

## 2. Using Dynamic Environment Manager as part of a Workspace ONE solution for usability and security.


Horizon and Dynamic Environment Manager (DEM) provide a great combination of capabilities to apply DLP controls depending on a range of endpoint parameters and location information.

There are some features that might be used in the context of security, in our research. we have discovered some constraints with certain parameters and we will address the potential and the downside to this functionality

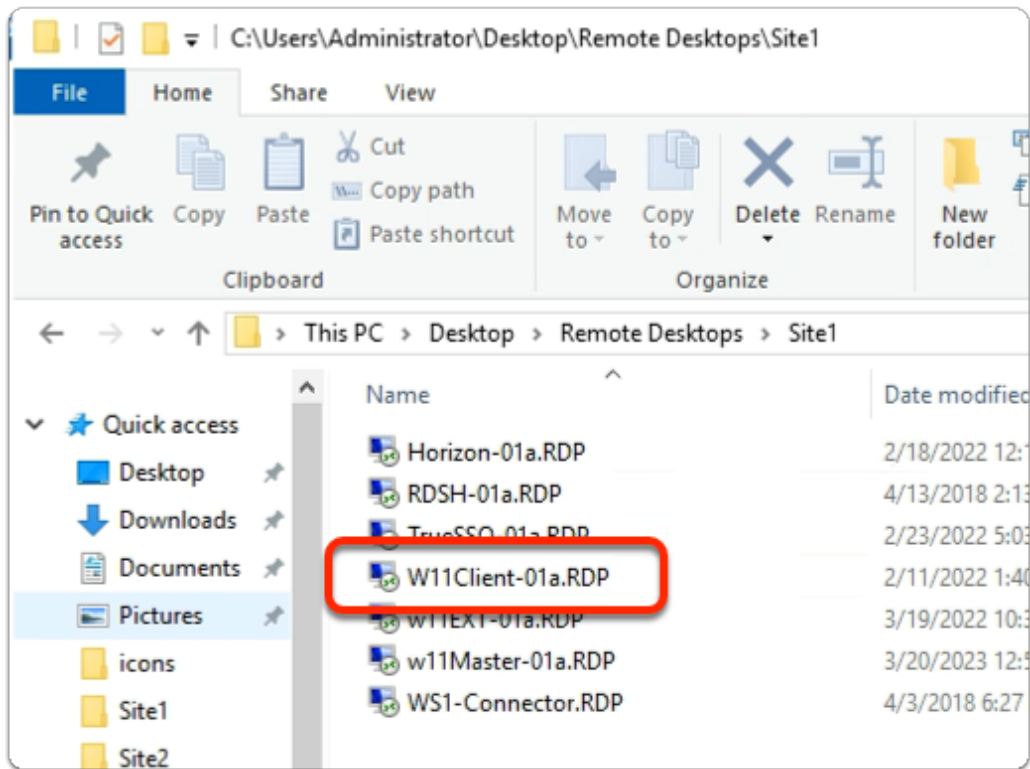
### Part 1: Identifying registry based configurations as a basis for the Conditional elements we could possibly use when using Horizon Smart Policies

This section will serve as an introduction to registry based configurations and what we choose from in the registry if we are wanting to use this configuration with Horizon Smart Policies

