


2. Integrating Workspace ONE Access with an existing Azure implementation

Introduction


The most common implementation of integrating with Microsoft Azure has and will always be, where a customer is already using Microsoft Azure and we want to bring Workspace ONE Access to the table.

In this lab we will look at the configurations and related requirements to setup Microsoft Azure as a 3rd Party IDP to Workspace ONE Access

 The above steps assume you have your own developer account

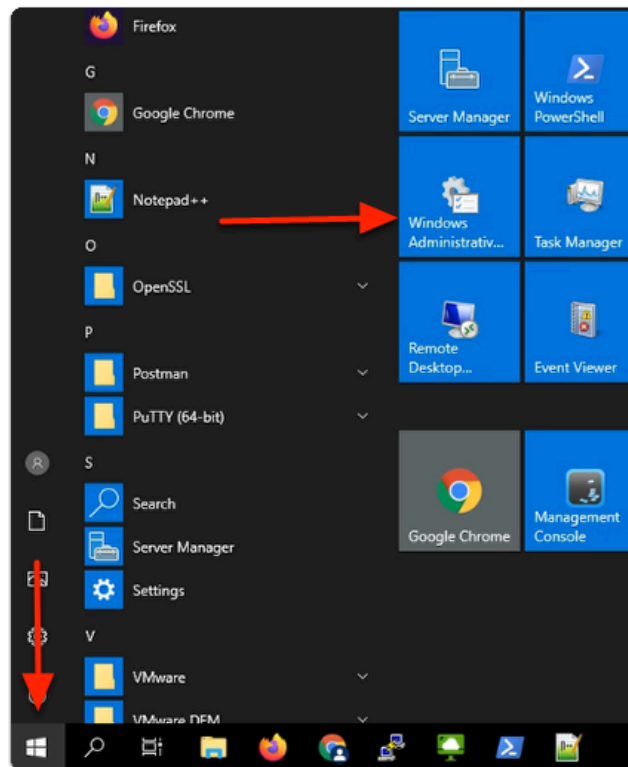
Intro

Part 1. Configuring Microsoft Active Directory Domains & Trusts

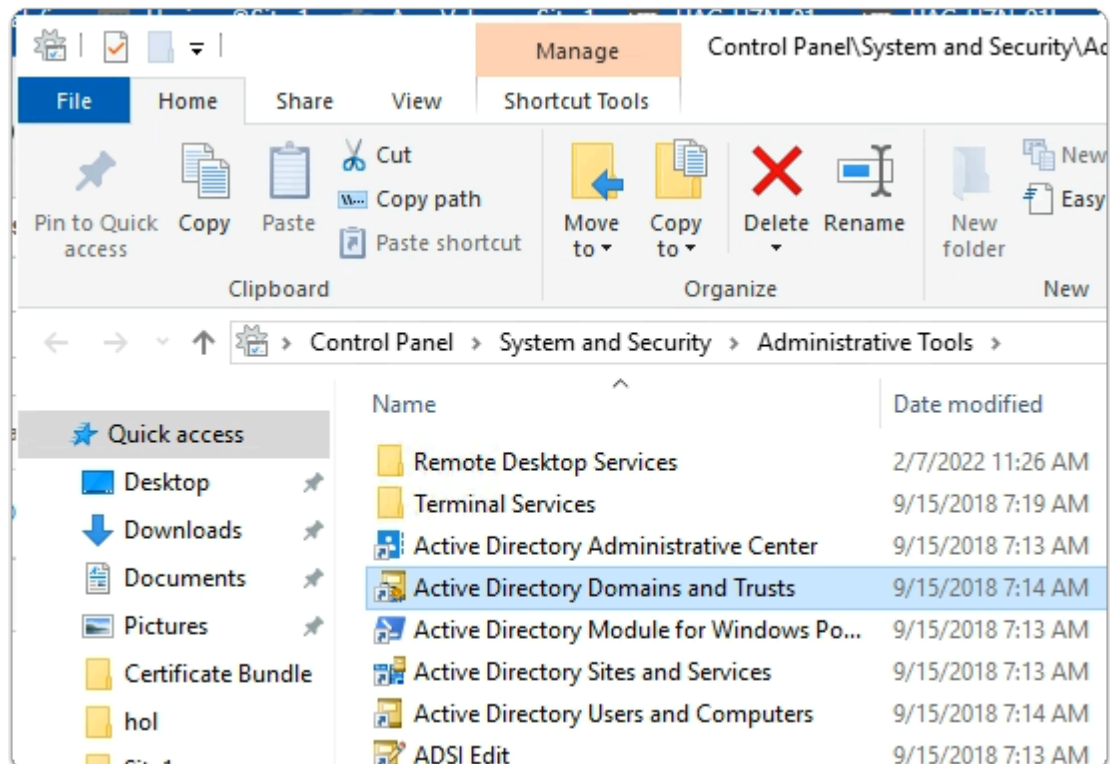
 This option might not be a mandatory requirement, if the namespace we are using internally is publicly resolvable, in other words is not a private namespace like .local or .priv. and is unique.

In our lab environments, the euc-livfire.com namespace is resolvable. This however, is not a unique namespace, as everyone's Microsoft Active Directory environment is sharing a common namespace. For us to be able to integrate our lab environments with Microsoft 365, it's necessary to associate a unique namespace with an individual Microsoft 365 account. Each attendee has been offered a unique DNS Zone namespace under the *.euc-livfire.com namespace.

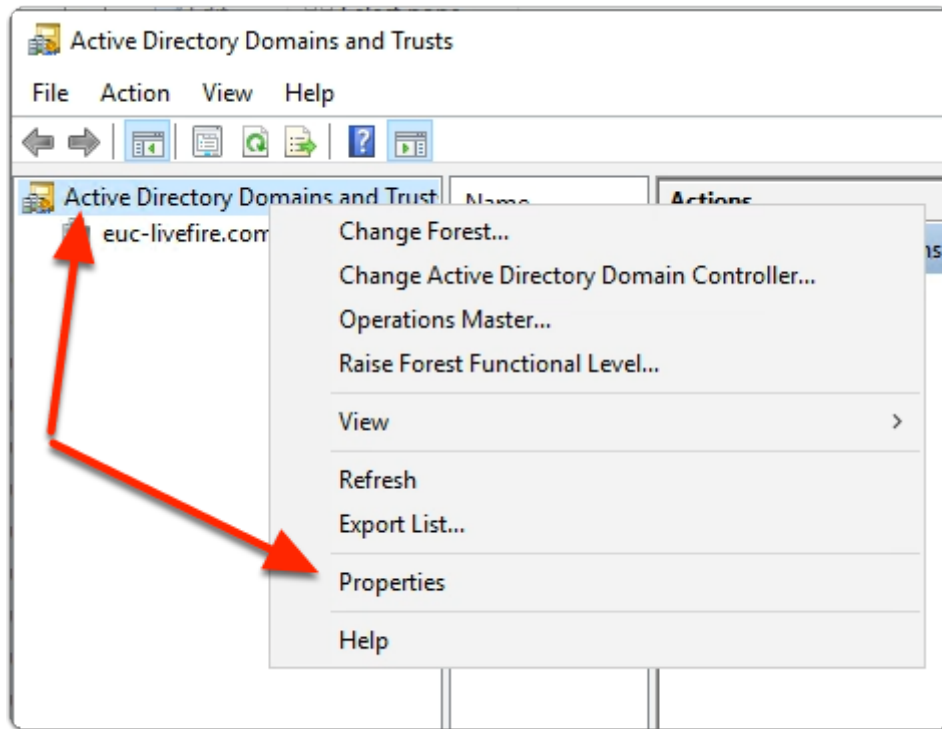
In this session we will associate this unique namespace with Microsoft Active Directory using the Active Directory Domains & Trusts feature



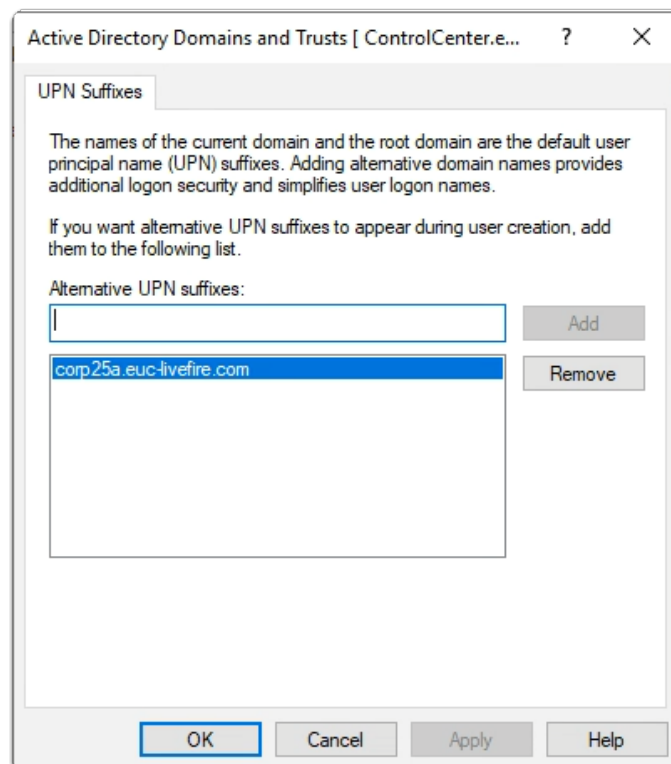
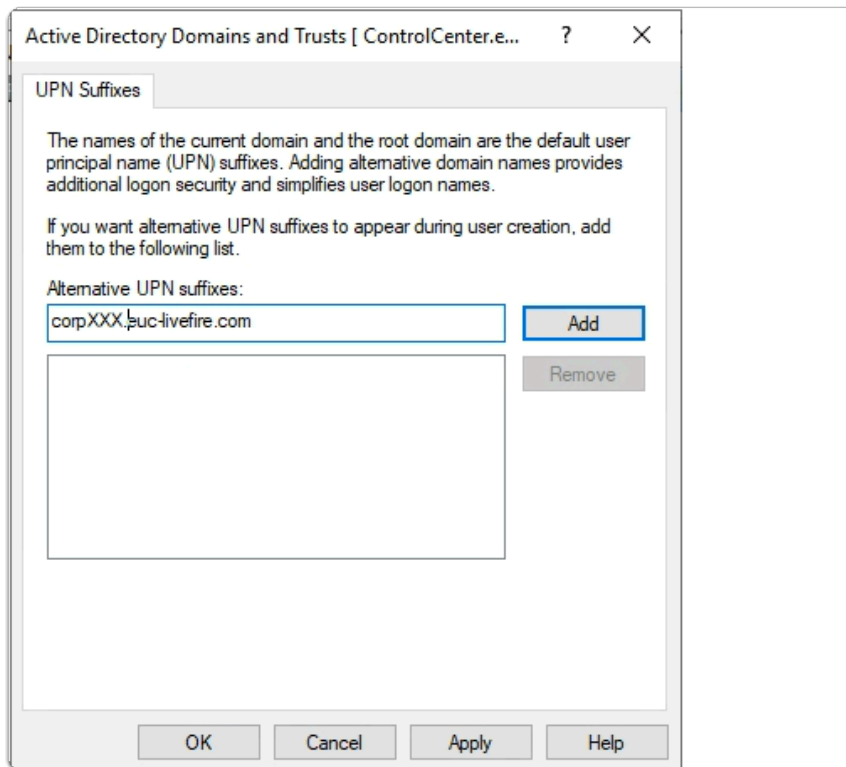
1. On your ControlCenter server
 - In the bottom left corner
 - Select the **Start** button
 - In the **Start Menu**
 - Select **Windows Administrative Tools**



2. In the **Administration Tools** menu
 - Select the **Active Directory Domains and Trusts** shortcut



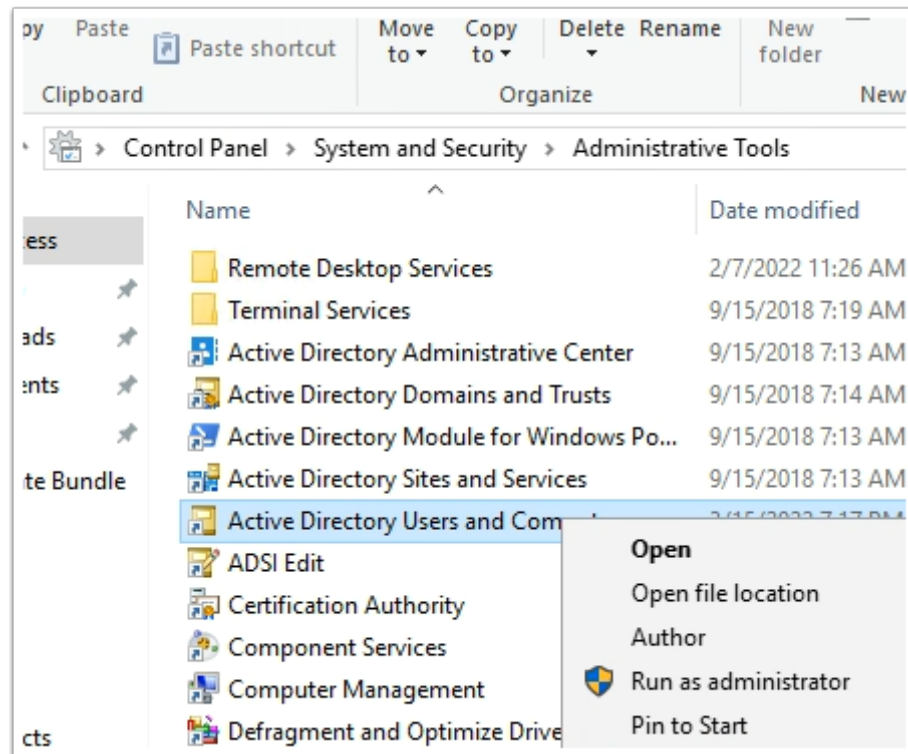
3. In **Active Directory Domains and Trusts**
 - In the Inventory
 - Select and right click
 - **Active Directory Domains and Trusts**
 - Select **Properties**



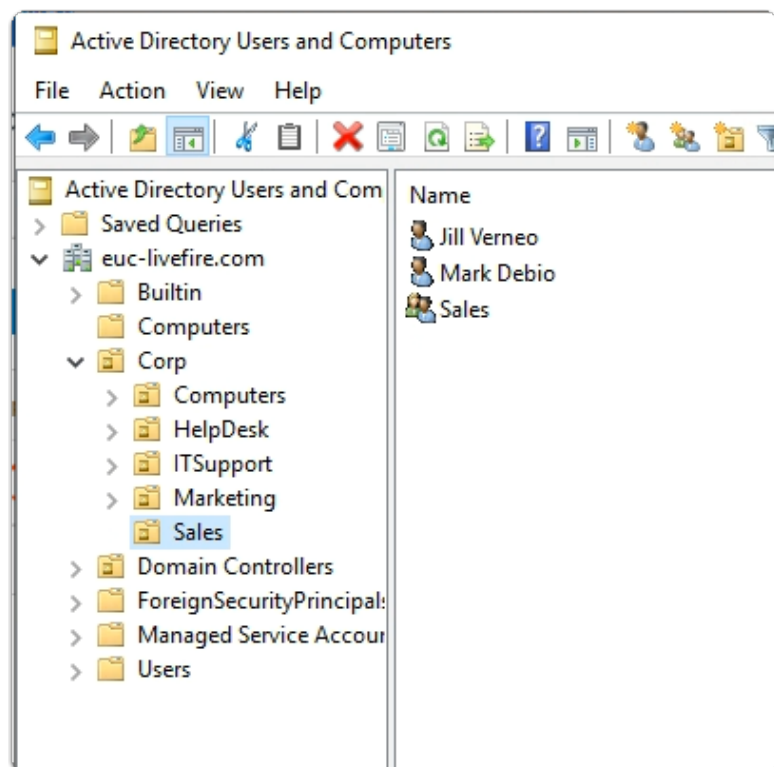
4. In the Active Directory Domains and Trusts window

- 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**

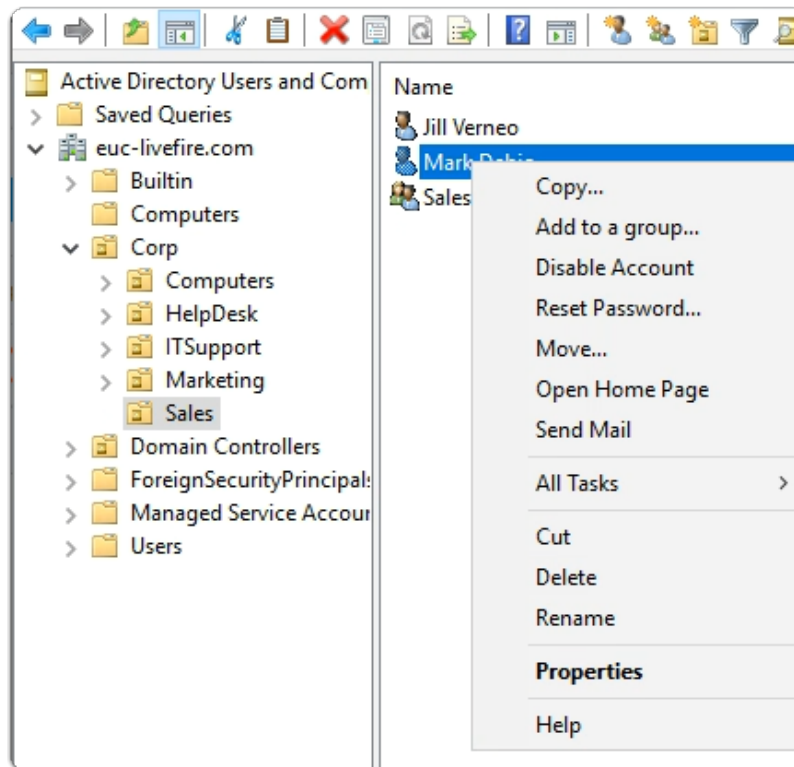


5. In the **Administrative tools** folder
 - Select **Active Directory Users and Computers** shortcut
 - Select **open**

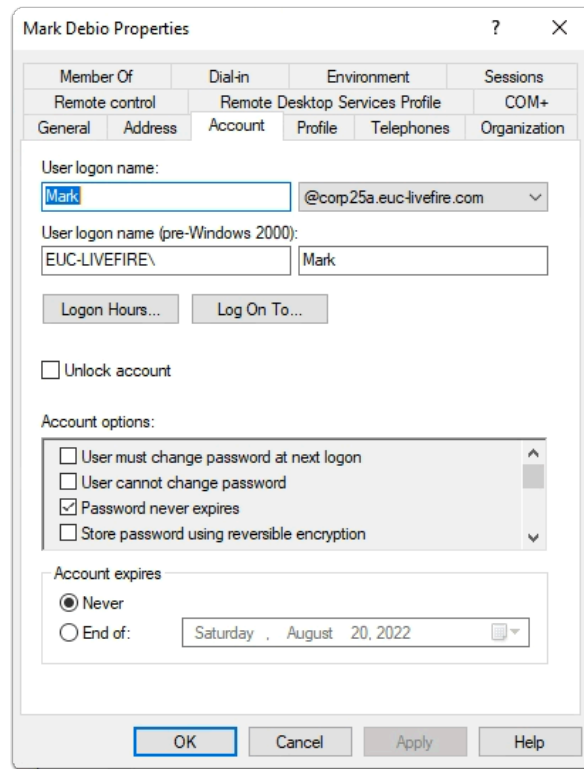


6. In the **Active Directory Users and Computers** Console

- **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-livfire.com
 - where **XXX** is your assigned **Domain ID**
 - To close **Mark Debio Properties**
 - Select **OK**

Jill Verneo Properties

Member Of: Remote control, Remote Desktop Services Profile, COM+
General Address Account Profile Telephones Organization

User login name: @corp25a.euc-livewire.com

User login name (pre-Windows 2000): EUC-LIVEFIRE\

Logon Hours... Log On To...

Fernando Properties

Member Of: Remote control, Remote Desktop Services Profile, COM+
General Address Account Profile Telephones Organization

User login name: @corp25a.euc-livewire.com

User login name (pre-Windows 2000): EUC-LIVEFIRE\

Logon Hours... Log On To...

Tom Marios Properties

Member Of: Remote control, Remote Desktop Services Profile, COM+
General Address Account Profile Telephones Organization

User login name: @corp25a.euc-livewire.com

User login name (pre-Windows 2000): EUC-LIVEFIRE\

Logon Hours... Log On To...

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

- Repeat the above mention steps for at least these accounts :
 - In the **Sales OU** :- **Jill Verneo**
 - In the **Marketing OU** :- **Fernando Dusello**
 - In the **Marketing OU** :- **Tom Marios**
 - In **IT Support OU** :- **Kim Markez**
 - In **Developers OU** :- **Craig Sroser, Jackie Puun, Malcolm Barneo, Nancy Encrarna**

Workspace ONE Access Search for users, groups, or applications

Monitor Accounts Resources **Integrations** Settings

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

Directories
Integrate your enterprise directories with VMware

ADD DIRECTORY

All Directories
SYNC

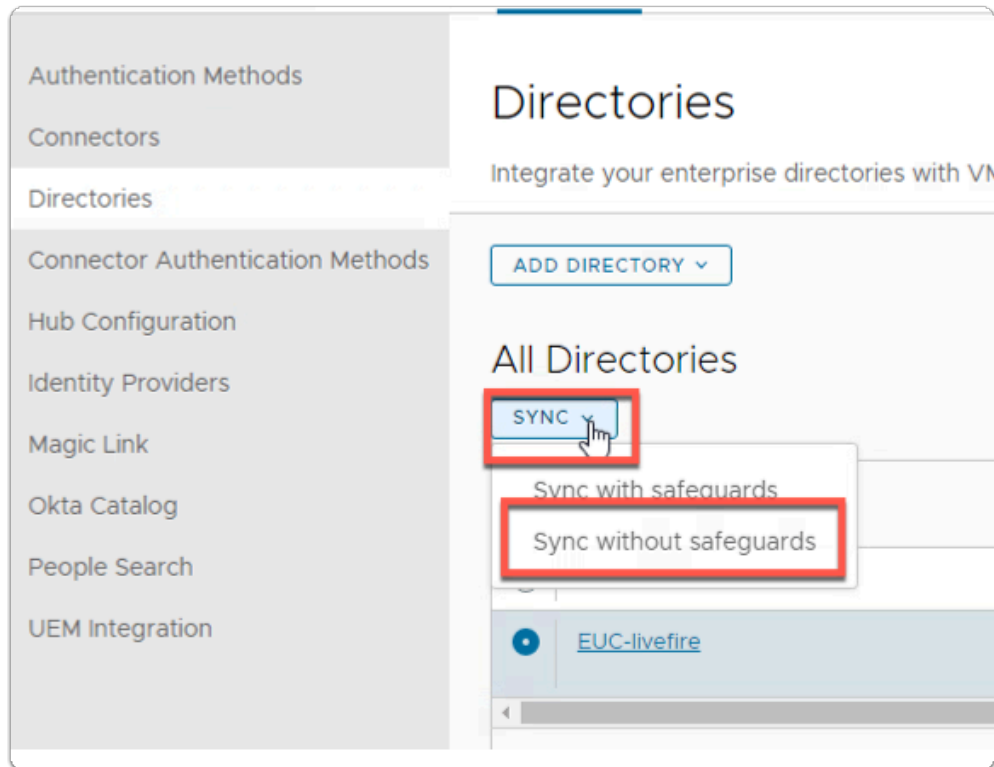
	Directory Name	Type	Domains	Synced Groups	Synced Users	Last
	System Directory	Local Directory	1	0	2	
	EUC-livewire (Directory is currently being synced. Refresh to see changes.)	Active Directory Over LDAP	1	53	12	Apr 12:58

Import Status: Sync started - This process happens in the background and you can continue working. Depending on the number of users and groups being synced, this process can take a while to complete. Check the Sync Logs for details.

10. On your ControlCenter server

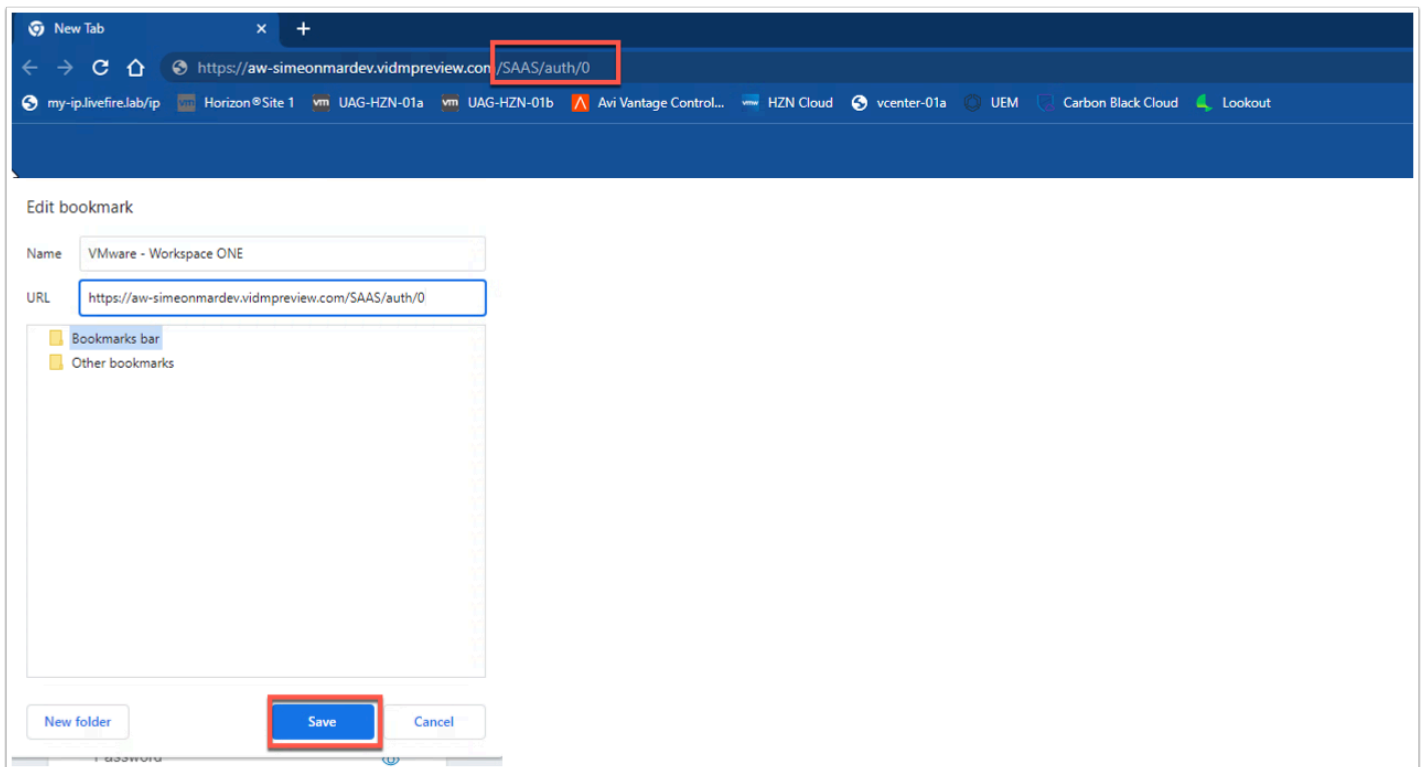
- Switch to your **Chrome** Browser

- Select your **Workspace ONE Access** session
- In the **Integrations > Directories area > EUC-Livefire area**



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

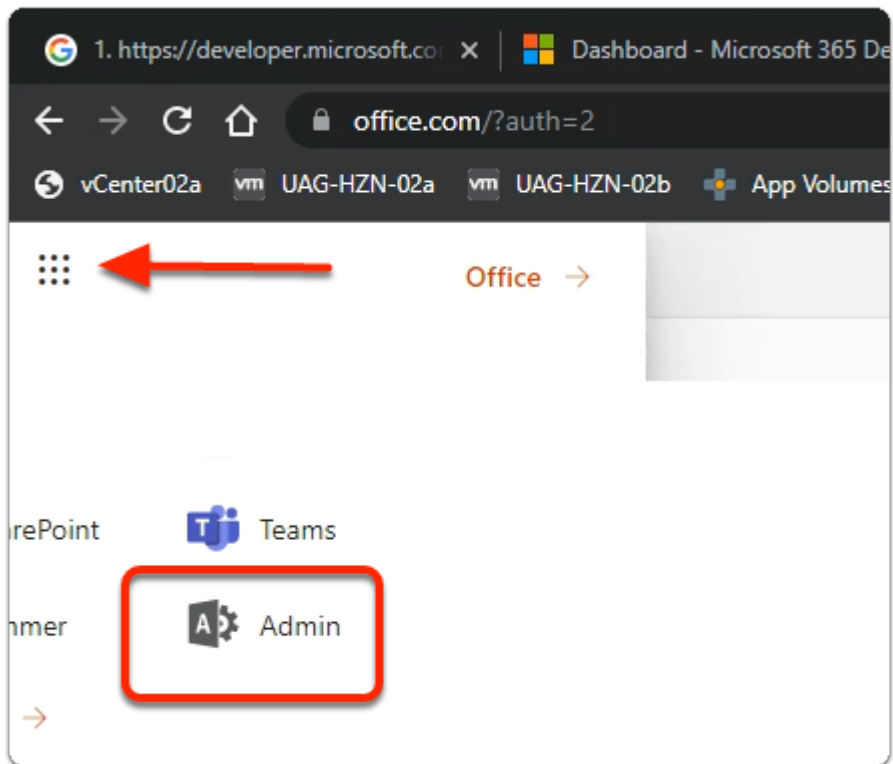
- Next to **Sync**
 - Select **the Dropdown**
 - Select **Sync without Safeguards**



12. Take the URL for WorkspaceONE Access and add **/SAAS/auth/0** and save it to your bookmarks. This will ensure we will be able to login after we have done the federation with Azure.

