

# Federating AZURE with Workspace ONE Access and Office 365 as a service

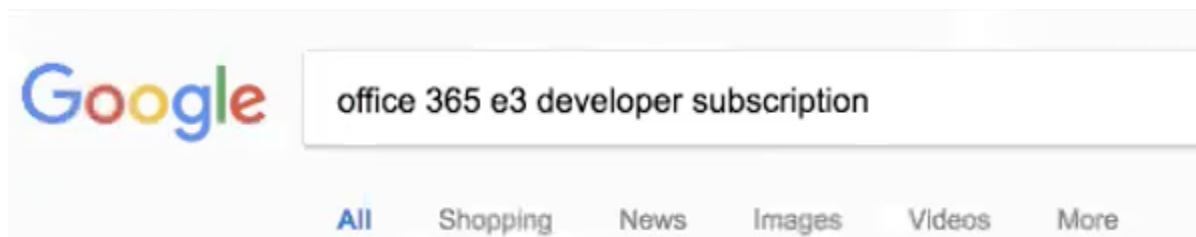
## Part 1: Setting Up a Developer Account

One needs to setup an **Office 365 E3 Developer** subscription account to be able to integrate with Workspace ONE. In this section we will walk through and setup the required developer subscription that allows you a 12 -month free trial.

### An Important NOTE!

- Be sure to take notes and document your configurations immediately.
- Be 100% clear from your document what your assigned domain name is.

1. Open a browser and go to **Google Chrome search engine** and type **office 365 e3 developer subscription**.



2. Find the option that says **Set up an Office 365 developer subscription** and **select**

About 464,000 results (0.32 seconds)

### Microsoft® Office 365™ | Empowering Productivity | office.com

(Ad) products.office.com/Microsoft/Business ▾

★★★★★ Rating for office.com: 4.8 - 1,263 reviews

Includes the Latest Office 2016 Apps! Office 365™ Business-Subscribe Today. Free eBook. Buy

Online. Types: Office 365, Office 2016, Office 365 for Mac, Office 2016 for Mac.

Support Center · Office For Business · Office For Home · Contact Us

### Deploying Office 365? | Avoid Key Mistakes | zscaler.com

(Ad) info.zscaler.com/office-365/deployment ▾

Learn what Microsoft Recommends for a Fast User Experience. Get the Guide. Direct to cloud. Zero

Trust Access. Infinitely Scalable. Redefine Network Security. Secure Remote Access. Always-on

Protection. Reduce Security Costs. Network Transformation. Unmatched Security.

Office 365 Best Practices · Definitive Guide for O365 · Office 365 Deployment



### Set up an Office 365 developer subscription | Microsoft Docs

https://docs.microsoft.com/.../office/developer.../office-365-developer-program-get-st... ▾

19 Mar 2018 - Set up an Office 365 developer subscription to build and test your solutions

independent of your production environment. The subscription is an Office 365 Enterprise E3 Developer subscription with 25 user licenses. It lasts for one year and is free to use for development purposes (coding and testing solutions).

Set up your subscription · Configure the subscription · Provision Office 365 services

3. On the **Set up an Office 365 developer subscription** page under **Set up your subscription** Under ! **Note**

Select the **join the Office 365 Developer Program** hyperlink

#### ⓘ Note

To set up a subscription, you must first **join the Office 365 Developer Program**. After joining, you'll see the option to set up a subscription.



4. On the **Welcome to the Office 365 Developer Program** page select the **Join the Office 365 Developer Program** page



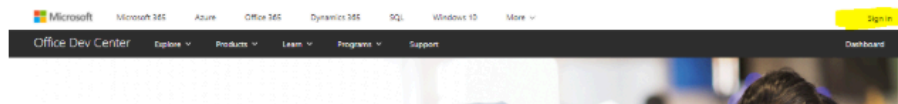
# Welcome to the Office 365 Developer Program

03/20/2018 • 2 minutes to read • Contributors

Join your friends and colleagues in the Office 365 Developer Program. Use the Office 365 developer subscription to develop and test your solutions independent of your production environment. You can build solutions for Microsoft Teams, Office Add-ins, Microsoft Graph, SharePoint Framework, SharePoint Add-ins, and more.

## Join the Office 365 Developer Program

1. Go to the [Join the Office 365 Developer Program](#) page.
2. In the upper-right corner, choose **Sign in** to sign in with your Microsoft account or Azure Active Directory-enabled email.



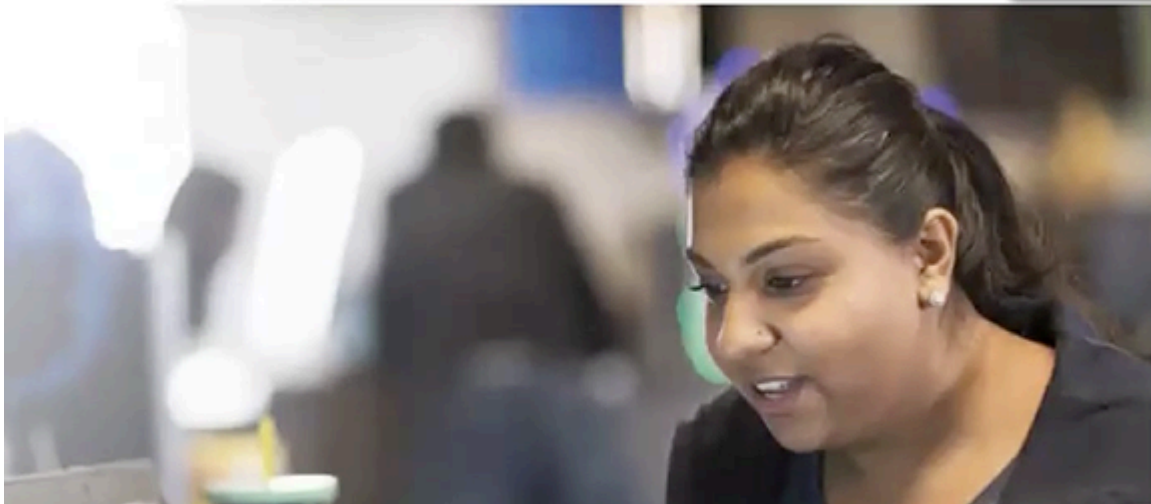
5. You will now be re-directed a 3<sup>rd</sup> time to the **Join the Office 365 developer program today!**  
**Do not select JOIN NOW**

## Join the Office 365 developer program today!

Do not Select!

**JOIN NOW >**

6. To the right of the page first select **Sign In**



7. On **Microsoft Sign in Page** type in the **email address** of an account you own (NB! If this account is already associated with an office 365 account you will have to create a new account)

7.1 Alternatively next to **NO account?** select **Create one!**

7.2 On the **Create account** page type your **custom email address**

7.3 Select **Next**

7.4 On the **Create a password** window type a unique **password** and select **Next**

7.5 On the **Create account** page type in your **country** and **Birthdate** and select **Next**

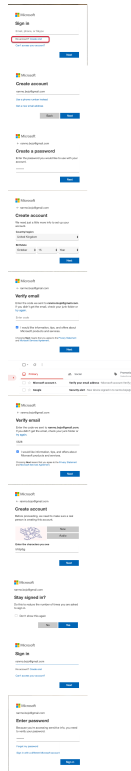
7.6 On the **Verify email** page notice you *need to enter a code*, log into your gmail account and select the email and find the code and then **enter the code** in the **Enter Code** area and select **Next**

7.7 On the **Create account**, page enter the **custom security** letters for your login

7.8 On the **Stay Signed in** page, select **Yes**

7.9 On the **Sign in** page type in your custom **email address** and select **Next**

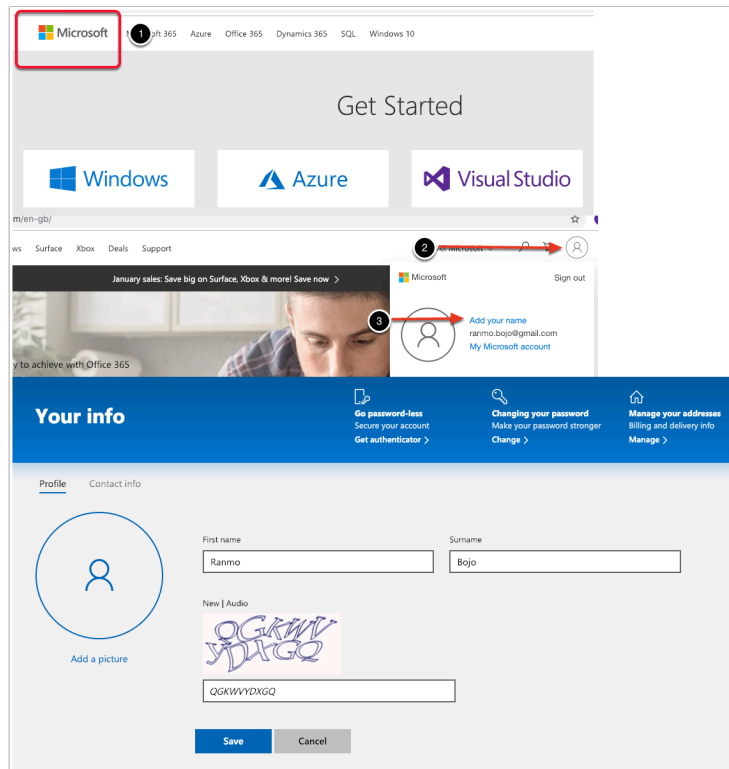
7.10 On the **Enter password** page, type in your **password** and select **Sign in**



8.1 To the left of the page, select the **Microsoft icon**

8.2 Then look to the right of the page and select your **account icon**, next select **Add your name**

8.3 On the **Your info** page under **First name** type your custom **name** and under **Surname** type your custom **Surname**, type in the **matching security letters** and select **Save**



9.0 Open an Incognito browser session with Google Chrome and copy the following url in the Browser address bar,

<https://developer.microsoft.com/en-us/office/dev-program>

9.1 To the right select **Sign In**, On the **Sign In** page type in your **custom email address** and select **Next**

9.2 On the **Enter password** window, type the **custom password** you created and select **Sign in**

9.3 On the **Stay signed in?** window select **Yes**

9.4 On the **Join Office 365 Developer program today** page select **JOIN NOW>**

9.5 On the **Office 365 Developer Program Signup** page select your **Country/Region** and type in the **name of your Company** and select the **two checkboxes** for **terms and conditions** and **information** and select **NEXT**

Join the Office 365 developer program today!

The developer program is designed to help you create intelligent, connected solutions that enable customers and organizations to do more.

**JOIN NOW**

**Office 365 Developer Program Signup**

Welcome to the Office 365 Developer Program!

First Name: Rammo  
Last Name: Bojo  
Email: rammo.bojo@gmail.com

Country/Region: United Kingdom

Company: B2CWorld

☒ I accept the terms and conditions of the Office 365 Developer Program. Note that certain data will be collected from use of the Office 365 Developer subscriptions to help us assess active development of applications as required under this program.

☒ I would like information, tips, and offers about the Office 365 Developer Program.

Please refer to the [privacy statement](#) for more information.

**Next**

10. On the **Office 365 Developer Program Preferences** page select **enough check box and options** to make sure the **Join** button becomes available and the select **JOIN**

## Office 365 Developer Program Preferences

Complete the following fields to help us personalize your experience.

What industry do you work in? \*

Education

What is your primary focus as a developer? \* (Choose only one)

☐ Applications to be sold in market  
☐ Applications for internal use at my company  
☐ Custom solutions for my own customers  
☒ Personal projects

What are you interested in developing? \* (Check all that apply)

☐ Applications to be sold in market  
☐ Applications for internal use at my company  
☐ Custom solutions for my own customers  
☒ Personal projects

What are your areas of interest?

Products (Check all that apply) \*

<input checked="" type="checkbox"/> Access	<input type="checkbox"/> OneNote	<input type="checkbox"/> Publisher
<input checked="" type="checkbox"/> Excel	<input type="checkbox"/> Outlook	<input type="checkbox"/> SharePoint
<input type="checkbox"/> Kaizala	<input type="checkbox"/> Planner	<input type="checkbox"/> Skype
<input type="checkbox"/> Microsoft identity platform	<input type="checkbox"/> PowerApps	<input type="checkbox"/> Skype for Business
<input type="checkbox"/> Microsoft Teams	<input type="checkbox"/> Power BI	<input type="checkbox"/> Visio
<input checked="" type="checkbox"/> Office 365	<input type="checkbox"/> PowerPoint	<input type="checkbox"/> Word
<input type="checkbox"/> OneDrive	<input type="checkbox"/> Project	<input type="checkbox"/> Yammer

Technologies (Check all that apply)

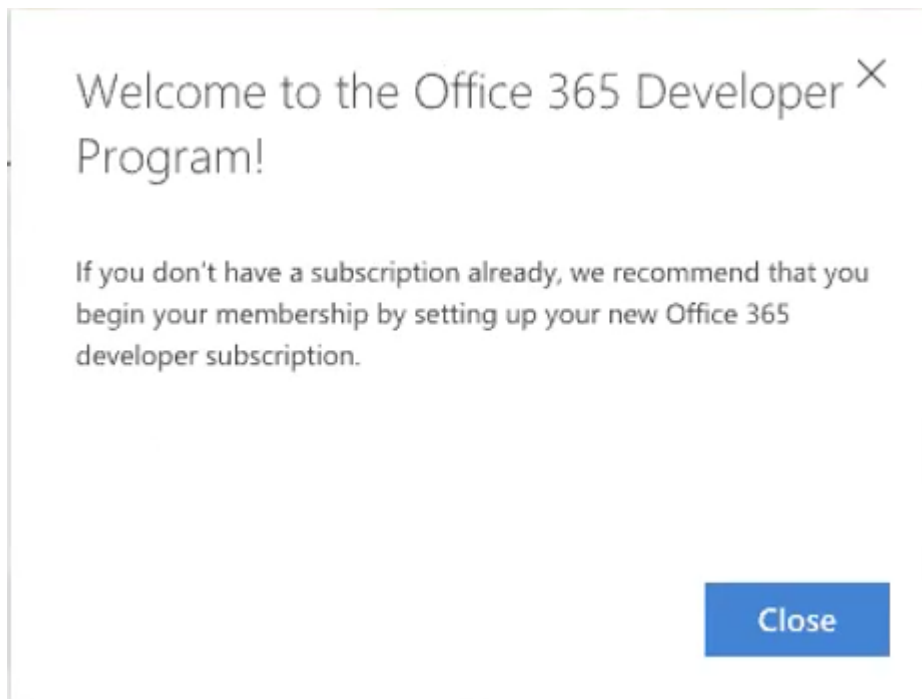
<input type="checkbox"/> Actionable messages	<input type="checkbox"/> Data visualizations	<input type="checkbox"/> OAuth 2.0
<input type="checkbox"/> Add-ins	<input type="checkbox"/> Microsoft Bot Framework	<input type="checkbox"/> SharePoint Framework
<input checked="" type="checkbox"/> Azure AD	<input type="checkbox"/> Microsoft Graph	<input type="checkbox"/> Tabs
<input type="checkbox"/> Connectors	<input type="checkbox"/> Office UI Fabric	<input type="checkbox"/> VBA

Code languages & platforms (Check all that apply)

