

VMware Verify (Intelligent Hub)

In this lab we will setup MFA using VMware's own Intelligent hub. This authentication method does not require a phone number (GSM) to be registration, but rather will use the already deployed intelligent hub as "soft token" during the authentication process.

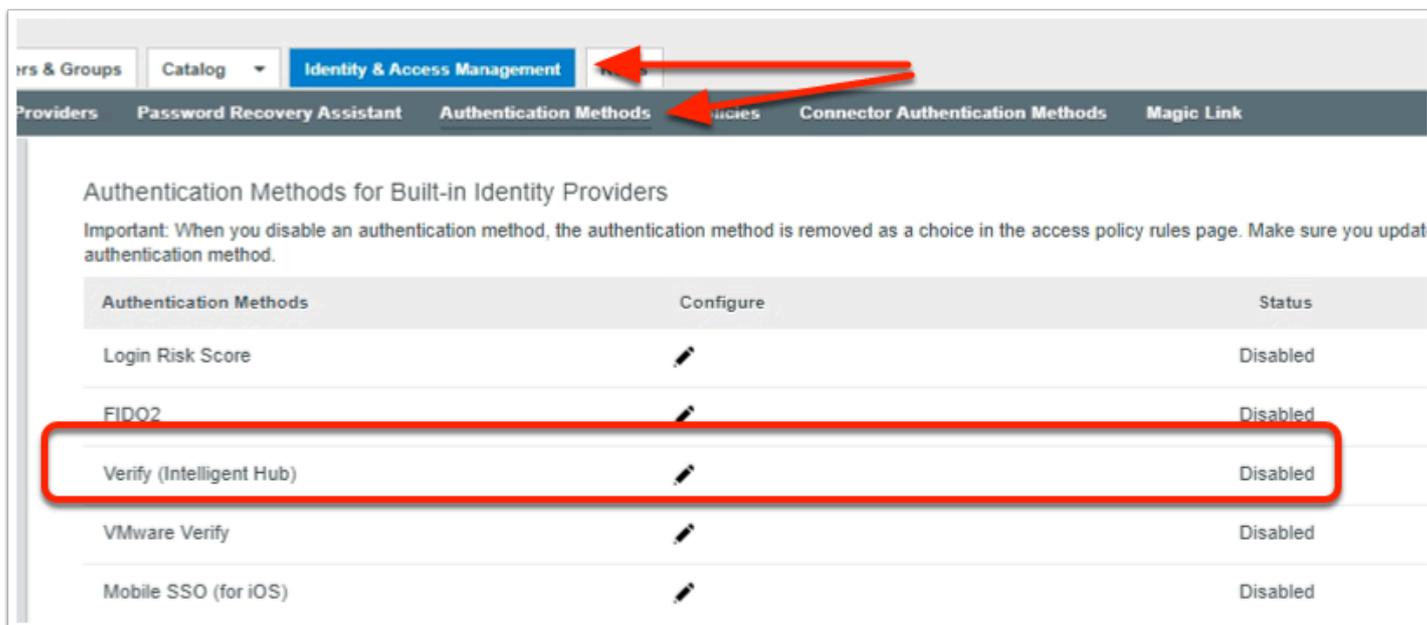
Prerequisites:

- Workspace ONE Access integrated with Workspace ONE UEM
- Hub Services activated with Notifications enabled.
- Workspace ONE Intelligent Hub app 20.05 or later installed on user devices.
- iOS or Android (physical or emulator) Device enrolled
- (Optional) Require device-level passcodes for managed devices and app-level passcode for registered devices.

NOTE: This authentication method is designed to be used in conjunction with another form of authentication, and should not be used as a stand alone authentication method.

NOTE: Please ensure you have a mobile device enrolled from the introduction labs from day 1. Currently VMware Verify (Intelligent Hub) is only supported on iOS & Android and does not support getting prompts on Windows devices.

Part 1: Configure Authentication method



1. On your **Workspace ONE Access** administrator console

- Login using your custom admin account.
- Select the **Identity & Access Management** tab
- To the right of the page select **Manage**
- Select **Authentication Methods**
- Next to **Verify (Intelligent Hub)** select the **pencil icon**

The screenshot shows the configuration page for 'Verify (Intelligent Hub)'. The 'Enable Verify (Intelligent Hub)' checkbox is checked. The 'MFA Action Timeout in Seconds' field is set to 60. The 'Enhanced Verification on Managed Devices' checkbox is checked. The 'Save' button is highlighted with a red box.

Verify (Intelligent Hub)

Enable Verify (Intelligent Hub)
This will enable Verify (Intelligent Hub)

