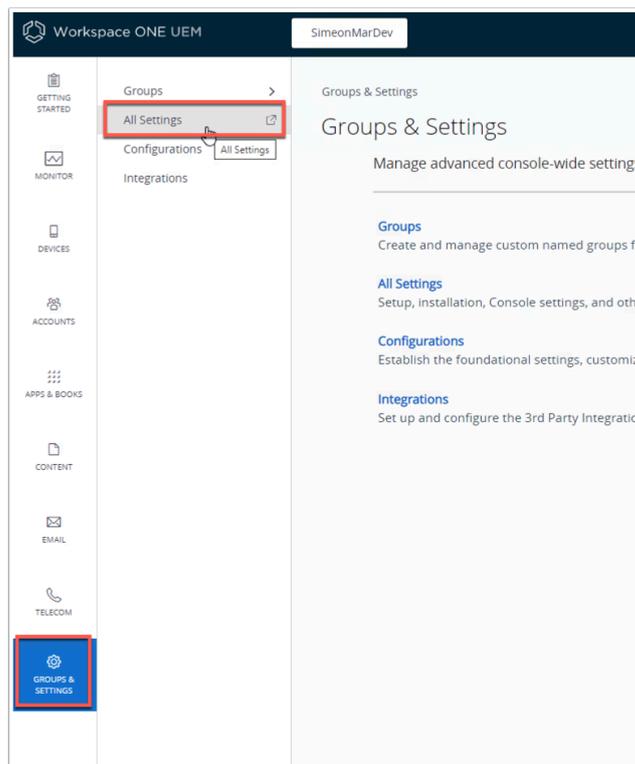


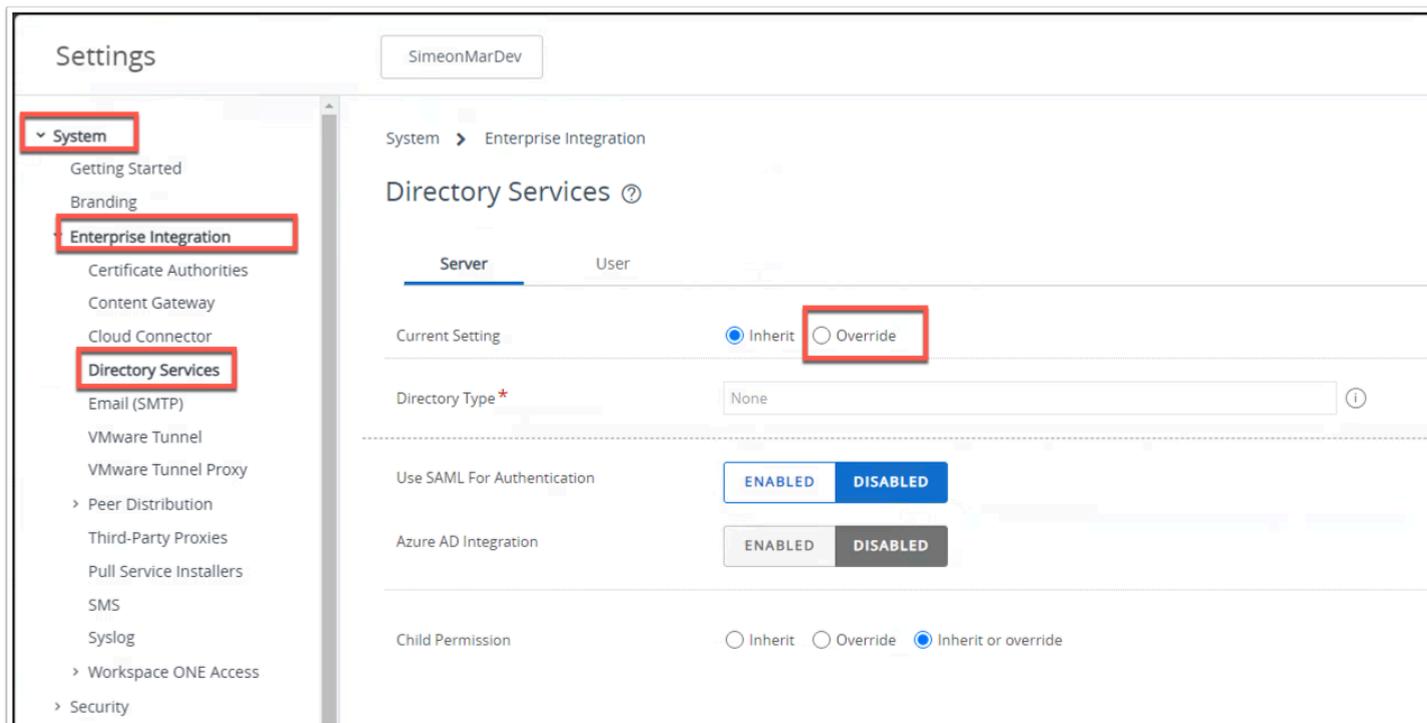
3. Manual and Automated Enrollment

This lab will demonstrate how enrollment can be done manually, but also how it might be automated using a staging account.

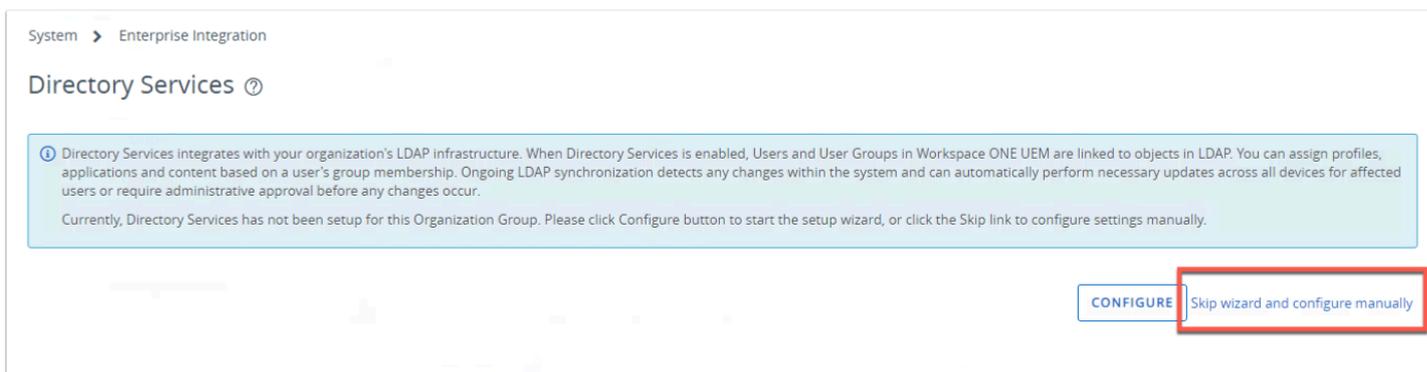
Part 1 : UEM SAML Authentication



1. On the Control Center open authenticate to the Workspace ONE UEM console. (dw-livewire.awmdm.com)
 - Navigate to **Groups & Settings > All Settings**



1. Navigate to **System > Enterprise Integration > Directory Services** and click **Override**.



2. Click **Skip wizard and configure manually**

Current Setting: Inherit Override

Directory Type*: ⓘ

Use SAML For Authentication: **ENABLED**

Enable SAML Authentication For*: Admin ⓘ Enrollment Self-Service Portal

Use New SAML Authentication Endpoint: **ENABLED** ⓘ

SAML 2.0

Import Identity Provider Settings:

⚠ To load the imported settings, click save. Any changes made to the form will be lost.

Service Provider (AirWatch) ID*:

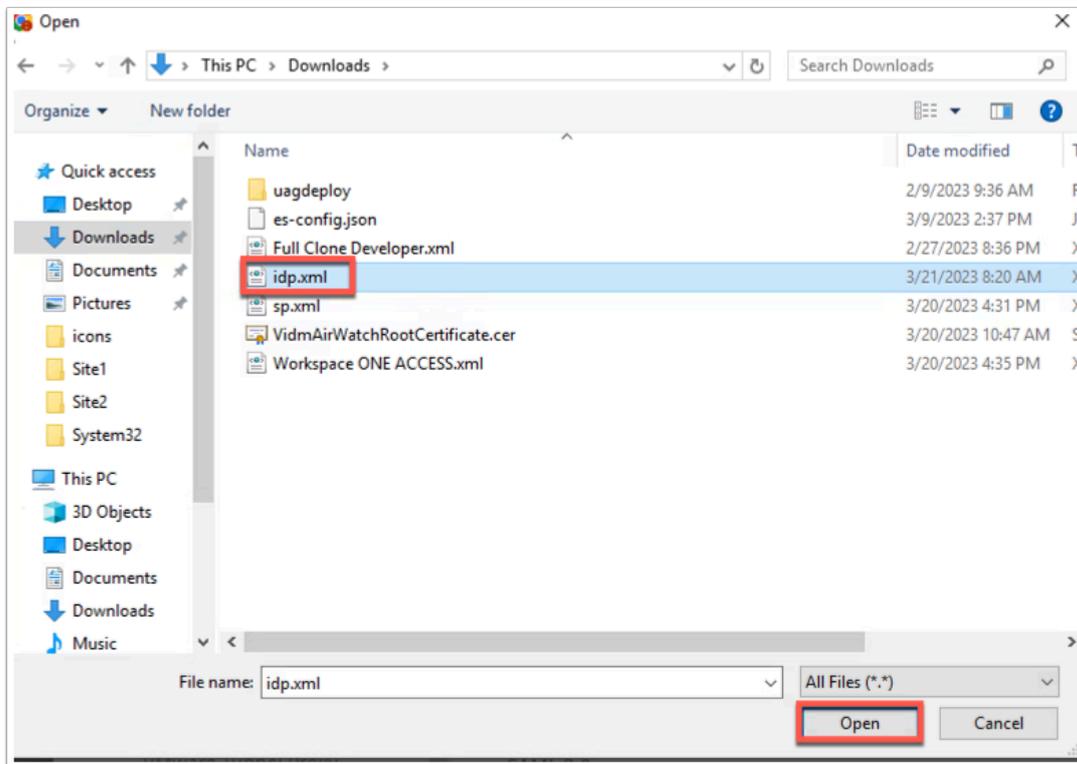
Identity Provider ID*:

⚠ Enabling SAML authentication for directory users will bypass other authentication modes. Ensure that the Identity Provider returns the 'objectGUID' attribute as part of the SAML response.

Request

Request Binding Type: Redirect POST Artifact

- Click **ENABLED** for **Use SAML For Authentication**
 - Click **UPLOAD** for **Import Identity Provider Settings**



- Navigate to the downloads folder and select the **idp.xml** previously downloaded.

Response

Response Binding Type Redirect POST Artifact

Sp Assertion URL

Authentication Response Security*

Allowed Clock Skew* ⓘ

Certificate

Identity Provider Certificate

Service Provider (AirWatch) Certificate

[Export Service Provider Settings](#)

Azure AD Integration

Child Permission Inherit Override Inherit or override

- Click **SAVE** at the bottom of the page. After the save you will see the page populated with the correct information.

Service Provider (AirWatch) ID*

Identity Provider ID*

⚠ Enabling SAML authentication for directory users will bypass other authentication modes. Ensure that the Identity Provider returns the 'objectGUID'

Request

Request Binding Type Redirect POST Artifact

Identity Provider Single Sign-On URL*

NameID Format*

Authentication Request Security*

Response

Response Binding Type Redirect POST Artifact

Sp Assertion URL

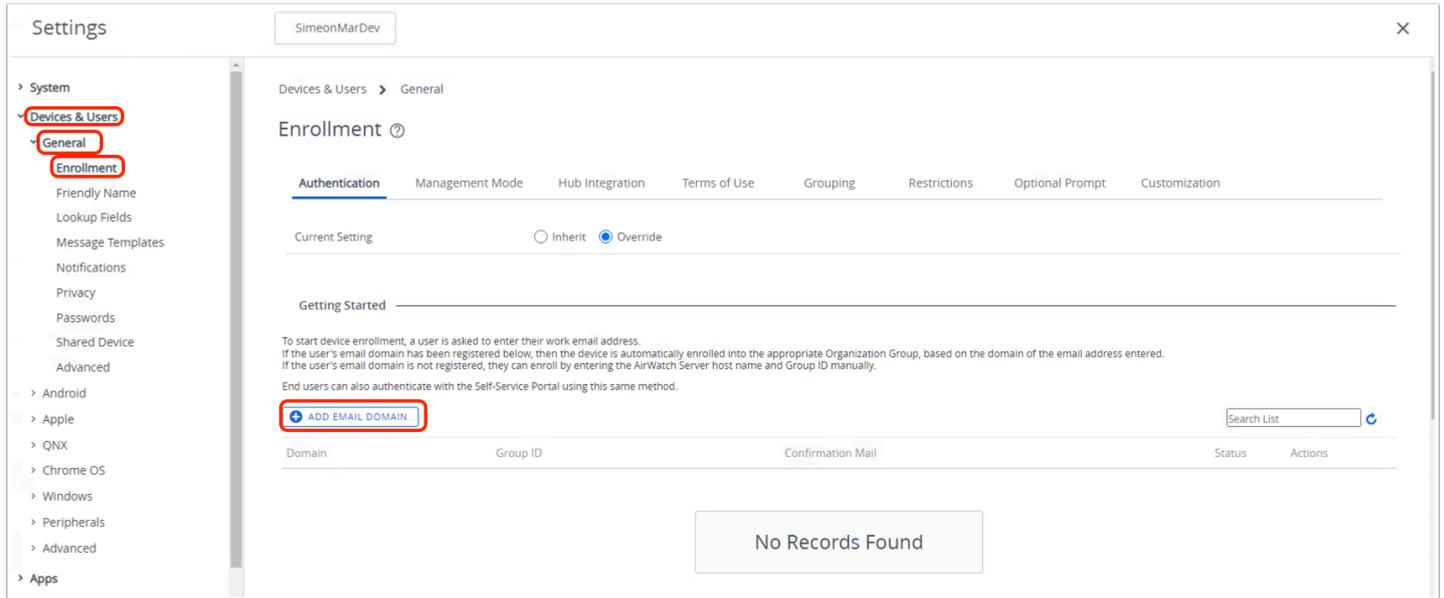
Authentication Response Security*

Allowed Clock Skew* ⓘ

Certificate

- Change both **Request Binding** and **Response Binding** to **POST**. Click **SAVE** at the bottom of the window.

