

# 1. Setting up Workspace ONE

In this lab you (as the admin) will be setting up the platform for the digital workspace. We will integrate Workspace ONE UEM with Workspace ONE Access, Hub Services and Workspace ONE intelligence.

You will install the Access connector and configure Active Directory integration to sync users.

Part 1: Access, UEM and Intelligence setup

Part 2: Enable Experience Management

Part 3: Workspace ONE Access

Part 4: Installing and configuring the Workspace ONE Access Connector

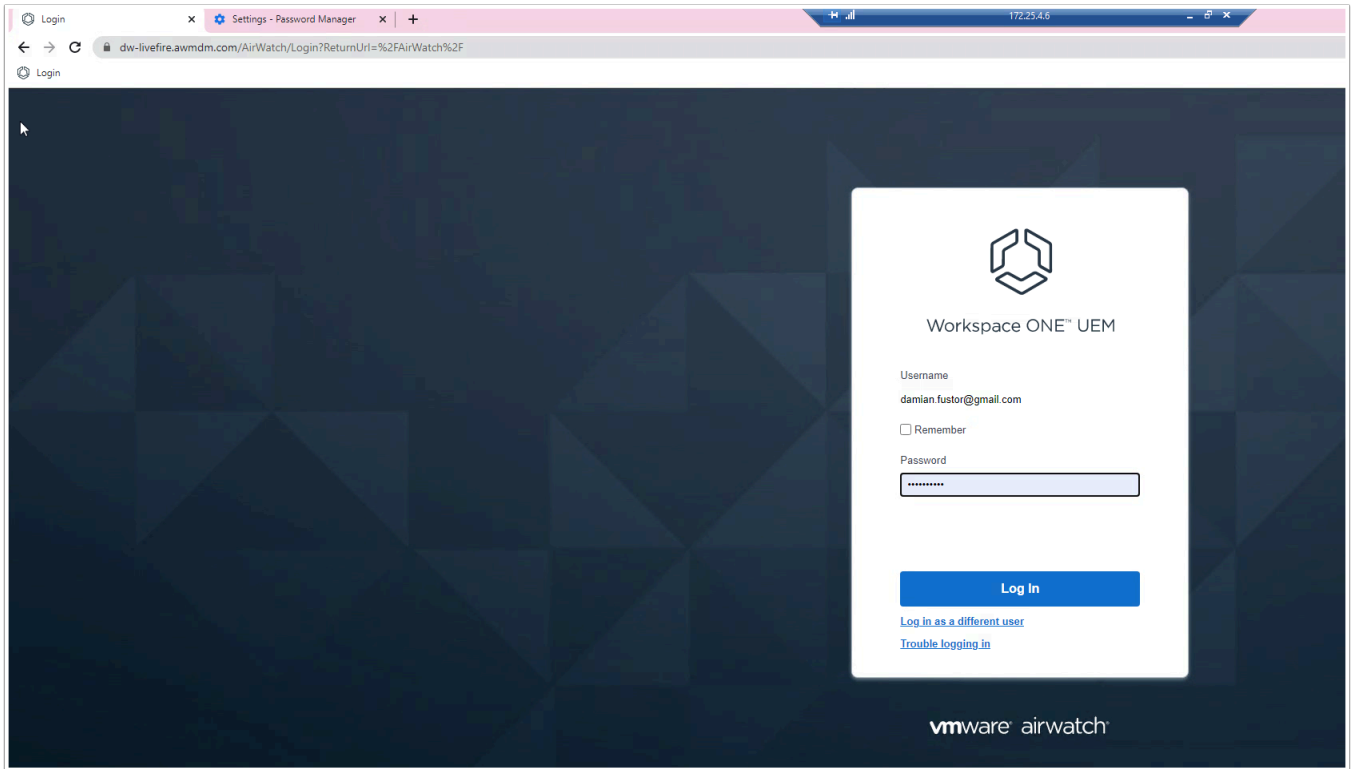
Part 5: Configure Directory Sync with Workspace ONE Access Connector

Part 6: Workspace ONE Hub Services Integration with Workspace ONE Access

Part 7: Configuring Workspace ONE Hub Services

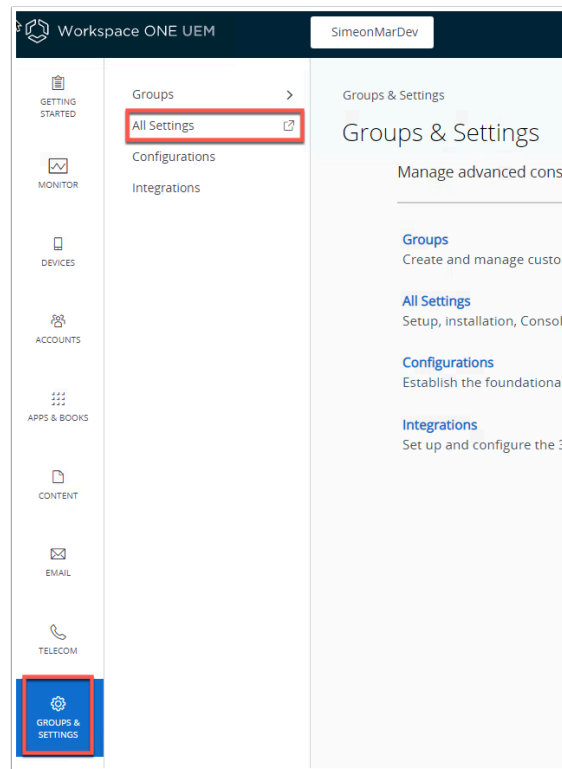
Part 8: User Provisioning to UEM

## Part 1: Access, UEM and Intelligence setup

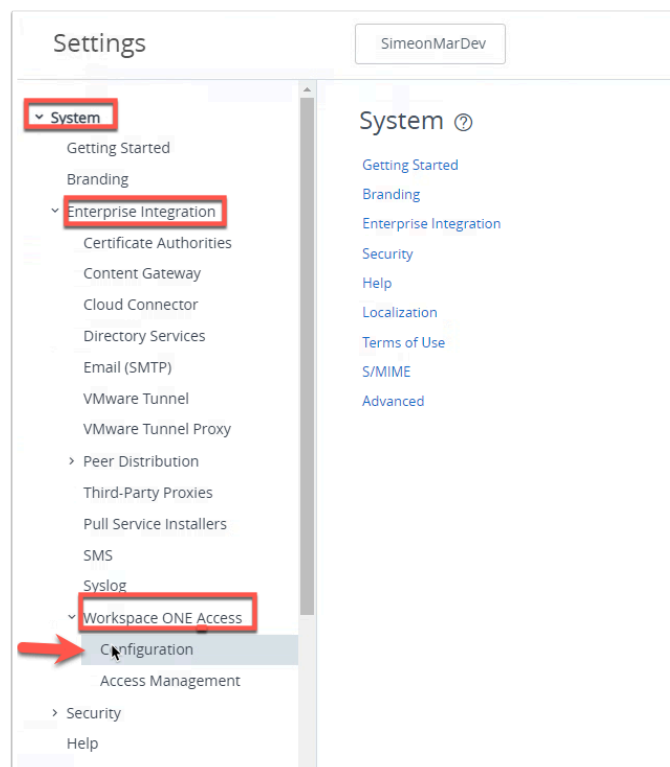


1. On the **Control Center** open Chrome and navigate to the **UEM admin** console sign in.
  - Browser to <https://dw-livefire.awmdm.com>
  - Sign in with your credentials (your **E-mail** + **VMware1!**)

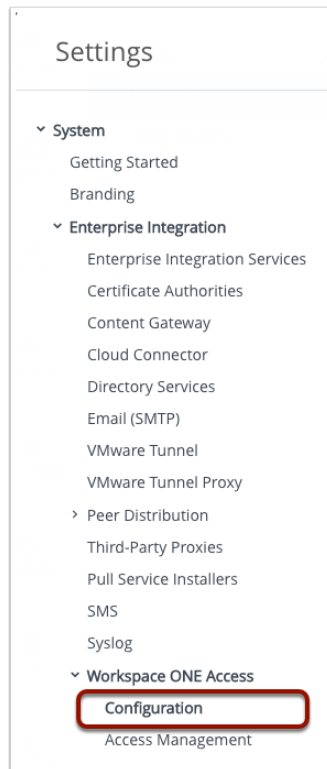
**NOTE:** If this is your first time signing in you will have to set a security question and a PIN.



2. In the UEM console navigate to **GROUPS & SETTINGS** > **All Settings**

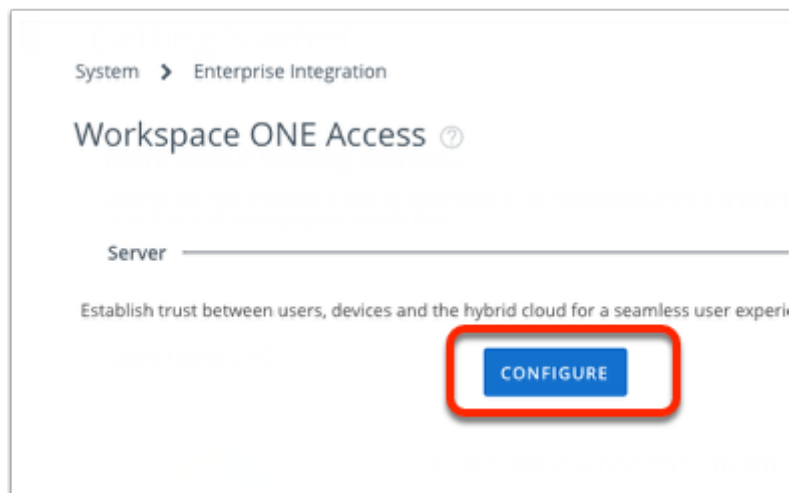


3. In the Settings page navigate to **System** > **Enterprise Integration** > **Workspace ONE Access** > **Configuration**



4. In your **Workspace ONE UEM Admin** console

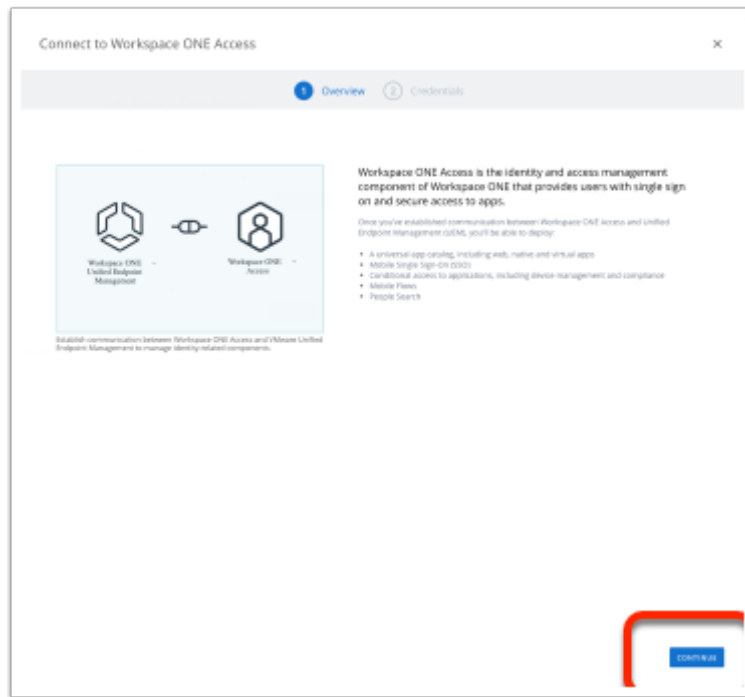
- Navigate to **Groups and Settings > All Settings > System > Enterprise Integration > Workspace ONE Access > Configuration**



5. Under the **Server** area,

- Select **CONFIGURE**





6. On the **Connect to Workspace ONE Access** window,
  - Select **CONTINUE**

Connect to Workspace ONE Access

1 Overview 2 Credentials

This will help you establish the connection between VMware Unified Endpoint Manager and Workspace ONE Access.

Tenant URL \*

Username \*

Password \*

If you have forgotten your password, you can recover it on the Workspace ONE / password link has expired, please contact Workspace ONE UEM support.

Test to confirm Workspace ONE UEM and Workspace ONE Access are communicating securely.

TEST CONNECTION

Test to confirm Workspace ONE UEM and Workspace ONE Access are communicating securely.

TEST CONNECTION

**Test connection successful!**

BACK SAVE

7. On the **Connect to Workspace ONE Access** window enter the following:
  - **Tenant URL:** **Your Tenant** (for example: <https://aw-livefirehorizonrn.vidmpreview.com/>)

**NOTE:** You should have received an e-mail from **no-reply@livefire.solutions** with this URL. Check your SPAM folder if you don't see it.

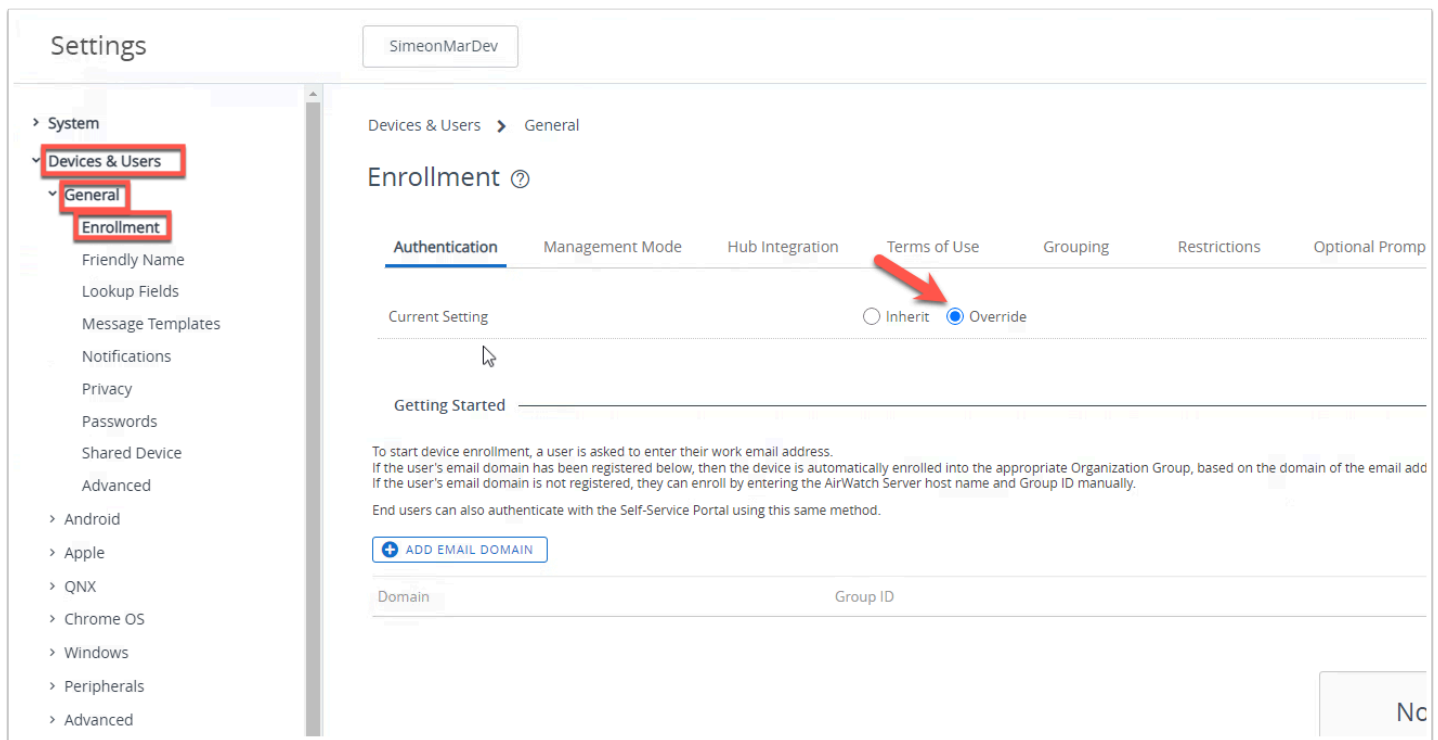
- **User Name:** Your Tenant Admin account
- **Password:** Your Tenant Password
- Select **TEST CONNECTION** to ensure Tenant configuration has been entered successfully.
- Select **SAVE** and close the settings window

The screenshot shows the 'Server' configuration section of the Workspace ONE UEM console. It includes fields for 'URL' (https://aw-simeonfebdvivefire.vidmpreview.com) and 'Admin Username' (administrator). There are toggle switches for 'Active Directory Basic' (set to DISABLED) and 'Basic User Sync' (with an 'ENABLE' button). A blue button labeled 'USE AUTOGENERATED API KEY' is present. Below this is the 'Certificate' section, which has an 'ENABLE' button highlighted with a red box. A 'DELETE' button is at the bottom right.

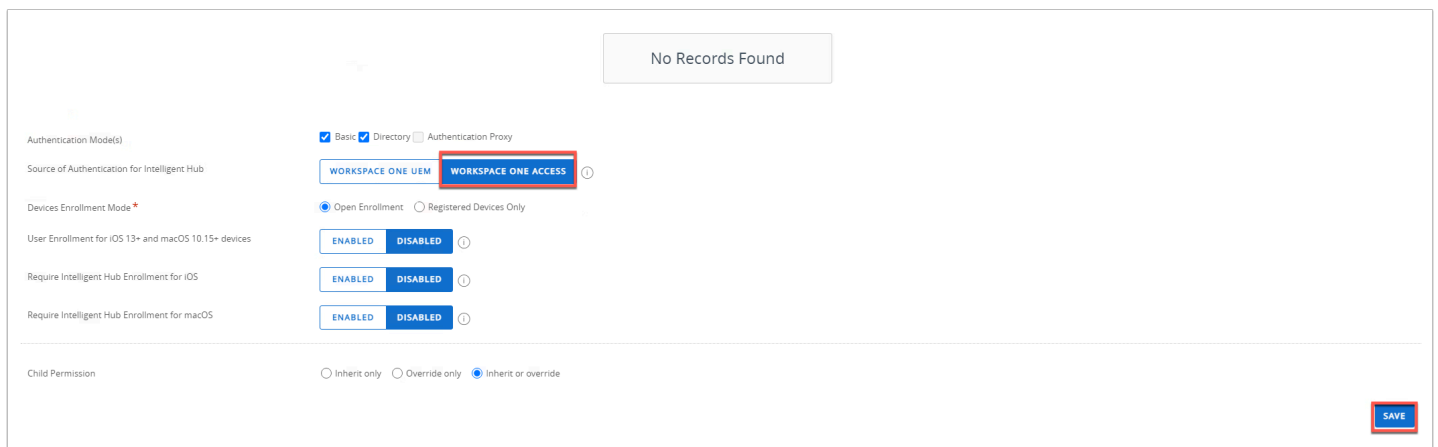
8. After you come back to the settings page for Workspace ONE Access Click **ENABLE** under **Certificate > Certificate Provisioning**

This screenshot shows the 'Certificate' provisioning details. It lists the 'Certificate' type, 'Valid From' date (3/7/2023), 'Valid To' date (3/9/2043), and a 'Thumbprint' (C6E34E63D4F289944855FF2686B61E836723B079). An 'EXPORT' button is highlighted with a red box. A 'DELETE' button is located at the bottom right.

9. After the certificate has been enabled click **EXPORT**, this should download the certificate to the downloads folder. We will come back to this certificate at a later stage.



10. In the left navigation panel of the Settings page navigate to **Devices & Users > General > Enrollment** and click **Override**.



11. Scroll down and change **Source of Authentication for Intelligent Hub** to **WORKSPACE ONE ACCESS** > Click **SAVE** at the bottom of the page.

**NOTE:** We are doing this as we want the user to authenticate during enrollment with Workspace ONE Access.

Devices & Users > General

## Enrollment ?

Authentication Management Mode Hub Integration Terms of Use Grouping **Restrictions** Optional Prompt Customization

Please save the restrictions before creating policy or assigning policies to groups.

Current Setting ☐ Inherit ☒ Override

### Enrollment Restrictions

User Access Control ☐ Restrict Enrollment To Known Users

☐ Restrict Enrollment To Configured Groups

Set limit for maximum enrolled devices at this Organization Group and below **ENABLED** **DISABLED** ?

### Policy Settings

[+ ADD POLICY](#)

Policy Name	Type	Organization Group	Dev
-------------	------	--------------------	-----

12. Scroll to the top of the page and click on the **Restrictions** tab > **uncheck** Restrict Enrollment to Known Users click **SAVE** at the bottom of the page

**NOTE:** The reason we are removing this check is because users will be created on the fly through the AirWatch provisioning adapter in Workspace ONE Access.

Settings

SimeonMarDev

Devices & Users > General

## Shared Device ?

Current Setting ☐ Inherit ☒ Override

### Grouping

Group Assignment Mode ☐ Prompt User For Organization Group ☒ Fixed Organization Group ☐ User Group Organization Group

Always Prompt for Terms of Use ☐ ?

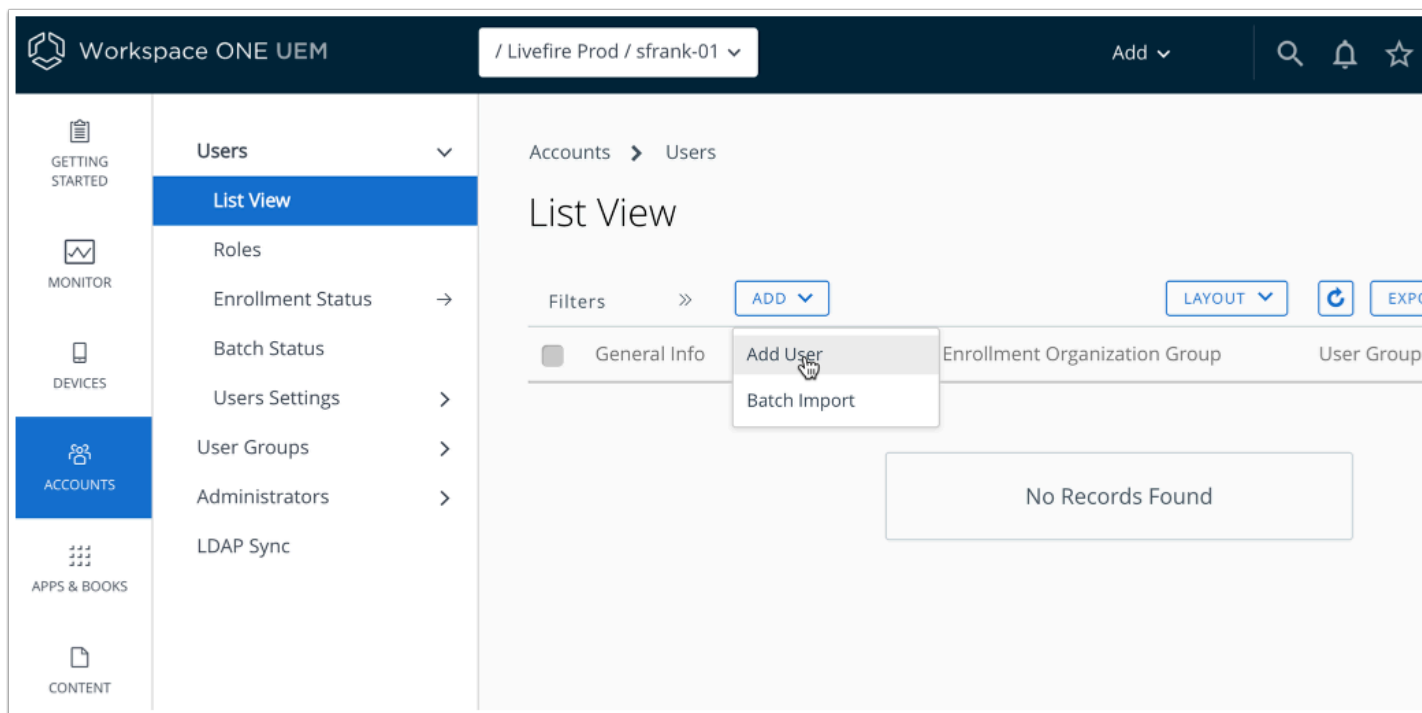
### Security

Require Shared Device Passcode ☐ ?

Auto Logout **ENABLED** **DISABLED** ?

13. In the left navigation page for **Settings** navigate to **Share Device** and click **Override**. For **Group Assignment Mode** click **Fixed Organization Group**. Click **SAVE** at the bottom of the page.

**TIP:** We will use staged devices later in the lab, this will allow devices that have been enrolled with the staging user to automatically be assigned to your organization group. This improves the user experience!