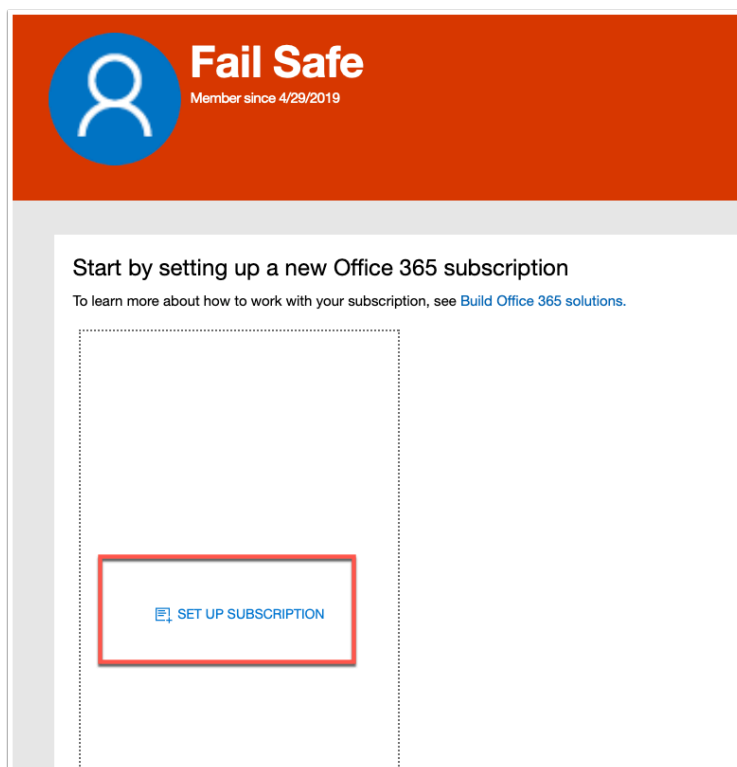
<input checked="" type="checkbox"/> Android	<input type="checkbox"/> JQuery	<input type="checkbox"/> Ruby
<input type="checkbox"/> Angular	<input type="checkbox"/> Knockout	<input type="checkbox"/> Swift
<input type="checkbox"/> AngularJS	<input type="checkbox"/> Node.js	<input type="checkbox"/> TypeScript
<input type="checkbox"/> ASP.NET	<input type="checkbox"/> Objective-C	<input type="checkbox"/> UWP
<input type="checkbox"/> C#	<input type="checkbox"/> PHP	<input type="checkbox"/> VBA
<input type="checkbox"/> HTML	<input type="checkbox"/> PowerShell	<input type="checkbox"/> Visual Basic .NET
<input type="checkbox"/> iOS	<input type="checkbox"/> Python	<input type="checkbox"/> Xamarin
<input type="checkbox"/> Java	<input type="checkbox"/> React	
<input type="checkbox"/> JavaScript	<input type="checkbox"/> REST API	

**PREVIOUS** **JOIN**

11. Close the **Welcome to the Office 365 Developer Program!** Window by selecting **Close**



12. On the **Office 365 Developer** Page select **SET UP SUBSCRIPTION**



13. In the **Setup your developer subscription** window, create a unique admin account , for example, your username could be CloudAdmin and your **Domain** could be your firstname and surname

*NB! Ensure you document these credentials*




14. When you are done select **Continue**

15. On the **Add phone number for security** windows type in your **Country Code** and your **phone number**

16. Select **SEND** code , follow through on the **security picture block** selecting your **relevant pictures**, and select **Next** Enter the Code from your phone and select Set up

The image displays three sequential screenshots of the Office 365 developer subscription setup process. The first screenshot, titled 'Set up your developer subscription', shows a form with fields for 'Country/Region' (set to United Kingdom), 'Username' (CloudAdmin), 'Password', and 'Confirm Password'. It includes a 'Cancel' button and a 'Continue' button. The second screenshot, titled 'Add phone number for security', shows a form for 'Country code' (United Kingdom +44) and 'Phone number' (796361), with a 'Send Code' button and 'Cancel'/'Set up' options. The third screenshot shows a 'security picture block' with a grid of images, including traffic lights, and a 'Next' button. Below this, another 'Add phone number for security' form is shown, but it is partially obscured and less legible than the second one.

17. Once **your** registration is complete you can login in using your new ADMIN account. On the your **Office 365 Subscription** page select and right click the **Go to subscription** hyper link and select **Open Link in New Tab**




**Alex Zohab**  
Member since 4/3/2019

### All your Office 365 developer subscriptions


To learn more about how to work with your subscription, see [Build Office 365 solutions](#).

**alexzohab.onmicrosoft.com**


[Go to subscription](#)

 Subscription

Expires on Apr 3, 2020

 Administrator

cloudadmin@alexzohab.onmicrosoft.com

 Users


25 accounts in total

365

/366

days left

18. On the **Sign In window** , Enter your **password** and select **Sign in**

 Microsoft

cloudadmin@alexzohab.onmicrosoft.com

## Enter password

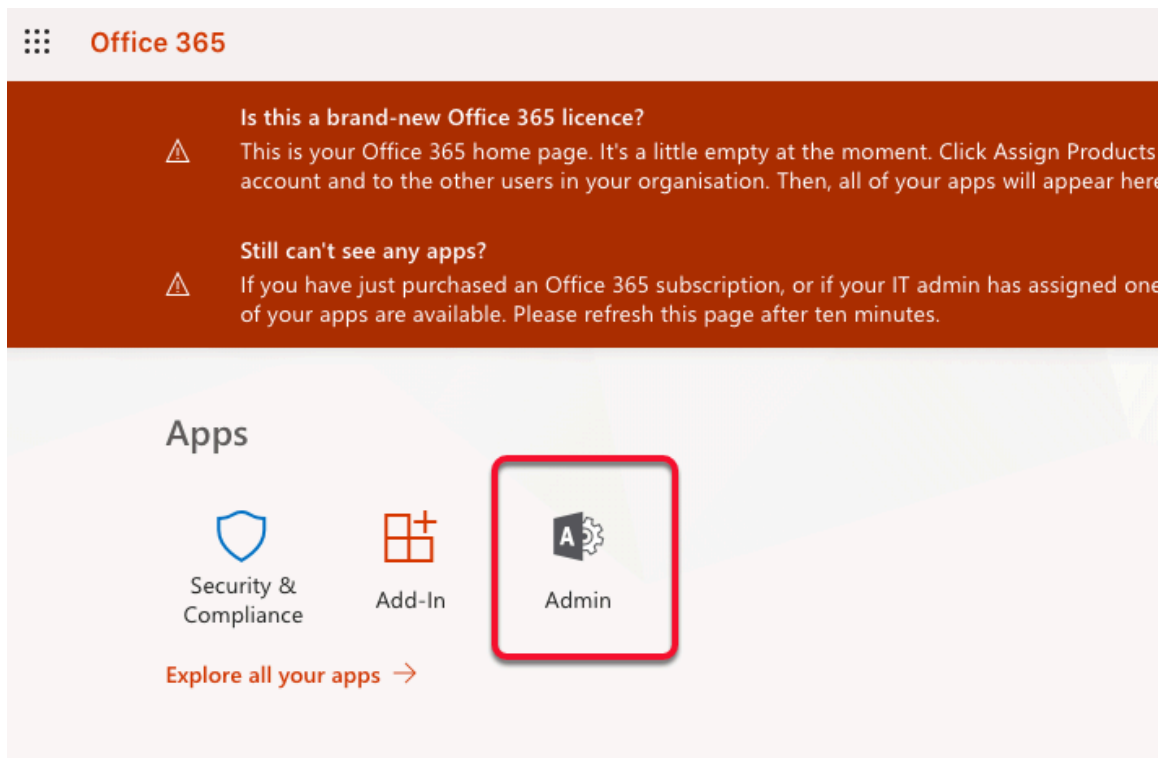
.....

[Forgotten my password](#)

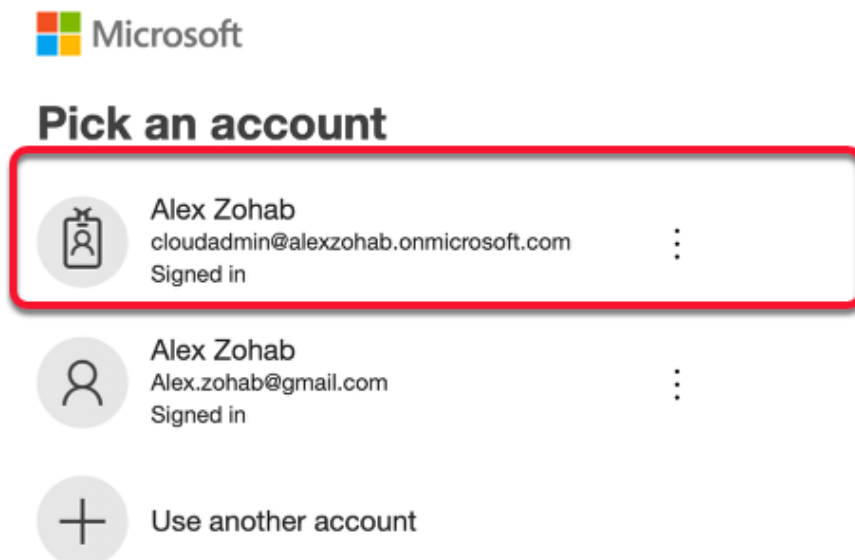
[Sign in with another account](#)

[Sign in](#)

19. On the **Office 365 Page** almost in the middle select **Admin**



20. On the **sign in** page pick your new **CloudAdmin** account



21. If you get prompted with a Welcome to **Office 365 Admin Center** Page select **Skip**

## Welcome to the Office 365 Admin Center

If you are new to Office 365 and administration we highly recommend that you take our quick tour to familiarize yourself with the basics. It takes less than a minute to finish.

Start the tour

Skip

22. Notice the **Office 365 E3 Developer Setup is incomplete**. Select **Go to Setup box**

**Office 365 Enterprise E3 Developer setup is incomplete. Get someone to help you.**

Go to setup

23. **NB!** 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.

For example if this training session was being delivered in Atlanta , your domain name might be **atlanta01.euc-livewire.com** for **student number 1**. If we have 18 attendees there will be 18 different registered Domain names using the above mentioned naming convention. we have automated the dns configuration for this lab, so we will use a **vrealize automation self service portal** to configure your dns zone.

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** (this example in the screenshot is only for demo purposes) select **Next**

**!** Note when registering your own domain name with Office 365, there are several approaches. The most seamless and trouble free approach is to register your own Domain Name with GODADDY. This provides a seamless experience and the verification takes seconds once you have your own domain name from GODADDY. GODADDY is an example of a name provider that seamlessly integrates with Microsoft's Office 365. If one chose this option your name that you use would belong to you for however long you choose to use your Office 365 Tenant

Another approach is to do this manually. EUC Livefire already owns a domain name which is hosted in AWS Route53. In the Office 365 setup wizard you will notice there is a step by step guide on how to setup your zone in AWS Route53 manually. We have chosen to automate this process for the sake of time.

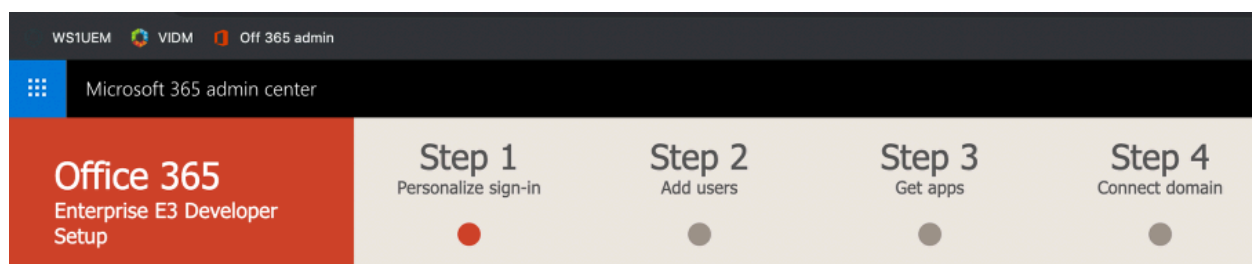
If you choose this option the zone provided to you by Livefire associated with your tenant will possibly only be active for a maximum of a month and you will then have to find your own Domain name.

If you choose to follow the Livefire option, we have automated this process for your convenience using VMware VRA. Generally DNS name configuration in AWS Area 53 is a completely Manual process. We have automated more than 98% of this process. You will however interface with VMware vRealize Automation for 2 configurations.

1. **MS record** modification

2. **MX record** modification

You do not have Access to AWS AREA53. You will be using VMware vRealize Automation to facilitate the edit of these records



## Personalize your sign-in and email

The domain you choose will become the part of your email address that comes after the @ symbol. You and your staff will use it to sign in and it's how cu

☒ Connect a domain you already own.

atlanta01.euc-livefire.com

[What's a domain and why do you need one?](#)

Your users' email addresses will look like this: username@atlanta01.euc-livefire.com

☐ Continue using alexzohab.onmicrosoft.com for email and signing in.

[Why would you use this domain?](#)

**Next** >

[Exit and continue later](#)

24. On the **Verify domain** page notice there are step-by-step instructions to follow,

Notice that there are DNS records called **TXT name**, **TXT value** and **TTL**

- Note!. We have our Hosted DNS service in called AREA53 on AWS. We have our own euc-livfire.com Zone. Each of you have your own registered Zone Database, that is part of the EUC-Livfire.com namespace. eg. Tokyo01.euc-livfire.com. Your Office 365 instance will need to be verified with this namespace .To do this will require to modify your DNS subzone, working with the vrealize automation portal in a different browser tab while your doing your o365 tenant.
  1. Click on the **copy** icon next to your MS record
  2. Select **Verify** at the bottom of the screen

***NB! At this point ignore any error messages !***

## Verify domain 1

To verify that you own this domain, add this DNS record to your domain (only the domain owner can do this).  
Don't worry, adding this record won't affect your existing email or other services and it can safely be removed at the end of setup.

Follow these [step-by-step instructions](#) → to create a new DNS record using the values below at [Amazon Web Services \(AWS\)](#) →. (Not your DNS host? [↗](#))

**TXT name:** [tokyo01](#)

**TXT value:** [MS=ms35097303](#)

**TTL:** [3600](#) or your provider default.

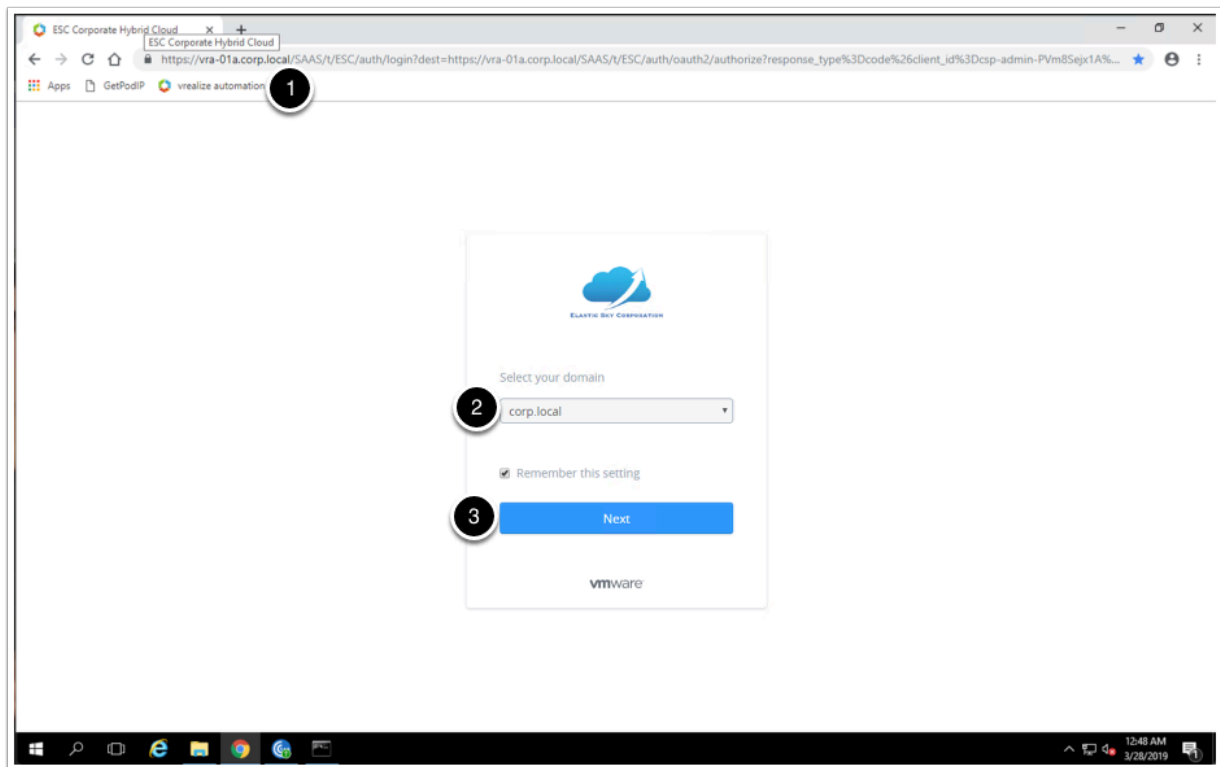
[Get someone to help you.](#) Let us help you set up your TXT records.

