

Federating AZURE with Workspace ONE Access and Microsoft 365

Introduction

Disclaimer:

FACT : Microsoft Azure Portal is updated every 36 hours. Please do not expect perfection in this guide as you will not get perfection

- As you might know its becoming increasingly difficult to create Microsoft 365 Developer trial Accounts. As Livefire Instructors we have consumed all our good will on the Microsoft side and we are unable to create any new Microsoft 365 Developer Accounts. For the time being we are able to use existing trial accounts
- If you are unsure regarding what to do or your next step or anything related to the Azure console and how it relates to the existing guide. Please ASK, we are happy to help
- Your understanding related to these challenges will be greatly appreciated

There are now two groups types that will attempt this lab:

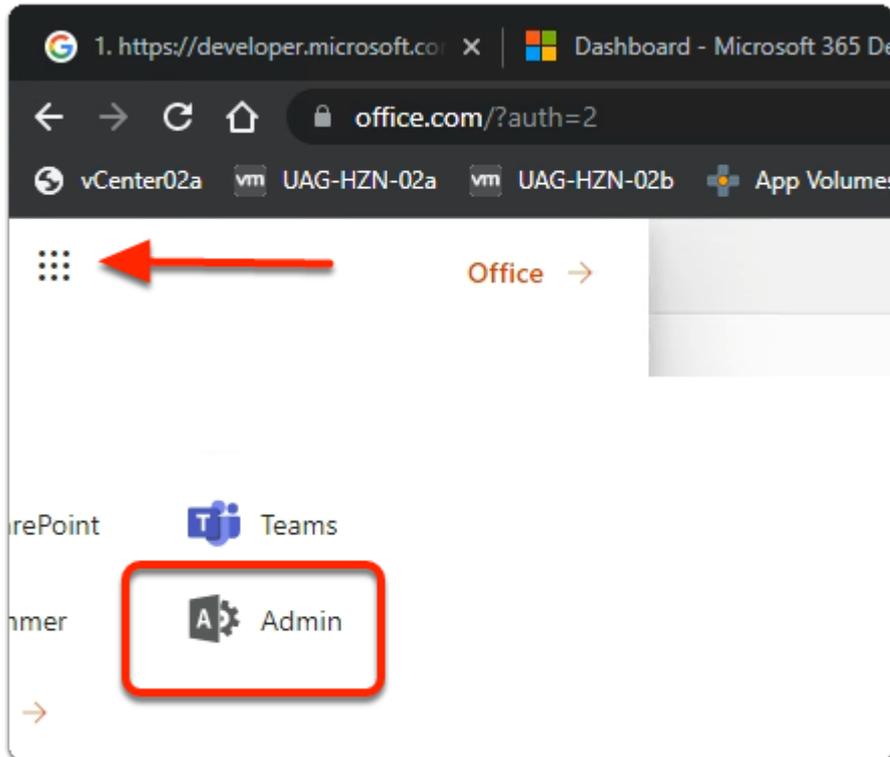
1. Attendees that have managed to register and subscribe to the Developer Microsoft 365 environment
OR
 2. Attendees that are using a trial account that has been used before
1. **Attendees that have managed to register and subscribe to the Developer Microsoft 365 environment**
 - On your **Controlcenter server**
 - Open a new Chrome Browser session and go to the following URL:
 - <https://developer.microsoft.com/en-us/microsoft-365/dev-program>
 - Login with your developer account
 - select **Join Now**
 - This should take you to the **Microsoft 365 Developer Program**,
 - select **Go to subscription**
 - Login with your **CloudAdmin** credentials

 The above steps assume you have your own developer account

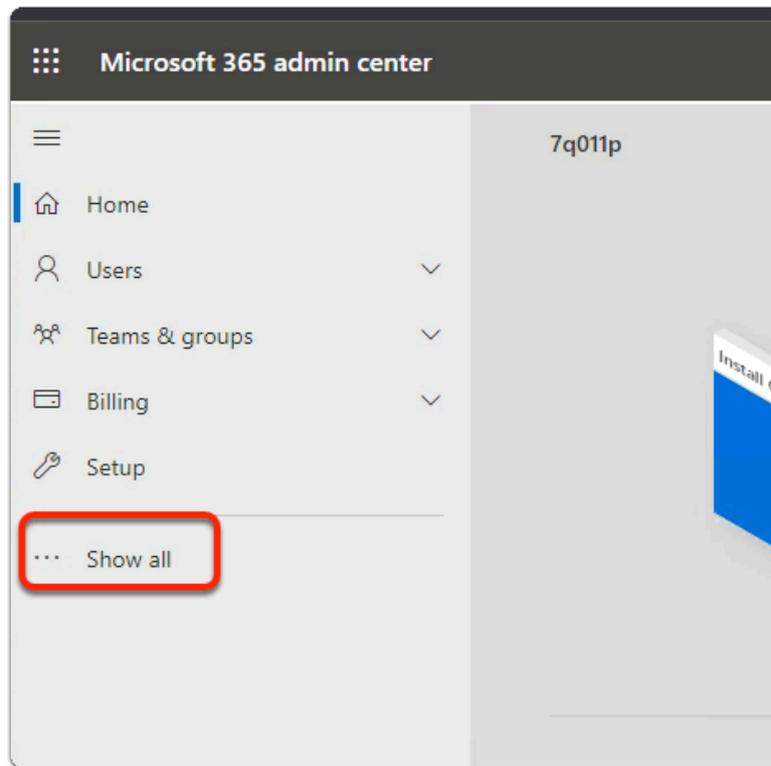
2. **Attendees that are using a trial account that has been used before**

- On your **Controlcenter server**
 - Open a new Chrome Browser session and go to the following URL:
 - <https://portal.office.com>
 - Login with your assigned Cloud Admin Credentials

Part 1: Preparing the Microsoft 365 environment to use a dedicated domain name

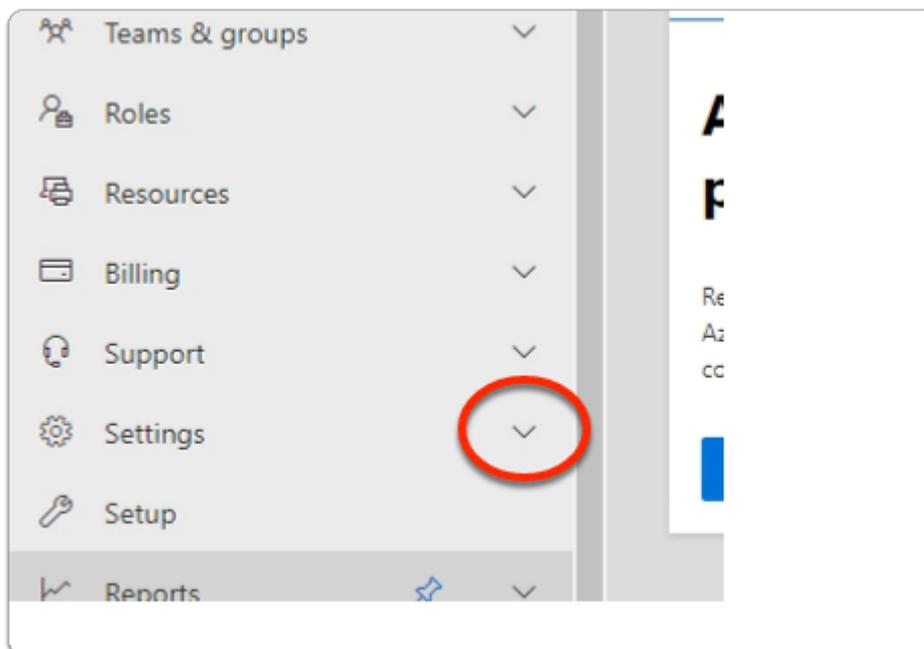


1. In the top left-hand corner off Microsoft 365
 - Select the **9 dotted square**
 - Once the **Apps** pop out expands
 - Select **Admin**



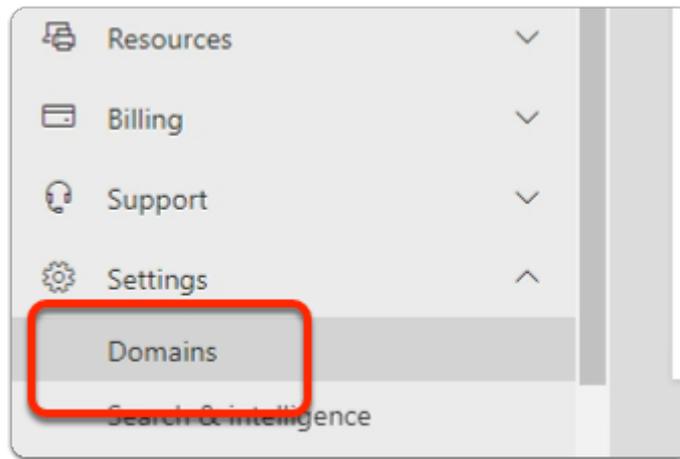
2. In the **Microsoft 365 admin center** window

- Select **Show all**

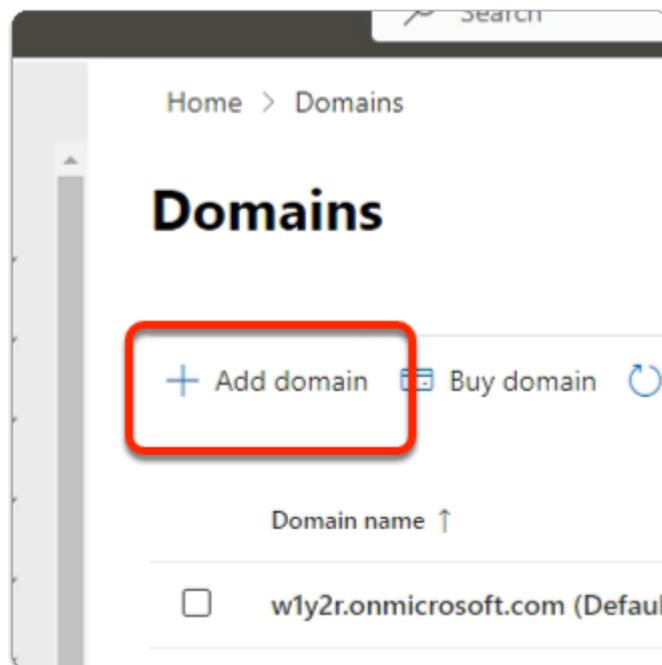


3. In the **Microsoft 365 admin center** window

- Under **Support**
 - expand **Settings**



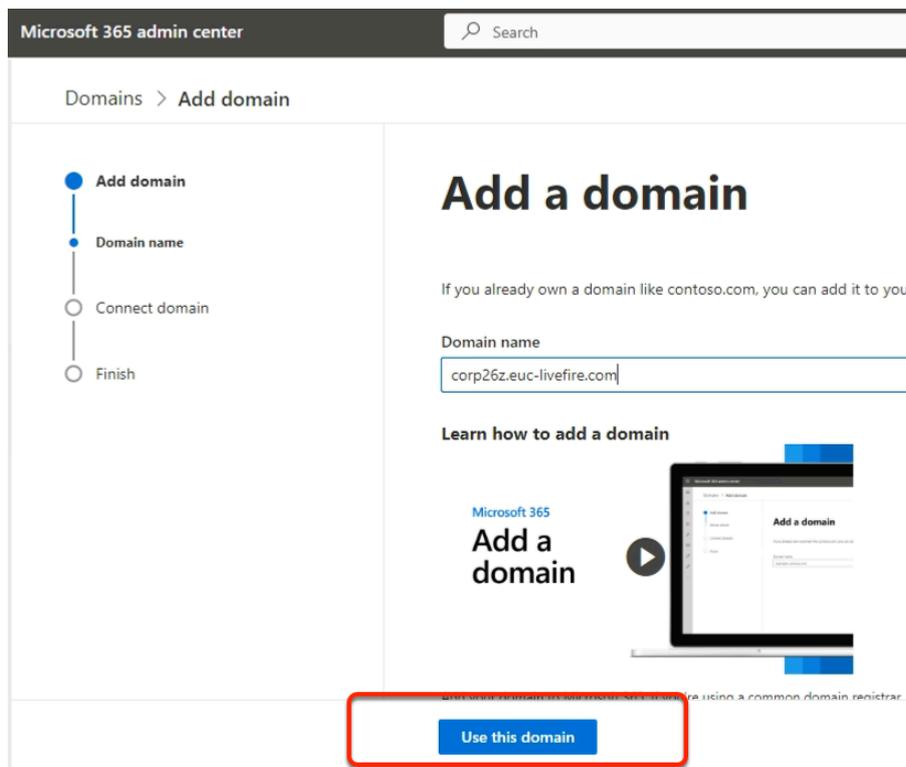
4. In the **Microsoft 365 admin center** window
 - Under **Settings**
 - select **Domains**



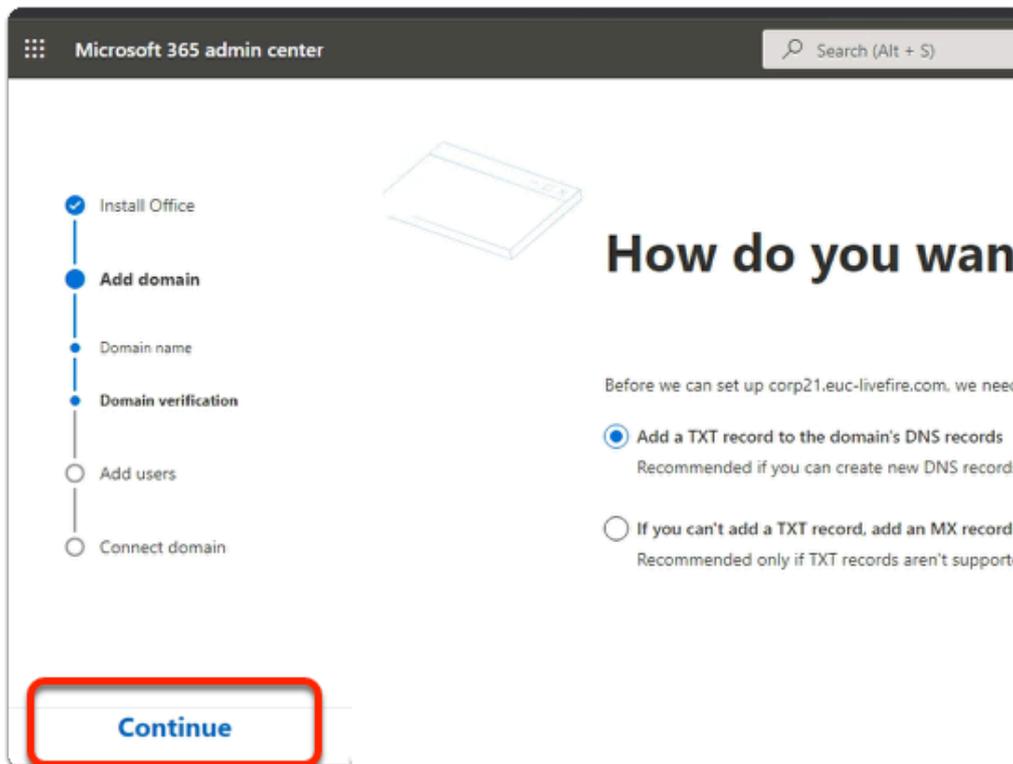
5. In the **Domains** area
 - Select **+ Add domain**

File Password	Assigned Domain	Landing
re1!	Corp01f	dwu
re1!	Corp02f	dwu
re1!	Corp03f	dwu
re1!	Corp04f	dwu
re1!	Corp05f	dwu
re1!	Corp06f	dwu

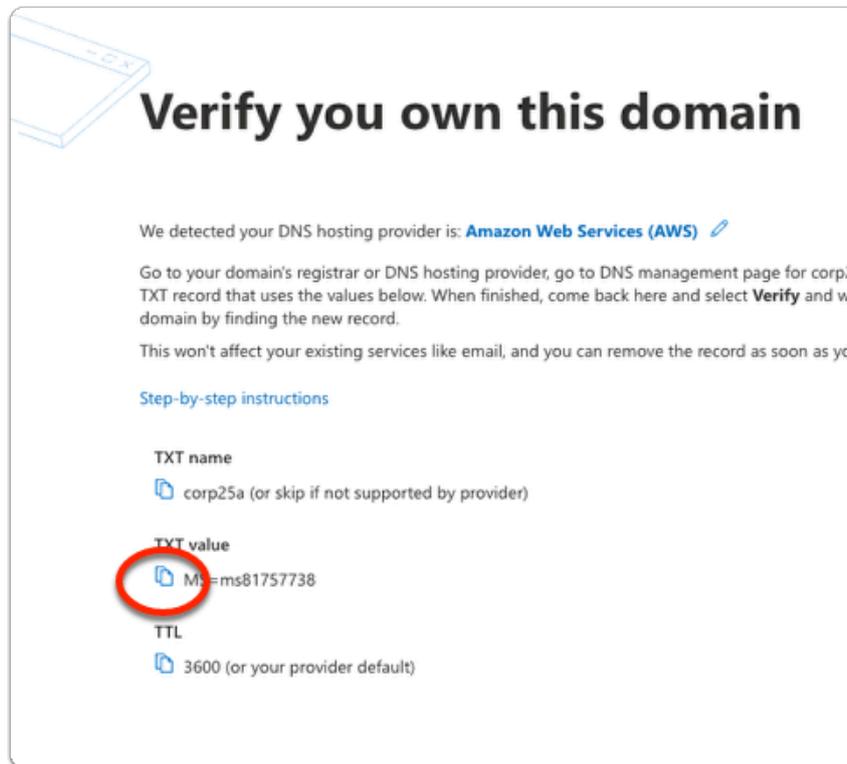
- i** NOTE: Before moving onto the next section, ensure that you are **100% clear** what **YOUR** registered Domain will be.
- In the course lab we will use a Domain naming convention based on the location we are delivering at.
 - We will use the convention corp**XXX**.euc-livefire.com
 - Where **XXX** is your Assigned Domain, which you will find in Microsoft Teams in the Attendee Accounts sections
 - On the **Microsoft 365 admin center** ensure the **Connect a domain you already own** radio button is selected and below *type your registered Domain name*



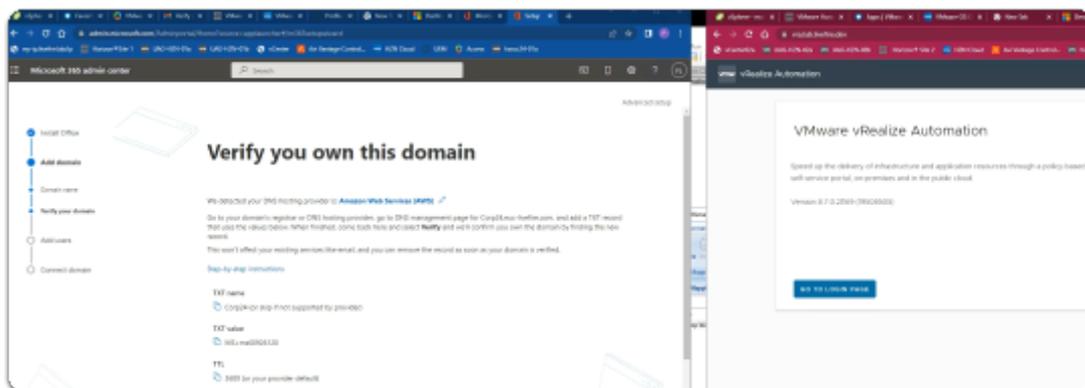
6. In the **Microsoft 365 admin center** window
 - In the **Add domain** area
 - Under **Yes, add this domain now**
 - enter **corpXXX.euc-livewire.com**
 - Where **XXX** is your assigned Domain identifier
 - At the **bottom of the page**
 - Select **Use this domain**



7. In the **Microsoft 365 admin center** window
 - In the **How do you want to verify your domain?**
 - Ensure the **radio button** next to **Add a TXT record to the domain's DNS records is enabled (default)**
 - Select **Continue**

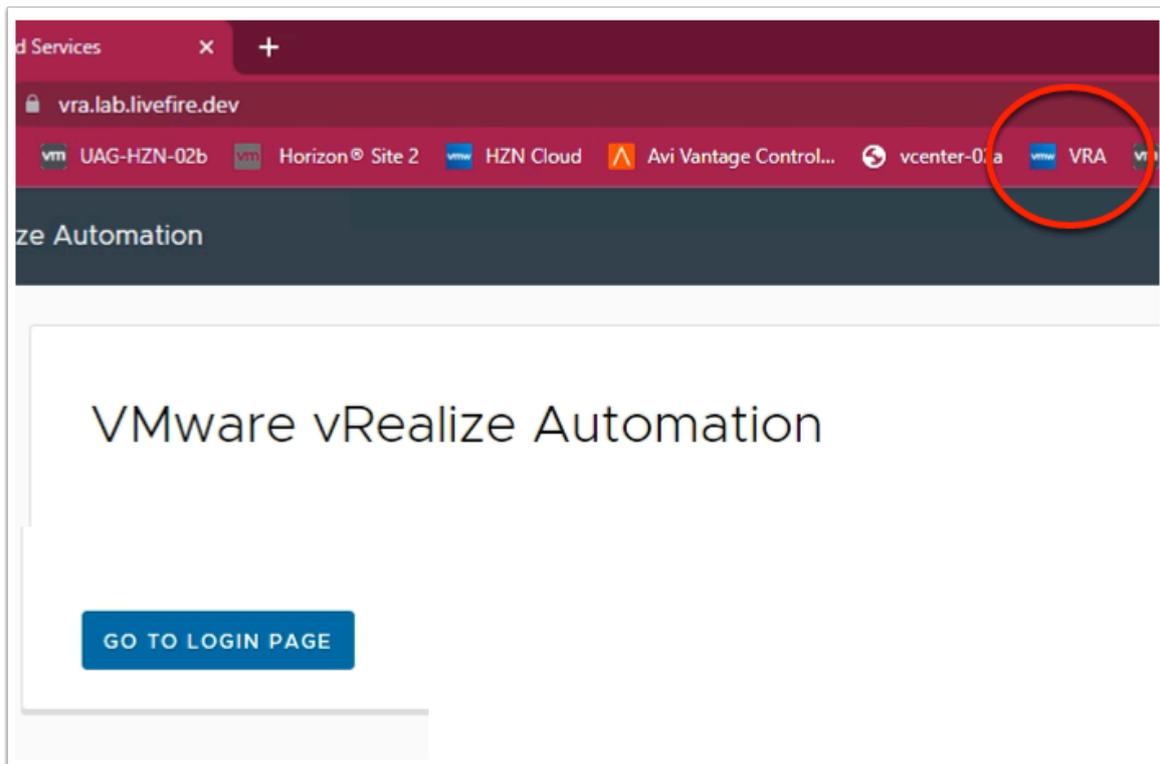


8. In the **Microsoft 365 admin center** window
 - In the **How do you want to verify your domain?**
 - **Below TXT value**
 - Copy the **MS= ms**
 - In the following steps, we will have this value entered into your assigned Zone database in AWS Route 53 using vRealize automation

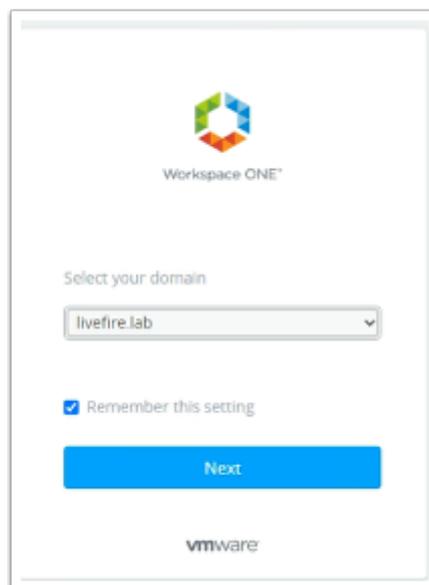


💡 Do step 9: VRA automation on a separate browser profile.