Part 2: UEM Auto-Discovery

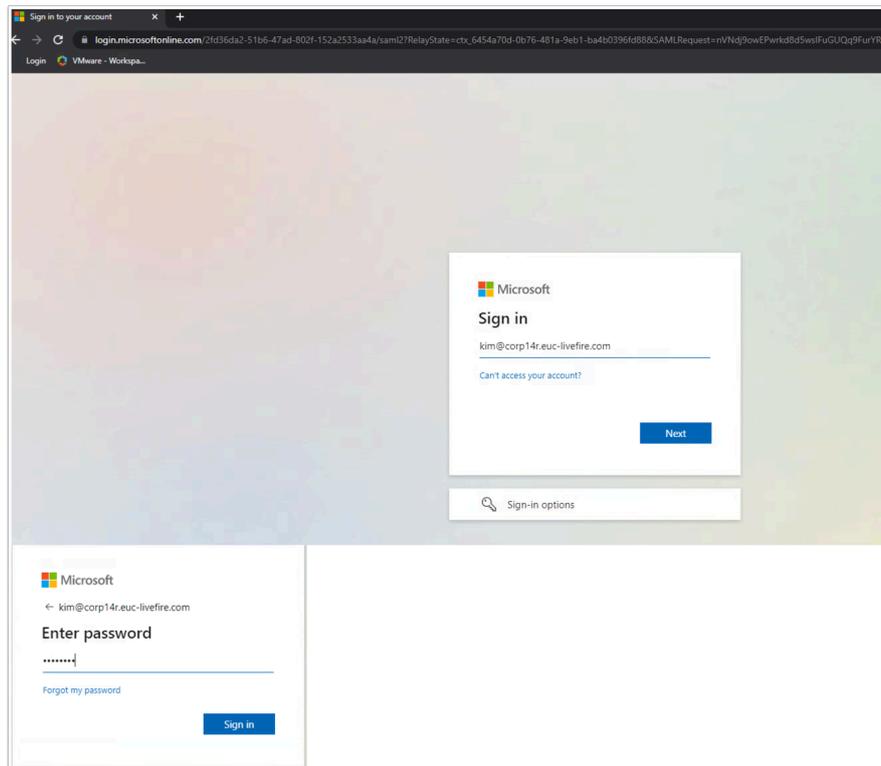


1. In the Settings page of Workspace ONE UEM click on **Devices & Users > General > Enrollment** and click **+ ADD EMAIL DOMAIN**

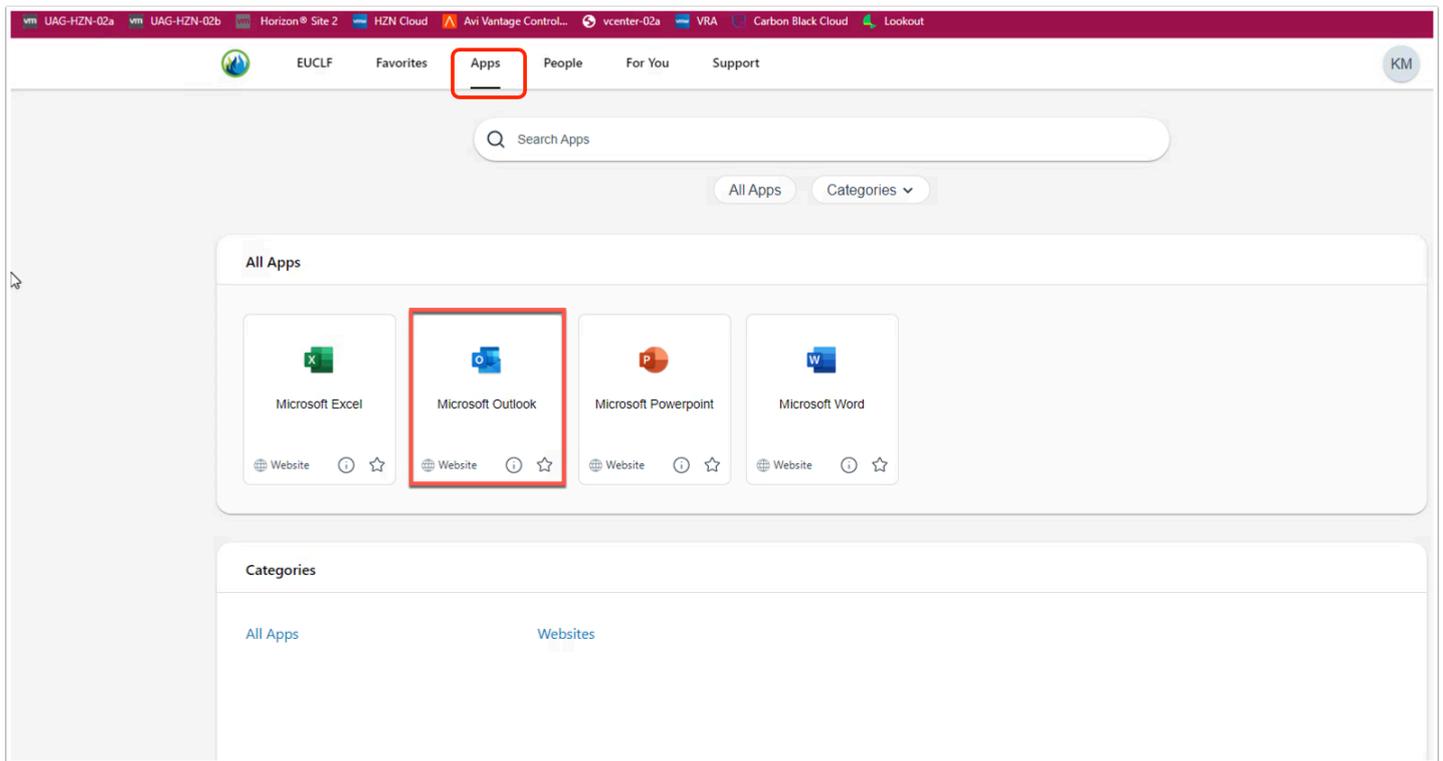
The 'Add Email Domain' dialog box contains three input fields: 'Organization Group' with the value 'SimeonMarDev', 'Business email Domain *' with the value 'corp14r.euc-liveware.com', and 'Confirmation email address *' with the value 'kim@corp14r.euc-liveware.com'. A blue 'SAVE' button is located at the bottom right of the dialog.

2. In the Add Email Domain option fill in the following:
 - Business email Domain - **corpXXX.euc-liveware.com**
 - Confirmation email address: **kim@corpXXX.euc-liveware.com**

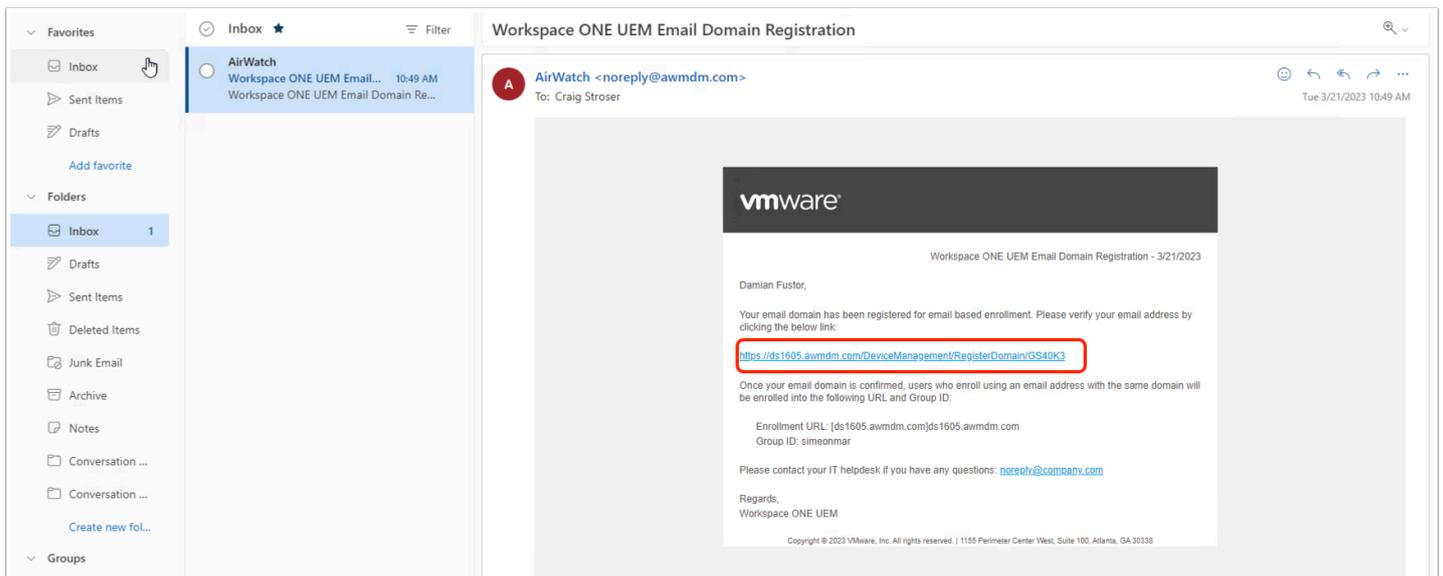
- Ensure you are filling in your unique corp identifiers in the fields. We are using Kim who is a member of the IT staff.
- Click **SAVE** at the bottom of the page.



3. Now open an Incognito window and navigate to **WorkspaceONE Access**. You will be re-directed to login.microsoftonline.com. Authenticate using **Kim@corpXXX.euc-livefire.com** and **VMware!** click **Sign in**



4. In the **VMware Intelligent Hub** click **Apps** at the top now click **Microsoft Outlook**



5. Once Outlook Mail Client opens, Navigate to the email from AirWatch in your Inbox.

- Click on the **link** in the Email to confirm the domain registration.



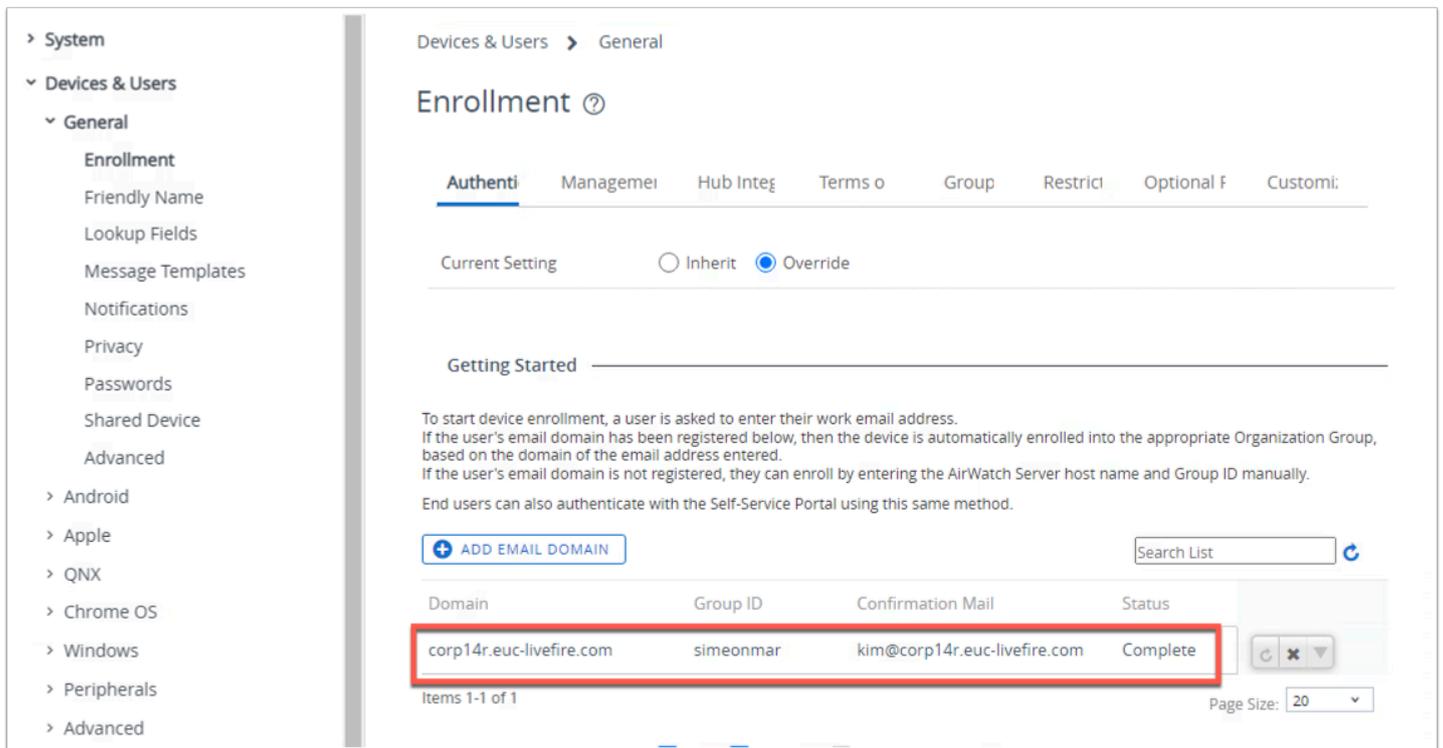
Email Domain Registration

Email Domain Registration Success

Your email domain has successfully been registered for simplified enrollment. Users enrolling devices using the following email domain will be activated into the server and group listed below.