Or, add an MX record to verify ownership instead.

[Back](#)
[Verify](#)
[Exit and continue later](#)

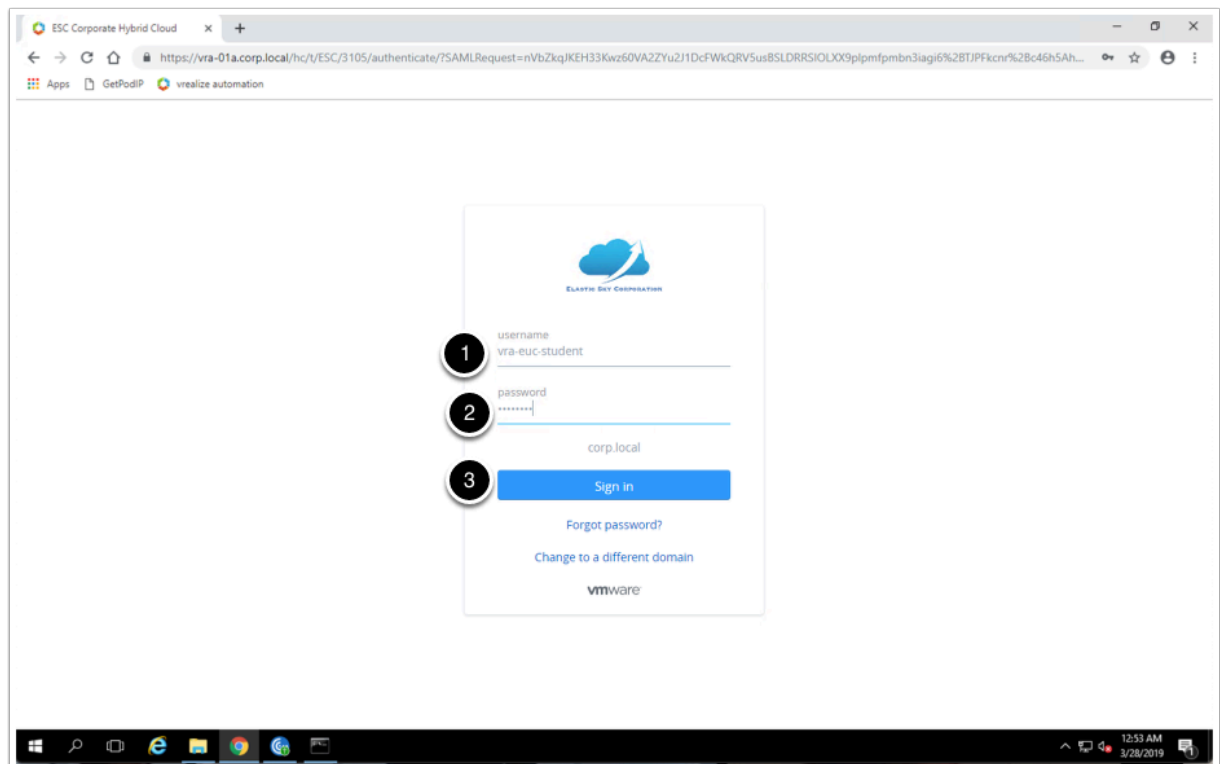
25

- On your **Controlcenter2 desktop**, from your task bar open your **FireFox Browser**
  1. Next to the bookmarks bar open **vrealize automation**
  2. Next to the "Select your domain" dropdown menu select **corp.local**
  3. Select **Next**



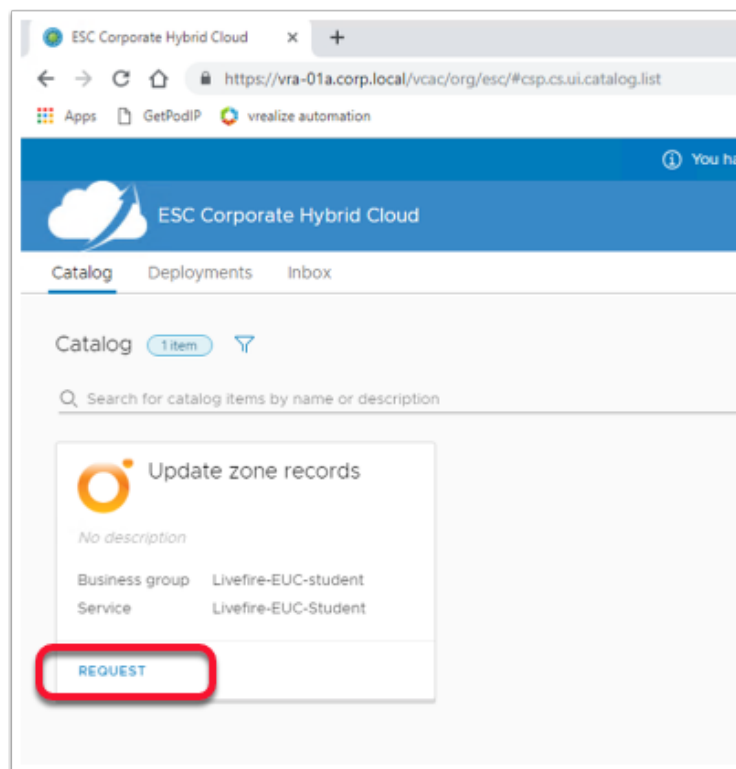
26.

- VRA automation continued ...
  1. In the **username** field type **vra-euc-student**
  2. In the **password** field type **VMware1!**
  3. select **Sign in**



## 27. VRA automation continued ...

- In the **update zone records** catalog object, select **Request**



## 27.

- VRA automation continued ...
  1. Next to **zone prefix** dropdown menu select the **city corresponding to your current location**.
  2. Next to **zone number** drop down menu select **your dns zone number** as described in your information sheet
  3. Under **Records update** next to **MS record** replace the existing record your MS record and Paste your **MS record**,  
NOTE ensure that your MS record is enclosed in Quotation Marks
  4. Select **Submit**



Catalog Deployments Inbox

Update zone records | Business group Livefire-EUC-student

**Zone selection**

\* Zone prefix: madrid 1

\* Zone number: 35 2

**Records update**

\* MS record: MS=ms78072832 3

\* MX record: 0 madrid35-euclivefire-com02i.mail.protection.outlook.com.

SUBMIT CANCEL 4

28. Wait until the progress shows 100% and continue with your lab. you might need to refresh your browser if you see no progress bar.

ESC Corporate Hybrid Cloud

Deployments 2 items

Search for deployments by name, description, IP address, resource name or machine status | Sort: Created Date (descending)


Update zone records	#129 - Workflow Execution Update zone records - Successful	100%	ACTIONS
No description Owner: vra EUC student Business group: Livefire-EUC-student	The request was successfully completed		4 minutes since submitted


29 .Go back to your o365 domain configuration and click on **verify**. it might give you an error because of the time it takes to replicate DNS configurations and it might require you to click on verify a couple more times.


## Verify domain

To verify that you own this domain, add this DNS record to your domain (only the domain owner can do this).  
Don't worry, adding this record won't affect your existing email or other services and it can safely be removed at the end of setup.

Follow these [step-by-step instructions](#) → to create a new DNS record using the values below at [Amazon Web Services \(AWS\)](#) →. (Not your DNS host? [↗](#))

**TXT name:**  tokyo01

**TXT value:**  MS=ms35097303

**TTL:**  3600 or your provider default.

[Get someone to help you.](#) Let us help you set up your TXT records.

[Or, add an MX record to verify ownership instead.](#)

[Back](#) **Verify**  [Exit and continue later](#)

30. On **Add new users** window select **Got it, thanks**, select **Next**

## Add new users

We detect that an email provider is already associated with atlanta01.euc-liv stop.

[Got it, thanks](#)

### Add new users

We'll assign a Office 365 Enterprise E3 Developer license to each user you add here. When you're done, we'll give you the sign-in information to share with the users.

[What happens if you don't do this now?](#)

You have 25 of 25 license(s) available. [View all users.](#)

First name	Last name	User name
<input type="text"/>	<input type="text"/>	<input type="text"/> @tokyo01.euc-livfire.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @tokyo01.euc-livfire.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @tokyo01.euc-livfire.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @tokyo01.euc-livfire.com
<input type="text"/>	<input type="text"/>	<input type="text"/> @tokyo01.euc-livfire.com

25 license(s) available

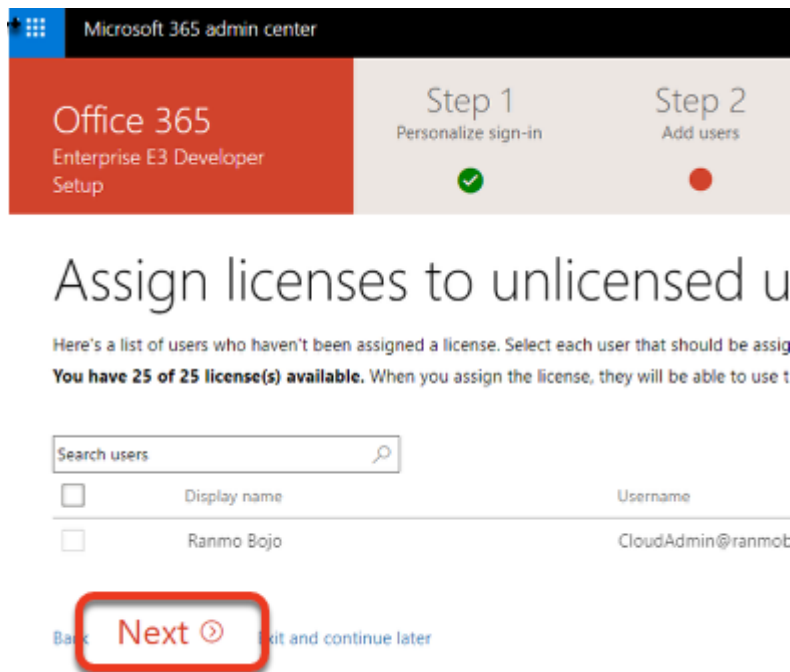
[+ Add another user](#)

☒ Send password for new users to my email

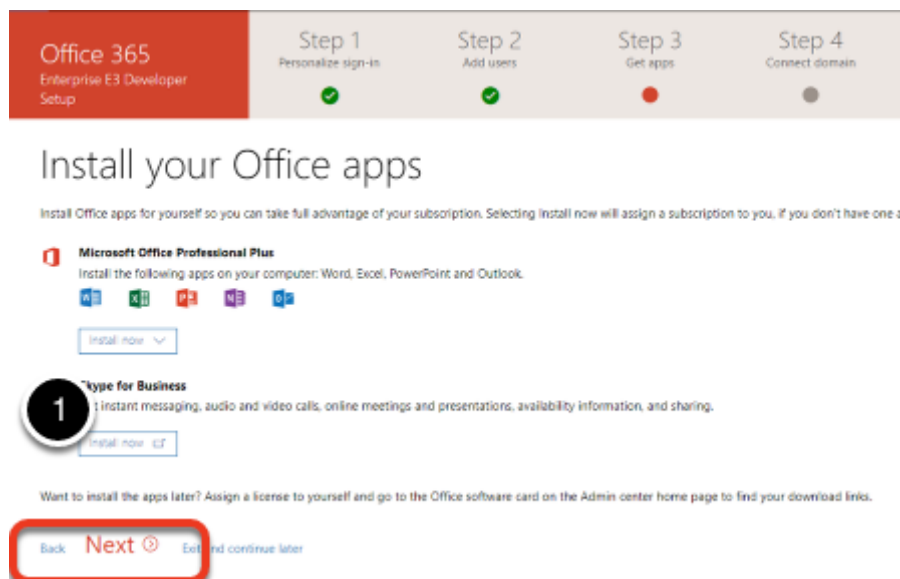
You can add more users anytime in the Office 365 admin center.

[Back](#) **Next**  [Exit and continue later](#)

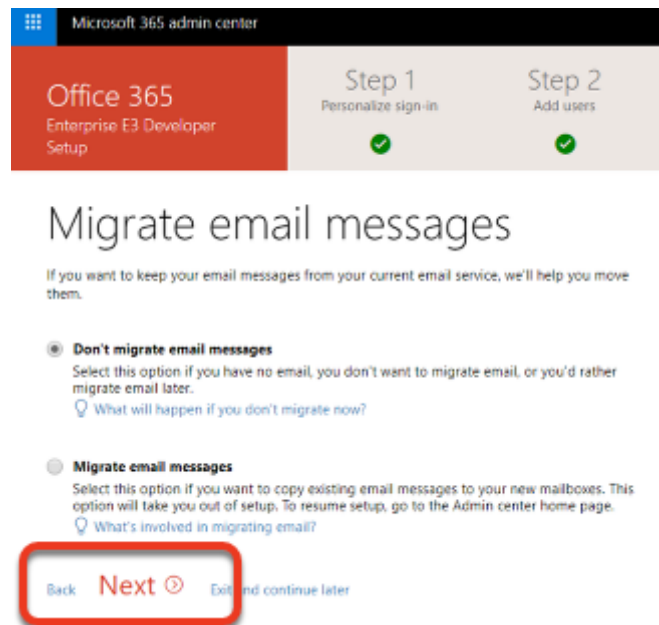
31. On the **Assign licenses to unlicensed users** page select **Next**



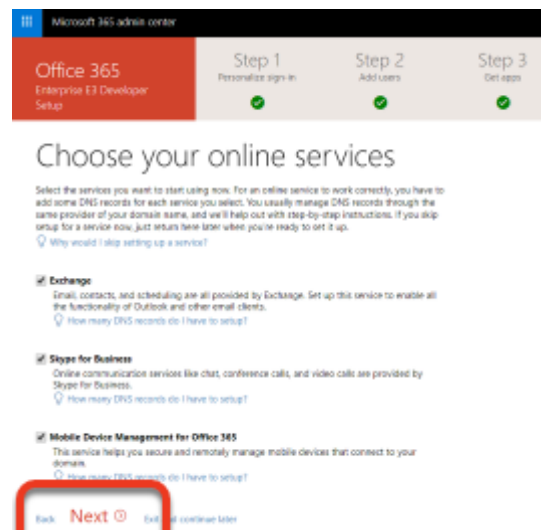
32. On **Install your Office apps** page select **Next**



33. On the **Migrate email messages** page leave the default **Don't migrate email messages** radio button and select **Next**

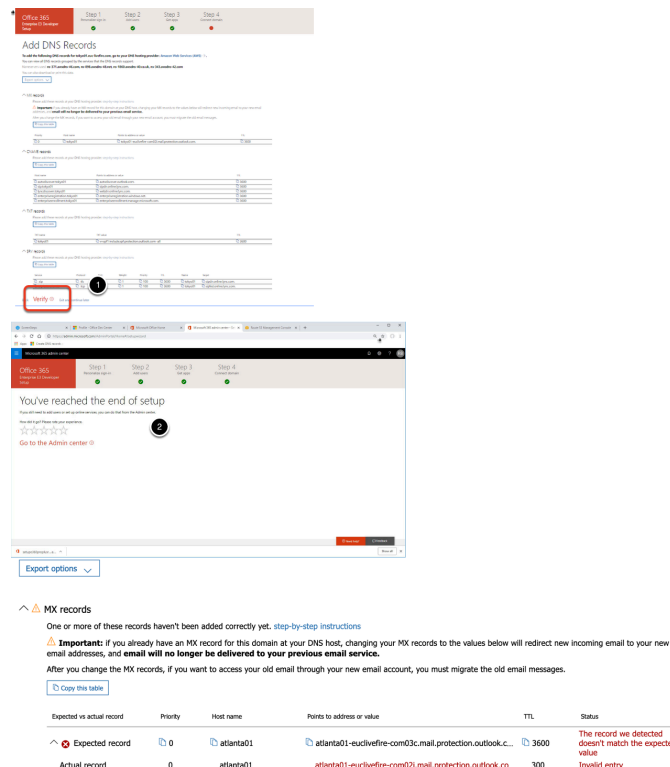


34. On the **Choose your online services** page, ensure that **Exchange, Skype for Business** and **Mobile Device Management for Office 365 checkboxes** are selected and select **Next**



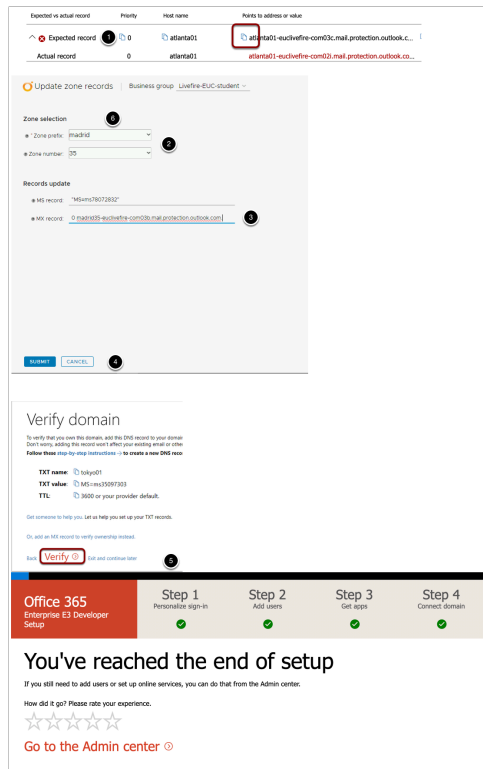
35.