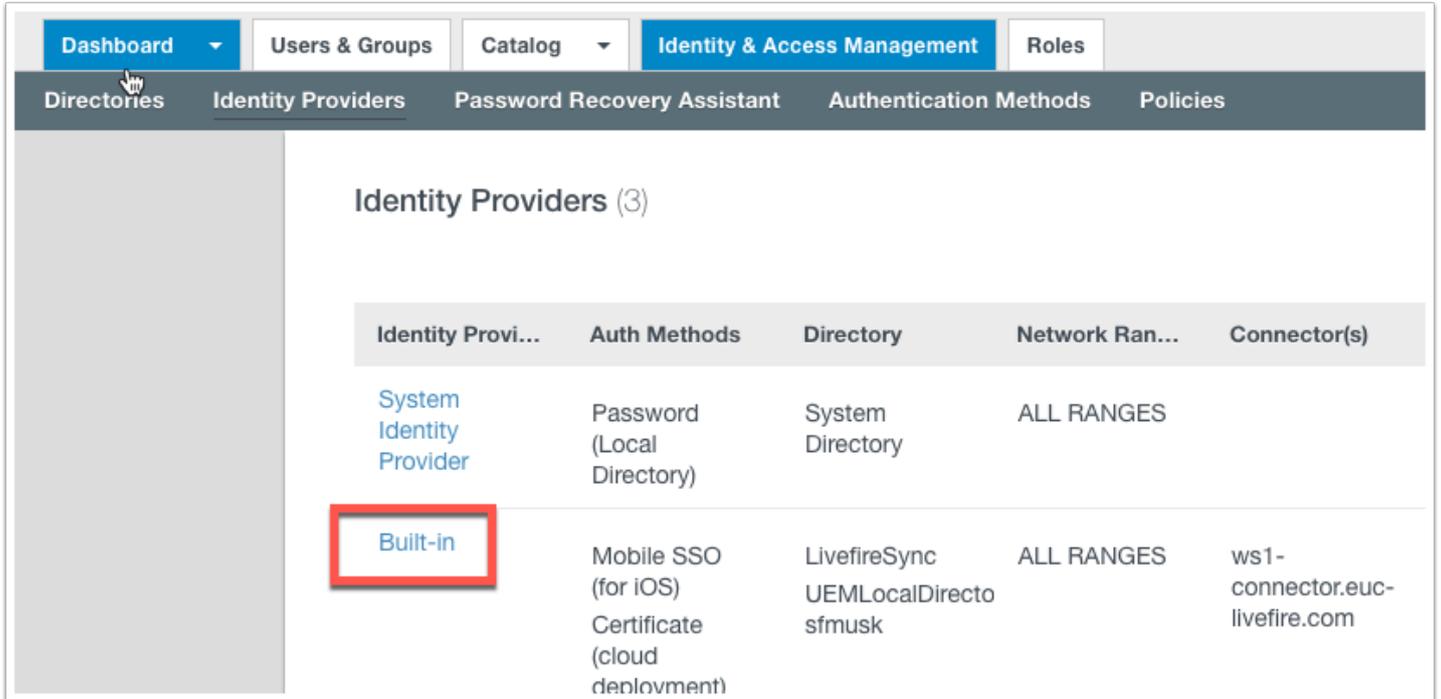
MFA Action Timeout in Seconds*
Enter the number of seconds after which the MFA request expires. This value can be between 30 and 90 seconds.

Enhanced Verification on Managed Devices
Users authenticating from Workspace ONE UEM managed devices will be prompted for biometric or passcode verification on approval.

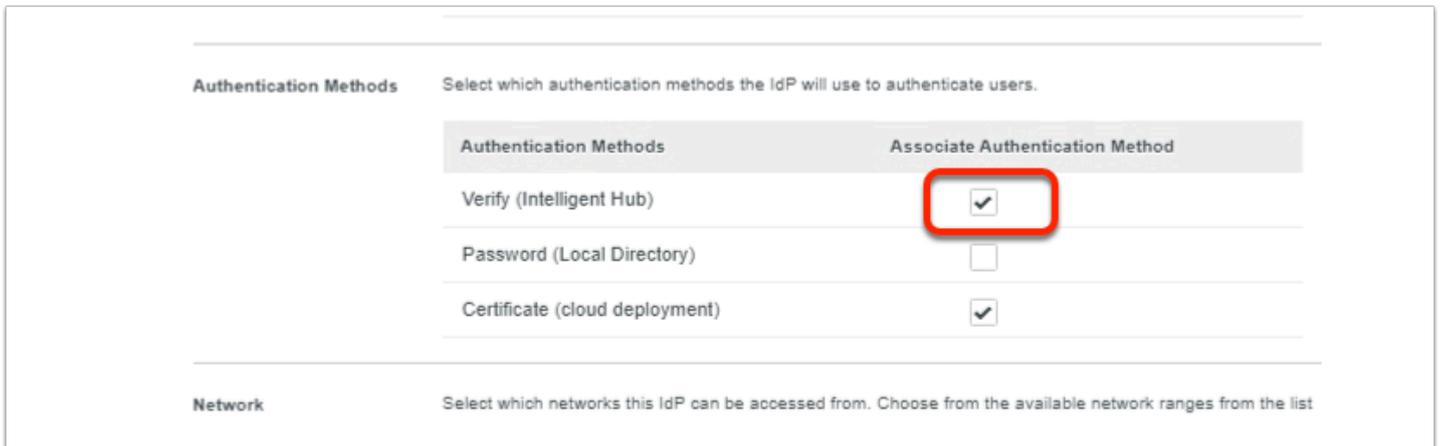
Enhanced Verification on Registered Devices
Users authenticating from Workspace ONE UEM registered devices will be prompted for biometric or passcode verification on approval.

Enhanced Verification on Requests from Mobile Devices
Requests initiating from a mobile device require biometric or passcode verification. You do not need to enable this if you've enabled enhanced verification on Managed and Registered devices.

