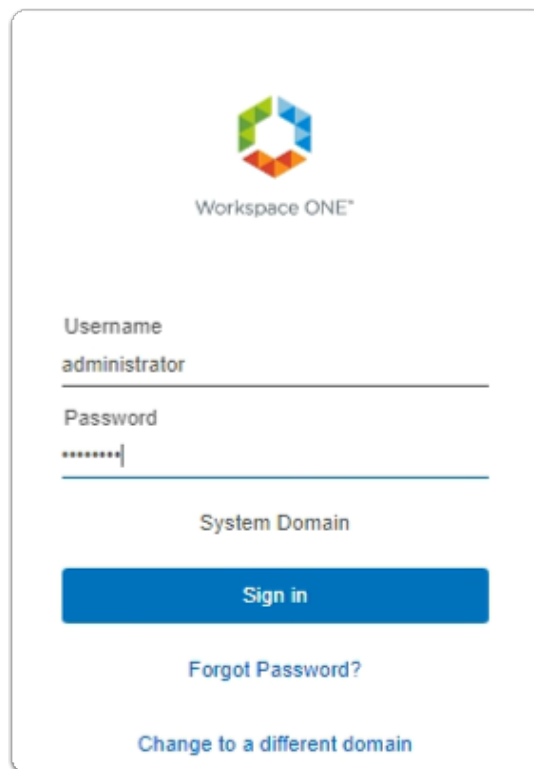


Integrating the Horizon Universal Console with Workspace ONE

Part 1 - Completing Workspace ONE Integration Prerequisites

- Part 1 contains 11 sections
 - We will build an integrated Workspace ONE platform and then we will integrate Horizon Cloud services with this platform
 - All of these sections have to be completed to complete further labs

Part 1:Section 1: Workspace ONE Access , Connector pairing pre-requisites



Workspace ONE™

Username
administrator

Password
.....

System Domain

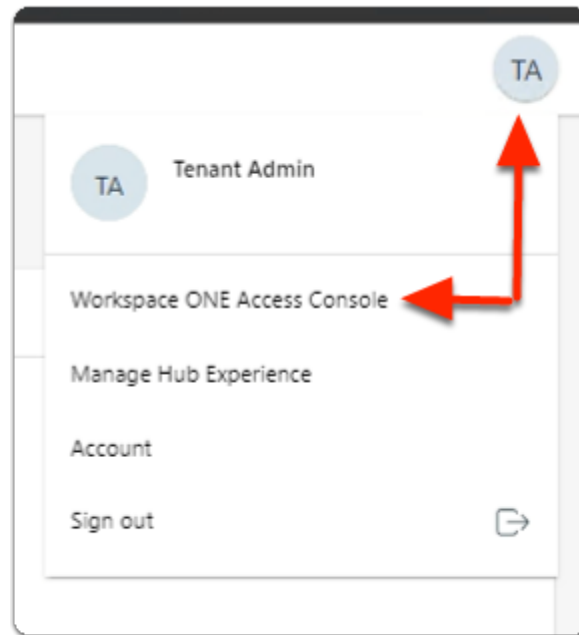
Sign in

[Forgot Password?](#)

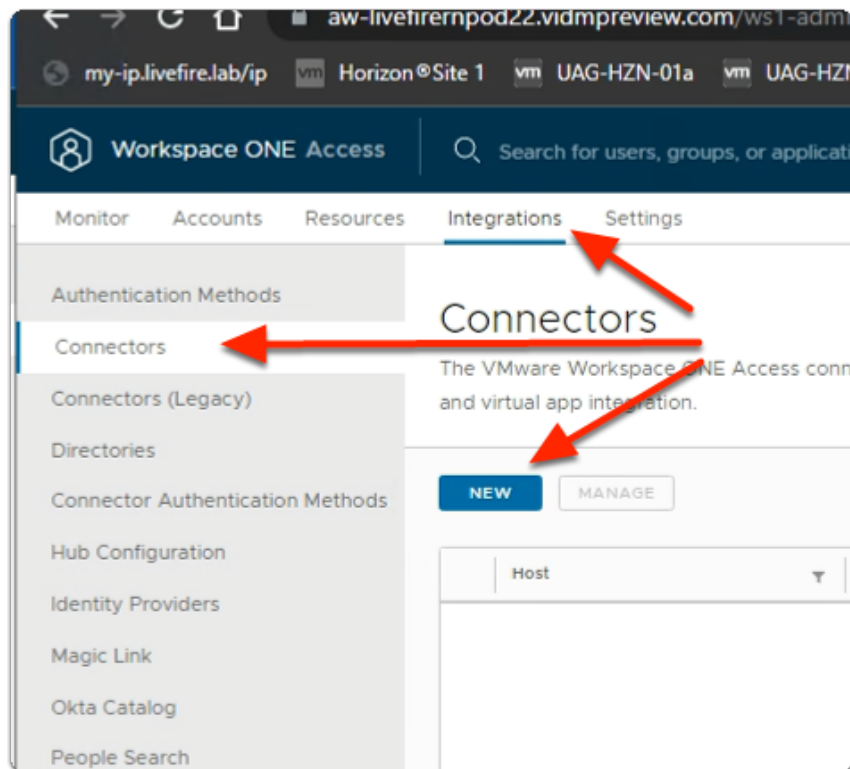
[Change to a different domain](#)

1. On your ControlCenter server
 - Open your **Workspace ONE Access**, Admin console URL
 - Under **Username**
 - enter **Administrator**

- Under **Password**
 - enter **VMware1!**
- Select **Sign In**



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



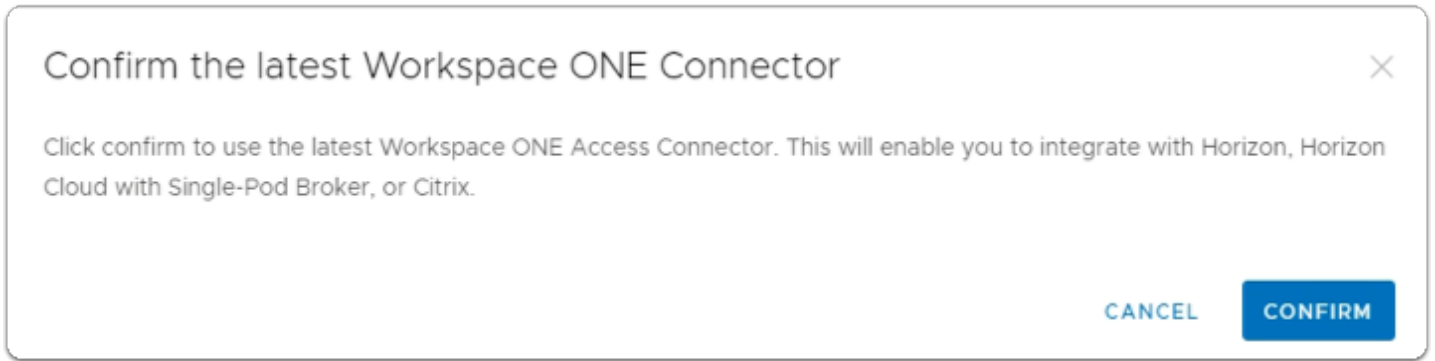
3. In the **Workspace ONE Access Console**

- Select **Integrations**
- Under **Integrations**
 - Select **Connectors**
- In the **Connectors** area
 - Select **NEW**

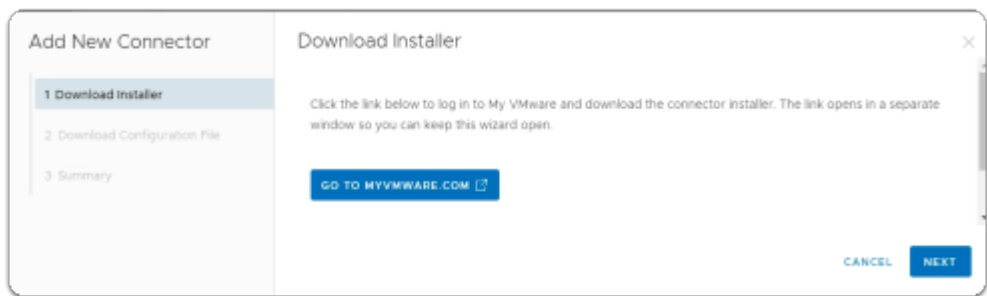


4. In the **Connector Usage Confirmation** window

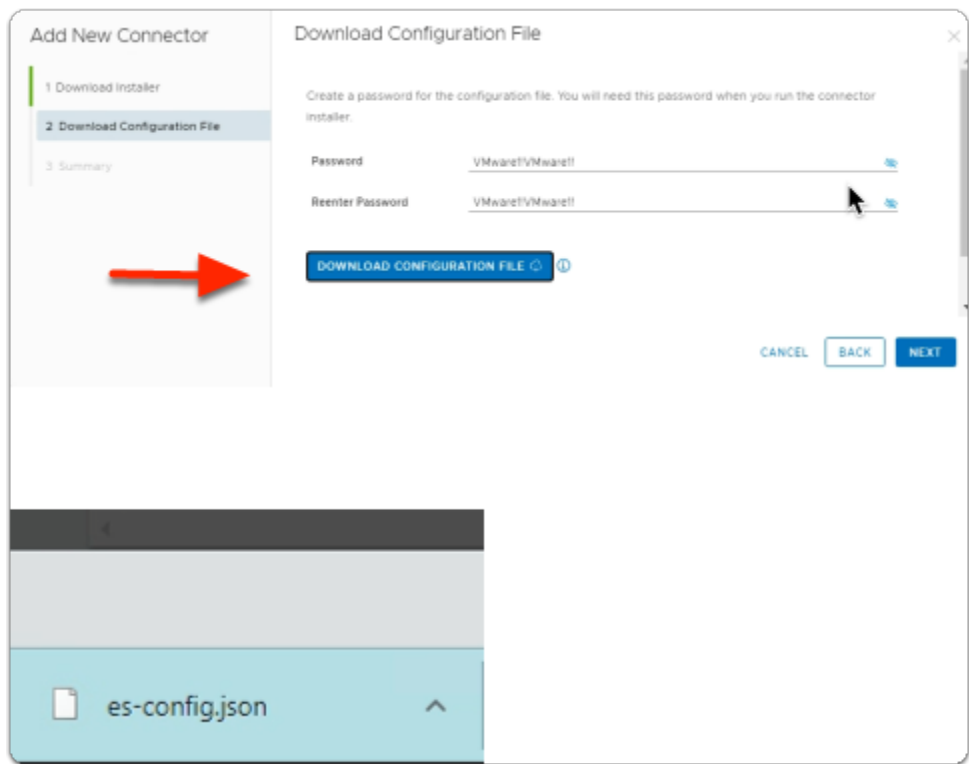
- Select the **radio button**, next to :-
 - **Latest Workspace ONE Access Connector**
- Select **OK**



5. In the **Confirm the latest Workspace ONE Connector** window
- Select **CONFIRM**



6. In the **Add New Connector** window
1. **Downloader Installer** area
 - Select **NEXT**



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

2. **Download Configuration File** area

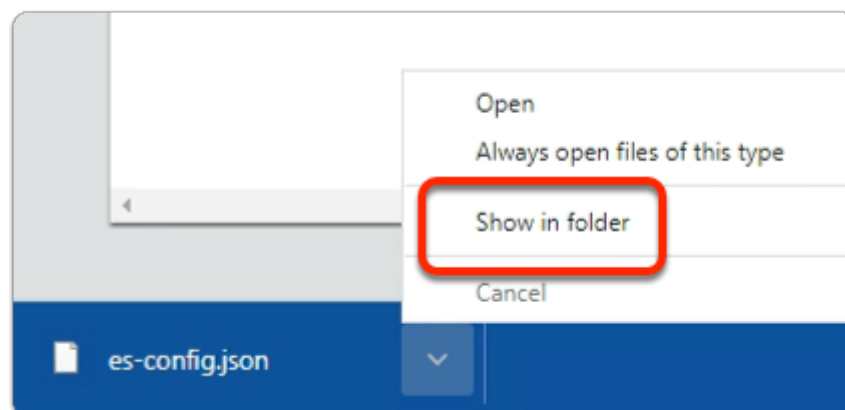
- Next to **Password:** enter **VMware1!VMware1!**
- Next to **Reenter Password:** enter **VMware1!VMware1!**
- Select **DOWNLOAD CONFIGURATION FILE**
 - note an **es-config.json** file gets downloaded
- Select **NEXT**



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

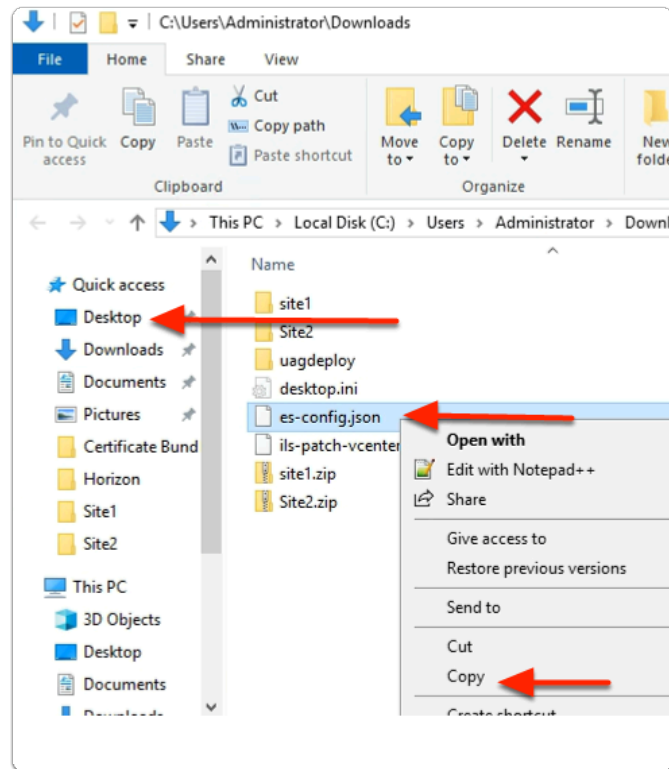
3. **Summary** window

- Select **CLOSE**

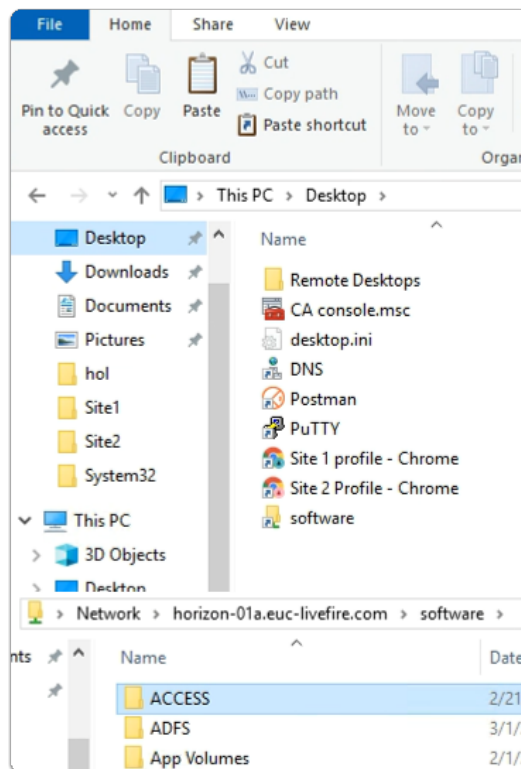


9. On your ControlCenter server browser

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

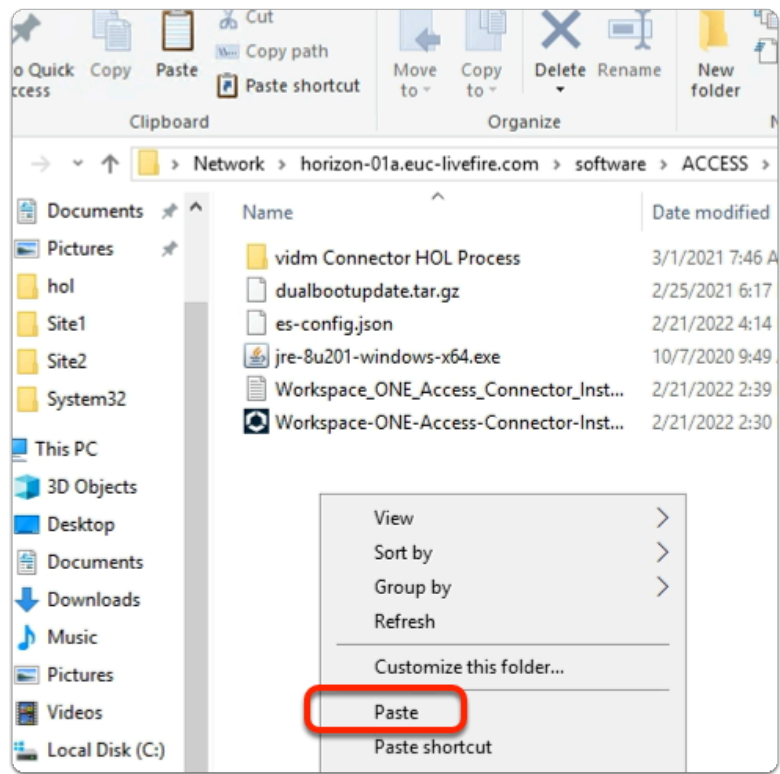


10. In the **File Explorer** window
- Select and right-click the **es-config.json** file
 - Select **Copy**
 - In the left pane
 - Select **Desktop**



11. In the **File Explorer** window

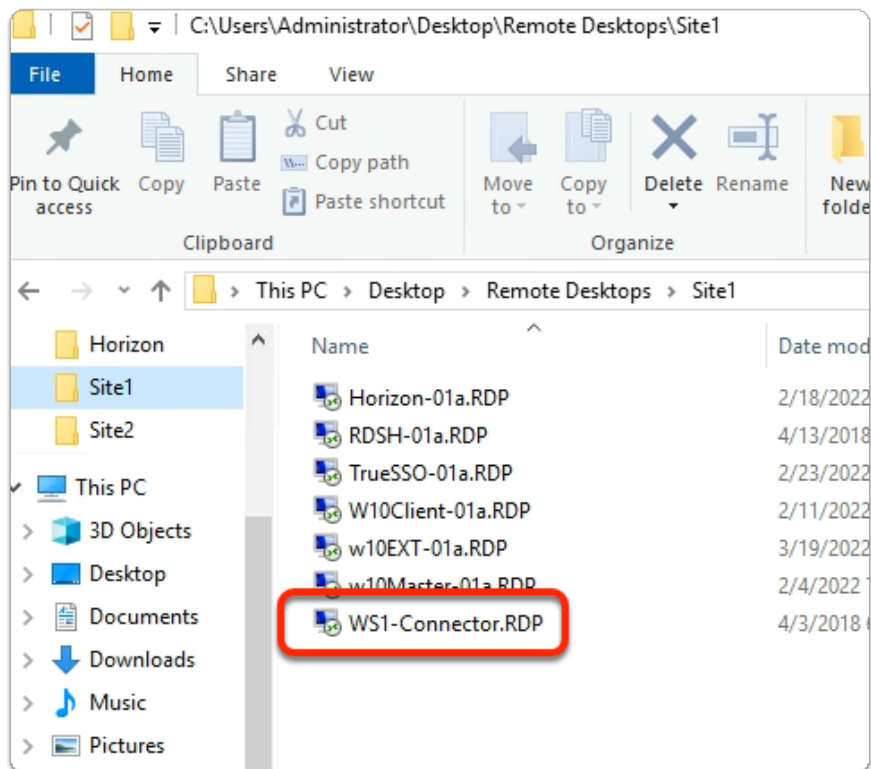
- **Desktop area**
 - Select the **Software** shortcut
 - In the **Software** folder
 - Open the **ACCESS** folder



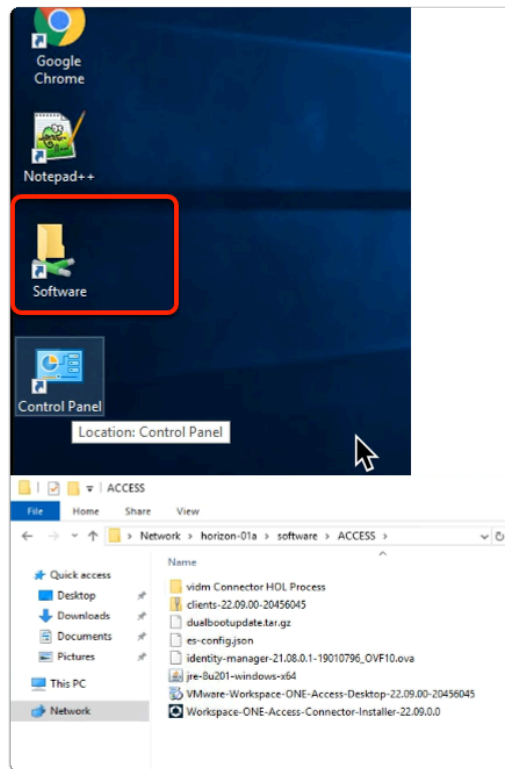
12. In the **File Explorer** window

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

Part 1:Section 2: Installing and Configuring the Workspace ONE Access connector

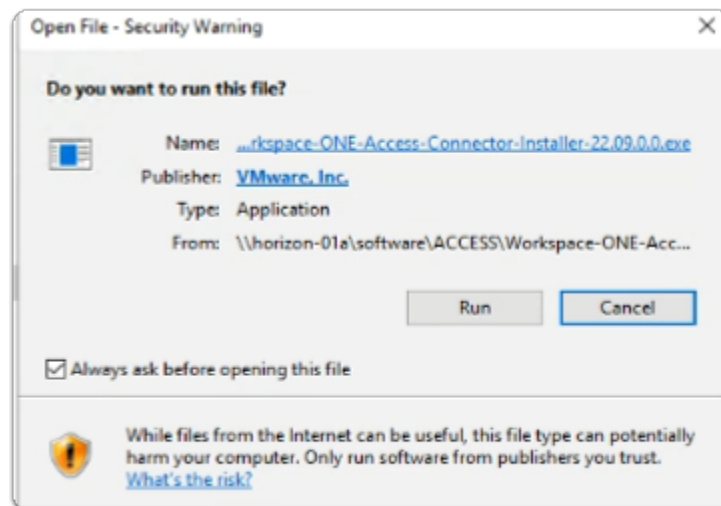


1. On your ControlCenter server
 - On the Desktop.
 - Open the **Remote Desktops\Site1** folder
 - Select and launch the **WS1-Connector.RDP** shortcut



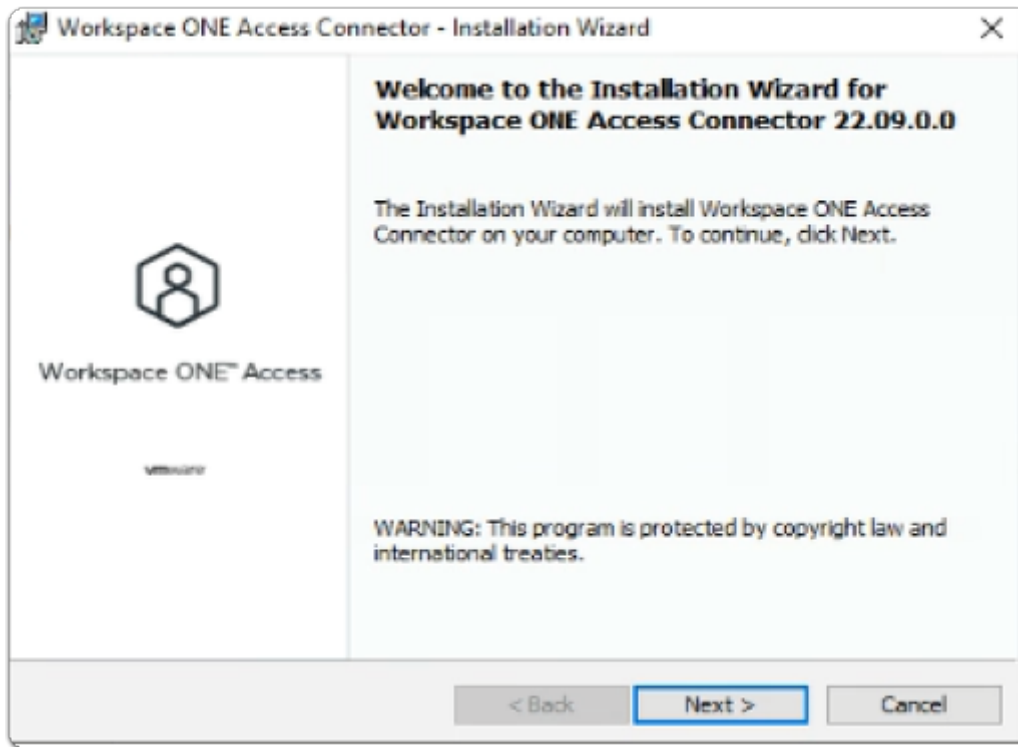
2. On your WS1-Connector server

- Open the **Software** Folder
- Select the **ACCESS** Folder
- Select and Launch
 - **Workspace-ONE-Access-Connector-Installer-22.09.0.0.exe**

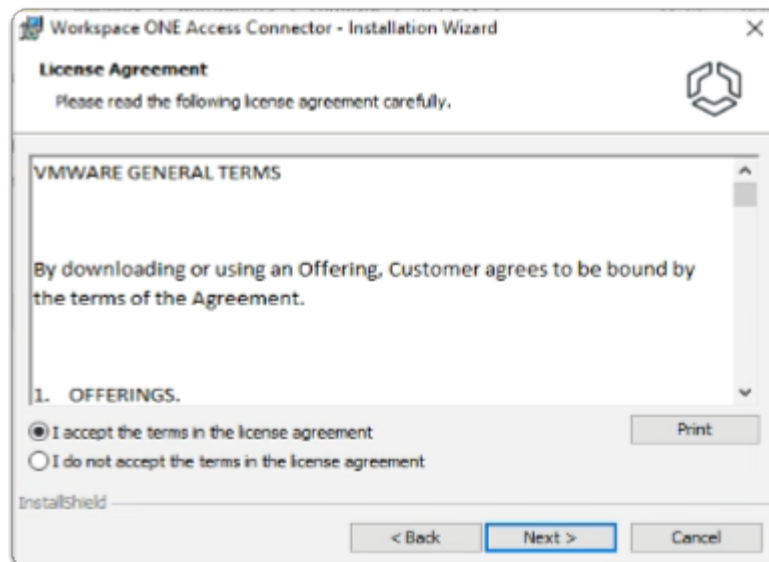


3. On your **WS1-Connector** server

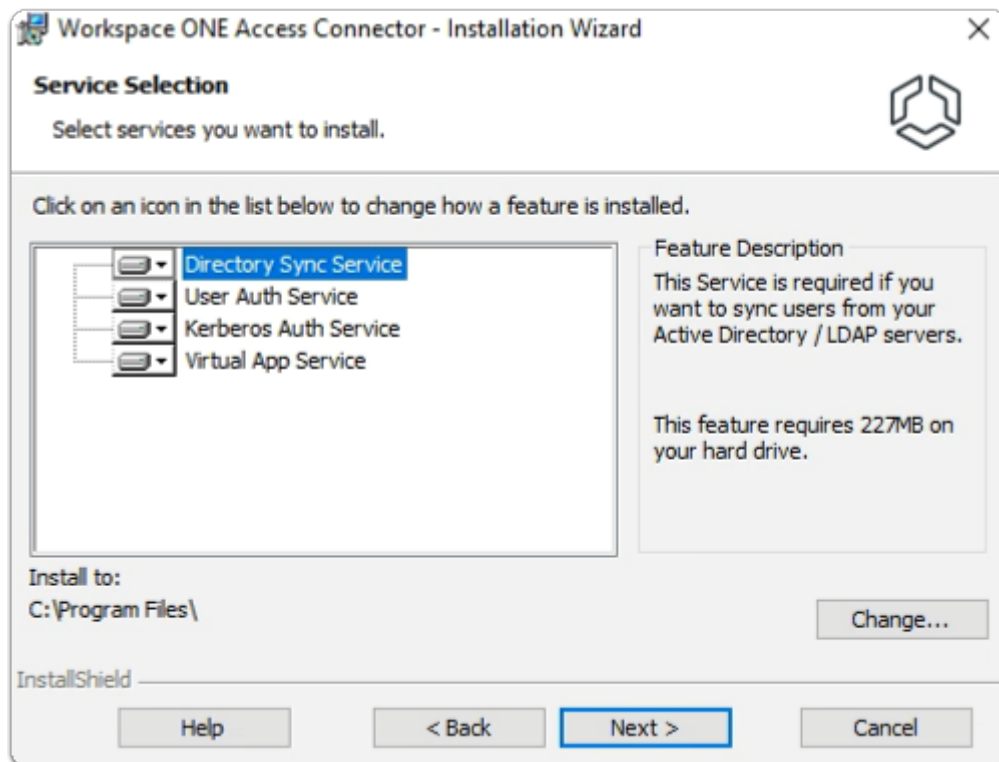
- On the **Open File - Security Warning** window
 - Select **Run**



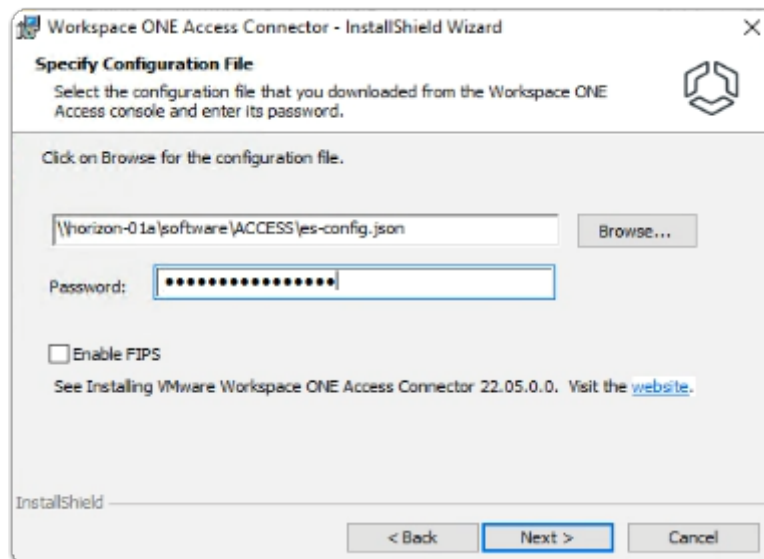
4. On the **Workspace ONE Access Connector - InstallShield** Wizard
 - In the **Welcome to the Installation Wizard for Workspace ONE Access Connector 22.09.0.0**
 - Select **Next**



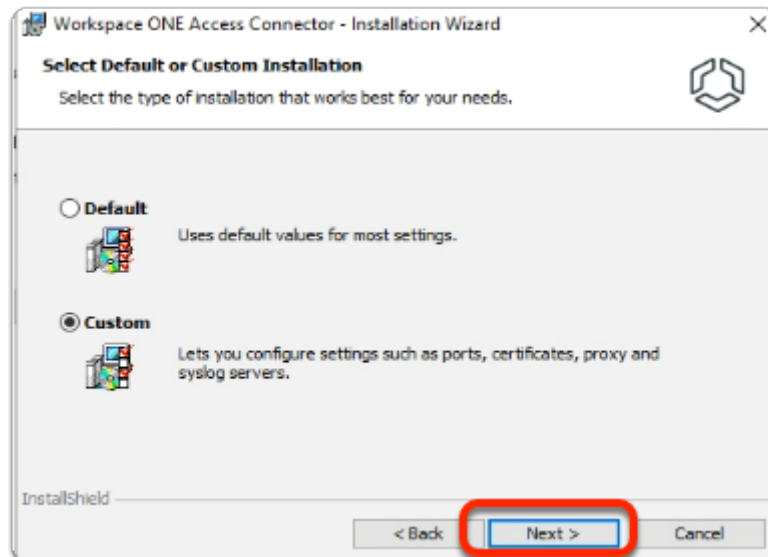
5. On the **Workspace ONE Access Connector - InstallShield** Wizard
 - **Licence Agreement** window
 - Select the **radio button** next to:-
 - **I accept the terms in the license agreement**
 - Select **Next**



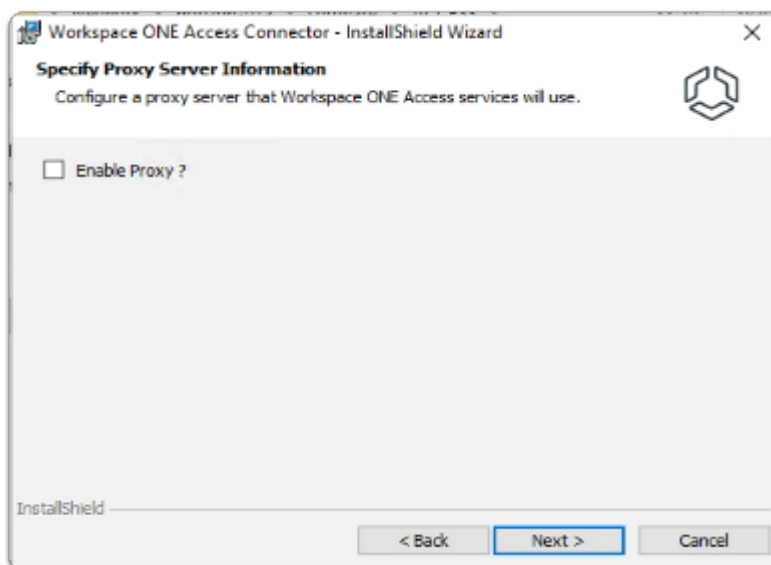
6. On the **Workspace ONE Access Connector - InstallShield Wizard**
 - **Service Selection** window
 - Select **Next**



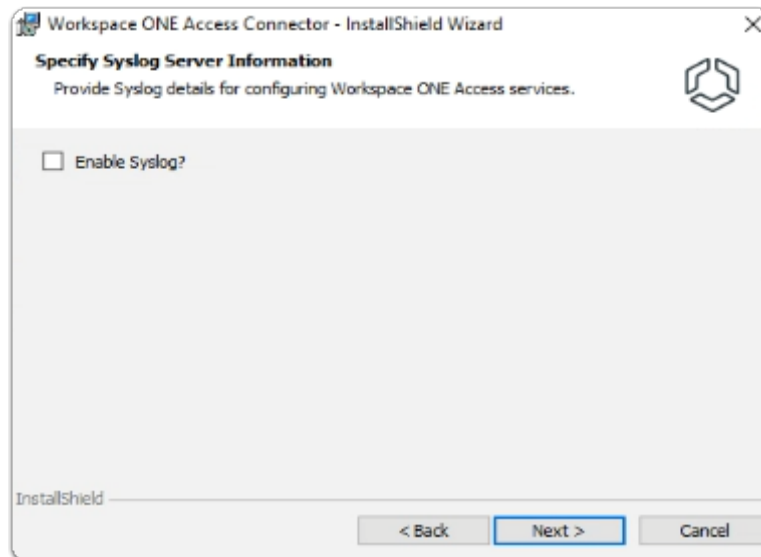
7. On the **Workspace ONE Access Connector - InstallShield Wizard**
 - **Specify Configuration File** window
 - In the box in front of **Browse...**
 - type **\\horizon-01a\software\ACCESS\es-config.json**
 - Next to **Password:** type **VMware1!VMware1!**
 - Select **Next**



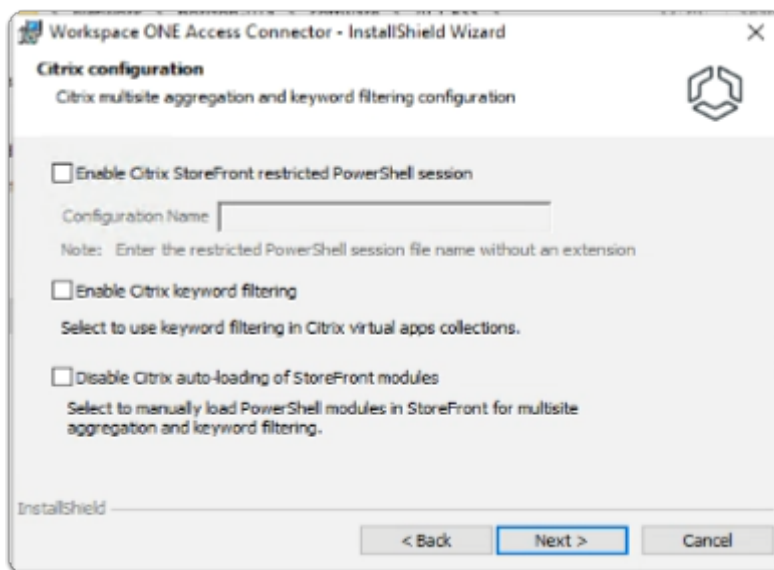
8. In the **Workspace ONE Access Connector - InstallShield** Wizard
- **Select Default or Custom Installation** window
 - Select the **radio button** next to **Custom**
 - Select **Next**



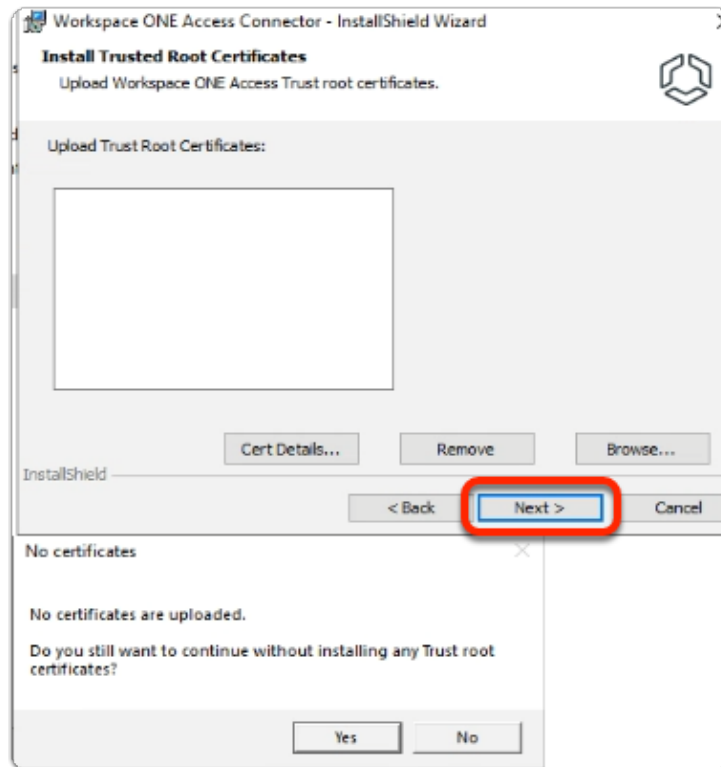
9. In the **Workspace ONE Access Connector - InstallShield** Wizard
- **Specify Proxy Server Information** window
 - Select **Next**



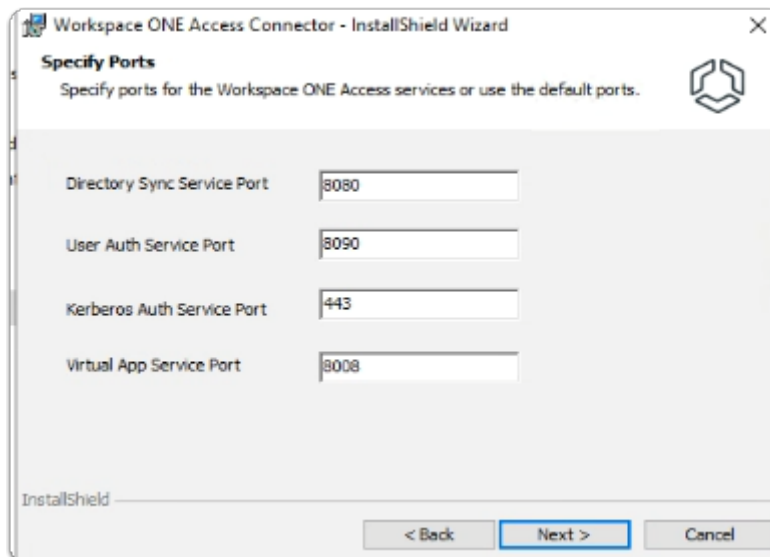
10. In the **Workspace ONE Access Connector - InstallShield** Wizard
- **Specify Syslog Server Information** window
 - Select **Next**