If you were doing your Azure registration on the Site 1 profile then might be helpful to do the VRA on the Site 2 Profile and have both profiles open side by side.

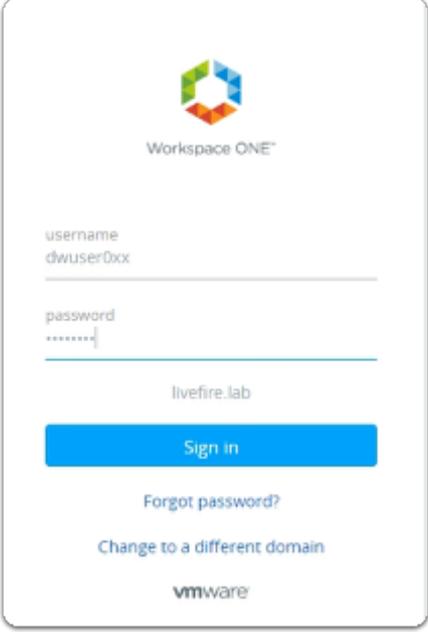


9. On your **Controlcenter desktop**,
 - On your **Site 2 browser**
 - Open a **new Tab**
 - In the **Address bar**
 - enter <https://vra.lab.livefire.dev/>
 - Select **GO TO LOGIN PAGE**



10. In the Workspace ONE Login

- Under **Select your domain**
 - Ensure **livefire.lab** selected
- select **Next**



Workspace ONE™

username
dwuser0xx

password
.....|

livefire.lab

Sign in

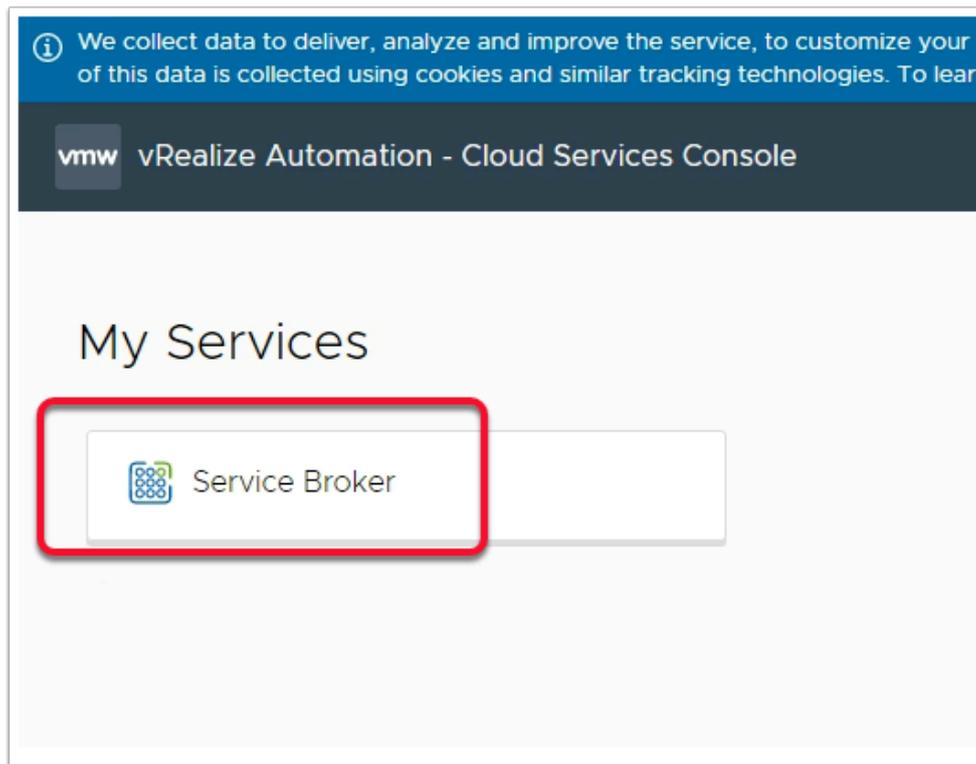
Forgot password?

Change to a different domain

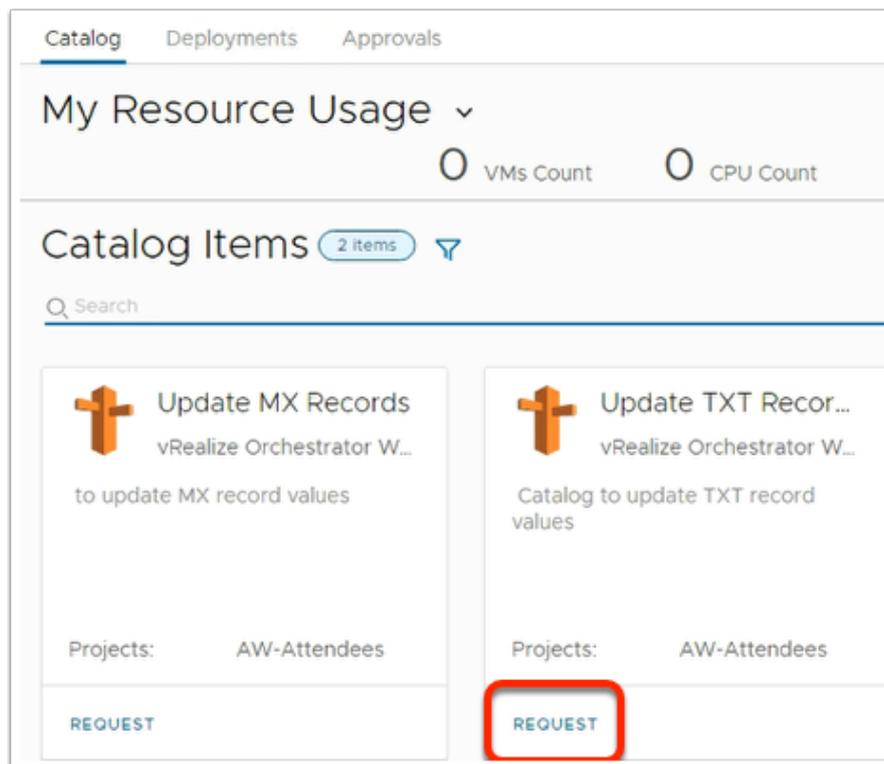
vmware

11. In the Workspace ONE login

- Under **username**
 - Enter your assigned **dwuser0XX** account
 - **XX** will be your **assigned Student Login ID**
- Under **password**
 - Enter your **assigned password**
- Select **Sign in**

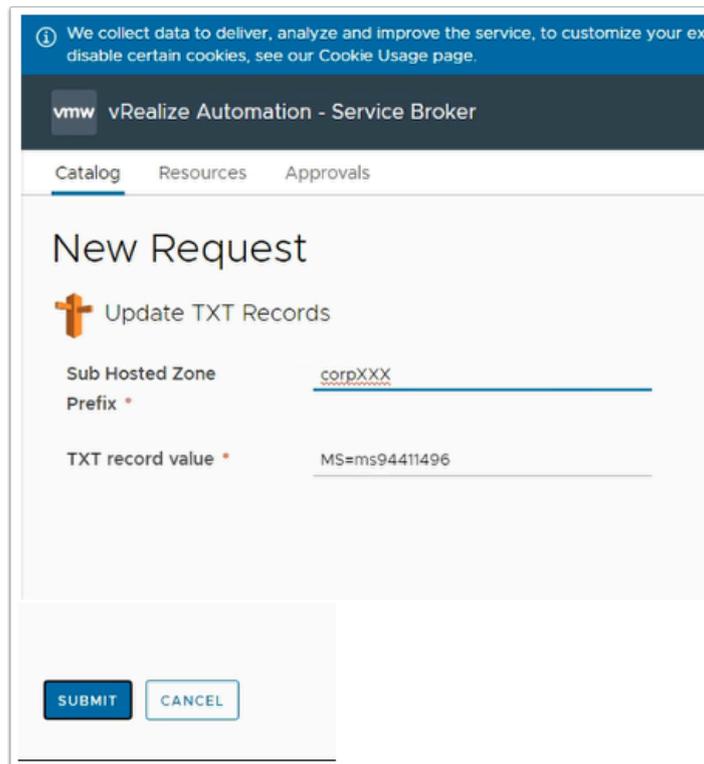


12. In the **vRealize Automation - Cloud Services Console**
 - Under **My Services**
 - Select **Service Broker**



13. In the **My Resource Usage** window
 - Under **update TXT Records**

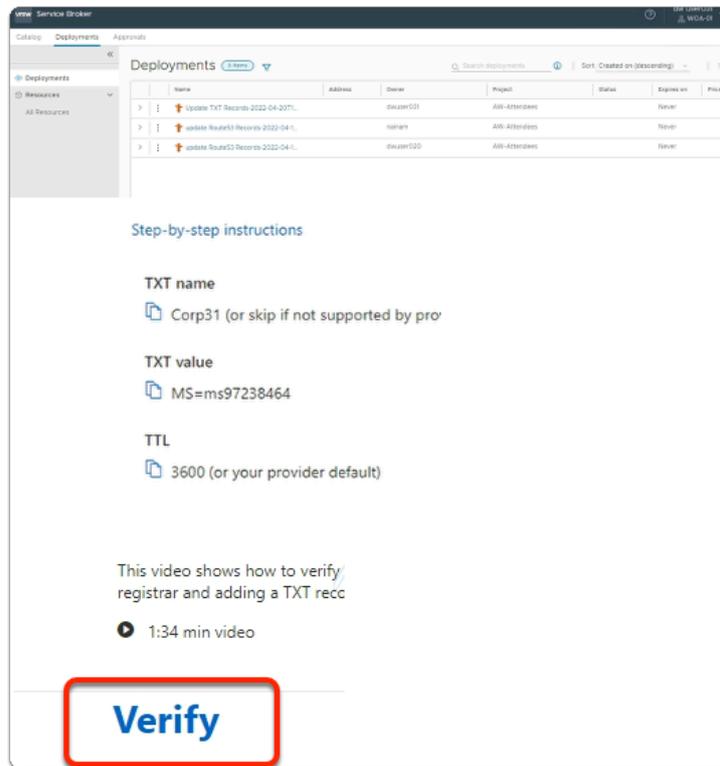
- Select **REQUEST**



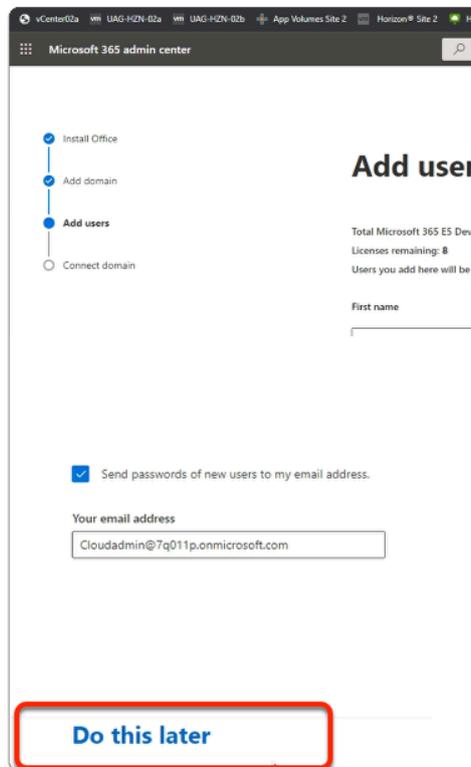
The screenshot shows the 'vRealize Automation - Service Broker' interface. At the top, there is a blue banner with a cookie notice: 'We collect data to deliver, analyze and improve the service, to customize your experience. You can manage preferences or disable certain cookies, see our Cookie Usage page.' Below the banner is a dark header with the 'vmw' logo and the text 'vRealize Automation - Service Broker'. A navigation bar contains 'Catalog', 'Resources', and 'Approvals', with 'Catalog' being the active tab. The main content area is titled 'New Request' and features a plus sign icon followed by 'Update TXT Records'. There are three input fields: 'Sub Hosted Zone Prefix *' with the value 'corpXXX', 'TXT record value *' with the value 'MS=ms94411496', and a third field that is empty. At the bottom left, there are two buttons: 'SUBMIT' (in blue) and 'CANCEL' (in white with a blue border).

14. In the **New Request** page

- Update the following next to:
 - **Sub Hosted Zone Prefix*** enter **your domain**
 - enter **CorpXXX**, **XXX** represents your assigned domain
 - TXT record value* Paste **your TXT value (from step 7)**
- Select **SUBMIT**

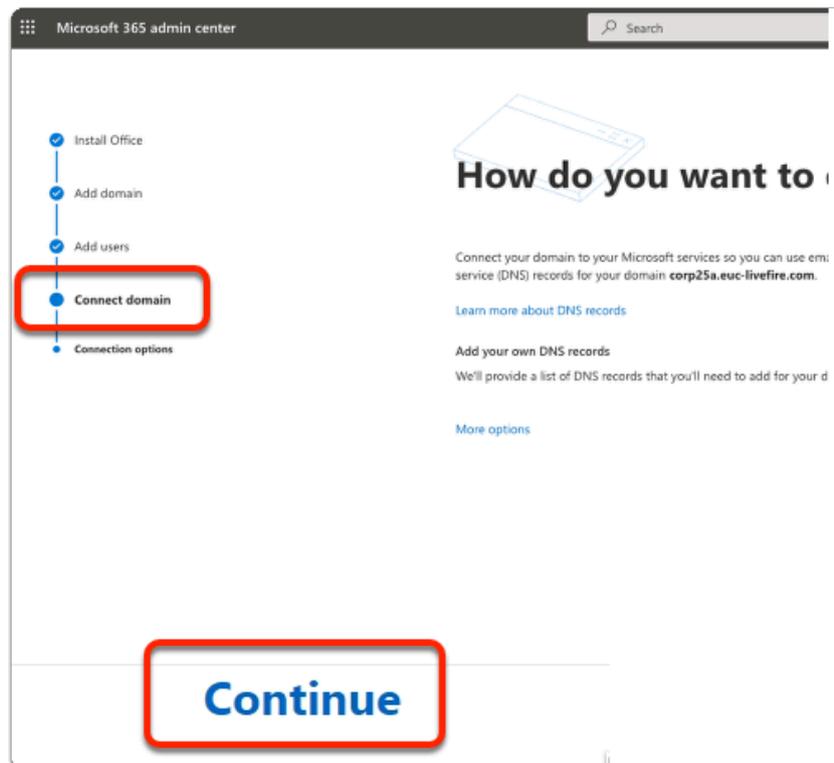


15. On your **Microsoft 365 admin center** page
 - When the **realize automation** is complete
 - Select **Verify**



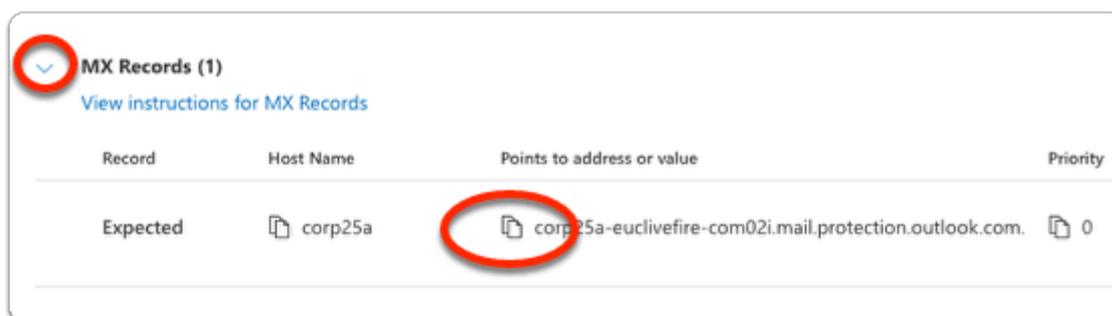
16. In the **Microsoft 365 admin center** window
 - In the **Add users and assign licenses** page

- At the bottom of the page
 - Select **Do this later**



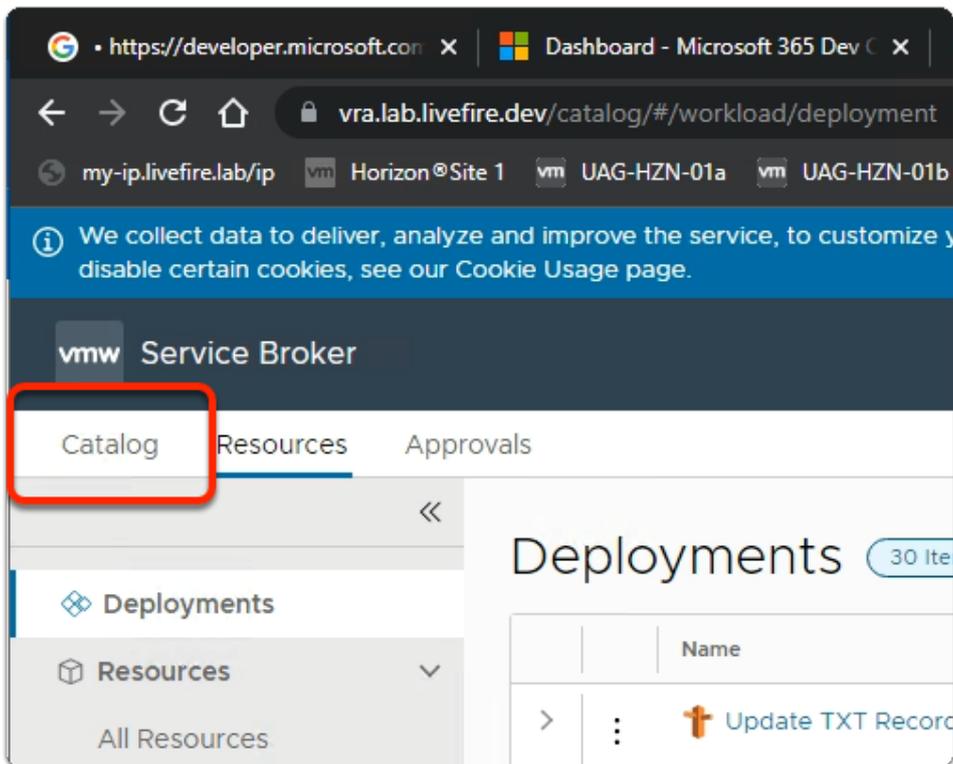
17. In the **Microsoft 365 admin center** window

- In the **Connect domain** section
 - At the bottom of the page
 - Select **Continue**

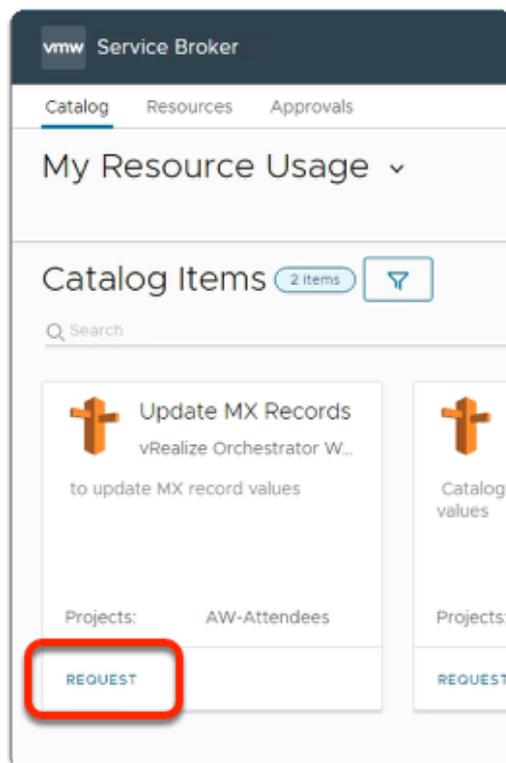


18. In the **Microsoft 365 admin center** window

- In the **Connect domain > ADD DNS records** section
 - Next to **MX records (1)**
 - Expand the **dropdown**
 - Under **Points to address or value** and in line with **Expected**
 - **Copy** the output



19. Switch back to your **Service Broker** session
 - Select the **Catalog** tab



20. In the **Catalog** area
 - Under **Update MX Records**
 - select **REQUEST**

Catalog Resources Approvals

New Request

 Update MX Records

Sub Hosted Zone

Prefix *

MX record value *

Please note xxx is your attendee identifier.

21. In the **Service Broker**

- **New Request**

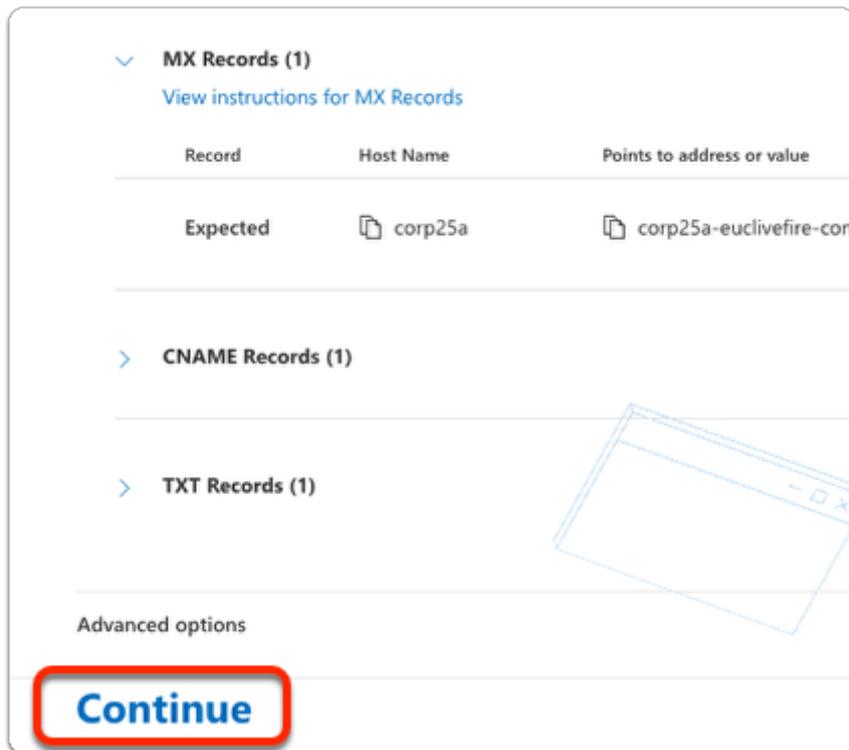
- **Update MX Records** page

- Next to:

- **Sub Hosted Zone Prefix*** enter **corpXXX**
 - Where **XXX** is your assigned Domain identifier

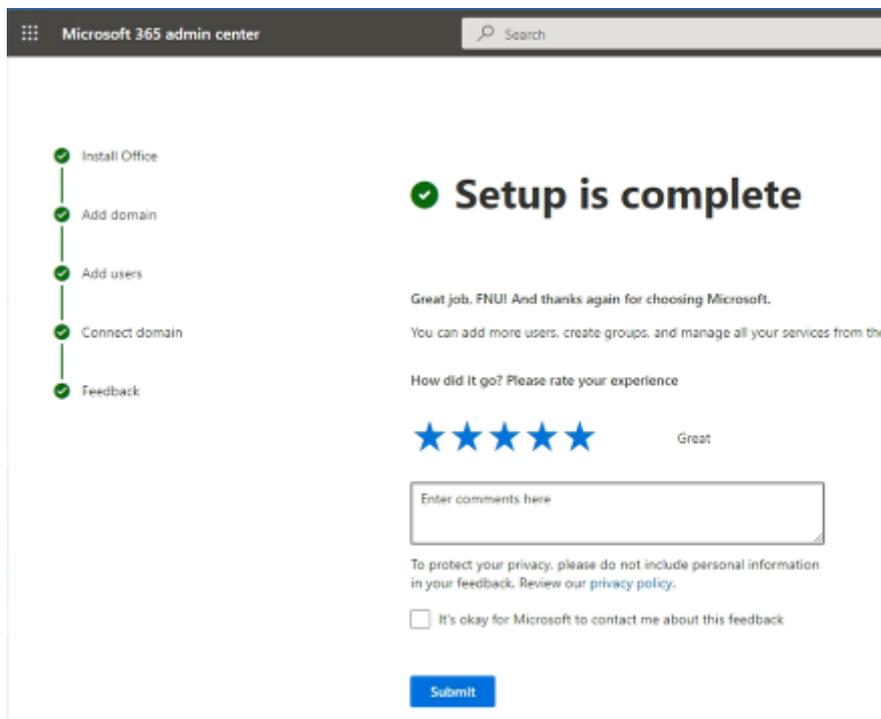
- **MX record value*** paste **your MX record**

