

4. Unified Access Gateway / VMware Horizon integration into Workspace ONE Access

Overview

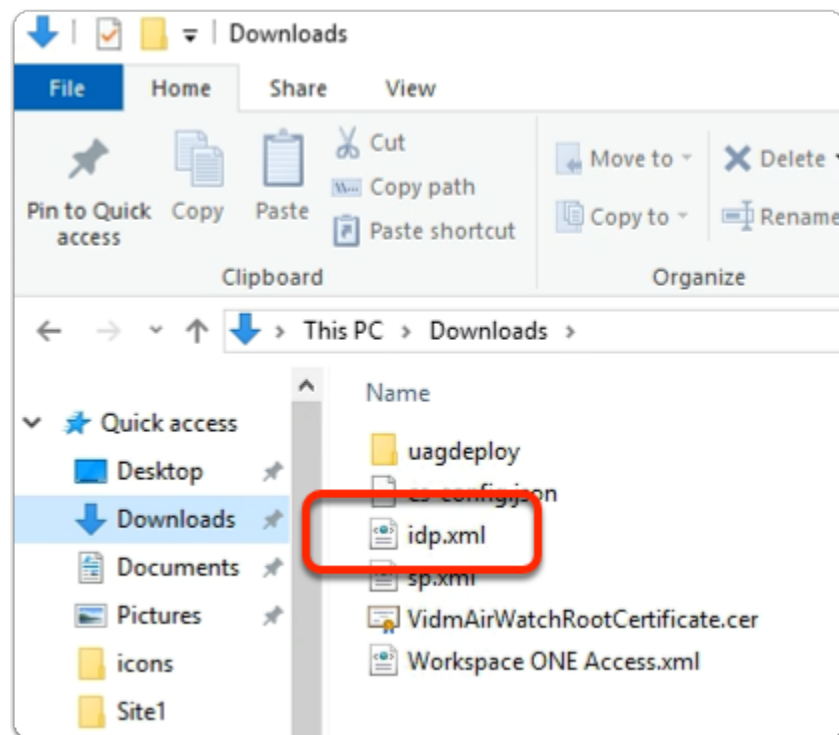
- Traditional Federation with VMware Horizon and Workspace ONE Access has been a popular approach and is used by many organizations.
- Organizations with High Security requirements do not like SAML artifacts being validated internally
- In this session we look at the option to validate the SAML artifact on the Unified Access Gateway instead of forwarding the artifact internally.

Part 1. Enabling SAML federation with the VMware Unified Access Gateway for Workspace ONE Access as the IDP

The Federation of Unified Access Gateway and VMware Horizon with Workspace ONE Access will be done in three phases

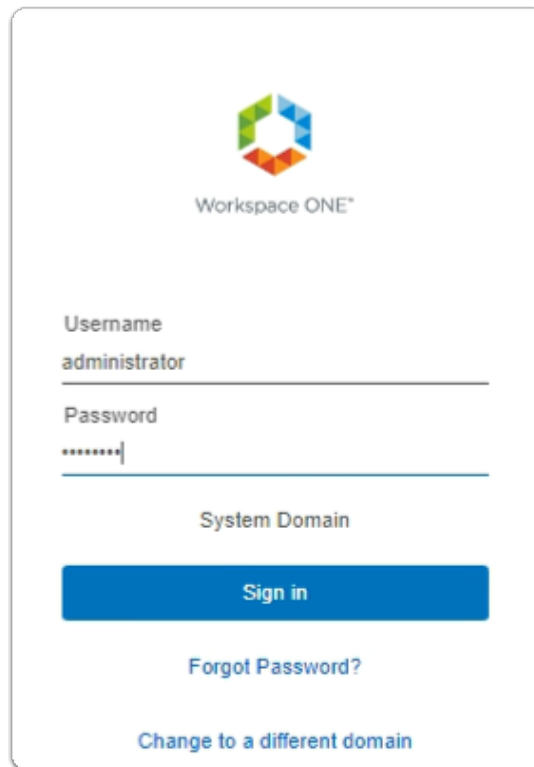
- Phase 1. We enable and configure the SAML federation on 4 VMware Unified Access Gateway servers in a multi-site scenario
- Phase 2. We enable and configure the SAML Integration as a Web App in Workspace ONE Access
- Phase 3. We will create deep links in Workspace ONE Access for our Desktop entitlements

Step 1. Preparing to Federate the Unified Access Gateway with Workspace ONE Access



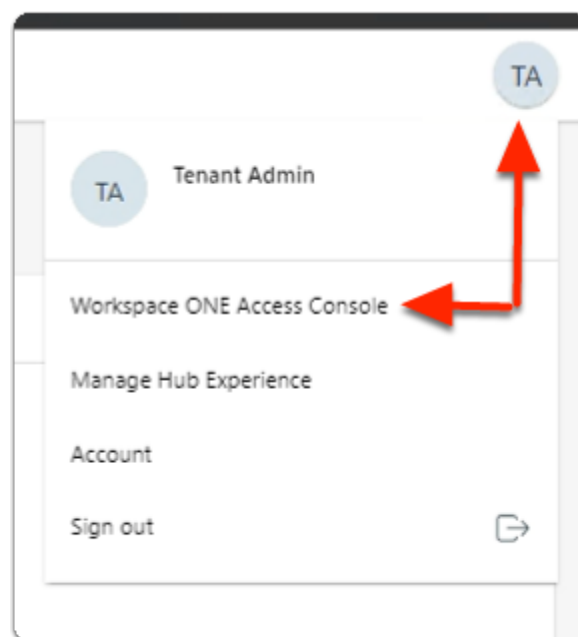
💡 Note exporting the IDP.XML was accomplished on Day 1. Step 1 is here to remind you of the process. If you have an IDP.xml file downloaded in your Downloads folder on your ControlCenter server.

Move on to Step 2.

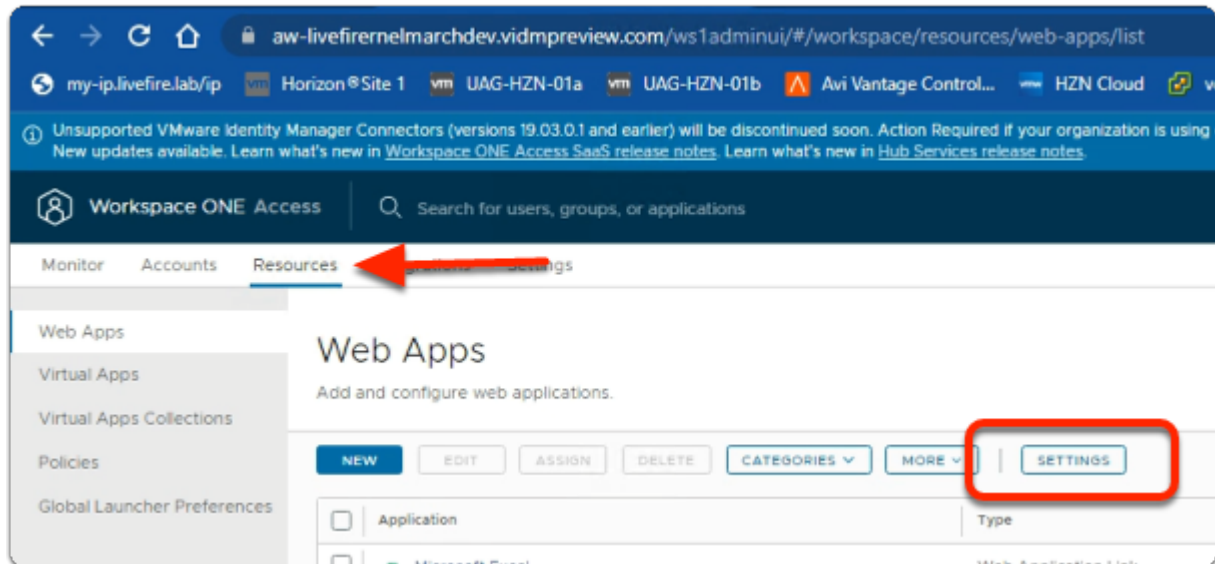


The image shows the Workspace ONE login interface. At the top is the Workspace ONE logo. Below it are two input fields: 'Username' with the text 'administrator' and 'Password' with masked characters '*****'. A 'System Domain' label is positioned above a blue 'Sign in' button. Below the button are two links: 'Forgot Password?' and 'Change to a different domain'.

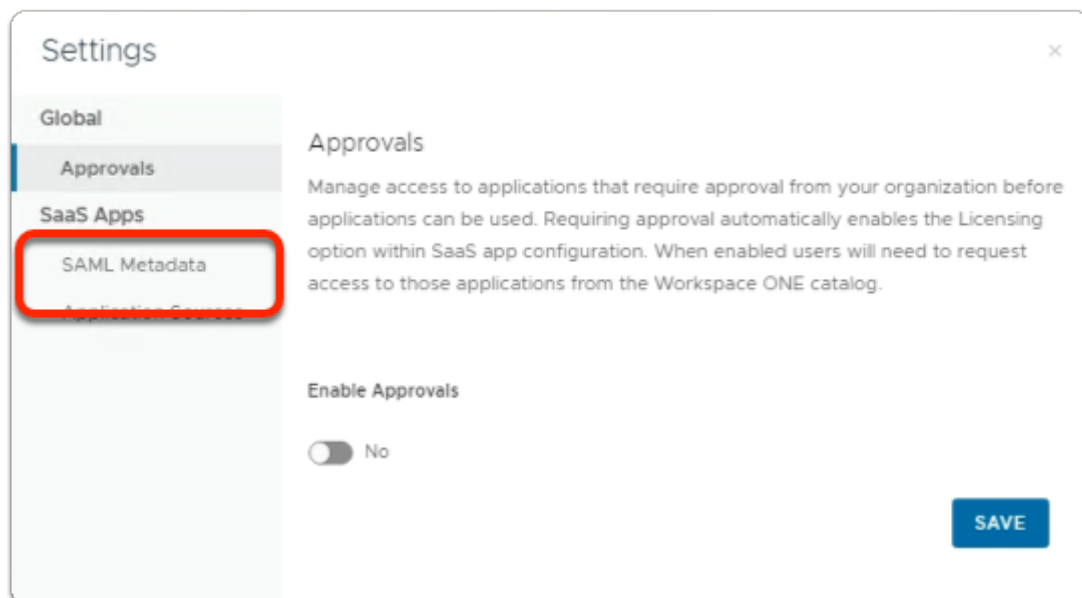
1. On your ControlCenter server
 - Open your **Workspace ONE Access**, Admin console URL
 - Under **Username**
 - enter **Administrator**
 - Under **Password**
 - enter **VMware1!**
 - Select **Sign In**



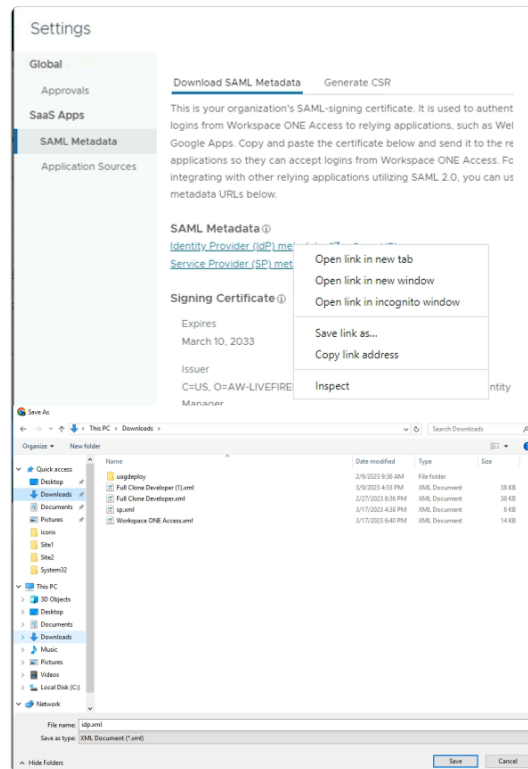
2. In the **Web Intelligent Hub** Console
 - To the right,
 - select **TA**
 - From the dropdown
 - select **Workspace ONE Access Console**



3. In the **Workspace ONE Access Console**
 - Select **Resources**
 - Under **the Resources > WEB Apps** area
 - Select **SETTINGS**

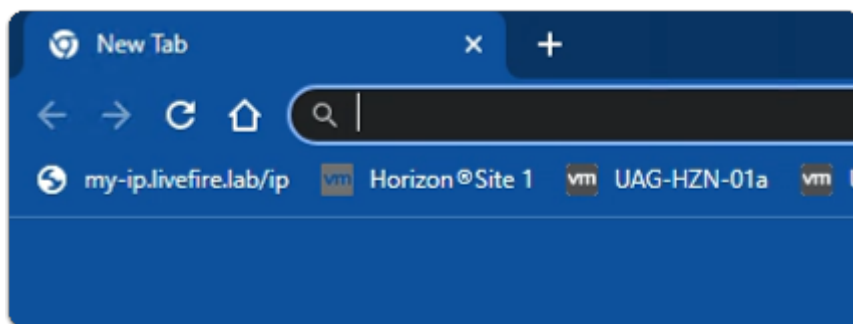


4. In the **Settings** window
 - below **SaaS Apps**
 - select **SAML Metadata**



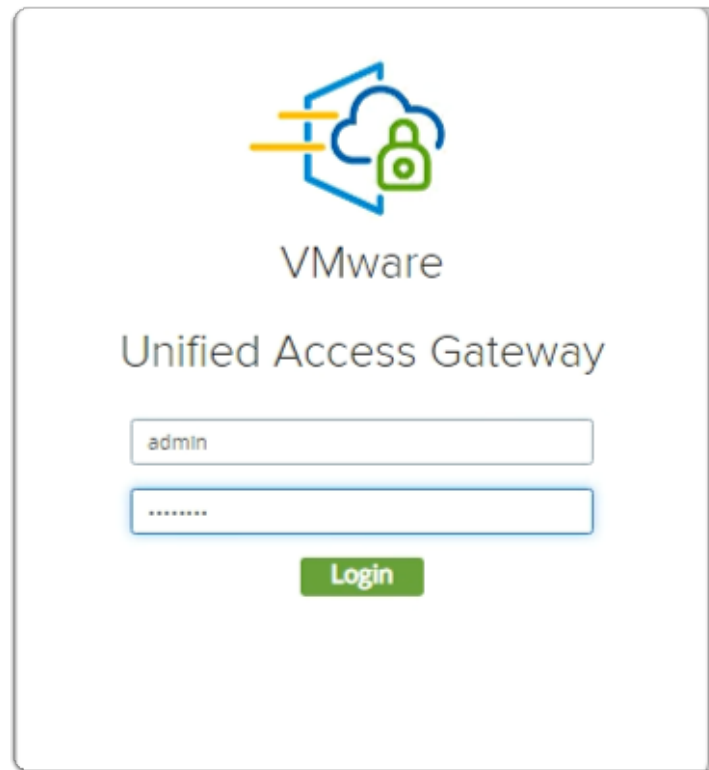
5. In the **Settings** window
 - in the right pane
 - below **SAML Metadata**
 - select & right click **Identity Provider (IdP) metadata**
 - in the **drop down** menu
 - select **Save link as...**
 - in File Explorer **Save As** window
 - ensure **Downloads** is selected **Quick Access** (default)
 - at the bottom of the window
 - select **Save**

Step 2. Enabling SAML Federation on Site 1 , UAG-HZN-01a

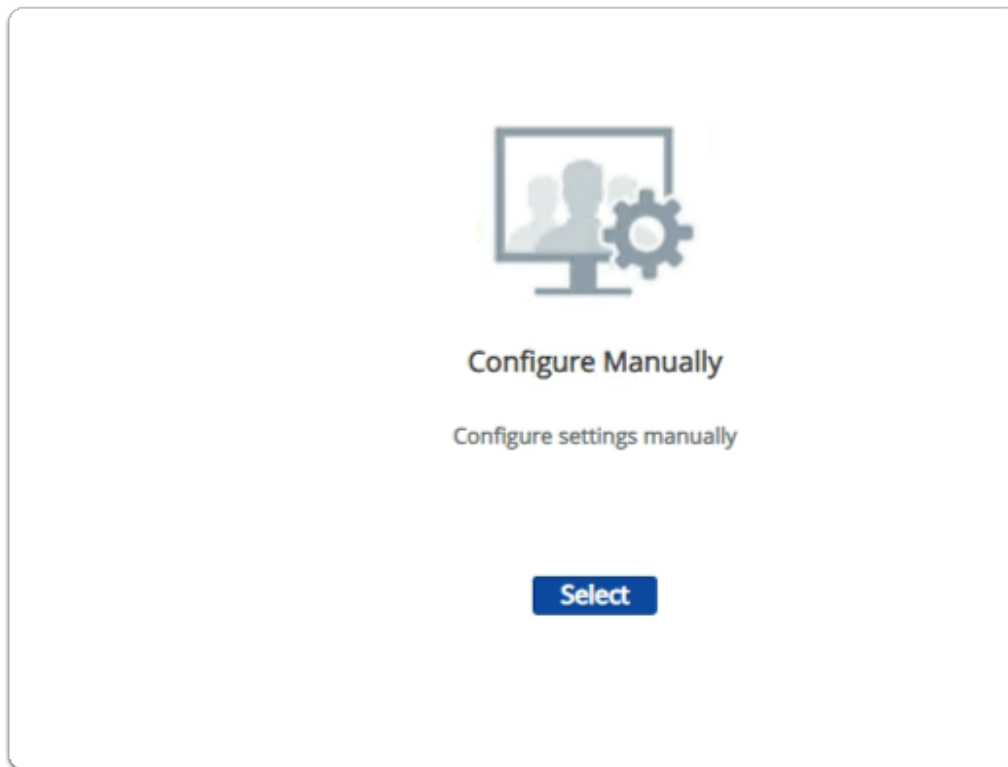


1. On your **Site 1 Browser** profile
 - In the **Favourites bar**

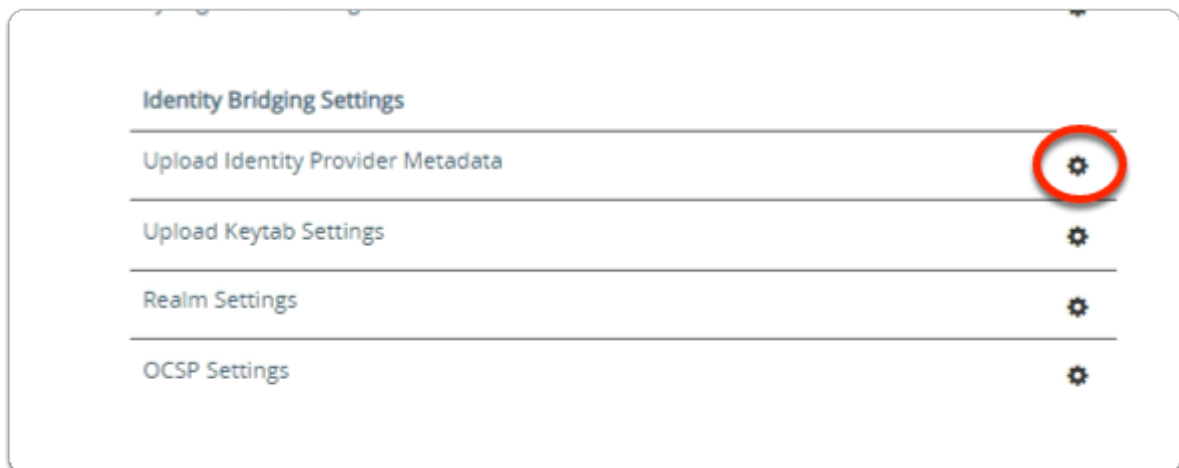
- select the **UAG-HZN-01a** shortcut



2. In the **VMware Unified Access Gateway** login
 - in the **Username** area
 - enter **admin**
 - in the **Password** area
 - enter **VMware1!**
 - select **Login**



3. In the **VMware Unified Access Gateway** admin console
 - below **Configure Manually**
 - click **Select**



4. In the **VMware Unified Access Gateway** admin console
 - **scroll down** to **Identity Bridging Settings**
 - to the right of **Upload Identity Provider Metadata**
 - select the **GEAR** icon

Upload Identity Provider Metadata

Entity ID ⓘ

+ IDP Metadata Select ⓘ

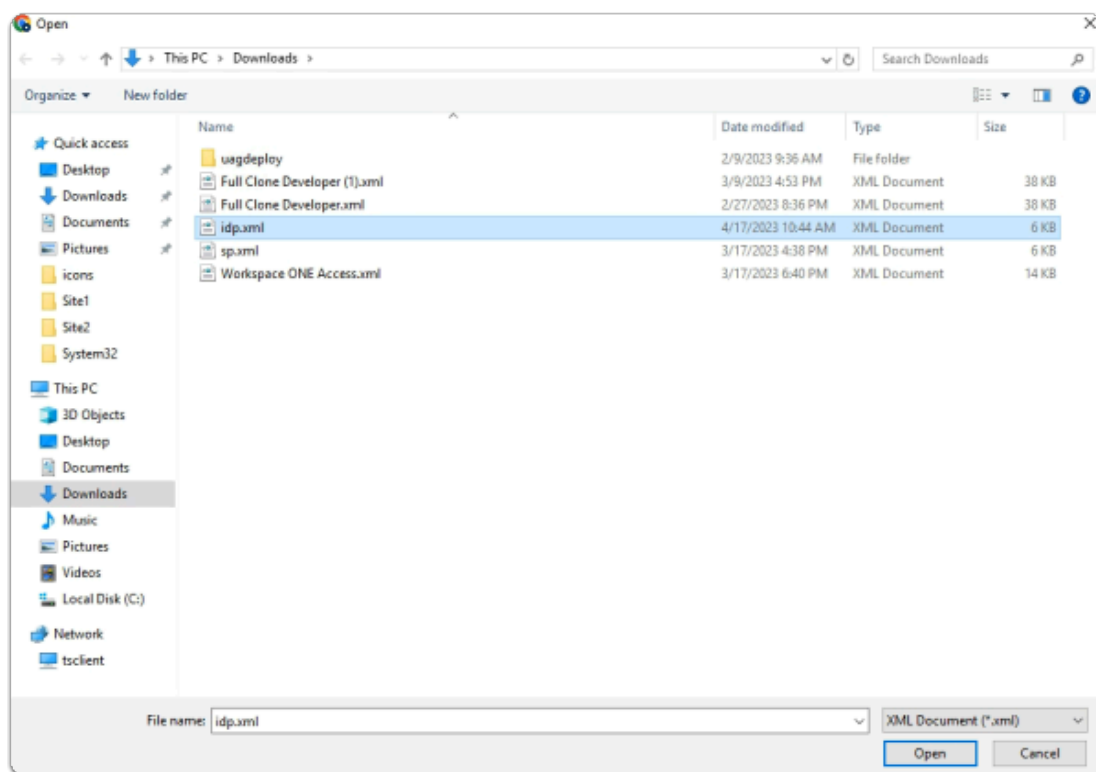
Encryption Certificate Type None ⓘ

Always force SAML auth ☐ ⓘ

Save **Cancel**

5. In the **Upload Identity Provider Metadata** window

- next to **Entity ID**
 - enter **Workspace ONE Access**
- next to **IDP Metadata**
 - click **Select**



6. In the **File Explorer - Open** window

- **Quick Access > Downloads** folder
 - (this should be the default)
 - select **idp.xml**
- in the bottom right corner
 - select **Open**

Upload Identity Provider Metadata

Entity ID ⓘ

* IDP Metadata [Change](#) ⓘ

Encryption Certificate Type ⓘ




Always force SAML auth ☒ ⓘ

Save **Cancel**

7. In the **Upload Identity Provider Metadata** window

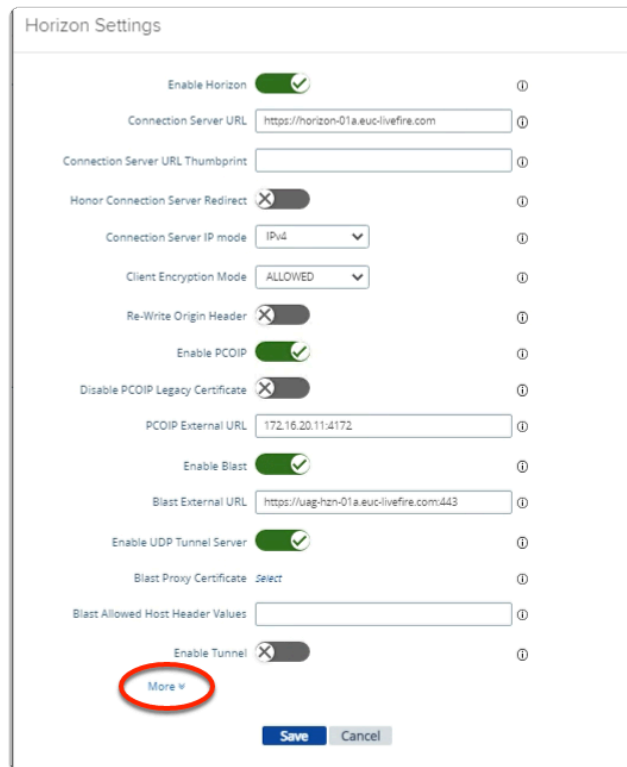
- next to **Always force SAML auth**
 - switch the **Toggle** from **OFF** to **ON**
 - select **Save**
- **scroll** back up to the top of UAG admin console

Edge Service Settings ☒ [Refresh](#) *Active Sessions: 0*

<input checked="" type="radio"/>	Horizon Settings	
<input type="radio"/>	Reverse Proxy Settings	
<input type="radio"/>	Tunnel Settings	

