

# Unified Access Gateway / VMware Horizon integration into Workspace ONE Access

## Overview

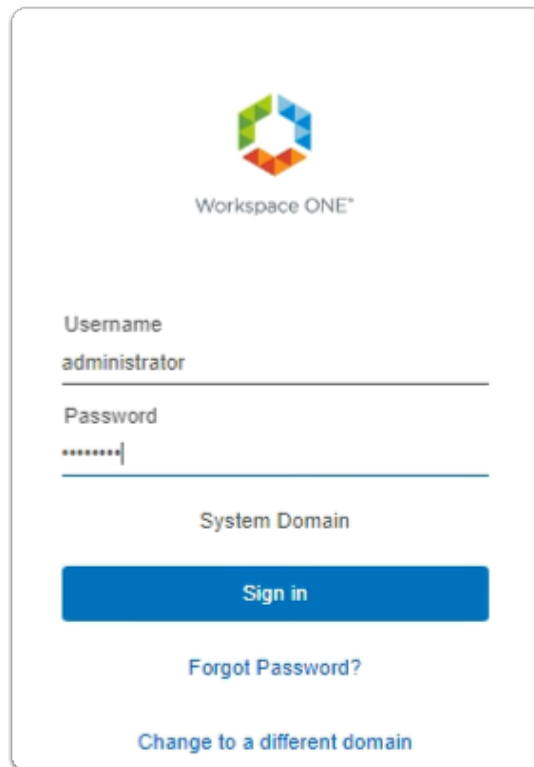
- Traditional Federation with VMware Horizon and Workspace ONE Access has been a popular approach and is used by many organizations.
- Organizations with high security requirements do not like a SAML Artifact being validated internally
- In this session we look at the option to validate the SAML Artifact 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



Workspace ONE™

Username  
administrator

Password  
\*\*\*\*\*

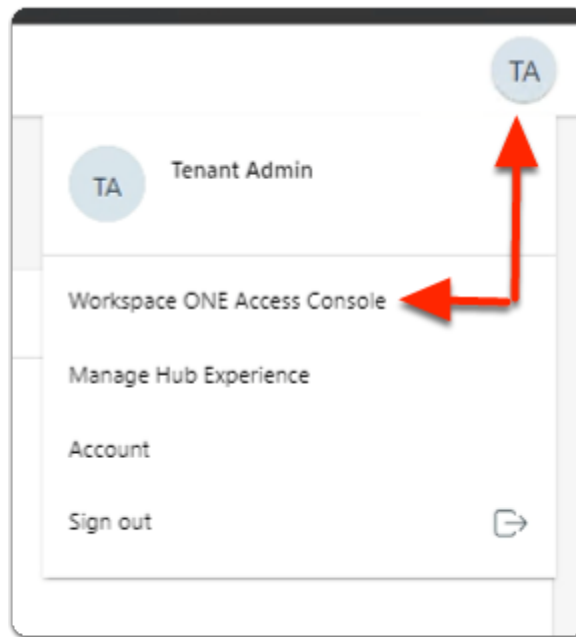
System Domain

Sign in

[Forgot Password?](#)

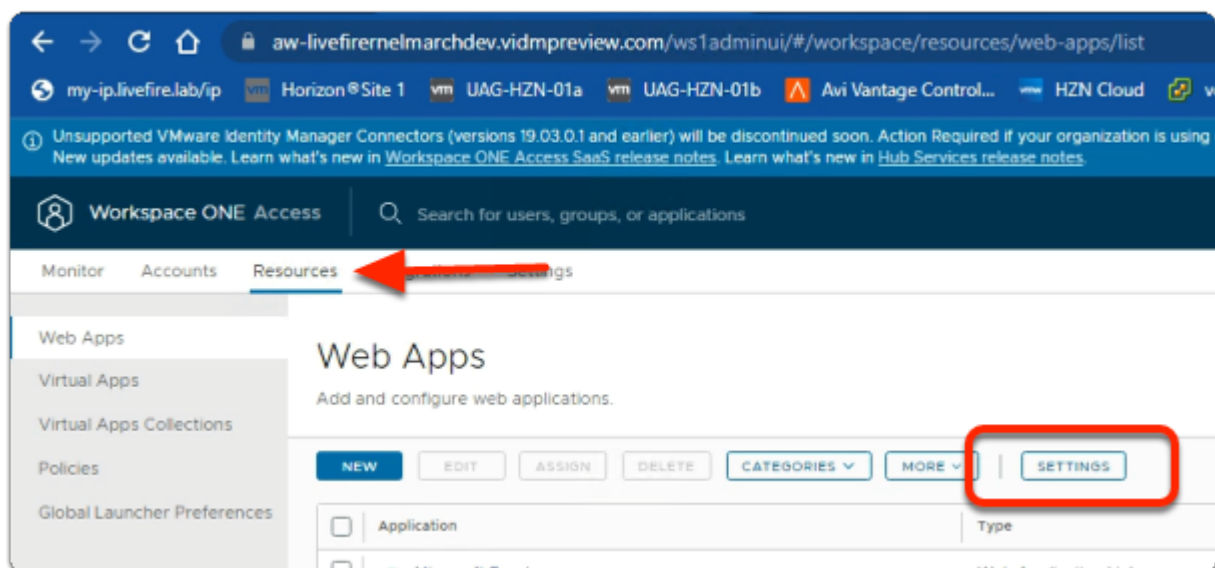
[Change to a different domain](#)

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



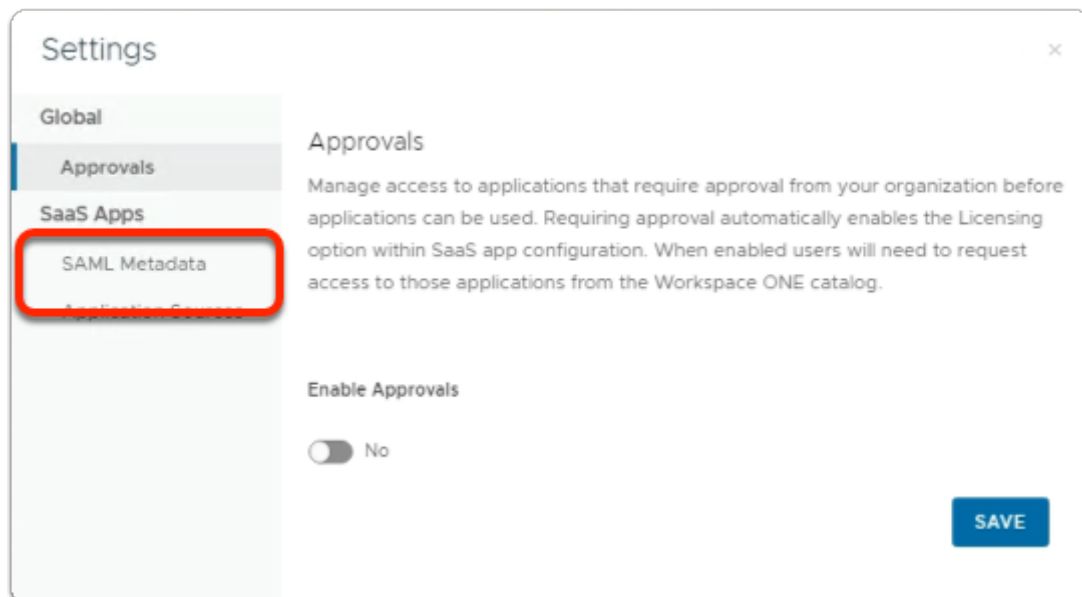
2. In the **Web Intelligent Hub** Console

- To the right,
  - select **TA**
- From the dropdown
  - select **Workspace ONE Access Console**

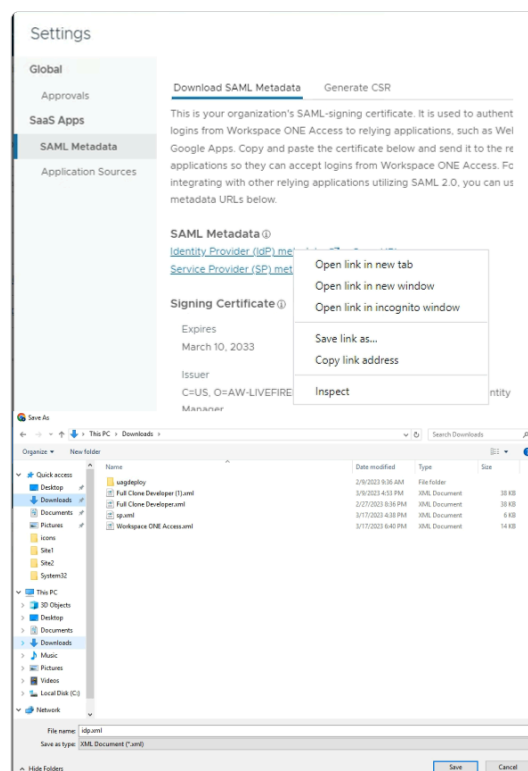


3. In the **Workspace ONE Access Console**

- Select **Resources**
- Under **the Resources > WEB Apps** area
  - Select **SETTINGS**



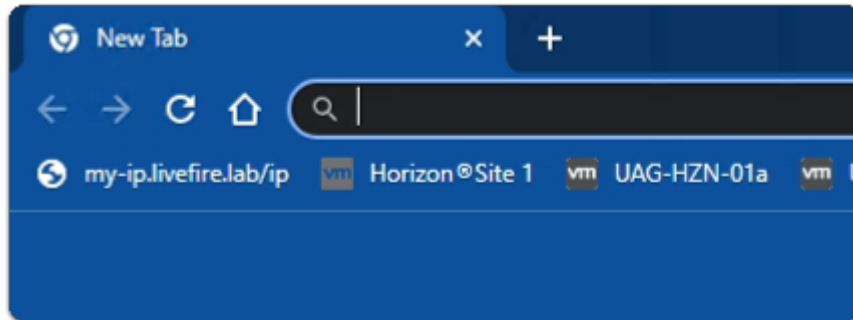
4. In the **Settings** window
  - below **SaaS Apps**
  - select **SAML Metadata**



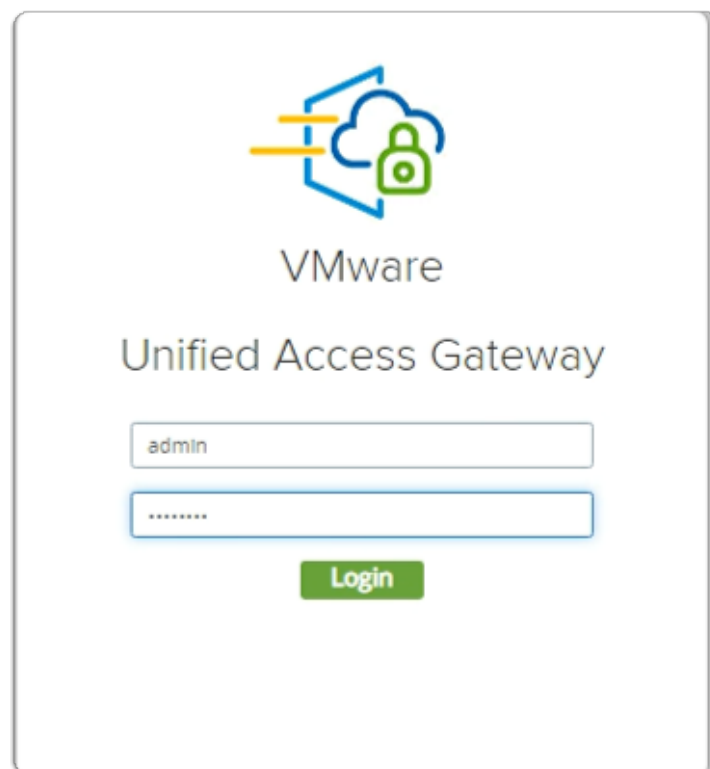
5. In the **Settings** window
  - in the right pane
  - below **SAML Metadata**
    - select & right click **Identity Provider (IdP) metadata**
    - in the **drop down** menu
      - select **Save link as...**

- 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

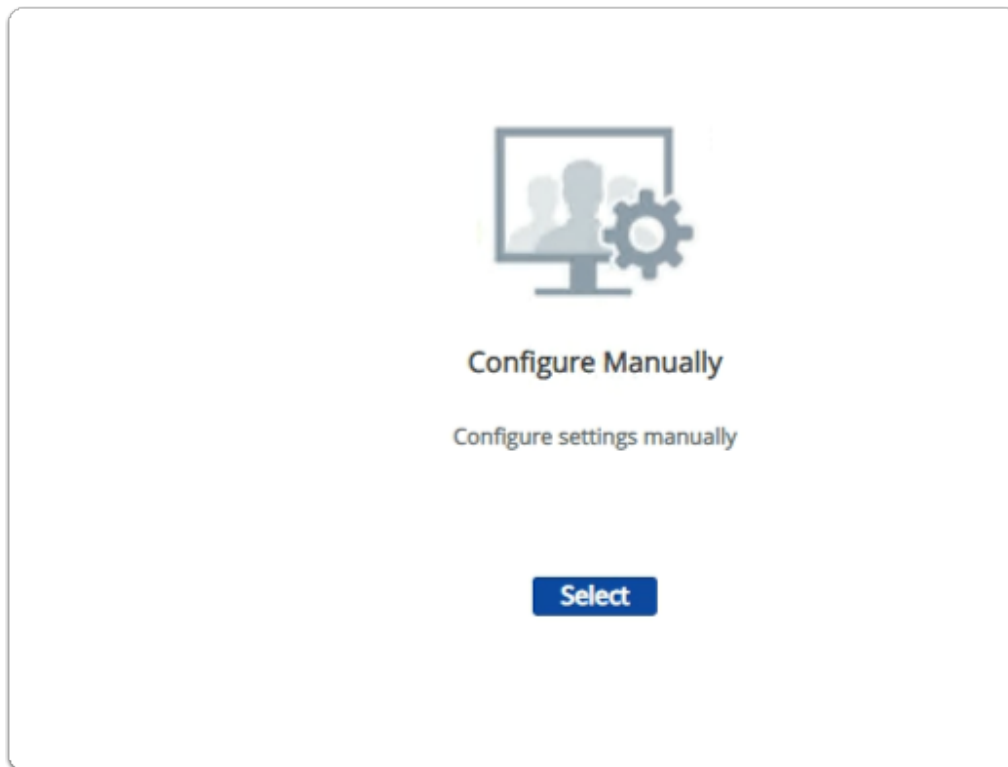


1. On your **Site 1 Browser** profile
  - In the **Favourites bar**
    - select the **UAG-HZN-01a** shortcut

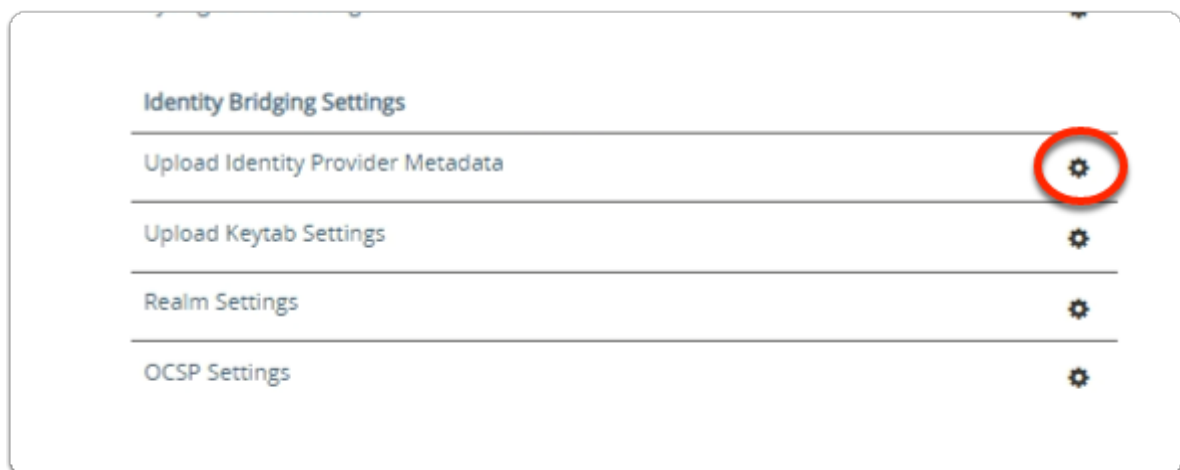


2. In the **VMware Unified Access Gateway** login
  - in the **Username** area
    - enter **admin**
  - in the **Password** area
    - enter **VMware1!**