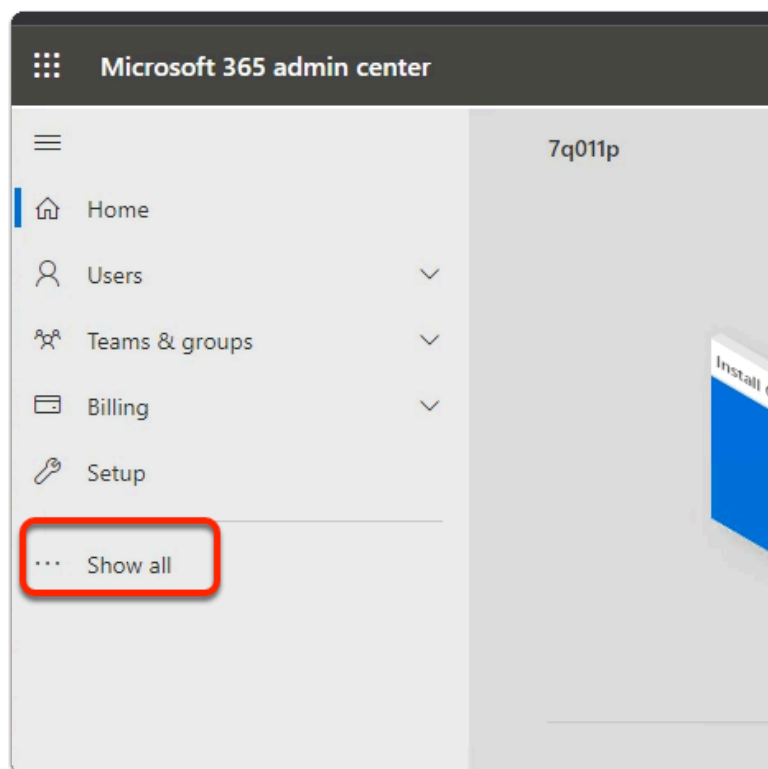
Part 2: Preparing the Microsoft 365 environment to use a dedicated domain name

- **Introduction: In preparation for Part 2**
 - In your browser open a **new tab**
 - In the address bar
 - enter **https://portal.office.com**
 - Log in with your Cloud admin credentials



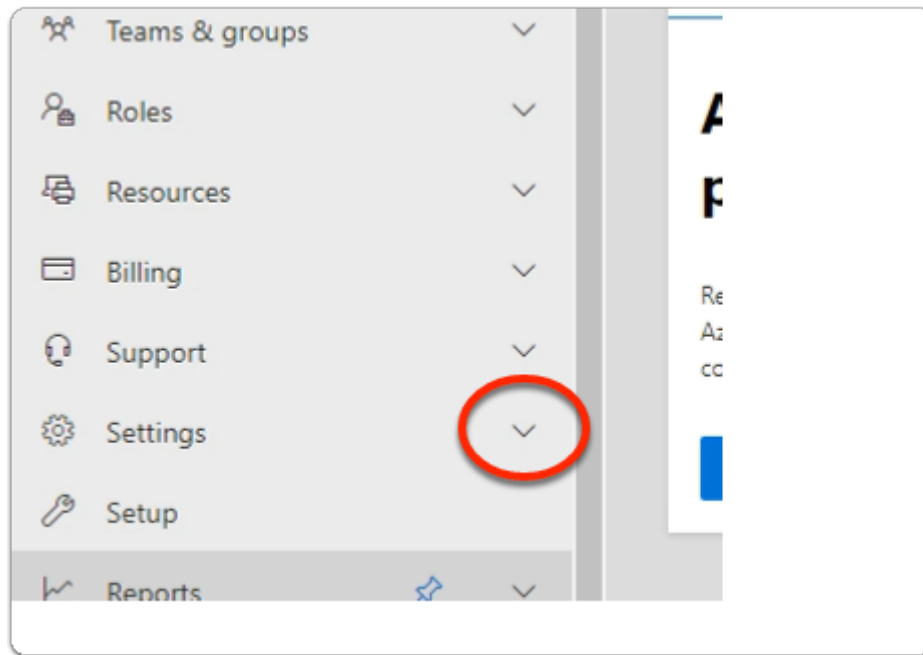
1. In the top left-hand corner off Microsoft 365

- Select the **9 dotted square**
- Once the **Apps** pop out expands
 - Select **Admin**



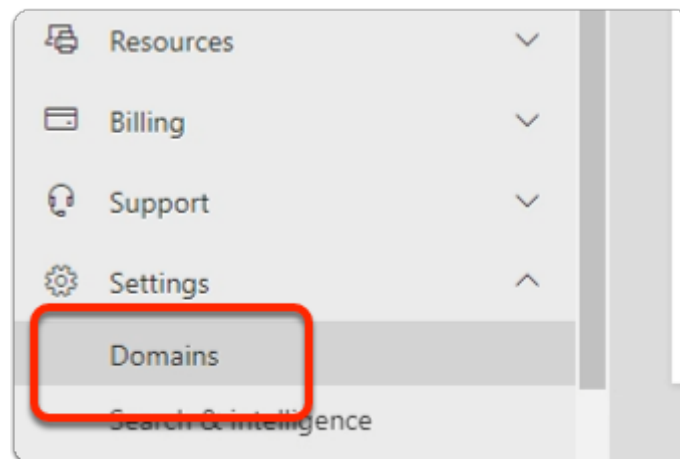
2. In the **Microsoft 365 admin center** window

- Select **Show all**



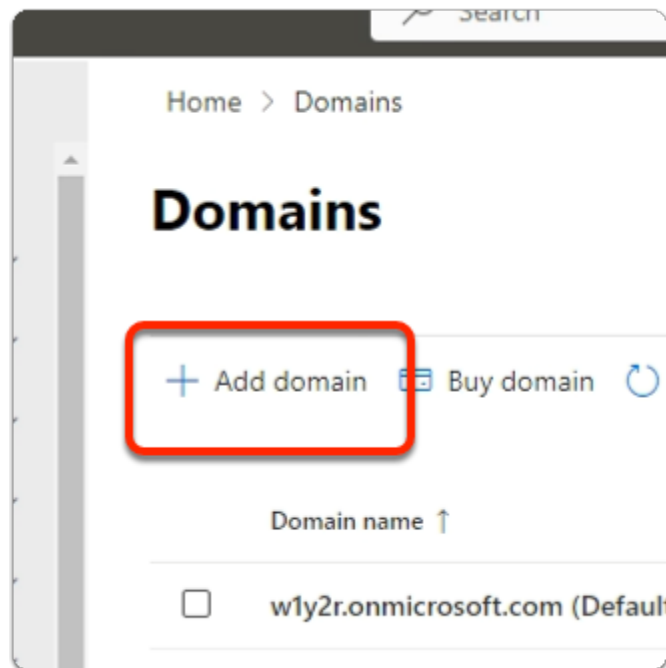
3. In the **Microsoft 365 admin center** window

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



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

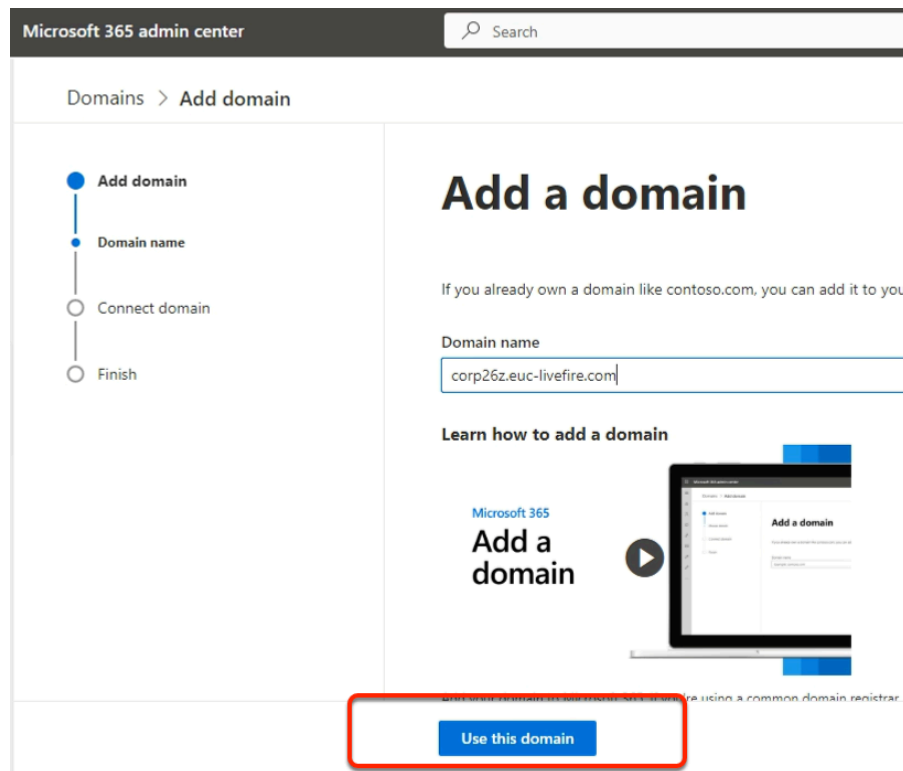
- Under **Settings**
 - select **Domains**



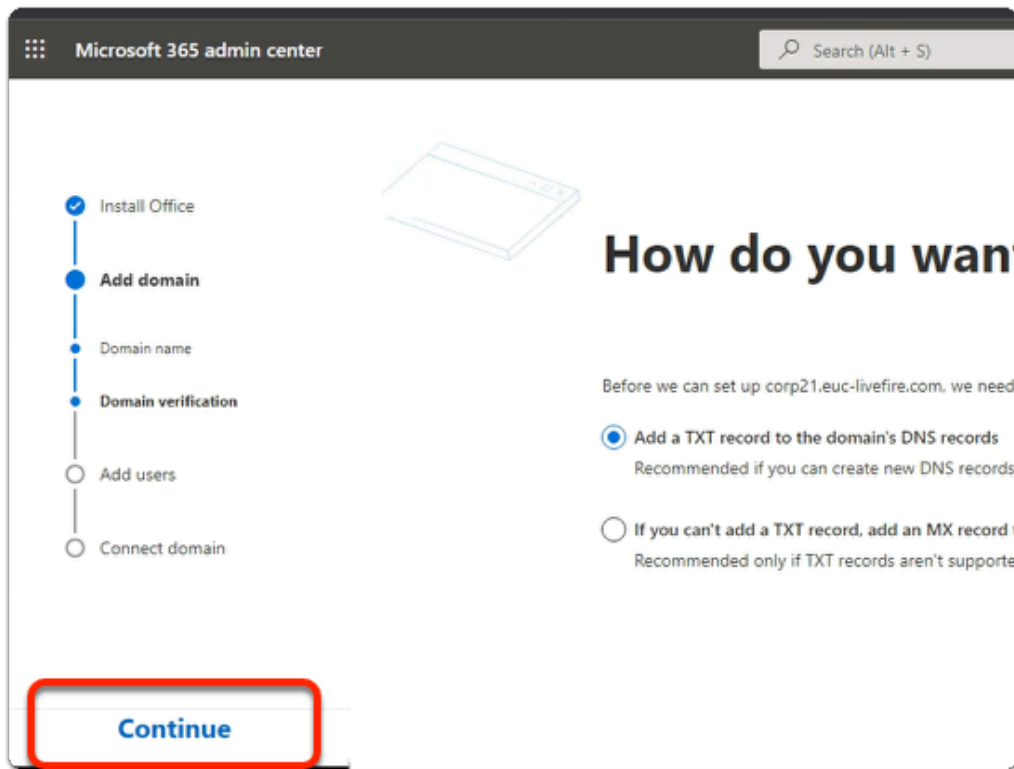
5. In the **Domains** area
 - Select **+ Add domain**

Styles		Cells
Role	Assigned Domain	Landing
rel!	Corp01f	dwu
rel!	Corp02f	dwu
rel!	Corp03f	dwu
rel!	Corp04f	dwu
rel!	Corp05f	dwu
rel!	Corp06f	dwu

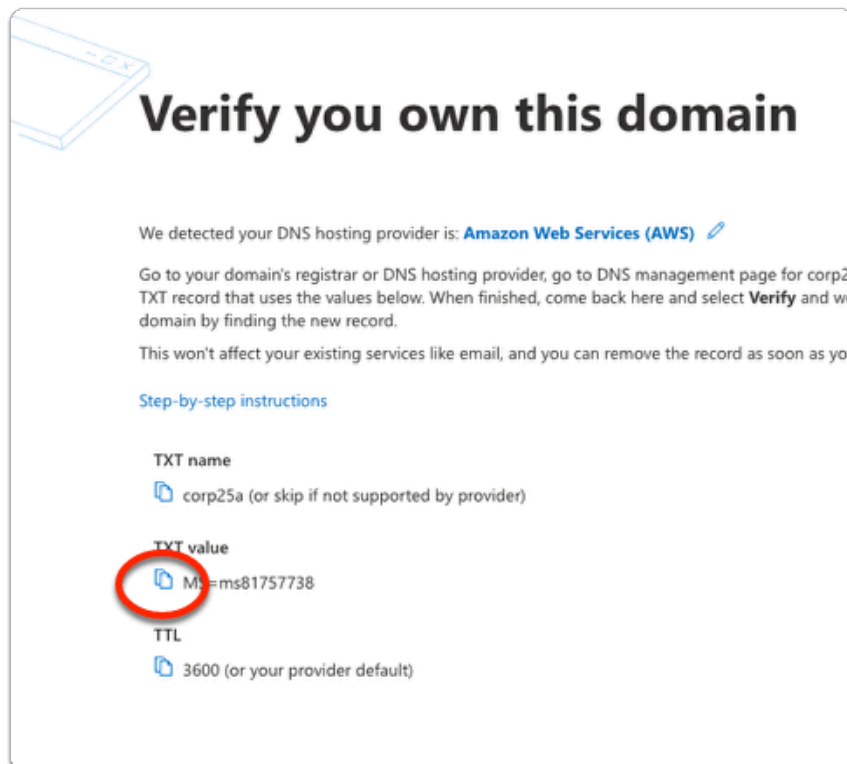
- i** NOTE: Before moving onto the next section, ensure that you are **100% clear** what **YOUR** registered Domain will be.
- In the course lab we will use a Domain naming convention based on the location we are delivering at.
 - We will use the convention corp**XXX**.euc-livefire.com
 - Where **XXX** 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**



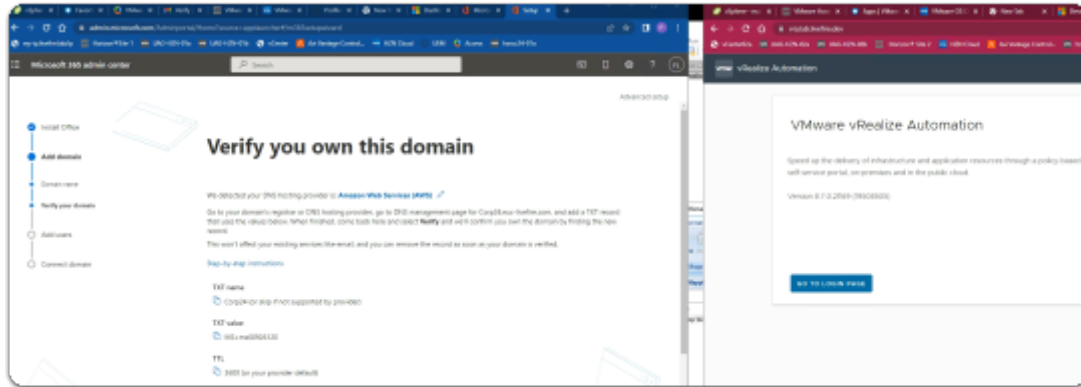
6. In the **Microsoft 365 admin center** window
 - In the **Add domain** area
 - Under **Yes, add this domain now**
 - enter **corpXXX.euc-livefire.com**
 - Where **XXX** is your assigned Domain identifier
 - At the **bottom of the page**
 - Select **Use this domain**



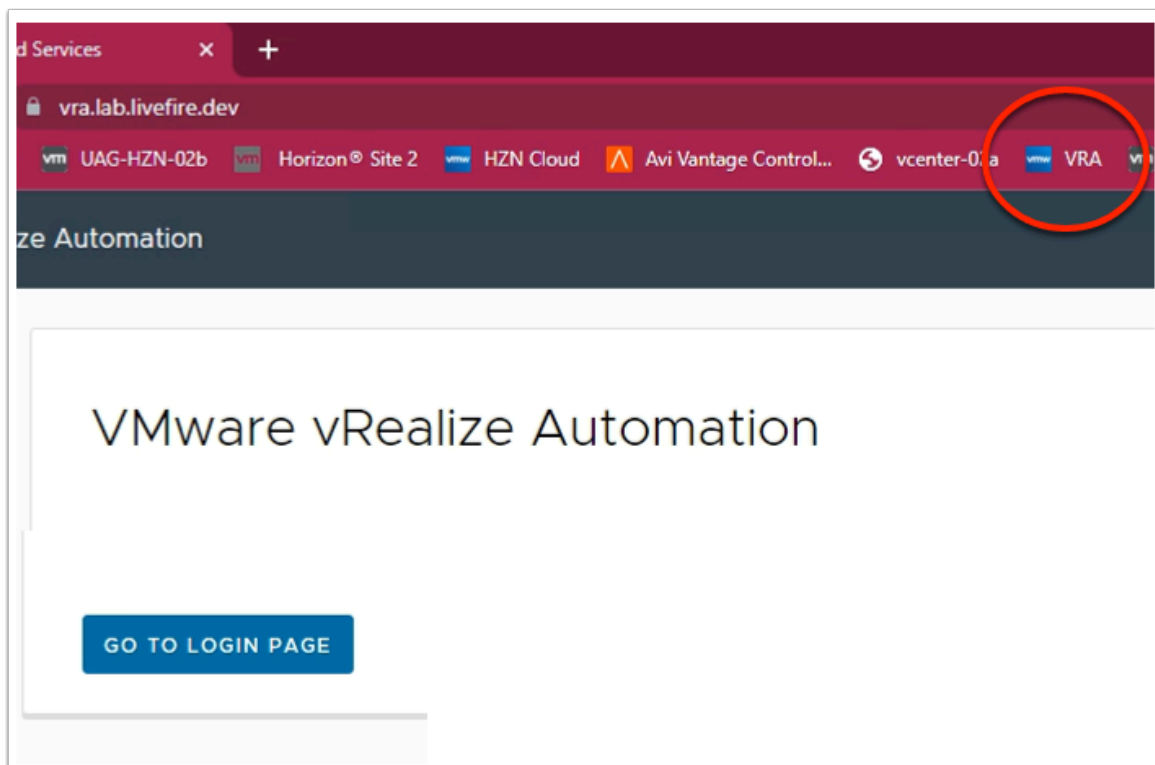
7. In the **Microsoft 365 admin center** window
 - In the **How do you want to verify your domain?**
 - Ensure the **radio button** next to **Add a TXT record to the domain's DNS records** is **enabled (default)**
 - Select **Continue**



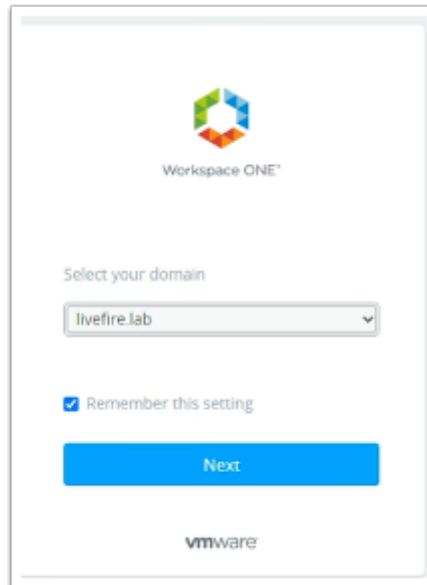
8. In the **Microsoft 365 admin center** window
- In the **How do you want to verify your domain?**
 - **Below TXT value**
 - Copy the **MS= ms**
 - In the following steps, we will have this value entered into your assigned Zone database in AWS Route 53 using vRealize automation



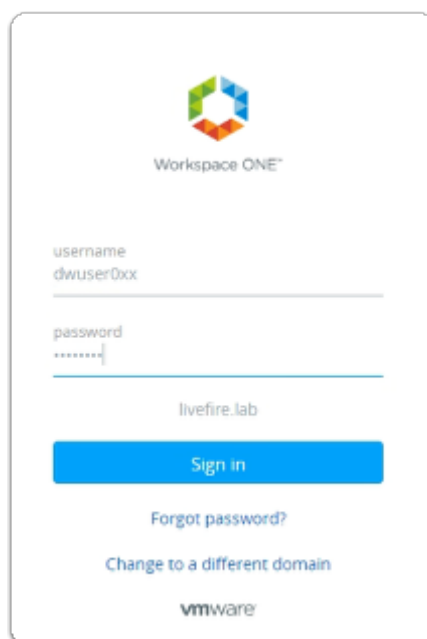
- 💡 Do step 9: VRA automation on a separate browser profile.
- If you were doing your Azure registration on the Site 1 profile then might be helpful to do the VRA on the Site 2 Profile and have both profiles open side by side.



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**

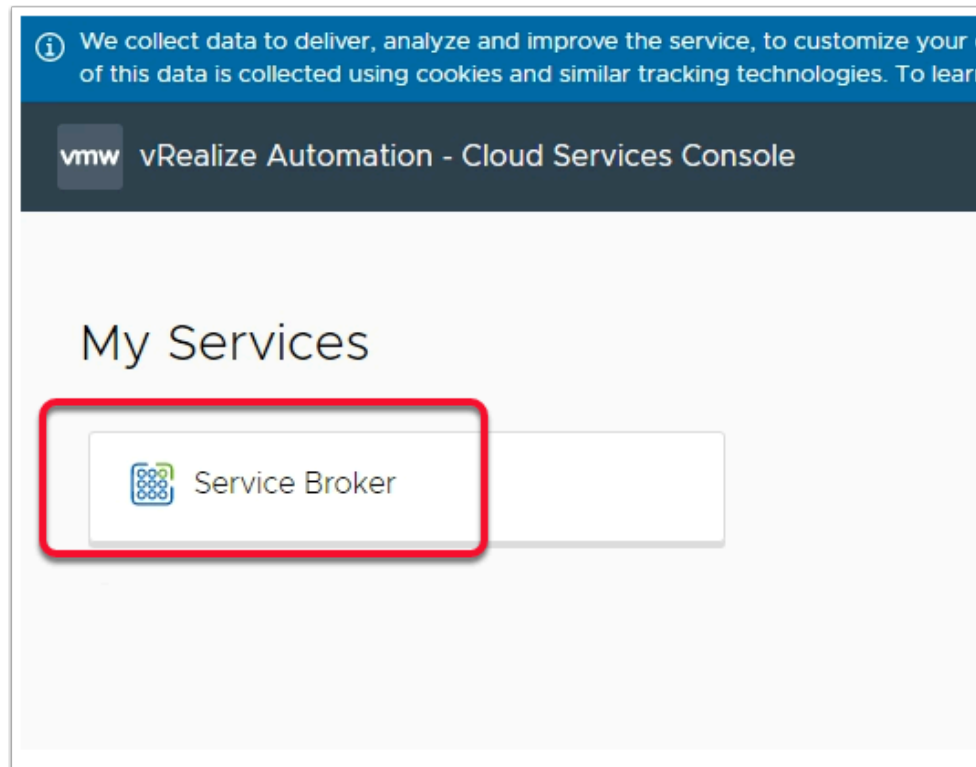


10. In the Workspace ONE Login
 - Under **Select your domain**
 - Ensure **livefire.lab** selected
 - select **Next**

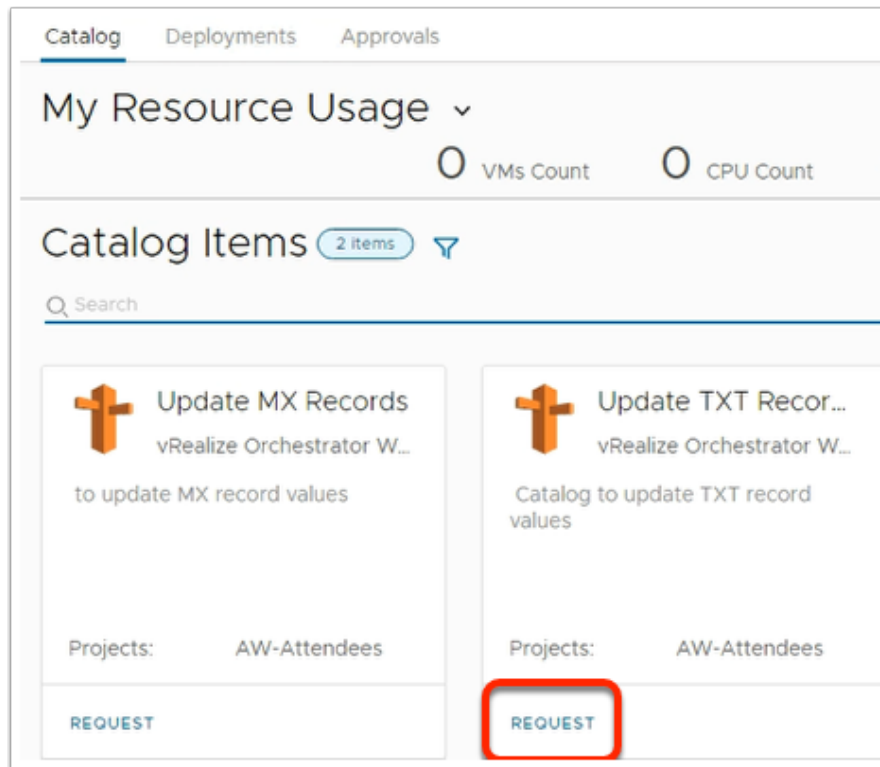


11. In the Workspace ONE login

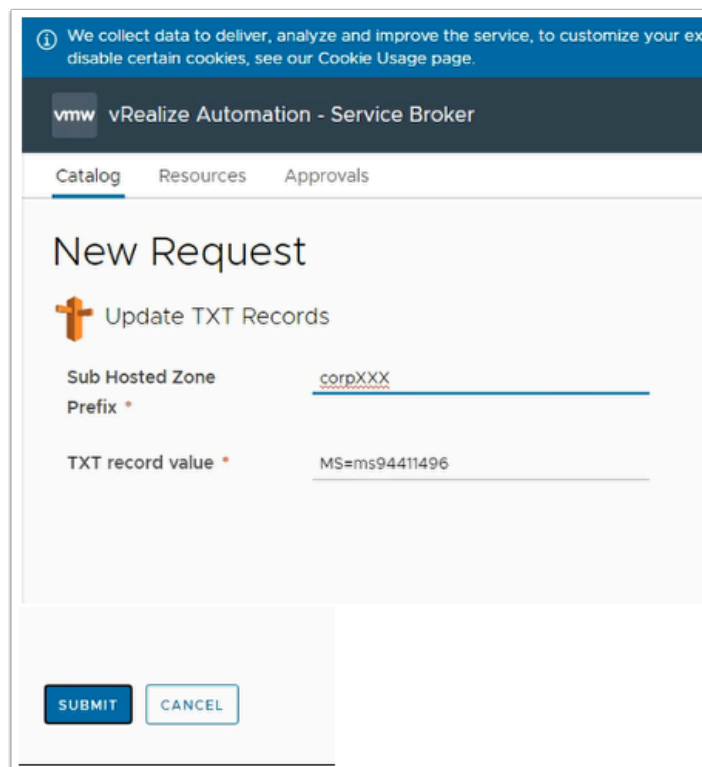
- Under **username**
 - Enter your assigned **dwuser0XX** account
 - **XX** will be your **assigned Student Login ID**
- Under **password**
 - Enter your **assigned password**
- Select **Sign in**



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

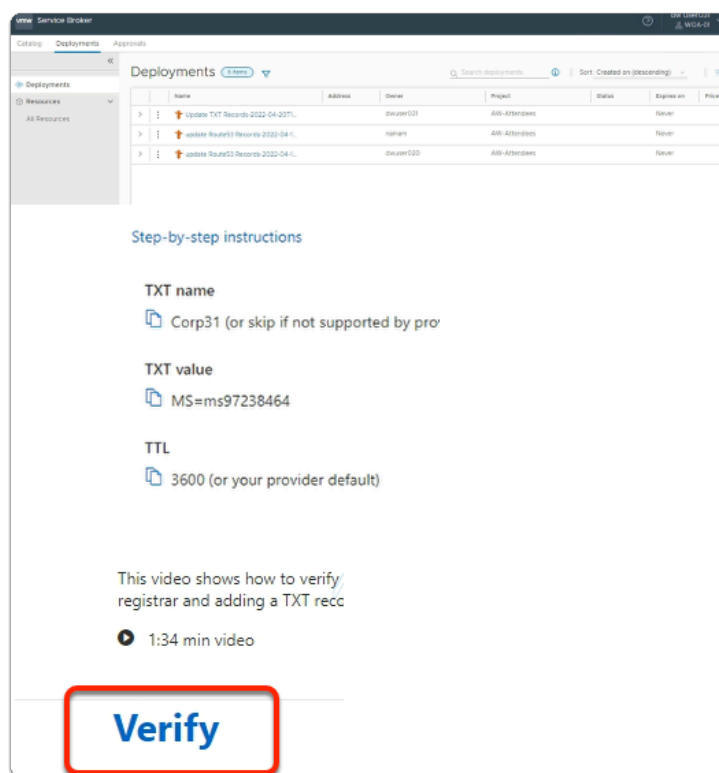


13. In the **My Resource Usage** window
 - Under **update TXT Records**
 - Select **REQUEST**

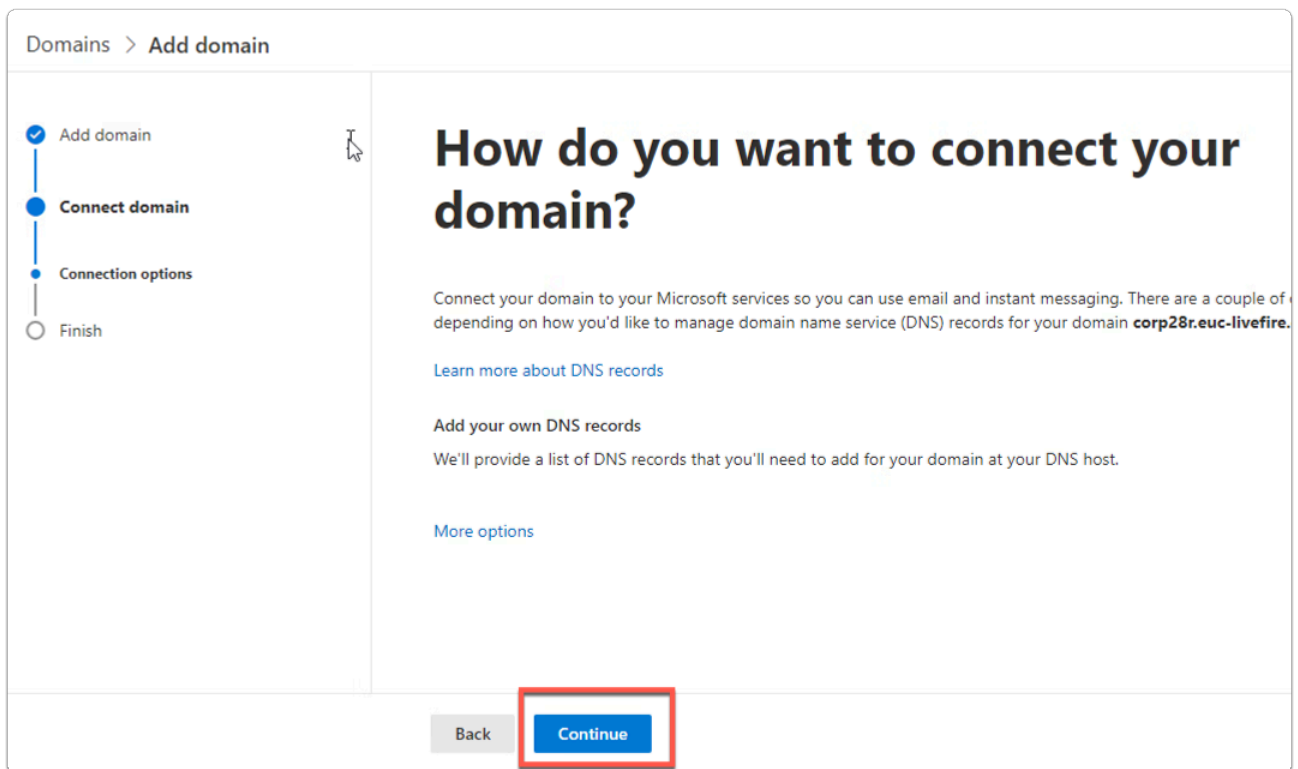


14. In the **New Request** page
 - Update the following next to:

- **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**

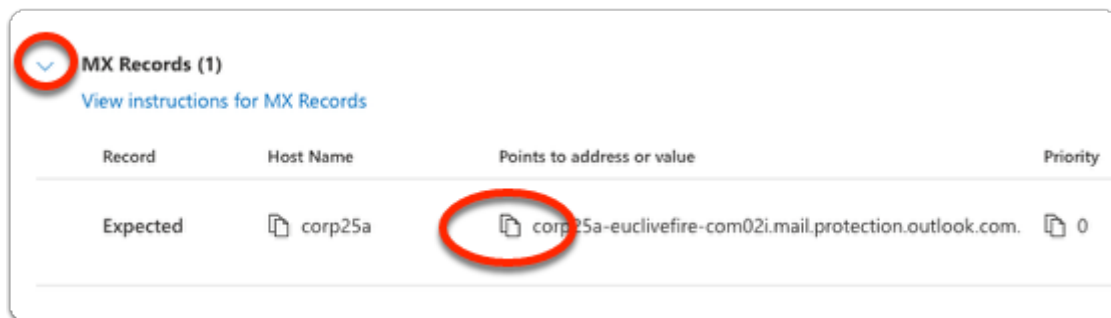


15. On your **Microsoft 365 admin** center page
 - When the **vrealize automation** is complete
 - Select **Verify**



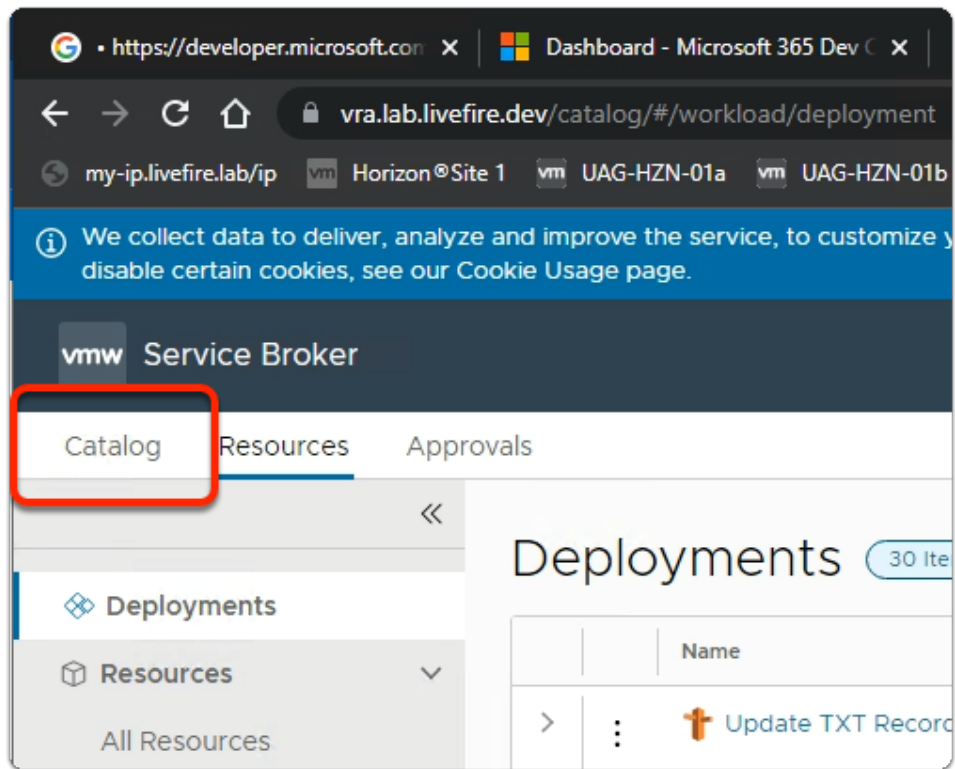
16. In the **Microsoft 365 admin center** window

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

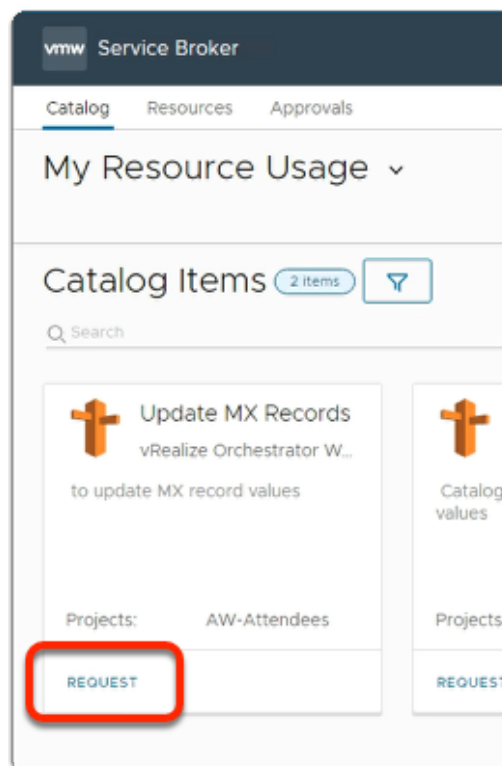


17. In the **Microsoft 365 admin center** window

- 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




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



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

[Catalog](#) [Resources](#) [Approvals](#)

New Request

 Update MX Records

Sub Hosted Zone	corpXXX
Prefix *	
MX record value *	corpXXX-euclivfire-com02i.mail.protec

Please note xxx is your attendee identifier.