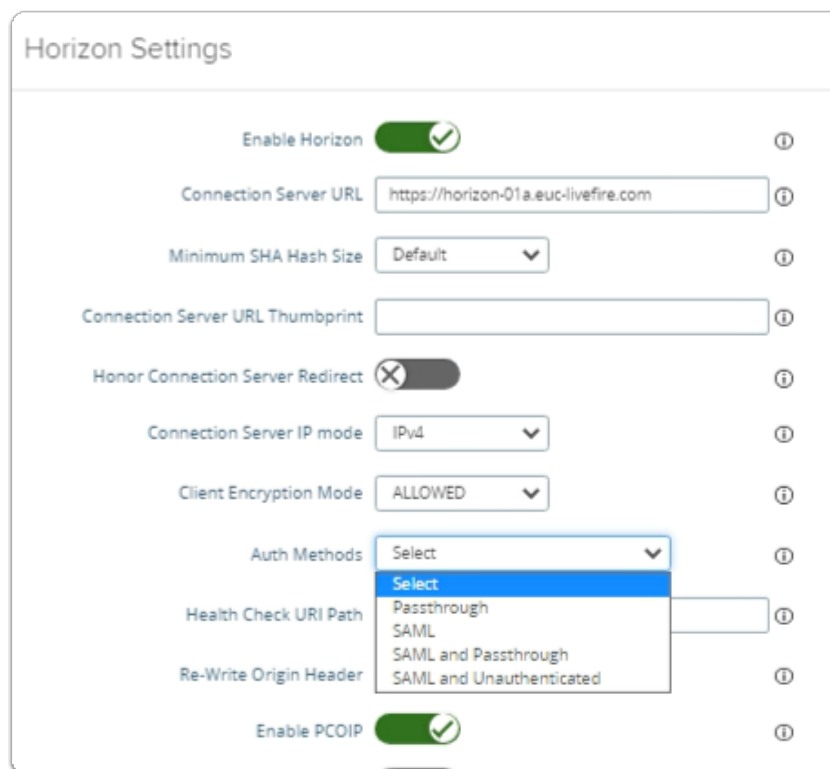
8. In the **VMware Unified Access Gateway** admin console

- In the **General Settings** area
 - next to **Edge Service Settings**
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon



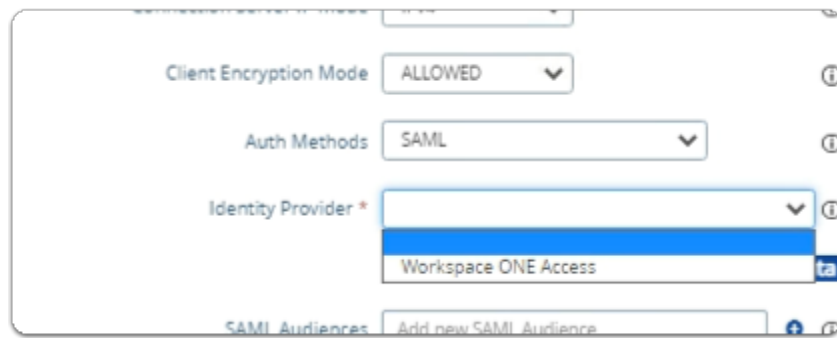
9. In the **Horizon Settings** window

- **scroll** down to the bottom
 - next to **More**
 - select the **expand** icon



10. In the **Horizon Settings** window

- next to **Auth Methods**
 - from the **dropdown**
 - select **SAML**



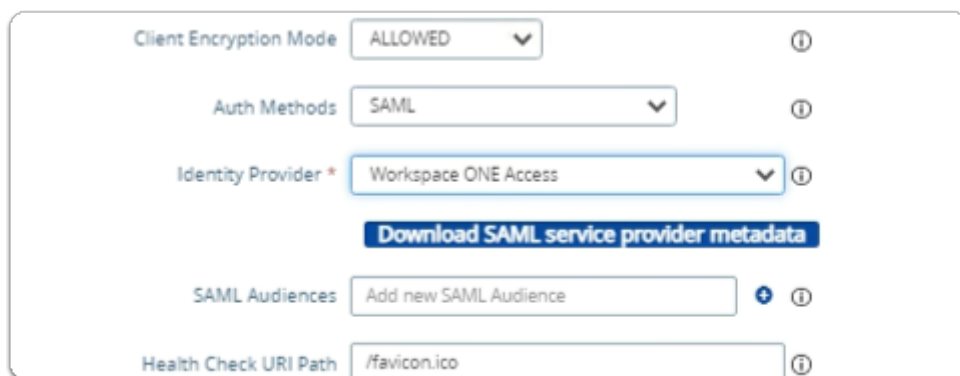
Client Encryption Mode: ALLOWED

Auth Methods: SAML

Identity Provider *: Workspace ONE Access

SAML Audiences: Add new SAML Audience

11. In the **Horizon Settings** window
 - below **Auth Methods**
 - next to **Identity Provider***
 - from the **dropdown**
 - select **Workspace ONE Access**



Client Encryption Mode: ALLOWED

Auth Methods: SAML

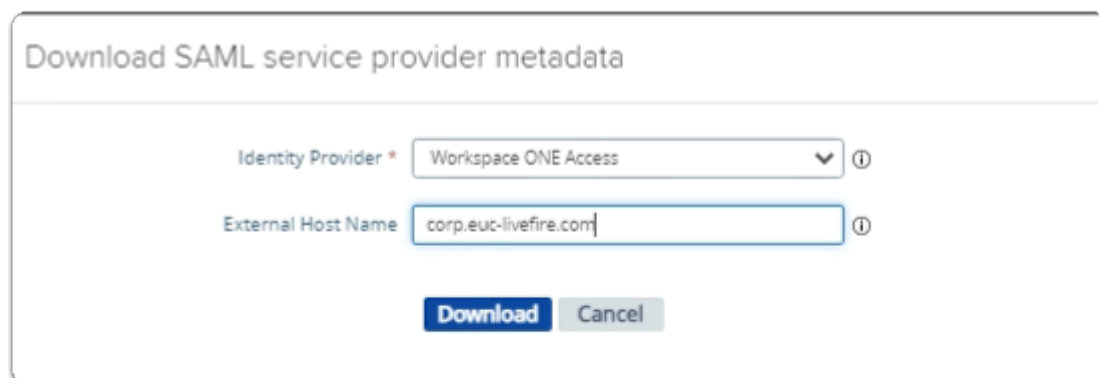
Identity Provider *: Workspace ONE Access

Download SAML service provider metadata

SAML Audiences: Add new SAML Audience

Health Check URI Path: /favicon.ico

12. In the **Horizon Settings** window
 - below **Identity Provider***
 - select **Download SAML service provider metadata**



Download SAML service provider metadata

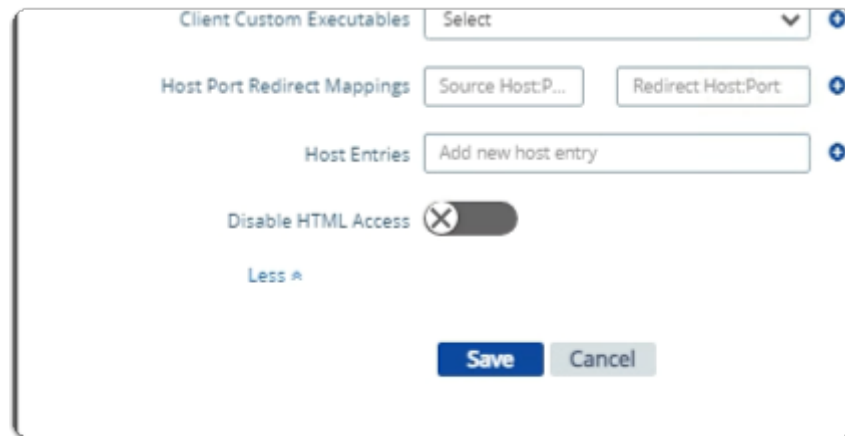
Identity Provider *: Workspace ONE Access

External Host Name: corp.euc-liveware.com

Download Cancel

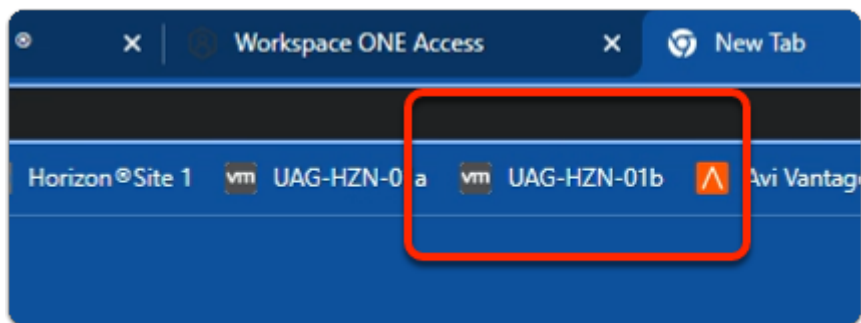
13. In the **Download SAML service provider metadata** window
 - next to **External Host Name**

- enter corp.euc-livewire.com
- select **Download**

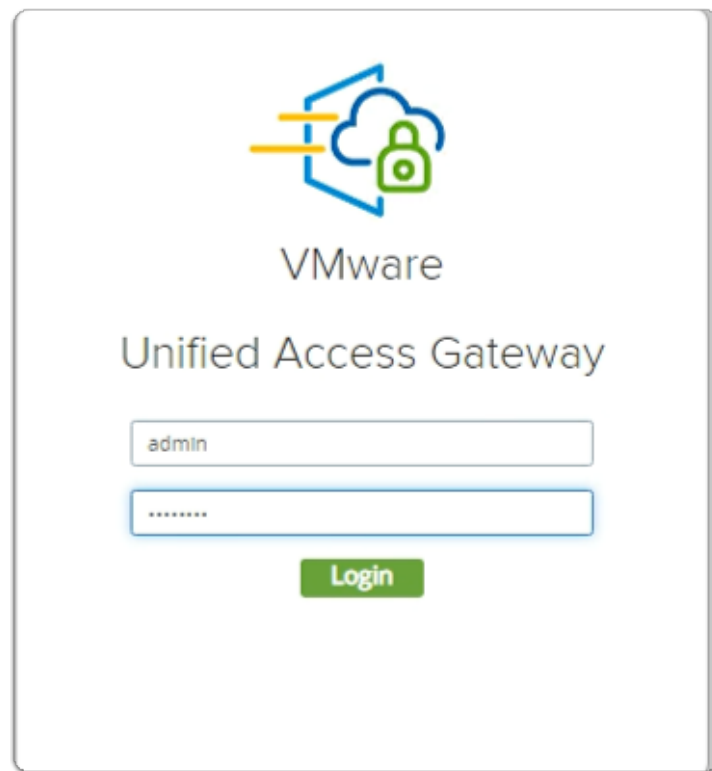


14. In the **Horizon Settings** window
 - **scroll down** to the bottom of the window
 - select **Save**

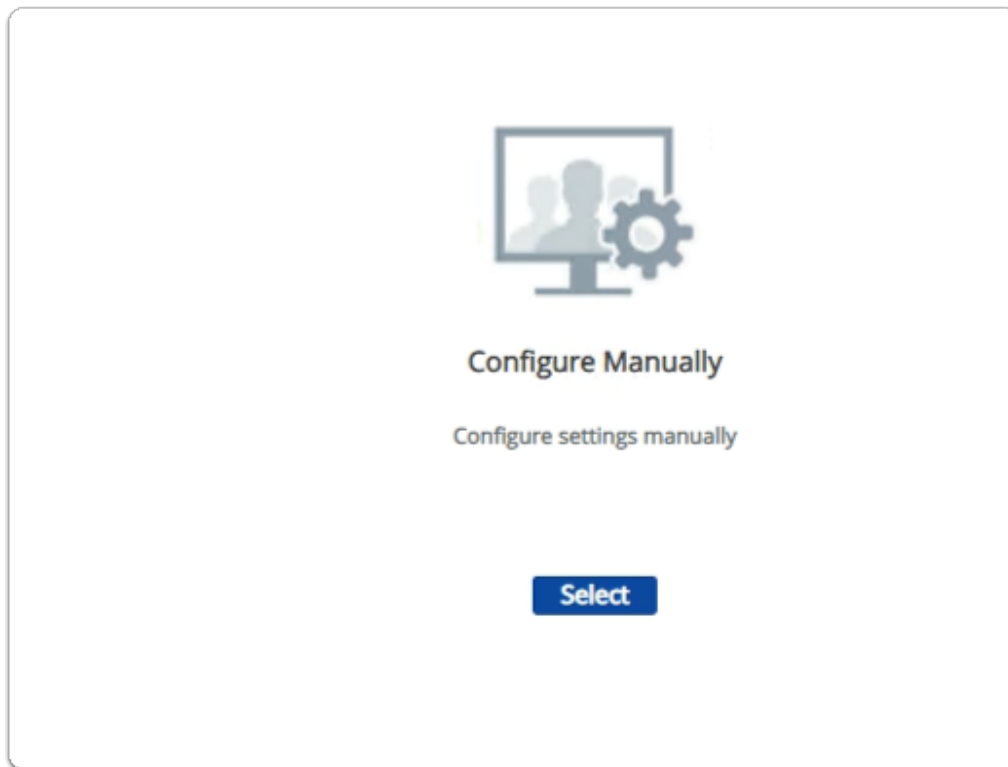
Step 3. Enabling SAML Federation on Site 1 , UAG-HZN-01b



1. On your **Site 1 Browser** profile
 - In the **Favourites bar**
 - select the **UAG-HZN-01B** shortcut



2. In the **VMware Unified Access Gateway** login
 - in the **Username** area
 - enter **admin**
 - in the **Password** area
 - enter **VMware1!**
 - select **Login**



3. In the **VMware Unified Access Gateway** admin console
 - below **Configure Manually**
 - click **Select**



4. In the **VMware Unified Access Gateway** admin console
 - **scroll down** to **Identity Bridging Settings**
 - to the right of **Upload Identity Provider Metadata**
 - select the **GEAR** icon

Upload Identity Provider Metadata

Entity ID ⓘ

+ IDP Metadata Select ⓘ

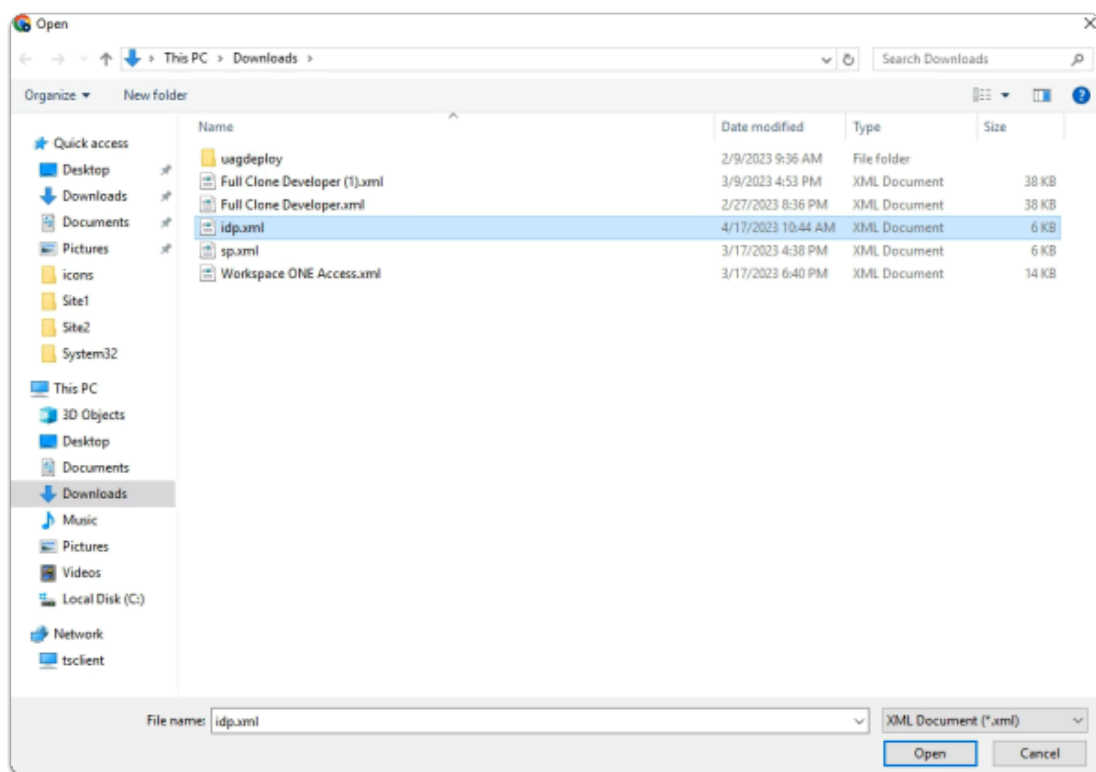
Encryption Certificate Type None ⓘ

Always force SAML auth ☐ ⓘ

Save **Cancel**

5. In the **Upload Identity Provider Metadata** window

- next to **Entity ID**
 - enter **Workspace ONE Access**
- next to **IDP Metadata**
 - click **Select**



6. In the **File Explorer - Open** window

- **Quick Access > Downloads** folder
 - (this should be the default)
 - select **idp.xml**
- in the bottom right corner
 - select **Open**

Upload Identity Provider Metadata

Entity ID ⓘ

* IDP Metadata [Change](#) ⓘ

Encryption Certificate Type ⓘ




Always force SAML auth ☒ ⓘ

Save **Cancel**

7. In the **Upload Identity Provider Metadata** window

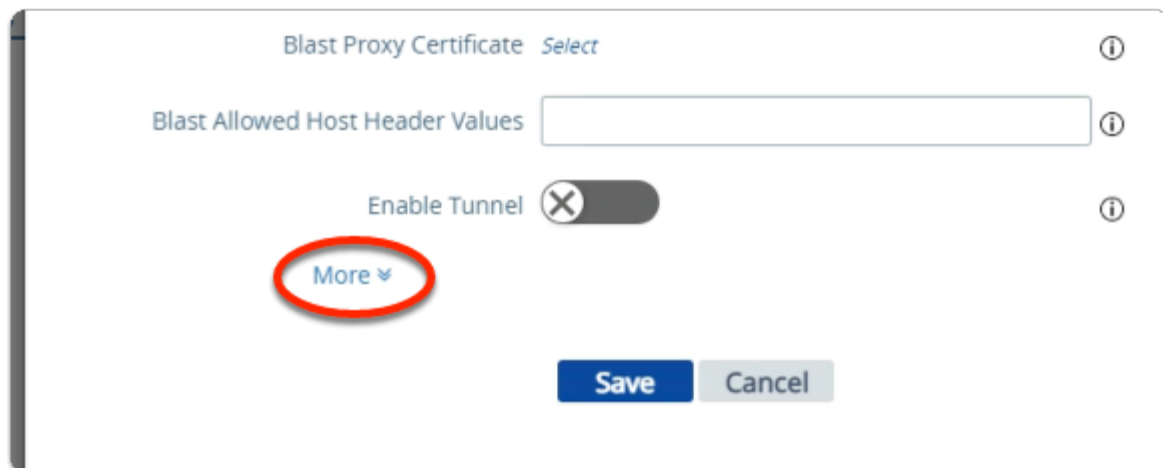
- next to **Always force SAML auth**
 - switch the **Toggle** from **OFF** to **ON**
 - select **Save**
- **scroll** back up to the top of UAG admin console

Edge Service Settings ☒ [Refresh](#) Active Sessions: 0

<input checked="" type="radio"/>	Horizon Settings	
<input type="radio"/>	Reverse Proxy Settings	
<input type="radio"/>	Tunnel Settings	

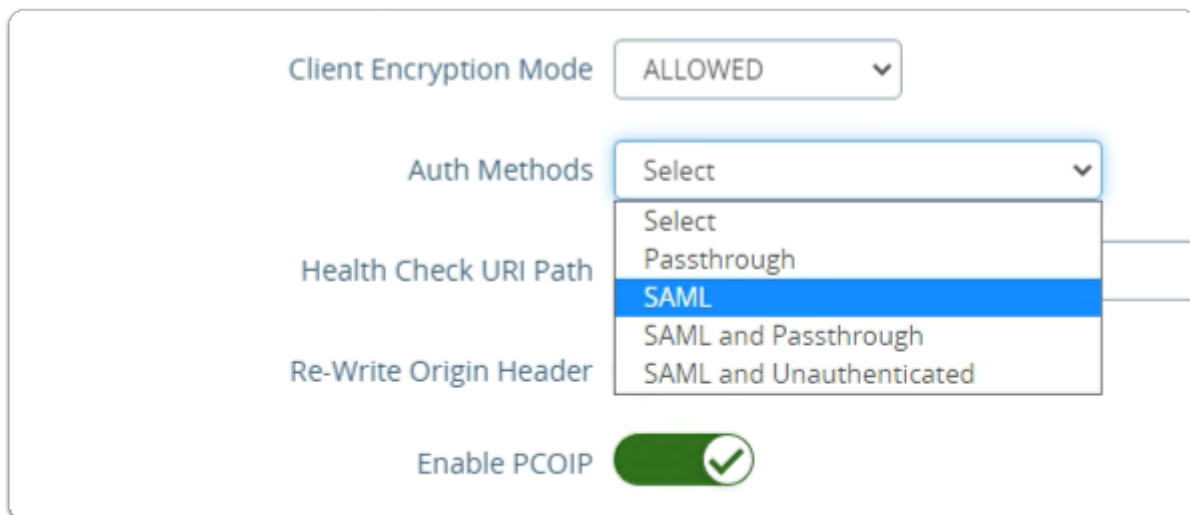
8. In the **VMware Unified Access Gateway** admin console

- In the **General Settings** area
 - next to **Edge Service Settings**
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon



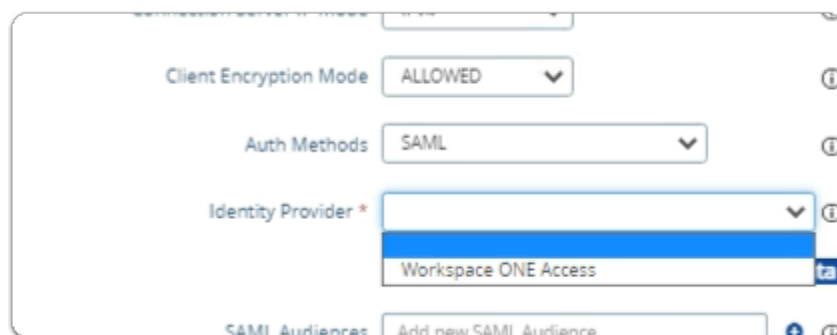
9. In the **Horizon Settings** window

- **scroll** down to the bottom
- next to **More**
 - select the **expand** icon

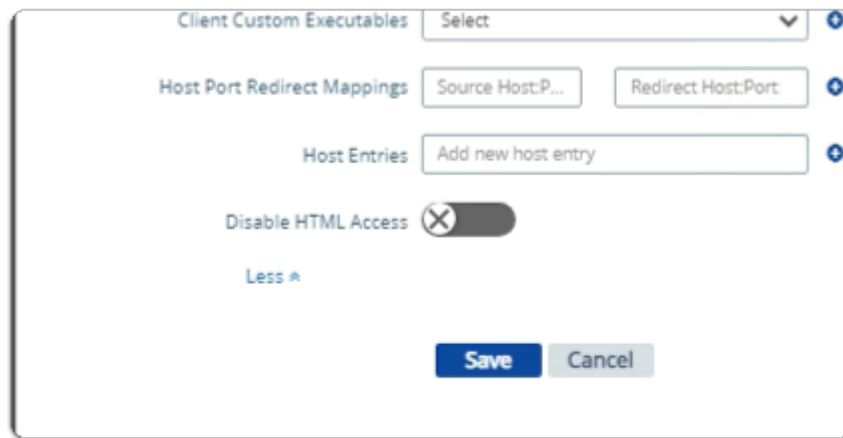


10. In the **Horizon Settings** window

- next to **Auth Methods**
 - from the **dropdown**
 - select **SAML**

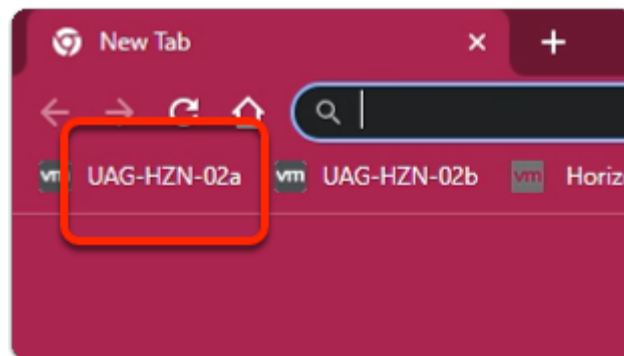


11. In the **Horizon Settings** window
 - below **Auth Methods**
 - next to **Identity Provider***
 - from the **dropdown**
 - select **Workspace ONE Access**

