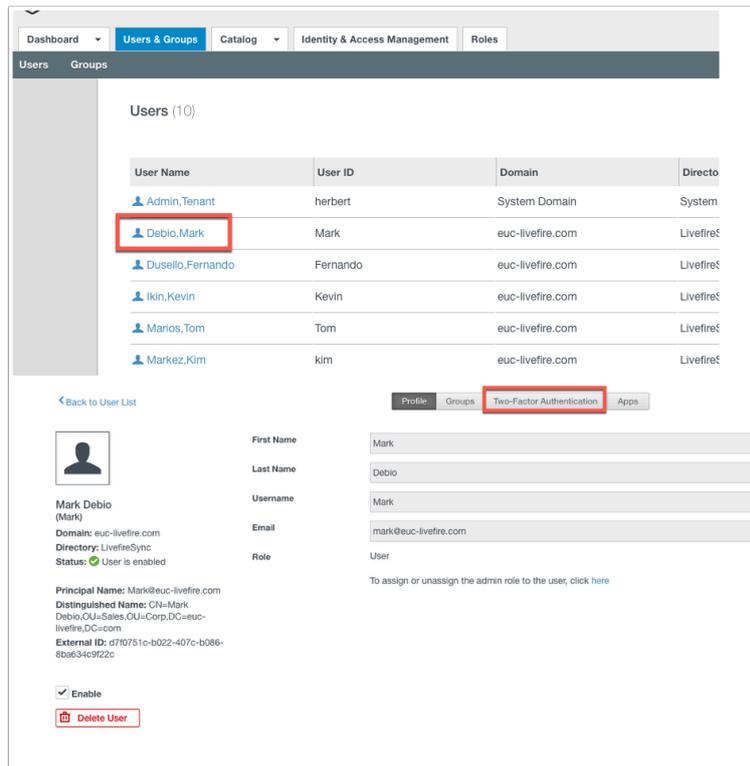
- Close the Chrome and re-open.
- Experience seamless FIDO2 authentication to Intelligent Hub.

Part 3: Administer FIDO2 Keys

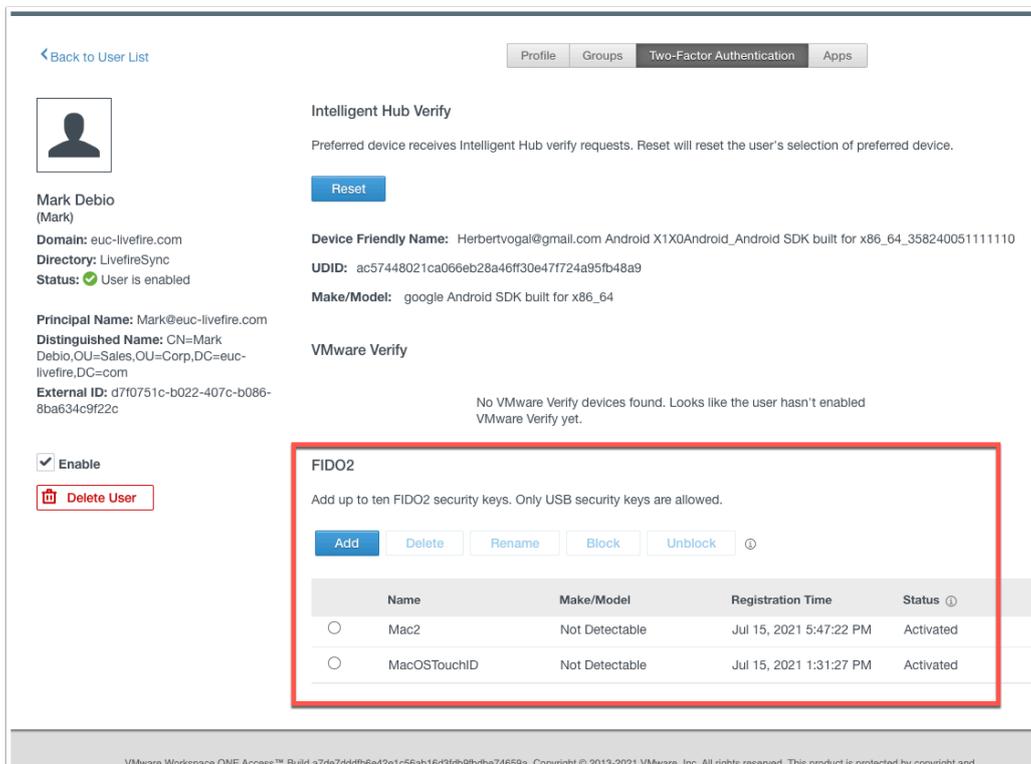
The WorkspaceONE Access admin console offers the ability to manage FIDO2 keys within the user attributes.



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**



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



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