Email: corp14r.euc-liveware.com
Server URL: ds1605.awmdm.com
Group ID: simeonmar

6. You will be redirected to the confirmation webpage.



Devices & Users > General

Enrollment

Authenti Management Hub Integ Terms o Group Restrict Optional F Customi:

Current Setting Inherit Override

Getting Started

To start device enrollment, a user is asked to enter their work email address. If the user's email domain has been registered below, then the device is automatically enrolled into the appropriate Organization Group, based on the domain of the email address entered. If the user's email domain is not registered, they can enroll by entering the AirWatch Server host name and Group ID manually. End users can also authenticate with the Self-Service Portal using this same method.

[+ ADD EMAIL DOMAIN](#) 

Domain	Group ID	Confirmation Mail	Status
corp14r.euc-liveware.com	simeonmar	kim@corp14r.euc-liveware.com	Complete

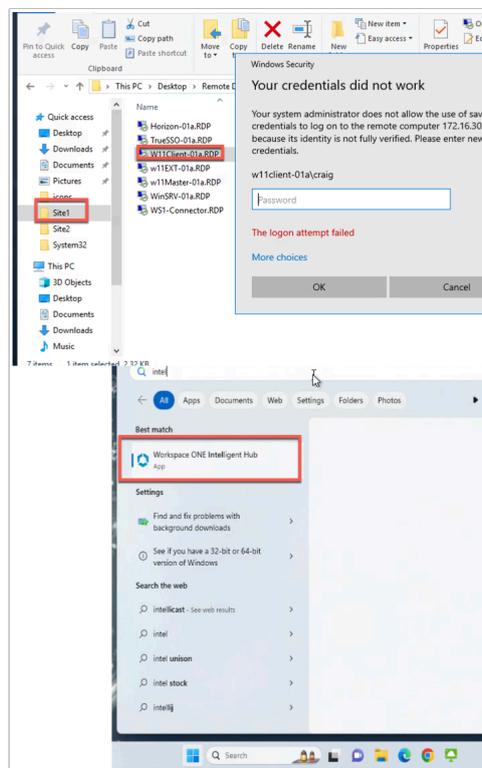
Items 1-1 of 1 Page Size: 20

7. In the UEM settings page. You will see the domain **Status** as Complete.

Part 3: Enrolling Intelligent Hub on Microsoft Windows 11

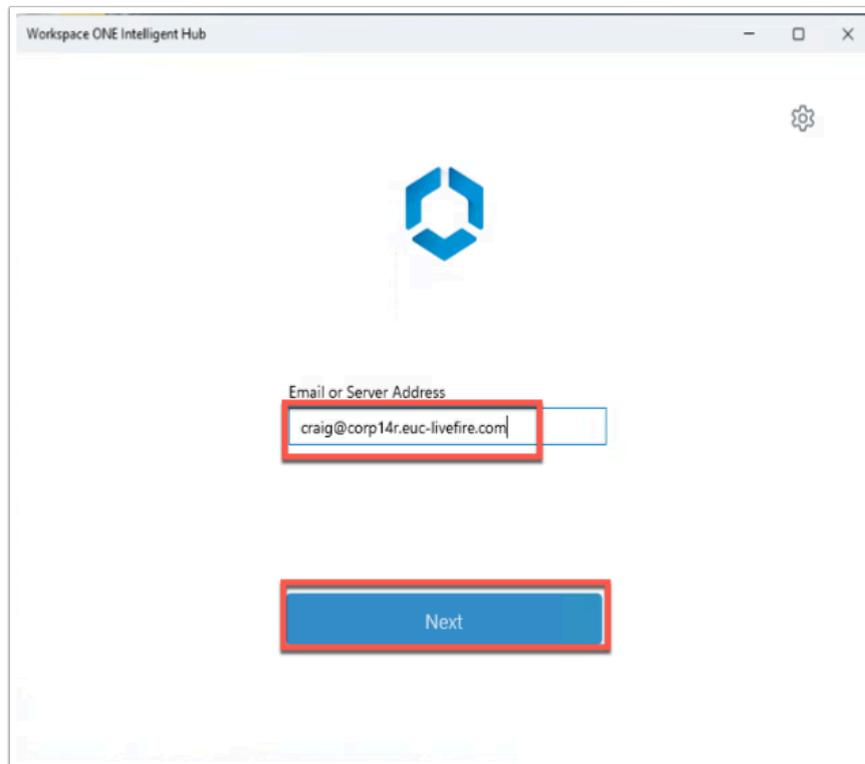
Step 1 : Enrolling W11Client-01a on Site 1 user Craig

Steps 1 & 2 could all be done in parallel, So whilst waiting for enrollment to complete on one virtual machine, feel free to move on the next step



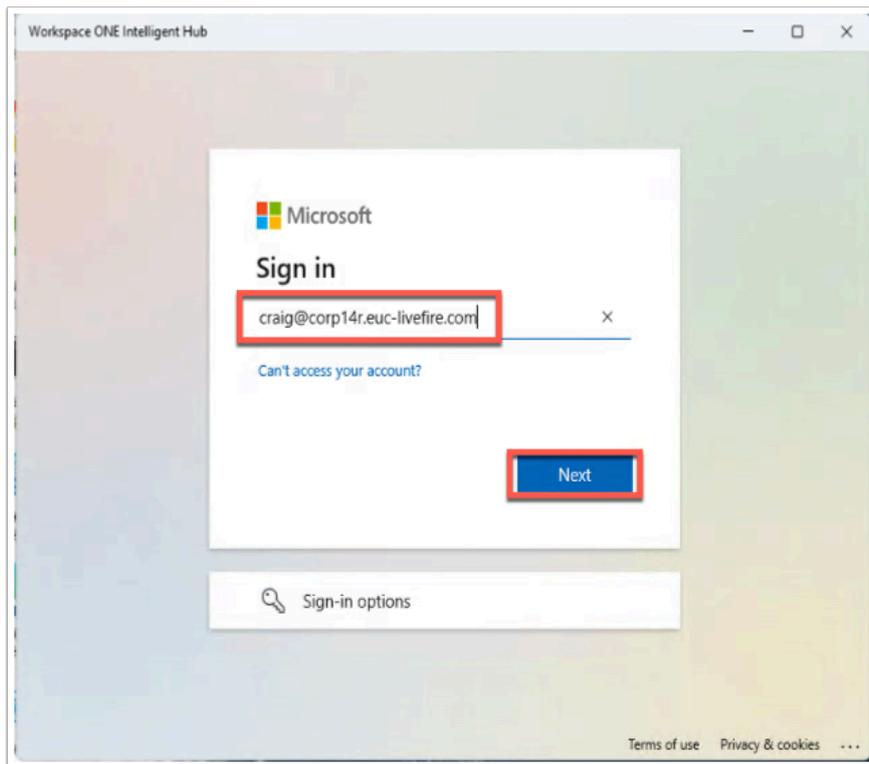
1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the **Site1** folder
 - Select the **W11Client-01a RDP** client and
 - Sign-in with
 - **username: w11client-01a\craig**
 - **Password: VMware1!**
 - To the right of the **Start** button
 - in the **search** area,
 - start typing **intel**
 - Select the **Workspace ONE Intelligent Hub**

- Please Note! If the **Workspace ONE Intelligent Hub** does not load,
 - From the **RUN > Services.msc** > Start the **Airwatch** service
 - Attempt to **re-launch** the hub

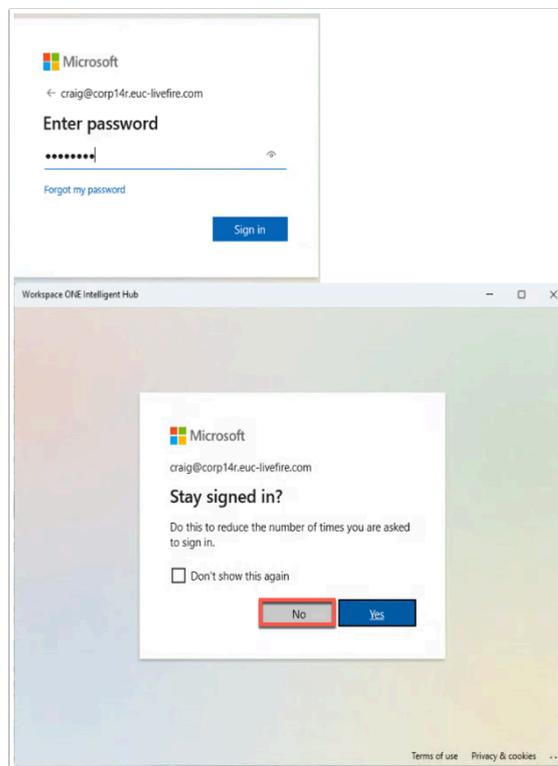


2. Under **Email or Server Address**,

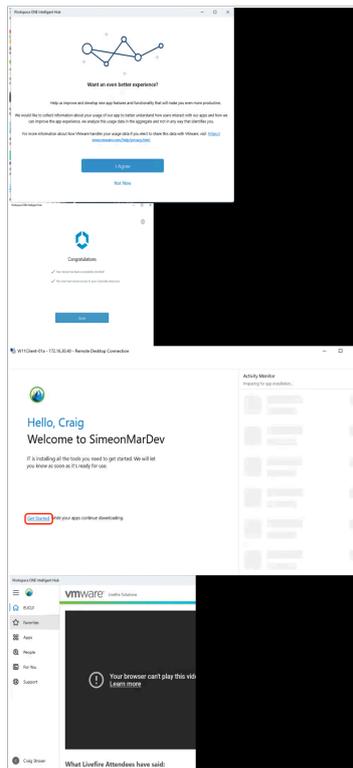
- Enter **craig@corpXXX.euc-livefire.com** (replacing XXX with your unique corp ID)
- Select **Next**



3. You will be re-directed to Microsoft Azure as your identity provider for authentication. Type in your user again and click Next.