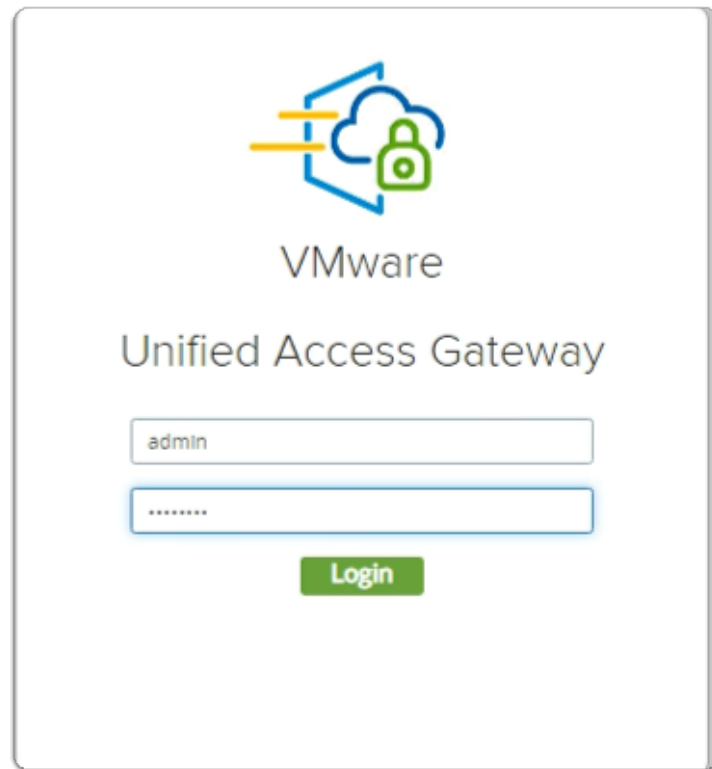


12. In the **Horizon Settings** window
 - **scroll down** to the bottom of the window
 - select **Save**

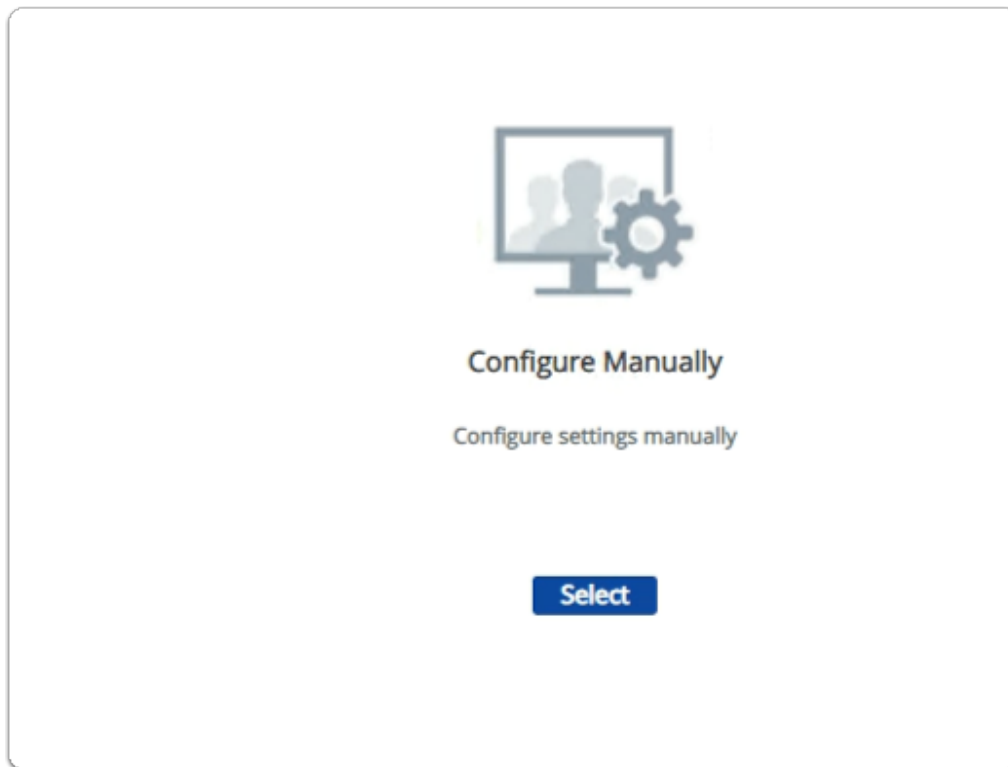
Step 4. Enabling SAML Federation on Site 2 , UAG-HZN-02a



1. On your ControlCenter server
 - switch to your **Site 2 Browser** profile
 - In the **Favourites bar**
 - select the **UAG-HZN-02a** shortcut



2. In the **VMware Unified Access Gateway** login
 - in the **Username** area
 - enter **admin**
 - in the **Password** area
 - enter **VMware1!**
 - select **Login**



3. In the **VMware Unified Access Gateway** admin console
 - below **Configure Manually**
 - click **Select**



4. In the **VMware Unified Access Gateway** admin console
 - **scroll down** to **Identity Bridging Settings**
 - to the right of **Upload Identity Provider Metadata**
 - select the **GEAR** icon

Upload Identity Provider Metadata

Entity ID ⓘ

+ IDP Metadata Select ⓘ

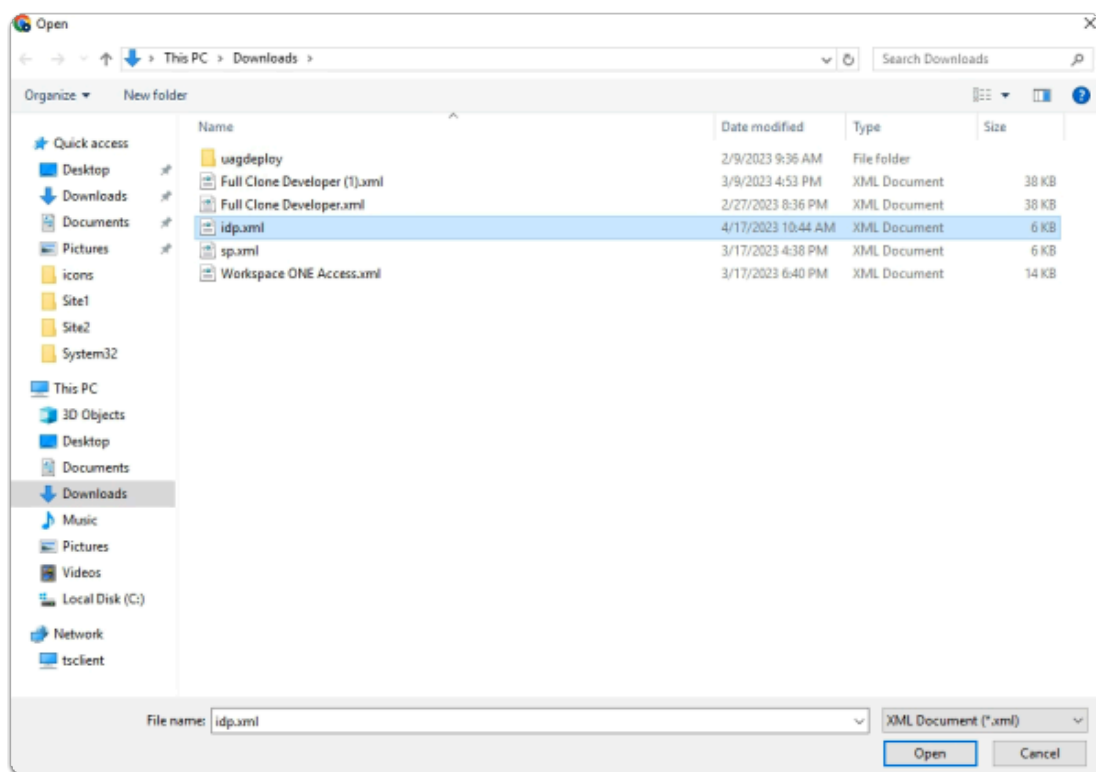
Encryption Certificate Type None ⓘ

Always force SAML auth ☐ ⓘ

Save **Cancel**

5. In the **Upload Identity Provider Metadata** window

- next to **Entity ID**
 - enter **Workspace ONE Access**
- next to **IDP Metadata**
 - click **Select**



6. In the **File Explorer - Open** window

- **Quick Access > Downloads** folder
 - (this should be the default)
 - select **idp.xml**
- in the bottom right corner
 - select **Open**

Upload Identity Provider Metadata

Entity ID ⓘ

* IDP Metadata [Change](#) ⓘ

Encryption Certificate Type ⓘ




Always force SAML auth ☒ ⓘ

Save **Cancel**

7. In the **Upload Identity Provider Metadata** window

- next to **Always force SAML auth**
 - switch the **Toggle** from **OFF** to **ON**
 - select **Save**
- **scroll** back up to the top of UAG admin console

Edge Service Settings ☒ [Refresh](#) Active Sessions: 0

<input checked="" type="radio"/>	Horizon Settings	
<input type="radio"/>	Reverse Proxy Settings	
<input type="radio"/>	Tunnel Settings	

8. In the **VMware Unified Access Gateway** admin console

- In the **General Settings** area
 - next to **Edge Service Settings**
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon

Blast Proxy Certificate *Select* ⓘ

Blast Allowed Host Header Values ⓘ

Enable Tunnel ☒ ⓘ

Tunnel External URL ⓘ

Tunnel Proxy Certificate *Select* ⓘ

More ⌵

Save **Cancel**

9. In the **Horizon Settings** window
- **scroll** down to the bottom
 - next to **More**
 - select the **expand** icon

Client Encryption Mode ⌵ ⓘ

Auth Methods ⌵ ⓘ

Health Check URI Path ⓘ

Re-Write Origin Header ⓘ

Enable PCOIP ☒ ⓘ

10. In the **Horizon Settings** window
- next to **Auth Methods**
 - from the **dropdown**
 - select **SAML**

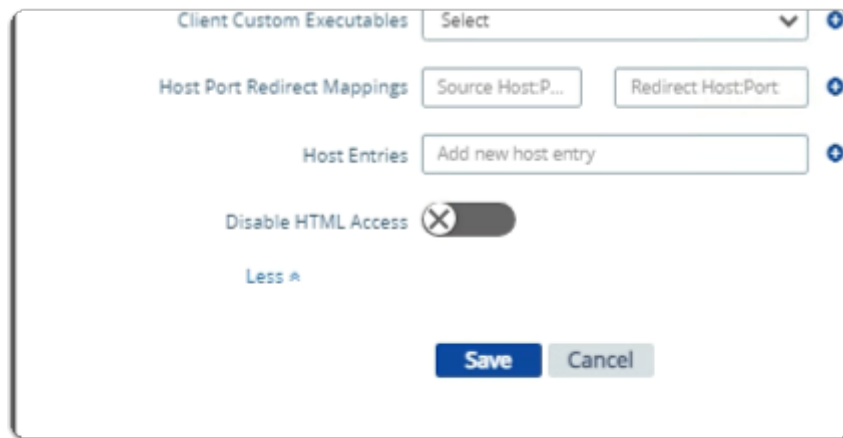
Client Encryption Mode ⌵ ⓘ

Auth Methods ⓘ

Identity Provider * ⓘ

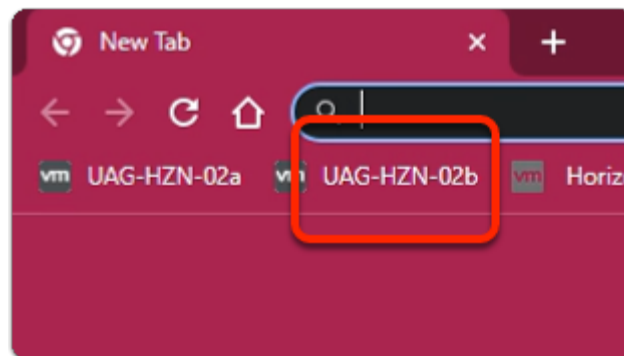
SAML Audiences ⓘ

11. In the **Horizon Settings** window
 - below **Auth Methods**
 - next to **Identity Provider***
 - from the **dropdown**
 - select **Workspace ONE Access**

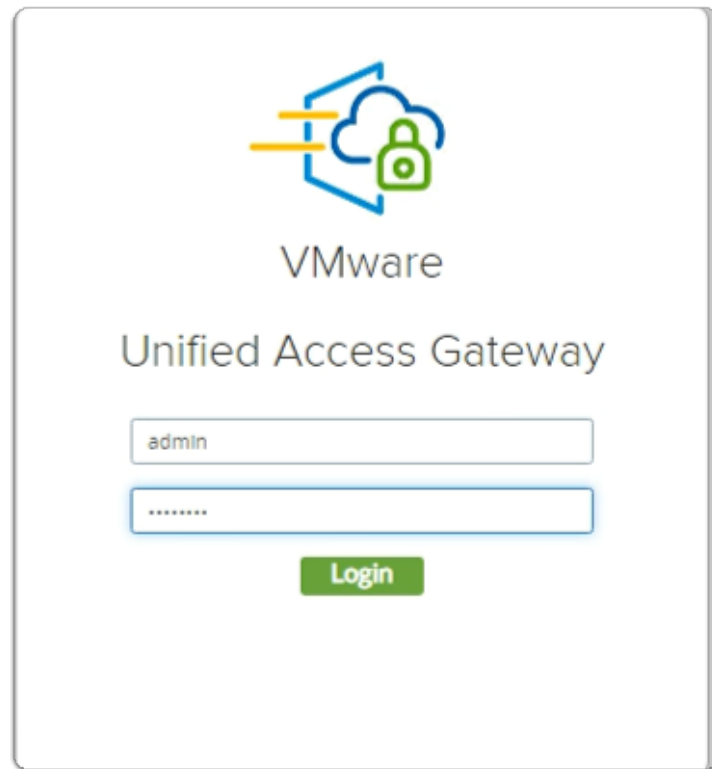


12. In the **Horizon Settings** window
 - **scroll down** to the bottom of the window
 - select **Save**

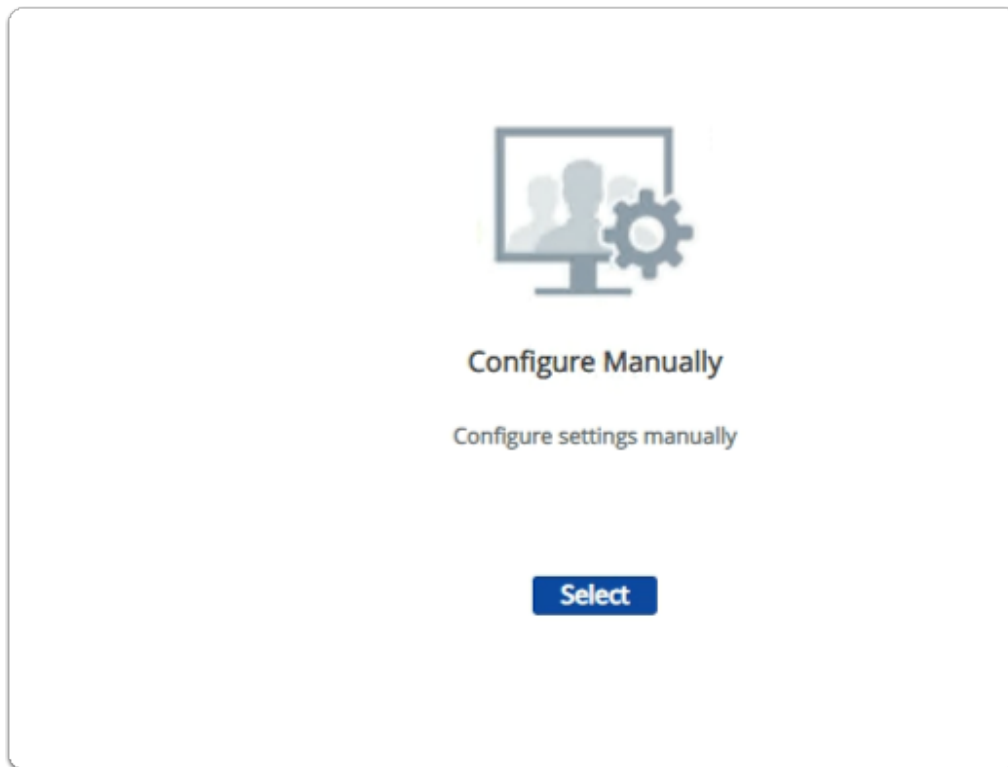
Step 5. Enabling SAML Federation on Site 2 , UAG-HZN-02b



1. On your ControlCenter server
 - on your **Site 2 Browser** profile
 - In the **Favourites bar**
 - select the **UAG-HZN-02b** shortcut



2. In the **VMware Unified Access Gateway** login
 - in the **Username** area
 - enter **admin**
 - in the **Password** area
 - enter **VMware1!**
 - select **Login**



3. In the **VMware Unified Access Gateway** admin console
 - below **Configure Manually**
 - click **Select**



4. In the **VMware Unified Access Gateway** admin console
 - **scroll down** to **Identity Bridging Settings**
 - to the right of **Upload Identity Provider Metadata**
 - select the **GEAR** icon

Upload Identity Provider Metadata

Entity ID ⓘ

+ IDP Metadata Select ⓘ

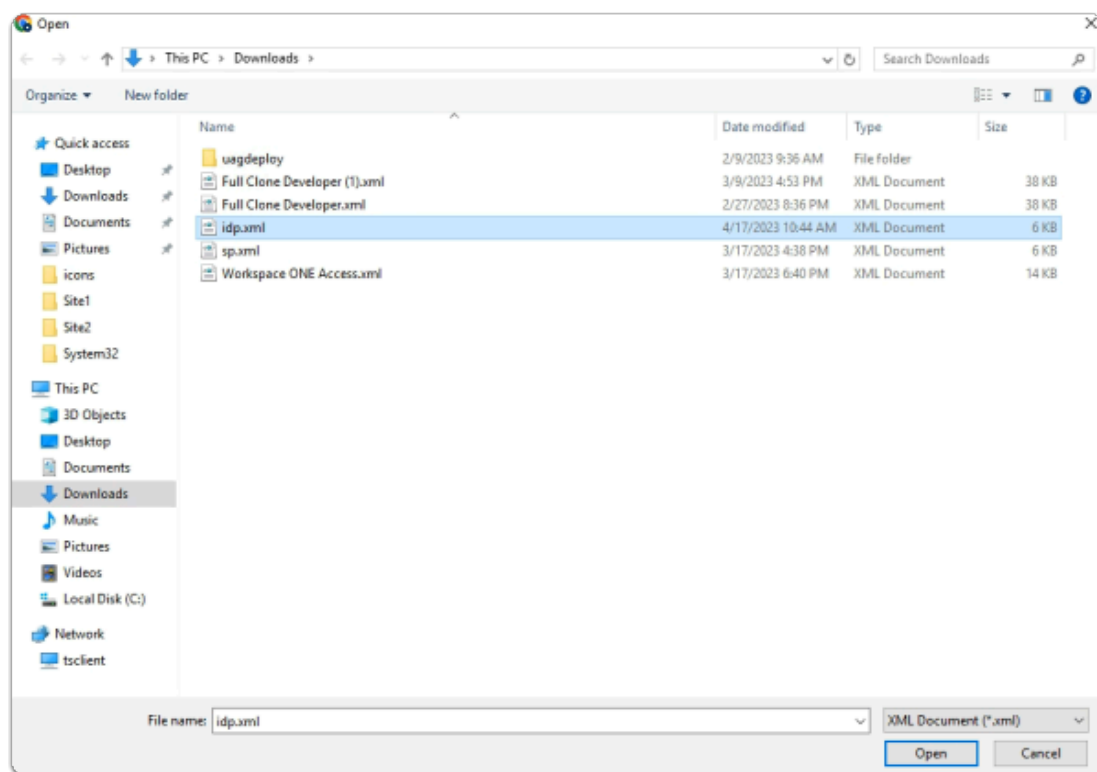
Encryption Certificate Type None ⓘ

Always force SAML auth ☐ ⓘ

Save **Cancel**

5. In the **Upload Identity Provider Metadata** window

- next to **Entity ID**
 - enter **Workspace ONE Access**
- next to **IDP Metadata**
 - click **Select**



6. In the **File Explorer - Open** window

- **Quick Access > Downloads** folder
 - (this should be the default)
 - select **idp.xml**
- in the bottom right corner
 - select **Open**

Upload Identity Provider Metadata

Entity ID ⓘ

* IDP Metadata [Change](#) ⓘ

Encryption Certificate Type ⓘ




Always force SAML auth ☒ ⓘ

Save **Cancel**

7. In the **Upload Identity Provider Metadata** window

- next to **Always force SAML auth**
 - switch the **Toggle** from **OFF** to **ON**
 - select **Save**
- **scroll** back up to the top of UAG admin console

Edge Service Settings ☒ [Refresh](#) Active Sessions: 0

<input checked="" type="radio"/>	>	Horizon Settings	
<input type="radio"/>		Reverse Proxy Settings	
<input type="radio"/>		Tunnel Settings	

8. In the **VMware Unified Access Gateway** admin console

- In the **General Settings** area
 - next to **Edge Service Settings**
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon

Blast Proxy Certificate Select ⓘ

Blast Allowed Host Header Values ⓘ

Enable Tunnel ☒ ⓘ

Tunnel External URL ⓘ

Tunnel Proxy Certificate Select ⓘ

More ▾

Save **Cancel**

9. In the **Horizon Settings** window
 - **scroll** down to the bottom
 - next to **More**
 - select the **expand** icon

Client Encryption Mode ▾

Auth Methods ▾

Health Check URI Path

Re-Write Origin Header

Enable PCOIP ☒

Select
Passthrough
SAML
SAML and Passthrough
SAML and Unauthenticated

10. In the **Horizon Settings** window
 - next to **Auth Methods**
 - from the **dropdown**
 - select **SAML**

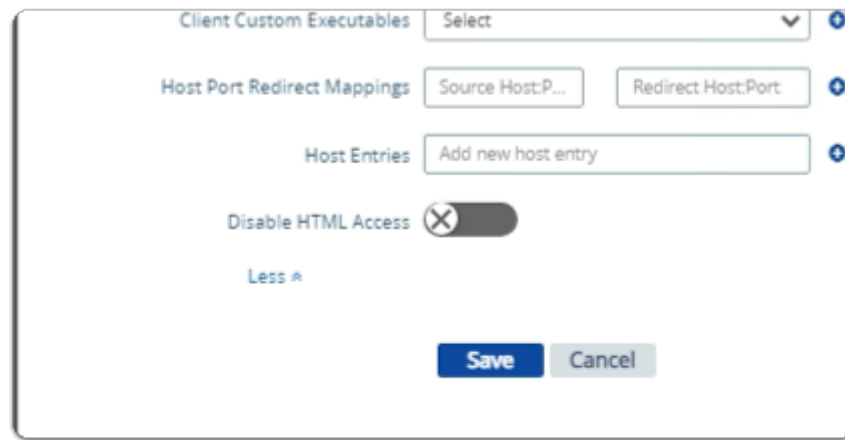
Client Encryption Mode ▾ ⓘ

Auth Methods ▾ ⓘ

Identity Provider * ▾ ⓘ

SAML Audiences ⓘ

11. In the **Horizon Settings** window
 - below **Auth Methods**
 - next to **Identity Provider***
 - from the **dropdown**
 - select **Workspace ONE Access**

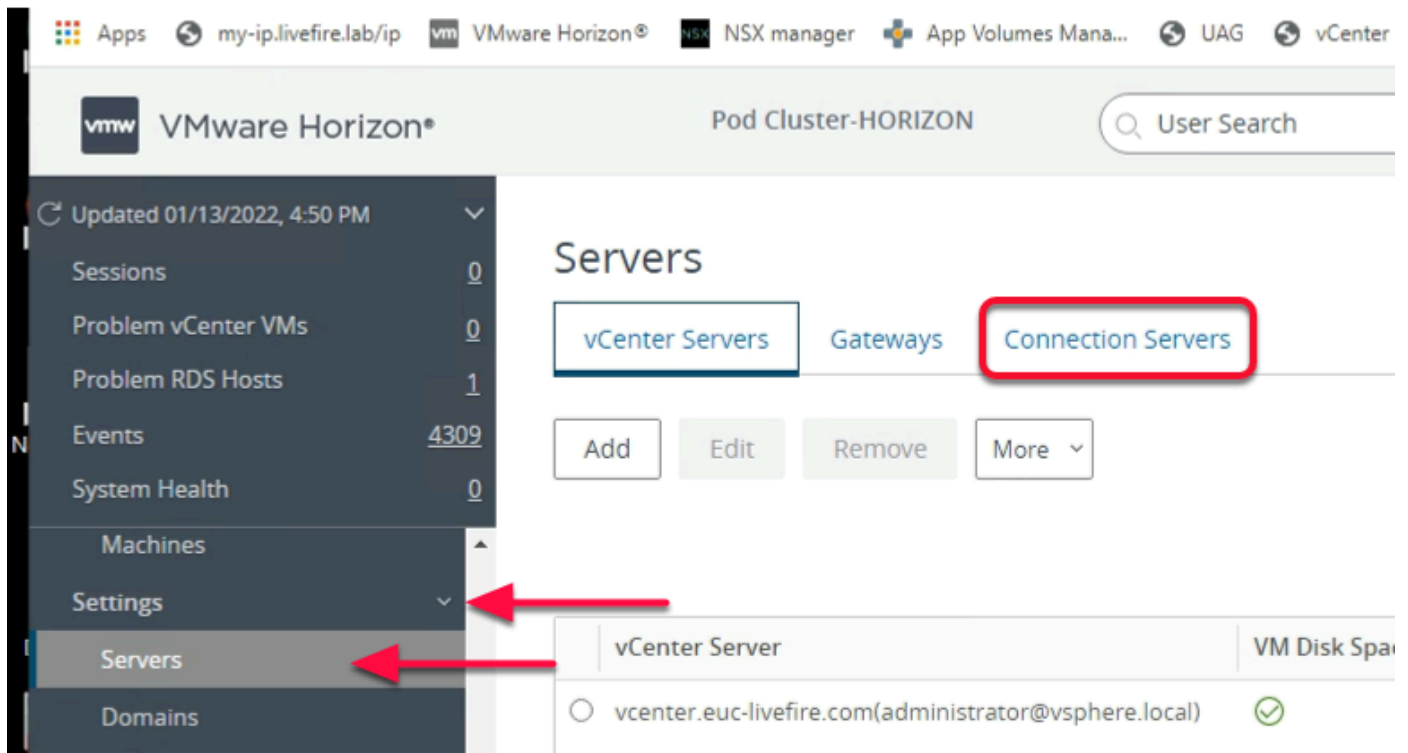


12. In the **Horizon Settings** window
 - **scroll down** to the bottom of the window
 - select **Save**

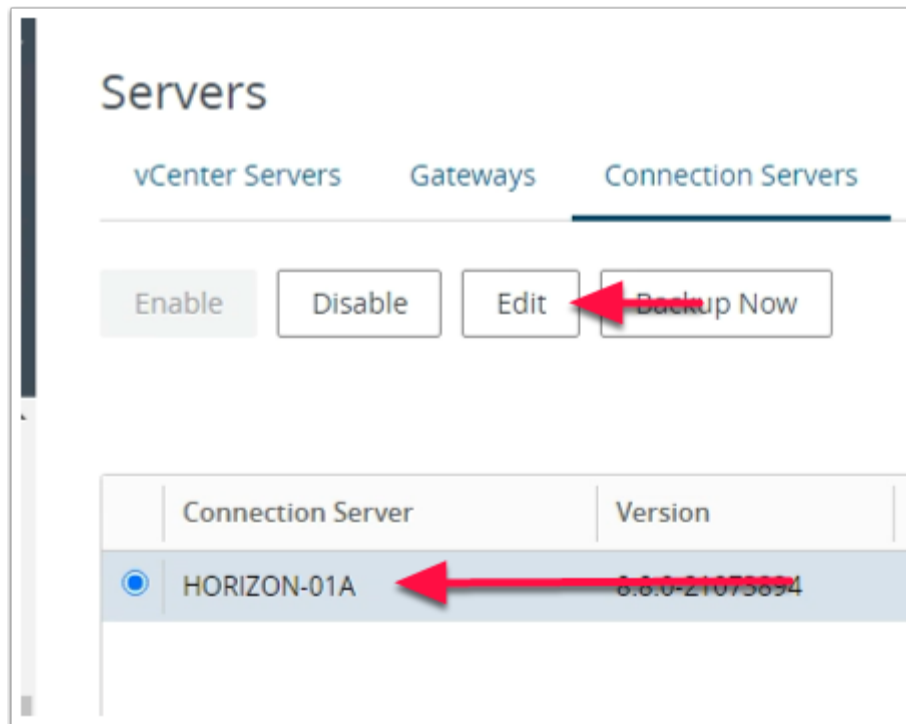
Part 2. Configuring the SAML Federation for Horizon

For TrueSSO to work the Horizon SAML authenticator is required.
We configure this on both Site 1 and Site 2

Step 1. Configuring the SAML federation with VMware Horizon on Site 1

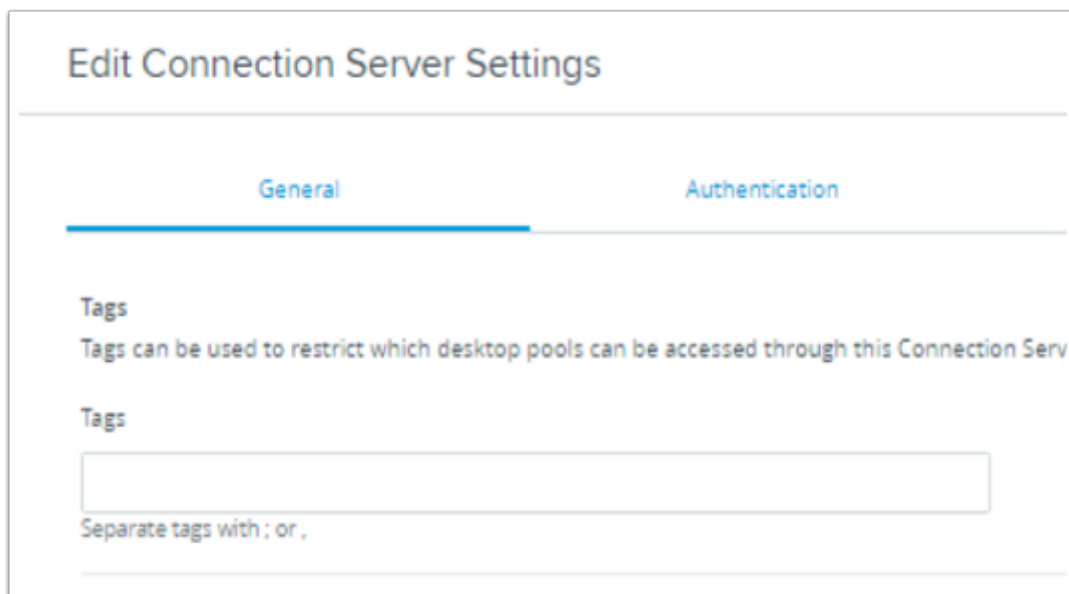


1. On your ControlCenter server
 - **Site 1** Browser
 - In the Horizon Admin Console
 - In the **Inventory**
 - expand **Settings**,
 - select **Servers**
 - In the **Servers** area
 - select the **Connection Servers** tab



2. Under **Servers**

- Select the **radio button** to next **HORIZON-01a**
- Select **Edit**



3. On the **Edit Connection Server Settings** page

- Select the **Authentication tab**.