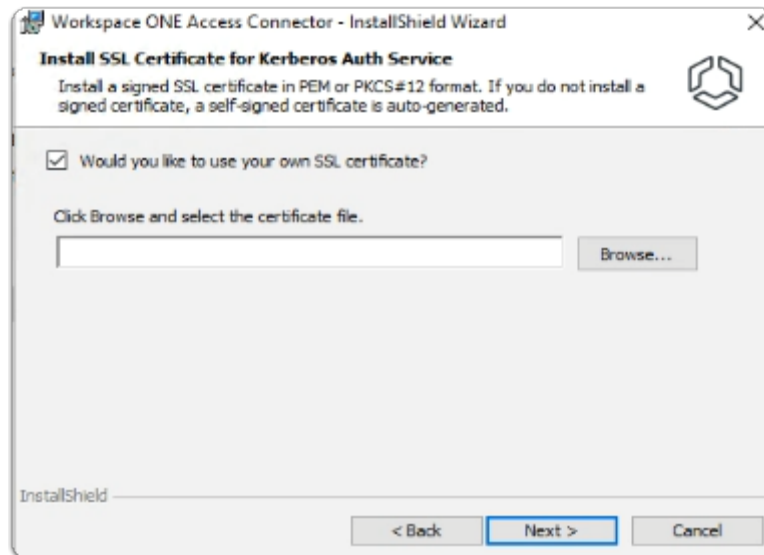
11. In the **Workspace ONE Access Connector - InstallShield** Wizard
- **Citrix configuration**
 - (leave default)
 - Select **Next**



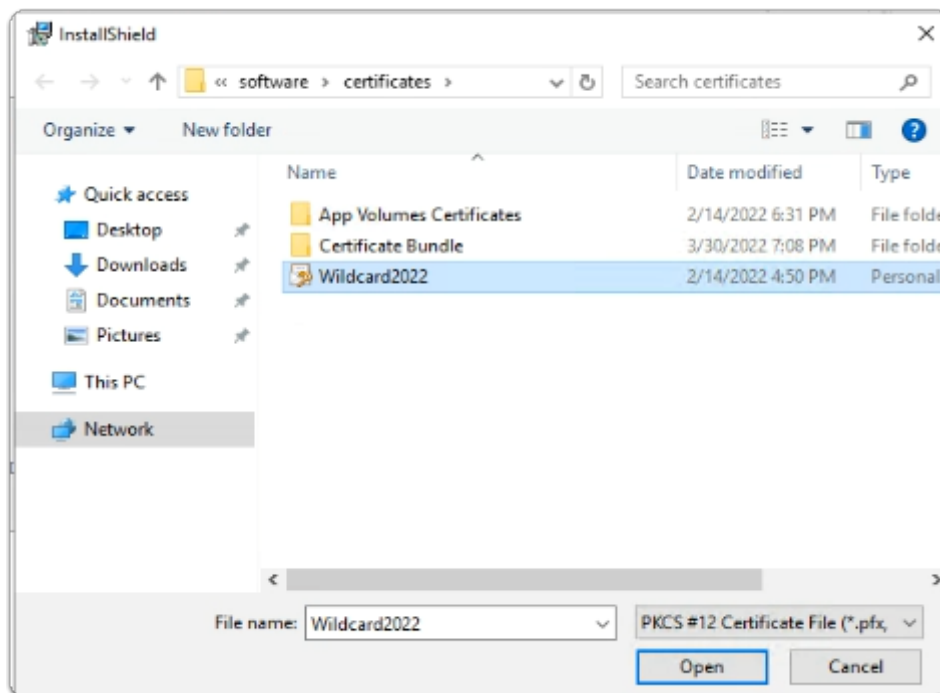
12. In the **Workspace ONE Access Connector - InstallShield** Wizard
 - **Install Trusted Root Certificates** window
 - Select **Next**
 - In the **No certificates** page
 - Select **Yes**



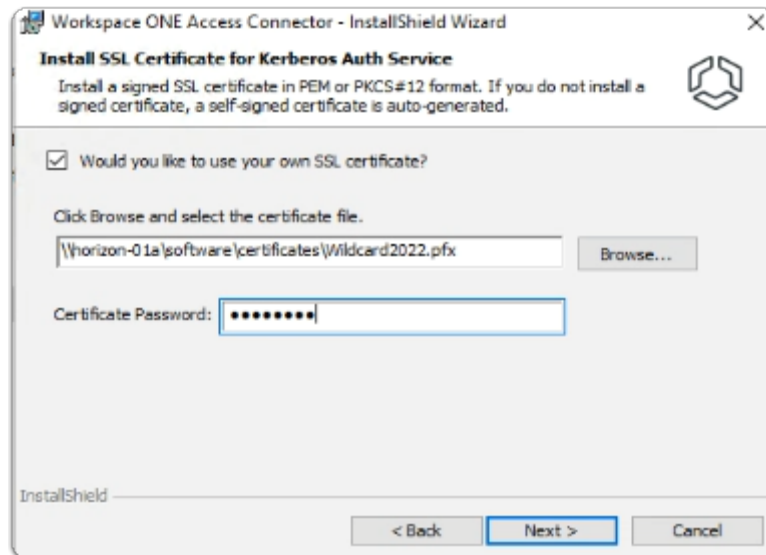
13. In the **Workspace ONE Access Connector - InstallShield** Wizard
 - **Specify Ports** window
 - Select **Next**



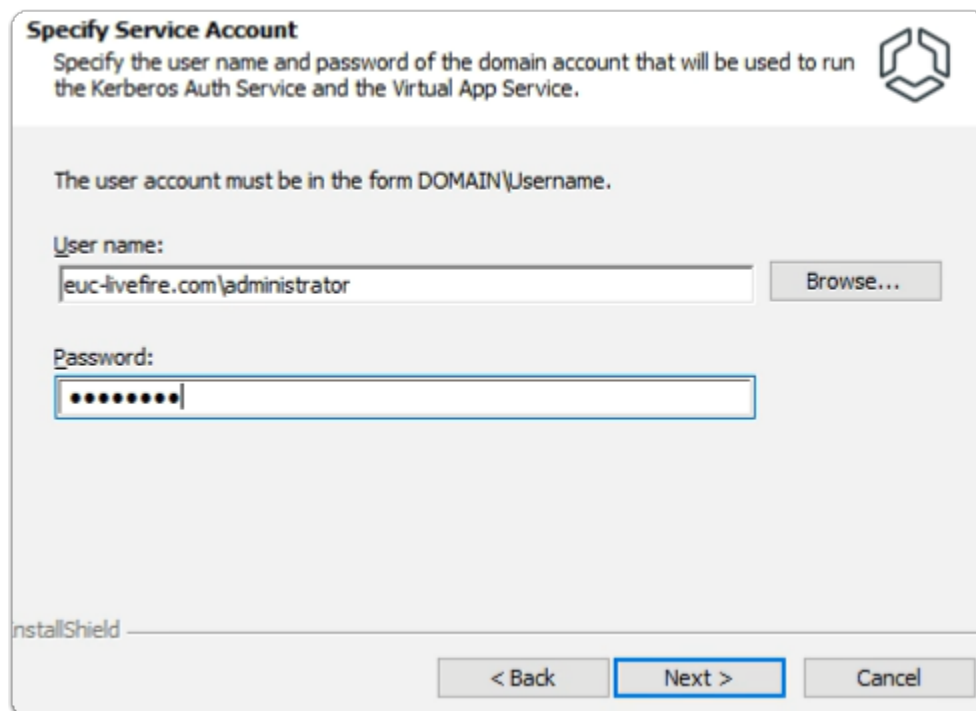
14. In the **Workspace ONE Access Connector - InstallShield** Wizard
 - **Install SSL Certificate for Kerberos Auth Service** window
 - Next to: **Would you like to use your own SSL certificate?**
 - Select the **Checkbox**
 - Under , **Click Browse and select the certificate file**
 - Select **Browse**



15. In the **InstallShield** window
 - **Browse** to:
 - **\\horizon-01a\software\certificates**
 - Select **Wildcard2022**
 - Select **Open**

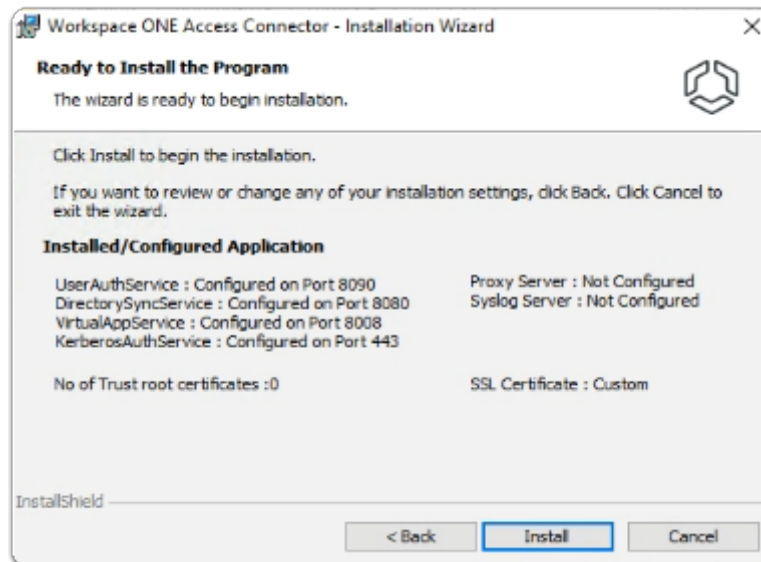


16. In the **Workspace ONE Access Connector - InstallShield Wizard**
- **Install SSL Certificate for Kerberos Auth Service** window
 - Next to: **Certificate Password:**
 - Enter : **VMware1!**
 - Select the **Next**



17. In the **Workspace ONE Access Connector - InstallShield Wizard**
- **Specify Service Account** window
 - Under User name: type
 - **euc-livfire.com\administrator**
 - Under **Password:**
 - type **VMware1!**

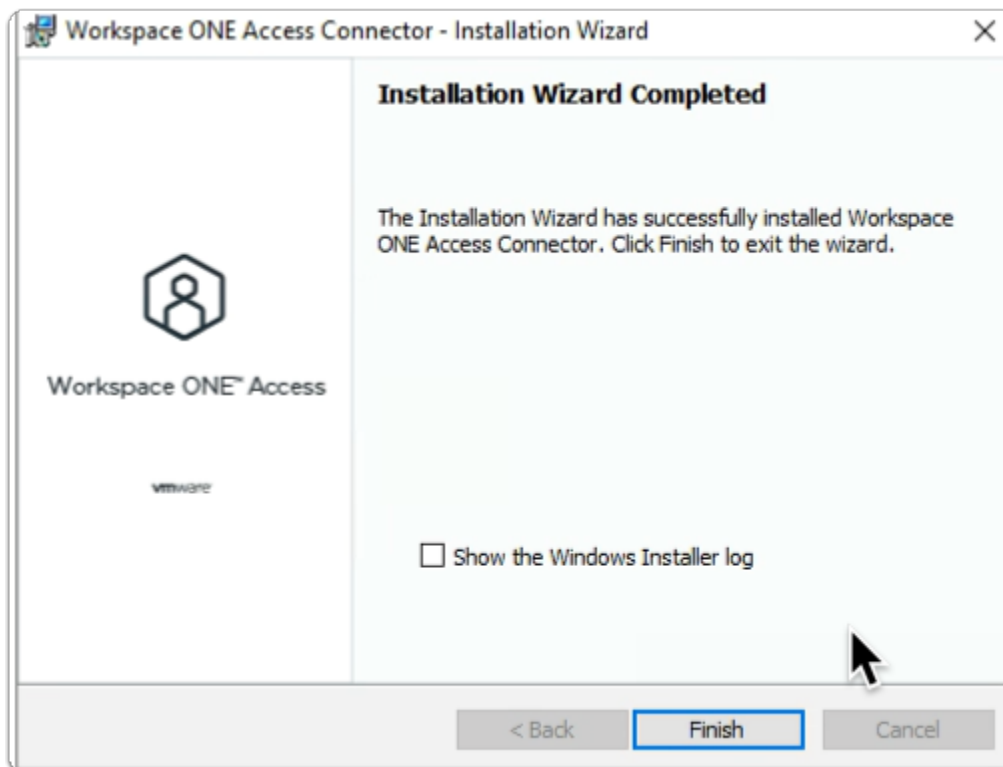
- Select **Next**



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

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

💡 The Installation of the Workspace ONE Access Connector will take about 10 minutes to complete

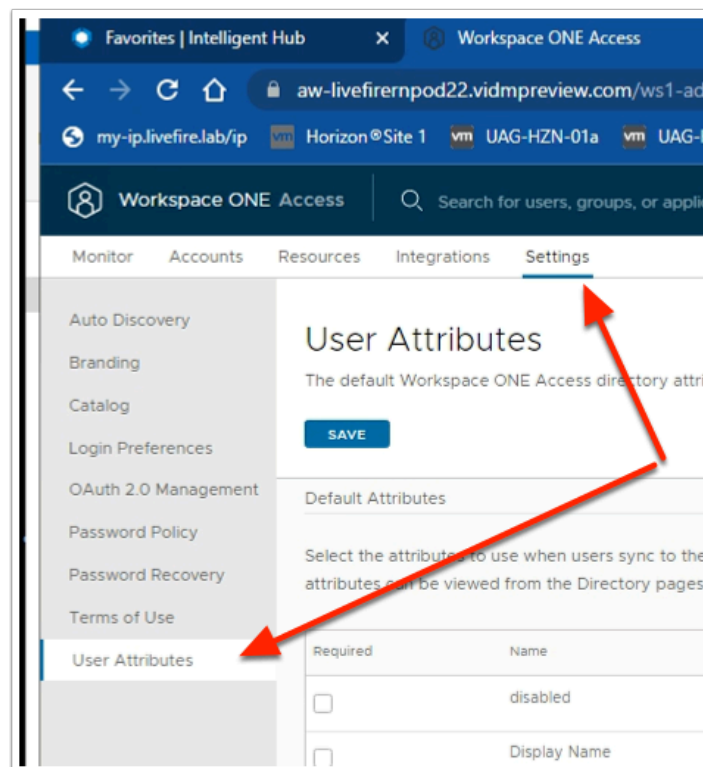


19. In the **Workspace ONE Access Connector - InstallShield Wizard**

- **Installation Wizard Completed** window
 - Select **Finish**

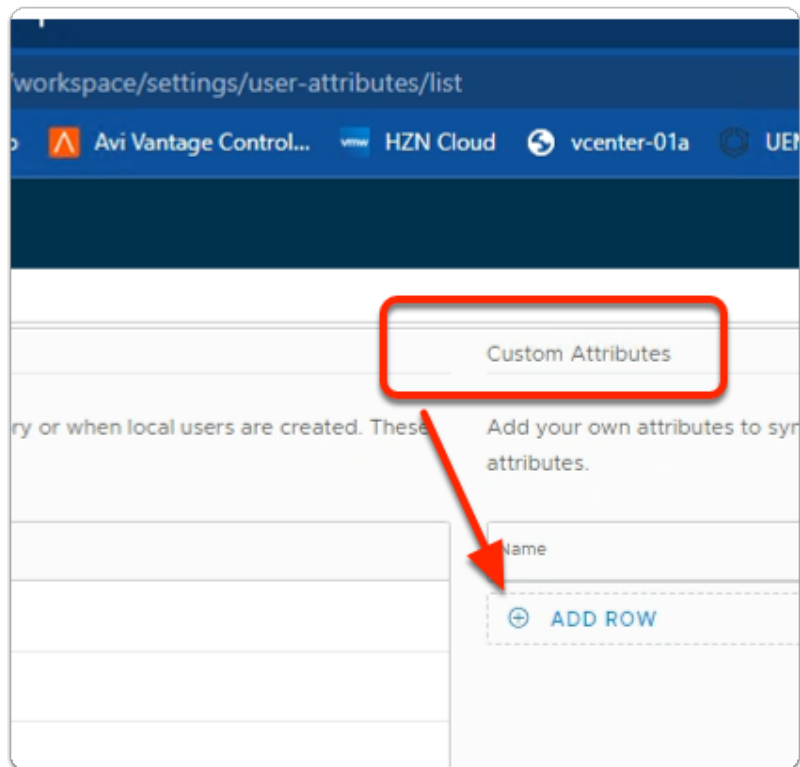
Part 1:Section 3: Configuring Directory Sync with Workspace ONE Access connector

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

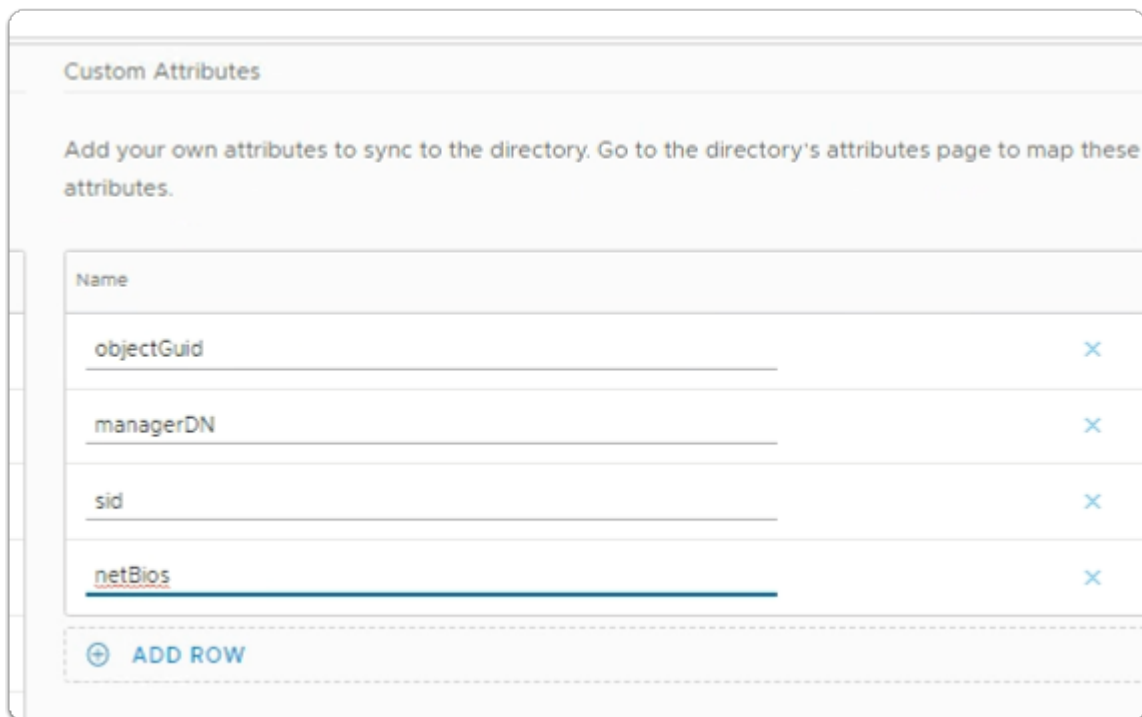


1. In the Workspace ONE Access Admin console

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

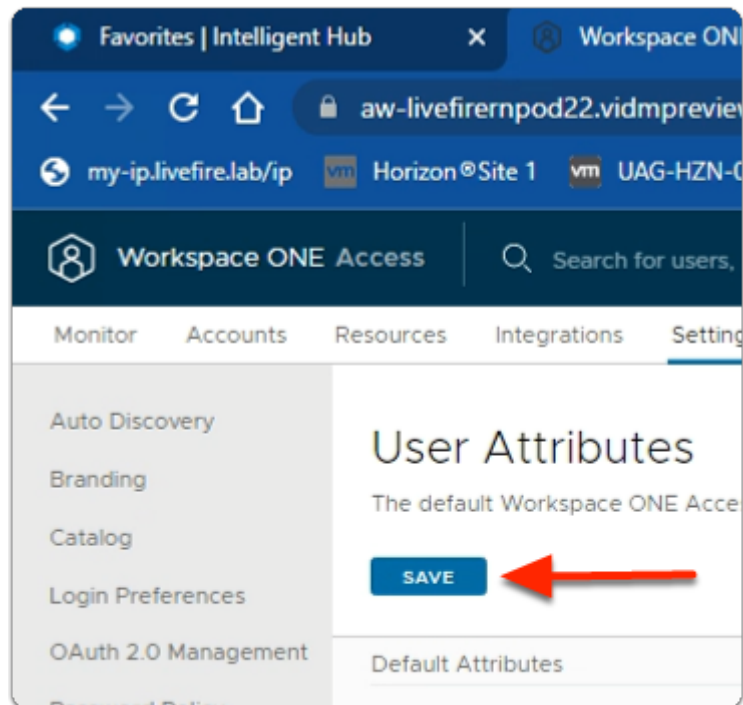


2. In the **User Attributes** console
 - In the right area under **Custom Attributes**
 - Select **+ ADD ROW** 4 times

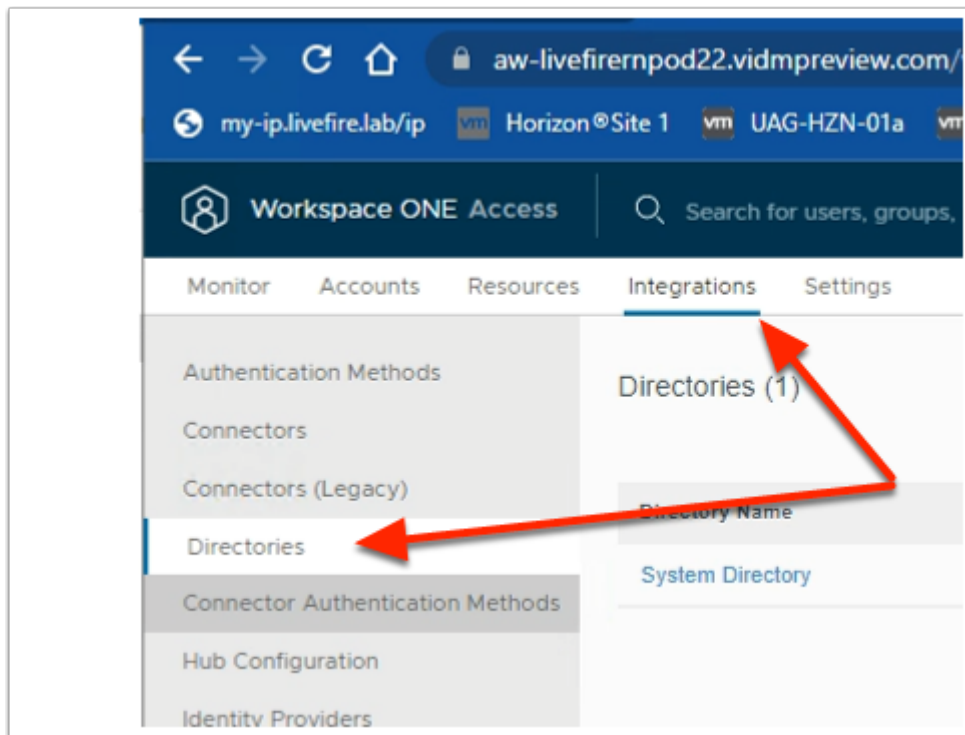


3. In the **User Attributes** console
 - Under **Name**
 - Add the following additional attributes

- note this is case sensitive :
- **objectGuid**
- **managerDN**
- **sid**
- **netBios**

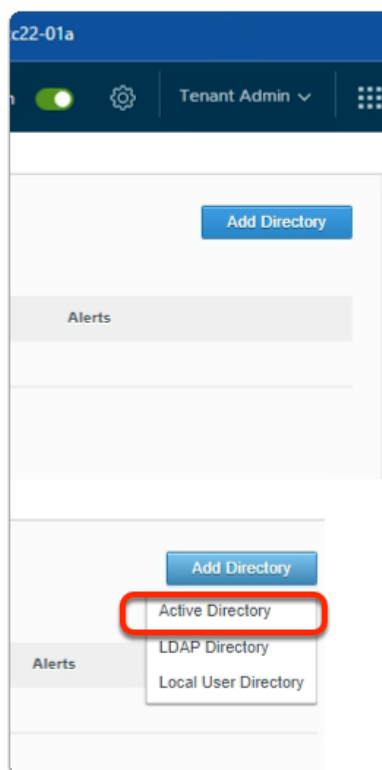


4. In the **User Attributes** console
 - Under **User Attributes**
 - Select **SAVE**



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

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



6. In the **Directories** area

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

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

Add Directory

Directory Name*

☒ Active Directory over LDAP
☐ Active Directory over Integrated Windows Authentication

Directory Sync and Select at least one active directory sync host that syncs users from Active Directory or Microsoft Access directory

7. In the **Add Directory** Page,
 - Configure the following: next to
 - **Directory Name:** type **EUC-Livefire**
 - Ensure the **Active Directory over LDAP** radio button is selected
 - **Scroll down** to **Bind User Details**

Bind User Details

In the Base DN field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. In the Bind User DN field, enter the account that can search for users. For example, CN=user1,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Base DN*

Bind User DN*

Bind User Password*

Enter your Active Directory bind account password.

Close **Save & Configure**

8. In the **Add Directory** Page,
 - In the **Bind User Details** area
 - Enter the following Next to :
 - **Base DN:** **dc=EUC-Livefire,dc=com**
 - **Bind DN:** **cn=administrator,ou=corp,dc=EUC-Livefire,dc=com**
 - **Bind DN Password:** **VMware1!**
 - Select **Save & Configure**

Select the Domains

If you are adding an Active Directory over LDAP, domains are auto

Domain
<input checked="" type="checkbox"/> euc-livfire.com (EUC-LIVEFIRE)

[Next](#)

- In the **Select the Domains** page,
 - **euc-livfire.com** (EUC-LIVEFIRE)
 - Select **Next**.

Map User Attributes

domain	canonicalName
employeeID	employeeID
managerDN	manager
managerId	Enter Custom Input...
netBios	msDS-PrincipalName

- On the **Map User Attribute** page
 - Map the following attributes : next to:-
 - (what you enter here is case sensitive)
 - **managerDN** select **custom input** and type **manager**
 - **netbios**: select **custom input** type **msDS-PrincipalName**

Enter Custom Input...

objectGuid objectGUID

organization Enter Custom Input... Enter Custom Input...

phone telephoneNumber

profileUrl Enter Custom Input... Enter Custom Input...

sid objectSid

Previous Close Next

11. On the **Map User Attribute** page
 - Map the following attributes :
 - **Scroll down** next to:-
 - **objectGuid**: select **objectGUID**
 - **sid**: select **custom input** type **objectSid**

sourceAnchor objectGUID

title title

userPrincipalName userPrincipalName

Previous Close Next

12. On the **Map User Attribute** page
 - Map the following attributes :
 - **Scroll down** next to:-
 - **title** : from the **dropdown**
 - select **title**
 - Validate that **userPrincipalName** maps to **userPrincipalName**
 - Select **Next**

Select the groups you want to sync

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

☒ Sync nested group members

Specify the top-level group Select All Groups to sync +

x +

2 3 1

Group DN Mapped Groups

13. On the **Select the Groups you want to sync** page,
 1. select the **green plus (+)** to the right of the page,
 2. Under **Specify the group DN**
 - enter **dc=euc-livewire,dc=com**
 3. Select the **Select All** writing
 - You will notice the **check box** now becomes available

Select the groups you want to sync

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

☒ Sync nested group members

Specify the top-level group Select All Groups to sync +

☒ All Select Groups x +

Group DN Mapped Groups

All groups in this DN are selected

Previous Close Next

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

Select the Users you would like to sync

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

Specify the user DN's

ou=corp,dc=EUC-Livefire,dc=com

Add a filter to exclude users

Previous Close Next

15. In the **Select Users you would like to sync** window
 - Under **Specify the user DN's**
 - edit the existing syntax so that it reads
 - **ou=corp,dc=EUC-Livefire,dc=com**
 - Select **Next**

Sync Frequency

Sync Frequency: Once per week

Day: Sunday

Time: 23:55

Hint: Sync schedule runs in UTC TimeZone.

Previous Close Save Sync Directory

16. On the **Sync Frequency** window
 - Select **Sync Directory**

Search for users, groups, or applications

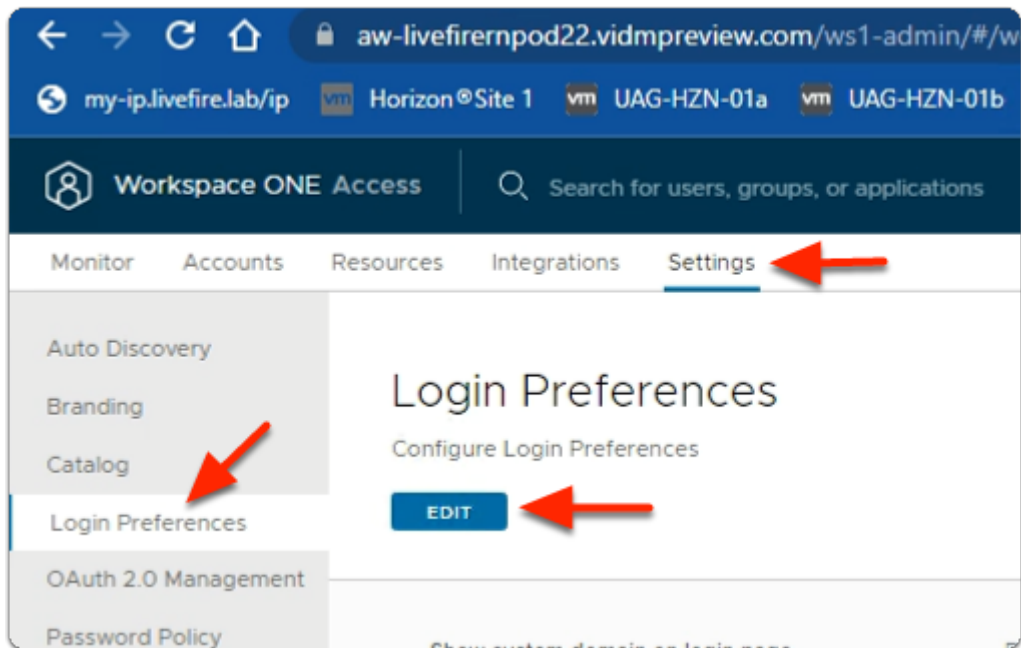
New Navigation

Integrations Settings

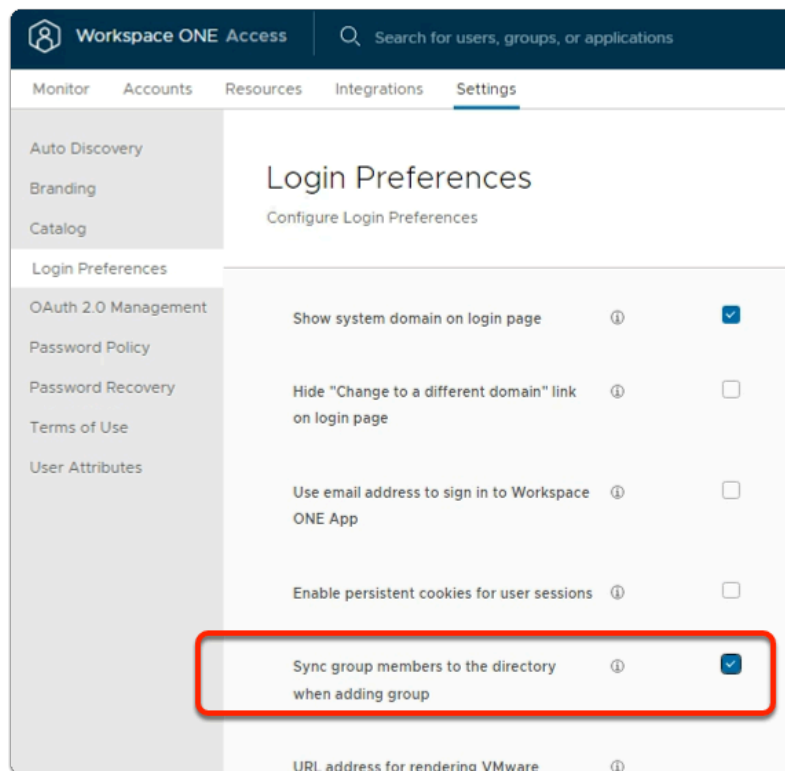
Directories (2)

Directory Name	Type	Domains	Synced Groups	Synced Users	Last Sync	Alerts
System Directory	Local Directory	1	0	1		
EUC-Livefire	Active Directory over LDAP	1	52	8	Oct 28, 2022 12:48:53 PM	1

17. On the **Directories** window
- **Refresh** your browser window
 - Note the **Synced Groups** and **Synced Users**

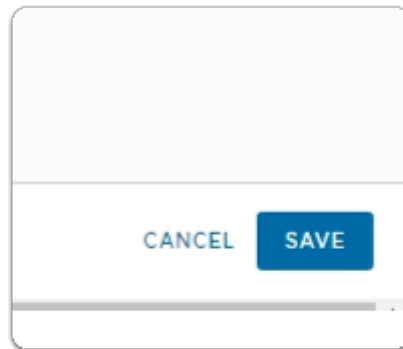


18. In your **Workspace ONE Access** admin console
- Select **Settings**
 - Select **Login Preferences**
 - Under **Login Preferences**
 - Select **EDIT**



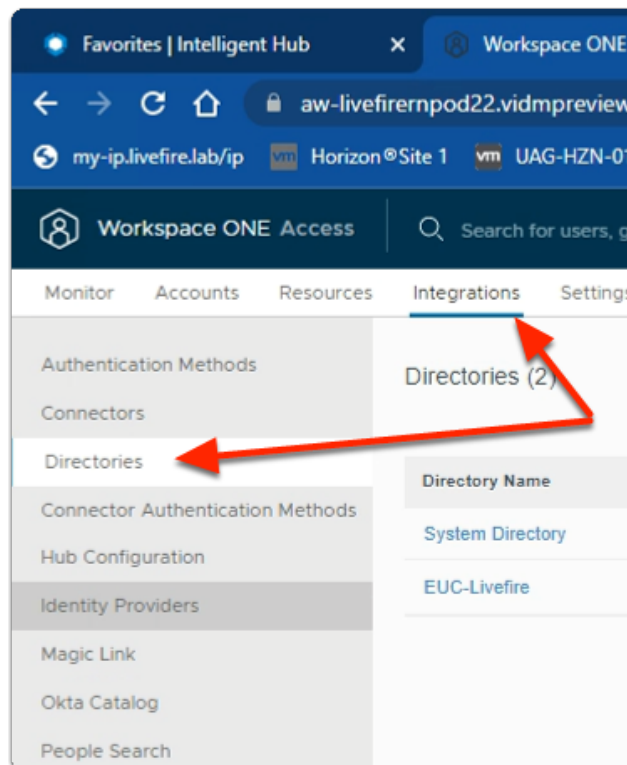
19. In the **Login Preferences** area

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



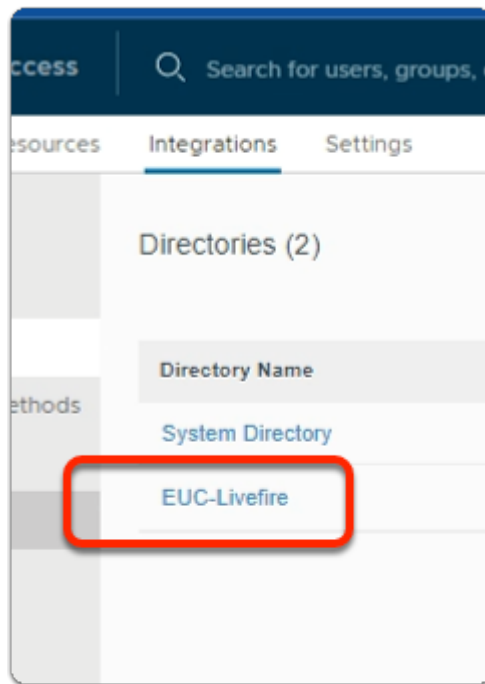
20. In the **Login Preferences** area

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

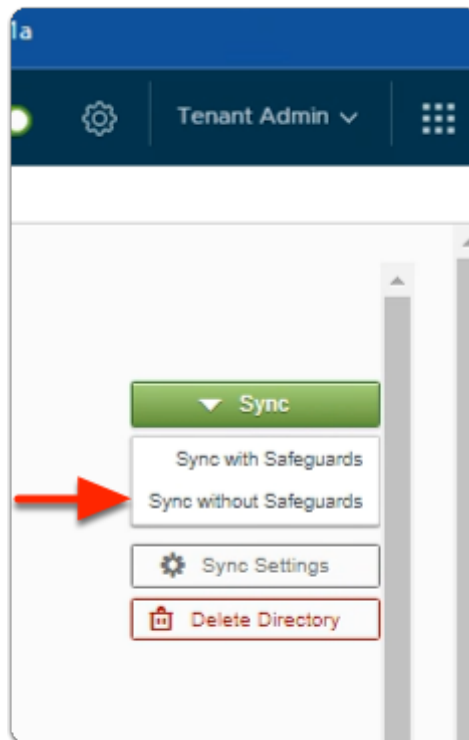


21. In the **Workspace ONE Access** console

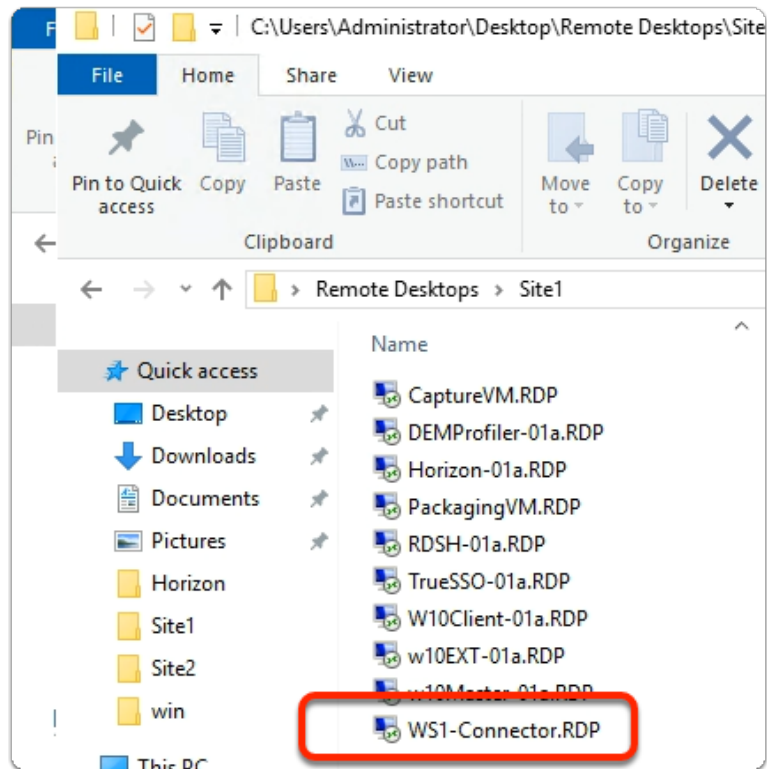
- select **Integrations**
 - select **Directories**



22. In the **Directories** area
- select **EUC-Livefire**

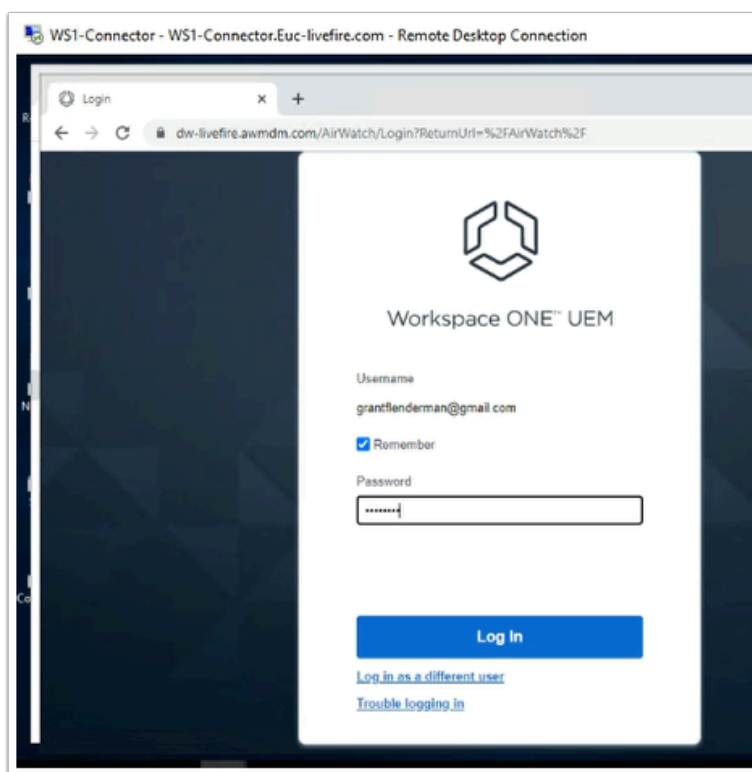


23. In the **EUC-Livefire** directory area
- In the right corner
 - Next to **Sync**
 - select the **dropdown**
 - select **Sync without Safeguards**