14. Close the settings page. Navigate to **Accounts > Users > List View** and click **ADD > Add User**

Add/Edit User

Security Type\*

BASIC

Username\*

staginguser

Password\*

VMware123

Hide

Confirm Password\*

VMware123

Hide

Full Name\*

Staging

Middle Name

User

Display Name

Email address\*

no-reply@euc-livefire.com

Email Username

SAVE

SAVE AND ADD DEVICE

CANCEL

15. Now fill in the following:
  - Username: **staginguser**
  - Password: **VMware123**
  - Confirm Password: **VMware123**

- Fullname: **Staging User**
- Email address: **no-reply@euc-liveware.com**

Add/Edit User

General **Advanced**

Advanced Info

Email Password  Show

Confirm Email Password  Show

Staging

Enable Device Staging **ENABLED** DISABLED

Single User Devices **ENABLED** DISABLED

Single User Devices\* Standard - Users are asked to log in a

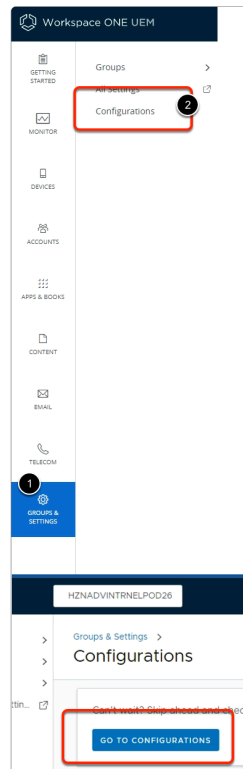
Multi User Devices ☐ ENABLED ☒ DISABLED

**SAVE** SAVE AND ADD DEVICE CANCEL

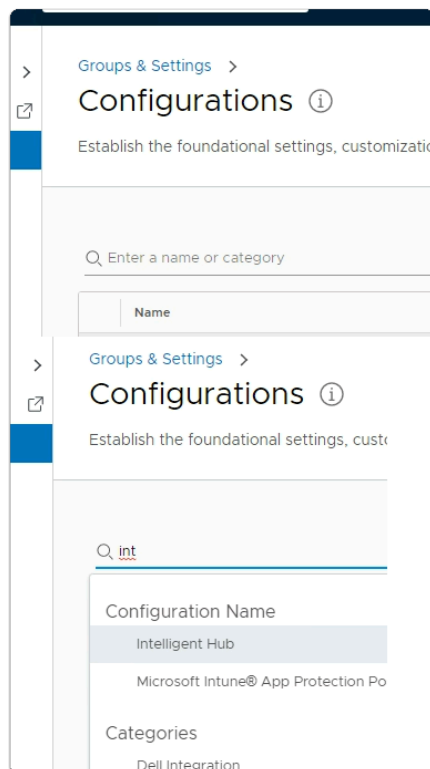
16. At the top of the Add/Edit User click **Advanced** tab. Scroll to the bottom and expand **Staging**.

- Enable Device Staging: **ENABLED**
- Single User Devices : **ENABLED**
- Single User Devices: **Standard - Users are asked to log in after staging**
- Multi User Devices: **DISABLED**
- Click **SAVE**.

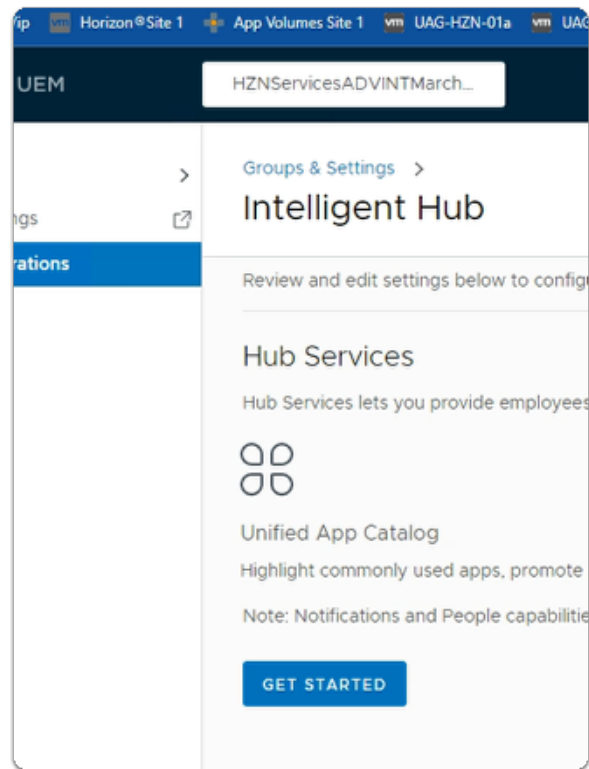
NOTE: In a future lab we will use an enrollment script to automate the enrollment of persistent desktops. This can be used also if IT or OEM is staging devices prior to delivery to end-user.



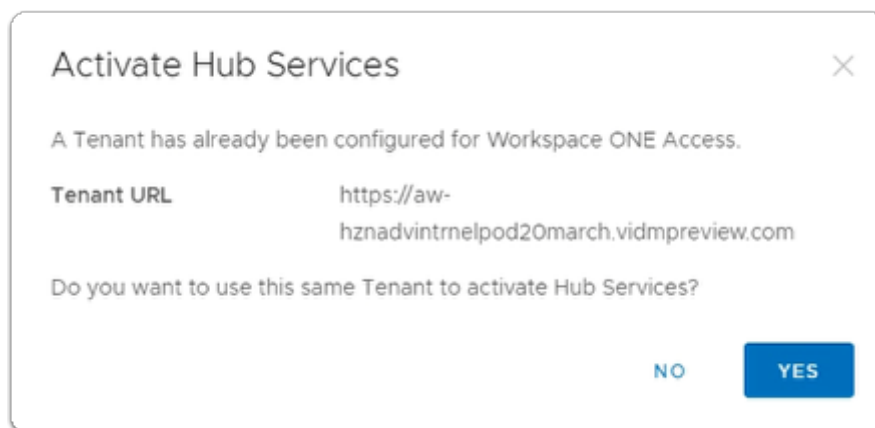
17. In the Workspace ONE UEM admin console
  1. Select **GROUPS & SETTINGS**
  2. Select **Configurations**
  3. In the **Group & Settings > Configurations** window
    - Select **GO TO CONFIGURATIONS**



18. Under **Configurations**
- In the **Enter a name or category** area
    - Type **Int**
  - Under **Configuration Name**
    - Select **Intelligent Hub**

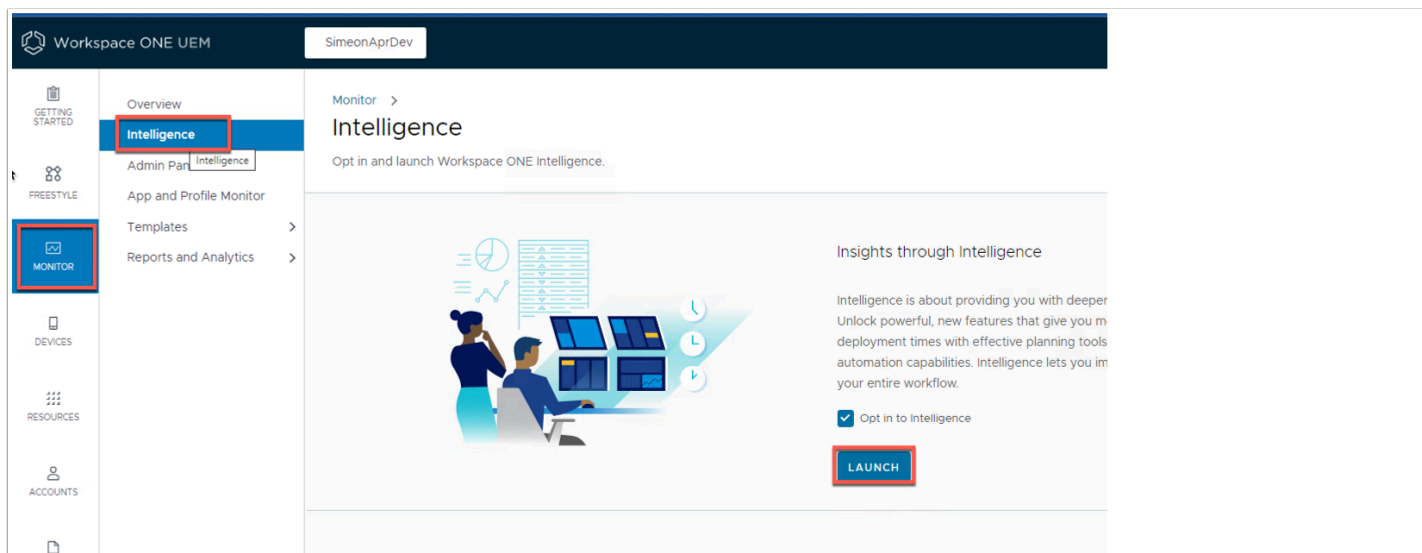


19. Under **Hub Services**
- Select **GET STARTED**

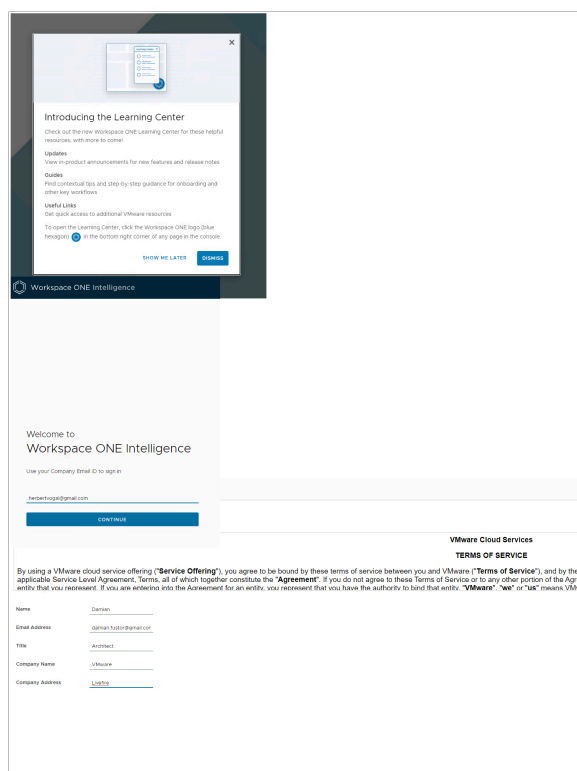


20. In the **Activate Hub Services**
- Select **YES**



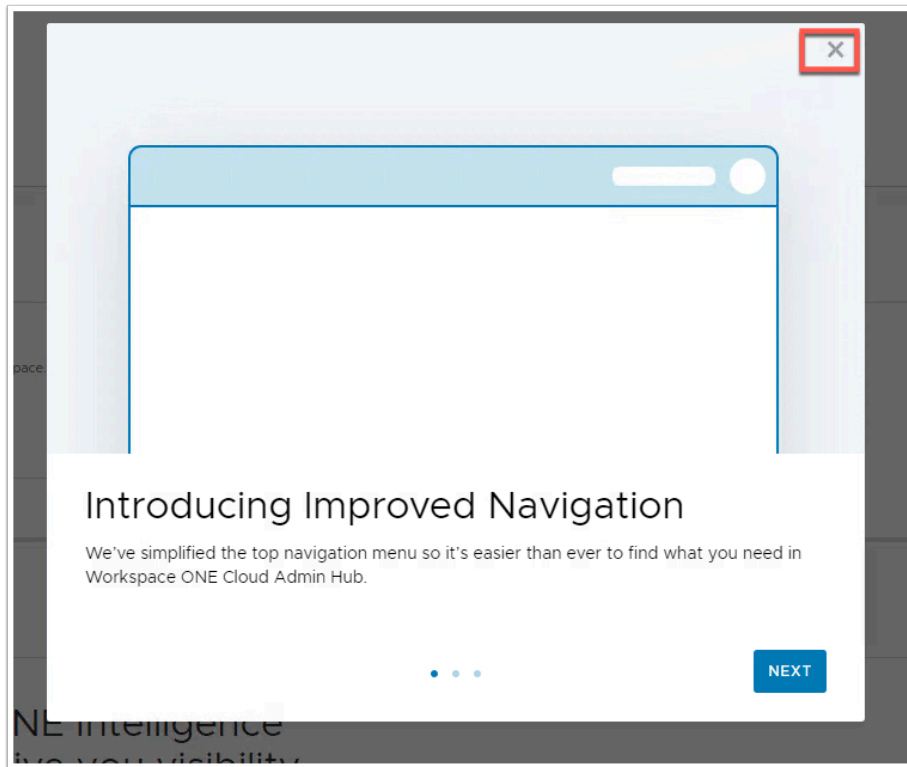


21. In the UEM admin console navigate to **MONITOR > Intelligence** and click **LAUNCH**

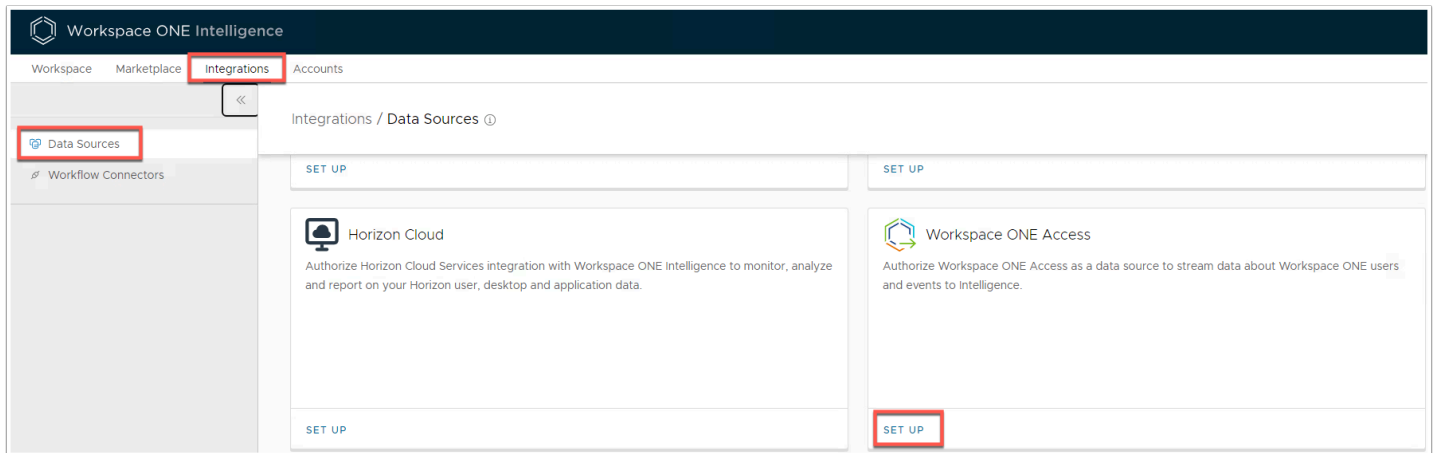


22. You will get a prompt for the new interface. Simply click **Dismiss**. Then type in your **e-mail address**.

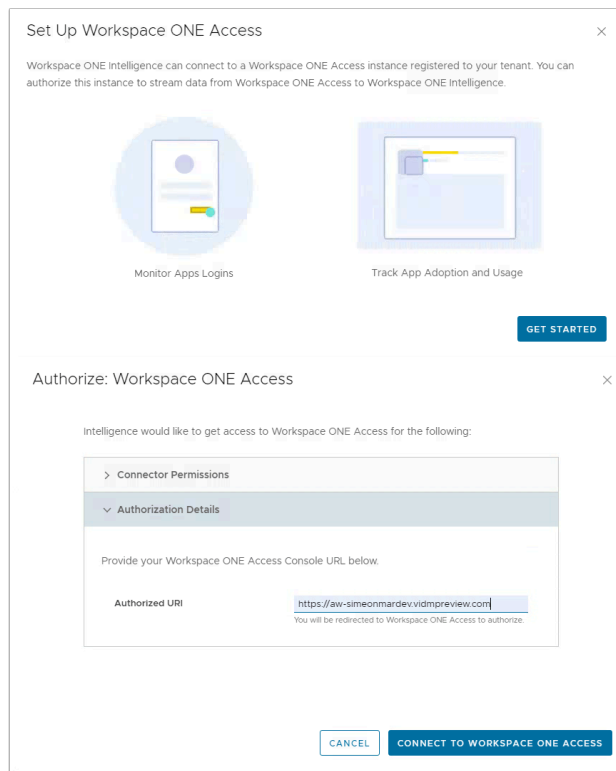
- Fill in the Details (Don't have to be real) for **Terms of Service** and click **ACCEPT**



23. (If there is a pop-up) **Close** the Introducing Improved Navigation pop-up.

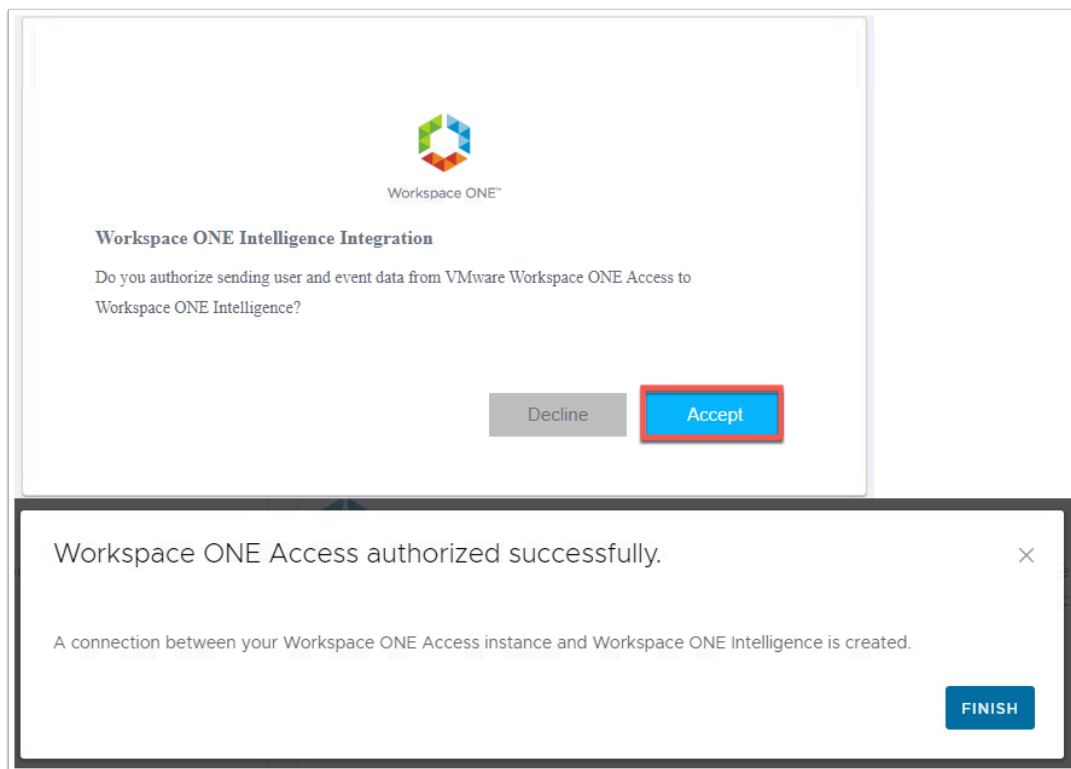


24. Navigate to **Integration > Data Sources > Workspace ONE Access > SET UP**



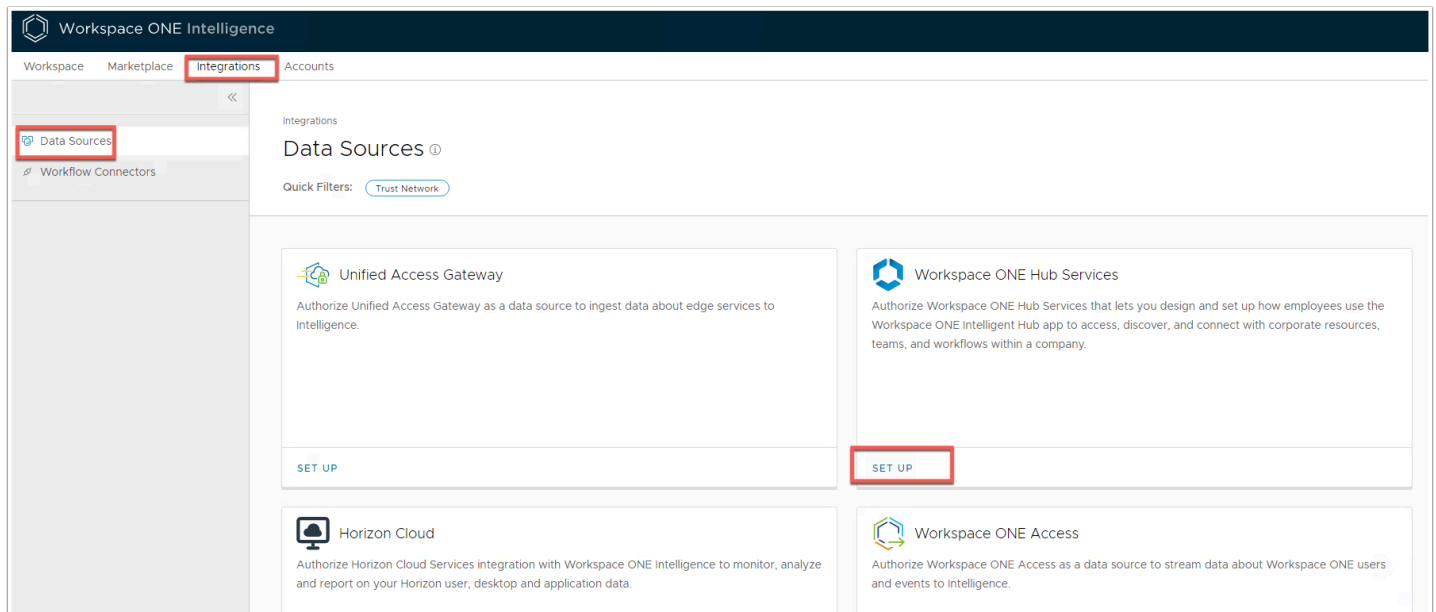
25. Click **GET STARTED** on the pop-up.

- Under **Authorization Details** > Authorized URI type in the URL for your ACCESS tenant.
- Click **CONNECT TO WORKSPACE ONE ACCESS**

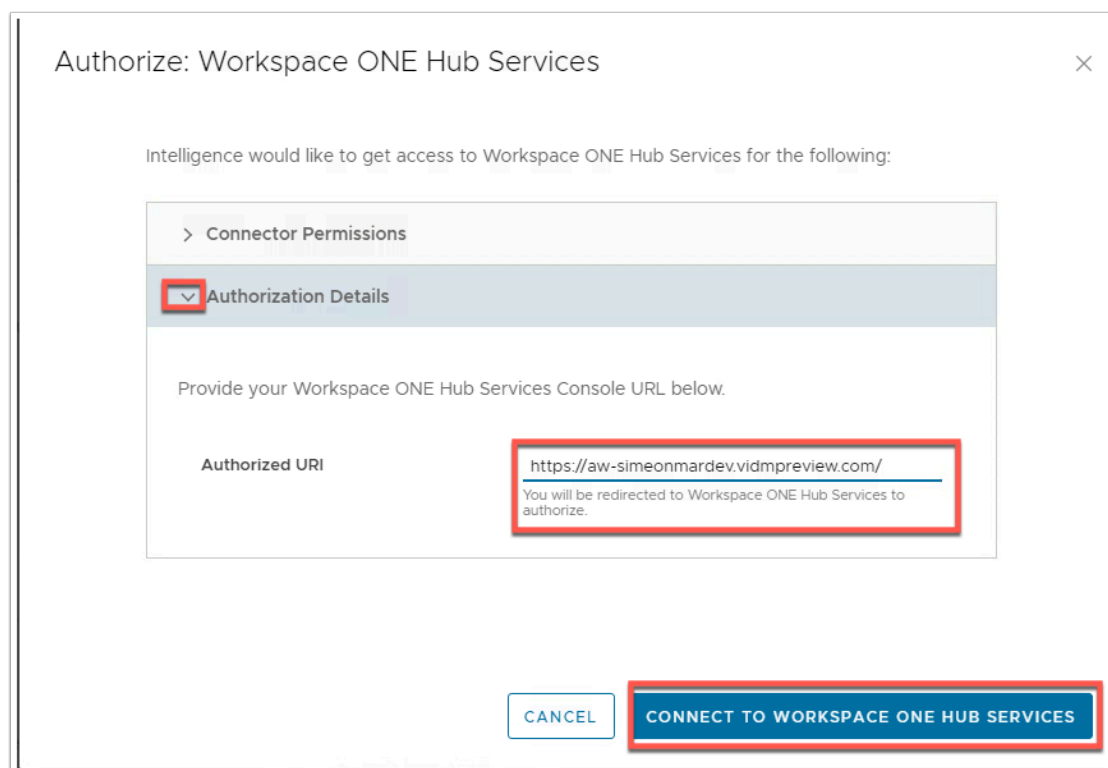


26. If you are already authenticated to Workspace ONE Access click **Accept** on the new tab that opens up.

- Otherwise authenticate to Access using your administrator account.
- Username: **administrator**
- Password: **VMware1!**
  - Click Finish when you are re-directed back to Access.