Edit Connection Server Settings

General Authentication

Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):

Disabled

Disabled

Allowed

Required

Manage SAML Authenticators

General

Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):

Allowed

SAML Authenticator

No Enabled Authenticator configured

Manage SAML Authenticators

Create at least one SAML Authenticator and enable it, for authentication to be successful.

☐ Enable Workspace ONE mode ⓘ

4. On the **Authentication** tab
 - below **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):**
 - On the **Drop down Arrow**
 - Select **Allowed**,
 - Select the **Manage SAML Authenticators** box

Manage SAML Authenticators

SAML Authenticators configured in this Horizon environment:

Add Edit Remove

Name	Description	Status
No records available.		

5. On the **Manage SAML Authenticators** box

- Select **Add**

Add SAML 2.0 Authenticator

* Type ☒ Dynamic ☐ Static

* Label
Workspace ONE Access

Description

* Metadata URL
https://aw-livefirewwkorn.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml

Administration URL

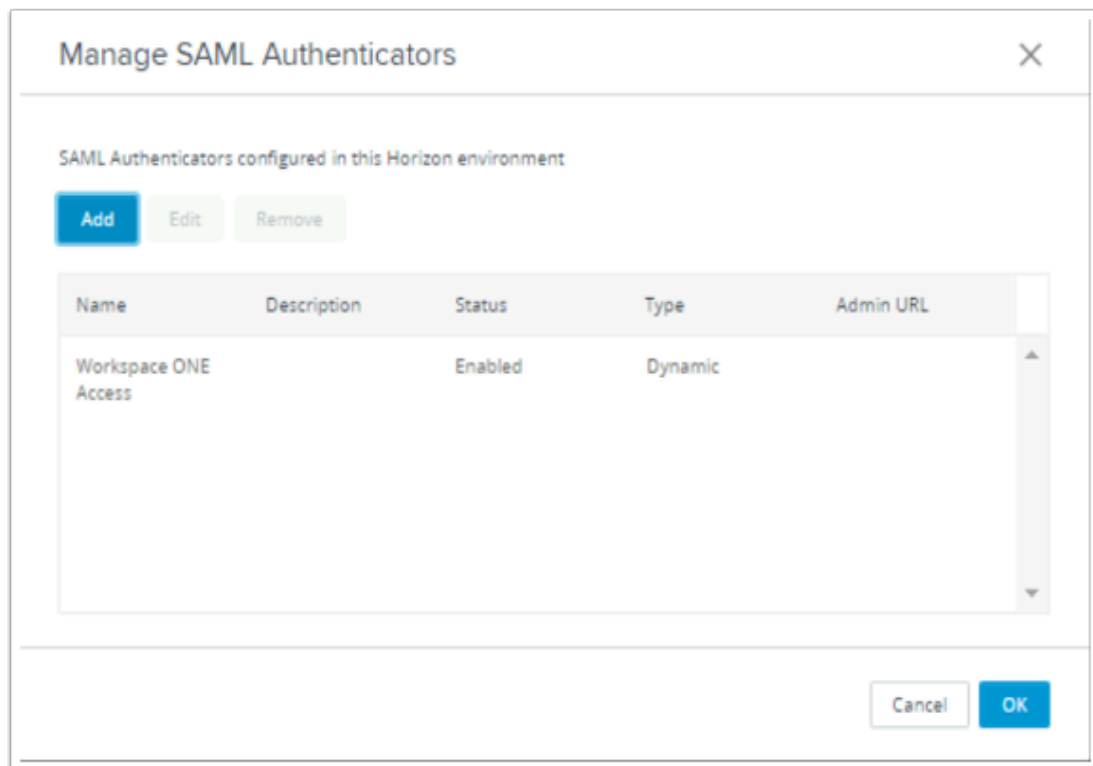
* TrueSSO Trigger Mode ⓘ
Enabled

☒ Enabled for Connection Server

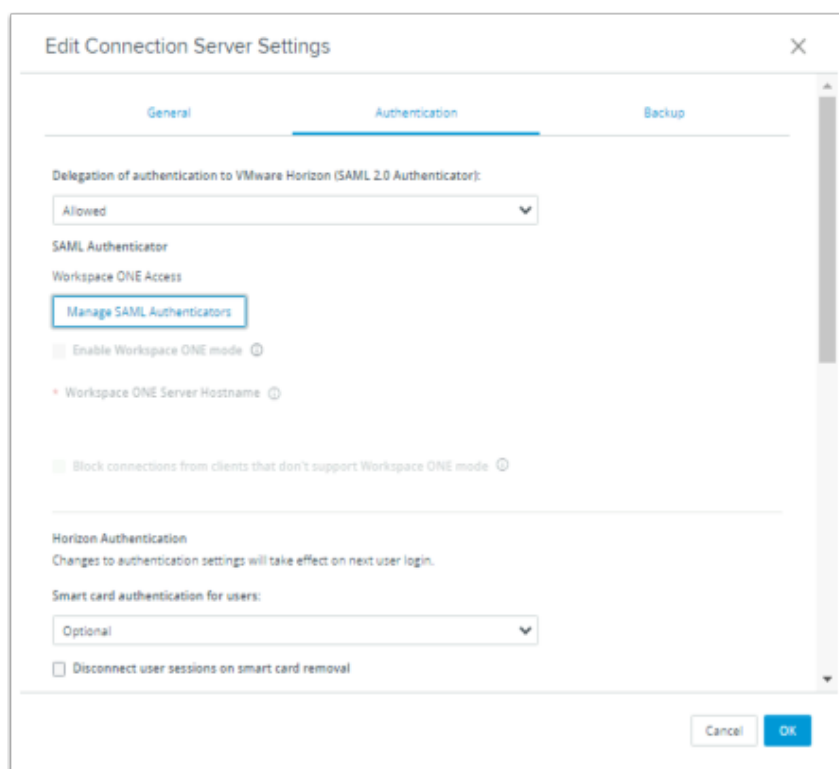
Cancel OK

6. In the **Add SAML 2.0 Authenticator** window.

- Ensure **Dynamic** radio button is selected,
- Enter the following:
 - Under **Label**:
 - type **Workspace ONE Access**
 - **Under Metadata URL** : enter
 - https://**YOUR CUSTOM Access URL**/SAAS/API/1.0/GET/metadata/idp.xml
 - e.g. https://aw-euclivefirefran.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml
 - Under * **TrueSSO Trigger Mode**
 - from the dropdown
 - select **Enabled**
- Select **OK**

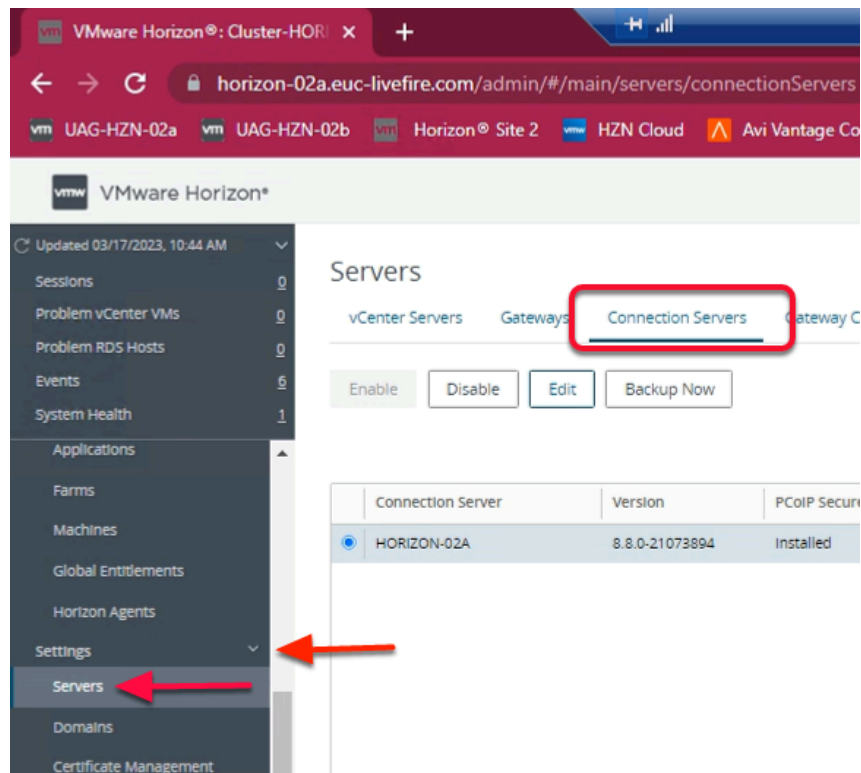


7. In the **Manage SAML Authenticators** window
- Select **OK** to close

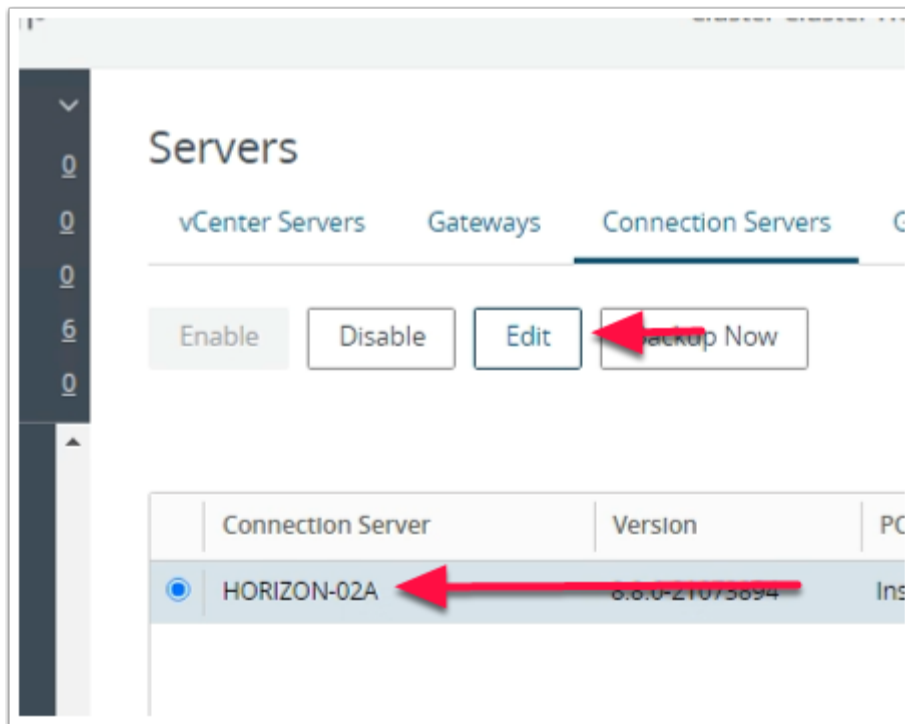


8. In the **Connection Server Settings**
- Select **OK**

Step 2. Configuring the SAML federation with VMware Horizon on Site 2

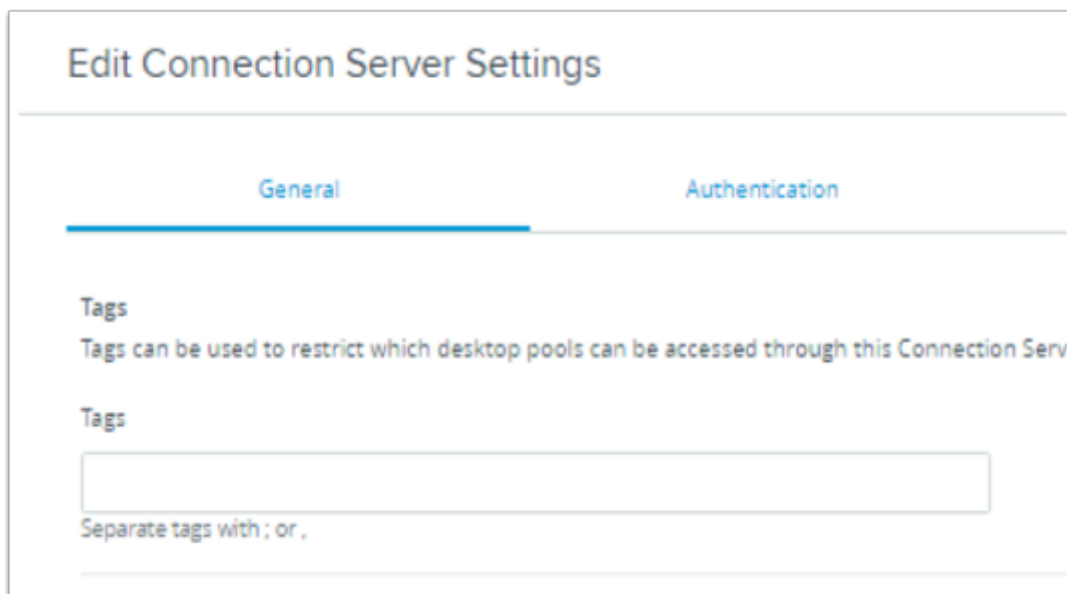


1. On your ControlCenter server
 - **Site 2 Browser**
 - In the **Horizon Admin Console**
 - Inventory pane
 - expand **Settings**,
 - select **Servers**
 - In the middle pane
 - select the **Connection Servers** tab



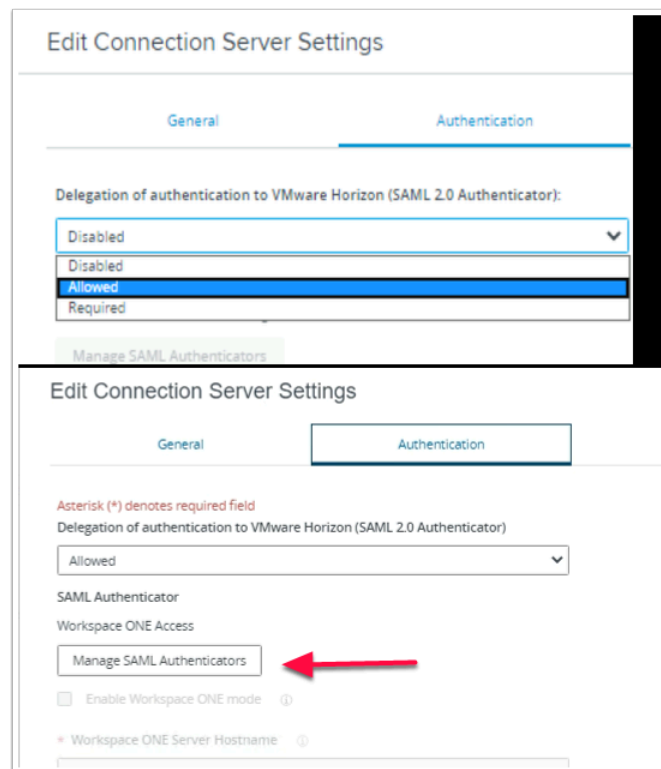
2. Under **Servers**

- select the **radio button** to next **HORIZON-02a**
- select **Edit**

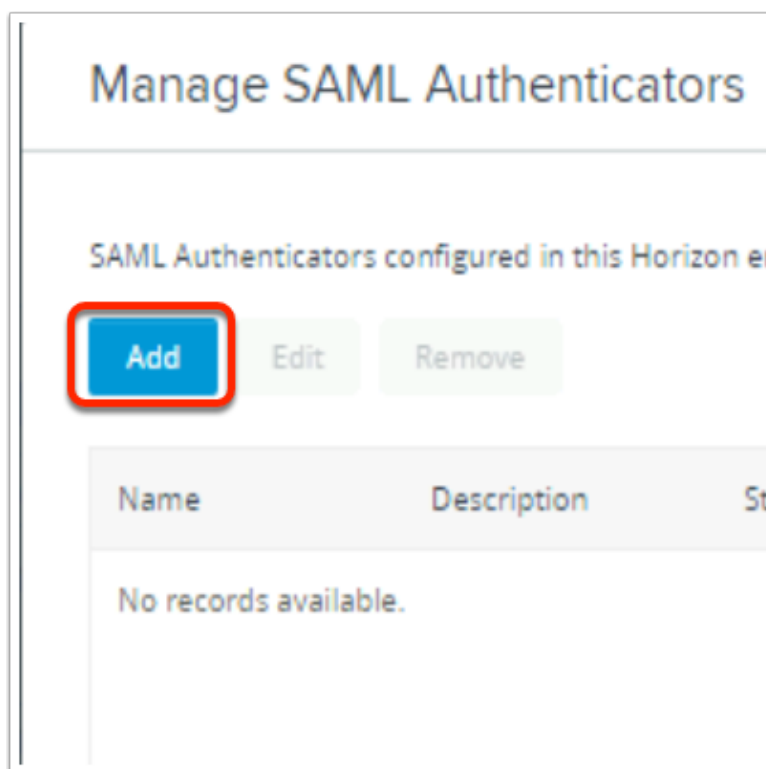


3. On the **Edit Connection Server Settings** page

- select the **Authentication tab**.



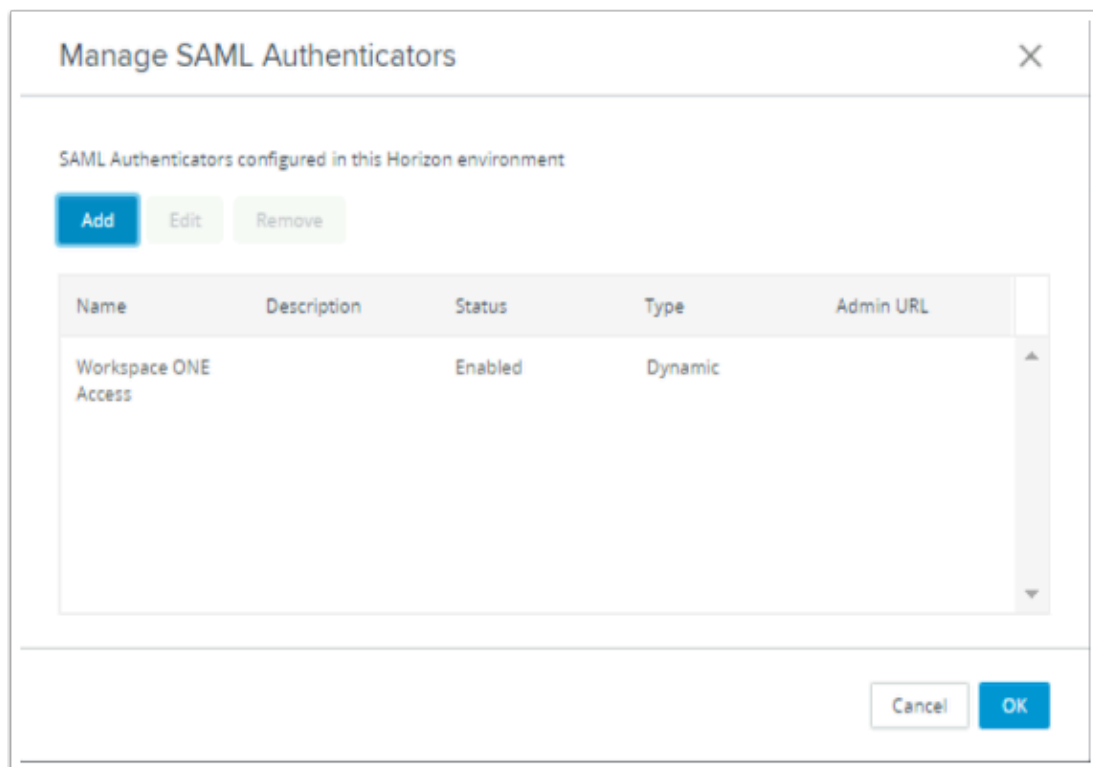
4. In the **Edit Connection Server Settings** window
 - on the **Authentication** tab,
 - under **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)**:
 - from the **Drop down Arrow**
 - select **Allowed**,
 - below **SAML Authenticator**
 - select the **Manage SAML Authenticators** box



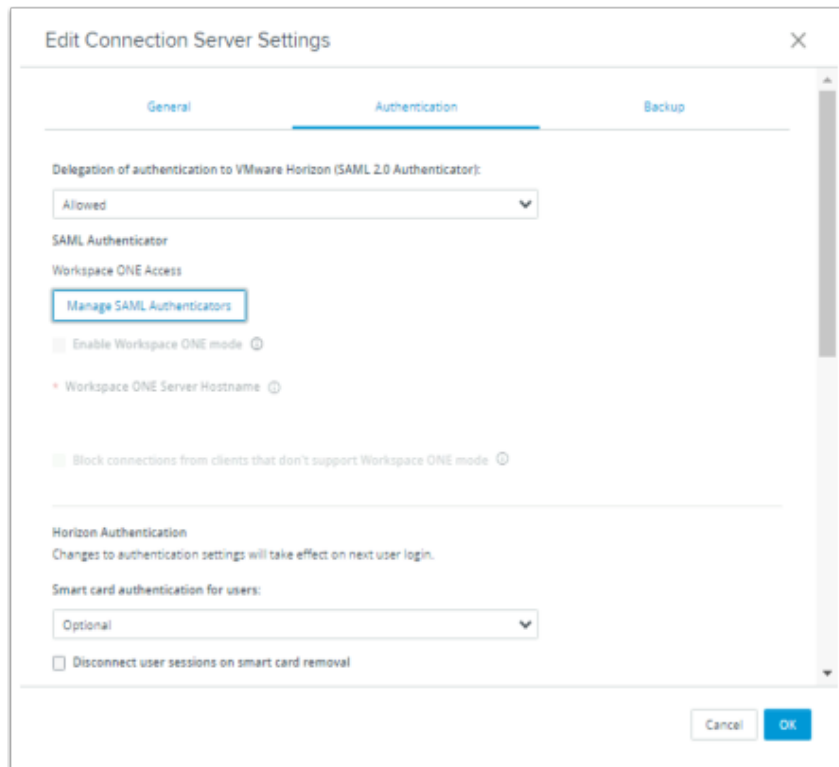
5. On the **Manage SAML Authenticators** box
 - Select **Add**

6. In the **Add SAML 2.0 Authenticator** window.
 - ensure **Dynamic** radio button is selected,
 - enter the following:

- under **Label:**
 - type **Workspace ONE Access**
- **Under Metadata URL :** enter
 - https://YOUR CUSTOM Access URL/SAAS/API/1.0/GET/metadata/idp.xml
 - e.g. https://aw-euclivefirefran.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml
- under *** TrueSSO Trigger Mode**
 - from the dropdown
 - select **Enabled**
- select **OK**