24. On your ControlCenter server
- On the **Desktop**
 - Open the **Remote Desktops\Site1** folder
 - Launch **WS1-Connector.RDP**

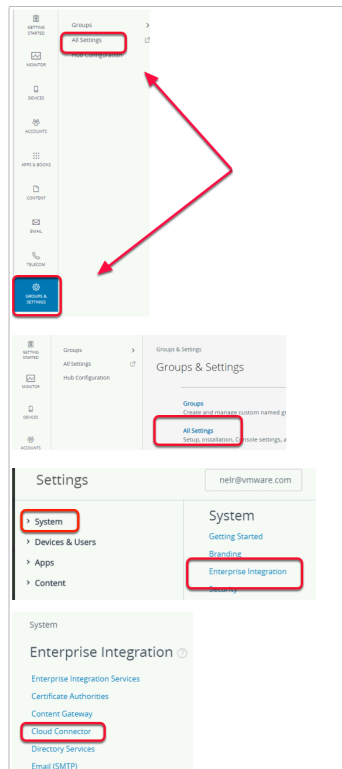
Part 1:Section 4: Configuring the AirWatch Cloud Connector



1. On the **WS1-Connector** desktop
 - Open your **chrome browser**
 - In the address bar, enter **dw-livefire.awmdm.com**,
 - Login using your **registered course email** (
 - **password VMware1!**

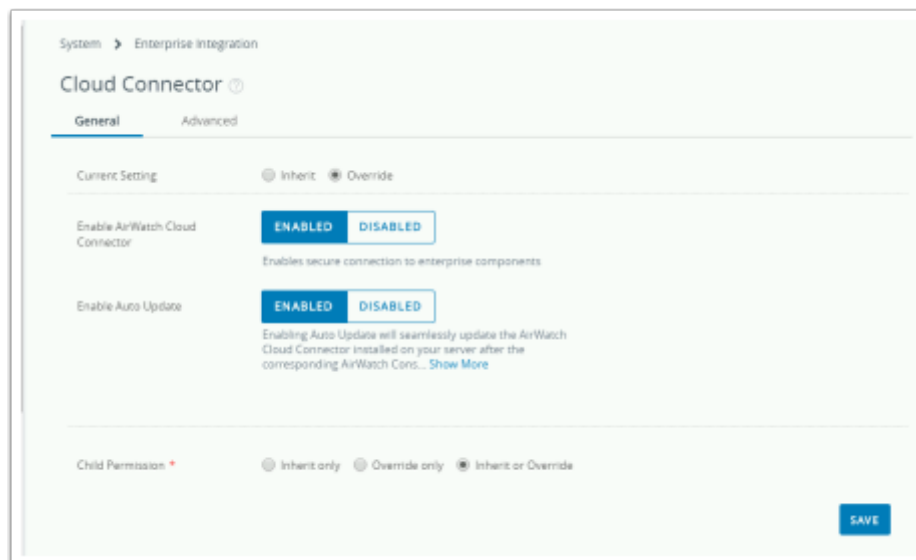
💡 If you are unclear what your registered course email is. Go back to your lab document you configured and filled in on Day 1, in the introduction

If you have not completed this, then please do



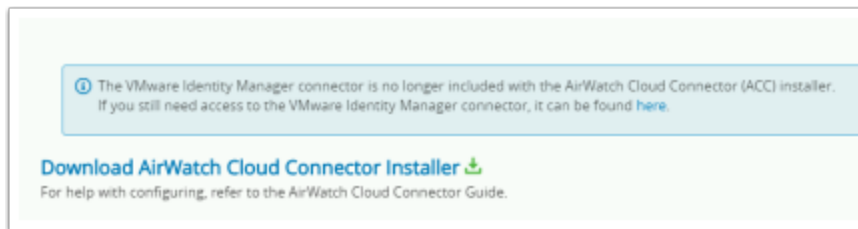
2. In the UEM Admin Console

- Navigate to **Groups & Settings** > **All Settings**
- Under **Settings** select **System** > **Enterprise Integration**
- Under **Enterprise Integration**
 - select **Cloud Connector**



3. In the Cloud Connector area

- Select the **Override** radio button
- Scroll down, select **Save** at the bottom of the page



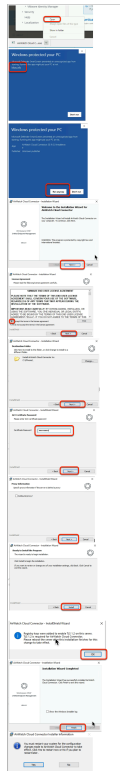
4. In the **Cloud Connector** area

- **Scroll down**
- Select the **Download AirWatch Cloud Connector Installer**

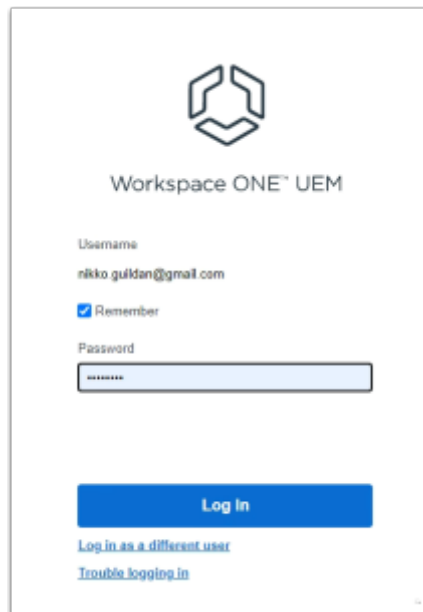
A screenshot of a dialog box titled "Download AirWatch Cloud Connector (ACC) Install...". Inside the dialog, there is a light blue information box at the top that says: "Password for the AirWatch Cloud Connector (ACC) certificate. You will need this to import the settings to a AirWatch Cloud Connector (ACC) server. Your password must be at least 6 characters in length." Below this, there are two password input fields. The first is labeled "Password" with a red asterisk, and the second is labeled "Confirm Password" with a red asterisk. Both fields have a "Show" button to their right. A red rectangle highlights these two input fields. At the bottom right of the dialog, there is a blue "DOWNLOAD" button, also highlighted with a red rectangle.

5. On the **Download AirWatch Cloud Connector (ACC-installer.exe)**

- Type **VMware1!** in the **Password** and **Confirm Password** boxes.
- Select **DOWNLOAD**

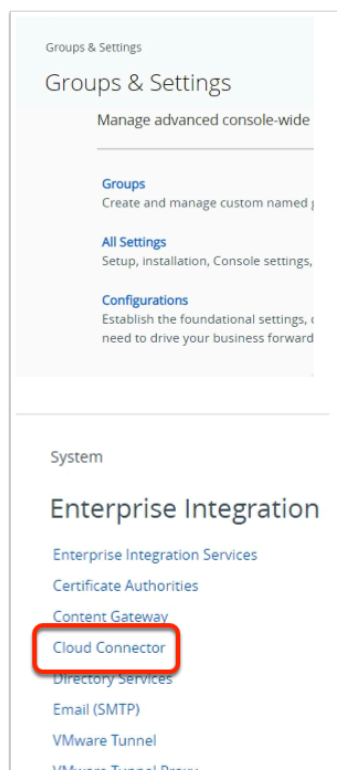


6. On the **WS1-Connector** machine,
 - Select the Select **Airwatch Cloud Connector.exe**
 - Select **open**
 - Select **More Info**
 - Select **Run Anyway**
 - Select **Next**
 - Select the **licensing to accept terms...** **radio button** , select **Next**
 - Select **Next**
 - In the **ACC Certificate Password** window
 - type the password **VMware1!**
 - select **Next**
 - Select **Next**
 - Select **Install**
 - Select **OK**
 - Select **Finish**
 - Select **Yes**
 - Wait for the **WS1-Connector** server to reboot
 - RDP to the server and re-login



7. On your ControlCenter server

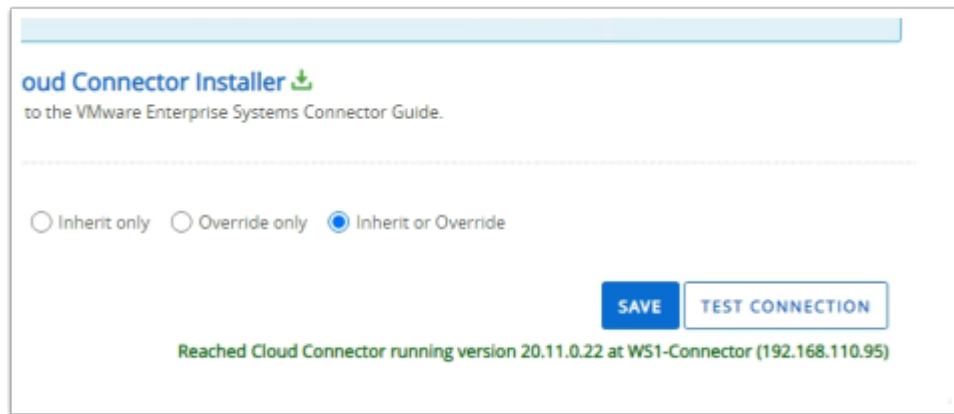
- Open a **new tab** on your Chrome browser
- Enter **dw-livefire.awmdm.com** in your address bar
- Login with your **custom email username**
- Enter your **custom Password**
- Select **Log In**



8. In the UEM Admin Console

- Go to **Groups & Settings > All Settings**
- Under **System**, select **Enterprise Integration**

- Under **Enterprise Integration**, select **Cloud Connector**

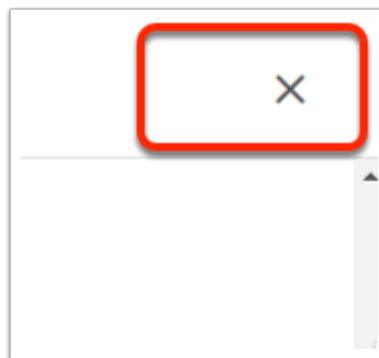


9. In the Cloud Connector window

- Scroll down
- Select **TEST CONNECTION**

Note the screenshot

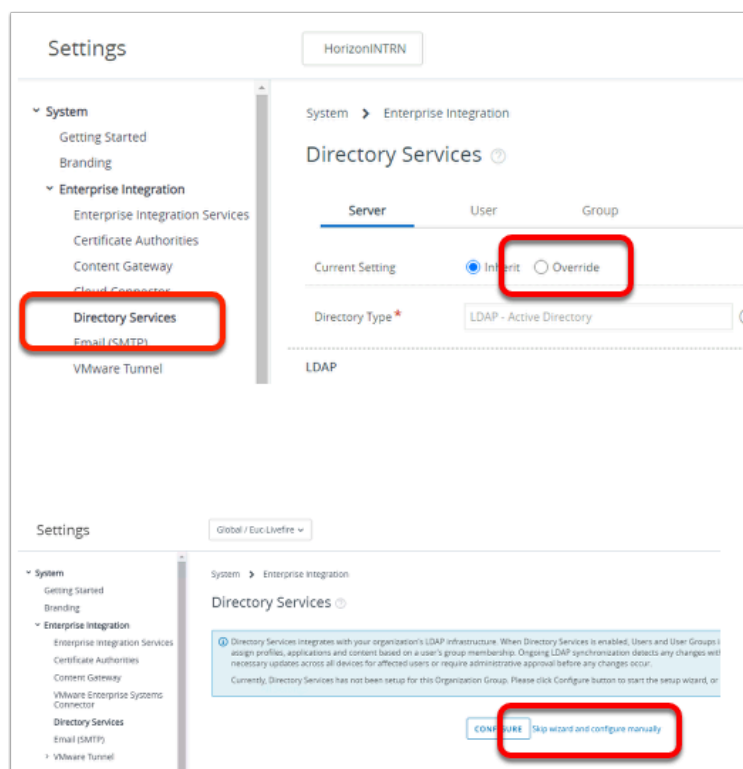
Your environment should also reflect that the Cloud Connector has been reached



10. In the Cloud Connector window

- Select the **X** to right to close the window

Part 1:Section 5: Workspace ONE UEM & Active Directory Integration



1. In the Workspace ONE UEM admin console
 - Select **Groups & Settings > All Settings > System > Enterprise Integration**
 - Under **Enterprise Integration**
 - Select **Directory Services**
 - In the **Directory Services** window
 - Select the **Override radio button**
 - Select **Skip wizard and configure manually**

The screenshot displays the 'LDAP - Active Directory' configuration page. At the top, a dropdown menu is set to 'LDAP - Active Directory'. Below this, there are two tabs: 'ENABLED' (selected) and 'DISABLED'. The 'controlcenter.euc-liveware.com' is entered in the 'Server' field. Under the 'NONE', 'SSL', and 'START TLS' tabs, 'NONE' is selected. The 'Port' is set to '389' and the 'Base DN' is set to '3'. Below these, there are two more tabs: 'ENABLED' (selected) and 'DISABLED'. Under the 'ANONYMOUS', 'BASIC', 'DIGEST', 'KERBEROS', 'NTLM', and 'GSS-NEGOTIATE' tabs, 'GSS-NEGOTIATE' is selected. The 'Bind User Name' is set to 'administrator'. There is a checkbox for 'Bind Password' which is unchecked. The 'Bind Password' field is masked with asterisks and has a 'CHANGE' button next to it. At the bottom, the 'Domain' is set to 'euc-liveware.com' and the 'Server' field is empty.

2. From the **Directory Services** Interface,
 - Under the **Server Tab** , **enable the** following .
 - Directory Type*: **LDAP-Active Directory**
 - DNS SRV: **Disabled (default)**
 - Server : **ControlCenter.euc-liveware.com**
 - Bind User Name: **administrator**
 - Bind Password: **VMware1!**
 - Domain: **euc-liveware.com**

System > Enterprise Integration

Directory Services ?

Server **User** Group

Current Setting ☐ Inherit ☒ Override

Domain euc-livewire.com Base DN* DC=euc-livewire,dc=com +

User Object Class* person ⓘ

User Search Filter* (&(objectCategory=person)(sAMAccountName={EnrollmentUser})) ⓘ

3. From the **Directory Services** Interface,
 - Under the **User Tab** ,
 - Validate the following configuration is configured
 - Under **Base DN**,
 - ensure that **DC=euc-livewire,DC=com** has automatically populated.
 - If not, click on the **+** icon
 - add **DC=euc-livewire,DC=com**
 - Next to **User Object Class**,
 - ensure **person** is the property
 - Next to **User Search Filter**,
 - ensure **(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))** is the string

Current Setting ☐ Inherit ☒ Override

Domain: euc-livfire.com Base DN*: DC=euc-livfire,DC=com

Group Object Class*: group

Organizational Unit Object Class*: organizationalUnit

> Advanced

Child Permission ☐ Inherit ☐ Override ☒ Inherit or Override

Test Connection ☒ X

livfire.com Connection successful with the given server name, bind username, and password.

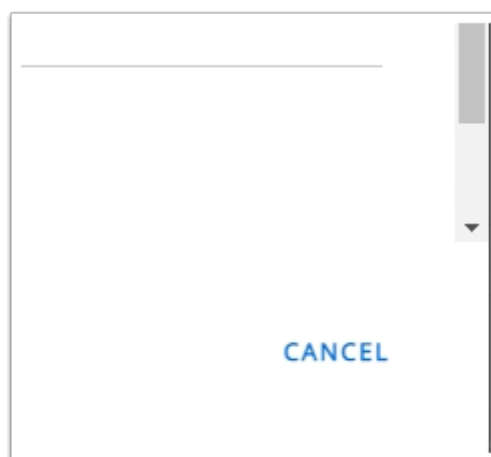
TEST AGAIN

User Group

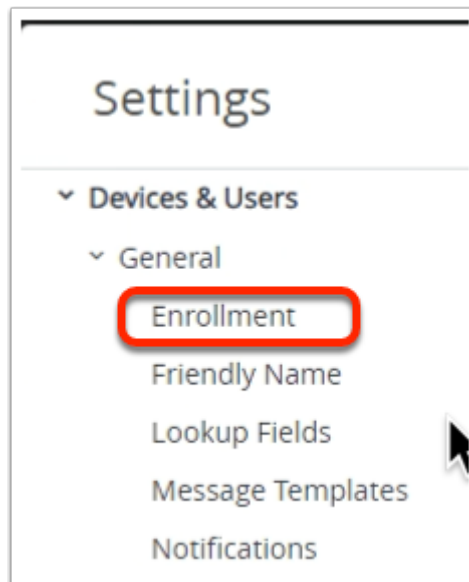
Domain: euc-livfire.co

CANCEL

4. From the **Directory Services** Interface,
 - Repeat these steps for the third tab **Group**
 - Under **Base DN**,
 - notice validate that **DC=euc-livfire,DC=com**, is entered.
 - **Scroll** to the bottom of the page
 - select **Save**
 - **Scroll** to the bottom of the page
 - Select **TEST CONNECTION**

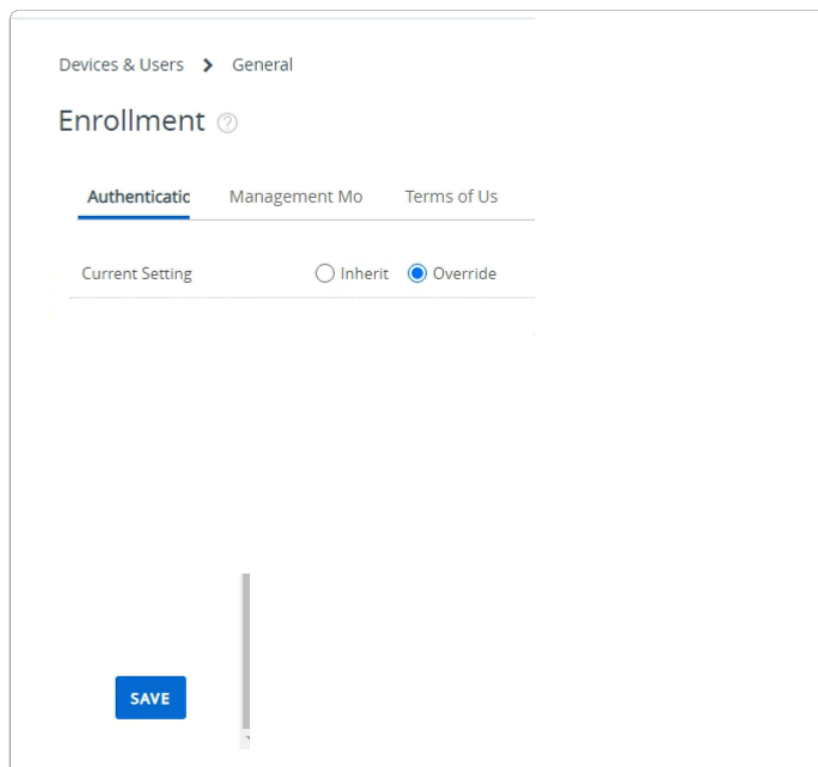


5. You should have a **Test Connection** window launch saying **Connection successful....**
 - Select **CANCEL** to close the window



6. Let's ensure users can enroll their devices using Active Directory credentials.

- Under **Settings** ,
 - select **Devices & Users**
 - Select > **General**
 - Select > **Enrollment**



7. Under the **Enrollment** area

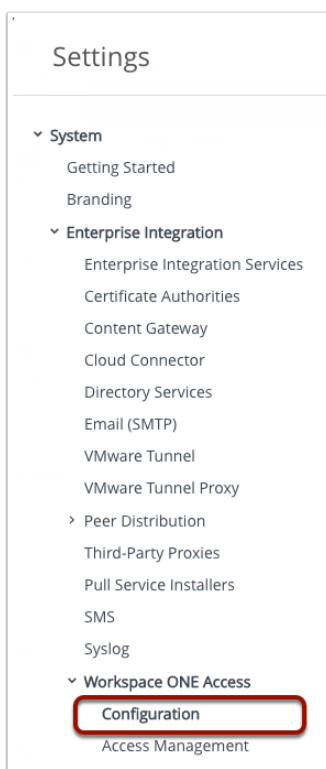
- Select the **Override** radio button
- **Scroll down.**

The screenshot shows a settings window for the Intelligent Hub. It contains three main sections: 'Authentication Mode(s)' with checkboxes for 'Basic' (checked), 'Directory' (checked), and 'Authentication Proxy' (unchecked); 'Source of Authentication for Intelligent Hub' with two tabs, 'WORKSPACE ONE UEM' and 'WORKSPACE ONE ACCESS' (selected); and 'Devices Enrollment Mode' with radio buttons for 'Open Enrollment' (selected) and 'Registered Devices Only' (unchecked). At the bottom, there is a blue 'SAVE' button and a link labeled 'Inherit or Override'.

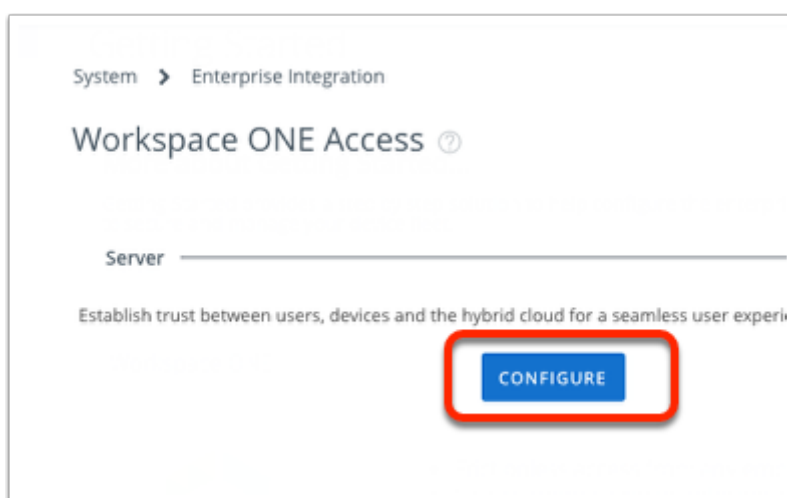
8. Under the **Enrollment** area

- In line with **Authentication Modes(s)**
 - ensure the the **Directory** check box is selected
- In line with **Source of Authentication for Intelligent Hub**,
 - select **Workspace ONE ACCESS**
- **Scroll down**
 - Select **SAVE**
- Close the **Settings** window,
 - by selecting the **X** on the right of the window

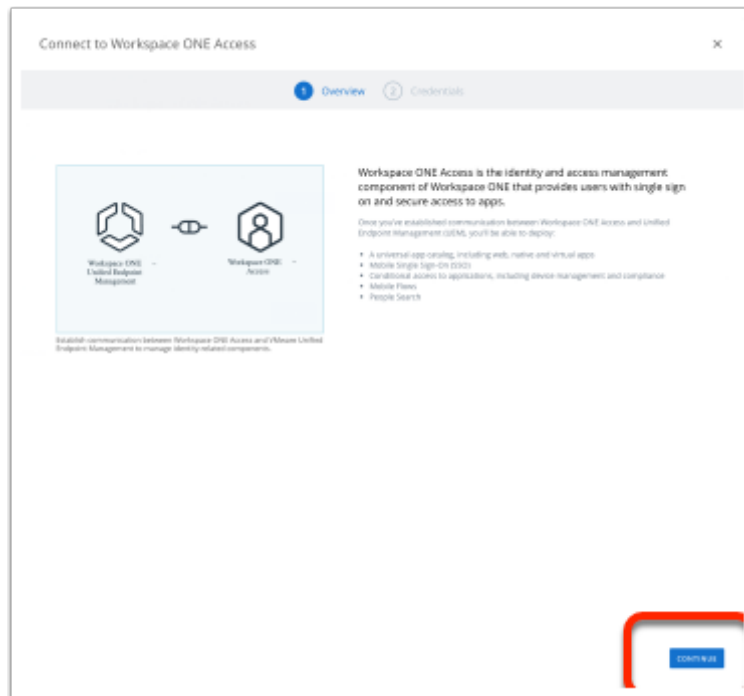
Part 1:Section 6: Workspace ONE Access and Workspace ONE UEM Integration



1. In your **Workspace ONE UEM Admin** console
 - Navigate to **Groups and Settings > All Settings > System > Enterprise Integration > Workspace ONE Access > Configuration**



2. Under the **Server** area,
 - Select **CONFIGURE**



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

Connect to Workspace ONE Access

Overview 2 Credentials

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

Tenant URL *

Username *

Password *

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

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

TEST CONNECTION

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

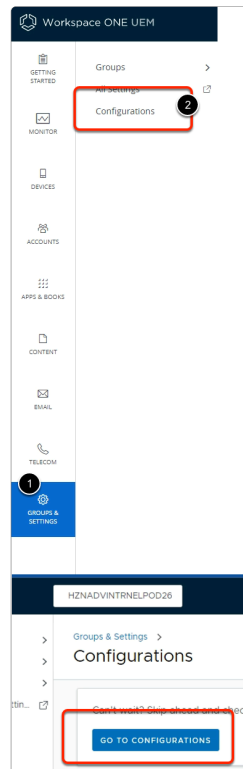
TEST CONNECTION

Test connection successful!

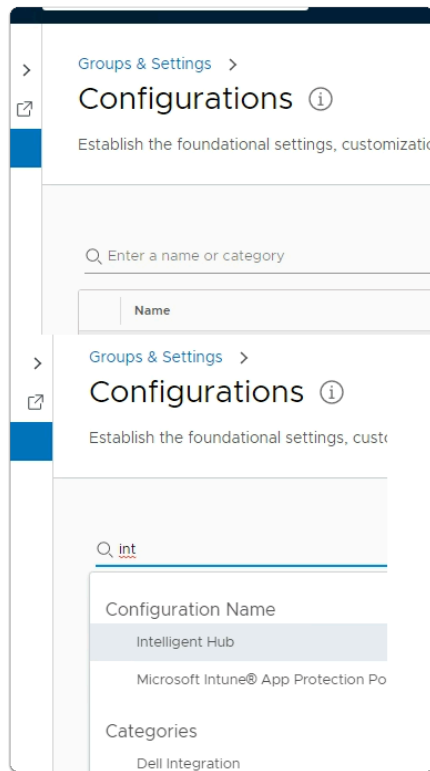
BACK SAVE

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

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

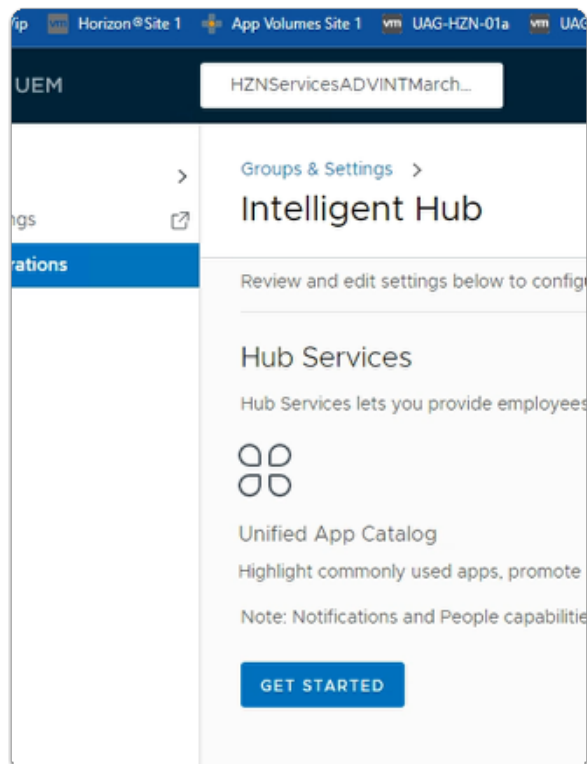


5. In the Workspace ONE UEM admin console
 1. Select **GROUPS & SETTINGS**
 2. Select **Configurations**
 3. In the **Group & Settings > Configurations** window
 - Select **GO TO CONFIGURATIONS**



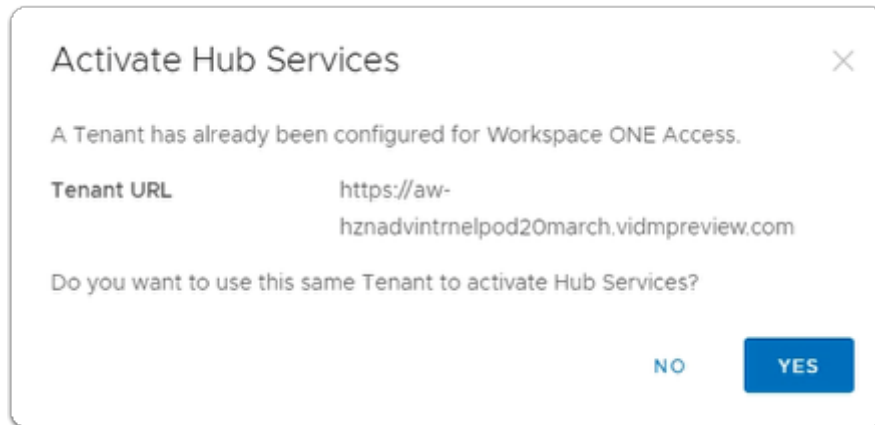
6. Under **Configurations**

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



7. Under **Hub Services**

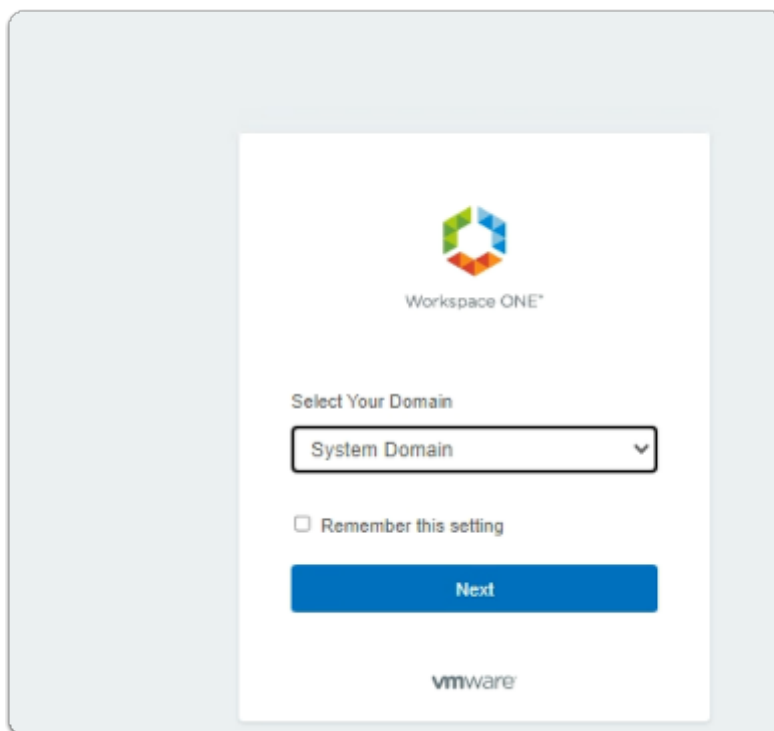
- Select **GET STARTED**



8. In the **Activate Hub Services**

- Select **YES**

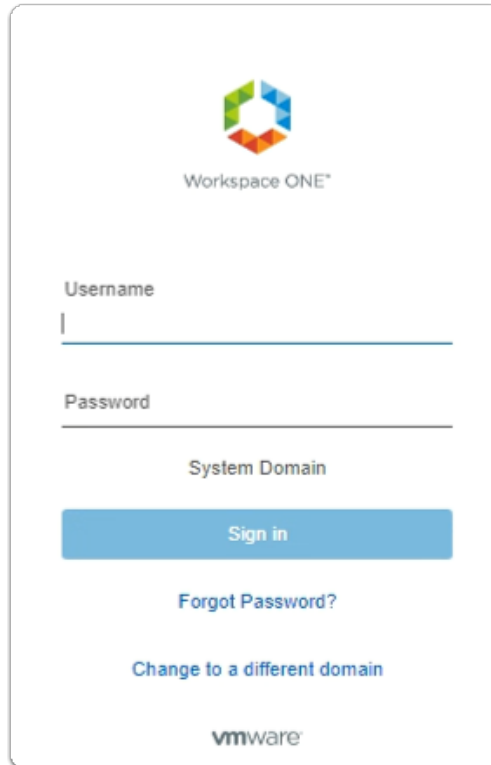
Part 1:Section 7: Workspace ONE Hub Services Integration with Workspace ONE Access



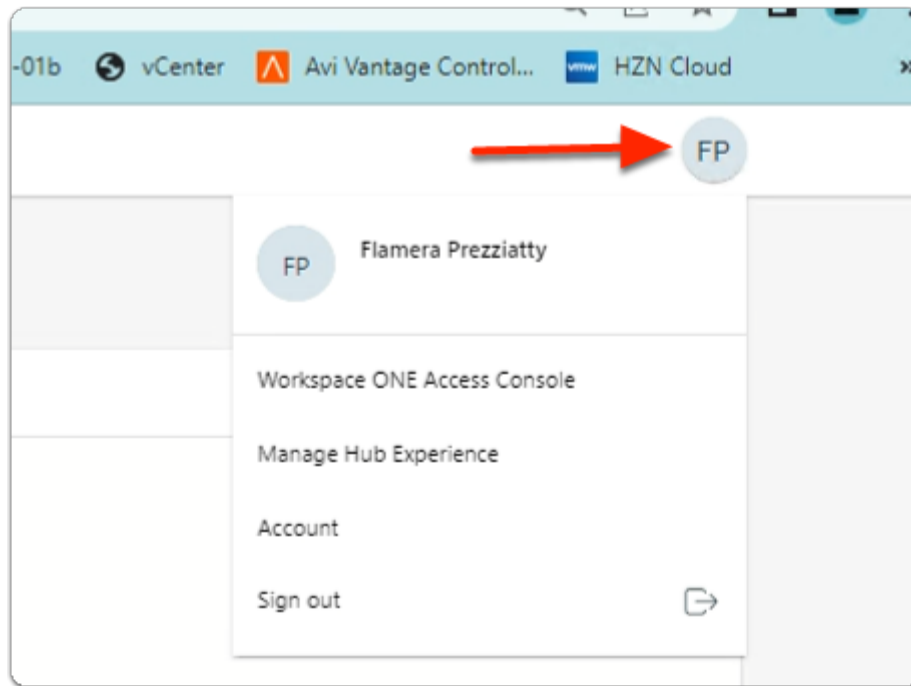
1. On your ControlCenter server

- **Open** a new tab on your Browser
- Paste your **custom Workspace ONE Access URL** in the address bar
- **Launch** your **custom Workspace ONE Access URL**
- In the **Select Your Domain** window

- Ensure **System Domain** is selected
- Select **Next**

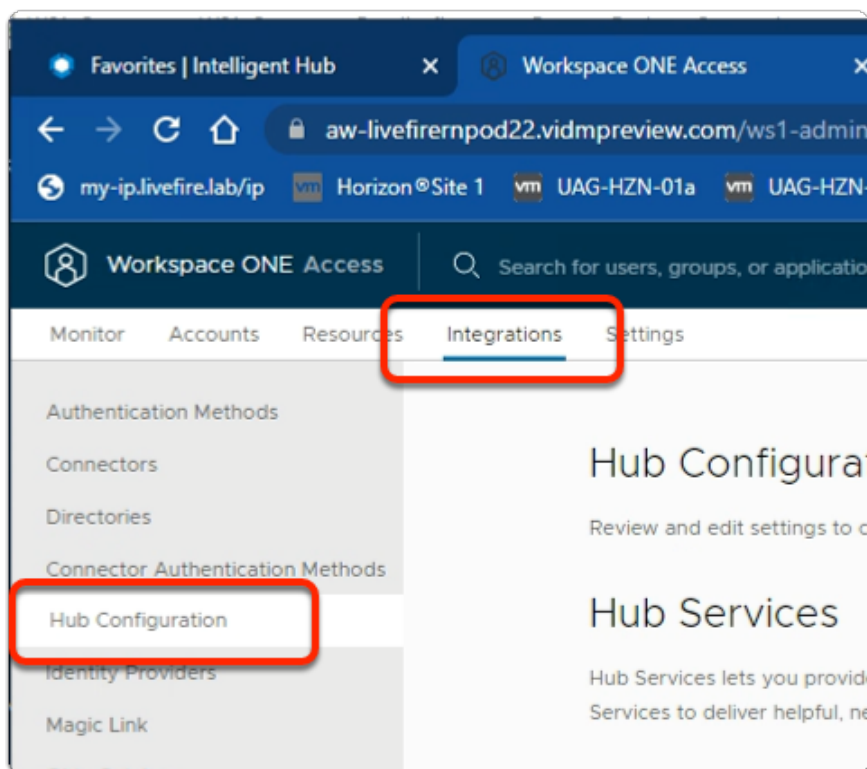
The image shows a login form for Workspace ONE. At the top is the Workspace ONE logo, which consists of a hexagon made of six colored triangles (green, blue, orange, red, yellow, and purple). Below the logo is the text "Workspace ONE". The form has two input fields: "Username" and "Password". Below these fields is a dropdown menu labeled "System Domain". There is a blue "Sign in" button. Below the button are two links: "Forgot Password?" and "Change to a different domain". At the bottom of the form is the VMware logo.