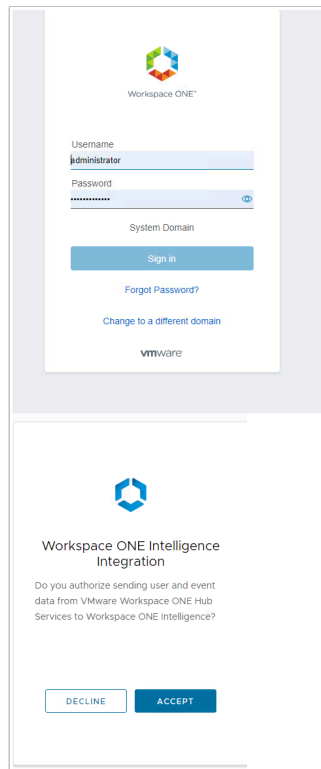


27. In the Intelligence console navigate to **Integration > Data Sources > Workspace ONE Hub Service** > click **SET UP**



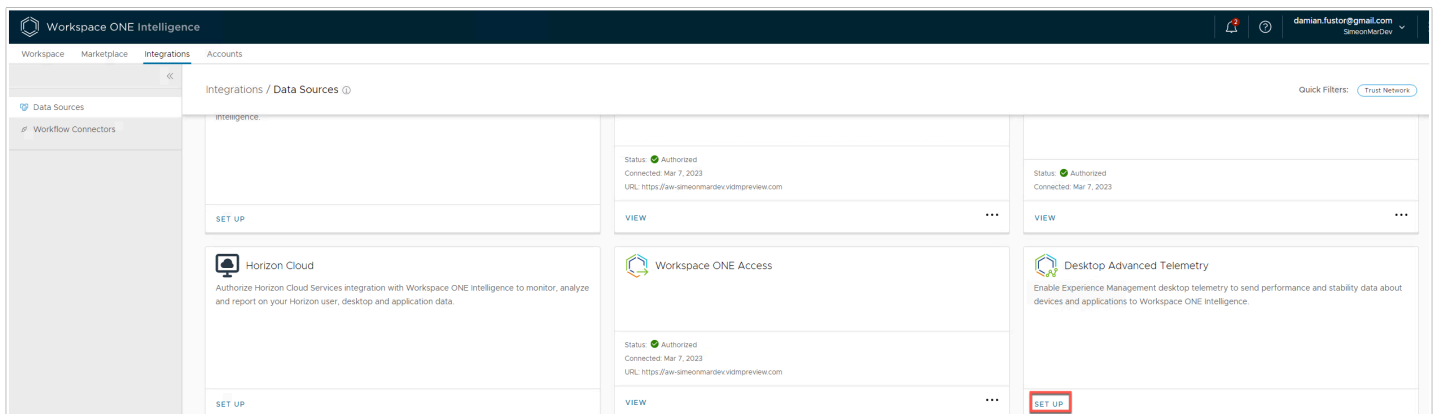
28. Click GET STARTED on the pop-up and click **Authorization Details** > the **Authorized URI** should be your Workspace ONE Access URL.

- Click **CONNECT TO WORKSPACE ONE HUB SERVICES**



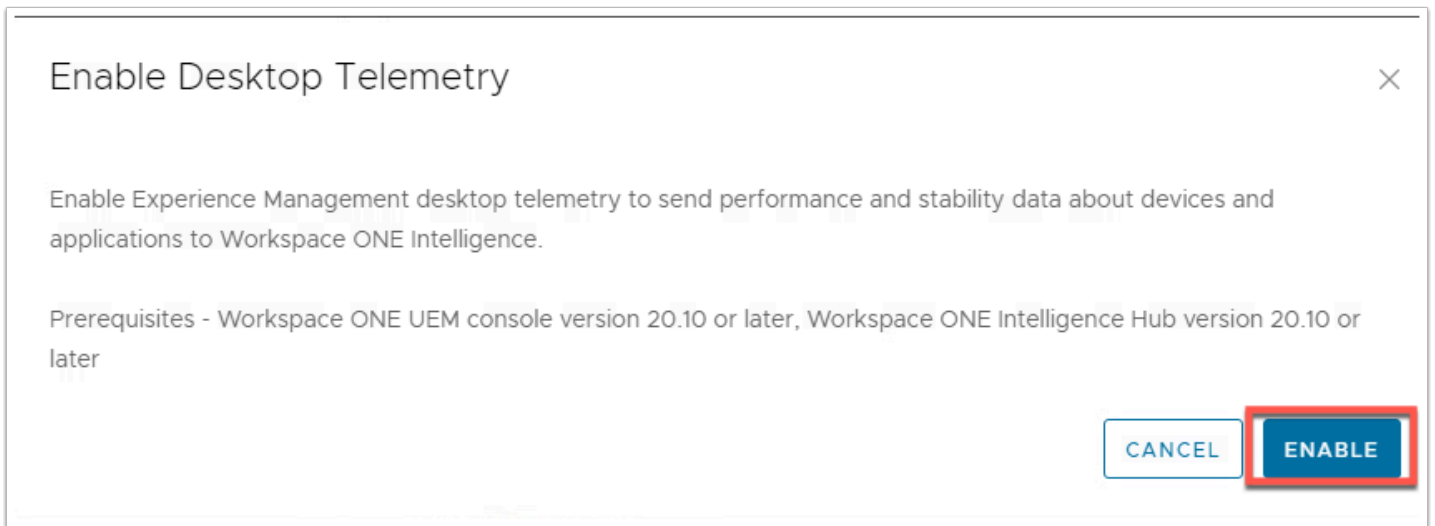
The image shows a mobile interface for Workspace ONE. The top section is a login form with fields for Username (pre-filled with 'administrator'), Password (masked with dots), and System Domain. Below these fields are buttons for 'Sign in', 'Forgot Password?', and 'Change to a different domain'. The VMware logo is at the bottom of this section. The bottom section is titled 'Workspace ONE Intelligence Integration' and asks for authorization to send user and event data from VMware Workspace ONE Hub Services to Workspace ONE Intelligence. It features 'DECLINE' and 'ACCEPT' buttons.

29. If you aren't already logged into Workspace ONE Acces you will be prompted to authenticate. Then **ACCEPT** the authorization to send data to Intelligence.

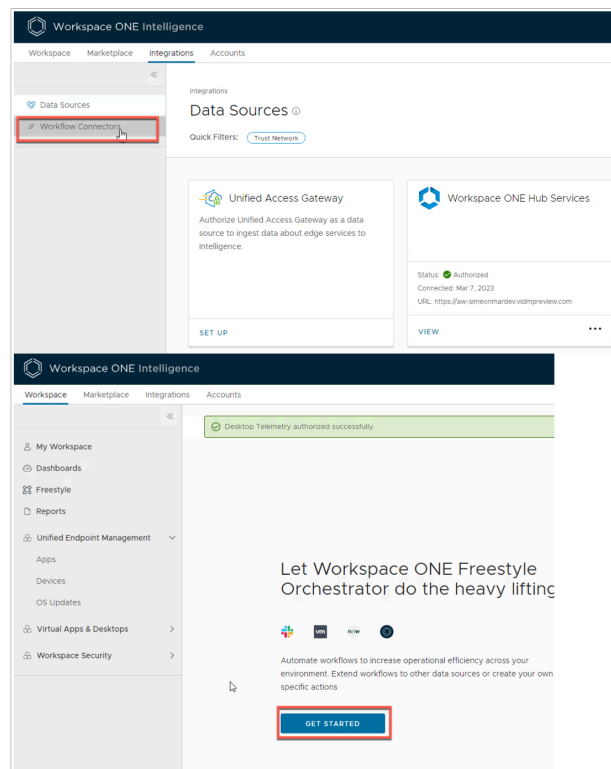


The screenshot shows the Workspace ONE Intelligence console. The top navigation bar includes 'Workspace', 'Marketplace', 'Integrations', and 'Accounts'. The left sidebar has 'Data Sources' and 'Workflow Connectors'. The main content area is titled 'Integrations / Data Sources' and shows a list of integrations. The integrations listed are 'Intelligence', 'Horizon Cloud', 'Workspace ONE Access', and 'Desktop Advanced Telemetry'. Each integration card shows its status (Authorized), connection date (Mar 7, 2023), and a URL. The 'Desktop Advanced Telemetry' card has a red box around the 'SET UP' button.

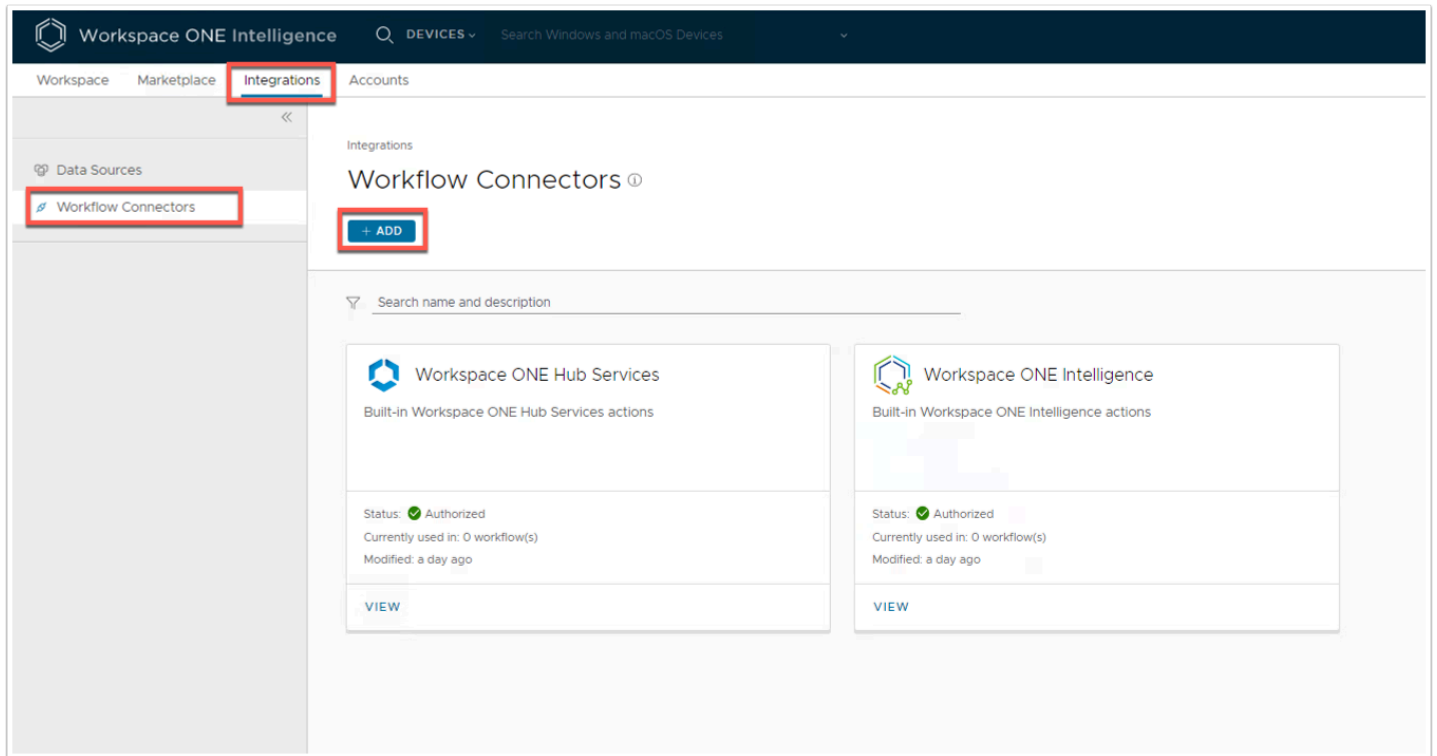
30. Back in the Intelligence console now find Desktop Advanced Telemetry in the Integrations Setup page and click on **SETUP**.



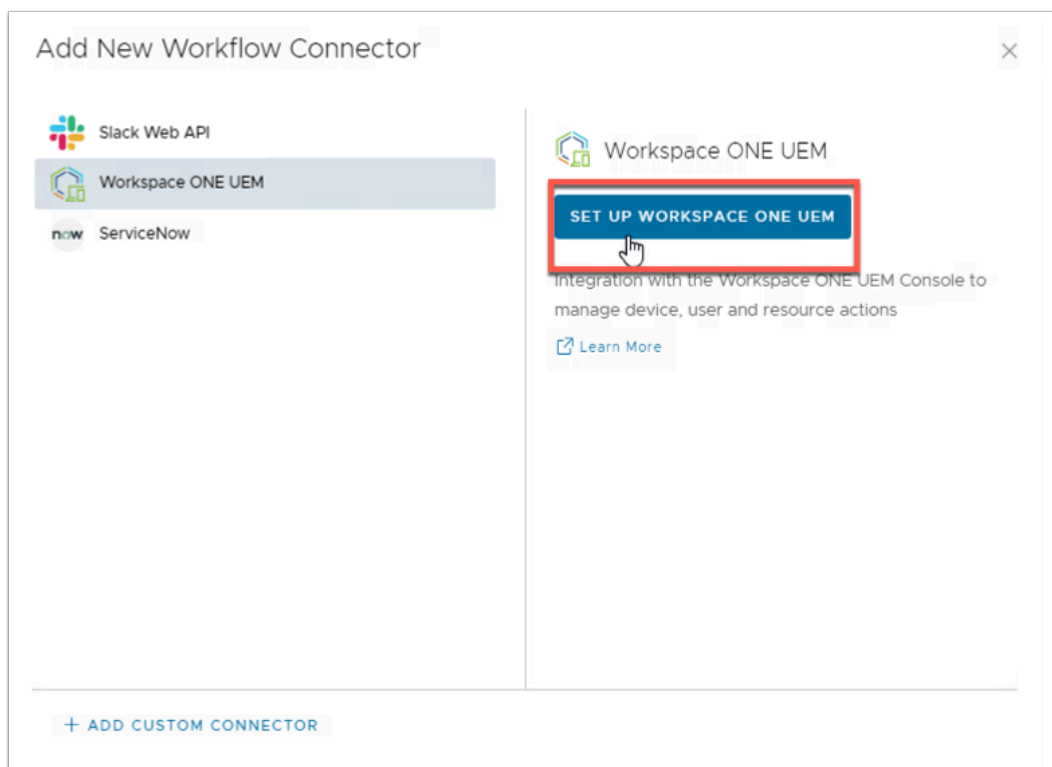
31. Click **ENABLE** at the prompt. You will now be able see device and application performance metrics in Intelligence. (We will come back to this at a later stage)



32. In the Workspace ONE Intelligence Admin console, click **Integrations** > click **Workflow Connector**.
- You will be redirected to **Workspace**. Click **GET STARTED**.



33. Navigate back to **Integrations > Workflow Connectors** and click **+ ADD**



34. Click on **Workspace ONE UEM** in the **Add New Workflow Connector** window.

- Click **SET UP WORKSPACE ONE UEM**

Authorize Connector: Workspace ONE UEM ⓘ

✓ Authorization Details

ⓘ Click here for more information on how to set up this connector. [More information](#)

Base URL

Auth Type

User Name

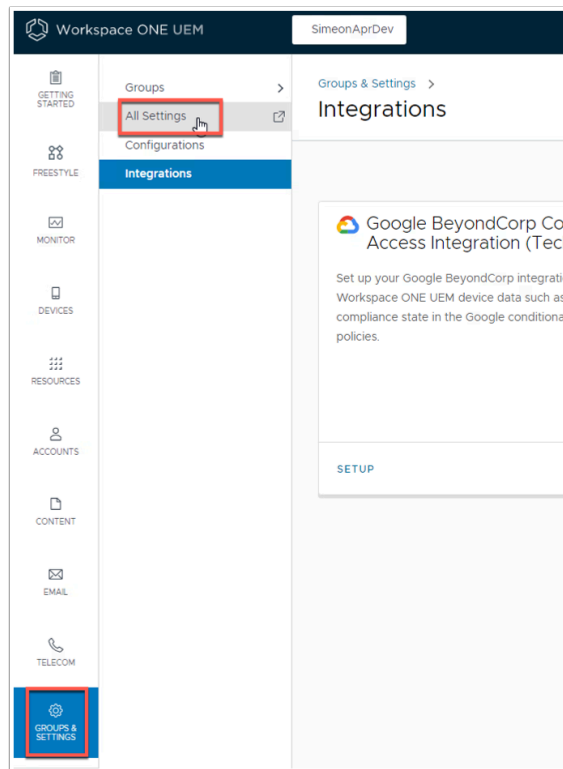
Password

Workspac...

35. Fill in the Authorize Connector: Workspace ONE UEM:

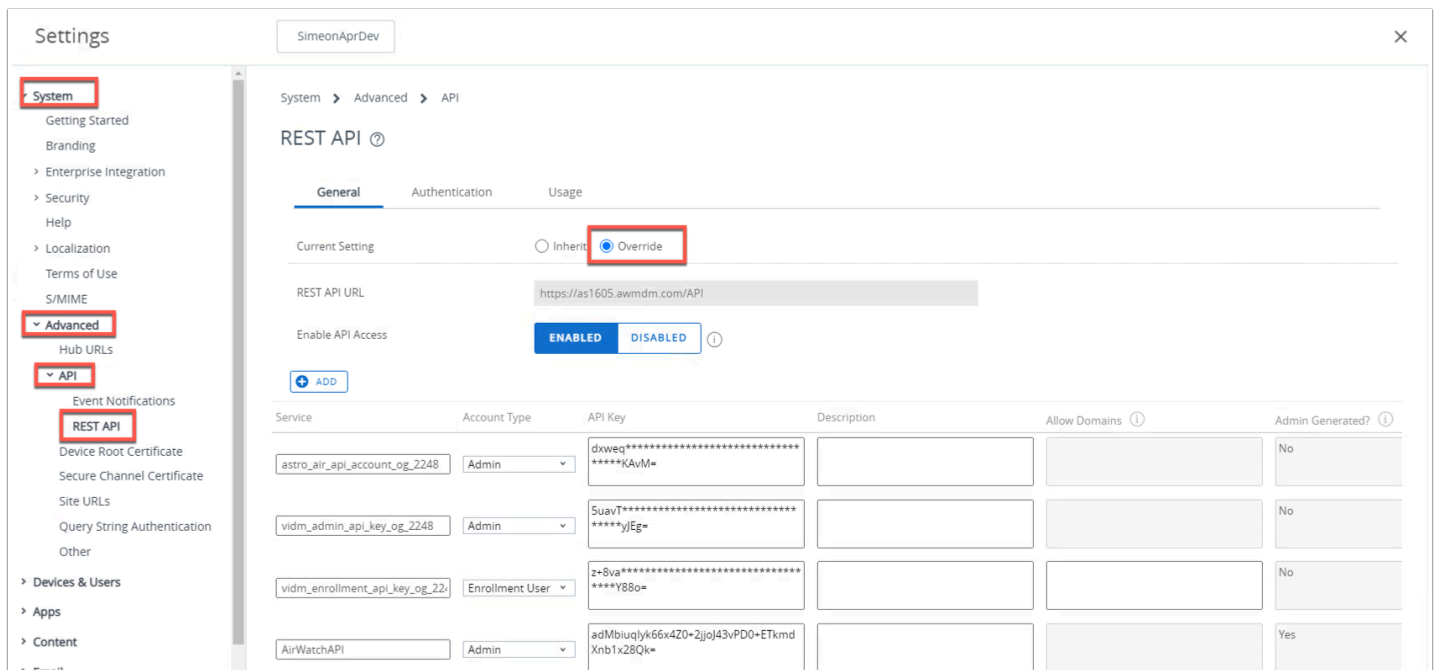
- Base URL: <https://dw-livefire.awmdm.com/>
- Auth Type: **Basic Authentication**
- User Name: **{YOUR EMAIL ADDRESS}**
- Password: **VMware1!**
- Workspace ONE UEM API Key - **Flip to Workspace ONE UEM Admin Console**





36. In a new tab open Workspace ONE UEM Admin Console - <https://dw-livefire.awmdm.com/>

- Navigate to **GROUPS & SETTINGS > All Settings**



37. In the **Settings** page navigate to **System > Advanced > API > REST API**.

- Click **Override**.

API Name	Account Type	API Key	Workspace UEM	Allow Domains	Admin Generated?
astro_air_api_account_og_2248	Admin	dxweq***** *****KAvM=			No
vidm_admin_api_key_og_2248	Admin	5uavT***** *****yJEg=			No
vidm_enrollment_api_key_og_2248	Enrollment User	z+8va***** *****Y88o=			No
AirWatchAPI	Admin	adMbiuglyk66x4Z0+2jjoJ43vPD0+ETkmd Xrb1x28Qk=			Yes

Child Permission ☒ Inherit only ☐ Override only ☐ Inherit or override

**SAVE**

38. Copy the **API Key** for the AirWatch API Service and click **SAVE**.

Authorize Connector: Workspace ONE UEM ⓘ

✕

Authorization Details

Click here for more information on how to set up this connector. [More information](#)

Base URL

Auth Type

User Name

Password

Workspac...

**CANCEL** **AUTHORIZE**

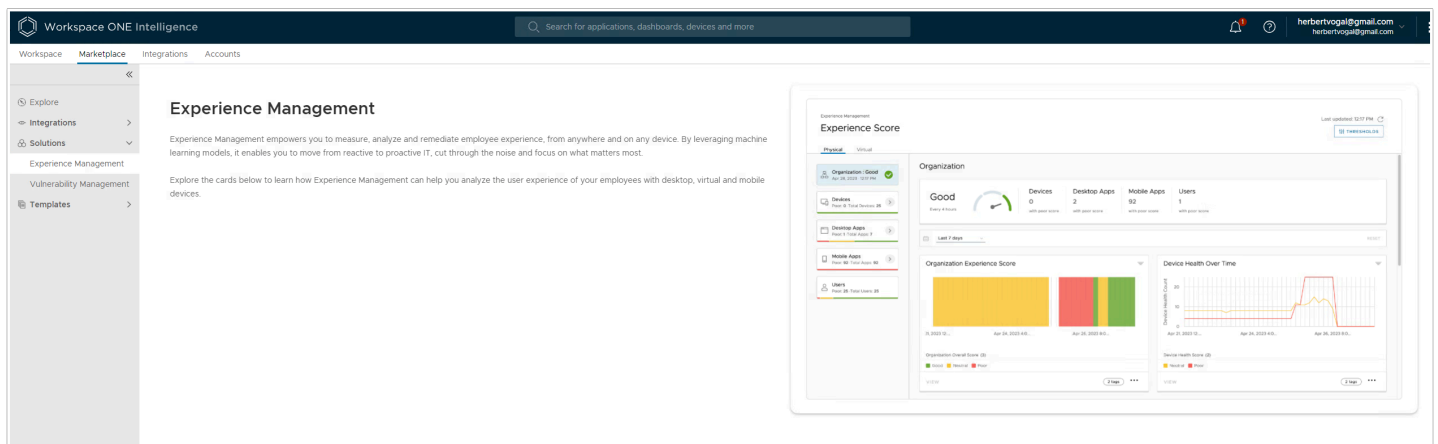
39. Navigate back to the browser Tab with Workspace ONE Intelligence.
- Click the Pencil icon in the Workspace ONE UEM API Key field
  - Paste the **API Key** into the **Workspace ONE UEM API Key** field
  - Click **AUTHORIZE**

## Part 2: Enable Experience Management

In this exercise you will enable [Experience Management](#) in Workspace ONE Intelligence. This will allow for the device to send telemetry and metrics to Intelligence and report on the following and more -

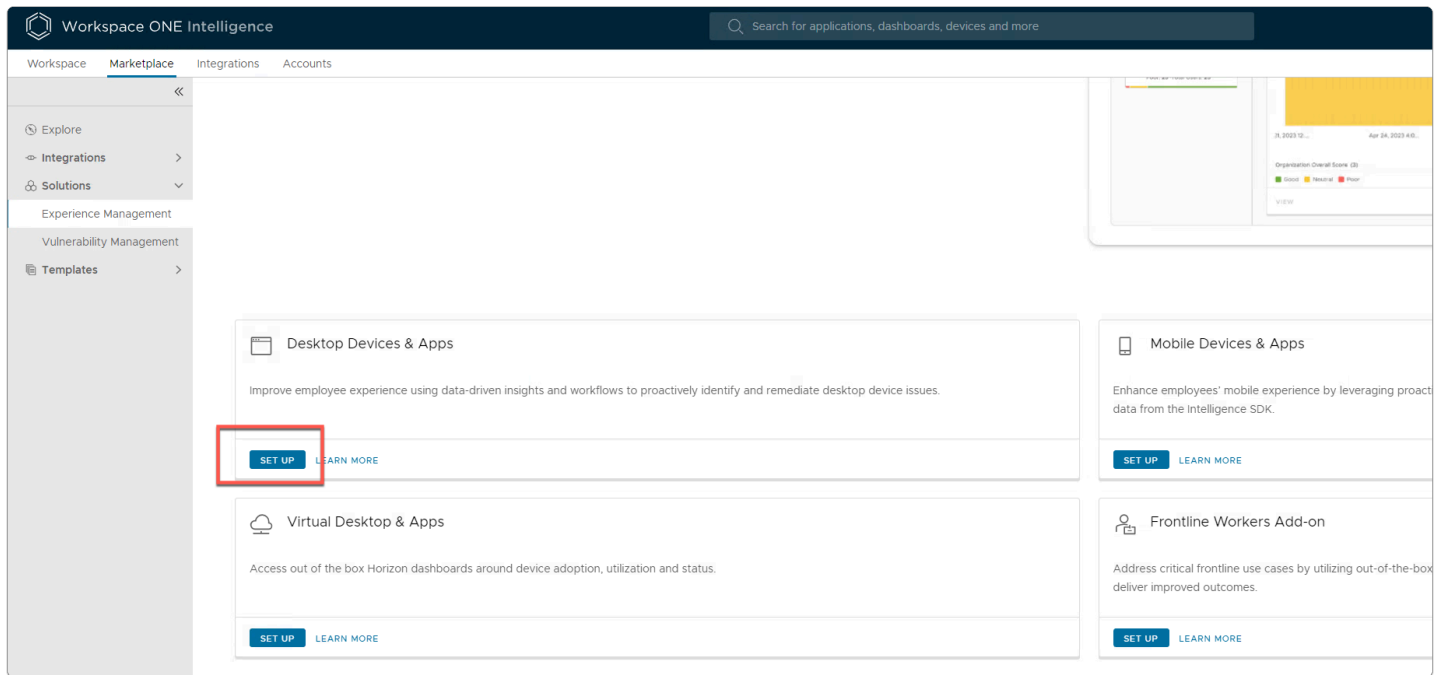
- Device Heal, Application Health
- Performance and Stability
- OS Crashes
- Login, and Logout
- Boot and Shutdown events and duration
- Windows Services Status
- Windows Performance Monitor Data

NOTE: In this lab we will simply enable this function so that devices will begin their reporting, we won't actually have any metrics at this point.