- 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 ⓘ

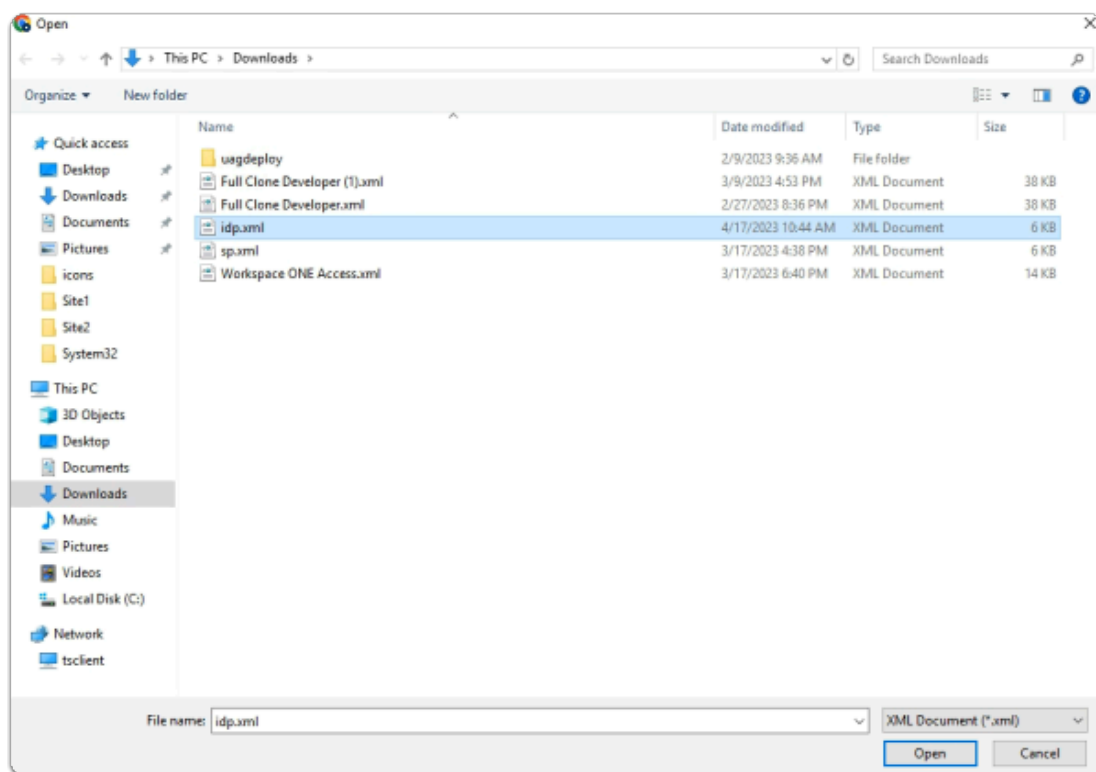
Encryption Certificate Type None ⓘ

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

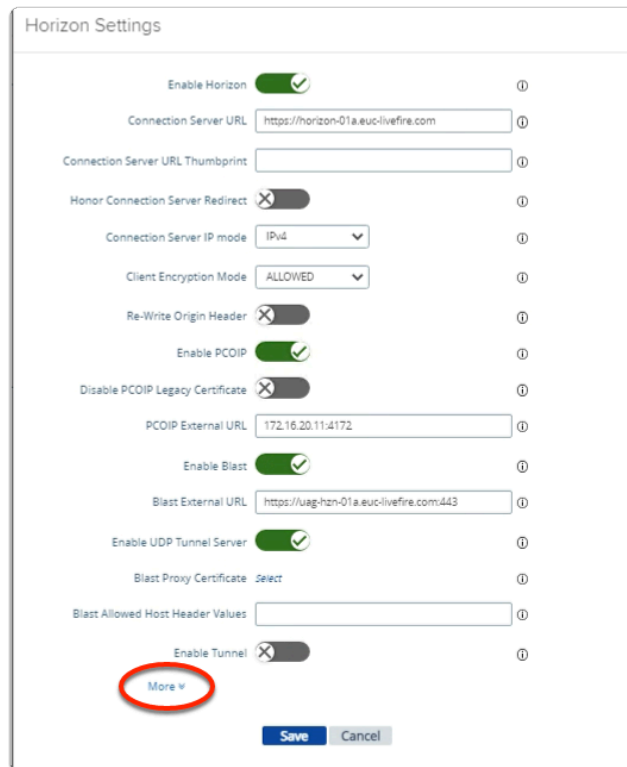
Edge Service Settings ☒ [Refresh](#) *Active Sessions: 0*

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

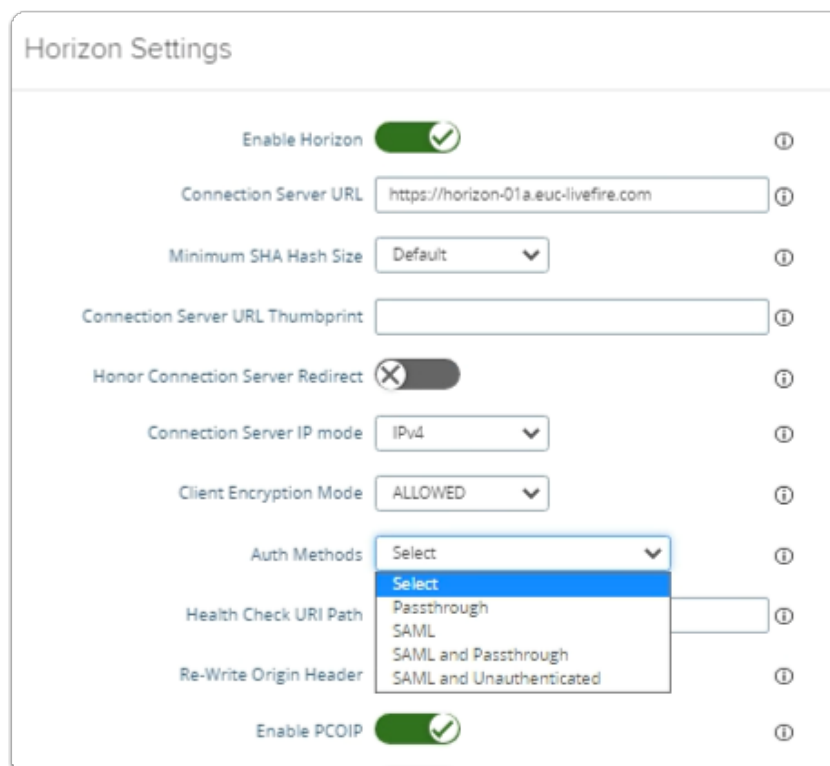
8. In the **VMware Unified Access Gateway** admin console

- 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

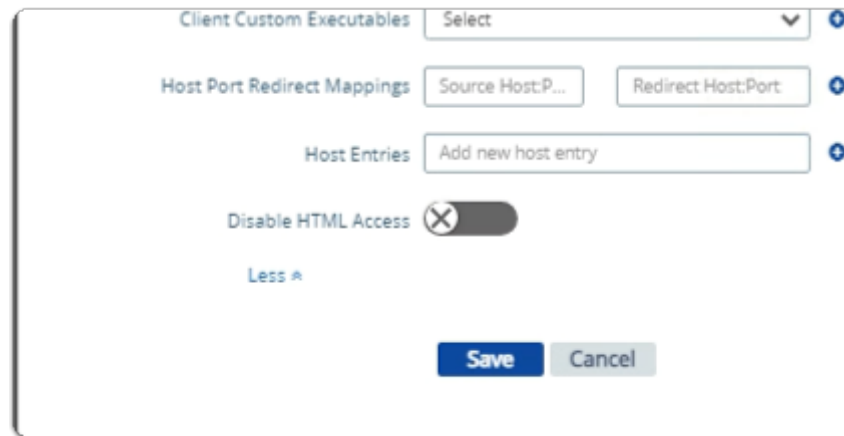
Identity Provider \*: Workspace ONE Access

External Host Name: corp.euc-liveware.com

**Download** Cancel

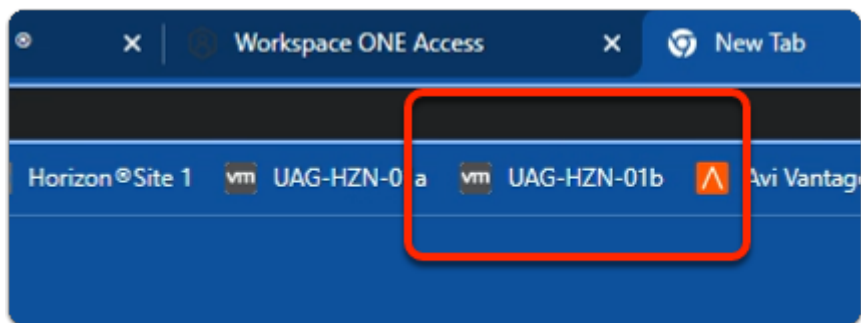
13. In the **Download SAML service provider metadata** window
  - next to **External Host Name**

- enter [corp.euc-livewire.com](https://corp.euc-livewire.com)
- select **Download**

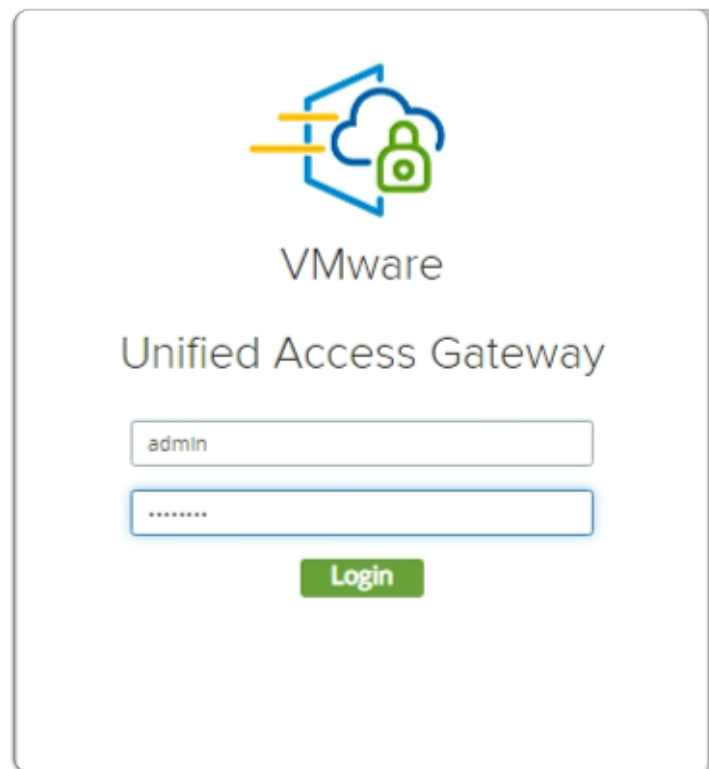


14. In the **Horizon Settings** window
  - **scroll down** to the bottom of the window
  - select **Save**

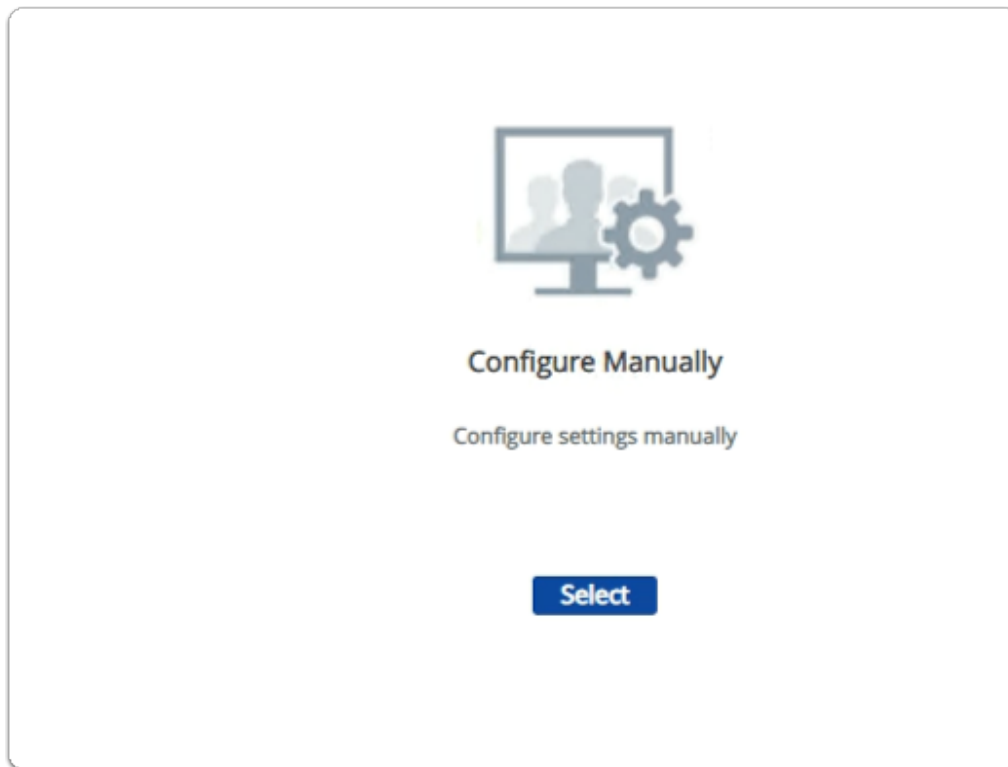
### Step 3. Enabling SAML Federation on Site 1 , UAG-HZN-01b



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 ⓘ

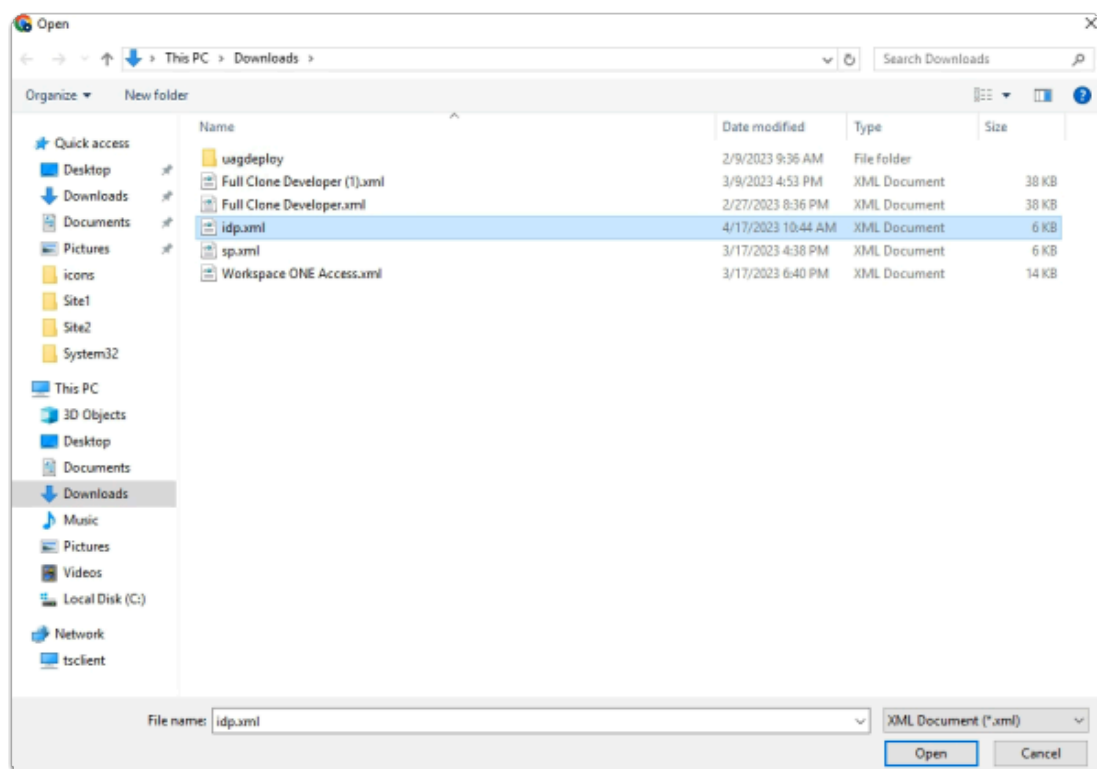
Encryption Certificate Type None ⓘ

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

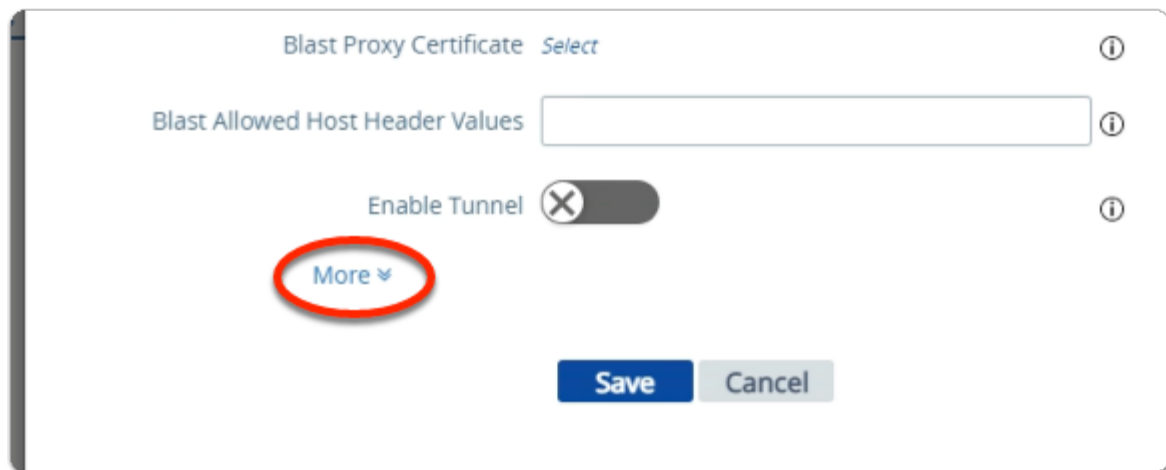
☒ > Horizon Settings ⓘ

☐ Reverse Proxy Settings ⓘ

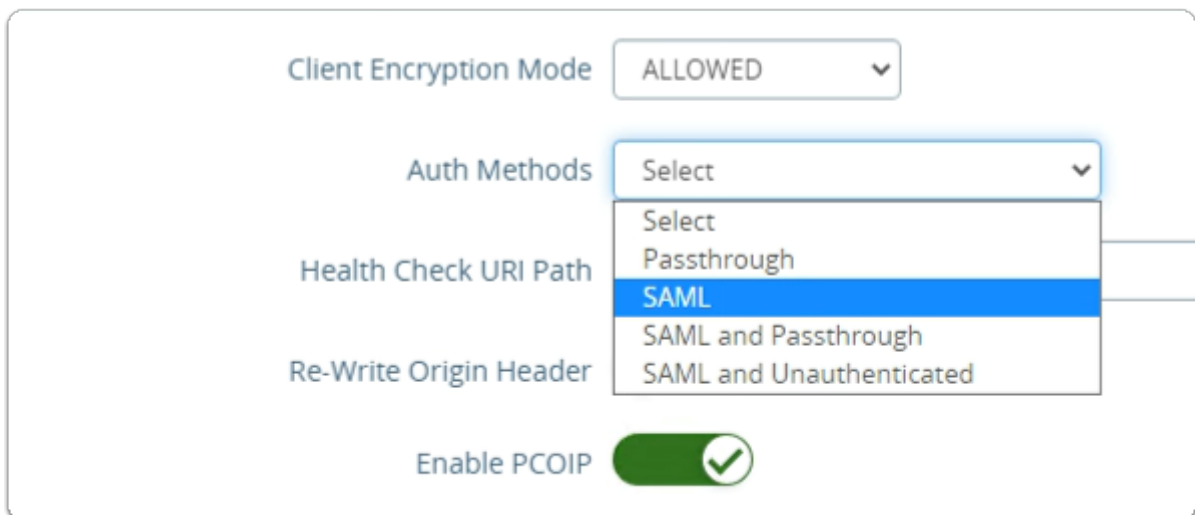
☐ Tunnel Settings ⓘ

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

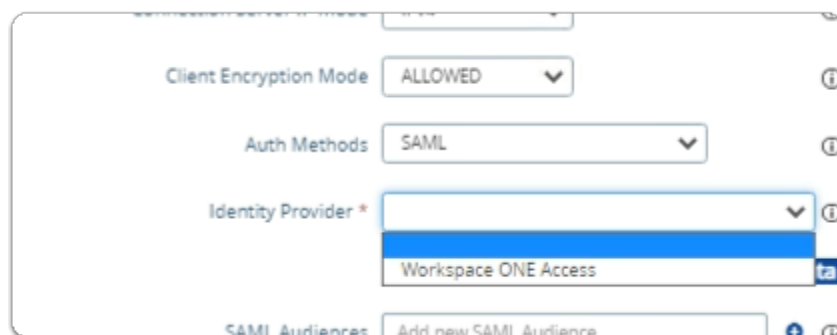
- In the **General Settings** area
  - next to **Edge Service Settings**
    - turn the **TOGGLE** from **OFF** to **ON**
  - to the right of **Horizon Settings**
    - select the **GEAR** icon