2. On the pop-up **Verify (Intelligent Hub)** window
 - Select **the box** next to **Enable Verify (Intelligent Hub)**
 - Select **the box** next to **Enhanced Verification on Managed Devices**
 - Select **Save** at the bottom right

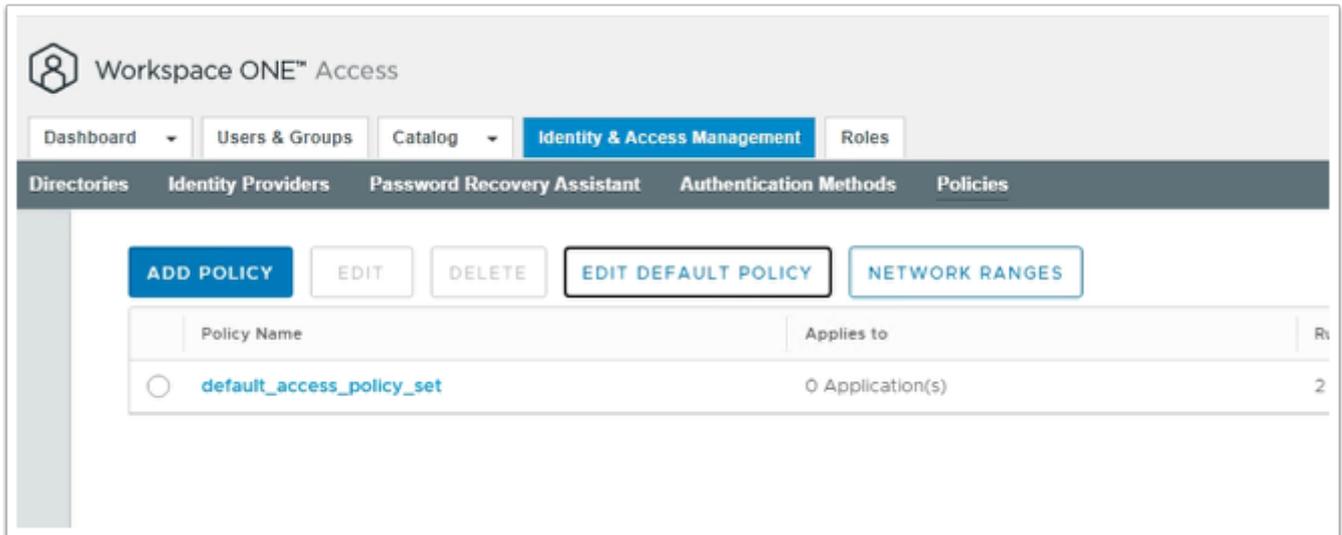


3. In Workspace ONE Access console
 - Navigate to **Identity Providers**
 - Select the **Built-in** Identity provider.

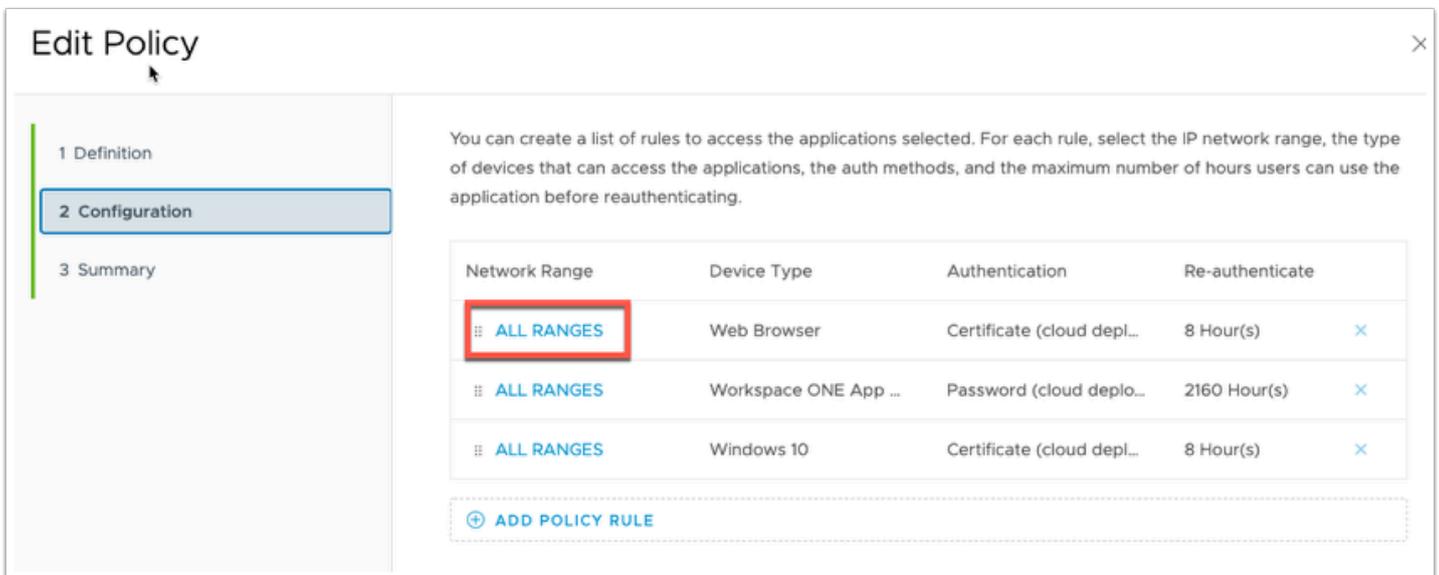


4. In the **Built-in** Identity provider window
 - Scroll down until the **Authentication methods** area
 - Select **the box** next to **Verify (Intelligent Hub)**
 - Select **Save** at the bottom of the page.

Part 2: Configure Access Policy



1. In the **Workspace ONE Access** admin console
 - Navigate to **Identity & Access Management**.
 - Select **Manage**
 - On the left hand side and click on **Policies**
 - Click **EDIT DEFAULT POLICY** on the **Policies** page.



2. In the **Edit Policy** window
 - In the left hand navigation, select **Configuration**
 - Select **ALL RANGES** next to **Device Type > Web Browser**.

URATION Edit Policy Rule

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.