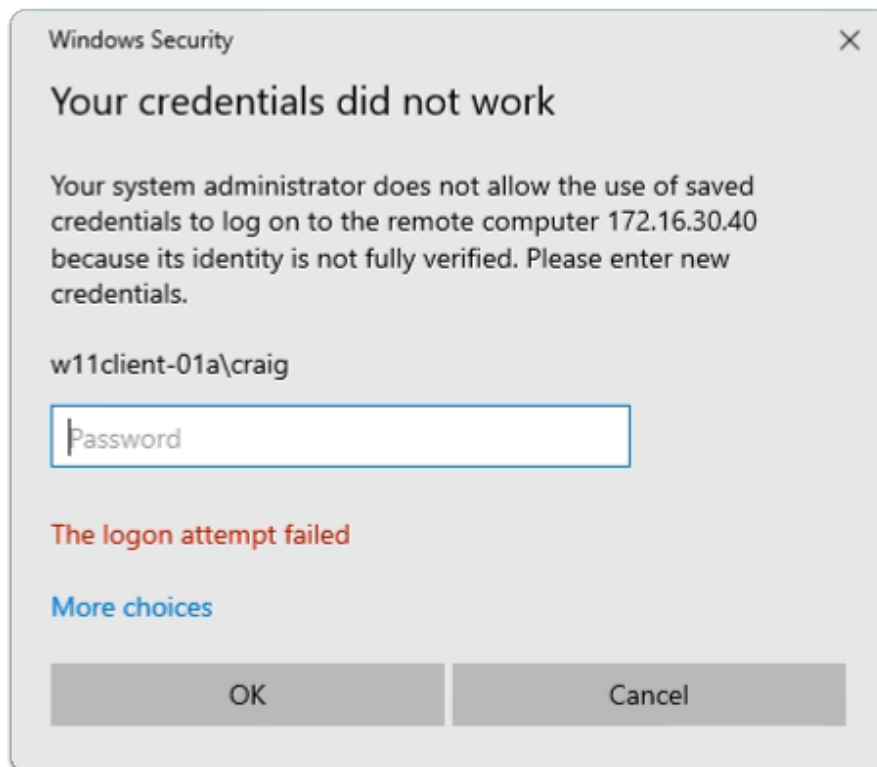
#### Identifying registry based configurations for the Condition based elements in Horizon Smart Policies

 You might still be logged in from a previous lab on the Horizon Client with the Craig accounts.

If you are you might be able to move down immediately to Step 9 in Part 1

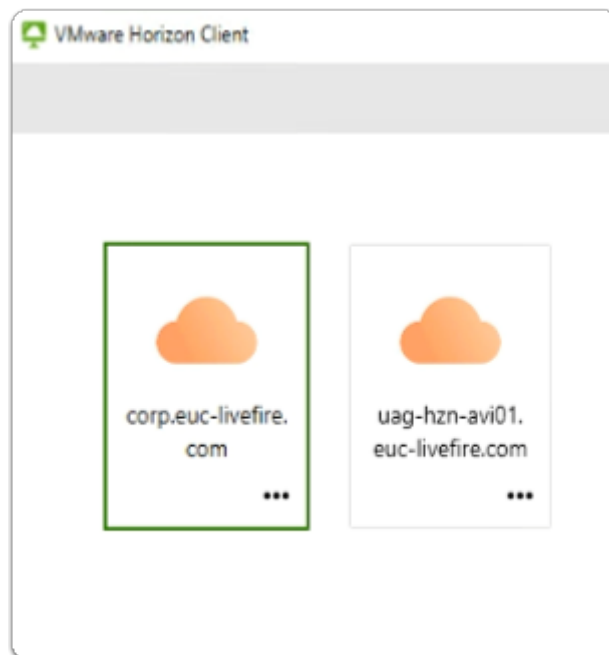


1. On your **ControlCenter** server
  - from the **Desktop**
    - Open the **Remote Desktops \ Site 1** folder
    - Launch the **W11Client-01a.rdp** shortcut

