

Session Protection with VMware Horizon

Introduction

This chapter has 3 primary objectives

- Securing a Horizon Blast sessions using HTML Access
- Securing the HTML Blast functionality when Origin Blocking refuses connections via the Unified Access Gateway
- Securing Workspace ONE Access and VMware Horizon Sessions with JWT TOKEN

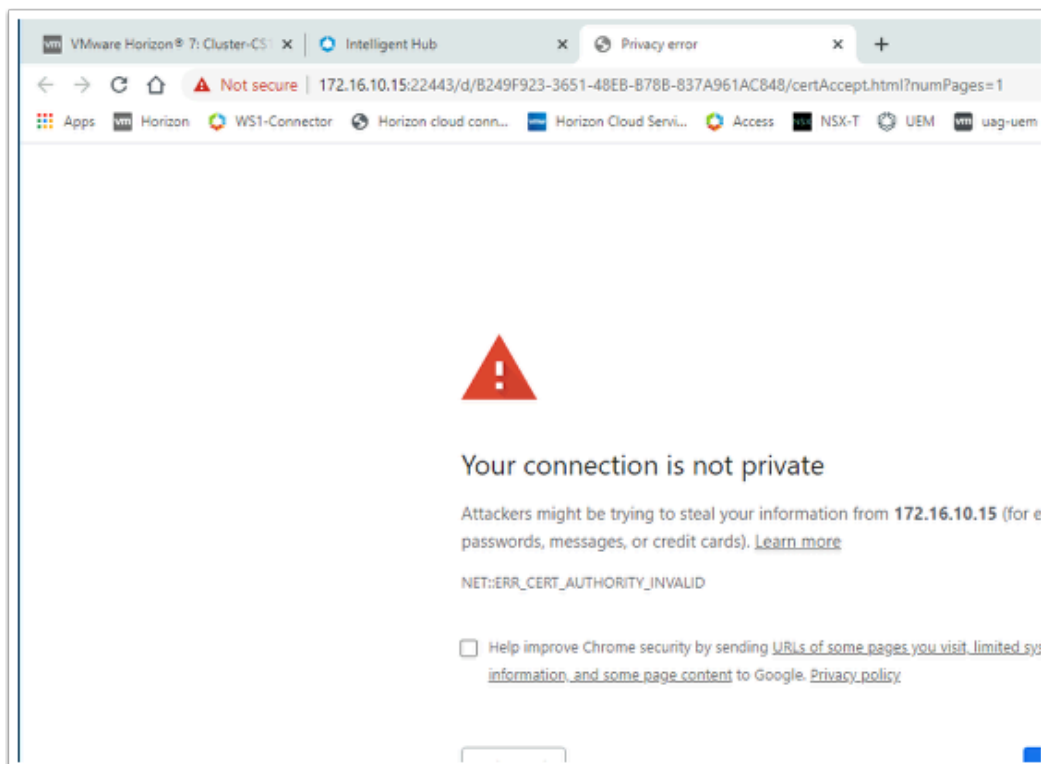
Overview

When launching an entitlement using the HTML client with Horizon Blast either through Workspace ONE Access or as a Direct connection with the broker **by default** one might observe the following:

You might notice that the Browser constantly gets stuck even though our Connection server had trusted CA signed certificates from a public source.

The problem also occurs when using HTML blast via Workspace ONE Access, even though Workspace ONE Access is using CA-signed certificates.

The result is an unsatisfactory User-Experience, a user would have to accept what appears to be an Invalid certificate, leaving them with concerns about the resource they are consuming



Background

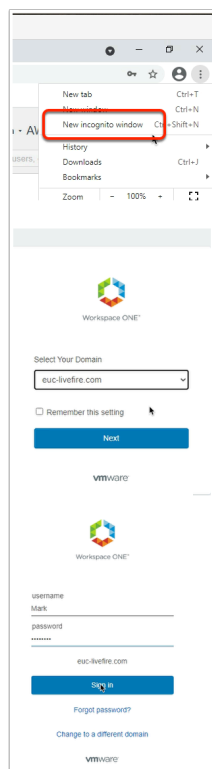
In earlier versions of Horizon, if we wanted to solve this problem we had to perform two primary operations.

1st an edit had to be made on the Broker to the LDS database using ADSIEDIT. The reason for this is as follows and it entails understanding how the transport works. The 2nd step entailed replacing the Agents self-signed cert with a CA signed cert. In a non-persistent environment the most practical way to do this was to use a wild-card certificate.

This exercise is divided into two parts.

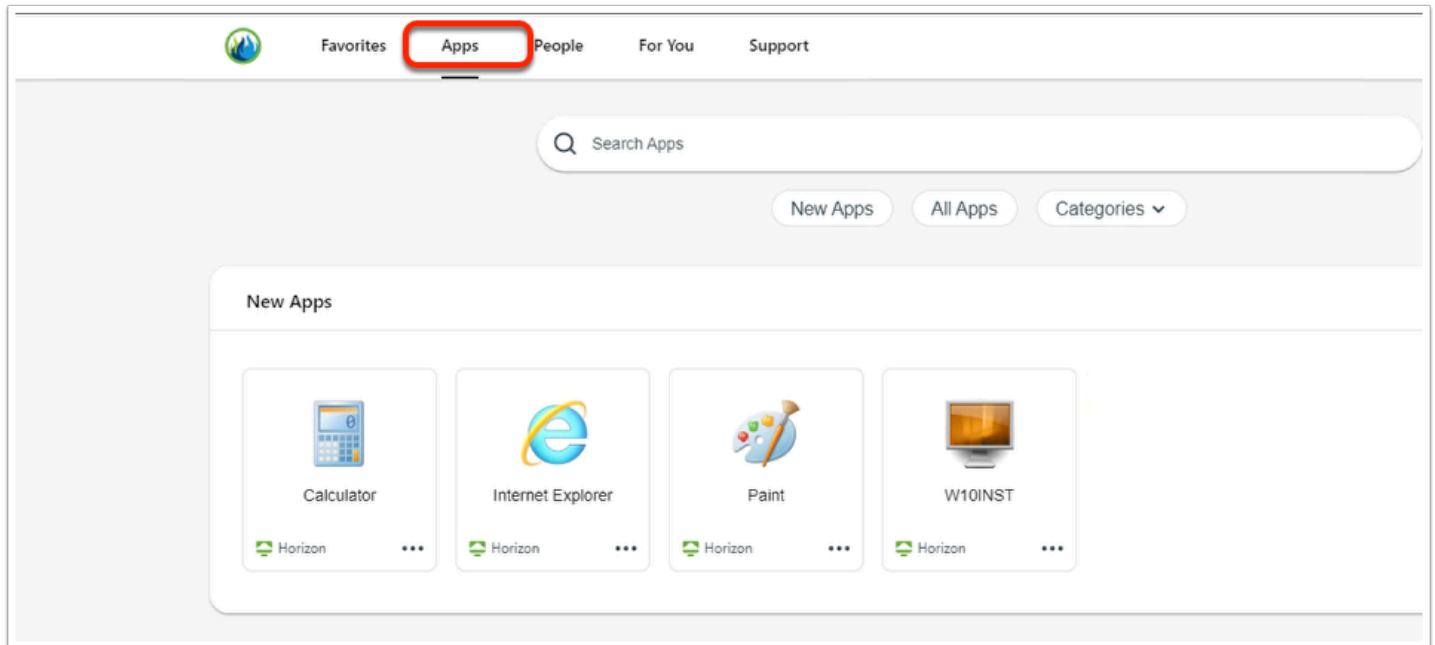
- Part 1 will cover understanding this issue with the Transport
- Part 2 we will use the latest approach to configuring Horizon Blast with Workspace ONE Access and you will notice how much better it works.

Introduction: Validating the default configuration on the Blast transport



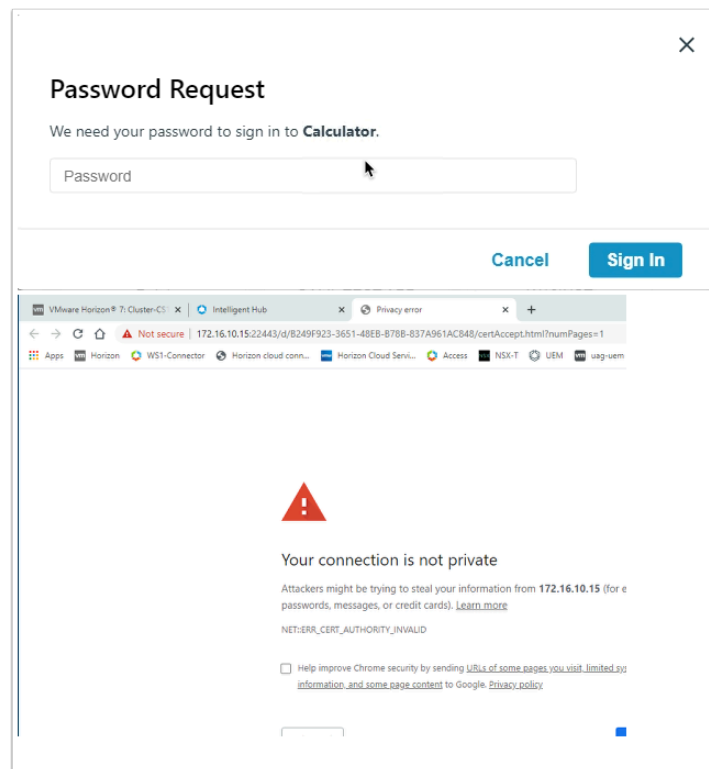
1. On the **ControlCenter** server.
 - Launch an **Incognito session** on your **Chrome browser** session
 - In the address bar enter your custom URL for Workspace ONE Access
 - Below **Select your domain**, ensure **euc-livewire.com** is the selection.
 - Select **Next**

- Under the **username** area
 - Enter the user name **Mark**
- In the **password** area
 - Enter **VMware1!** as the password
- Select **Sign in**



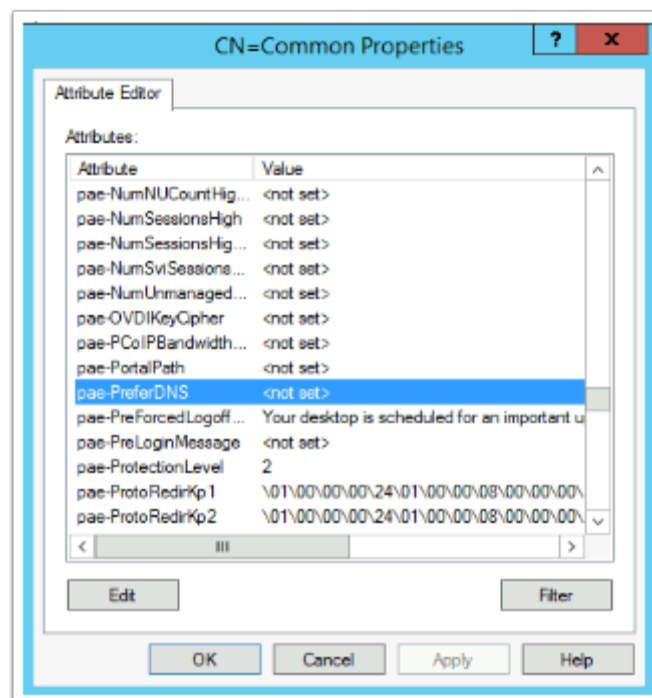
2. In the **Workspace ONE Access Console**

- Select **Apps**
- Under **Categories**, select **Virtual**
- Select and launch, **Calculator**



3. In the **Password Request** window

- In the **Password** area Enter **VMware1!** as the password
- Select **Sign In**
 - In the address bar, notice you have an IP address, also you will notice it says the certificate is not Valid.