- Select **SUBMIT**



22. On the **Connect domain** page

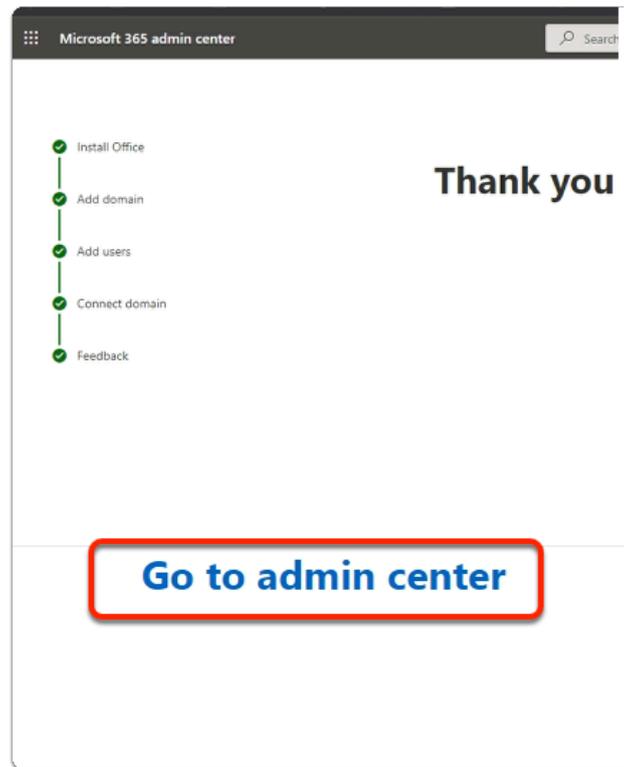
- At the bottom
- Select **Continue**



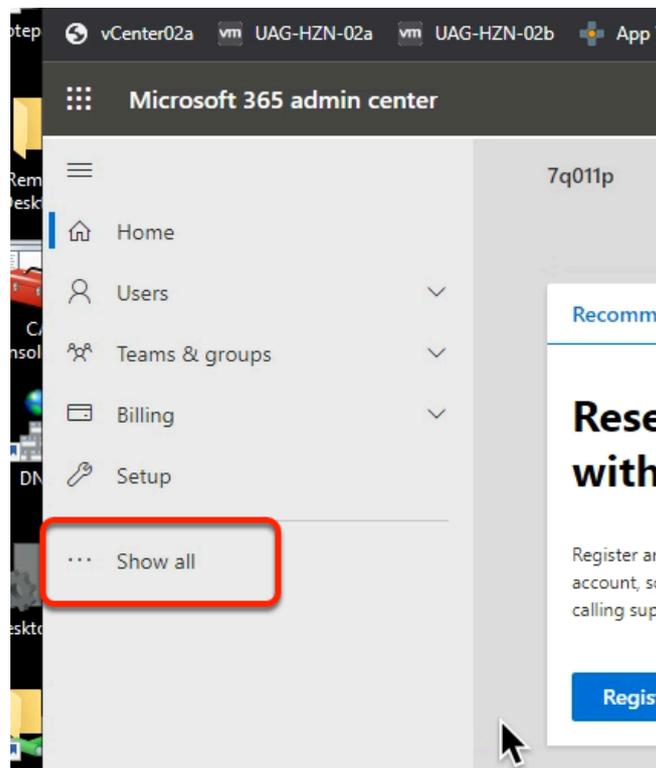
23. In the **Microsoft 365 admin center** window

- In the **Setup is Complete** page
- Offer a 5 star rating

- Select **Submit**

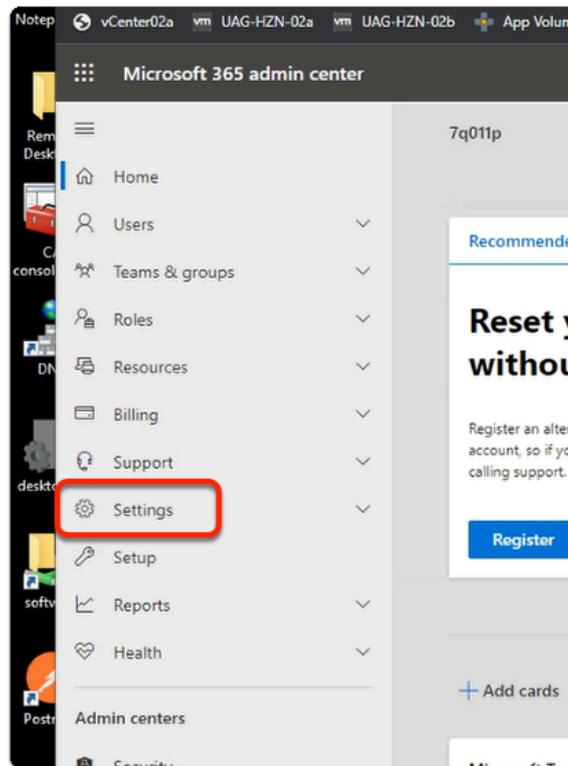


24. In the **Microsoft 365 admin center** window
- In the **Thank you for your feedback** page
 - At the bottom of the page
 - Select **Go to admin center**



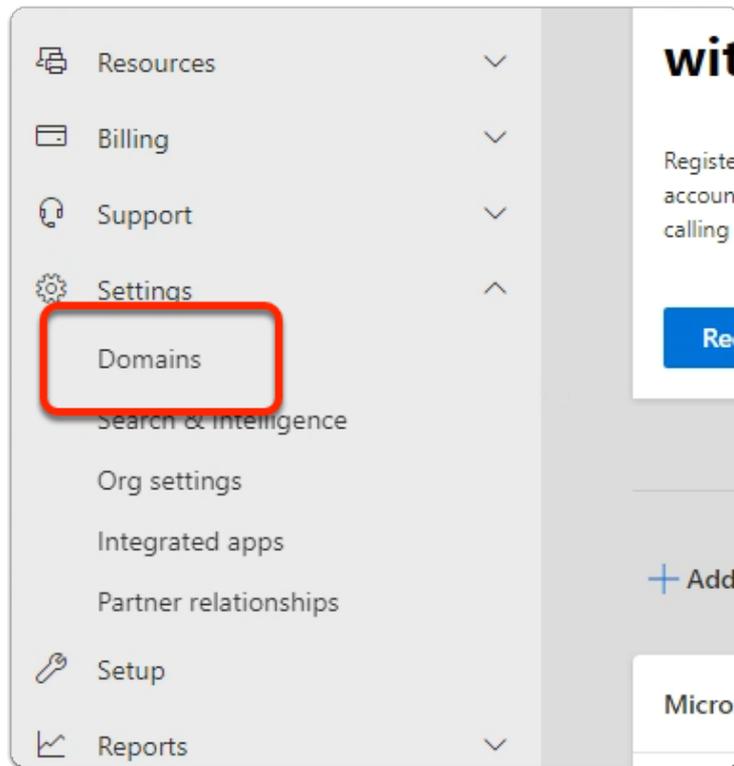
25. In the **Microsoft 365 admin center** window

- In the left-hand pane **Inventory**
 - Select ... **Show all**



26. In the **Microsoft 365 admin center** window

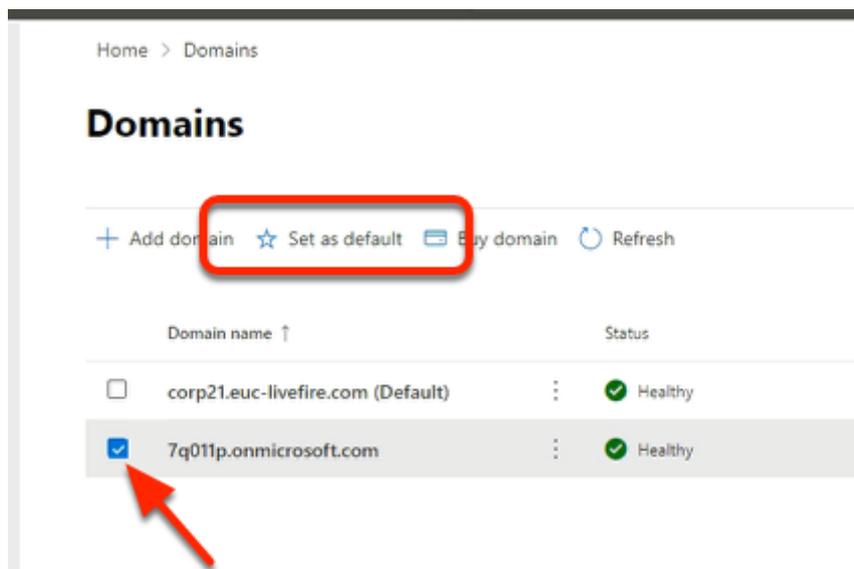
- In the left-hand pane **Inventory**
 - Expand **Settings**



22. In the **Microsoft 365 admin center** window

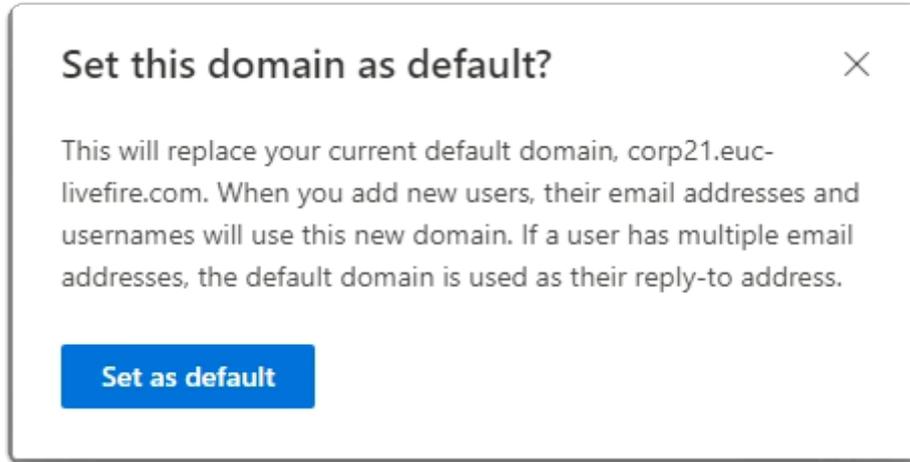
- In the left-hand pane **Inventory**
 - Under **Settings**
 - Select **Domains**

💡 If you are using an existing account, its very likely you wont have to change your default domain. Validate and if necessary do the change



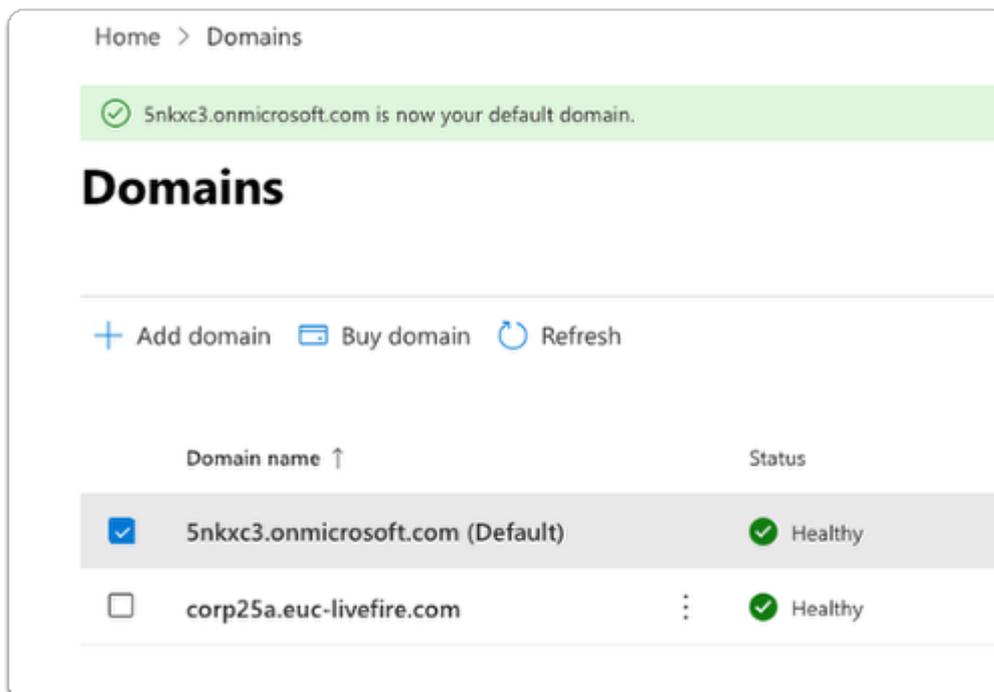
22. In the **Domains** area

- Under **Domain name**
 - Next to your unique ***.onmicrosoft.com** domain
 - select the **checkbox**
- Under **Domains**, in the **Task area**
 - Select **Set as default**



23. In the **Set this domain as default?** window

- Select **Set as default**



24. In the **Domains** page

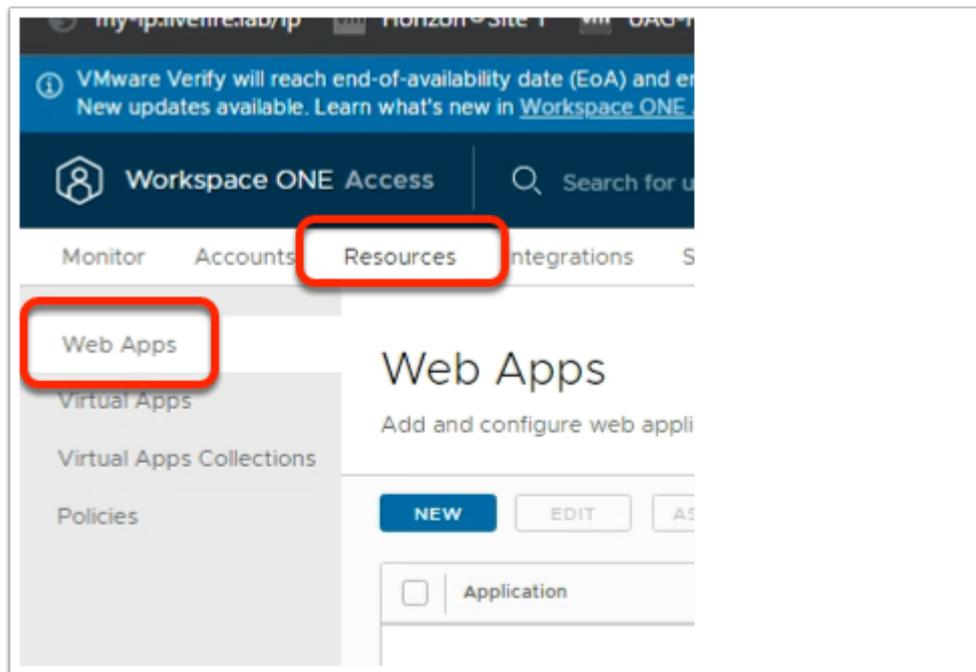
- Validate your default configuration

i Your assigned domain should NOT be your (Default) domain. Your setup should look like the above example

Part 2: Setting the authentication status of Azure from Managed to Federated.

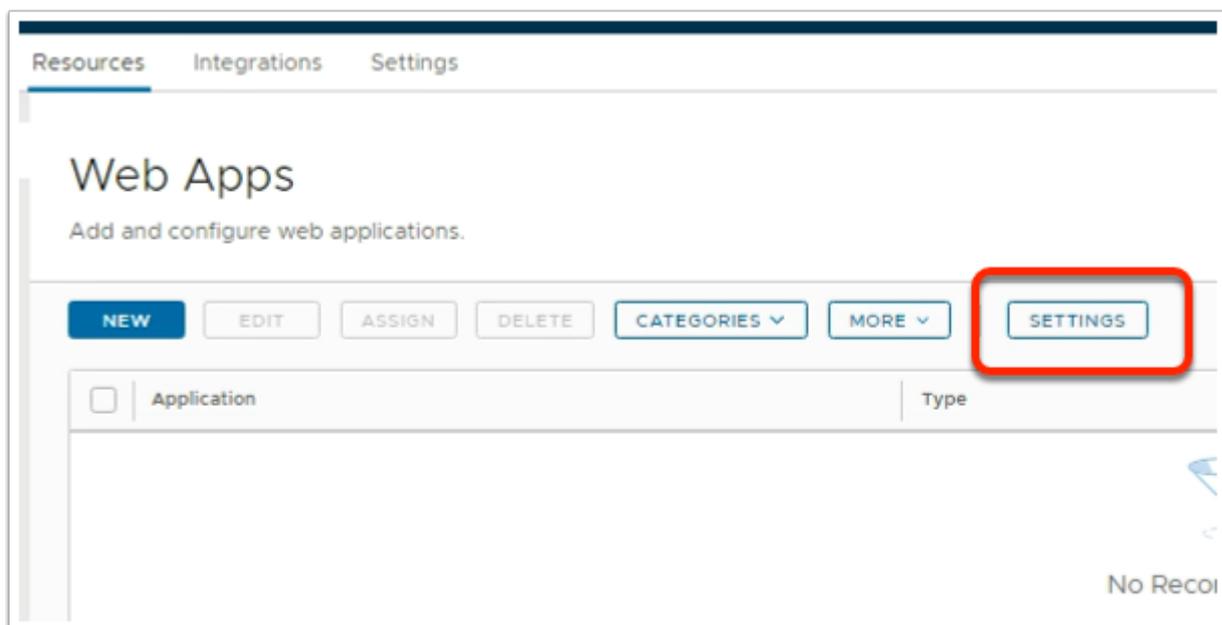
The screenshot displays the Workspace ONE login page. It includes a 'Select Your Domain' dropdown menu with 'System Domain' selected, a 'Remember this setting' checkbox, and a 'Next' button. Below this is the VMware logo and another Workspace ONE logo. The login form contains fields for 'Username' (filled with 'administrator'), 'Password' (masked with dots), and 'System Domain'. A 'Sign in' button and a 'Forgot Password?' link are also visible. At the bottom, a navigation bar shows 'TA Tenant Admin' and a 'Workspace ONE Access Console' menu with options for 'Manage Hub Experience', 'Account', and 'Sign out'.

1. On your ControlCenter server
 - **Open** a new browser tab
 - Enter your Workspace ONE Access **tenant url**
 - Log in with your Sysadmin credentials
 - To the right of the **Intelligent Hub Console** console
 - Select and right-click **TA**
 - Select **Workspace ONE Access Console**



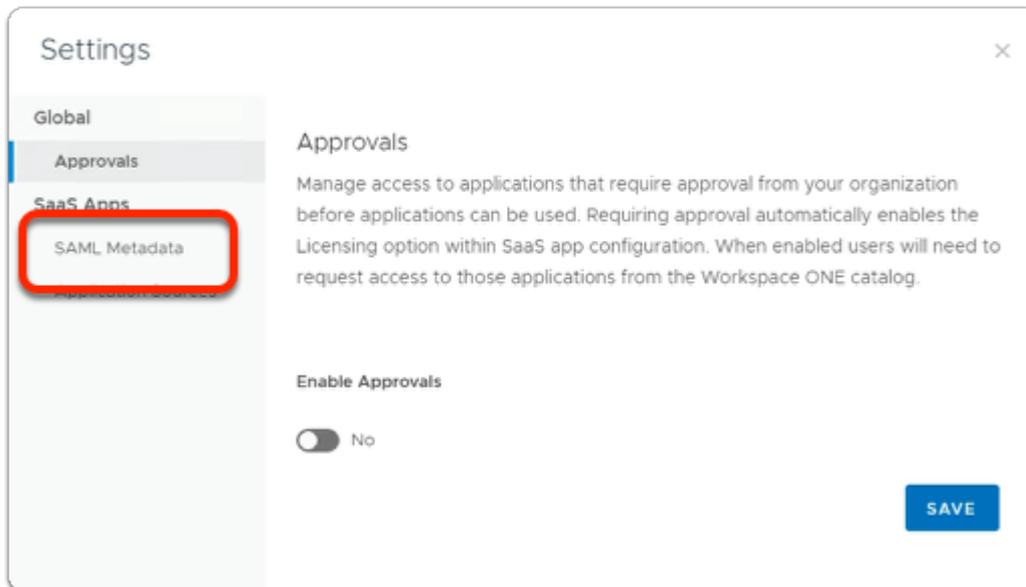
2. In the Workspace ONE Access Console

- Select **Resources**
- In the left menu
 - Select **Web Apps**

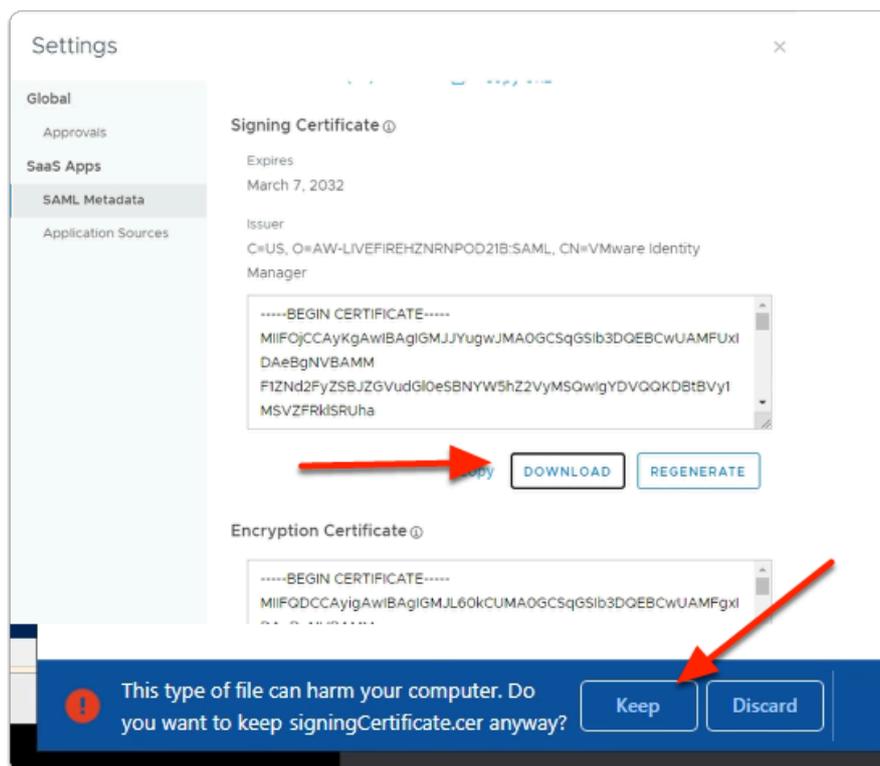


3. In the Workspace ONE Access console

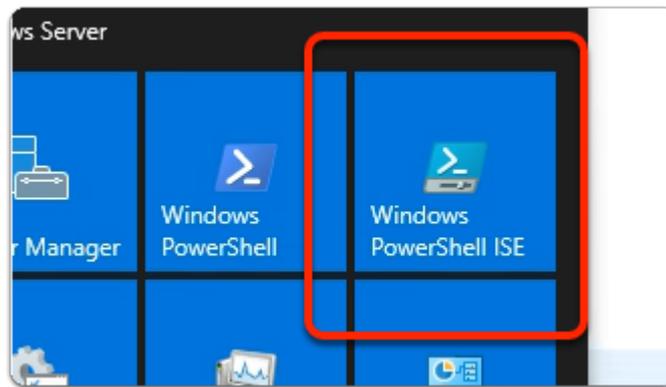
- In the right-hand side of the **Web Apps** area
 - Select **SETTINGS**