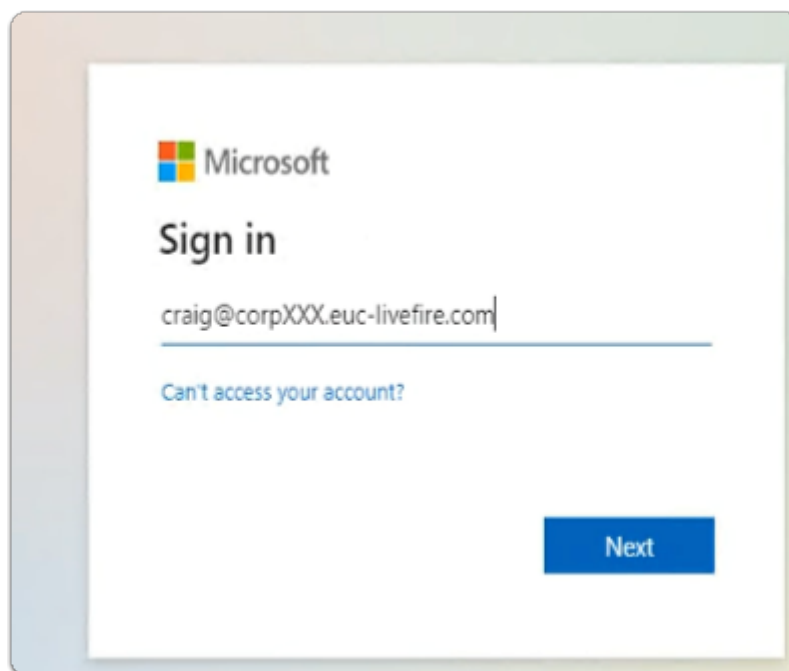


2. In the **Windows Security** page

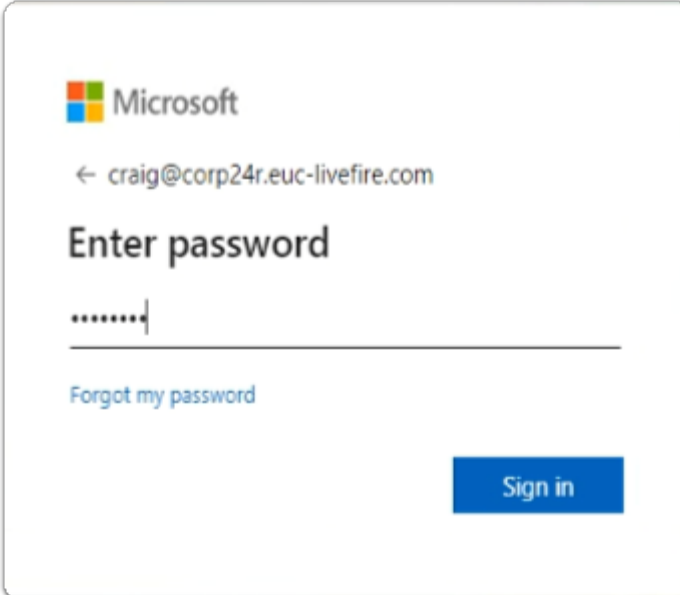
- ensure **Craig** is the username
- in the **password** area
  - enter **VMware1!**
- select **OK**



- 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

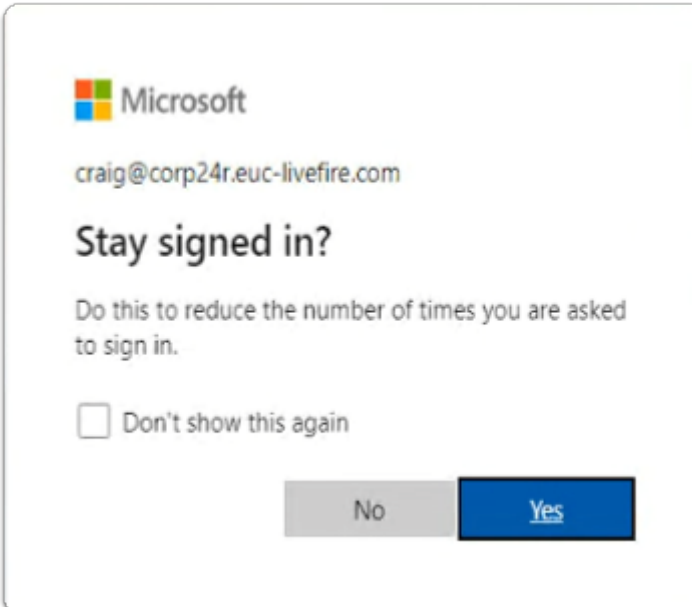


4. In the **Microsoft Sign in** window
- enter **Craig@corpXXX.euc-livfire.com**
    - where **XXX** is your assigned Domain identifier
  - select **Next**



The image shows a Microsoft sign-in window. At the top is the Microsoft logo. Below it is the email address 'craig@corp24r.euc-livfire.com' with a back arrow to its left. The main heading is 'Enter password'. Below this is a password input field with a masked password '.....'. To the left of the password field is a link that says 'Forgot my password'. At the bottom right is a blue button labeled 'Sign in'.