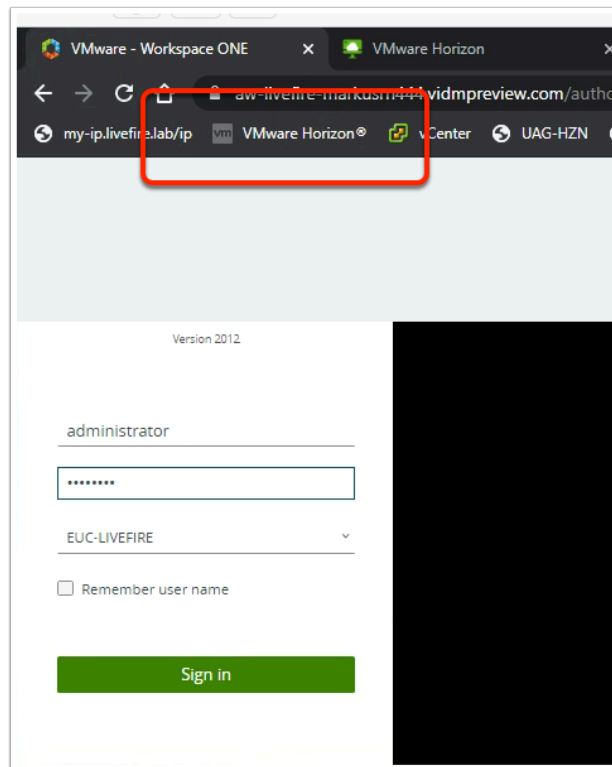


4. So there are two problems here, our Agent is using a self-signed cert, but even if we had a CA signed cert it would not be trusted as by default Horizon prefers to use IP address rather than domain name.
 1. In the **past** this was a two part process, where we had to edit the LDS database using ADSIEDIT (above screenshot of the config) and we would have configure Horizon to Prefer using a FQDN rather than an IP Address. The reason for this was, even if we had a valid certificate it would not be recognized as the address in the certificate would not map to the address in the browser.
 2. On the virtual desktop we would replace the self-signed cert with a CA signed Wild CARD cert .
 - And that was a problem as no one liked that, it was not secure, it gave the impression of being secure, but it was an open door waiting to be exploited.
 3. Thankfully this issue has been rectified and we will look at Part 2 on how secure our Horizon environment properly when we integrate with Access using the Blast Protocol
4. **Log off** from Workspace ONE Access and **Close** any open Browsers
5. Reference
 - <https://kb.vmware.com/s/article/2088354>
 - <https://docs.vmware.com/en/VMware-Horizon-7/7.5/horizon-installation/GUID-8E7FBB9D-F2DB-4787-B11B-7506126DEB7F.html>
6. We will also in the next lab teach an implement TRUESSO for a single sign-on experience

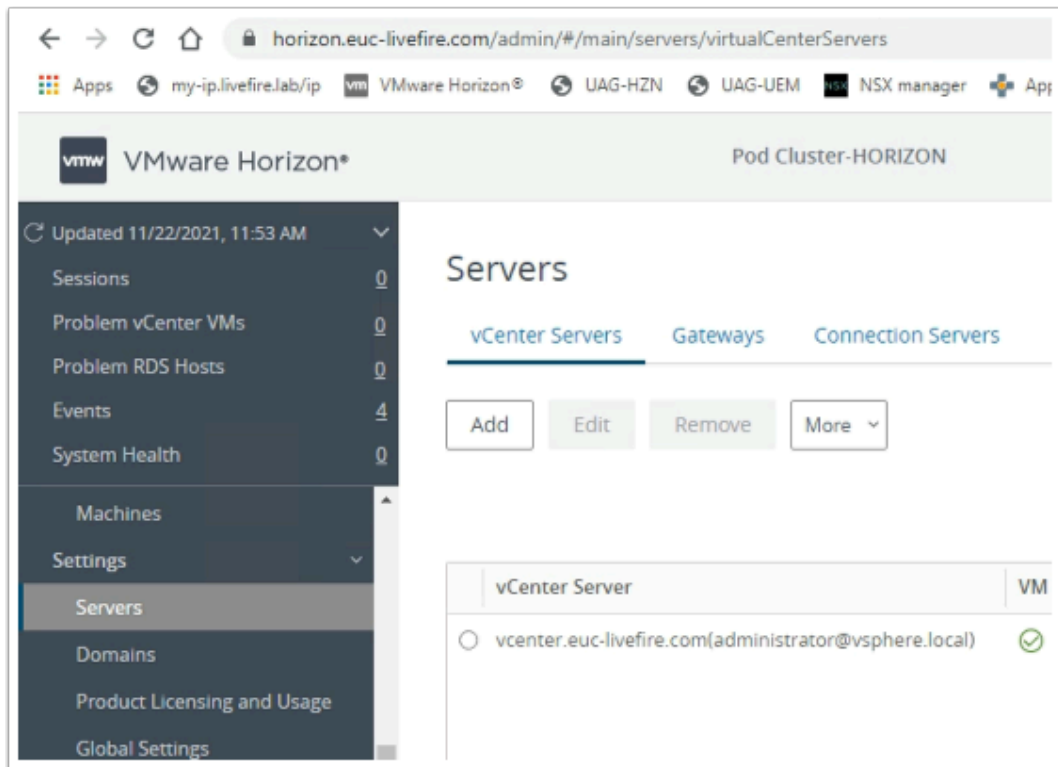
Part 1. Securing a Horizon Blast sessions using HTML Access.

What the Product development team have done is give us the ability to Tunnel HTML Blast traffic through the Broker.

- This has a two advantages. The Broker can use its own CA signed certificate when launching the session with the client and we do not have to configure the Broker to prefer to use DNS as the client is connecting directly with the Broker.
- Best practice now is to configure the HTML BLAST SECURE GATEWAY on the Broker for internal Horizon Clients. In the past we would not configure Blast to Tunnel through the Horizon Connection Server if we wanted to use the Unified Access Gateway.
- With this new configuration we are able to use this Connection Server for both Internal and External use.
 - We will now implement this configuration on the Horizon Connection server and then test this configuration out in this Part

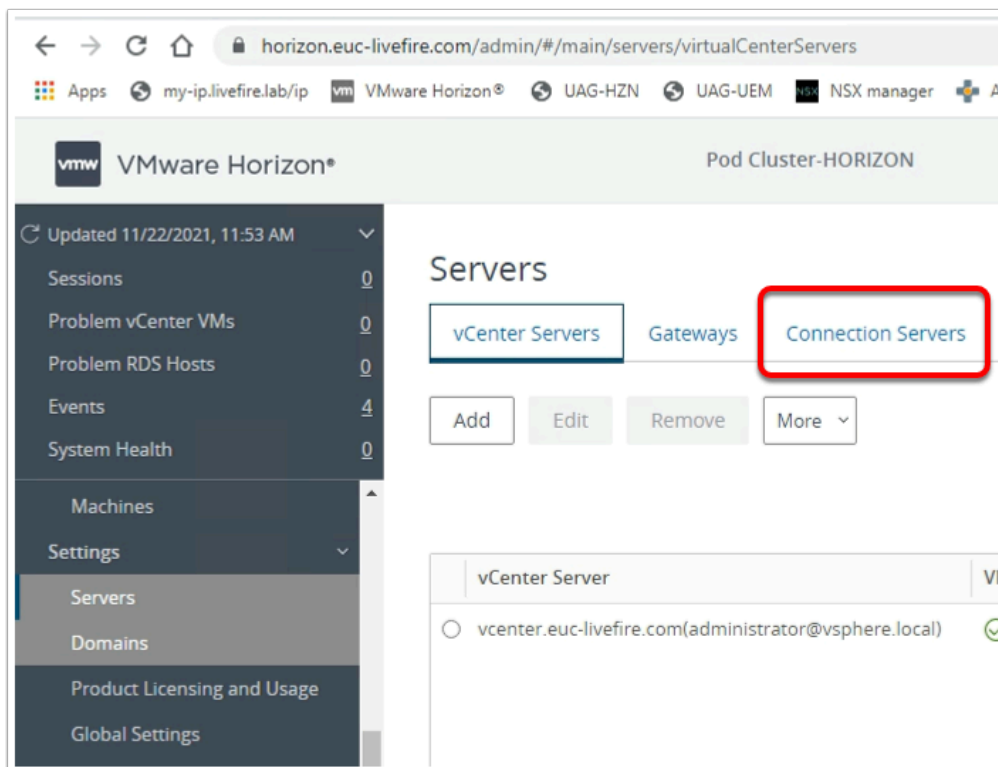


1. On your **ControlCenter** server,
 - Launch the **Chrome Browser**,
 - Select the **VMware Horizon** shortcut in the **Favourites Bar**
 - Login as **Administrator**
 - For password us **VMware1!**
 - Select **Sign in**



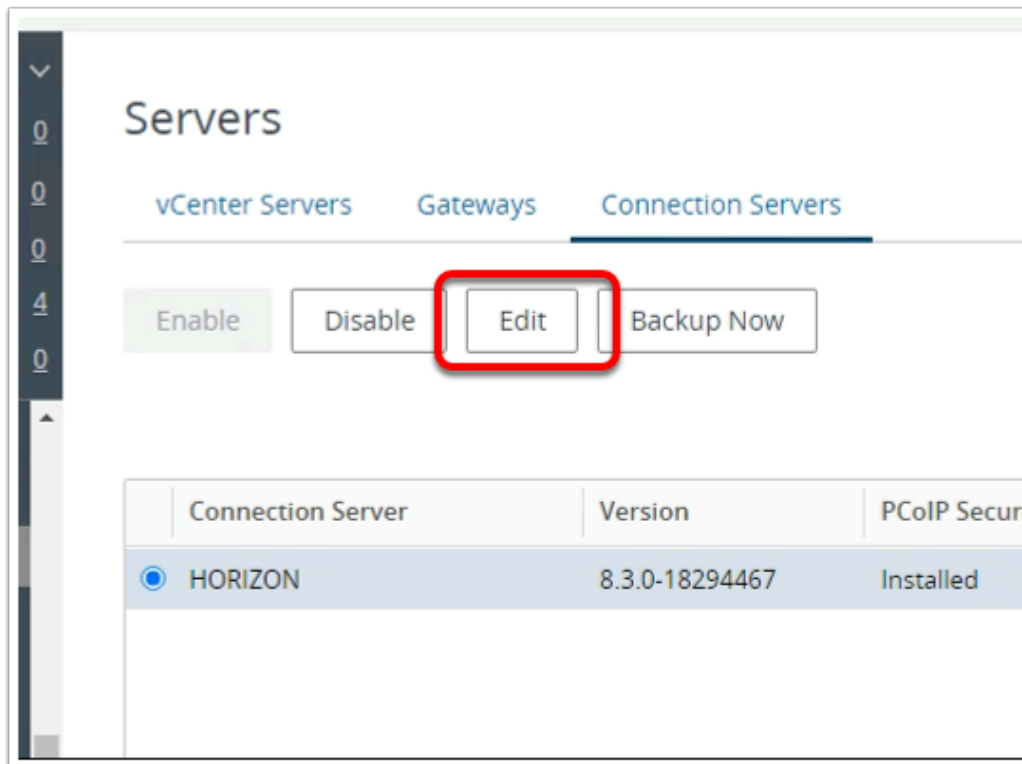
2. In the **Horizon Console**

- **Expand Settings**
- Under **Settings** select **Servers**

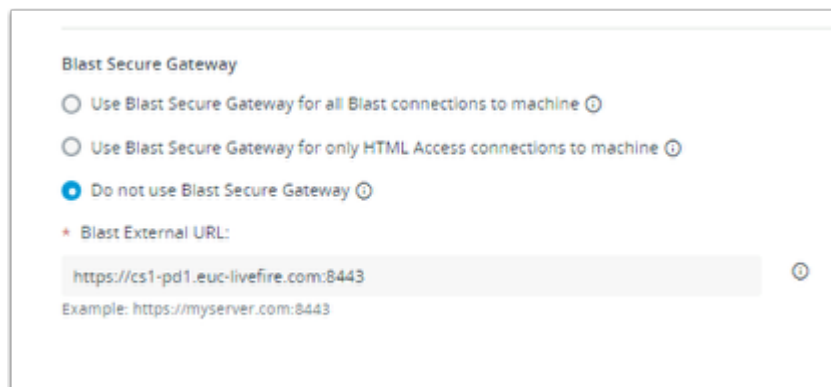


3. Under **Servers**,

- Select the **Connection Servers** tab



4. On the **Connection Servers** tab,
 - Select the **radio button** next to **Horizon**
 - Select **Edit**



5. Notice that the existing configuration
 - This issue occurs when the setting **Do not use Blast Secure Gateway** is selected
 - This configuration was a default with Horizon 7,
 - In Horizon 8, the default configuration when Horizon is fresh-installed is **Use Blast Secure Gateway for all Blast Connections to machine**

Blast Secure Gateway

☐ Use Blast Secure Gateway for all Blast connections to machine ⓘ
☒ Use Blast Secure Gateway for only HTML Access connections to machine ⓘ
☐ Do not use Blast Secure Gateway ⓘ

* Blast External URL:

ⓘ

Example: https://myserver.com:8443

6. In the **Edit Connection Server Settings** window

- Select the **radio button** next to **Use Blast Secure Gateway for only HTML Access Connections to machine**
- Close the **Edit Connection Server Settings** by selecting **OK**

Part 2. Validating our Horizon HTML Blast Configuration and configuring Single Sign-On for password based Authentication.