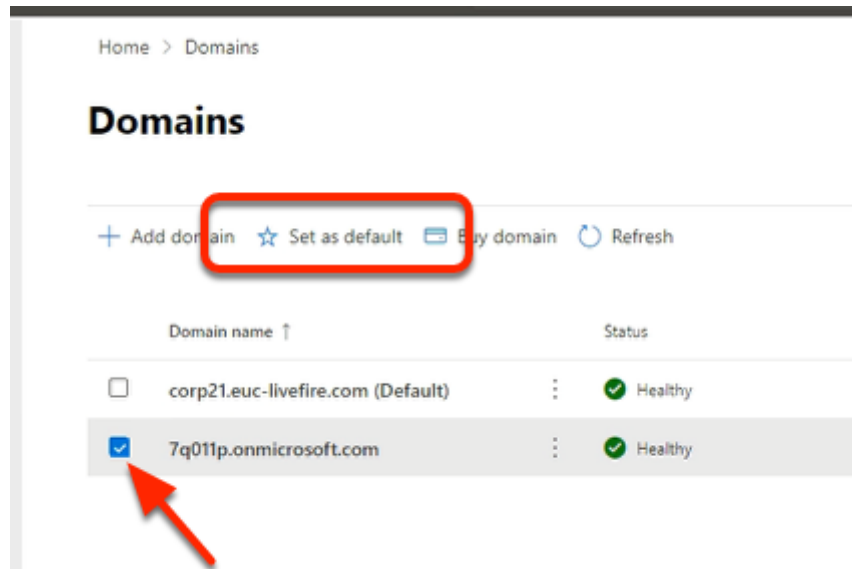
20. In the **Service Broker**

- **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**

- Select **Done**

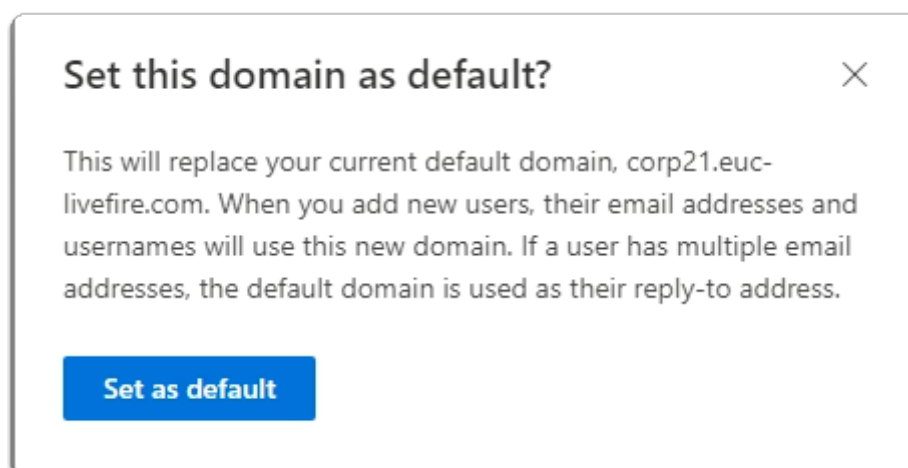


If you are using an existing account, its very likely you wont have to change your default domain. Validate and if necessary do the change



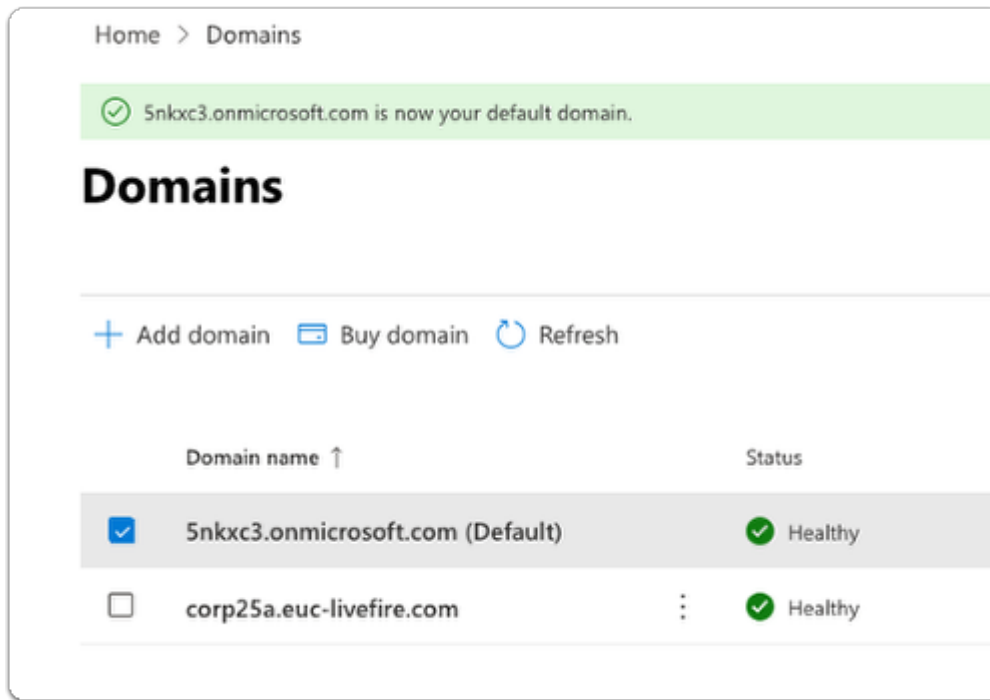
23. In the **Domains** area

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



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

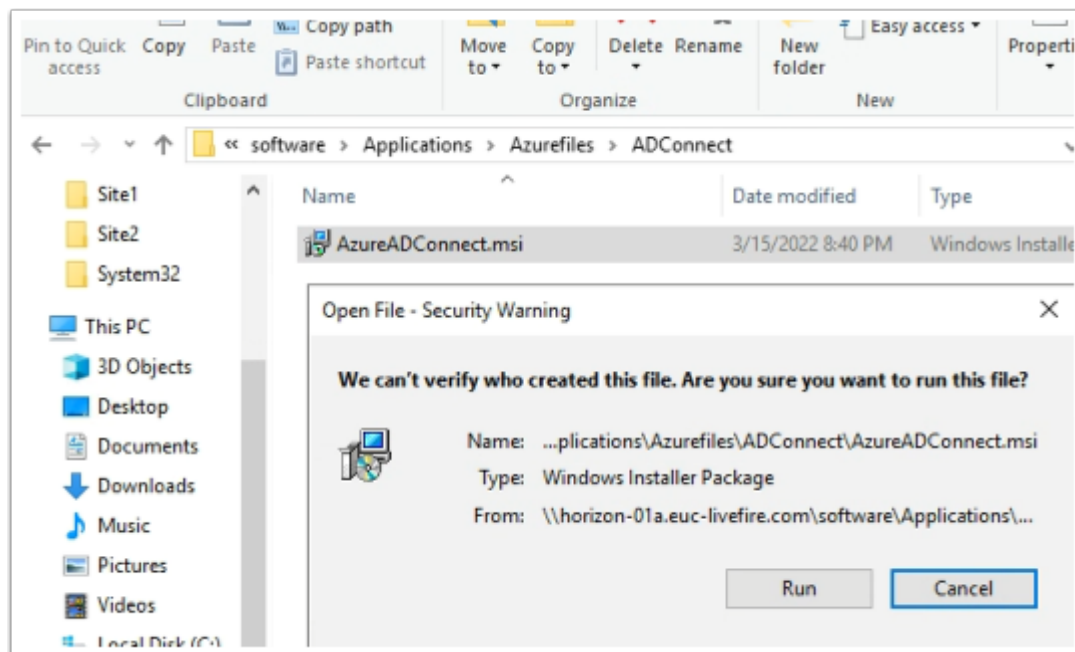
- Select **Set as default**



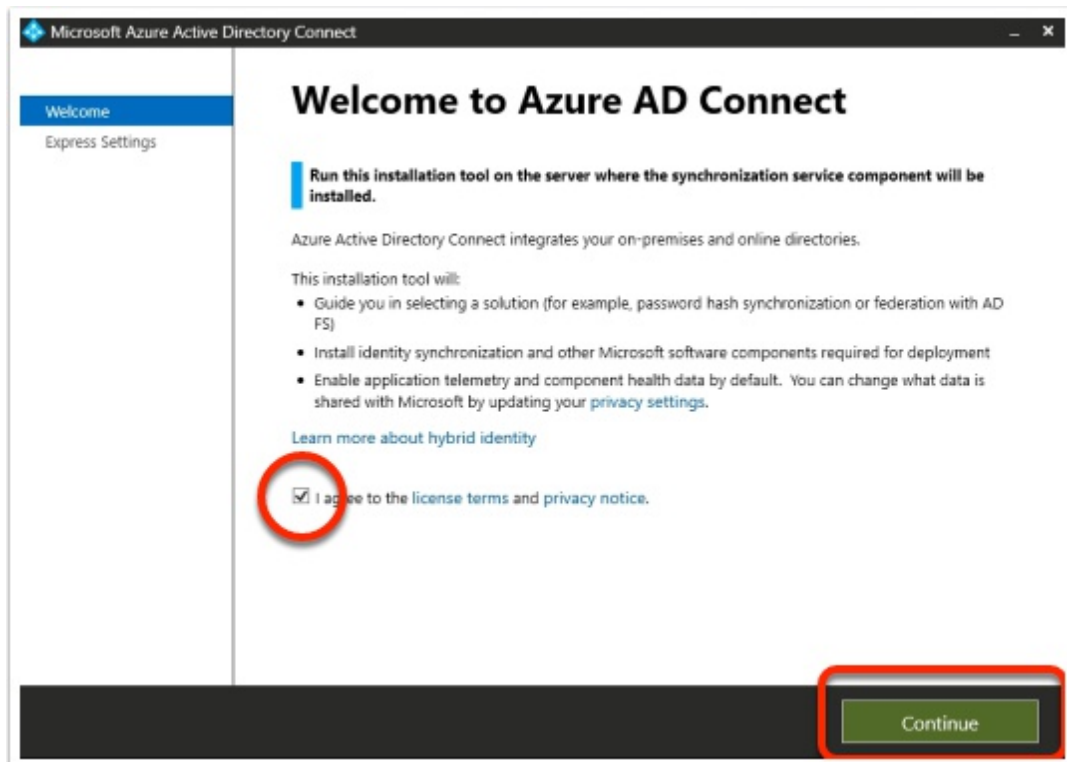
25. In the **Domains** page
- Validate your default configuration

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

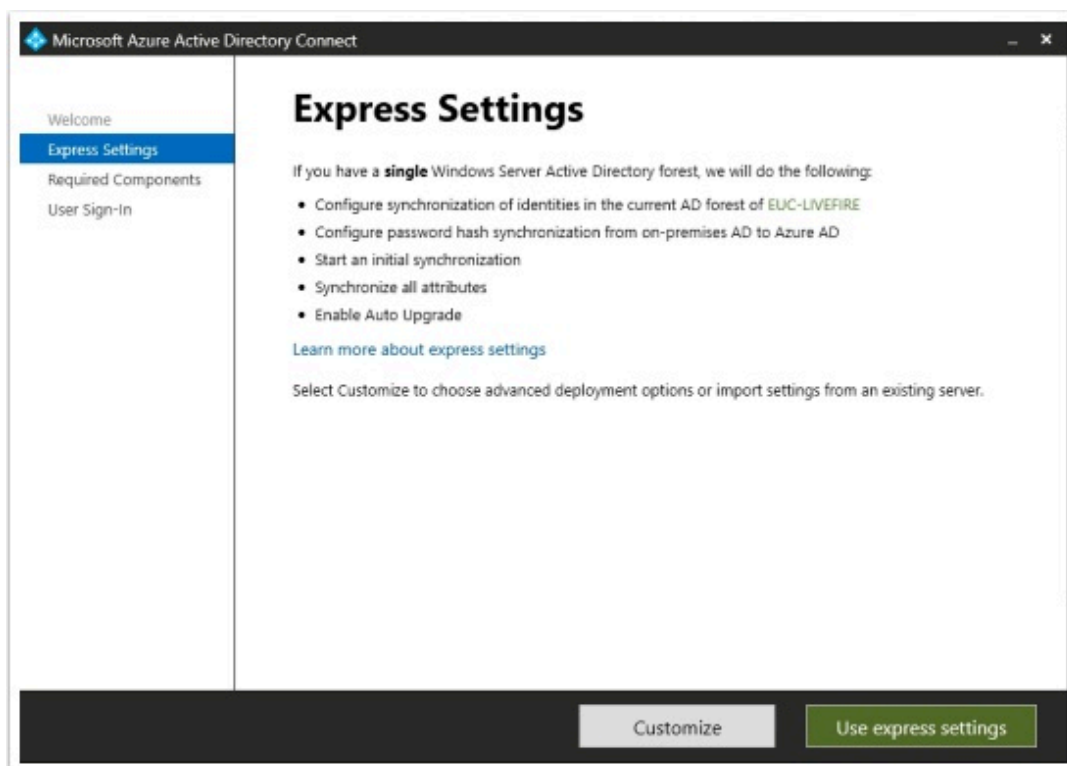
Part 3: Using Microsoft Azure AD Connect for user provisioning to Microsoft Azure



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**

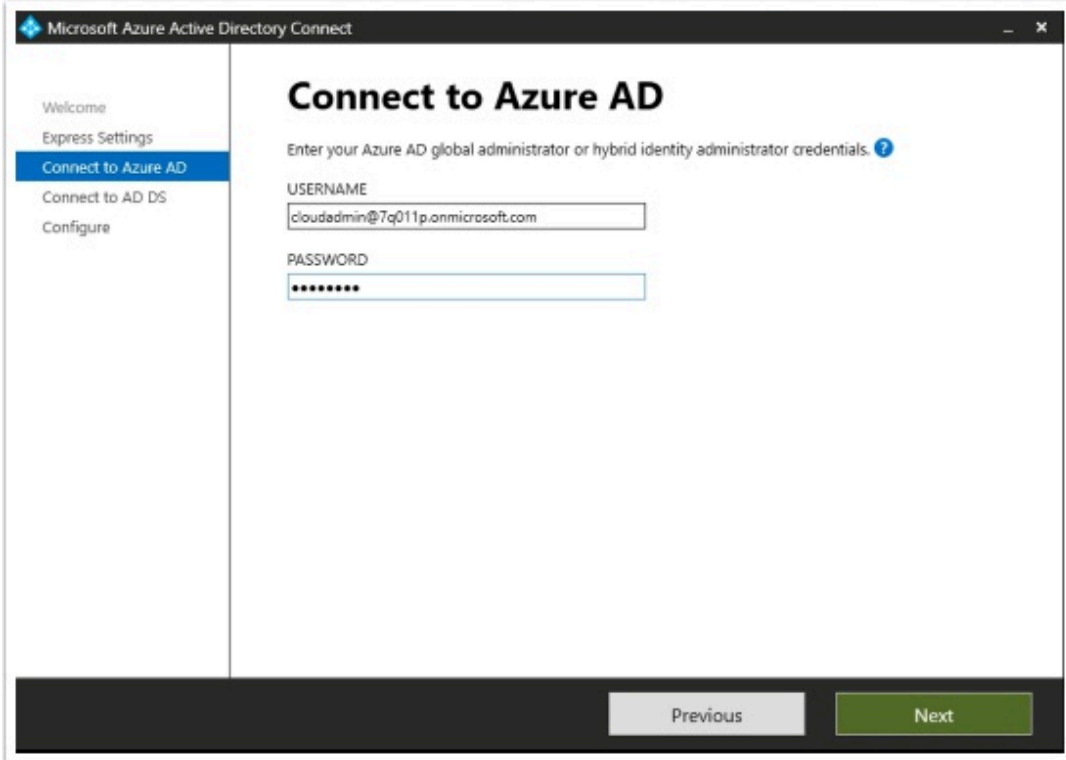


2. On the **Welcome to Azure AD Connect** window
 - Next to **I agree to the license terms and privacy notice**
 - Enable the **check box**
 - Select **Continue**



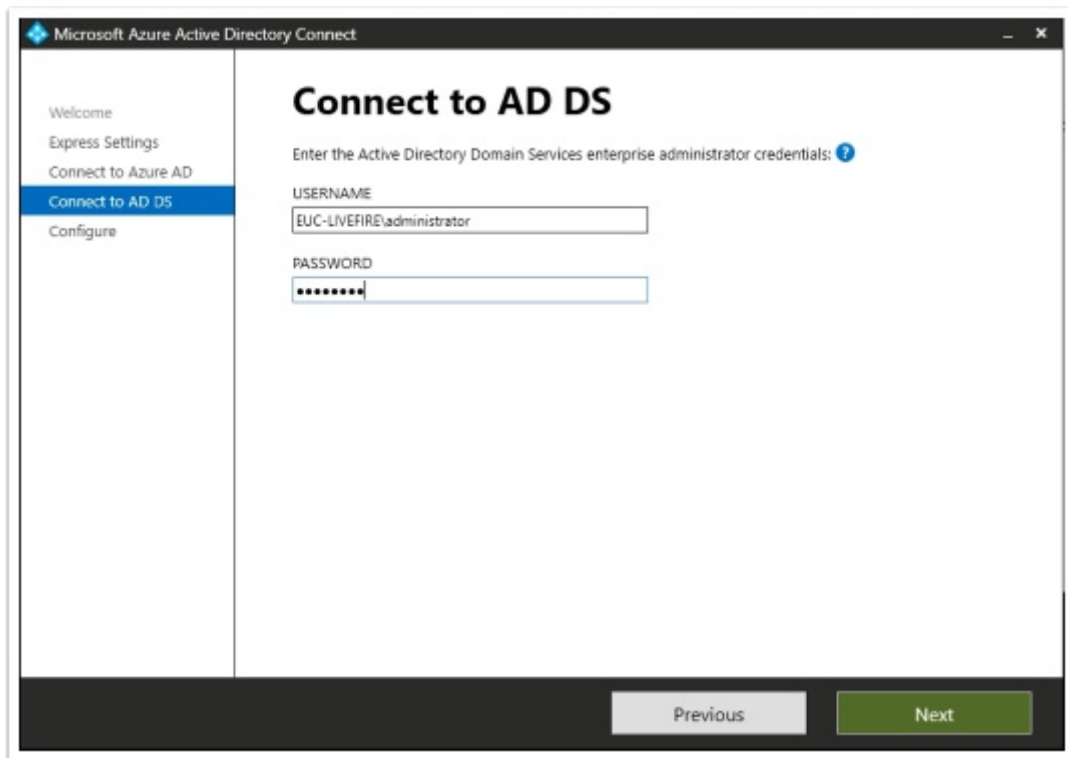
3. In the **Express Settings** window

- Select **Use express settings**

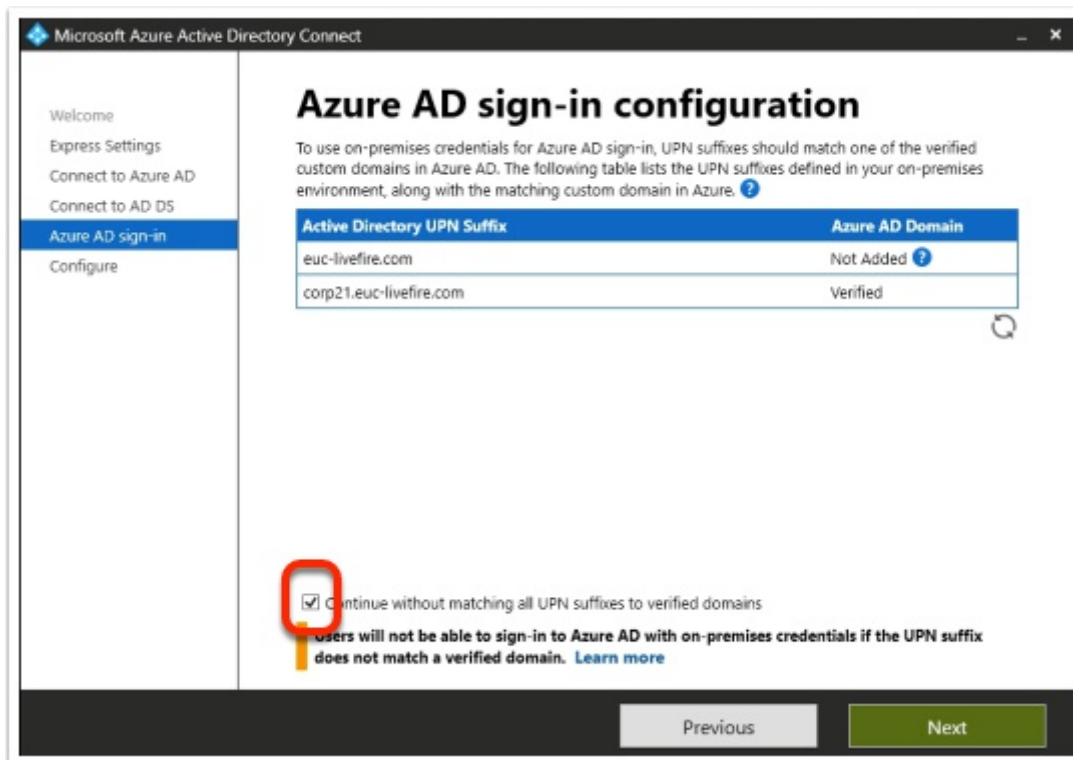


The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. On the left is a navigation pane with the following options: 'Welcome', 'Express Settings', 'Connect to Azure AD' (which is highlighted with a blue bar), 'Connect to AD DS', and 'Configure'. The main area of the window is titled 'Connect to Azure AD' and contains the instruction 'Enter your Azure AD global administrator or hybrid identity administrator credentials.' followed by a question mark icon. Below this are two input fields: 'USERNAME' with the text 'cloudadmin@7q011p.onmicrosoft.com' and 'PASSWORD' with masked characters '*****'. At the bottom right of the window are two buttons: 'Previous' (disabled) and 'Next' (active).

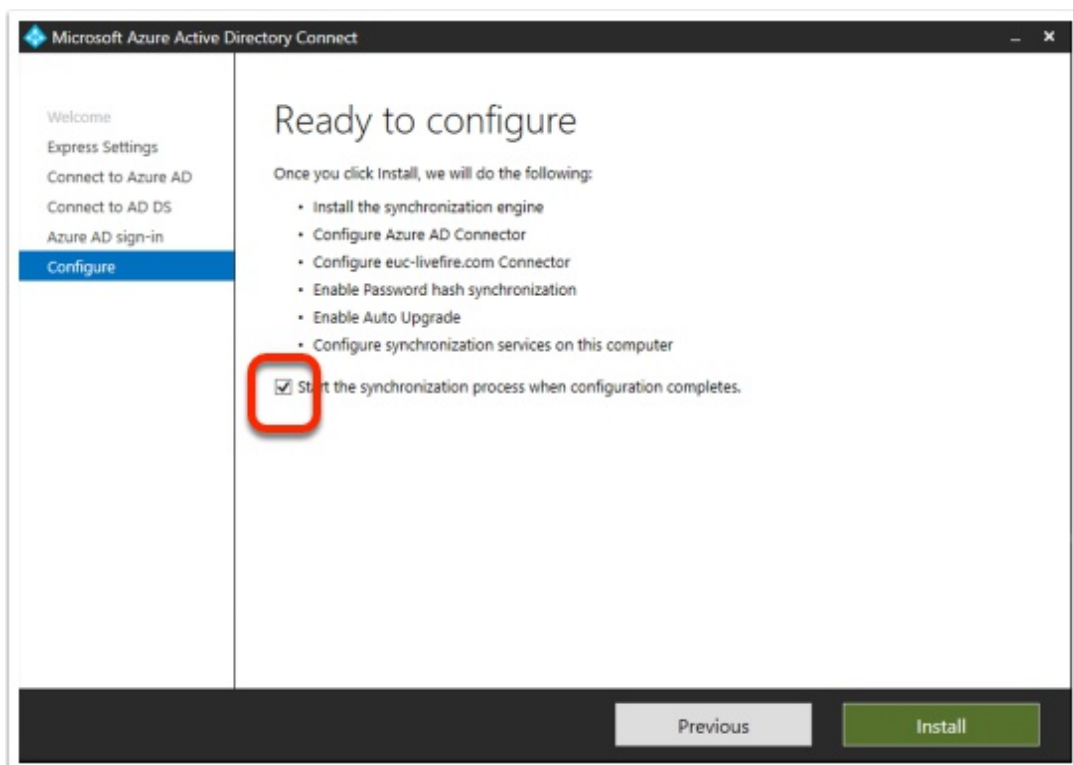
5. On the **Connect to Azure AD** window,
 - Under **USERNAME**
 - Enter your documented Azure Cloud Admin **account**
 - Under **PASSWORD**
 - Enter your documented Azure Cloud Admin **password**
 - Select **Next**



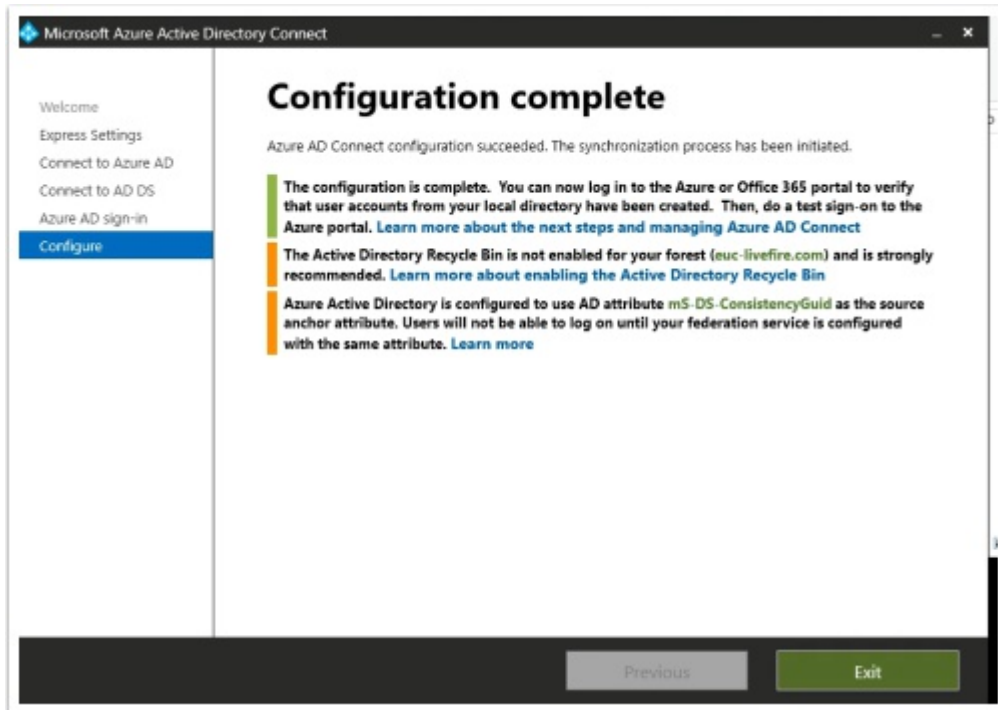
6. On the **Connect to AD DS** window,
 - Under **USERNAME**
 - Enter **EUC-Livefire\administrator**
 - Under **PASSWORD**
 - Enter **VMware1!**
 - Select **Next**



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.

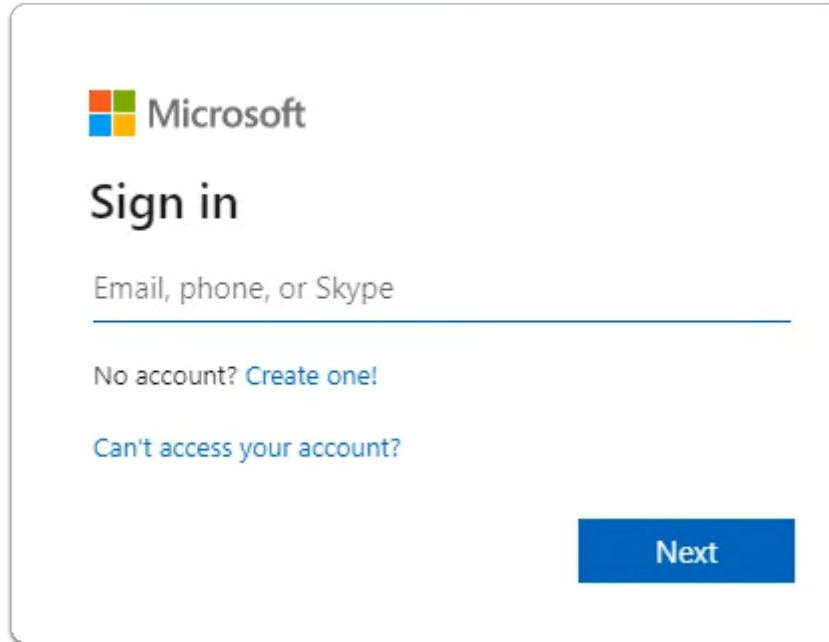


9. On the **Configuration complete** window
 - Select **Exit**



Give the replication about 5 minutes to work

Part 4: Configuring Microsoft 365 licensing

A screenshot of the Microsoft sign-in interface. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed in a large, bold font. Underneath "Sign in" is a text input field with the placeholder text "Email, phone, or Skype". Below the input field are two links: "No account? Create one!" and "Can't access your account?". At the bottom right of the sign-in area is a blue button with the text "Next".