- On the **Add DNS Records** page.
  1. When ready select **Verify** at the bottom of the **Add DNS Records** window. If there is a failure on any records reach out to the EUC-livefire instructor team to get the records fixed and select **Verify** again. Note you might have to give a few minutes for the records to update in DNS before selecting **Verify**
  2. Notice that when **Verify** is successful the **you just configured your Office 365 Tenant successfully** will show and you are ask to provide feedback related to your experience.
- However, If Verify is Not successful and its MX related in the message go to the next step in this exercise.



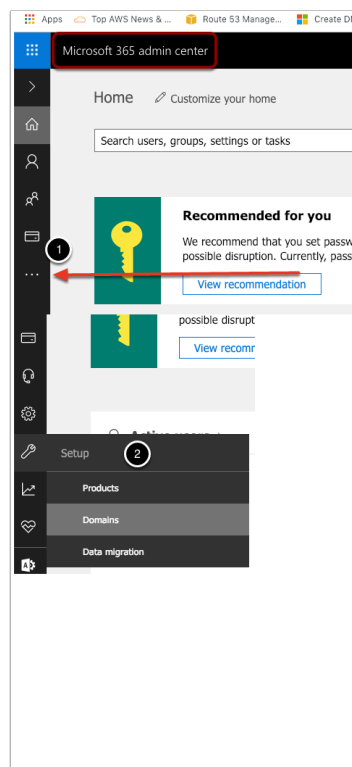
36

- If you get an error mentioning your **MX records** follow these steps:
  - Click on the the **copy** icon next to **Expected record**
  - On your **ControlCenter2** server, Go back to the **update zone records tool**, select **REQUEST**
  - Get to your zone and paste the **MX records**,
    - NOTE the example, there is a zero in front MX record, this is a priority field and should not be deleted.
  - Select **SUBMIT**
  - Go to your 0365 domain configuration and **Verify** the domain again.
  - You should get a message saying You've reached the end of the setup



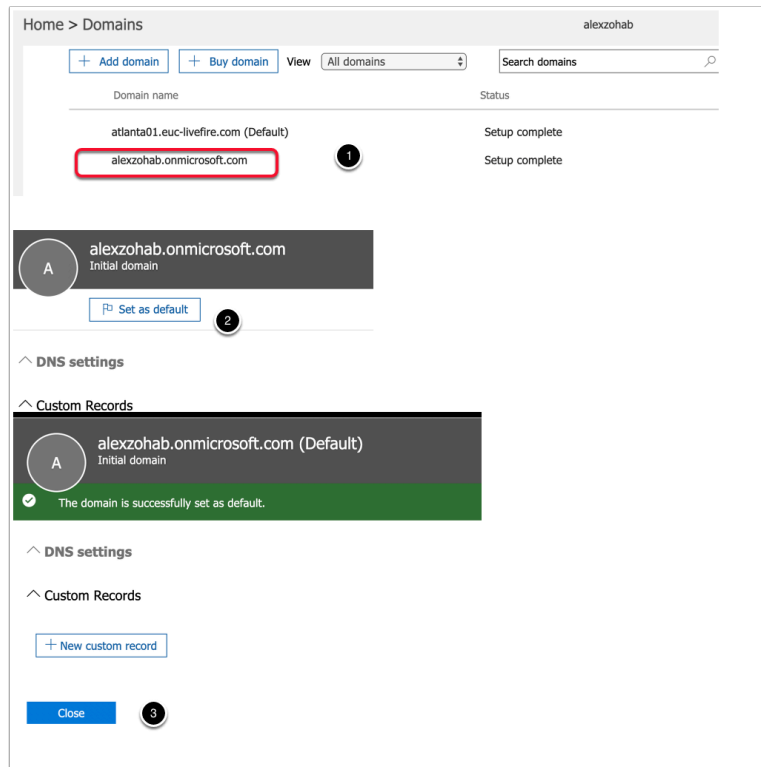
37. Select **Microsoft 365 Admin center** next to the **9 dot blue square** in the top left corner.

- In your Microsoft 365 Admin center,
  1. Select the 3 parallel dots in the black bar to the left of the console, this will expand the console
  2. Select the **Spanner** icon for **Setup** and select **Domains**



38.

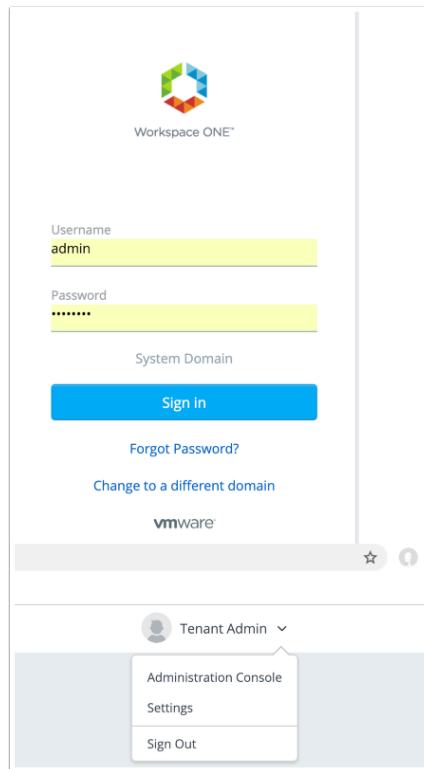
- In the **Home > Domains** interface, check to see if your namespace you have associated with your Office 365 setup has a **(Default)** next to it. If this is the case do the following.
  1. Select your **account name** that is not set to default :
  2. Select **Set as default**
  3. Your custom domain cannot be the default domain when federating with Workspace ONE Access. Select **Close**. Check to see that you have a corresponding configuration in the domain portion of your setup as the screenshot.



## Part 2: Federating Office 365 with Workspace ONE Access.

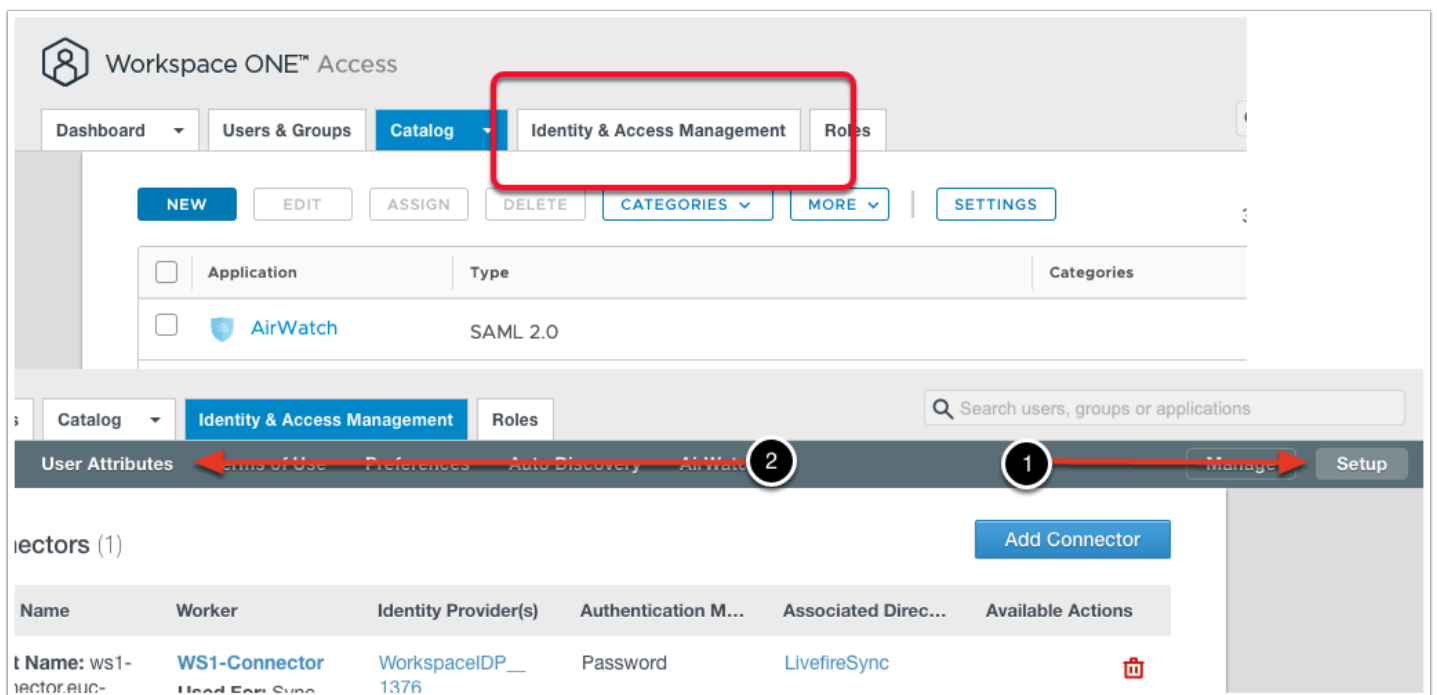
In Part 2 of this lab session we will now federate our Office 365 Tenant with a Workspace ONE Access SAAS tenant.

1. Using your **Tenant Admin** credentials, login into your **SAAS Workspace ONE Access** Tenant.
  1. To the right of the **Workspace ONE Access** console under **Tenant Admin** select **Administration Console**



2. Select the **Identity & Access Management** tab

- To the right in the **Identity & Access Management** tab select **Setup > User Attributes**



3. In the **User Attributes** interface notice you have already set **userPrincipalName** and **distinguishedName** to **Required** and you have already created the **objectGUID** attribute.



These are pre-req requirements for Federating Office 365 with Workspace ONE Access.

Attribute	Selected
disabled	<input type="checkbox"/>
distinguishedName	<input checked="" type="checkbox"/>
domain	<input type="checkbox"/>
email	<input checked="" type="checkbox"/>
employeeID	<input type="checkbox"/>
firstName	<input checked="" type="checkbox"/>
lastName	<input checked="" type="checkbox"/>
mfaId	<input type="checkbox"/>
mfaPhoneNumber	<input type="checkbox"/>
phone	<input type="checkbox"/>
userName	<input checked="" type="checkbox"/>
userPhotoChecksum	<input type="checkbox"/>
userPrincipalName	<input checked="" type="checkbox"/>

o Add other attributes to sync to the directory. Go to the directory's attributes page to map these attributes.

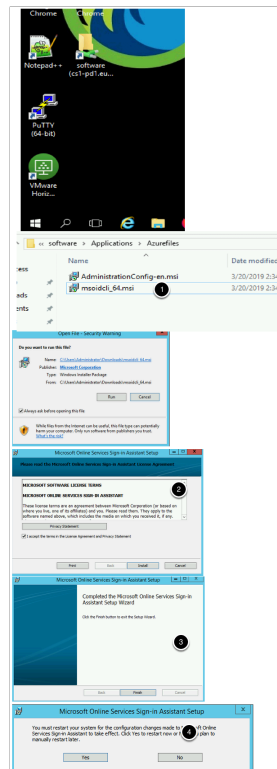
Attributes +

objectGUID ✖ +

Save

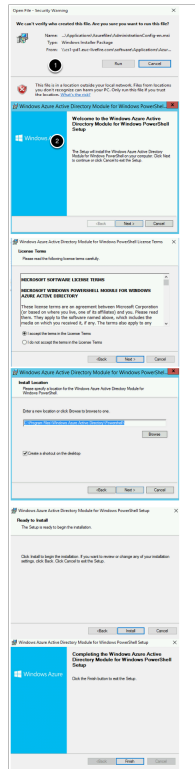
4.

- On your **ControlCenter2** desktop server select your **Software** shortcut and open the path to the **Applications** folder. In the **Applications** folder open the **Azurefiles** folder.
  - Open** the **msoidcli\_64.msi** installer and when prompted select **Run**
  - On the **Microsoft Online Services Sign-in Assistant Setup** page select the **I accept the terms in the Licence agreement...** **checkbox**. Select **Install**,
  - When the installer is done select **Finish**
  - If** prompted to **restart** then do so and login as administrator



5.

- Under the same **Azurefiles** folder,
  1. Select and launch the **AdministrationConfig-en.msi** , select **Run**. On the **Open File - Security Warning** window select **Run**
  2. On the **Windows Azure Active Directory Module for Windows Powershell Setup** window select **Next**
  3. On the **License Terms** window , ensure the **I accept the terms** **radio button** is selected and select **Next**
  4. On the **Install Location** window, select **Next**
  5. On the **Ready to Install** window select **Install**
  6. Select **Finish**



6.