Workspace ONE™

Select Your Domain

☐ Remember this setting

Next

vmware

Workspace ONE™

username

password

Sign in

[Forgot password?](#)

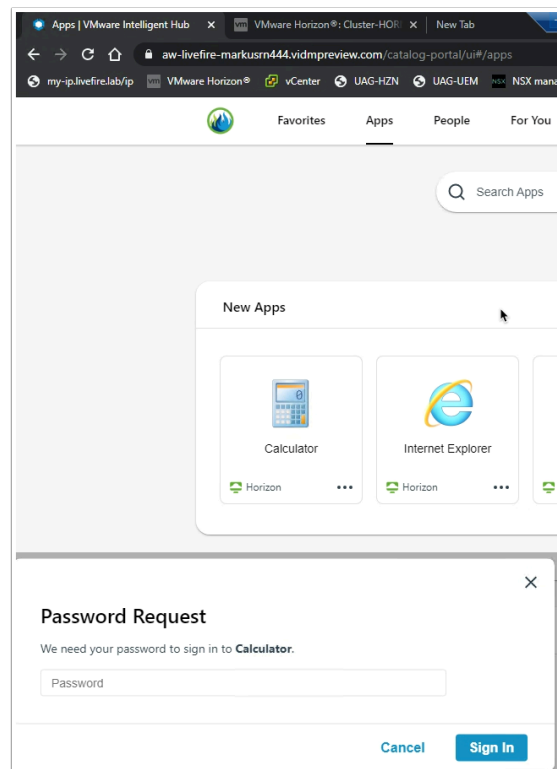
[Change to a different domain](#)

vmware

1. On the **ControlCenter** server.

- From your **Chrome browser** Open an Incognito browser se new tab

- In the address bar enter **your custom Workspace ONE Access URL**
- In the **Select your domain**, ensure **euc-livewire.com** is the selection. Select **Next**
- Enter the username **Mark** and the password **VMware1!** Select **Sign in**

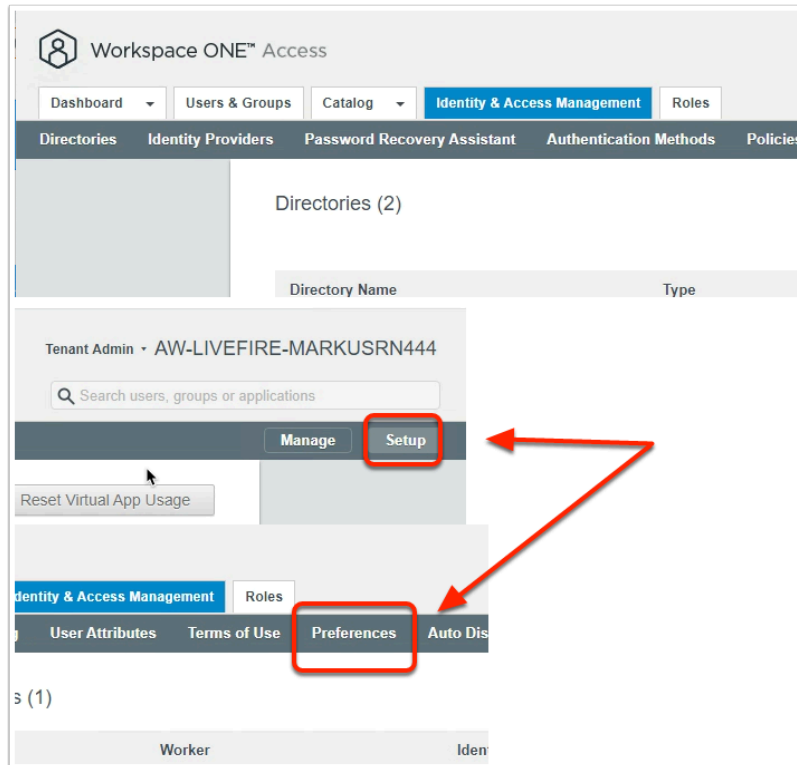


2. In the **Workspace ONE Access Console**

- Select **Apps**
- Under **Categories**, select **Virtual**
- Select and launch, **Calculator**
- In the **Password Request** window, enter **VMware1!**
- Select **Sign In**



3. On your **Chrome Browser**, a new tab should be launch
- **Close** your **Incognito Chrome Browser** session
 - As mentioned earlier, we will address the single Sign-On issue for password based Authentication



4. On your **ControlCenter** server
- Switch to your **Chrome browser** and select your **custom Workspace ONE Access URL** session tab
 - If necessary **log in again with your custom System Admin** credentials
 - In the Workspace ONE Access admin Console
 - Select the **Identity & Access Management** tab
 - To the right of the **Identity & Access Management** console,
 - Select **Setup**
 - Under **Setup**,
 - Select **Preferences**

allowed

Password Caching ☒ Enable

If enabled, a user's password is cached when first logging in to Workspace ONE Access using password-based authentication. If using an alternate method of authentication (such as a third-party IdP, RADIUS, certificate-based, etc.), a user's password is cached when they are challenged with password-based authentication during the first launch of a virtual app.

Enable this to provide single sign-on for users running Horizon, Horizon Cloud, and Citrix virtual apps from the Workspace ONE Catalog. For Horizon and Horizon Cloud, for better user experience and security set up True SSO instead of caching passwords.

[Save](#)

5. In the **Preferences** area

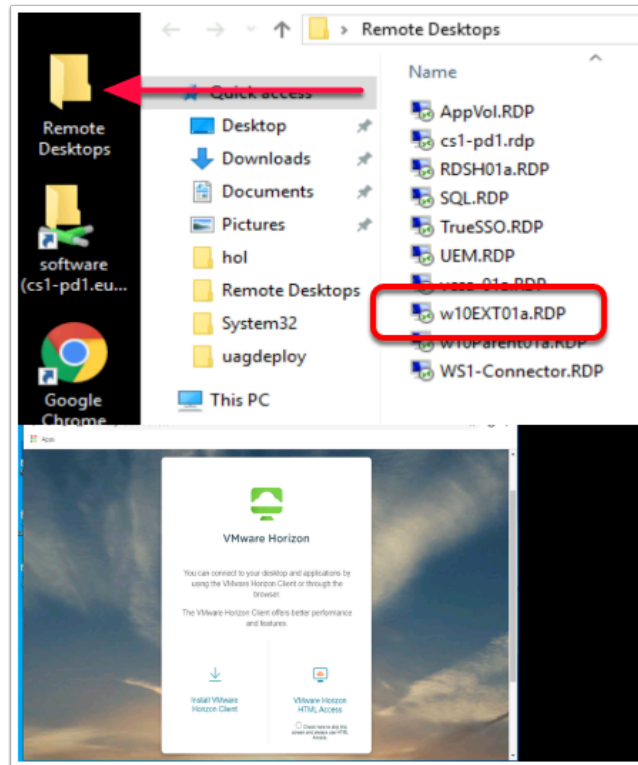
- **Scroll right down**, to the bottom of the **Preferences** area
- Next to **Password Caching**, select the **check-box** next to **Enable**
- Select **Save**
- The Password Caching check box in Preferences will only provide single sign-on for Password based authentication.
 - The Caching of Password for Horizon is a feature that was disabled In December 2019 and this check box was re-introduced for those customers that wanted to accept the security risks of password based caching.
 - This solution does not work for 3rd-Party auth methods

Conclusion

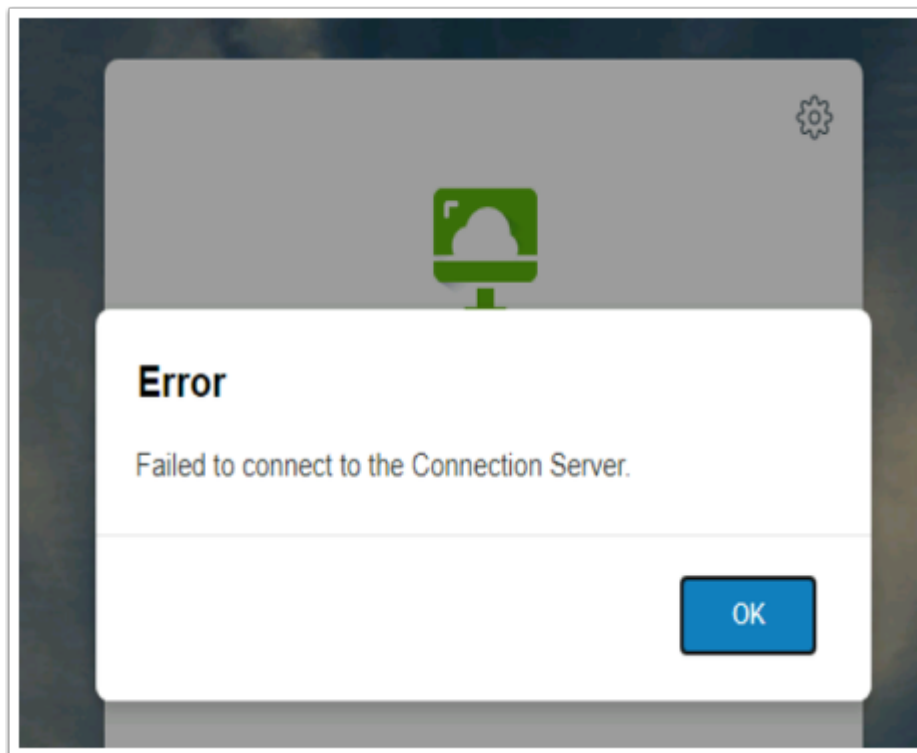
In this session we have seen how we secure internal HTML Blast traffic

If we were external our traffic would tunnel through the Blast Secure Gateway on the UAG. However, when external we would not then tunnel again through the Horizon Connection server. The Unified Access Gateway would come into play. In the next part we will look at how we configure the Unified Access Gateway for secure the HTML Blast Transport for external Access.

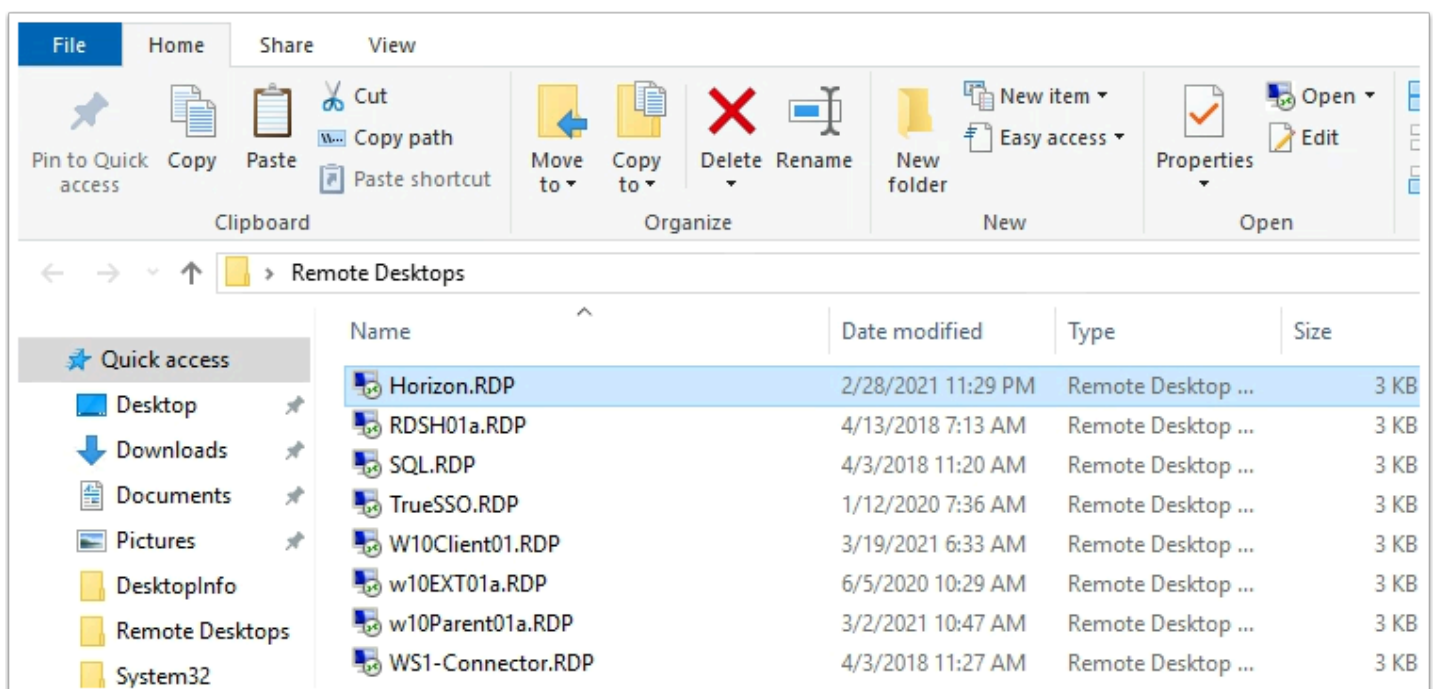
Part 3: Securing the HTML Blast functionality when Origin Blocking refuses connections via the Unified Access Gateway



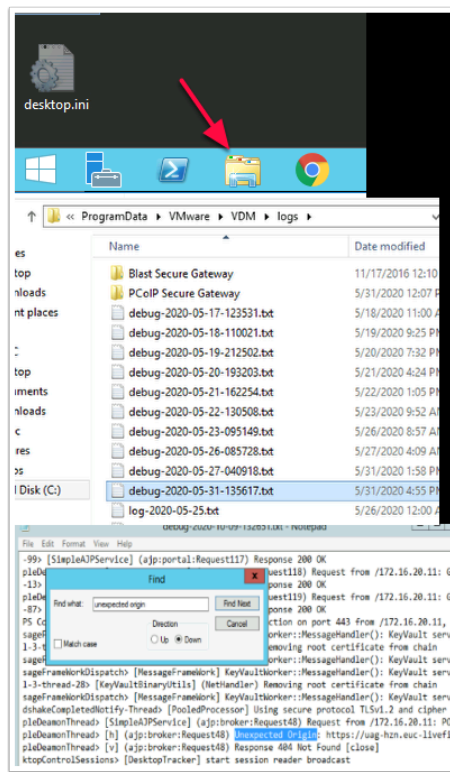
1. On your **ControlCenter** Server
 - Open your **Remote Desktop** folder, launch **W10EXT01a.RDP**
 - Login as **Administrator@euc-livefire.com**
 - With the password **VMware1!**
 - On the **W10Ext01a** desktop, open your **Chrome** browser, in the address bar, type **uag-hzn.euc-livefire.com** or select the **UAG-Client shortcut**
 - Select the **VMware Horizon HTML Access** shortcut