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

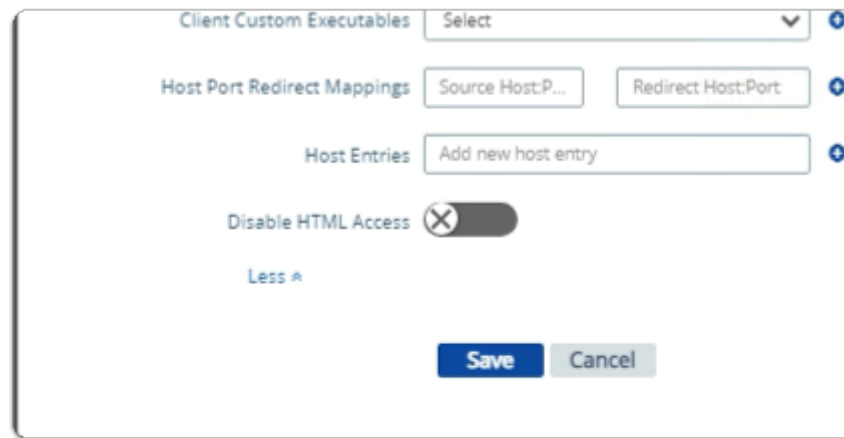


10. In the **Horizon Settings** window
  - next to **Auth Methods**
    - from the **dropdown**
      - select **SAML**



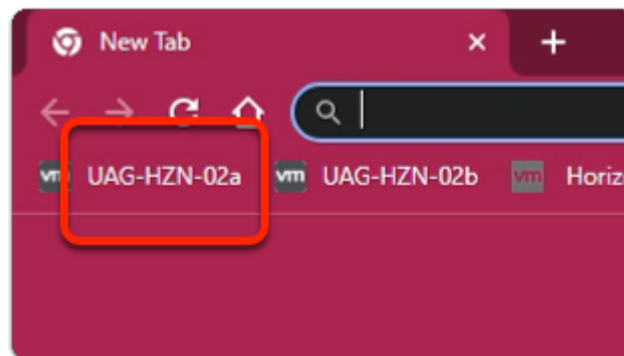


11. In the **Horizon Settings** window
  - below **Auth Methods**
    - next to **Identity Provider\***
      - from the **dropdown**
        - select **Workspace ONE Access**

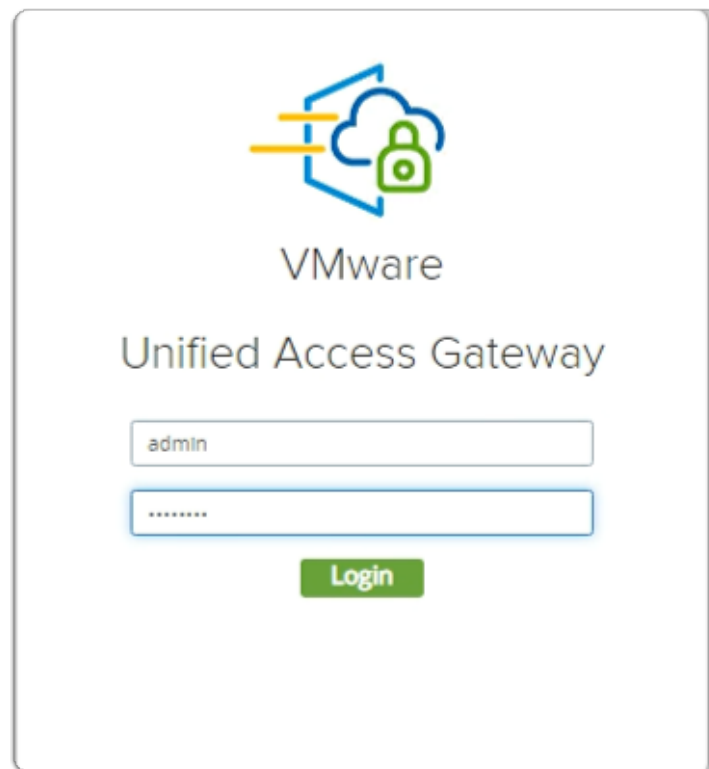


12. In the **Horizon Settings** window
  - **scroll down** to the bottom of the window
  - select **Save**

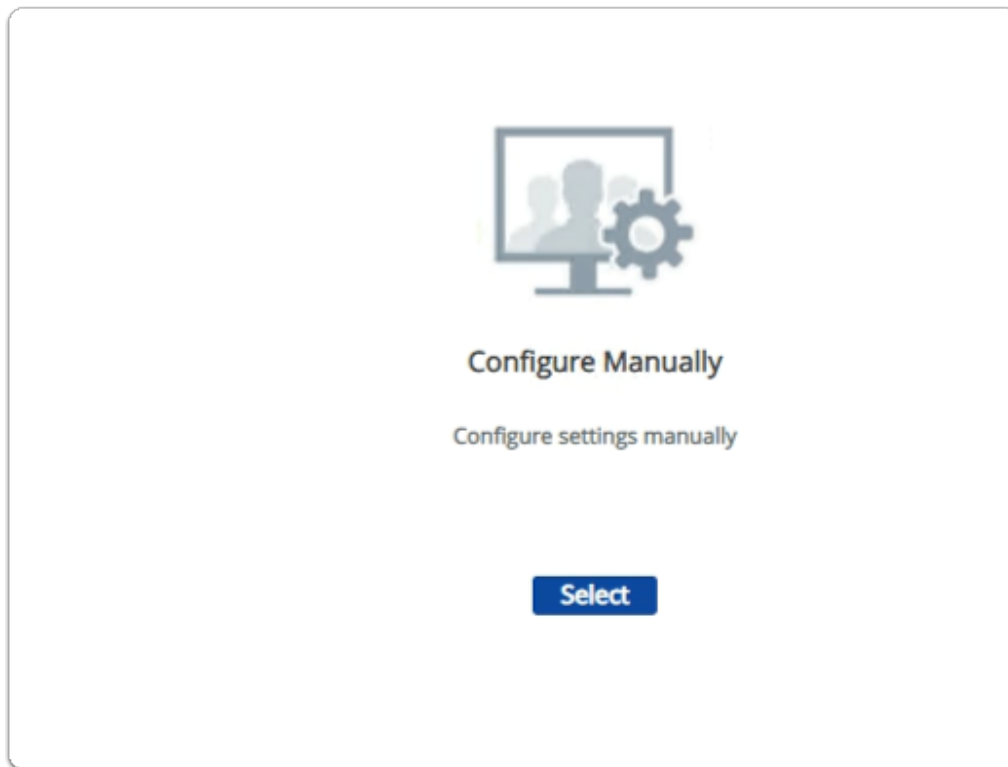
## Step 4. Enabling SAML Federation on Site 2 , UAG-HZN-02a



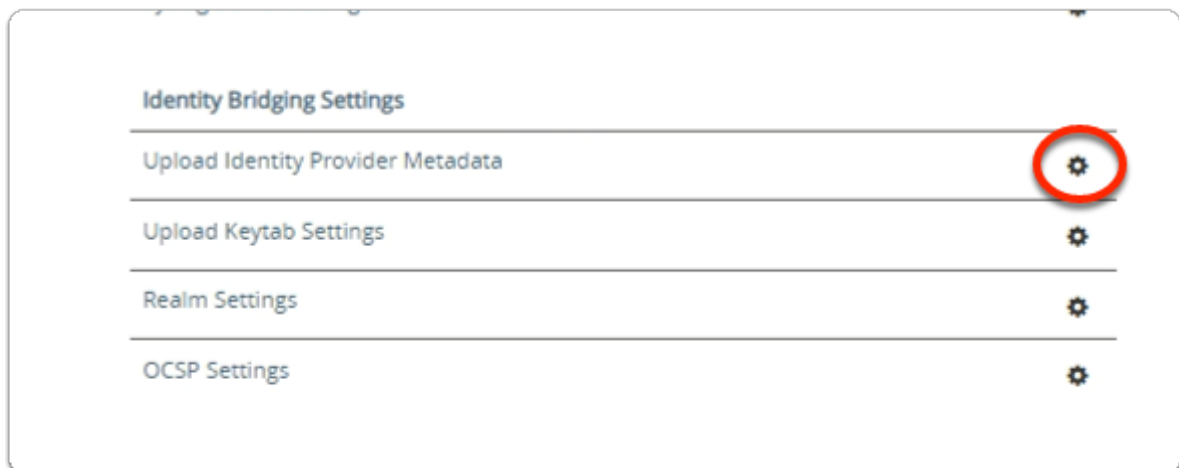
1. On your ControlCenter server
  - switch to your **Site 2 Browser** profile
    - In the **Favourites bar**
      - select the **UAG-HZN-02a** shortcut



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 ⓘ

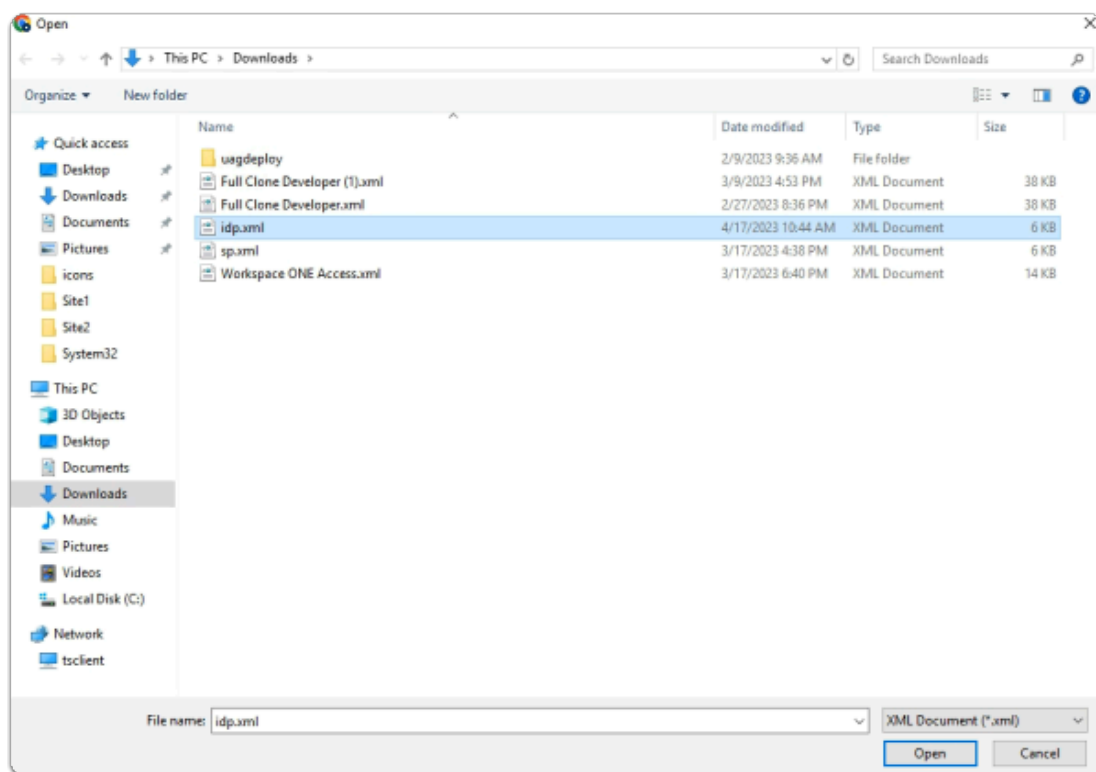
Encryption Certificate Type None ⓘ

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

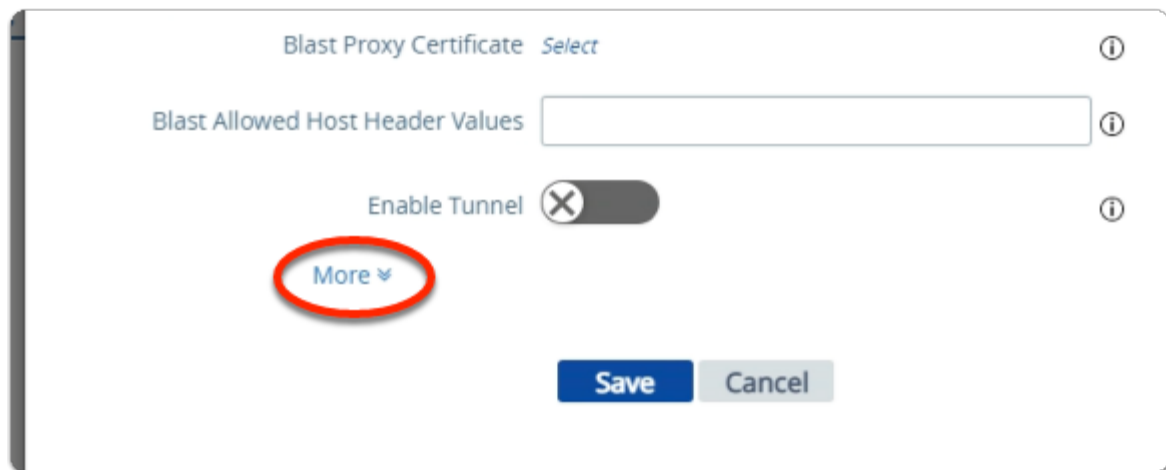
- next to **Always force SAML auth**
  - switch the **Toggle** from **OFF** to **ON**
    - select **Save**
- **scroll** back up to the top of UAG admin console

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

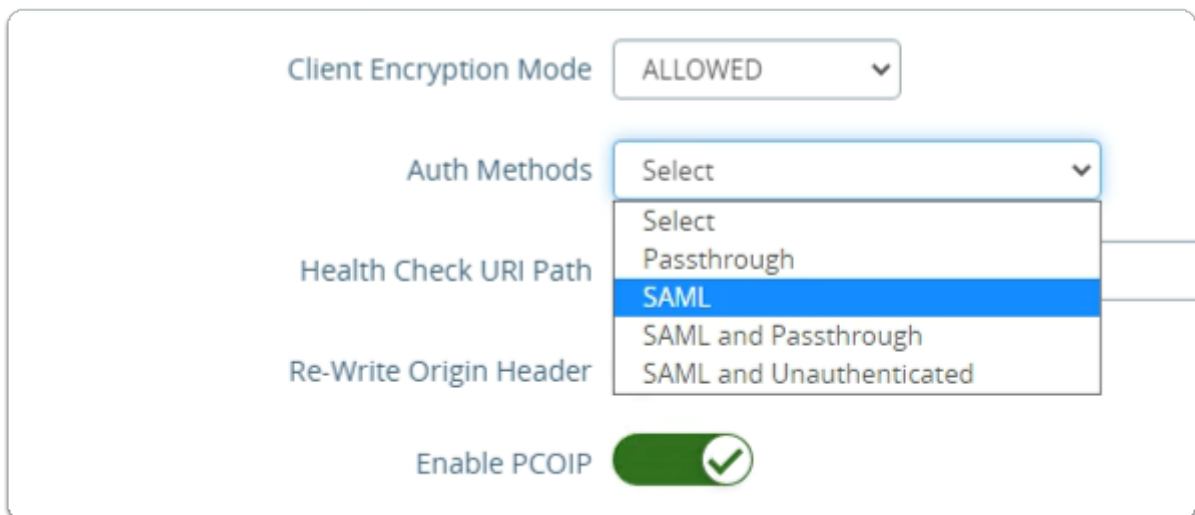
<input checked="" type="radio"/>	<a href="#">Horizon Settings</a>	
<input type="radio"/>	<a href="#">Reverse Proxy Settings</a>	
<input type="radio"/>	<a href="#">Tunnel Settings</a>	