- On your **ControlCenter** server desktop, you will notice a **Windows Azure Active Directory for Powershell** Shortcut.
  - Right click the **Windows Powershell** and select **Run as administrator**
  - For your convenience we have added all the powershell commands to a TXT file that is available in the software folder on the desktop. You can copy the commands from the file directly into the powershell. **Please note some of the commands require editing**
  - Simply browse to **\\cs1-pd1.euc-livewire.com\software\Applications\Azurefiles** where you will find the file **powershell commands.txt**
  - In the Powershell Console type the following

```
Connect-MsolService
```

- When prompted for **User name** and **Password**, use your Cloud Admin account e.g. **cloudadmin@ranmobojo.onmicrosoft.com**
- Next we have to create a Service Principal account type in the powershell

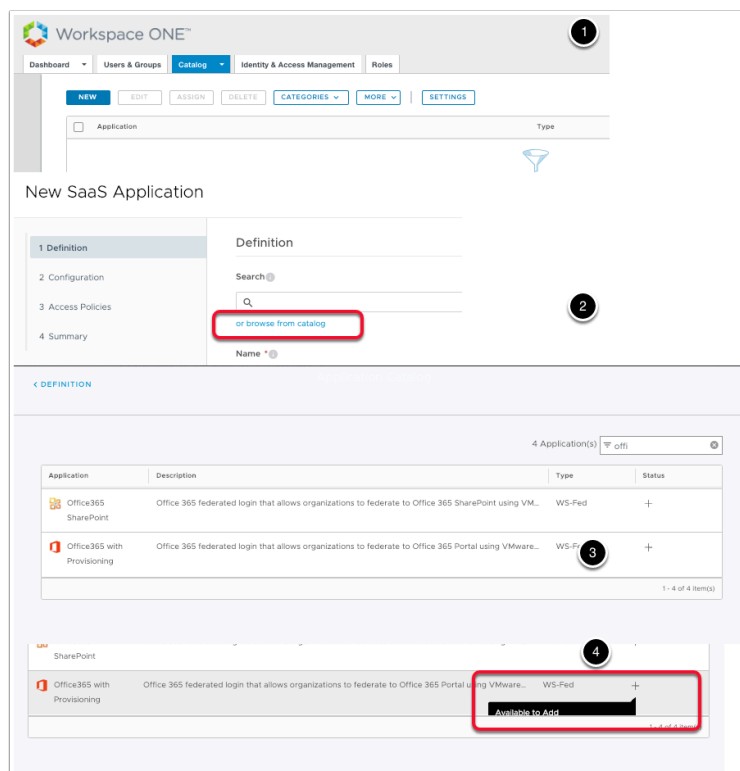
```
$sp = New-MSOLServicePrincipal -DisplayName 'ServPrinc1' -Type password -Value 'VMware1!'
```

- Next we are going to assign a role to the ServPrinc1 user

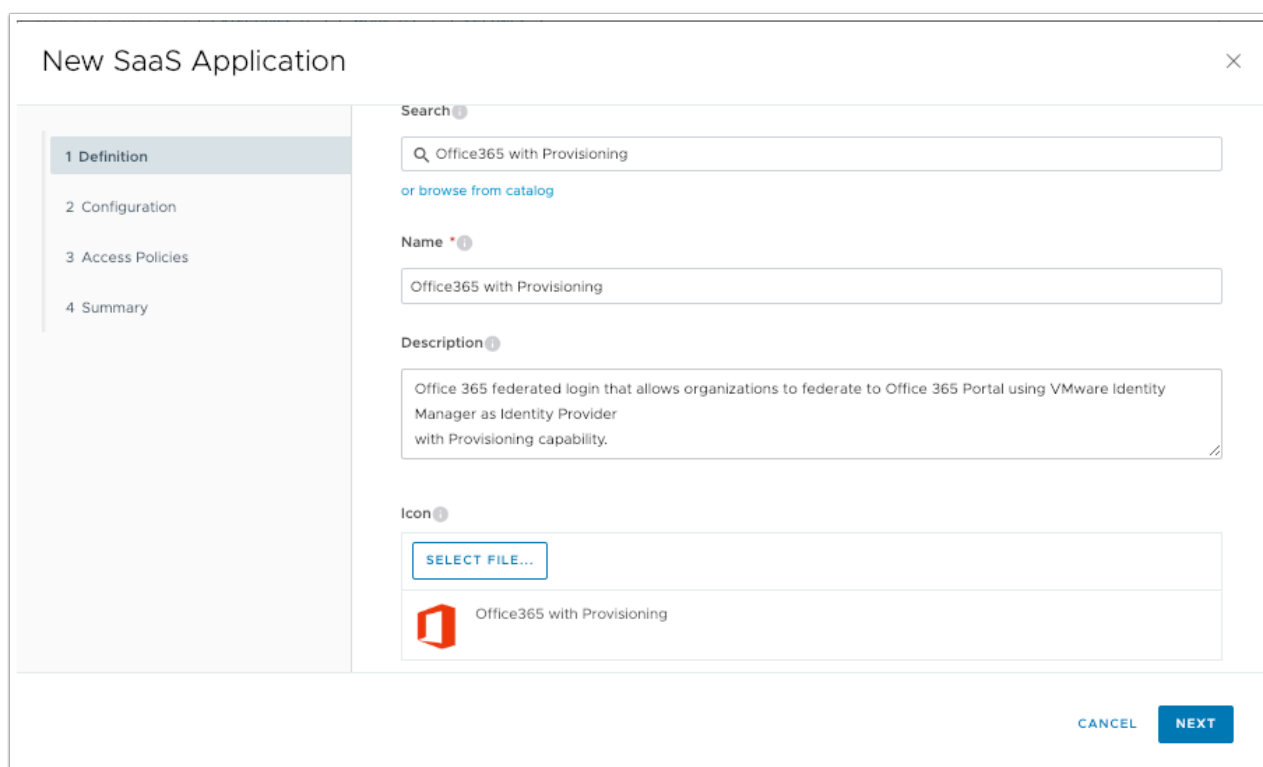
```
Add-MsolRoleMember -RoleName 'User Account Administrator' -RoleMemberType ServicePrincipal -RoleMemberObjectId $sp.ObjectId
```



4. Select **Office365 with Provisioning** by selecting the **+** sign to the right



8 On the New SAAS Application window select **Next**



9. In the **New SaaS Application** window, in the **Configuration** section add the following:

- Under **Target URL** add the following. Actual text to copy to edit into the configuration is in **BLUE**
- **edit the last area** after hint=  
.....[domain\\_hint=tokyo01.euc-livewire.com](https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&domain_hint=tokyo01.euc-livewire.com)


```
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&domain_hint=tokyo01.euc-livewire.com
```

**Target URL**

[https://login.microsoftonline.com/common/oauth2/authorize?client\\_id=00000002-0000-0ff1-ce00-000000000000](https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000)

**Target URL**

[scope=openid+profile&redirect\\_uri=https%3a%2f%2foutlook.office365.com&domain\\_hint=tokyo01.euc-livewire.com](https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&response_type=code+id_token&scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&domain_hint=tokyo01.euc-livewire.com)

**Single Sign-On URL** 

10

- In the **New SaaS Application** window, in the **Configuration** section leave the following default:

**-Single Sign-On URL / Application ID / Username Format / Username Value**

1. Add the following: under **Application Parameters** in the **tenant** line under **Value** add **YOUR** custom Fully Qualified Domain Name ie [tokyo01.euc-livewire.com](https://login.microsoftonline.com/tokyo01.euc-livewire.com)
2. Under **Application Parameters** in the **issuer** line under **Value** add your custom domain name (without the .com part) ie [tokyo01.euc-livewire](https://login.microsoftonline.com/tokyo01.euc-livewire)

**Make sure there are no hidden carriage returns if you paste this in**

**Edit SaaS Application** ×

1 Definition


**2 Configuration** 1

3 Access Policies 2

4 Summary

**Application Parameters**

Name	Description	Default Value	Value
tenant	Office 365 Domain		<a href="https://login.microsoftonline.com/tokyo01.euc-livewire.com">sanjose33.euc-livewire.cc</a>
issuer	Office 365 issuer URI		<a href="https://login.microsoftonline.com/tokyo01.euc-livewire">sanjose33.euc-livewire</a>

[Advanced Properties](#) 

11. In the **New SaaS Application** window, in the **Configuration** section under **Advanced Properties** **leave the following default:**

**-Enable Multiple O365 Email Domains / Credential Verification / Signature Algorithm / Digest Algorithm / Assertion Time**

-Under Custom Attribute Mapping in the *UPN* and *ImmutableID* keep the values default

- In the **New SaaS Application** window, in the **Access Policies** section select **NEXT**

.

The screenshot shows the 'New SaaS Application' window with the 'Access Policies' section selected. The left sidebar contains four steps: 1 Definition, 2 Configuration, 3 Access Policies (highlighted), and 4 Summary. The main content area is titled 'Access Policies' and includes a description: 'Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.' Below this is a dropdown menu showing 'default\_access\_policy\_set'. A section titled 'Client Access Policies for Username/Password Clients' explains that these policies apply to Office 365 clients using username and password authentication. A warning box states: 'These client access policy apply to all WS-Fed Web (Office 365) applications configured in the catalog. Creating a new rule or editing an existing rule impacts all users that access any of these apps.' Below the warning is a table with columns: Clients, Network Range, Device Type, Groups, and Action. At the bottom of the table is a dashed box with a plus icon and the text 'ADD POLICY RULE'. At the bottom right of the window are three buttons: CANCEL, BACK, and NEXT (highlighted in blue).

12. In the **New SaaS Application** window, in the **Summary** section select **SAVE**

New SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Summary

Definition


Name

Office365 with Provisioning

Description

Office 365 federated login that allows organizations to federate to Office 365 Portal using VMware Identity Manager as Identity Provider with Provisioning capability.

Icon



Categories

—

Configuration

Authentication Type

WSFed 1.2

Single Sign-On URL

https://login.microsoftonline.com/login.crf

CANCEL

BACK

SAVE & ASSIGN

SAVE

13

- We will now do the Entitlement configuration of the User
  - In the **Catalog** for Web Apps select the **Office 365 with Provisioning** and select **Assign**
  - In the **Assign** wizard type **Mark** in the **search area** under **Users / User Groups**, select **Marketing@euc-livewire.com**
  - Under **Deployment Type**, select the **drop down arrow** change the **Deployment Type** to **Automatic**
  - In the **Assign** wizard, review your configuration, in the bottom right hand corner select **SAVE**



NEW EDIT **ASSIGN** DELETE CATEGORIES 1

Application

Office365 with Provisioning

Selected App(s): Office365 with Provisioning

Users / User Groups

Q mark 2

Marketing@euc-livewire.com

No

Selected Users / User Groups

Marketing@euc-livewire.com

Deployment Type 3

Automatic

Assign

Selected App(s): Office365 with Provisioning

Users / User Groups

Q Search for Users or Groups

Selected Users / User Groups

Marketing@euc-livewire.com

Deployment Type

Automatic

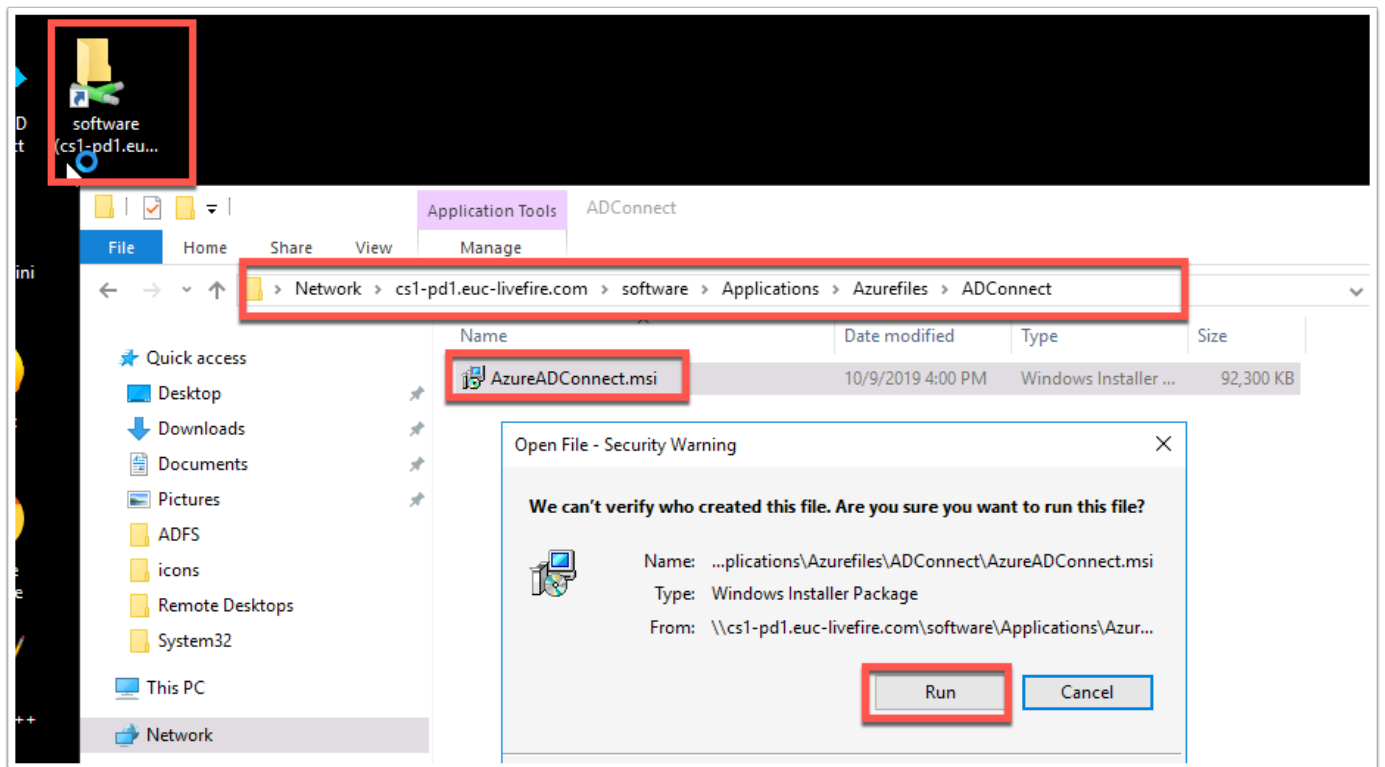
4 SAVE

## Part 3: Using Azure ADconnect for user provision to Azure AD

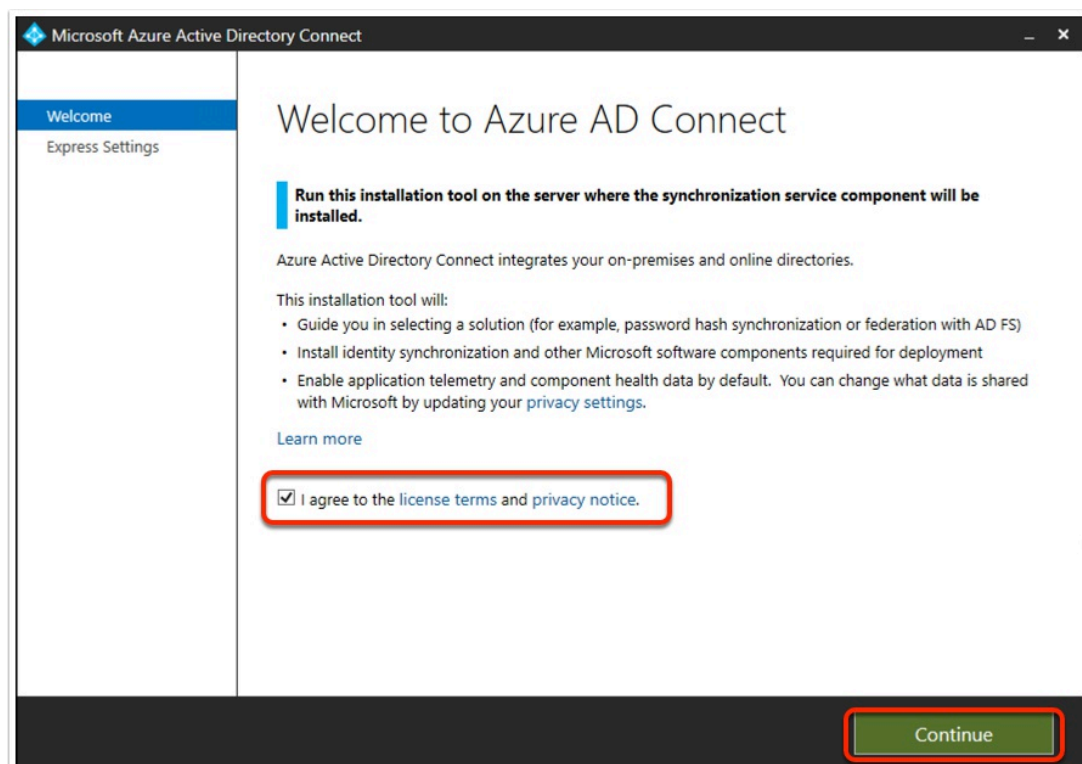
In this part we are going to install Azure AD Connect tool to provision users to Azure AD from on-premise Active Directory.