4. Type in the password **VMware1!** and click **Sign in** and select **No**.

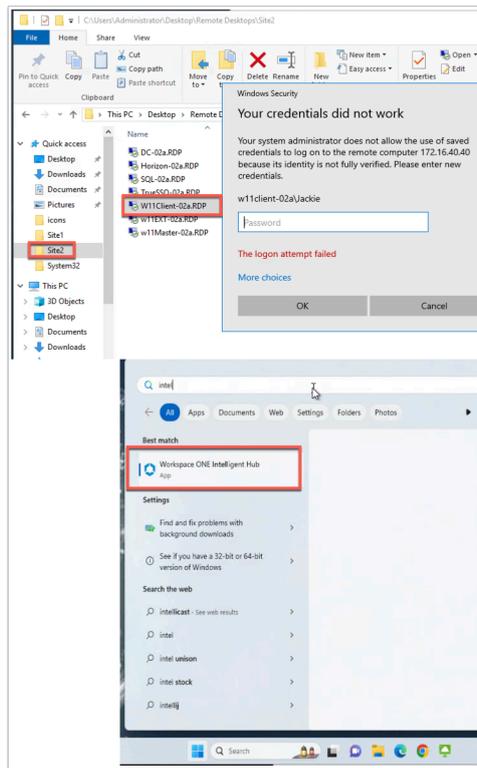


5. On the **Congratulations** window,

- Select **I agree**
- Click **Done**
- Select **Get Started**

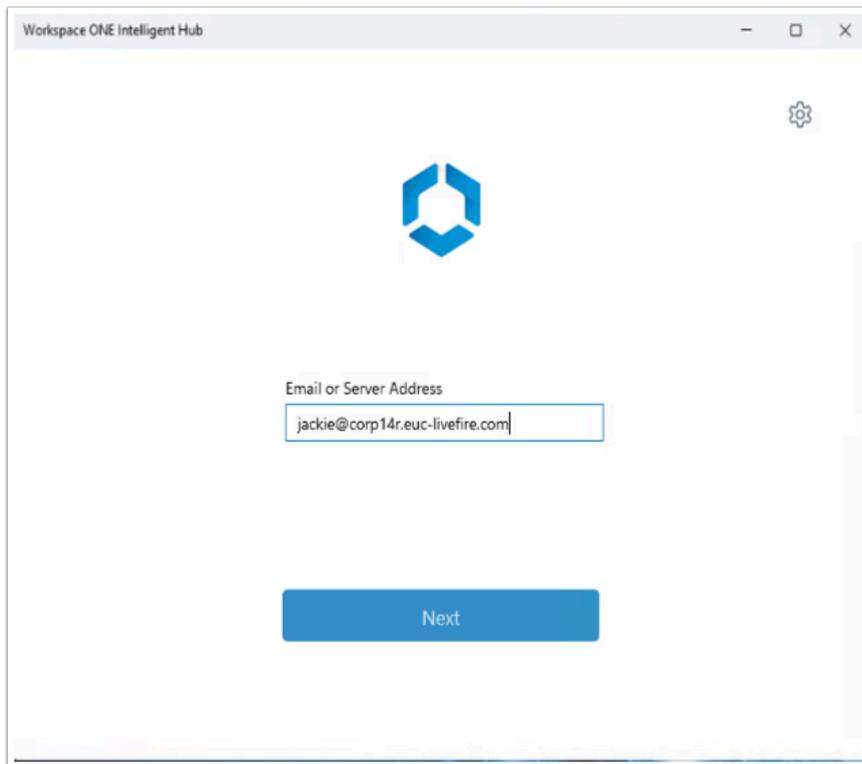


Step 2 : Enrolling W11Client-02a on Site 2 with the user Jackie

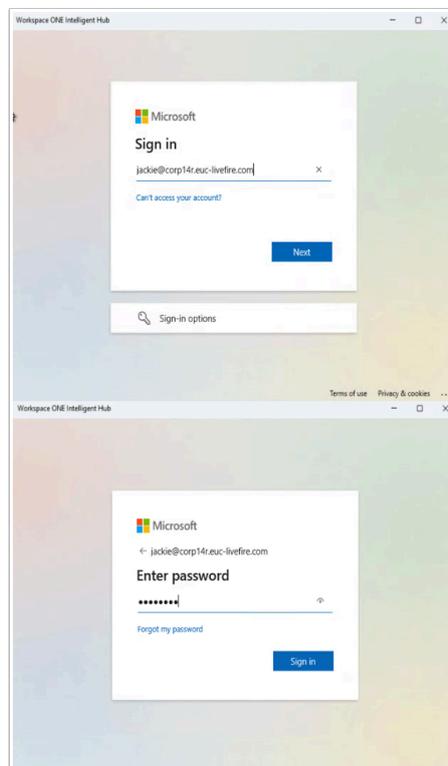


6. On your **ControlCenter** server

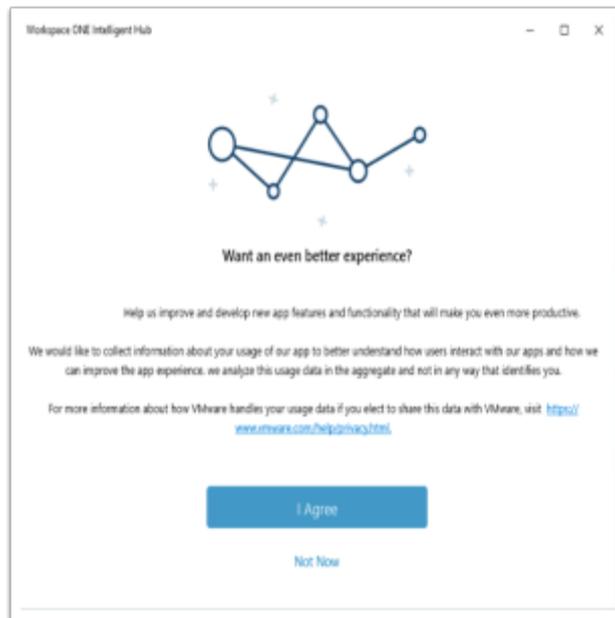
- On the Desktop open the **Remote Desktop** folder.
 - Open the **Site 2** folder
- Select the **W11Client-02a.RDP** client and
 - Sign-in with
 - **username w11client-02a\jackie**
 - **Password VMware1!**
- To the right of the **Start** button in the search area, start typing **intel**
- Select the **Workspace ONE Intelligent Hub**
 - Please Note! If the **Workspace ONE Intelligent Hub** does not load,
 - From the **RUN > Services.msc > Start the Airwatch service**
 - Attempt to **re-launch** the hub



7. Under **Email or Server Address**,
- Enter jackie@corpXXX.euc-livefire.com
 - Select **Next**

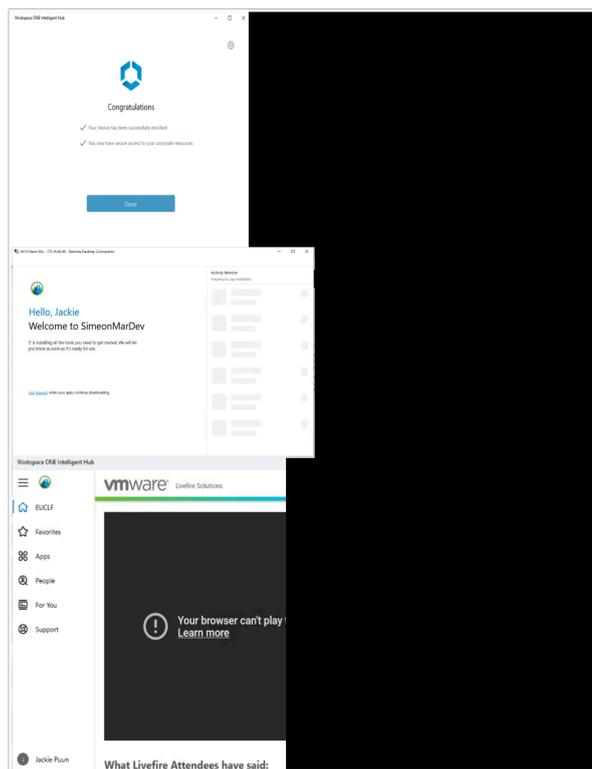


8. Fill in the same email again and click **Next**. Then type **VMware1!** for the password and click **Sign in**



9. In the **Workspace ONE Intelligent Hub**

- Select **I Agree**



10. On the **Congratulations** window,

- Select **Done**
- **Re-open** the Intelligent Hub
- Select **Get Started**

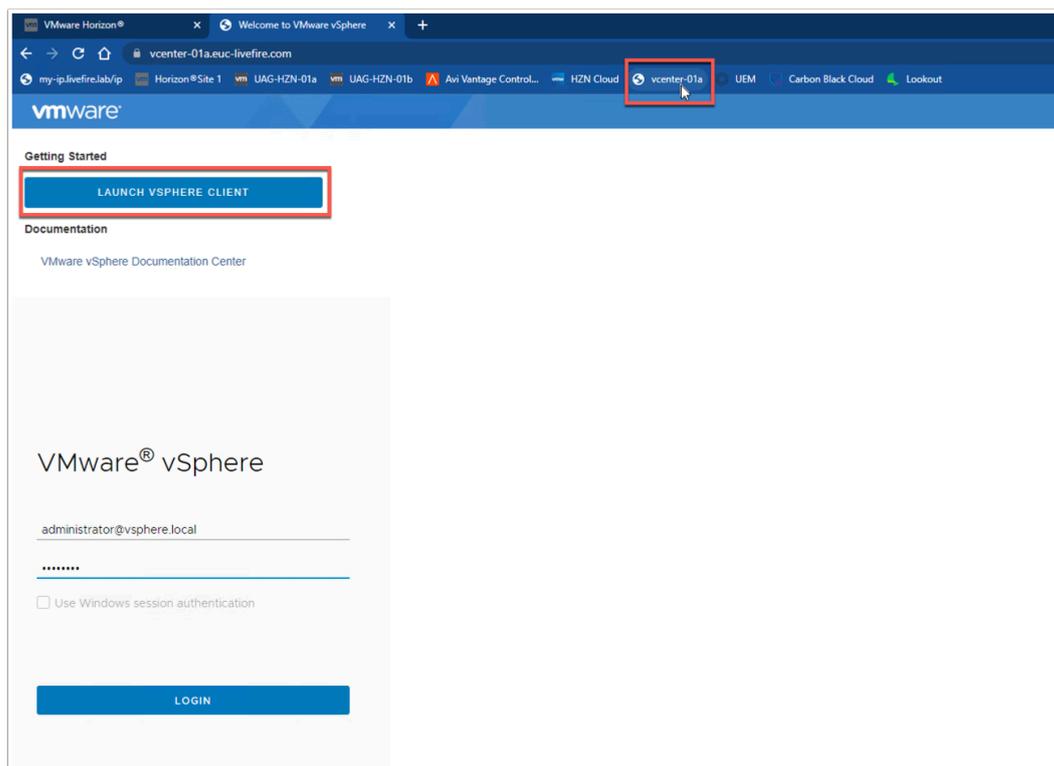
Part 4: Automated enrollment of persistent desktops

In order to standardize day-2 operations for specific use-cases it may be beneficial to enroll persistent desktops (VDI). As these desktops are dedicated and not floating this gives the users greater flexibility to customize their workspace.

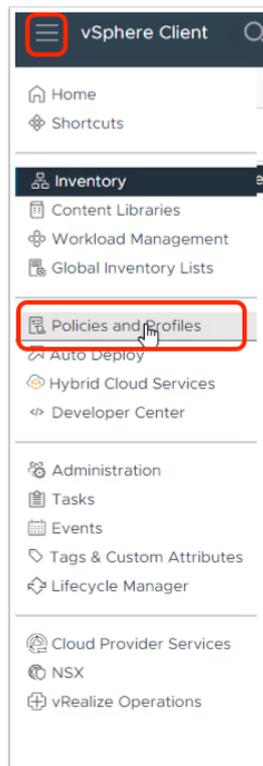
Please note this [KB](#) for further explanation of supported virtual platforms for enrollment.

Note: UEM does not support non-persistent desktop enrollments

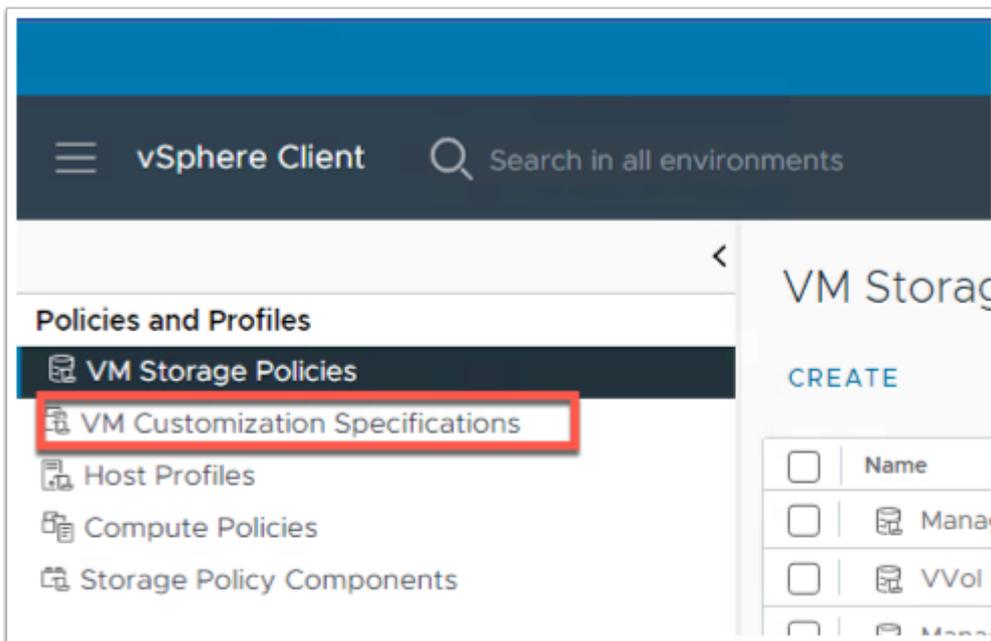
In this exercise you will use vSphere VM Customization Specifications to execute a script that will enroll the Workspace ONE Hub with UEM after a successful login to a persistent desktop. This script will include UEM server URL, GroupID, Staging user and msixexec switches. You can read further about command-line [enrollment here](#).



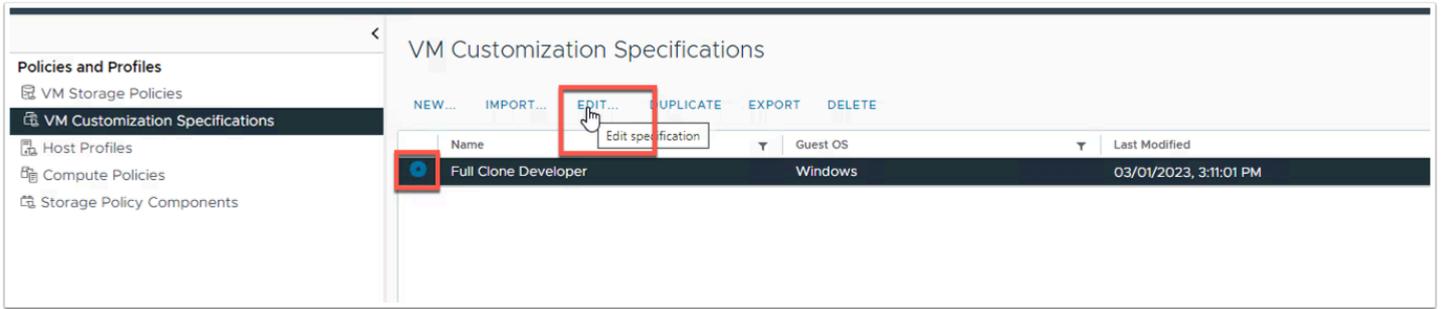
1. On the Control Center open Chrome site 1 Profile. and click on the **vcenter-01a** bookmark.
 - Click on **Launch vSphere Client**
 - Now Authenticate with **administrator@vsphere.local** and **VMware1!**