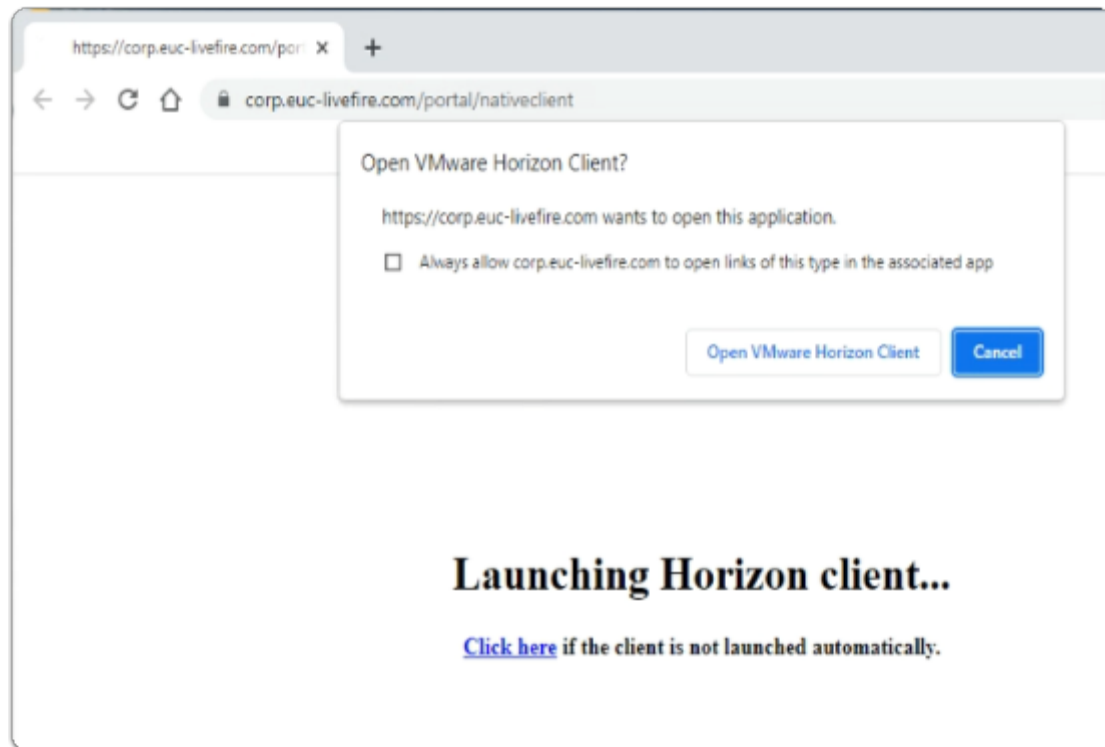
5. In the **Microsoft Enter password** window
- enter **VMware1!**
  - select **Sign in**