Please note: It is best practice to use Azure AD connect tool but not a requirement. You can also provision users to Azure AD from Workspace ONE Access using Office365 with Provision application with Setup Provisioning ENABLED.

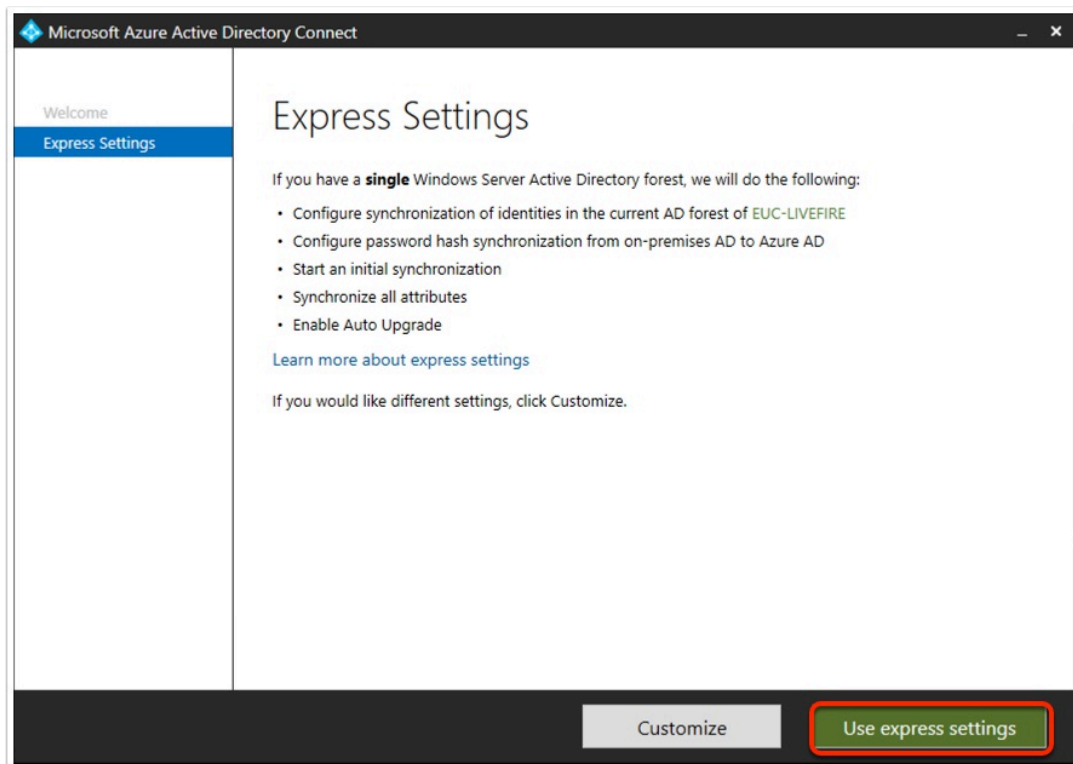
1. From your **Controlcenter** machine desktop, open the **Software** shortcut on your desktop and navigate to the **Applications > Azurefiles > ADconnect** folder.
2. Double-click on **AzureADConnect.msi** and click **run** on the security warning



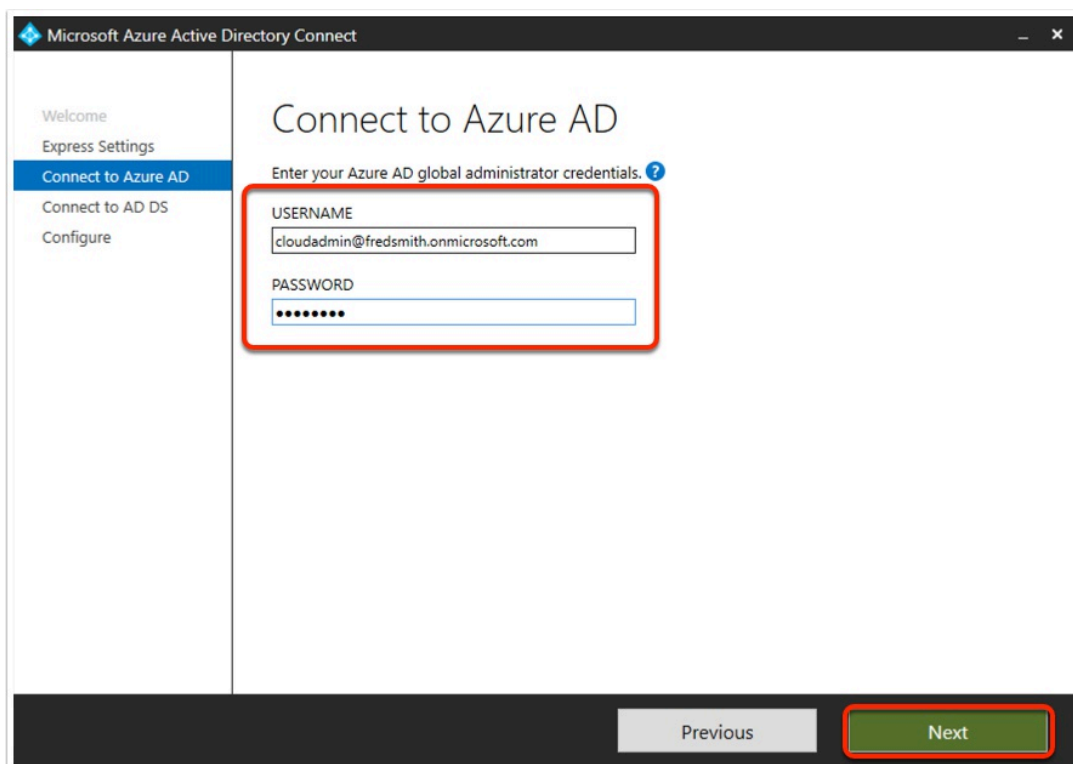
3. On the **Welcome to Azure AD Connect** window check the box next to **"I agree to the license terms and privacy notice"** and click **Continue**



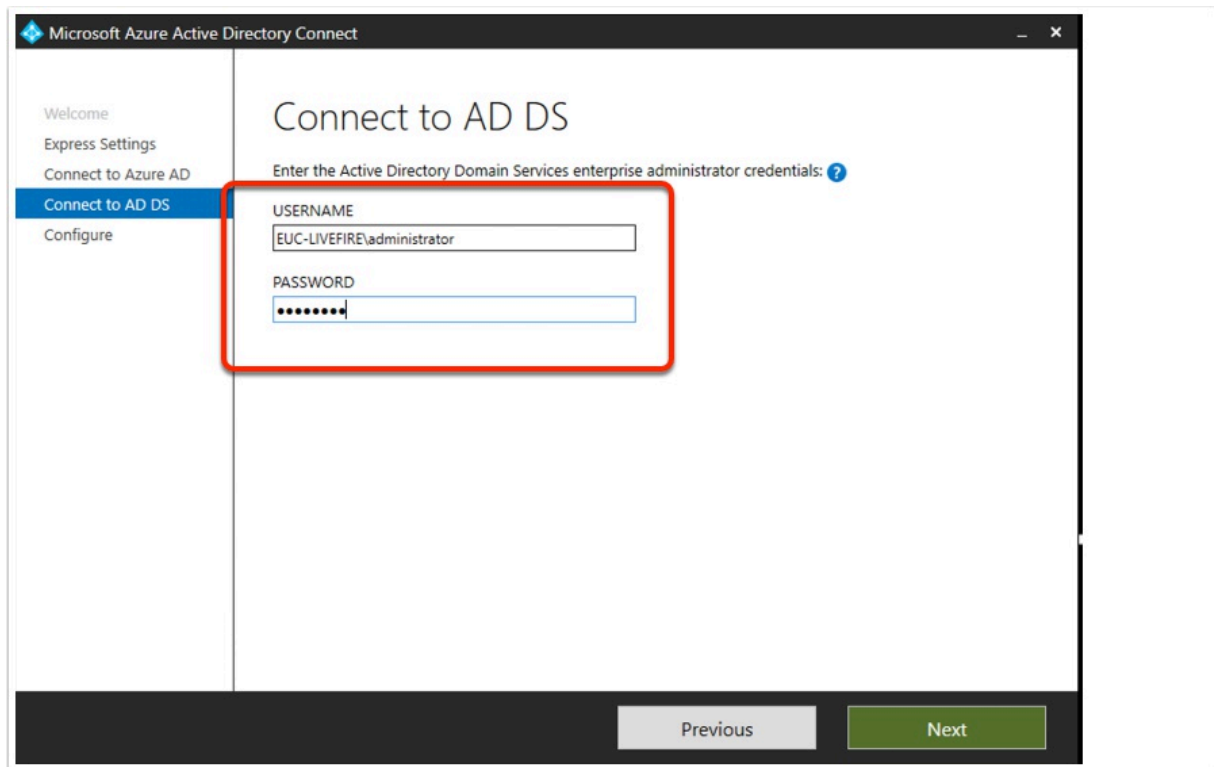
4. In the **Express Settings** window click on **"Use express settings"**



5. On the "**Connect to Azure AD**" window, **fill in your credentials** for your microsoft account and click **Next**

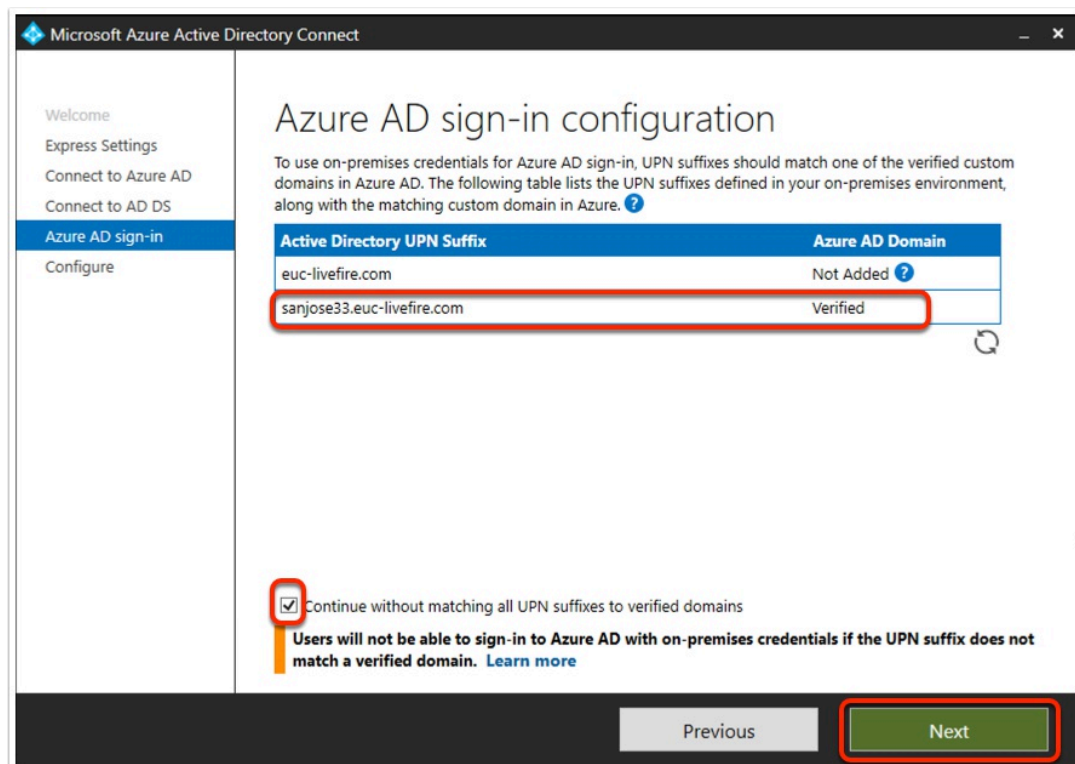


6. In the "**Connect to AD DS**" window fill in your domain credentials, **USERNAME:** EUC-LIVEFIRE\ADMINISTRATOR, **PASSWORD:** VMware1!

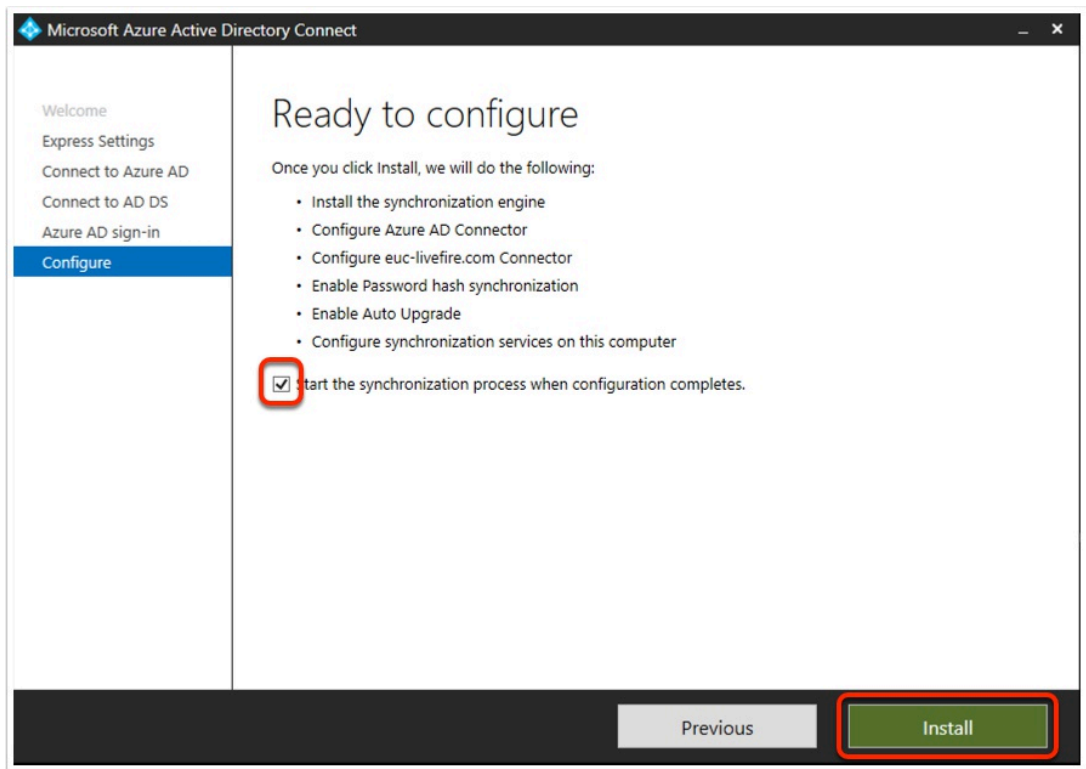


7. Verify your custom domain is verified

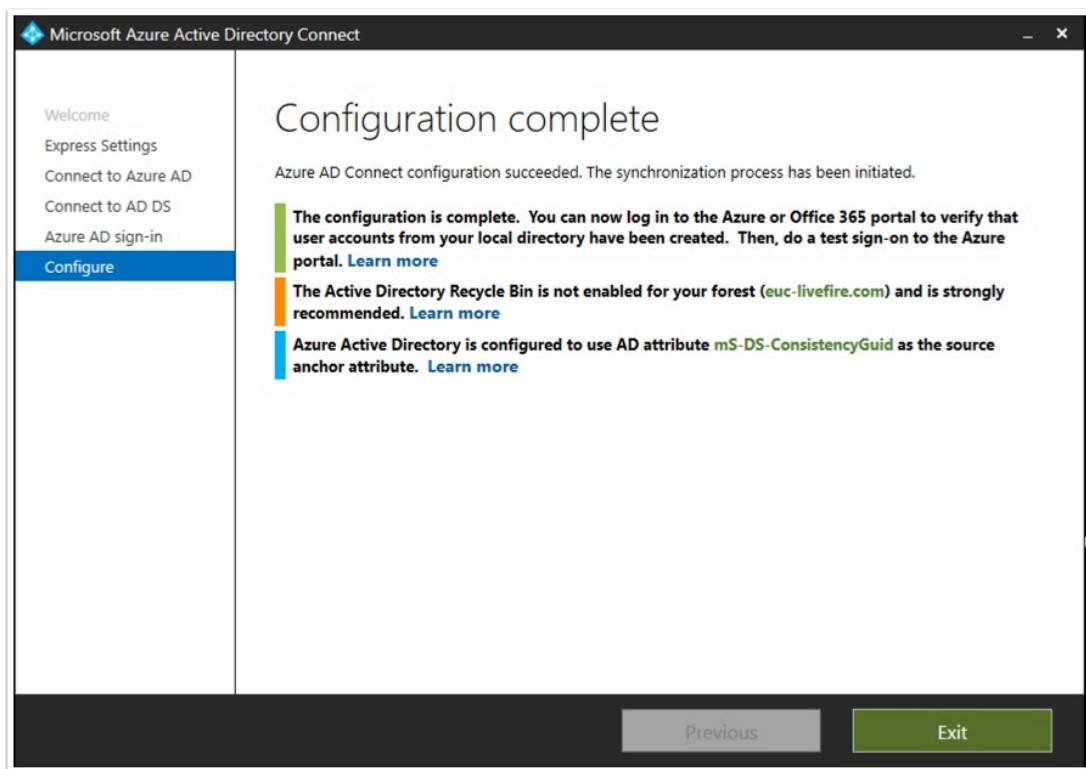
8. **Check the box** next to "Continue without matching all UPN suffixes to verified domains" and click **Next**



9. On the **"Ready to configure"** window make sure the box next to **"Start synchronization process when configuration completes"** is checked and click **Install**. Getting to the following step should take a couple of minutes.