7. In the **Manage SAML Authenticators** window
 - Select **OK** to close



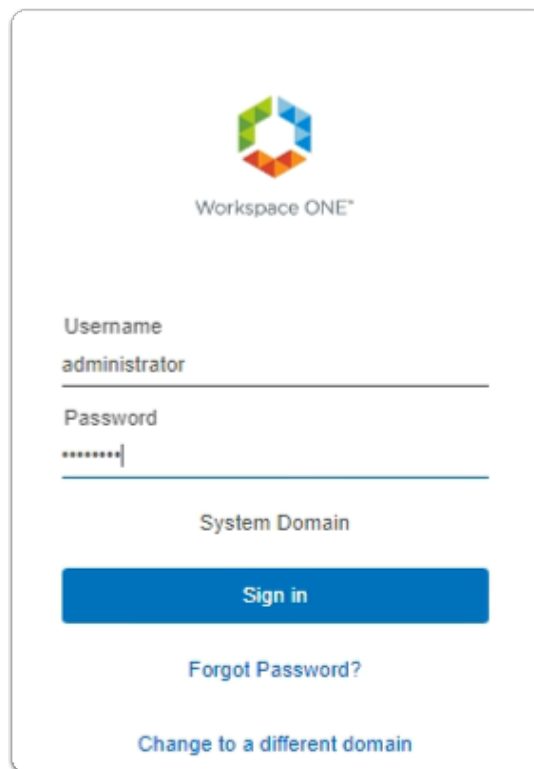
8. In the **Connection Server Settings**

- Select **OK**

Part 3. Configuring Workspace ONE Access for VMware Unified Access as the Service Provider

In this section perform the Workspace ONE Access part of the SAML Federation process with VMware Unified Access Gateway

Configuring Workspace ONE Access for VMware Unified Access as the Service Provider



Workspace ONE™

Username
administrator

Password

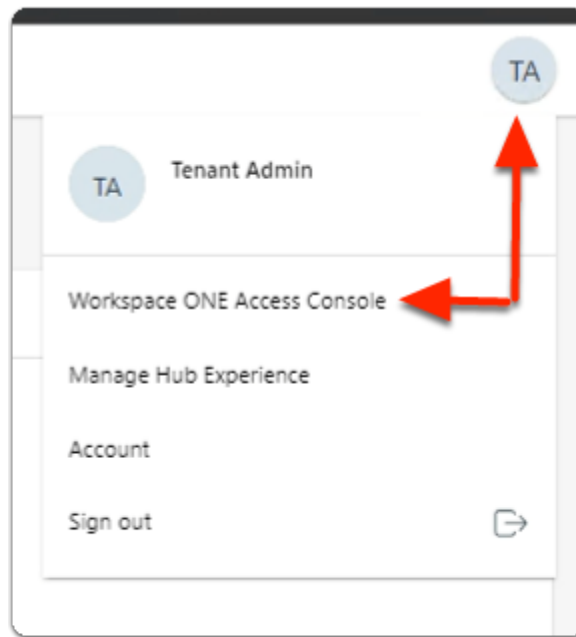
System Domain

Sign in

[Forgot Password?](#)

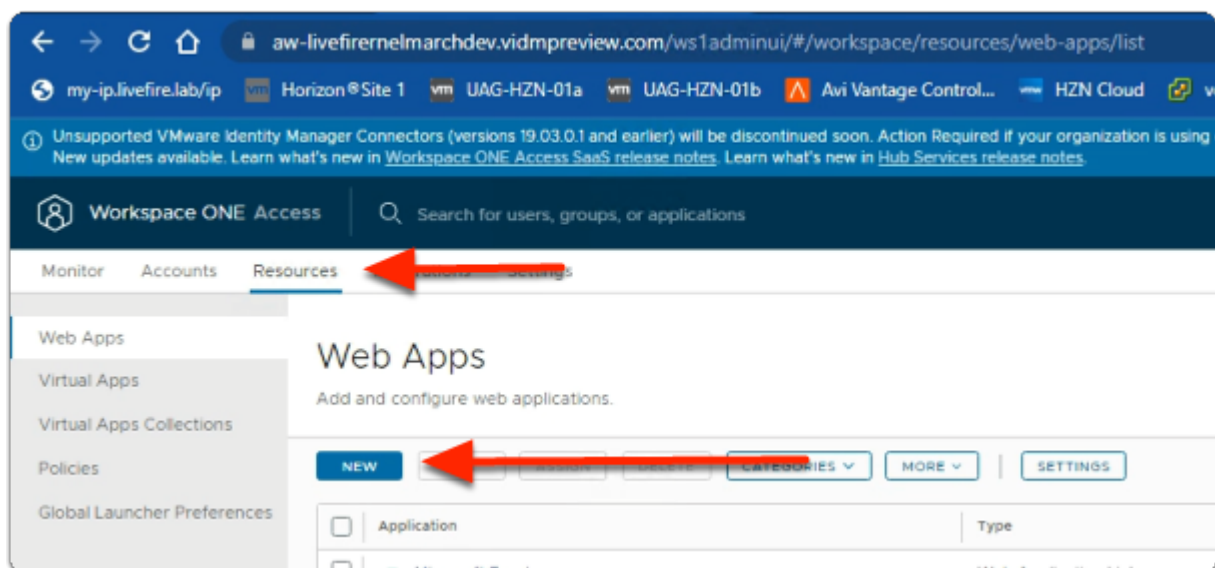
[Change to a different domain](#)

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**

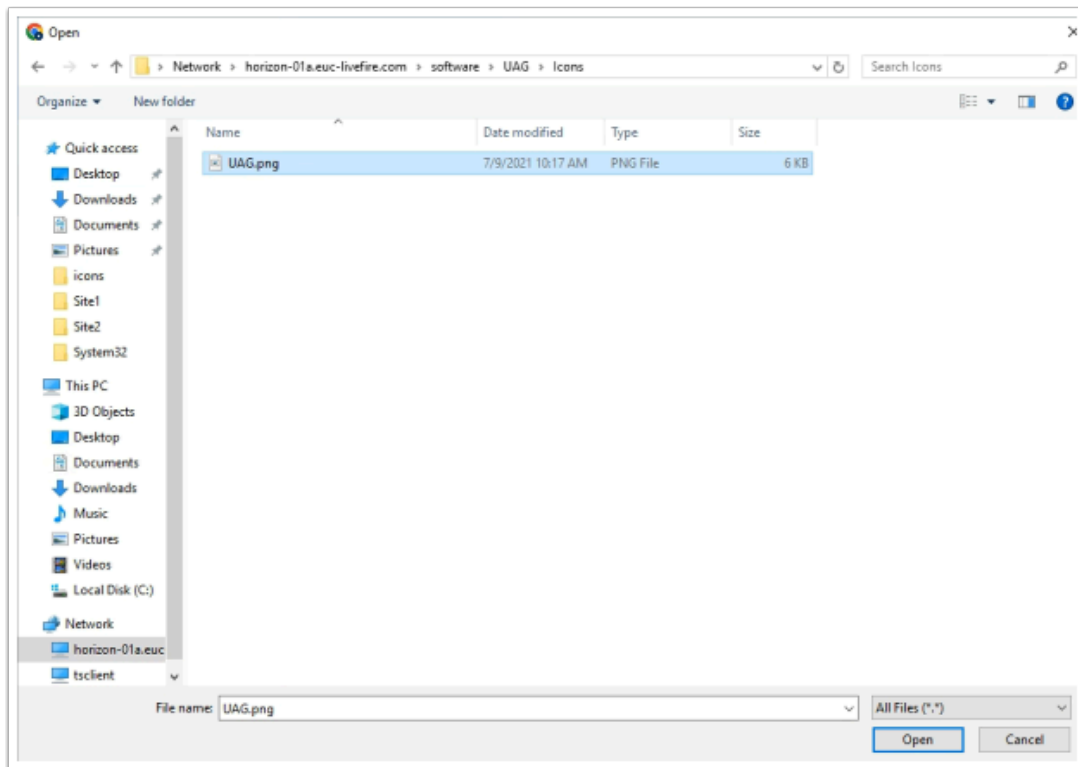


3. In the **Workspace ONE Access Console**

- select **Resources**
- Under **the Resources > WEB Apps** area
 - select **NEW**

The screenshot shows the 'New SaaS Application' window with the 'Definition' tab selected. On the left is a sidebar with steps: 1 Definition, 2 Configuration, 3 Access Policies, and 4 Summary. The main area is divided into two columns. The left column contains a 'CANCEL' button and a 'NEXT' button. The right column contains the 'Definition' form with fields for 'Search', 'Name' (containing 'Unified Access Gateway SAML SP'), 'Description', and 'Icon'. The 'Icon' field has a 'SELECT FILE...' button highlighted with a red rectangle. Below the 'Icon' field is a cloud icon.

4. In the **New SaaS Application** window
 1. **In the Definition** area
 - under **Name**
 - enter **Unified Access Gateway SAML SP**
 - Under Icon
 - select **SELECT FILE ...**



5. In the **File Explorer > Open** window
 - In the **Quick Access** pane
 - select **Desktop**
 - in the **Desktop** area
 - select **software > UAG > Icons**
 - in the **Icons** folder
 - select **UAG.png**
 - select **Open**

New SaaS Application

OR BROWSE FROM CATALOG

1 Definition

2 Configuration


3 Access Policies

4 Summary

Name * ⓘ
Unified Access Gateway SAML SP

Description ⓘ

Icon ⓘ

 Unified Access Gateway

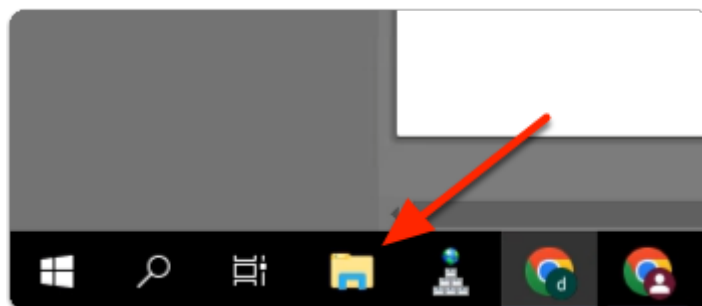
Category ⓘ

Selected Categories

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

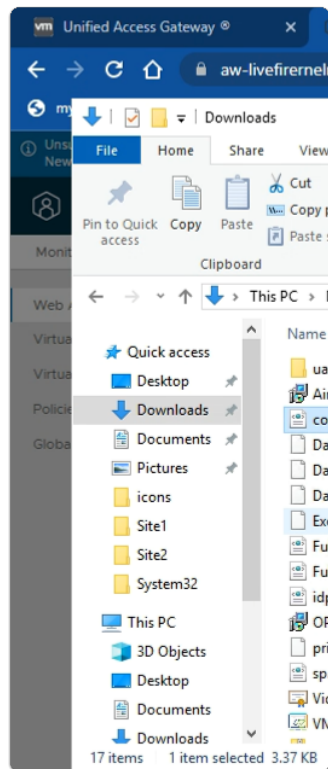
1. In the **Definition** area

- Select **NEXT**

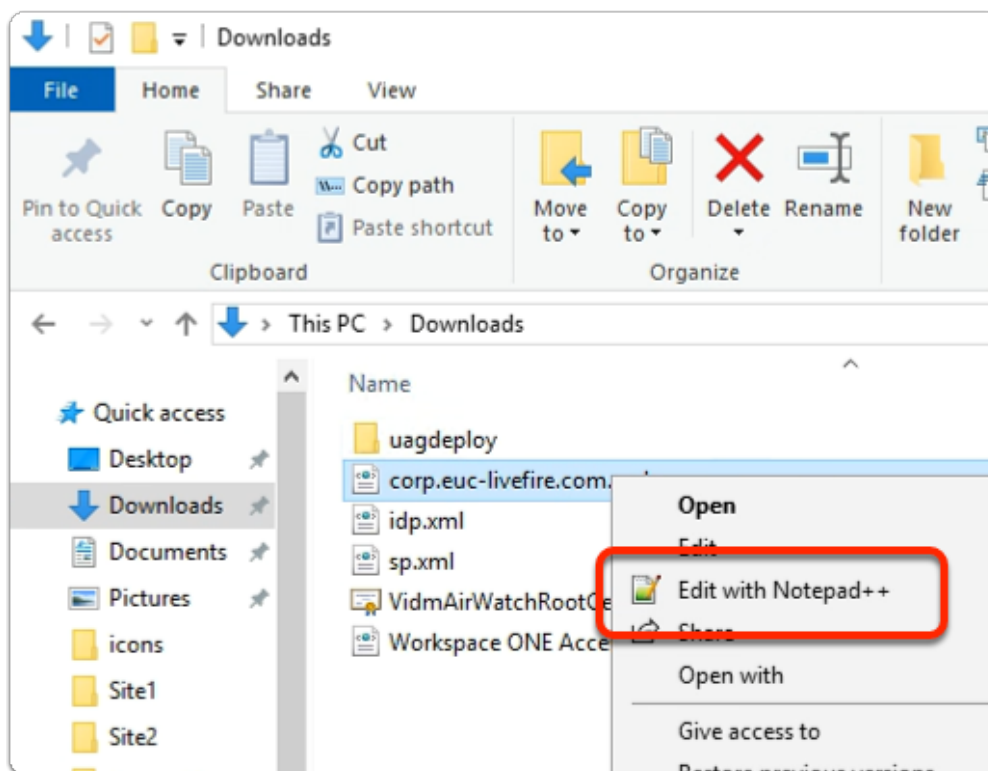


7. On the **ControlCenter** server

- from the **Taskbar**
- select the **Folder** icon

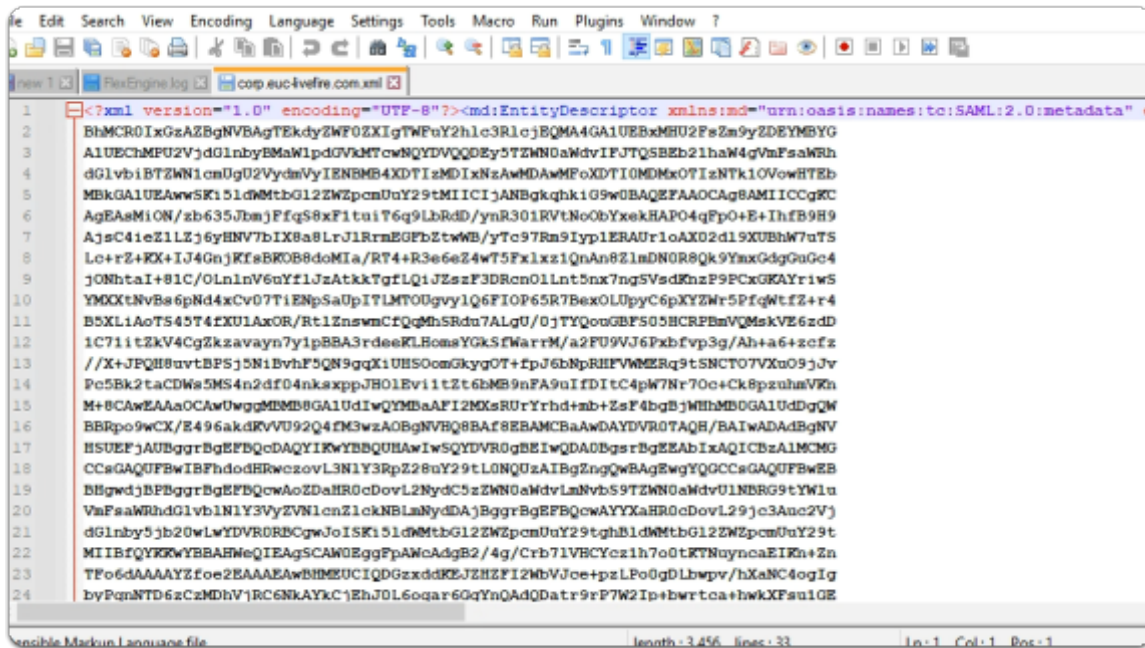


8. In the **File Explorer** window
 - from the **Quick Access** pane
 - select **Downloads**



9. In the **File Explorer** window
 - **Downloads** folder

- select **corp.euc-livewire.com**
 - select & right-click **Edit with Notepad++**



10. In the **Notepad++** application

- with your **keyboard**
 - enter **CTRL + A**
 - enter CTRL + C
- switch back to the **New SaaS Application** wizard

New SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type * ⓐ

SAML 2.0

Configuration * ⓐ

URL/XML ☒ Manual

URL/XML * ⓐ

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...>
```

Relay State URL ⓐ

ADVANCED PROPERTIES ▾

Open in Workspace ONE Web ⓐ

☒ Yes

Show in User Portal ⓐ

☐ No

11. In the **New SaaS Application** window
 2. In the **Configuration** area
 - the box below **URL / XML**
 - **paste** your **corp.euc-livefire.com.xml** metadata
 - **scroll down** the Configuration area to the bottom
 - below **Show in User Portal**
 - change the **Toggle** from **ON** to **OFF**
 - select **NEXT**

New SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Summary

Access Policies

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.

default_access_policy_set

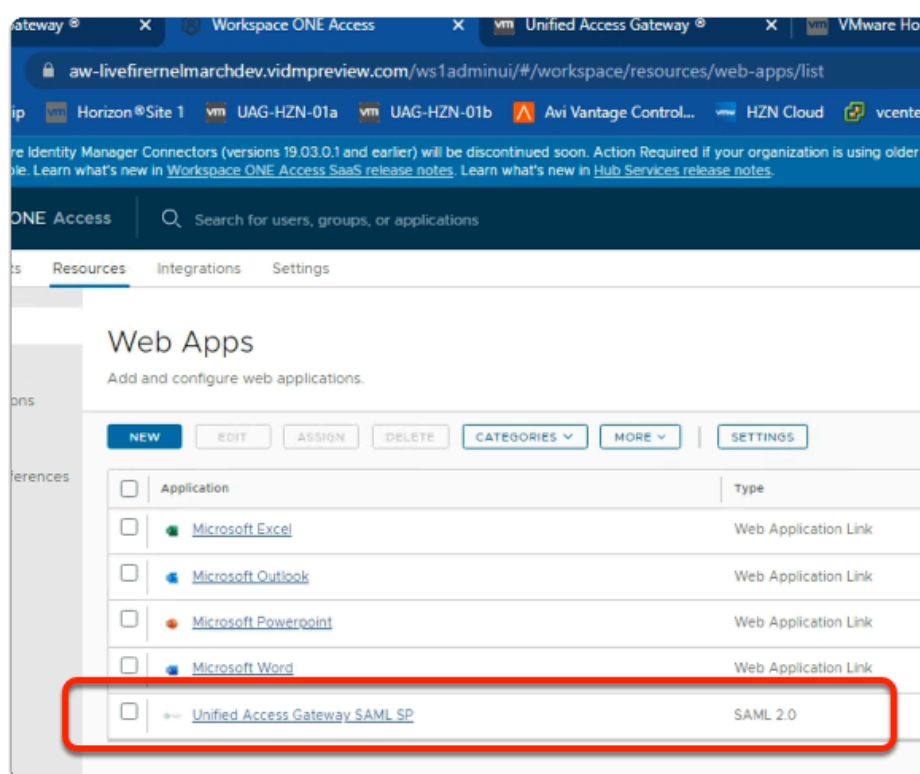
CANCEL BACK NEXT

12. In the **New SaaS Application** window,
 3. In the **Access Policies** section
 - Select **NEXT**

13. In the **New SaaS Application** window,
4. In the **Summary** section
 - Select **SAVE & ASSIGN**

14. In the **Assign** window
 - Under **Users / Groups**

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



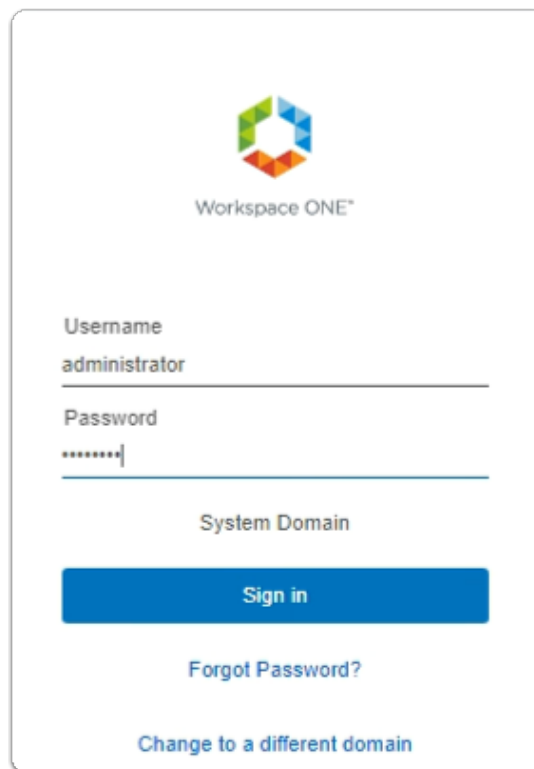
15. In your **Workspace ONE Access** Console
 - **Web Apps** interface
 - Note your **Unified Access Gateway SAML SP Web APP**

Part 4. Deploying VMware Horizon Deep Links for entitlements

As we are not using the Workspace ONE Access Connector to sync entitlements, we will create Deep Links for our Entitlements and assign these to our Security Groups

In this Part we will create Deep Links for existing entitlements

Step 1. Deploying a Deep link for the Enterprise Corp Instant Clone Global Entitlementment

A screenshot of the Workspace ONE login interface. At the top is the Workspace ONE logo, which consists of a hexagon made of smaller colored hexagons. Below the logo is the text "Workspace ONE". The login form has three input fields: "Username" with the text "administrator", "Password" with masked characters "*****", and "System Domain". Below these fields is a blue "Sign in" button. At the bottom of the form are two links: "Forgot Password?" and "Change to a different domain".

Workspace ONE

Username
administrator

Password

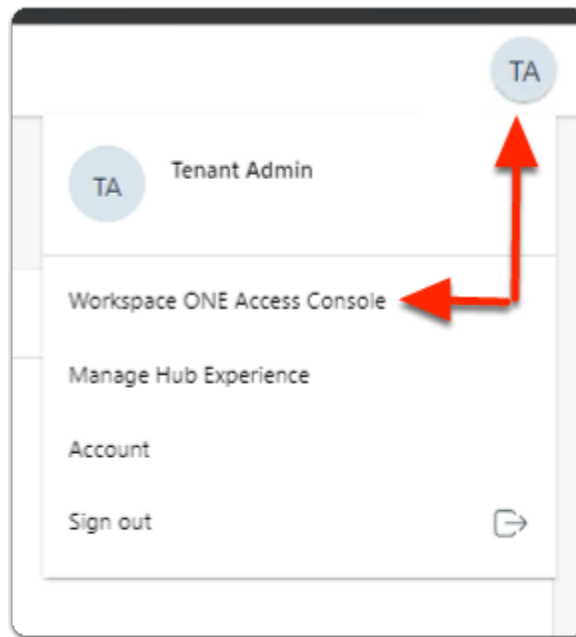
System Domain

Sign in

Forgot Password?

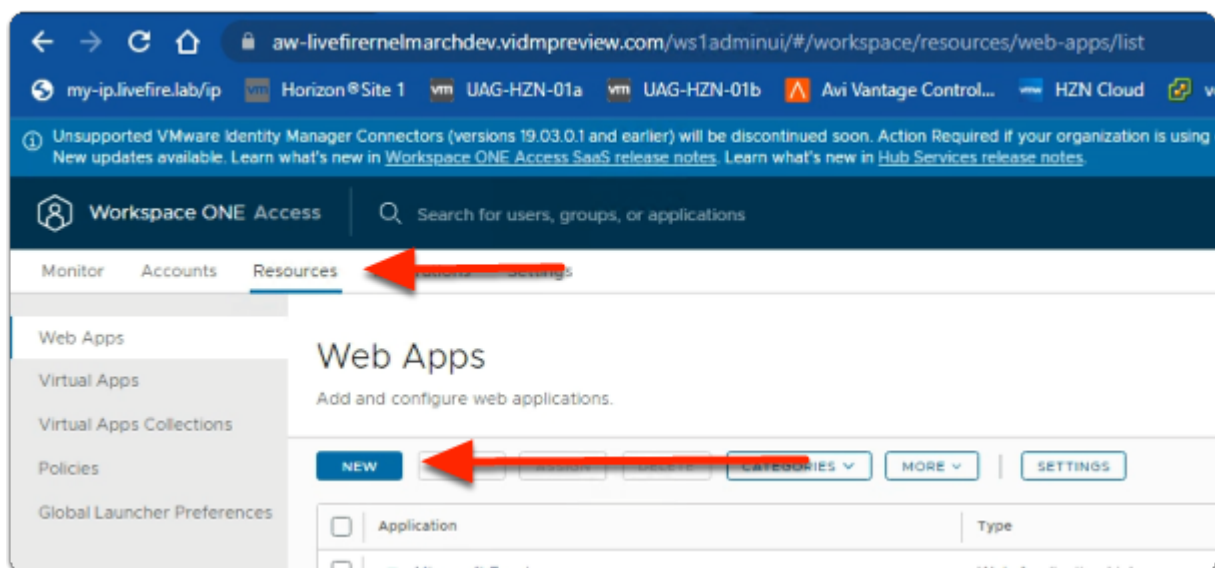
Change to a different domain

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 **Resources**
- Under **the Resources > WEB Apps** area
 - select **NEW**

1 Definition

2 Configuration

3 Summary

Definition

Name ⓘ

Enterprise Instant Clone Windows 11 Desktops

Description ⓘ

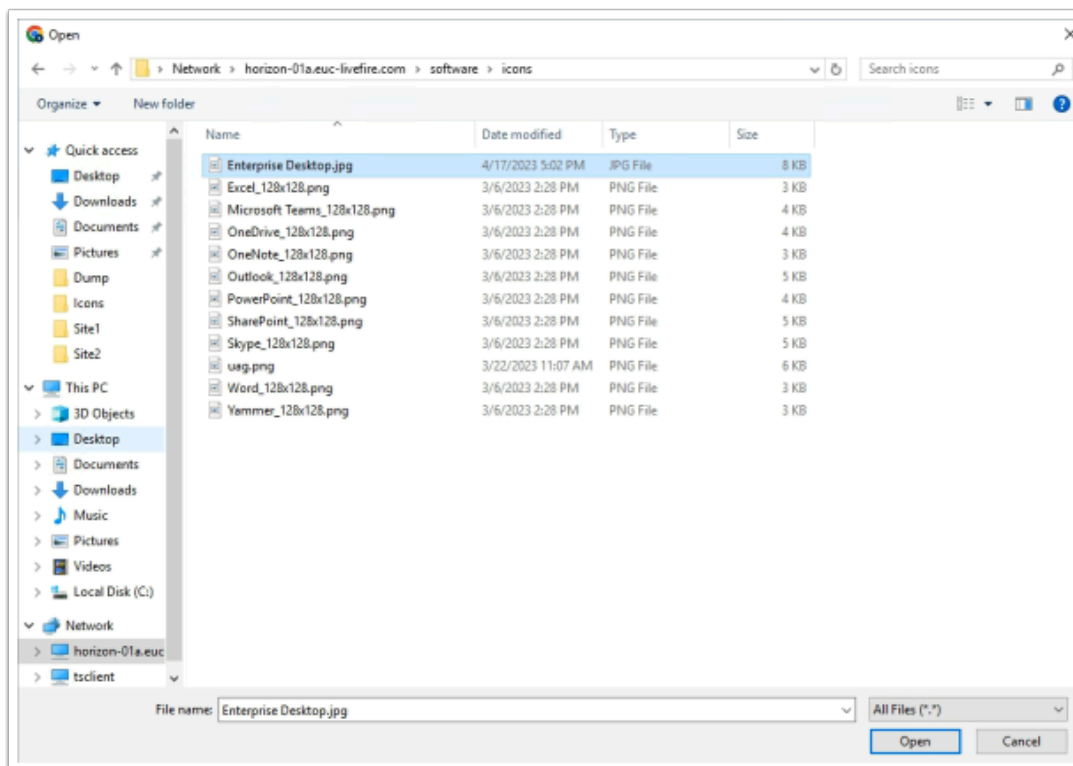
Icon ⓘ

SELECT FILE...

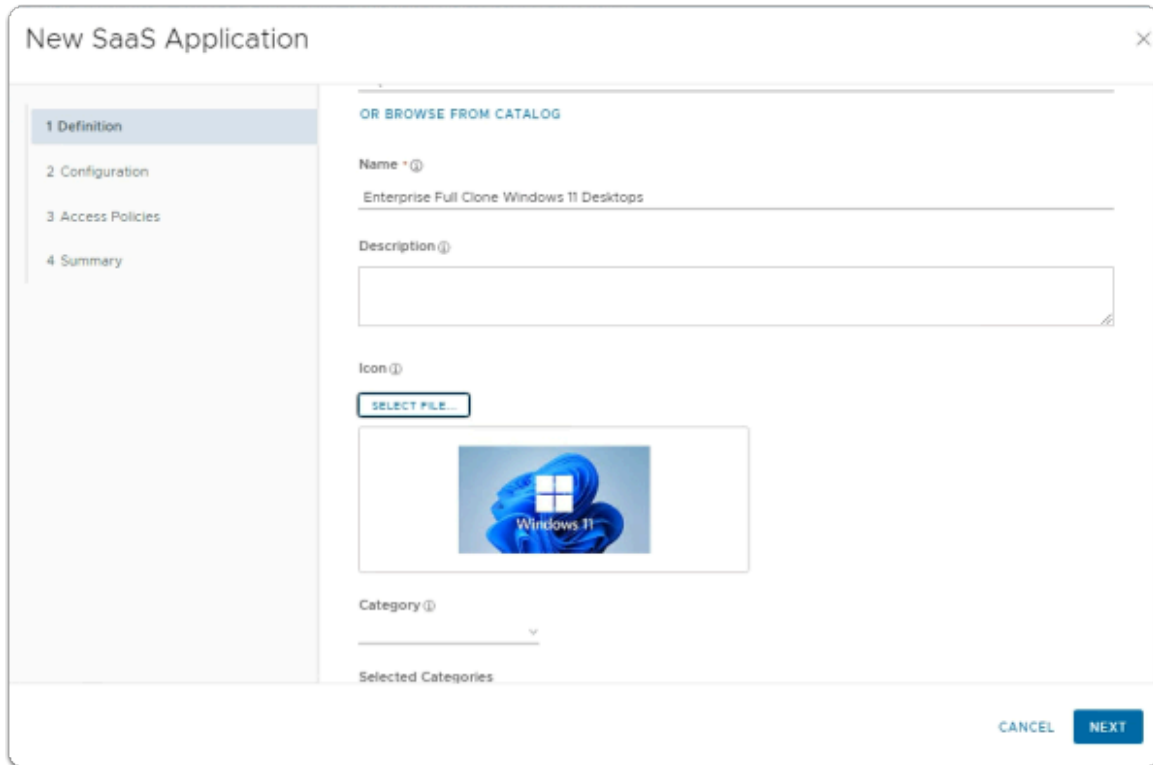
5. In the **New SaaS Application** window

1. **In the Definition** area

- under **Name**
 - enter **Enterprise Instant Clone Windows 11 Desktops**
- under **Icon**
 - select **SELECT FILE ...**



6. In the **File Explorer > Open** window
 - In the **Quick Access** pane
 - select **Desktop**
 - in the **Desktop** area
 - select **software > software > Icons**
 - in the **Icons** folder
 - select **Enterprise Desktop.jpg**
 - select **Open**



The screenshot shows a window titled "New SaaS Application" with a close button (X) in the top right corner. On the left is a sidebar with four tabs: "1 Definition" (selected), "2 Configuration", "3 Access Policies", and "4 Summary". The main area is titled "OR BROWSE FROM CATALOG" and contains the following fields:

- Name *** (required): A text field containing "Enterprise Full Clone Windows 11 Desktops".
- Description** (optional): A large text area.
- Icon** (optional): A section with a "SELECT FILE..." button and a preview image of a Windows 11 logo.
- Category** (optional): A dropdown menu.
- Selected Categories**: A list of categories.

At the bottom right are "CANCEL" and "NEXT" buttons.

7. In the **New SaaS Application** window
 1. In the **Definition** area
 - Select **NEXT**

New SaaS Application

1 Definition
2 Configuration
3 Access Policies
4 Summary

Single Sign-On

Authentication Type ⓘ

- SAML 2.0
- OpenID Connect
- SAML 1.1
- SAML 2.0
- Web Application Link**

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

New SaaS Application

1 Definition
2 Configuration
3 Summary

Single Sign-On

Authentication Type ⓘ

Web Application Link

Target URL *

<https://corp.euc-livefire.com/portal/nativeclient>

Open in Workspace ONE Web ⓘ

☐ No

CANCEL BACK NEXT

9. In the **New SaaS Application** window
 2. In the **Configuration** area
 - below **Target URL ***
 - enter the following URL