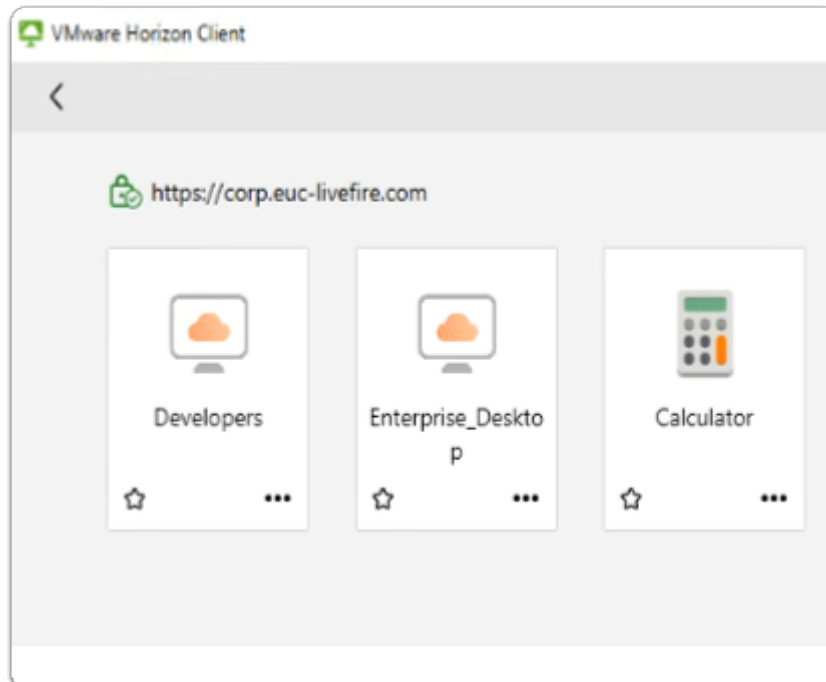
The image shows a Microsoft 'Stay signed in?' window. At the top is the Microsoft logo. Below it is the email address 'craig@corp24r.euc-livfire.com'. The main heading is 'Stay signed in?'. Below this is a sub-heading 'Do this to reduce the number of times you are asked to sign in.' followed by a checkbox and the text 'Don't show this again'. At the bottom are two buttons: a grey button labeled 'No' and a blue button labeled 'Yes'.

6. In the **Microsoft Stay signed in?**
- select **Yes**

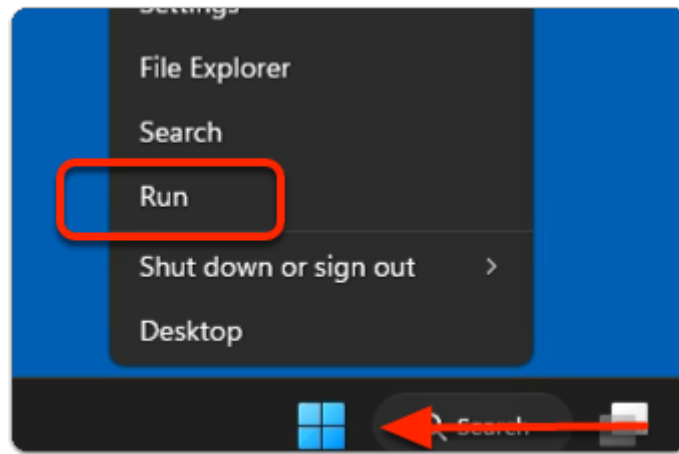




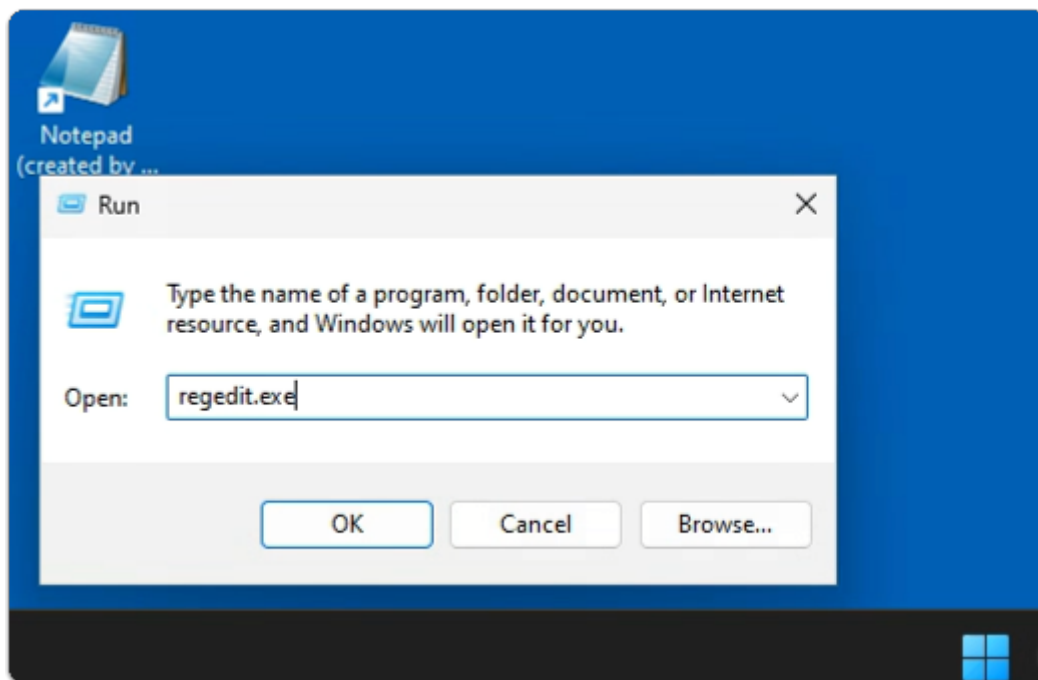
7. On your **W11Client-01a** desktop
  - on the **Open VMware Horizon Client?** window
    - select **Open VMware Horizon Client**