Microsoft

Sign in

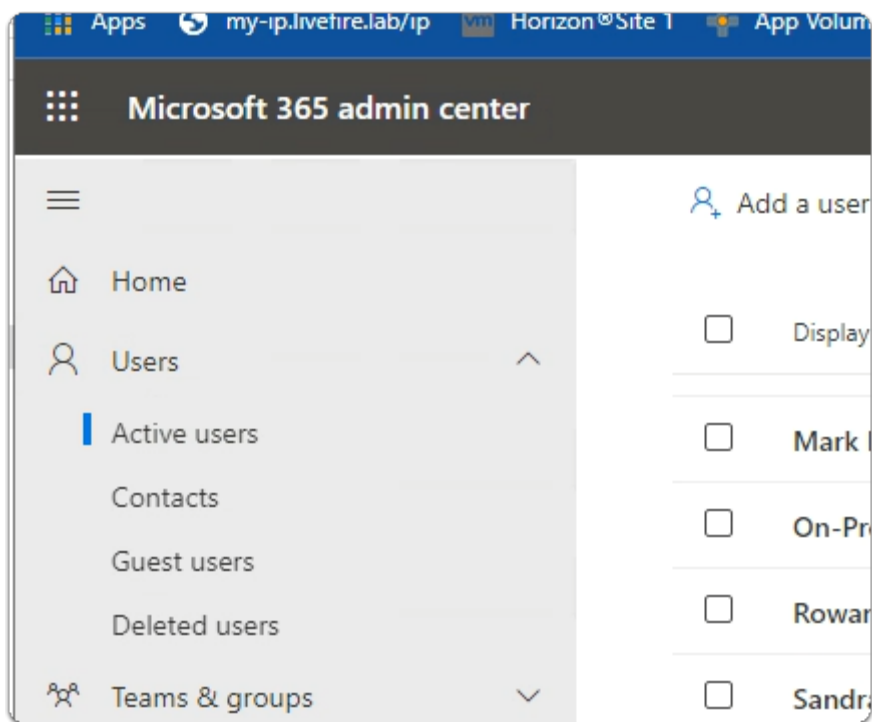
Email, phone, or Skype

No account? [Create one!](#)

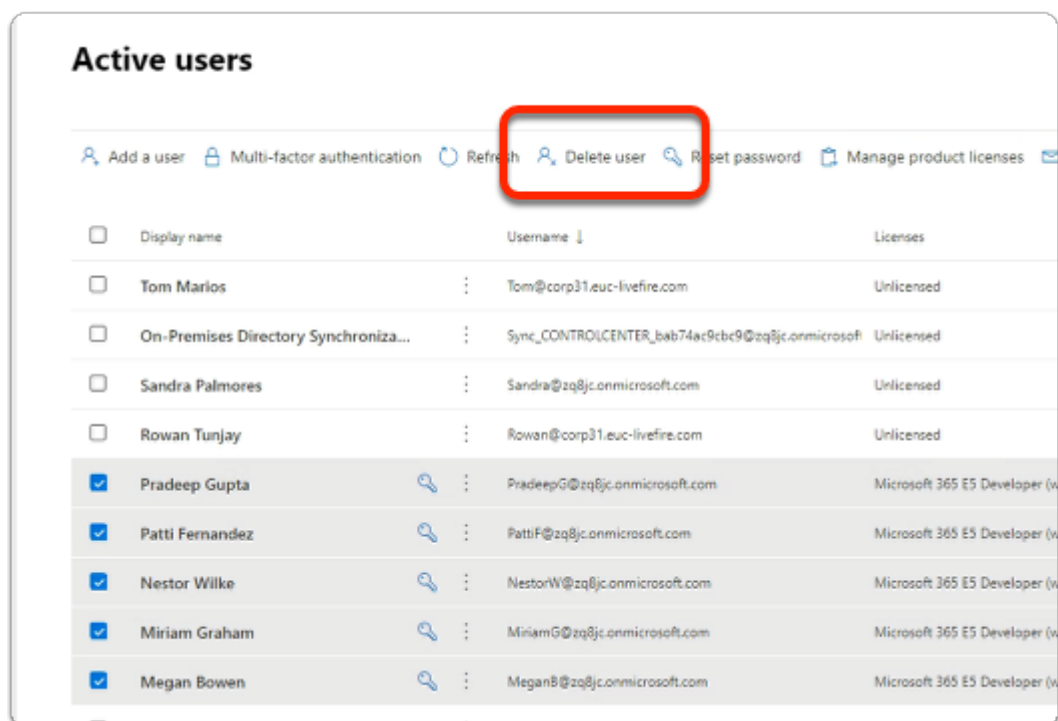
[Can't access your account?](#)

Next

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**.



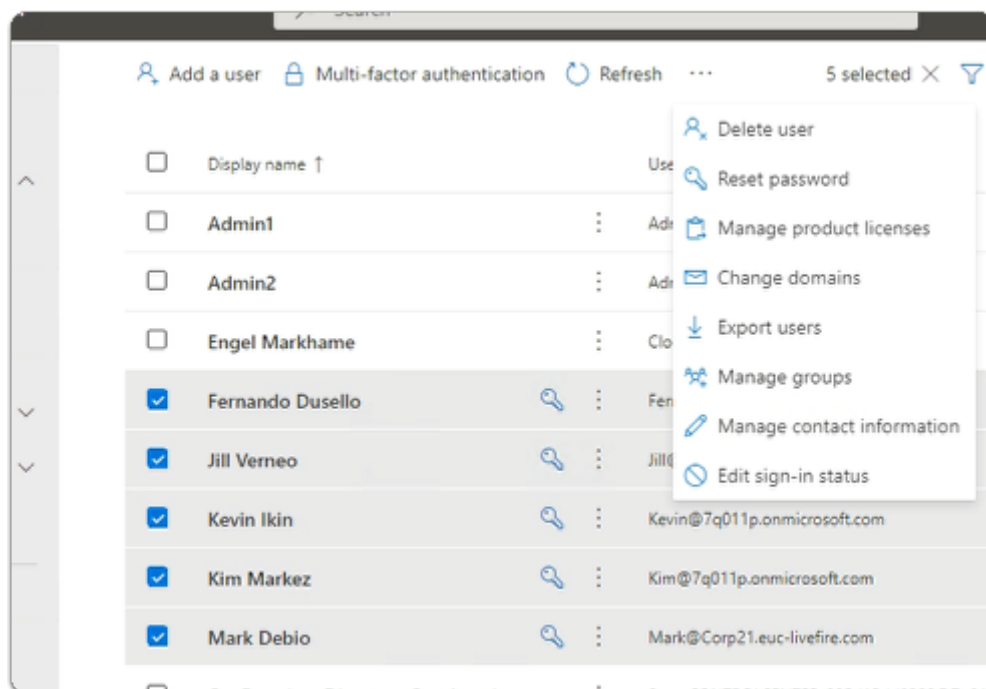
4. In the **Active Users** area
 - Notice that you have **Licensed** and **Unlicensed** users

- 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

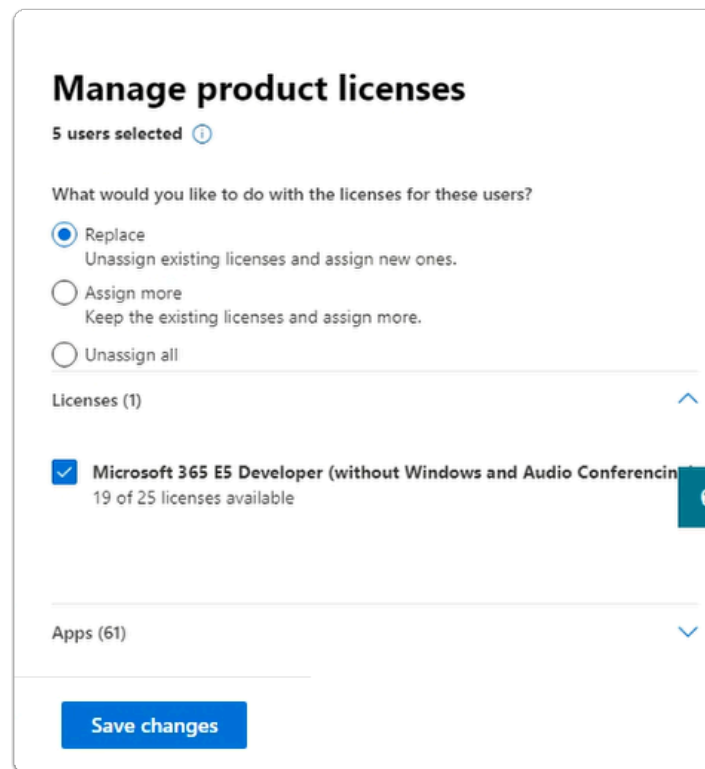


5. In the **Active Users** area

- 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**



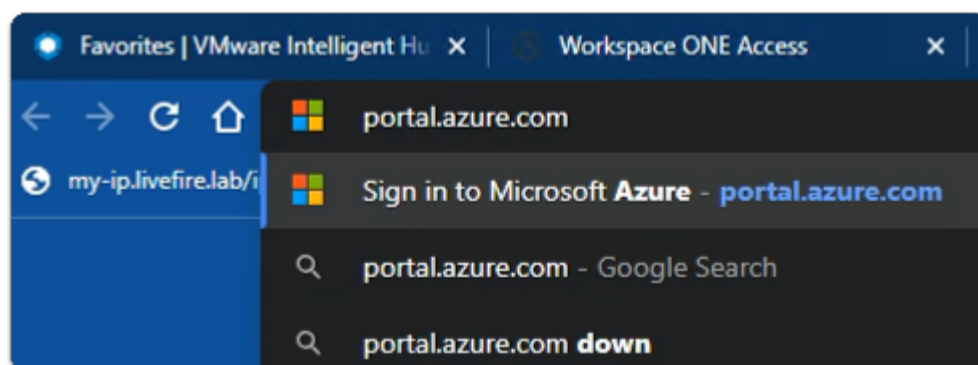
everyone needs to license their newly synced accounts in Microsoft 365



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**.

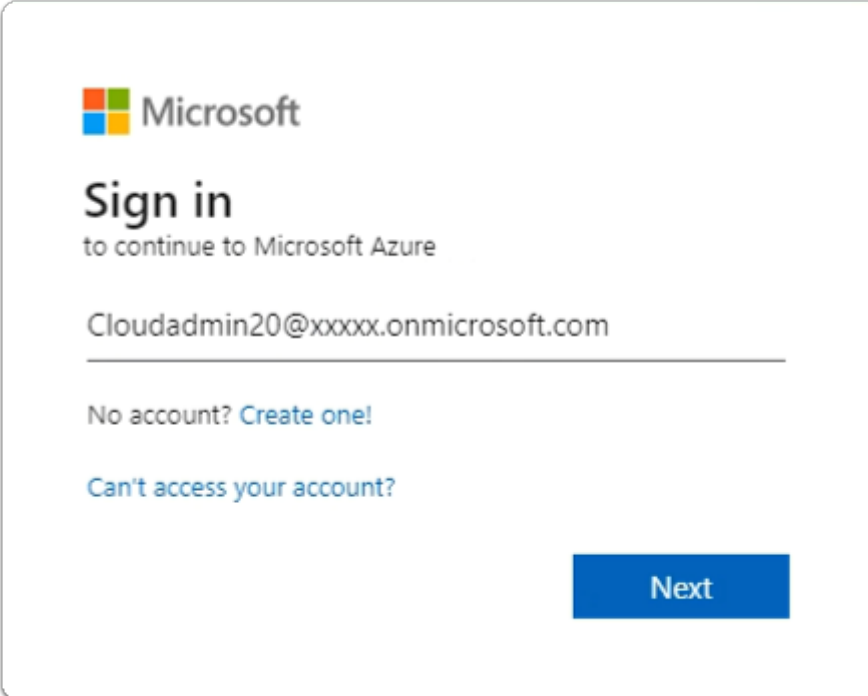
Part 5: Configuring Microsoft Azure for Workspace ONE Access authentication



1. On your ControlCenter server

- Open your **Site 1 Chrome** Browser
- Open a **new Tab**

- In the **Chrome address bar**
 - enter <https://portal.azure.com>

A screenshot of the Microsoft Sign in page. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed in a large font, followed by "to continue to Microsoft Azure" in a smaller font. A text input field contains the email address "Cloudadmin20@xxxxx.onmicrosoft.com". Below the input field are two links: "No account? Create one!" and "Can't access your account?". A blue "Next" button is located at the bottom right of the form.

Microsoft

Sign in
to continue to Microsoft Azure

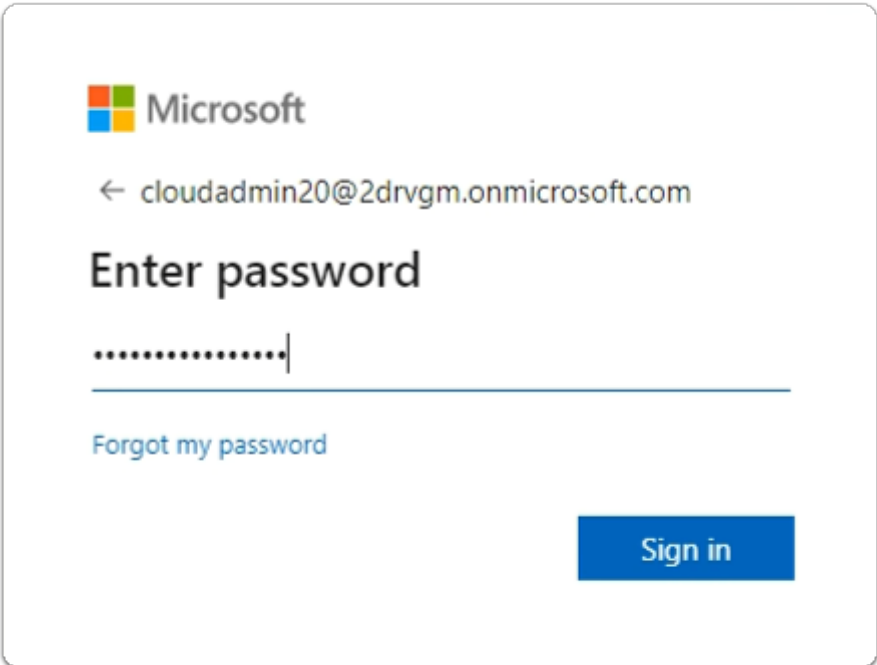
Cloudadmin20@xxxxx.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

Next

2. In the **Microsoft Azure Sign in** page
 - enter **YOUR CloudAdmin account**
 - select **Next**

A screenshot of the Microsoft Enter password page. At the top left is the Microsoft logo. Below it, a back arrow icon is followed by the email address "cloudadmin20@2drvgm.onmicrosoft.com". The text "Enter password" is displayed in a large font. Below it is a password input field with masked characters ".....". A link "Forgot my password" is located below the input field. A blue "Sign in" button is located at the bottom right of the form.

Microsoft

← cloudadmin20@2drvgm.onmicrosoft.com

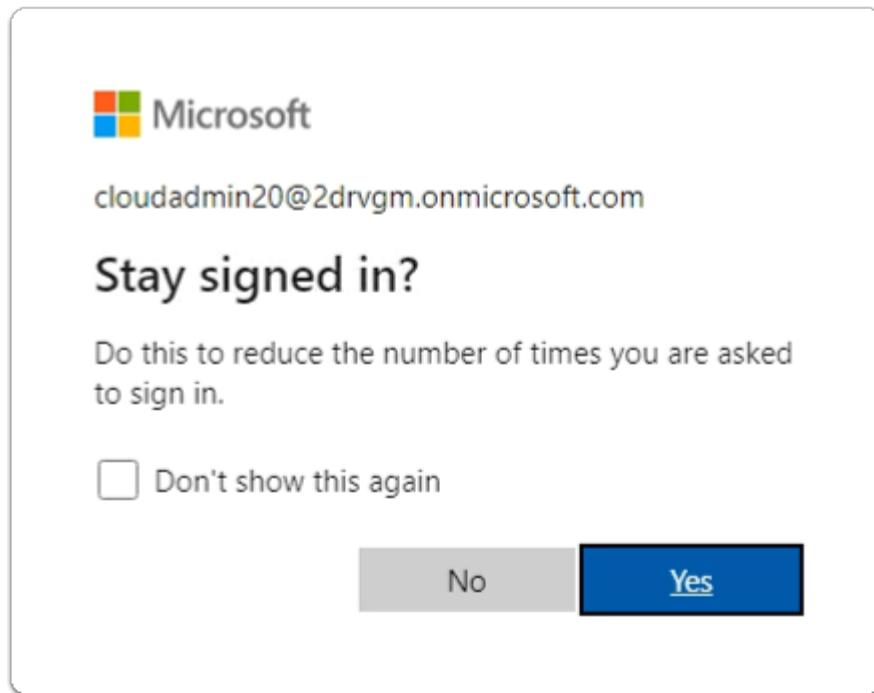
Enter password

.....

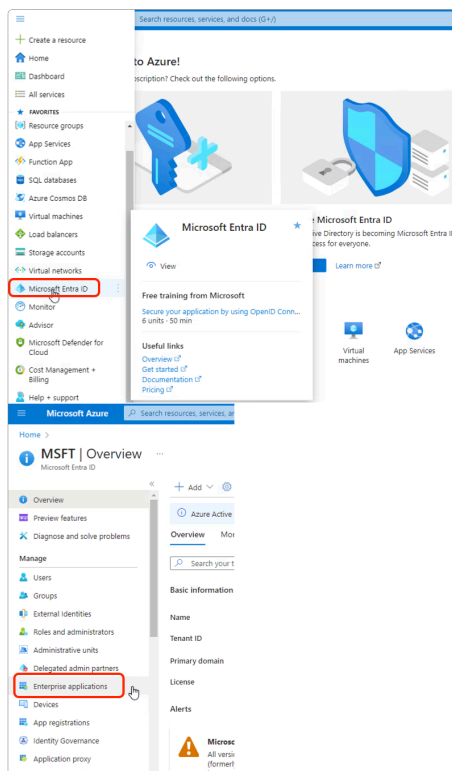
[Forgot my password](#)

Sign in

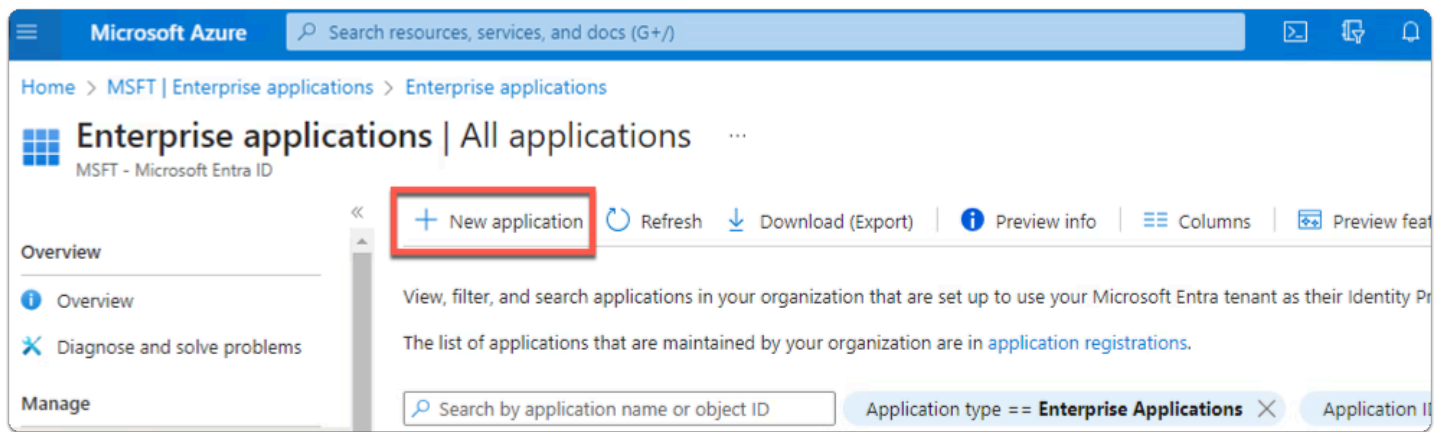
3. In the **Microsoft Azure Enter password** page
 - enter **your Password**
 - select **Sign in**



4. In the **Microsoft Azure Stay signed in?** page
- select **Yes or No**

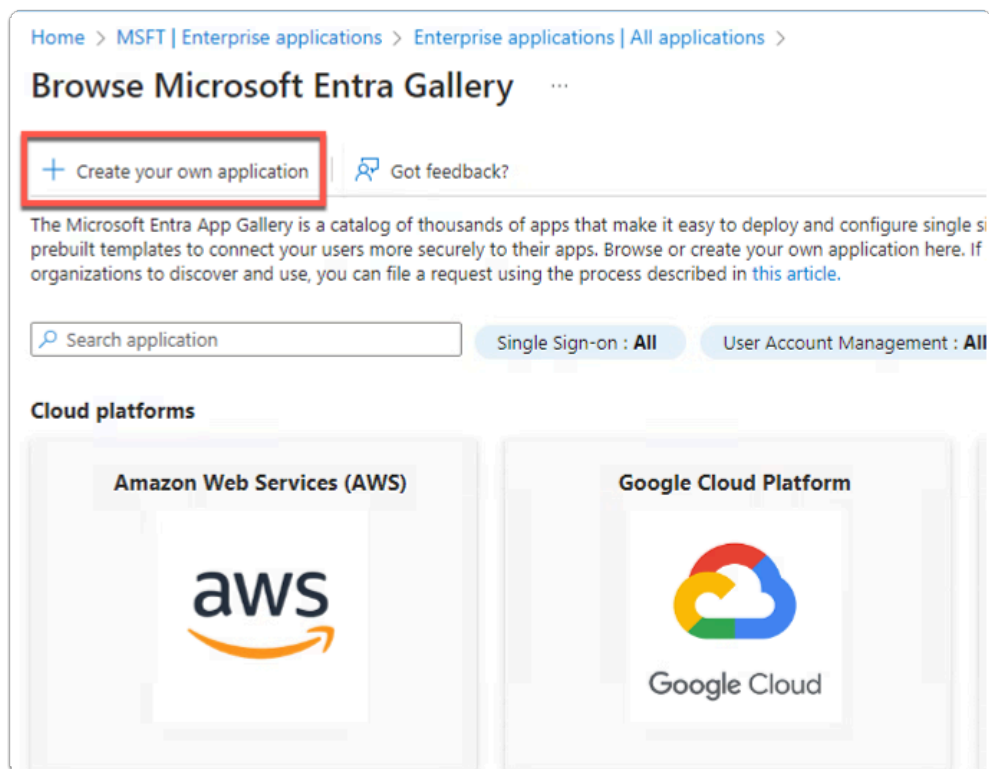


5. In the **Microsoft Azure Admin Portal**
- In the left Inventory
 - select **Microsoft Entra ID**
 - select **Enterprise Applications**



6. In the **Enterprise applications** area

- select + **New application**



7. In the **Browse Azure AD Gallery** area

- select + **Create your own application**

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

☐ Configure Application Proxy for secure remote access to an on-premises application
☐ Register an application to integrate with Azure AD (App you're developing)
☒ Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry
We recommend using gallery applications when possible.

MyWorkspace

Create

8. In the **Create your own application** area
 - below **What's the name of your app?**
 - enter **Workspace ONE Access**
 - select **Create**

[Home](#) > [2drvgn | Enterprise applications](#) > [Enterprise applications | All applications](#) > [Browse Azure AD Gallery](#)

Workspace ONE Access | Overview

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Workspace ONE Access

Application ID

ef933494-d532-4f96-b6ed-...

Object ID

82977526-6930-4149-9291-...

Getting Started

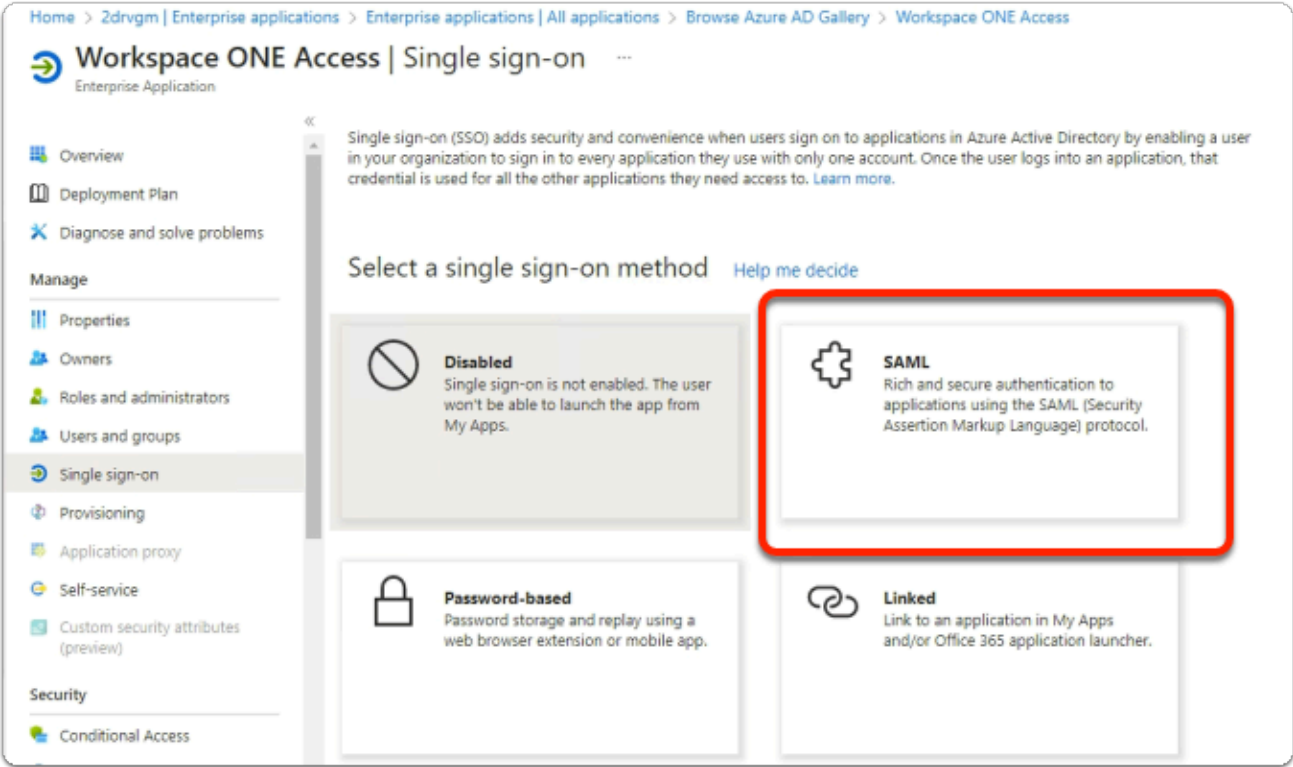
1. Assign users and groups
 Provide specific users and groups access to the applications
[Assign users and groups](#)

2. Set up single sign on
 Enable users to sign into their application using their Azure AD credentials
[Get started](#)

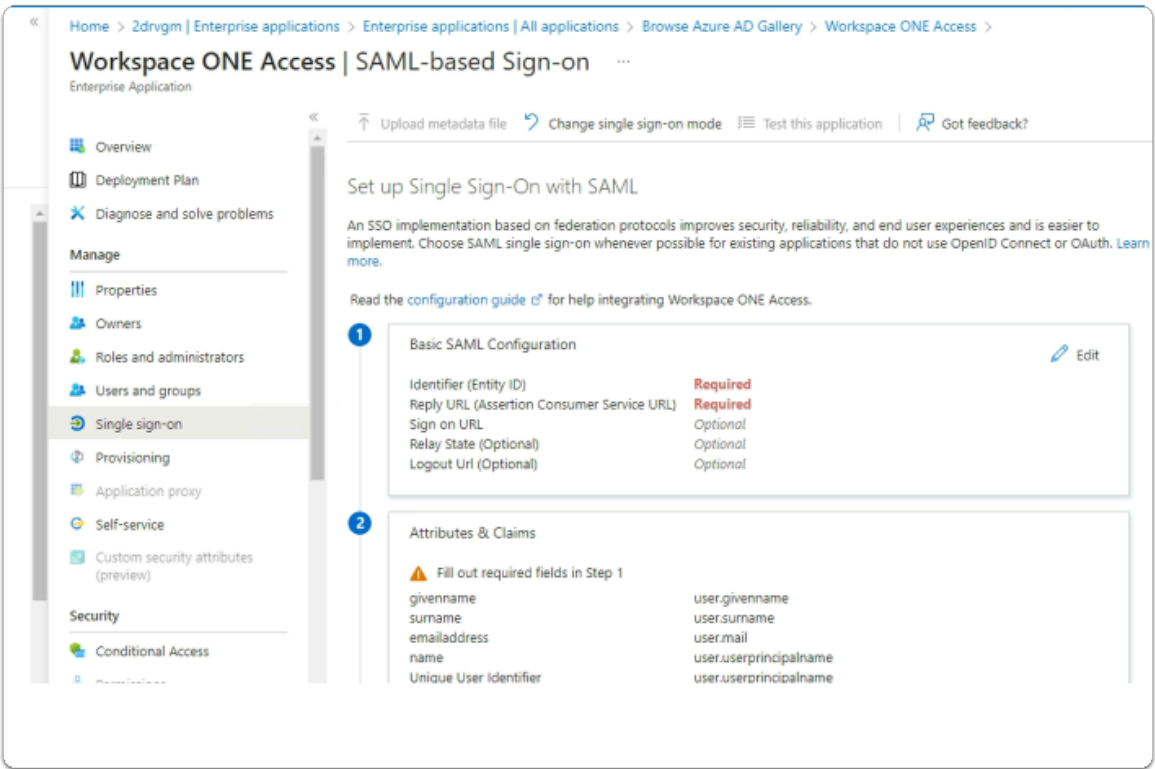
3. Provision User Accounts
 Automatically create and delete user accounts in the application
[Get started](#)