```
https://corp.euc-liveware.com/portal/nativeclient/  
Enterprise_Desktop?action=start-  
session&desktopProtocol=BLAST&launchMinimized=false
```

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

The screenshot shows the 'New SaaS Application' window with the 'Summary' tab selected. The window is divided into two main sections: a left sidebar with tabs '1 Definition', '2 Configuration', and '3 Summary', and a main content area. The 'Definition' section includes fields for 'Name' (Enterprise Full Clone Windows 11 Desktops), 'Description' (empty), 'Icon' (a blue icon with a computer monitor), 'Categories' (empty), and 'Configuration' (Authentication Type: None, Target URL: https://corp.euc-liveware.com/portal/nativeclient/Enterprise_Desktop?action=start-session&desktopProtocol=BLAST). The 'Access Policies' section includes 'Open in Workspace ONE Web' (No). At the bottom right, there are four buttons: 'CANCEL', 'BACK', 'SAVE & ASSIGN', and 'SAVE'.

10. In the **New SaaS Application** window,
 3. In the **Summary** section
 - Select **SAVE & ASSIGN**

The screenshot shows the 'Assign' window. At the top, it says 'Assign'. Below that, it says 'Selected App(s): Enterprise Full Clone Windows 11 Desktops'. Under the heading 'Users / User Groups', there is a search bar with the text 'dev' and a red arrow pointing to it. Below the search bar, there is a list of users. The first user is 'Developers@euc-liveware.com' with a red arrow pointing to it. Below this, there is a table with columns 'User', 'Deployment Type', and 'Entitlement Type'. The first row shows 'Developers@euc-liveware.com' with 'Automatic' in the 'Deployment Type' column and 'Include' in the 'Entitlement Type' column. A red arrow points to the 'Automatic' value.

11. In the **Assign** window

- Under **Users / Groups**
 - Enter **Devel**
 - Select **Developers@euc-livewire.com**

Assign

Application: Enterprise Instant Clone Windows 11 Desktops updated successfully

Selected App(s): Enterprise Instant Clone Windows

Users / User Groups

sales

Sales@euc-livewire.com

Deployment Type

Developers@euc-livewire.com

Automatic

Selected Users / User Groups

Deployment Type

Developers@euc-livewire.com

Automatic

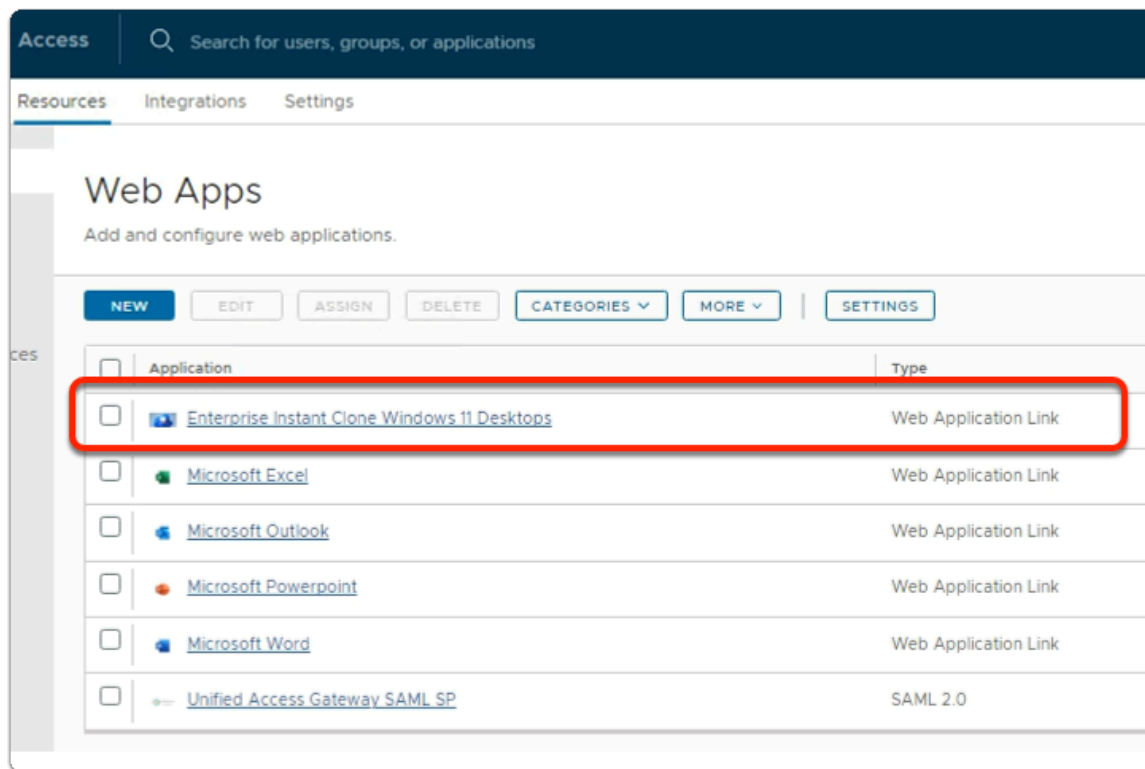
Sales@euc-livewire.com

Automatic

CANCEL SAVE

12. In the **Assign** window

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

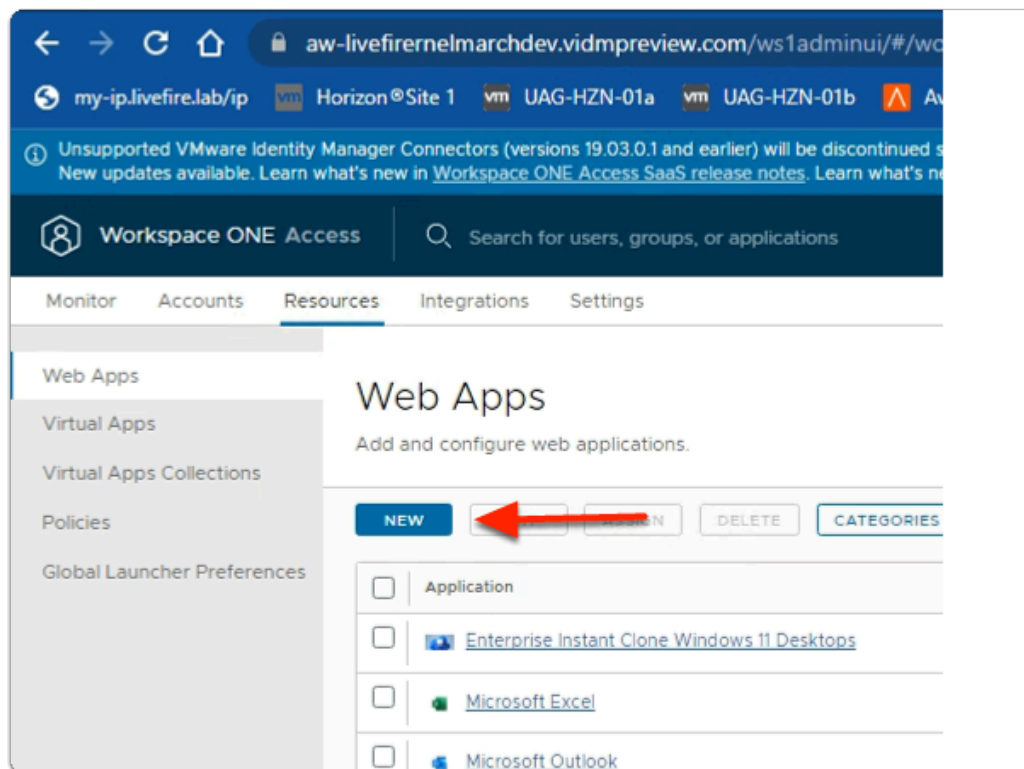


13. In your **Workspace ONE Access** Console

- **Web Apps** interface

- Note your **Enterprise Instant Clone Windows 11 Desktops Web Application Link**

Step 2. Deploying a Deep link for the Enterprise Full Clone Global Entitlement



1. In the **Workspace ONE Access Console**
 - under **the Resources > WEB Apps** area
 - select **NEW**

New SaaS Application

1 Definition

2 Configuration

3 Access Policies

4 Summary

Definition

Search ⓘ

Q

OR BROWSE FROM CATALOG

Name * ⓘ

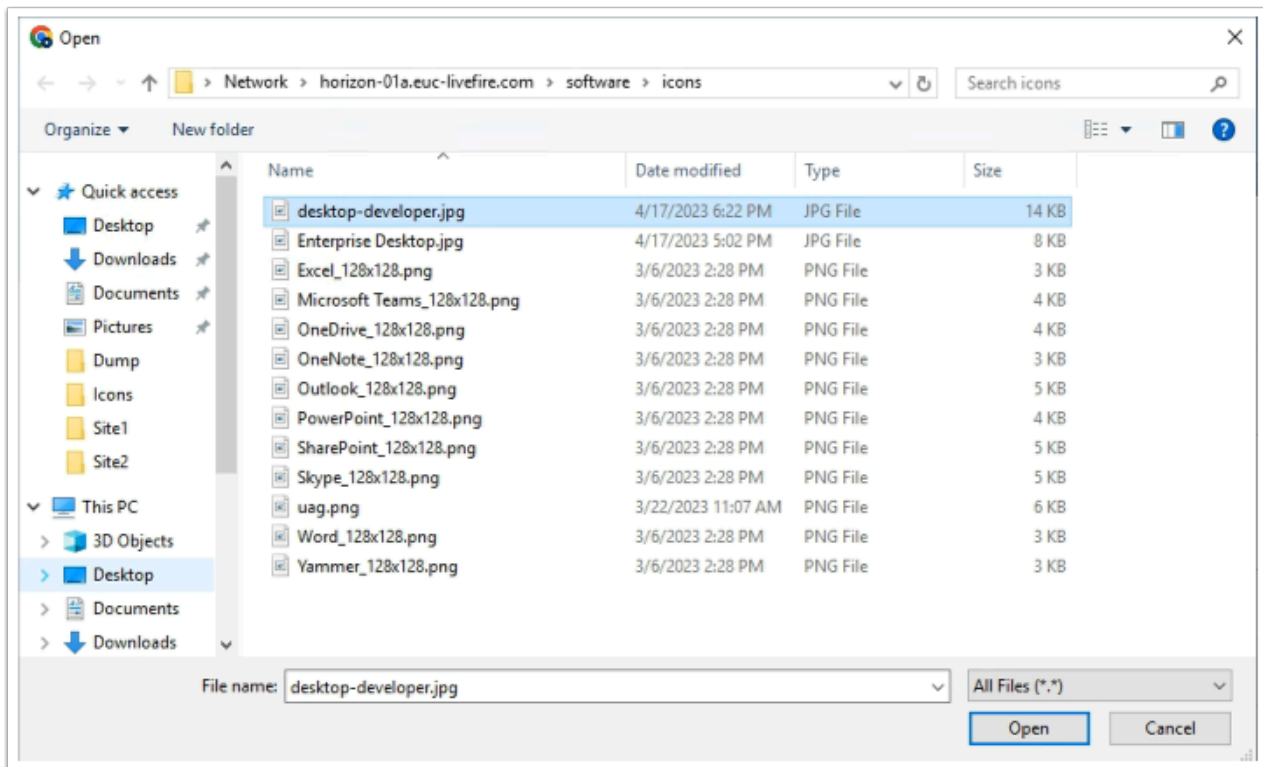
Enterprise Full Clone Desktops

Description ⓘ

Icon ⓘ

SELECT FILE...

2. In the **New SaaS Application** window
 1. **In the Definition** area
 - under **Name**
 - enter **Enterprise Full Clone Desktops**
 - under **Icon**
 - select **SELECT FILE ...**



3. In the **File Explorer > Open** window
 - In the **Quick Access** pane
 - select **Desktop**
 - in the **Desktop** area
 - select **software > software > Icons**
 - in the **Icons** folder
 - select **desktop-developer.jpg**
 - select **Open**

The screenshot shows the 'New SaaS Application' window with the 'Definition' tab selected. The left sidebar contains four tabs: '1 Definition', '2 Configuration', '3 Access Policies', and '4 Summary'. The main area is titled 'OR BROWSE FROM CATALOG'. It contains the following fields:

- Name ***: A text input field containing 'Enterprise Full Clone Desktops'.
- Description ***: A text input field that is currently empty.
- Icon ***: A button labeled 'SELECT FILE.' and a preview image showing a red square with the text 'Developer.'.
- Category ***: A dropdown menu that is currently empty.
- Selected Categories**: A text input field that is currently empty.

At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

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

1. In the **Definition** area

- Select **NEXT**

The screenshot shows the 'New SaaS Application' window with the 'Configuration' tab selected. The left sidebar contains four tabs: '1 Definition', '2 Configuration', '3 Access Policies', and '4 Summary'. The main area is titled 'Single Sign-On'. It contains the following fields:

- Authentication Type ***: A dropdown menu with the following options: 'SAML 2.0', 'OpenID Connect', 'SAML 1.1', 'SAML 2.0', and 'Web Application Link'. The 'Web Application Link' option is currently selected and highlighted in blue.

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

2. In the **Configuration** area

- below **Authentication Type ***
 - from the **dropdown**
 - select **Web Application Link**

New SaaS Application

1 Definition
2 Configuration
3 Summary

Single Sign-On

Authentication Type * ⓘ
Web Application Link

Target URL *
<https://corp.euc-livefire.com/portal/nativeclient>

Open in Workspace ONE Web ⓘ
☐ No

CANCEL BACK NEXT

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

2. In the **Configuration** area

- below **Target URL ***
 - enter the following URL