Then perform this action Authenticate using... ⓘ

then the user may authenticate using * Certificate (cloud deployment) ⓘ +

If the preceding method fails or is not applicable, then Password (cloud deployment) ⓘ +

If the preceding method fails or is not applicable, then Password (Local Directory) ⓘ + ×

+ ADD FALLBACK METHOD

3. In the **Edit Policy Rule** page click the **+** next to the first form of authentication.

This could be **Certificate (cloud deployment)** or it could be **Password (cloud deployment)**.
 This could depend on previous labs or use-cases. The important concept is that we are using the "and" function in authentication rather than "or".

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 Authenticate using... ⓘ

then the user may authenticate using * Certificate (cloud deployment) ⓘ +

and

If the preceding method fails or is not applicable, then Password (cloud deployment) ⓘ +

- ✓ Select authentication method...
- Password (Local Directory)
- Password (cloud deployment)
- Certificate (cloud deployment)
- Verify (Intelligent Hub)
- Password

CANCEL SAVE

The screenshot displays two alternative authentication configurations, each starting with "OR".

Configuration 1:

- then the user may authenticate using * Certificate (cloud deployment)
- and Verify (Intelligent Hub)
- If the preceding method fails or is not applicable, then Password (cloud deployment)
- If the preceding method fails or is not applicable, then Password (Local Directory)

Configuration 2:

- then the user may authenticate using * Password (cloud deployment)
- and Verify (Intelligent Hub)
- If the preceding method fails or is not applicable, then Password (Local Directory)

Buttons: CANCEL, SAVE (highlighted in red boxes).

4. You should now get a new authentication method drop down next to "and"

a. Select **Verify (Intelligent Hub)**

b. Once you have confirmed that you either have Certificate (cloud deployment) and Verify (Intelligent Hub) or you have Password (cloud deployment) and Verify (Intelligent Hub) you can click **SAVE** at the bottom right

NOTE: Ensure you have password (local directory) still as the fallback authentication method to ensure you can get back in to the administrator console.

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

CANCEL BACK NEXT

5. Click **NEXT** on the **Edit Policy** page

Edit Policy ✕

1 Definition

2 Configuration

3 Summary

Definition

Name
default_access_policy_set

Description
Default access policy set

Applications
4 Application(s)

Configuration

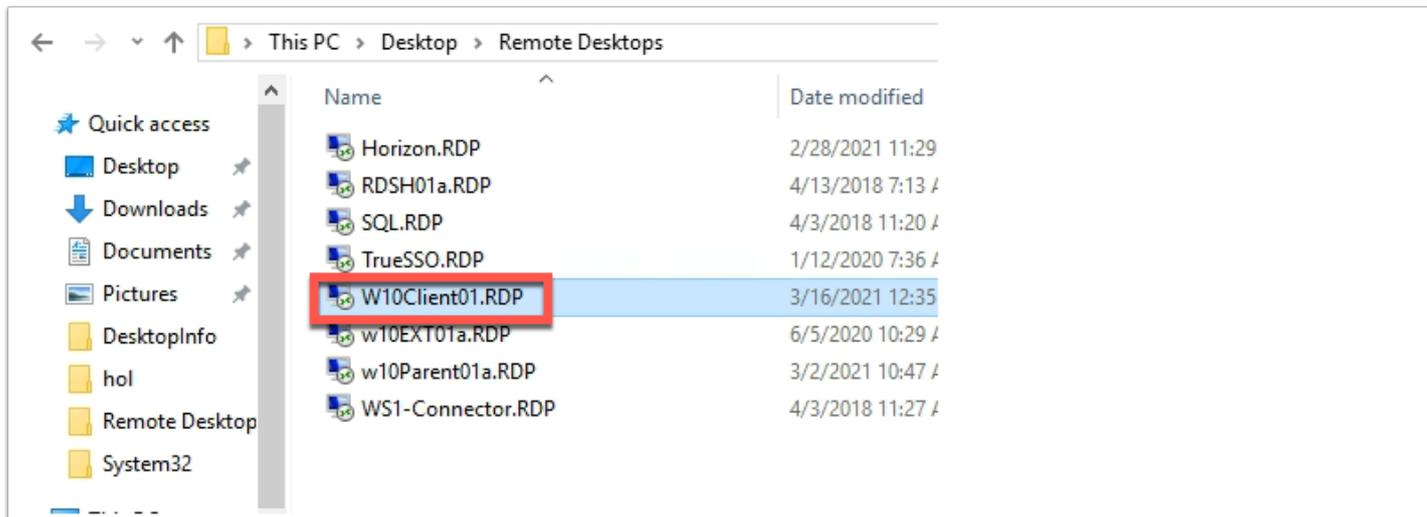
Policy Rule 1

If a user's network range is **ALL RANGES**
and the user is accessing content from **Web Browser**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **Certificate (cloud deployment) & Verify (Intelligent Hub)**