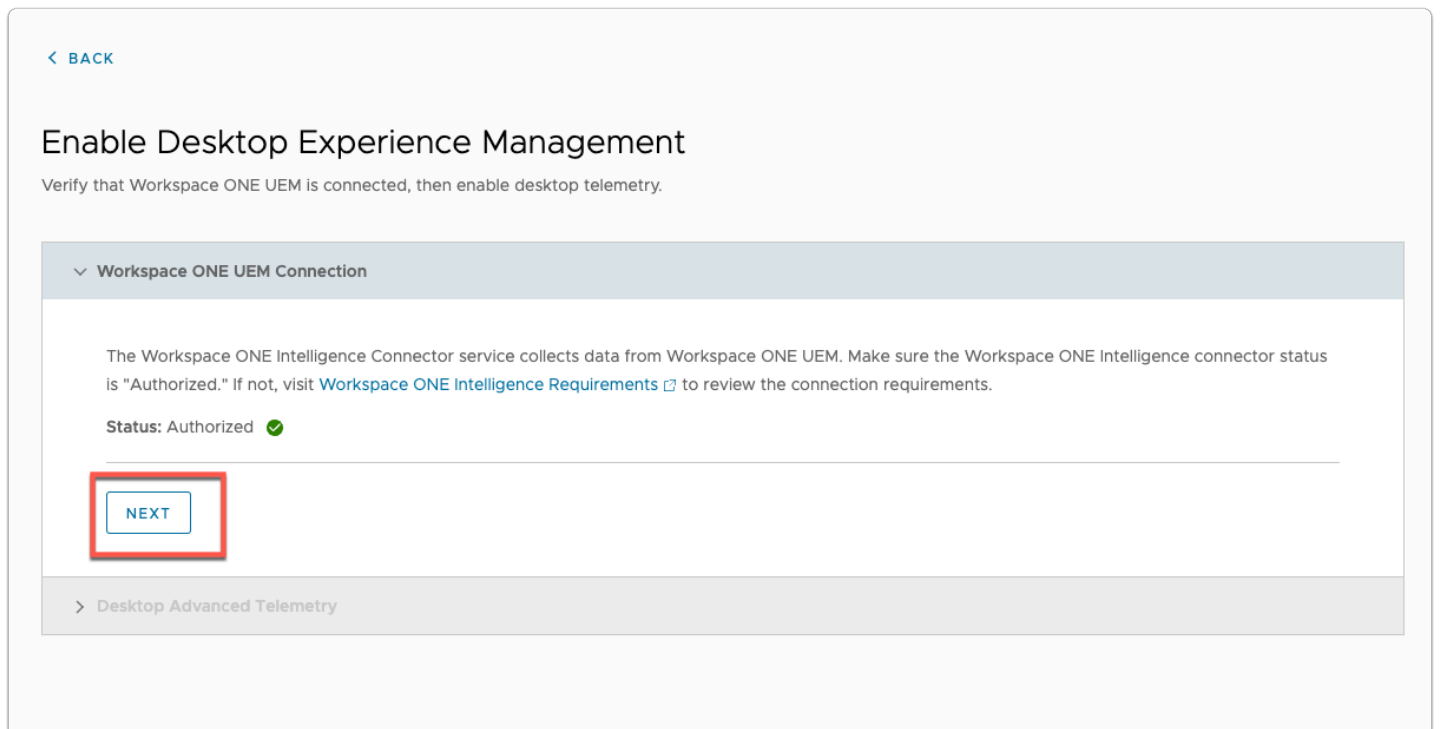
### 1. In the Workspace ONE Intelligence Console

- navigate to **Marketplace** > **Solutions** > **Experience Management**



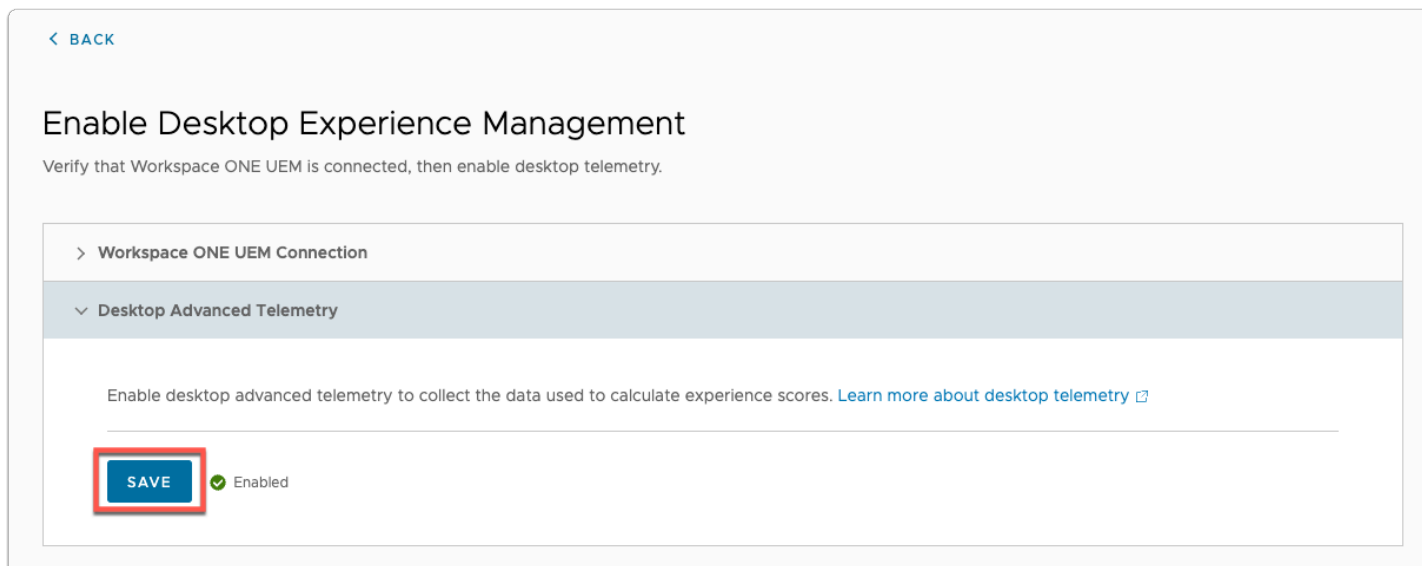
## 2. In the Experience Management page

- Click **SET UP** on the **Desktop Experience Management**

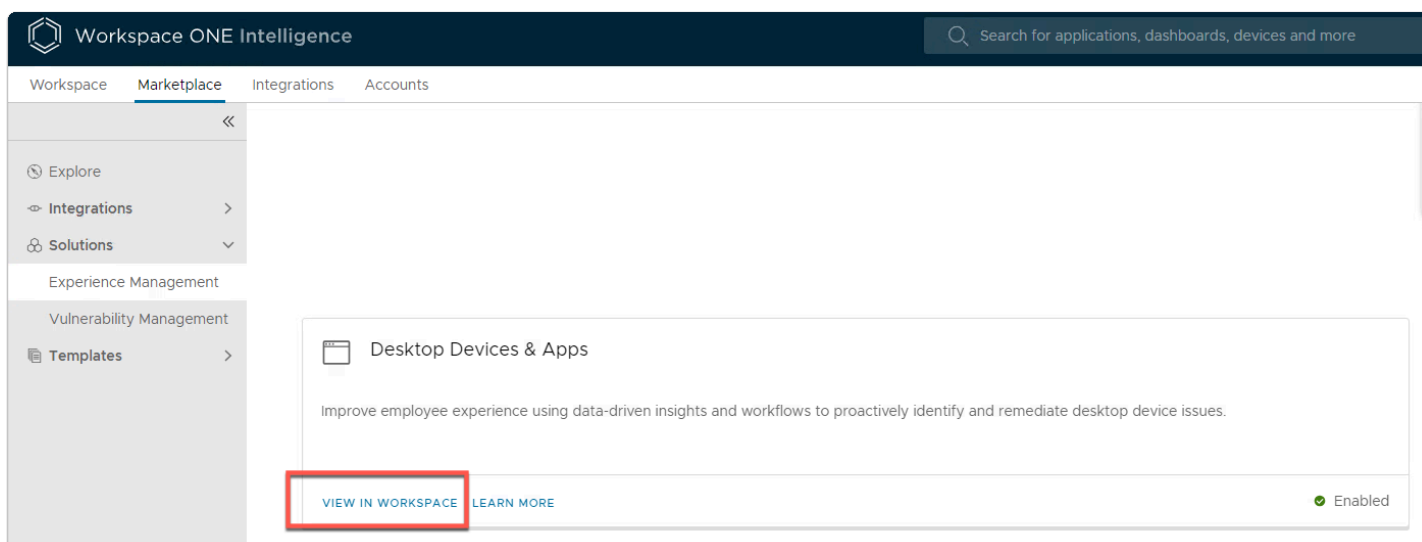


## 3. In the **Enable Desktop Experience Management**

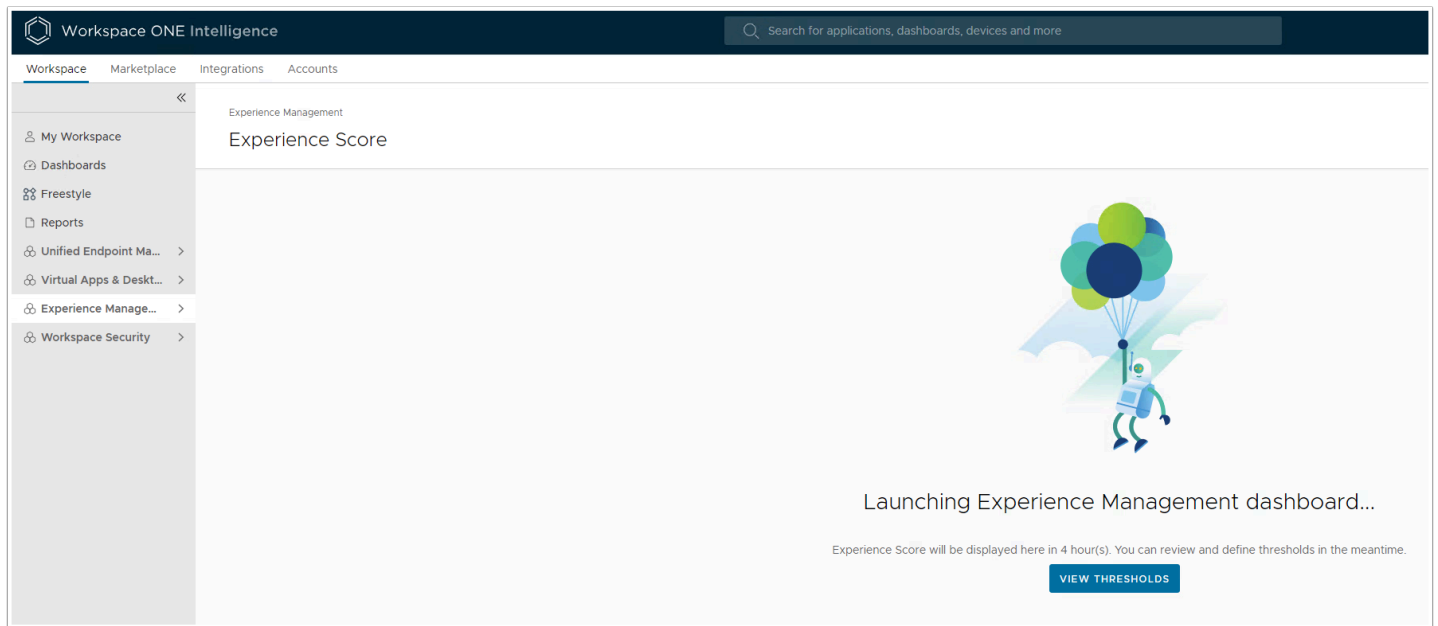
- select **NEXT** to authorize the right server.



4. In the **Enable Desktop Experience Management** wizard
- Under **Desktop Advanced Telemetry**
    - select **SAVE**



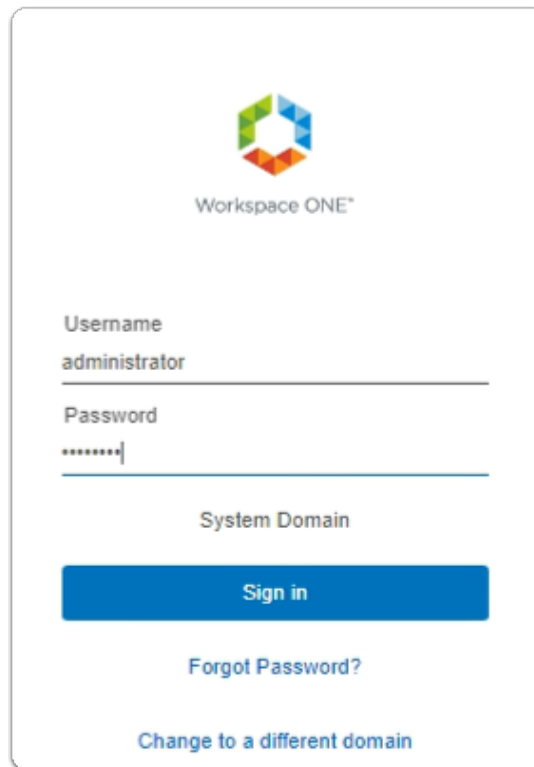
5. You should now have Desktop Experience Management Enabled.
- Click **View** this will take you to the Workspace Tab.
  - NOTE: There is no data in here as of yet.



After device have registered with UEM we will see Desktop telemetry here.

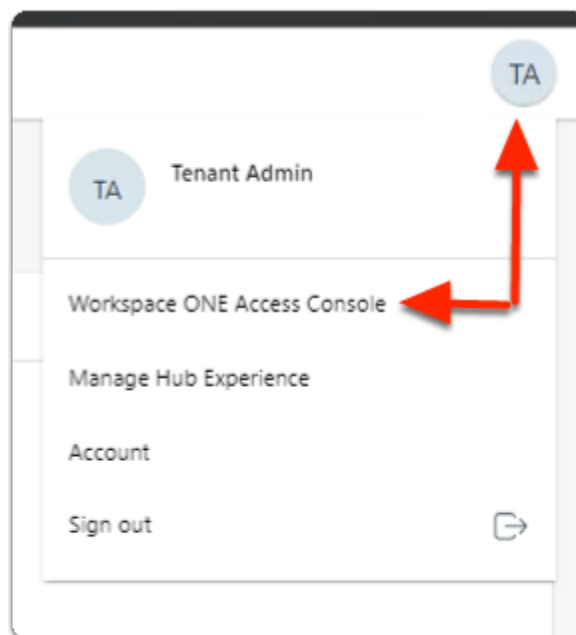
## Part 3: Workspace ONE Access , Connector pairing pre-requisites

In this lab you will download the Workspace ONE Access connector configurations. These configurations will be used later in Part 4 to install the Workspace ONE Access connector.

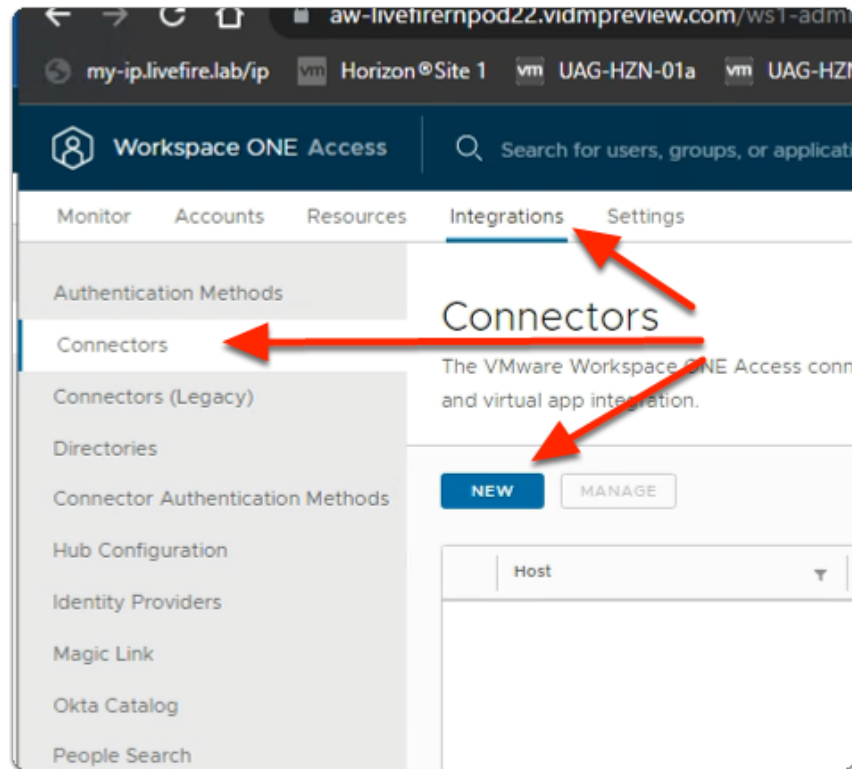


The image shows the Workspace ONE login interface. At the top is the Workspace ONE logo. Below it are two input fields: 'Username' with the text 'administrator' and 'Password' with masked characters '\*\*\*\*\*'. A 'System Domain' label is positioned above a blue 'Sign in' button. Below the button are two links: 'Forgot Password?' and 'Change to a different domain'.

1. On your ControlCenter server
  - Open your **Workspace ONE Access**, Admin console URL
    - Under **Username**
      - enter **Administrator**
    - Under **Password**
      - enter **VMware1!**
    - Select **Sign In**



2. In the **Web Intelligent Hub Console**
  - To the right,
    - select **TA**
  - From the dropdown
    - select **Workspace ONE Access Console**



3. In the **Workspace ONE Access Console**
  - Select **Integrations**
  - Under **Integrations**
    - Select **Connectors**
  - In the **Connectors** area
    - Select **NEW**

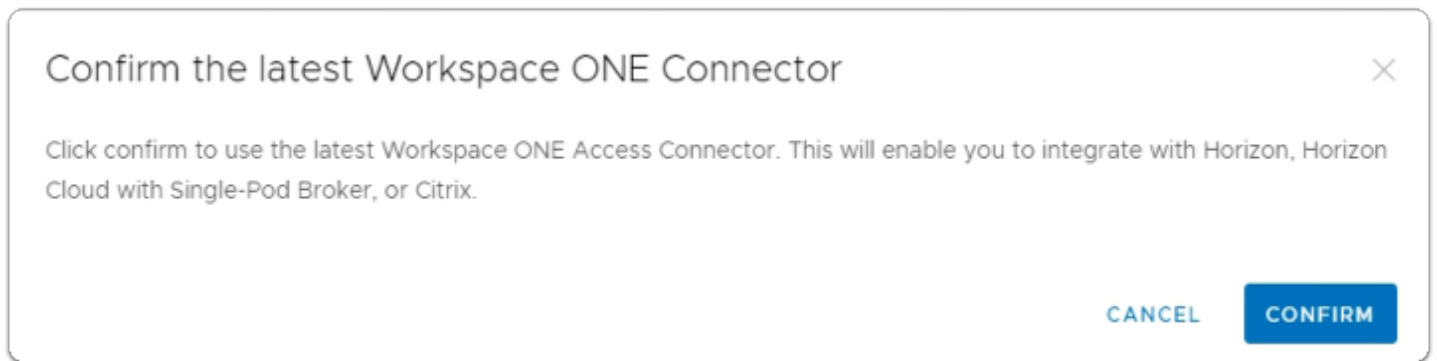


4. In the **Connector Usage Confirmation** window
  - Select the **radio button**, next to :-



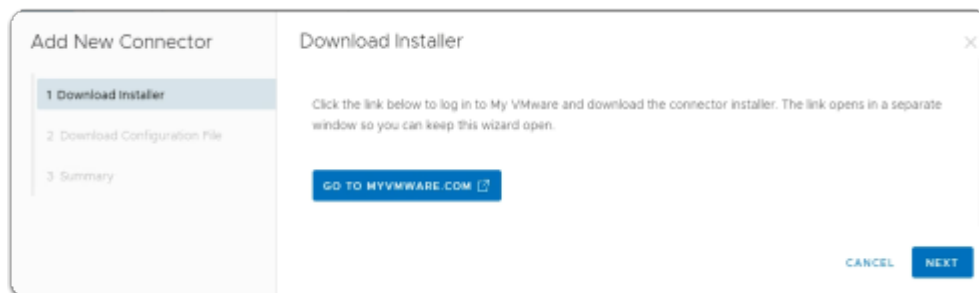
- **Latest Workspace ONE Access Connector**