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

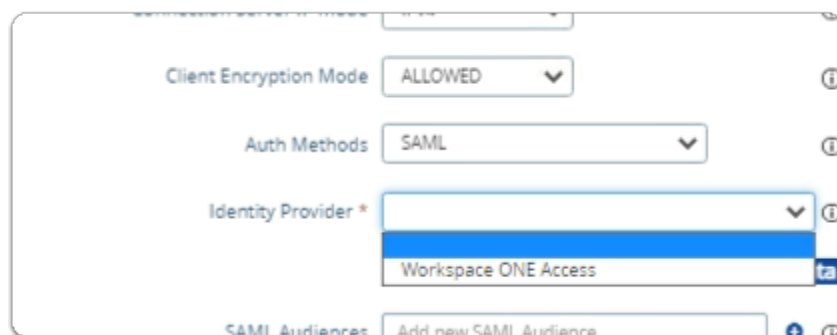
- In the **General Settings** area
  - next to **Edge Service Settings**
    - turn the **TOGGLE** from **OFF** to **ON**
  - to the right of **Horizon Settings**
    - select the **GEAR** icon



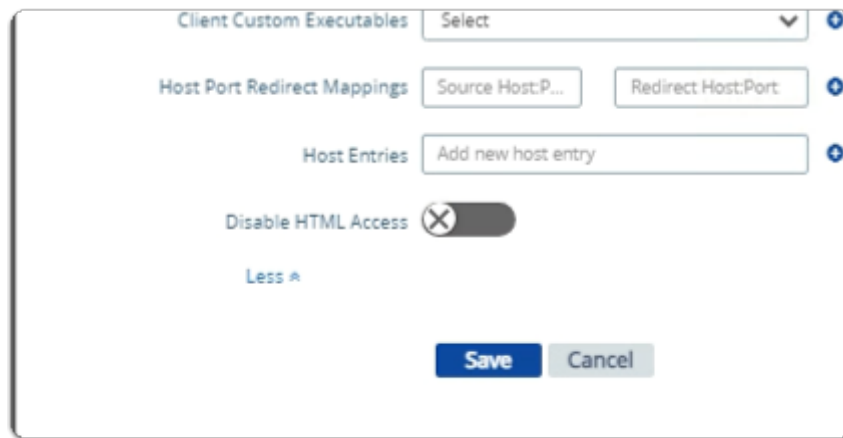
9. In the **Horizon Settings** window
- **scroll** down to the bottom
  - next to **More**
    - select the **expand** icon



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

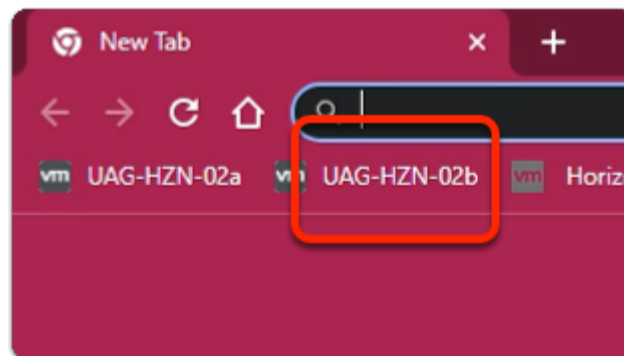


11. In the **Horizon Settings** window
  - below **Auth Methods**
    - next to **Identity Provider\***
      - from the **dropdown**
        - select **Workspace ONE Access**

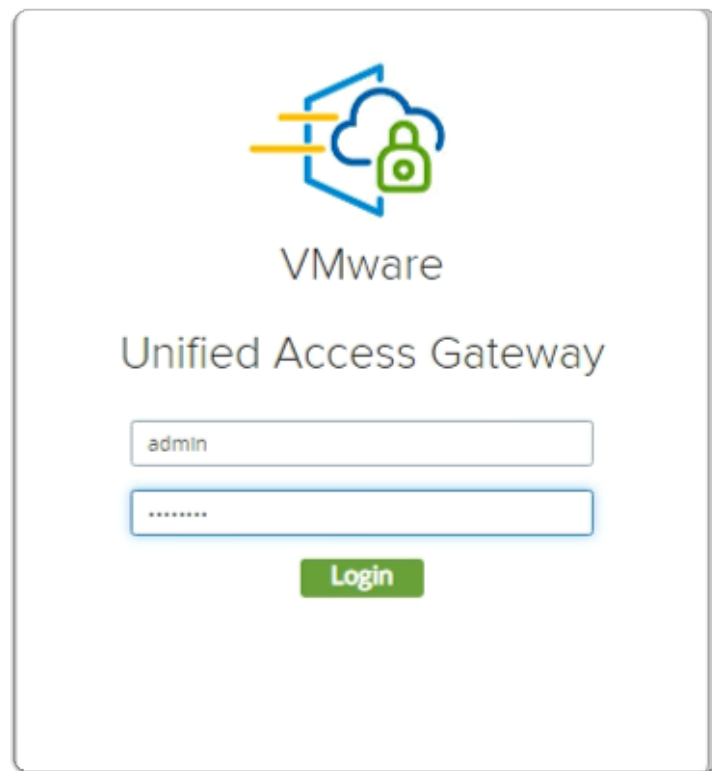


12. In the **Horizon Settings** window
  - **scroll down** to the bottom of the window
  - select **Save**

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

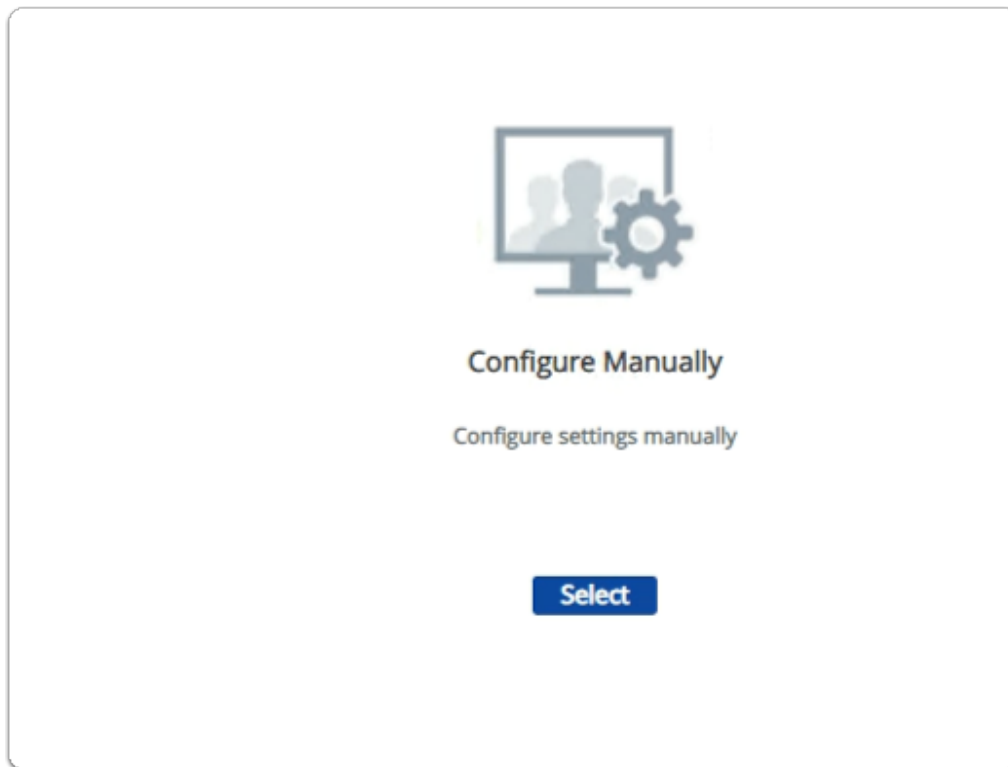


1. On your ControlCenter server
  - on your **Site 2 Browser** profile
    - In the **Favourites bar**
      - select the **UAG-HZN-02b** shortcut

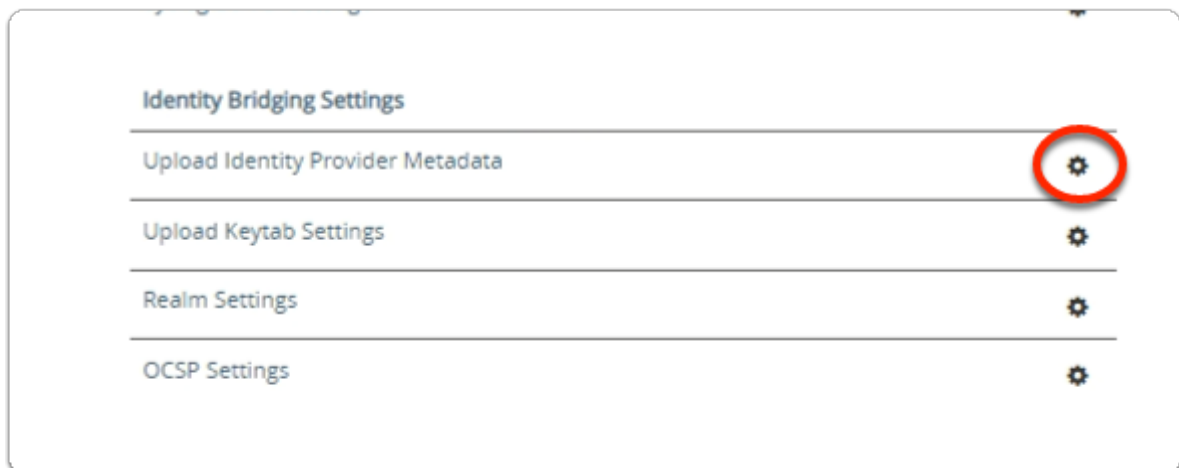


2. In the **VMware Unified Access Gateway** login
  - in the **Username** area
    - enter **admin**
  - in the **Password** area
    - enter **VMware1!**
  - select **Login**





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 ⓘ

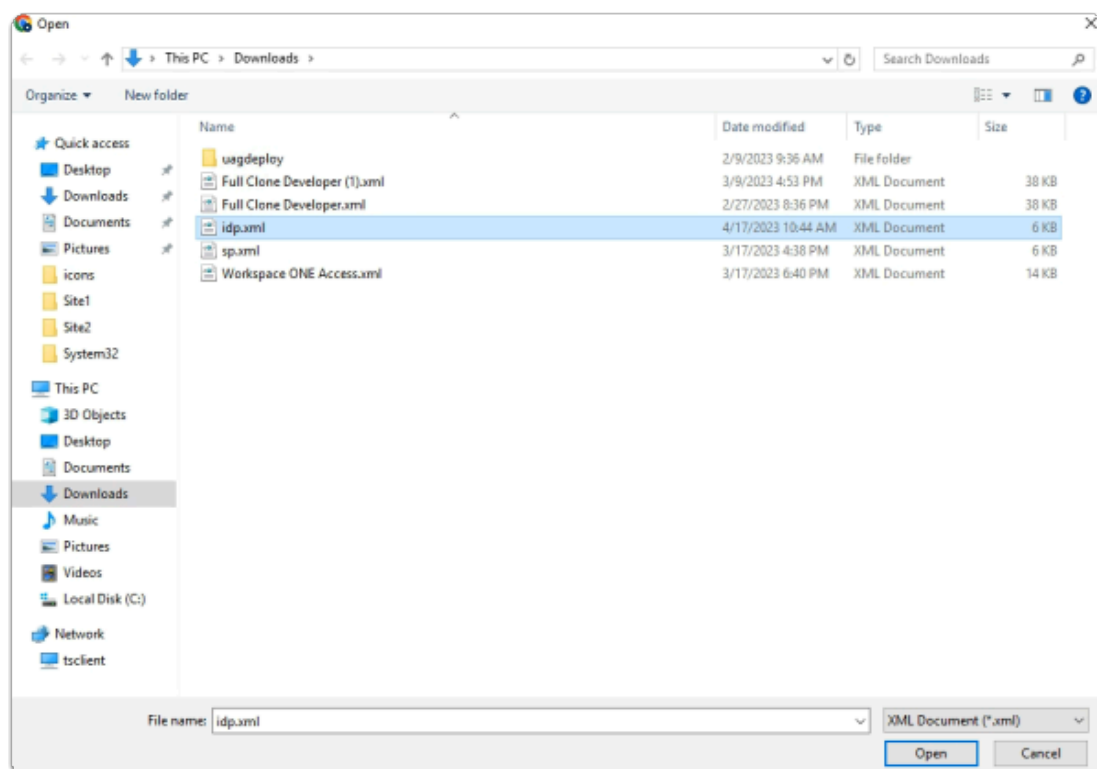
Encryption Certificate Type None ⓘ

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

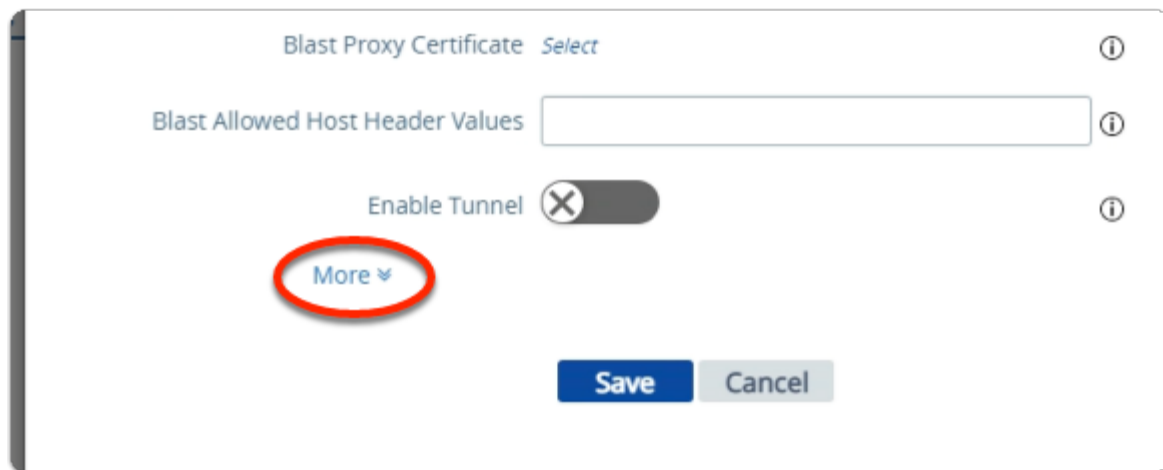
☒ > Horizon Settings ⓘ

☐ Reverse Proxy Settings ⓘ

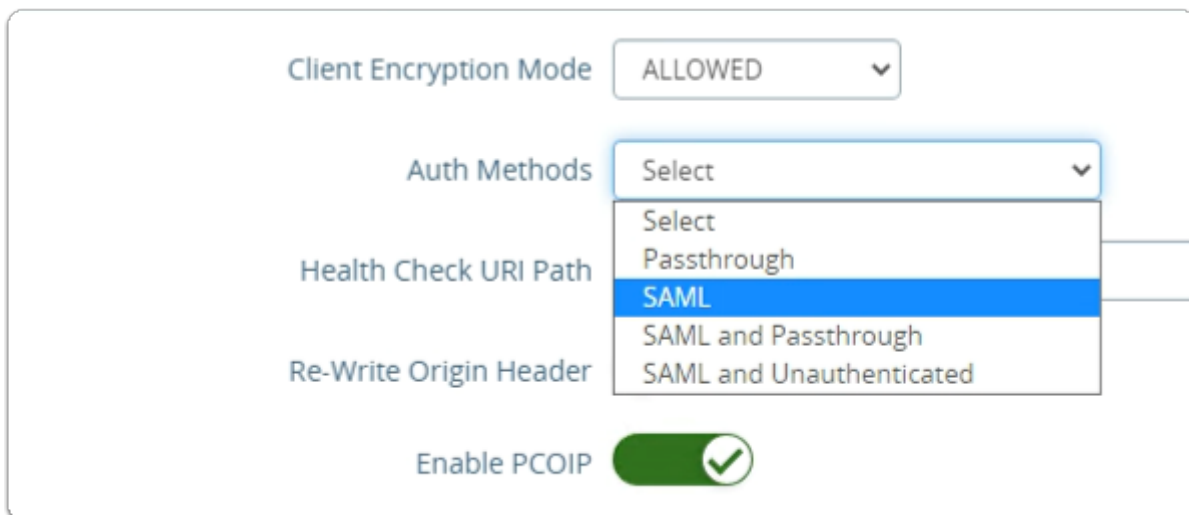
☐ Tunnel Settings ⓘ

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

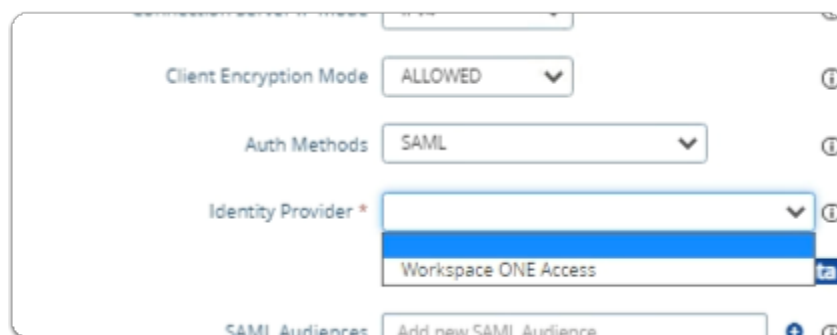
- In the **General Settings** area
  - next to **Edge Service Settings**
    - turn the **TOGGLE** from **OFF** to **ON**
  - to the right of **Horizon Settings**
    - select the **GEAR** icon