CANCEL BACK SAVE

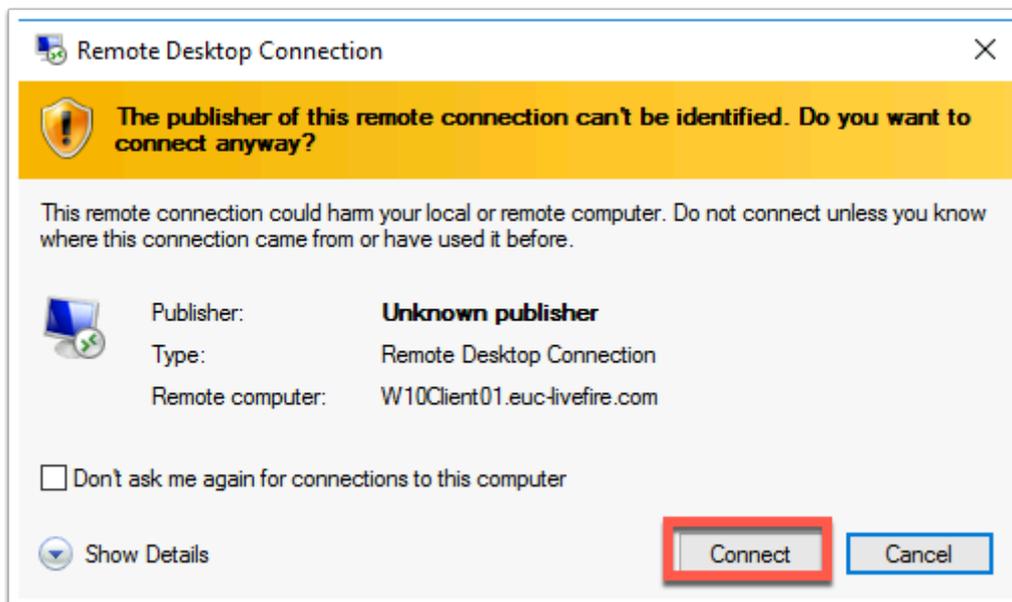
6. Click **SAVE** on the **Summary** page

Part 3: Test Verify (Intelligent Hub) Implementation

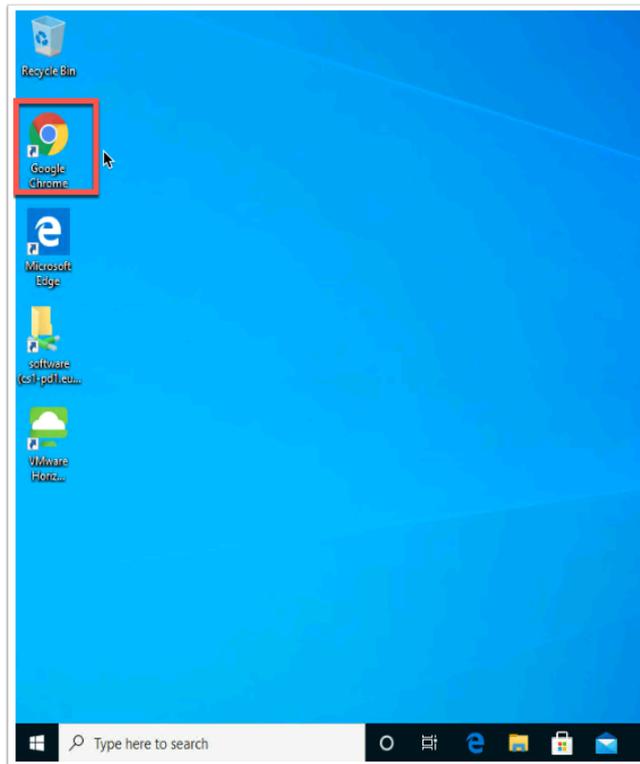


1. Navigate to your on-premise lab environment and click into the **Remote Desktops** folder on the **Desktop** of the **ControlCenter** virtual machine.

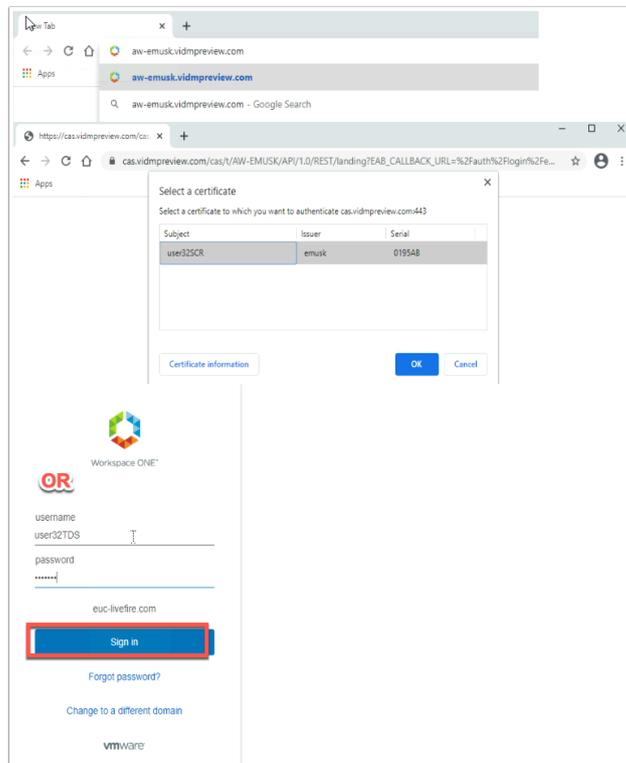
a. **Double Click** the **W10Client01.RDP** to connect to the Windows 10 Client.



2. Click **Connect** when the **Remote Desktop Connection** windows pops up.



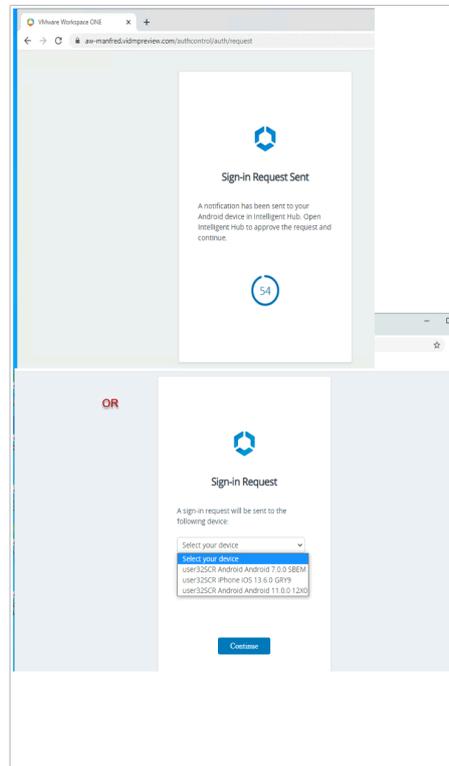
3. On the Desktop of the **W10Client01** click **Google Chrome** on the desktop