4. In the **Settings** window
 - Select **SAML Metadata**

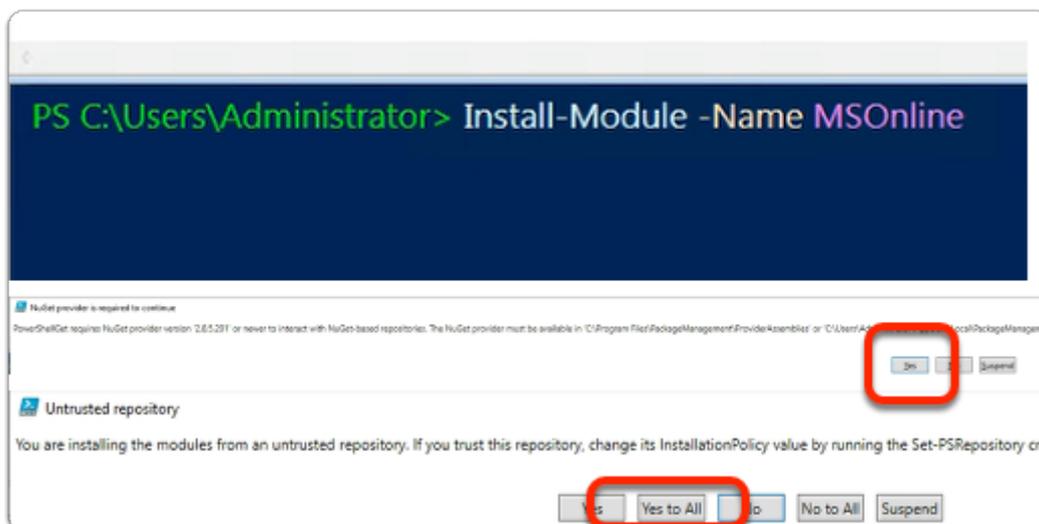


5. In the **SAML Metadata** area
 - In the right-pane, **scroll down** until you find **Signing Certificate**
 - Below **Signing Certificate**
 - Select **DOWNLOAD**
 - In the bottom left-corner of your browser
 - When prompted to keep a potentially harmful file
 - Select **Keep**



6. On your **ControlCenter** server

- On the **Desktop**
 - Select the **START** button
 - From the **Start Menu**
 - select the **Windows Powershell ISE** Shortcut



7. In the **Azure Powershell ISE** module

Enter the following:-

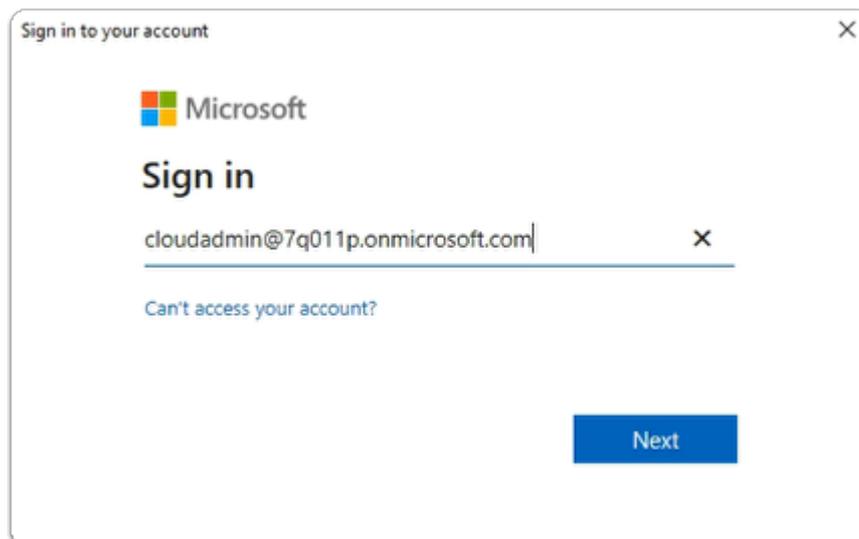
- `Install-Module -Name MSOnline`
 - with your keyboard
 - select **ENTER**
 - When prompted; with the :-
 - " **NUGET provider is required to continue** " window
 - select **Yes**
 - When prompted; with the :-
 - "**Untrusted repository**" window
 - select **Yes to All**

```
PS C:\Users\Administrator> Install-Module -Name MSOnline

PS C:\Users\Administrator> Connect-MsolService
```

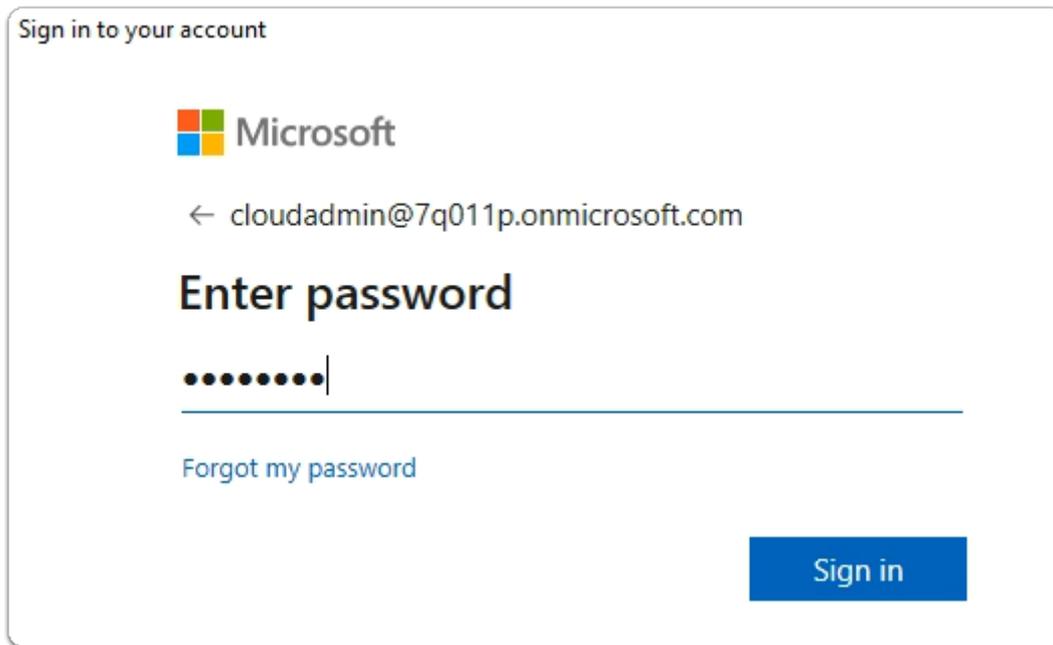
8. In the **Azure Powershell ISE module**

- Enter the following:-
 - `Connect-MsolService`
 - with your keyboard
 - select **ENTER**

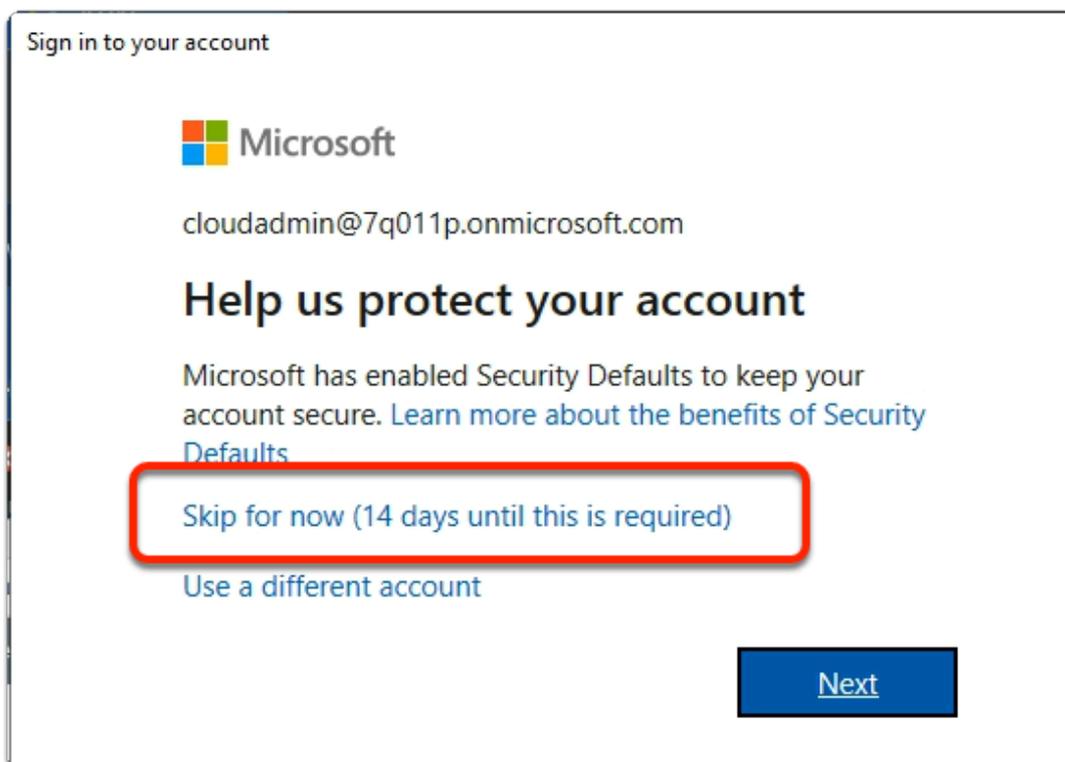


9. In the **Sign-in** to your account window

- Under Sign in
 - enter your **Cloud Admin account**
- Select **Next**



10. In the **Sign in to your account** window
 - Under **Enter password**
 - **Enter your *Cloud Admin Password***
 - Select **Sign in**



11. In the **Sign in to your account** window
 - Select **Skip for now (14 days until this is required)**

💡 If you are using your own account you will get this, If you are using an assigned account ignore this

```
PS C:\Users\Administrator> Install-Module -Name MSOnline

PS C:\Users\Administrator> Connect-MsolService

PS C:\Users\Administrator> Get-MsolDomain

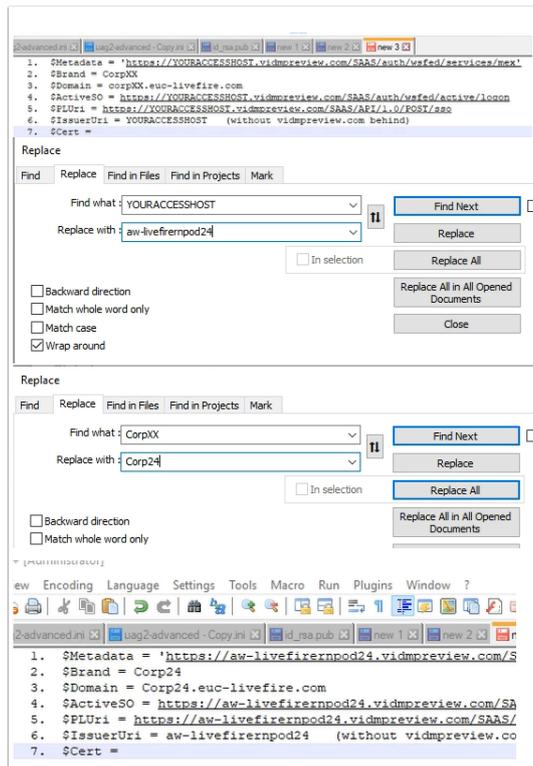
PS C:\Users\Administrator> Get-MsolDomain

Name                Status Authentication
-----
ym1m2.onmicrosoft.com Verified Managed
Corp24.euc-livewire.com Verified Managed
```

12. In the **Azure Powershell ISE module**

- Enter the following:-
 - **Get-MsolDomain**
 - with your keyboard
 - select **ENTER**

- Note that both your Domains are Authentication status are **Managed**
- When we are done
 - our aim is to change the status of your custom domain to **Federated**
- We will now proceed step-by-step to achieve this goal



Disable Clickable Link Settings in Notepad++

Select **Settings > Preferences >**

Select **Cloud & Link**

Under **Clickable Link Settings**

Next **Enable**

Uncheck the **checkbox**

13. On your ControlCenter server

- **Copy** and **Paste** the below commands into **Notepad++**
 - Where you have **YOURACCESSHOST**
 - Replace with your **Workspace ONE Access Tenant Identifier**
 - Where you have **CorpXXX**
 - Replace with your **assigned Domain Identifier**
- \$Cert = We will look at this later

```

1. $Metadata = 'https://YOURACCESSHOST.vidmpreview.com/SAAS/auth/wsfd/services/mex'
2. $Brand = 'corpXXX'
3. $Domain = 'corpXXX.euc-livefire.com'

```


- With your **Keyboard**
 - select **Enter**

```
PS C:\Users\Administrator> $Metadata = 'https://aw-livefirernpod27.vi  
  
PS C:\Users\Administrator> $Brand = 'corp027'  
  
PS C:\Users\Administrator> $Domain = 'corp027.euc-livefire.com'
```

16. On your **ControlCenter** server

- Copy your **third** variable from **Notepad++**
 - **Paste** into **Powershell**
- 3. **\$Domain = 'corpXXX.euc-livefire.com'**
 - Where **XXX** is your assigned **domain identifier**
 - With your **Keyboard**
 - select **Enter**

```
PS C:\Users\Administrator> $Brand = 'corp027'  
  
PS C:\Users\Administrator> $Domain = 'corp027.euc-livefire.com'  
  
PS C:\Users\Administrator> $ActiveSO = 'https://aw-livefirernpod27.vidmpreview.com/SAAS/auth/wsfed/active/logon'
```

17. On your **ControlCenter** server

- Copy your **Fourth** variable from **Notepad++**
 - **Paste** into **Powershell**
- 4. **\$ActiveSO = 'https://YOUR VERSION.vidmpreview.com/SAAS/auth/wsfed/active/logon'**
 - With your **Keyboard**
 - select **Enter**

```
PS C:\Users\Administrator> $Domain = 'corp027.euc-livefire.com'

PS C:\Users\Administrator> $ActiveSO = 'https://aw-livefirenpod27.vidmpreview.com/SAAS/auth/wsfed/active

PS C:\Users\Administrator> $PLUri = 'https://aw-livefirenpod27.vidmpreview.com/SAAS/API/1.0/POST/sso'
```

18. On your **ControlCenter** server

- Copy your **Fifth** variable from **Notepad++**
 - **Paste** into **Powershell**
- 5. **\$PLUri = 'https://YOUR VERSION.vidmpreview.com/SAAS/API/1.0/POST/sso'**
 - With your **Keyboard**
 - select **Enter**

```
PS C:\Users\Administrator> $Domain = 'corp24.euc-livefire.com'

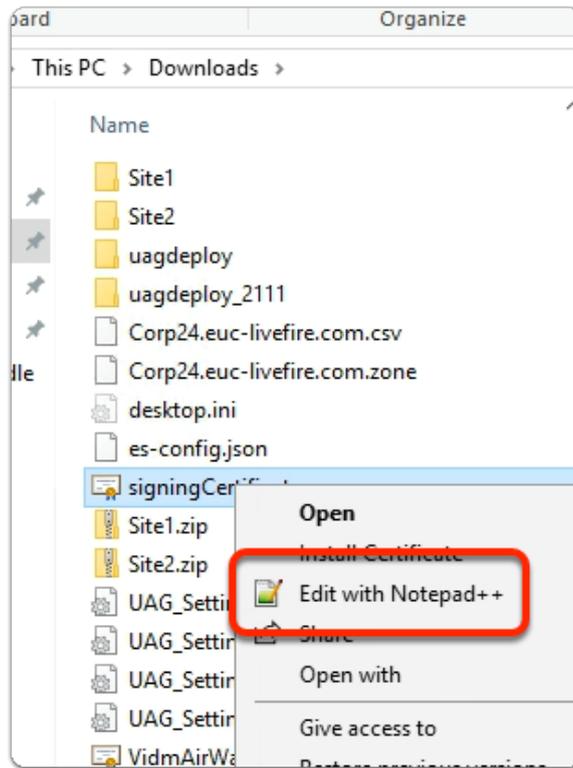
PS C:\Users\Administrator> $ActiveSO = 'https://aw-livefirenpod24.vidmpreview.com/SAAS/auth/wsfed/active

PS C:\Users\Administrator> $PLUri = 'https://aw-livefirenpod24.vidmpreview.com/SAAS/API/1.0/POST/sso'

PS C:\Users\Administrator> $IssuerUri = 'aw-livefirenpod24'
```

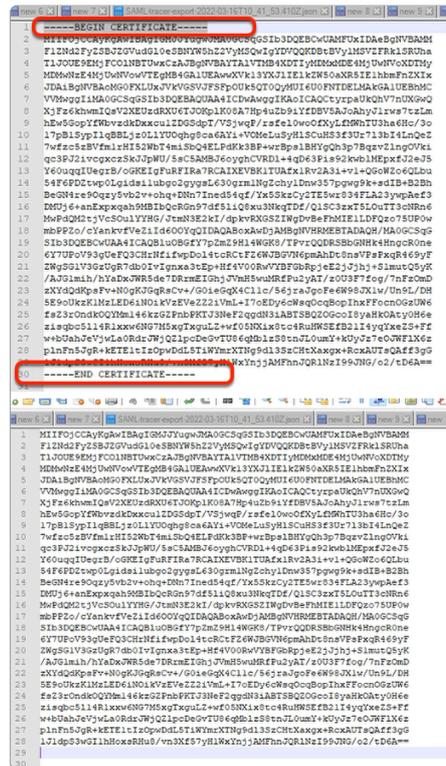
19. On your **ControlCenter** server

- Copy your **sixth** variable from **Notepad++**
 - **Paste** into **Powershell**
- 6. **\$IssuerUri = 'YOUR VERSION'**
 - With your **Keyboard**
 - select **Enter`**



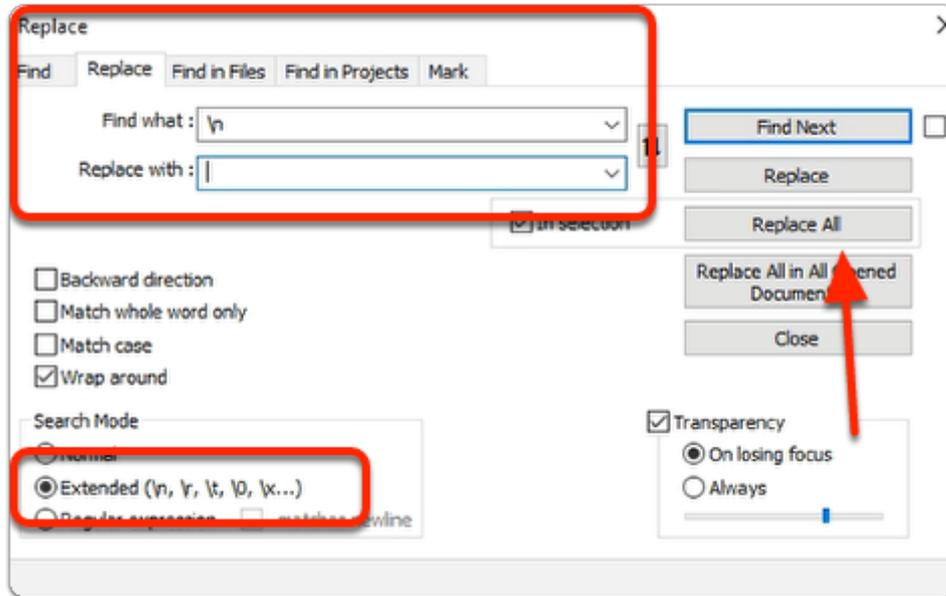
20. On your ControlCenter server

- Open your **DOWNLOADS** folder
- Select the **signingCertificate.cer**
- right-click and select **Edit with Notepad++**



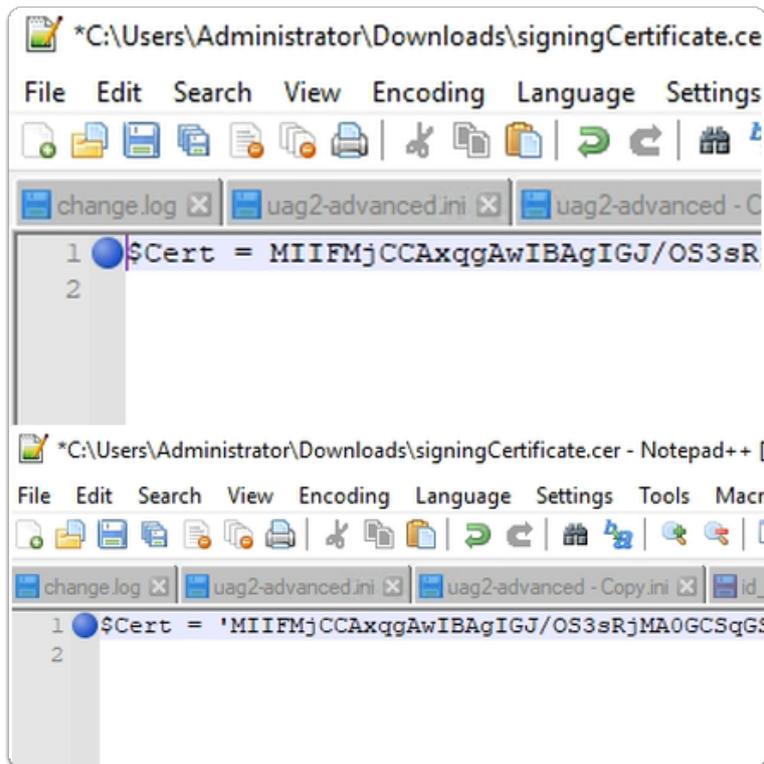
21. In **Notepad++**

- Remove the
 - -----BEGIN CERTIFICATE-----
 - and
 - -----END CERTIFICATE-----
- lines from the certificate.