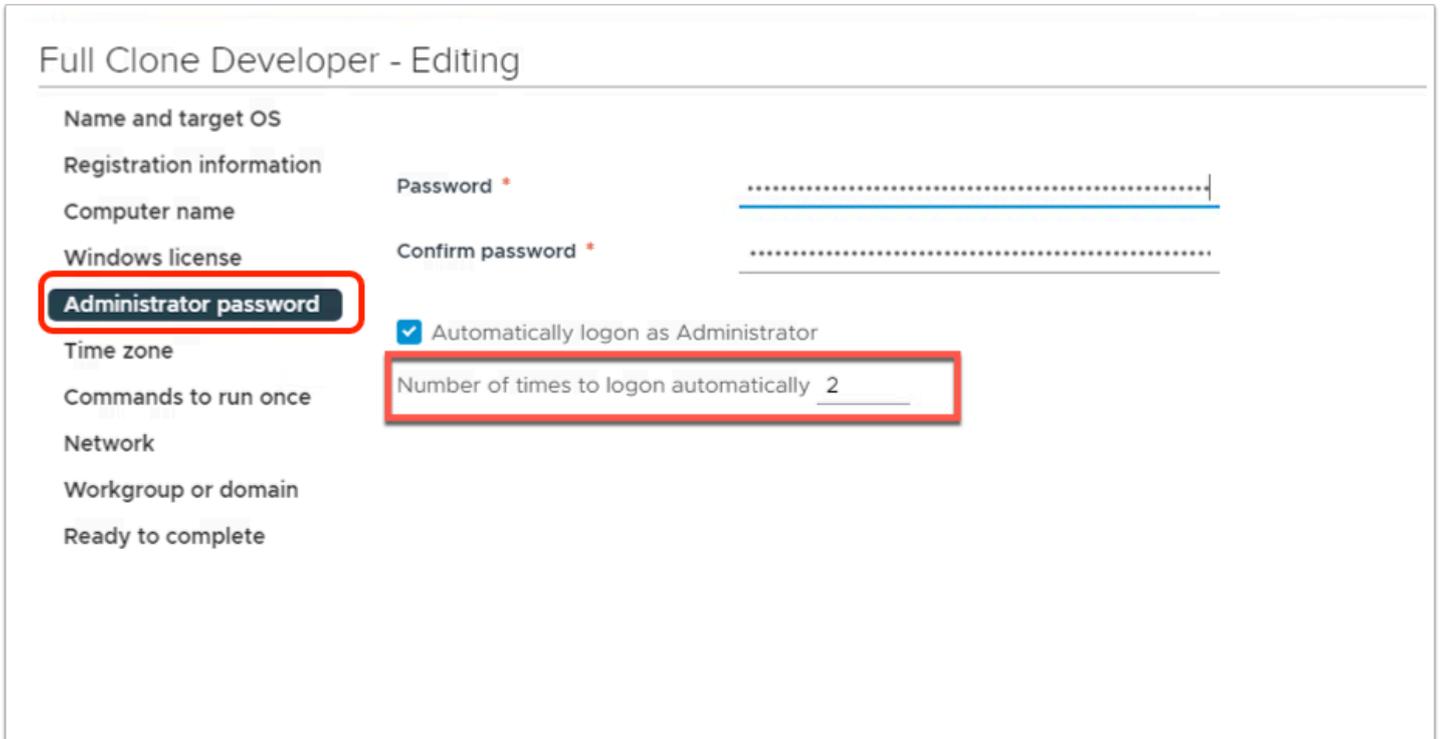
2. Expand the hamburger menu on the left and click **Policies and Profiles**.

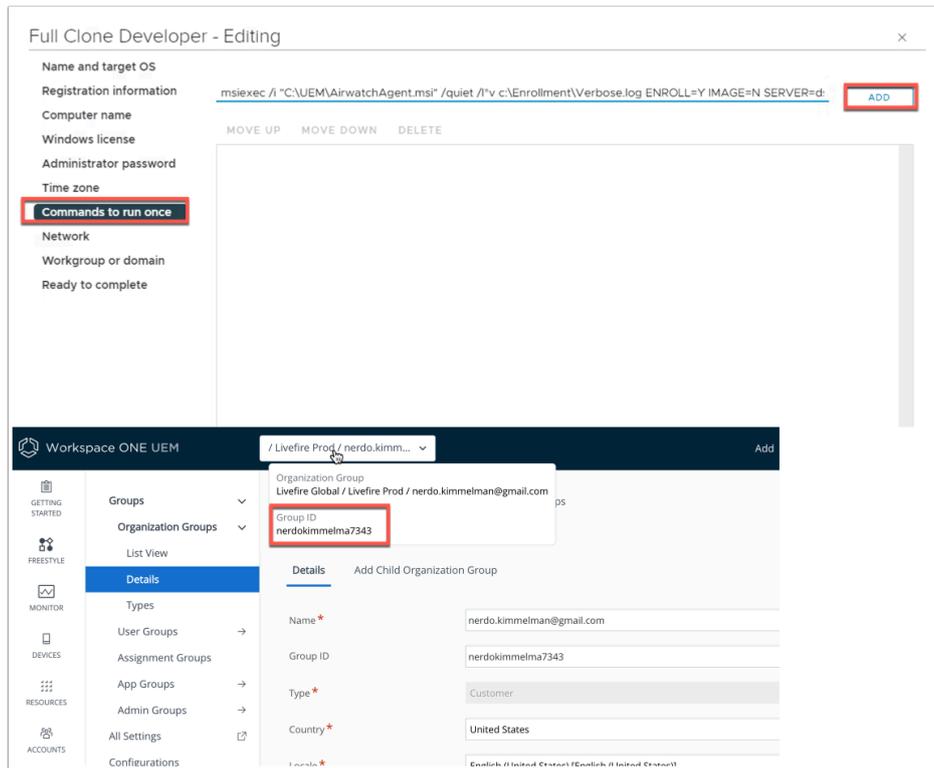


3. Click on **VM Customization Specifications**



4. Click on **Full Clone Developer** and click **EDIT...**





5. a. On the left navigation click on **Administrator password** and change the "number of times to logon automatically" to **2**

b. On the left navigation click on **Commands to run once** - now type in the below command (Make sure to change the GroupID) and click **ADD**

NOTE: Your group ID can be found in WorkspaceONE UEM by hovering over your Organization Group.

```
msiexec /i "C:\UEM\AirwatchAgent.msi" /quiet /!v c:\Enrollment\Verbose.log ENROLL=Y
IMAGE=N SERVER=ds1605.awmdm.com LGName=YOURGROUPID USERNAME=staginguser
PASSWORD=VMware123 ASSIGNTOLOGGEDINUSER=Y
```

💡 Breakdown of the above script:

/i = install

/quiet = completely silent

/! = log levels and log paths path must be in quotes

ENROLL = Select 'Y' to enroll

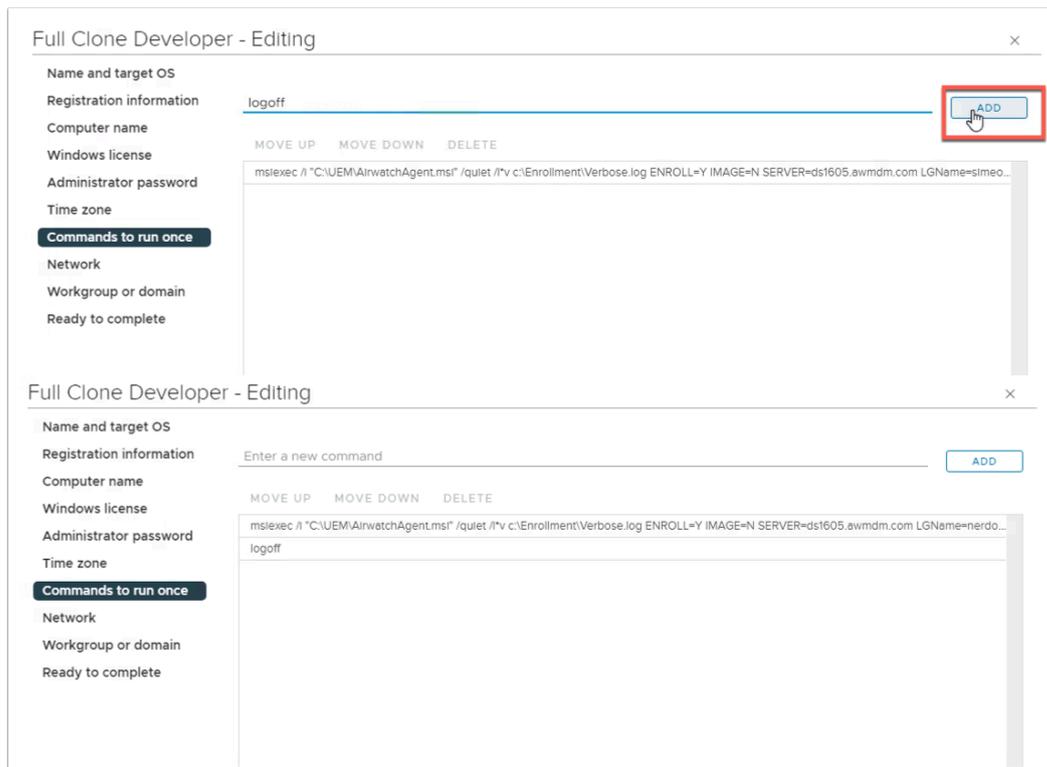
IMAGE= if this flag is set to 'Y', the agent will be put into image mode.

LGName = organization group id.

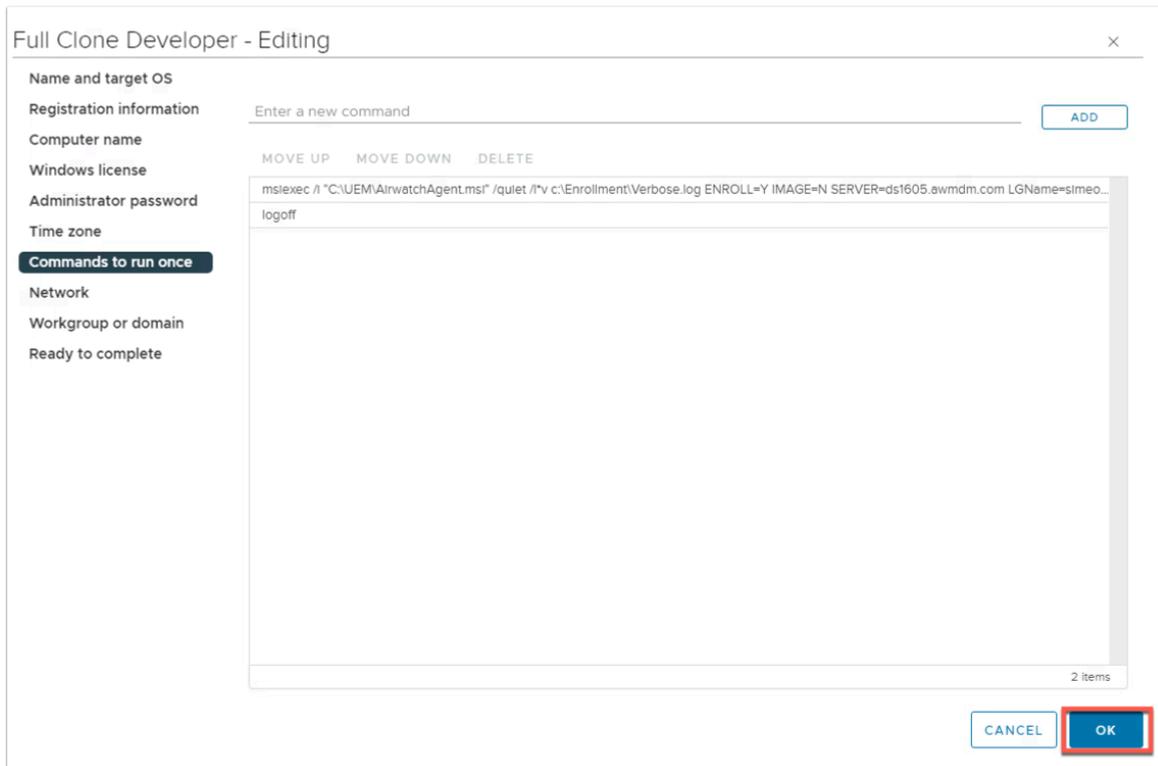
USERNAME = Enter the username for the user you are enrolling or the staging username if staging the device on the behalf of a user.

ASSIGNTOLOGGEDINUSER = Select 'Y' to assign the device to the logged in domain user.

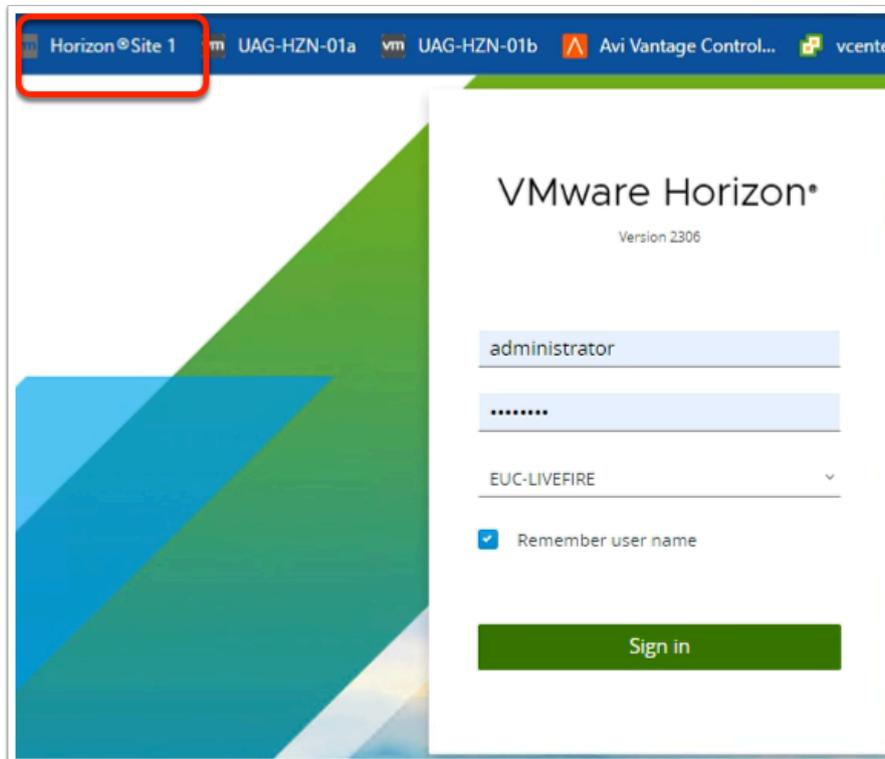
For further switches click [HERE](#).