4. Conditional Access
 Secure access to this application with a customizable access policy.
[Create a policy](#)

9. In the **Workspace ONE Access | Overview** page
- select **2. Setup single sign on**

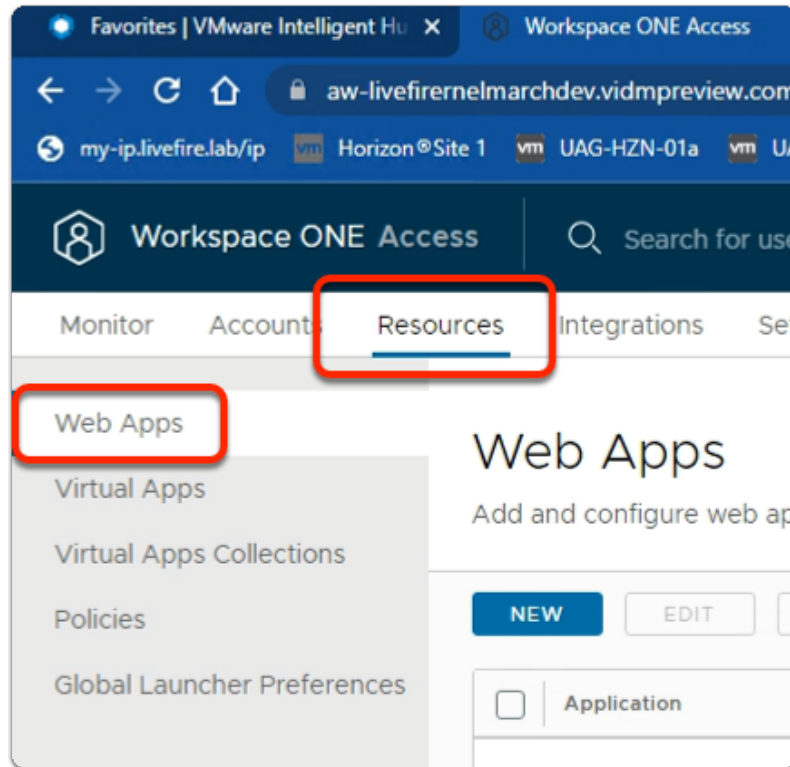


10. In the **Workspace ONE Access | Single sign-on** page
- select **SAML**

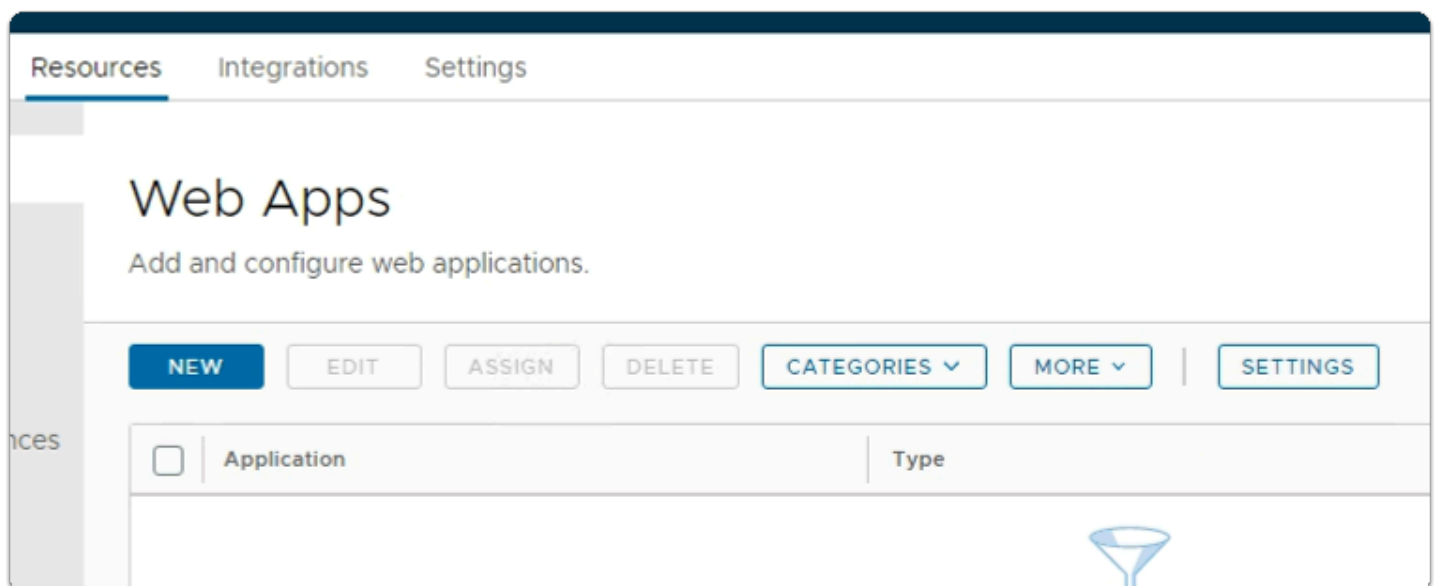


11. In the **Workspace ONE Access | SAML-based Sign-on** page

- In the **Basic SAML Configuration** area
 - note that **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** are required
 - We will now switch to Workspace ONE Access for this information
 - On your ControlCenter server
 - switch to your **Workspace ONE Access sysadmin console**

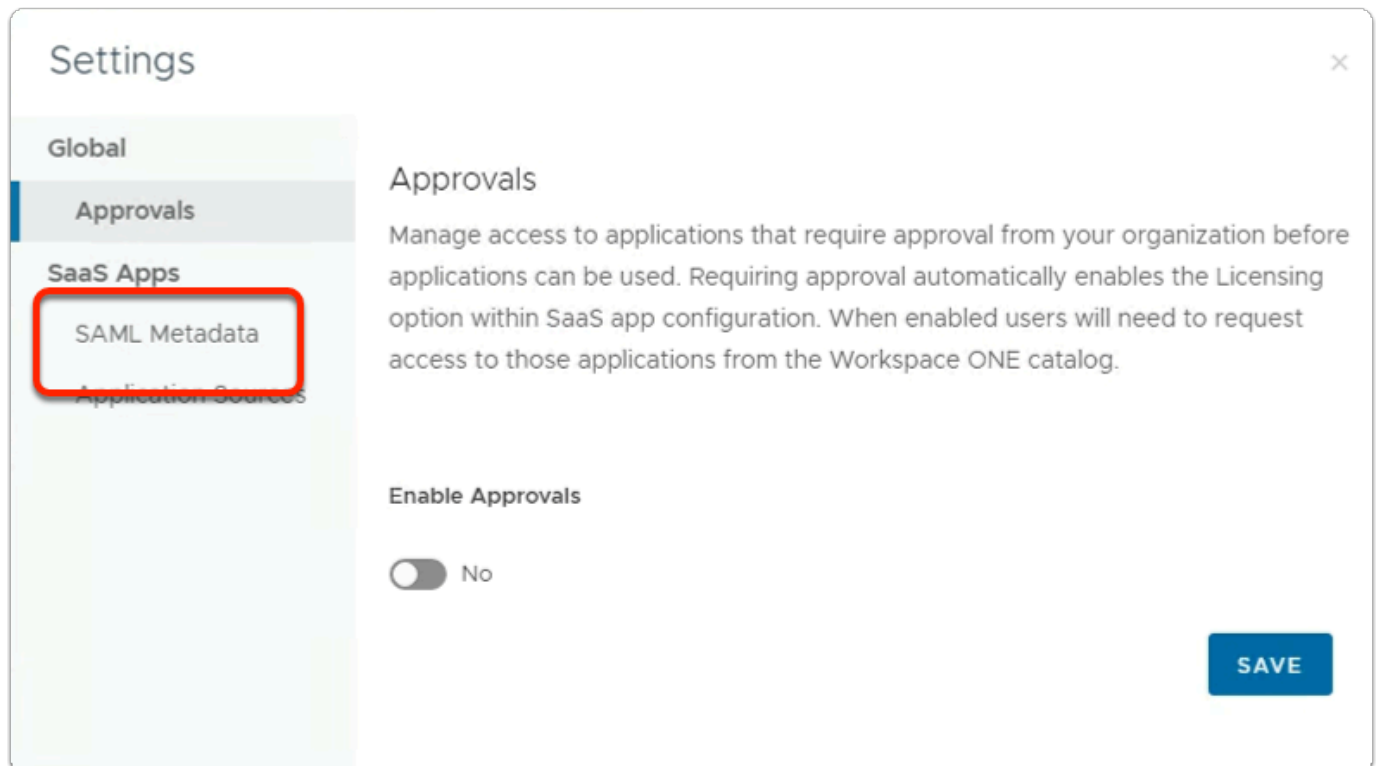


12. In the **Workspace ONE Access** admin Console
 - select the **Resources** tab
 - In the **Resources** inventory
 - select **Web Apps**



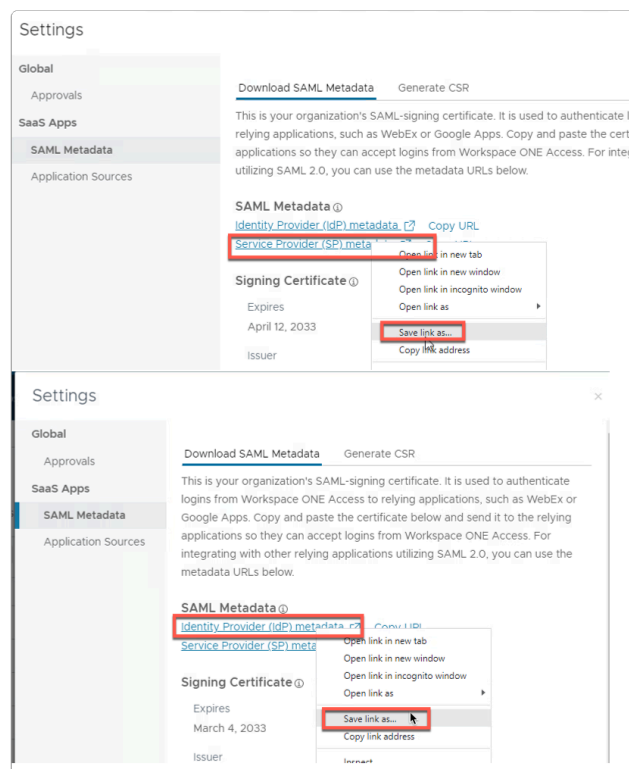
13. In the **Web Apps** area

- select **SETTINGS**



14. In the **Settings** window

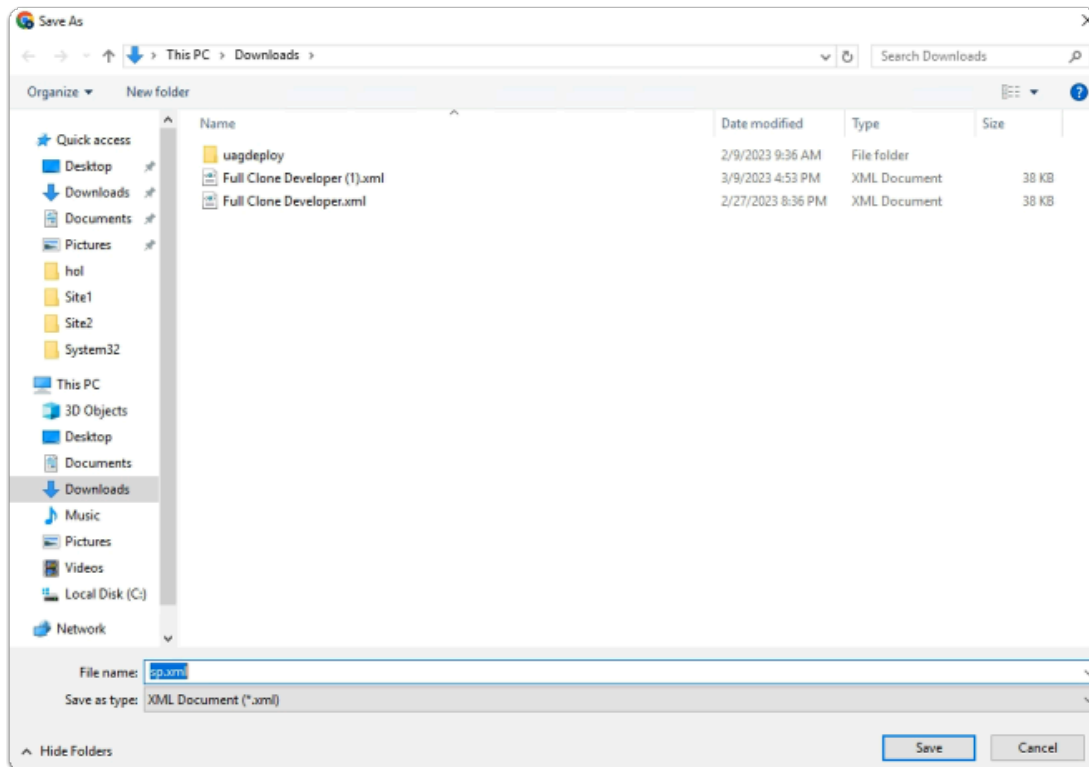
- select **SAML Metadata**



15. In the **Settings** window

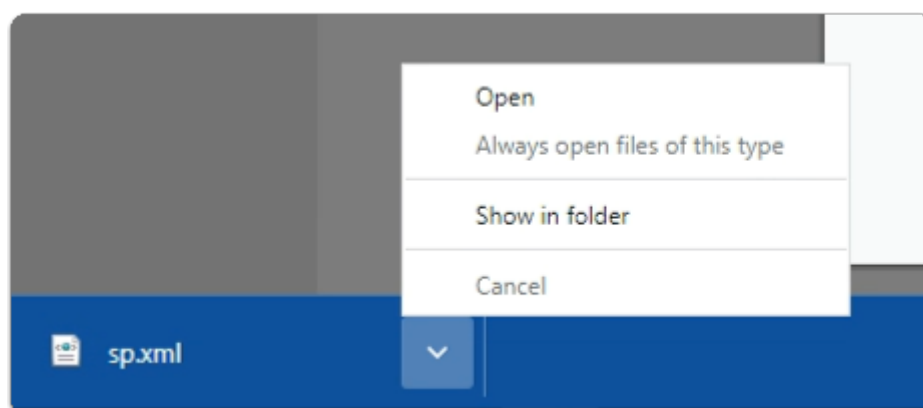
- under **SAML Metadata**
 - **select** and **right-click** **Service Provider (SP) metadata**
 - select **Save link as.....**
 - **select** and **right-click** **Identity Provider (IdP) metadata**
 - select **Save link as.....**

NOTE: In this exercises we will only use the Service Provider metadata. In a later exercise we will use the Identity Provider metadata.



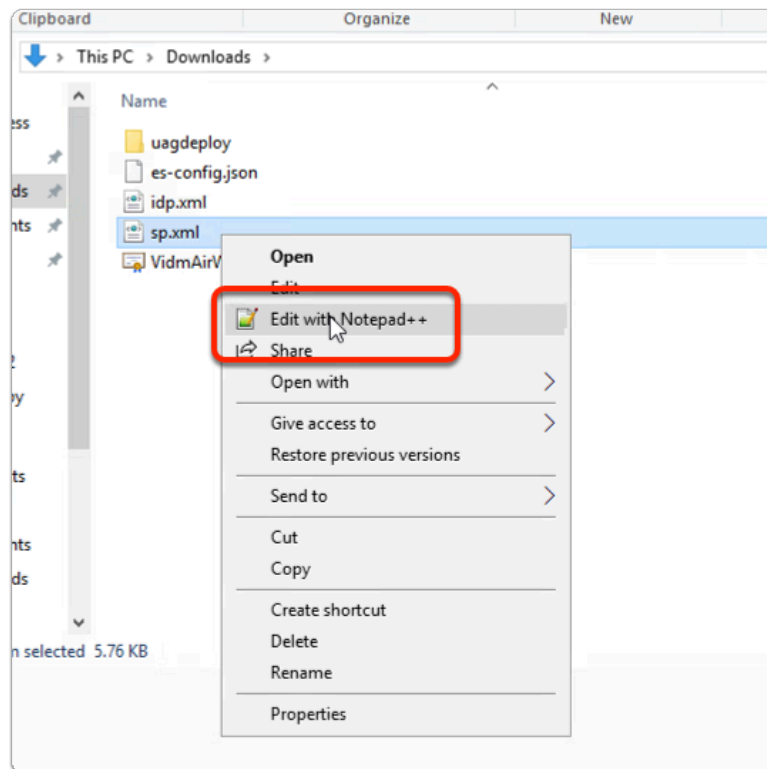
16. In the **Save As** window

- select **Save**

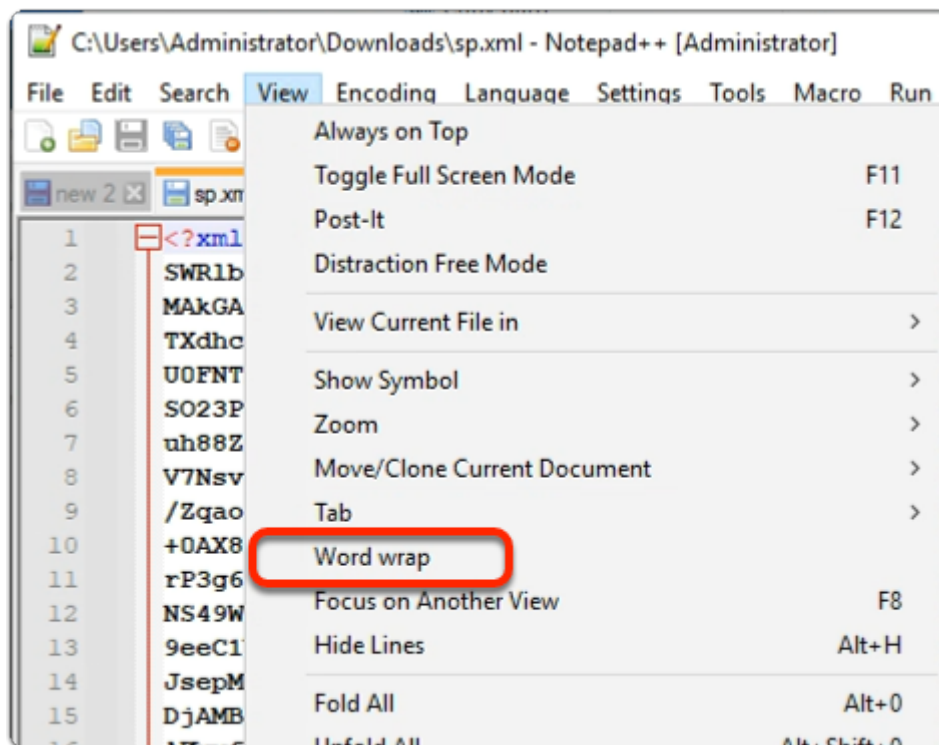


17. In the bottom left-corner of your browser

- next to **sp.xml**
 - select the **dropdown**
 - select **Show in folder**

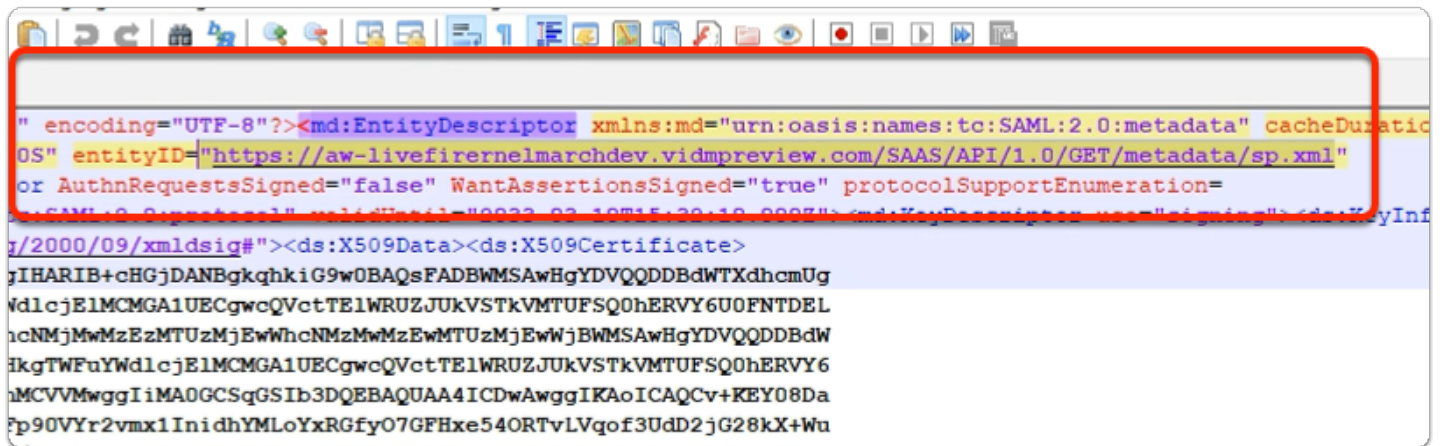


18. In the **Downloads** folder
 - select and right-click **sp.xml**
 - select **Edit with Notepad++**



19. In the **Notepad ++** application
 - select **View**

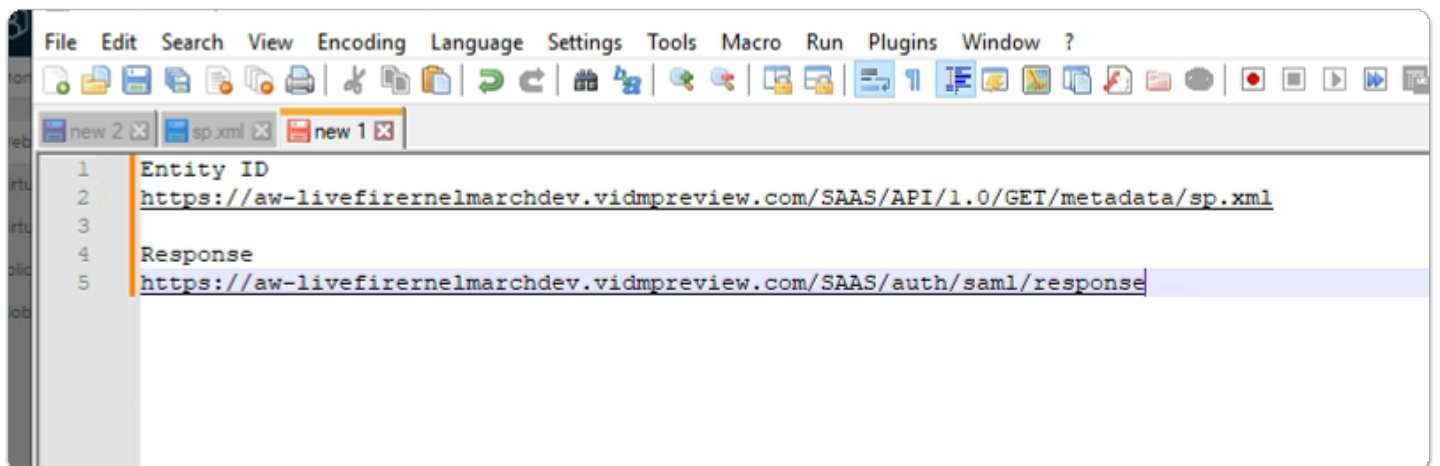
- select **Word wrap**



20. In the **Notepad ++** application
 - In the **XML code**
 - find **entityID**
 - **Copy the URL** which ends in **sp.xml**
 - Save the URL in a **new tab** in **Notepad++**

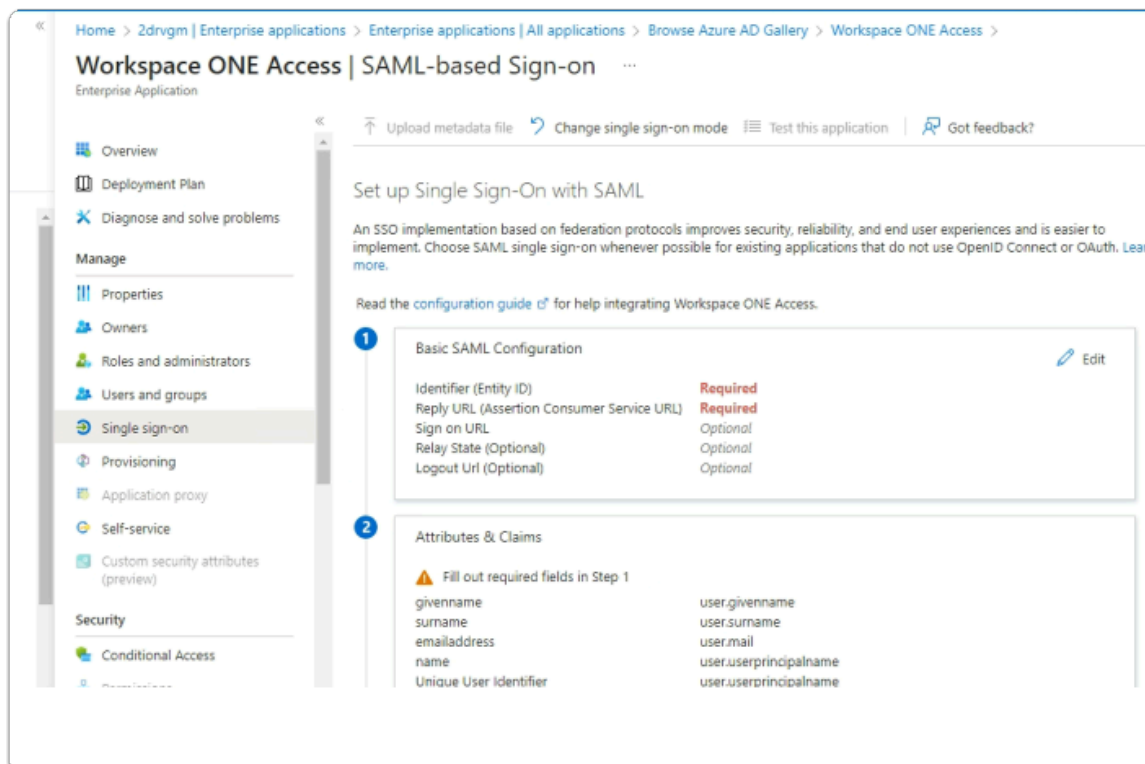
```
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat><md:NameIDFormat>  
urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat><md:NameIDFormat>  
urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName</md:NameIDFormat><md:AssertionConsumerService Binding=  
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aw-livefirerhnelmarchdev.vldmpreview.com/SAAS/auth/saml/response"  
index="0" isDefault="true"/><md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location=  
"https://aw-livefirerhnelmarchdev.vldmpreview.com/SAAS/auth/saml/artifact" index="1" isDefault="false"/>
```

21. In the **Notepad ++** application
 - In the **XML code**
 - **Find the code**
 - **AssertionConsumerService**
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location
 - **Copy the URL** that ends in **response** after this
 - **Save the URL** in your new tab in **Notepad++**



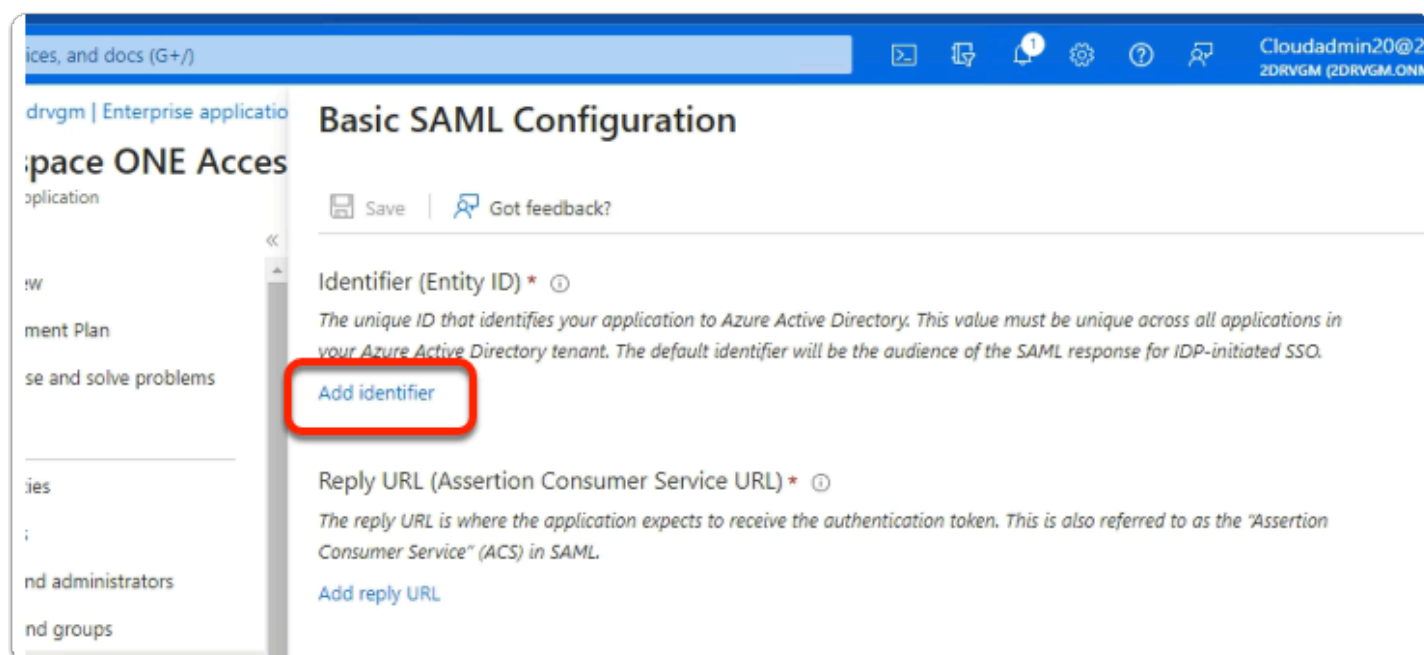
22. In the Notepad++ application

- Note which is your **entity ID**
- Note which is your **Response**
- Switch back to your **Azure Admin Portal**



23. In the **Workspace ONE Access | SAML-based Sign-on** page

- In the **Basic SAML Configuration** area
 - select **Edit**



24. In the **Basic SAML Configuration** window

- under **Identifier (Entity ID) ***
 - select **Add Identifier**

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

✓ ⓘ

Add identifier

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Add reply URL

25. In the **Basic SAML Configuration**

- under **Identifier (Entity ID) ***
- Paste your **Entity ID**

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

✓ ⓘ

Add identifier

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

26. In the **Basic SAML Configuration**

- under **Reply URL (Assertion Consumer Service URL) ***
- select **Add reply URL**

resources, services, and docs (G+)

Cloudadmin
2DRVGM (2DRV)

Home > Browse Azure AD Gallery > W

Workspace ONE Access
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://aw-livelifirnelmarchdev.vidmpreview.com/SAAS/API/1.0/GET/metadata/sp.xml ✓ [X] ⓘ [X]

Add identifier

Reply URL (Assertion Consumer Service URL) * ⓘ
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

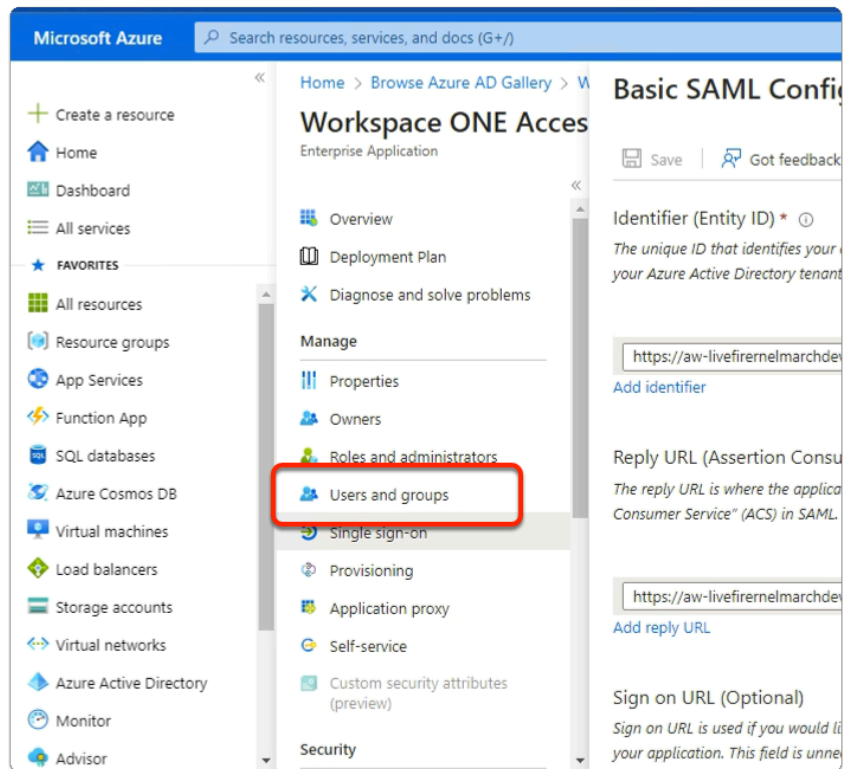
https://aw-livelifirnelmarchdev.vidmpreview.com/SAAS/auth/saml/response ✓ [X] ⓘ [X]