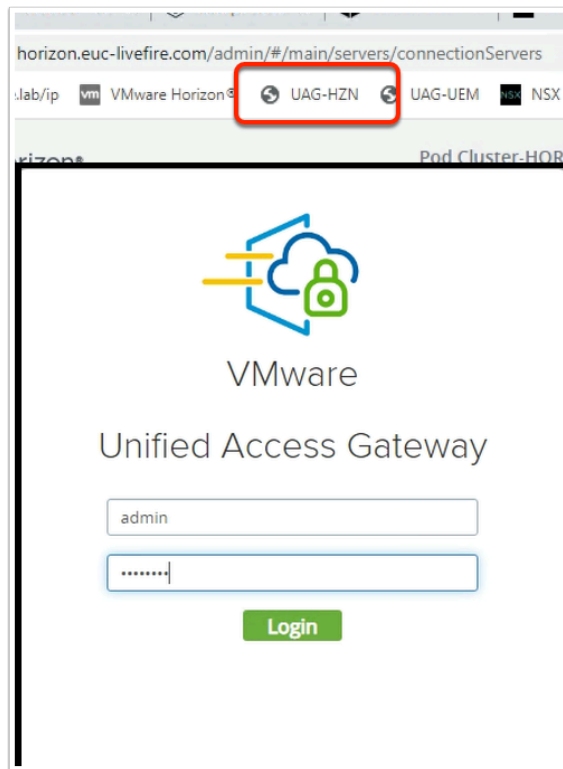
2. Notice you have a **Failed to connect to the Connection Server** issue
 - Select **OK** to close the **Error** message
 - This is not a UAG issue and nothing is broken. This due to a new secure feature that has been enabled in Horizon 7 called **Origin checking** which is enabled by default and is a new standard defined in **RFC 6454**
 - <https://docs.vmware.com/en/VMware-Horizon-7/7.1/com.vmware.horizon-view.security.doc/GUID-AA5D0A57-51A7-4FC1-A79B-AFD15A72499A.html>
 - **Close all** Windows, **minimise** your **W10Ext01a.RDP** session



3. On your **ControlCenter** server Desktop
 - In the **Remote Desktops** folder
 - Launch **Horizon.RDP**
 - Login as username **Administrator@euc-livefire.com**
 - Password is **VMware1!**

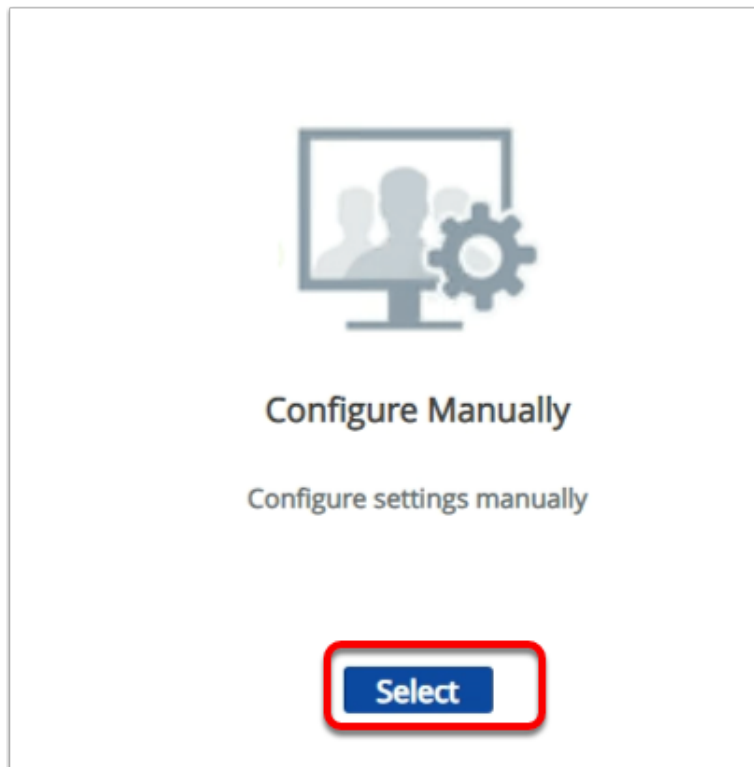


4. On your **Horizon Connection server**, go to your **logs** folder to validate this is the issue.
 - On the Task bar launch **File Explorer**
 - Go to **c:\ProgramData\VMware\VDM\logs**
 - Open the most **current debug log** and
 - Search for a keyword "**unexpected origin**"
- This validates the issue we are having. To solve this proceed with the following step

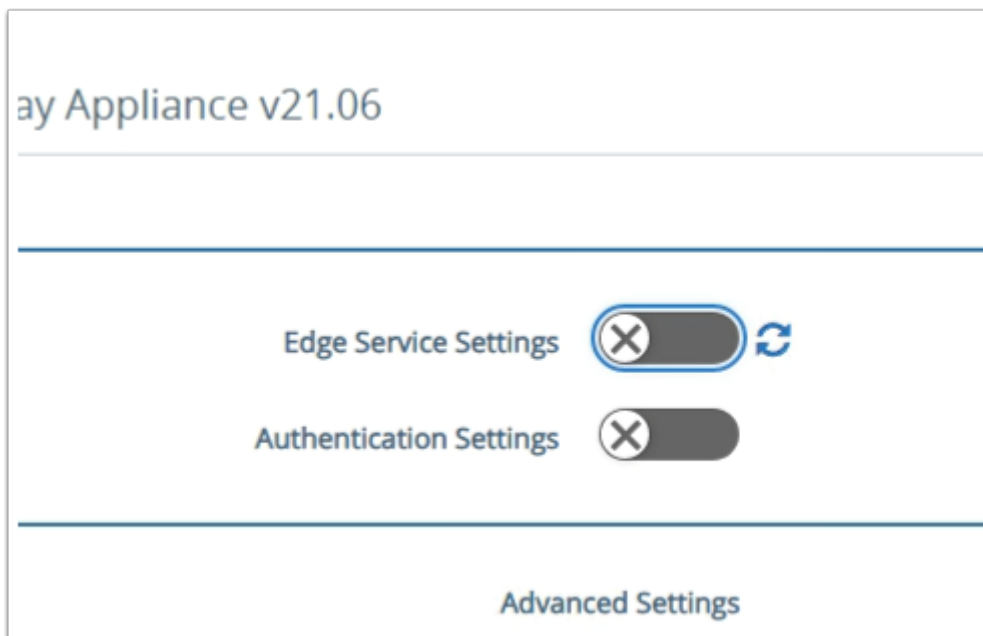


5. On your **ControlCenter** server Desktop

- Open your **Chrome Browser**, open a new tab and select the **UAG_HZN** shortcut
- In the UAG Admin login, type
 - In the **Username** area type : **admin**
 - In the **Password** area type: **VMware1!**
 - Select **Login**



6. On the **Unified Access Gateway Appliance** admin console
 - Under **Configure Manually**
 - Click on, **Select**



7. On the **Unified Access Gateway Appliance v20.12** Admin console
 - Under **General** Settings
 - Next to **Edge Service Settings**, move the **toggle** next to **Edge Service Settings** from Left to Right

Edge Service Settings



➔ Horizon Settings



Reverse Proxy Settings



8. To the right of **Horizon Settings**,

- Select the **gear wheel**

admin/index.html#/configAccessPointGateway/Form

vCenter UAG-HZN UAG-UEM NSX manager

Enable Horizon **YES**

Connection Server URL

Connection Server URL Thumbprint

Connection Server IP mode

Re-Write Origin Header **NO**

Enable PCOIP **YES**

Disable PCOIP Legacy Certificate **NO**

Connection Server IP mode

Re-Write Origin Header **YES**

Enable PCOIP **YES**

Disable PCOIP Legacy Certificate **NO**

PCOIP External URL

Enable Blast **YES**

Blast External URL

Enable UDP Tunnel Server **YES**

Blast Proxy Certificate

Enable Tunnel **YES**

Tunnel External URL

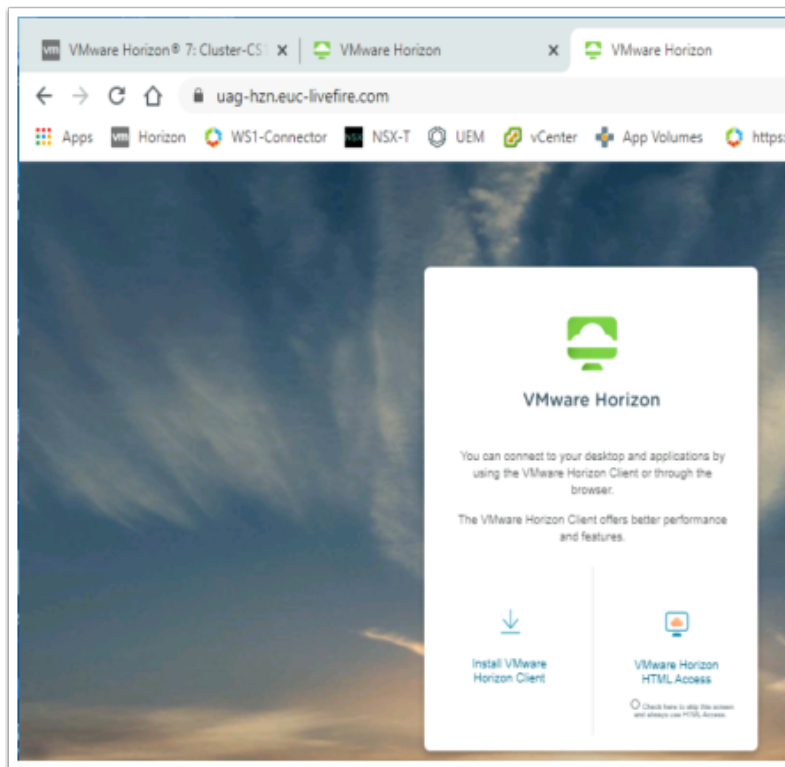
Tunnel Proxy Certificate

More »

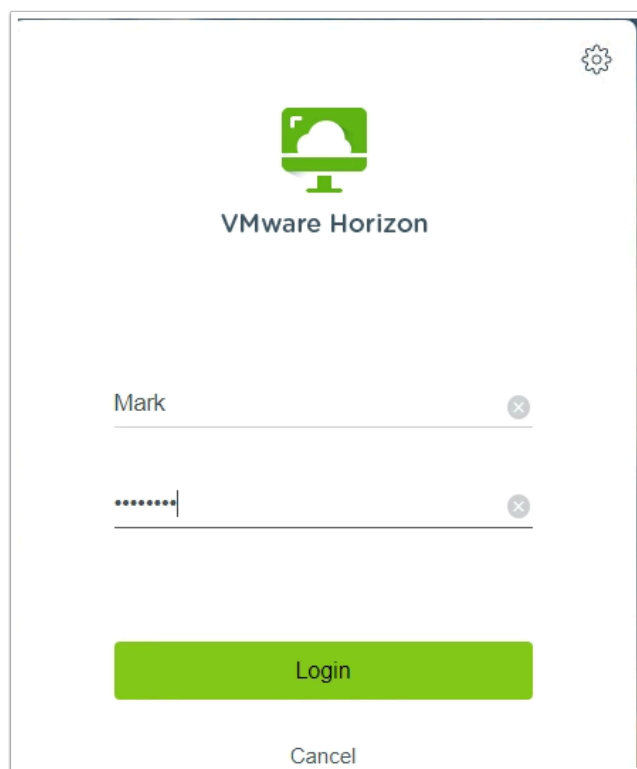
Save **Cancel**

9. In the **Horizon Settings**, next to

- **Re-write Origin Header**, move the **toggle** from **No** on the left to **Yes** on the right.
- Select **Save** at the bottom of the window.
- **Logout** from the UAG Admin console