2. In the **Workspace ONE Access** login
 - Under **Username**
 - Enter your **custom SysAdmin username**
 - Under **Password**
 - Enter **VMware1!** (hopefully that is what you have changed it to)
 - Select **Sign in**



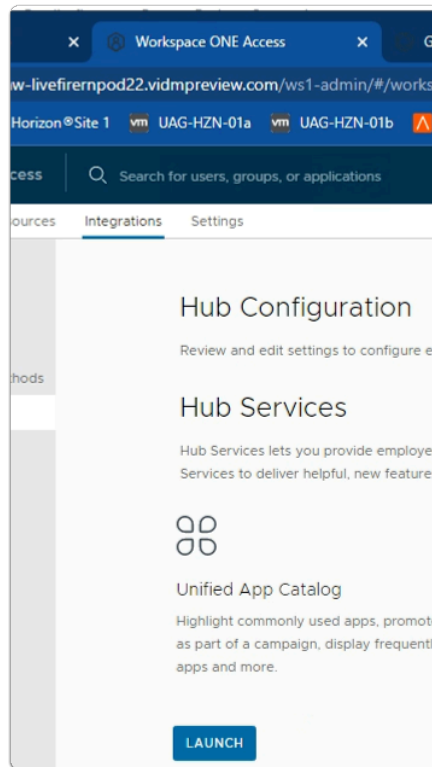
3. In the Web version of **Intelligent Hub**

- In the top right - corner
 - Select and right-click your **Sysadmin Initial Icon**
 - Select **Workspace ONE Access Console**



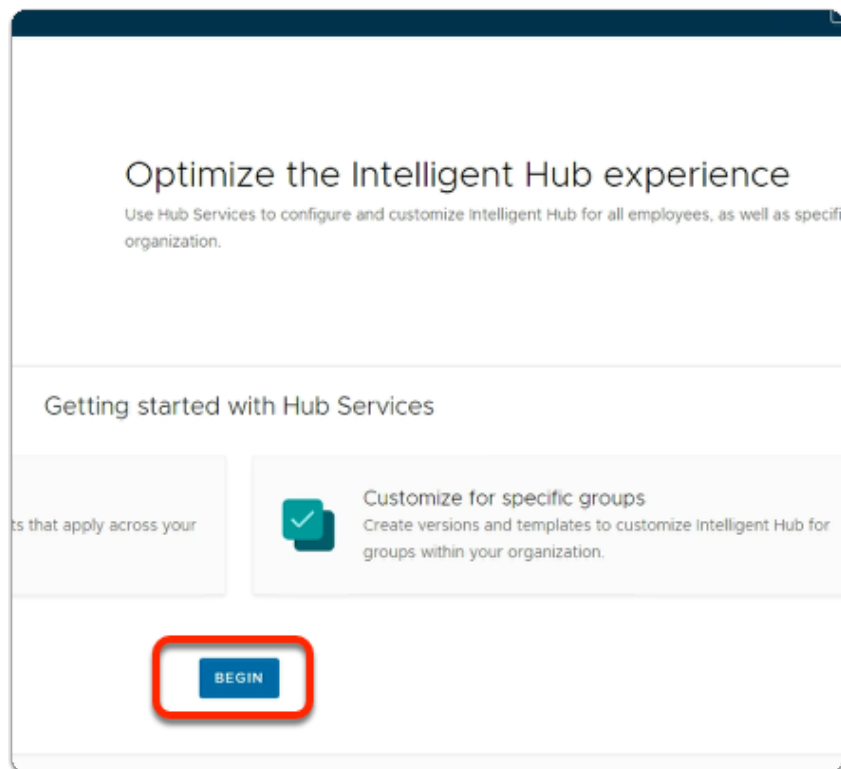
4. In the **Workspace ONE Access admin** console

- Select **Integrations**
- Select **Hub Configuration**



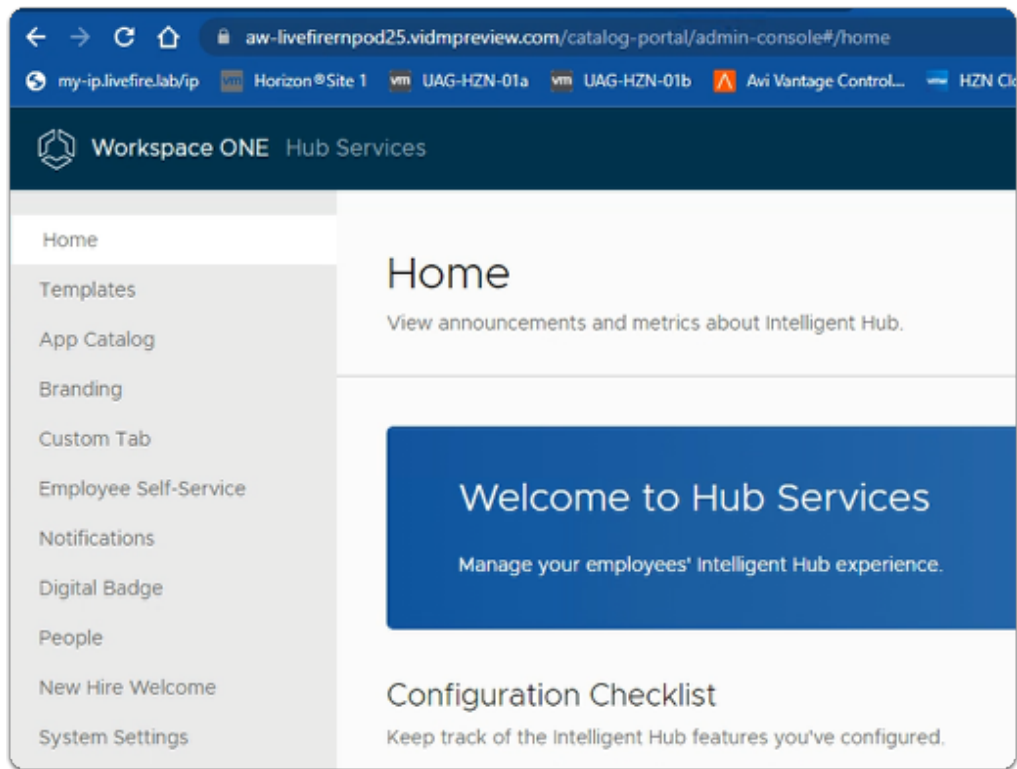
5. In the **Hub Configuration** window

- Under **Hub Services**
 - Select **LAUNCH**



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

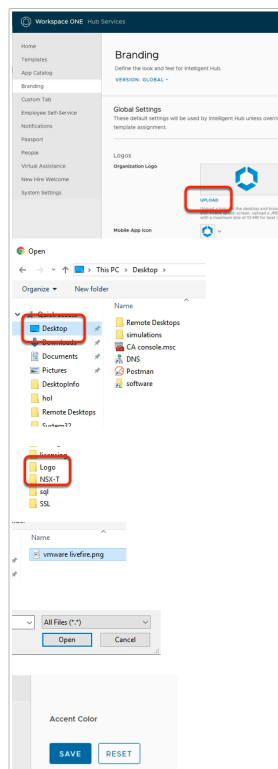
- Select **BEGIN**



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

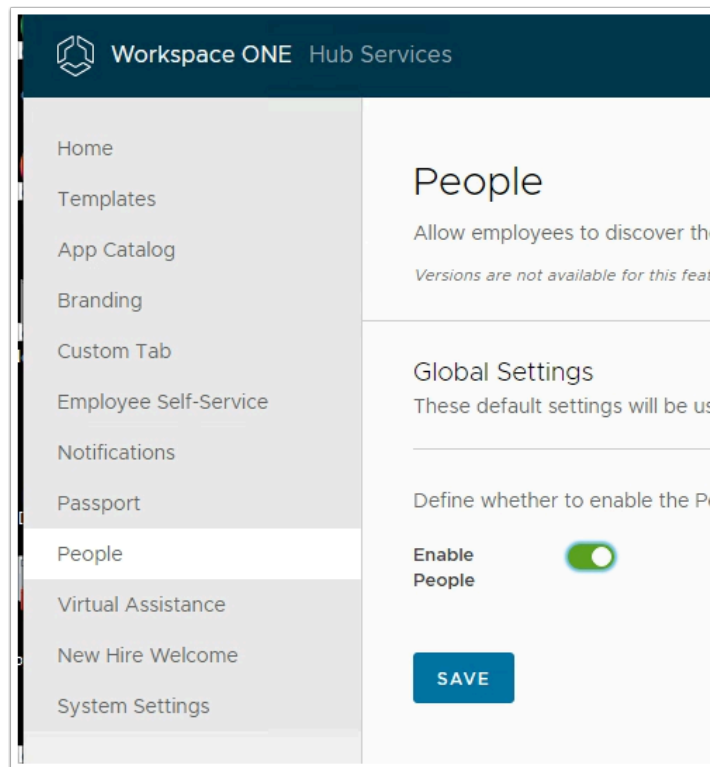
- Review the associated options.
- In Section 8: We will configure Hub Services

Part 1:Section 8: Configuring Workspace ONE Hub Services

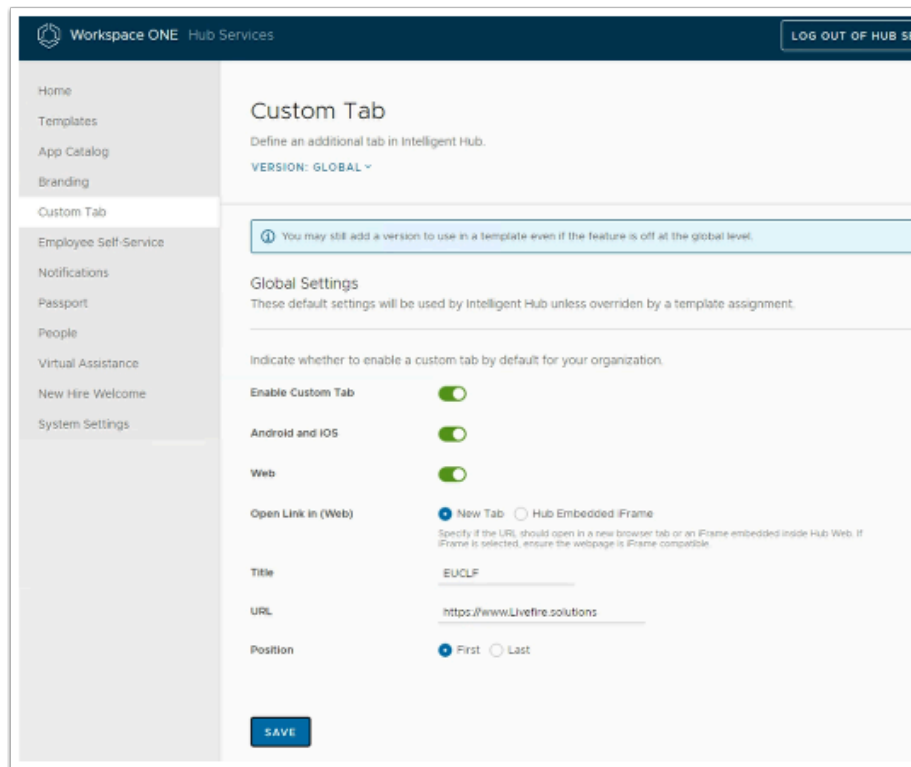


1. In **Workspace ONE Hub Services**

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

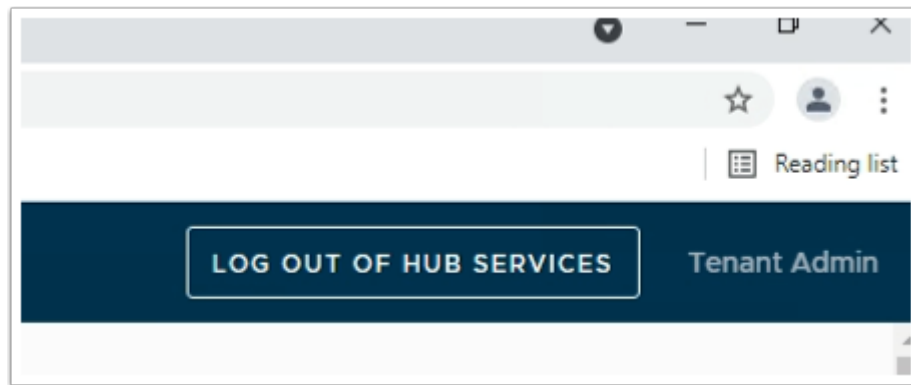


2. In the **Workspace ONE Hub Services** page
 - In the left pane, select **People**
 - Under **People** area,
 - next to **Enable People**,
 - move the **toggle** to the right
 - Select **SAVE**



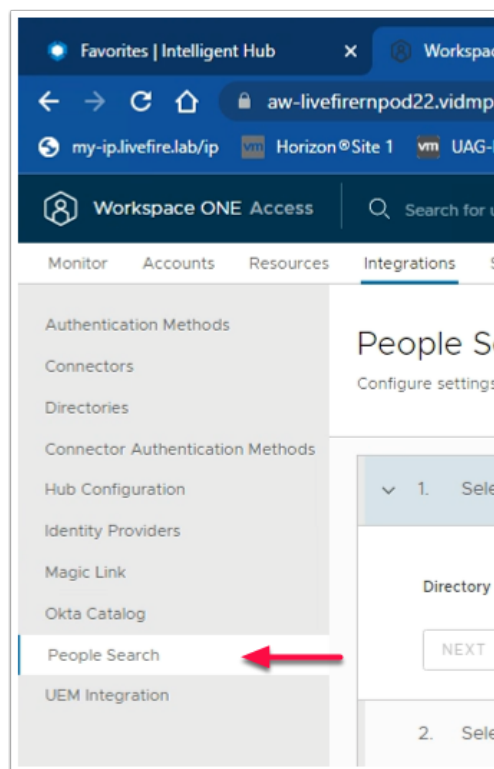
3. In the **Workspace ONE Hub Services** page

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



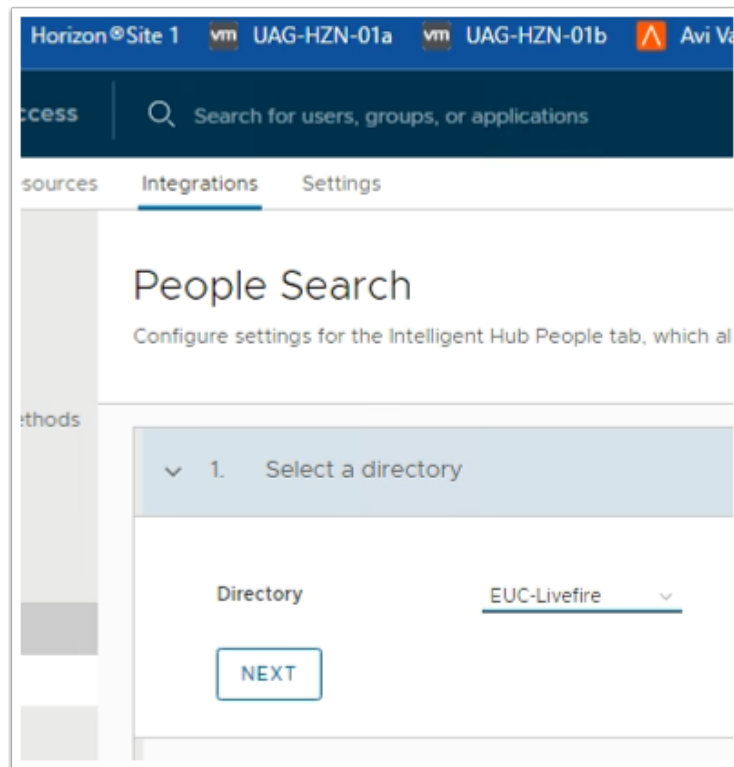
4. To the top right of the **Workspace ONE Hub Services** page

- Select **LOG OUT OF HUB SERVICES**

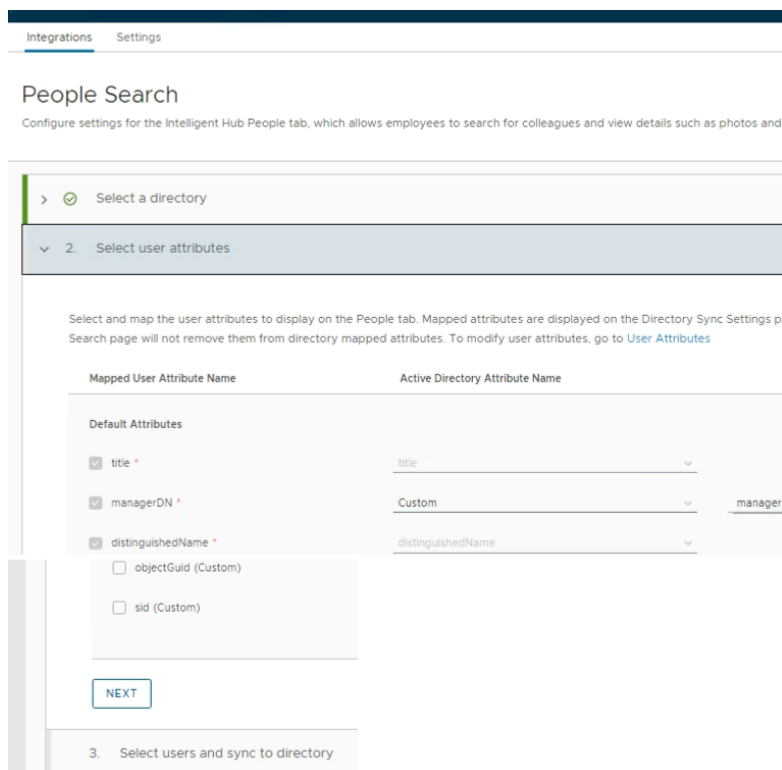


5. In the **Workspace ONE Access** Console

- Under **Integrations**
 - Select **People Search**



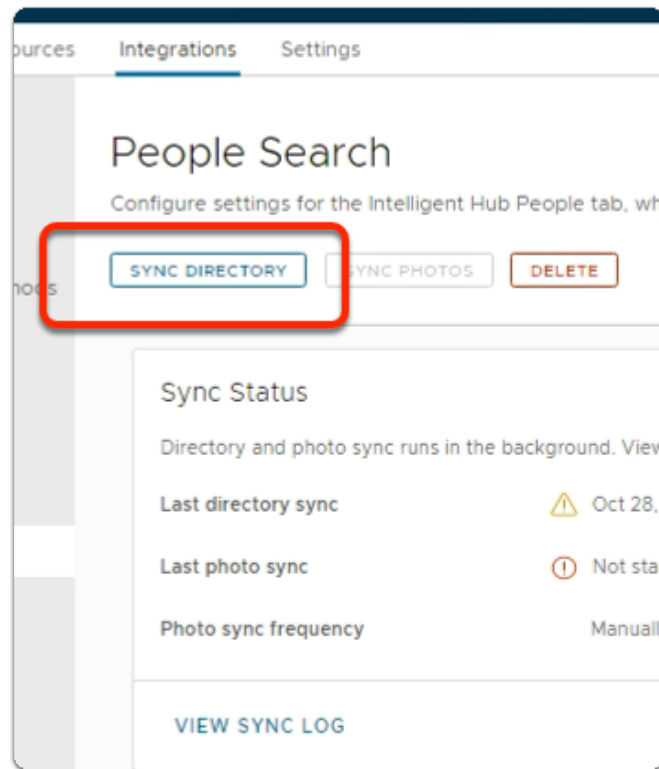
6. In the **People Search** area
 - Next to Directory,
 - from the dropdown
 - Select the **EUC-Livefire**
 - Select **NEXT**



7. In the **People Search** page
- Step 2 **Select User attributes**
 - note the attributes
 - **Scroll down**
 - In the bottom left
 - Select **NEXT**

The screenshot shows the 'People Search' configuration page. At the top, there are tabs for 'ces', 'Integrations', and 'Settings'. The main heading is 'People Search' with a subtitle 'Configure settings for the Intelligent Hub People tab, which allows employee'. Below this, there is a list of steps: 1. Select a directory (checked), 2. Select user attributes (checked), and 3. Select users and sync to directory (expanded). Under step 3, there is a text input field for 'User DNs' with the value 'ou=corp,dc=EUC-Livefire,dc=com' and an example 'Ex: *CN=admin,CN=users,DC=mycompany,DC'. There is an 'ADD' button next to the input field. At the bottom, there are two buttons: 'SAVE & SYNC' and 'SAVE'.

8. In the **People Search** page`
- Step 3 **Select users and sync to directory**
 - review the User DNs
 - It should read
 - **ou=corp,DC=euc-livefire,DC=com**
 - Select **SAVE & SYNC**



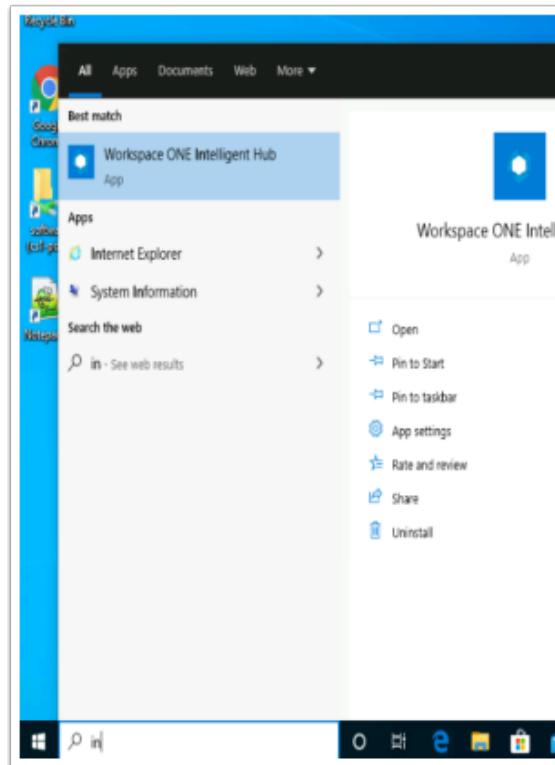
9. Under **People Search**

- Select **SYNC DIRECTORY**

Part 1:Section 9: Enrolling Intelligent Hub on Microsoft Windows 10

i Step 1 : Enrolling W10Client-01a on Site 1 with the Active Directory Domain User Mark

💡 Steps 1 - 4 could all be done in parallel, So whilst waiting for enrollment to complete on one virtual machine, feel free to move on the next step



1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the **Site1** folder
 - Select the **W10Client-01a RDP** client and
 - Sign-in with
 - **username: mark@euc-livewire.com**
 - **Password: VMware1!**
 - To the right of the **Start** button
 - in the **search** area,
 - start typing **intel**
 - Select the **Workspace ONE Intelligent Hub**
 - Please Note! If the **Workspace ONE Intelligent Hub** does not load,
 - From the **RUN > Services.msc > Start the Airwatch** service
 - Attempt to **re-launch** the hub

Workspace ONE Intelligent Hub

Email or Server Address

<https://dw-livefire.awmdm.com>

Next

2. Under **Email or Server Address**,
 - Enter <https://dw-livefire.awmdm.com>
 - Select **Next**

Groups & Settings > Groups

HorizonNTRN

Organization Group
HorizonNTRN
Group ID
HorizonNTRN

Workspace ONE UEM

GETTING STARTED

Groups

All Settings

Configurations

MONITOR

Workspace ONE Intelligent Hub

Email or Server Address

<https://dw-livefire.awmdm.com>

Group ID

HorizonNTRN

Next

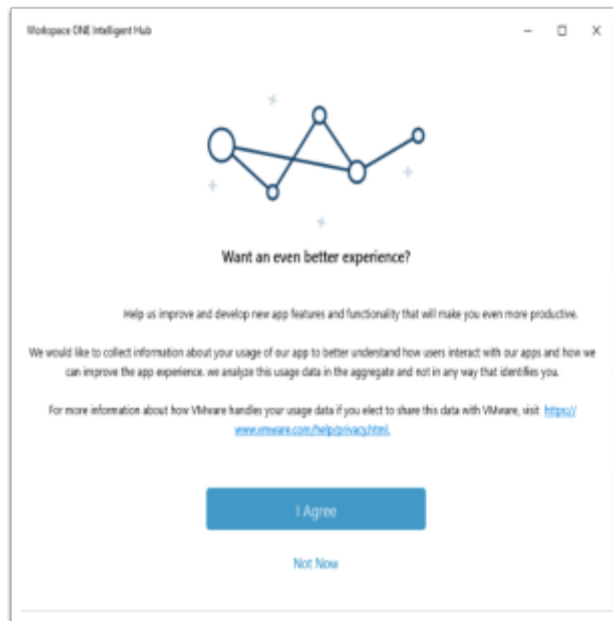
Cancel

3. Under **Group ID** unique enter your unique your **Workspace ONE UEM** tenant Group ID

- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE UEM** tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select **NEXT**

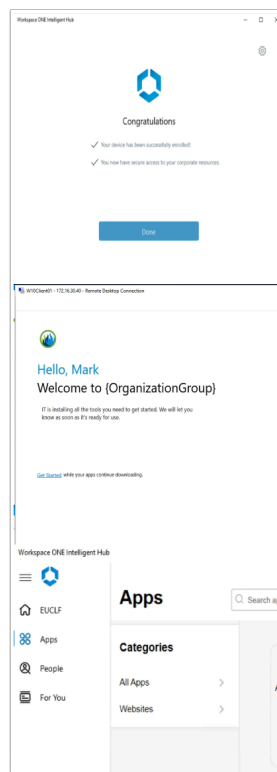
4. In the **Workspace ONE Intelligent Hub** under

- Under **Select Your Domain**
 - Select **euc-livewire.com**
 - Select **Next**
- Under the **Username** area
 - Enter **Mark**
- Under the **Password** area
 - Enter **VMware1!**
- Select **Sign in**



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

- Select **I Agree**

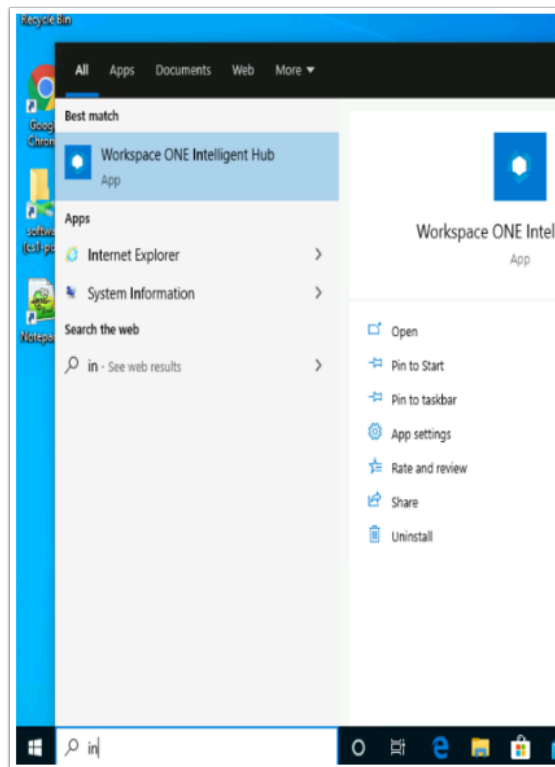


6. On the **Congratulations** window,

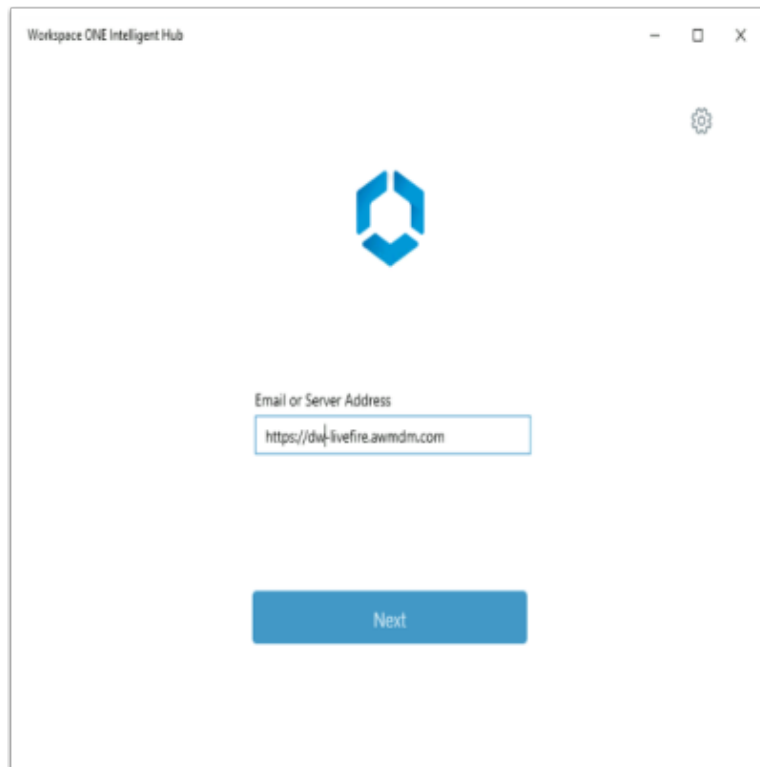
- Select **Done**
- **Re-open** the Intelligent Hub
- Select **Get Started**



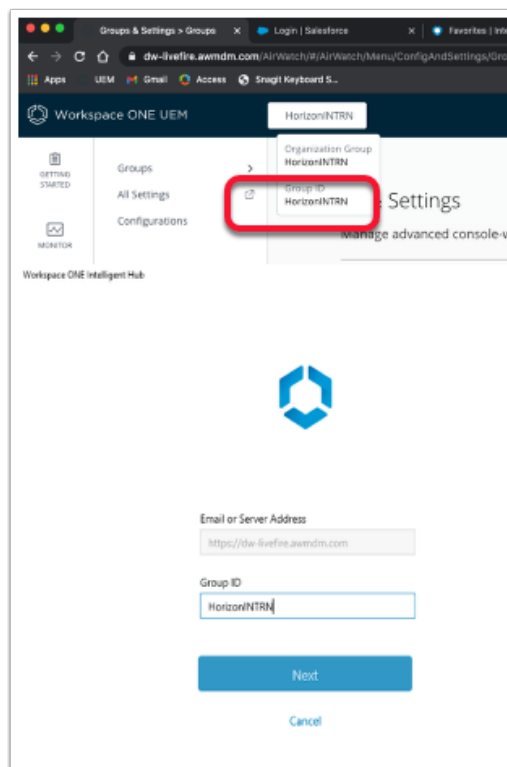
Step 2 : Enrolling W10Ext-01a on Site 1 with the Active Directory Domain User Jill



1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the **Site1** folder
 - Select the **W10EXT-01a.RDP** client and
 - Sign-in with
 - **username** **jill@euc-livewire.com**
 - **Password** **VMware1!**
 - To the right of the **Start** button in the search area, start typing **intel**
 - Select the **Workspace ONE Intelligent Hub**
 - Please Note! If the **Workspace ONE Intelligent Hub** does not load,
 - From the **RUN > Services.msc > Start the Airwatch service**
 - Attempt to **re-launch** the hub



2. Under **Email or Server Address**,
- Enter <https://DW-livfire.awmdm.com>
 - Select **Next**



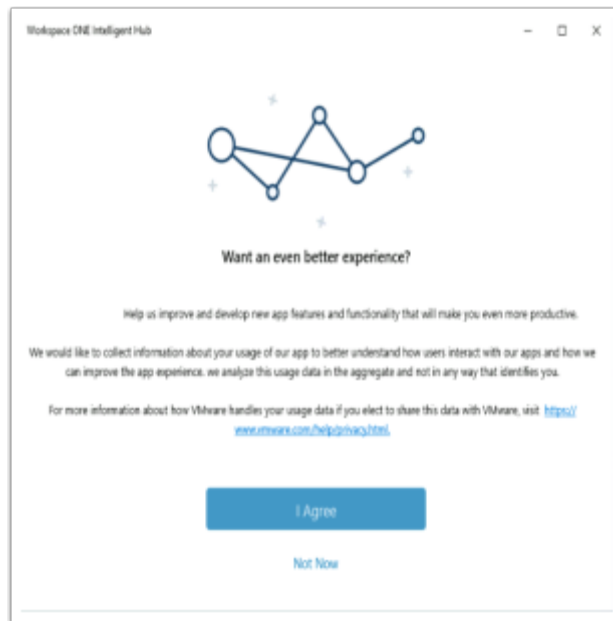
3. Under **Group ID** unique enter your unique your **Workspace ONE UEM** tenant Group ID

- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE UEM** tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select **NEXT**

The screenshot displays the Workspace ONE UEM login screen. At the top, the Workspace ONE logo is visible. Below it, the text 'Select Your Domain' is followed by a dropdown menu showing 'euc-livewire.com'. A checkbox for 'Remember this setting' is present. A blue 'Next' button is located below the domain selection. The lower portion of the screen features the 'VMware Workspace ONE' logo, a 'username' field containing 'jill', a 'password' field with masked characters, and a blue 'Sign In' button. Links for 'Forgot password?' and 'Change to a different domain' are provided, along with a 'Cancel' button at the bottom.

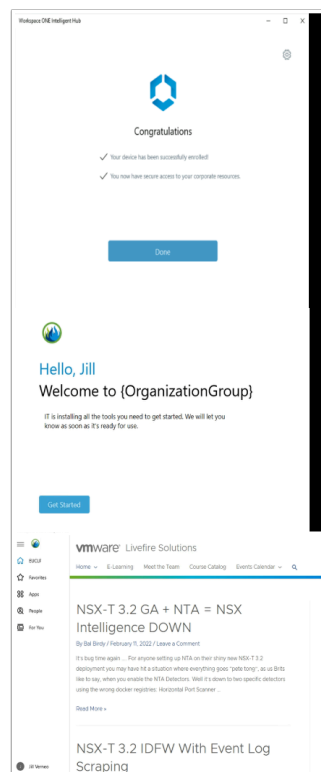
4. In the **Workspace ONE Intelligent Hub** under

- Under **Select Your Domain**
 - Select **euc-livewire.com**
 - Select **Next**
- Under the **Username** area
 - Enter **jill**
- Under the **Password** area
 - Enter **VMware1!**
- Select **Sign in**



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

- Select **I Agree**

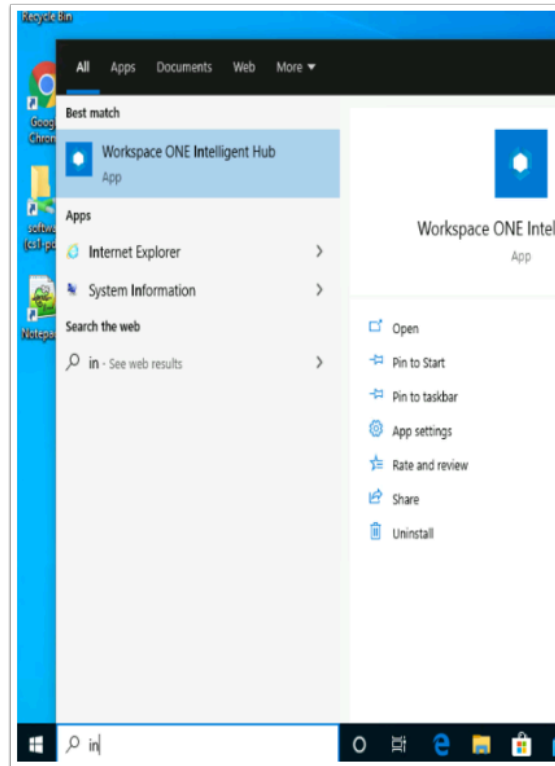


6. On the **Congratulations** window,

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



Step 3 : Enrolling W10Client-02a on Site 2 with the Active Directory Domain User Fernando



1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the **Site2** folder
 - Select the **W10Client-02a RDP** client and
 - Sign-in with
 - **username fernando@euc-livefire.com**
 - **Password VMware1!**
 - Select **OK**
 - To the right of the **Start** button in the search area, start typing **intel**
 - Select the **Workspace ONE Intelligent Hub**
 - Please Note! If the **Workspace ONE Intelligent Hub** does not load,
 - From the **RUN > Services.msc > Start the Airwatch service**
 - Attempt to **re-launch** the hub

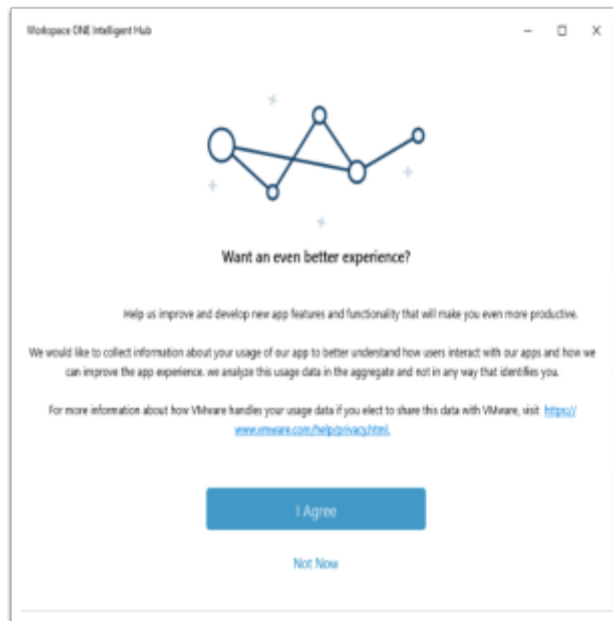
2. Under **Email or Server Address**,
 - Enter <https://dw-livfire.awmdm.com>
 - Select **Next**

3. Under **Group ID** unique enter your unique your **Workspace ONE UEM** tenant Group ID

- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE UEM** tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select **NEXT**

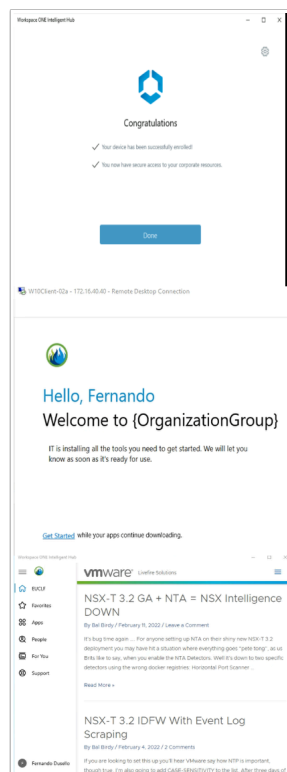
4. In the **Workspace ONE Intelligent Hub** under

- Under **Select Your Domain**
 - Select **euc-livewire.com**
 - Select **Next**
- Under the **Username** area
 - Enter **Fernando**
- Under the **Password** area
 - Enter **VMware1!**
- Select **Sign in**



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

- Select **I Agree**

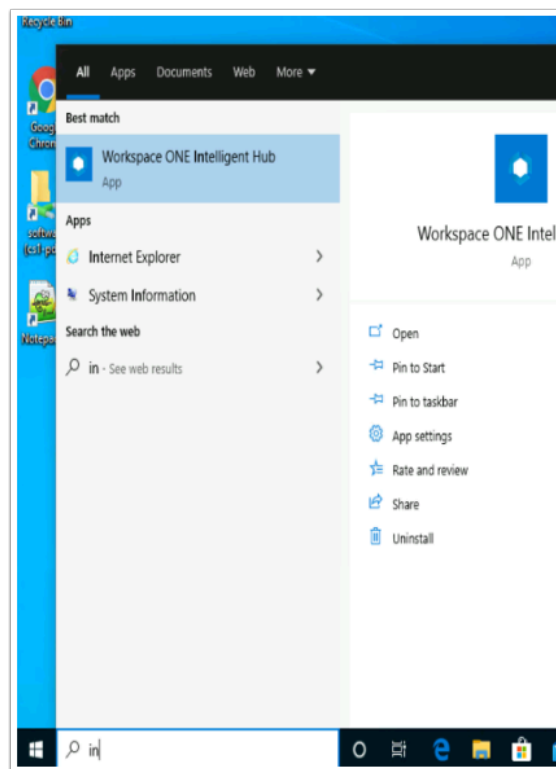


6. On the **Congratulations** window,

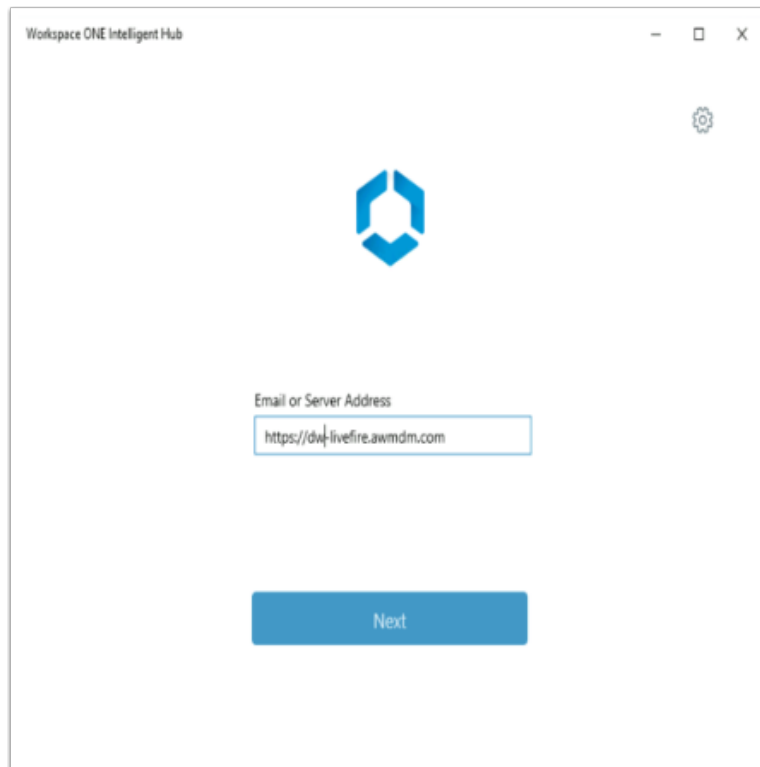
- Select **Done**
- **Re-open** the Intelligent Hub
- Select **Get Started**



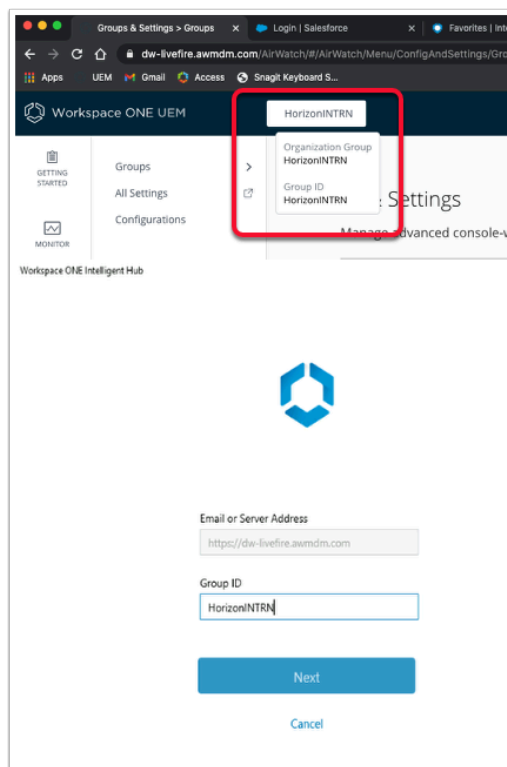
Step 4: Enrolling W10Ext-02a on Site 2 with the Active Directory Domain User Tom



1. On your **ControlCenter** server
 - On the Desktop open the **Remote Desktop** folder.
 - Open the **Site1** folder
 - Select the **W10EXT-02a.RDP** client and
 - Sign-in with
 - **username tom@euc-livefire.com**
 - **Password VMware1!**
 - To the right of the **Start** button in the search area, start typing **intel**
 - Select the **Workspace ONE Intelligent Hub**
 - Please Note! If the **Workspace ONE Intelligent Hub** does not load,
 - From the **RUN > Services.msc > Start the Airwatch service**
 - Attempt to **re-launch** the hub

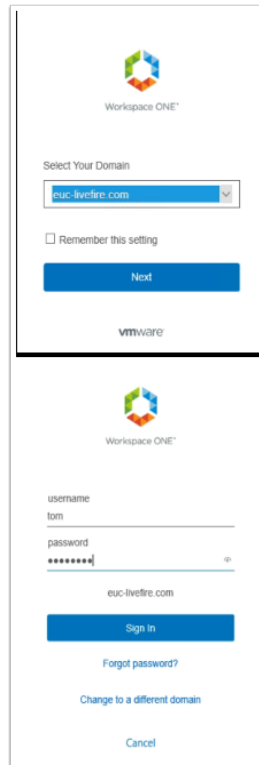


2. Under **Email or Server Address**,
 - Enter <https://dw-livefire.awmdm.com>
 - Select **Next**



3. Under **Group ID** unique enter your unique your **Workspace ONE UEM** tenant Group ID

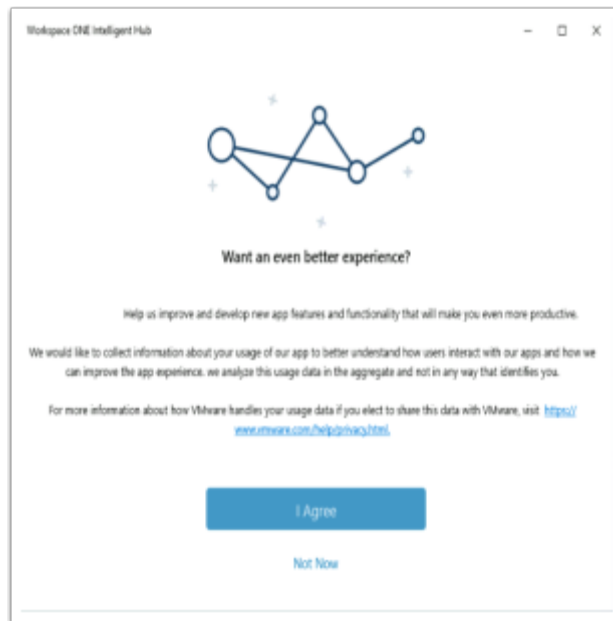
- To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE UEM** tenant and look for the following next to the **Workspace ONE UEM logo**, select your **Organization Group** and note your **Group ID**
- Select **NEXT**



The screenshot shows the Workspace ONE UEM login interface. It is divided into two main sections. The top section, titled 'Select Your Domain', features the Workspace ONE logo, a dropdown menu with 'euc-livewire.com' selected, a 'Remember this setting' checkbox, and a blue 'Next' button. The bottom section is the login area, also with the Workspace ONE logo. It contains fields for 'username' (with 'tom' entered) and 'password' (with '*****' entered). Below these fields is a blue 'Sign In' button, and at the bottom are links for 'Forgot password?' and 'Change to a different domain'.