22. In **Notepad++**

- We will now remove all carriage returns the document
 - **Select ALL** of the certificate portion of the file
 - Select **ctrl + F**
 - In the **Find** window
 - Select the **Replace** tab
 - Next to **Find what:**
 - **clear all entries (if necessary)**
 - enter **\n**
 - Next to **Replace with:**
 - **leave blank**
 - At the bottom of the **Replace** window.
 - In the **Search Mode** area
 - Next to **Extended.**
 - select the **radio button**
 - Select **Replace All.**



23. In **Notepad++**

- Switch back to your sample scripts
 - **Copy** the following: `$Cert =`
 - Switch back to the **tab** with your **Signing Certificate**
 - On your ControlCenter server In **Notepad++**
 - In front of your **certificate with no carriage returns**
 - Insert and **Paste** `$Cert =`
 - Insert a **single Quotation** at the **beginning** and **end** of your certificate
 - In **Notepad++**
 - **Select All (Ctrl + A)** and **copy (Ctrl + C)**

```

PS C:\Users\Administrator> $ActiveSO = 'https://aw-livefireernpod24.vidm
PS C:\Users\Administrator> $PLUri = 'https://aw-livefireernpod24.vidmpr
PS C:\Users\Administrator> $IssuerUri = 'aw-livefireernpod24'
PS C:\Users\Administrator> $Cert = 'MIIIFMjCCAxqgAwIBAgIGJ/OS3sRjMA0GCSqG

```

24. On your **ControlCenter** server

- **Switch back your Powershell**
 - **Paste** into **Powershell**
 - `$Cert = 'XX'` signing cert
 - Where **XX** is your cert string version
 - With your **Keyboard**
 - select **Enter`**

```
PS C:\Users\Administrator> $IssuerUri = 'aw-livefirernpod24'  
  
PS C:\Users\Administrator> $Cert = 'MIIFMjCCAxqgAwIBAgIGJ/OS3sRjMA0GCSqGSIb3DQEBCw  
  
PS C:\Users\Administrator> Set-MsolDomainAuthentication -DomainName $Domain -Authentic
```

25. In the **Azure Powershell ISE module** window

- Using the below code

```
Set-MsolDomainAuthentication -DomainName $Domain -Authentication Federated  
-FederationBrandName $brand -PassiveLogOnUri $PLUri -SigningCertificate $Cert -IssuerUri  
$IssuerUri -ActiveLogOnUri $ActiveSO -LogOffUri $PLUri -MetadataExchangeUri $metadata
```

```
PS C:\Users\Administrator> $IssuerUri = 'aw-livefirernpod24'  
  
PS C:\Users\Administrator> $Cert = 'MIIFMjCCAxqgAwIBAgIGJ/OS3sRjMA0GCSqGSIb3DQEBCw  
  
PS C:\Users\Administrator> Set-MsolDomainAuthentication -  
  
PS C:\Users\Administrator> Get-MsolDomain
```

26. In the **Azure Powershell ISE module**

- Enter the following:-
 - **Get-MsolDomain**

```
PS C:\Users\Administrator> Get-MsolDomain

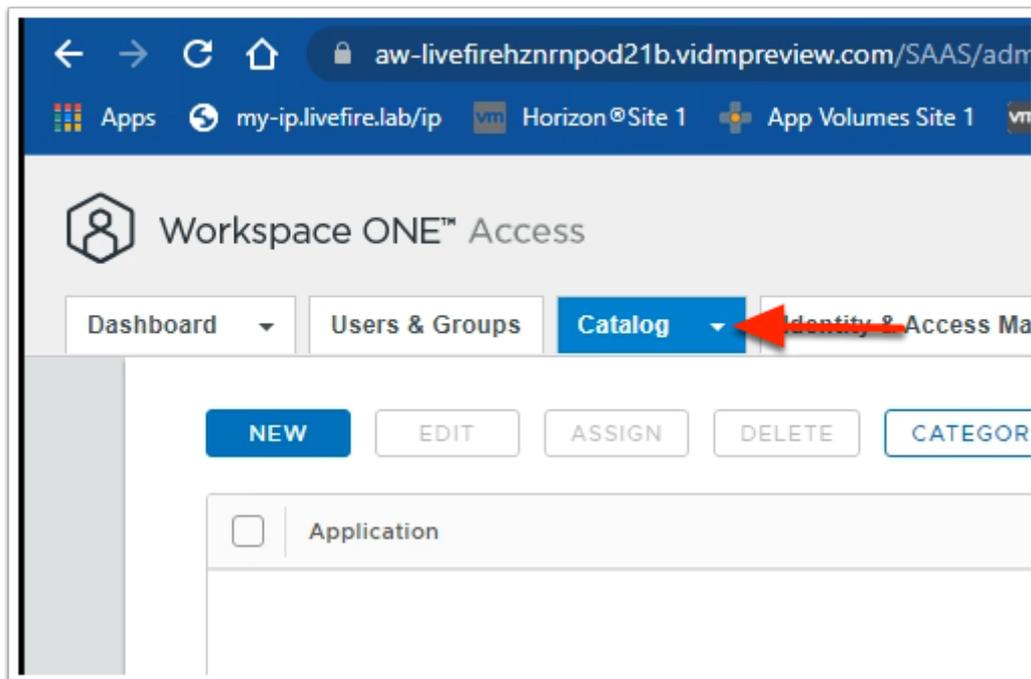
Name                Status  Authentication
-----
wzvx.onmicrosoft.com Verified Managed
corp027.euc-livfire.com Verified Federated

PS C:\Users\Administrator>
```

27. In the **Azure Powershell ISE module**

- Notice that your **Custom Domain** now **Verified** as **Federated**

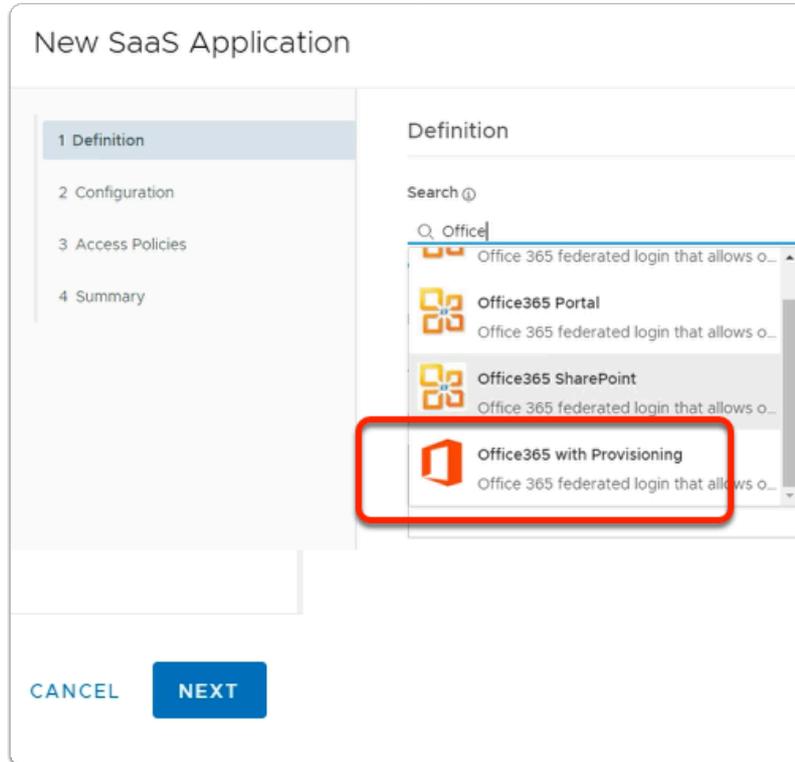
Part 3: Setting up Workspace ONE Access for Azure Federation



1. In your Workspace ONE Access SAAS Admin Console

- Under **Resources** > **Web Apps**

- In the **Web Apps** area
 - select **NEW**



2. In the **New SaaS Application** window
 1. **In the Definition** area
 - Under **Search**
 - Enter **Office**
 - From the **dropdown**
 - Select **Office365 with Provisioning**
 - In the bottom right corner
 - Select **NEXT**

Application Parameters			
Name	Description	Default Value	Value
tenant	Office 365 Domain		corp027.euc-livefire.com
issuer	Office 365 issuer URI		aw-livefirempod27

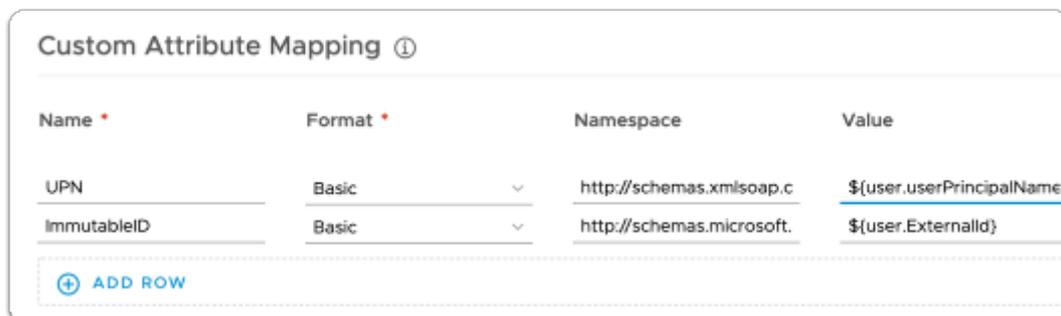
[Advanced Properties](#) ^

💡 Go back to Notepad++ and copy the value for \$IssuerUri = 'aw-livefirernpod26' {without the quotes}

3. In the **New SaaS Application** window

2. **Configuration** area

- **Scroll down** until you find **Application Parameters**
 - Under **Name**, you have two parameters
 - **tenant**
 - **issuer**
 - In line with **tenant**, under **Value**
 - enter your **Azure domain FQDN**.
 - e.g. Corp**XXX**.euc-livefire.com
 - where **XXX** is your **assigned domain identifier**
 - In line with **issuer**, under **Value**
 - enter your **Workspace ONE Access name** without vidmpreview.com
 - e.g. If your tenant name is **aw-livefirernpod31.vidmpreview.com**
 - then your you will enter **aw-livefirernpod31**
 - Expand **Advanced Properties**

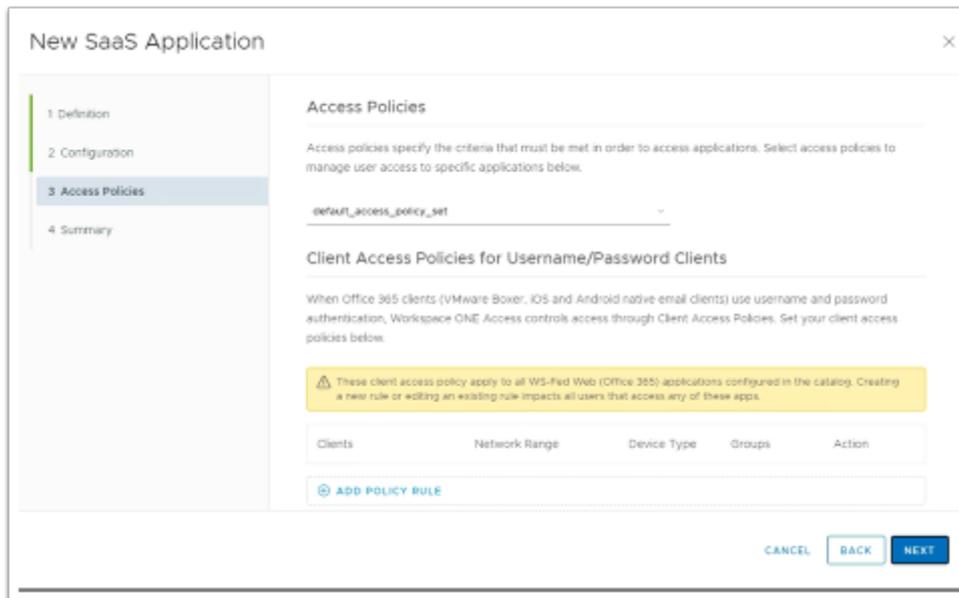


Name *	Format *	Namespace	Value
UPN	Basic	http://schemas.xmlsoap.c	<u><code>\${user.userPrincipalName}</code></u>
ImmutableID	Basic	http://schemas.microsoft.	<code>\${user.ExternalId}</code>

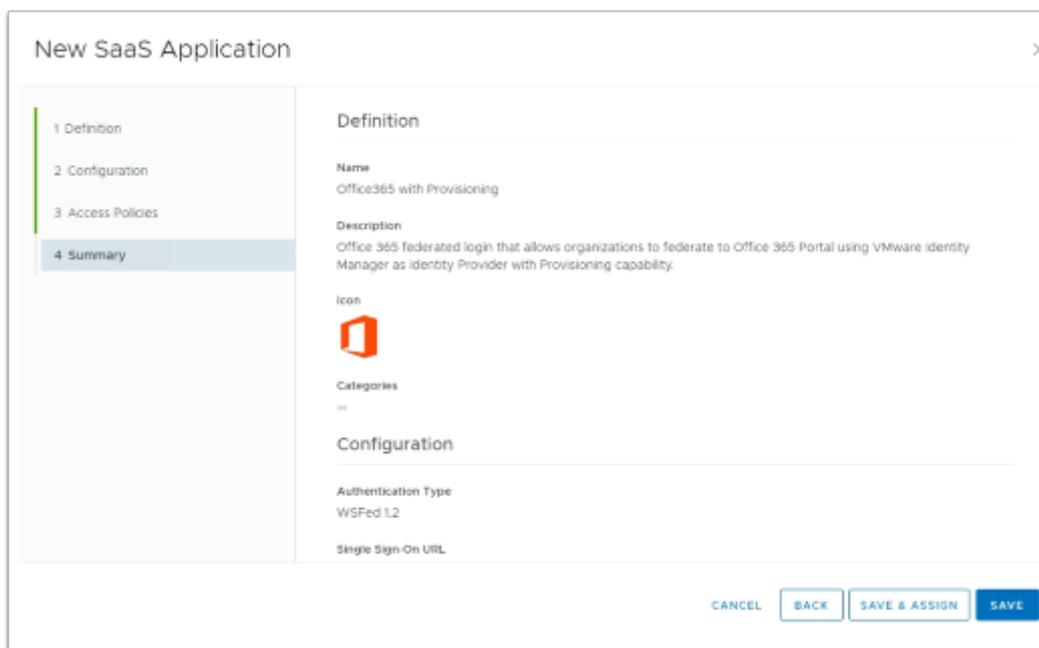
+ ADD ROW

4. In the **New SaaS Application** window

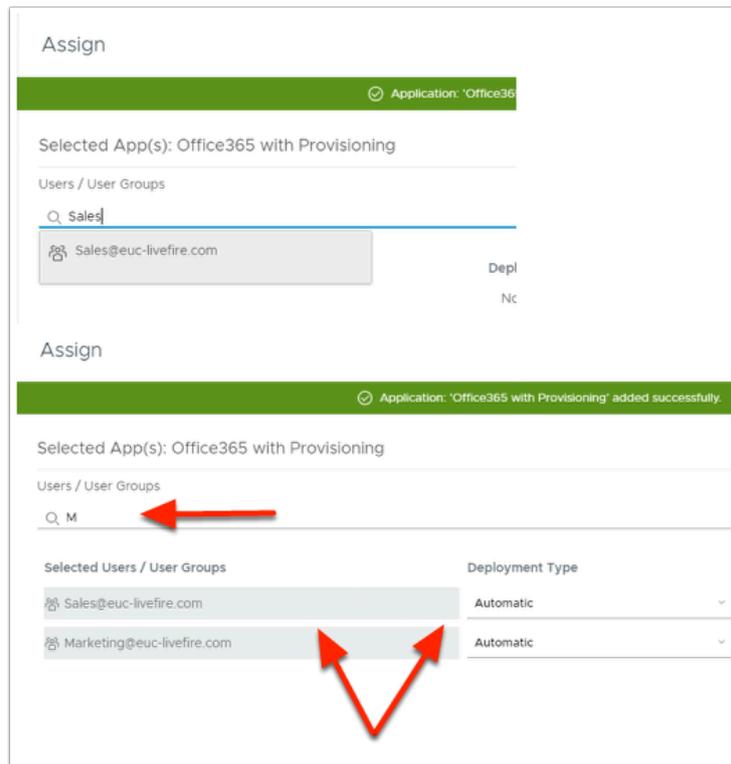
- In the **Configuration** area
 - **Scroll down** to **Custom Attribute Mapping**
 - Under **Name**
 - In the with **UPN** row
 - Under the **Value** column
 - validate that the configuration is:-
 - **`${user.userPrincipalName}`**
 - In the **ImmutableID** row
 - Under the **Value** column
 - Replace **`${user.objectGUID}`**
 - with **`${user.ExternalId}`**
 - Select **NEXT**



5. In the **New Saas Application** window,
 - In the **Access Policies** section
 - Select **NEXT**

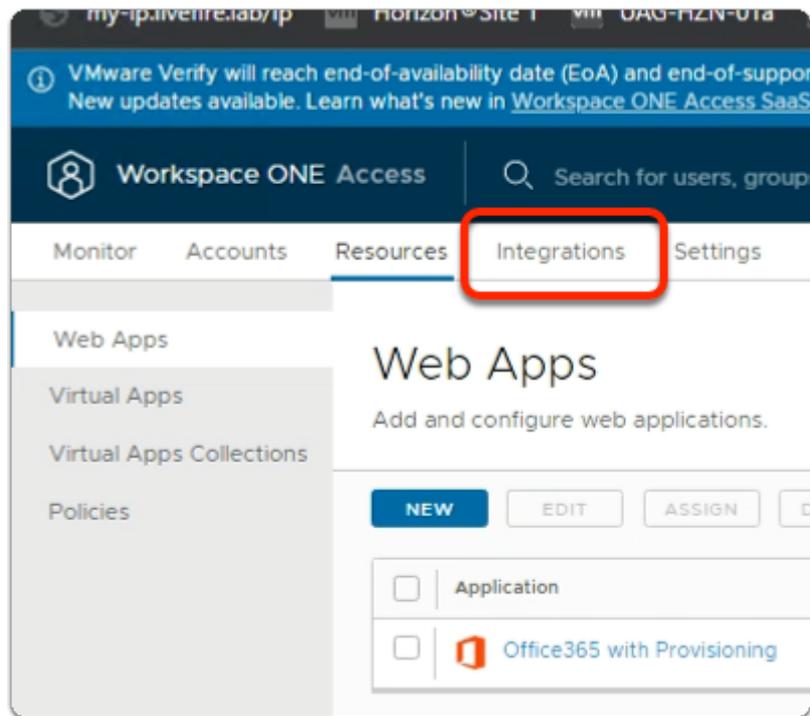


6. In the **New Saas Application** window,
 - In the **Summary** section
 - Select **SAVE & ASSIGN**



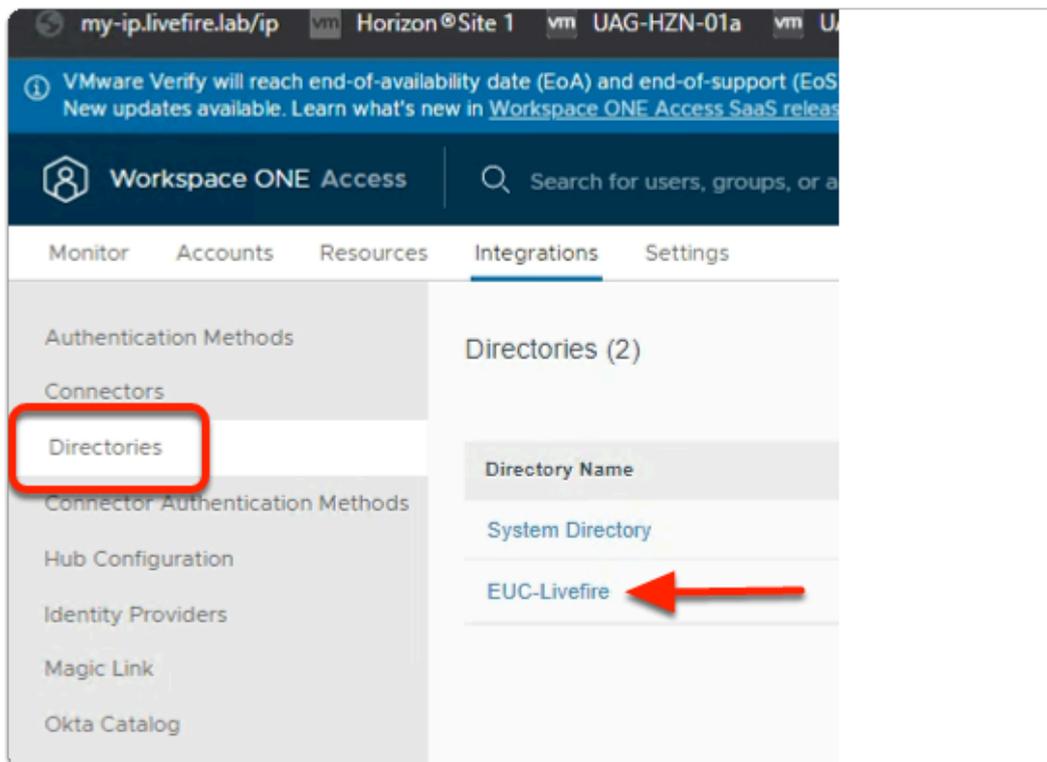
7. In the **Assign** window

- Under **Users / Groups**
 - Enter **Sales**
 - Select **Sales@euc-livewire.com**
 - Enter **Mark**
 - Select **Marketing@euc-livewire.com**
- Under **Deployment** type
 - From the **dropdowns**
 - Ensure both **Sales** and **Marketing** are set to
 - **Automatic**
- In the bottom right corner
 - select **SAVE**



8. In your **Workspace ONE Access** Console

- select the **Integrations** tab
- You will notice it takes you to the **Directories** area by default



9. Under **Directories**

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

- select **EUC-Livefire**

EUC-Livefire

Active Directory over LDAP
 Active Directory over Integrated Windows Authentication

LDAP

Directory Sync and Authentication

Select at least one active directory sync host that syncs users from Act

Identity Providers Built-in, IDP for EUC-Livefire

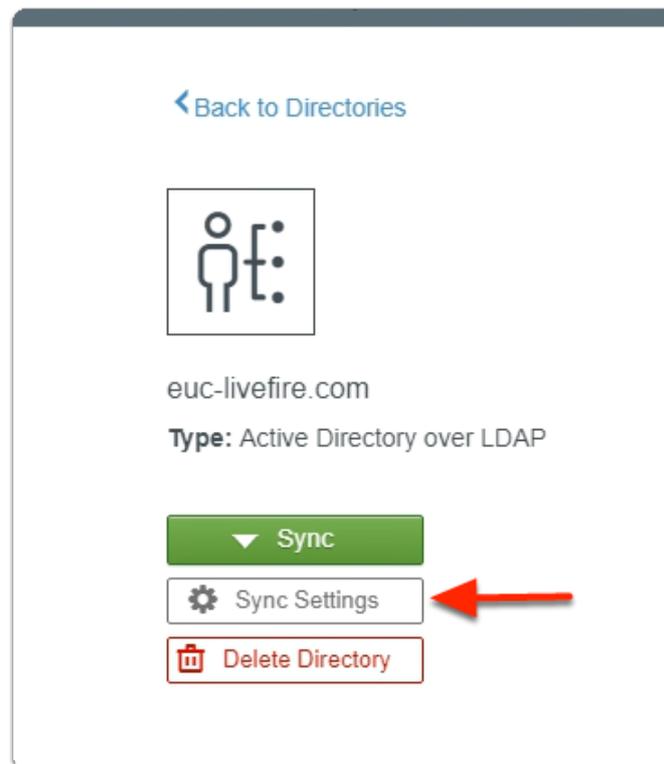
User Name* sAMAccountName

External ID* objectGUID

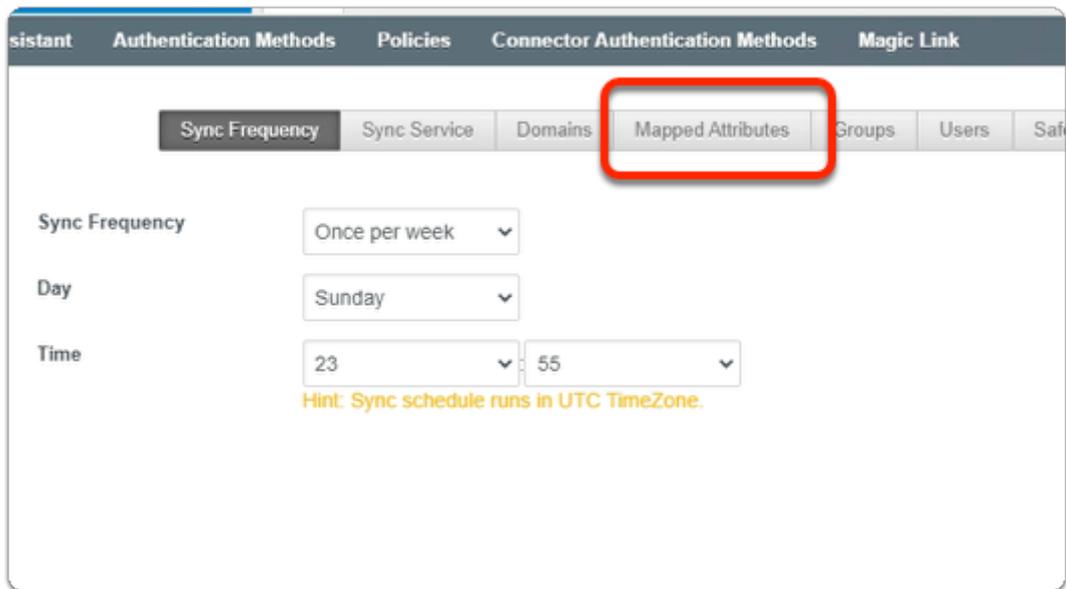
The attribute to use as the unique ident

Server Location Check this box to use the DNS Service Location records to locate the s

10. In the **euc-livefire.com** Directory
 - In the **Directory Sync and Authentication** area
 - next to **External ID***
 - validate that **objectGUID** is the value