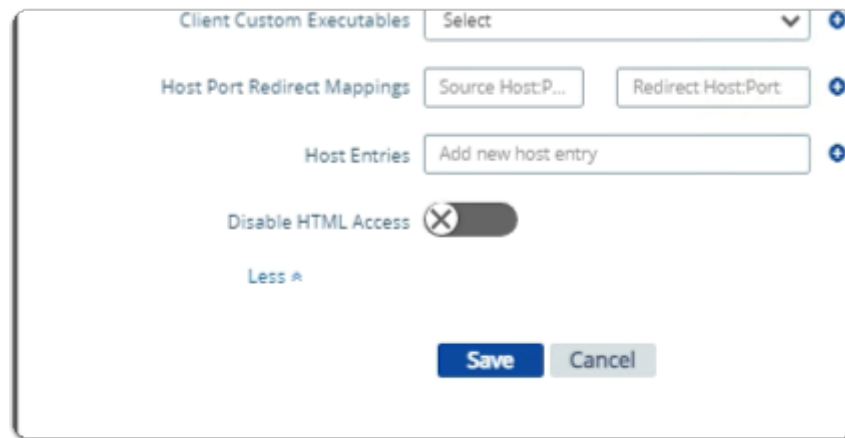
9. In the **Horizon Settings** window
  - **scroll** down to the bottom
  - next to **More**
    - select the **expand** icon



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**

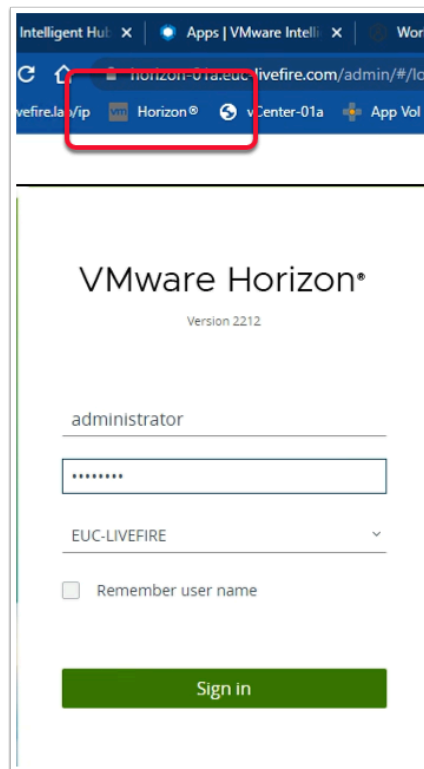


12. In the **Horizon Settings** window
  - **scroll down** to the bottom of the window
  - select **Save**

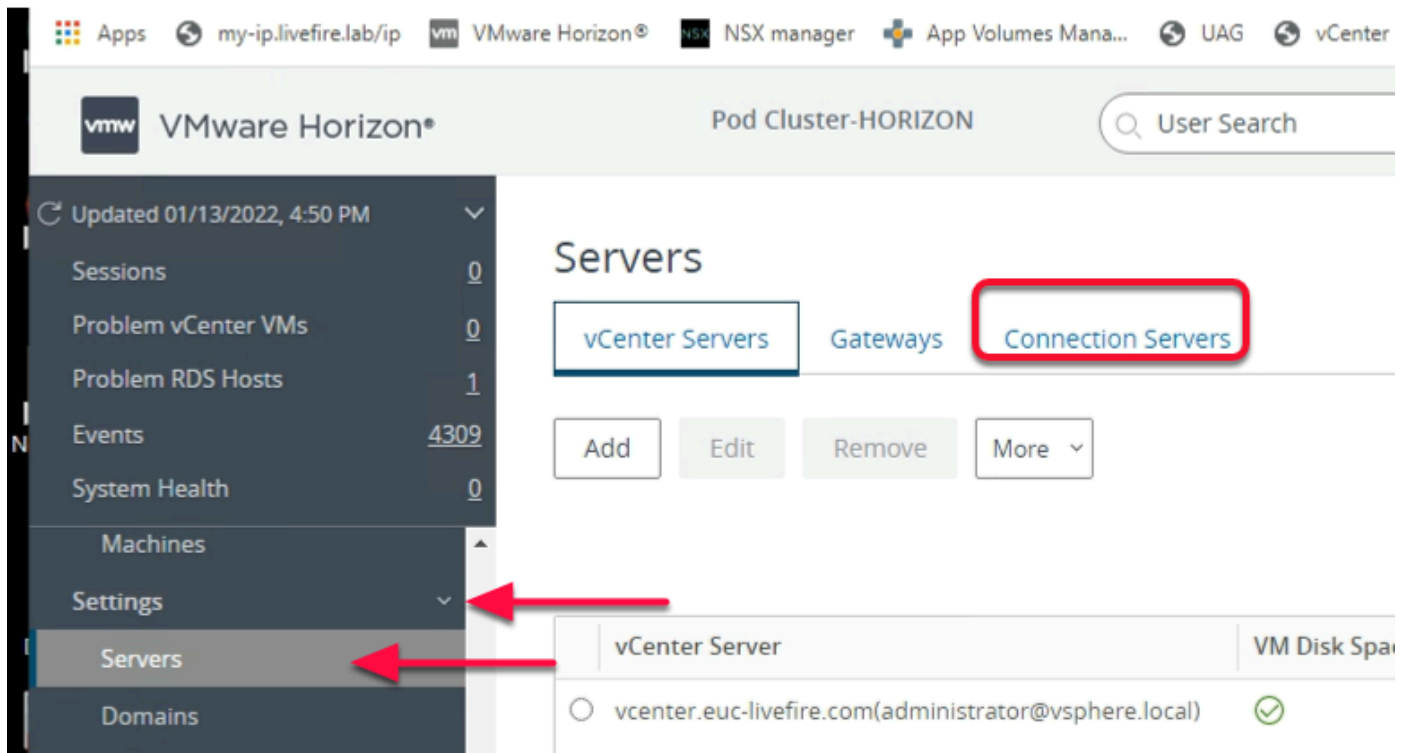
## Part 2. Configuring the SAML Federation for Horizon

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

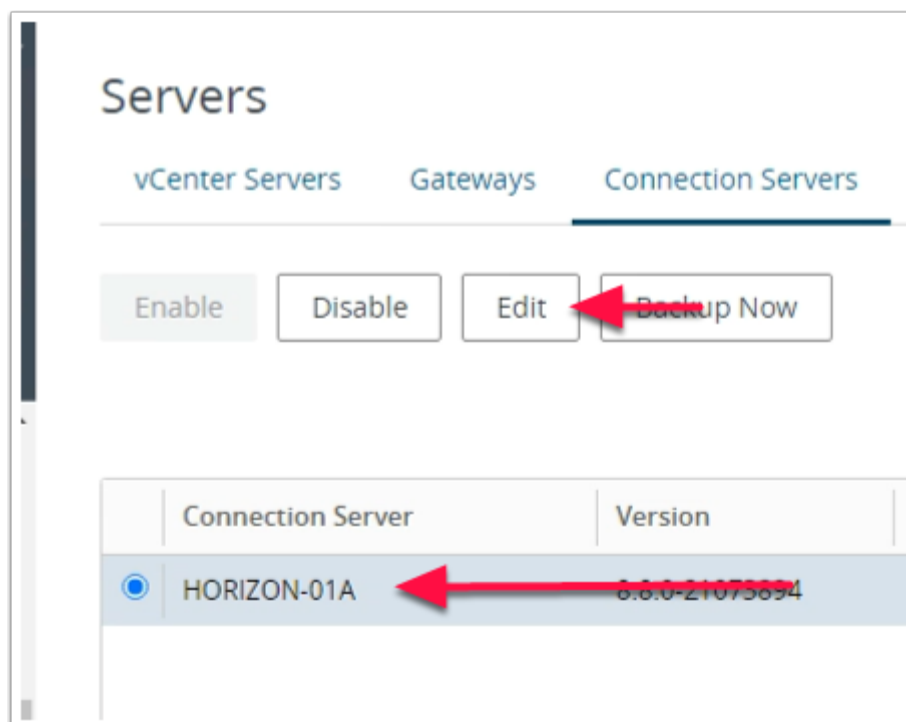


1. On your **ControlCenter** desktop
  - On your Site 1 Chrome Browser
    - Open a **new tab**
  - In the Favourites bar
    - Select the **Horizon shortcut**
  - In the **User Name** area
    - enter **administrator**
  - In the **Password** area
    - enter **VMware1!**
  - Select **Sign in**



## 2. In the Horizon Admin Console

- In the **Inventory**
  - expand **Settings**,
  - select **Servers**
- In the **Servers** area
  - select the **Connection Servers** tab



3. Under **Servers**

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

The screenshot shows the 'Edit Connection Server Settings' page with the 'General' tab selected. The 'Authentication' tab is also visible. Under the 'Tags' section, there is a text input field and a note: 'Tags can be used to restrict which desktop pools can be accessed through this Connection Serv'. Below the input field, it says 'Separate tags with ; or ,'.

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

- Select the **Authentication tab**.

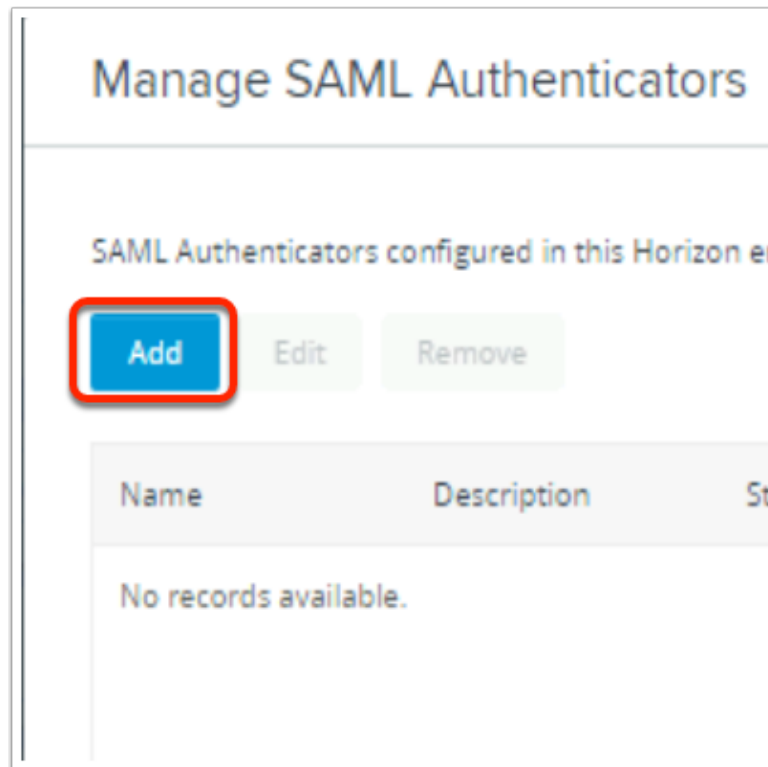
The screenshot shows the 'Edit Connection Server Settings' page with the 'Authentication' tab selected. The 'General' tab is also visible. Under the 'Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):' section, there is a dropdown menu with options: 'Disabled', 'Allowed', and 'Required'. The 'Allowed' option is selected. Below the dropdown, there is a 'Manage SAML Authenticators' button. A red arrow points to this button. Below the button, there is a message: 'No Enabled Authenticator configured'. At the bottom, there is a checkbox for 'Enable Workspace ONE mode' with an information icon.

5. On the **Authentication** tab

- below **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):**
  - On the **Drop down Arrow**
    - Select **Allowed**,



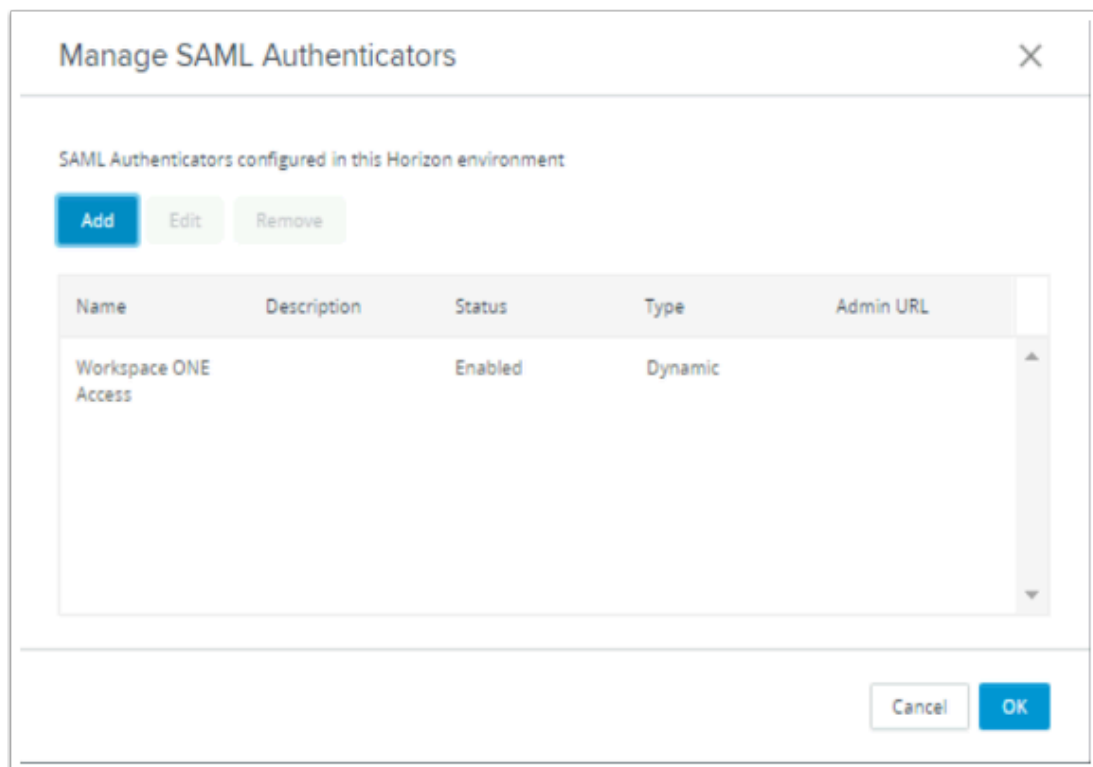
- Select the **Manage SAML Authenticators** box



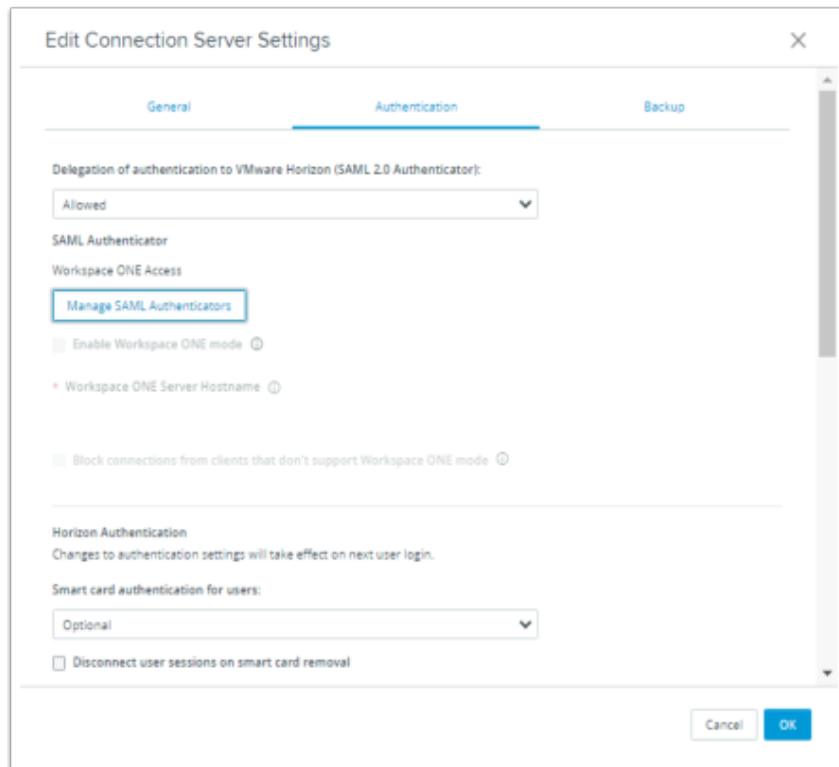
6. On the **Manage SAML Authenticators** box
  - Select **Add**

7. 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](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**



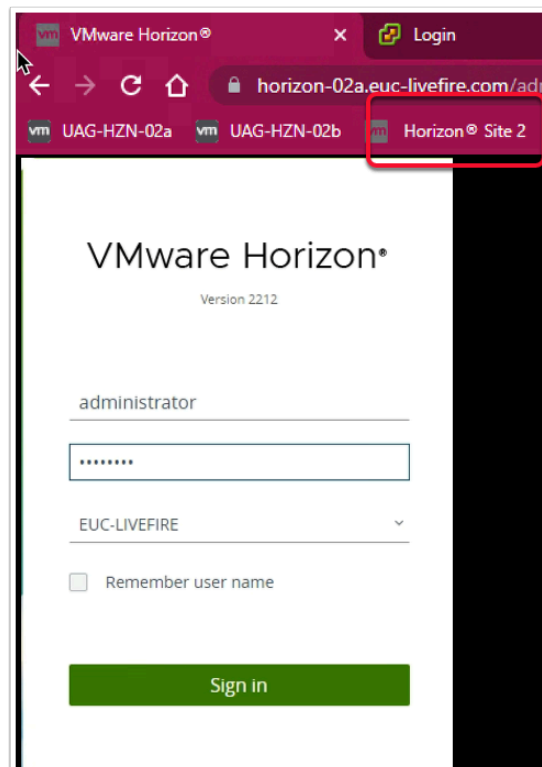
8. In the **Manage SAML Authenticators** window
  - Select **OK** to close