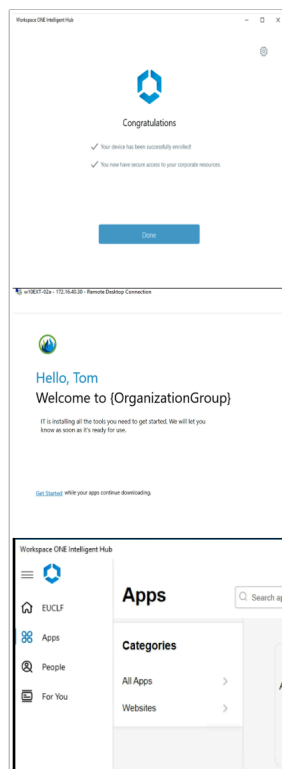
4. In the **Workspace ONE Intelligent Hub** under

- Under **Select Your Domain**
 - Select **euc-livewire.com**
 - Select **Next**
- Under the **Username** area
 - Enter **tom**
- Under the **Password** area
 - Enter **VMware1!**
- Select **Sign in**



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

- Select **I Agree**



6. On the **Congratulations** window,

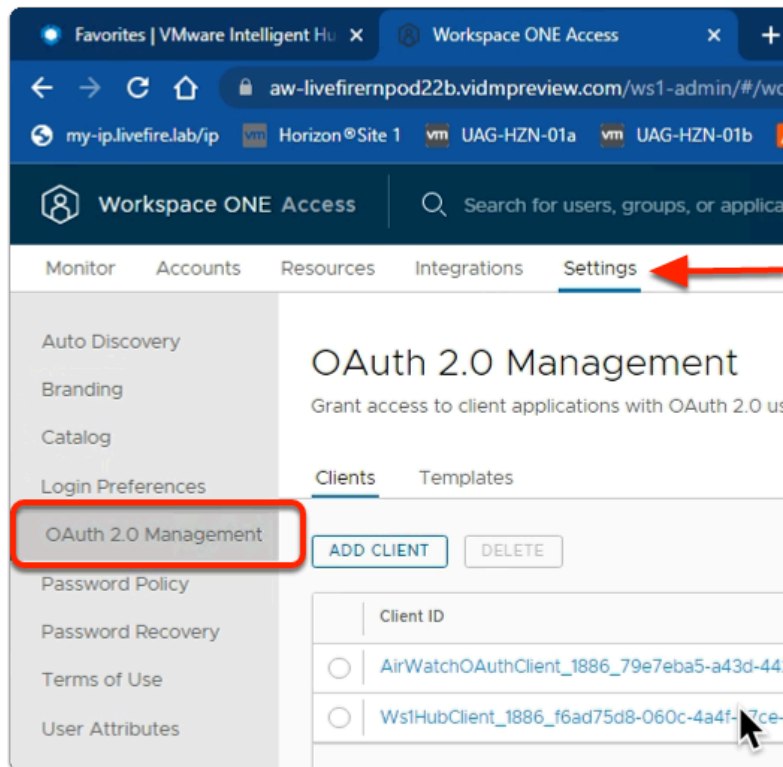
- Select **Done**
- **Re-open** the Intelligent Hub
- Select **Get Started**

Part 2. Integrating Workspace ONE Access with Horizon Cloud services

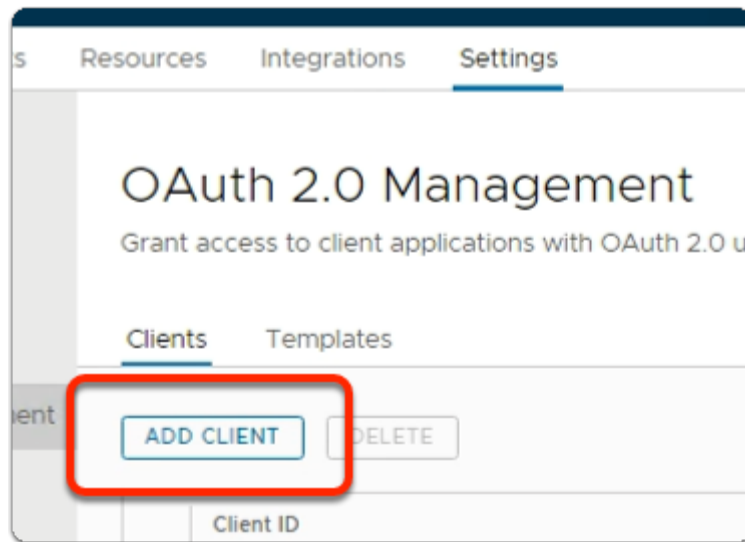
In Part 2 , we will work through the requirement to setup a federation with Horizon Cloud Services and Workspace ONE Access.

The approach to federating Horizon Cloud Services with Workspace ONE Access differs from the approach we following with on-premises Horizon PODS

Part 2: Integrating Workspace ONE Access with Horizon Cloud services



1. In the **Workspace ONE Access** Console
 - Select **Settings**
 - Under **Settings**
 - Select **OAuth 2.0 Management**



2. In the **OAuth 2.0 Management** window

- Select **ADD CLIENT**

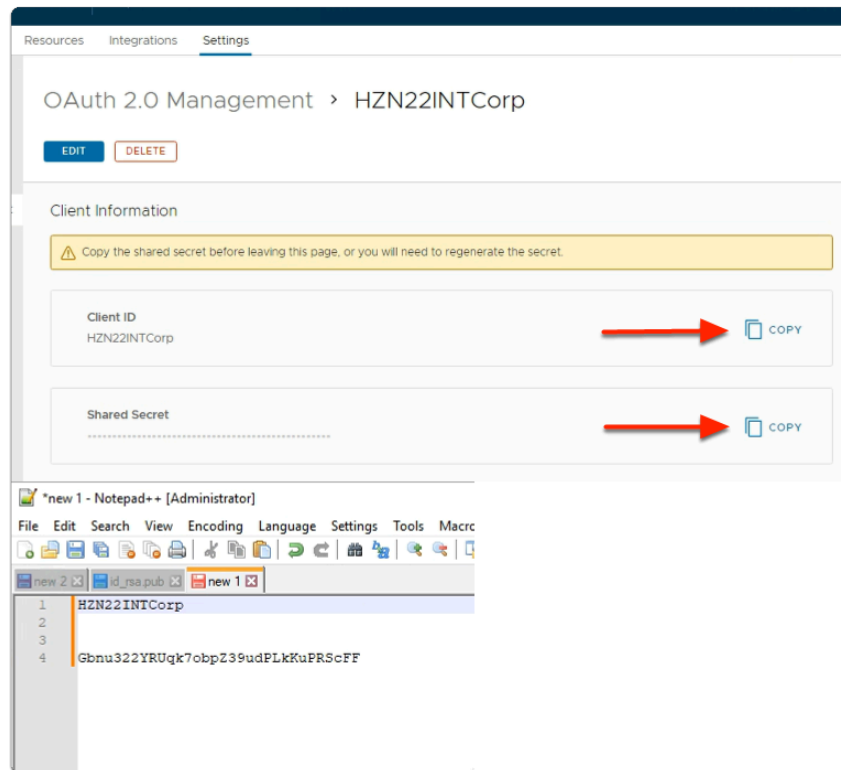
 A screenshot of the 'Add Client' form within the 'OAuth 2.0 Management' window. The breadcrumb path is 'OAuth 2.0 Management > Add Client'. At the top left of the form are 'SAVE' and 'CANCEL' buttons. A message states: 'A secret will be available and autogenerated when you click save'. The form contains several fields:

- Access type***: A dropdown menu with 'Service Client Token' selected.
- Client ID***: A text input field containing 'HZNxxlNTCorp'. Below the field, a note specifies: 'Characters allowed are: alphanumeric (A-Z, a-z, 0-9) period (.), underscore (_), and hyphen (-) and at sign (@). 256 characters max.'
- Scope***: A text input field containing 'Admin'.
- Access token time-to-live (TTL) ***: A field with '3' and a dropdown menu with 'hours' selected.
- Idle token TTL**: A field with '10' and a dropdown menu with 'days' selected.
- Token type**: A text input field containing 'Bearer'.

3. In the **Add Client** interface

- Configure the following information next to:-
 - **Access Type***,
 - select **Service Client Token**
 - **Client ID***,
 - type **HZNXXINTCorp**
 - (xx is your POD ID)

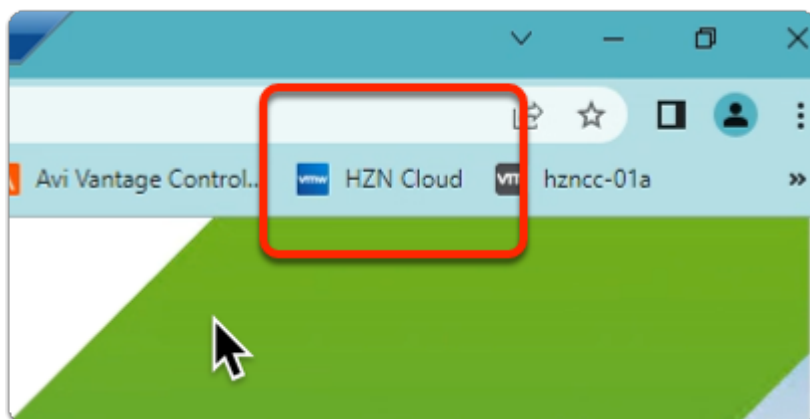
- Select **SAVE**



4. In the **OAuth 2.0 Management** window
 - **COPY** the **Client ID**
 - **COPY** the **Shared Secret**
 - **Save** to **Notepad++** on the **ControlCenter** server



Don't move from this page until you have saved the **Client ID** and **Shared Secret**



5. On your **Site 1 profile - Chrome** browser
 - On the **Favourites** bar
 - Select **HZN Cloud**

Welcome to
VMware Horizon®

My VMware Credentials

Username

Password

☒ Remember me

LOGIN

[Forgot password?](#)

6. On the **Welcome to VMware Horizon®** page
 - Under **My VMware Credentials**, enter the following
 - In the **Username** area,
 - type your, **assigned Horizon Cloud email**
 - In the **Password** area,
 - type , **VMware1!**
 - Select **LOGIN**

Welcome to
VMware Horizon®

Active Directory Credentials

Username

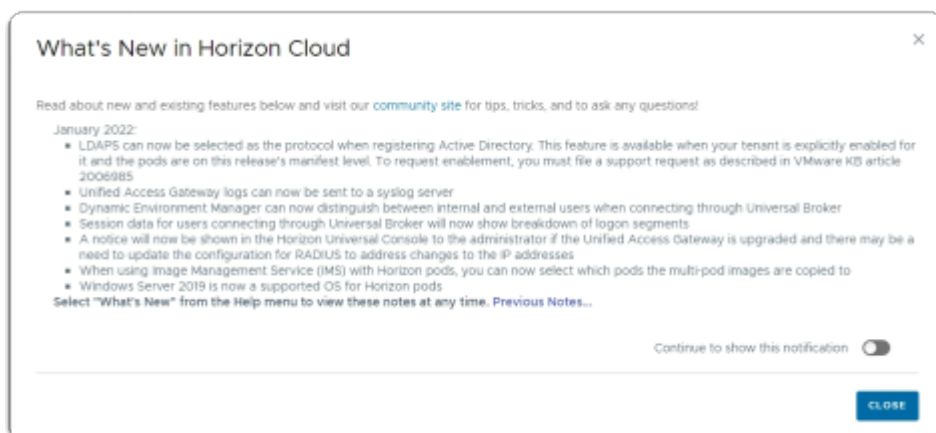
Password

EUC-LIVEFIRE

LOGIN

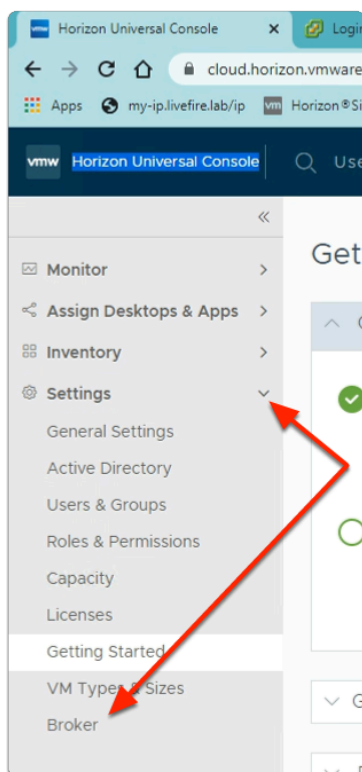
7. On the **Welcome to VMware Horizon®** page
 - Under **Active Directory Credentials**, enter the following
 - In the **Username** area,
 - type **Administrator**

- In the **Password** area,
 - type , **VMware1!**
- Select **LOGIN**



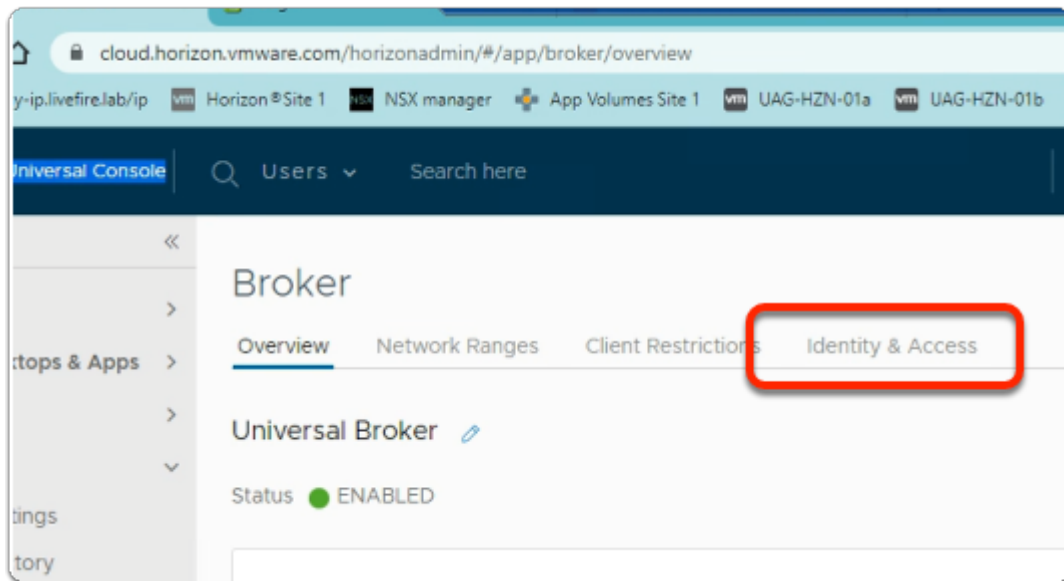
8. In the **What's New in Horizon Cloud** window

- **Turn off the toggle** next to :-
 - **Continue to show this Notification**
- Select **CLOSE**



9. In the **Horizon Universal Console**

- Expand **Settings**
 - Under **Settings**,
 - Select **Broker**



10. In the **Broker** area
 - Select the **Identity & Access** tab

1. Provide Workspace ONE Access Cloud Tenant

Add an existing Workspace ONE Access cloud tenant.

Workspace ONE Access Cloud Tenant *
 Add existing cloud tenant ⓘ

<https://aw-livefirempod22b.vidmpreview.com>

Provide the following information from the Workspace ONE Access console.

OAuth Client ID *
 HZN22INTCorp ⓘ

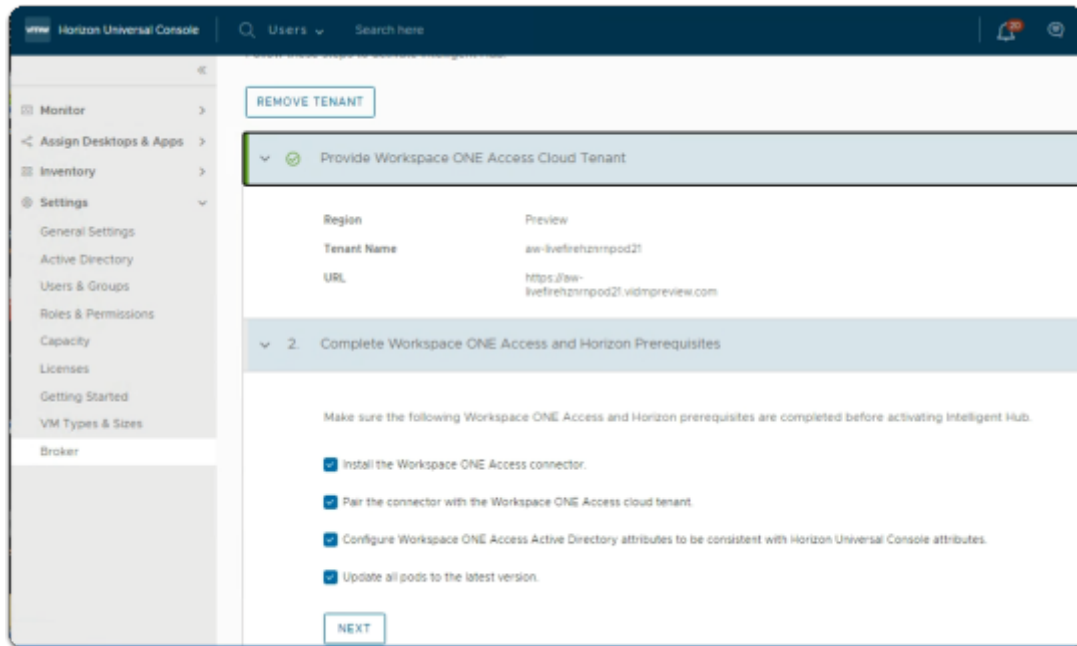
Shared Secret *
 Gbnu322YRUqk7obpZ39udPLkKuPRScFF ⓘ

☒ I have read and agree to the [Terms of Service](#).

NEXT

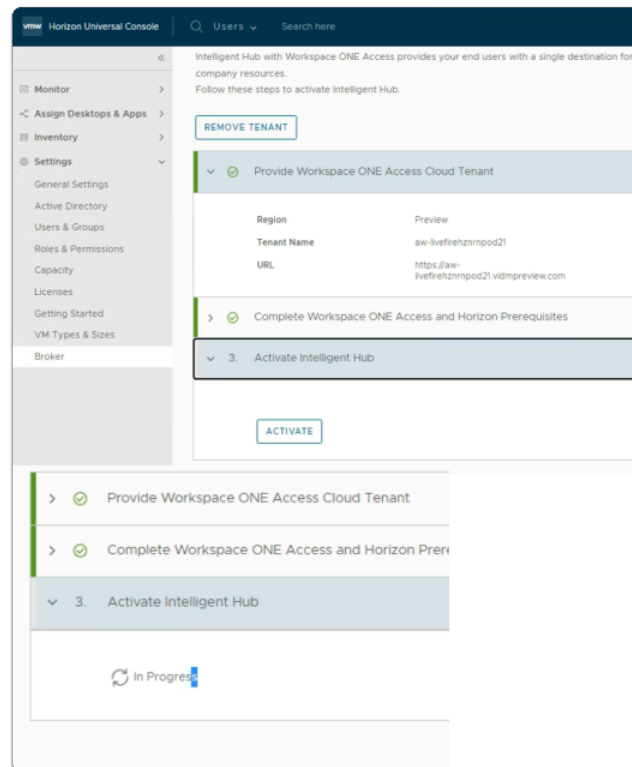
11. In the **Workspace ONE Access and Intelligent Hub** window
 1. **Provide Workspace ONE Access Cloud Tenant** section
 - Enter the following next to:
 - **Workspace ONE Access Cloud Tenant***
 - select **Add existing cloud tenant cloud tenant.**
 - Under **Add existing cloud tenant cloud tenant.**

- enter your **assigned Access tenant FQDN**
- **Next to :-**
 - **OAuth Client ID *** : enter **your recorded Client ID**
 - **Shared Secret *** : enter **Your Shared Secret**
- Select the **check box**, next to :-
 - **I have read and agree to the Terms of Service.**
- Select **NEXT**



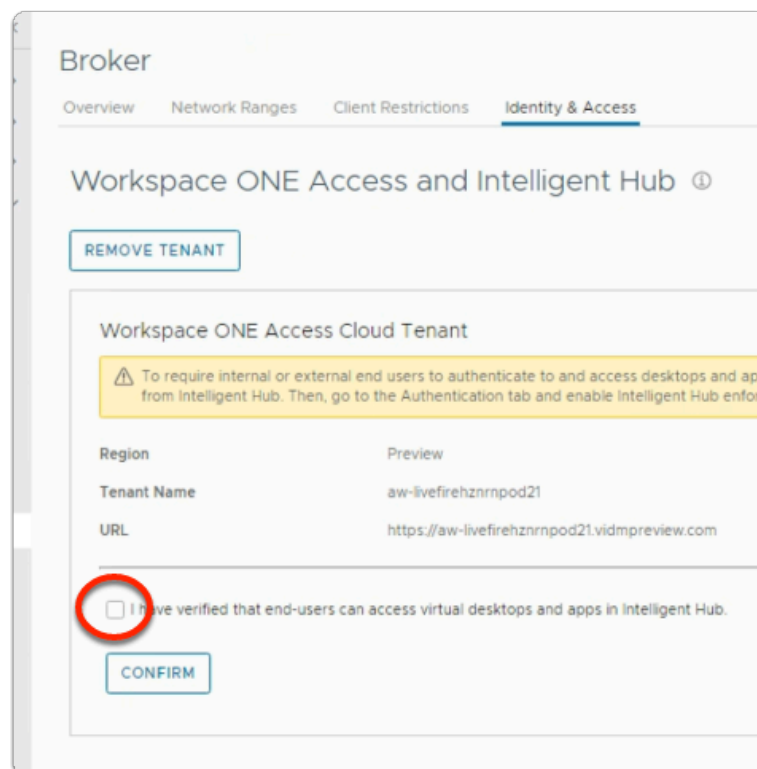
12. In the **Workspace ONE Access and Intelligent Hub** window

- In the following sections:-
 2. **Complete Workspace ONE Access and Horizon Prerequisites** section
 - Note the following requirements before you carry one:
- **Expand** the **Provide Workspace ONE Access Cloud** area above step 2.:
 - Note your tenant information
- Select **NEXT**



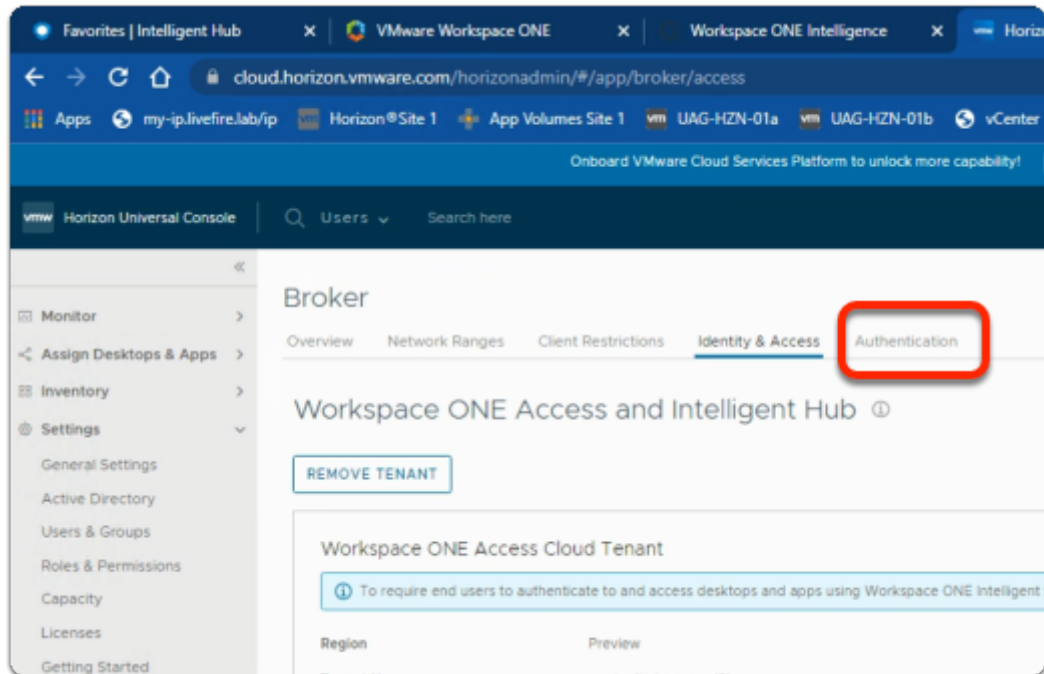
13. In the **Workspace ONE Access and Intelligent Hub** window

- In the following section:-
 3. **Activate Intelligent Hub**
 - Select **ACTIVATE**



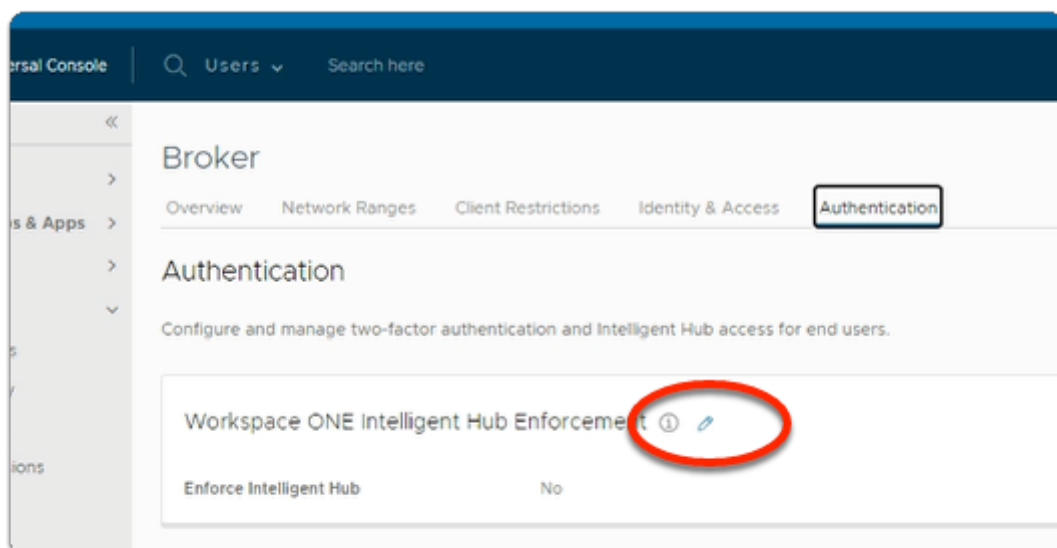
14. In the **Workspace ONE Access and Intelligent Hub** window

- Under the **Workspace ONE Access Cloud Tenant** area
 - select the **checkbox** next to
 - **I have verified that end-users can access virtual desktops and apps in Intelligent Hub.**
 - Select **CONFIRM**



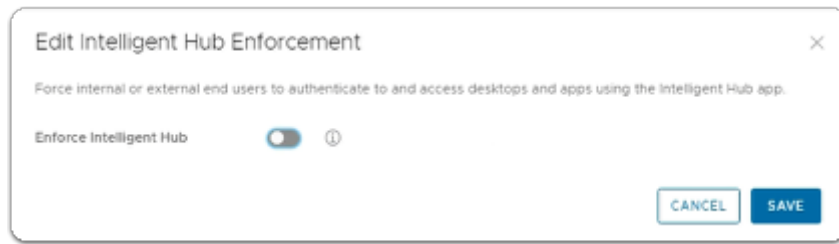
15. In the **Broker** window

- Notice you now have an **Authentication** tab next to **Identity & Access**
- Select the **Authentication** Tab

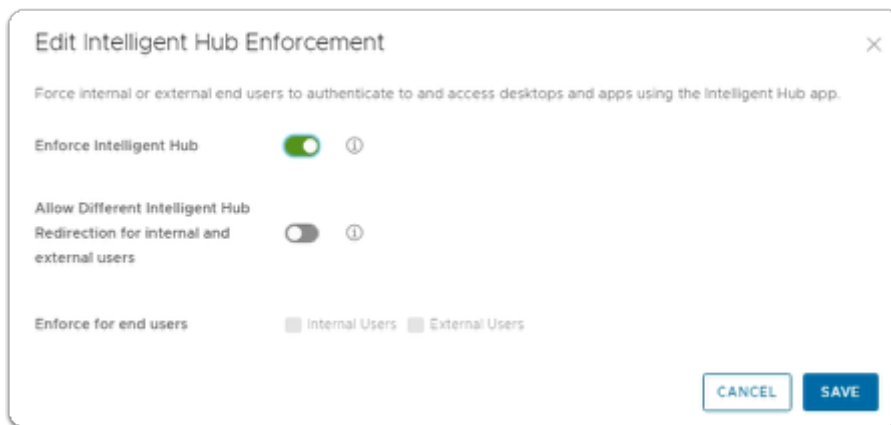


16. In the **Broker** window

- Under the **Authentication** tab
 - Next to **Workspace ONE Intelligent Hub Enforcement**
 - select the **Pencil Icon**



17. In the **Edit Intelligent Hub Enforcement** window
- Next to **Enforce Intelligent Hub**
 - Select the **toggle** and move it to the right



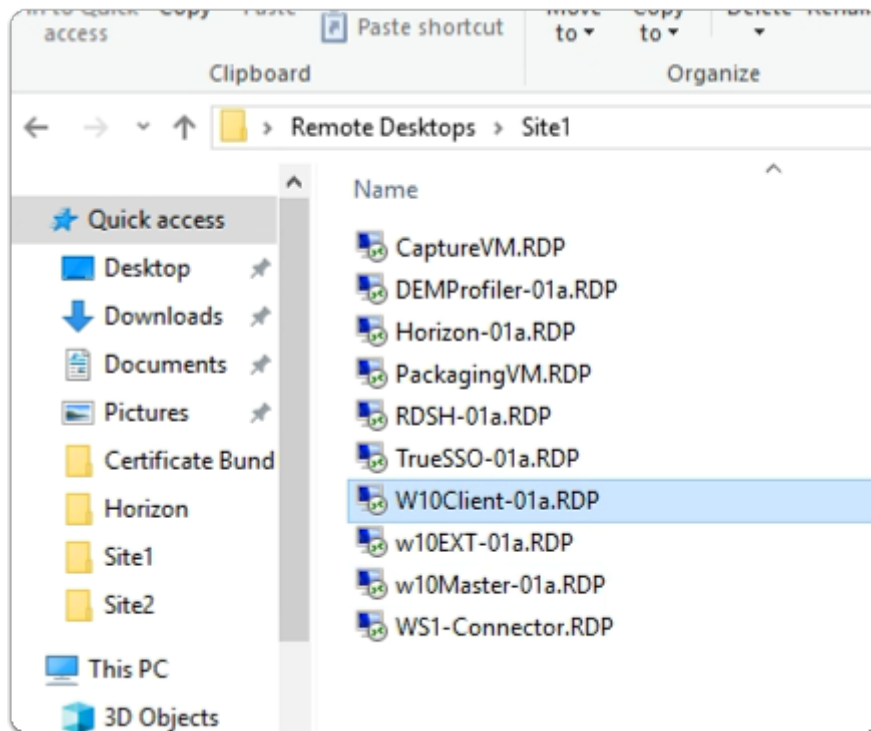
18. In the **Edit Intelligent Hub Enforcement** window
- Select **SAVE**

Part 3 : Testing client integration with the Universal Broker platform

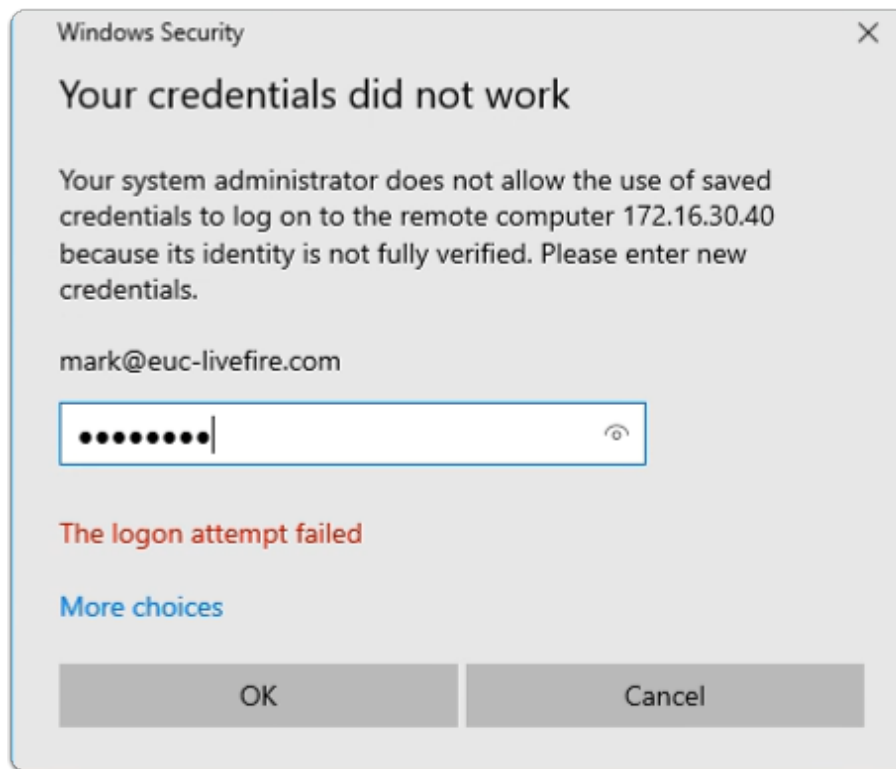
In this part of the we will test our configuration and view how this works

This part also serves as an introduction to Part 4 as to why we need VMware Horizon TRUESSO

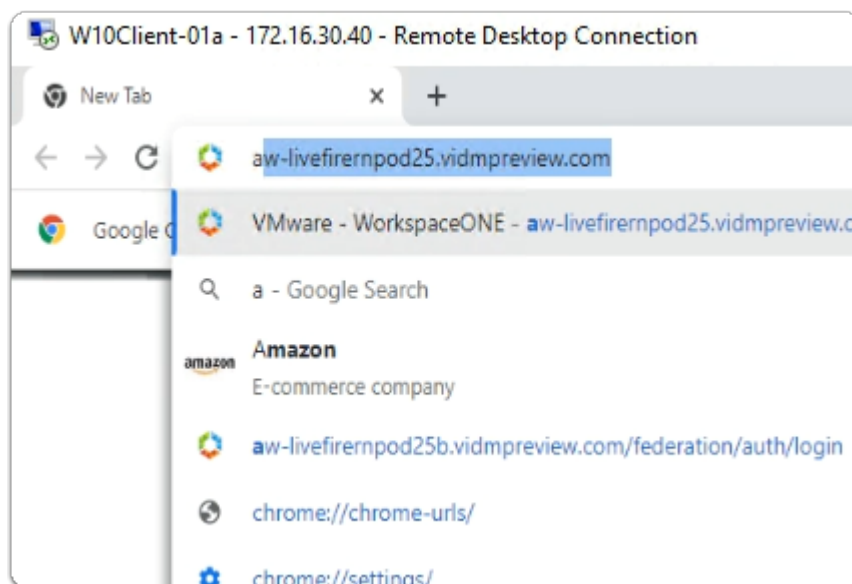
Part 3: Testing client integration with the Universal Broker platform



1. On your ControlCenter server
 - Open your **Remote Desktops** folder
 - Open the **Site 1** folder
 - Launch **w10Client-01a.RDP**

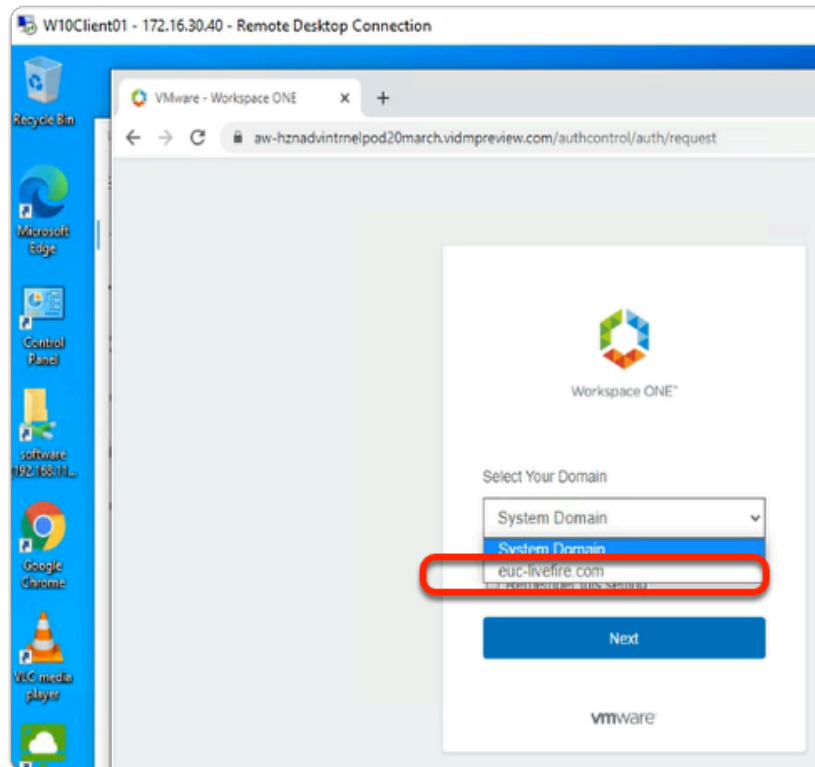


2. In the **Windows Security** window
 - Under **mark@euc-livefire.com**
 - enter **VMware1!** as the password
 - Select **OK**