6. Type **logoff** and click **ADD**

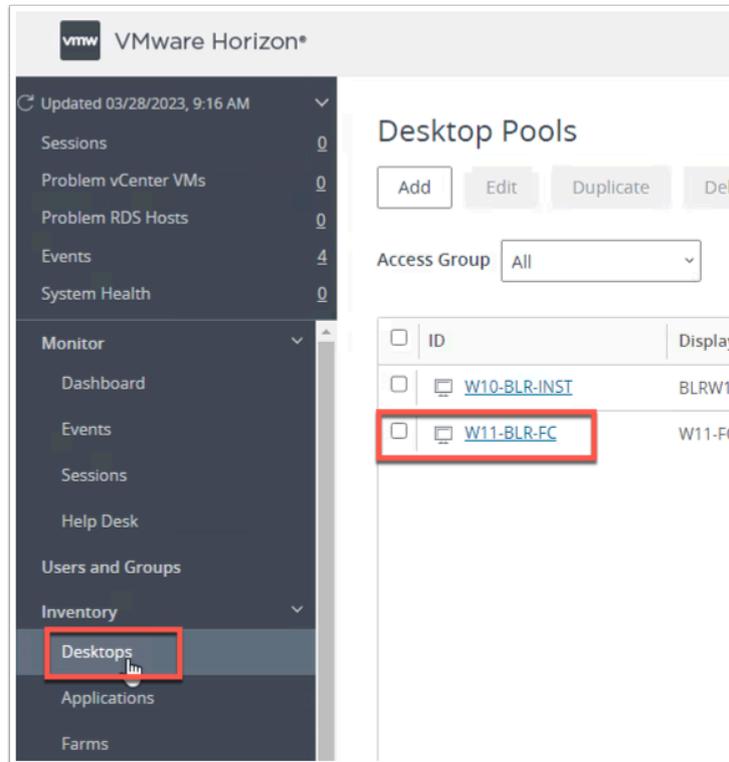


7. Click **OK** at the bottom of the page.

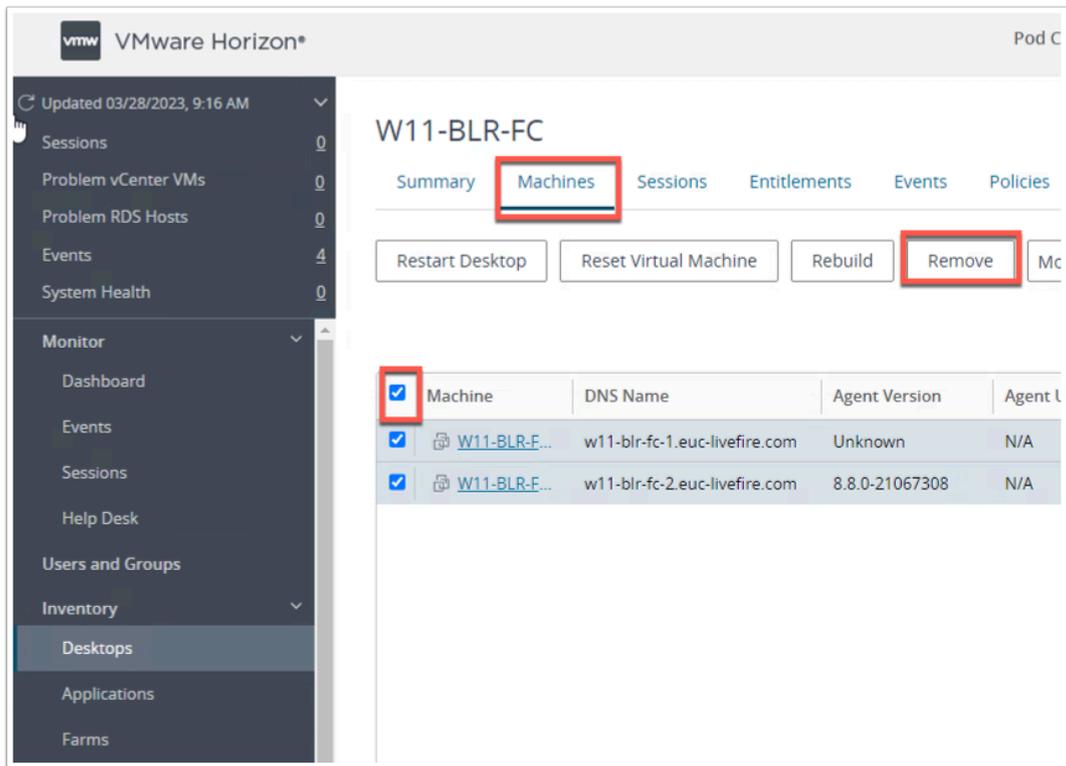


8. On your **Site 1 browser** session
- In the **Bookmarks bar**
 - click on the **Horizon Site 1** shortcut
 - In the **VMware Horizon** login

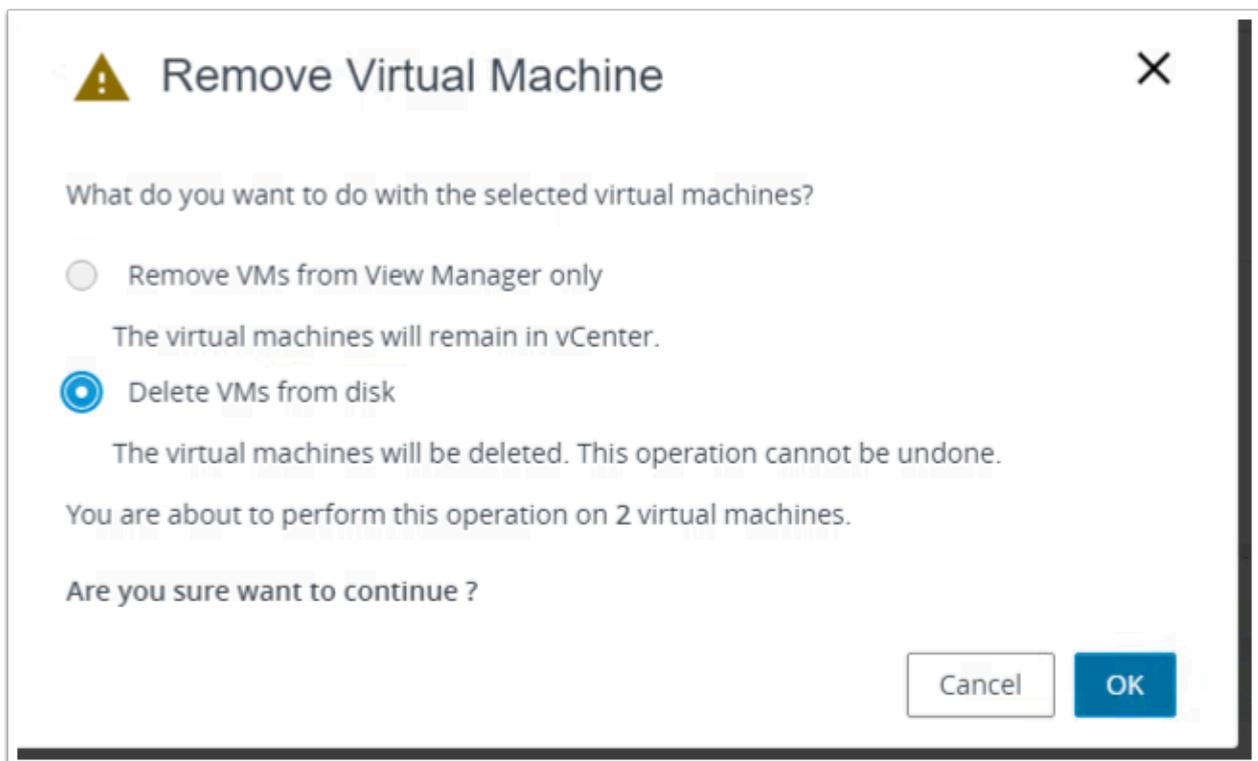
- In the **username** area
 - enter **Administrator**
- In the **password** area
 - enter **VMware1!**
- select **Sign in**



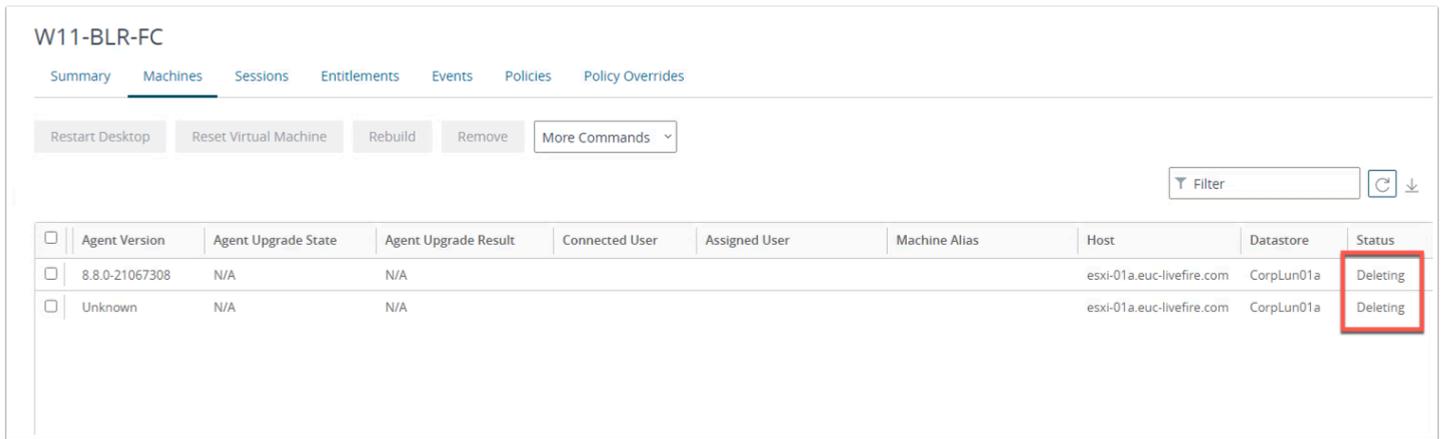
9. On the left navigate to **Desktops** and click **W11-BLR-FC**



- Click on **Machines** then click the **check box** to check the two existing VMs. Now click **Remove**

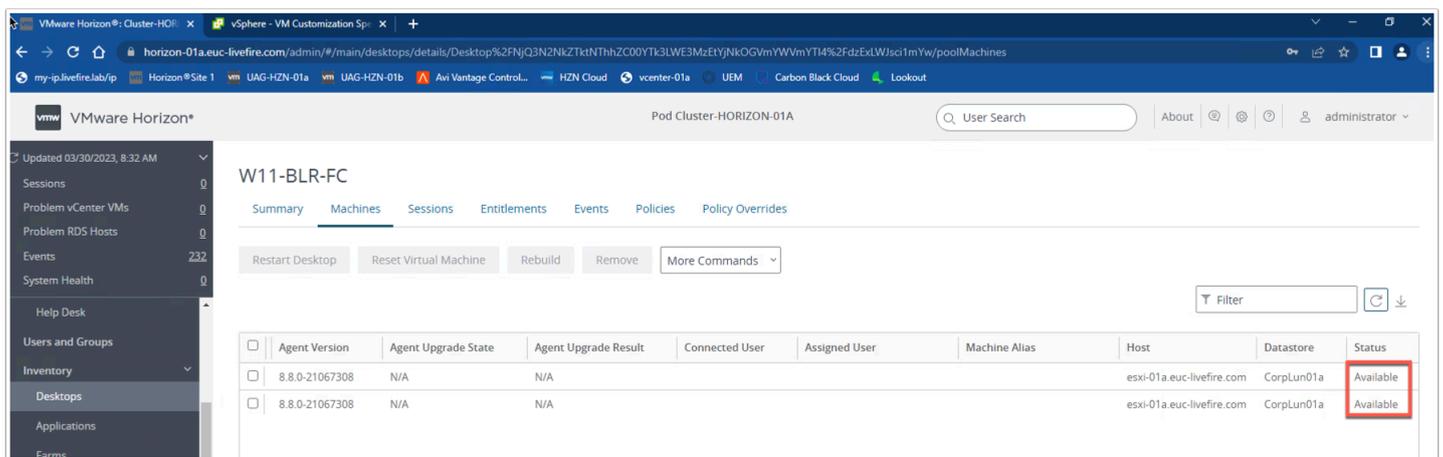


- Select **Delete VMs from disk** and click **OK**.