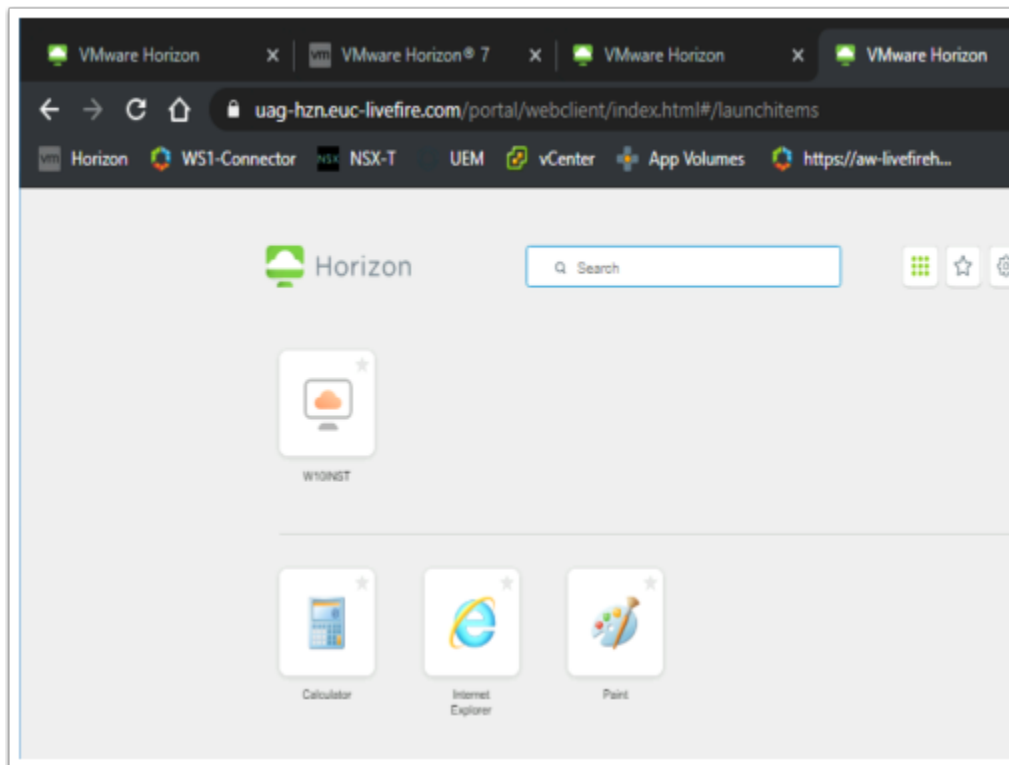


10. Switch back to your **W10Ext01a** server,
- Launch your **Chrome Browser**
 - Enter **UAG-HZN.euc-livfire.com** in the Address **Bar**
 - Select **VMware Horizon HTML Access**

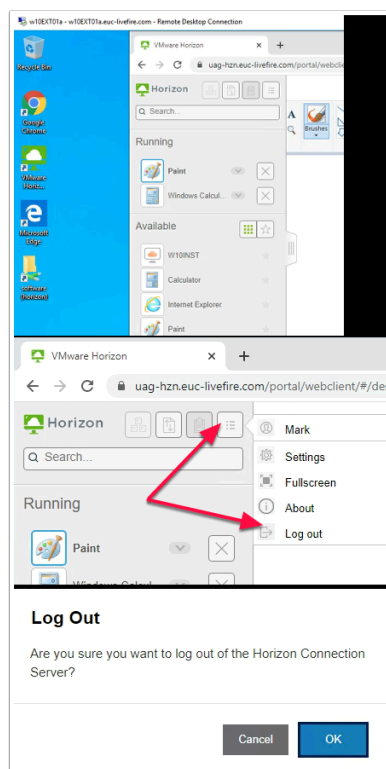


11. In the Login window type in the following:

- Username: **Mark**
- Password: **VMware1!**
- Select **Login**



12. In the Horizon HTML entitlements,
- Launch **Paint**



13. Notice your entitlement launches without any further prompts

- Select **Log out**
- On the **Log Out** window select **OK**
- **Close** your Browser
- **Minimize** your **W10Ext01a.RDP** Session

Conclusion

This concludes this part

We have Configured HTML Blast for external access using the Unified Access Gateway and the HTML Blast Secure Gateway

Part 4: Configuring secure sessions when Integrating Workspace ONE Access with VMware Horizon and the Unified Access Gateway.

Introduction

When configuring the Transport integration with Workspace ONE Access a customer might have deployed an On-premises, LAN deployed Workspace ONE Access server or DMZ deployed Workspace ONE Access server or the customer might have subscribed to a SAAS deployment of Workspace ONE Access.

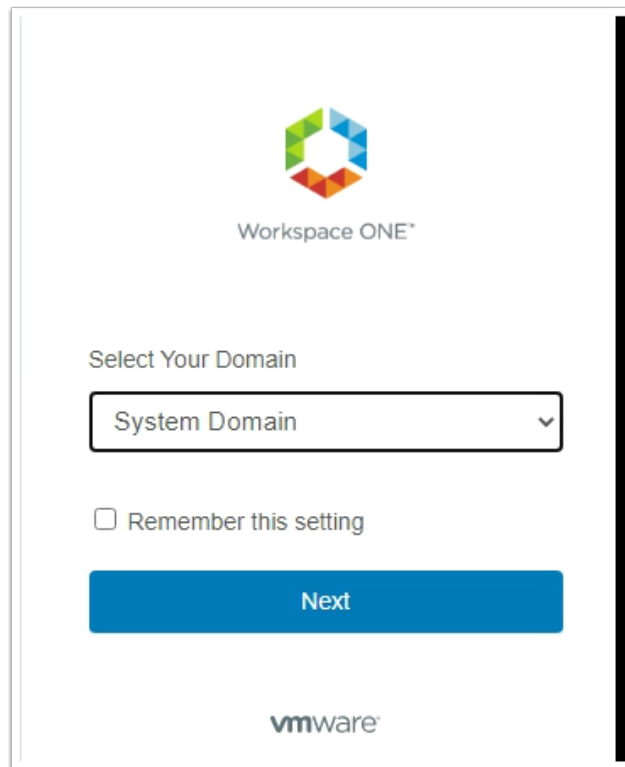
VMware Horizon will always be on a Microsoft Active Directory Domain joined LAN connected network. The Unified Access Gateway will be deployed in the DMZ to facilitate all external access for Horizon Based resources and will not be domain joined.

Internal Users should / could connect and tunnel directly through the Connection Server with HTML Blast or have a direct session to the Horizon Agent on the LAN.

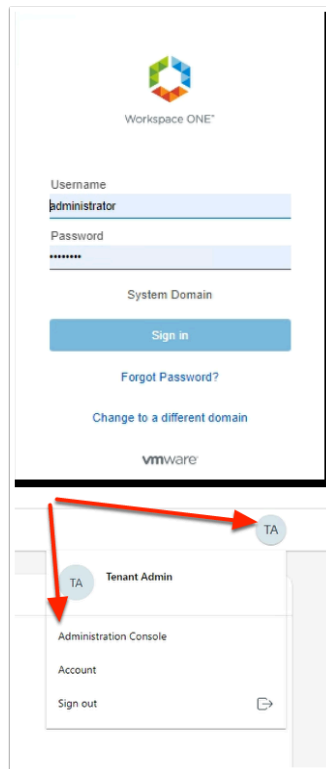
External Users should always connect and tunnel via the Unified Access Gateway and should never have a Direct session on the Transport from an external network to a domain joined desktop.

In this scenario all we are doing is securing North / South traffic. To ensure East / West traffic within networks are secure we would use the Micro-segmentation feature of VMware NSX

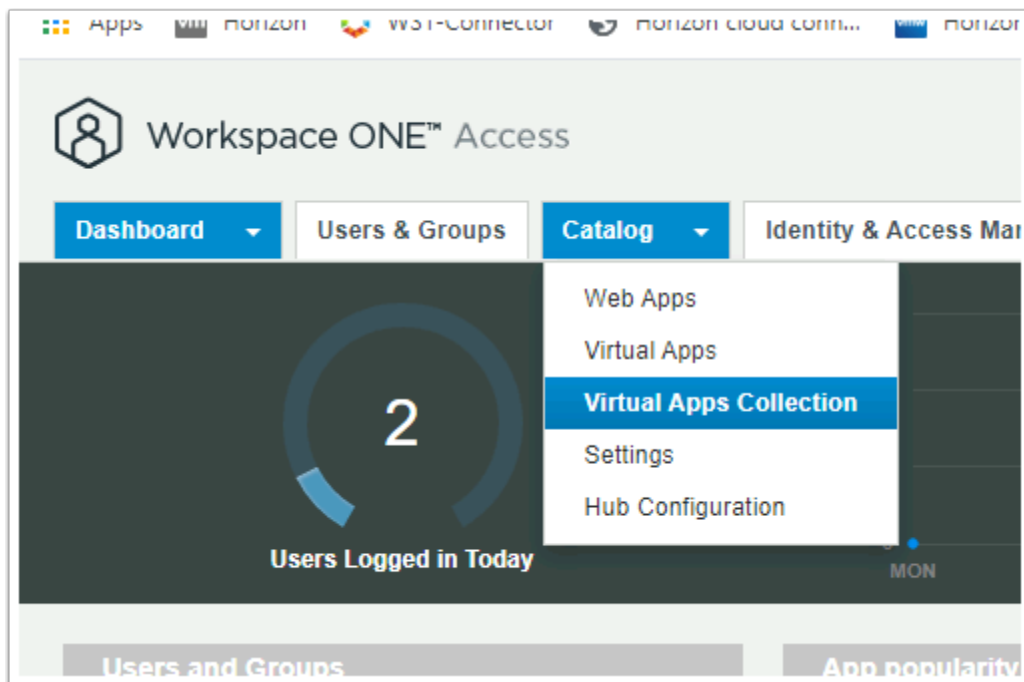
The objective of this session is demonstrate the Networking configuration requirements when Workspace ONE Access integrates with VMware Horizon and the VMware Unified Access Gateway.



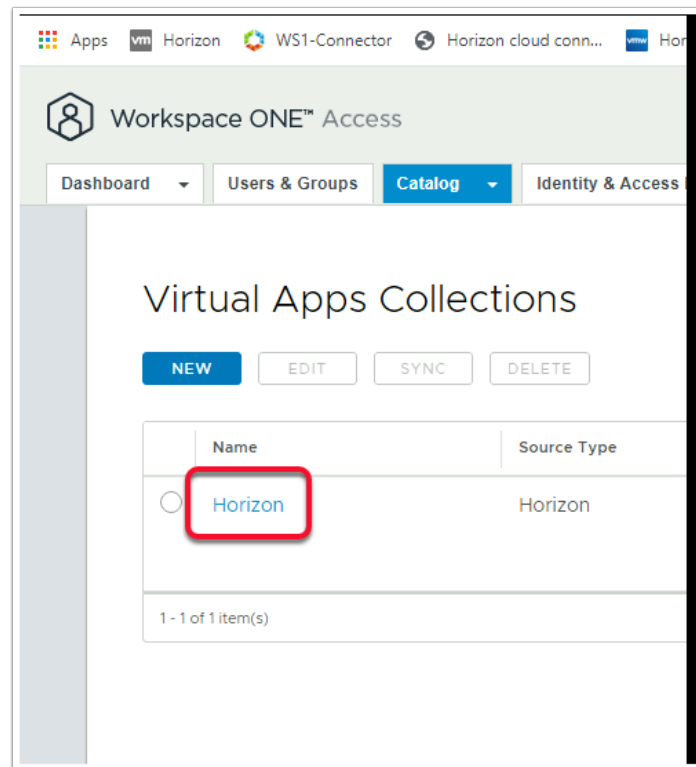
1. On your **ControlCenter** server,
 - On your **Google Chrome** browser,
 - Open a **new tab**
 - Enter your custom **Workspace ONE Access URL**
 - Ensure that in the **Select your Domain** window,
 - You have **System Domain** selected in the **dropdown**
 - Select **Next**



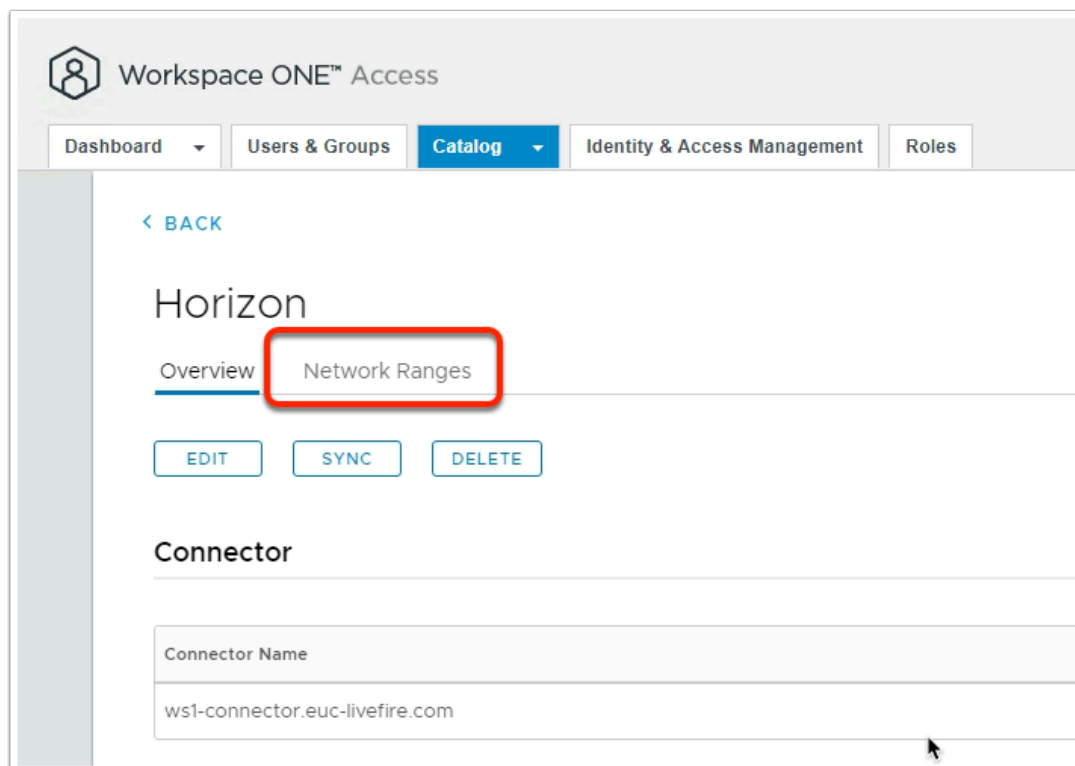
2. In the **Workspace ONE Sign-In** page
 - Under **Username** type **administrator**,
 - Under **Password** type enter **your custom password**
 - Select **Sign In**
 - In the right-hand corner, select **TA** > **Administration Console**