11. In the **euc-livefire Directory**
 - Under **Sync**
 - Select **Sync Settings**

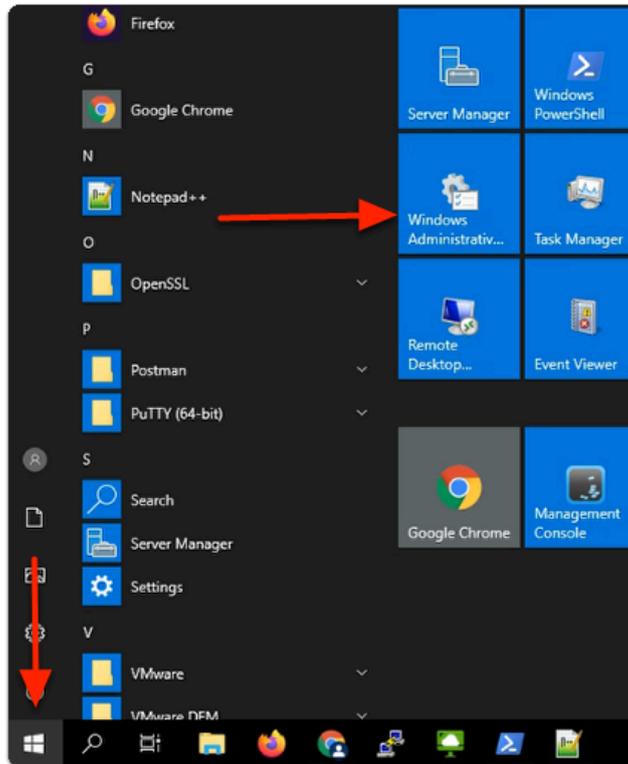


12. In the **Sync settings** window
- Select **Mapped Attributes**

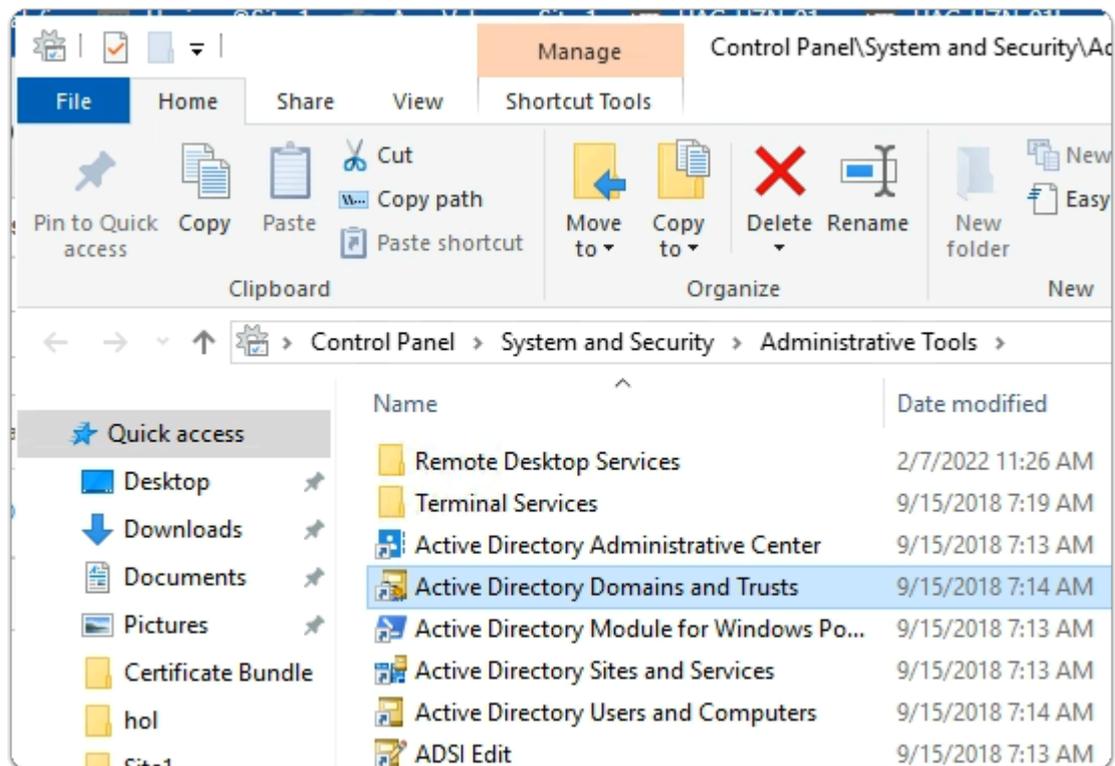
sid	<input type="text" value="objectSid"/>
sourceAnchor	<input type="text" value="mS-DS-ConsistencyGuid"/>
title	<input type="text" value="title"/>
userPrincipalName	<input type="text" value="userPrincipalName"/>

13. In the **Mapped Attributes** window
- **Scroll down** until you find **sourceAnchor**
 - To the right of **sourceAnchor**
 - Edit the existing value **objectGUID**
 - From the **dropdown**
 - select **Enter Custom Input**
 - In the **Enter Custom Input** area
 - enter **mS-DS-ConsistencyGuid**
 - At the bottom of the **Mapped Attributes** area
 - select **Save**
 - select **Close**

Part 4. Configuring domain trust

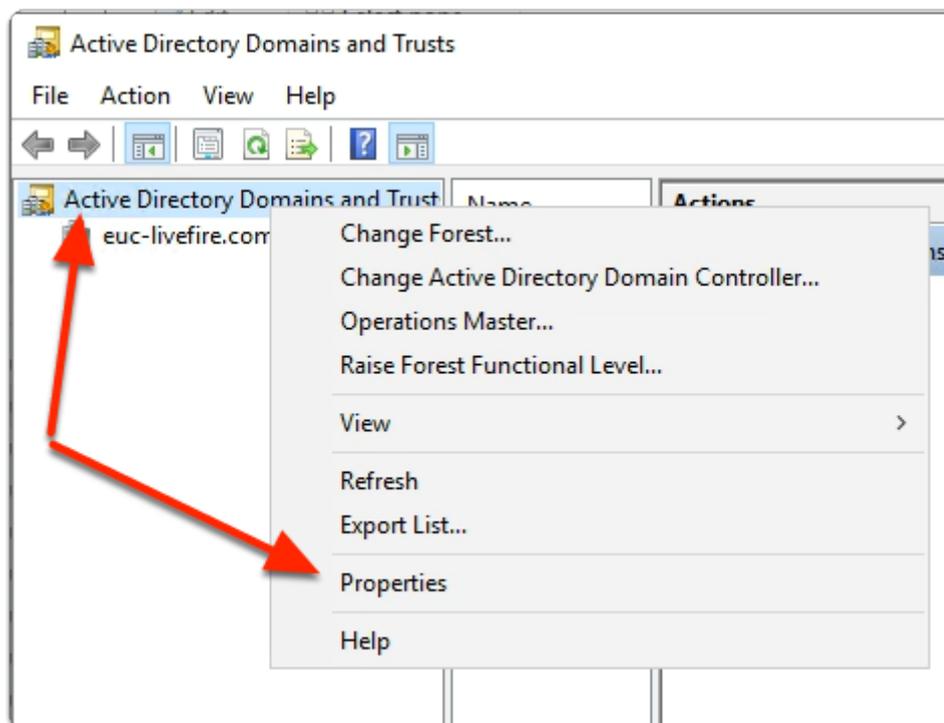


1. On your ControlCenter server
 - In the bottom left corner
 - Select the **Start** button
 - In the **Start Menu**
 - Select **Windows Administrative Tools**



2. In the **Administration Tools** menu

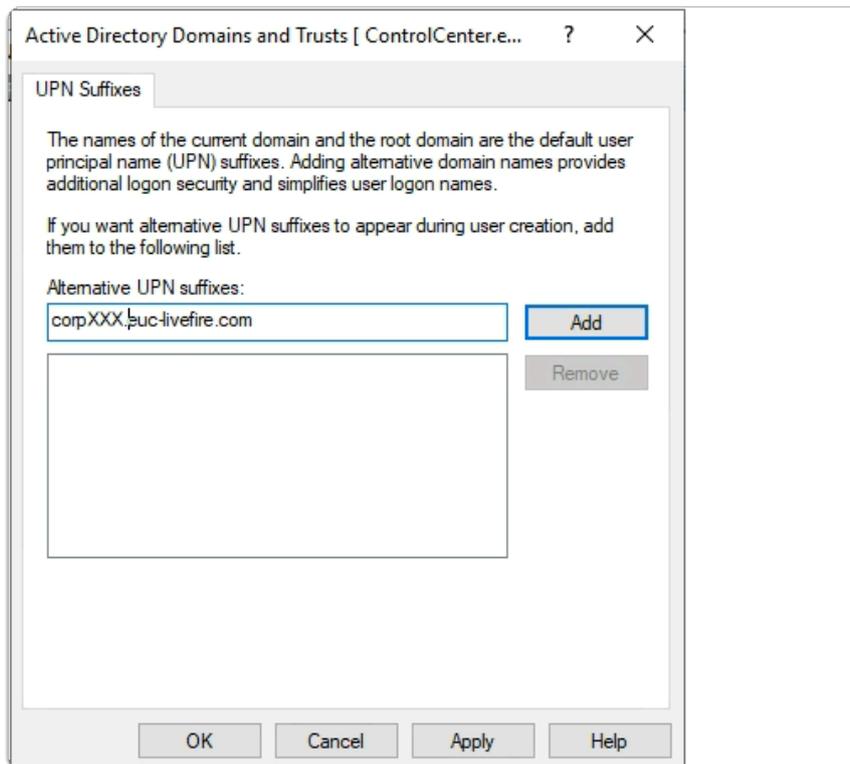
- Select the **Active Directory Domains and Trusts** shortcut



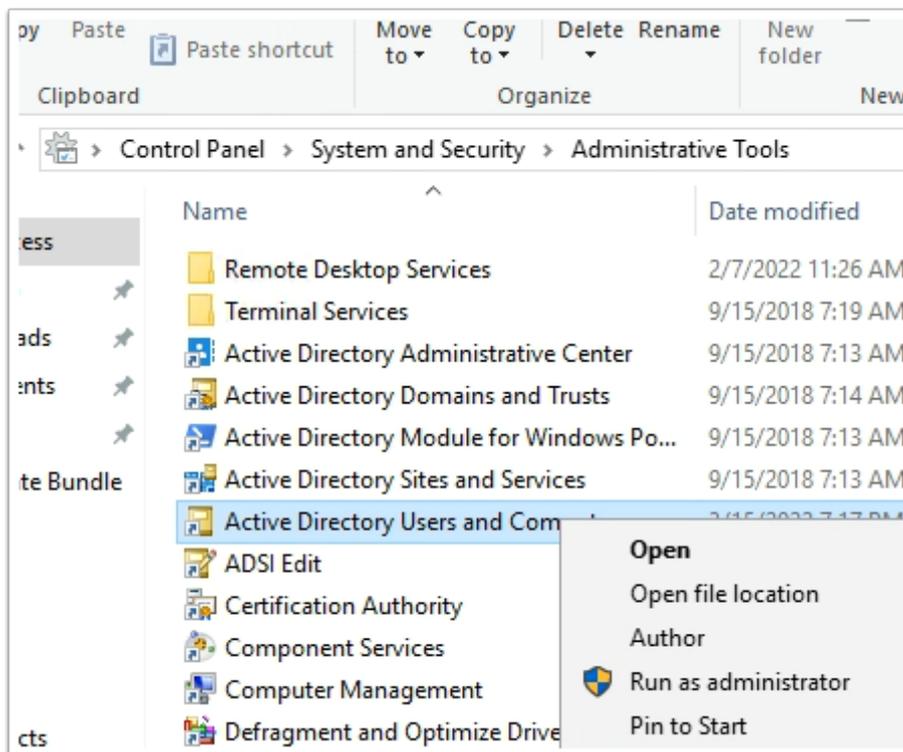
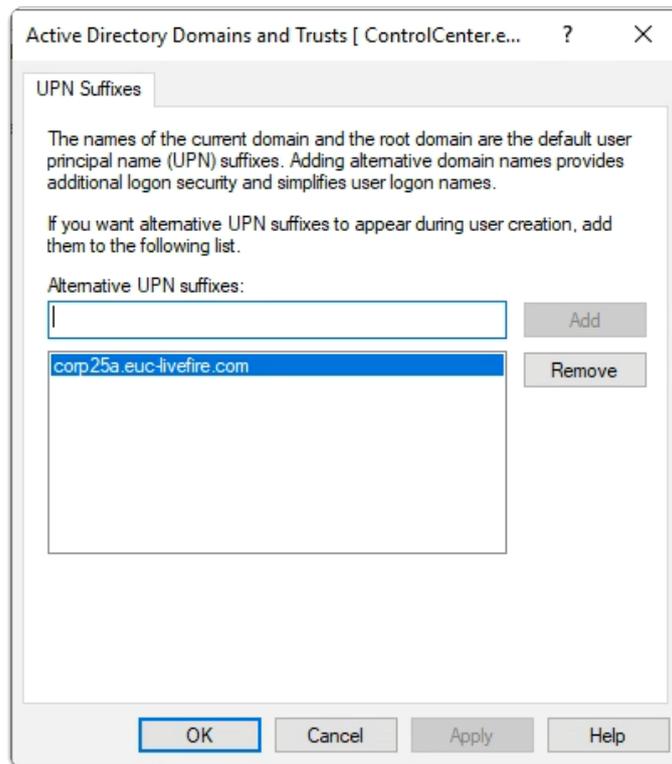
3. In **Active Directory Domains and Trusts**

- In the Inventory
 - Select and right click
 - **Active Directory Domains and Trusts**

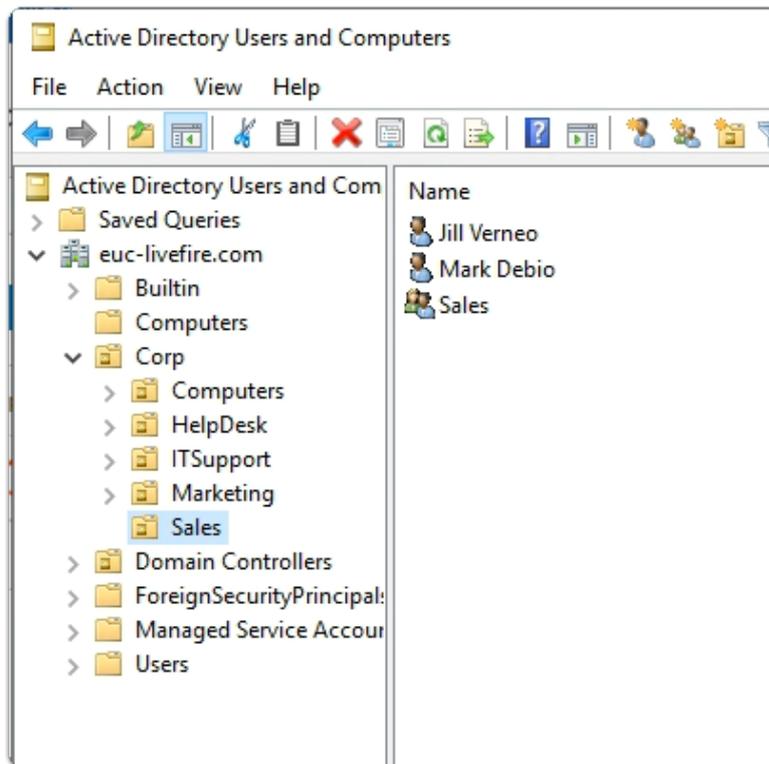
- Select **Properties**



4. In the Active Directory Domains and Trusts window
 - Under **Alternative UPN Suffixes**
 - Enter the FQDN of your Azure Domain
 - e.g. **CorpXXX.euc-livewire.com**
 - where **XXX** is your assigned **Domain Identifier**
 - Select **Add**

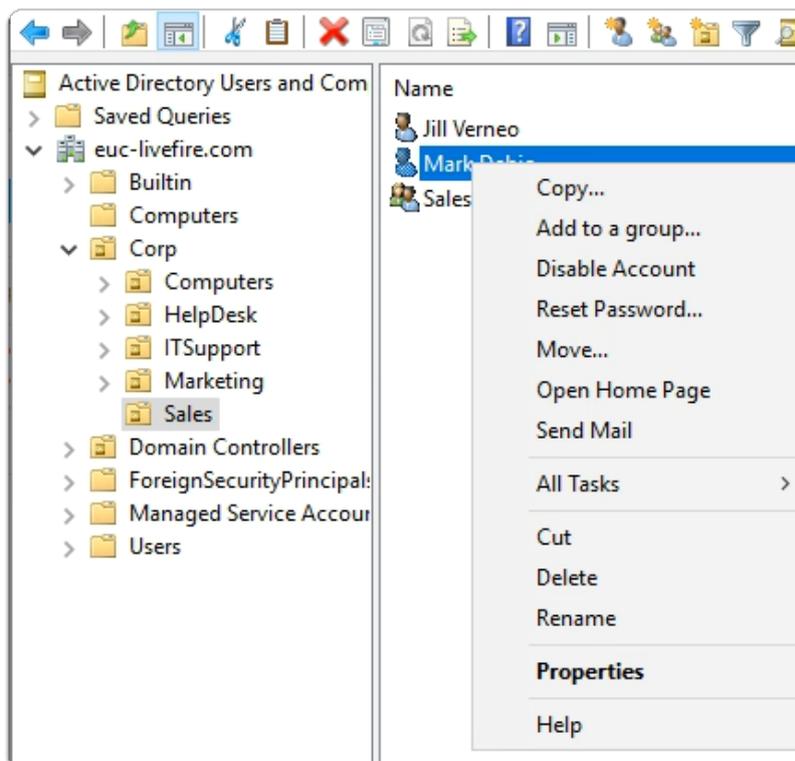


5. In the **Administrative tools** folder
 - Select **Active Directory Users and Computers** shortcut
 - Select **open**



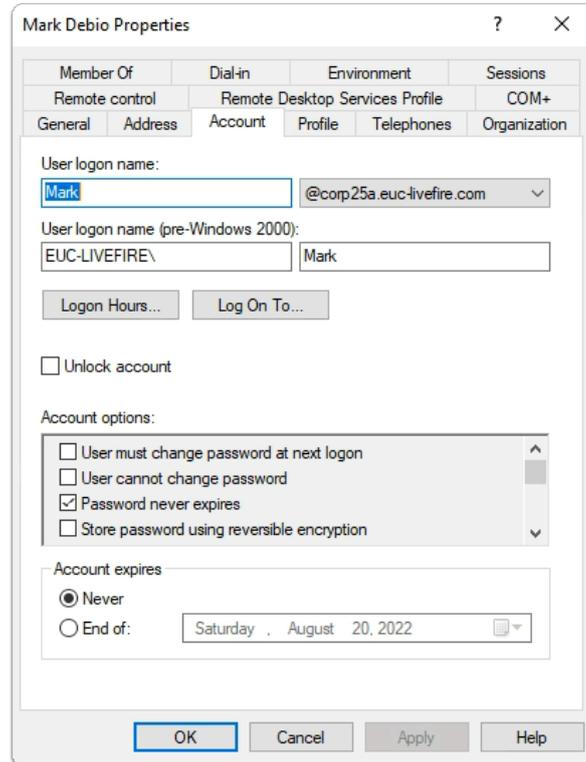
6. In the **Active Directory Users and Computers** Console

- **Expand** the **euc-livfire.com** hierarchy
 - **Select Corp OU** and expand
 - Select **Sales**



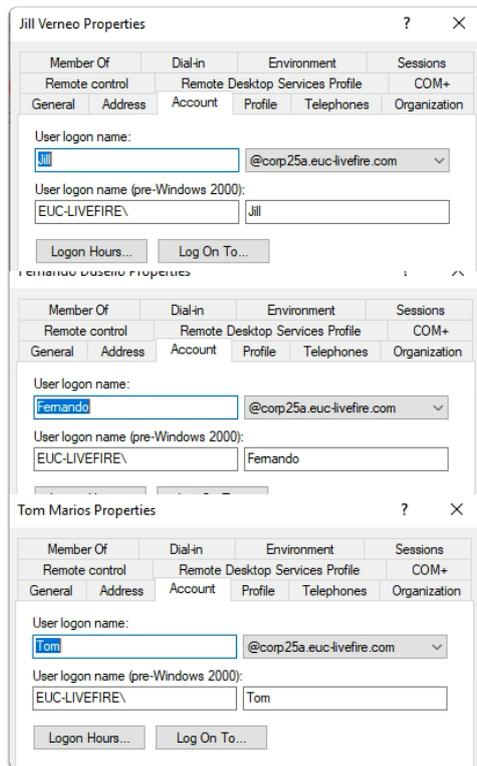
7. In the **Active Directory Users and Computers** Console

- Select the **Mark Debio** user object
 - Select **Properties**



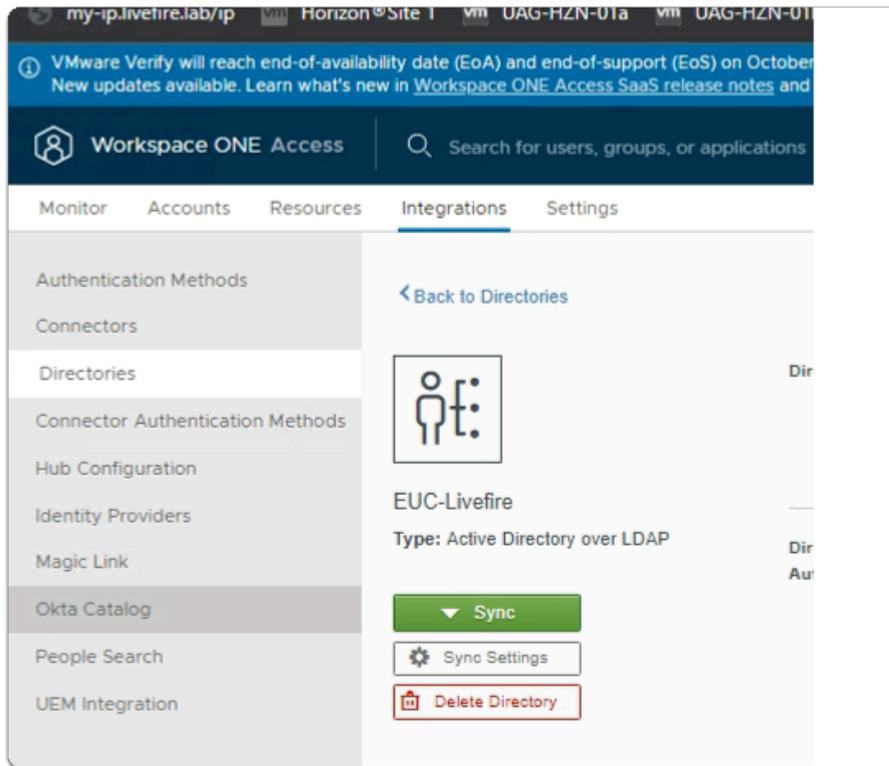
8. In the **Mark Debio** properties

- To the right and In line with **Mark**
 - From the **Dropdown**
 - Select your **Alternate suffix** eg. Corp**XXX**.euc-livefire.com
 - where **XXX** is your assigned **Domain ID**
- To close **Mark Debio Properties**
 - Select **OK**



9. In the **Active Directory Users and Computers** Console

- Repeat the above mention steps for at least these accounts :
 - In the **Sales OU** :- **Jill Vernio**
 - In the **Marketing OU**: - **Fernando Dusello**
 - In the **Marketing OU**: - **Tom Marios**
 - In **IT Support OU**: - **Kim Markez**