Add reply URL

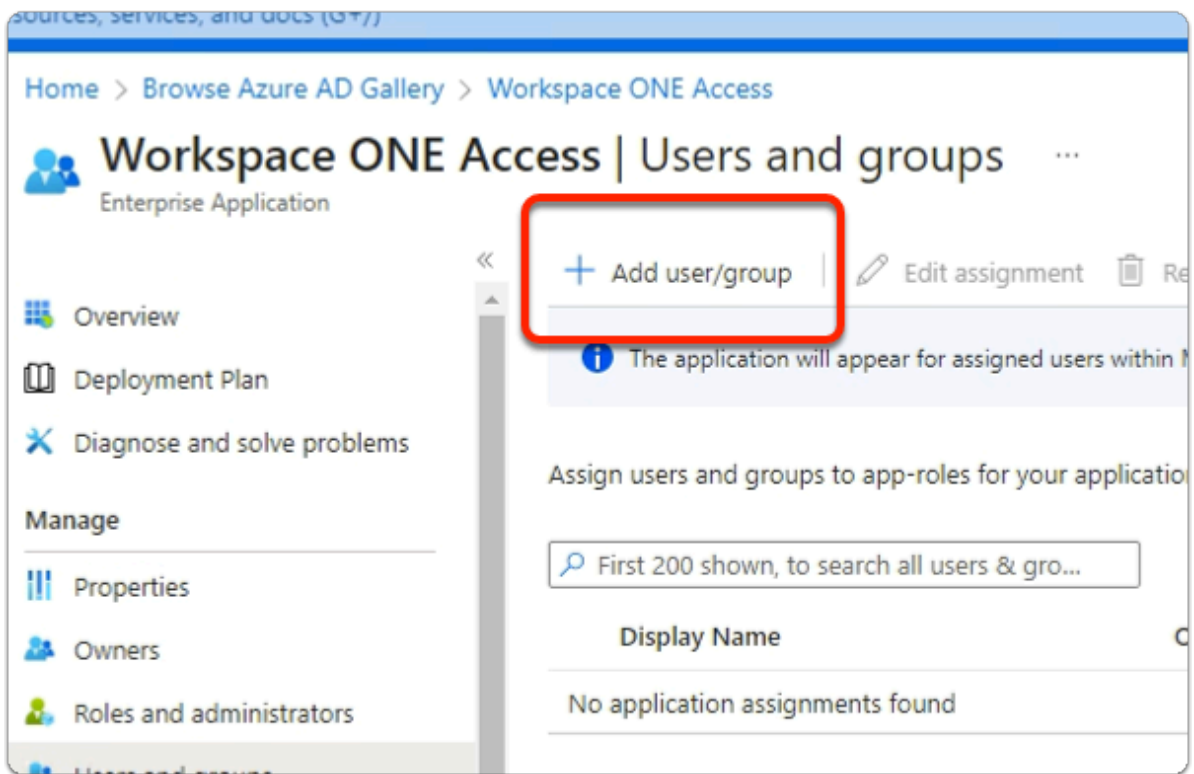
Sign on URL (Optional)

27. In the **Basic SAML Configuration**

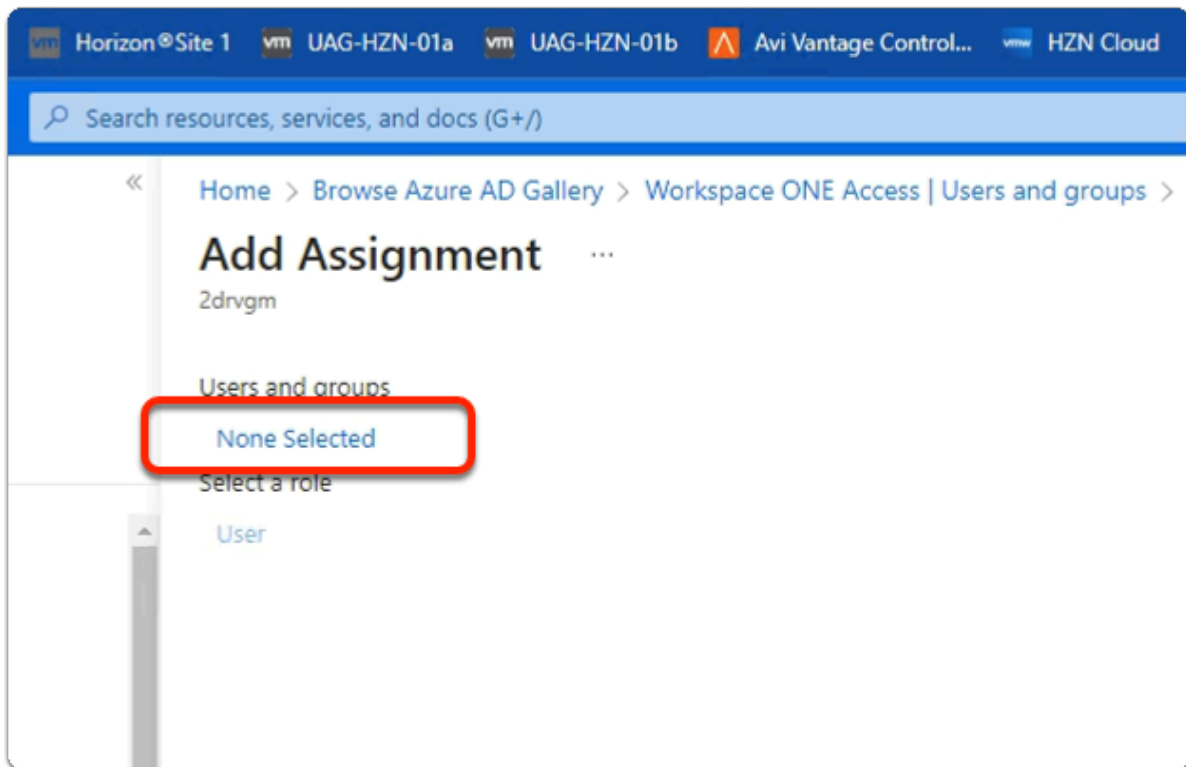
- under **Reply URL (Assertion Consumer Service URL) ***
- **Paste** YOUR **Response URL**
- At the top of the page
 - select **Save**



28. In the **Workspace ONE Access** area
- Just above **Single sign-on**
 - select **Users and groups**

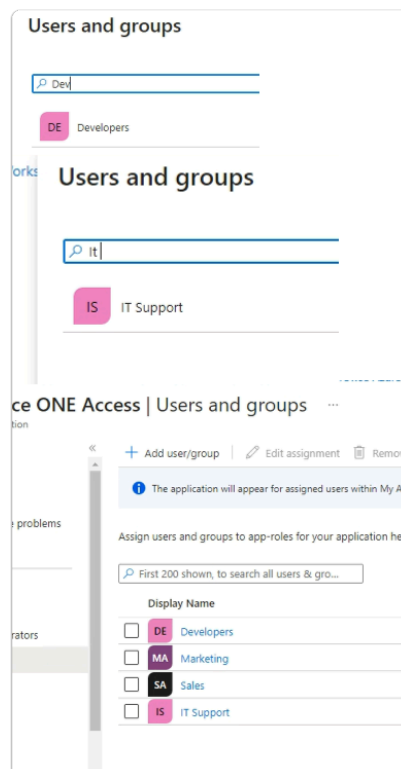


29. In the **Workspace ONE Access | Users and groups** area
- select **+ Add user / group**



30. In the **Add Assignment** area

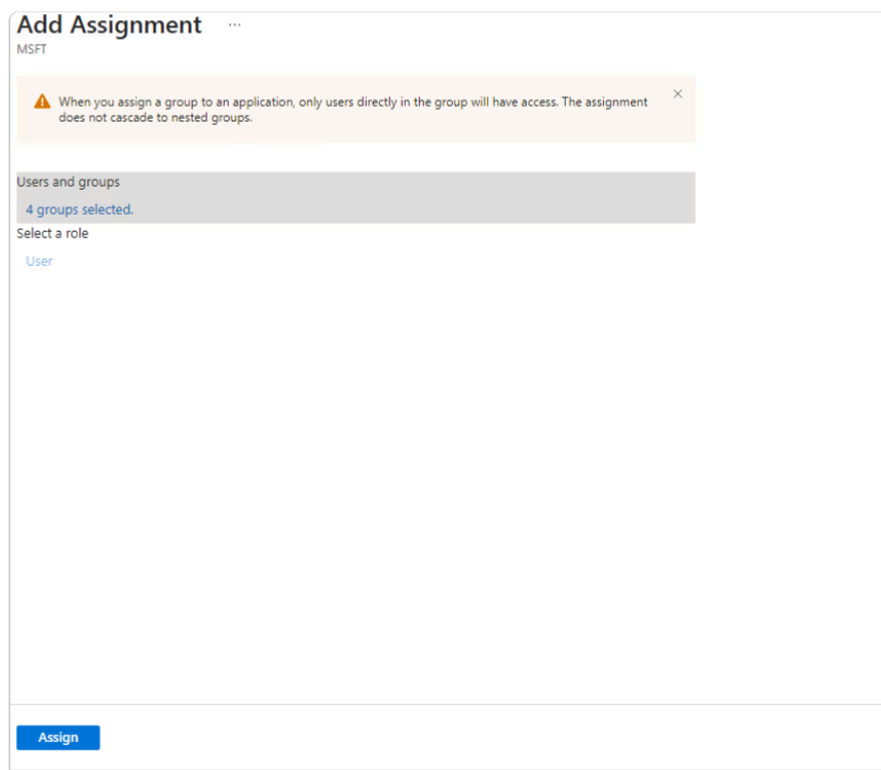
- click on **None Selected**



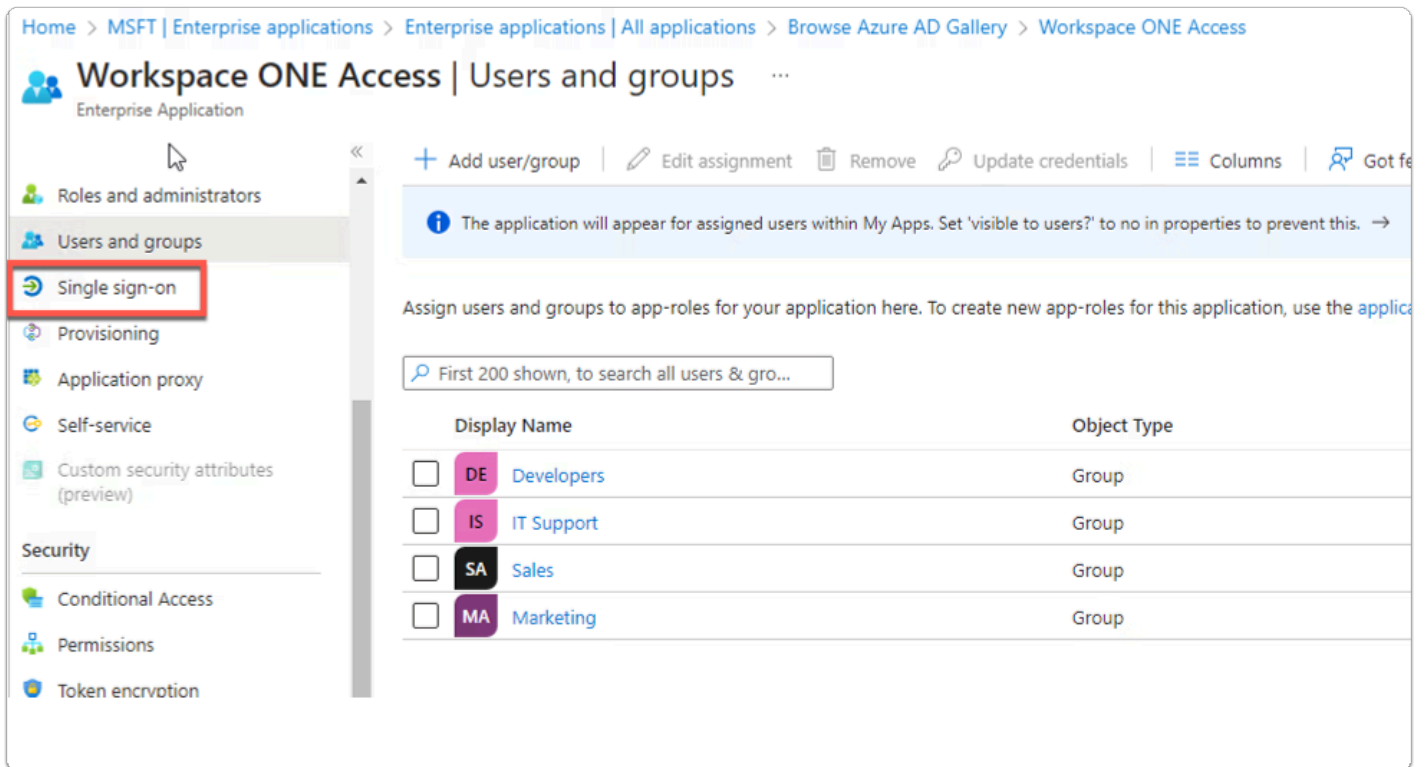
31. In the **Users and groups** area

- In the **search** area
- enter **DEV**

- select **Developers**
- In the **search** area
 - enter **Sales**
 - select **Sales**
- In the **search** area
 - enter **Marketing**
 - select **Marketing**
- In the **search** area
 - enter **IT support**
 - select **IT support**
- In the bottom right-corner
 - click on **Select**

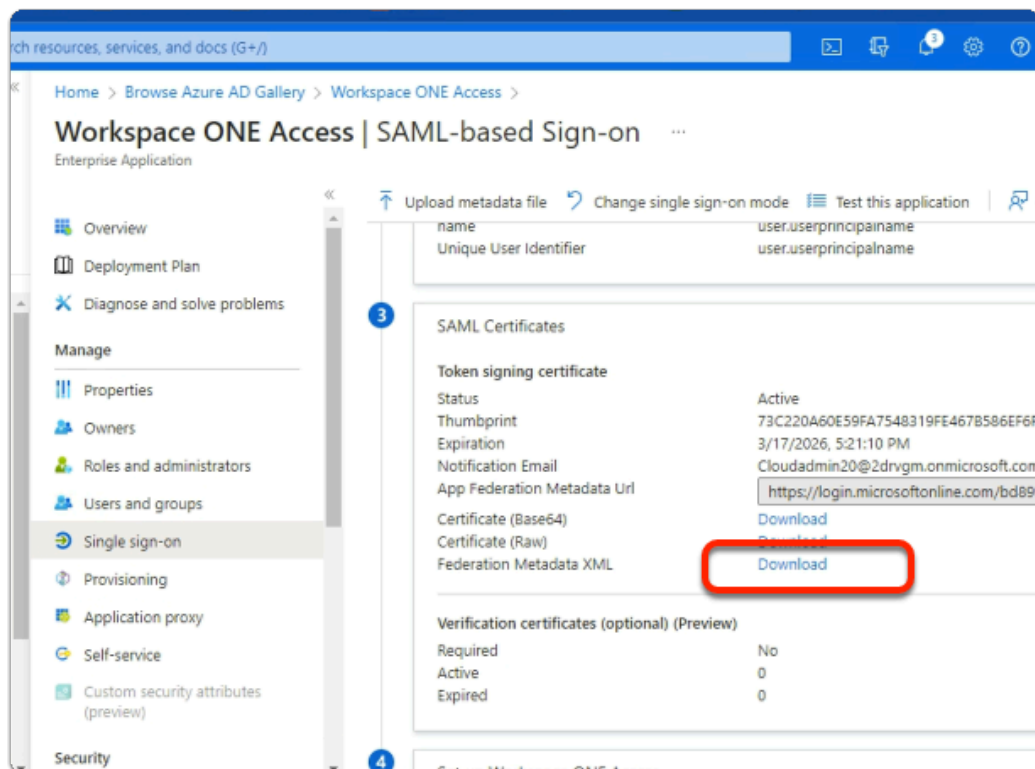


32. In the **Add Assignment** area
- At the bottom of the page
 - select **Assign**



33. In the **Workspace ONE | Users and groups** area

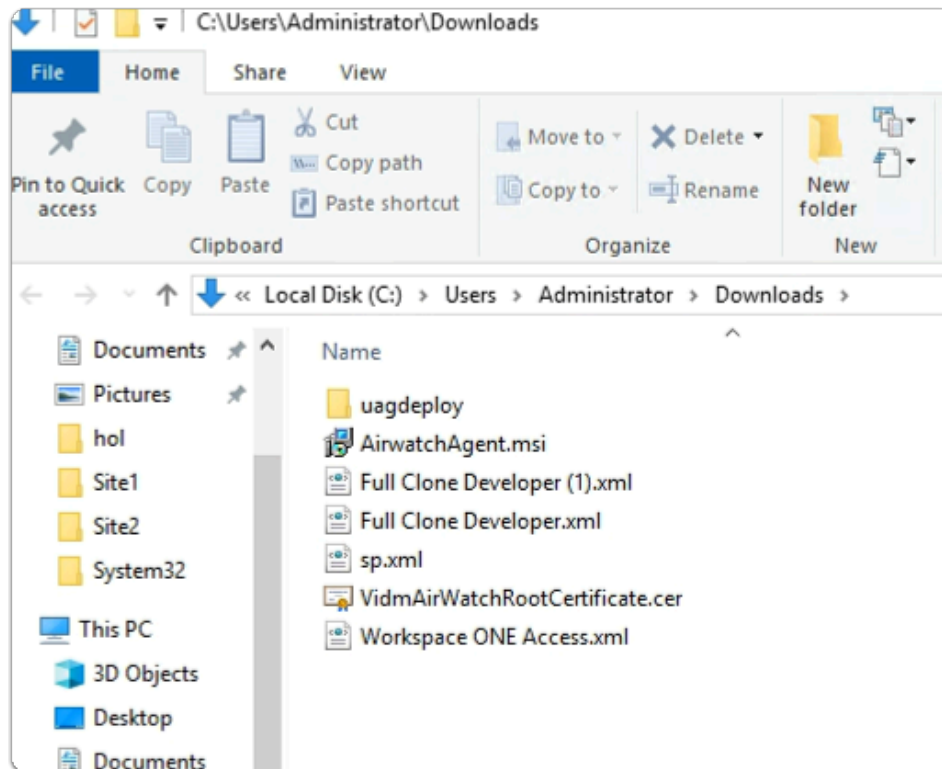
- note the assigned groups
- select **Single sign-on**



34. In the **Workspace ONE Access | SAML-based Sign-on** area

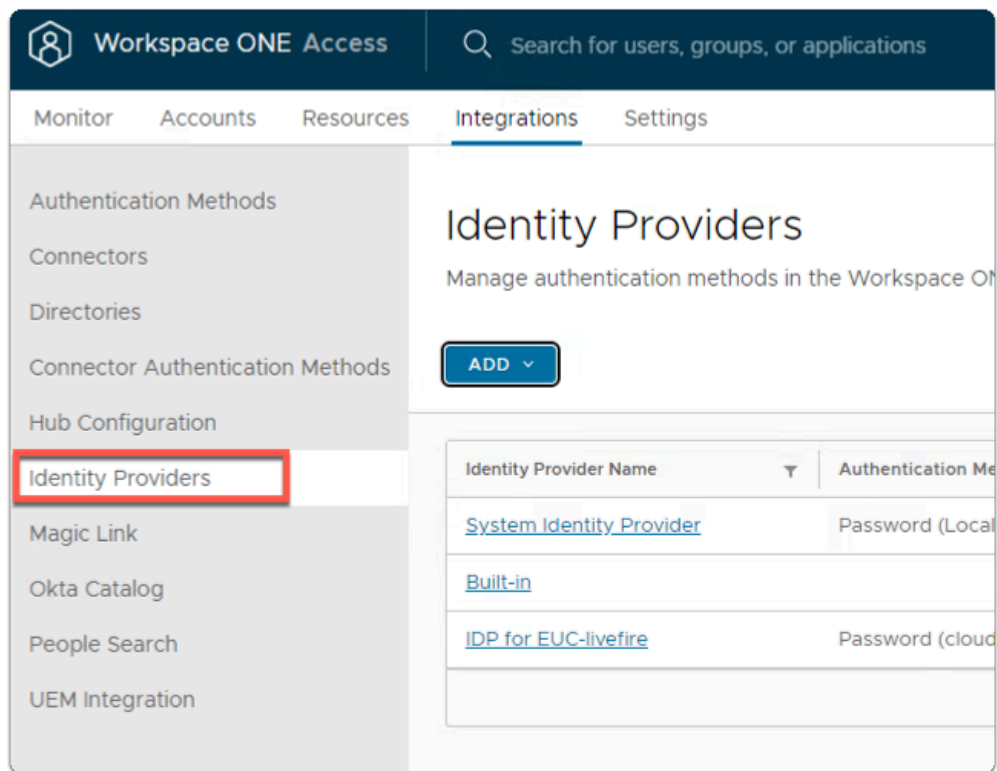
- In the **SAML Certificates** area

- next to **Federation Metadata XML**
 - select **Download**

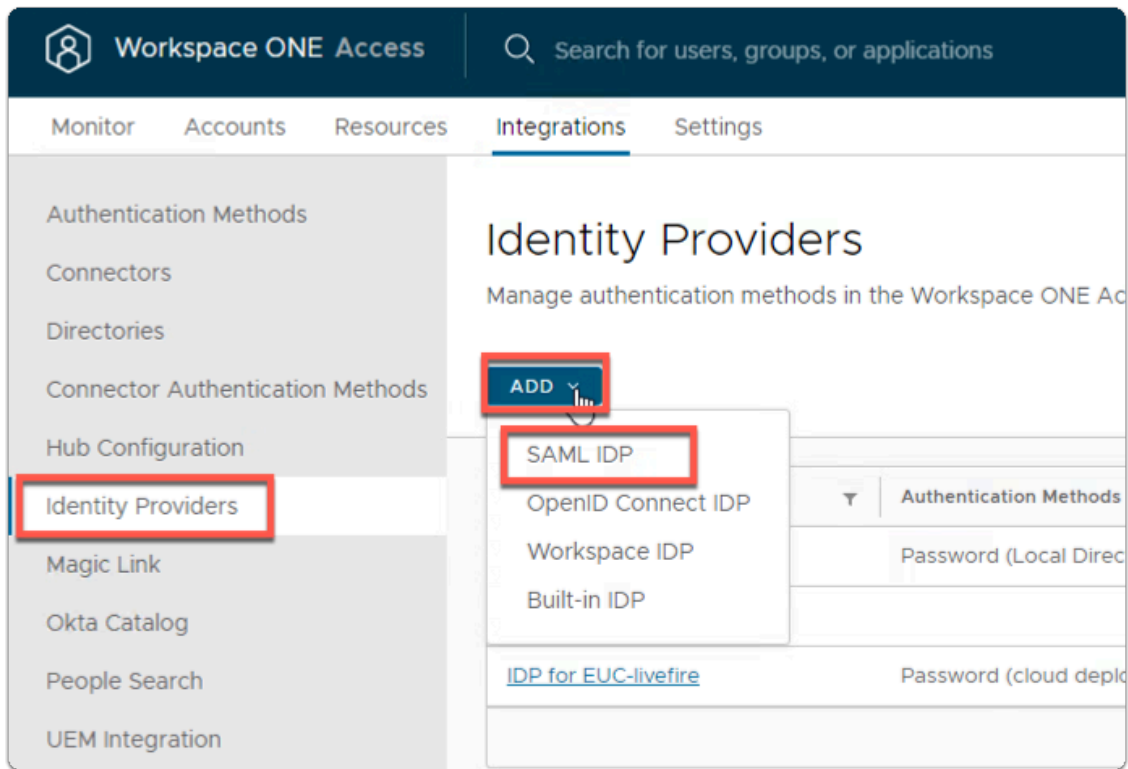


35. On your ControlCenter server
- **browse** to your **Downloads** folder
 - In the **Downloads** folder
 - note you have a **Workspace ONE Access.xml** file
 - In preparation for the next Part switch to your **Workspace ONE Access Admin** console

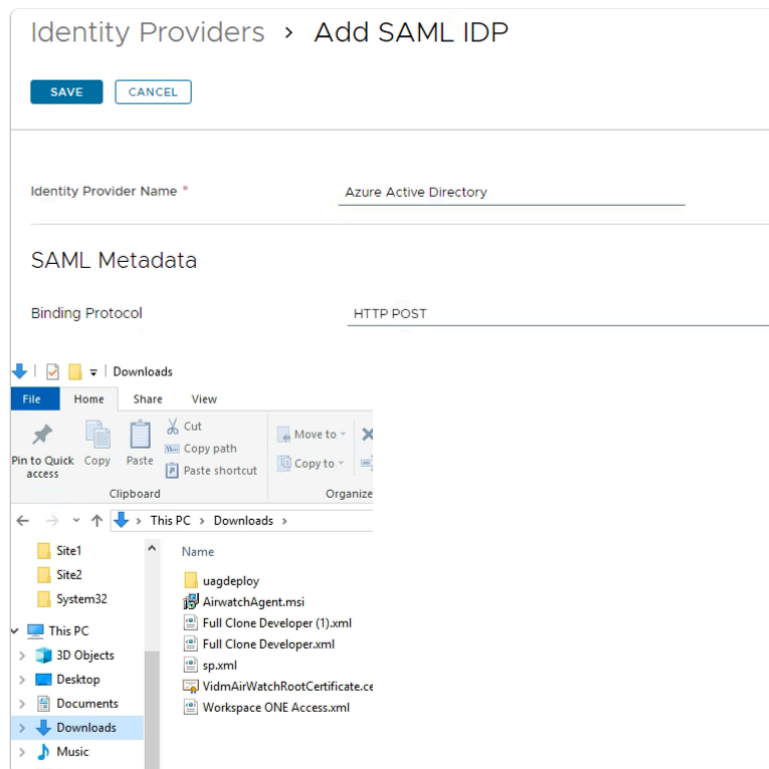
Part 6: Configuring Workspace ONE Access to be an Identity Provider for Microsoft Azure



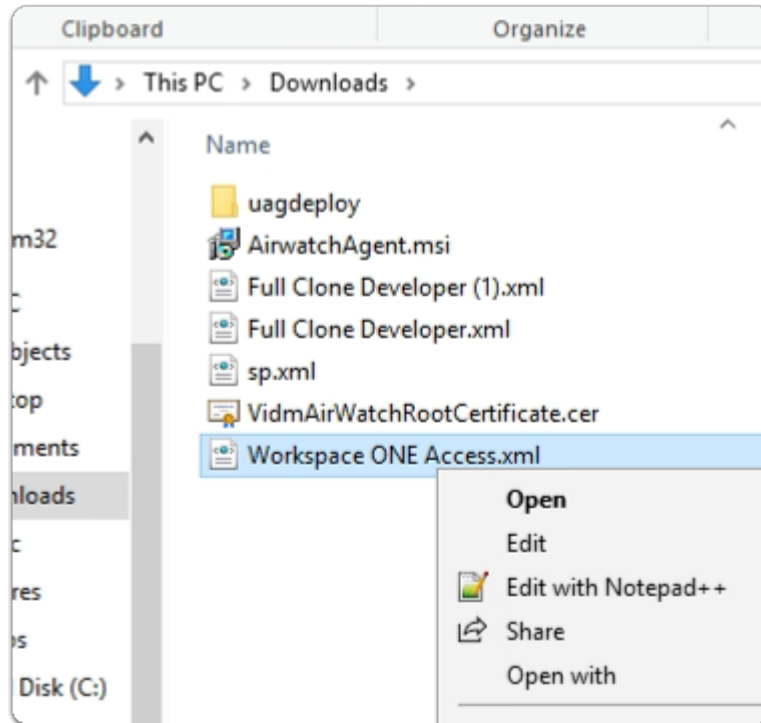
1. On your **Workspace ONE Access** admin console
 - select **Integrations**
 - In the **Integrations** inventory
 - select **Identity Providers**



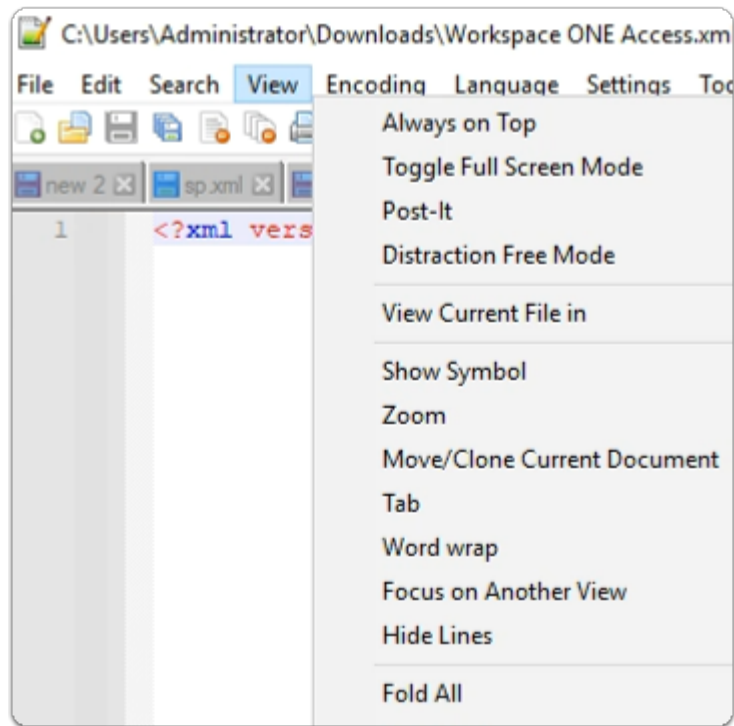
2. In the **Identity Providers** area
 - in the top right corner
 - select **ADD**
 - In the drop down menu
 - select **SAML IDP**



3. In the **New Identity Provider** window
 - next to
 - **Identity Provider Name**
 - enter **Azure Active Directory**
 - Switch to your **Downloads** folder



4. In the **Downloads** folder
 - select and right-click the **Workspace ONE Access.xml** file
 - select **Edit with Notepad++**



5. In the **Notepad++** application
 - In the title bar
 - select **View**
 - disable **word wrap**
 - Click your mouse in the **Notepad++** area
 - With your Keyboard
 - Enter **CTRL+A**
 - Enter **CTRL+C**

Monitor Accounts Resources **Integrations** Settings

Authentication Methods
Connectors
Directories
Connector Authentication Methods
Hub Configuration
Identity Providers

Binding Protocol HTTP POST

SAML metadata is used to establish trust with the IdP.

Identity Provider Metadata (URL or XML)

```
nqMYykHq8iWdE+VD98gCpgkC9O+Xk++UI+re6DBPMvPBOLXok3Jc/X509Certificate>
</X509Data></KeyInfo></KeyDescriptor><SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/741d8c10-6b83-4ab8-addf-2cd6b43b52be/saml2" />
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://login.microsoftonline.com/741d8c10-6b83-4ab8-addf-2cd6b43b52be/saml2" />
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://login.microsoftonline.com/741d8c10-6b83-4ab8-addf-2cd6b43b52be/saml2" />
</IDPSSODescriptor></EntityDescriptor>
```

PROCESS IDP METADATA

Identify User Using ☒ NameID Element ☐ SAML Attribute

Name ID format mapping from SAML Response

Name ID Format	Name ID Value

+ ADD

Name ID Policy in SAML Request urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

☐ Send Subject in SAML Request (when available) ⓘ

6. In the **Azure Active Directory** window

- next to
- **SAML Metadata**
 - under **Identity Provider Metadata (URL or XML)**
 - **paste** your XML Metadata

Identify User Using ☒ NameID Element ☐ SAML Attribute

Name ID format mapping from SAML Response

Name ID Format	Name ID Value

+ ADD

Name ID Policy in SAML Request urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

☐ Send Subject in SAML Request (when available) ⓘ

7. In the **Azure Active Directory** window

- In line with
- **Name ID Format**
 - to the right
 - select the **+ ADD** twice

Name ID format mapping from SAML Response	Name ID Format	Name ID Value
	urn:oasis:names:tc:SAML:1.1:nameid-format:...	userName
	urn:oasis:names:tc:SAML:1.1:nameid-format:...	userPrincipalName

+ ADD

8. In the **Azure Active Directory** window

- below
 - **Name ID Format**
 - 1st row
 - from the drop down
 - select **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**
 - **Name ID Format**
 - 2nd row
 - from the drop down
 - select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**

Name ID format mapping from SAML Response	Name ID Format	Name ID Value
	urn:oasis:names:tc:SAML:1.1:nameid-format:...	userName
	urn:oasis:names:tc:SAML:1.1:nameid-format:...	userPrincipalName

+ ADD

9. In the **Azure Active Directory** window

- below
 - **Name ID Value**
 - 1st row
 - from the drop down
 - select **username**
 - **Name ID Format**
 - 2nd row
 - from the drop down
 - select **userprincipalname**

Users

Select which users can authenticate using this IdP. Choose from the available directories from the list below.