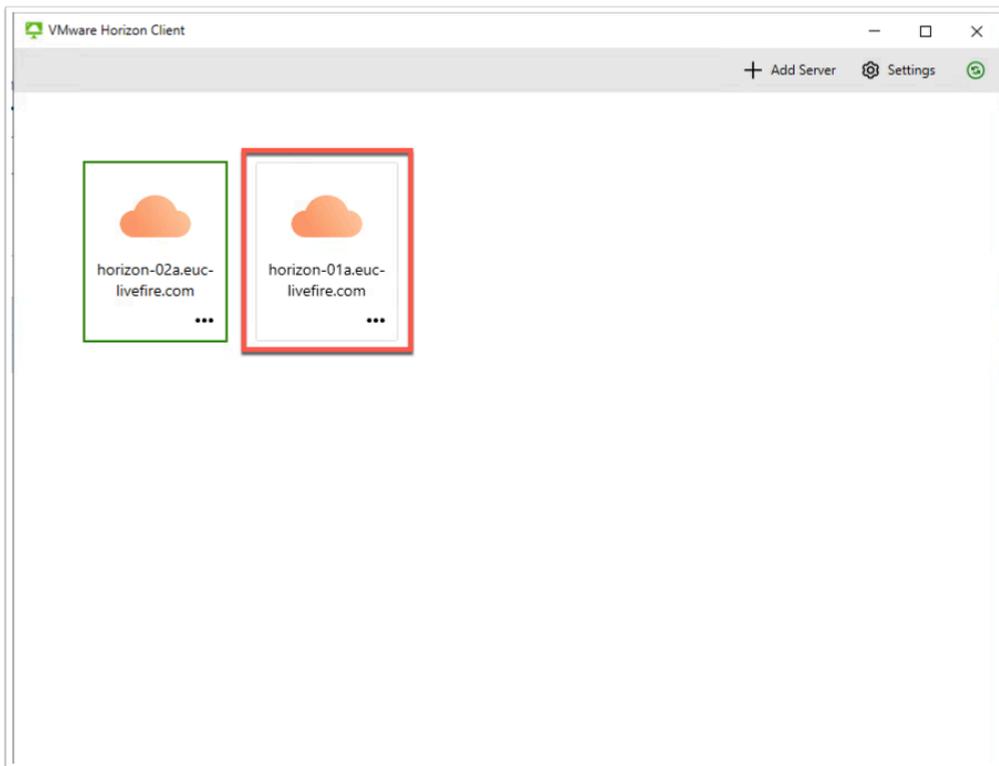


12. This process will take some time **grab a coffee and come back** (up to 20 minutes). It will first delete the existing VMs then re-build them with the customization we have set.
- NOTE:** Use the Status column to see what task is currently being worked on.

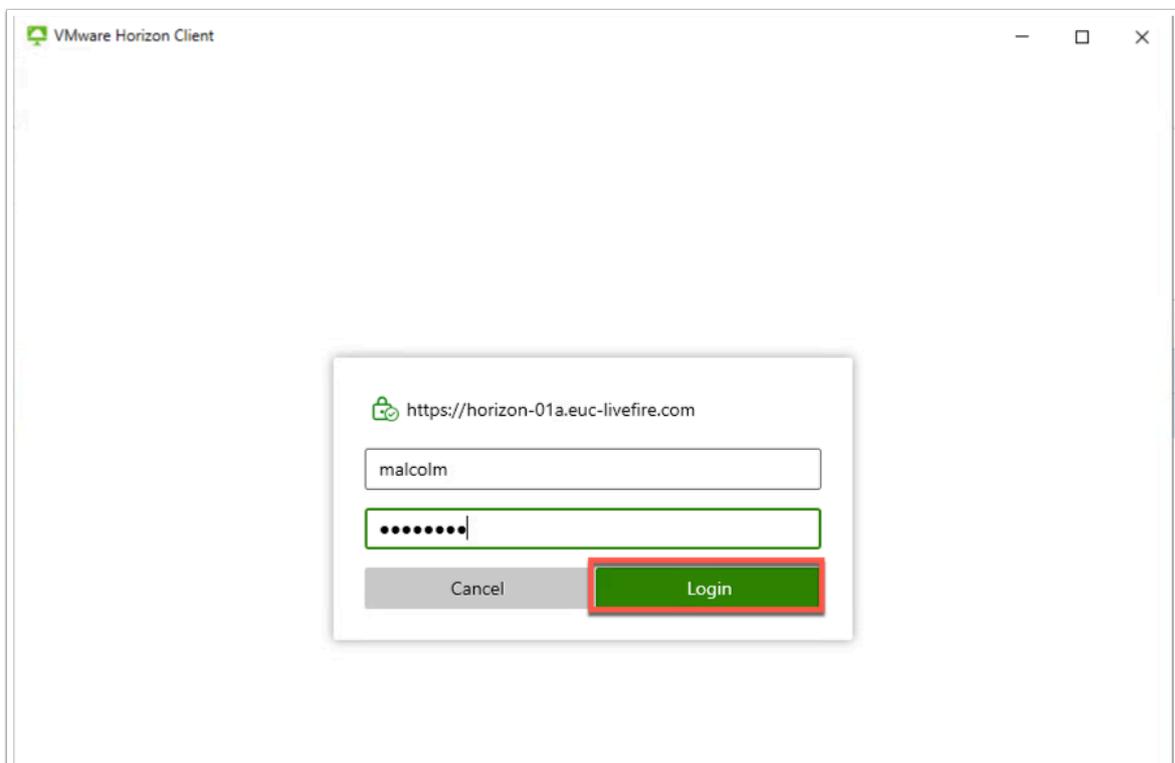
Part 5: Final Testing



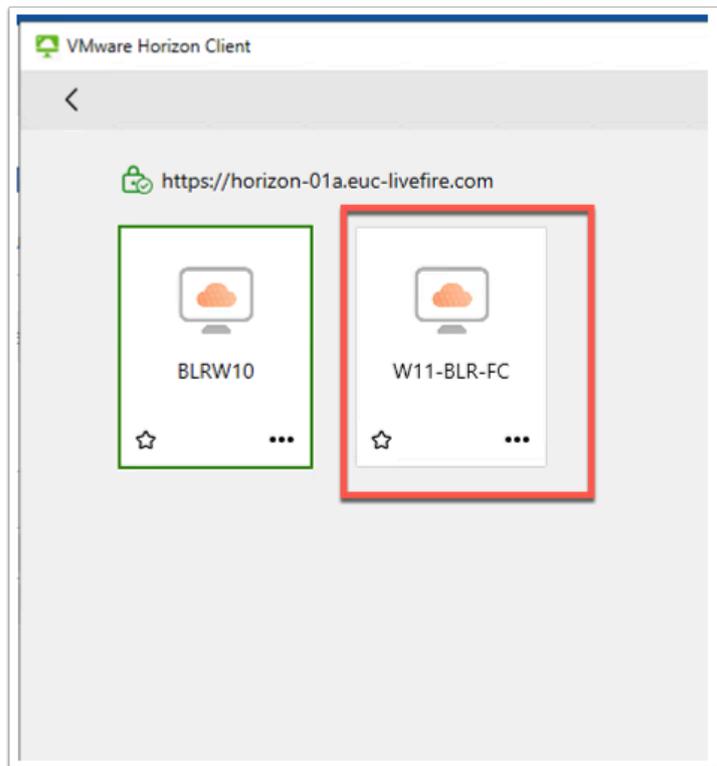
1. Flip back to **Chrome profile Site 1** and in **Horizon** ensure your Machines are in the Status **Available**.



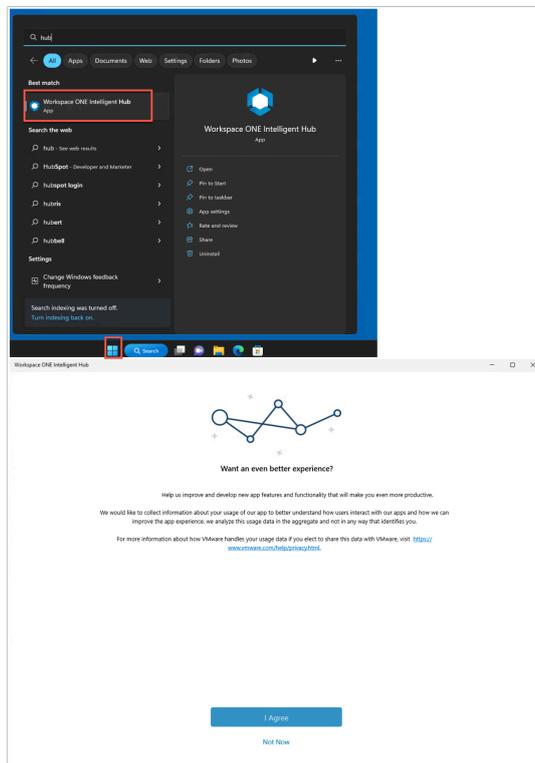
2. Open the **Horizon Client** on your Control Center machine and connect to server **horizon-01a.euc-livefire.com**



3. Now authenticate with **malcolm** and **VMware1!** click **Login**.



4. Double click the **W11-FC (Machine not assigned)** desktop.



5. Once the desktop has loaded click **Start** and type **Hub**. Launch the **Workspace ONE Intelligent Hub**.

- You can slo just wait eventually the Hub will launch on it's own.
- Click **I Agree**

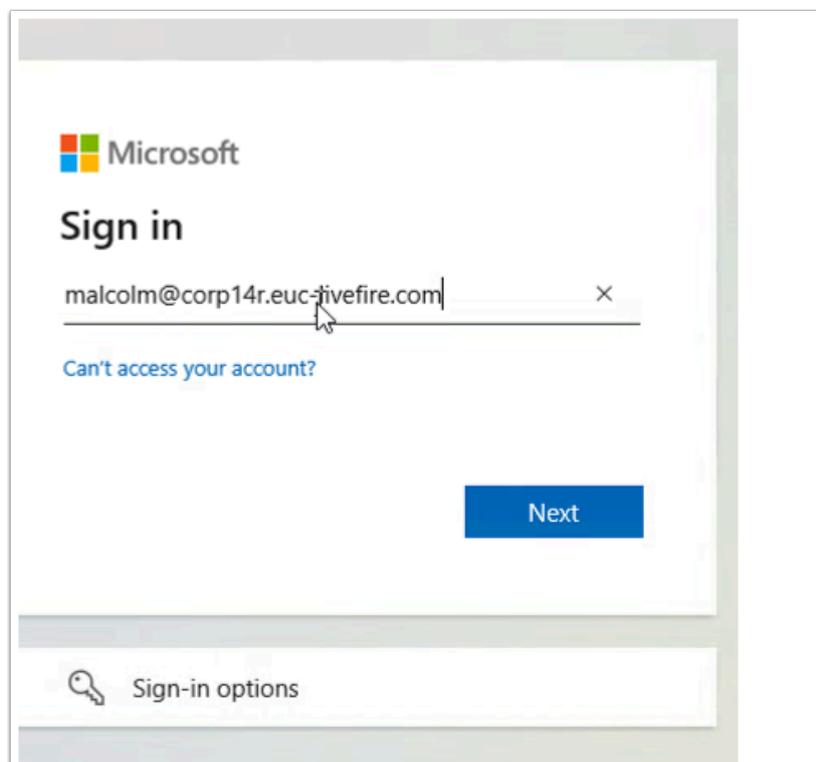
Devices

List View

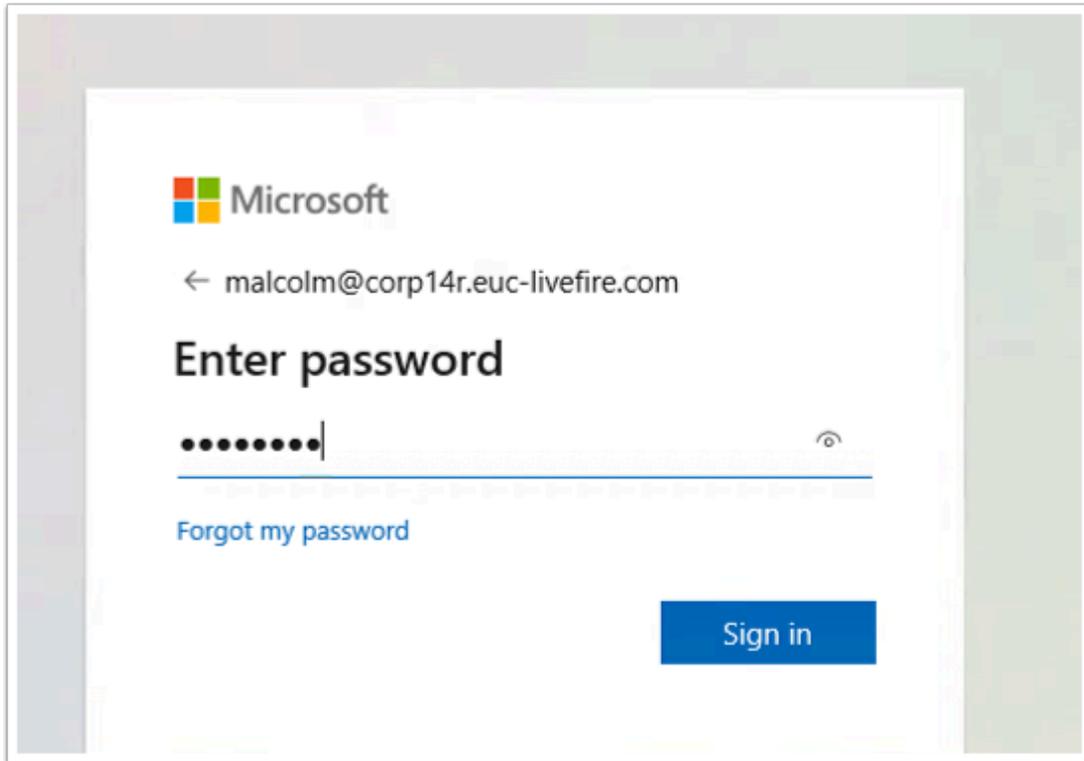
Filters >> [+ ADD DEVICE](#) [LAYOUT](#) [↻](#) [EXPORT](#)