4. Type in the **Workspace ONE Access URL** for your tenant and click enter

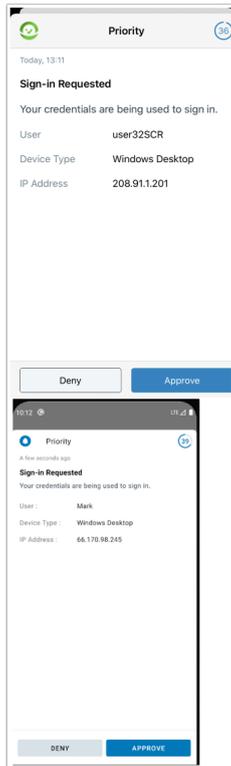
a. if you have configured **Certificate (cloud deployment)** as your first authentication method you will be prompted to select a certificate click **OK**. (If you did the extra material on the previous lab you will not be prompted.)

b. **OR** If you have configured Password (cloud deployment) as your first authentication method select your domain and enter username and password.



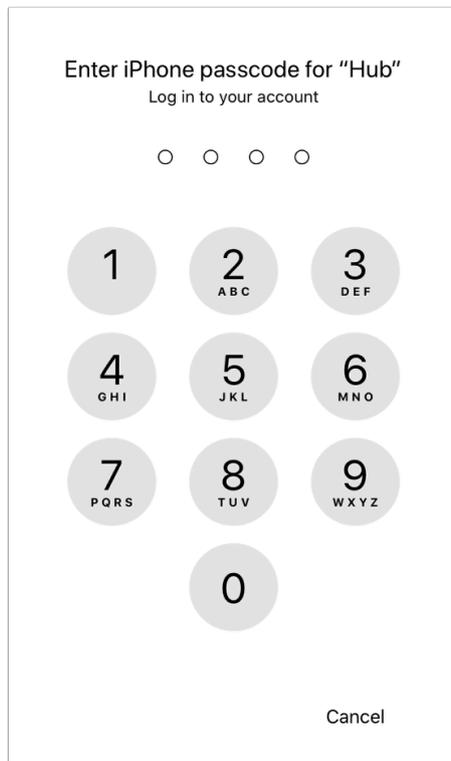
5. If you have multiple devices configured for this user you will be asked to select your device. Confirm the device and click **Continue**.

NOTE: If you only have a single device configured you will not be prompted to select a device. This device becomes the default/preferred device and will be remember for future authentication requests. (See part 5 to reset)

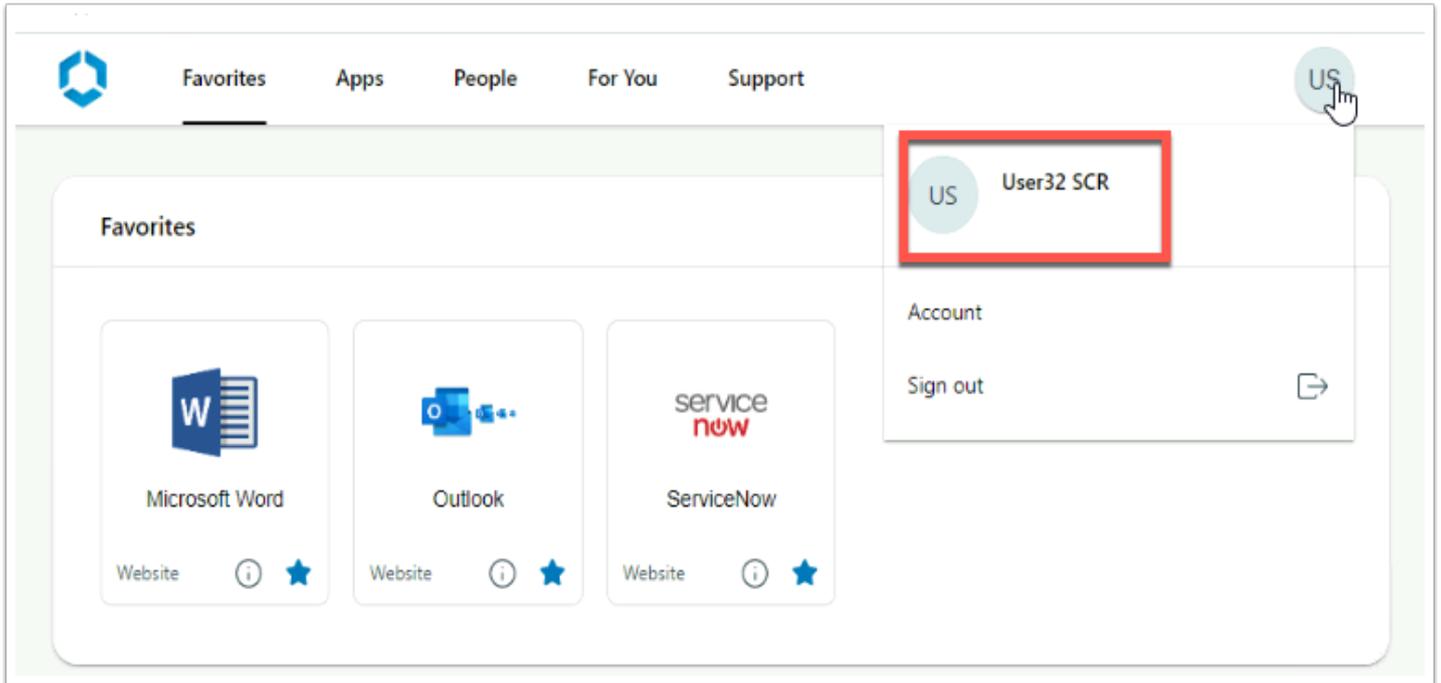


6. The browser will now give you **60 seconds** to respond to the request on your mobile device. If notification are enabled from the Intelligent Hub you will see the notification on the lock screen, otherwise navigate to the **Intelligent Hub** and click **Approve** on the **Sign-in Request**.