☒ EUC-livewire

Network

Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

☒ ALL RANGES

10. In the **Azure Active Directory** window

- In the **Users area**
 - next to **EUC-livewire**
 - select the **checkbox**
- In the **Network area**
 - next to **ALL RANGES**
 - select the **checkbox**

Authentication Methods

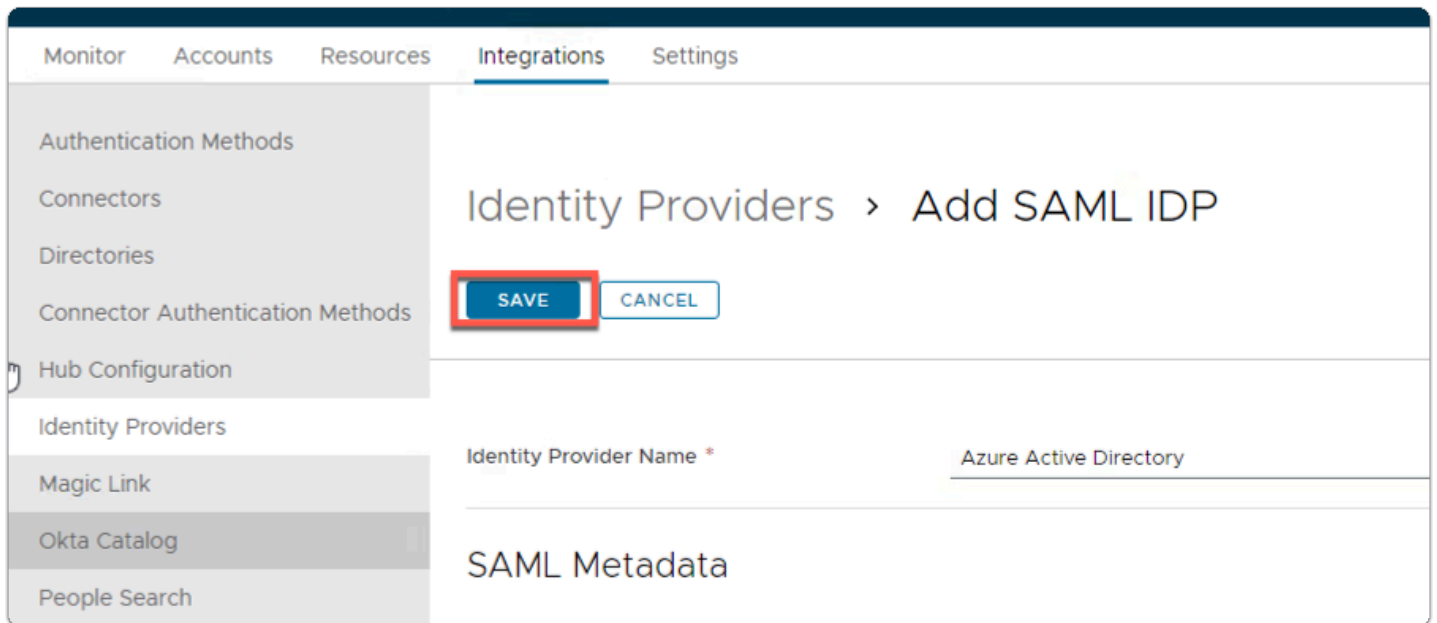
Select which authentication methods the IdP will use to authenticate users..

Authentication Method	SAML Context
AAD Password	urn:oasis:names:tc:SAML:2.0:ac:classes:Password

+ ADD

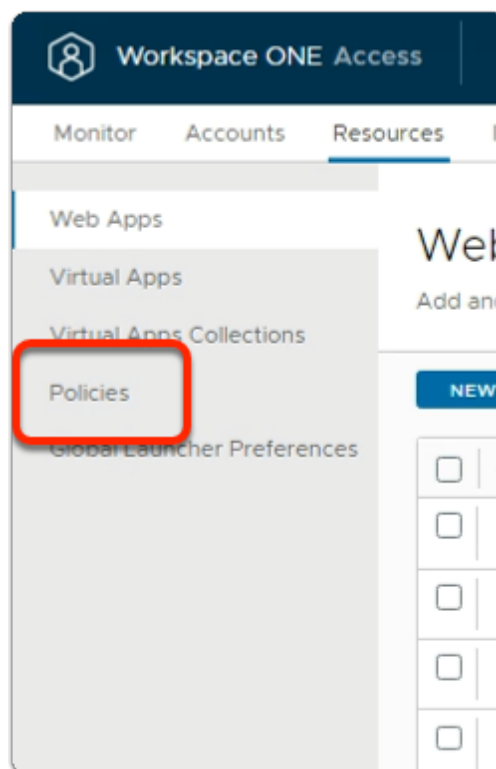
11. In the **Azure Active Directory** window

- In the **Authentication Methods area**
 - below **Authentication Methods**
 - type **AAD Password**
 - below **SAML Context**
 - from the dropdown
 - select **urn:oasis:names:tc:SAML:2.0:ac:classes:Password**



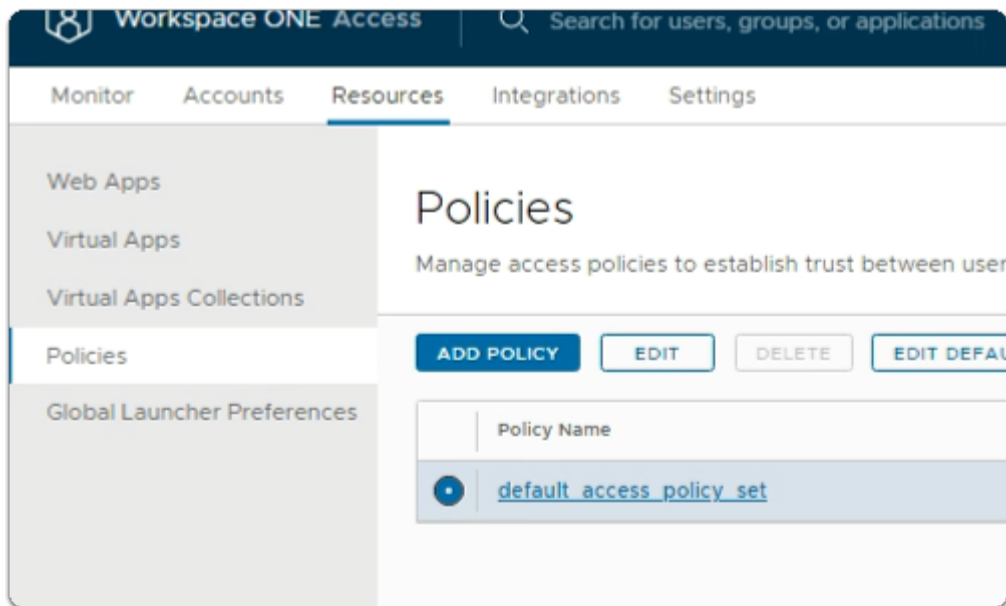
12. In the **Azure Active Directory** window

- **scroll to the top** of the page
- select **SAVE**

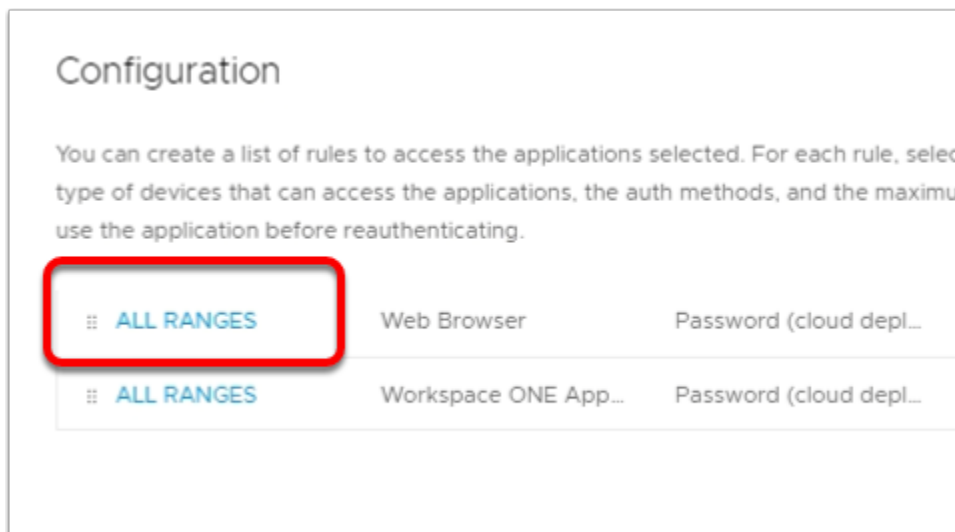


13. In the **Workspace ONE Access Admin** Console

- Select the **Resources** tab
- select **Policies**



14. In the **Policies** interface
 - next to **default access policy set**
 - select the **radio button**
 - select **EDIT**



15. In the **Edit Policy** window,
 - In the left column
 - Select **Configuration**
 - To the left of **Web Browser**,
 - Select **All Ranges**

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

and user is registering FIDO2 authenticator * ☐ No ⓘ

Then perform this action Authenticate using... ⓘ

then the user may authenticate using * AAD Password ⓘ ⓘ ⓘ

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

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

16. In the **Edit Policy Rule** window

- Next to **then the user may authenticate using ***
 - select **AAD Password**
- Next to **if preceding method fails or is not applicable, then ***
 - select **Password (cloud deployment),**
- Select **ADD FALLBACK METHOD**
 - Next to **if preceding method fails or is not applicable, then ***
 - select **Password (Local Directory)**
- Select **SAVE** at the bottom of the window

Configuration

You can create a list of rules to access the applications selected. For each rule, select the IP network range, of devices that can access the applications, the auth methods, and the maximum number of hours users can application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
⌵ ALL RANGES	Web Browser	AAD Password+2	8 Hour(s)
⌵ ALL RANGES	Workspace ONE App ...	Password (cloud depl...	2160 Hour(s)

+ ADD POLICY RULE

17. In the **Edit Policy Rule** window

- Select **+ ADD POLICY RULE**

< CONFIGURATION
Add Policy Rule

If a user's network range is * ALL RANGES

and the user accessing content from * Windows 10

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

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

and user is registering FIDO2 authenticator * ☐ No

Then perform this action Authenticate using...

then the user may authenticate using * AAD Password

If the preceding method fails or is not applicable, then

Password (cloud deployment)

Password (Local Directory)

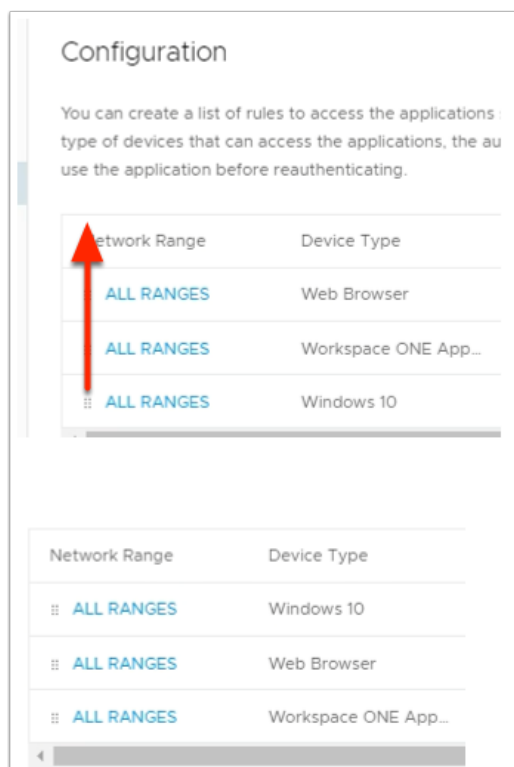
CANCEL

SAVE

18. In the **Edit Policy Rule** window

- Next to: -
 - **and user accessing content from***
 - select **Windows 10**

- then the user may authenticate using*
 - select **AAD Password**
- if the preceding method fails or is not applicable, then
 - select **Password (cloud deployment)**
- Select **+ ADD FALLBACK METHOD**
 - if the preceding method fails or is not applicable, then
 - Select **Password (Local Directory)**
- At the bottom right hand side of the page
 - Select **SAVE**



19. In the **Edit Policy** window
- Next to **ALL RANGES for Windows 10**
 - Select the **6 DOTS** and drag to the top
 - Select **NEXT** on the **Edit Policy Page**

Edit Policy

- 1 Definition
- 2 Configuration
- 3 Summary

Summary

Definition

Name
default_access_policy_set

Description
Default access policy set

Applications
4 Application(s)

Configuration

Policy Rule 1
If a user's network range is **ALL RANGES**
and the user is accessing content from **Windows 10**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **AAD Password**

[CANCEL](#) [BACK](#) [SAVE](#)

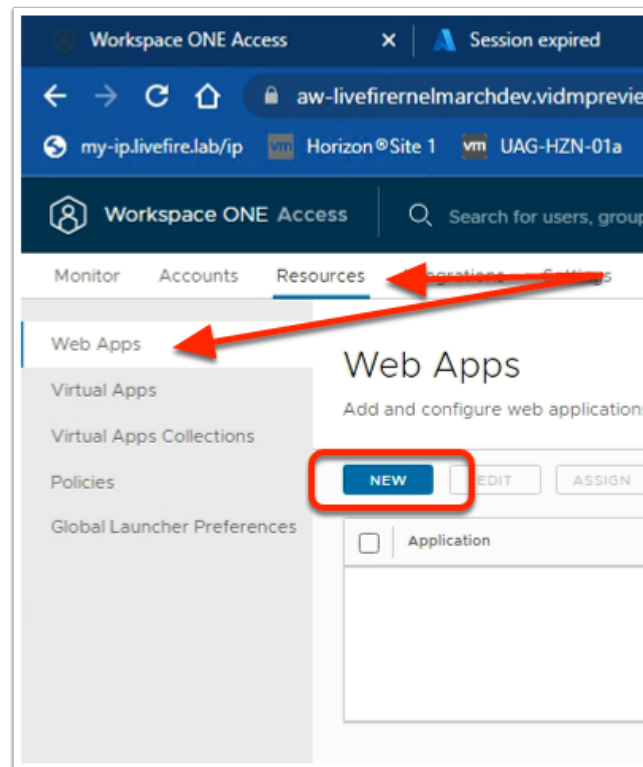
20. On the **Edit Policy** Page.

- Summary tab
- Select **SAVE**

Part 7: Inserting Office 365 Deep Links into Workspace ONE Access

We will divide this Part into 4 steps

Step 1. Inserting Deep links for Microsoft Word



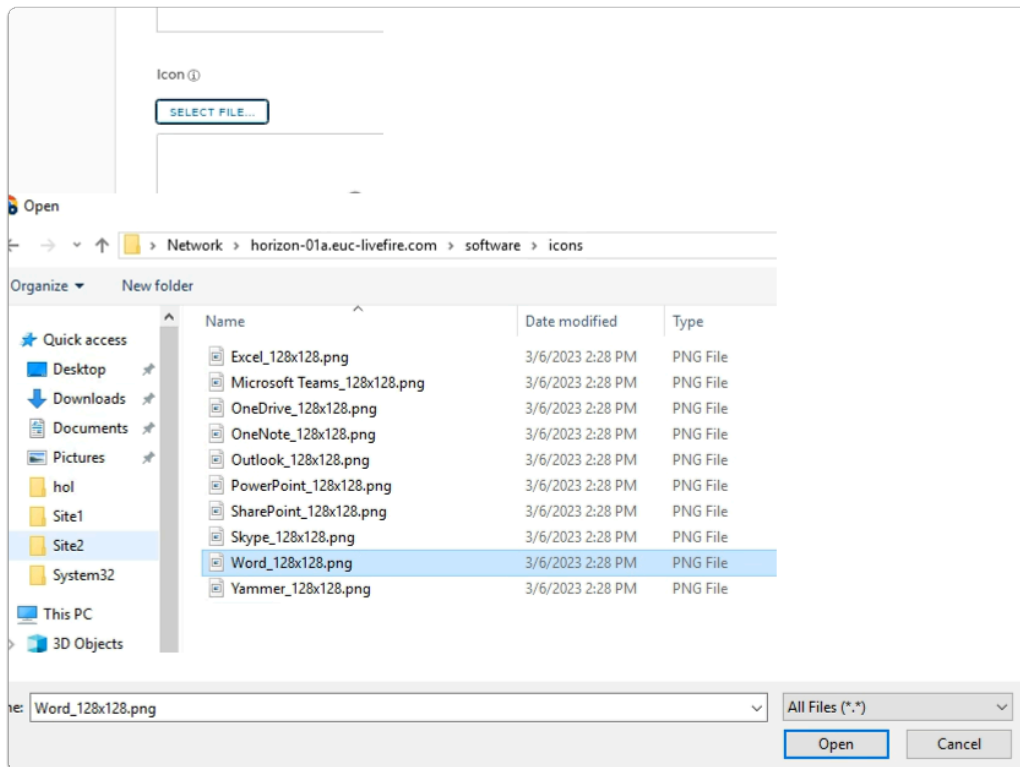
1. On your **Controlcenter** server.
 - In the Workspace ONE Access Admin Console
 - Select the **Resources** tab
 - In the Resources menu
 - Select **Web Apps**
 - Select **NEW**

A screenshot of the 'New SaaS Application' form in the Workspace ONE Access Admin Console. The form has a left sidebar with four steps: '1 Definition', '2 Configuration', '3 Access Policies', and '4 Summary'. The '1 Definition' step is selected. The main area is titled 'OR BROWSE FROM CATALOG'. It contains two input fields: 'Name' (with a red asterisk and an information icon) and 'Description' (with an information icon). The 'Name' field is filled with 'Microsoft Word'. The 'Description' field is empty.

2. In the **New SaaS Application** wizard

1. **Definition** area

- below **Name ***
 - type **Microsoft Word**



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

1. **Definition** area

- below **Icon ***
 - click on **SELECT FILE**
 - **browse** to
 - **\\horizon-01a.euc-livewire.com\software\icons**
 - select **Word_128x128.png**
 - select **Open**
- In the bottom right-corner
 - select **NEXT**

4. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Authentication Type** *
 - from the dropdown
 - select **Web Application Link**

5. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Target URL** *
 - Copy the URL below and edit in **Notepad++** the following in Blue with **your assigned domain suffix** and then **copy** the edited URL and Paste under the **Target URL**
 - <https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=EXAMPLEDOMAIN.euc-livefire.com&wreply=https://office.live.com/start/Word.aspx?auth=2>
 - In the bottom right corner

- select **NEXT**

New SaaS Application

1 Definition
2 Configuration
3 Summary

Definition

Name
Microsoft Word

Description
—

Icon

Categories
—

Configuration

Authentication Type
None

Target URL
https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpXXX.euc-liveware.com&wreply=https://office.live.

Access Policies

CANCEL BACK **SAVE & ASSIGN** SAVE

6. In the **New SaaS Application** wizard

3. **Summary** area

- bottom right corner
- select **SAVE & ASSIGN**

Assign

✓ Application: 'Microsoft Word' added successfully.

Selected App(s): Microsoft Word

Users / User Groups

🔍 Developers

Developers@euc-liveware.com

Selected Users / User Groups

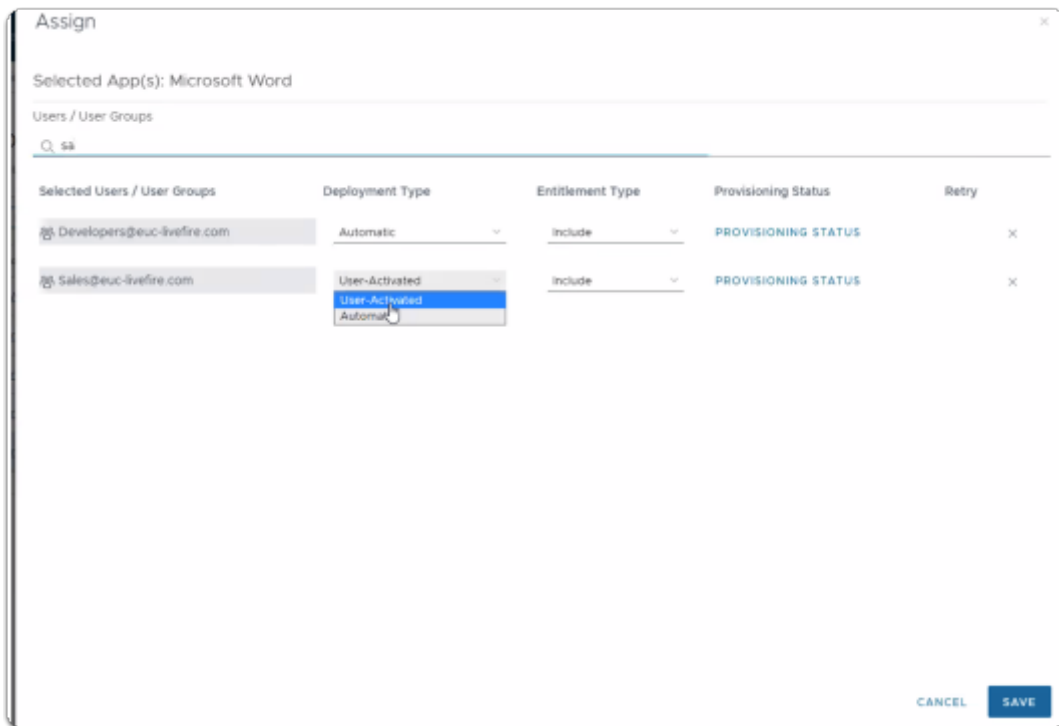
Developers@euc-liveware.com

Deployment Type

Automatic

CANCEL **SAVE**

7. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Developers**,
 - select **Developers@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**



8. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Sa**,
 - select **Sales@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Assign

Selected App(s): Microsoft Word

Users / User Groups

Q mark

	Deployment Type	Entitlement Type	Provisioning Status	Retry
Marketing@euc-livewire.com	automatic	Include	PROVISIONING STATUS	×
kim@euc-livewire.com	automatic	Include	PROVISIONING STATUS	×

CANCEL SAVE

9. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Mark**,
 - select **Marketing@euc-livewire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Assign

Selected App(s): Microsoft Word

Users / User Groups

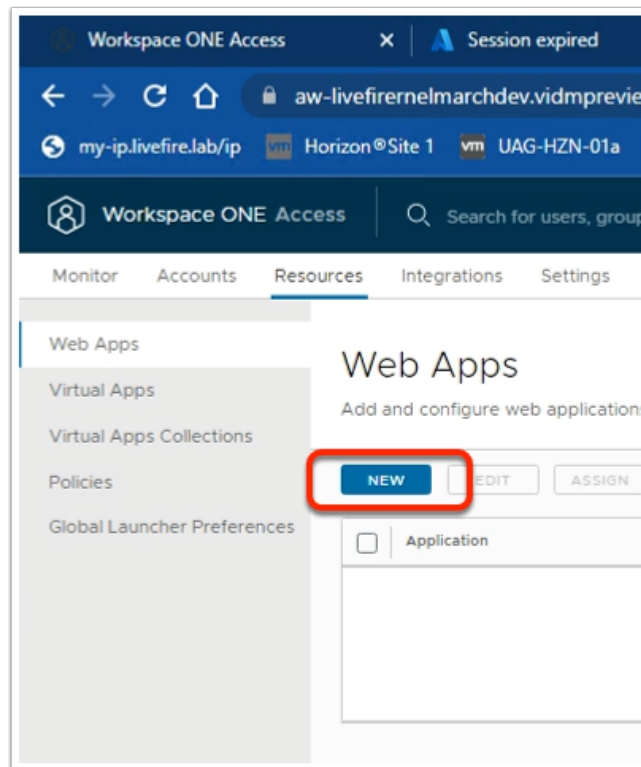
Q It

Selected Users / User Groups	Deployment Type	Entitlement Type	Provisioning Status	Retry
Developers@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
Sales@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
Marketing@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
IT Support@euc-liveware.com	<div> User-Activated User-Activated Automatic </div>	Include	PROVISIONING STATUS	X

CANCEL SAVE

9. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **IT**,
 - select **ITsupport@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Step 2. Inserting Deep links for Microsoft Excel



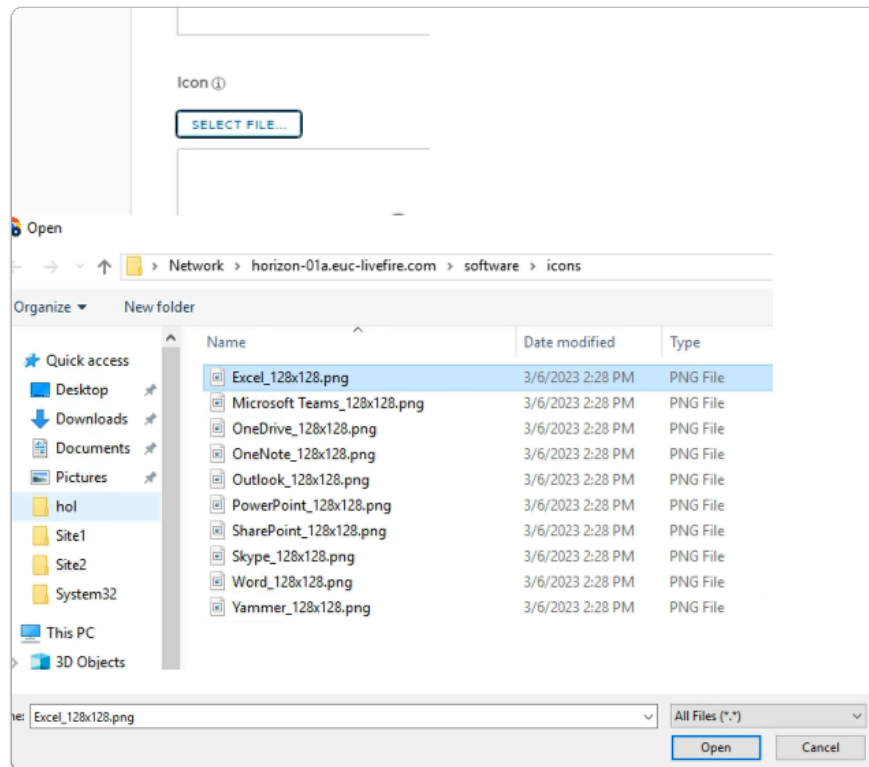
1. In the **Web Apps** area.
 - Select **NEW**

A screenshot of the 'New SaaS Application' wizard. The title 'New SaaS Application' is at the top. On the left is a sidebar with four steps: '1 Definition' (selected), '2 Configuration', '3 Access Policies', and '4 Summary'. The main area is titled 'Definition' and contains a 'Search' field with a magnifying glass icon and a help icon. Below the search field is a link that says 'OR BROWSE FROM CATALOG'. Further down is a 'Name' field with a red asterisk and a help icon, containing the text 'Microsoft Excel'. At the bottom is a 'Description' field with a help icon.

2. In the **New SaaS Application** wizard

1. Definition area

- below **Name ***
 - type **Microsoft Excel**



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

1. Definition area

- below **Icon ***
 - click on **SELECT FILE**
 - **browse** to
 - **\\horizon-01a.euc-livewire.com\software\icons**
 - select **Excel_128x128.png**
 - select **Open**
- In the bottom right-corner
 - select **NEXT**

4. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Authentication Type ***
 - from the dropdown
 - select **Web Application Link**

5. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Target URL ***
 - Copy the URL below and edit in **Notepad++** the following in Blue with **your assigned domain suffix** and then **copy** the edited URL and Paste under the **Target URL**
 - [https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpXXX.euc-liv...&wreply=https://www.office.com/launch/excel?auth=2&home=1](https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpXXX.euc-liv...)

- In the bottom right corner
 - select **NEXT**

New SaaS Application

1 Definition
2 Configuration
3 Summary

Definition

Name
Microsoft Word

Description
-

Icon

Categories
-

Configuration

Authentication Type
None

Target URL
https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpXXX.euc-livewire.com&wreply=https://office.live.

Access Policies

CANCEL BACK **SAVE & ASSIGN** SAVE

6. In the **New SaaS Application** wizard
3. **Summary** area
 - bottom right corner
 - select **SAVE & ASSIGN**

Assign

✔ Application: 'Microsoft Excel' added successfully.