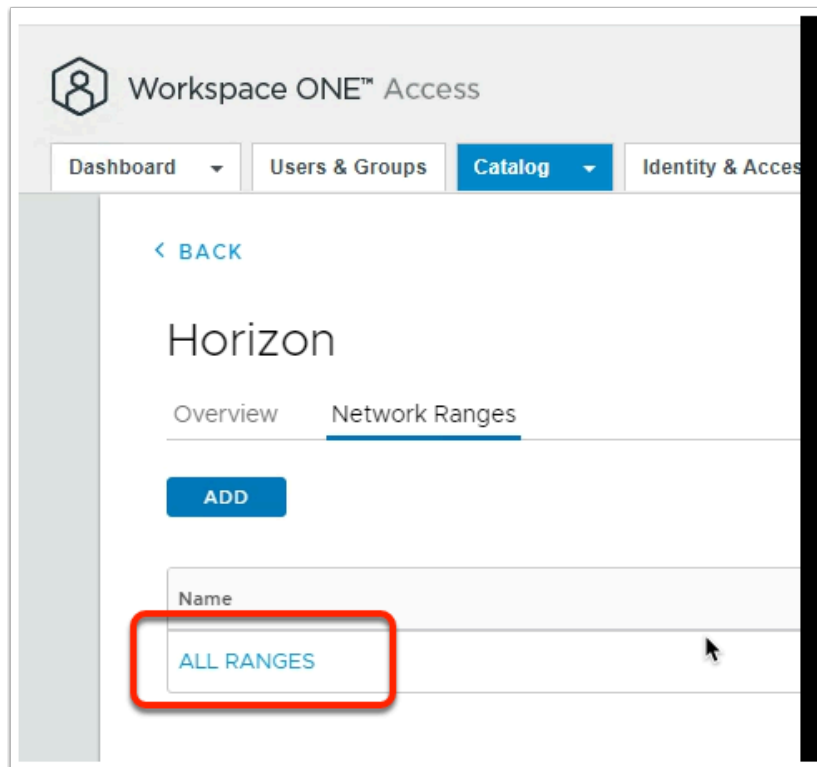
3. In the **Workspace ONE Access** console
 - Select **Catalog** > **Virtual Apps Collection**



4. In the **Virtual Apps Collections** window,
 - Double-Click **Horizon**

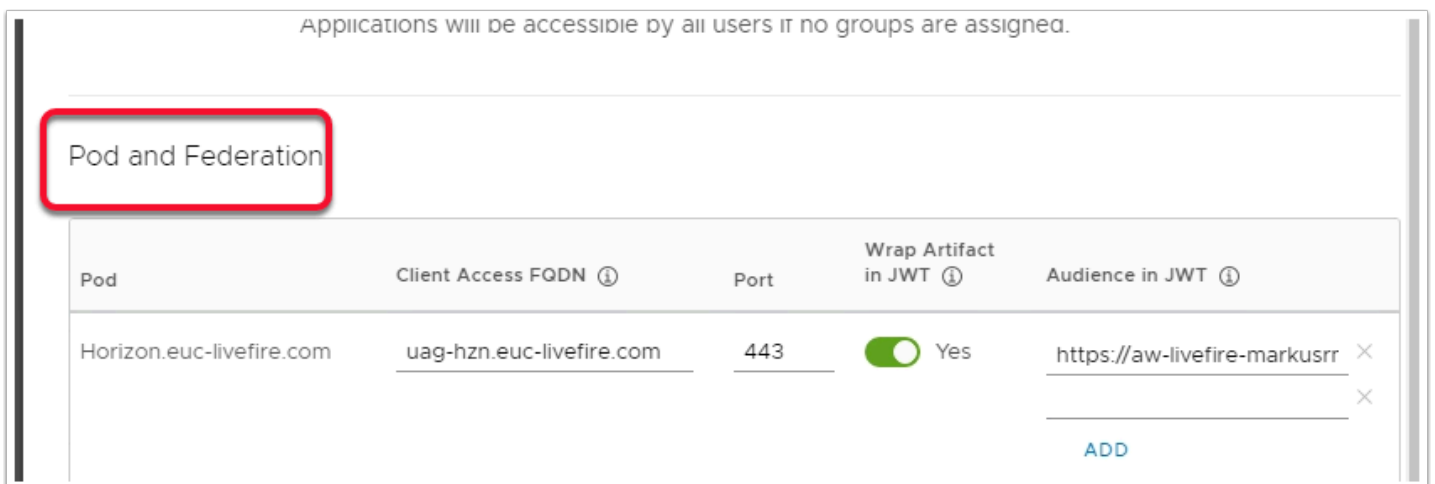


5. In the **Horizon** window,
 - Select the **Network Ranges** tab



6. In **Network Ranges** window

- Select **ALL RANGES**

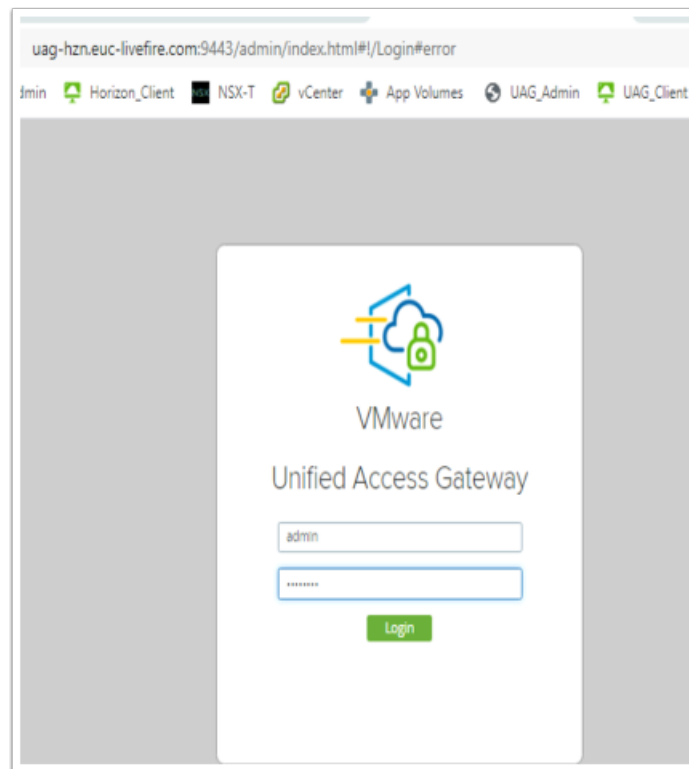


7. In the **Assign Pods to Network Ranges** window

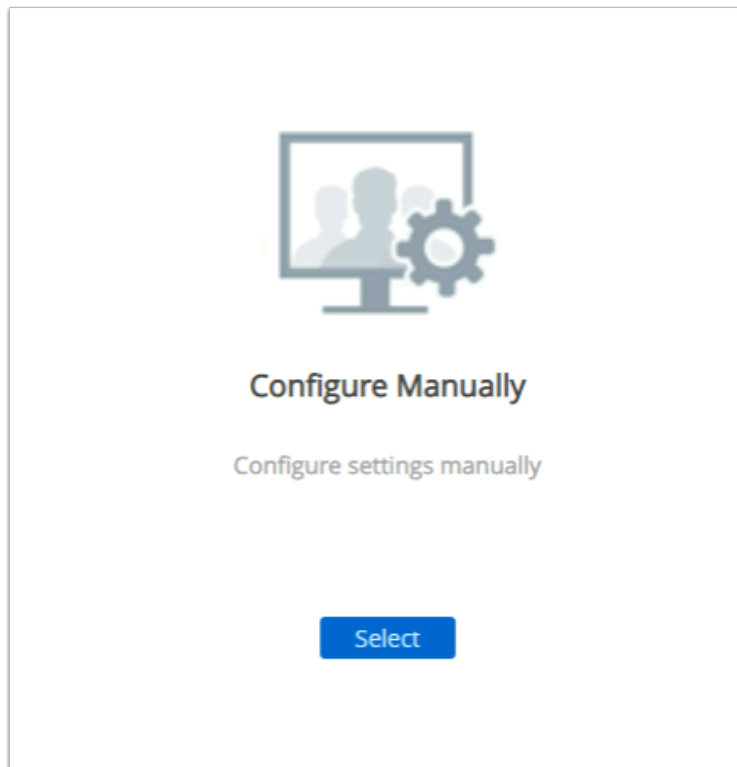
- **Scroll** down to **Pod and Federation**
 - Under **Client Access FQDN**
 - Enter **uag-hzn.euc-livewire.com**
 - Under **Wrap Artifact in JWT**
 - Switch the **Toggle** to **Yes**
 - Under **Audience in JWT**

- Type your custom **Workspace ONE Access URL**. e.g. <https://aw-livfire-markusrn444.vidmpreview.com>
- Select **ADD**
- Select **SAVE**

Part 5: Configuring Unified Access Gateway and VMware Horizon Sessions with JWT TOKEN

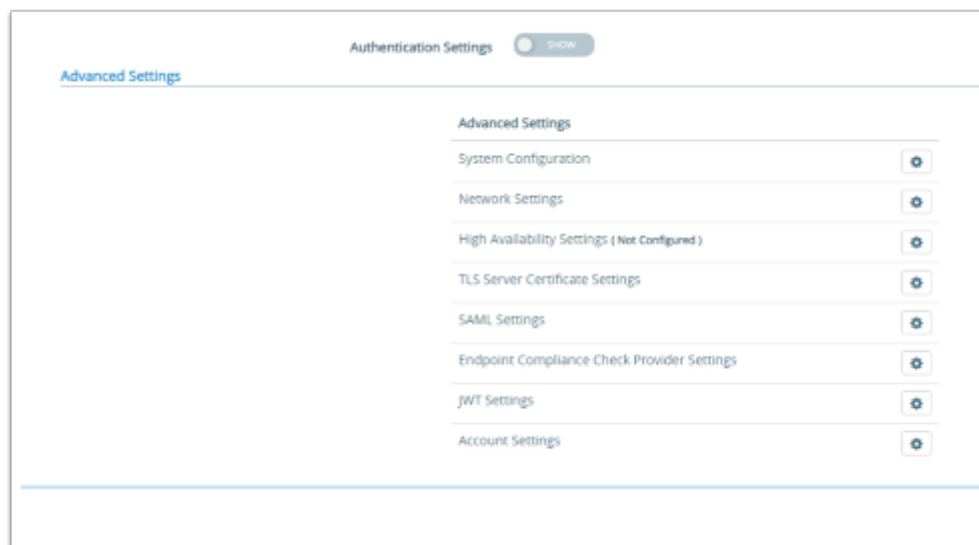


1. On the **ControlCenter** server
 - On your **Chrome** browser, Open a **new Tab**, select the **UAG-HZN** admin shortcut session
 - In the **Username** area, login as **admin**
 - In the **password** area, enter **VMware1!**,
 - Select **Login**