```
https://corp.euc-livefire.com/portal/nativeclient/  
Developers?action=start-  
session&desktopProtocol=BLAST&launchMinimized=false
```

• In the bottom right corner

- select **NEXT**

New SaaS Application

1 Definition
2 Configuration
3 Summary

Definition

Name
Enterprise Full Clone Desktops

Description
—

Icon

Categories
—

Configuration

Authentication Type
None

Target URL
https://corp.euc-livewire.com/portal/nativeclient/Developers?action=start-session&desktopProtocol=BLAST&launch

Access Policies

Open in Workspace ONE Web
No

CANCEL BACK SAVE & ASSIGN SAVE

7. In the **New SaaS Application** window,
 3. In the **Summary** section
 - Select **SAVE & ASSIGN**

Assign

Selected App(s): Enterprise Full Clone Windows 11 Desktops

Users / User Groups

Q dev

	Employment Type	Entitlement Type
Developers@euc-livewire.com	Automatic	Include

8. In the **Assign** window
 - Under **Users / Groups**
 - Enter **Devel**
 - Select **Developers@euc-livewire.com**

Assign

✓ Application: 'Enterprise Full Clone Desktops' added successfully.

Selected App(s): Enterprise Full Clone Desktops

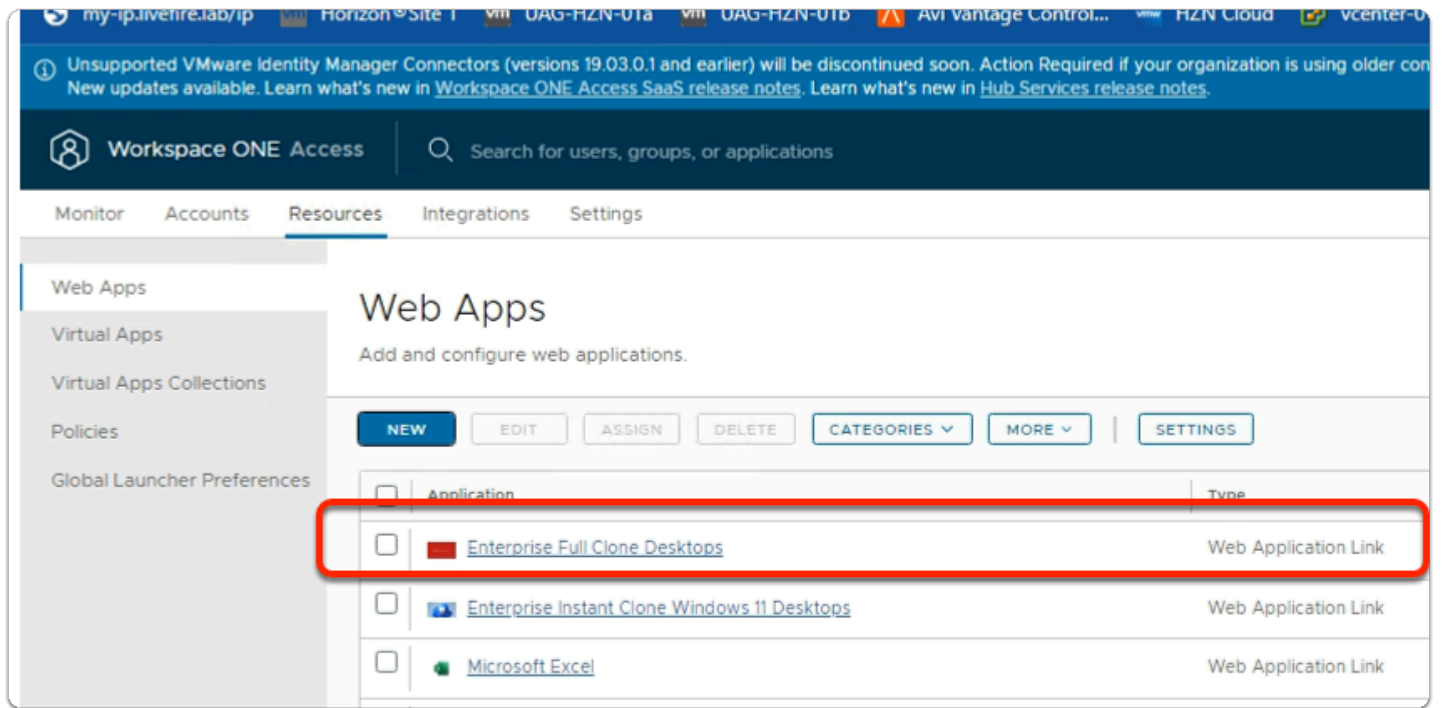
Users / User Groups

Q Search for Users or Groups

Selected Users / User Groups	Deployment Type
🔗 Developers@euc-livewire.com	Automatic

CANCEL SAVE

9. In the **Assign** window
 - Under **Deployment** type
 - From the **dropdown**
 - **Developers** are set to
 - **Automatic**
 - In the bottom right corner
 - select **SAVE**



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

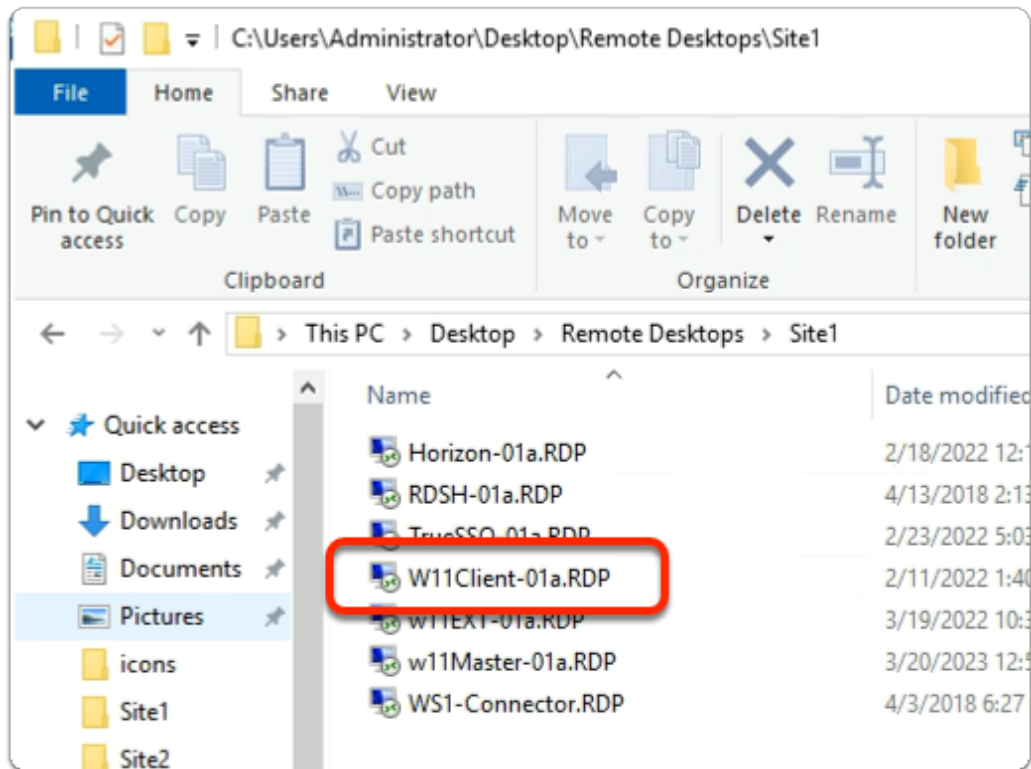
- **Web Apps** interface
 - Note your **Enterprise Full Clone Desktops Web Application Link**

Part 5. Testing the Horizon desktop sessions in Workspace ONE Access

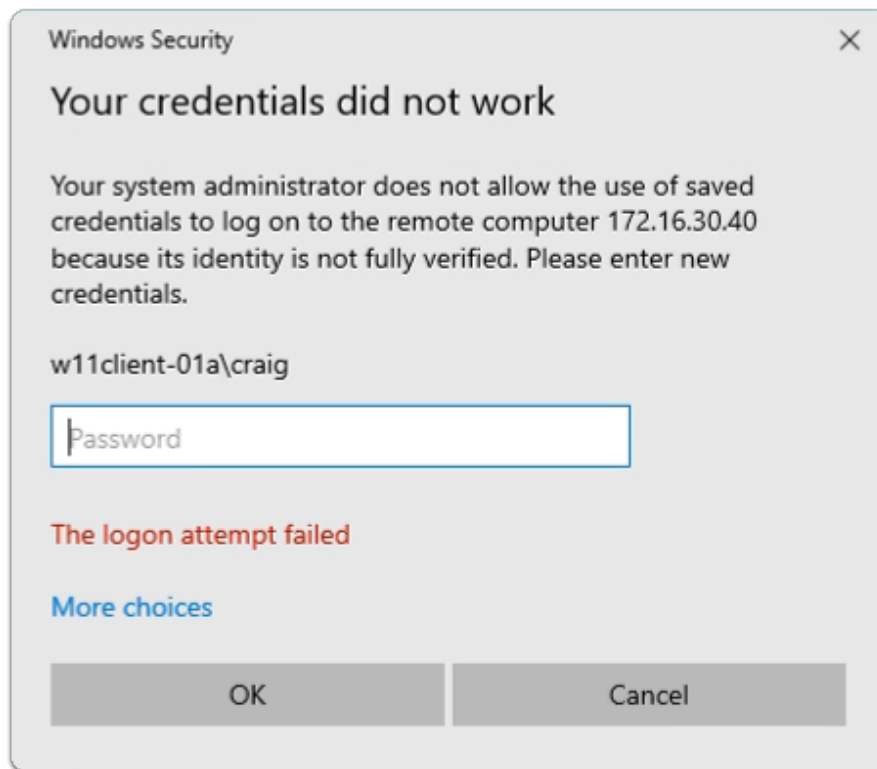
Part 5 brings everything we have done on Day 2 together.

We will look at 3 primary testing scenarios

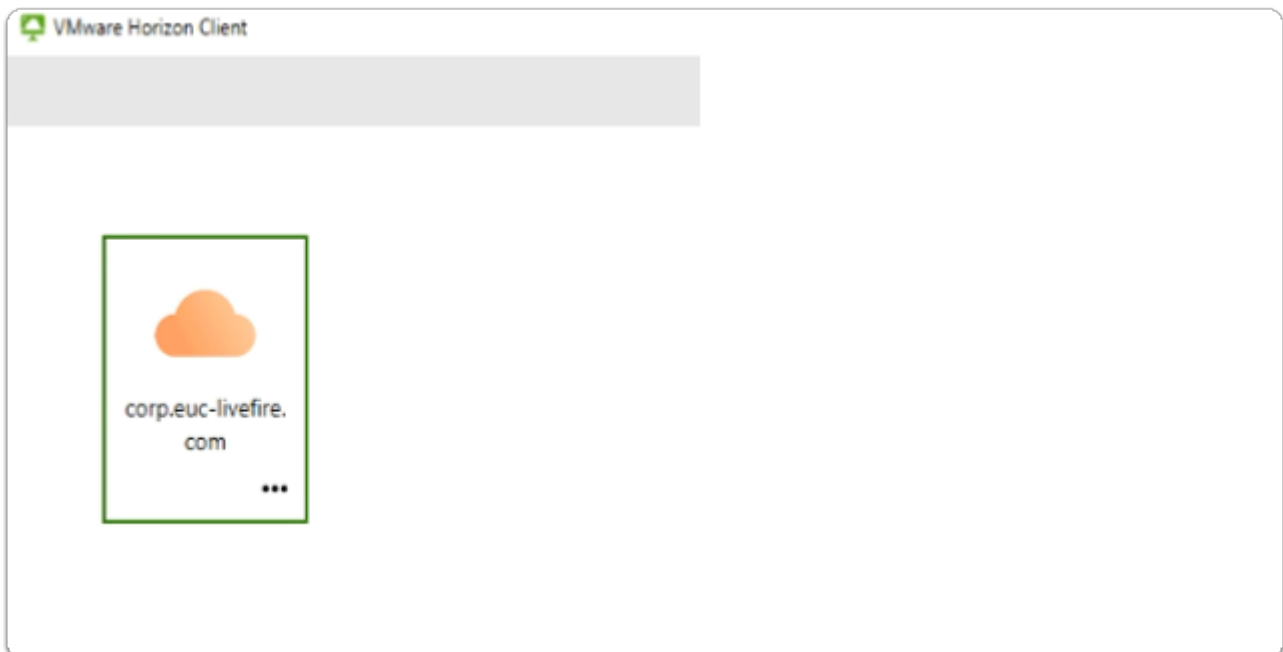
Step 1: Testing Site 1 based network traffic



1. On your **ControlCenter** server
 - from the **Desktop**
 - Open the **Remote Desktops \ Site 1** folder
 - Launch the **W11Client-01a.rdp** shortcut

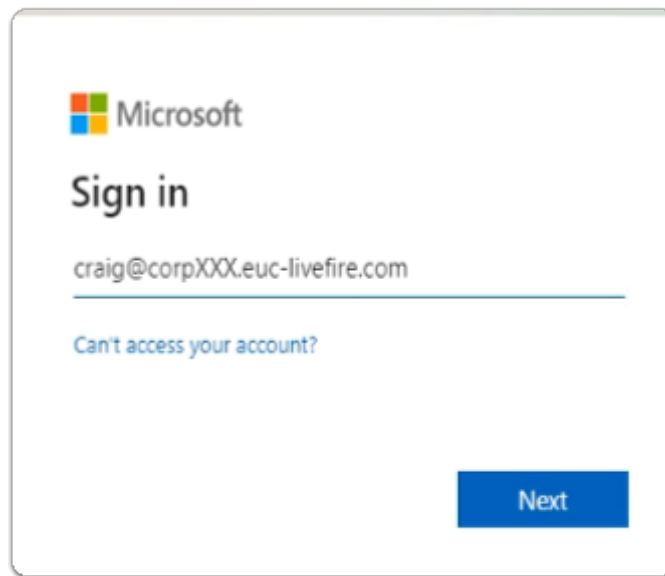


2. In the **Windows Security** page
 - ensure **Craig** is the username
 - in the **password** area
 - enter **VMware1!**
 - select **OK**

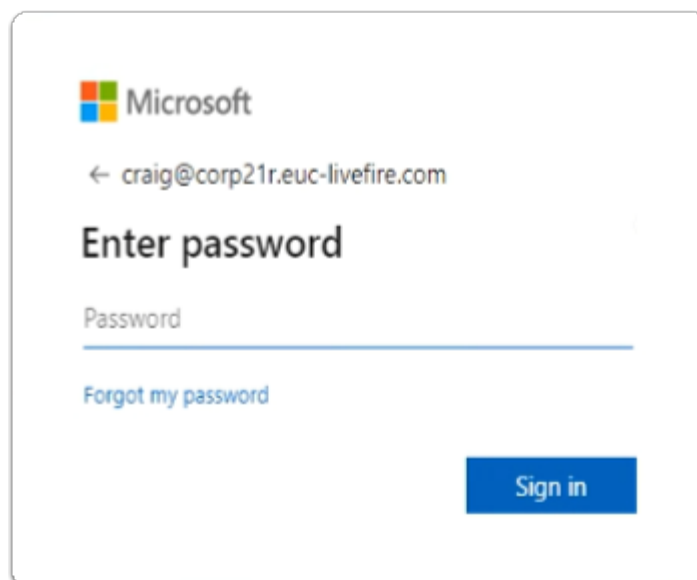


3. On your **W11Client-01a** desktop
 - From the **taskbar** or **Desktop**

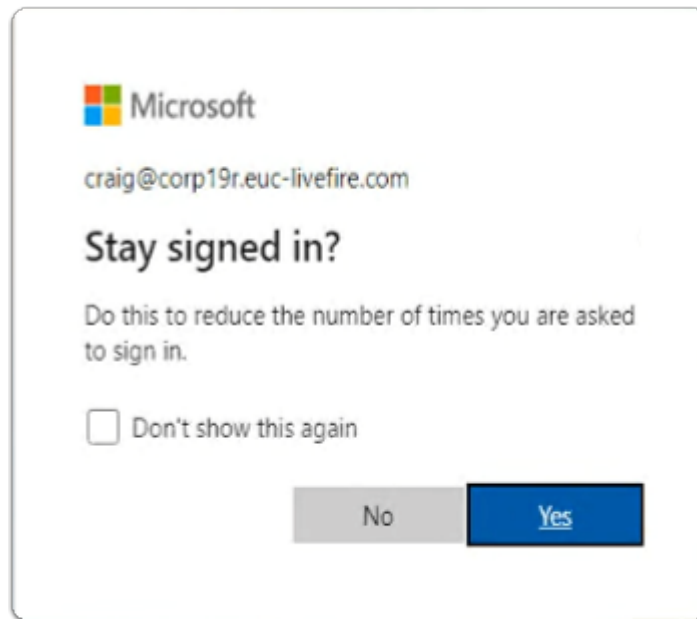
- launch your **VMware Horizon Client**
- In the **VMware Horizon Client** window
 - select **corp.euc-livewire.com** broker URL



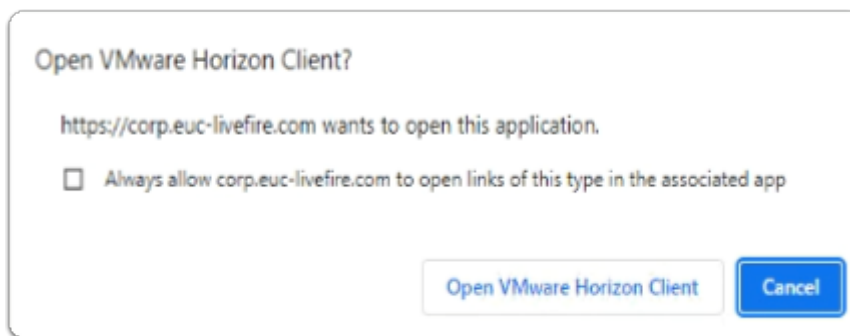
4. In the **Microsoft login** login window
 - in the **username** area
 - enter **craig@corpXXX.euc-livewire.com**
 - XXX is your assigned domain name
 - select **Next**



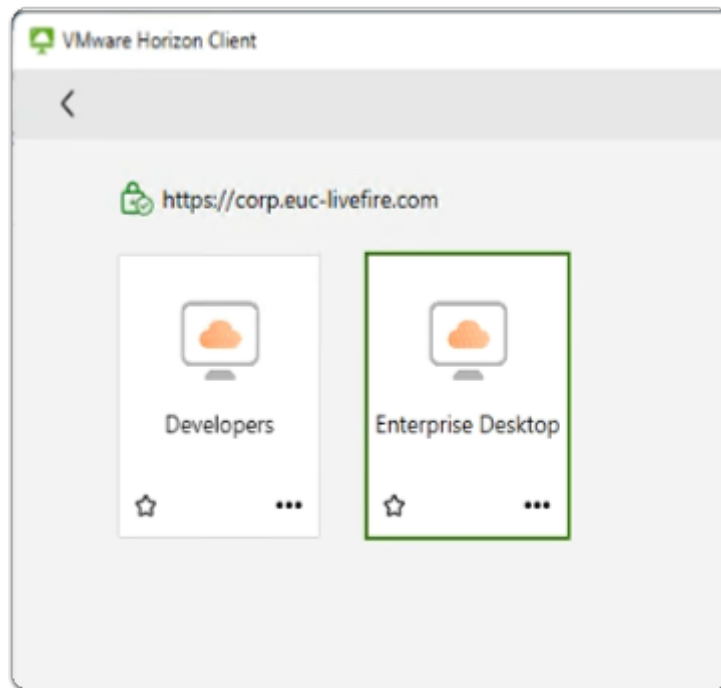
5. In the **Microsoft login** login window
 - below **Enter password**
 - enter **VMware1!**
 - select **Sign in**



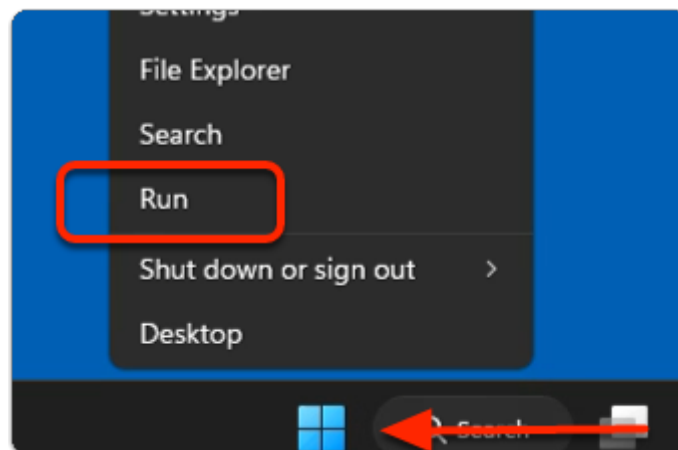
6. In the **Microsoft login** login window
 - below **Stay signed in?**
 - select **No**



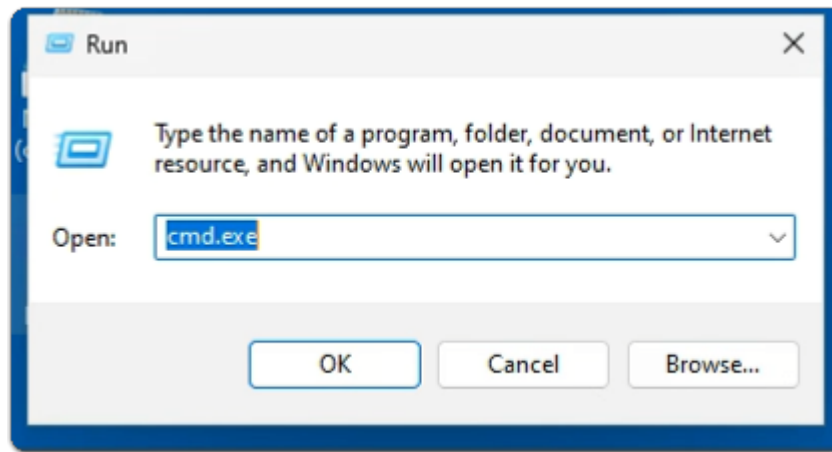
7. In the **Open VMware Horizon Client?** window
 - select **Open VMware Horizon Client**



8. In the **VMware Horizon Client** login window
- select the **Enterprise Desktop** entitlement

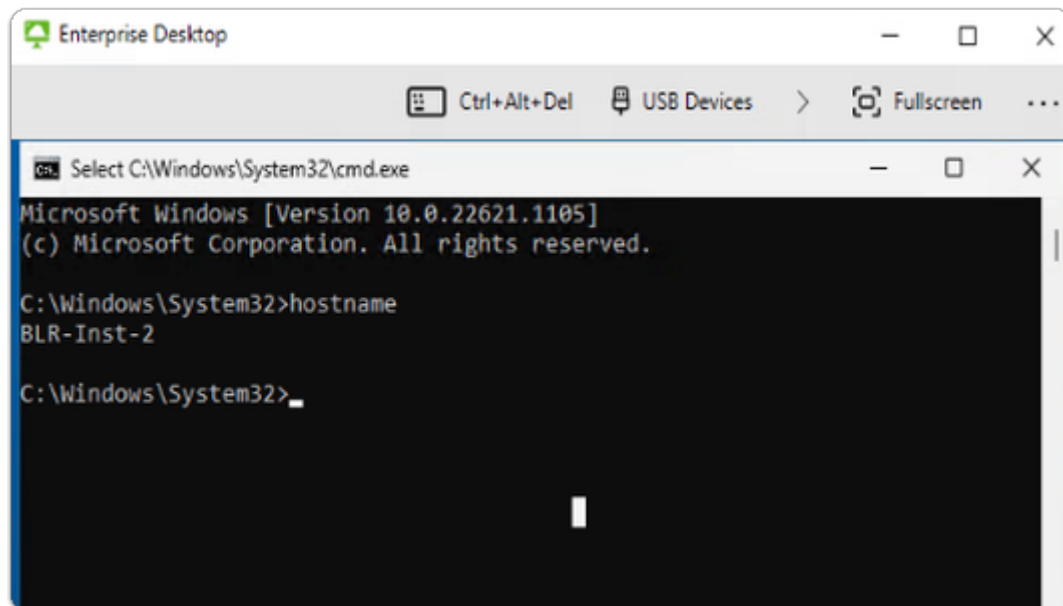


9. On your **Horizon Desktop** session
- from the **taskbar**
 - select and right-click the **START** button
 - from the **inventory**
 - select **Run**



10. In the **Run** window

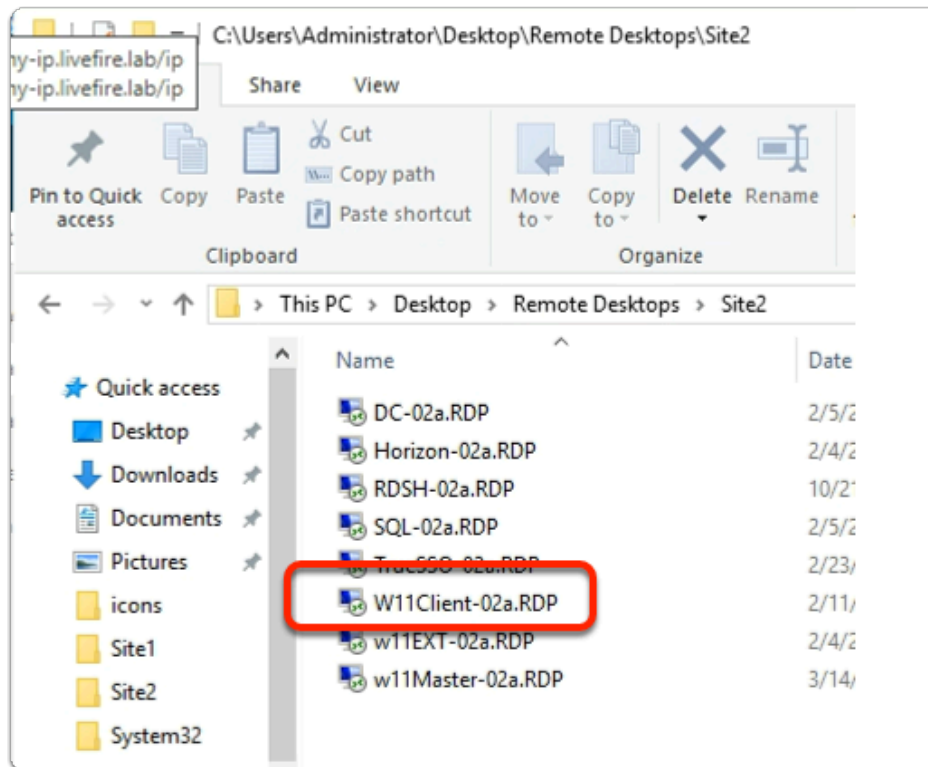
- next to **Open:**
 - enter **cmd.exe**
 - select **OK**



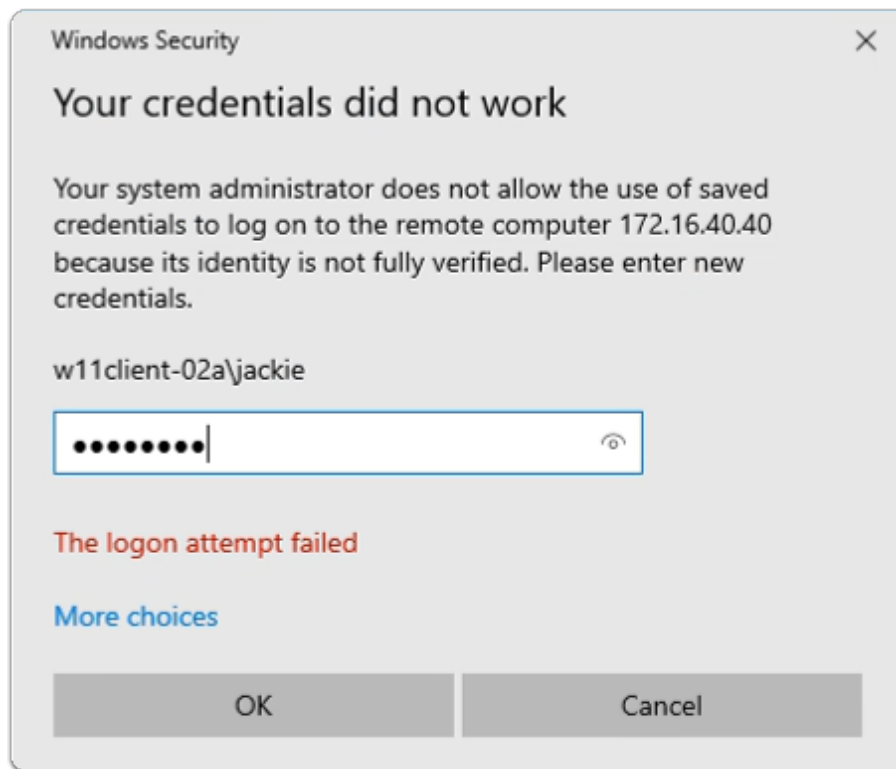
11. In the **CMD.exe** window

- In the **prompt area:**
 - enter **hostname**
 - with your **keyboard**
 - select **ENTER**
- Notice that you have a **Horizon virtual desktop** with the **BLR** naming convention representing **Bangalore**

Step 2: Testing Site 2 based network traffic



1. On your **ControlCenter** server
 - from the **Desktop**
 - Open the **Remote Desktops \ Site 2** folder
 - Launch the **W11Client-02a.rdp** shortcut

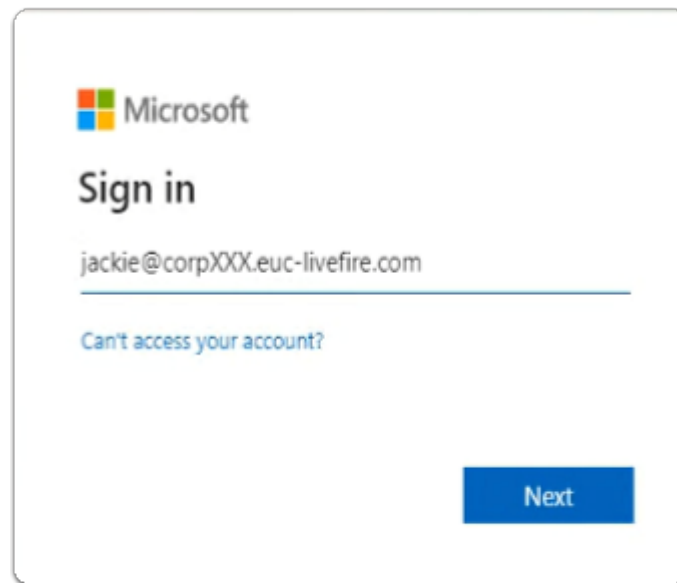


2. In the **Windows Security** page
 - ensure **Jackie** is the username
 - in the **password** area
 - enter **VMware1!**
 - select **OK**



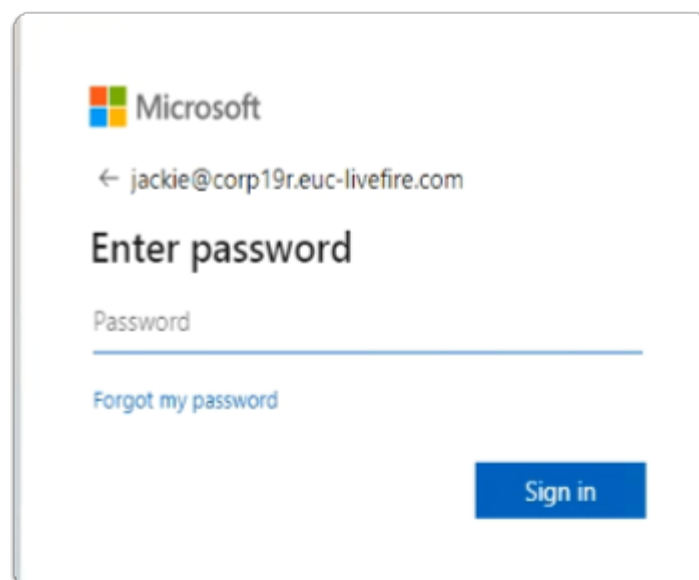
3. On your **W11Client-02a** desktop
 - From the **taskbar** or **Desktop**

- launch your **VMware Horizon Client**
- In the **VMware Horizon Client** window
 - select **corp.euc-livewire.com** broker URL



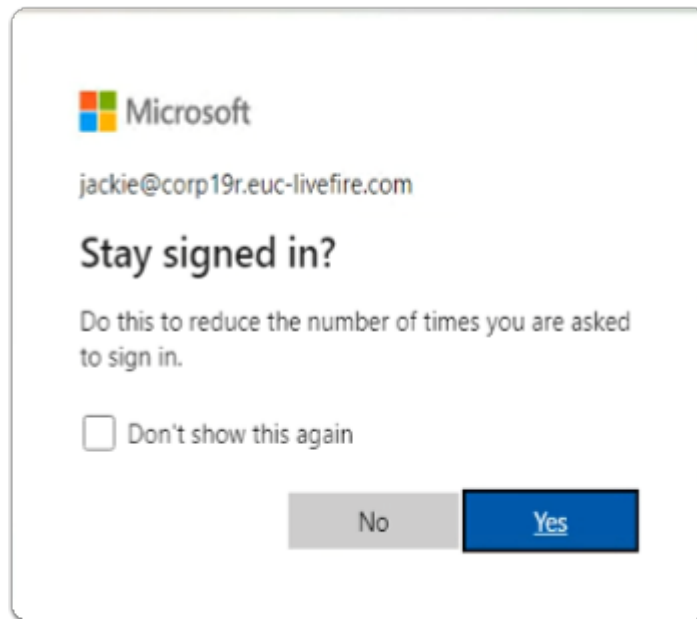