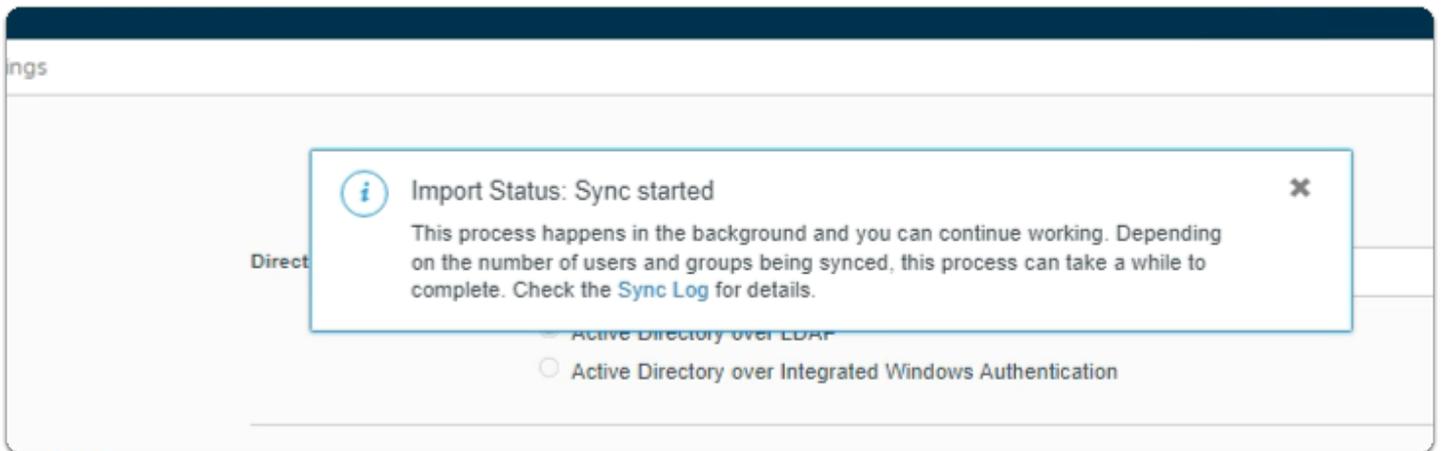


10. On your ControlCenter server
 - Switch to your **Chrome** Browser
 - Select your **Workspace ONE Access** session
 - In the **Integrations > Directories area > EUC-Livefire area**



11. In the **EUC-Livefire** Directory

- Next to **Sync**
 - Select **the Dropdown**
 - Select **Sync without Safeguards**



12. In the **EUC-Livefire** Directory
 - In the **Import Status: Sync started** pop up
 - select **Sync Log**

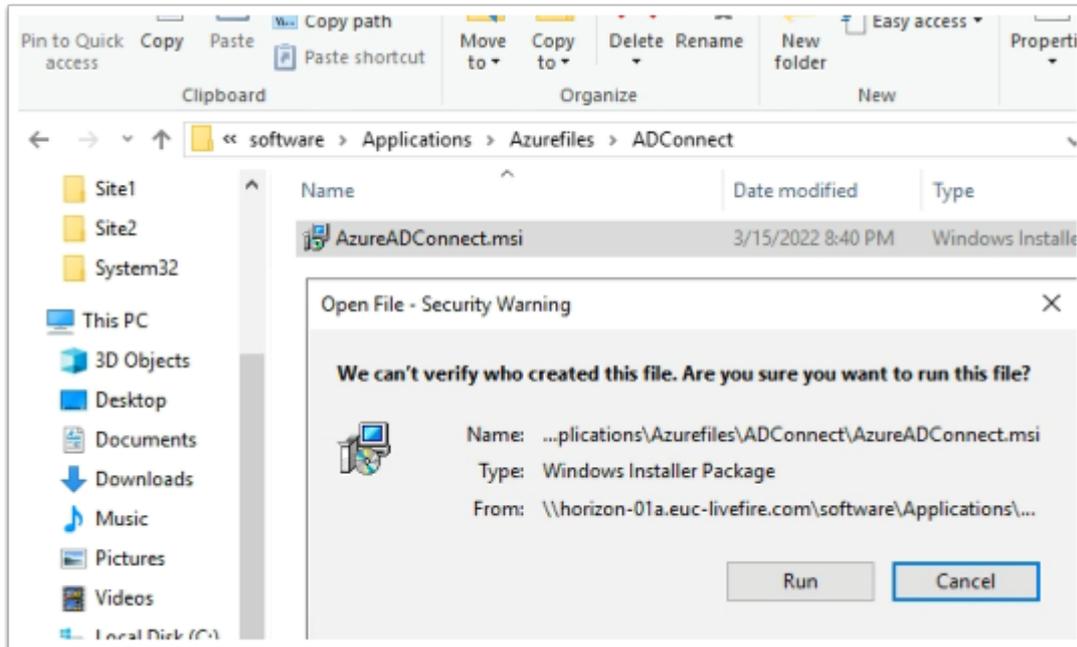
Timestamp	Sync Service	Sync Details	Alerts
Nov 3, 2022 2:33:07 PM +0000	WS1-Connector.euc-livefire.com	0 Groups and 8 Users were affected	5
Nov 2, 2022 2:25:19 PM +0000	WS1-Connector.euc-livefire.com	0 Groups and 0 Users were affected	5
Nov 2, 2022 2:23:51 PM +0000	WS1-Connector.euc-livefire.com	0 Groups and 0 Users were affected	5

13. In the Sync Log
 - Validate that sync was successful

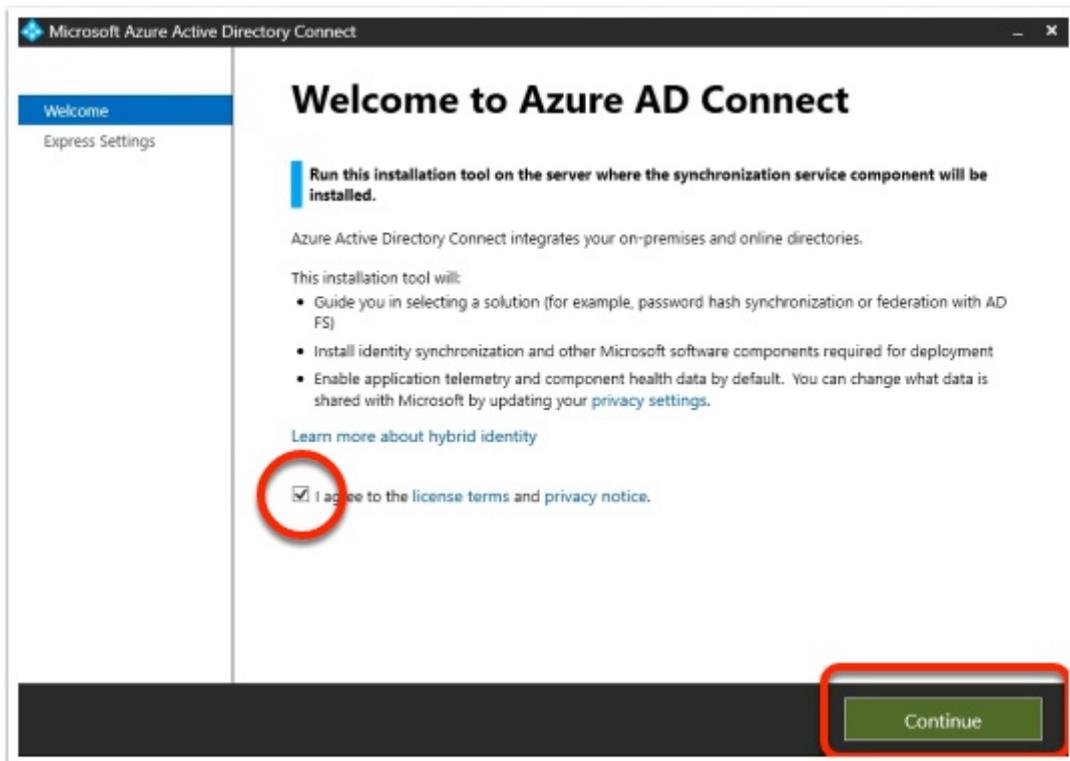
A green tick is a validation that sync was successful A red cross indicates sync failure

- Ignore the Alerts

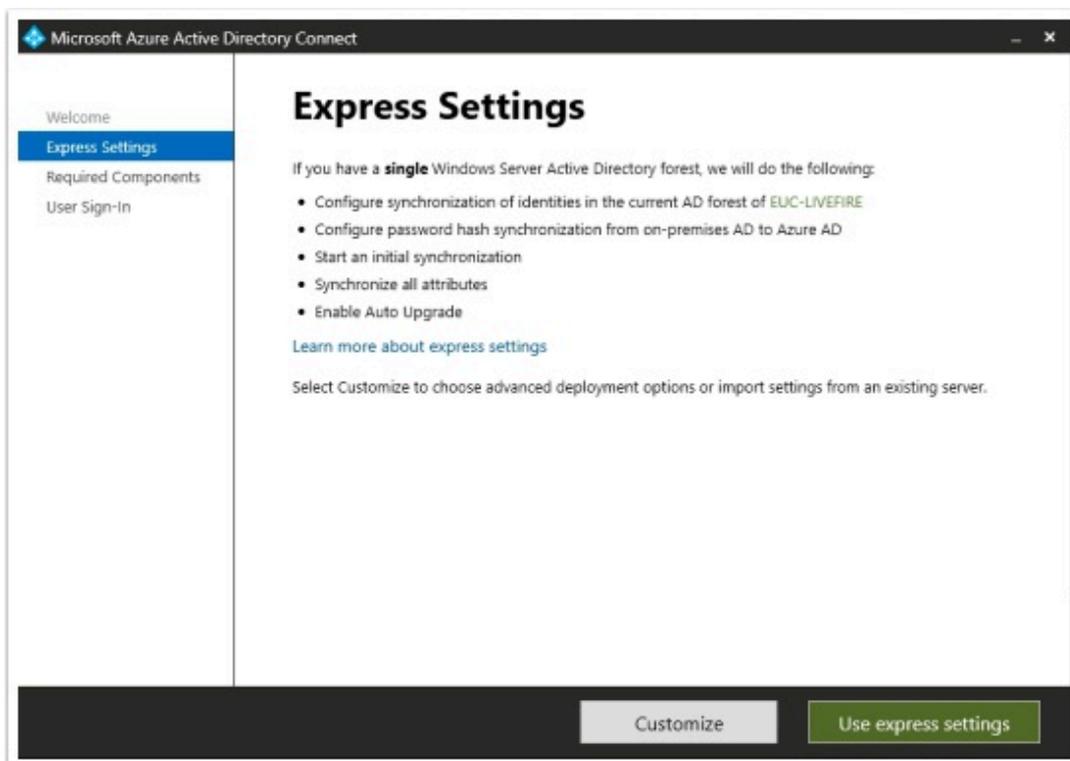
Part 5: Using Azure AD Connect for user provisioning to Azure



1. On your ControlCenter server
 - Open the **Software** shortcut
 - Navigate to the **Applications > Azurefiles >ADConnect** folder.
 - Double- click the **AzureADConnect.msi**
 - On the **Open File - Security Warning** window
 - Select **Run**



2. On the **Welcome to Azure AD Connect** window
 - Next to **I agree to the license terms and privacy notice**
 - Enable the **check box**
 - Select **Continue**



3. In the **Express Settings** window

- Select **Use express settings**

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure

Connect to Azure AD

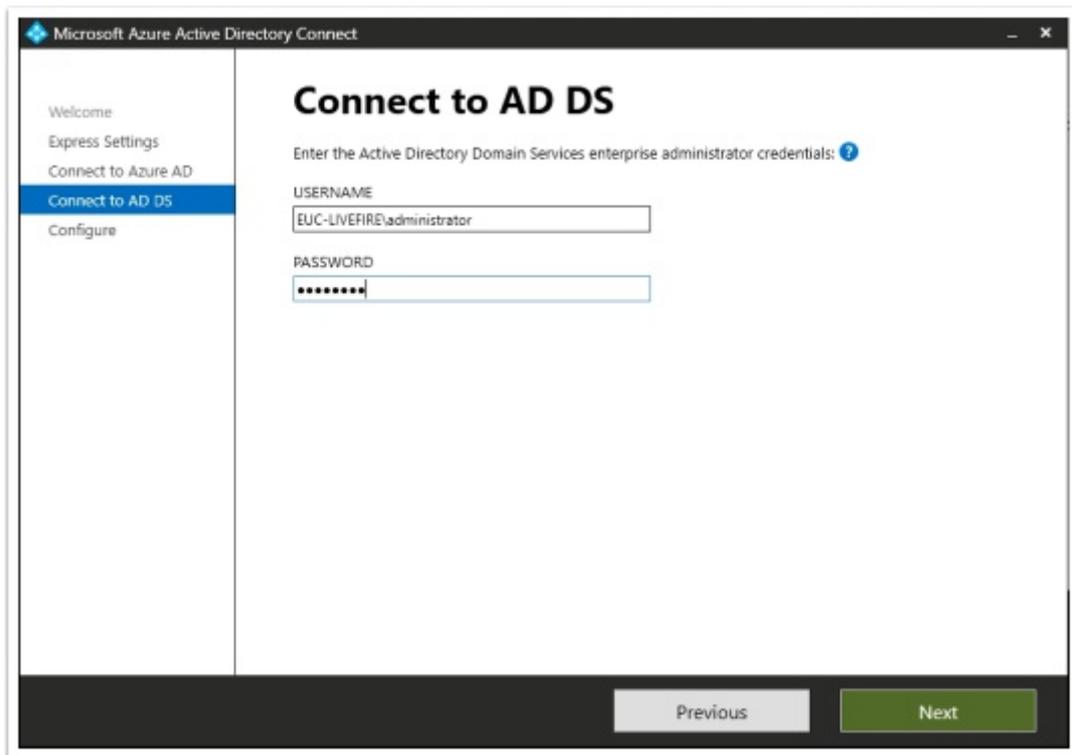
Enter your Azure AD global administrator or hybrid identity administrator credentials. ?

USERNAME
cloudadmin@7q011p.onmicrosoft.com

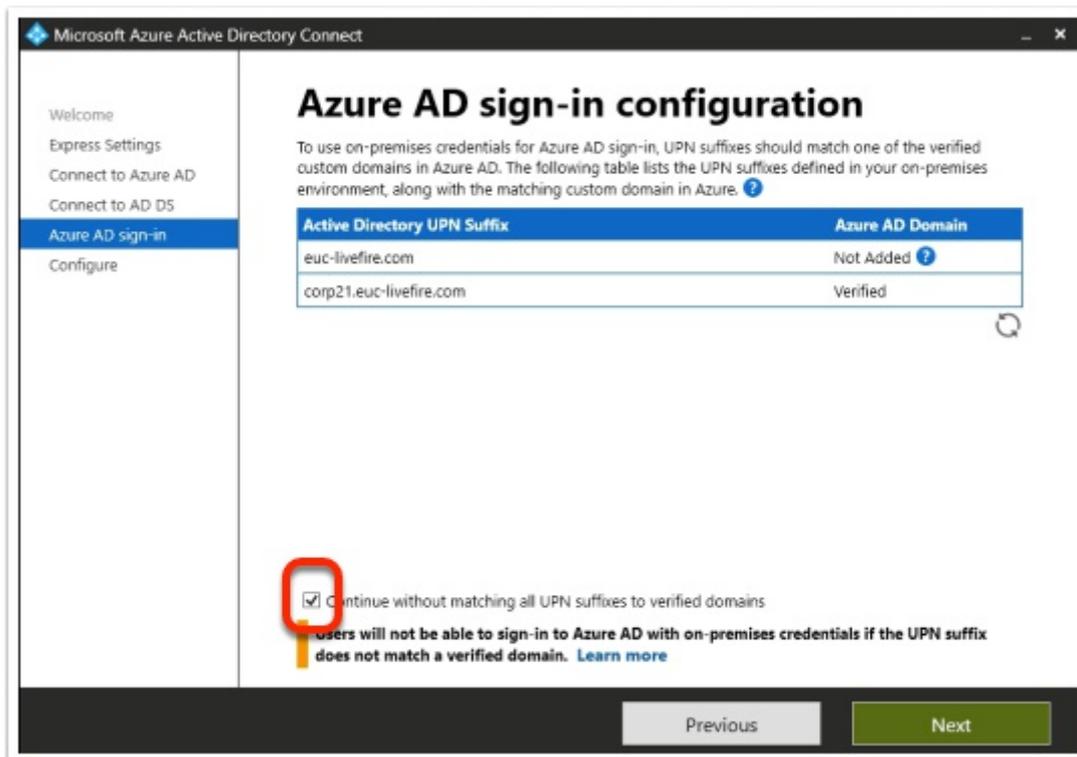
PASSWORD

Previous Next

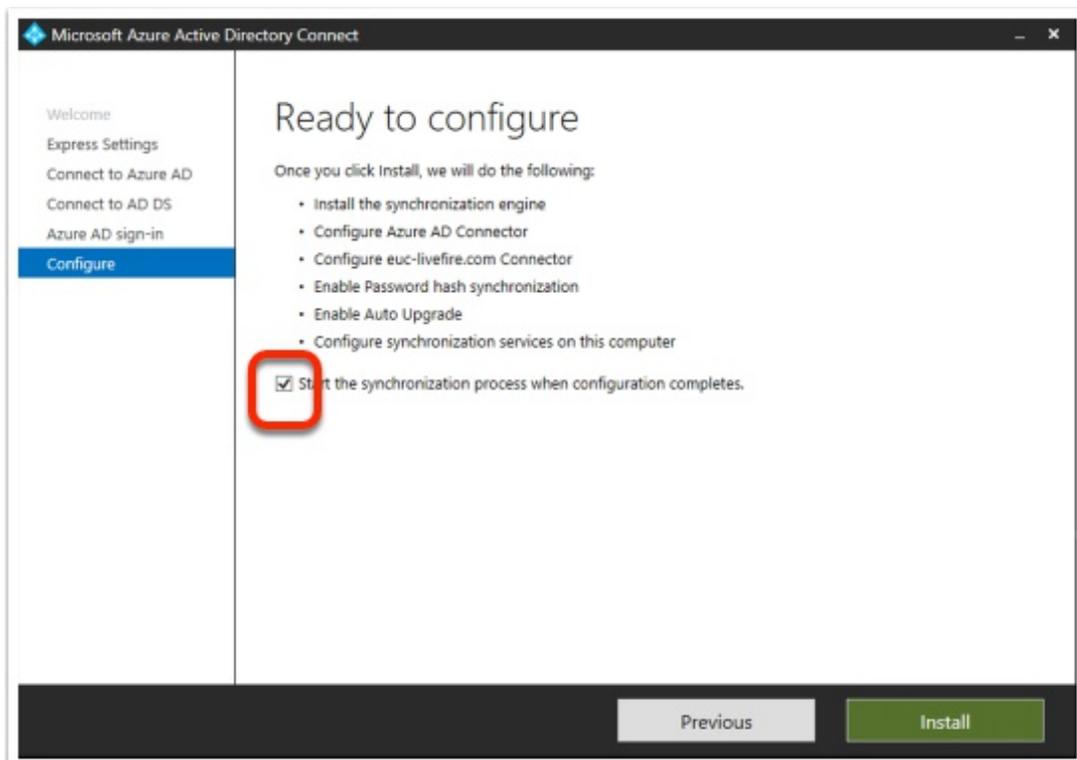
5. On the **Connect to Azure AD** window,
 - Under **USERNAME**
 - Enter your documented Azure Cloud Admin **account**
 - Under **PASSWORD**
 - Enter your documented Azure Cloud Admin **password**
 - Select **Next**



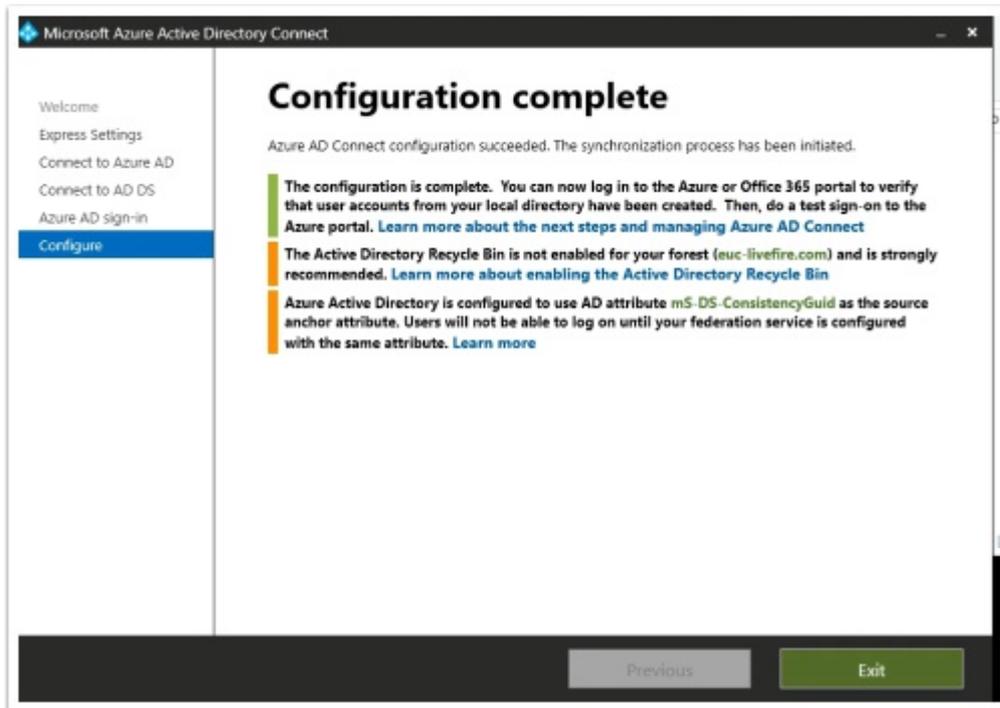
6. On the **Connect to AD DS** window,
 - Under **USERNAME**
 - Enter **EUC-Livefire\Administrator**
 - Under **PASSWORD**
 - Enter **VMware1!**
 - Select **Next**



7. On the **Azure AD sign-in configuration** page
 - Validate that your custom Azure Domain has been Verified
 - Next to **Continue without matching all UPN suffixes to verified domains**
 - Select the **Check box**
 - Select **Next**

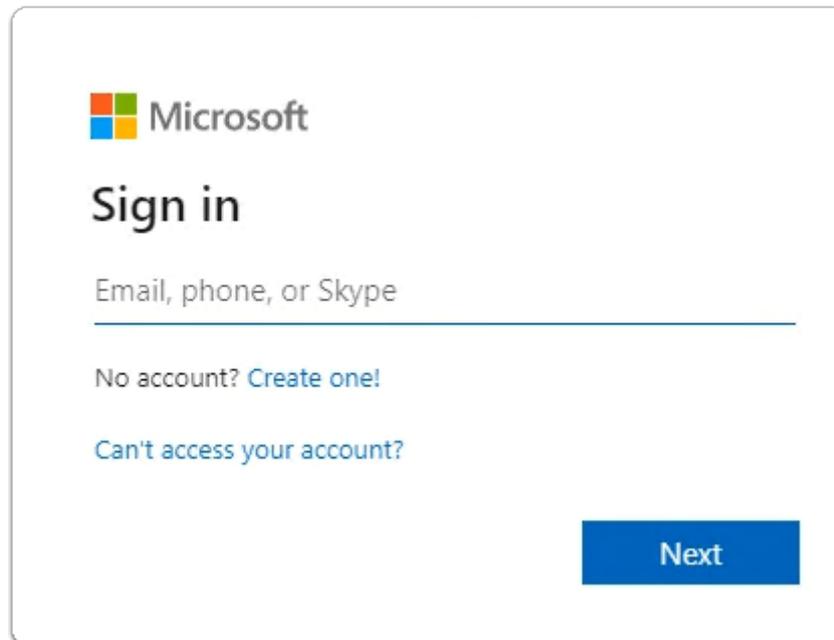


8. On the **"Ready to configure"** window
 - Next to **Start the synchronization process when configuration completes**
 - Enable the check box
 - Select **Install.**
 - Getting to the next step could take a few minutes.