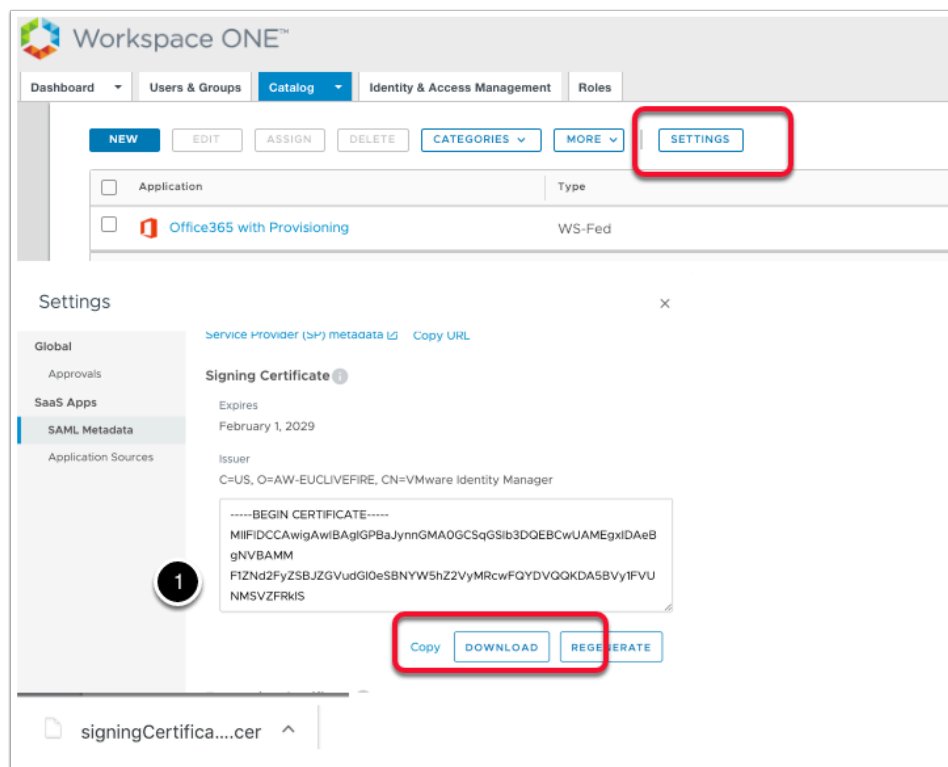


10. In the **"Configuration complete"** window click **"Exit"**



## Part 4: Setting up the SAML between Workspace ONE Access and Office 365

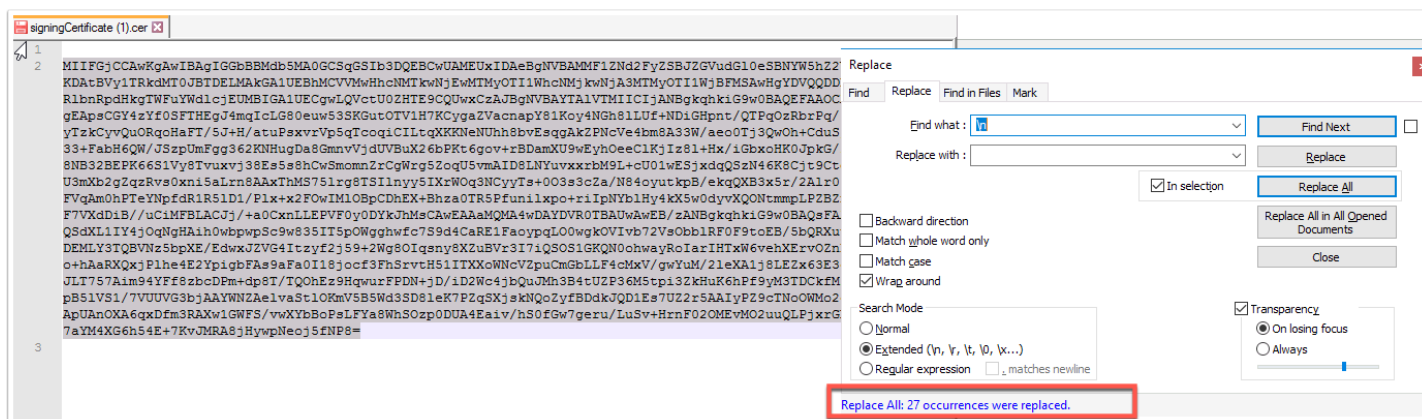
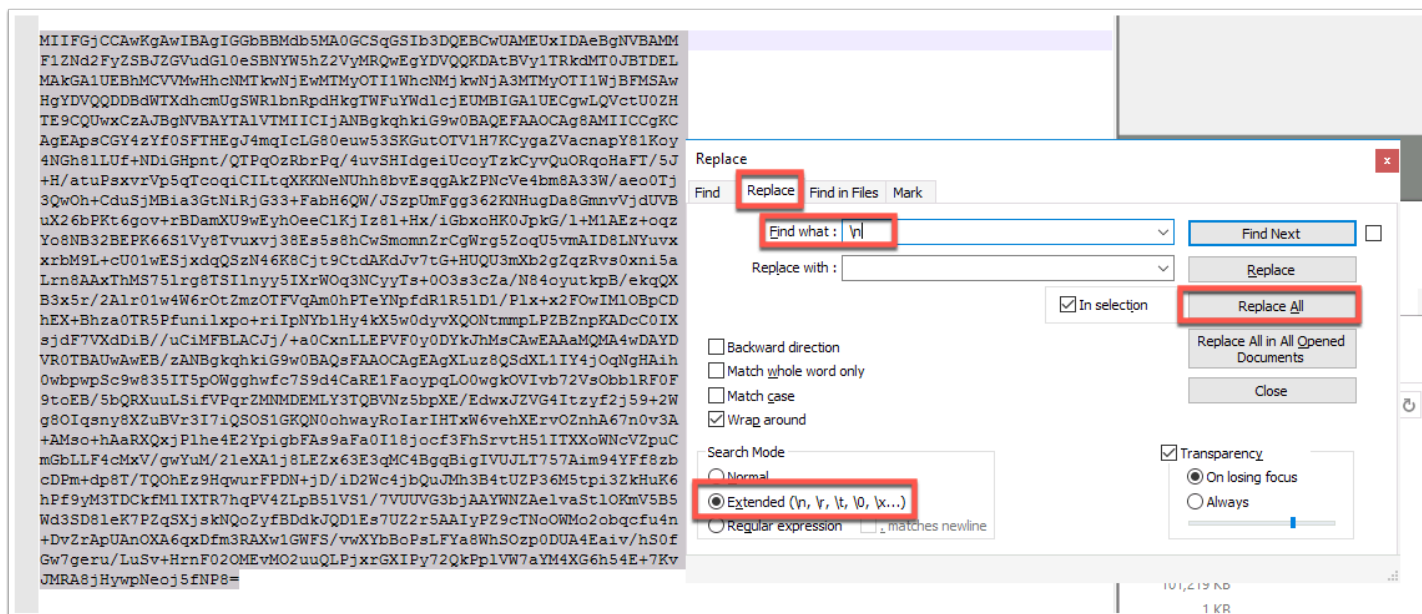
1. Ensure you do the next section on your **ControlCenter2** server .
  1. Login to your to the **Workspace ONE Access** Admin Console, as **Admin**, under the **Catalog > Web Apps** tab to the right select **SETTINGS**
  2. In the **Settings** window under **SaaS Apps**, select **SAML Metadata**, in the right hand pane under the **SAML Metadata** heading select **DOWNLOAD** under **Signing Certificate**
  3. Using Notepad++ Open the **signingCertificate.cer** from your default download location .



2. In the **signingCertificate.cer** we will remove all carriage returns the document

Do this with Notepad++ on your **ControlCenter server**. Any hidden carriage returns will cause this exercise to FAIL

1. Remove the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines from the certificate.
2. Then select the certificate portion of the file and click **ctrl + F** in the **Replace** tab at the top type **\n** in the Find what field. Leave the Replace with field empty. Make sure the Search Mode at the bottom is **Extended**. Then click on **Replace All**.
3. Your certificate should now no longer have carriage returns. Notepad++ will tell you how many instances were replaced and your certificate will look different.



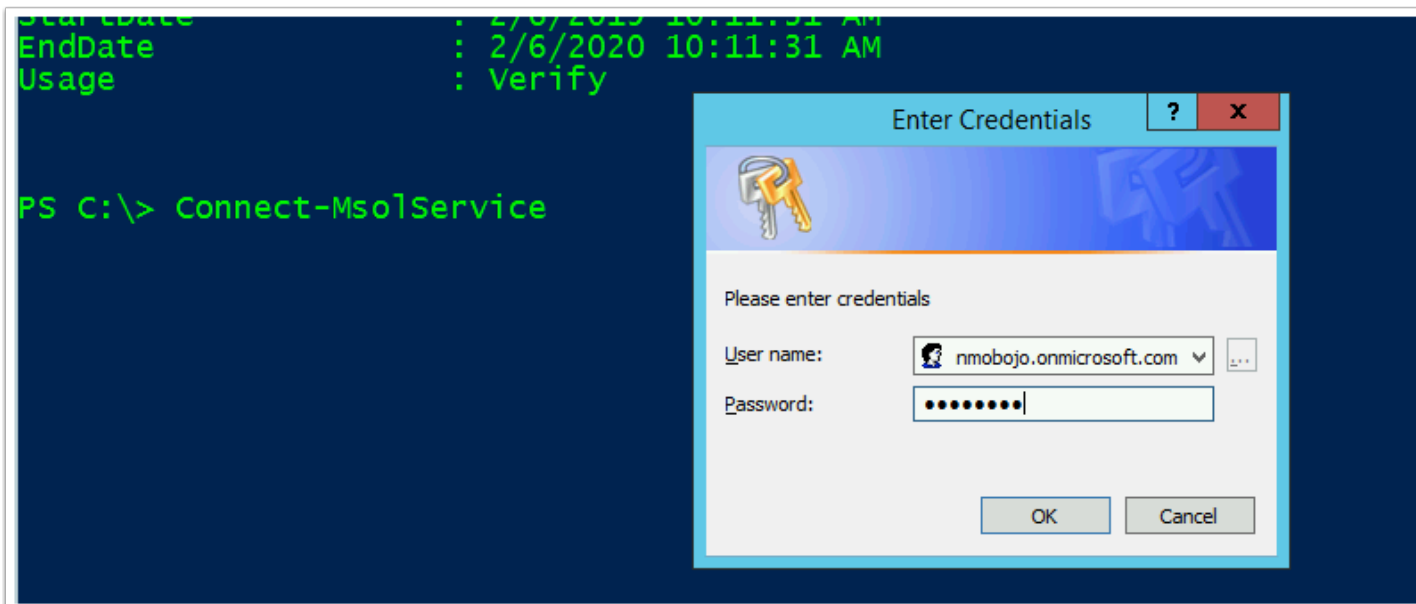
3. On the **ControlCenter2** server and open the existing **Powershell** interface we were working with earlier (from the shortcut on your desktop). please copy, edit and paste the commands from the text file called powershell commands, located in your Software folder (linked in your control center desktop), in the \Applications\Azurefiles folder.

Run the following command:

### Connect-MsolService

- In the **Powershell Console** type the following using your **Cloudadmin** credentials. The example we use is **cloudadmin@ranmobojjo.onmicrosoft.com** and your password





4. Next we edit the following Powershell commands for our environment and include the certificate string as part of this command.

1. Edit the sample string by replacing any instance of **tokyo01** with the city and number from *YOUR CUSTOM Fully Qualified Domain name, i.e. london08*
2. Edit the sample string by replacing **aw-euclivefire.vidmpreview.com** with **YOUR CUSTOM SAAS Workspace ONE Access Tenant Fully Qualified Domain name**

**example 1 is the string without the certificate |**

**example 2 is the string with the certificate which you will have to append without introducing any hidden returns into Powershell**

```

Set-MsolDomainAuthentication -DomainName tokyo01.euc-livefire.com -Authentication
Federated -IssuerUri "tokyo01.euc-livefire" -FederationBrandName "tokyo01Corp" -
PassiveLogOnUri "https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/POST/sso" -
ActiveLogOnUri "https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/active/logon" -
LogOffUri "https://login.microsoftonline.com/logout.srf" -MetadataExchangeUri
"https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/services/mex" -
SigningCertificate
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```

```

Set-MsolDomainAuthentication -DomainName tokyo01.euc-livefire.com -Authentication
Federated -IssuerUri "tokyo01.euc-livefire" -FederationBrandName "tokyo01Corp" -
PassiveLogOnUri "https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/POST/sso" -
ActiveLogOnUri "https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/active/logon" -
LogOffUri "https://login.microsoftonline.com/logout.srf" -MetadataExchangeUri
"https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/services/mex" -
SigningCertificate
MIIFIDCCAwigAwIBAgIGPBaJynnGMA0GCSqGSIb3DQEBCwUAMEGxIDAeBgNVBAMMF1ZNd2FyZSBjZGVudG10eSBN
YW5hZ2VyMRcwFQYDVQQKDA5BVy1FVUNMSVZFk1SRTElMAkGA1UEBhMCVVMwHhcNMjkwMjA0MjEzMTA5WhcNMjkw

```