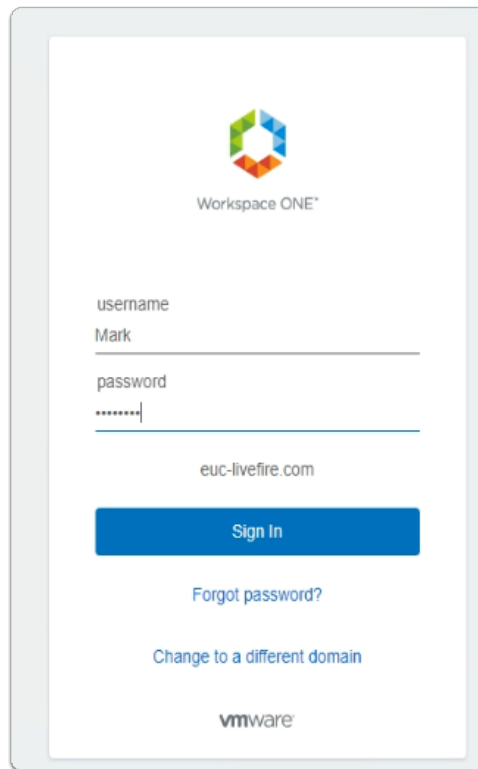


3. On the **W10client-01a** desktop
 - Launch your **Chrome** browser
 - In the Chrome browser **address bar**
 - enter your **Assigned Workspace ONE ACCESS Url**
 - e.g. <https://aw-livefirernpod25.vidmpreview.com/>

- On your keyboard
 - select **ENTER**

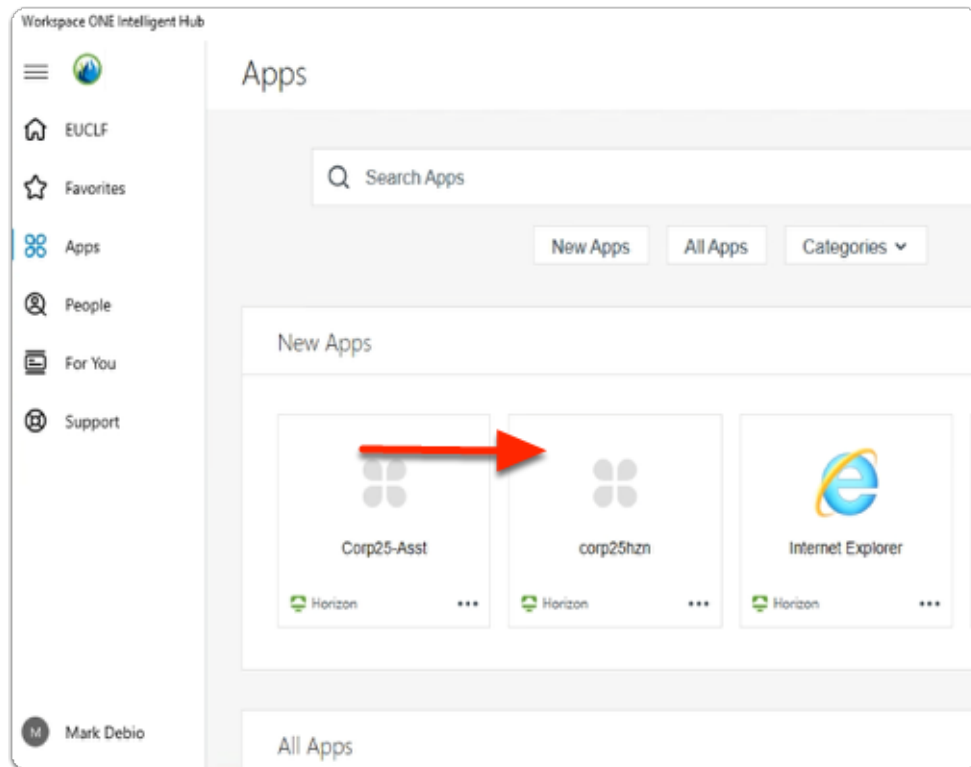


4. In the **Workspace ONE** auth page
 - Under **Select Your Domain**
 - From the **dropdown**
 - Select **euc-livewire.com**
 - Select **Next**



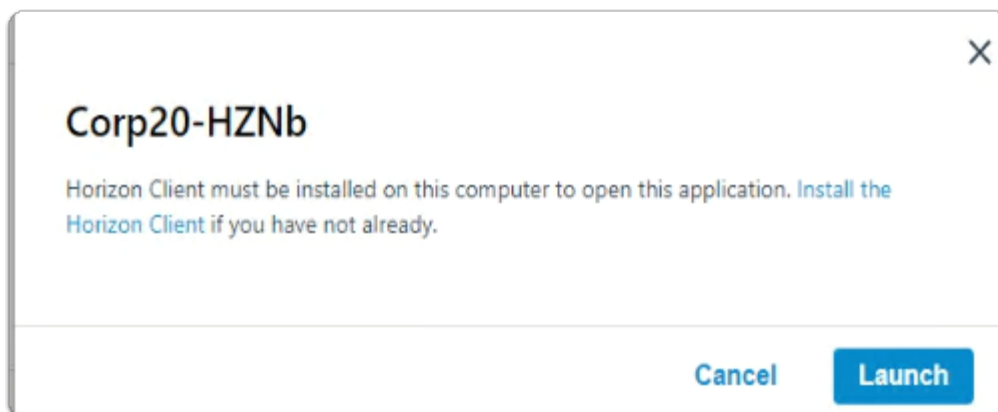
5. In the **Workspace ONE** auth page

- Under **username**
 - type **Mark**
- Under **password**
 - type **VMware1!**
- Select **Sign In**



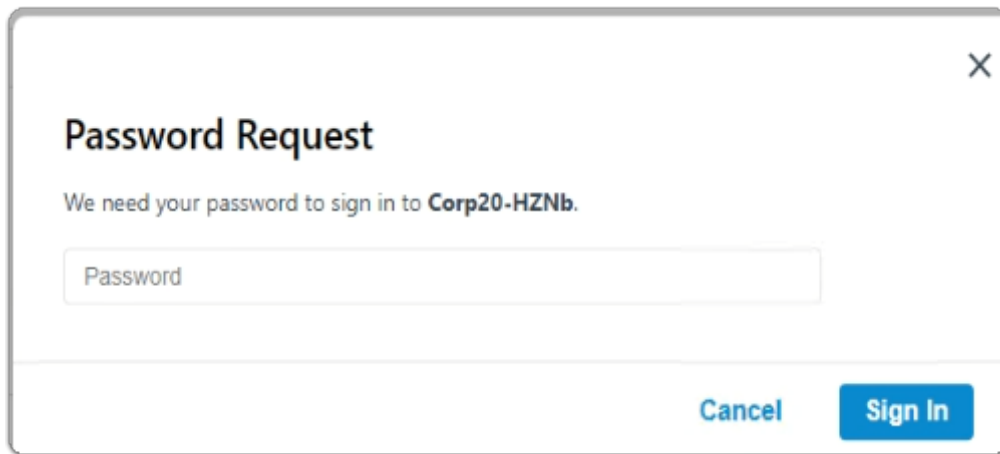
6. In the **Intelligent Hub** console

- Note that now you have your Desktop Entitlement and Published Application assignments
- Launch your **CorpXX-HZN**
 - **XX** is representative of your assigned POD ID



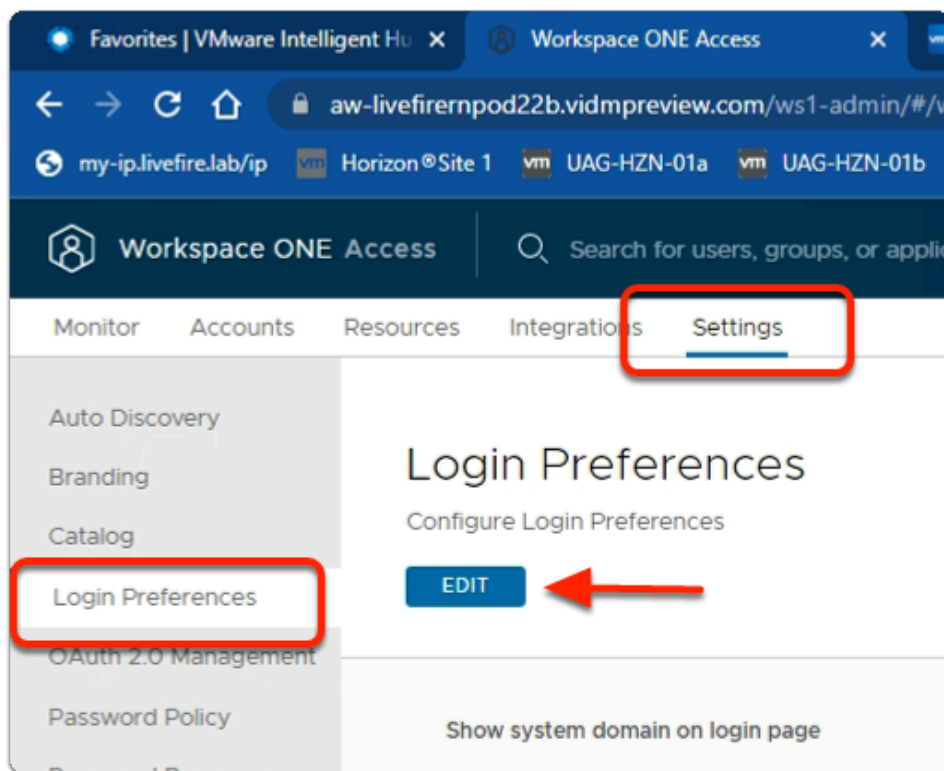
7. In the Horizon Client window

- Select **Launch**



8. In the Password Request window

- Note that you have not received a Single Sign-On experience
- For Password-based authentication we can solve this
- With any other authentication method, only the use of VMware Horizon TRUESSO will solve this
- Select **Cancel**



9. On your ControlCenter server

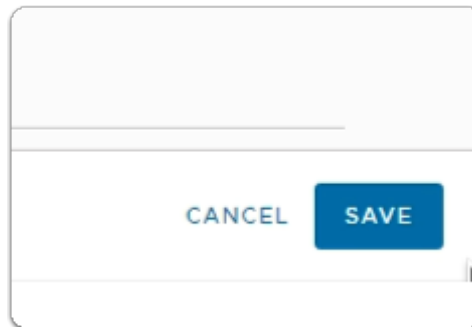
- Revert back to your **Workspace ONE Access Admin Console**
- Select the **Settings** tab
- Under **Settings**
 - Select **Login Preferences**
 - Under **Login Preferences**

- Select **EDIT**



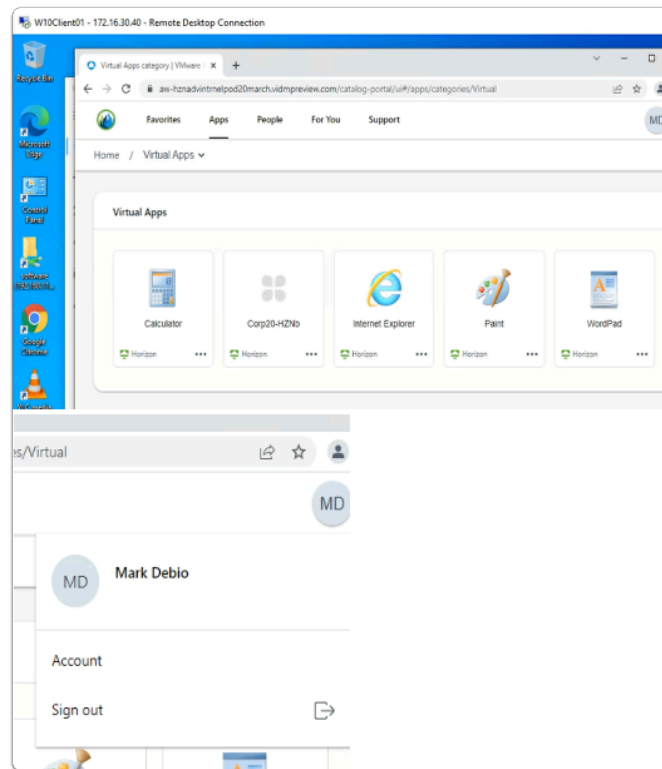
10. Under **Login Preferences**

- Scroll down
- Next to **Cache passwords**
 - Select the **Checkbox**



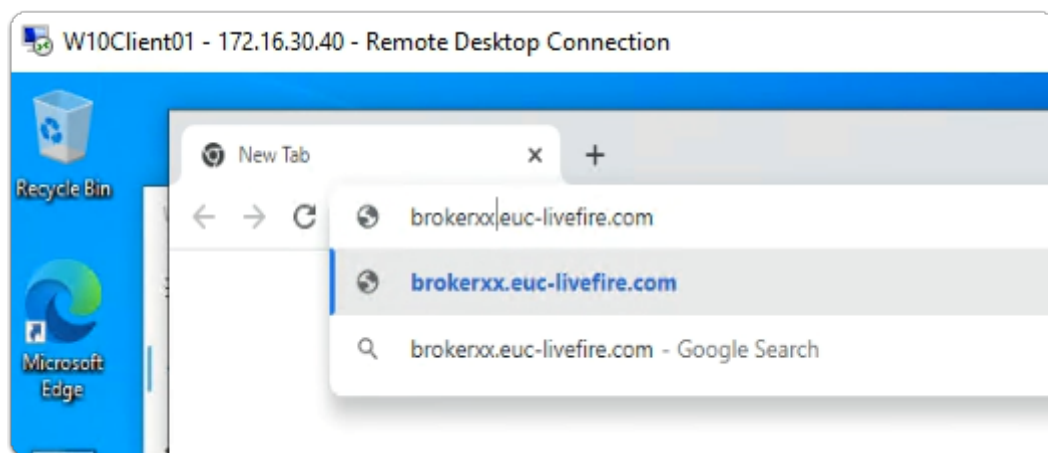
11. Under **Login Preferences**

- To the bottom right. corner of this window
 - Select **SAVE**



12. On the Controlcenter server

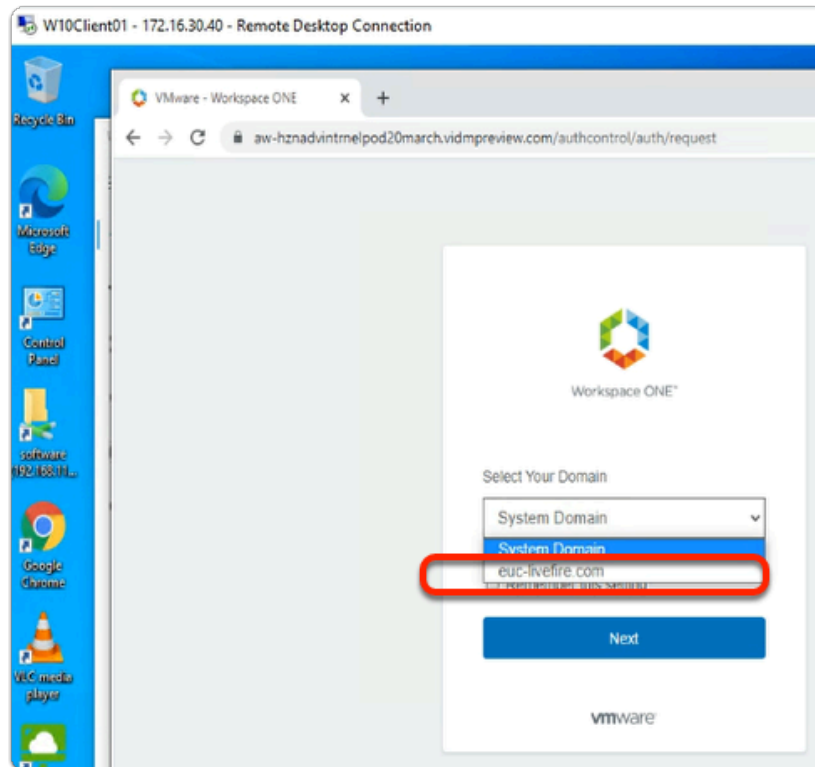
- Revert back to your **W10Client-01a.rdp** session
 - **Sign out** of your existing Intelligent Hub session
 - **Close** your browser



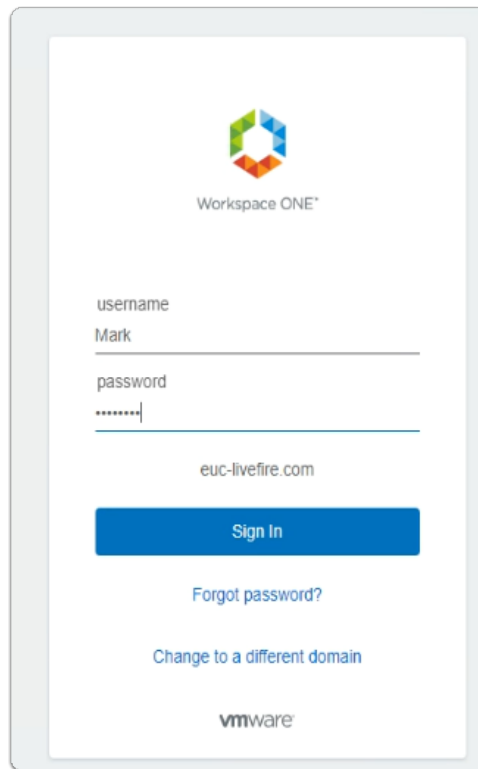
13. On the **W10client-01a** desktop

- If necessary
 - **Close** your **Chrome** browser
 - **Re-Launch** your **Chrome** browser
- In the Chrome browser **address bar**
 - enter your **Assigned Pod broker ID**
 - e.g. **brokerXX.euc-livewire.com**
 - **XX** represents your assigned **POD ID**

- On your keyboard
 - select **ENTER**

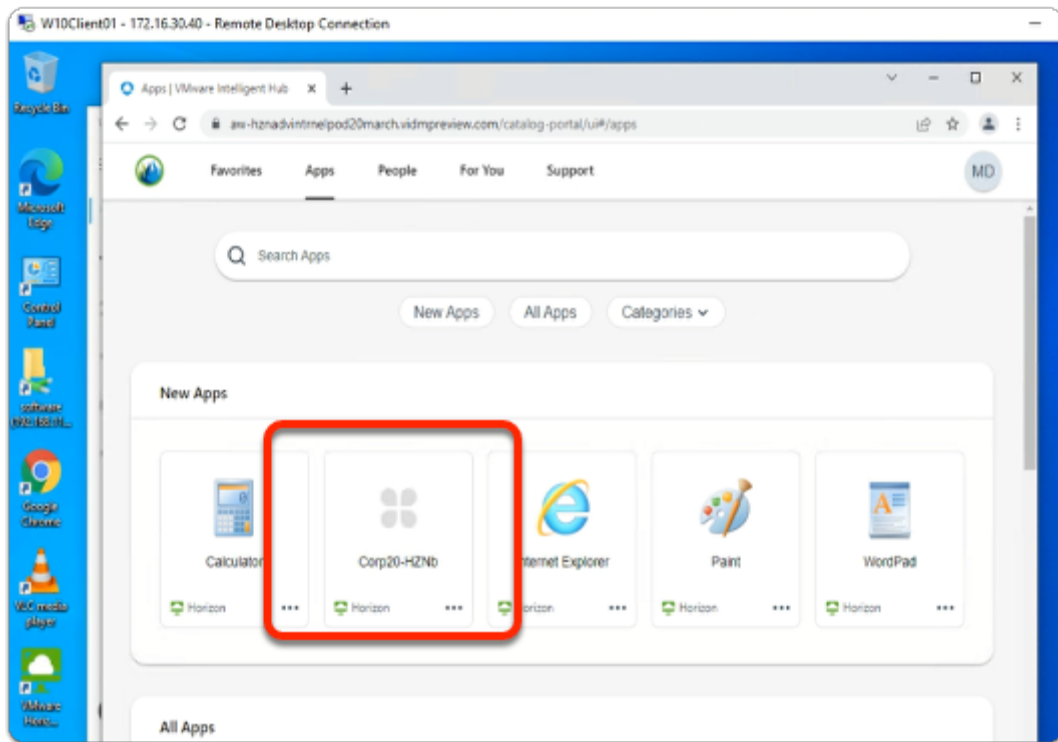


14. In the **Workspace ONE** auth page
- Under **Select Your Domain**
 - From the **dropdown**
 - Select **euc-livewire.com**
 - Select **Next**

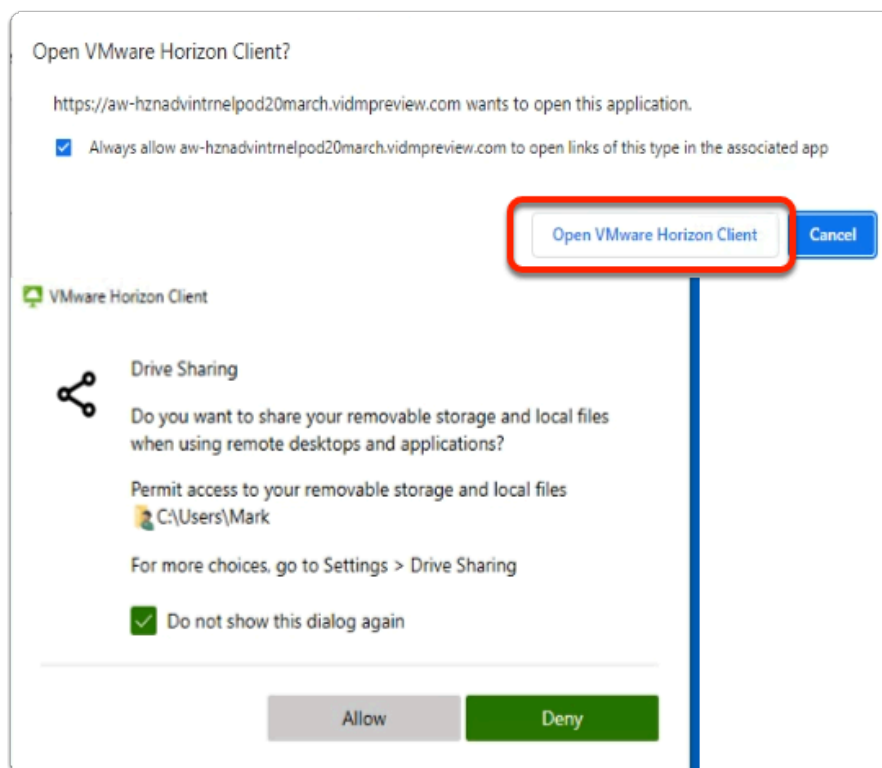


15. In the **Workspace ONE** auth page

- Under **username**
 - type **Mark**
- Under **password**
 - type **VMware1!**
- Select **Sign In**

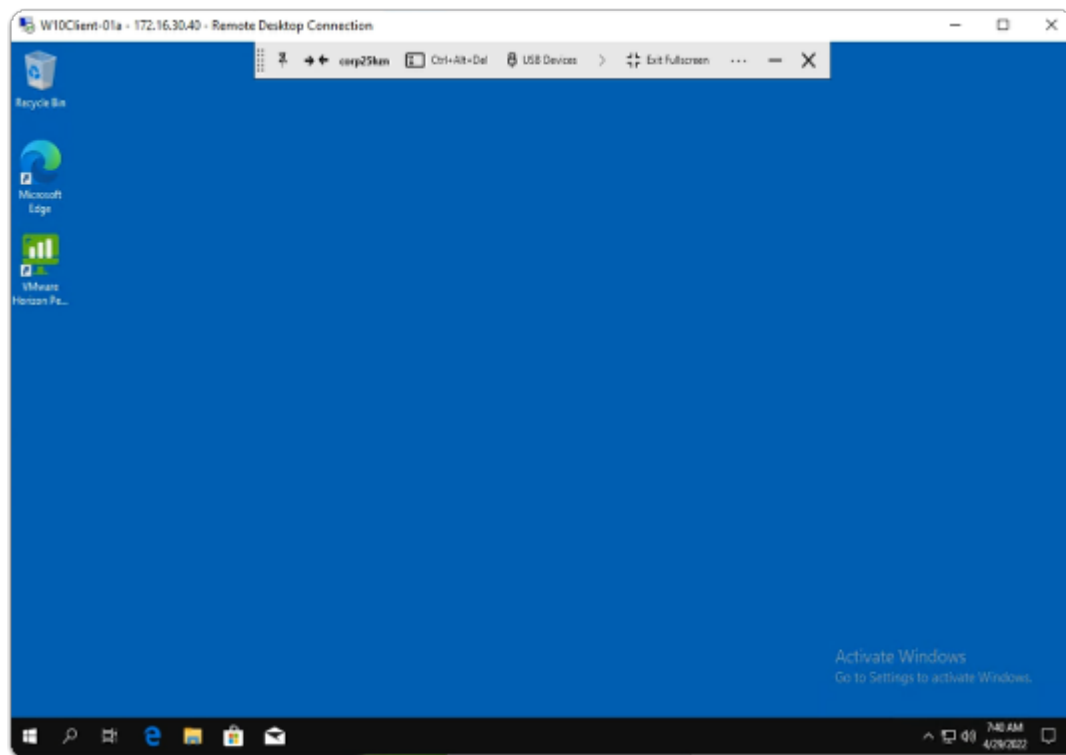


16. In the Web version of the Intelligent Hub
 - Under **Apps**
 - Launch your **Desktop Assignment**



17. In the Open VMware Horizon Client?

- Next to **Always allow YOURSERVER.vidmpreview.com to open links of this type in the associated app**
 - select the **Checkbox**
- Select **Open VMware Horizon Client**
- When prompted by the **VMware Horizon Client** for **Drive Sharing**
 - Select **Allow**



18. In your Horizon Client Session

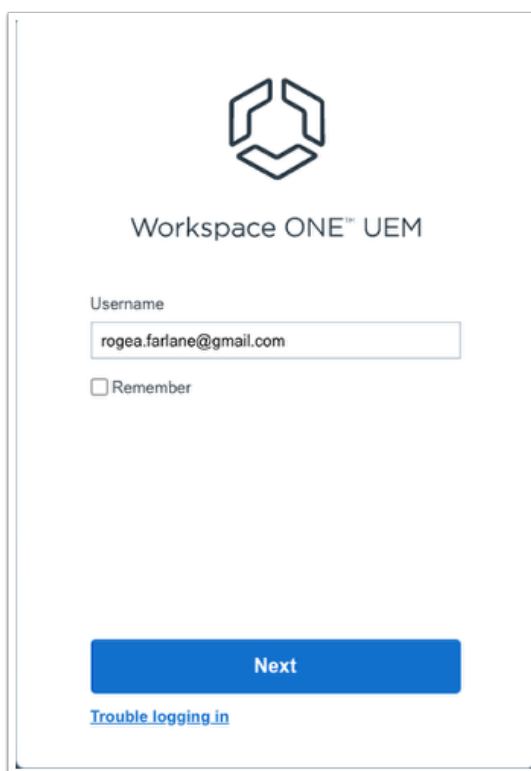
- Note that you were not prompted a second time for a password
- This will only work provided you authenticate with a password on Workspace ONE Access and Password caching remains enabled.
- Password Caching was disabled in **Workspace ONE Access** as a default configuration for security reasons.
- We will now look at Part 4 and the implementation of VMware Horizon TRUESSO to allow for a single sign on experience, irrespective of the Authentication method, even when Password Caching feature is disabled.

Part 4: Integration VMware Horizon TRUESSO with Horizon Cloud services

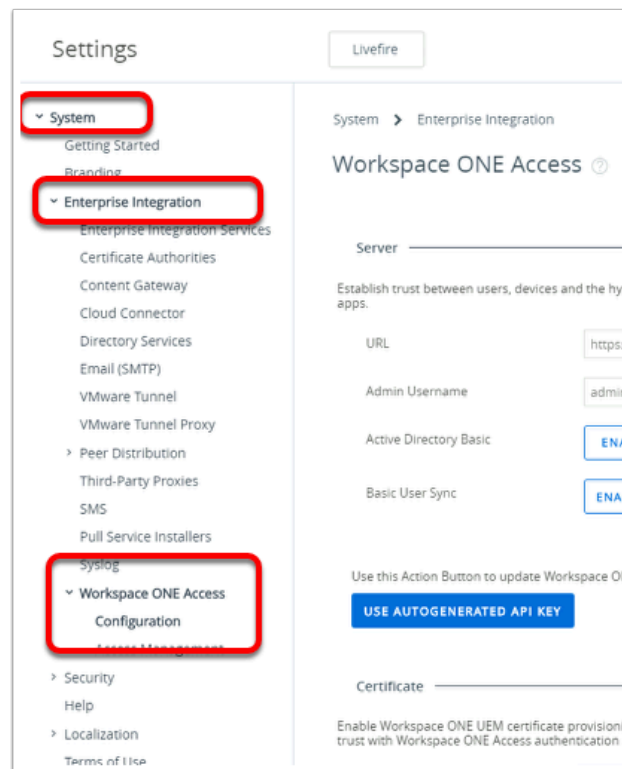
When using Horizon with Workspace ONE Access and a 3rd Party Authentication method, the only way we can get a good user experience with Single Sign-On is to deploy Enrollment Services also known as TRUESSO.

We will not be deploying Horizon Enrollment services but integrating it with Horizon Cloud and seeing how it works with Workspace ONE Access.

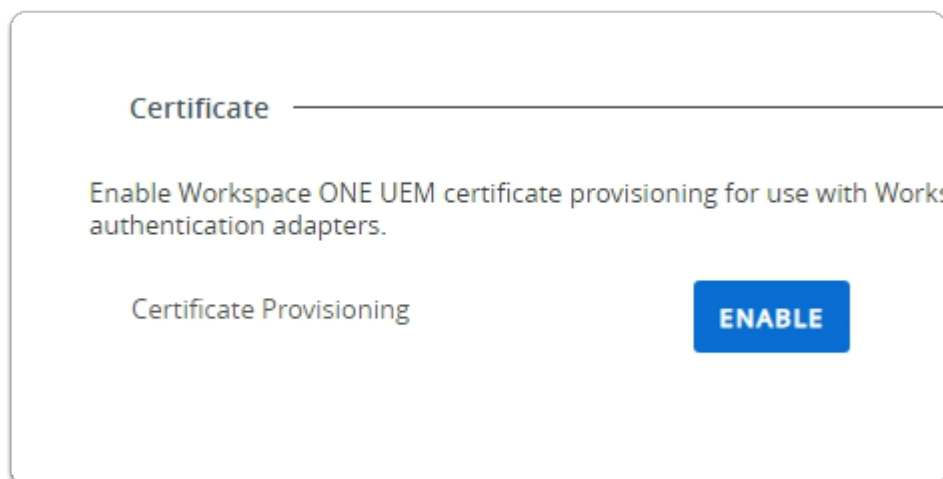
Part 4 Section 1: Deploying a Workspace ONE UEM - Certificate Profile

A screenshot of the Workspace ONE UEM login interface. At the top center is the Workspace ONE logo, a stylized hexagon. Below it, the text "Workspace ONE™ UEM" is displayed. Underneath is a "Username" label followed by a text input field containing the email address "rogea.farfane@gmail.com". Below the input field is a checkbox labeled "Remember". At the bottom of the form is a large blue button with the text "Next". Below the button is a link that says "Trouble logging in" in blue text.

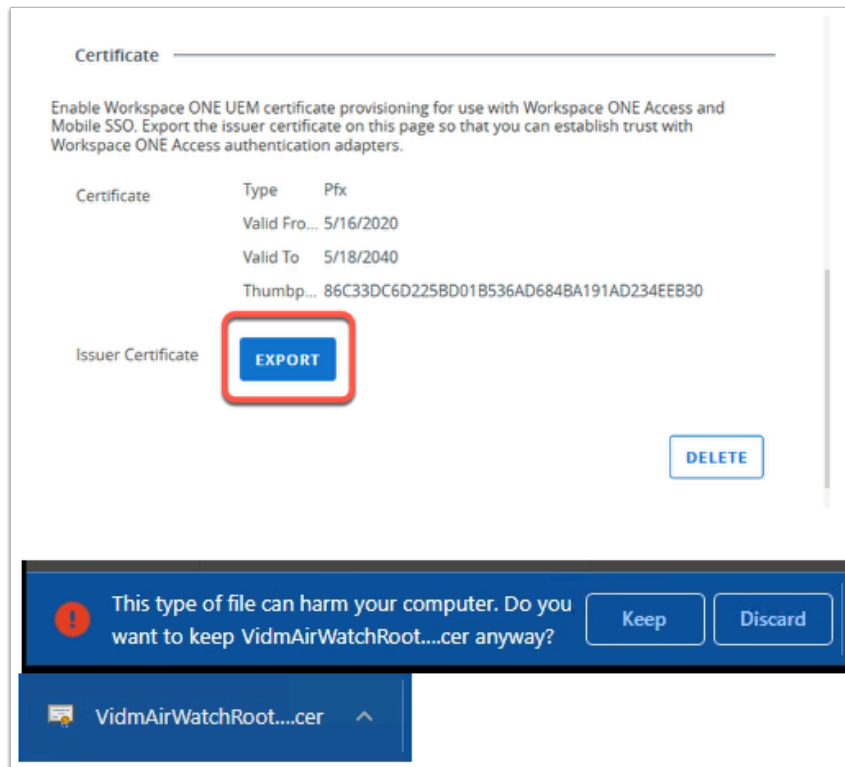
1. On your ControlCenter server
 - Switch to your **custom UEM Saas Tenant**
 - If necessary, authenticate using your Saas Admin credentials



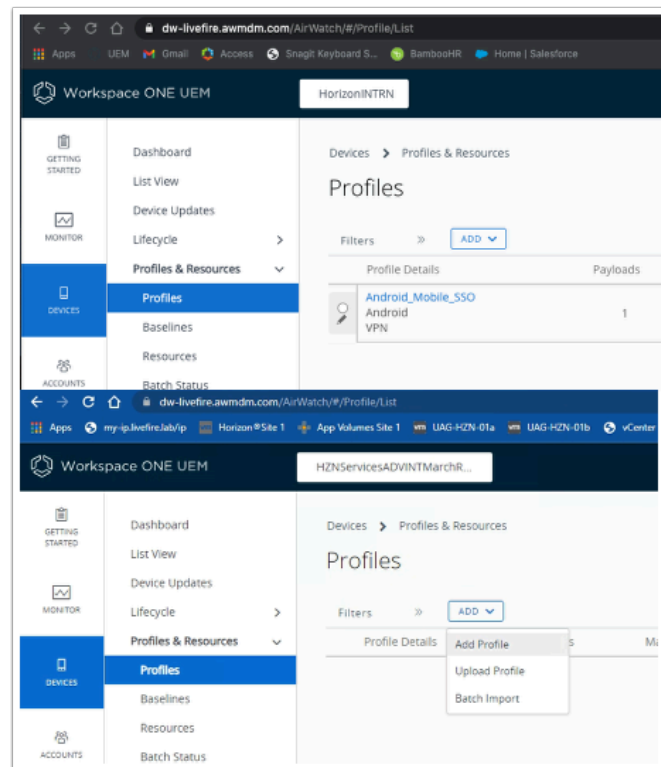
2. In the **Workspace ONE UEM Admin Console**
 - Navigate to **Groups & Settings > All Settings >**
 - In the **Settings** window under
 - **Select System**
 - Select **Enterprise Integration >**
 - Select **Workspace ONE Access >**
 - Select **Configuration**



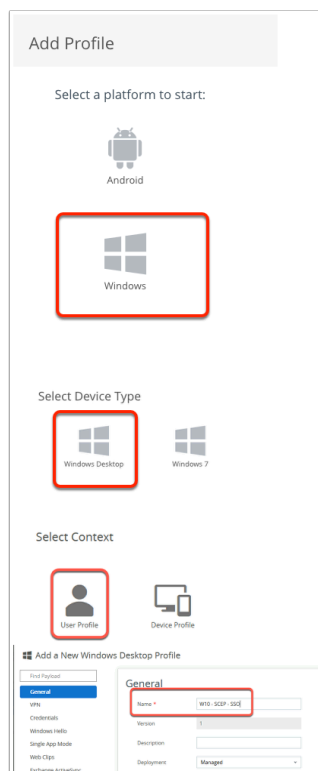
3. In the Workspace ONE Access area
 - Below **Certificate**
 - Next to **Certificate Provisioning**
 - Select **ENABLE**



4. In the Workspace ONE Acces window
 - **Scroll down** to the **Certificate** area
 - Select **EXPORT**
 - At the bottom of your browser
 - select **Keep**
 - Note this will download :-
 - **VidmAirWatchRootCertificate.cer**
 - To close the **Settings** window
 - Select **X**



4. From the UEM Console
 - Navigate to **Devices > Profiles & Resources > Profiles**
 - Select > **ADD > Add Profile**



5. In the **Add Profile** window
 - Select **Windows > Windows Desktop > User Profile**

- Next to **Name*** enter: **W10 - SCEP - SSO** .