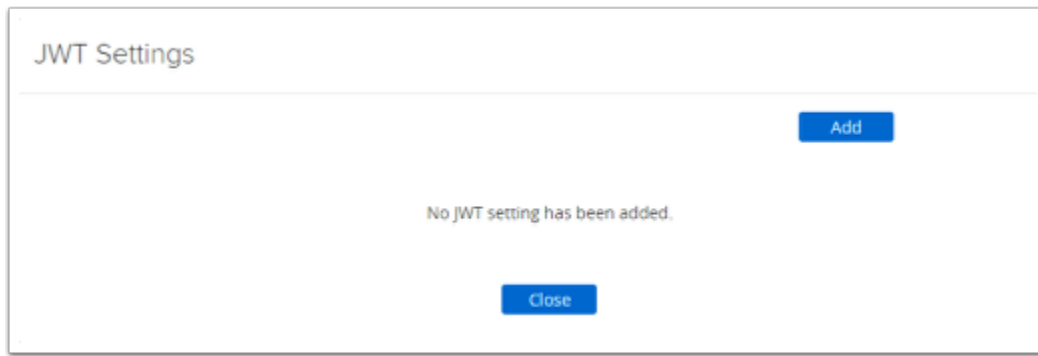
2. In the UAG ADMIN Console

- Under **Configure Manually**, select the Blue **Select** button

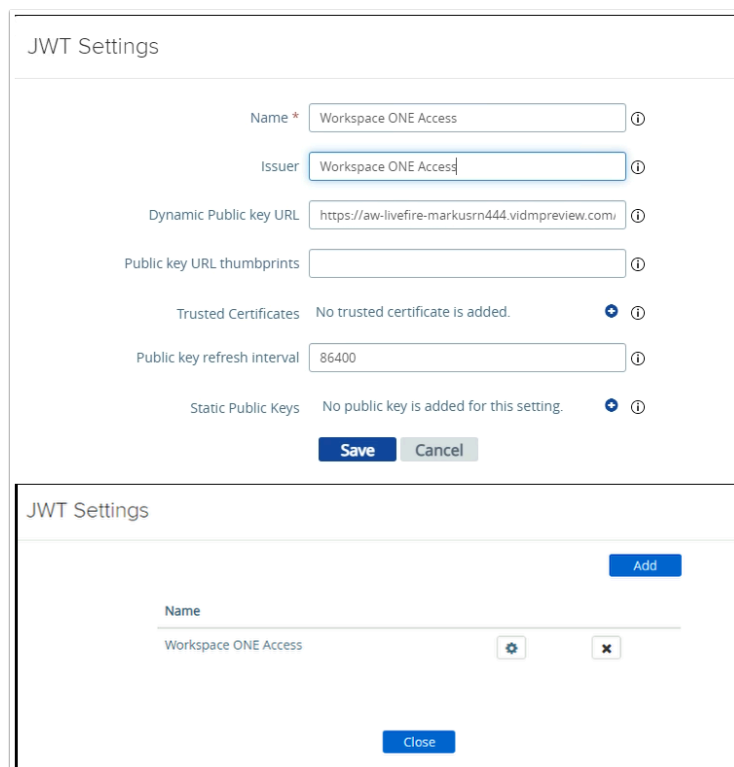


3. In the UAG ADMIN Console

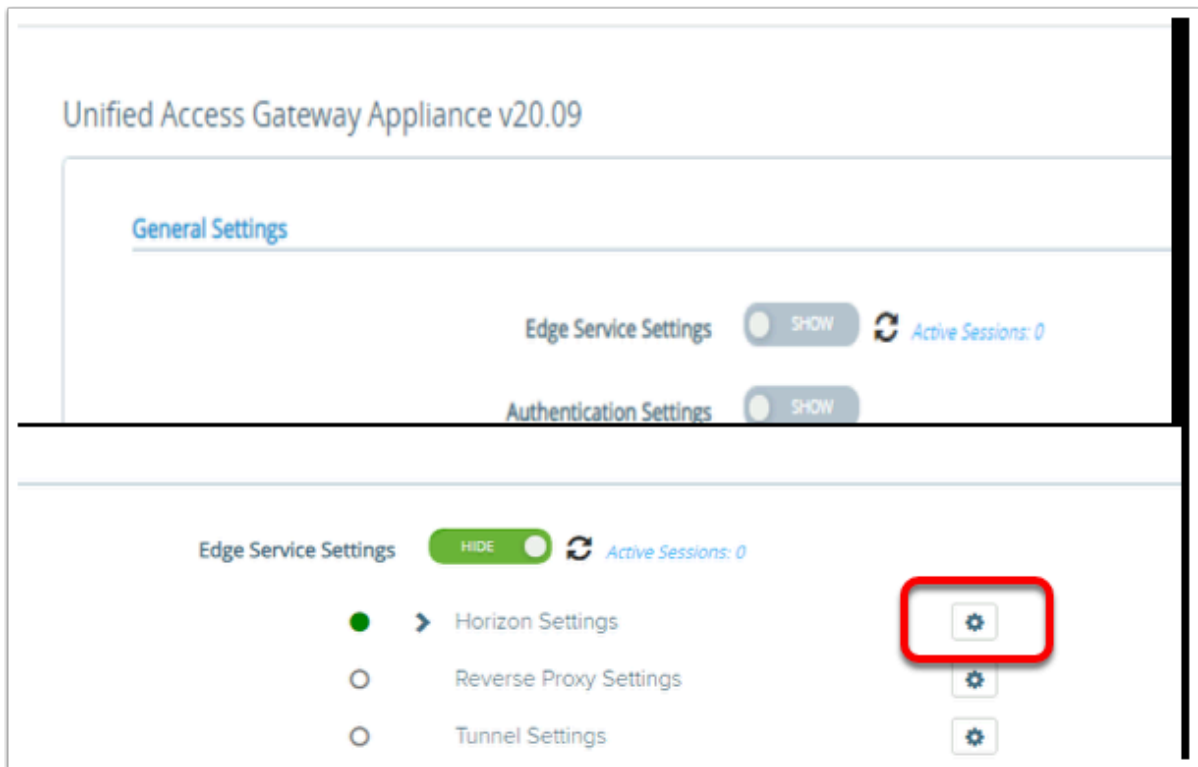
- Under **Advanced Settings**
 - Select the **Gear** to the right of **JWT Settings**



4. In the **UAG ADMIN** Console
 - In the **JWT Settings** window, select **Add**

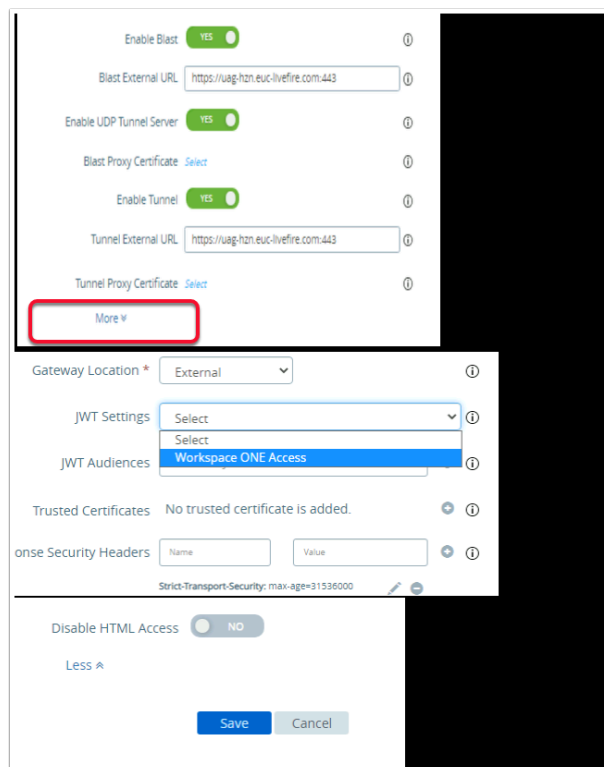


5. In the **JWT Settings** window, enter the following, next to
 - **Name:** **Workspace ONE Access**
 - **Dynamic Public key URL:** **https://YOUR CUSTOM ACCESS FQDN/SAAS/API/1.0/REST/auth/token?attribute=publicKey&format=pem**
 - **Public key refresh interval:** **86400**
 - Select **Save**
 - Select **Close**



6. In the **UAG Admin Console**

- In the **General Settings** area
 - Next to **Edge Service Settings**, select and move the **toggle** to the right
 - To the right of **Horizon Settings**, select the **GEAR**



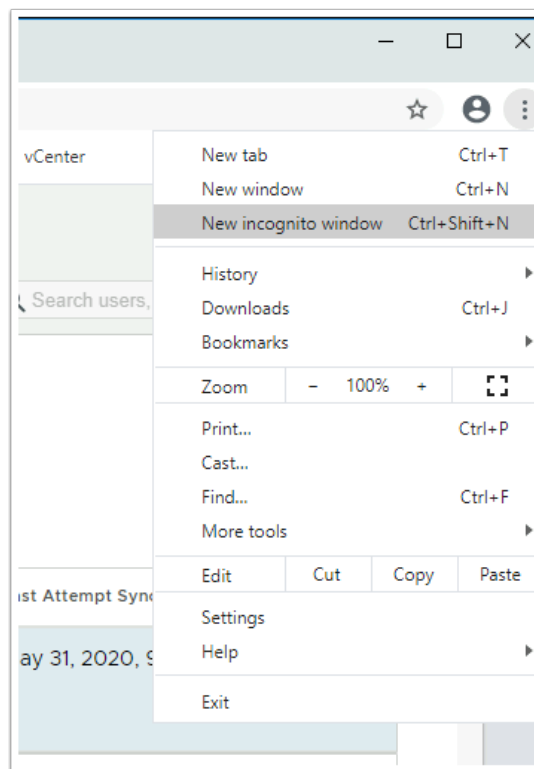
7. In the **Horizon Settings** window

- At the bottom of the page, select **More**
- To the right of **JWT Settings** select the **dropdown** and select **Workspace ONE Access**
- **Scroll** to the bottom of the window and select **Save**

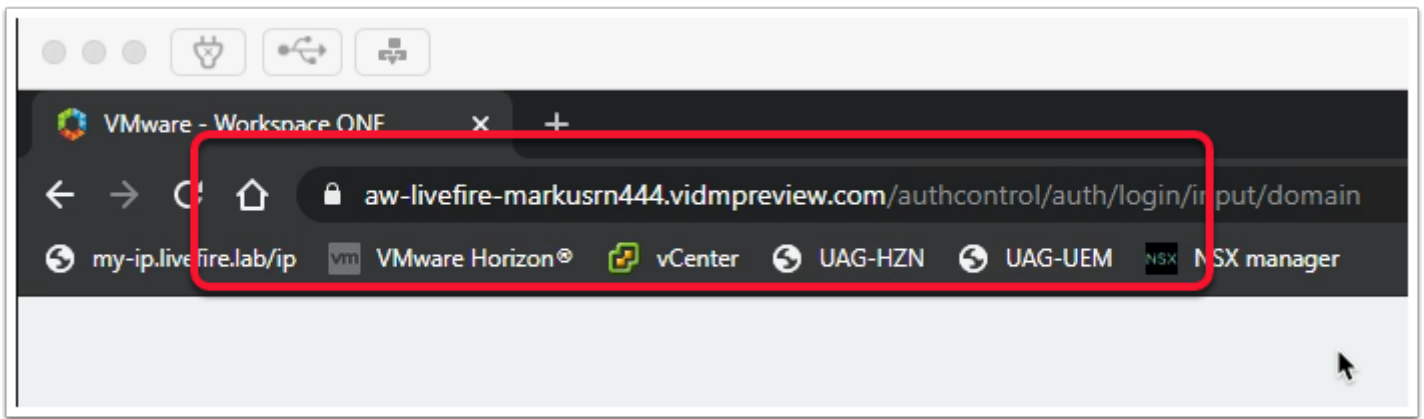
Part 6: Validating Workspace ONE Access Transport Configurations with VMware Horizon

INTRODUCTION

All Horizon sessions configured to communicate with Workspace ONE Access have been configured to be secure. We will now test the session

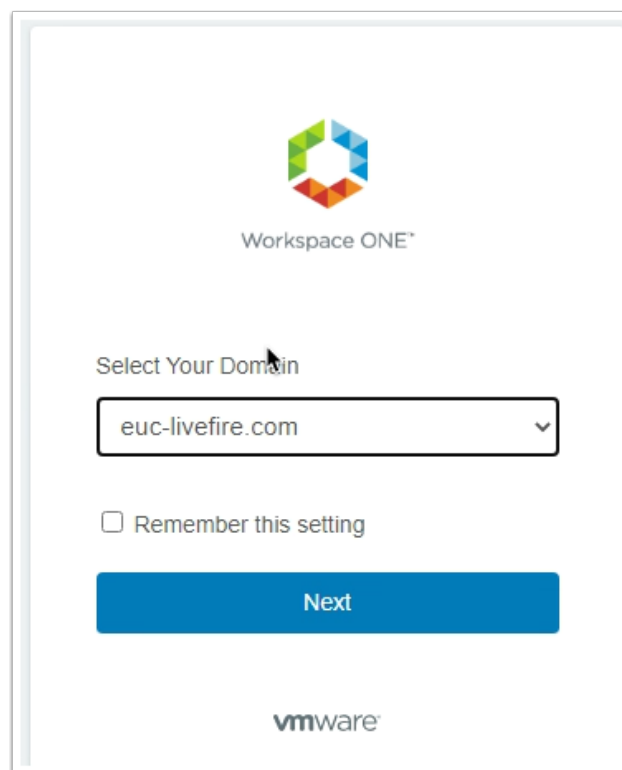


1. On your **ControlCenter** server
 - On your **Chrome Browser** in the top right hand corner,
 - Select the **3 DOTS**
 - Select **New incognito window**