Selected App(s): Microsoft Excel

Users / User Groups

🔍 Developer

👤 Developers@euc-livewire.com

Selected Users / User Groups

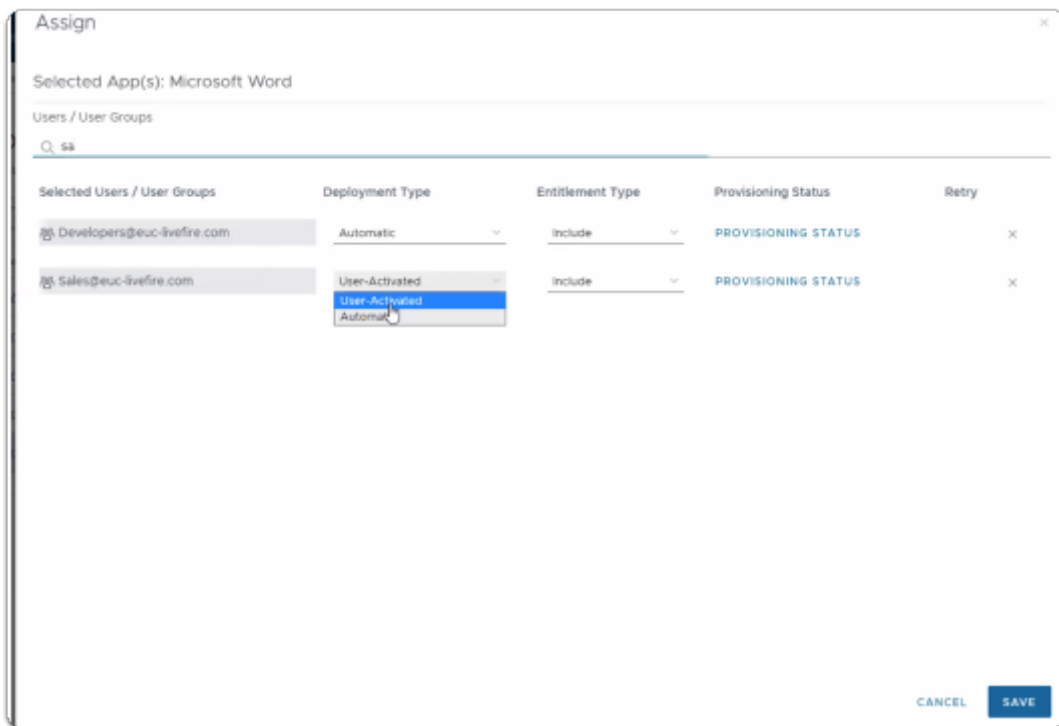
👤 Developers@euc-livewire.com

Deployment Type

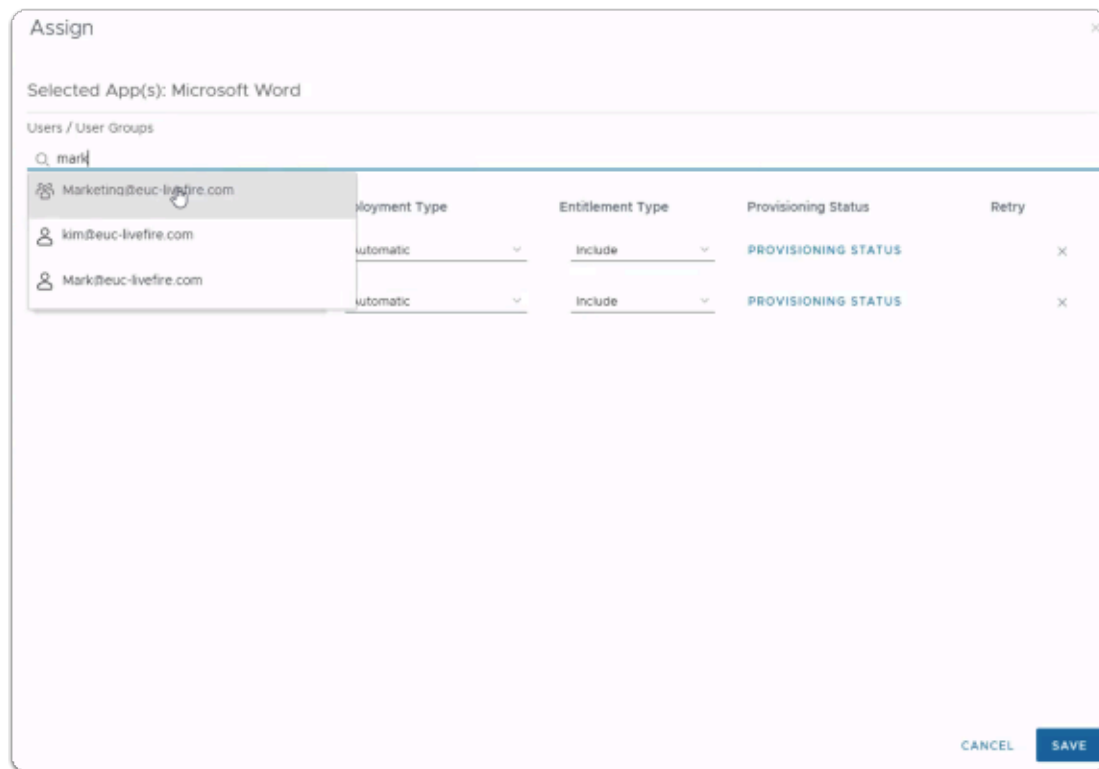
Automatic

CANCEL SAVE

7. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Developers**,
 - select **Developers@euc-livewire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**



8. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Sa**,
 - select **Sales@euc-livefire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**



9. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Mark**,
 - select **Marketing@euc-livewire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Assign

Selected App(s): Microsoft Word

Users / User Groups

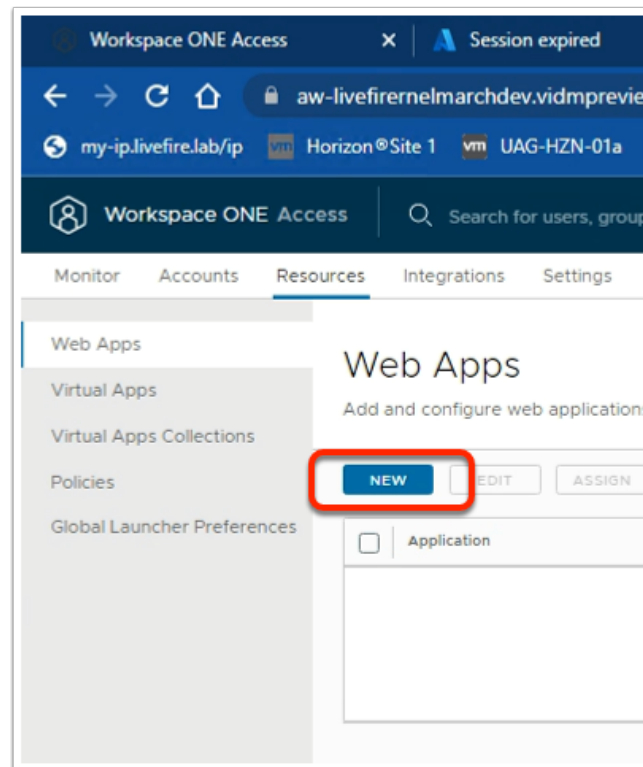
Q It

Selected Users / User Groups	Deployment Type	Entitlement Type	Provisioning Status	Retry
Developers@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
Sales@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
Marketing@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
IT Support@euc-liveware.com	User-Activated User-Activated Automatic	Include	PROVISIONING STATUS	X

CANCEL SAVE

9. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **IT**,
 - select **ITsupport@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Step 3. Inserting Deep links for Microsoft Powerpoint



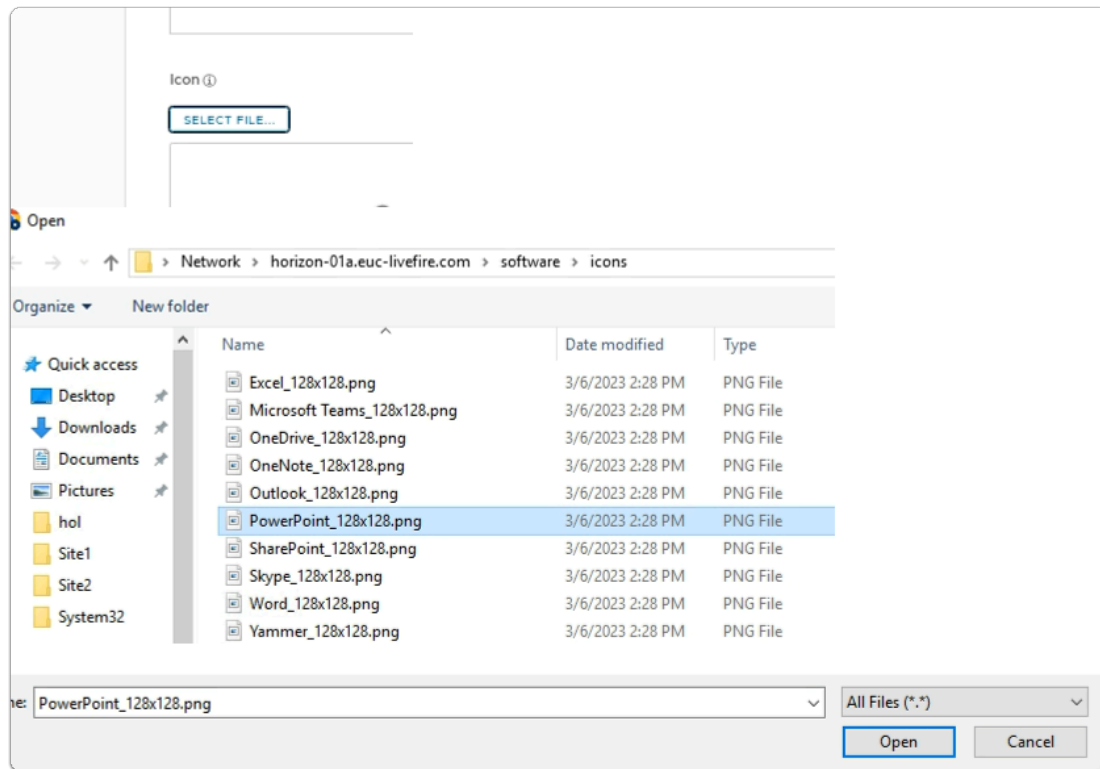
1. In the **Web Apps** area.
 - Select **NEW**

A screenshot of the 'New SaaS Application' wizard. The title is 'New SaaS Application'. On the left is a sidebar with four steps: '1 Definition' (selected), '2 Configuration', '3 Access Policies', and '4 Summary'. The main area is titled 'Definition' and contains a 'Search' field with a magnifying glass icon. Below the search field is a link that says 'OR BROWSE FROM CATALOG'. Further down is a 'Name' field with a red asterisk and a help icon; it contains the text 'Microsoft Powerpoint'. Below the name field is a 'Description' field with a help icon.

2. In the **New SaaS Application** wizard

1. Definition area

- below **Name ***
 - type **Microsoft Powerpoint**



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

1. Definition area

- below **Icon ***
 - click on **SELECT FILE**
 - **browse** to
 - **\\horizon-01a.euc-livewire.com\software\icons**
 - select **PowerPoint_128x128.png**
 - select **Open**
- In the bottom right-corner
 - select **NEXT**

4. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Authentication Type** *
 - from the dropdown
 - select **Web Application Link**

5. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Target URL** *
 - Copy the URL below and edit in **Notepad++** the following in Blue with **your assigned domain suffix** and then **copy** the edited URL and Paste under the **Target URL**
 - <https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpXXX.euc-livewire.com&wreply=https://www.office.com/launch/powerpoint?auth=2>
 - In the bottom right corner

- select **NEXT**

New SaaS Application

1 Definition
2 Configuration
3 Summary

Definition

Name
Microsoft Powerpoint

Description
—

Icon

Categories
—

Configuration

Authentication Type
None

Target URL
https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpxxx.euc-livfire.com&wreply=https://www.office

Access Policies

CANCEL BACK **SAVE & ASSIGN** SAVE

6. In the **New SaaS Application** wizard

3. **Summary** area

- bottom right corner
- select **SAVE & ASSIGN**

Assign

✓ Application: 'Microsoft Powerpoint' added successfully.

Selected App(s): Microsoft Powerpoint

Users / User Groups

Q devel

Developers@euc-livfire.com

Selected Users / User Groups

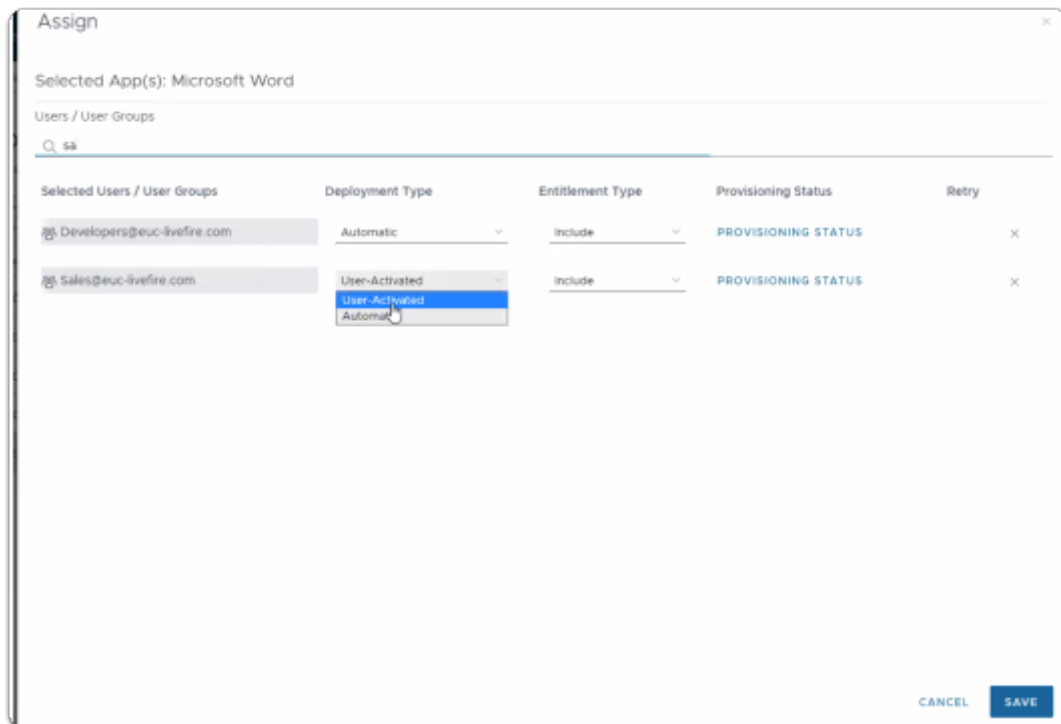
Developers@euc-livfire.com

Deployment Type

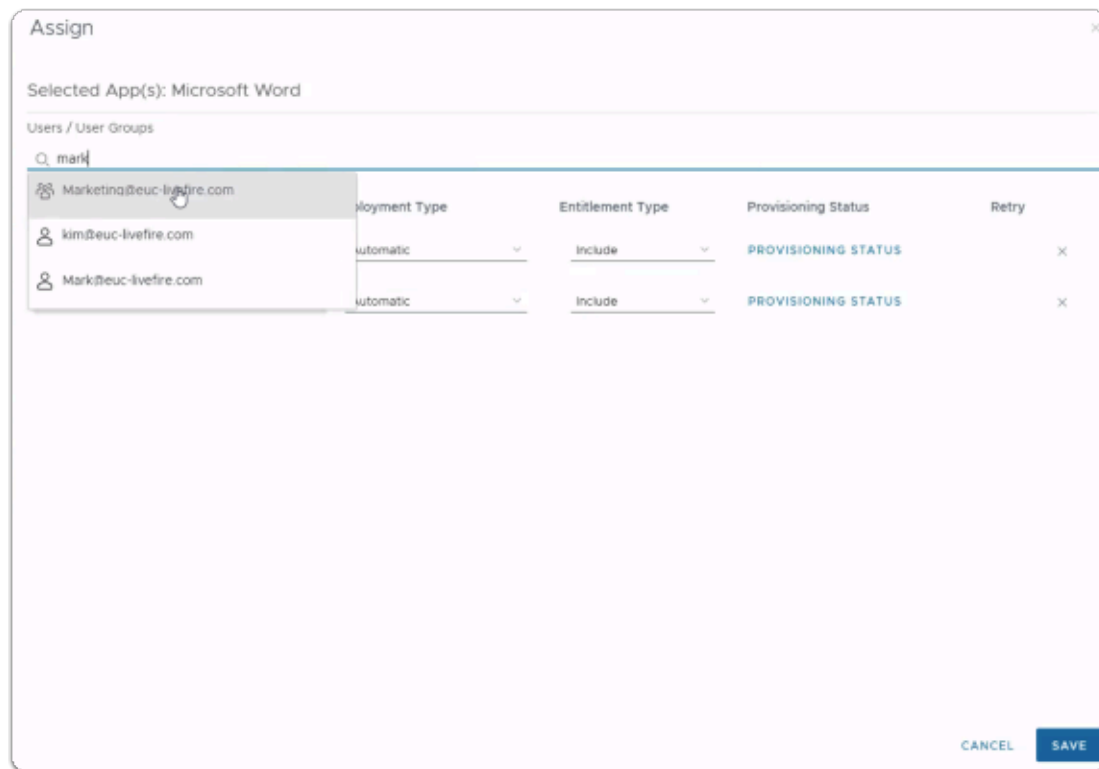
Automatic

CANCEL SAVE

7. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Developers**,
 - select **Developers@euc-livefire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**



8. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Sa**,
 - select **Sales@euc-livefire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**



9. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **Mark**,
 - select **Marketing@euc-livewire.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Assign

Selected App(s): Microsoft Word

Users / User Groups

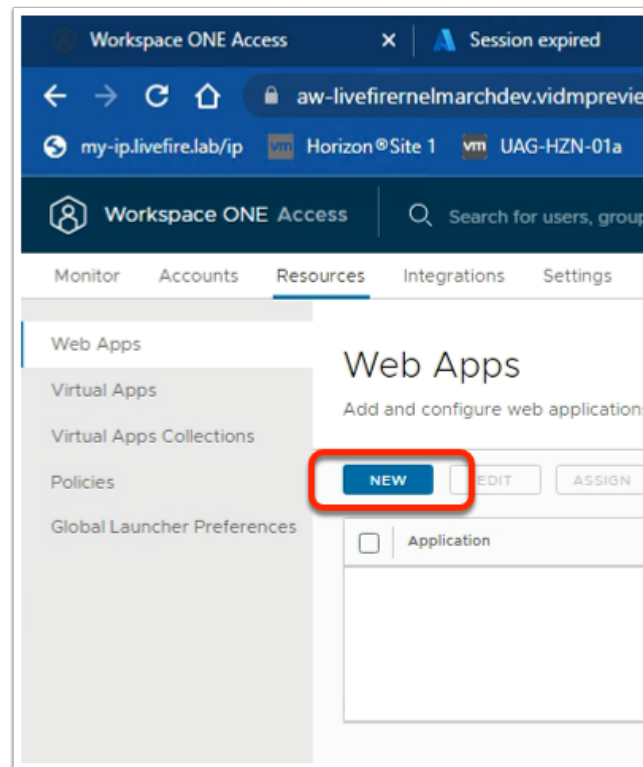
Q IT

Selected Users / User Groups	Deployment Type	Entitlement Type	Provisioning Status	Retry
Developers@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
Sales@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
Marketing@euc-liveware.com	Automatic	Include	PROVISIONING STATUS	X
IT Support@euc-liveware.com	User-Activated User-Activated Automatic	Include	PROVISIONING STATUS	X

CANCEL SAVE

9. In the **Assign** window
 - Under **Users / User Groups**
 - In the **Search** area
 - type **IT**,
 - select **ITsupport@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Step 4. Inserting Deep links for Microsoft Outlook



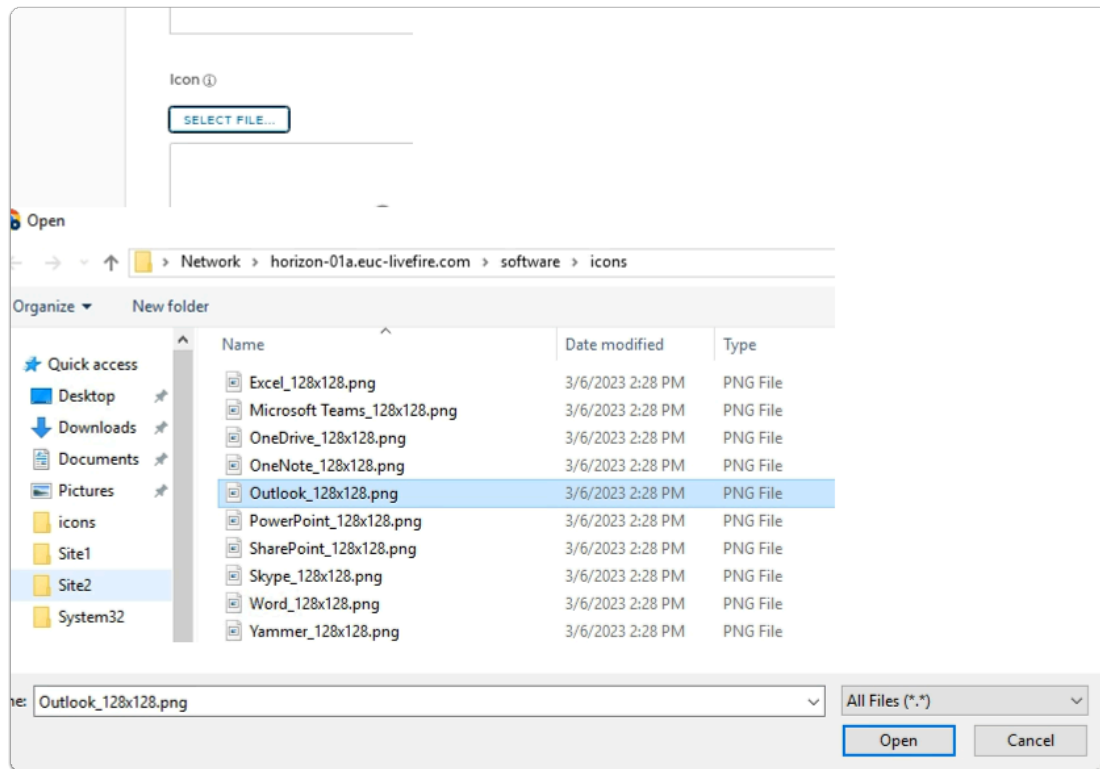
1. In the **Web Apps** area.
 - Select **NEW**

A screenshot of the 'New SaaS Application' wizard. The title is 'New SaaS Application'. On the left is a sidebar with four steps: '1 Definition' (selected), '2 Configuration', '3 Access Policies', and '4 Summary'. The main area is titled 'Definition' and contains a 'Search' field with a magnifying glass icon, a text input field, and a link 'OR BROWSE FROM CATALOG'. Below this is a 'Name' field with a red asterisk and a help icon, containing the text 'Microsoft Outlook'. A 'Description' field is partially visible at the bottom.

2. In the **New SaaS Application** wizard

1. Definition area

- below **Name ***
 - type **Microsoft Outlook**



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

1. Definition area

- below **Icon ***
 - click on **SELECT FILE**
 - **browse** to
 - **\\horizon-01a.euc-livewire.com\software\icons**
 - select **Outlook_128x128.png**
 - select **Open**
- In the bottom right-corner
 - select **NEXT**

New SaaS Application

1 Definition

2 Configuration

3 Summary

Single Sign-On

Authentication Type * ⓘ

Web Application Link

Target URL *

4. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Authentication Type** *
 - from the dropdown
 - select **Web Application Link**

Application

Single Sign-On

Authentication Type * ⓘ

Web Application Link

Target URL *

https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&domain_hint=corpxxx.euc-liveware.com

Invalid URL

Open in Workspace ONE Web ⓘ

☐ No

5. In the **New SaaS Application** wizard
 2. **Configuration** area
 - below **Target URL** *
 - Copy the URL below and edit in **Notepad++** the following in Blue with **your assigned domain suffix** and then **copy** the edited URL and Paste under the **Target URL**
 - https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&domain_hint=corpxxx.euc-liveware.com
 - In the bottom right corner

- select **NEXT**

New SaaS Application

1 Definition
2 Configuration
3 Summary

Definition

Name
Microsoft Powerpoint

Description
—

Icon

Categories
—

Configuration

Authentication Type
None

Target URL
https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=corpxxx.euc-livewire.com&wreply=https://www.office

Access Policies

CANCEL BACK **SAVE & ASSIGN** SAVE

6. In the **New SaaS Application** wizard
3. **Summary** area
 - bottom right corner
 - select **SAVE & ASSIGN**

Assign

✓ Application: 'Microsoft Outlook' added successfully.

Selected App(s): Microsoft Outlook

Users / User Groups

Q deve

Developers@euc-livewire.com

Selected Users / User Groups

Developers@euc-livewire.com

Deployment Type

Automatic

CANCEL **SAVE**

7. In the **Assign** window
- Under **Users / User Groups**
 - In the **Search** area
 - type **Developers**,
 - select **Developers@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**

Selected App(s): Microsoft Outlook

Users / User Groups

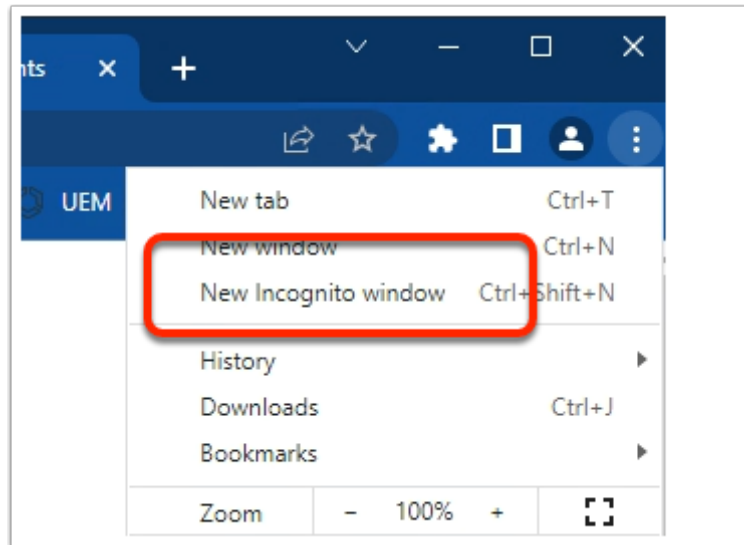
Q It

IT Support@euc-liveware.com Deploy

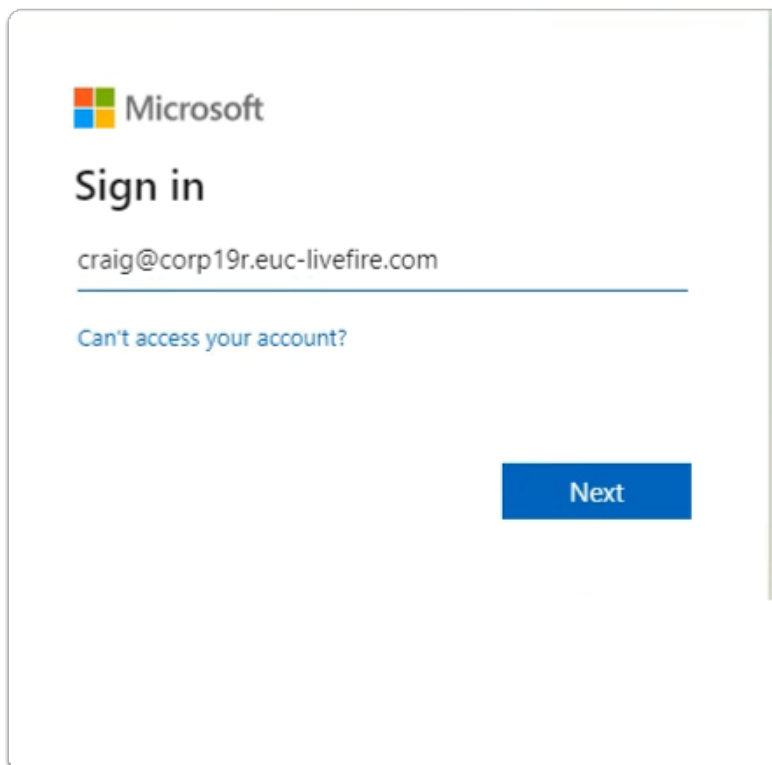
Developers@euc-liveware.com Autom

8. In the **Assign** window
- Under **Users / User Groups**
 - In the **Search** area
 - type **IT support**
 - select **IT support@euc-liveware.com**
 - Under **Deployment Type**
 - select **Automatic**
 - In the bottom right corner
 - select **SAVE**

Part 8: Testing to see if the Federation works

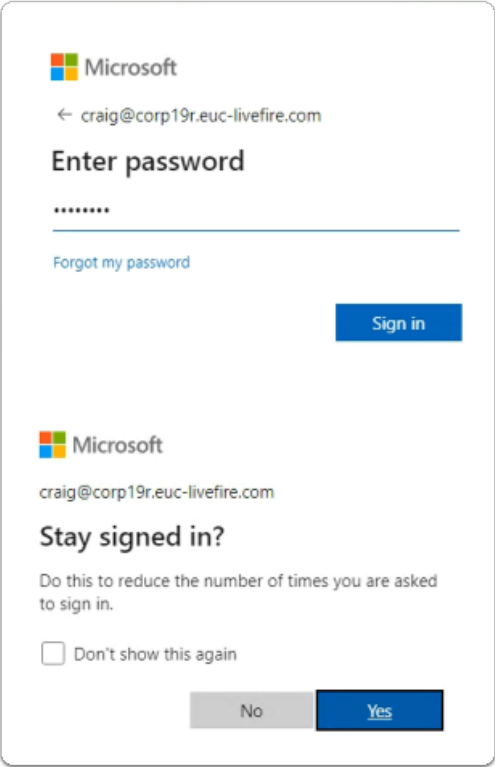


1. On your Control Center server
 - On your Chrome browser
 - Open up an **Incognito** session
 - In the address bar enter [your Workspace ONE Access tenant url](#)



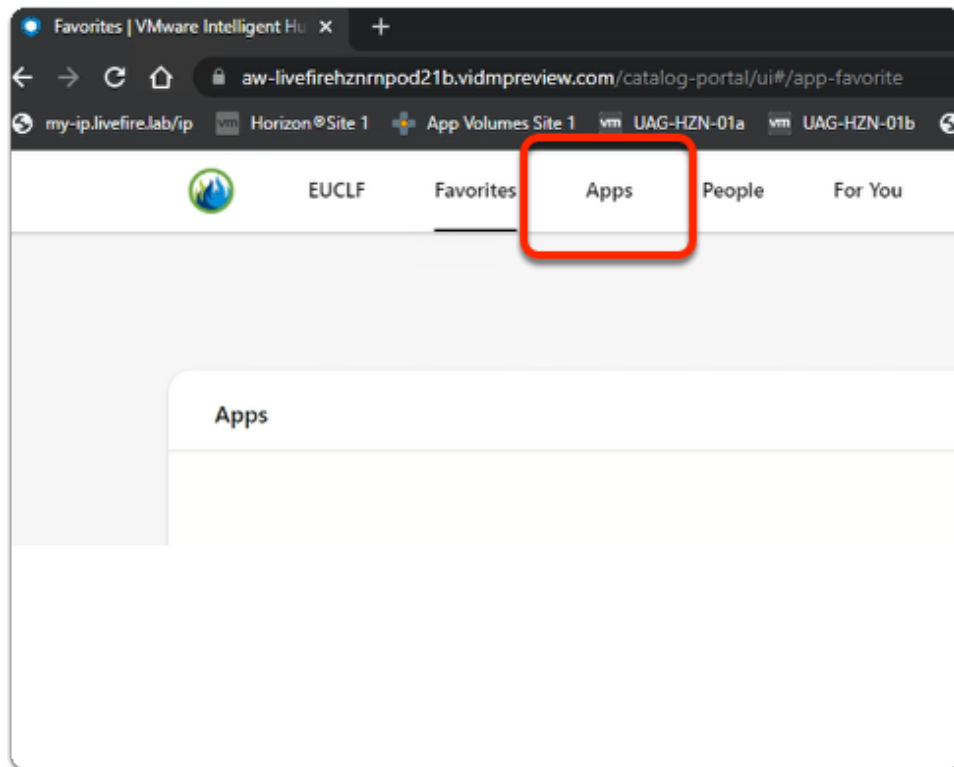
2. In the **Microsoft Sign in** window
 - enter
 - [craig@corpXXX.euc-livefire.com](#)

- XXX = your assigned domain
- select **Next**



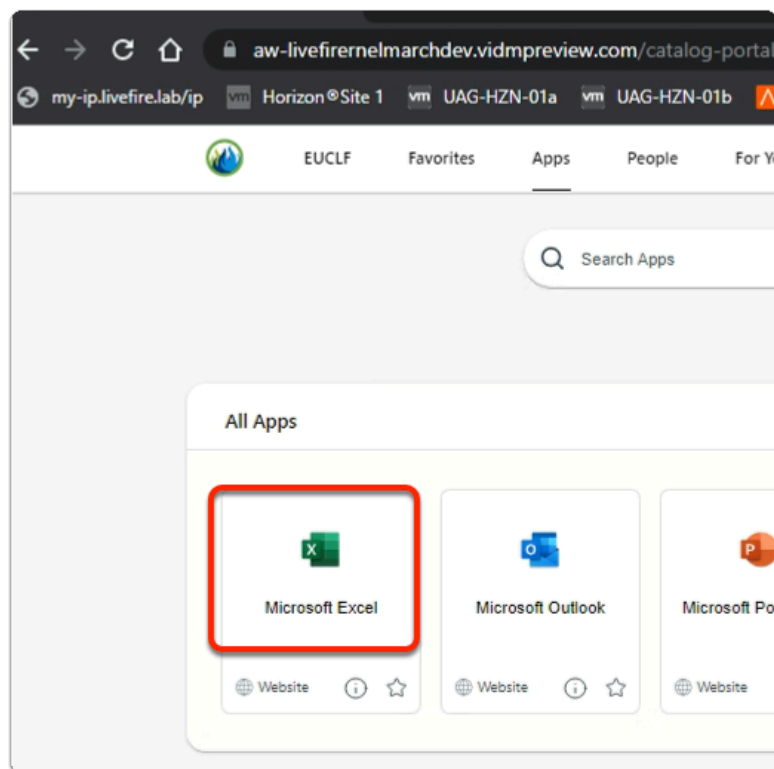
The screenshot displays the Microsoft Sign in interface. At the top, the Microsoft logo is followed by the email address 'craig@corp19r.euc-livewire.com'. Below this, the 'Enter password' section features a password input field with masked characters (dots) and a 'Forgot my password' link. A blue 'Sign in' button is positioned to the right. The lower section, titled 'Stay signed in?', includes a checkbox labeled 'Don't show this again' and two buttons: a grey 'No' button and a blue 'Yes' button.

3. In the **Microsoft Sign in** window
 - Under **Enter password**
 - enter **VMware1!**
 - select **Sign in**
 - In the **Stay signed in?** window
 - select **NO**



4. In the **web Intelligent Hub**

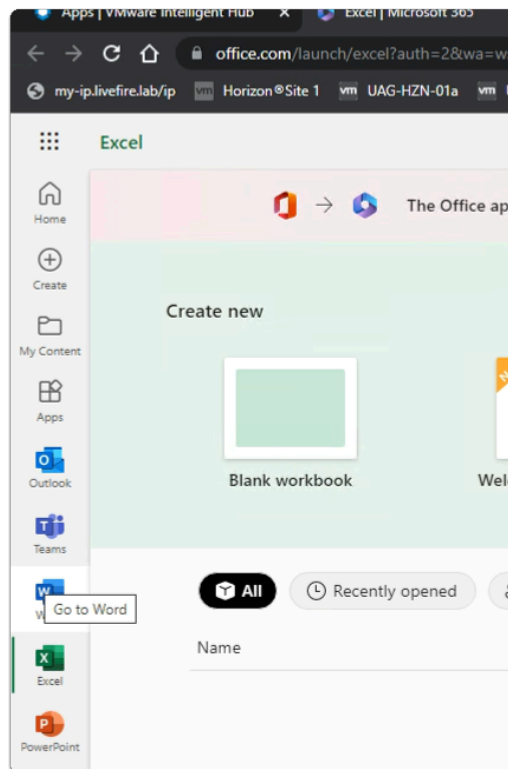
- Select **Apps**



4. In the **web Intelligent Hub**

- Under **Apps**
- Select **Microsoft Excel**

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**



6. 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