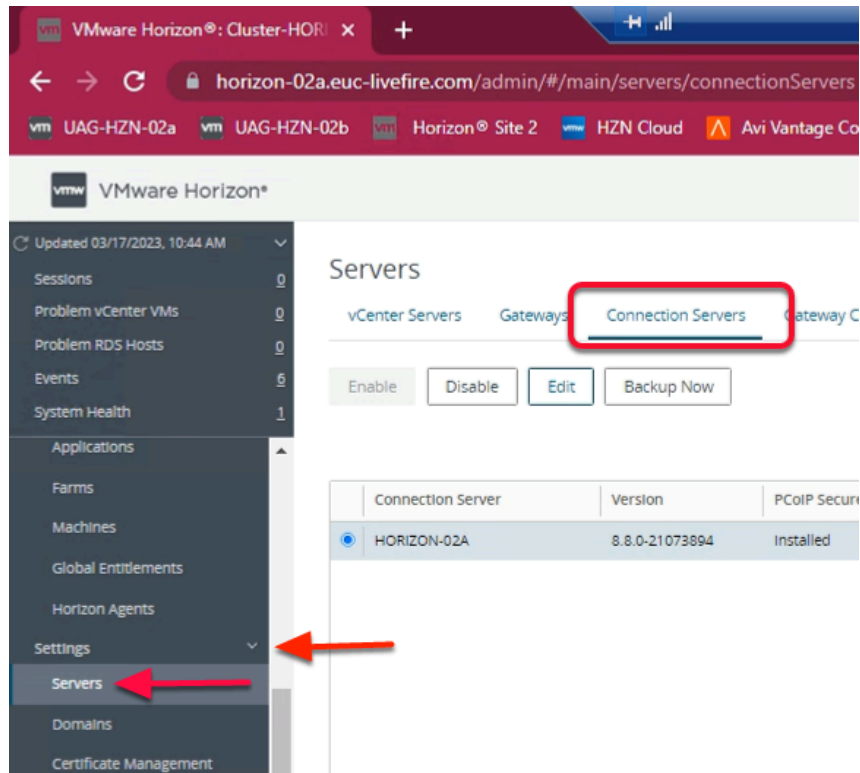
## 9. In the **Connection Server Settings**

- Select **OK**

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

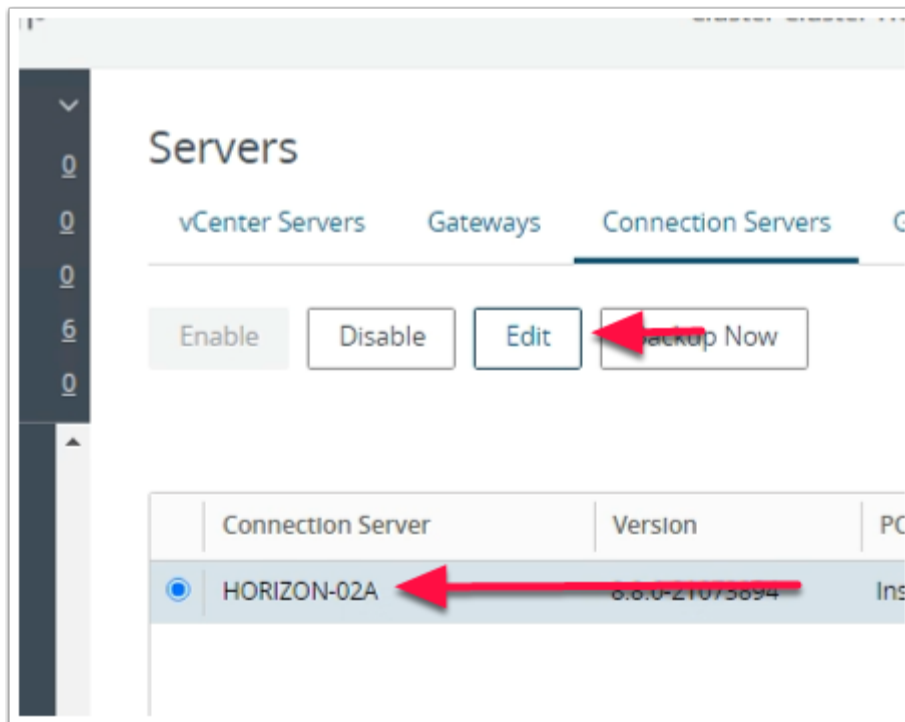


1. On your **ControlCenter** desktop
  - switch to your **Site 2 Chrome browser**
    - Open a **new tab**
  - from the **Favourites bar**
    - select the **Horizon Site 2 shortcut**
  - In the **User Name** area
    - login as **administrator**
  - In the **Password** area
    - type **VMware1!**
  - Select **Sign in**



## 2. In the **Horizon Admin Console**

- Inventory pane
  - expand **Settings**,
  - select **Servers**
- In the middle pane
  - select the **Connection Servers** tab



3. Under **Servers**
  - select the **radio button** to next **HORIZON-02a**
  - select **Edit**

The screenshot shows the 'Edit Connection Server Settings' window with the 'General' tab selected. The 'Tags' section is visible, with a text box for entering tags and a note: 'Tags can be used to restrict which desktop pools can be accessed through this Connection Serv'. Below the text box is a label 'Tags' and a note 'Separate tags with ; or ,'. The 'Authentication' tab is also visible but not selected.

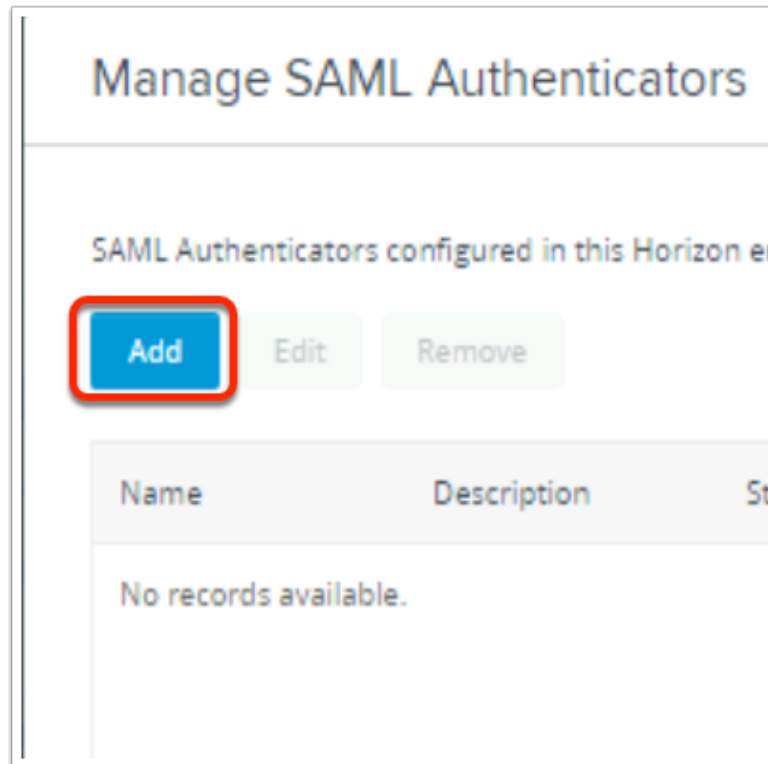
4. On the **Edit Connection Server Settings** page
  - select the **Authentication tab**.

The top screenshot shows the 'Edit Connection Server Settings' window with the 'Authentication' tab selected. The 'Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):' dropdown menu is open, showing options: 'Disabled', 'Allowed', and 'Required'. The 'Allowed' option is selected. Below the dropdown is a button labeled 'Manage SAML Authenticators'.

The bottom screenshot shows the same window with the 'Authentication' tab selected. The 'Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):' dropdown menu is set to 'Allowed'. Below it is the 'SAML Authenticator' section, which includes a 'Workspace ONE Access' section with a button labeled 'Manage SAML Authenticators' and a red arrow pointing to it. Below this is a checkbox for 'Enable Workspace ONE mode' and a text field for 'Workspace ONE Server Hostname'.

5. 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



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

**Add SAML 2.0 Authenticator**

\* Type: ☒ Dynamic ☐ Static

\* Label:

Description:

\* Metadata URL:

Administration URL:

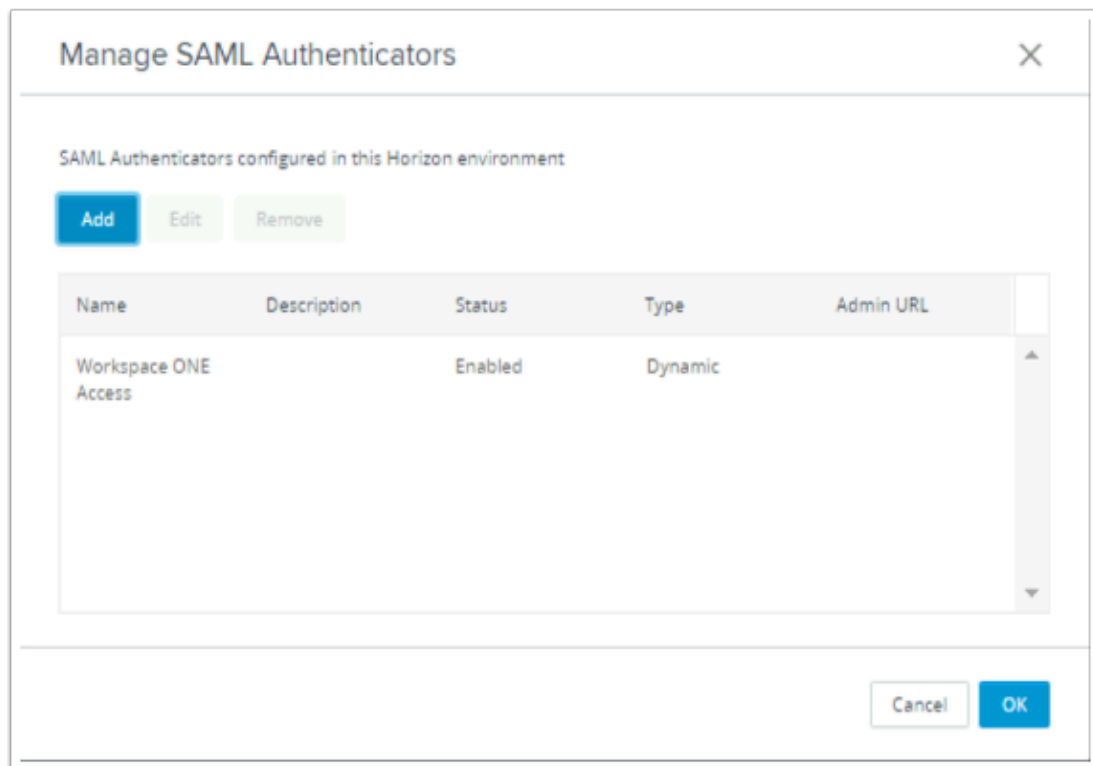
\* TrueSSO Trigger Mode ⓘ:

☒ Enabled for Connection Server

Cancel OK

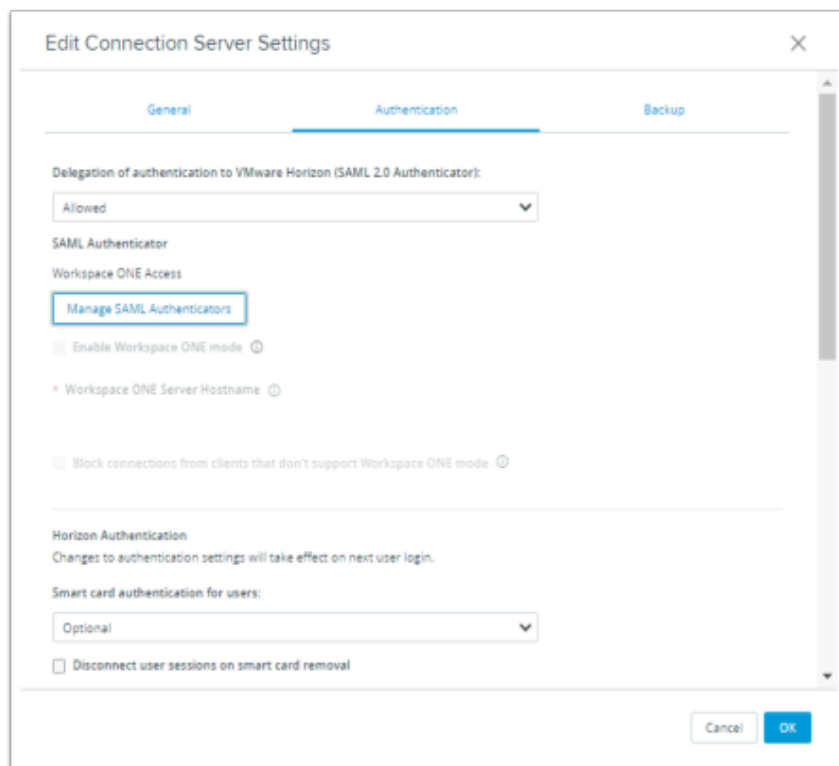
7. In the **Add SAML 2.0 Authenticator** window.
  - ensure **Dynamic** radio button is selected,
  - enter the following:
    - under **Label**:
      - type **Workspace ONE Access**
    - **Under Metadata URL** : enter
      - [https://YOUR\\_CUSTOM\\_Access\\_URL/SAAS/API/1.0/GET/metadata/idp.xml](https://YOUR_CUSTOM_Access_URL/SAAS/API/1.0/GET/metadata/idp.xml)
        - 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**





8. In the **Manage SAML Authenticators** window

- Select **OK** to close



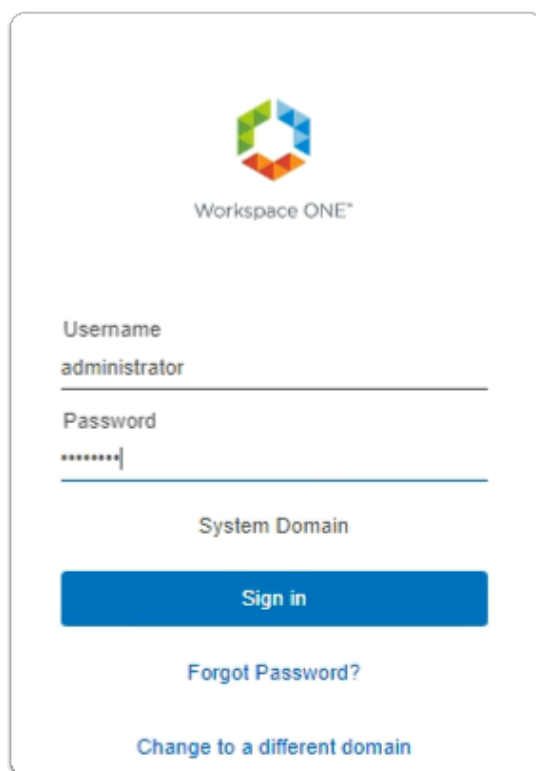
9. In the **Connection Server Settings**

- Select **OK**

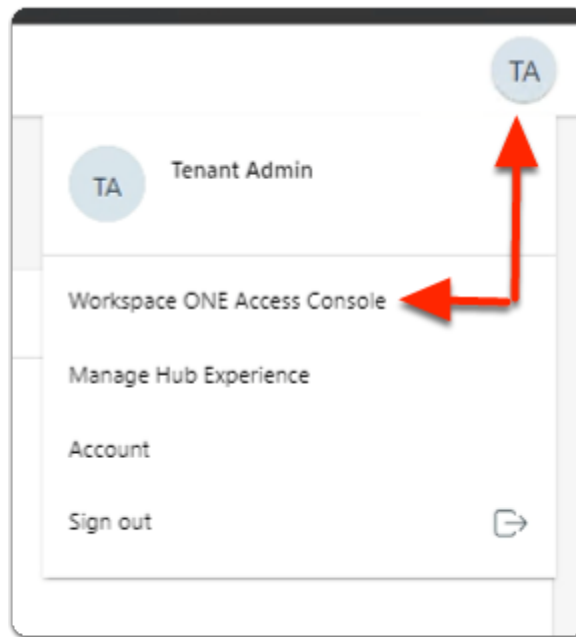
## Part 3. Configuring Workspace ONE Access for VMware Unified Access as the Service Provider

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

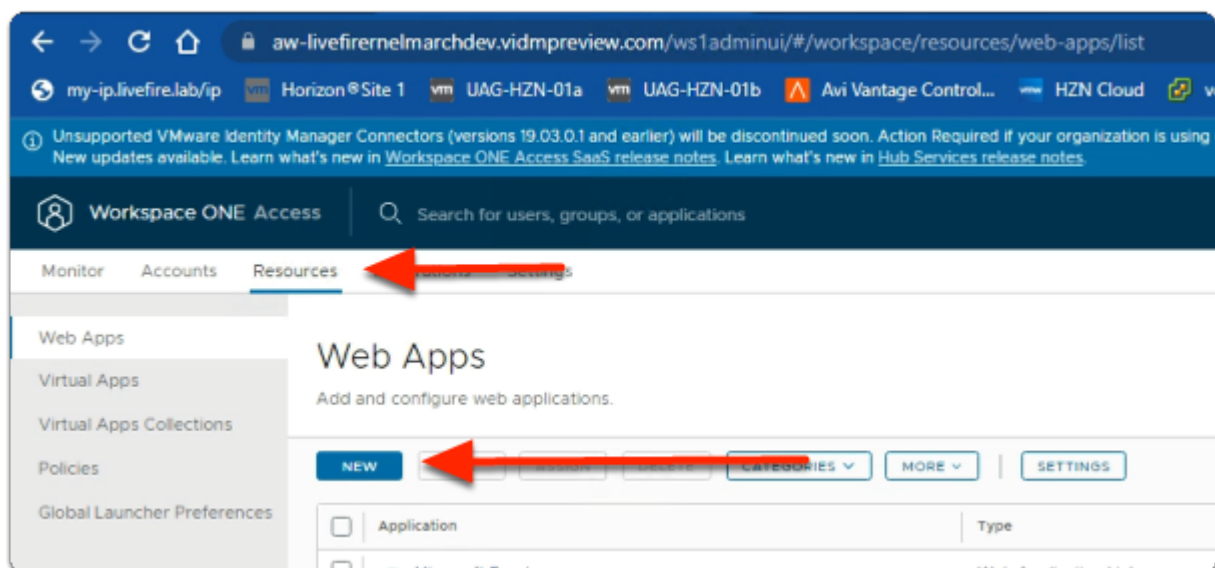


1. On your ControlCenter server
  - Open your **Workspace ONE Access**, Admin console URL
    - Under **Username**
      - enter **Administrator**
    - Under **Password**
      - enter **VMware1!**
    - Select **Sign In**