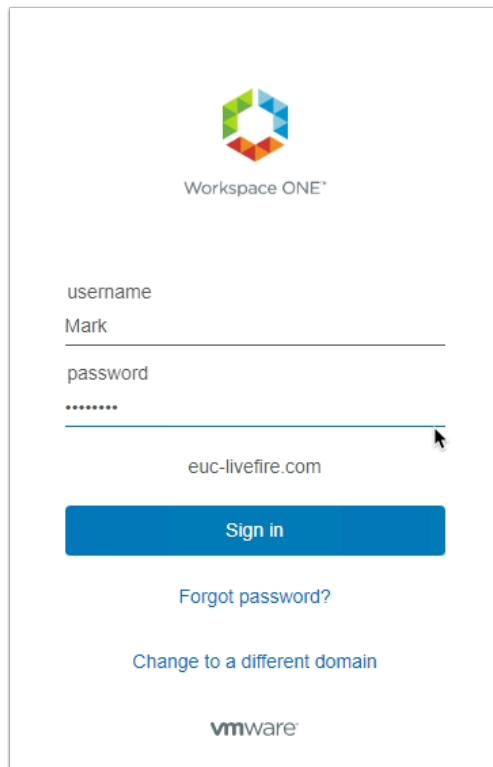
2. On your **Chrome Browser**

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



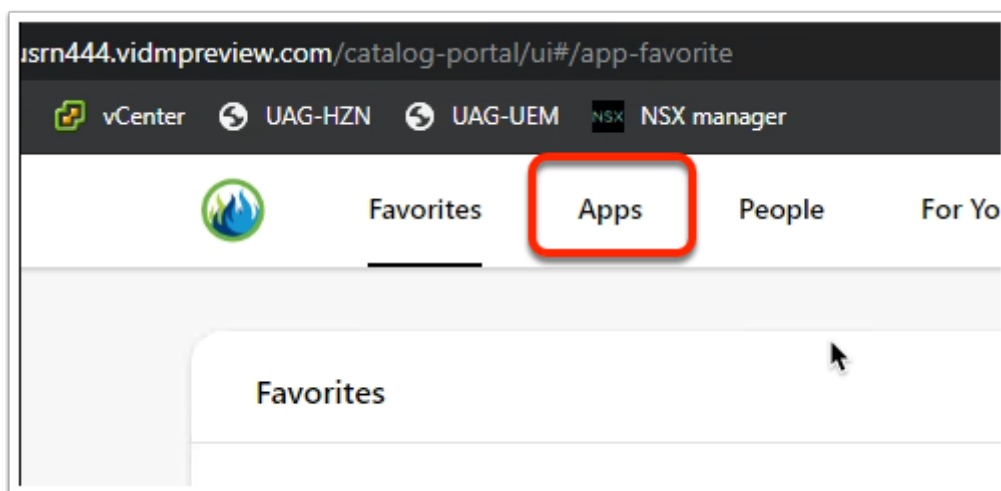
3. In the **Select Your Domain** window.

- Validate that the default domain **euc-livefire.com** is selected
- Select **Next**

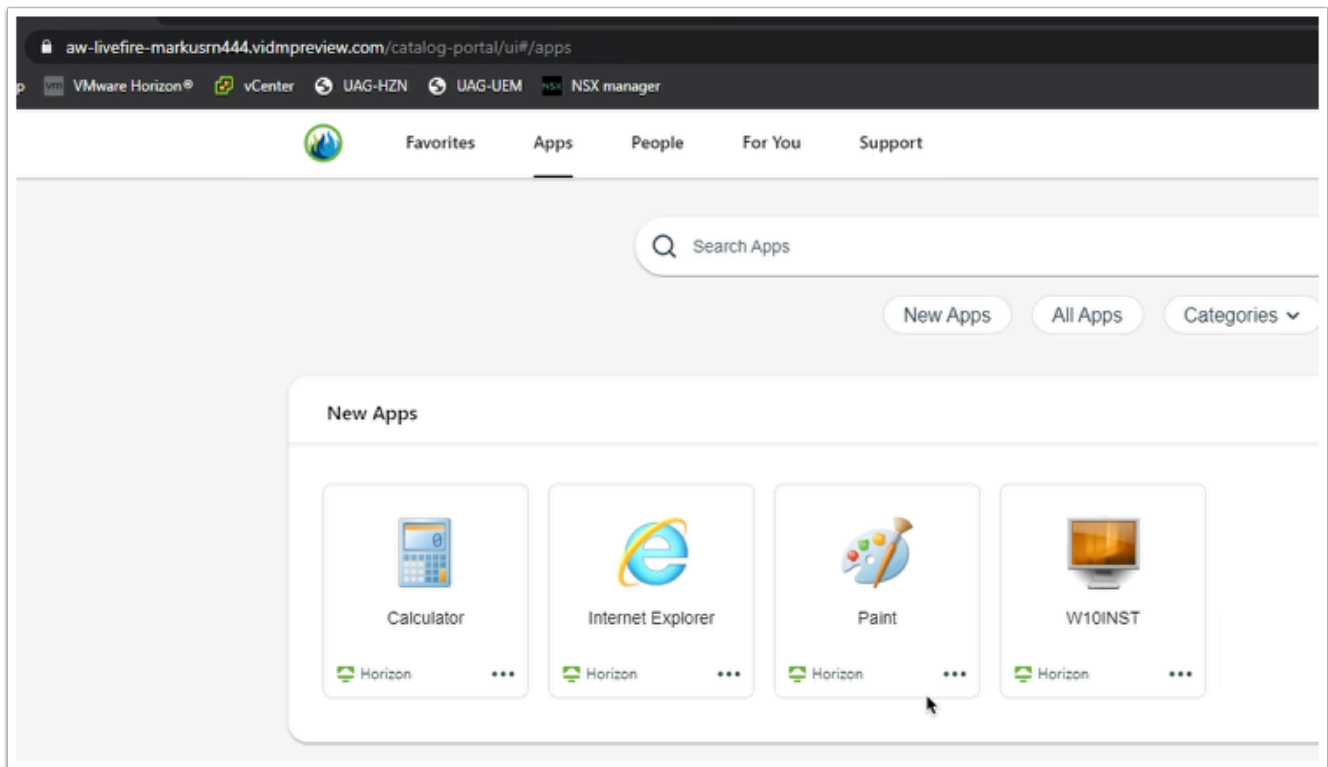


The image shows the Workspace ONE login interface. At the top is the Workspace ONE logo. Below it are two input fields: 'username' with the text 'Mark' and 'password' with masked characters '*****'. A blue 'Sign in' button is positioned below the password field. Under the button are two links: 'Forgot password?' and 'Change to a different domain'. At the bottom is the VMware logo.

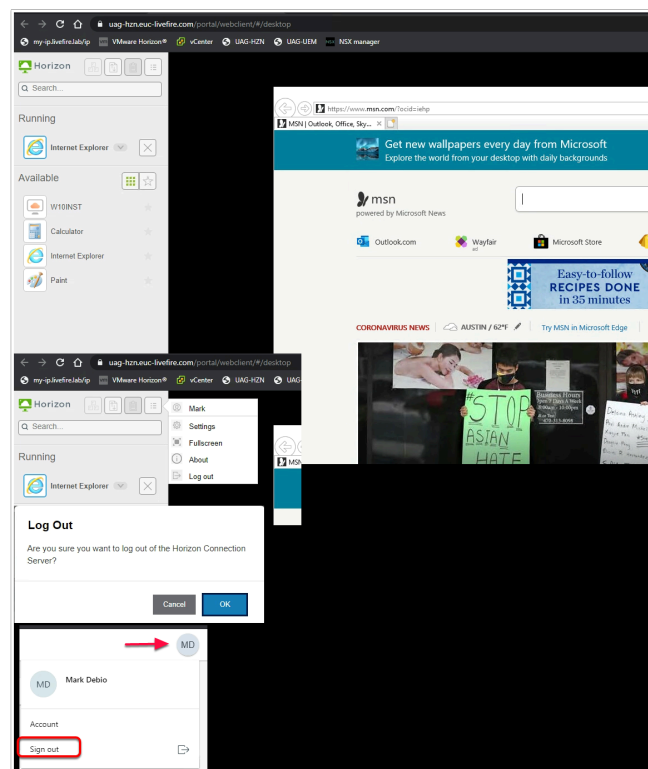
4. In the **Log in** window
- Under **username** enter **Mark**,
 - Under **password** enter **VMware1!**,
 - Select **Sign in**



5. Next to **Favorites**,
- Select **Apps**

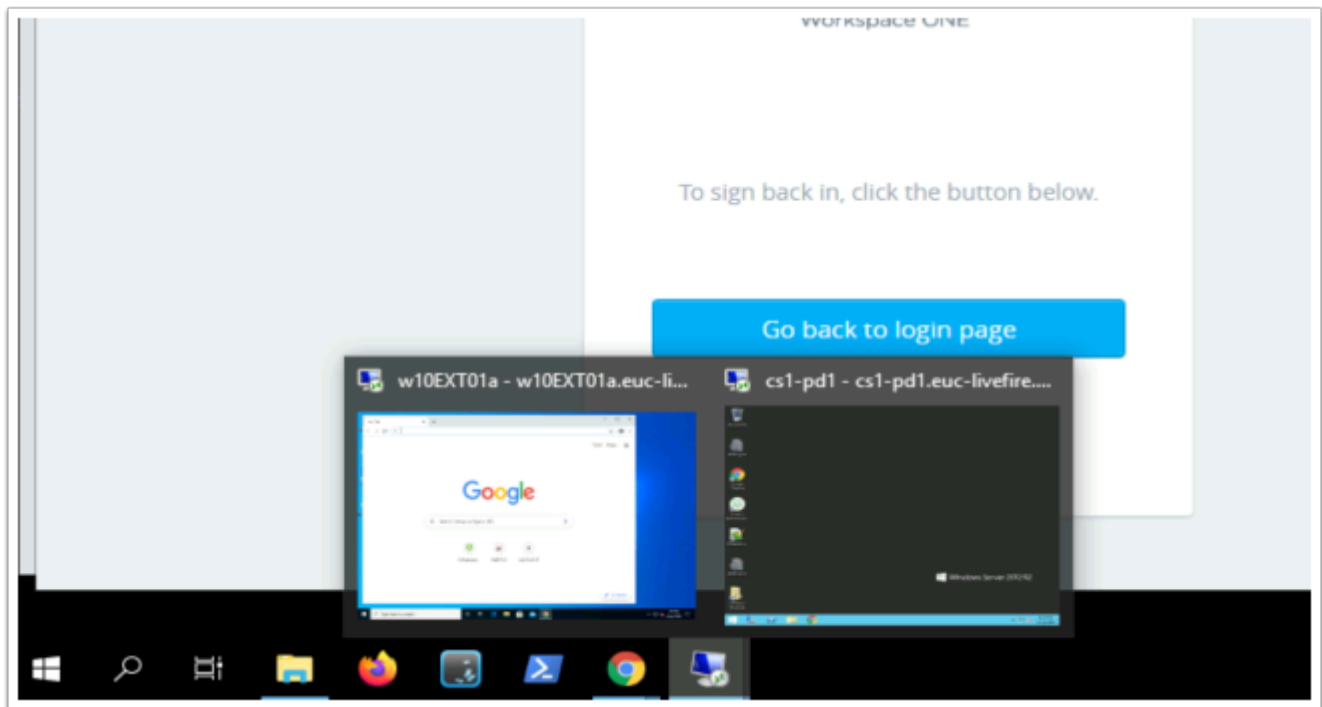


6. In the **Apps** area
 - Select **Internet Explorer**



7. Notice the Address in the Browser is our **Horizon Connection** server.
 - In this example, We have launched a Virtual Application from **Workspace ONE ACCESS** and our secure session is Tunneling through the Unified Access

- Select **Log out**
- On the **Log Off** window select **OK**
- In the top right hand corner, select your account Icon. In this example its **MD**, right-click, select **Sign Out**
- **Close** the browser



Conclusion

In Summary we looked at Best practice with the regard to configuring the Blast protocol for using with HTML Client. It is important to note that Native Client by default offers the same and possibly better user experience and we do not necessarily, see the errors we see with the HTML client. However best practices and configurations we saw in this exercise apply to both the Native and the HTML client

Acknowledgements and References

As author of this material, I wish to thank Graeme Gordon from TechMarketing for their continued support and guidance on getting this lab right

Some useful resource links to continue your development

https://techzone.vmware.com/resource/understand-and-troubleshoot-horizon-connections#HTML_Client_Access

<https://techzone.vmware.com/resource/zero-trust-secure-access-traditional-applications-vmware>

<https://docs.vmware.com/en/VMware-Horizon-7/7.1/com.vmware.horizon-view.security.doc/GUID-AA5D0A57-51A7-4FC1-A79B-AFD15A72499A.html>

<https://kb.vmware.com/s/article/2088354>

<https://theidentityguy.ca/2021/02/25/workspace-one-access-best-practices-in-policy-management/>

About the Author: Reinhart Nel

<https://www.livefire.solutions/meet-the-team/reinhartnel/>

For any questions related to this session, email Reinhart at RACE-Livefire-EUC@vmware.com