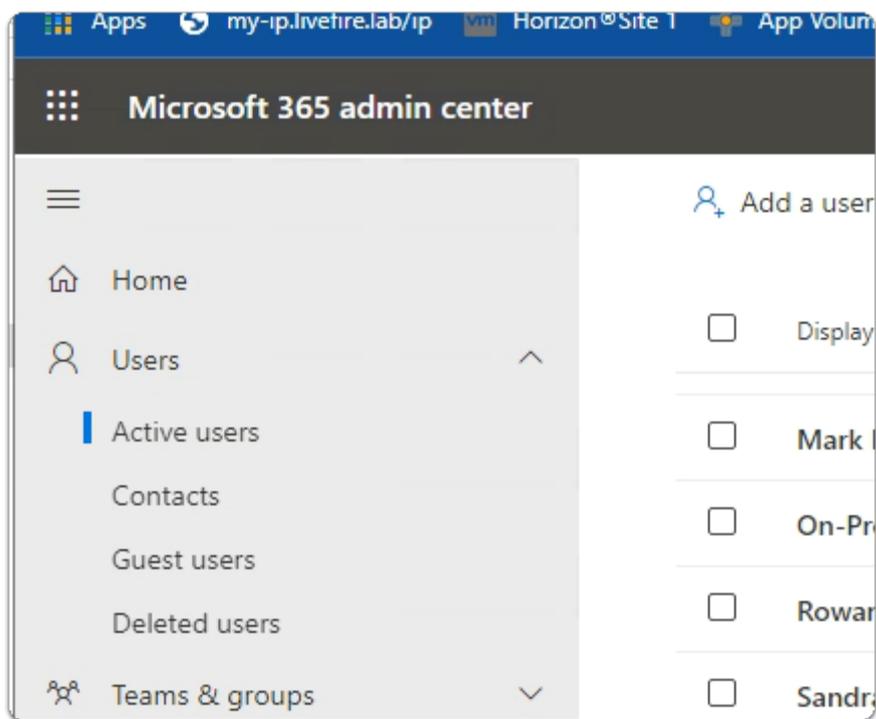


9. On the **Configuration complete** window
 - Select **Exit**

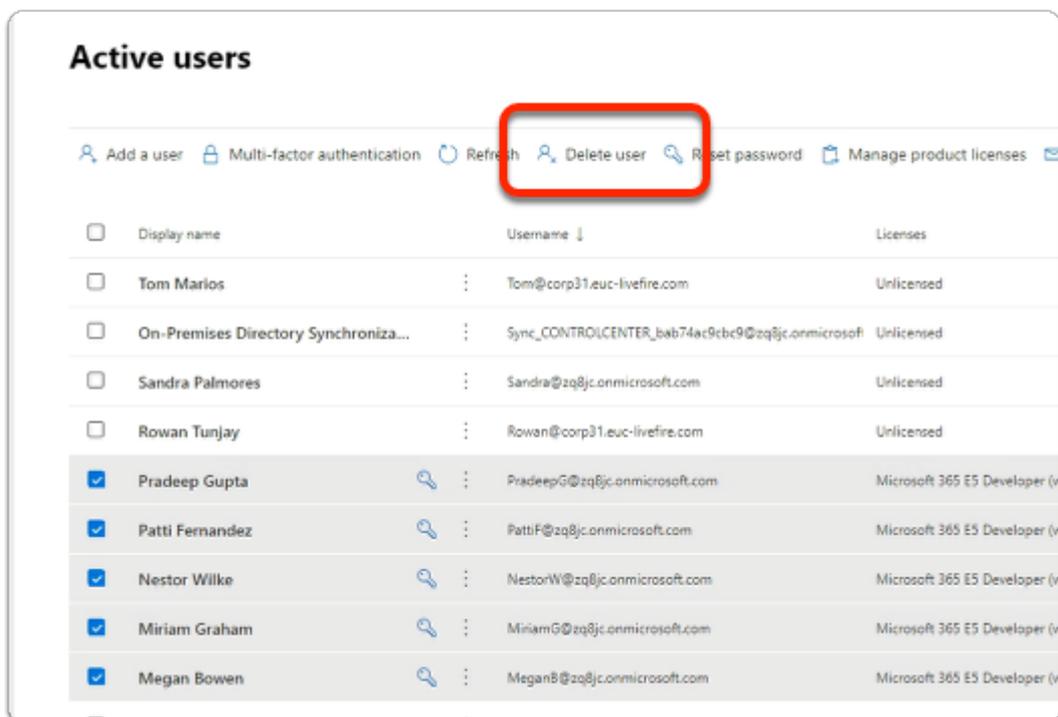
Part 6: Configuring Microsoft 365 licensing



1. On your ControlCenter server
 1. Using the following URL
 - <https://admin.microsoft.com/Adminportal/Home?source=applauncher#/homepage>
 2. Login back to your **Microsoft 365 Tenant**
 - With **cloudadmin** username
 - With your CloudAdmin **password**



3. In the Microsoft 365 Admin center
 - In the left-hand pane under **Home**,
 - Select **Users**
 - Select **Active users**.



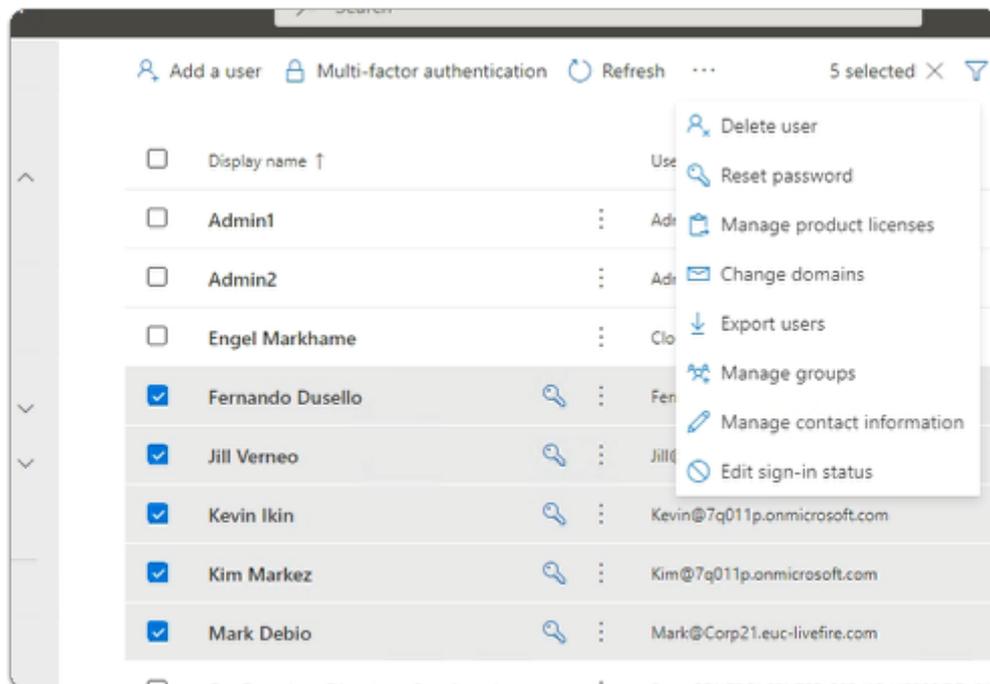
4. In the **Active Users** area
 - Notice that you have **Licensed** and **Unlicensed** users

- It appears that in addition to us syncing in our account Microsoft creates dummy accounts for use
- The dummy user accounts have already been licensed and we only can have up to 25 licensed users
- Ensure you **select** only DUMMY accounts with **Microsoft 365 E5 Developer licensing**
- At the top of browser select **Delete user**
- DO NOT Delete your **Cloudadmin** account



This process is purely to keep it clean with euc-livefire accounts.

It wont be necessary to do this step if you have a pre-assigned account

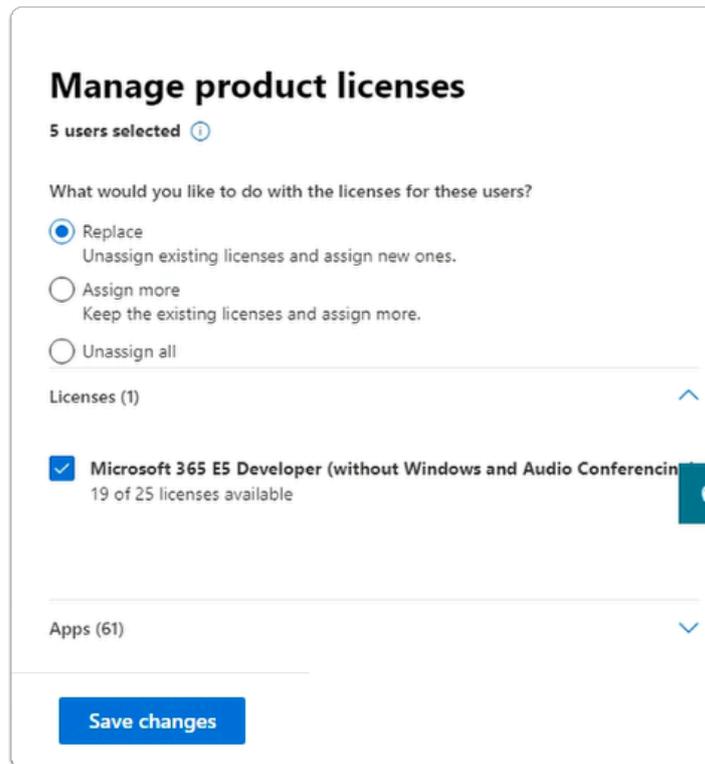


5. In the **Active Users** area

- Select the **radio buttons** next to
 - **Fernando Dusello**
 - **Jill Verneo**
 - **Kevin Ikin**
 - **Kim Markez**
 - **Mark Debio**
- From the **top menu** options
 - At the top of the **Active Users** area, next to **Refresh**,
 - select **Manage product licenses**



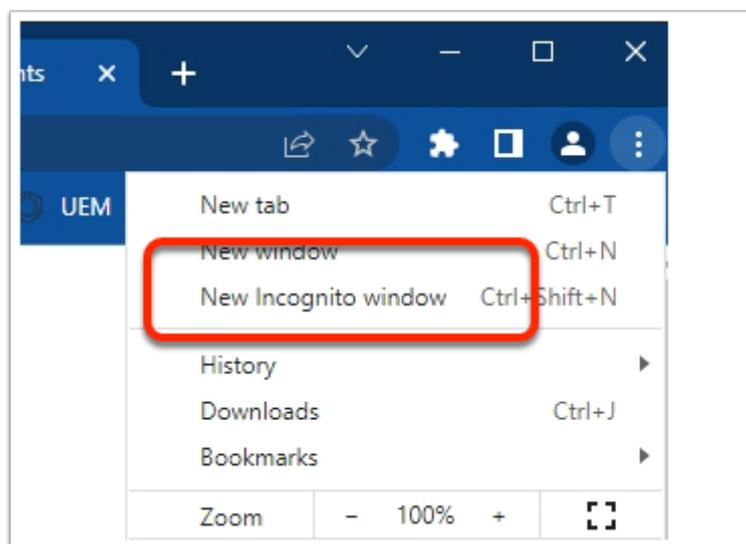
everyone needs to license their newly synced accounts in Microsoft 365



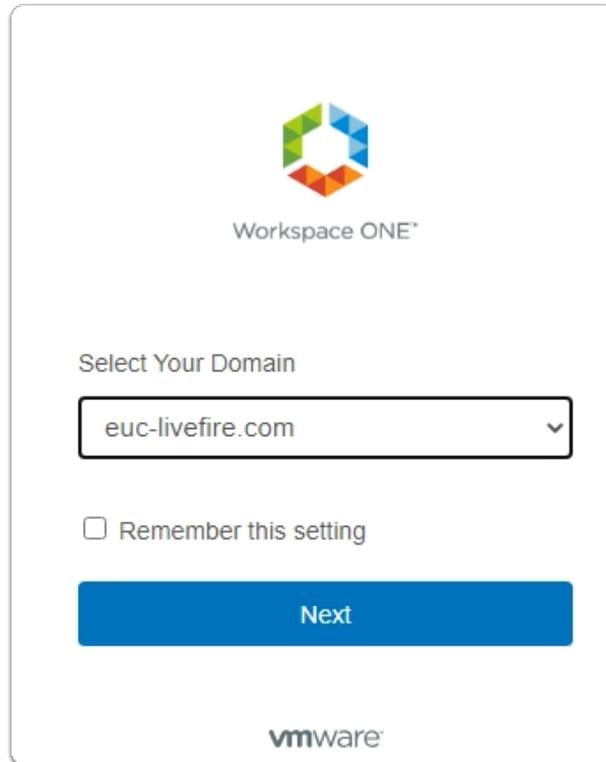
6. In the **Manage Product licenses** window

- Next to **Replace** ,
 - Select the **radio button**
- Next to **Microsoft E5 Developer (without Windows and Audio Conferencing)**
 - Select the **Checkbox**
 - Select **Save Changes**.

Part 7: Testing to see if the Federation works



1. On your Control Center server
 - On your Chrome browser
 - Open up an **Incognito** session
 - In the address bar enter **your Workspace ONE Access tenant url**



Workspace ONE

Select Your Domain

euc-livewire.com

Remember this setting

Next

vmware

2. On the **login** window
 - Under **select Your Domain**
 - from the **dropdown** select , **euc-livewire.com**
 - Select **Next**

Workspace ONE

username
Jill

password

euc-liveware.com

Sign In

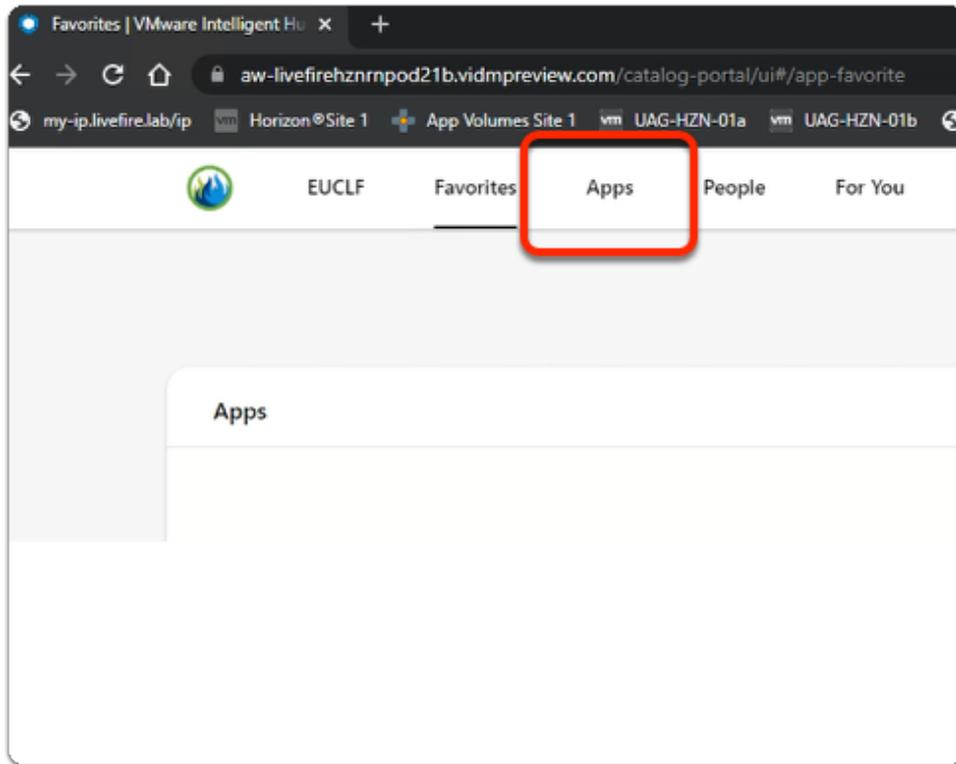
[Forgot password?](#)

[Change to a different domain](#)

vmware

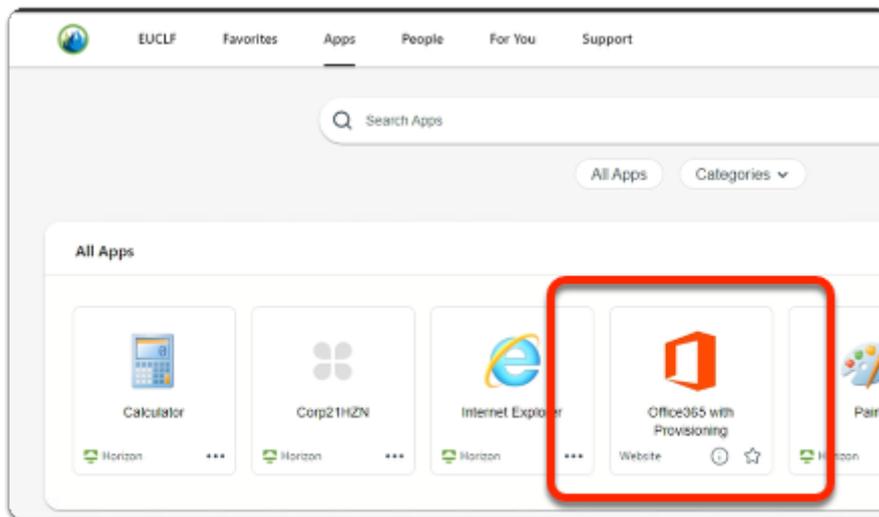
3. On the **login** window

- Under **username**
 - enter **Jill**
- Under **password**
 - enter **VMware1!**
- select **Sign in**



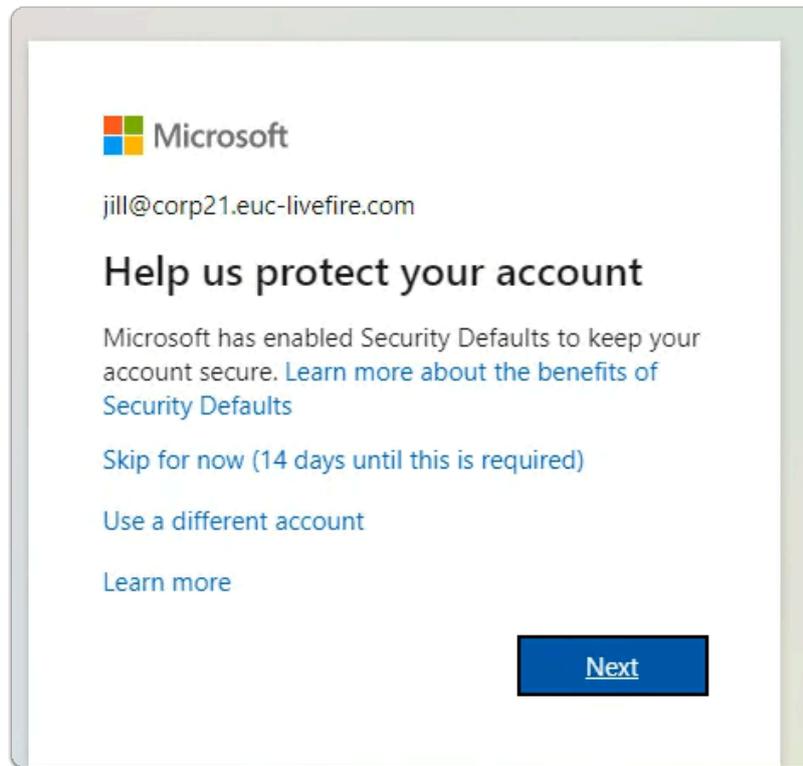
4. In the **web Intelligent Hub**

- Select **Apps**



4. In the **web Intelligent Hub**

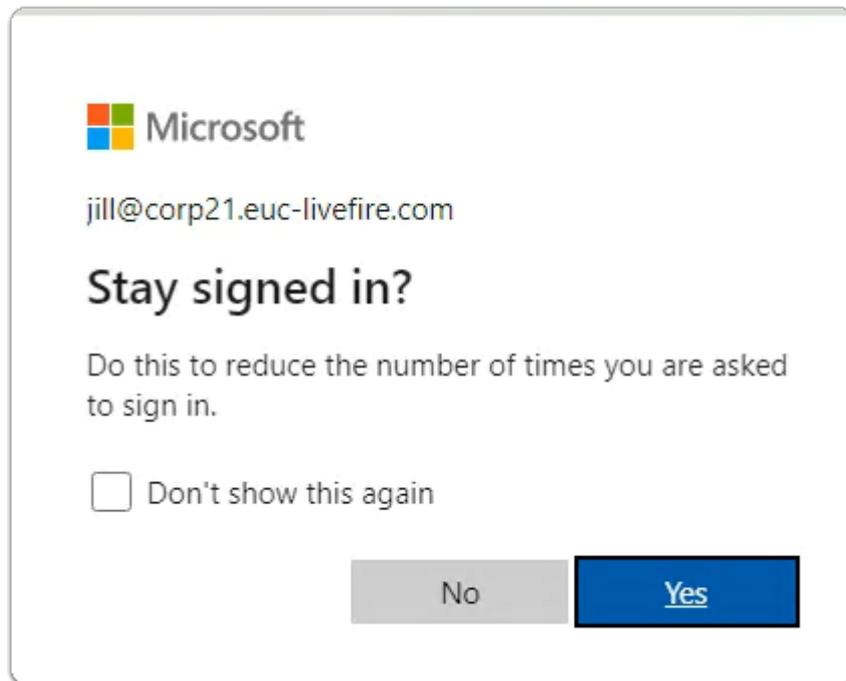
- Under **Apps**
 - Select **Office 365 with Provisioning**



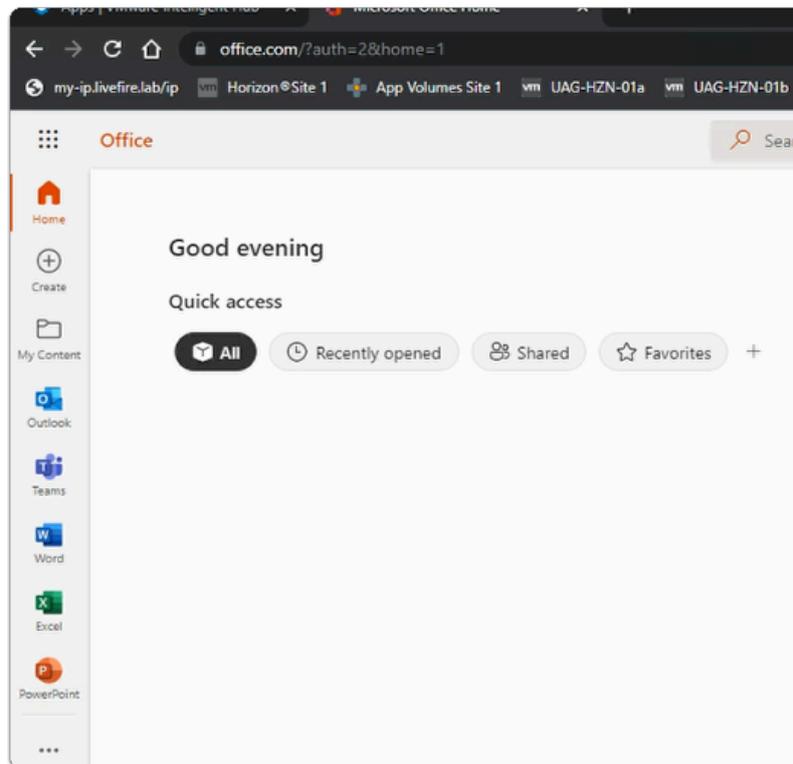
5. In the Help us protect your account window
 - Select , **Skip for now (xx days until this is required)**
 - **xx** represents whatever you see on your screen)
 - Select **Next**



You wont be prompted for this when you have an assigned account



6. On the **Stay signed in?** page
 - Select **Yes**



7. In the office.com window
 - Notice you have access to your Microsoft 365 applications
 - Using deep links, we are able to publish these applications individually to Workspace ONE Access

Acknowledgements

A BIG and wholehearted thank you to Sascha Warno for his support and guidance.

Sascha is a **Staff End User Computing Architect** at VMware

About the Author

About the content author Reinhart Nel

<https://www.livefire.solutions/meet-the-team/reinhartnel/>

For any questions please email Reinhart at RACE-Livefire-EUC@vmware.com