Last Seen	General Info	Platform	User
7s	Malcolm W11-BLR-FC-1 Desktop 6 15 / Livefire Prod / SimeonMarDev UEM Managed Corporate - Dedicated	Windows Desktop VMware20,1 10.0.22621	malcolm@euc-livefire.com Malcolm Malcolm Barneo
1m	Craig W11CLIENT-01A VMware7,1 a ba / Livefire Prod / SimeonMarDev UEM Managed Corporate - Dedicated	Windows Desktop VMware7,1 10.0.22621	craig@livefire.com Craig Craig Stroser
2m	Jackie W11CLIENT-02A VMware7,1 a ba / Livefire Prod / SimeonMarDev UEM Managed Corporate - Dedicated	Windows Desktop VMware7,1 10.0.22621	jackie@euc-livefire.com Jackie Jackie Puun

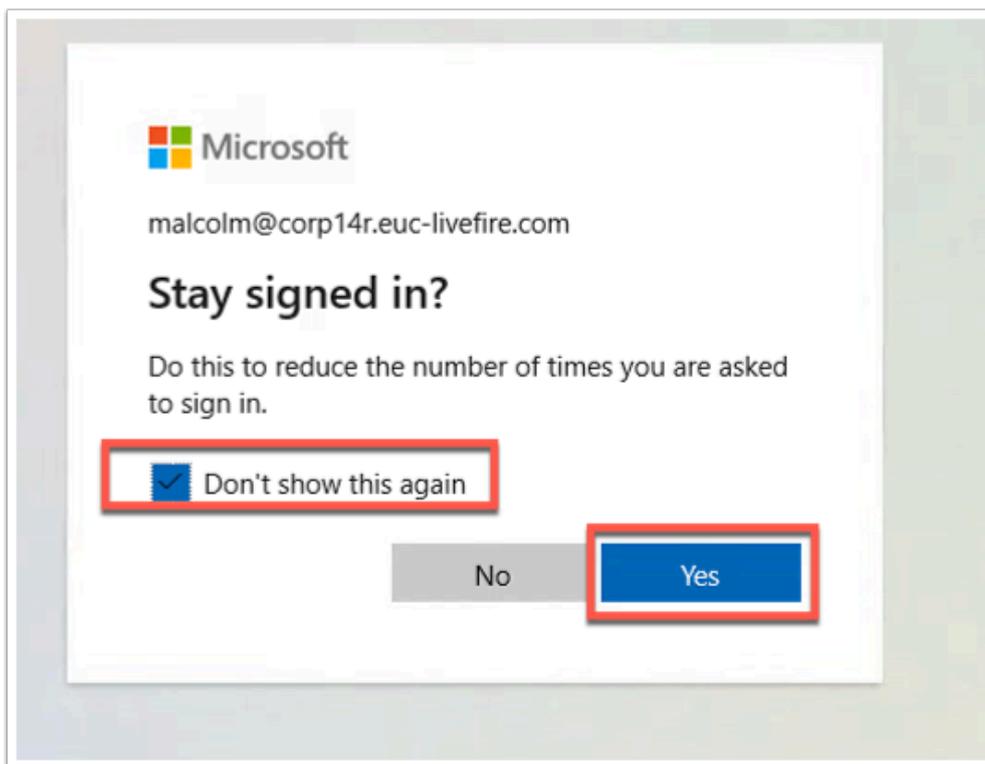
6. If you open **Workspace ONE UEM** you will see that the device has been enrolled to **Malcolm**. Device name is W11-BLR-FC-1
- Notice I haven't had to authenticate Malcolm to the Hub it took these credentials from the signed in user as defined by the installation script.



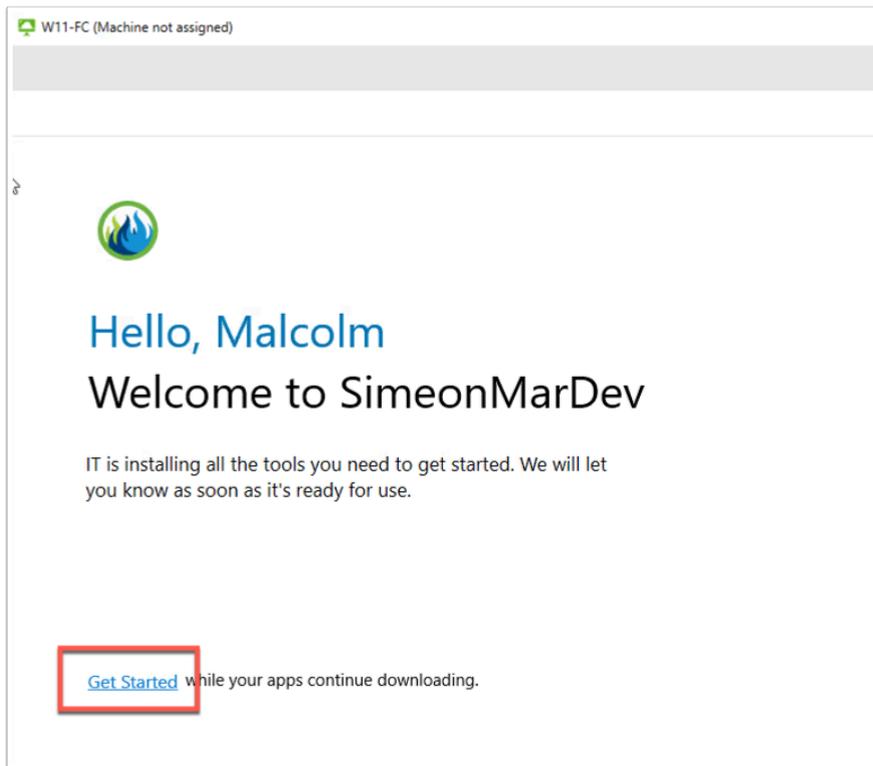
7. In the Intelligent hub you will now be re-directed to Azure for authentication as we have set the authentication method.
- type **Malcolm@corpXXX.euc-livewire.com** and click **Next**.



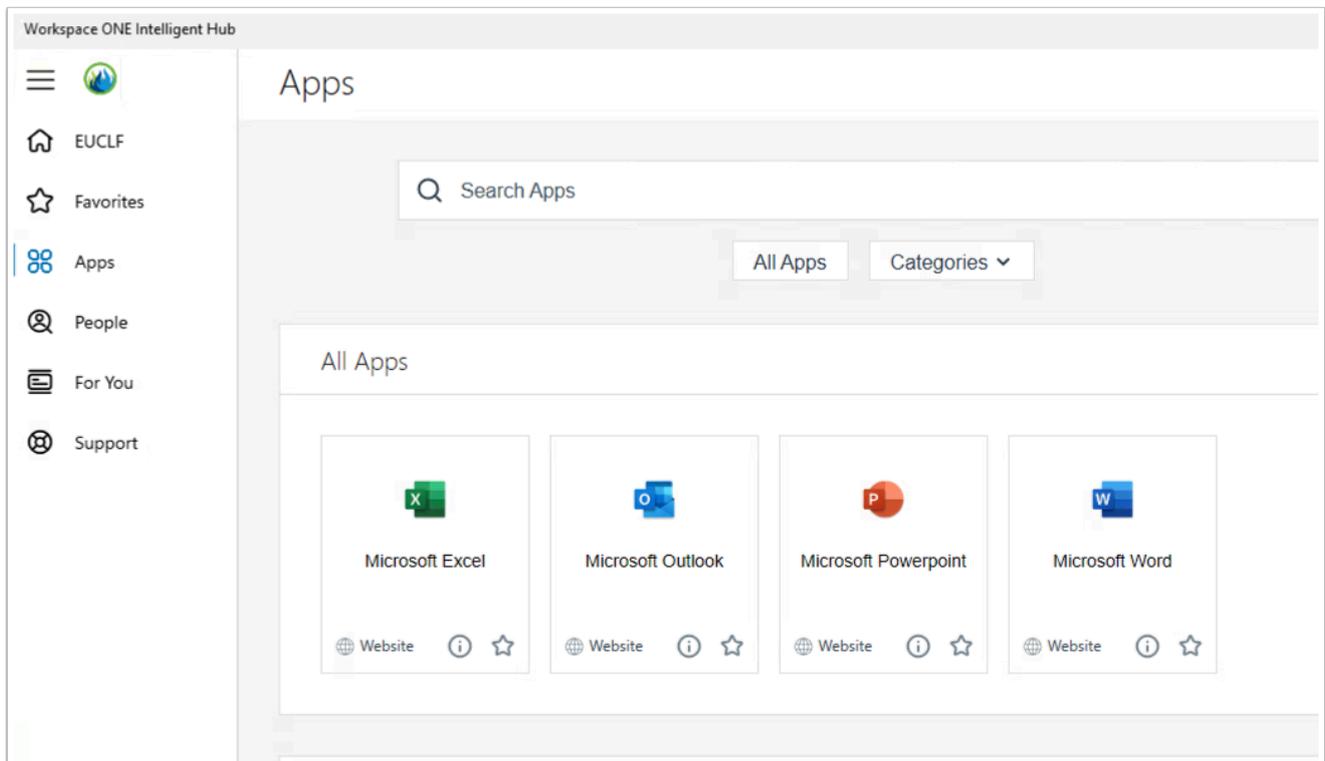
8. Type password **VMware1!** and click **Sign in**.



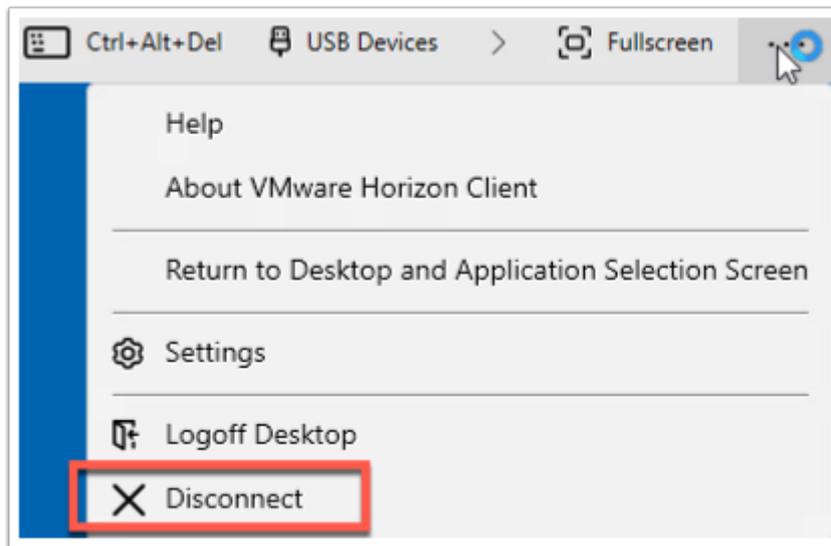
9. Check **Don't show this again** and click **Yes**.



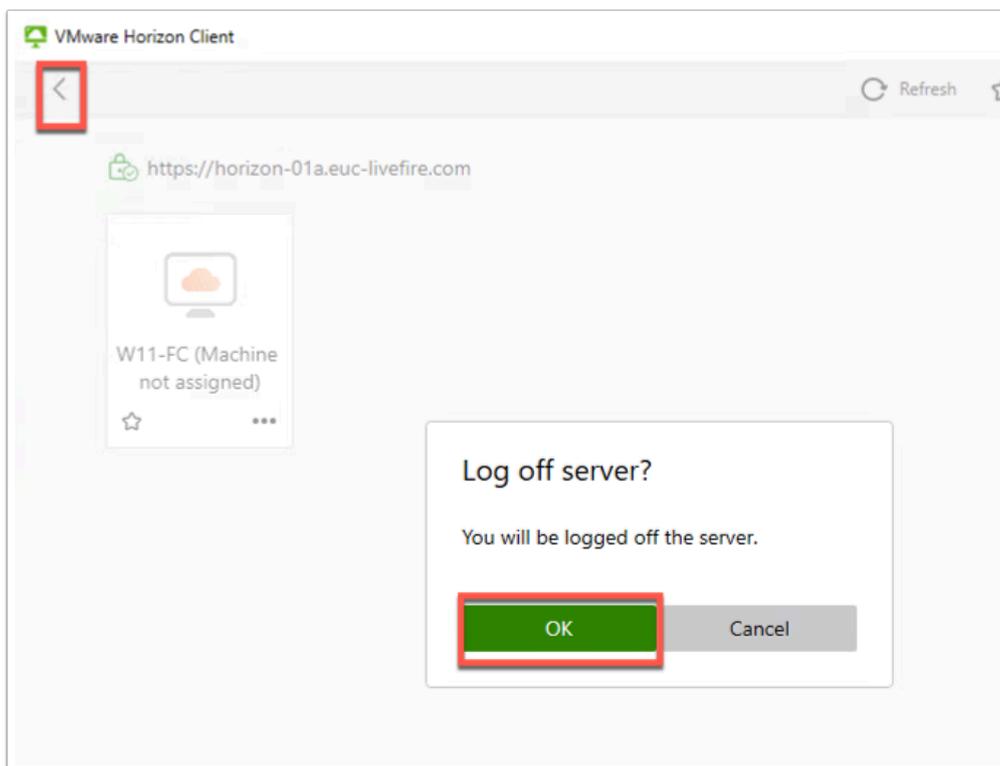
10. Click **Get Started**. You are now logged into the **Intelligent Hub**.



11. You should see your apps now as pre-configured in previous labs.



12. **Disconnect** from this Horizon Session.



13. Click the **back arrow** then you are asked if you want to log off, click **OK**.

This concludes the manual enrollment of device in to Workspace ONE UEM and automated enrollment of persistent VMs into Workspace ONE UEM.

Author: Simeon Frank