Managed By: HZNServicesADVINTMarchRNELOD20

Smart Groups: All Devices (HZNServicesADVINTMarchRNELOD20)

Exclusions: NO YES

VIEW DEVICE ASSIGNMENT

6. In the **General** tab,

- **Scroll down** to **Smart Groups**
 - Select **All Devices(YOUR SAAS Tenant)**

General

VPN

Credentials

Windows Hello

Single App Mode

Web Clips

Exchange ActiveSync

SCEP

Exchange Web Services

SCEP

CONFIGURE

7. In the **Add Profile** window

- In the left inventory menu
 - Navigate down to the **SCEP** tab
 - Select **SCEP**
- In the **SCEP** area
 - Select **CONFIGURE**

Add a New Windows Desktop Profile

Find Payload

General

VPN

Credentials

Windows Hello

Single App Mode

Web Clips

Exchange ActiveSync

SCEP

SCEP

Credential Source: AirWatch Certificate Authority

Certificate Authority *: AirWatch Certificate Authority

Certificate Template *: Single Sign-On

Key Location: Software

SAVE AND PUBLISH CANCEL

8. In the **SCEP** window
 - Change the following:
 - **Next to :**
 - **Key Location:** from the **dropdown**
 - select **Software**
 - At the bottom right of the window
 - Select **SAVE AND PUBLISH**

View Device Assignment

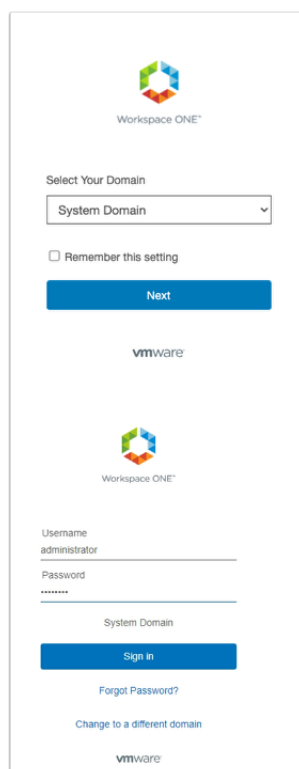
Assignment Status	Friendly Name	User
Added	HZNServicesAD\NTMarchRNELP0020 VM...	Mark
Added	HZNServicesAD\NTMarchRNELP0020 VM...	Jill
Added	HZNServicesAD\NTMarchRNELP0020 VM...	Fernando
Added	HZNServicesAD\NTMarchRNELP0020 VM...	Tom

Items 1-4 of 4

PUBLISH CANCEL

9. In the **View Device Assignment** page
 - Confirm your devices are showing
 - In the bottom right corner
 - Select **PUBLISH**

Part 4 Section 2: Configuring Workspace ONE Access for Certificate Authentication



Workspace ONE™

Select Your Domain

System Domain

☐ Remember this setting

Next

vmware

Workspace ONE™

Username
administrator

Password

System Domain

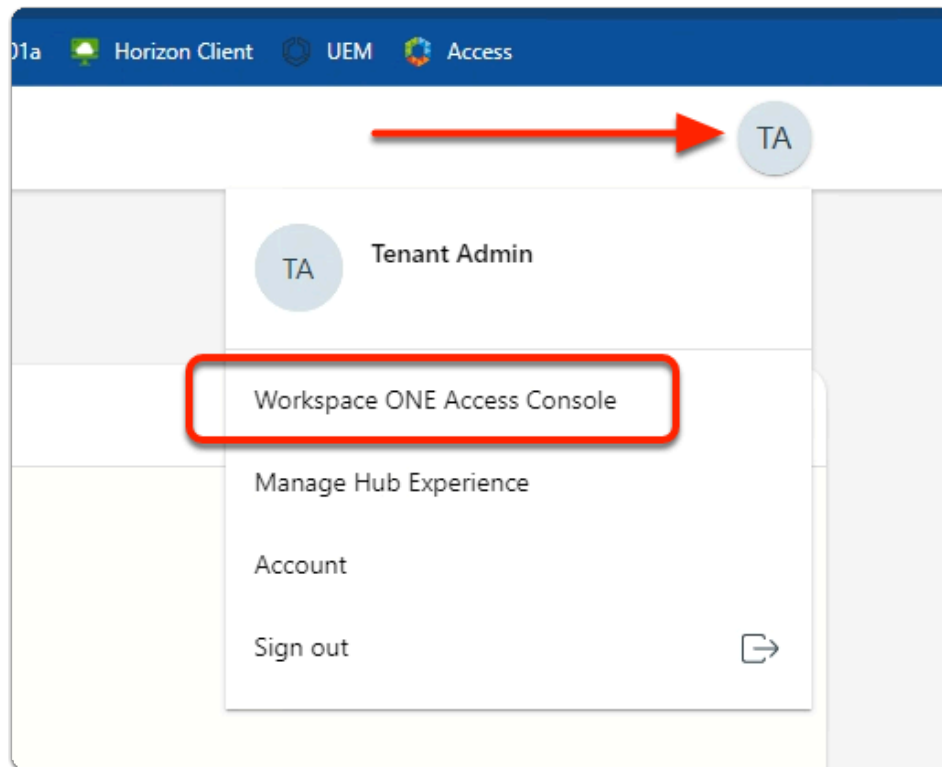
Sign in

[Forgot Password?](#)

[Change to a different domain](#)

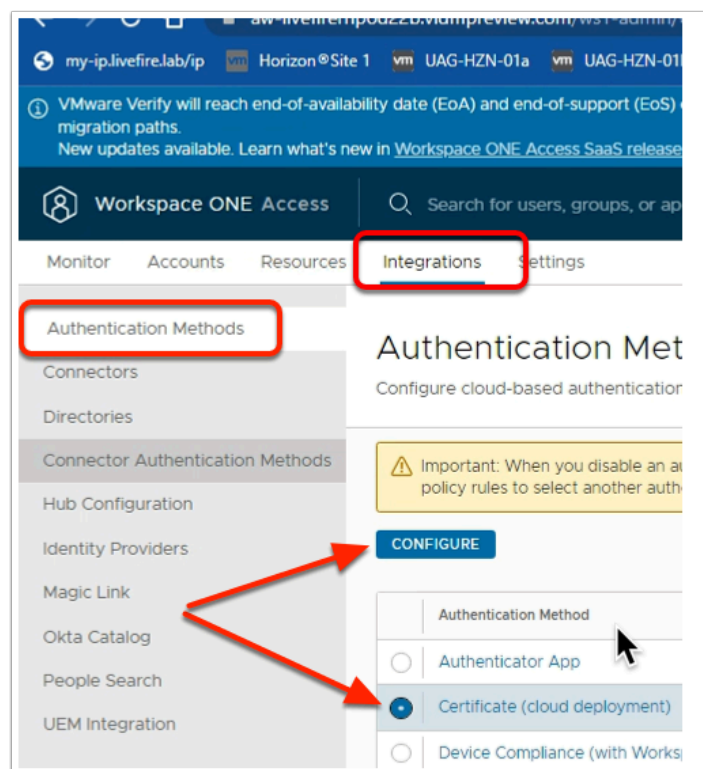
vmware

1. On your ControlCenter
 - Switch to your custom SaaS **Workspace ONE Access** tenant
 - In the **Workspace ONE** Login
 - Under **Select Your Domain**
 - Select **System Domain**,
 - Select **Next**
 - Under **Username**
 - type **administrator**
 - Under **Password**
 - type **VMware1!**
 - Select **Sign in**



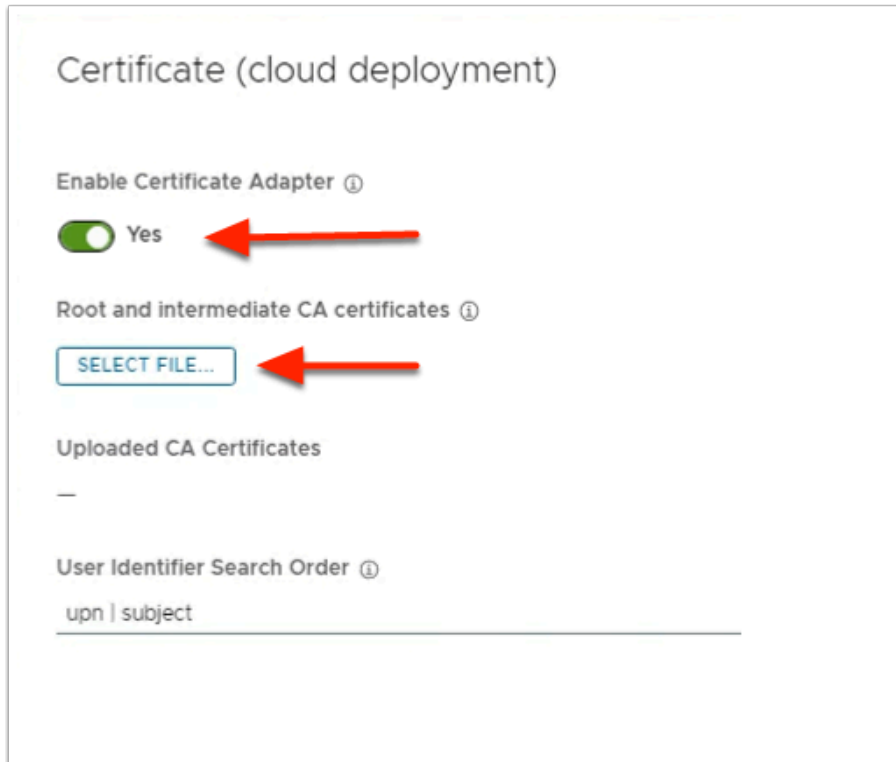
2. In the Intelligent Hub Console

- Top right corner
 - Select the **TA** icon
 - Select **Workspace ONE Access Console**



2. In the Workspace ONE Access admin console

- Navigate to the **Integrations** tab
 - In the Integrations area, validate you are in Authentication Methods
 - **Next Certificate (Cloud Deployment)**
 - Select the **pencil icon**



Certificate (cloud deployment)

Enable Certificate Adapter ⓘ

☒ Yes

Root and intermediate CA certificates ⓘ

[SELECT FILE...](#)

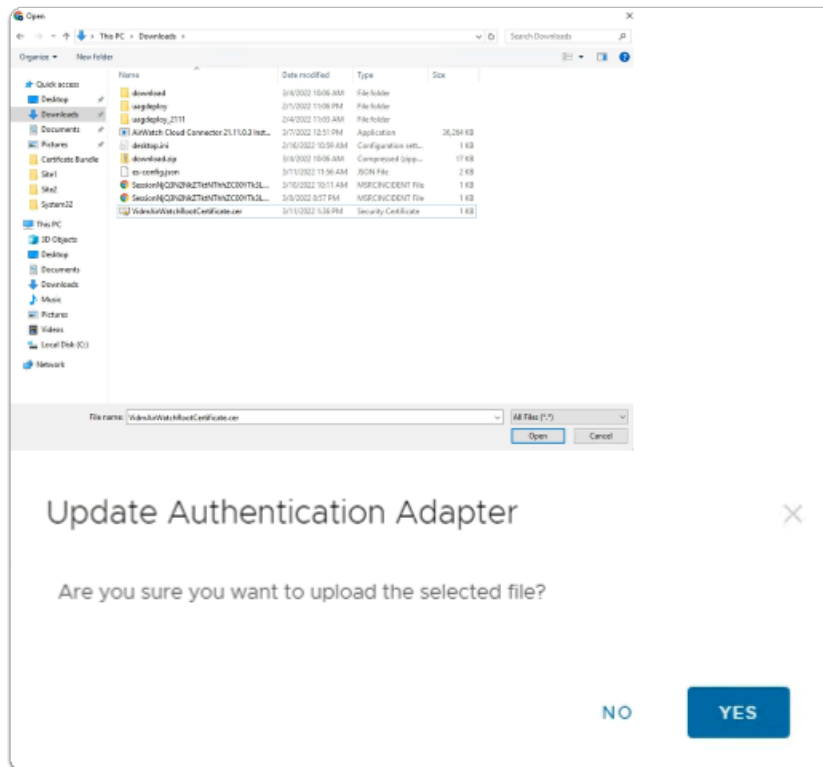
Uploaded CA Certificates

—

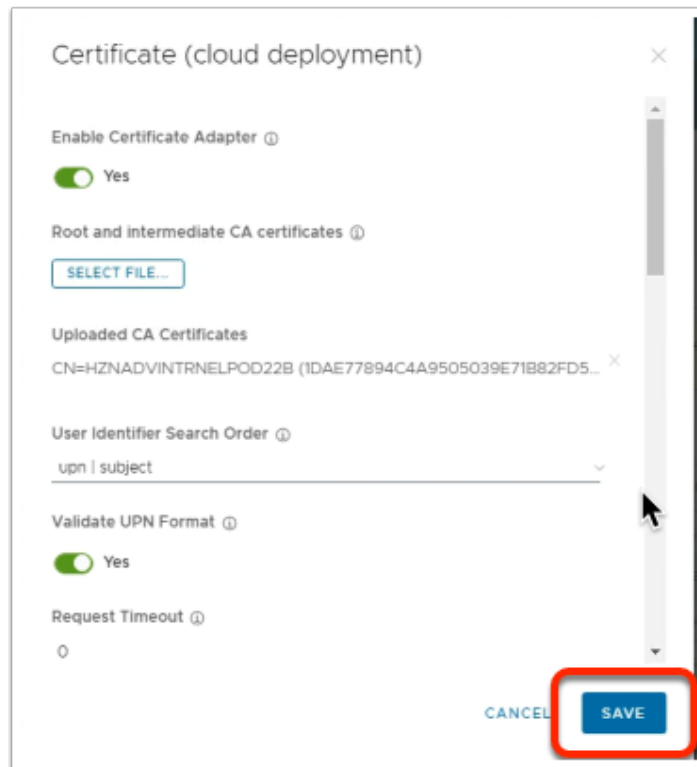
User Identifier Search Order ⓘ

upn | subject

3. In the **Certificate (Cloud Deployment)** page
 - Below **Enable Certificate Adapter**
 - Below **Root and Intermediate CA Certificates**
 - select **SELECT FILE...**

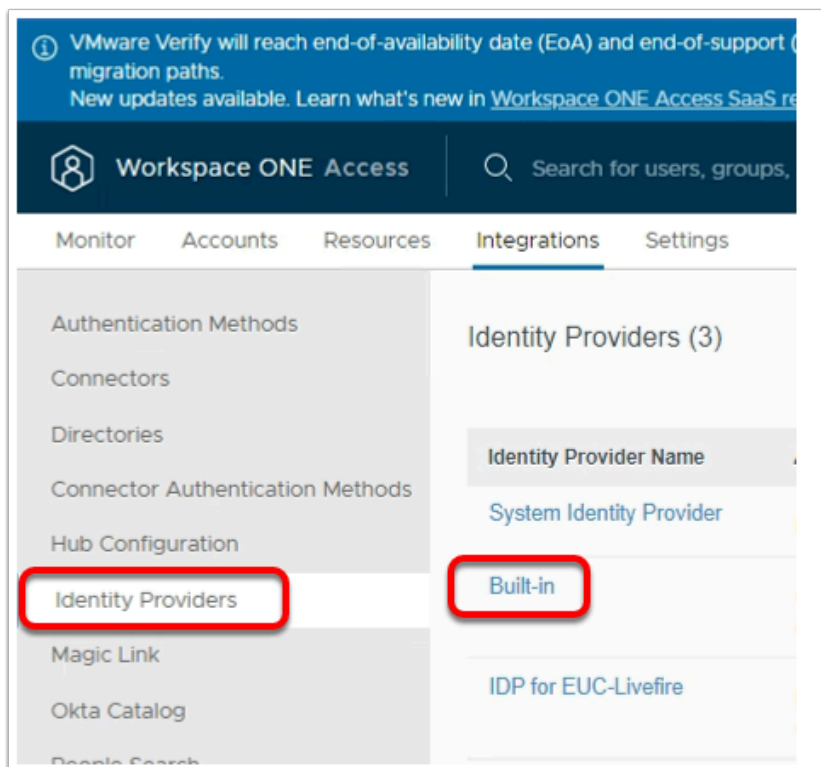


4. In the **File Explorer** window
 - In the **Quick Access** Menu
 - Select **Downloads**
 - Select the **VIDMAirWatchRootCertificate.Cer** certificate
 - Select **Open**
 - In the **Update Authentication Adapter** window
 - select **YES**



5. In the **Certificate (cloud deployment)** window

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



6. In the **Workspace ONE Access** Console

- Under **Integrations**

- Select **Identity Providers**
 - In the **Identity Providers** area
 - Select **Built-in**

Search for users, groups, or applications

New

Integrations Settings

Connector Authentication Methods Select a directory first to see a list of available authentication methods.

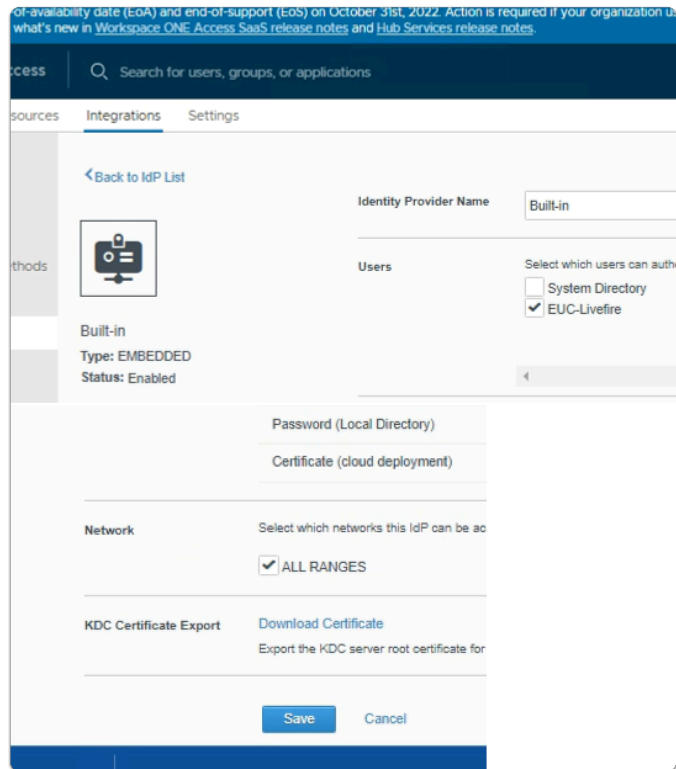
Authentication Methods Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication
Password (Local Directory)	<input type="checkbox"/>
Certificate (cloud deployment)	<input checked="" type="checkbox"/>

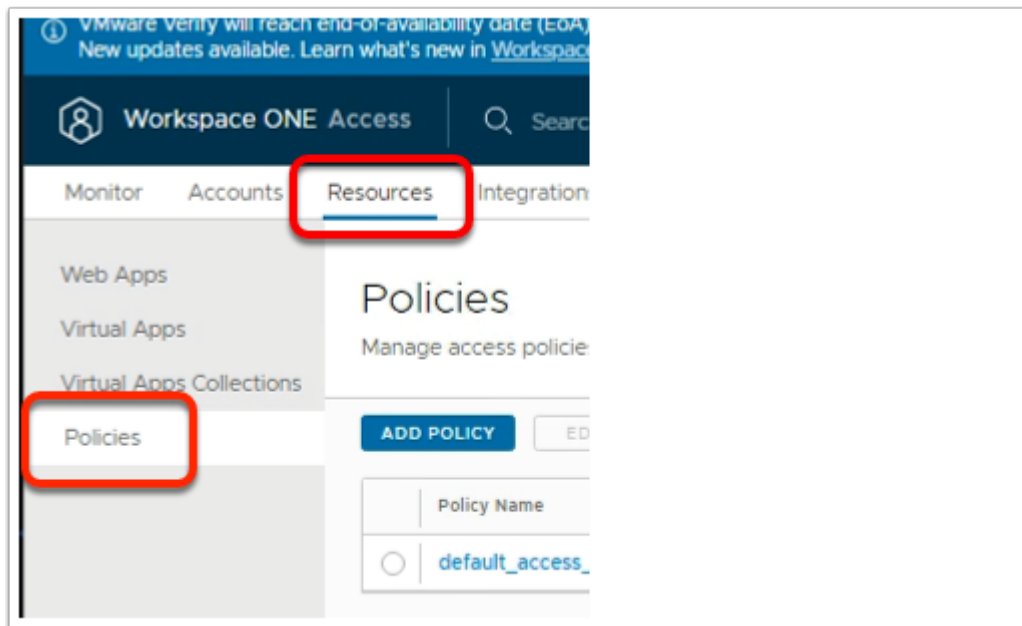
Network Select which networks this IdP can be accessed from. Choose from the available network ranges from the

7. In the **Built-In** Identity Providers window

- **NOTE :**
 - In the **Authentication Methods** area
 - The **checkbox** next **Certificate (cloud deployment)** is already enabled

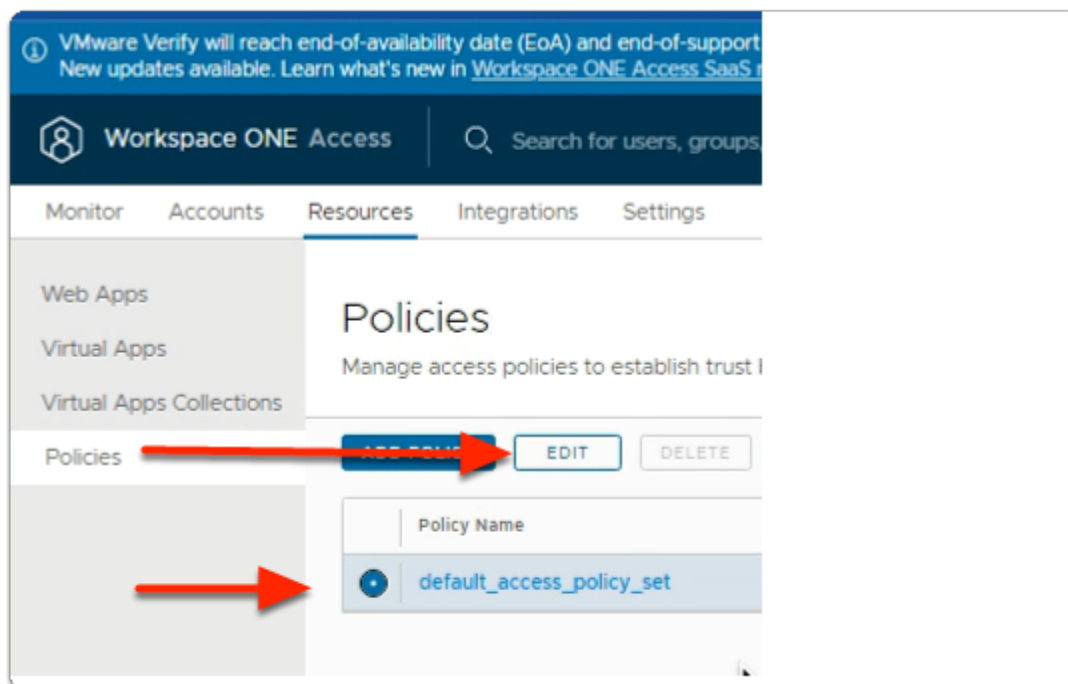


8. In the **Built-In** window
 - In the **Users** area
 - Next to **EUC-Livefire**
 - select the **checkbox**
 - In the **Network** area
 - Next to **ALLRANGES**
 - select the **checkbox**
 - At the bottom of the page.
 - Select **Save**



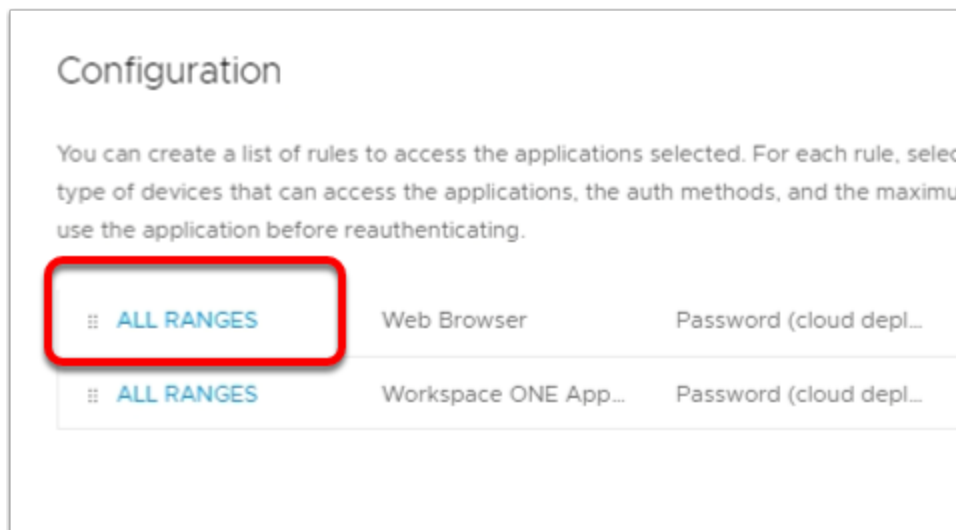
9. In the Workspace ONE Access Admin console

- Select the **Resources** tab
- In the **Resources** area
 - Select **Policies**

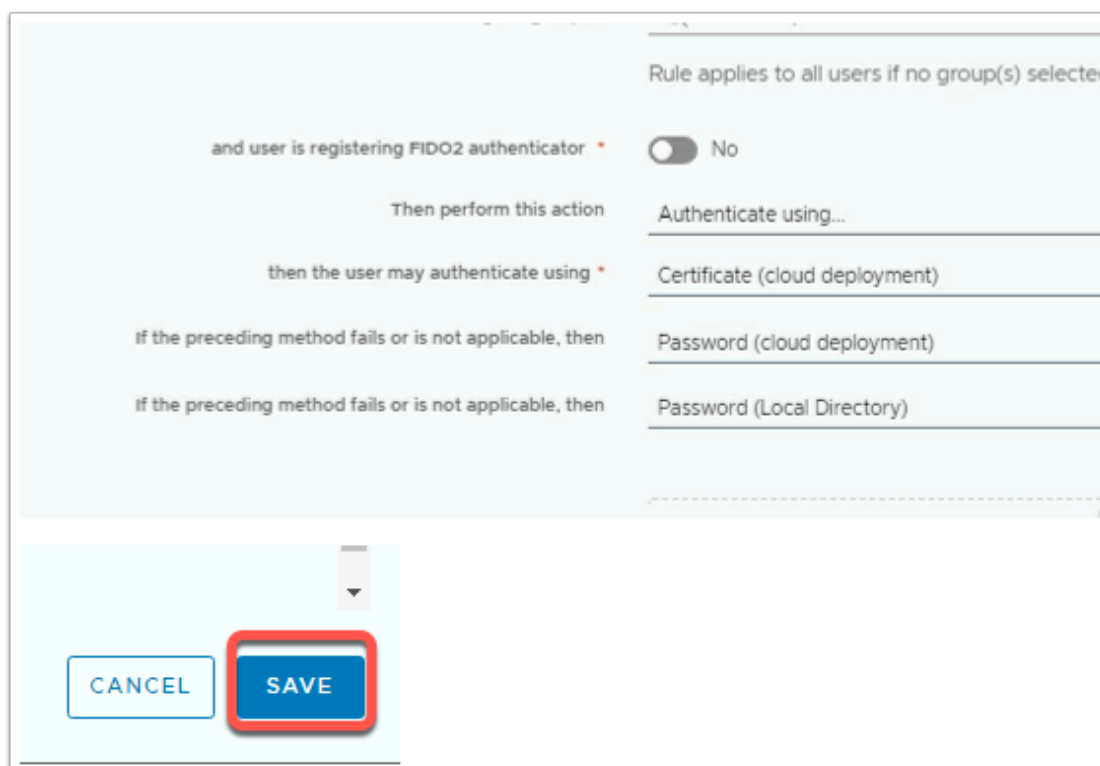


10. In the Workspace ONE Access Admin console

- Under the **Policies** area
 - Next to **default_access_policy_set**
 - Select the **radio button**
 - Select **EDIT**

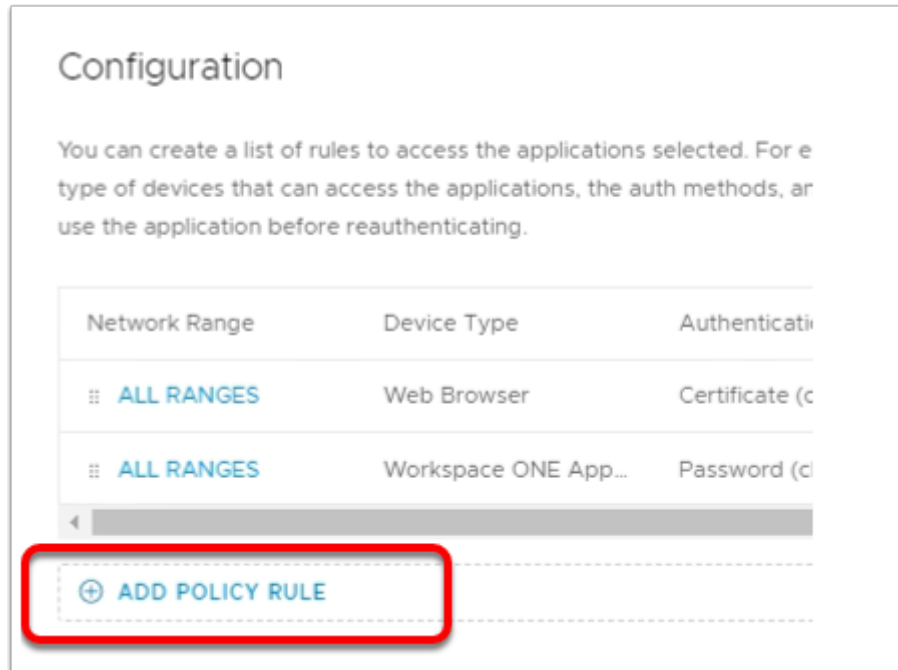


11. In the **Edit Policy** window,
 - In the left column
 - Select **Configuration**
 - To the left of **Web Browser**,
 - Select **All Ranges**



12. In the **Edit Policy Rule** window
 - Next to **then the user may authenticate using ***
 - select **Certificate (cloud deployment)**
 - 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



13. In the **Edit Policy Rule** window
 - Select **+ ADD POLICY RULE**

RATION 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)

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 * Certificate (cloud deployment)

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)

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

- Next to: -
 - **and user accessing content from***
 - select **Windows 10**
 - **then the user may authenticate using***
 - select **Certificate (cloud Deployment)**
 - **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 botom right hand side of the page
 - Select **SAVE**

Configuration

You can create a list of rules to access the applications, the type of devices that can access the applications, the user can use the application before reauthenticating.

Network Range	Device Type
ALL RANGES	Web Browser
ALL RANGES	Workspace ONE App...
ALL RANGES	Windows 10

Network Range	Device Type
ALL RANGES	Windows 10
ALL RANGES	Web Browser
ALL RANGES	Workspace ONE App...

15. 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
0 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 **Certificate (cloud deployment)**
Fallback method 1: **Password (cloud deployment)**

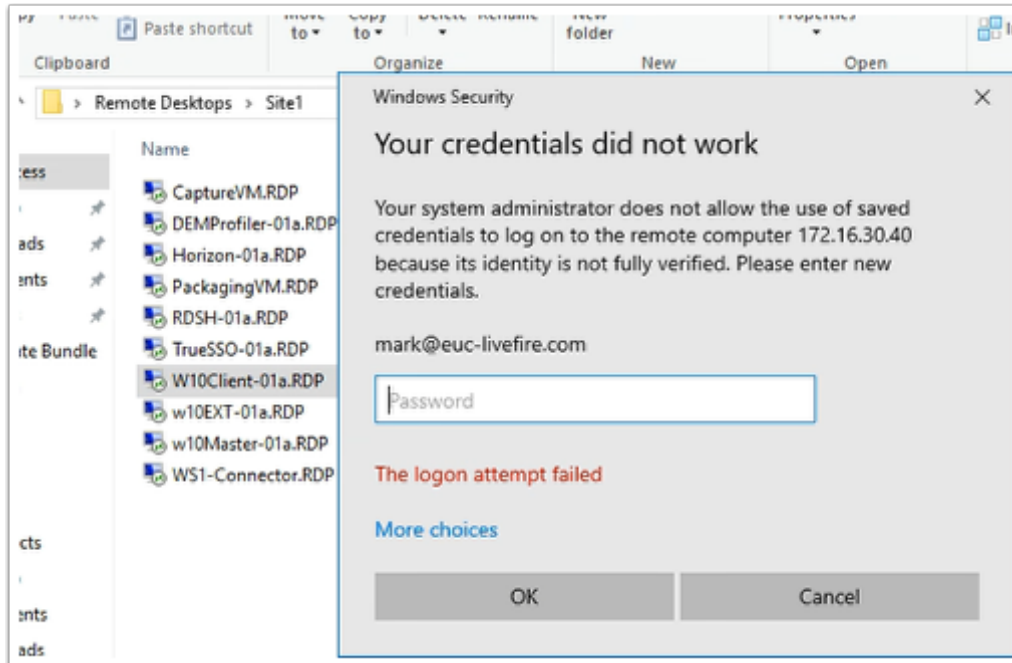
CANCEL BACK SAVE

16. On the **Edit Policy** Page.

- Summary tab
 - Select **SAVE**

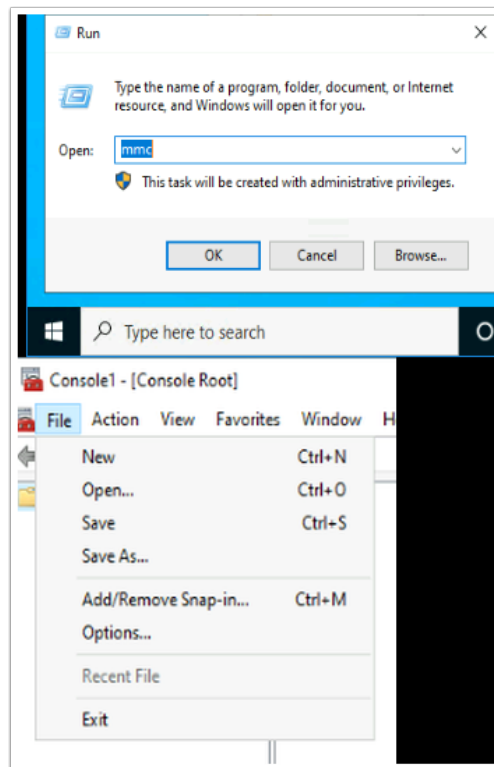
You have now enabled Certificate (Cloud Deployment) as an authentication method on the default access policy. Our next step is to ensure this implementation is working.

Part 4 Section 3: Log into a Windows 10 Desktop and demonstrate the limitation



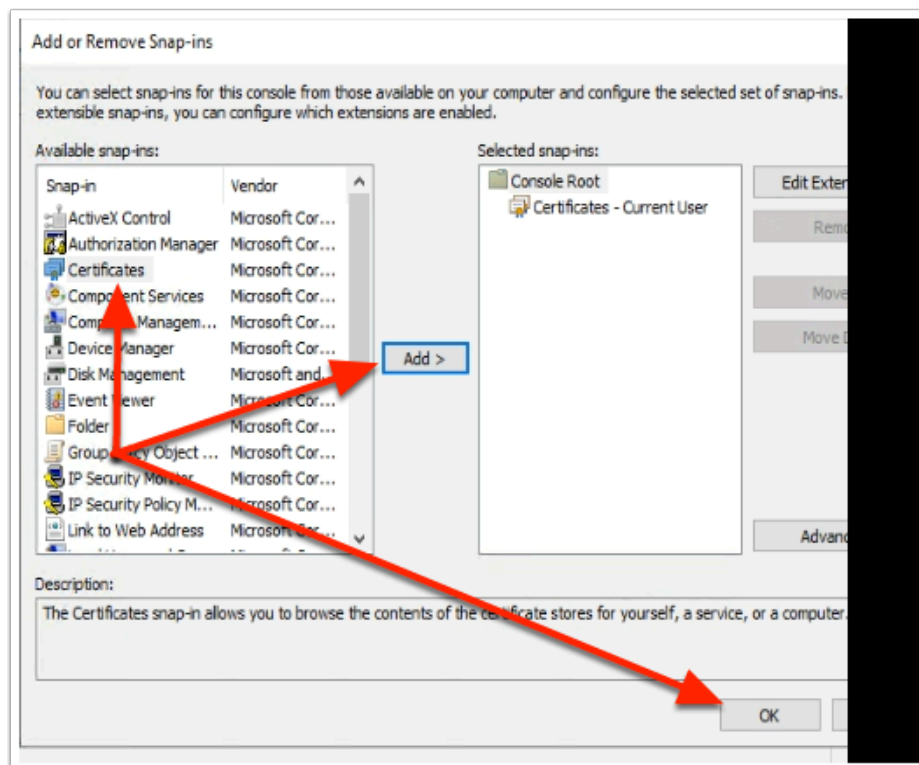
1. On the **ControlCenter** server Desktop,
 - Open the **Remote Desktops** folder,
 - Select the **W10Client-01a.RDP** shortcut
 - Log in as **mark@euc-livewire.com**,
 - enter the password **VMware1!**,
 - Select **OK**

💡 If there are any existing Horizon Desktop sessions , Workspace ONE Access logins still open. Log out and close all sessions and browsers



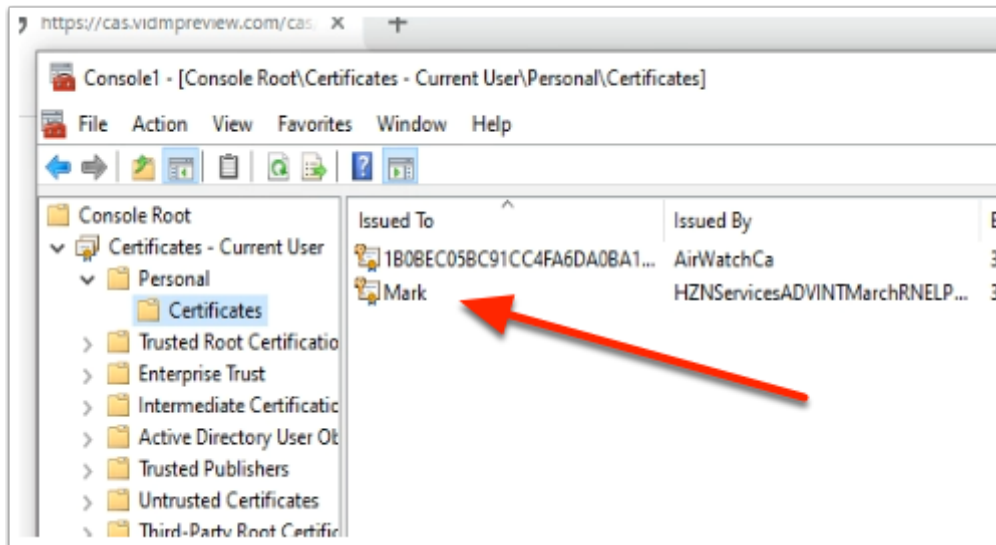
2. On **W10Client-01a** desktop

- Select **Start** > **Run**,
- Next to **Open**, type **mmc**,
- Select **OK**
- In the **Console**, select **Add/Remove Snap-in**



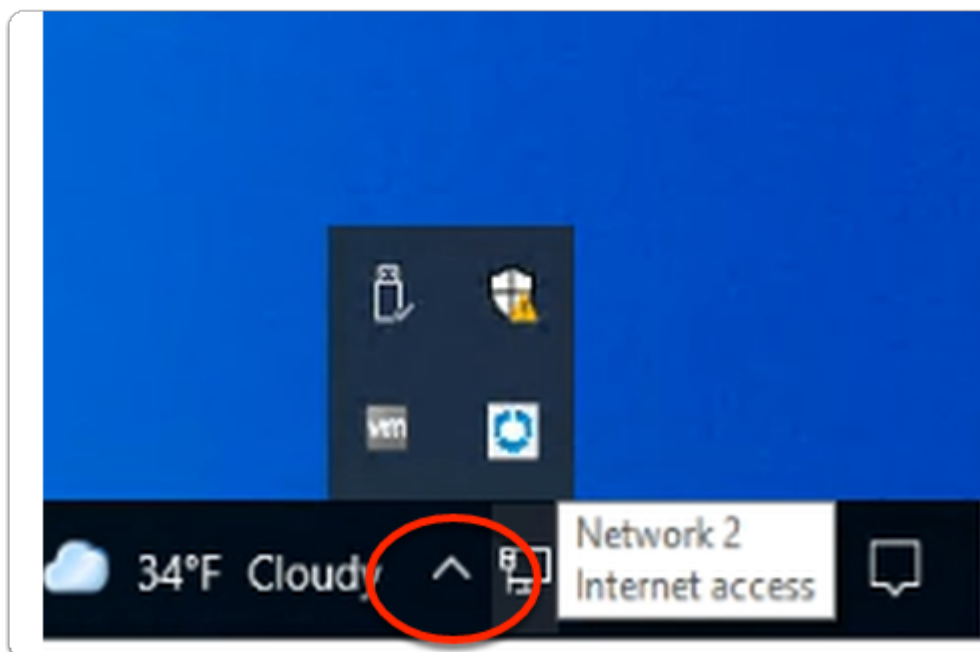
3. In the **Add or Remove Snap-ins** window

- Select **Certificates**,
- Select **Add**
- Select **OK**



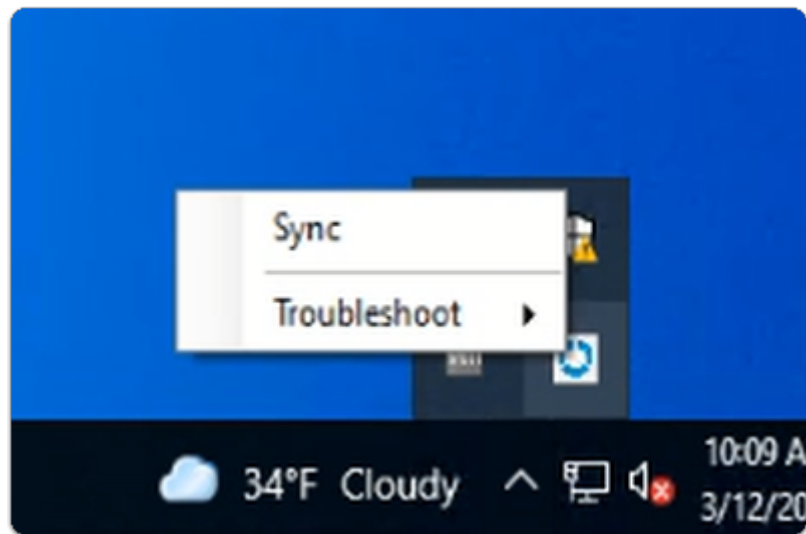
5. **Expand Certificates - Current User**

- **Expand Personal**
- Select **Certificates**
 - Note you have an enrolled certificate. If you don't have a certificate,
 - Follow steps 6 - 8.
 - If you have an enrolled certificate
 - Carry on from step 9