A screenshot of the Microsoft Sign in window. At the top left is the Microsoft logo. Below it, the text "Sign in" is displayed. Underneath, the email address "jackie@corpXXX.euc-livewire.com" is entered into a text field. Below the text field is a link that says "Can't access your account?". At the bottom right, there is a blue button labeled "Next".

4. In the **Microsoft login** login window
 - in the **username** area
 - enter **jackie@corpXXX.euc-livewire.com**
 - XXX is your assigned domain name
 - select **Next**

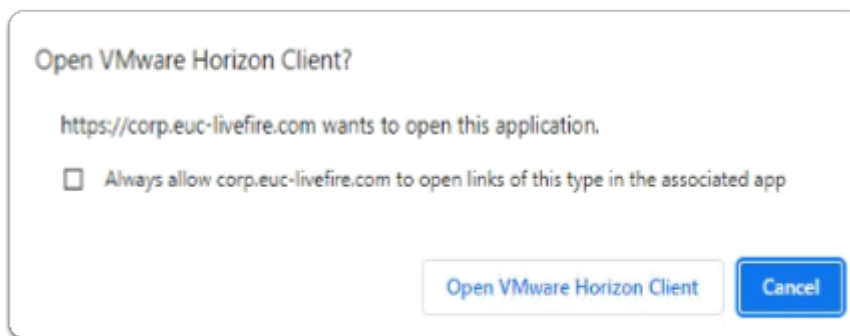


A screenshot of the Microsoft Enter password window. At the top left is the Microsoft logo. Below it, the text "Enter password" is displayed. Underneath, the email address "jackie@corp19r.euc-livewire.com" is shown with a back arrow to its left. Below the email address is a text field labeled "Password". Below the text field is a link that says "Forgot my password?". At the bottom right, there is a blue button labeled "Sign in".

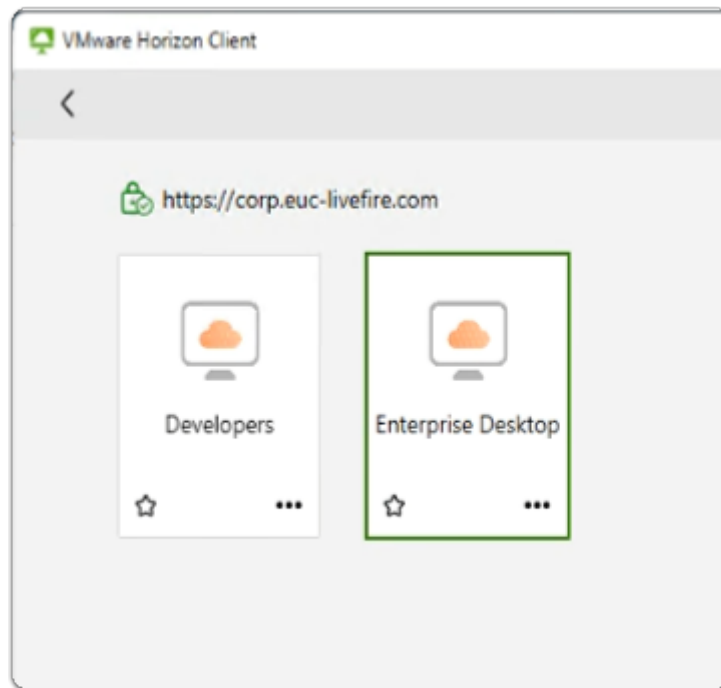
5. In the **Microsoft login** login window
 - below **Enter password**
 - enter **VMware1!**
 - select **Sign in**



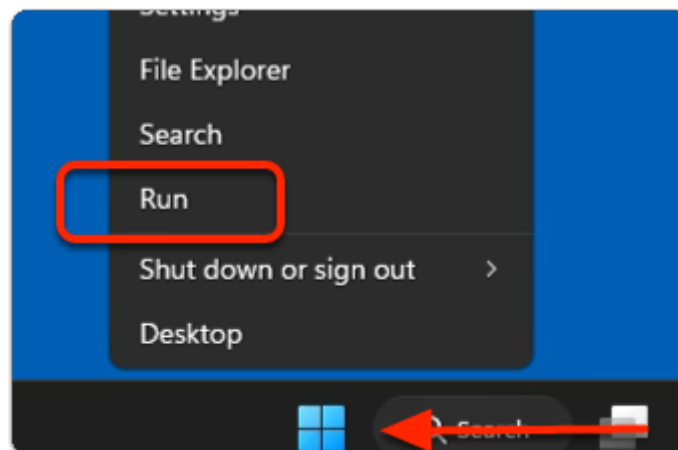
6. In the **Microsoft login** login window
 - below **Stay signed in?**
 - select **No**



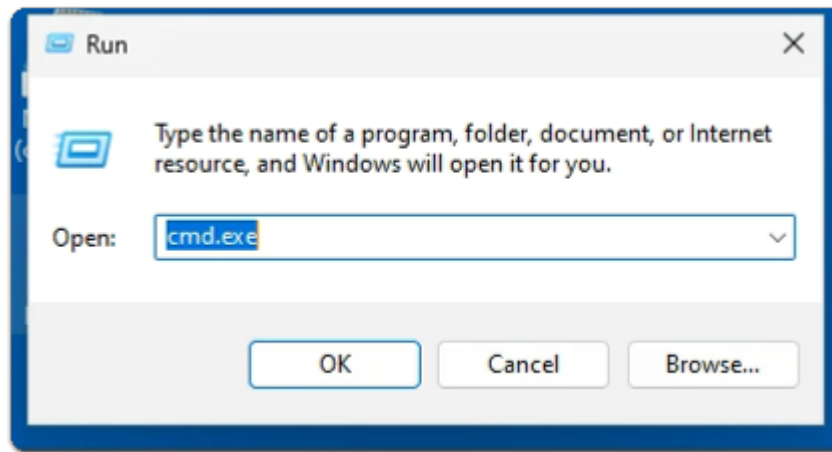
7. In the **Open VMware Horizon Client?** window
 - select **Open VMware Horizon Client**



8. In the **VMware Horizon Client** login window
- select the **Enterprise Desktop** entitlement

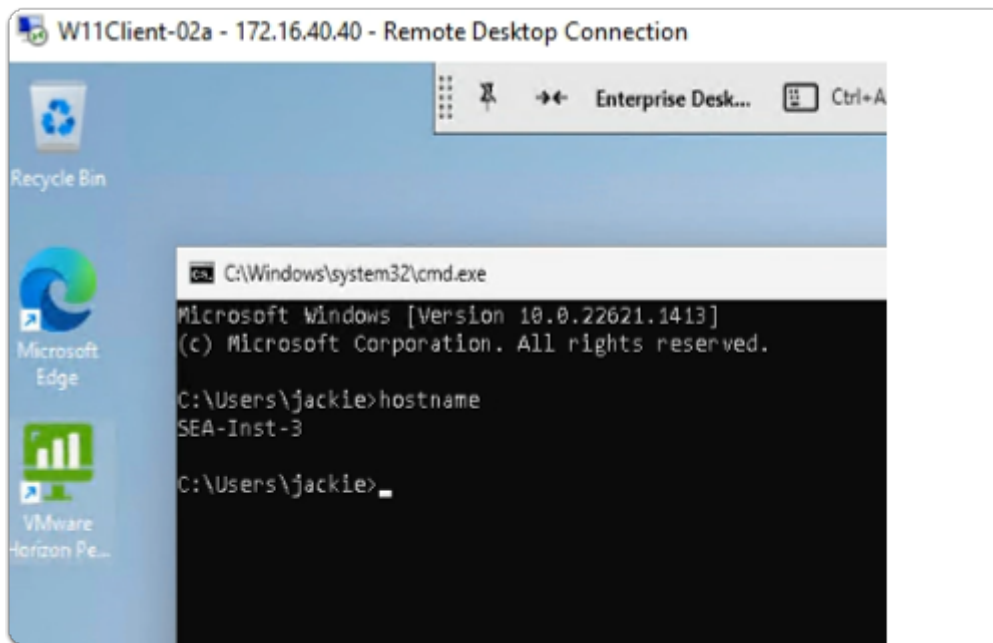


9. On your **Horizon Desktop** session
- from the **taskbar**
 - select and right-click the **START** button
 - from the **inventory**
 - select **Run**



10. In the **Run** window

- next to **Open:**
 - enter **cmd.exe**
 - select **OK**

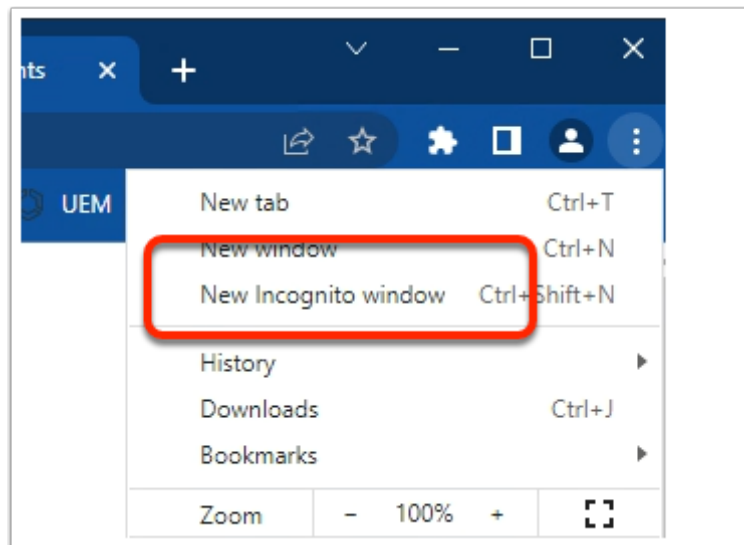


11. In the **CMD.exe** window

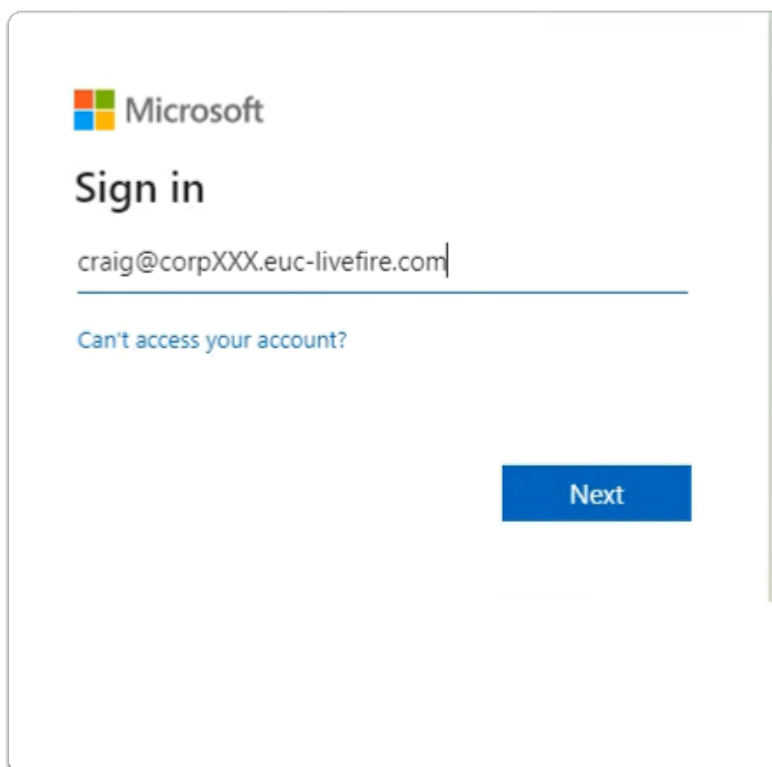
- In the **prompt area:**
 - enter **hostname**
 - with your **keyboard**
 - select **ENTER**
- Notice that you have a **Horizon virtual desktop** with the **SEA** naming convention representing **Seattle**

Step 3. Testing Horizon integration with Workspace ONE Access

using CPA Global Entitlements



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

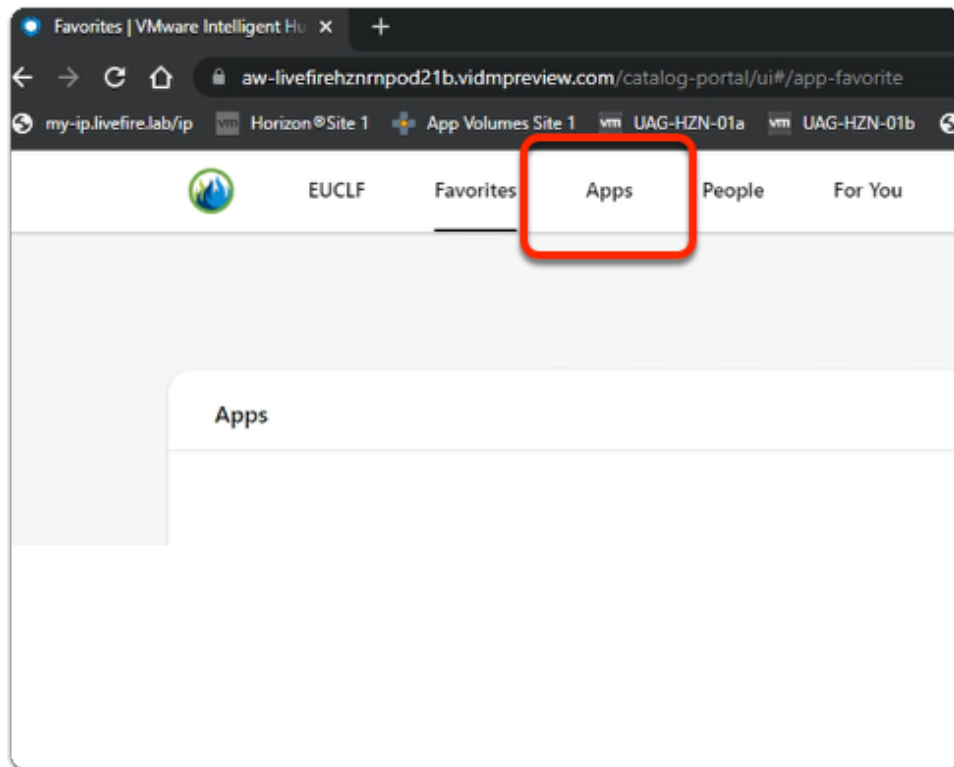


2. In the **Microsoft Sign in** window
 - enter
 - **craig@corpXXX.euc-livefire.com**

- where **XXX** is your assigned domain
- select **Next**

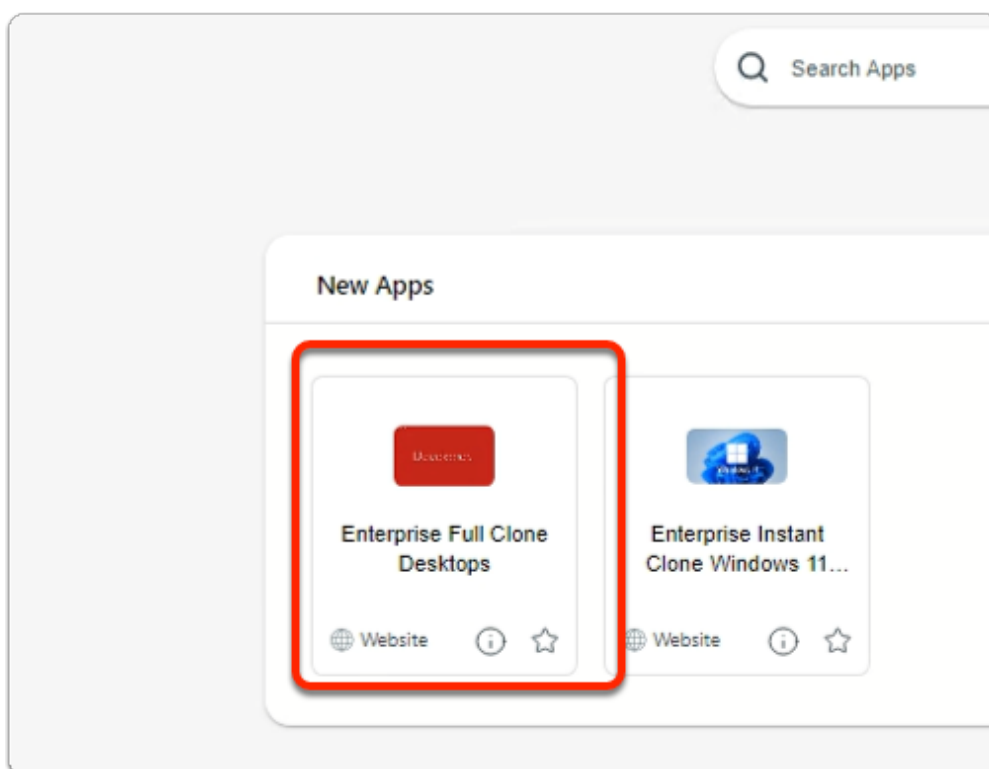
The image displays two sequential steps of the Microsoft Sign in process. The top window, titled 'Microsoft', shows the user 'craig@corp19r.euc-liveware.com' at the 'Enter password' stage. A password field with seven dots is visible, along with a 'Forgot my password' link. The bottom window, also titled 'Microsoft', shows the same user at the 'Stay signed in?' stage. It includes a checkbox for 'Don't show this again' and two buttons: 'No' and 'Yes'.

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



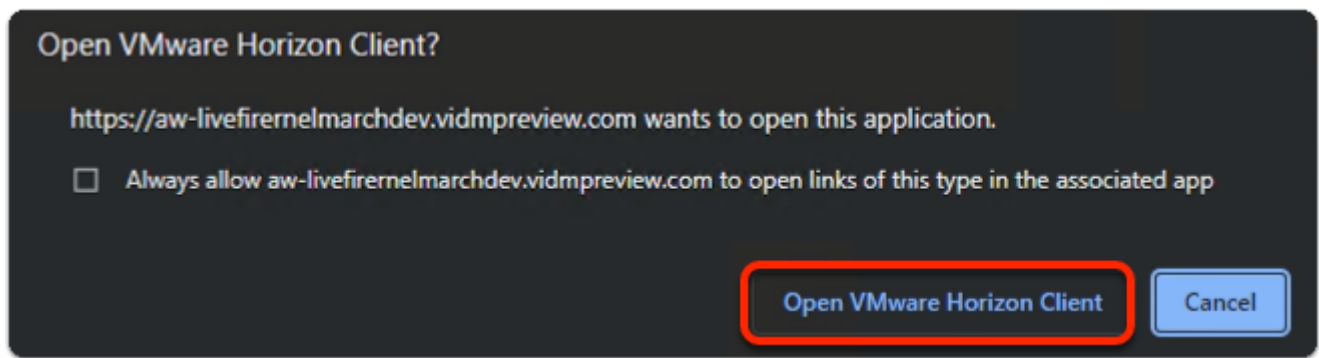
4. In the **web Intelligent Hub**

- Select **Apps**

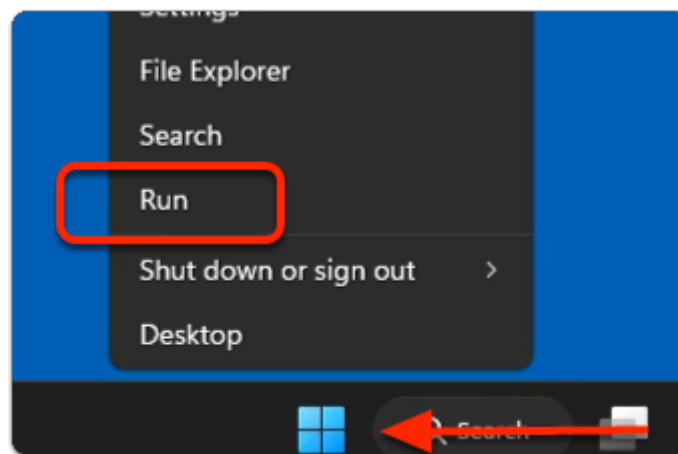


5. In the **web Intelligent Hub**

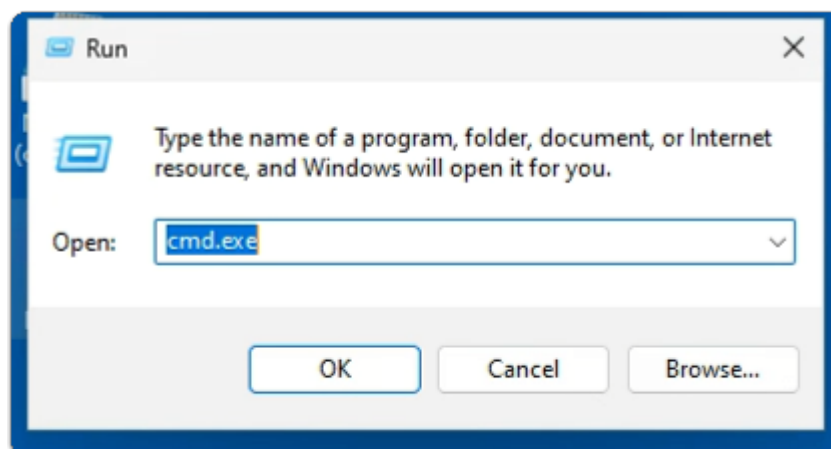
- Under **New Apps**
 - select **Enterprise Desktop**



6. In the **Open VMware Horizon Client?** window
- select **Open VMware Horizon Client**

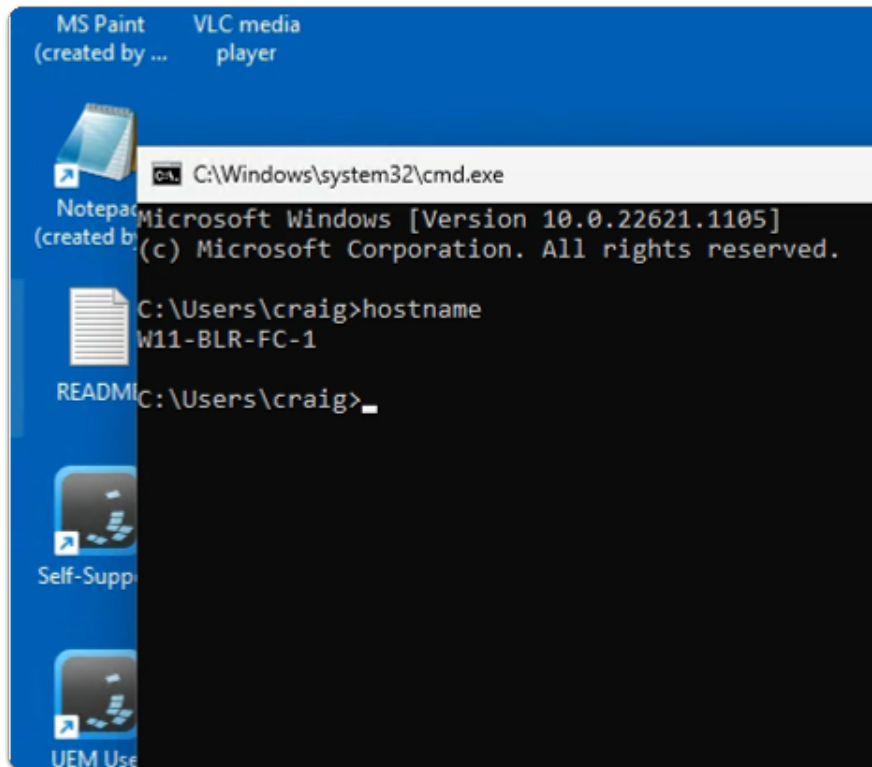


7. On your **Horizon Desktop** session
- from the **taskbar**
 - select and right-click the **START** button
 - from the **inventory**
 - select **Run**



8. In the **Run** window
- next to **Open:**

- enter **cmd.exe**
- select **OK**



9. In the **CMD.exe** window
 - In the **prompt area**:
 - enter **hostname**
 - with your **keyboard**
 - select **ENTER**
 - Notice that you have a **Horizon virtual desktop** with the **BLR** naming convention representing **Bangalore**

i Conclusion

To summarize. The started off the labs for Day 2 with first configuring

1. On both Site 1 and Site 2 using VMware AVi Local load-balancing of 4 UAG servers
2. Using a VMware AVi . You configured a Global Load balancing solution across site 1 and site 2
3. We then enabled and configured VMware Horizon Cloud Pod Architecture across site 1 and site 2
4. We then enabled a Federation of Workspace ONE access with Unified Access Gateway and VMware Horizon
 - From our ControlCenter server. We launched a Web based Intelligent Hub session

- From the Intelligent Hub we did a Horizon Desktop launch and our GLSB redirected us to Site 1
- Feel free to repeat the same steps on a Site 2 based desktop for Intelligent Hub