- Select **OK**



5. In the **Confirm the latest Workspace ONE Connector** window

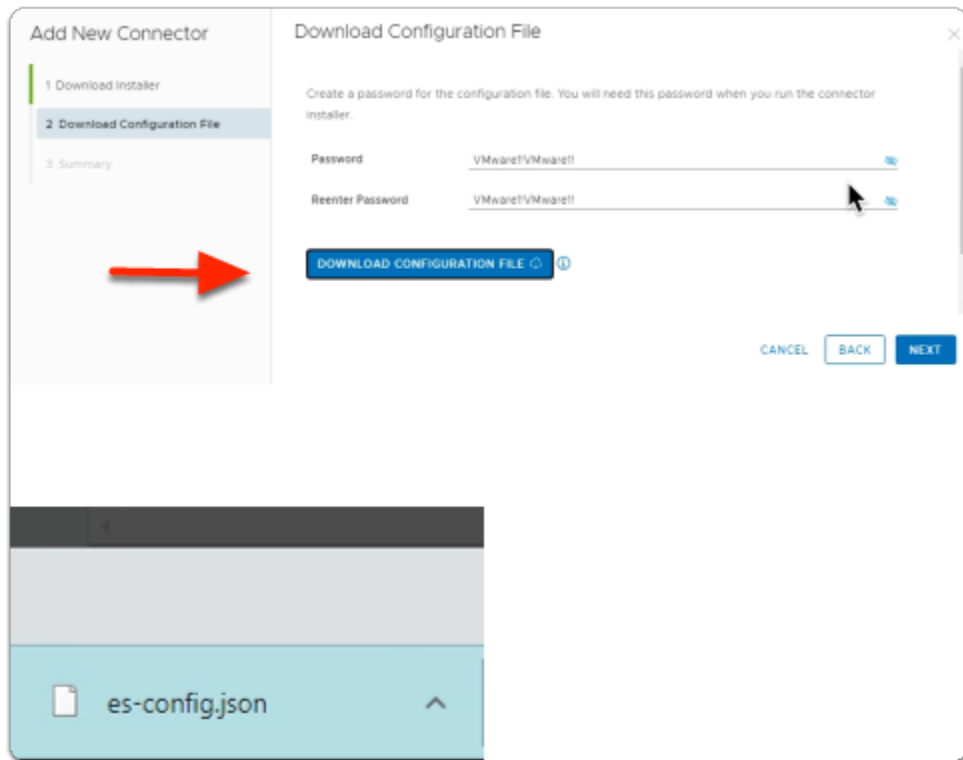
- Select **CONFIRM**



6. In the **Add New Connector** window

1. **Downloader Installer** area

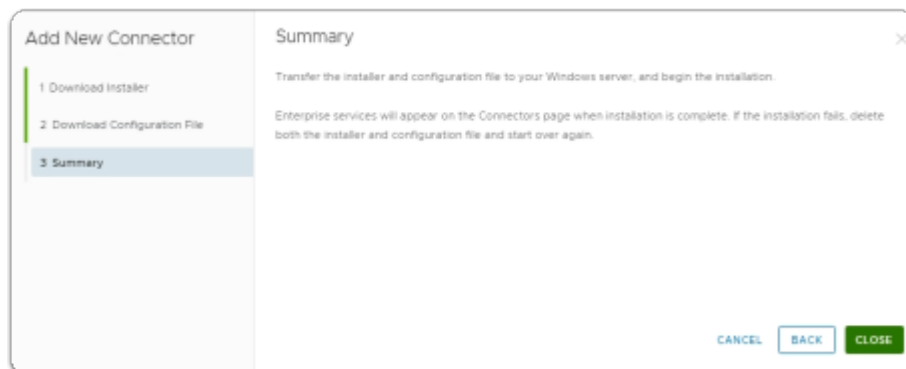
- Select **NEXT**



7. In the **Add New Connector** window

2. **Download Configuration File** area

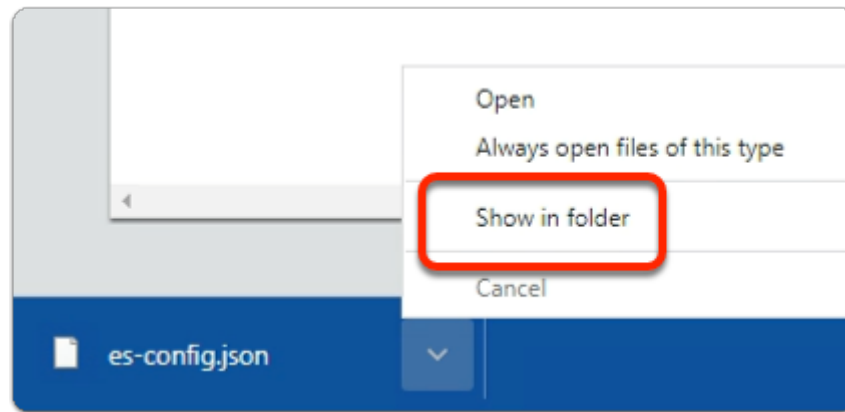
- Next to **Password:** enter **VMware!VMware!**
- Next to **Reenter Password:** enter **VMware!VMware!**
- Select **DOWNLOAD CONFIGURATION FILE**
  - note an **es-config.json** file gets downloaded
- Select **NEXT**



8. In the **Add New Connector** window

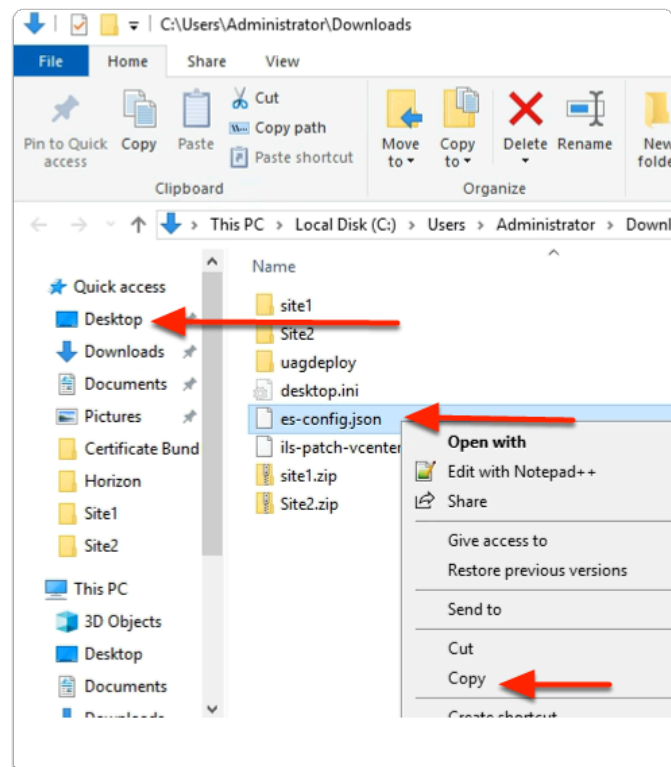
3. **Summary** window

- Select **CLOSE**



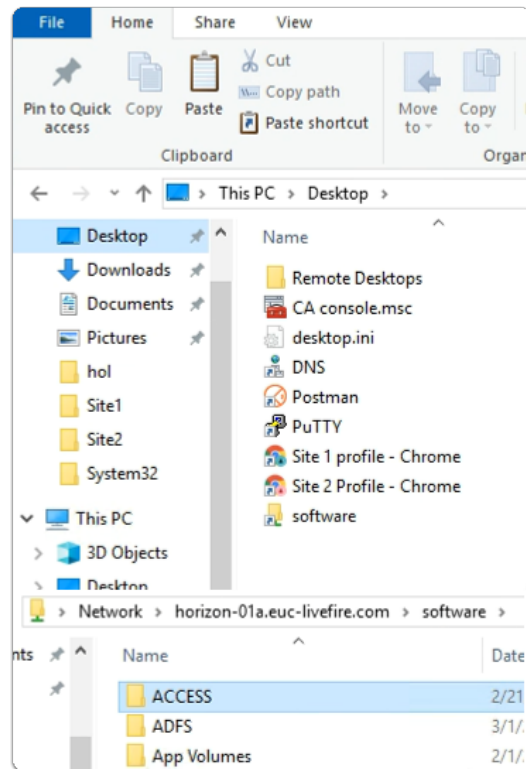
9. On your ControlCenter server browser

- Next to the **es-config.json**
  - Select the **Dropdown**
  - Select **Show in folder**



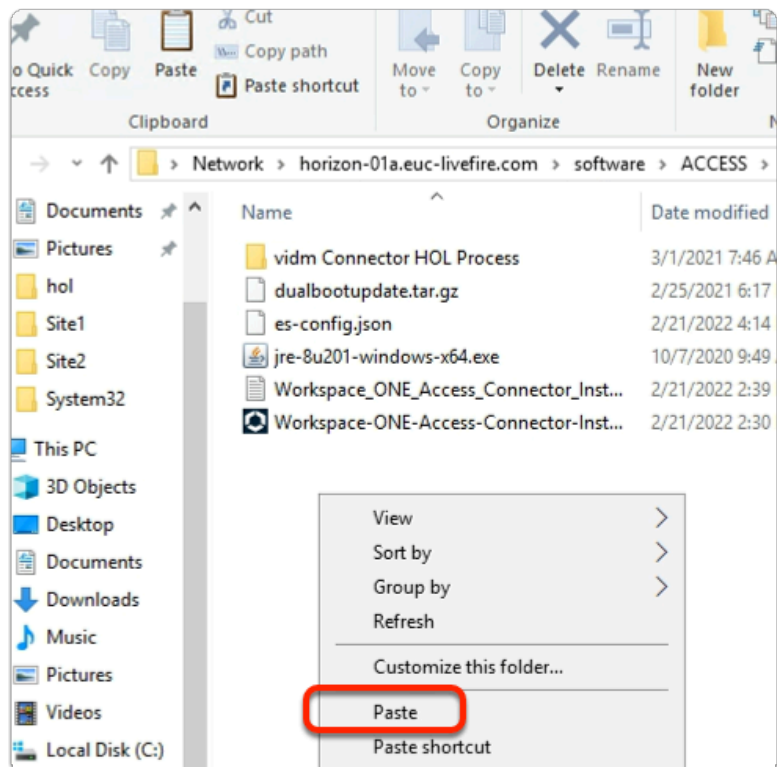
10. In the **File Explorer** window

- Select and right-click the **es-config.json** file
- Select **Copy**
- In the left pane
  - Select **Desktop**



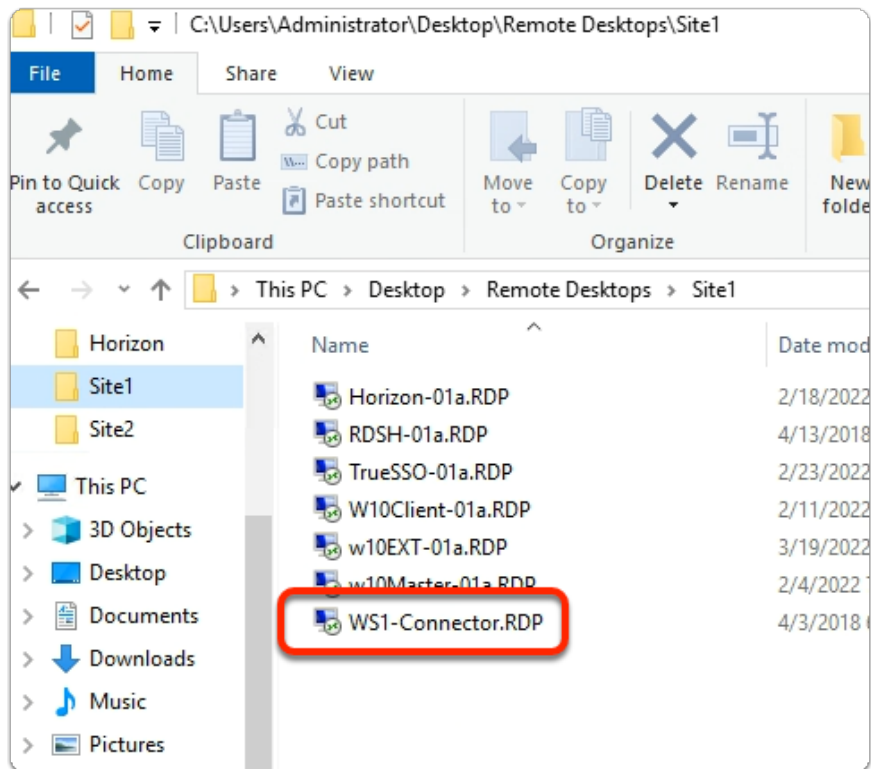
11. In the **File Explorer** window

- **Desktop area**
  - Select the **Software** shortcut
  - In the **Software** folder
    - Open the **ACCESS** folder

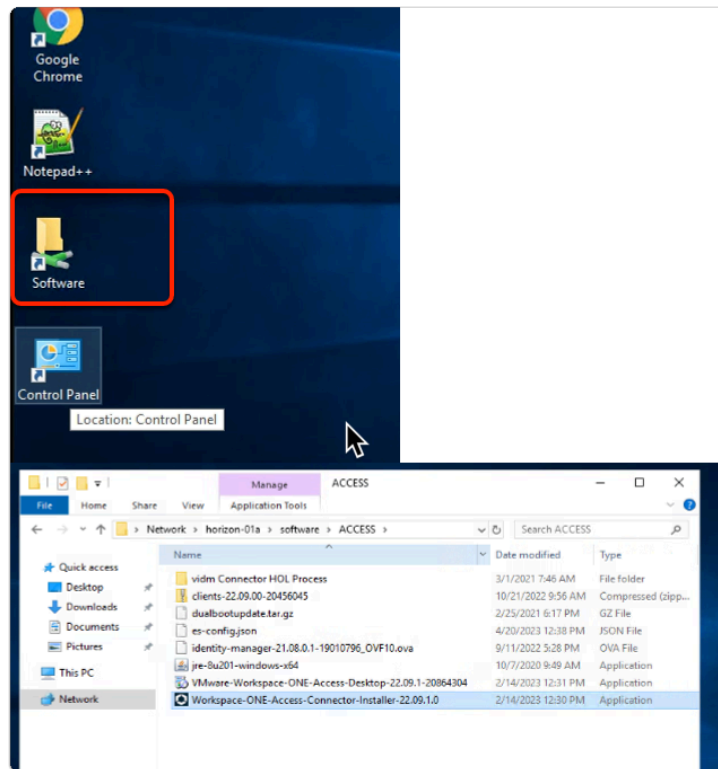


12. In the **File Explorer** window
  - **ACCESS** folder
    - **Paste** your **es-config.json** file
  - **Close** your **File Explorer** window

## Part 4: Installing and Configuring the Workspace ONE Access connector

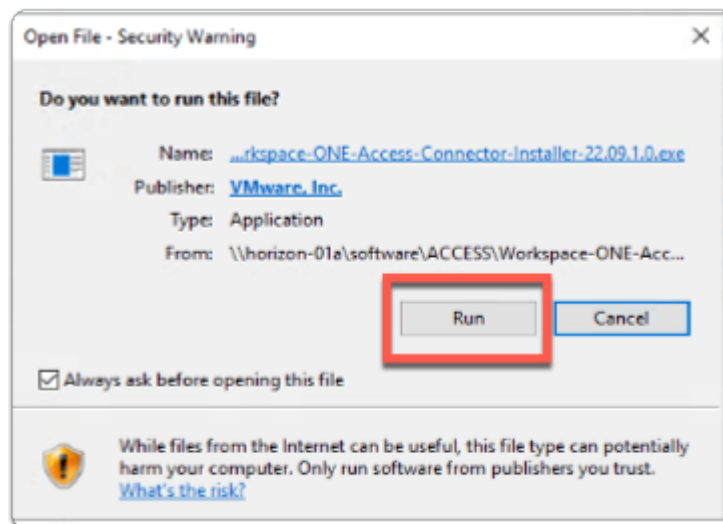


1. On your ControlCenter server
  - On the Desktop.
    - Open the **Remote Desktops\Site1** folder
    - Select and launch the **WS1-Connector.RDP** shortcut



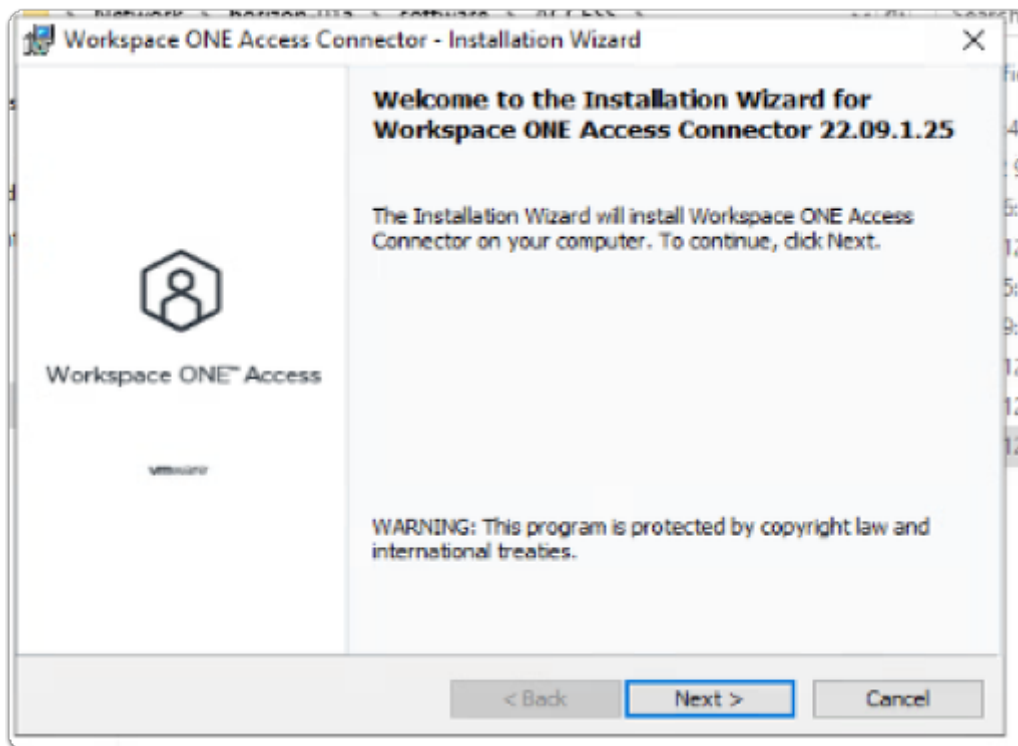
2. On your WS1-Connector server

- Open the **Software** Folder
- Select the **ACCESS** Folder
- Select and Launch
  - **Workspace-ONE-Access-Connector-Installer-22.09.1.0.exe**

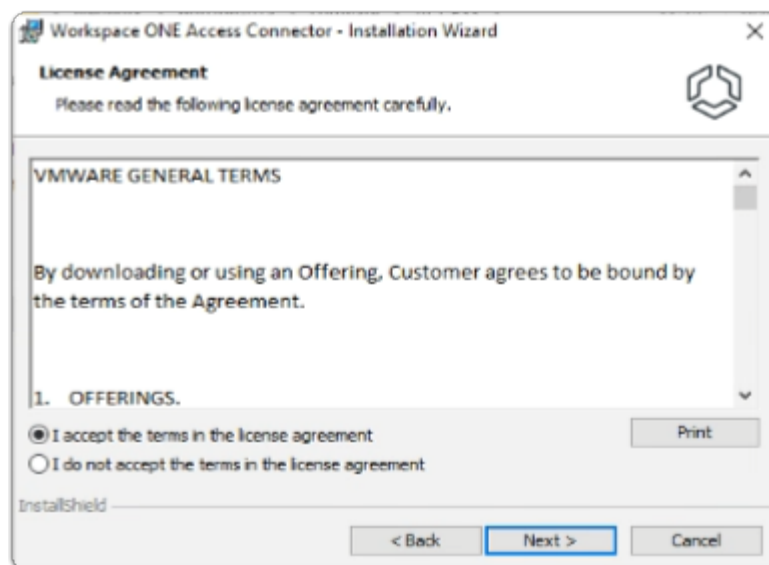


3. On your **WS1-Connector** server

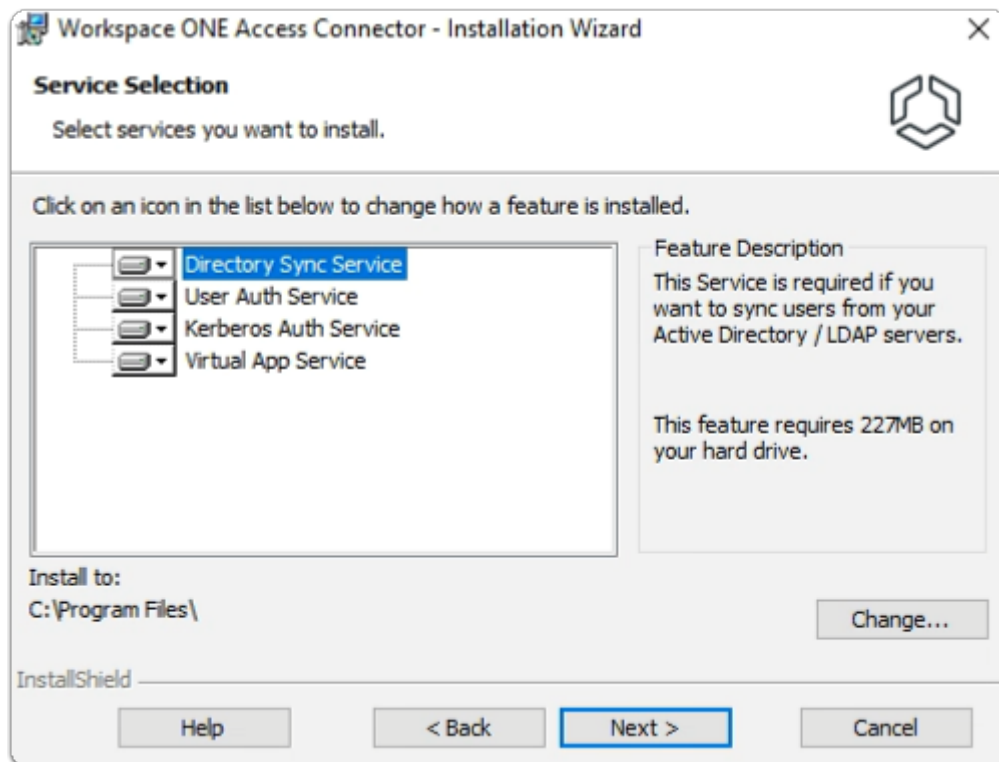
- On the **Open File - Security Warning** window
  - Select **Run**



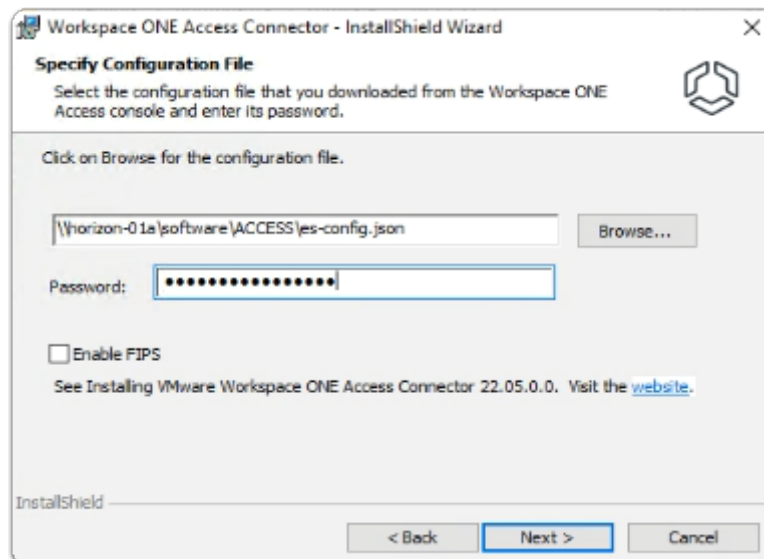
4. On the **Workspace ONE Access Connector - InstallShield** Wizard
  - In the **Welcome to the Installation Wizard for Workspace ONE Access Connector 22.09.0.0**
    - Select **Next**



5. On the **Workspace ONE Access Connector - InstallShield** Wizard
  - **Licence Agreement** window
    - Select the **radio button** next to:-
      - **I accept the terms in the license agreement**
    - Select **Next**

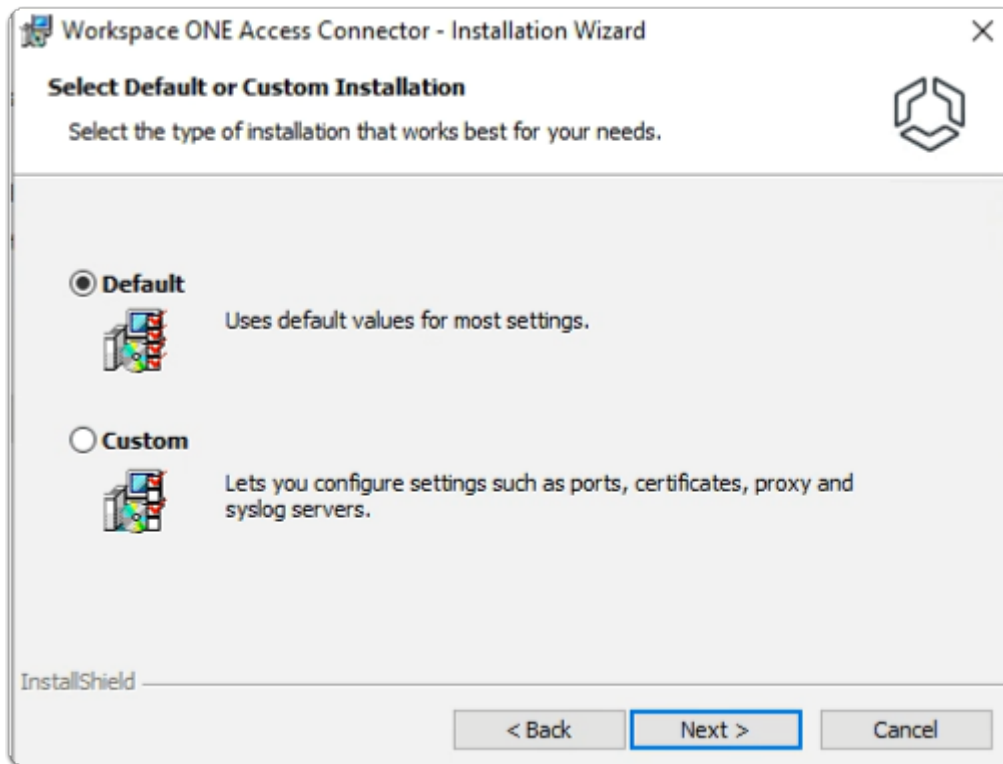


6. On the **Workspace ONE Access Connector - InstallShield Wizard**
  - **Service Selection** window
    - Select **Next**