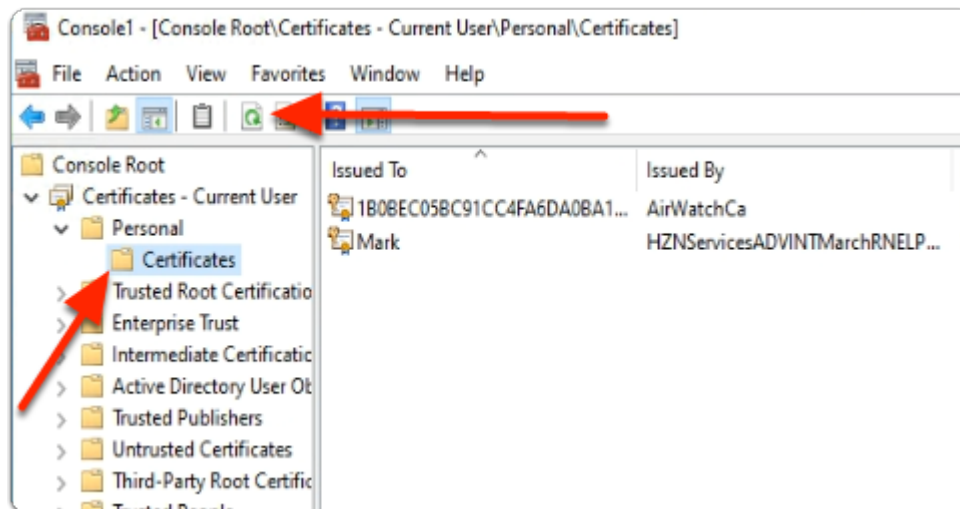


6. On your W10Client-01a desktop

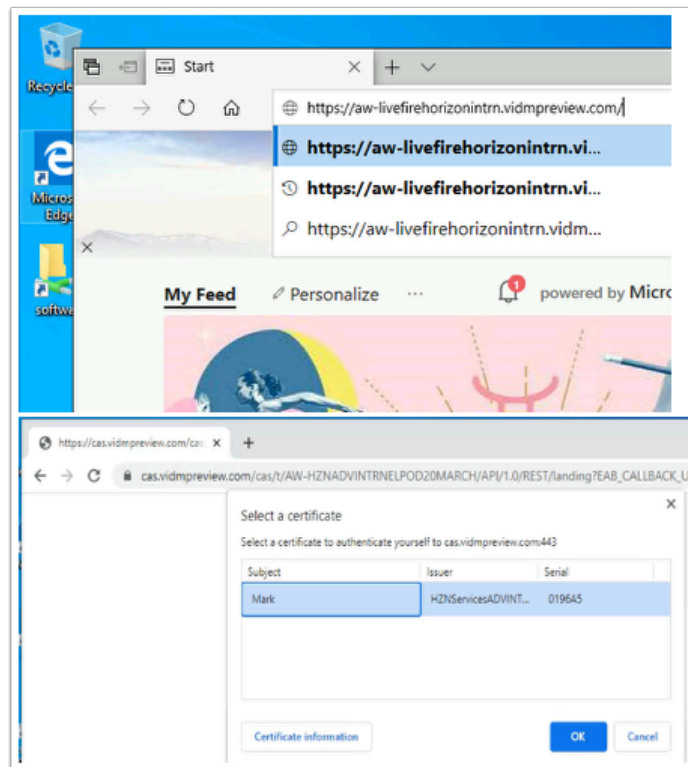
- In the right bottom corner of your **Taskbar**
 - To the left of the **Network** icon
 - Select the **UP** arrow



7. On your W10Client-01a desktop
 - **Select** and **right-click** the **Intelligent Hub** icon
 - Select **Sync**

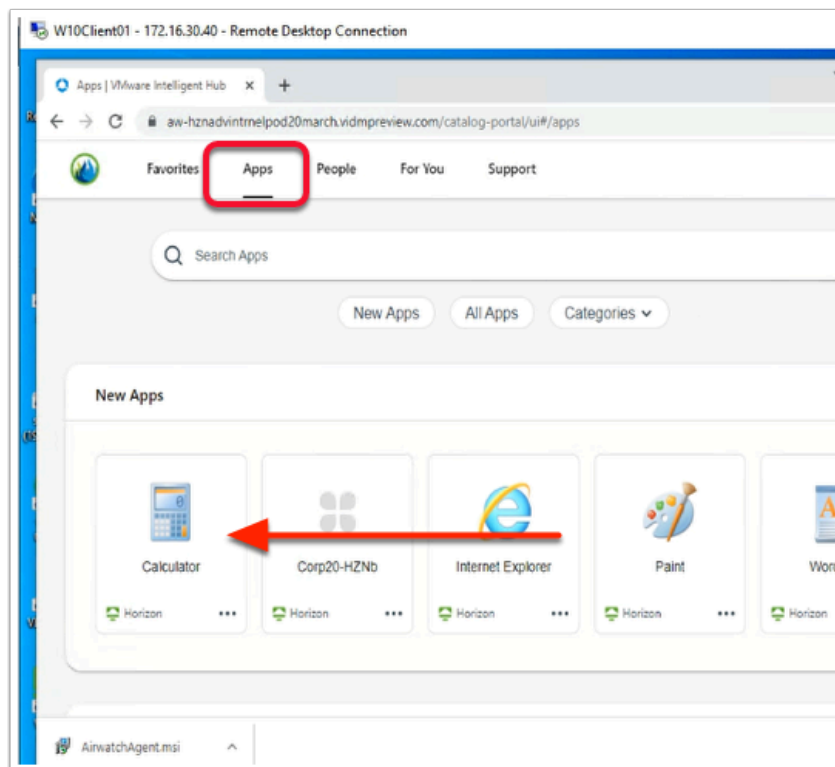


8. In the **Certificates** snap-in
 - Under **Personal**
 - Select **Certificates**
 - In the **Toolbar**
 - Select **Refresh**



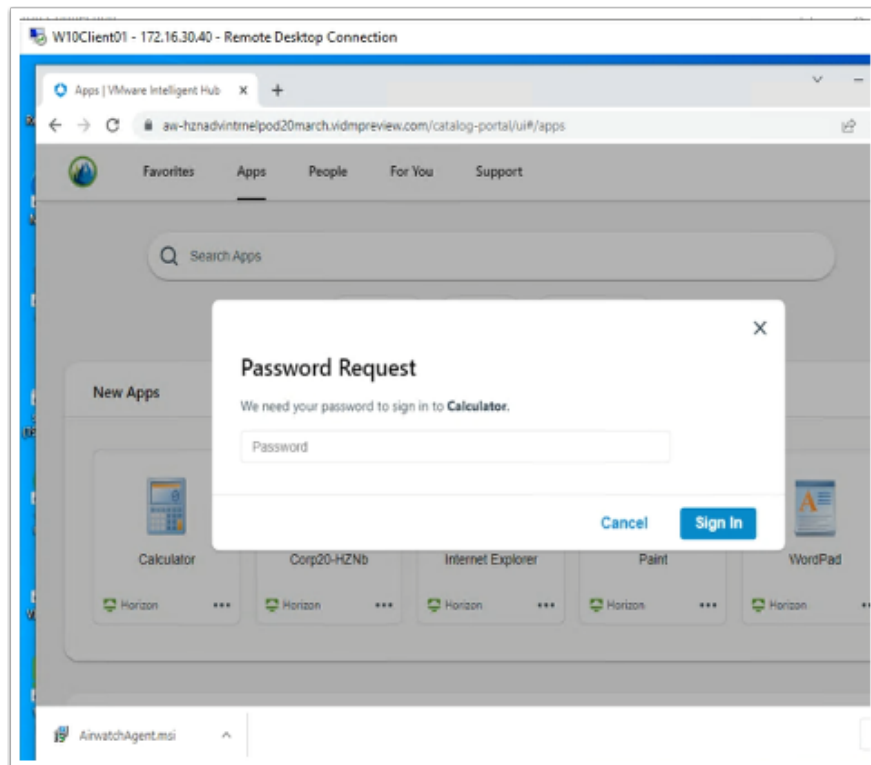
9. On your **W10Client-01a** Desktop

- Open a **browser** on your windows 10 desktop
- In the **address bar** enter the **URL of your Saas Access Tenant**
- In the **Select a certificate** window
 - Select **OK**



10. On the **Workspace ONE** console ,

- In the **Apps** tab
- Select **Calculator**

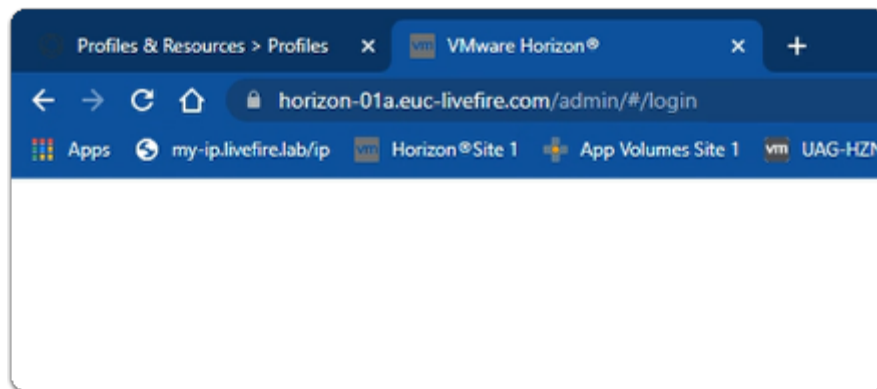


11. In the Intelligent Hub

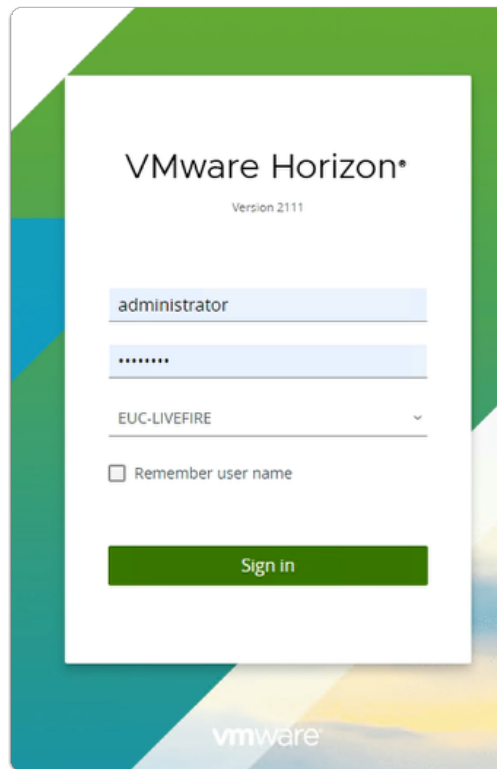
- Notice we are getting a Password request.
 - We used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password Auth method, to pass on to the Horizon Agent.
 - We will now move forward with Configuring HORIZON TRUESSO
- Select **Cancel** to close the **Password Request** window.
- **Logout** and **close** all windows on **W10Client-01a**

Part 5. Integrating Horizon TRUESSO with the Horizon Universal Console

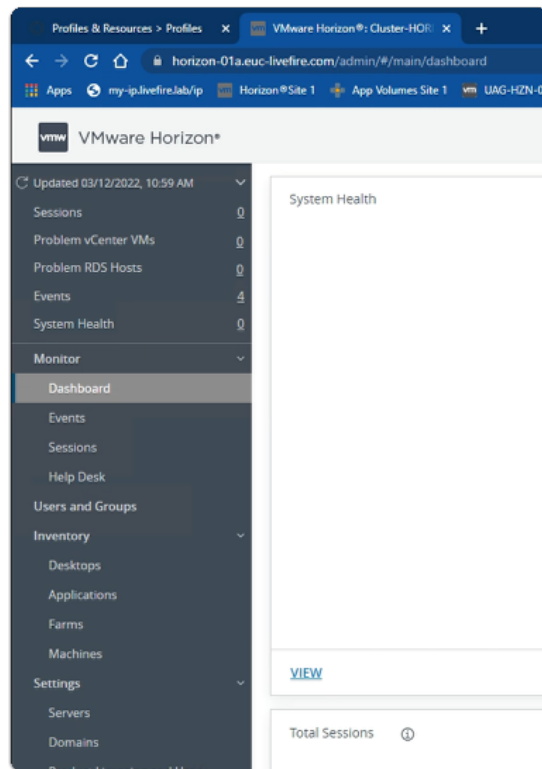
Part 5 Section 1: Integrating Horizon TRUESSO with Horizon Universal Console



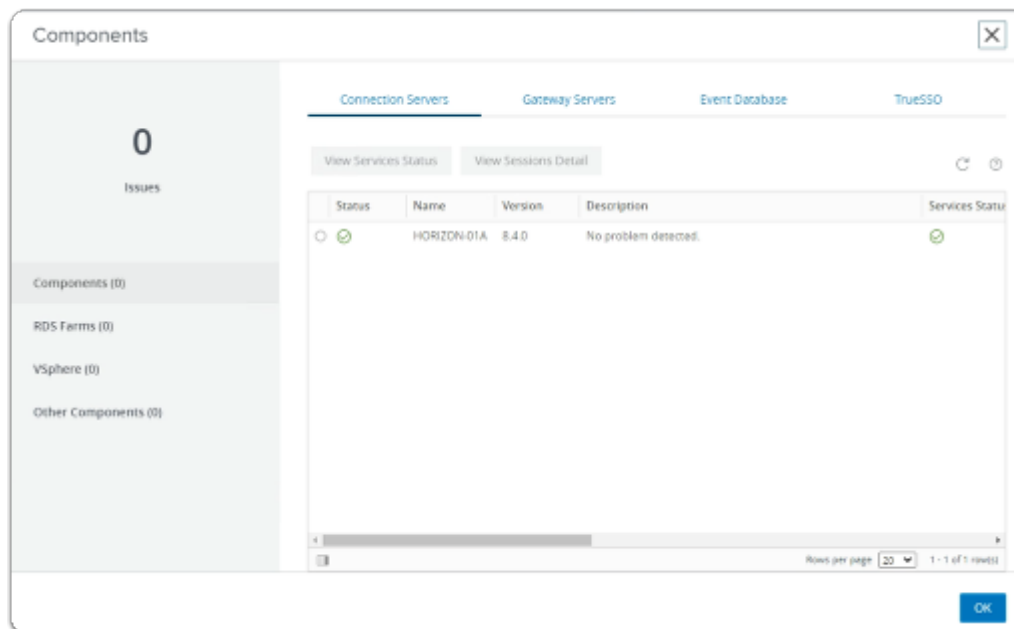
1. On your ControlCenter server
 - On your **Site 1** Browser
 - Open a **new Tab**
 - Select **Horizon Site 1**



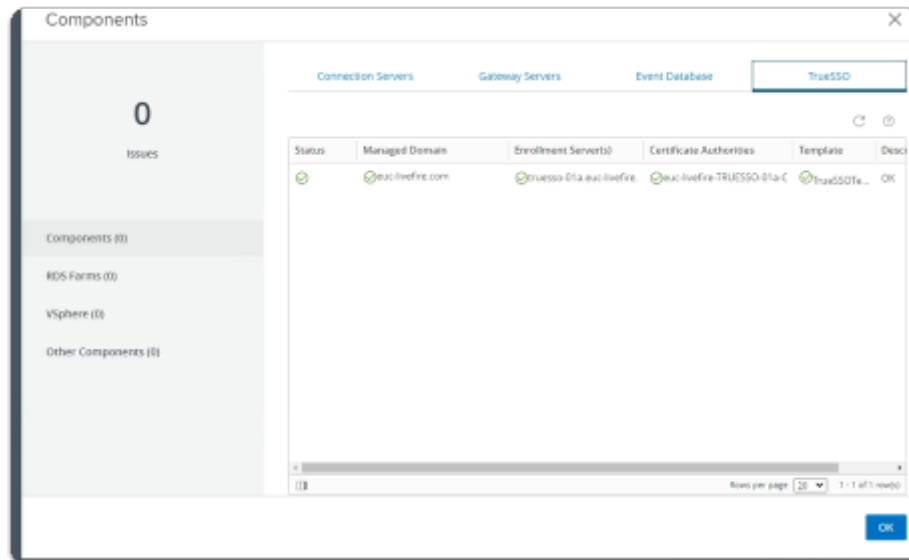
2. On **VMware Horizon** login
 - In the **Username** area
 - type **Administrator**
 - In the **Password** area
 - type **VMware1!**
 - Select **Sign In**



3. In the Horizon Admin console
 - In the **Dashboard** area
 - Select **VIEW**

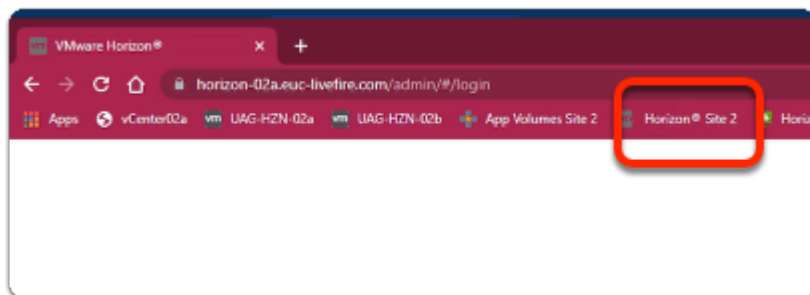


4. In the **Components** window
 - Select **TrueSSO**



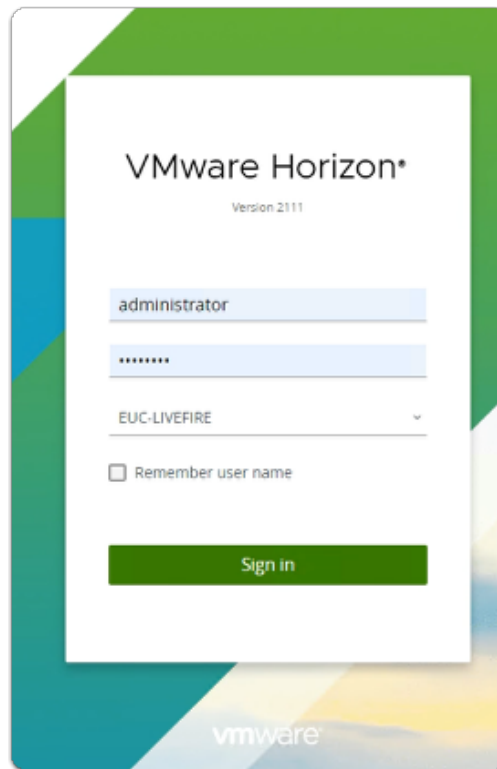
5. In the **TrueSSO** area of Components

- Note that **Enrollment** and **Sub-ordinate CA** servers have been deployed and configured
- To Close the **Components** window
 - Select **OK**

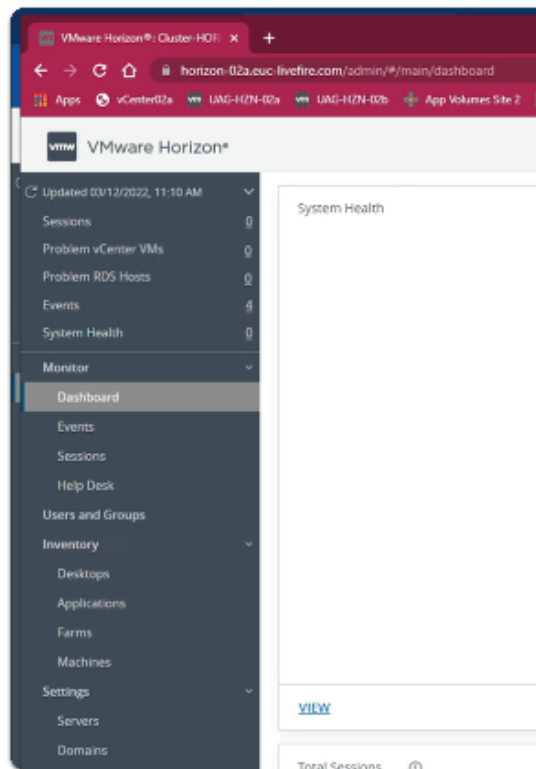


6. On your ControlCenter server

- On your **Site 2** Browser
 - Open a **new Tab**
- Select **Horizon Site 2**

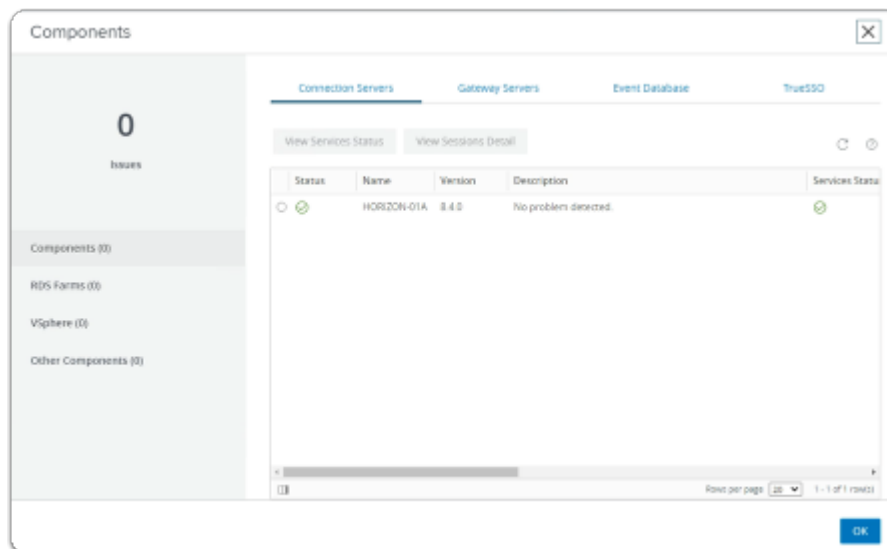


7. On **VMware Horizon** login
 - In the **Username** area
 - type **Administrator**
 - In the **Password** area
 - type **VMware1!**
 - Select **Sign In**



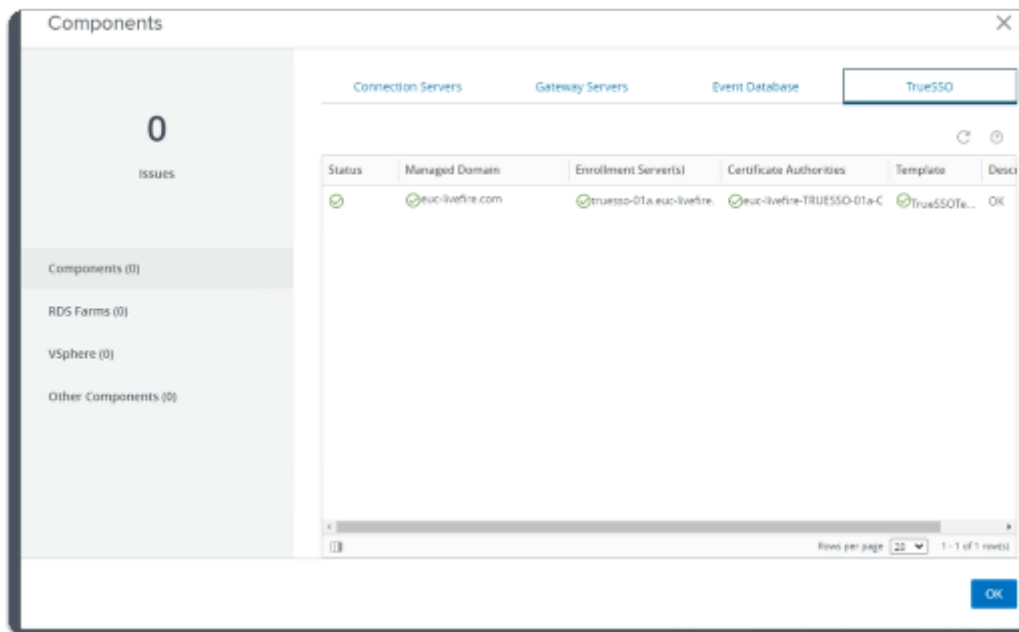
8. In the Horizon Admin console

- In the **Dashboard** area
 - Select **VIEW**



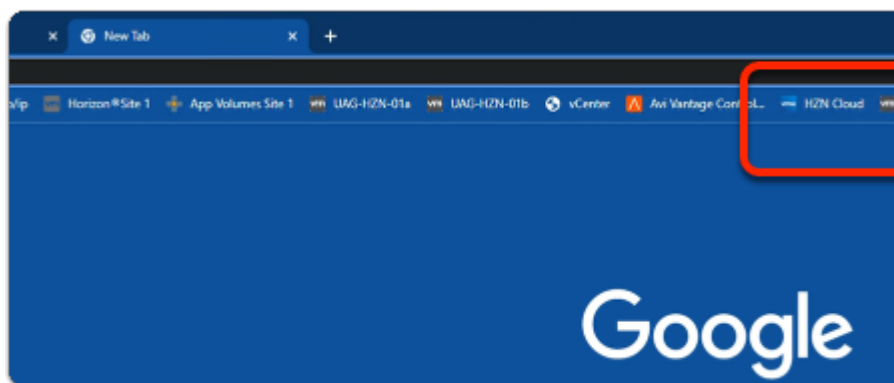
9. In the **Components** window

- Select **TrueSSO**



10. In the TrueSSO area of Components

- Note that **Enrollment** and **Sub-ordinate CA** servers have been deployed and configured
- To Close the **Components** window
 - Select **OK**



11. On your ControlCenter server

- **Revert** to your **Site 1** browser
- **Open** a new tab
- Select the **HZN Cloud** shortcut

Welcome to
VMware Horizon®

My VMware Credentials

Username

Password

☒ Remember me

LOGIN

[Forgot password?](#)

12. On the **Welcome to VMware Horizon®** page
- Under **My VMware Credentials**, enter the following
 - In the **Username** area, type your, **assigned Horizon Cloud email**
 - In the **Password** area, type , **VMware1!**
 - Select **LOGIN**

Welcome to
VMware Horizon®

Active Directory Credentials

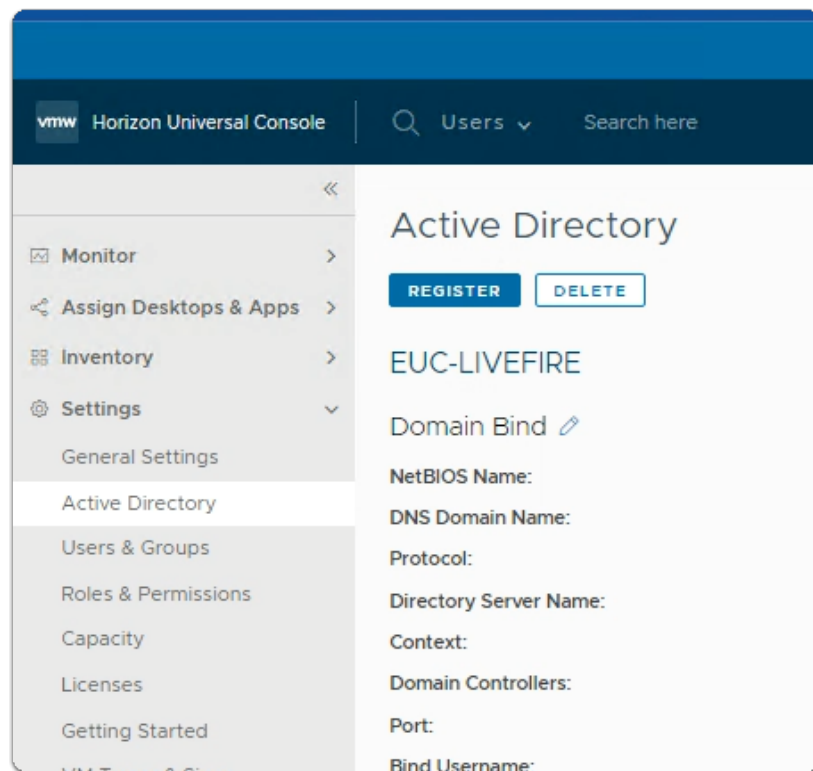
Username

Password

EUC-LIVEFIRE

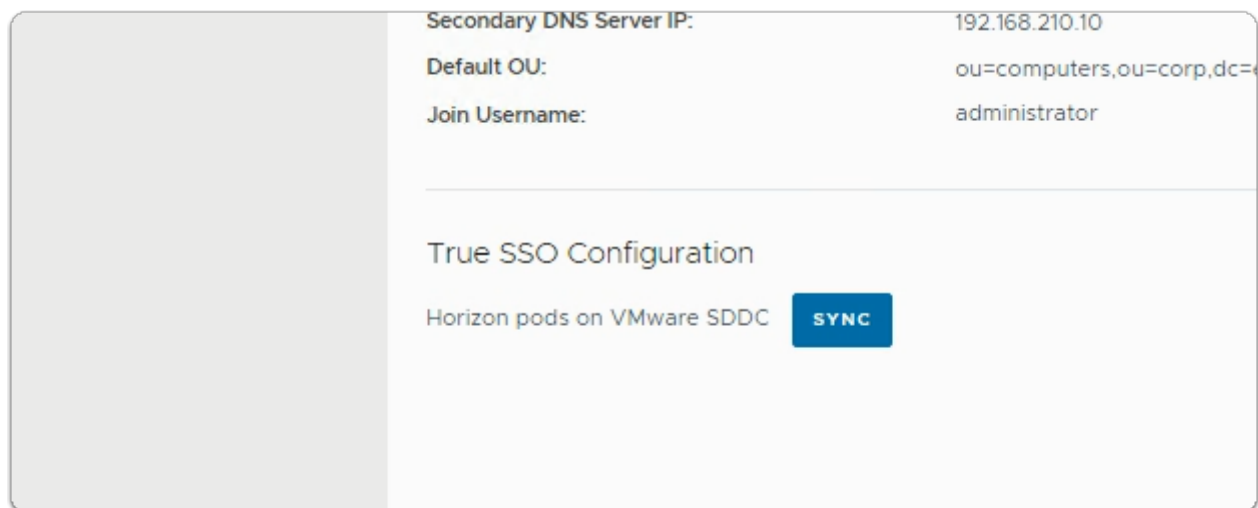
LOGIN

13. On the **Welcome to VMware Horizon®** page
- Under **Active Directory Credentials**, enter the following
 - In the **Username** area, type **Administrator**
 - In the **Password** area, type , **VMware1!**
 - Select **LOGIN**



14. In the Horizon Universal Console

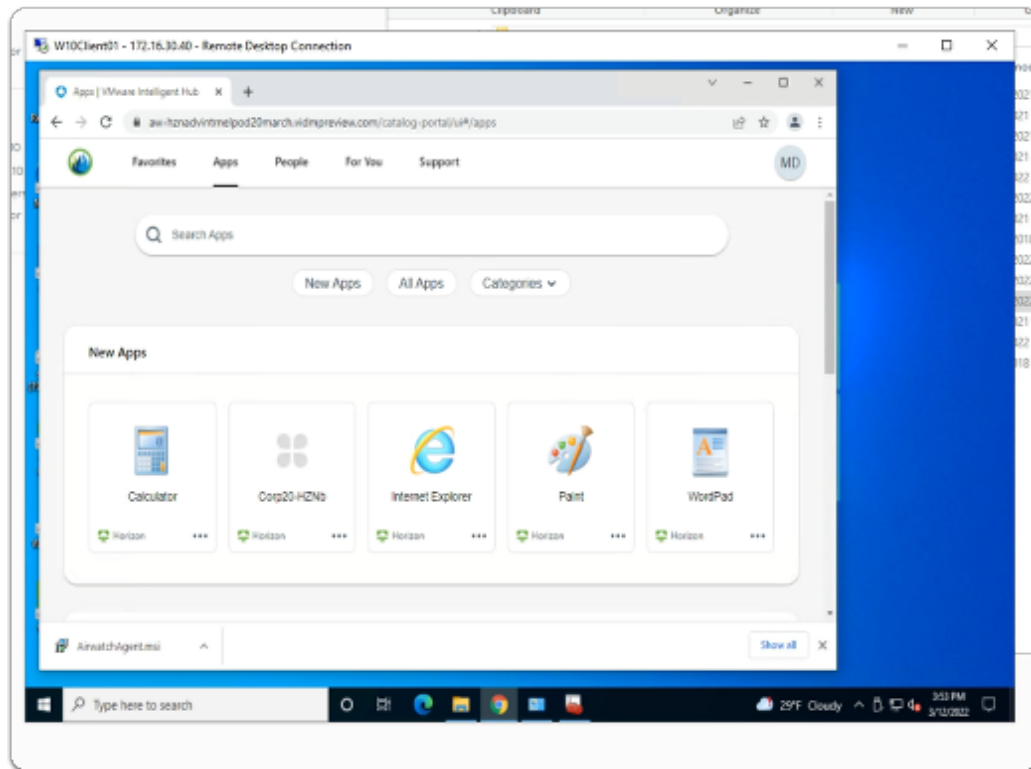
- Expand **Settings**
- Select **Active Directory**



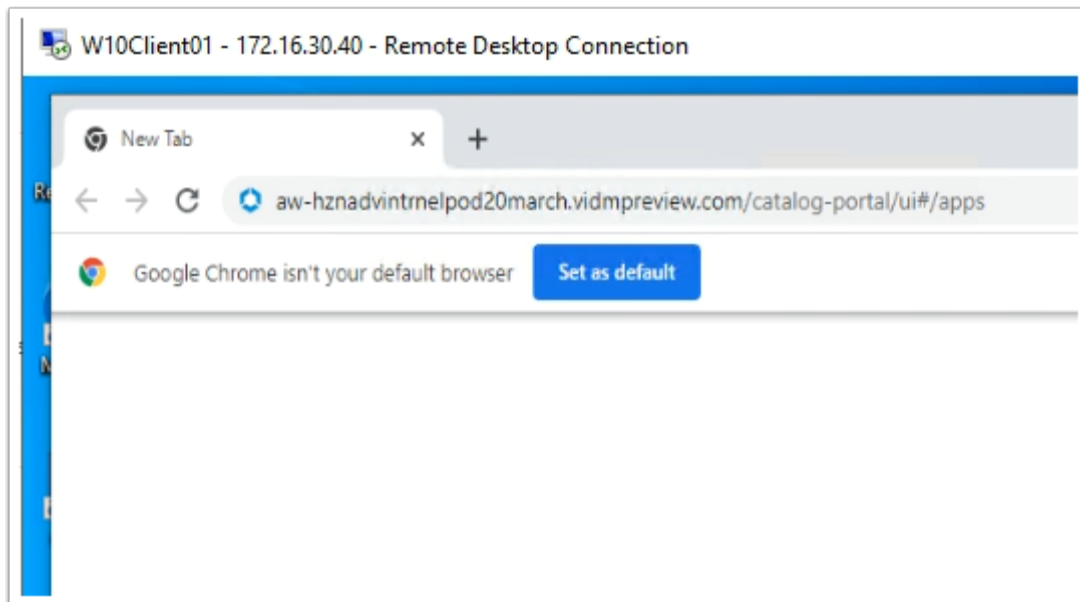
15. In the **Active Directory** area

- In the **True SSO Configuration** area
 - Next to **Horizon pods on VMware SDDC**
 - Select **SYNC**

Part 5 Section 2: Testing to see if TRUESSO works

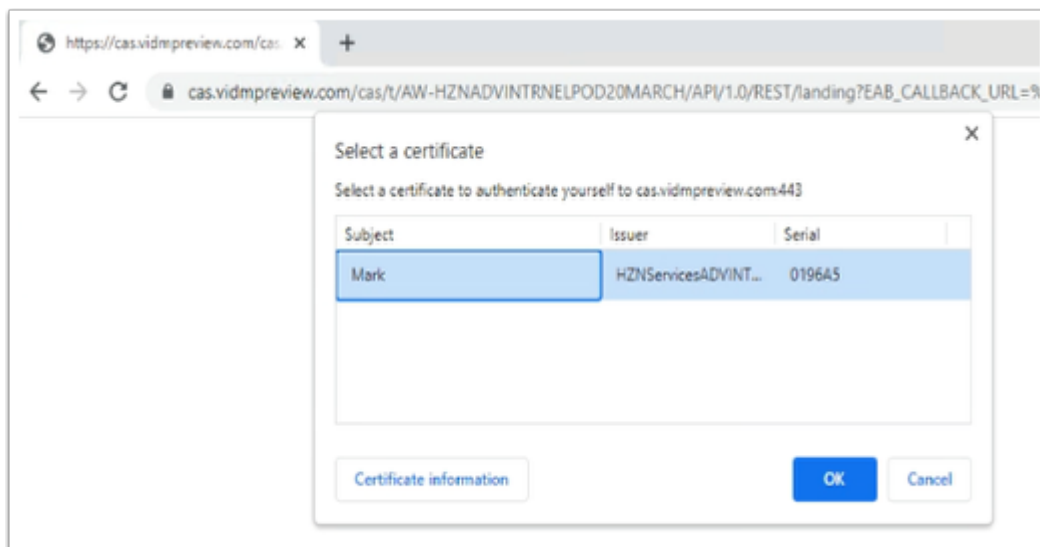


1. On your **ControlCenter** server,
 - Switch to your **Remote Desktops** session to **W10Client-01a.RDP** session.
 - If necessary, login again with
 - **Username :** **Mark@euc-livefire.com**
 - **Password:** **VMware1!**
 - **Sign out** of any existing sessions,
 - **close** all windows



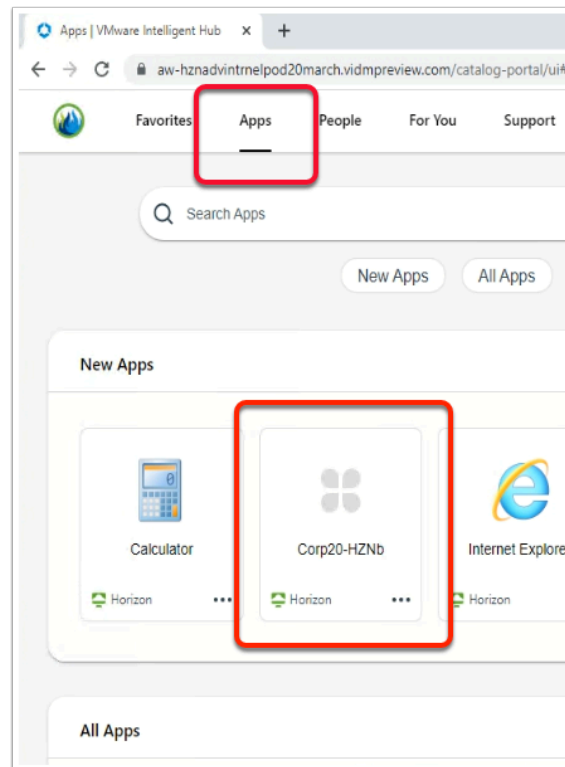
2. On your **W10Client-01a** desktop,

- **Open** your browser
- Enter your **custom Workspace ONE Access URL**



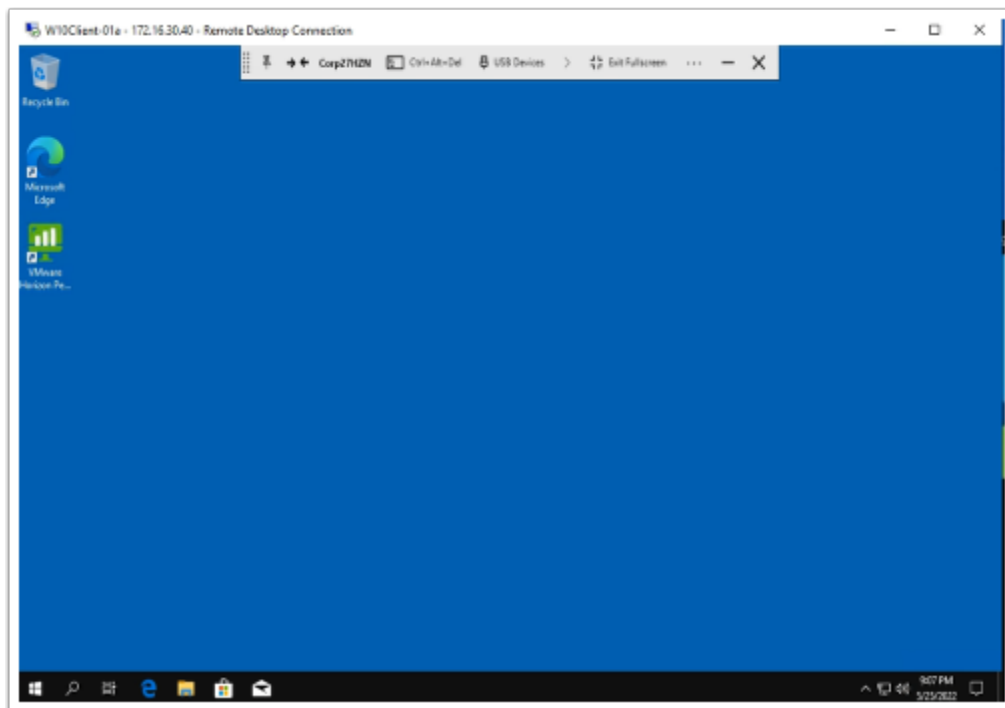
3. On the **Select a certificate** window,

- Select **OK**



4. In the **Intelligent Hub**


- Under **Apps**
 - Select **CorpXX-HZN**
 - where **XX** is your assignment



5. On the **W10Client-01a**

- Note that you have now observed a Single sign-on session

- Possibly launch a RDSH session from your Workspace ONE Access console
- This concludes this lab

 After initiating the TRUESSO SYNC, the initial testing of this Horizon Cloud Connector and version of Horizon 2209. I took up to 10 minutes for the SYNC, to take effect. Keep trying until it works