```

PS C:\> Get-MsolDomainFederationSettings -domainName tokyo01.euc-liveware.com

ActiveLogOnUri           : https://aw-eucliveware.vidmpreview.com/SAAS/auth/w
                          : sfed/active/login
DefaultInteractiveAuthenticationMethod :
FederationBrandName      : Liveware
IssuerUri                : tokyo01.euc-liveware.com
LogOffUri                : https://login.microsoftonline.com/logout.srf
MetadataExchangeUri      : https://aw-eucliveware.vidmpreview.com/SAAS/auth/w
                          : sfed/services/mex
NextSigningCertificate   :
OpenIdConnectDiscoveryEndpoint :
PassiveLogOnUri          : https://aw-eucliveware.vidmpreview.com/443/SAAS/AP
                          : I/1.0/POST/sso
SigningCertificate        : MIIIFKDCCAxCGAwIBAgIGPBcCTXRSMAGCSqGSIb3DQEBAQUAAQIB
                          : wxIDAeBgNVBAMMF1ZNd2FyZSB1ZGVudG10eSBuYw5hZ2V2YMRsw
                          : GQYDVQQKDBJBVW51FVUNMSVZFRk1SRtpFTkMxCzAJBgNVBAYTA1
                          : VTMB4XDTE5MDIwNDIxMzEwNFoXDTE5MDIwMTIxMzEwNFowTDEg
                          : MB4GA1UEAwVxYk13YXJ1IE1kZW50aXR5IE1hbmFnZXIwGzAZBg
                          : NVBAoMEKFXLUVVQ0xJVkVGSVJFokVOQzELMAKGA1UEBhMCVVMw
                          : ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCpYVvr3N
                          : U7cGmIVGdu9ut7xhK6MDTgU0/qs1toLBZ+kY7NrNXMSXJ0LCK
                          : DR8L0/GSkncHGFrsBHndYnN64SbY4SI1KFXkjmgyYumtk8j1
                          : G8waKCyz7Nhrx+1Z6TgsEwJ9nn7rhPfSj9YCKyDwtF1+YE2zLL
                          : vx0gGRC7e5TDFwGCGvTUMwkeaywi3Q3VTibh4z36T7G8h9YwY6

```

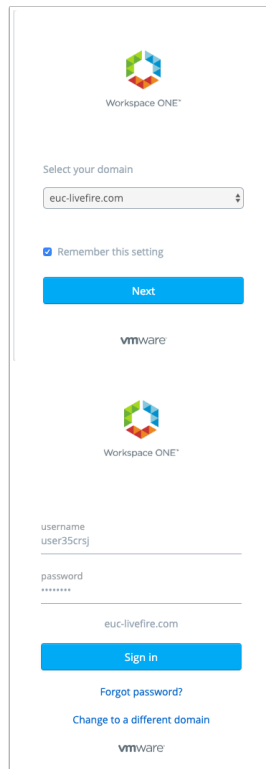
## Part 5: In this part, we will now start testing the federation to see and ensure it it working properly

1.
  - Login back to your **office 365 Tenant** with your office Admin account with this url <https://admin.microsoft.com/Adminportal/Home?source=applauncher#/homepage> and use your **cloudadmin account**
    1. In the left-hand pane under **Home**, select **Users** > **Active users**. Notice that Marketing group **Users 1 - 8** has been automatically provisioned with the unique suffix appended for the user principle name. Also notice that your users are Unlicensed. Select users 1-8
    2. Select the **radio buttons** next to **User 1 to User 8**. This is includes your **Custom User**
    3. Next to **Assign to group** select the **3 dots** which will expand the menu and select **Manage product licenses**
    4. In the **Manage Product licenses** window select **Next**
    5. On the **Replace existing products** window under **Location**, select a location ie **United Kingdom**.
    6. Next to **Microsoft E5 Developer (without Windows and Audio Conferencing)**, turn the **slider bar** to **On**
    7. **Scroll down** and select **Replace** select **Close**.
    8. **NB!** - Validate that your **Cloudadmin** account is licensed as well. This will depend on whether you started off with a custom Outlook account or used another email in the beginning of the course labs. If not re-apply to the licensing to this account and then ensure that you can open the Cloudadmin mailbox. This requirement must be done before starting your OKTA lab.

The screenshot displays a multi-step process in the Workspace ONE Access console. At the top, a list of users is shown, with 7 users selected. Below this, a 'Replace existing products' dialog is open. It provides options to either replace or add to existing product license assignments. The 'Replace' option is selected. The dialog then prompts the user to select product licenses for the selected users, showing a list of available licenses for the 'United Kingdom' location. The 'Microsoft 365 E5 Developer (without Windows and Audio Conferencing)' license is selected, and it indicates that 24 of 25 licenses are available. The 'Replace' button is highlighted in blue.

2.

- Open up an **Incognito** session of your browser and connect to your SAAS instance of Workspace ONE Access.
  1. On the login window ensure that on the select your domain window, **euc-livefire.com** is selected, select **Next**
  2. In the **username** section, use your custom **username** ie **user35scr** and the **password** **VMware1!** select **Sign in**



Workspace ONE™

Select your domain

euclivfire.com

☒ Remember this setting

Next

vmware

Workspace ONE™

username  
user35crsj

password  
\*\*\*\*\*

euclivfire.com

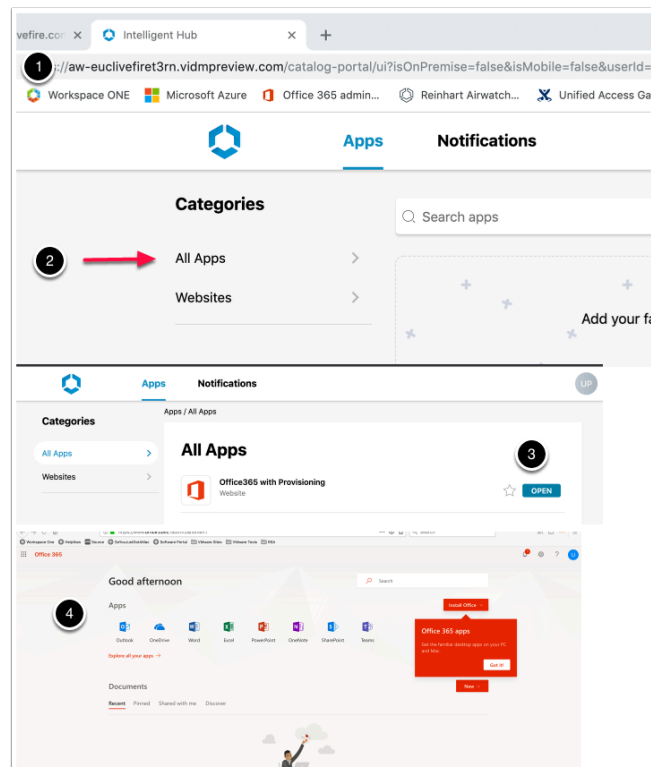
Sign in

[Forgot password?](#)

[Change to a different domain](#)

vmware

3.
  - In the **Workspace ONE** console
    1. Under **Apps** select **All Apps**
    2. Next **Office 365 with Provisioning** select **Open**
    3. You should now see the Microsoft Office365 console



## Part 6: Inserting Office 365 Deep Links into Workspace ONE Access

Having a Portal to Portal single sign-on experience very rarely excites a customer. In this section we will insert Deep Links within Workspace ONE Access to enhance the user experience.

### 1. Inserting Office 365 Deep links

- On your **Controlcenter** server. **Log in** to your to your Workspace ONE Access Console as Admin and select the **Catalog** tab > **Web Apps**
  - Select **NEW**
  - In the **New SaaS Application** window under **Name** type **Microsoft Word**
  - Under Icon, click on **browse**, search for the software link on your desktop, and navigate to \Applications\Azurefiles\icons. select your **Word.png** Icon and select **Open**. At the bottom right select **NEXT**
  - On **2. Configuration** in the **Single Sign-On** section under **Authentication type** to the right select the **drop down** and then select **Web Application Link**

The screenshot displays the Workspace ONE Access console interface. At the top, there's a navigation bar with 'Dashboard', 'Users & Groups', 'Catalog', and 'Identity & Acc'. Below this, a 'NEW' button is highlighted. The main section is titled 'New SaaS Application'. On the left, a sidebar shows four steps: '1 Definition', '2 Configuration', '3 Access Policies', and '4 Summary'. The '1 Definition' step is currently active. In the 'Definition' section, there's a 'Search' field and a link 'or browse from catalog'. The 'Name' field is filled with 'Microsoft Word'. Below this, the '2 Configuration' step is highlighted in the sidebar. In the 'Configuration' section, under 'Single Sign-On', the 'Authentication Type' dropdown is set to 'Web Application Link'. The 'Target URL' field is empty. At the bottom right, there's a link 'Open in VMware Browser'.

### 2. Inserting Office 365 Deep links (Part 5)

- 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=wsigin1.0&whr=EXAMPLEDOMAIN.euc-**  
**livefire.com&wreply=https://office.live.com/start/Word.aspx?auth=2**

Target URL \*

<https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=lisbona35.euc-liveware.com&wreply>

### 3. Inserting Office 365 Deep links (Part 5)

- Select **NEXT > SAVE & ASSIGN**
  1. Under **Users / User Groups** in the **Search** area type **Mark**, select **Marketing@euc-liveware.com**
  2. Under **Deployment Type** select **Automatic** and select **SAVE**

CANCEL BACK SAVE & ASSIGN SAVE

Selected App(s): Microsoft Word

Users / User Groups

Q Mark

Marketing@euc-liveware.com

Deployment Type

Automatic

CANCEL SAVE

### 4. Inserting Office 365 Deep links (Part 5)

- Repeat the above steps for
  1. **OneDrive**
    - <https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=lisbonb35.euc-liveware.com&wreply=https://zingaramanwell-my.sharepoint.com>
    - Replace **Lisbonb** with your domain
    - Replace **zingaramanwell** with your unique Office 365 domain name. eg in this example the domain name is cloudadmin@zingaramanwell.onmicrosoft.com, **zingaramanwell** is the domain name
  2. **Excel**








- <https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=lisbonb35.euc-livewire.com&wreply=https://www.office.com/launch/excel?auth=2&home=1>

### 3. PowerPoint

- <https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=lisbonb35.euc-livewire.com&wreply=https://www.office.com/launch/powerpoint?auth=2>

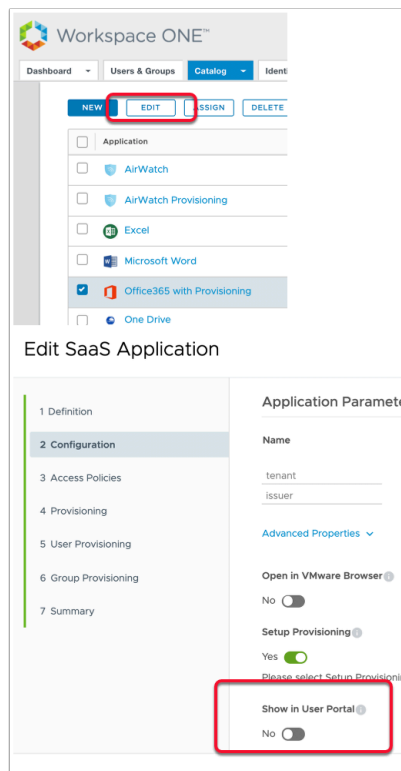
### 4. Outlook

- [https://login.microsoftonline.com/common/oauth2/authorize?client\\_id=00000002-0000-0ff1-ce00-000000000000&response\\_mode=form\\_post&livewire.com](https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&livewire.com)

NEW EDIT ASSIGN DELETE CATEGORIES MORE SETTINGS		
<input type="checkbox"/>	Application	Type
<input type="checkbox"/>	 AirWatch	SAML 2.0
<input type="checkbox"/>	 AirWatch Provisioning	SAML 2.0
<input type="checkbox"/>	 Excel	Web Application Link
<input type="checkbox"/>	 Microsoft Word	Web Application Link
<input type="checkbox"/>	 Office365 with Provisioning	WS-Fed
<input type="checkbox"/>	 One Drive	Web Application Link
<input type="checkbox"/>	 Powerpoint	Web Application Link

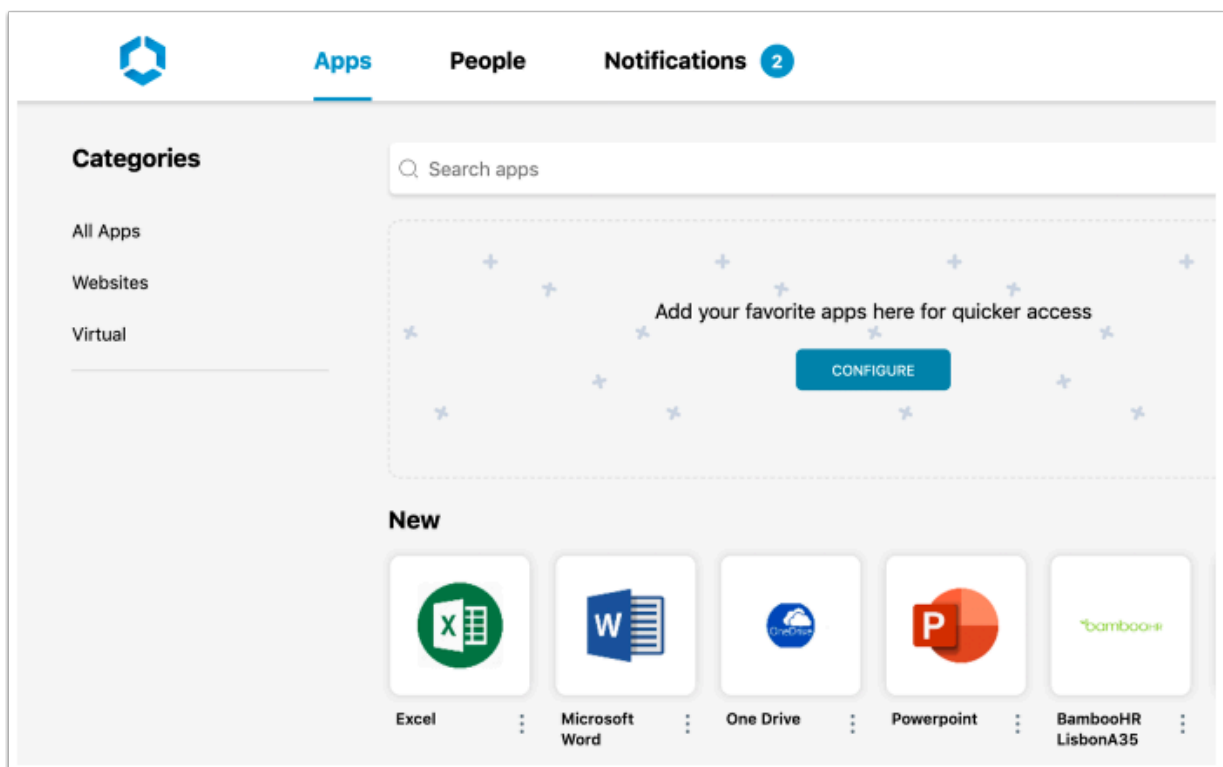
### 5. Inserting Office 365 Deep links (Part 5)

- The Office 365 application has been assigned to Marketing. It has to remain assigned to Marketing for the Deep links to work. However, we do not necessarily want this to be visible to the End-User. We will now solve this issue as part of a well thought out solution.
  1. In the **Catalog**, select the **Check-box** next to **Office365 with Provisioning**, select **EDIT**
  2. in the **Edit SaaS Application** window, select step **2 Configuration** and scroll down to the bottom. Change **Show in the User Portal** toggle from **Yes** to **No**
  3. Select **NEXT > NEXT > NEXT > NEXT > SAVE**



## 6. Inserting Office 365 Deep links (Part 5)

- Switch to a Browser in Incognito Mode . Using your Workspace ONE Access URL login as User1 with the password VMware1!
- Test your individual links for office 365





## 7. Tidying up the Catalog in Workspace ONE Access for a better User Experience

- Switch back to your **Workspace ONE Access Admin** Console and select the **Catalog** tab
  1. In the **Catalog** next to **Office 365 with Provisioning** select the **check box** and then at the top select **EDIT**
  2. In the **Edit SaaS Application** wizard select **2 Configuration** and **scroll down** to the bottom,
  3. Change the **toggle** under **Show in User Portal** from **Yes** to **No** and select **NEXT > NEXT > SAVE**
  4. Repeat the exact same process and validate that that the **AirWatch** and **AirWatch Provisioning** applications do not show in the User Portal

The screenshot shows the 'Edit SaaS Application' page in the AWS IAM console. The 'EDIT' button at the top is highlighted with a red box. Below the header, there is a list of applications. The application 'Office365 with Pro...' is selected, indicated by a blue checkmark. The right-hand pane displays the configuration for this application, including fields for 'Name', 'tenant', 'Issuer', and 'Show in User Portal'. The 'Show in User Portal' checkbox is checked.