2. In the **Web Intelligent Hub** Console

- To the right,
  - select **TA**
- From the dropdown
  - select **Workspace ONE Access Console**

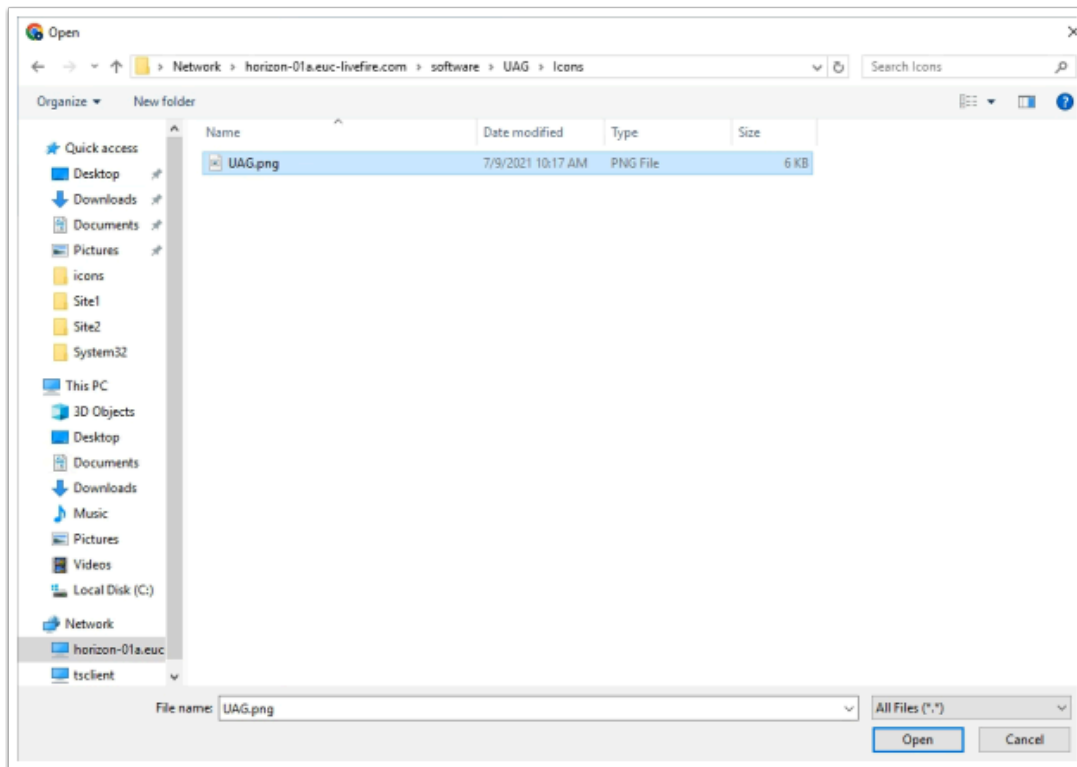


3. In the **Workspace ONE Access Console**

- 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, a sidebar lists four 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, titled 'Definition', contains several input fields: 'Search' with a magnifying glass icon, 'OR BROWSE FROM CATALOG' (a blue link), 'Name' with a red asterisk and an information icon, containing the text 'Unified Access Gateway SAML SP'; 'Description' with an information icon and an empty text box; and 'Icon' with an information icon and a 'SELECT FILE...' button highlighted by a red rectangle. Below the 'Icon' field is a cloud icon with an upward arrow.

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

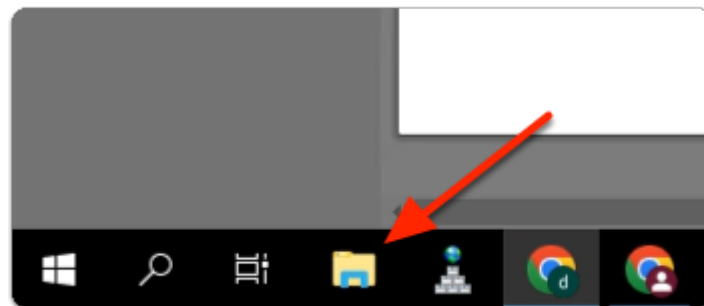
Category ⓘ

Selected Categories

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

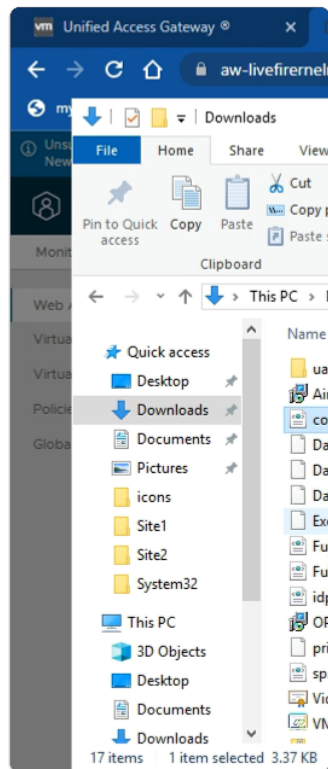
1. In the **Definition** area

- Select **NEXT**

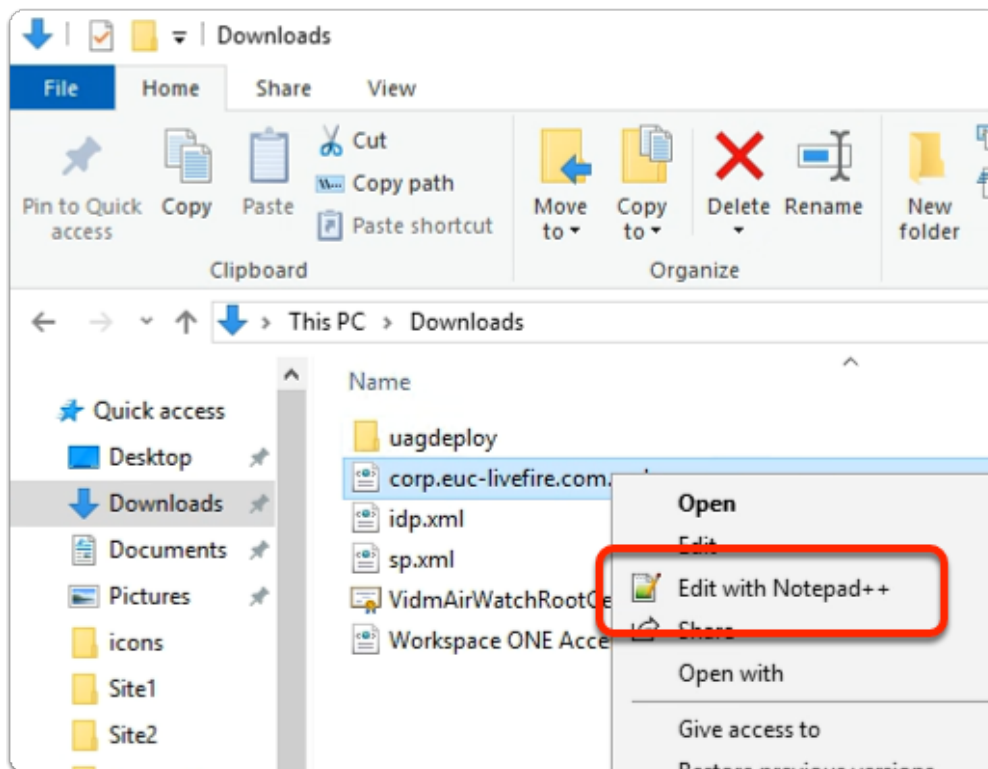


7. On the **ControlCenter** server

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

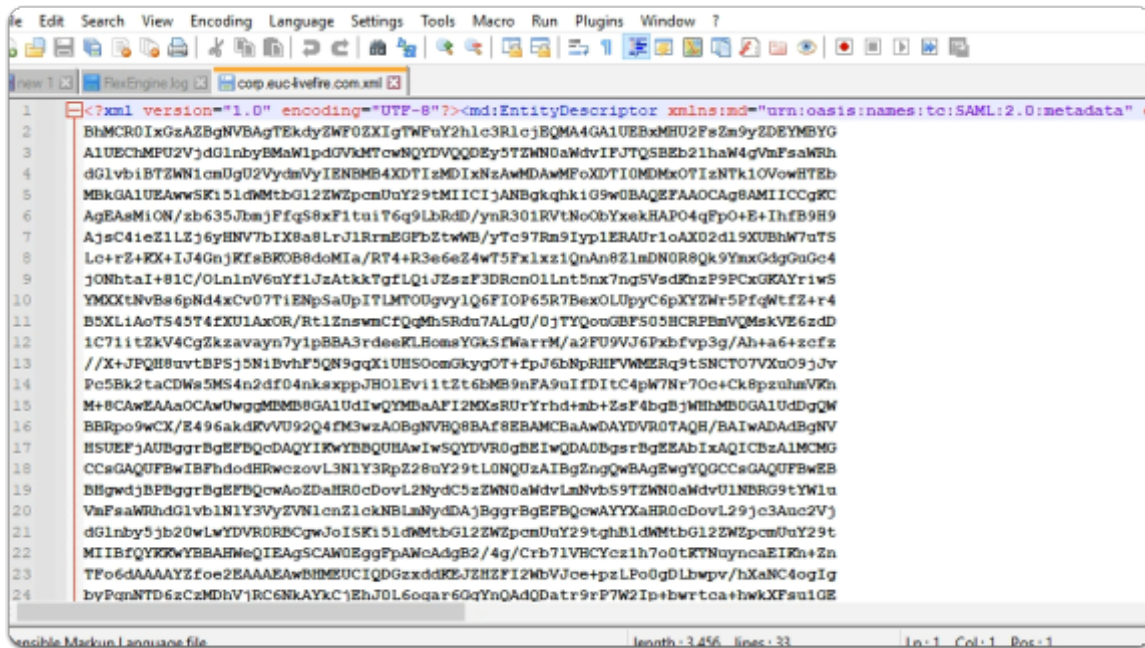


8. In the **File Explorer** window
  - from the **Quick Access** pane
    - select **Downloads**



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

- select **corp.euc-livfire.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 ⓘ  
`<binding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST ArtifactLocation=https://corp.euc-livefire.com/portal/samlsoo/index?0= isDefault=true"/><md:AssertionConsumerService Binding=urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST Location=https://corp.euc-livefire.com/portal/samlsoo/index?1"/></md:SPSSODescriptor></md:EntityDescriptor>`

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**

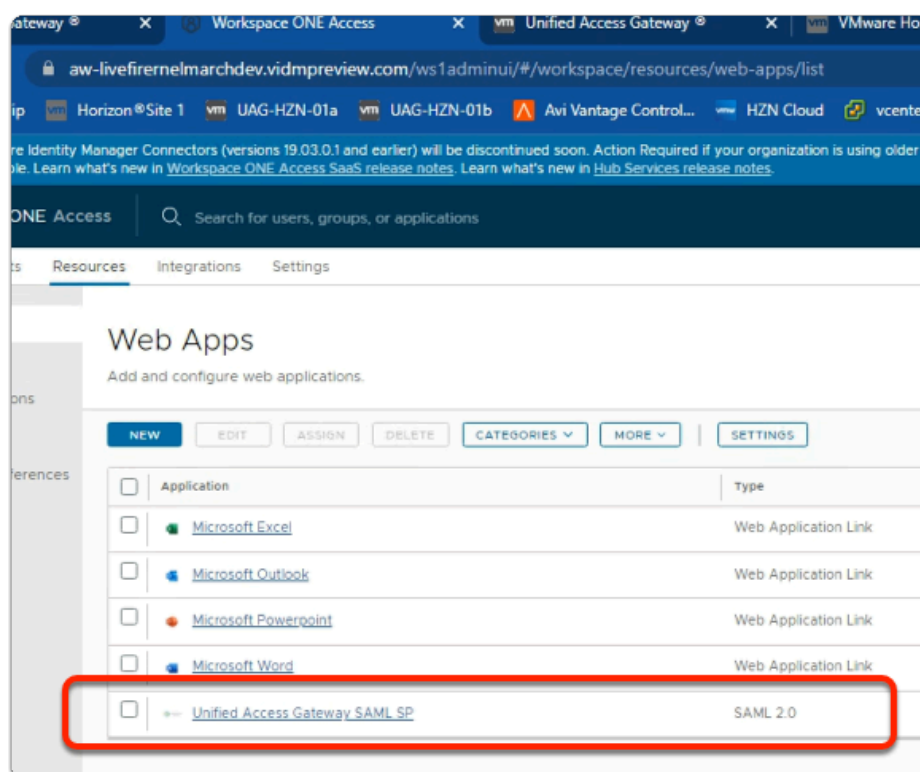
The screenshot shows a web interface titled "New SaaS Application" with a close button (X) in the top right corner. On the left, there is a vertical sidebar with four steps: "1 Definition", "2 Configuration", "3 Access Policies" (which is highlighted with a blue bar), and "4 Summary". The main content area is titled "Access Policies" and contains the text: "Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below." Below this text is a dropdown menu with the text "default\_access\_policy\_set" and a downward arrow. At the bottom right of the window, there are three buttons: "CANCEL", "BACK", and "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 **Marketing@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**



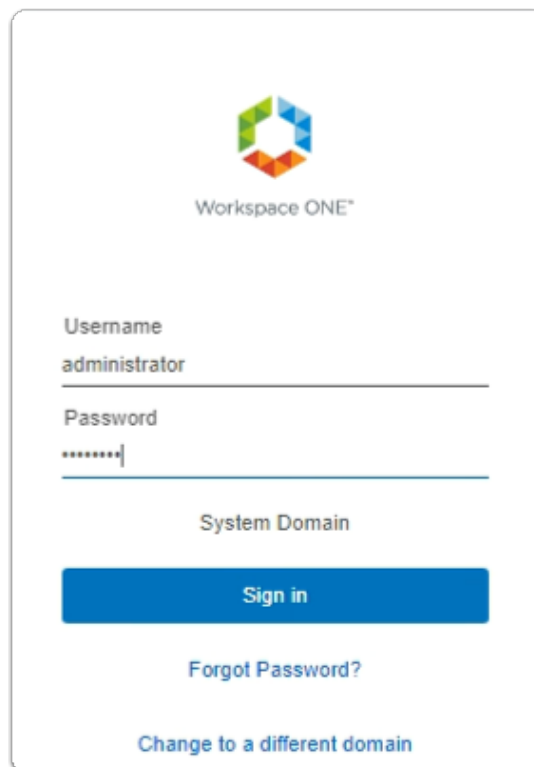
15. In your **Workspace ONE Access** Console
  - **Web Apps** interface
    - Note your **Unified Access Gateway SAML SP Web APP**

## 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 Entitlement

A screenshot of the Workspace ONE login interface. 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) surrounding a white center. 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  
\*\*\*\*\*

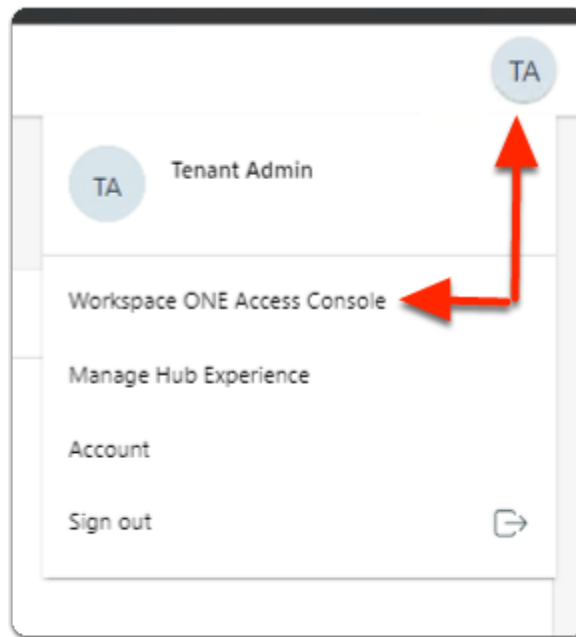
System Domain

Sign in

Forgot Password?