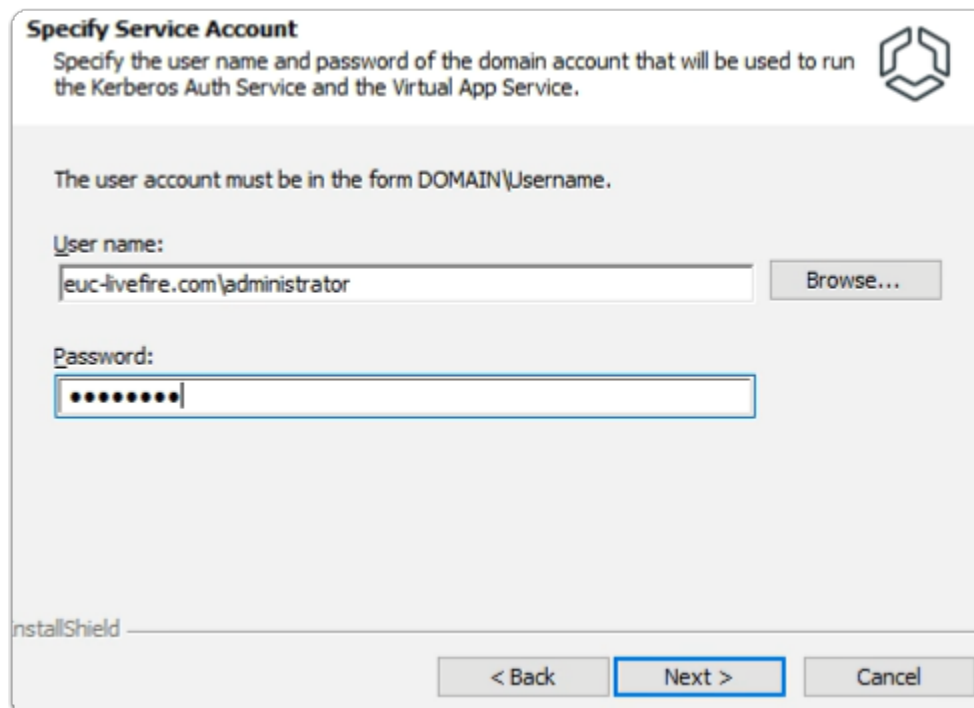


7. On the **Workspace ONE Access Connector - InstallShield Wizard**
  - **Specify Configuration File** window
    - In the box in front of **Browse...**
      - type **\\horizon-01a\software\ACCESS\es-config.json**
    - Next to **Password:** type **VMware1!VMware1!**
  - Select **Next**



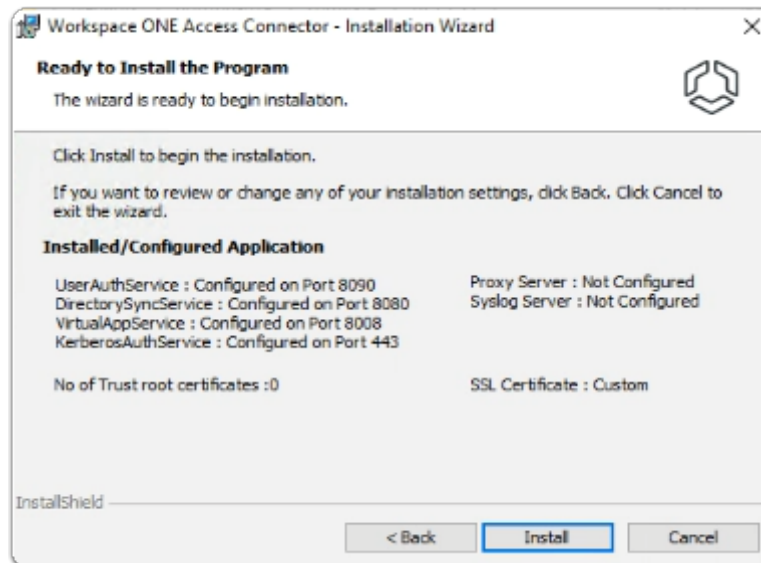


8. In the **Workspace ONE Access Connector - InstallShield** Wizard
- keep **Default**
  - select **Next**



9. In the **Workspace ONE Access Connector - InstallShield** Wizard
- **Specify Service Account** window
  - Under User name: type

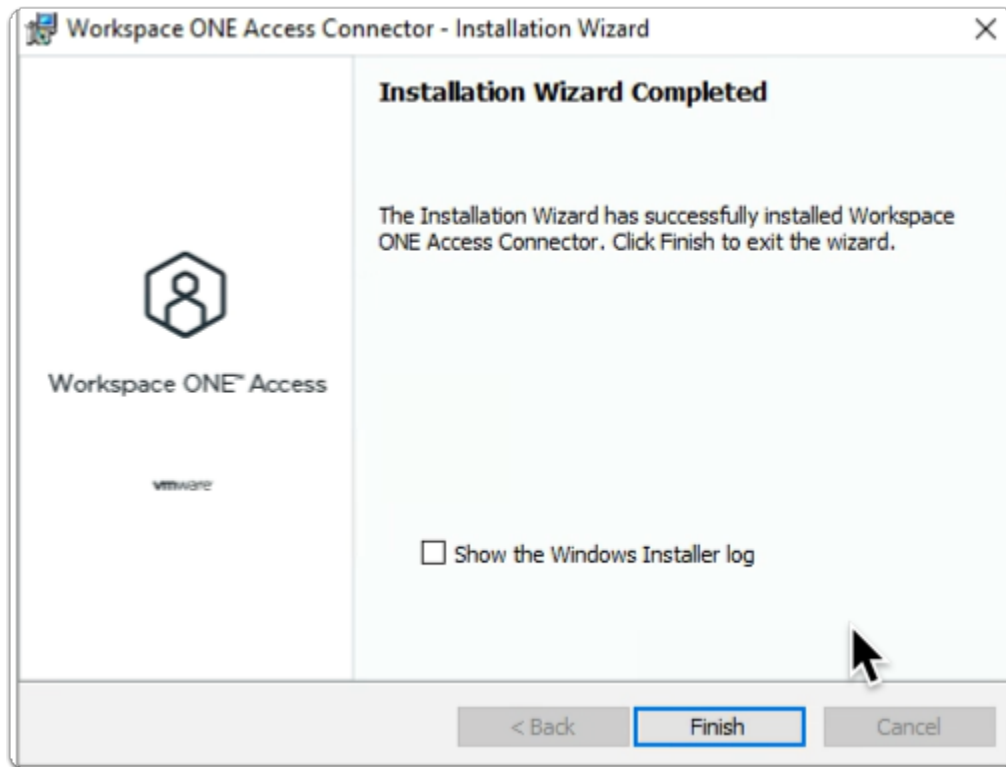
- [euc-livefire.com/administrator](https://euc-livefire.com/administrator)
- Under **Password:**
  - type **VMware1!**
- Select **Next**



10. In the **Workspace ONE Access Connector - InstallShield** Wizard

- **Ready to Install** window
  - Select **Install**

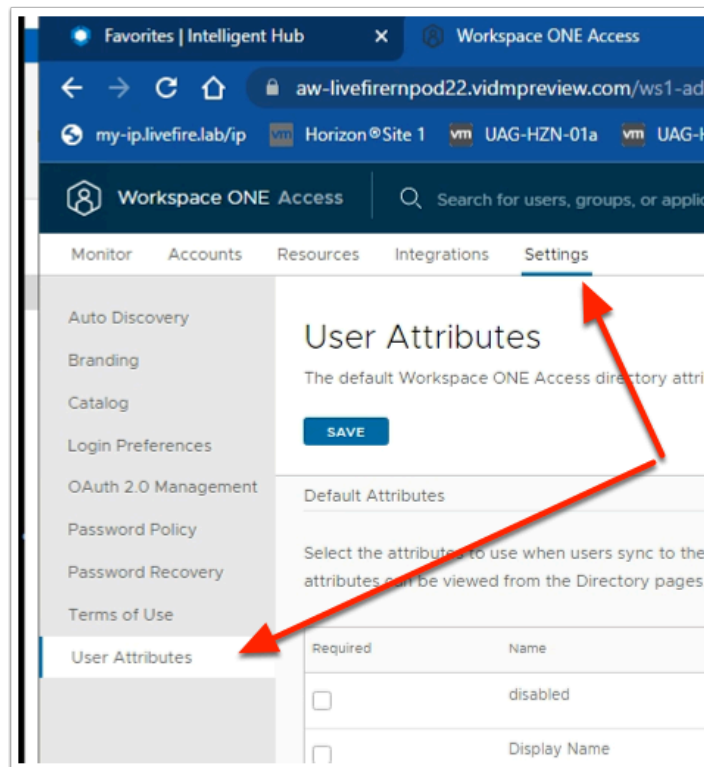
💡 The Installation of the Workspace ONE Access Connector will take about 10 minutes to complete. Continue with Part 5 while the installation is going. Check back periodically to ensure it has successfully installed.



11. In the **Workspace ONE Access Connector - InstallShield** Wizard
  - **Installation Wizard Completed** window
    - Select **Finish**

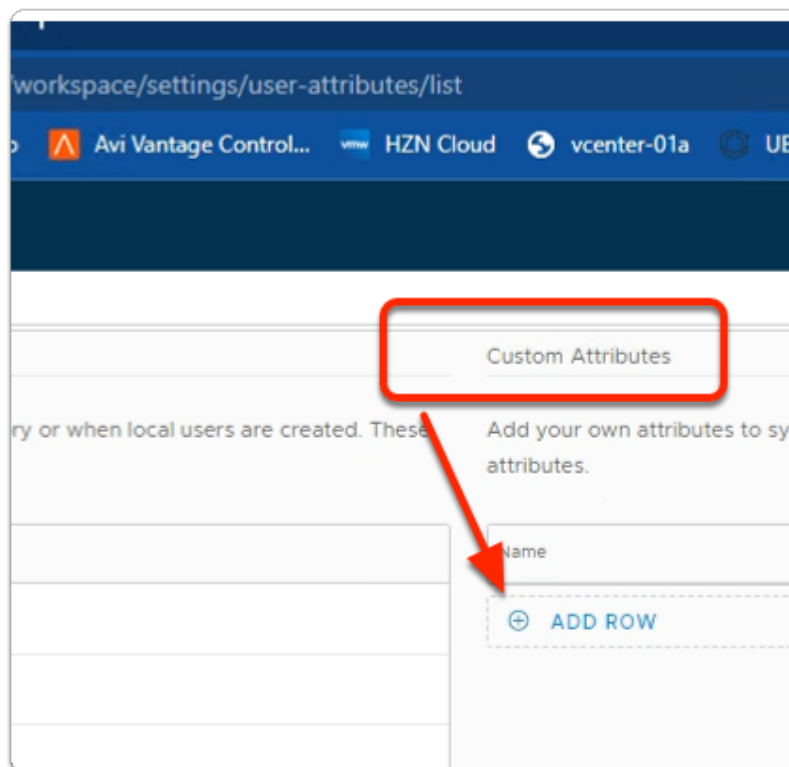
## Part 5: Configuring Directory Sync with Workspace ONE Access connector

- i First we will configure the Attributes. Note! Every organisation will need to research their requirements when deciding whether or not to set attributes to **required**. For specific applications where this needs to be considered, if the associated user object does not have the attribute, authentication might fail.



1. In the Workspace ONE Access Admin console

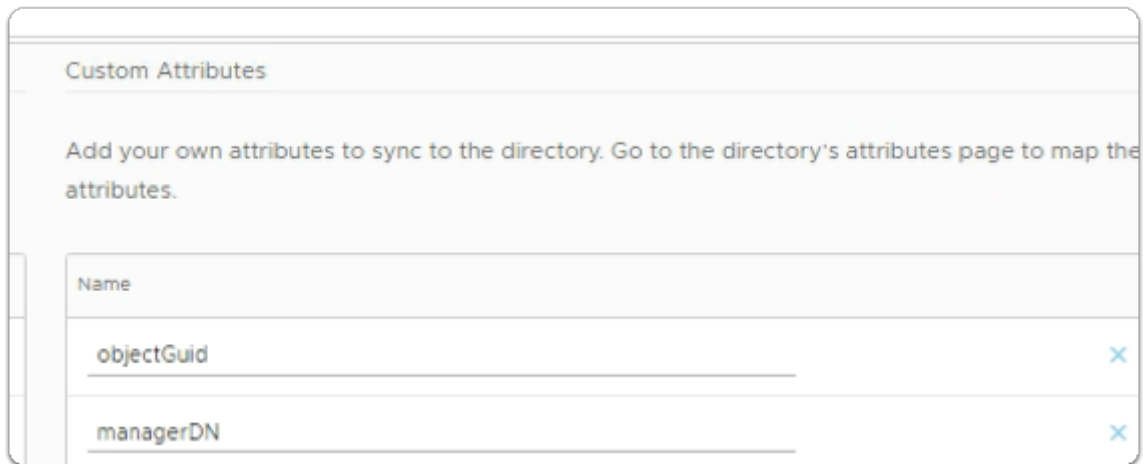
- Select **Settings**
- Select **User Attributes**



2. In the **User Attributes** console

- In the right area under **Custom Attributes**

- Select **⊕ ADD ROW** 2 times



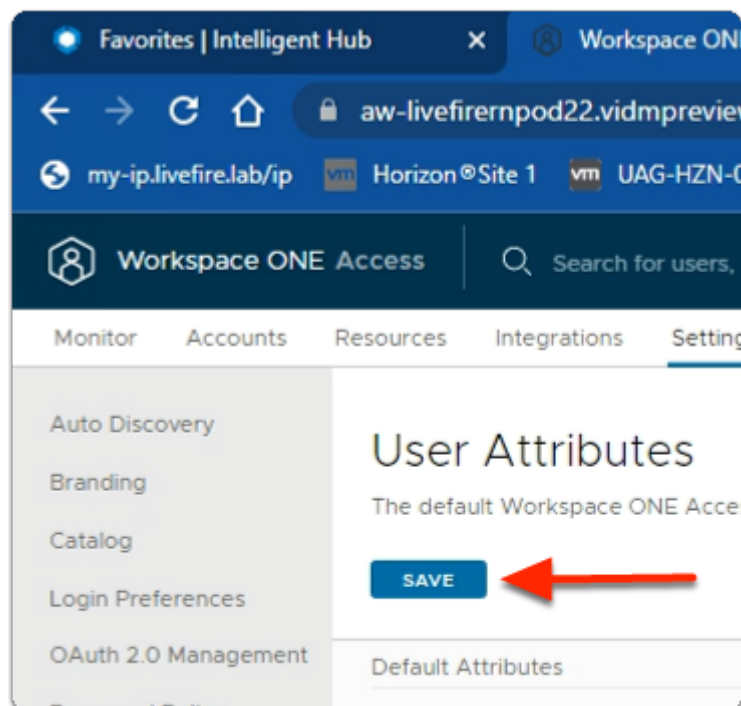
Custom Attributes

Add your own attributes to sync to the directory. Go to the directory's attributes page to map the attributes.

Name	
objectGuid	<span>×</span>
managerDN	<span>×</span>

3. In the **User Attributes** console

- Under **Name**
  - Add the following additional attributes
    - note this is case sensitive :
- **objectGuid**
- **managerDN**



Workspace ONE Access

Monitor Accounts Resources Integrations Settings

User Attributes

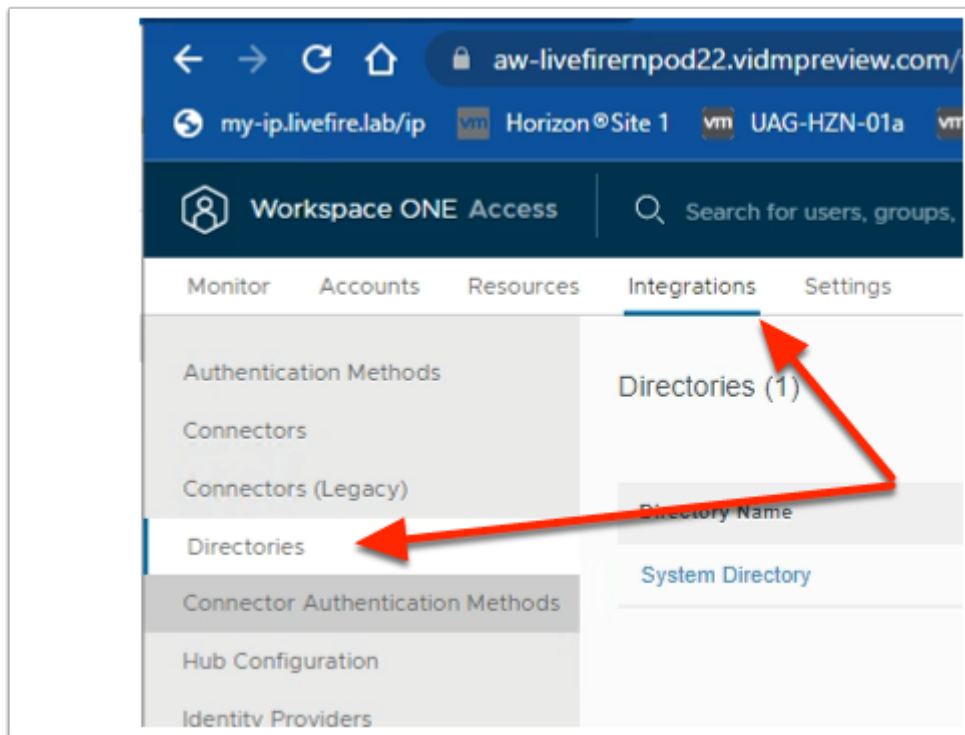
The default Workspace ONE Access

**SAVE**

Default Attributes

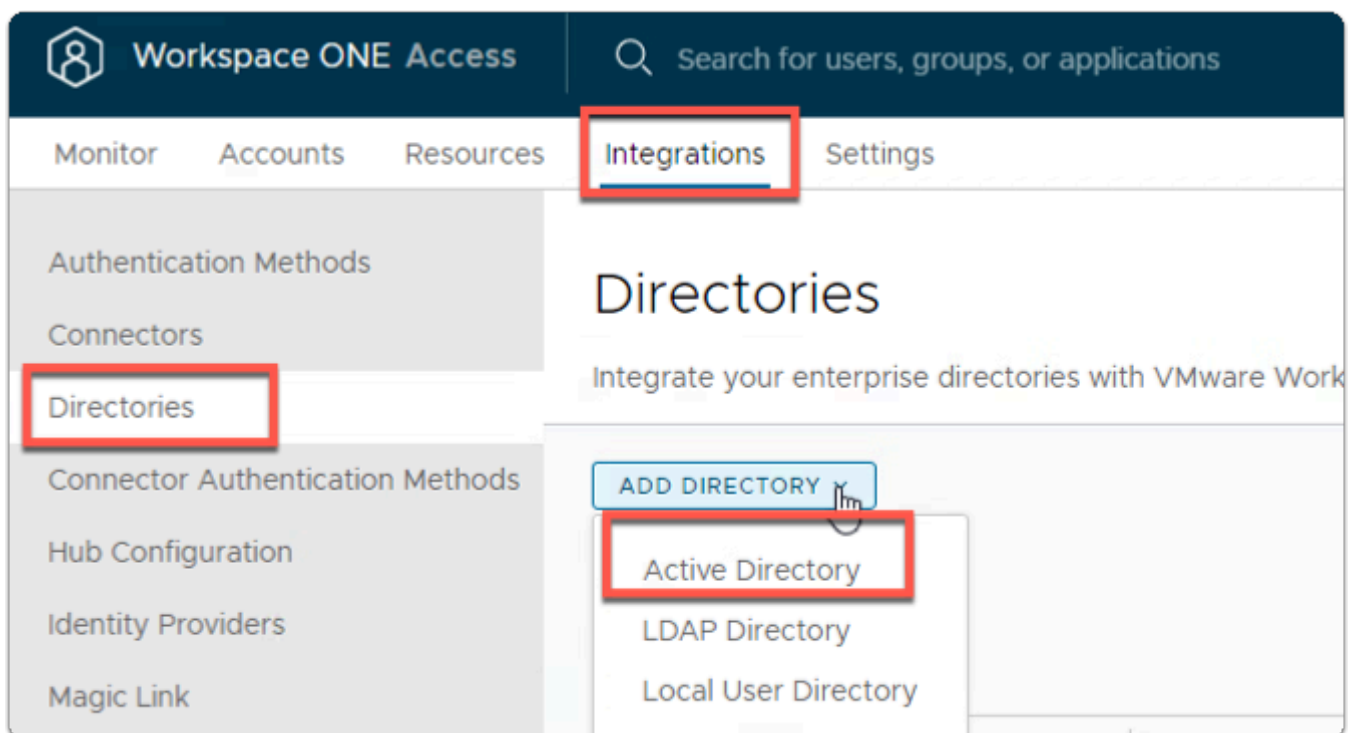
4. In the **User Attributes** console

- Under **User Attributes**
- Select **SAVE**



5. In the **Workspace ONE Access** admin console.

- Select **Integrations**,
- Select **Directories**



6. In the **Directories** area

- To the right
- Select **Add Directory**

- In the **Add Directory** dropdown
  - Select **Active Directory**

7. In the **Add Active Directory** Page,

- Under Directory Information
  - **Directory Name:** type **EUC-Livfire**
  - Ensure the **Active Directory over LDAP** radio button is selected
  - Click **NEXT**

8. In the **Configure Directory** section,

- Leave the **Directory Sync and Authentication** as default
- In the **Bind User Details** area
  - Enter the following Next to :
    - **Base DN:** **dc=EUC-Livfire,dc=com**

- **Bind DN:** **cn=admin,ou=corp,dc=EUC-Livefire,dc=com**
- **Bind DN Password:** **VMware1!**
- Select **Save**

3. Select Domain(s)

Select at least one domain.

Domains

☒ euc-livefire.com

**SAVE**

9. In the **Select the Domains** page,
- **euc-livefire.com** (EUC-LIVEFIRE)
  - Select **Save**.

Map the Workspace ONE Access attributes to Active Directory attributes. To manage the list of required attributes or to add attributes that are not listed, click the plus icon in the top right corner.

Attribute Name in VMware Workspace ONE Access	Attribute Name in Active Directory
employeeID	employeeID
managerDN	manager
Employee Manager ID	Custom Value
NickName	Custom Value
objectGuid	objectGUID
Employee organization ID	Custom Value
Phone	telephoneNumber
Profile of an user	Custom Value

**SAVE**

5. Sync groups

10. On the **Map User Attribute** page
- Map the following attributes :
  - (what you enter here is case sensitive)
  - **managerDN** select **custom input** and type **manager**
    - **Scroll down** next to:-
      - **objectGuid:** select **objectGUID**
  - Click **SAVE**



Directories > Add Active Directory

Connectors  
Connectors (Legacy)  
Directories  
Connector Authentication Methods  
Hub Configuration  
Identity Providers  
Magic Link  
Okta Catalog  
People Search  
UEM Integration

> ☒ Directory Information  
> ☒ Configure Directory  
> ☒ Select Domain(s)  
> ☒ Map User Attributes  
5. Sync groups

Select the groups you want to sync

Enter the top-level group that you would like to use as a filter. Click the Select Groups button to apply your filters, and select specific groups to sync to the directory.

Sync nested group members ☒

**+ ADD**

Top-level group name	Groups to sync	Actions

Create Group

Give a name to the top-level group

Name

**CANCEL** **ADD**

11. On the **Select the Groups you want to sync** page,
  1. Click the **+ADD**
  2. Under **Create Group**
    - enter **dc=euc-livewire,dc=com**
  3. Click **ADD**

5. Sync groups

Select the groups you want to sync

Enter the top-level group that you would like to use as a filter. Click the Select Groups button to apply your filters, and select specific groups to sync to the directory.

Sync nested group members ☒

**+ ADD**

Top-level group name	Groups to sync	Actions
dc=euc-livewire,dc=com	All <input checked="" type="checkbox"/> Select all <b>SELECT GROUPS</b>	

Top-level Group(s) per page 10 1 Top-level Group(s)

Mapped Group Results

Group DN	Mapped Group(s)
dc=euc-livewire,dc=com	All groups in this DN are selected

Mapped Group(s) Results per page 10 1 Mapped Group(s) Result

**SAVE**

12. On the **Select the Groups you want to sync** page,
- Under Select All
    - Select the **check box**
  - Select **Save**.

6. Sync users

Select the users you want to sync

Enter the User DNs to sync, for example, CN=Users,DC=example,DC=com. All users found under the DN are also synced. To use LDAP filters with the DNs, append a semicolon to the DN, then enter the filter, for example, CN=Users,DC=sales,DC=example,DC=com;(&(objectClass=User)(objectCategory=Person)(UserAccountControl=512)). To exclude any users from syncing, provide exclusion filters.