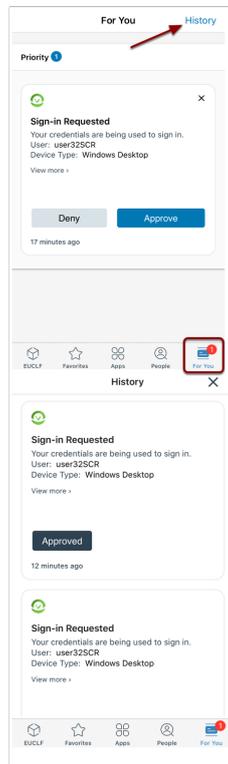
Note: The screen shots are for both iOS and Android above depending on which platform you are using.



7. You will then be prompted for the device passcode (or Touch-ID/Face-ID) used to unlock the device if you have one.

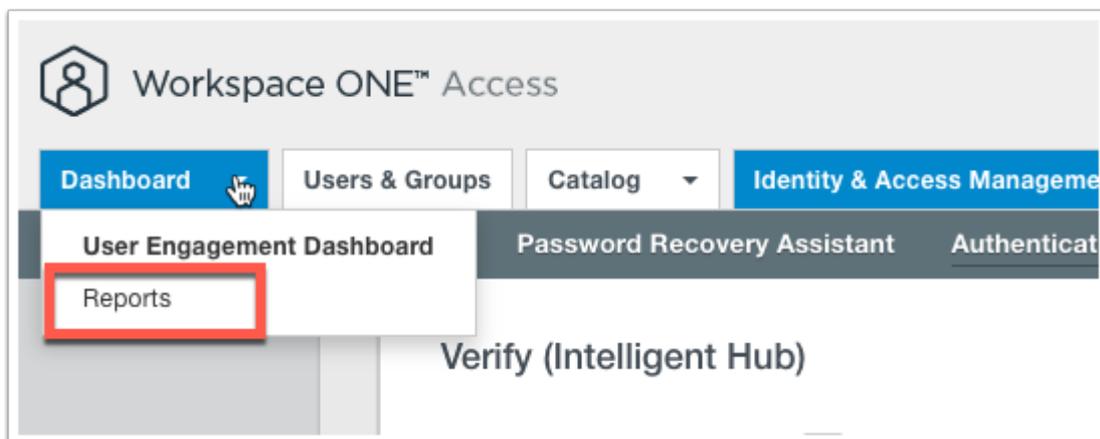


8. Once approved, you will be authenticated in the web browser to your Intelligent hub.



9. In the Intelligent Hub on the mobile device click on **For You**. Here you can view the current Notifications. Then click in the top right corner on **History**. Here you will see the Authentication requests that have been made.

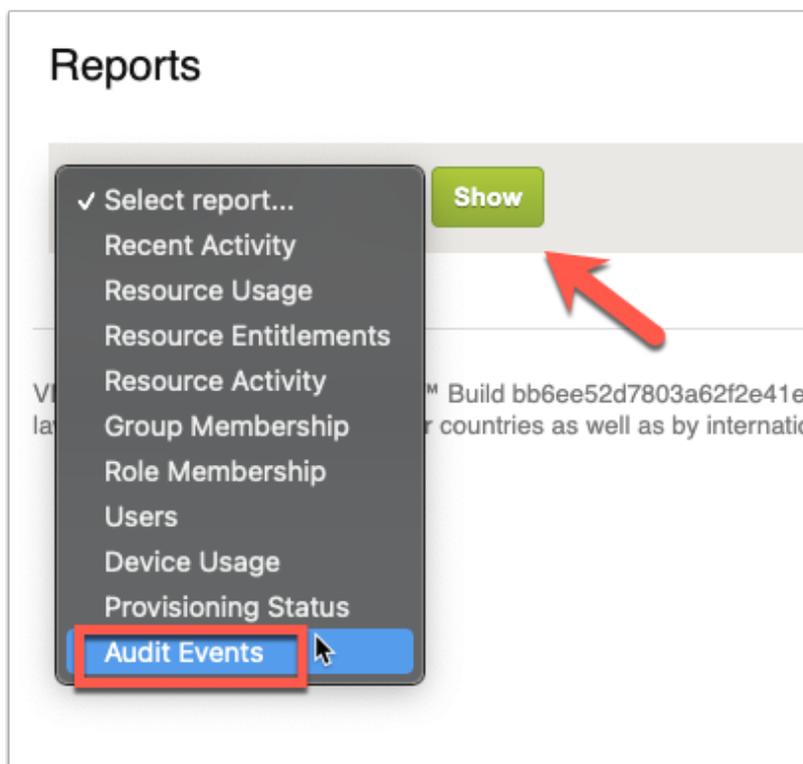
Part 4: Troubleshooting / Reporting



Troubleshooting / Reporting step:

Let's have a look what events are created as a result of the authentication.