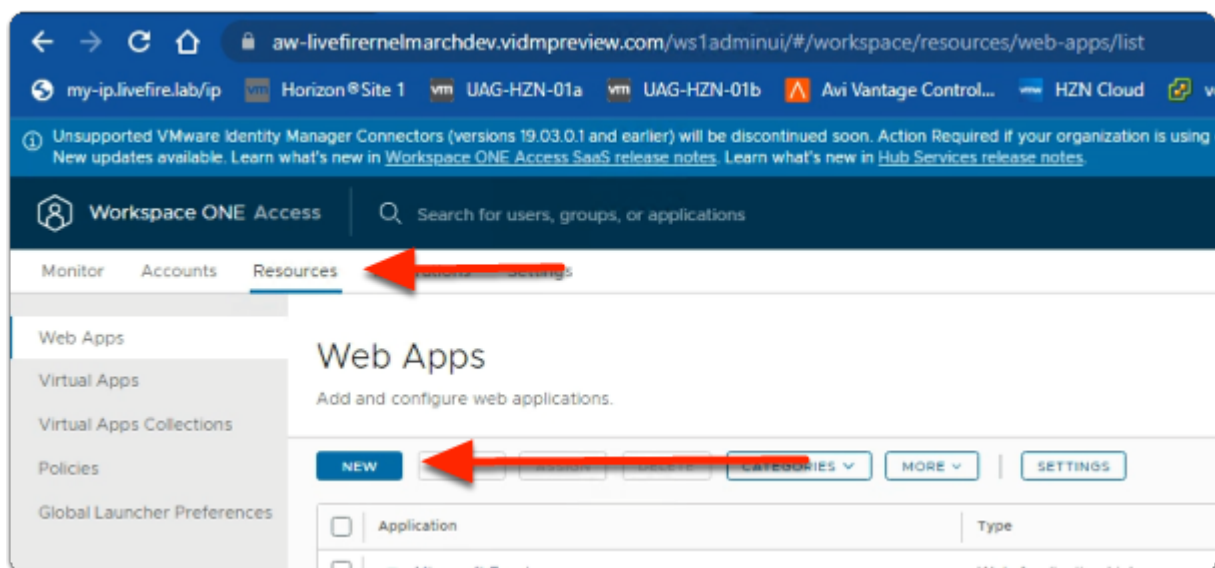
Change to a different domain

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** ⓘ

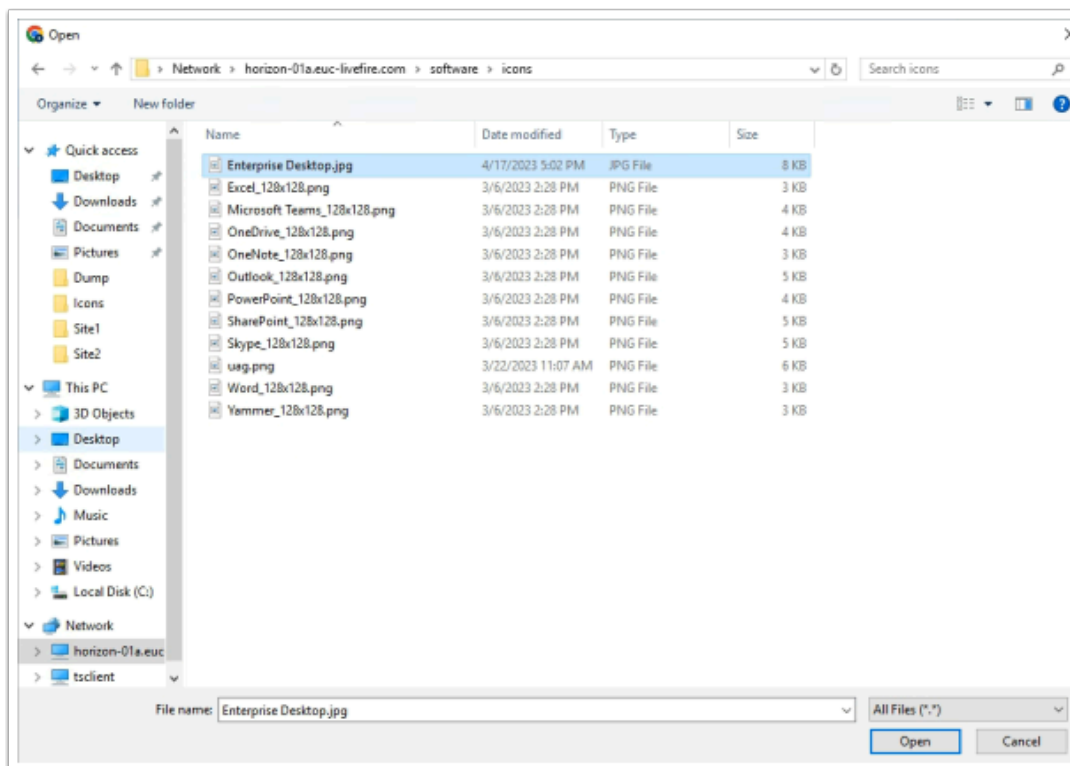
**Icon** ⓘ

**SELECT FILE...**

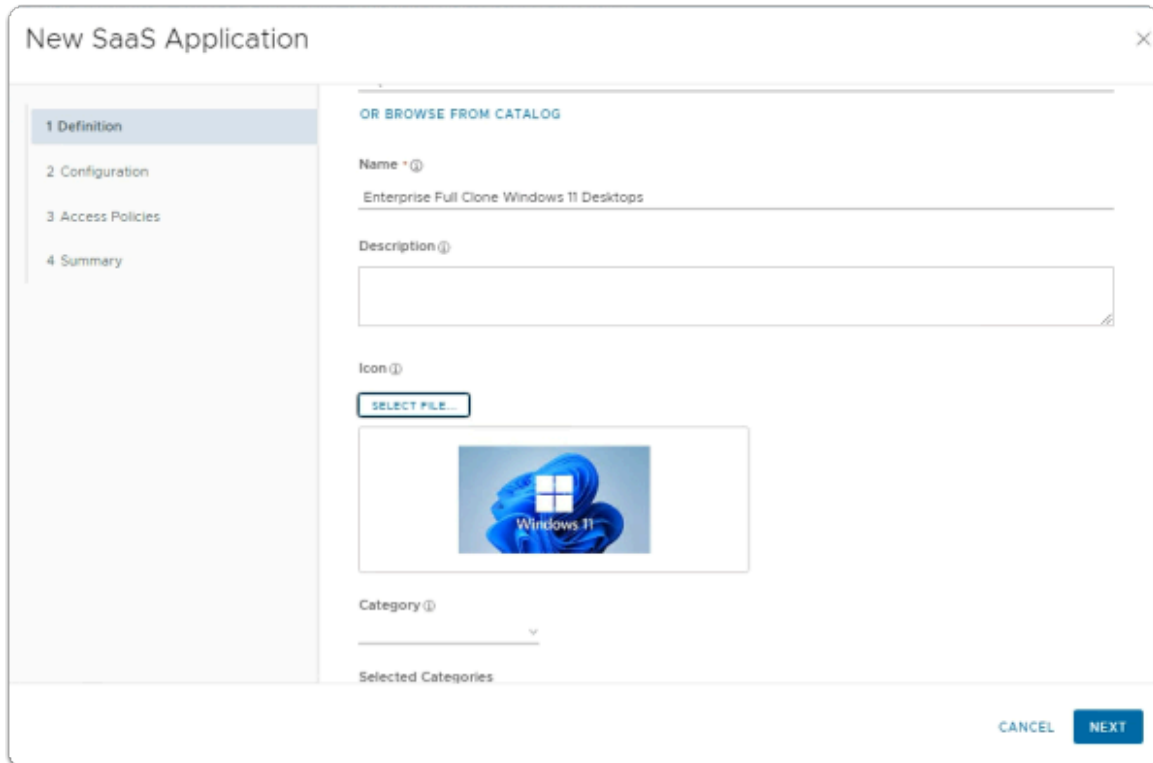
5. In the **New SaaS Application** window

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 desktop.
- Category** (optional): A dropdown menu.
- Selected Categories**: A list of selected 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](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 navigation tabs (1 Definition, 2 Configuration, 3 Summary) and a main content area. The 'Definition' section includes fields for Name (Enterprise Full Clone Windows 11 Desktops), Description, Icon, and Categories. The 'Configuration' section includes Authentication Type (None) and Target URL (https://corp.euc-liveware.com/portal/nativeclient/Enterprise\_Desktop?action=start-session&desktopProtocol=BLAST&launchMinimized=false). 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 with the 'Users / User Groups' section. The 'Selected App(s)' is 'Enterprise Full Clone Windows 11 Desktops'. Below this, there is a search bar with 'dev' entered. A red arrow points to the search bar. Below the search bar, there is a list of users. The first user is 'Developers@euc-liveware.com'. A red arrow points to this user. Below the user list, there is a table with columns 'Deployment Type' and 'Entitlement Type'. The first row shows 'Automatic' and 'Include'. 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

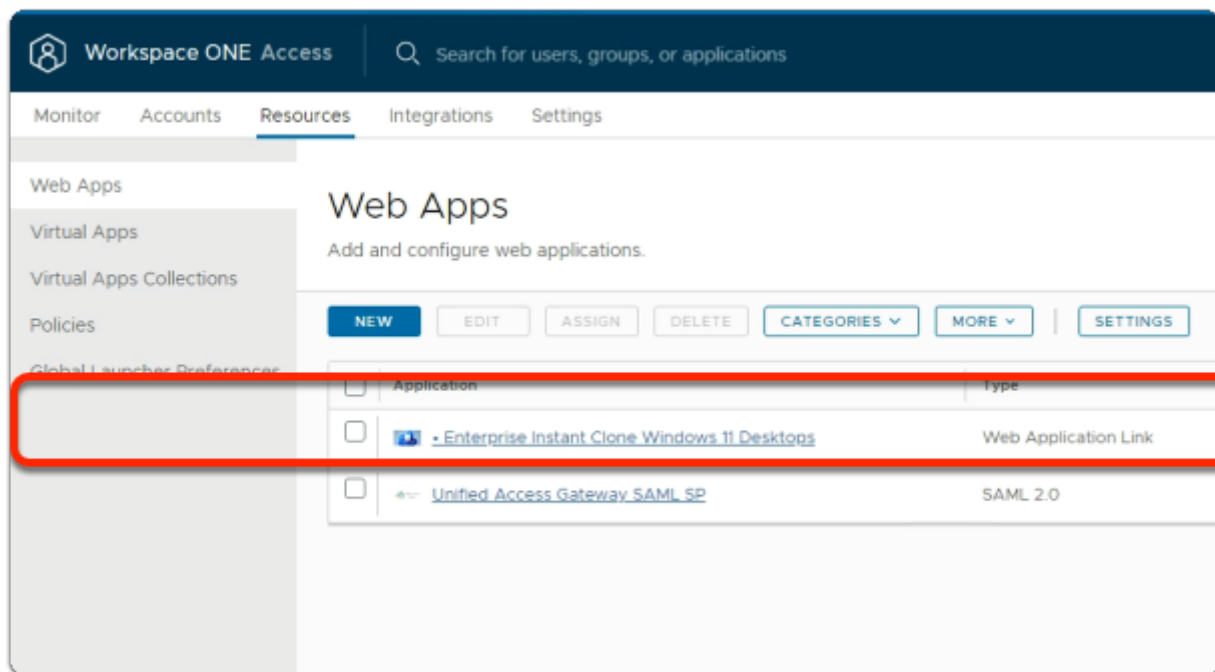
Sales@euc-livewire.com

Automatic

CANCEL SAVE

12. In the **Assign** window

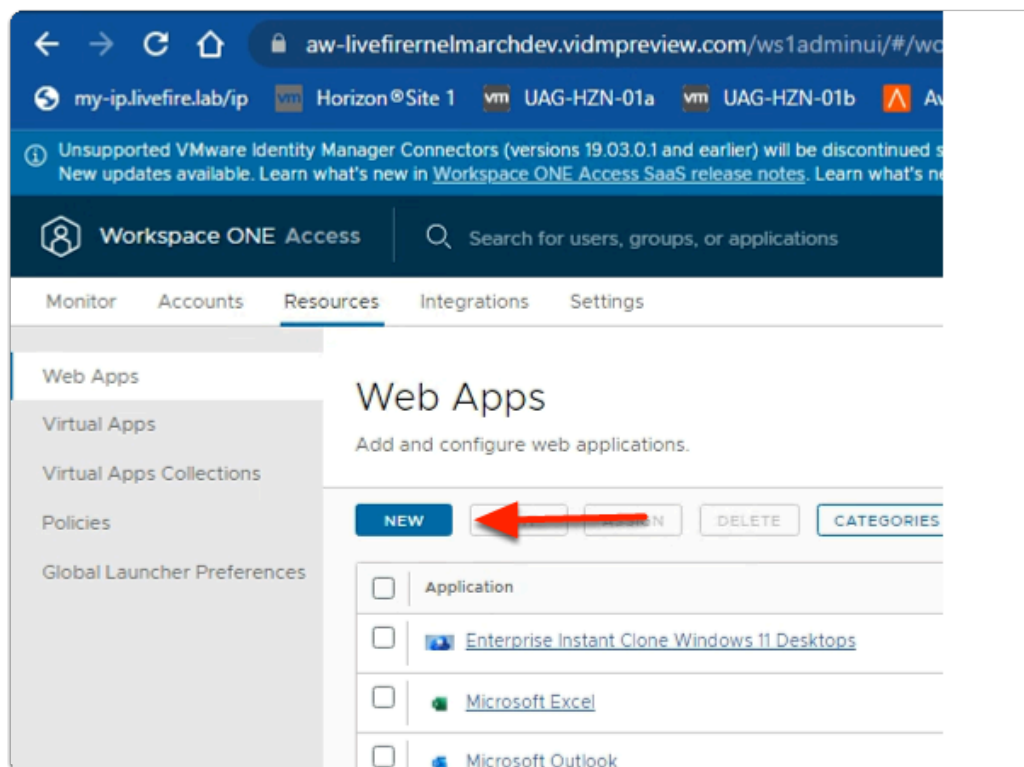
- Under **Users / Groups**
  - Enter **sales**
  - select **sales@euc-livewire.com**
- Under **Deployment** type
  - From the **dropdowns**
    - Ensure both **Sales** and **Developers** are set to
      - **Automatic**
- In the bottom right corner
  - select **SAVE**



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 ⓘ

OR BROWSE FROM CATALOG

Name \* ⓘ

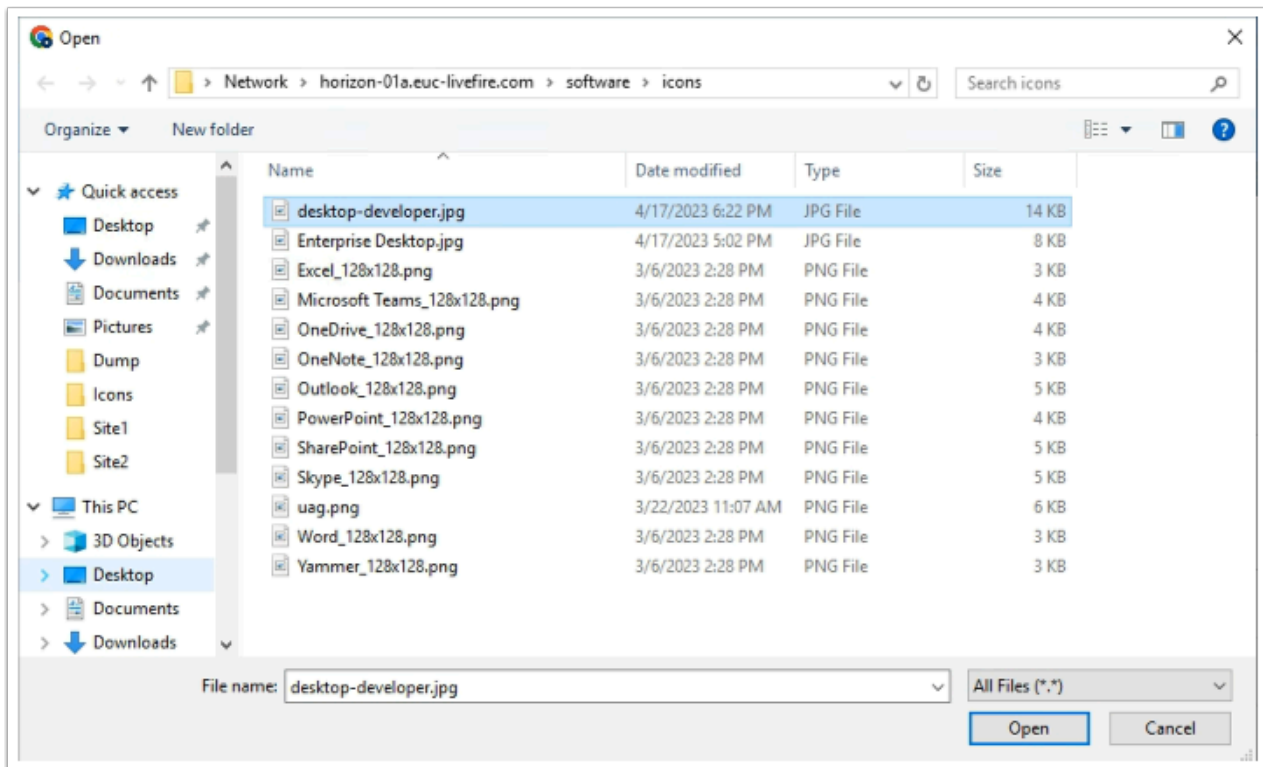
Enterprise Full Clone Desktops

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 \***: Enterprise Full Clone Desktops
- Description**: (empty text area)
- Icon**: A button labeled 'SELECT FILE' and a preview image showing a red square with the text 'Developer'.
- Category**: (empty dropdown menu)
- Selected Categories**: (empty list)

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

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 field:

- 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 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-livewire.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-livewire.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

Developers@euc-livewire.com

Users / User Groups	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**

Workspace ONE Access

Search for users, groups, or applications

Monitor Accounts Resources Integrations Settings

Web Apps

Virtual Apps

Virtual Apps Collections

Policies

Global Launcher Preferences

Web Apps

Add and configure web applications.

NEW EDIT ASSIGN DELETE CATEGORIES MORE SETTINGS

Application	Type
👤 Enterprise Instant Clone Windows 11 Desktops	Web Application Link
👤 Enterprise Full Clone Desktops	Web Application Link
👤 Unified Access Gateway SAML SP	SAML 2.0

10. In your **Workspace ONE Access** Console
  - **Web Apps** interface

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