+ ADD

Specify the user DNs	Verify	Action(s)
ou=corp,dc=EUC-Livefire,dc=com	TEST	

User Dn(s) per page 10 1 User Dn(s)

Filters to exclude users

+ ADD

13. In the **Select Users you would like to sync** window
- Under **Specify the user DNs**
    - edit the existing syntax so that it reads
      - **ou=corp,dc=EUC-Livefire,dc=com**
  - Select **Save**

> ✓ Sync groups

> ✓ Sync users

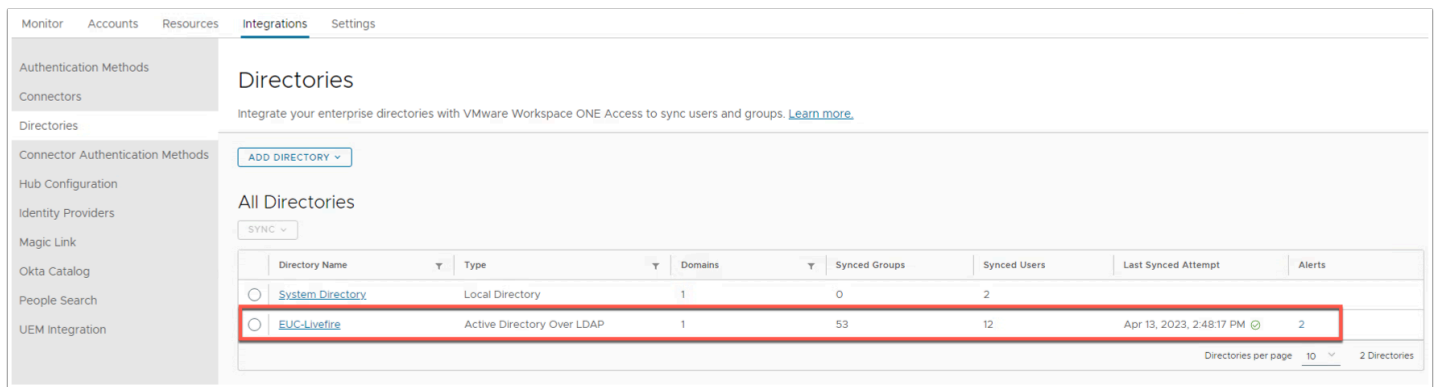
7. Sync Frequency

Sync Frequency Every hour

SAVE SAVE & SYNC

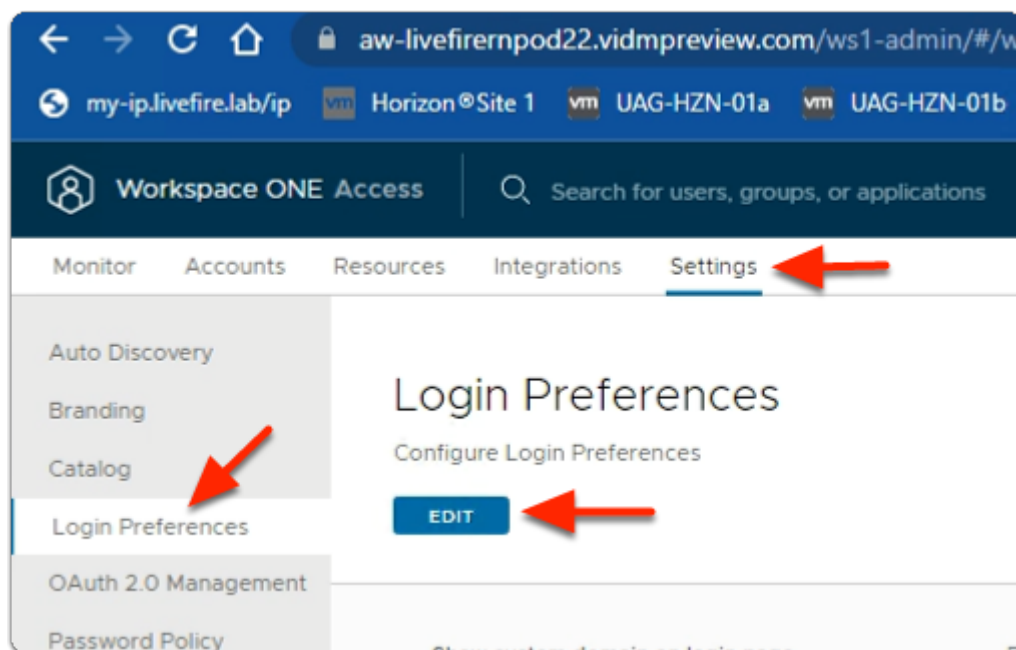
14. On the **Sync Frequency** window
- On Change the **Sync Frequency** to **Every hour**

- Click **SAVE & SYNC**



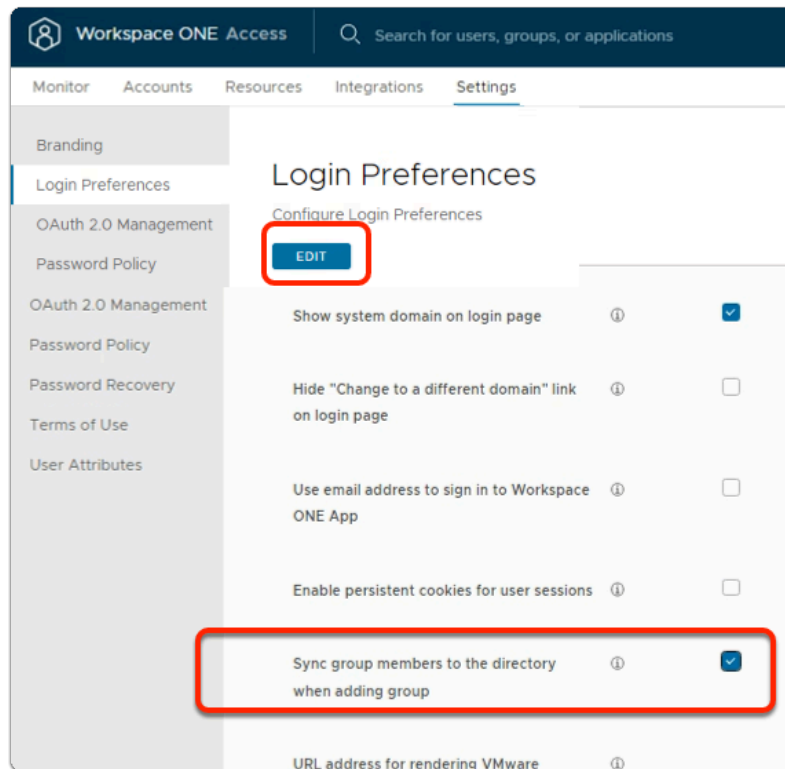
15. On the **Directories** window

- **Refresh** your browser window
- Note the **Synced Groups** and **Synced Users**



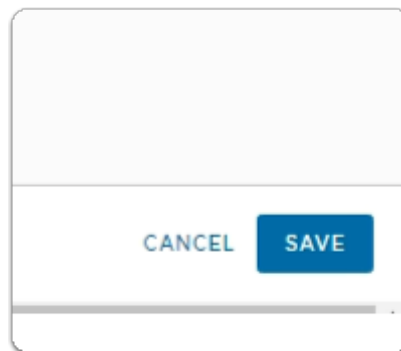
16. In your **Workspace ONE Access admin** console

- Select **Settings**
- Select **Login Preferences**
- Under **Login Preferences**
  - Select **EDIT**



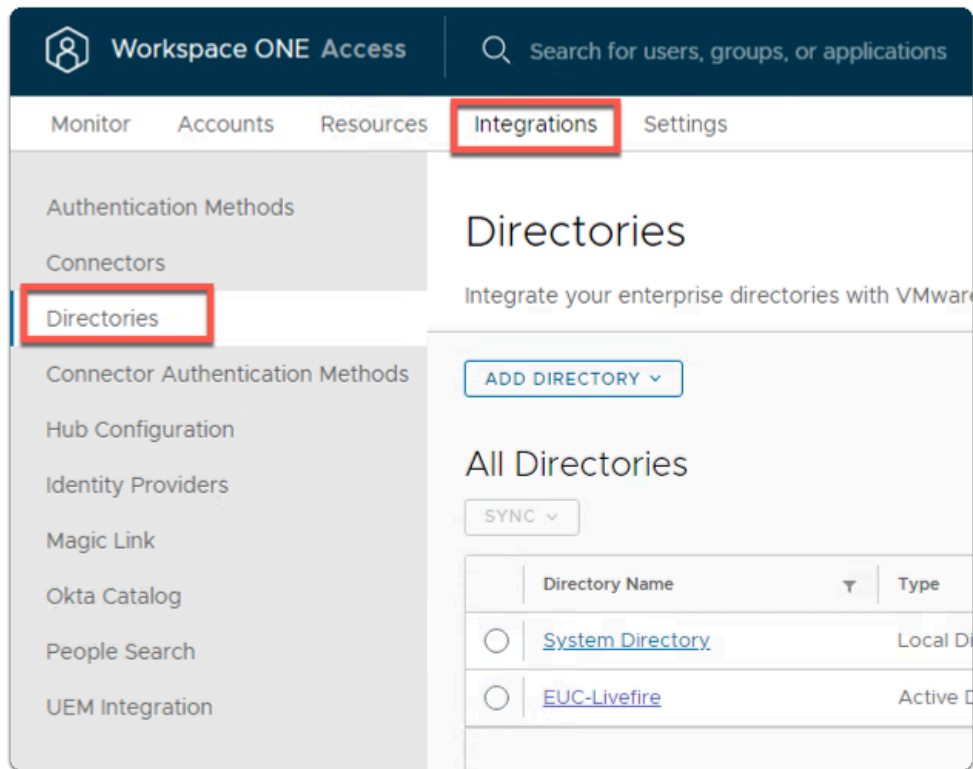
17. In the **Login Preferences** area

- **In line with:**
  - **Sync Group Members to the Directory When Adding Group**
    - select the **Checkbox**



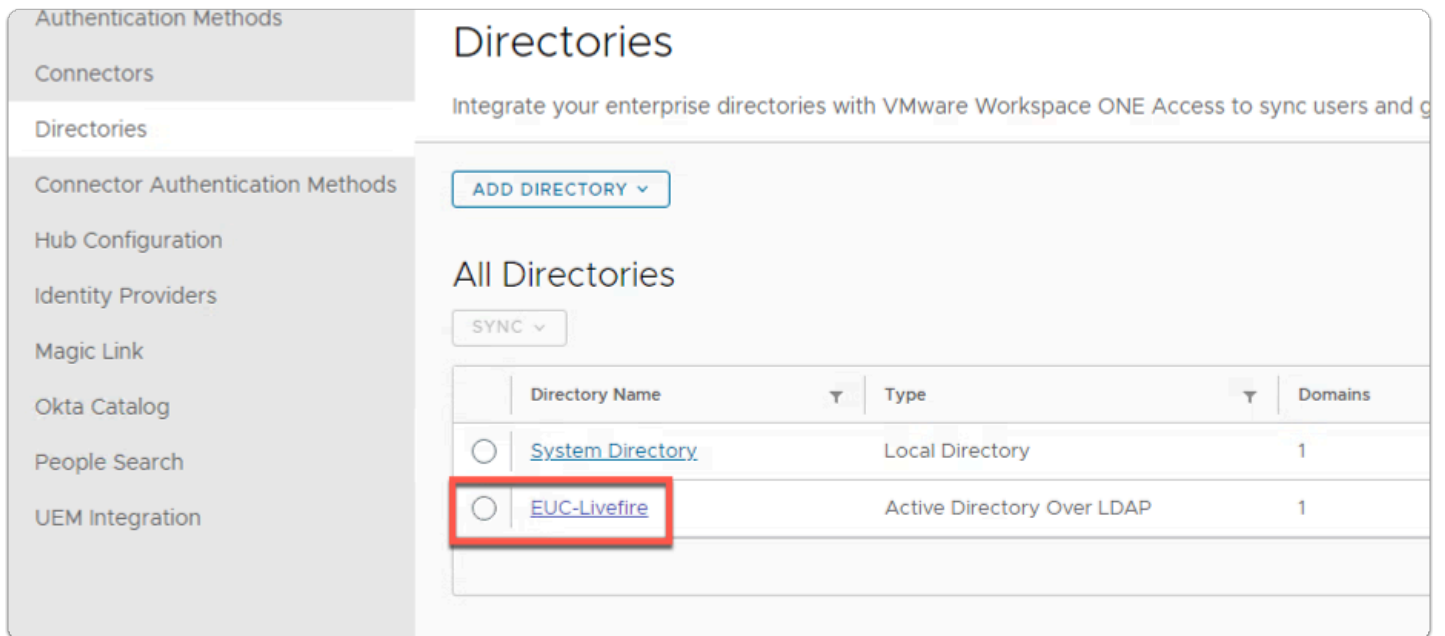
18. In the **Login Preferences** area

- In the bottom right
  - select **SAVE**



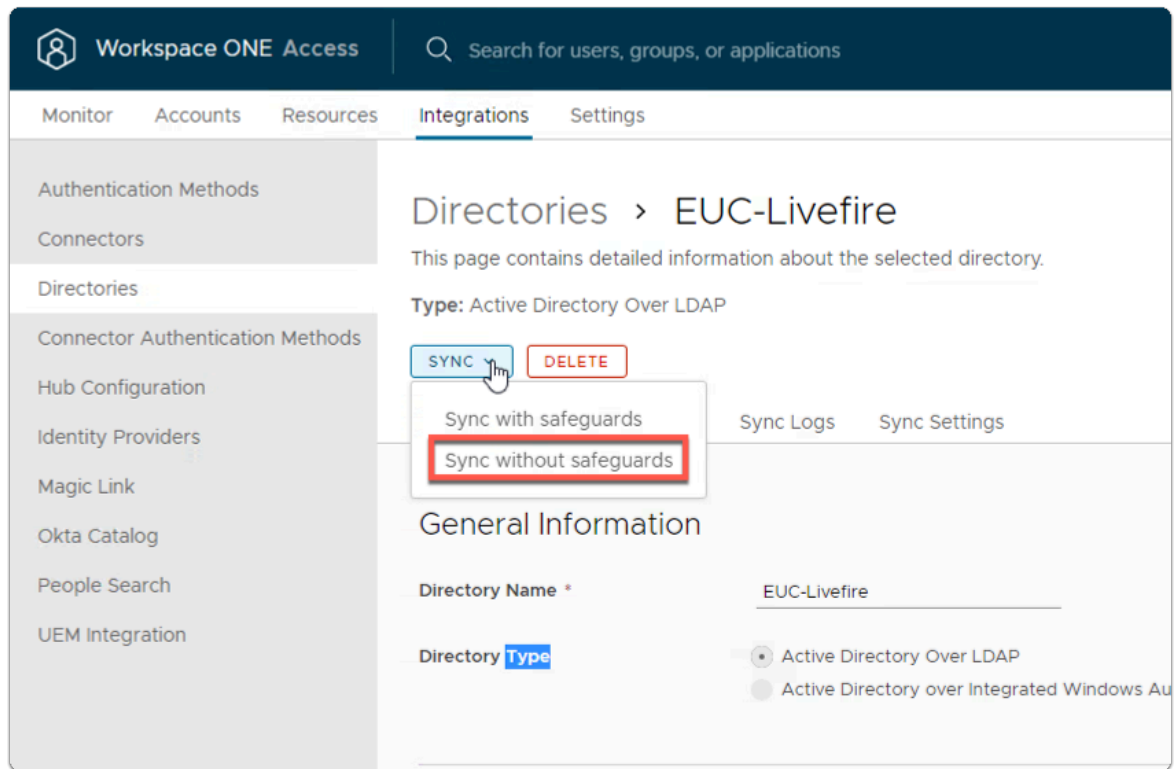
19. In the **Workspace ONE Access** console

- select **Integrations**
- select **Directories**



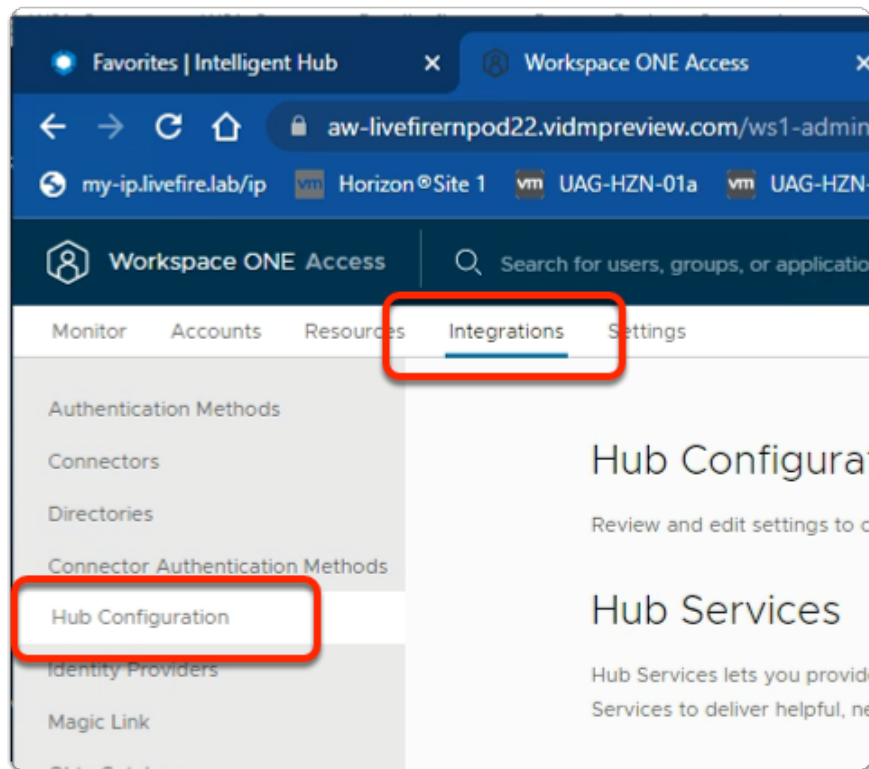
20. In the **Directories** area

- select **EUC-Livefire**

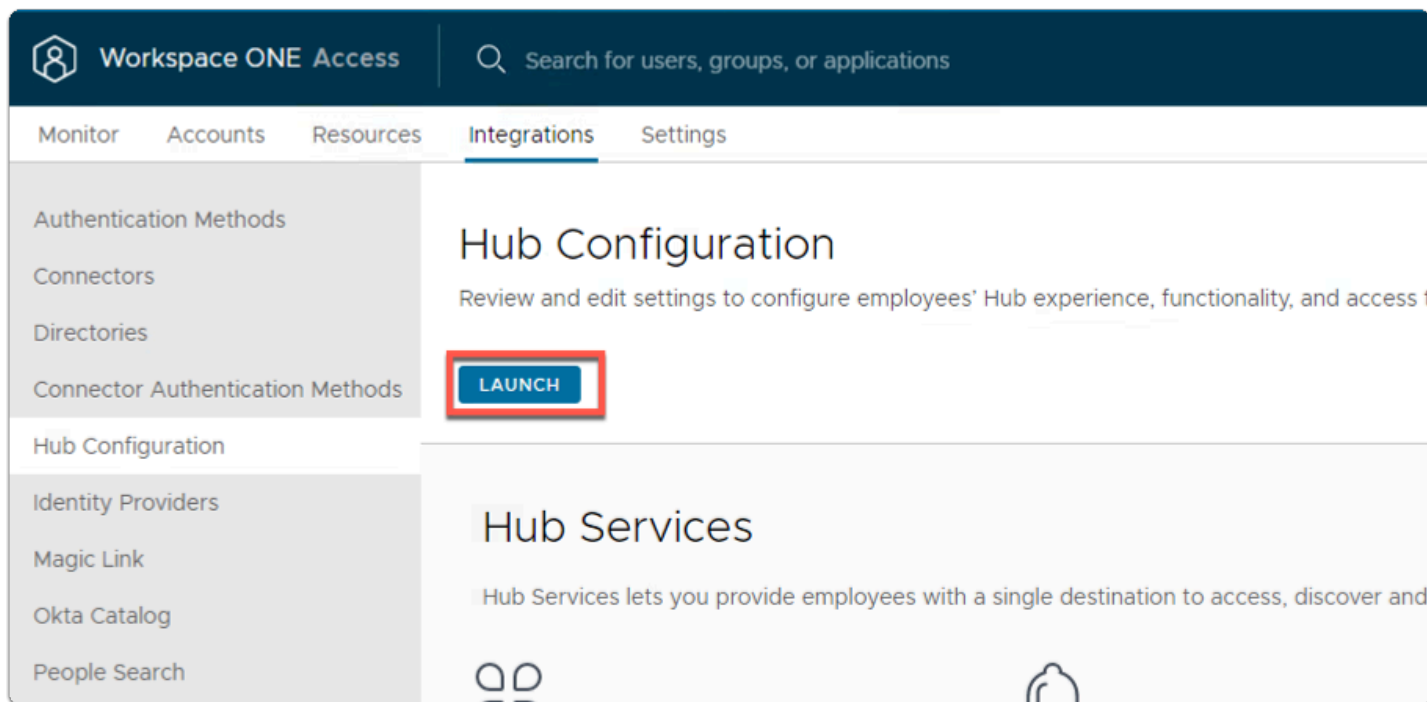


21. In the **EUC-Livefire** directory area
- In the right corner
    - Next to **Sync**
      - select the **dropdown**
        - select **Sync without Safeguards**

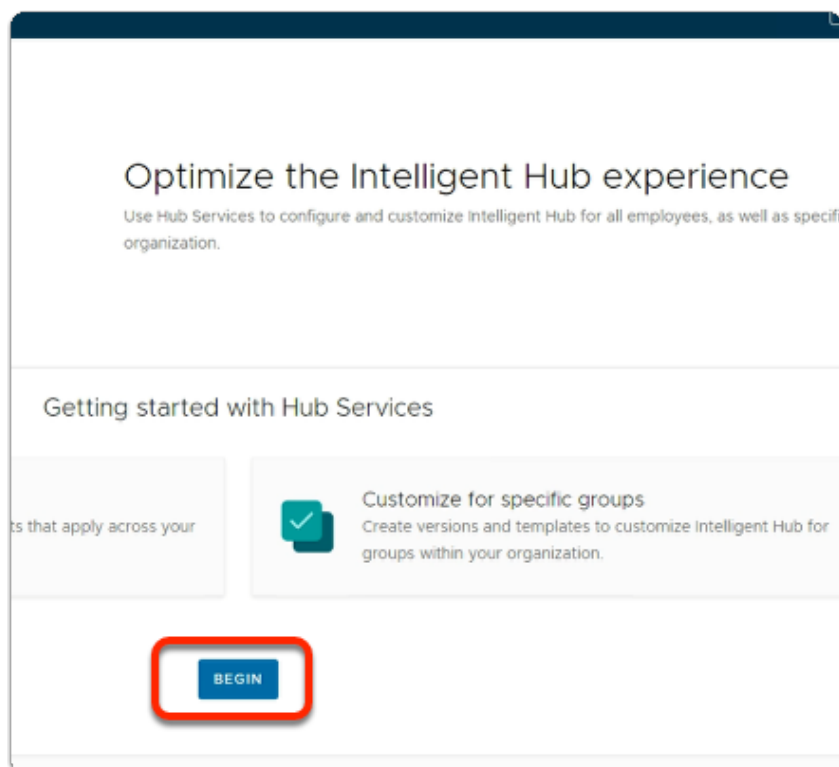
## Part 6: Workspace ONE Hub Services Integration with Workspace ONE Access