1. Navigate back to the **Workspace ONE Access** administration console and click on the **down arrow** next to Dashboard and select **Reports**.



2. Click on **Audit Events** from the Reports drop down and **Show**

DATE, TIME (UTC+03:00)	USER (DOMAIN NAME)	EVENT	OBJECT	
Jan 21, 2021 1:33:24 PM	user32SCR (euc-livewire.com)	LOGIN (Certificate (cloud deployment), Verify (Intelligent Hub))	f8ef9d1d-64b1-4ccd-8399-1b318c0389cb	View Details

3. Click **View Details** on the the most current event labeled **LOGIN (Certificate (cloud deployment), Verify (Intelligent Hub))**

```

View audit events detail
{
  "deviceId": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36",
  "workspaceId": "EFFA05C70C7B5648A453CC63E1A15757",
  "sourceIp": "208.91.1.201",
  "objectType": "LOGIN",
  "objectId": "f8ef9d1d-64b1-4ccd-8399-1b318c0389cb",
  "objectName": null,
  "values": {
    "isForceAuth": "false",
    "tokenId": "f9b72d0a-4f71-4896-ad6e-e6661531bdbd",
    "successAuthMethods": "identityProvider.embedded.authMethod.certificate,identityProvider.embedded.authMethod.hubmfa",
    "success": "true",
    "authMethods": "identityProvider.embedded.authMethod.certificate,identityProvider.embedded.authMethod.hubmfa",
    "actorExternalId": "20885284-bf5c-4bbe-9730-34c9e55d4196"
  }
}

```

4. In the details view of the event, you should see that the **Authentication Method** is hubmfa and that **"success" : "true"**.

Part 5: Reset preferred device

What's New in the April 2021 Release

Verify (Intelligent Hub) New Features

- **Geolocation in Hub Notification is included in Verify (Intelligent Hub).** There is now geolocation information within Verify (Intelligent Hub) push MFA notifications. this will allow end users to see the geolocation of the device that is making the MFA request.
- **Ability to reset user device selection for Verify (Intelligent Hub) - Administrator Flow.** Workspace ONE Access now has the ability for administrators to unlink a device that end users configured with Verify (Intelligent Hub) within the Workspace ONE Access console. After unlinking the device, the next time that an end user logs in, they will go through the initial Verify (Intelligent Hub) flow and re-select the device that they wish to link with Verify (Intelligent Hub). This allows administrators to service users that do not have access to the device that is linked to Verify (Intelligent Hub).

In a previous version of this lab you would have used an API string to reset the preferred device setting for the Verify (Intelligent Hub) as of April 2021, Access now has a GUI based reset action for administrator to reset end-users prior selected device for MFA.

The screenshot shows the Workspace ONE Access admin console. The top navigation bar includes 'Dashboard', 'Users & Groups' (highlighted with a red box), 'Catalog', 'Identity & Access Management', and 'Roles'. A search bar is present on the right. Below the navigation, the 'Users' tab is selected, and a table of users is displayed. The user 'Debio, Mark' is highlighted with a red box.

User Name	User ID	Domain	Directory	VMware Verify Phone Nu...	Groups	Status
Admin, Tenant	manfred	System Domain	System Directory	N/A	ALL USERS	Enabled
Debio, Mark	Mark	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Marketing@...	Enabled
Dusello, Fernando	Fernando	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Marketing@...	Enabled
empowerlisbon, Empo...	empowerlisbon@gmail.c...	Auth0	Auth0-Directory	N/A	ALL USERS	Enabled
Ikin, Kevin	Kevin	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Domain Us...	Enabled
manfred, manfred@eu...	manfred@euc-livefire.com	Auth0	Auth0-Directory	N/A	ALL USERS	Enabled
Marios, Tom	Tom	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Marketing@...	Enabled
mark, mark@euc-livefir...	mark@euc-livefire.com	Auth0	Auth0-Directory	N/A	ALL USERS	Enabled

1. In the WorkspaceONE Access admin console navigate to **Users & Groups**
 - In the **Users** tab click on the user **Debio, Mark**

[Back to User List](#)

Profile Groups **Two-Factor Authentication** Apps



Mark Debio
(Mark)
Domain: euc-liveware.com
Directory: LivefireSNC
Status: ✔ User is enabled

Principal Name: Mark@euc-liveware.com
Distinguished Name: CN=Mark
Debno,OU=Marketing,OU=Corp,DC=euc-liveware,DC=com
External ID: d7f0751c-b022-407c-b086-8ba634c9f22c

First Name: Mark
Last Name: Debno
Username: Mark
Email: mark@euc-liveware.com
Role: User

To assign or unassign the admin role to the user, click [here](#)

2. In the user view click on **Two-Factor Authentication**

[Back to User List](#)

Profile Groups **Two-Factor Authentication** Apps



Mark Debio
(Mark)
Domain: euc-liveware.com
Directory: LivefireSNC
Status: ✔ User is enabled

Principal Name: Mark@euc-liveware.com
Distinguished Name: CN=Mark
Debno,OU=Marketing,OU=Corp,DC=euc-liveware,DC=com
External ID: d7f0751c-b022-407c-b086-3ba634c9f22c

Enable Delete User

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

Reset 

Device Friendly Name: Mark Android Android 10.0.0 X3X0
UDID: b304064d9a9c078bc47413095a28a2548bac23061b
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.

3. You will now find the option under the title **Intelligent Hub Verify** to Reset. **Don't click** on Reset for this lab as we will continue to use this device as the preferred device for Hub MFA.

This concludes the VMware Verify - Intelligent Hub lab.

Authored by: Simeon Frank