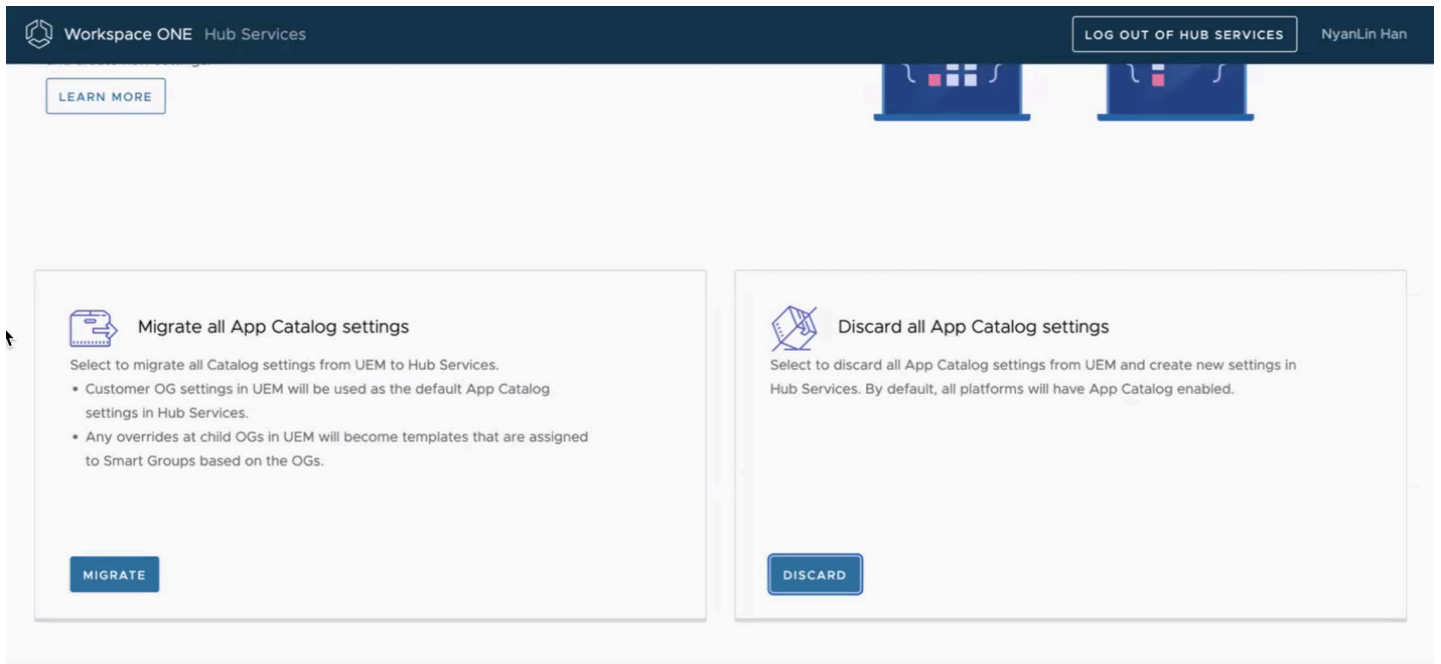
1. In the **Workspace ONE Access admin** console
  - Select **Integrations**
  - Select **Hub Configuration**



2. In the **Hub Configuration** window
  - Under **Hub Services**
  - Select **LAUNCH**

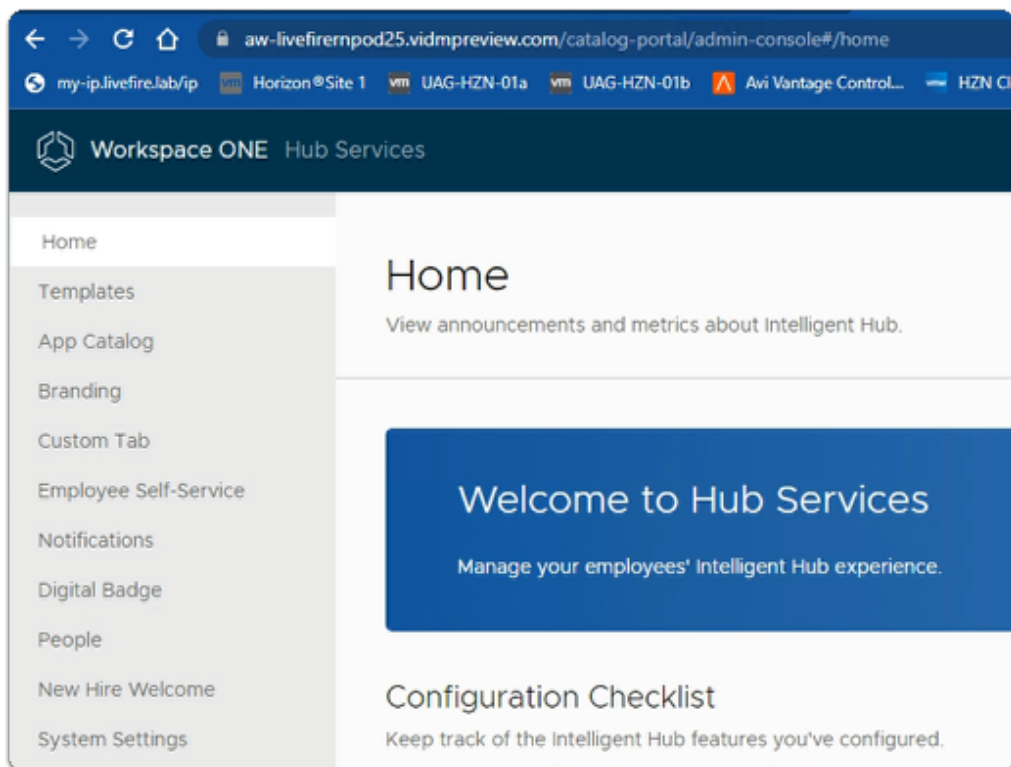






3. In the **Optimize the Intelligent Hub Experience** window

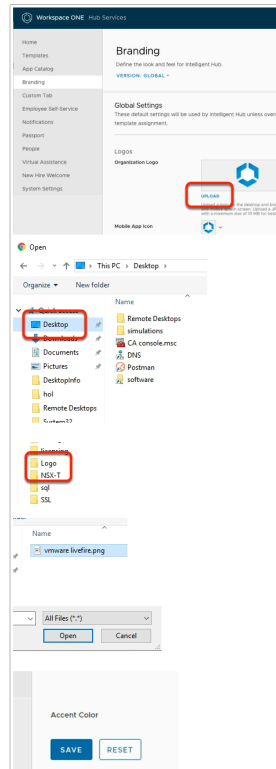
- Select **BEGIN**
- If you get a choice select **DISCARD**



4. In the **Welcome to Hub Services**

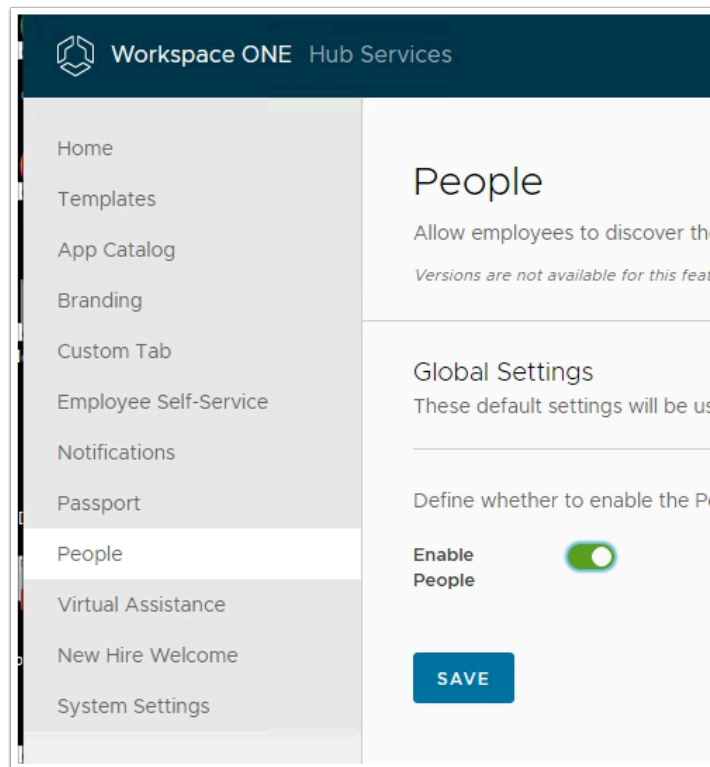
- Review the associated options.
- In Section 7: We will configure Hub Services

# Part 7: Configuring Workspace ONE Hub Services

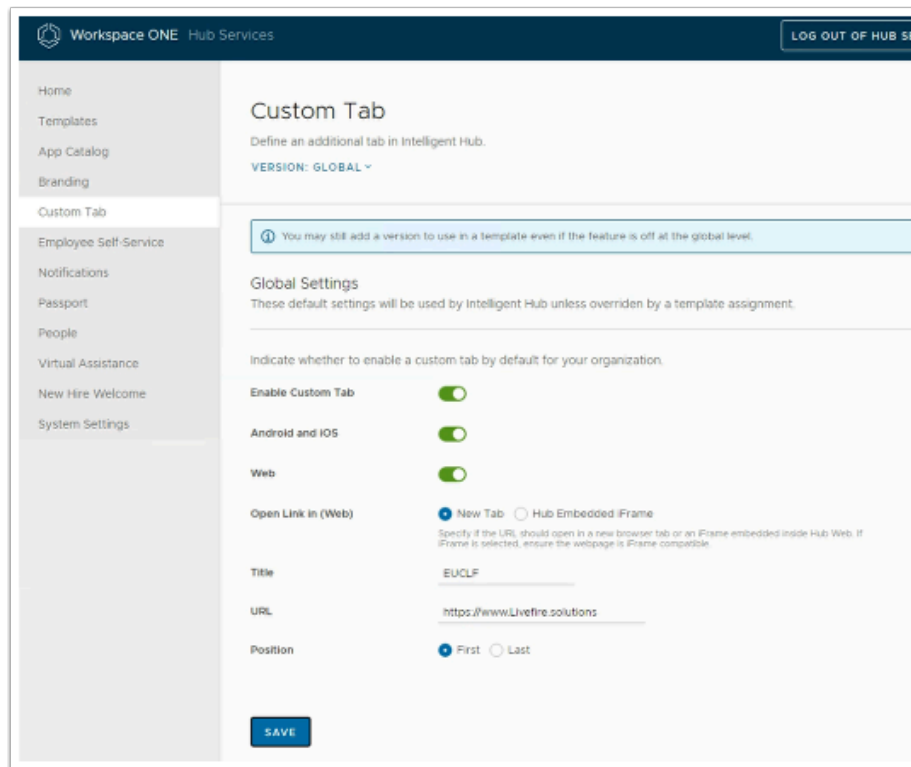


## 1. In **Workspace ONE Hub Services**

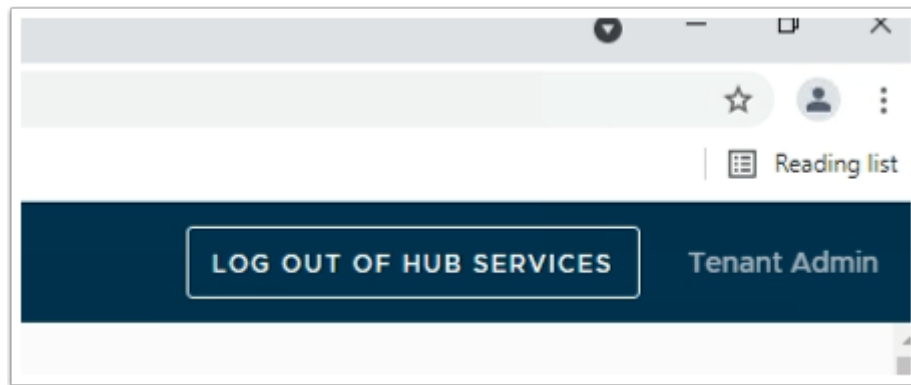
- Select the **Branding** section
  - Find **Logos > Organization Logo** , to the right select **UPLOAD**
- In the left pane,
  - Under **Quick access**, select **Desktop**
  - Select **Software**
  - Select and open **Logo**
  - Select **vmware livefire.png**
  - Select **Open**
  - **Scroll down**
    - and select **SAVE**



2. In the **Workspace ONE Hub Services** page
  - In the left pane, select **People**
  - Under **People** area,
    - next to **Enable People**,
    - move the **toggle** to the right
  - Select **SAVE**



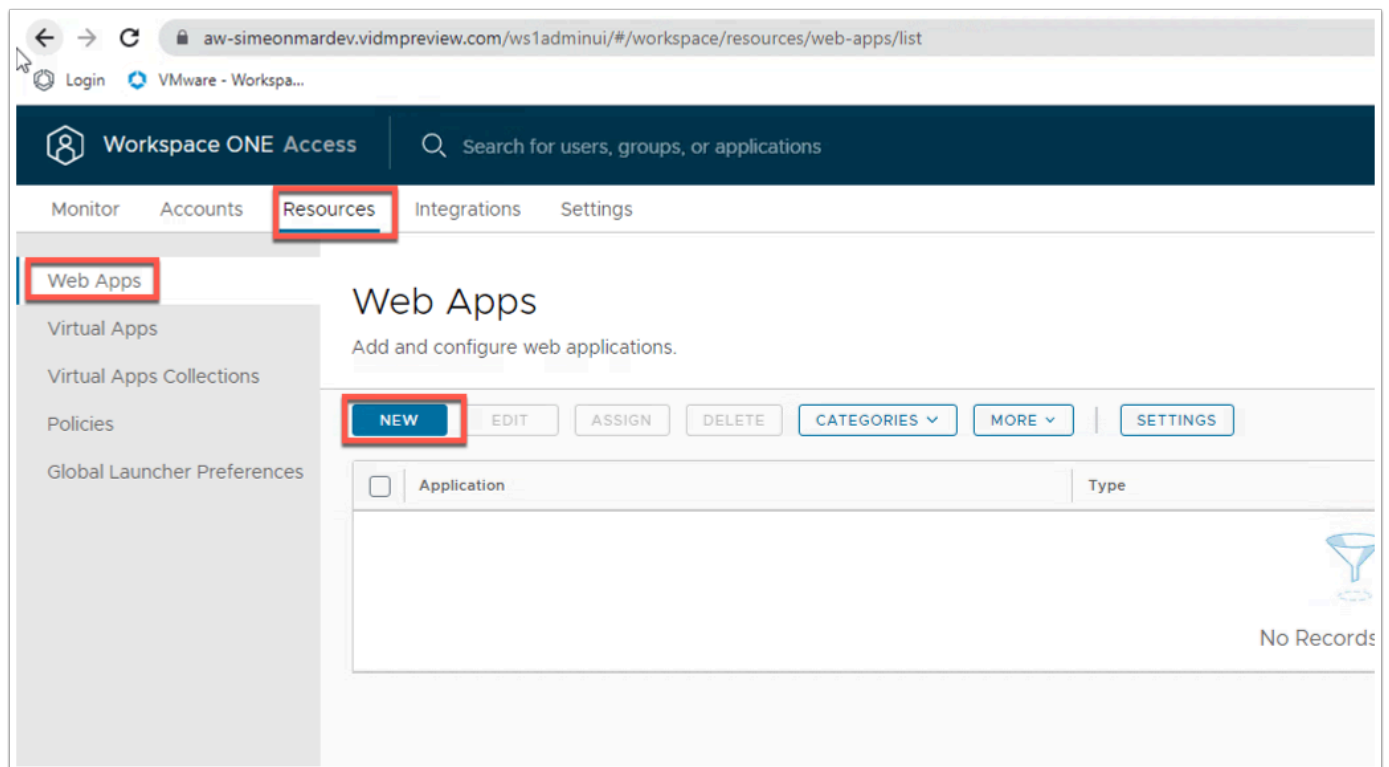
3. In the **Workspace ONE Hub Services** page
  - From the **left menu**,
    - **Select the Custom Tab.**
      - Next to **Enable Custom Tab**,
        - move the **toggle right**.
      - Next to **Web**
        - move the **toggle right**.
      - Next to **Title**
        - enter: **EUCLF** (Best practice is not use a label longer than 6 characters).
      - Next to **URL**:
        - enter **https://www.Livefire.solutions**
      - Next to **Position**,
        - enable the **First radio button**.
    - Select **SAVE**



4. To the top right of the **Workspace ONE Hub Services** page
  - Select **LOG OUT OF HUB SERVICES**

## Part 8: User Provisioning to UEM

Organizations can leverage the provisioning adapter in WorkspaceONE Access to provision users into Workspace ONE UEM. This implementation does not require the AirWatch Cloud Connector and will leverage SAML JIT to create users in UEM during the enrollment process.



2. In the Workspace ONE Access admin console navigate to **Resources** > **Web Apps** > **NEW**

**New SaaS Application**

1 Definition  
2 Configuration  
3 Access Policies  
4 Summary

**Definition**

Search ⓘ

**OR BROWSE FROM CATALOG**

Name ⓘ

Description ⓘ

Icon ⓘ

**SELECT FILE...**

3. Click on **OR BROWSE FROM CATALOG**

**< DEFINITION**

3 Application(s)

Application	Description	Type	Status
AirWatch	AirWatch Mobile Device Management	SAML 2.0	+
AirWatch Admin		SAML 2.0	+
AirWatch Provisioning	AirWatch Provisioning App	SAML 2.0	+

Available to Add 1 of 3 items

**New SaaS Application**

1 Definition  
2 Configuration  
3 Access Policies  
4 Summary

**Definition**

Search ⓘ  
AirWatch Provisioning

**OR BROWSE FROM CATALOG**

Name ⓘ  
AirWatch Provisioning

Description ⓘ  
AirWatch Provisioning App

Icon ⓘ

**SELECT FILE...**

**CANCEL NEXT**

4. Search for **AirWatch** and click on the **+** Next to AirWatch Provisioning. Click **NEXT** after your return to the New SaaS Application page.

NOTE: Ensure you are not selecting the AirWatch without the Provisioning.

**Edit SaaS Application**

- 1 Definition
- 2 Configuration**
- 3 Access Policies
- 4 Provisioning
- 5 User Provisioning
- 6 Group Provisioning
- 7 Summary

### Single Sign-On

**Authentication Type \*** ⓘ  
SAML 2.0

**Configuration \*** ⓘ  
☐ URL/XML ☒ Manual

**Single Sign-On URL \*** ⓘ  
https://dw-livefire.awmdm.com/identityService/SAML/AssertionService.ashx?binding=HttpPost

**Recipient URL \*** ⓘ  
https://dw-livefire.awmdm.com/identityService/SAML/AssertionService.ashx?binding=HttpPost

**Application ID \*** ⓘ  
donotchange

**Username Format \*** ⓘ  
Unspecified

**Username Value** ⓘ  
\${user.userName}

- Change the **Single Sign-On URL** and **Recipient URL** to match [dw-livefire.awmdm.com](https://dw-livefire.awmdm.com) (leave what comes after the URL there) and click **NEXT**

**New SaaS Application**

- 1 Definition
- 2 Configuration
- 3 Access Policies**
- 4 Summary

### Access Policies

Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.

default\_access\_policy\_set

CANCEL BACK **NEXT**

- Click **NEXT** on the **Access Policies**

New SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Summary

Configuration

Manual

Single Sign-On URL

https://www.dw-livefire.awmdm.com/identityService/SAML/AssertionService.ashx?binding=HttpPost

Recipient URL

https://www.dw-livefire.awmdm.com/identityService/SAML/AssertionService.ashx?binding=HttpPost

Application ID

donotchange

Username Format

Unspecified

Username Value

\$(user.userName)

Relay State URL

—

ADVANCED PROPERTIES

Access Policies

Access Policy

Open in Workspace ONE Web

No

CANCEL

BACK

SAVE & ASSIGN

SAVE

7. Click **SAVE**

MonitorAccountsResourcesIntegrationsSettings

Web Apps

Virtual Apps

Virtual Apps Collections

Policies

Global Launcher Preferences

Web Apps

Add and configure web applications.

NEW

EDIT

ASSIGN

DELETE

CATEGORIES

MORE

SETTINGS

<input checked="" type="checkbox"/>	Application	Type
<input checked="" type="checkbox"/>	AirWatch Provisioning	SAML 2.0
<input checked="" type="checkbox"/>	1	

8. Now in the Web Apps screen select the application and clic **EDIT**



## Edit SaaS Application

1 Definition  
2 Configuration  
3 Access Policies  
**4 Provisioning**  
5 User Provisioning  
6 Group Provisioning  
7 Summary

### Provisioning Adapter Configuration

You can use the Provisioning Adapter for Workspace ONE UEM to automatically provision Workspace ONE UEM tenant from the VMware Workspace ONE Access service. Make sure the provisioning tool is enabled when you set up the Workspace ONE UEM provisioning adapter.

**Enable Certificate Auth** ⓘ

☒ Yes

**Workspace ONE UEM Group ID \***

simeonmar

TEST CONNECTION

**Enable Provisioning**

☐ No

9. In the **Edit SaaS Application** you will now see more options, click on Provisioning and change **Enable Certificate Auth** enter your UEM GroupID.
- Click **TEST CONNECTION**

## Edit SaaS Application

1 Definition  
2 Configuration  
3 Access Policies  
**4 Provisioning**  
5 User Provisioning  
6 Group Provisioning  
7 Summary

### Provisioning Adapter Configuration

You can use the Provisioning Adapter for Workspace ONE UEM to automatically provision users and groups in the Workspace ONE UEM tenant from the VMware Workspace ONE Access service. Make sure that no other account provisioning tool is enabled when you set up the Workspace ONE UEM provisioning adapter.

**Enable Certificate Auth** ⓘ

☒ Yes

**Workspace ONE UEM Group ID \***

simeonmar

TEST CONNECTION

**Enable Provisioning**

☒ Yes

CANCEL BACK **NEXT**

10. The connection should be successful and now ensure **Enable Provisioning** is ticked and click **NEXT**.

Edit SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Provisioning

5 User Provisioning

6 Group Provisioning

7 Summary

User Provisioning

Select the attributes with which to provision users in Workspace ONE UEM. For example, the information sent from the VMware Workspace ONE Access service can be the user name, first name, last name, and email address. Attribute names with an asterisk are required for provisioning.

Attribute Name	Value
* User Name	\$(user.userName)
* First Name	\$(user.firstName)
* Last Name	\$(user.lastName)
* User Email	\$(user.email)
* User Principal Name	\$(user.userPrincipalName)
* External Id	\$(user.ExternalId)
User Domain	\$(user.domain)
Role	Full Access

⊕ ADD MAPPING

CANCEL

BACK

NEXT

11. Leave the **User Provisioning** values as default and click **NEXT**

Edit SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Provisioning

5 User Provisioning

6 Group Provisioning

7 Summary

Group Provisioning

Group provisioning creates corresponding security groups in Workspace ONE UEM. Note: Provisioning a group does not entitle members of the group to the application. To entitle Workspace ONE UEM to members of the group, go to the Assign page and add the group.

<input type="checkbox"/> Group Name	Group Mail Nickname	Status
<div>No groups found.</div>		

⊕ ADD GROUP

DEPROVISION

CANCEL

BACK

NEXT

12. On the **Group Provisioning** click **ADD GROUP**

Add Group to Provision

Group Name \*  
🔍 Developers@euc-liveware.com

Nickname \*  
Developers

CANCEL SAVE

13. Type **Developers@euc-liveware.com** and give it the nickname **Developers**. Click **SAVE**.

Edit SaaS Application

1 Definition  
2 Configuration  
3 Access Policies  
4 Provisioning  
5 User Provisioning  
6 Group Provisioning  
7 Summary

Group Provisioning

Group provisioning creates corresponding security groups in Workspace ONE UEM. Note: Provisioning a group does not entitle members of the group to the application. To entitle Workspace ONE UEM to members of the group, go to the Assign page and add the group.

<input type="checkbox"/>	Group Name	Group Mail Nickname	Status
<input type="checkbox"/>	Developers@euc-liveware.com	Developers	Ready to provision

① ADD GROUP

DEPROVISION

CANCEL BACK NEXT

14. Now click **ADD GROUP** again.

← GROUP PROVISIONING

## Add Group to Provision

Group Name \*

Q Sales@euc-livefire.com

Nickname \*

Sales

CANCEL SAVE

15. Type **Sales@euc-livefire.com** and give it the nickname **Sales**. Click **SAVE**
- Repeat the process for **Marketing** and **IT support**

## Edit SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Provisioning

5 User Provisioning

**6 Group Provisioning**

7 Summary

### Group Provisioning

Group provisioning creates corresponding security groups in Workspace ONE UEM. Note: Provisioning a group does not entitle members of the group to the application. To entitle Workspace ONE UEM to members of the group, go to the Assign page and add the group.

<input type="checkbox"/>	Group Name	Group Mail Nickname	Status
<input type="checkbox"/>	Sales@euc-livefire.com	Sales	Provisioned
<input type="checkbox"/>	Marketing@euc-livefire.com	Marketing	Provisioned
<input type="checkbox"/>	Developers@euc-livefire.com	Developers	Provisioned
<input type="checkbox"/>	IT Support@euc-livefire.com	IT	Provisioned

ADD GROUP

DEPROVISION

CANCEL BACK NEXT

16. Click **NEXT**.

Edit SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Provisioning

5 User Provisioning

6 Group Provisioning

7 Summary

Definition

Name

AirWatch Provisioning

Description

AirWatch Provisioning App

Icon

Categories

—

Configuration

Authentication Type

SAML 2.0

Configuration

Manual

Single Sign-On URL

https://www.dw-livefire.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost

Recipient URL

https://www.dw-livefire.awmdm.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost

CANCEL

BACK

SAVE & ASSIGN

SAVE

17. Click **SAVE & ASSIGN** on the summary page.

Assign

Application: "AirWatch Provisioning" updated successfully.

Selected App(s): AirWatch Provisioning

Users / User Groups

Search for Users or Groups

Selected Users / User Groups

ALL USERS

Deployment Type

Automatic

Entitlement Type

Include

CANCEL

SAVE

18. Search for **ALL USERS** and add them. Change **Deployment Type** to **Automatic** and click **SAVE**.

You have finished setting up and integrating Workspace ONE UEM, Access, and Intelligence. Now that our digital workspace platform is prepared we can think about integrating with Microsoft Azure.