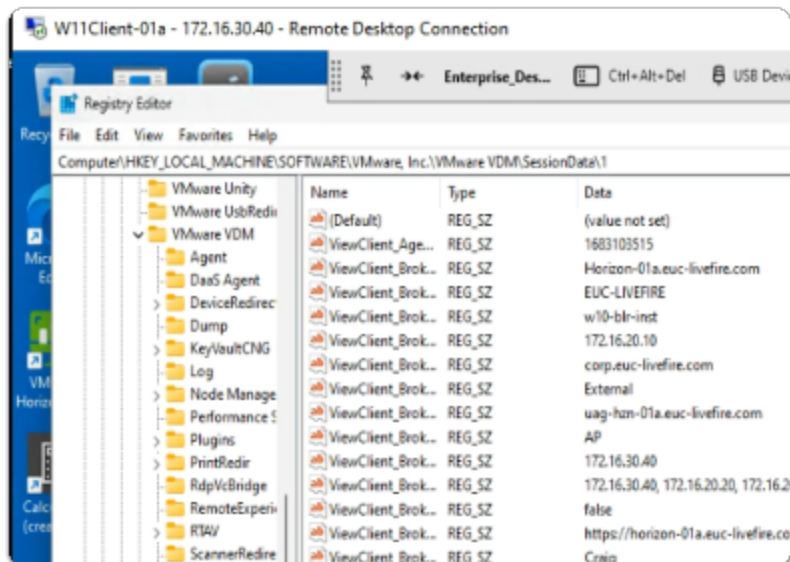
8. In the **VMware Horizon Client** login window
  - select the **Enterprise\_Desktop** entitlement



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

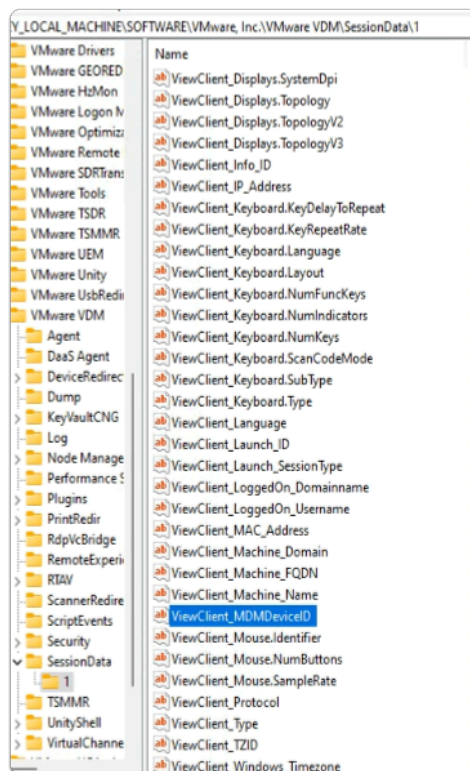


10. In the **Run** window
  - next to **Open:**
    - enter **regedit.exe**
  - select **OK**



11. In the **Registry Editor** window

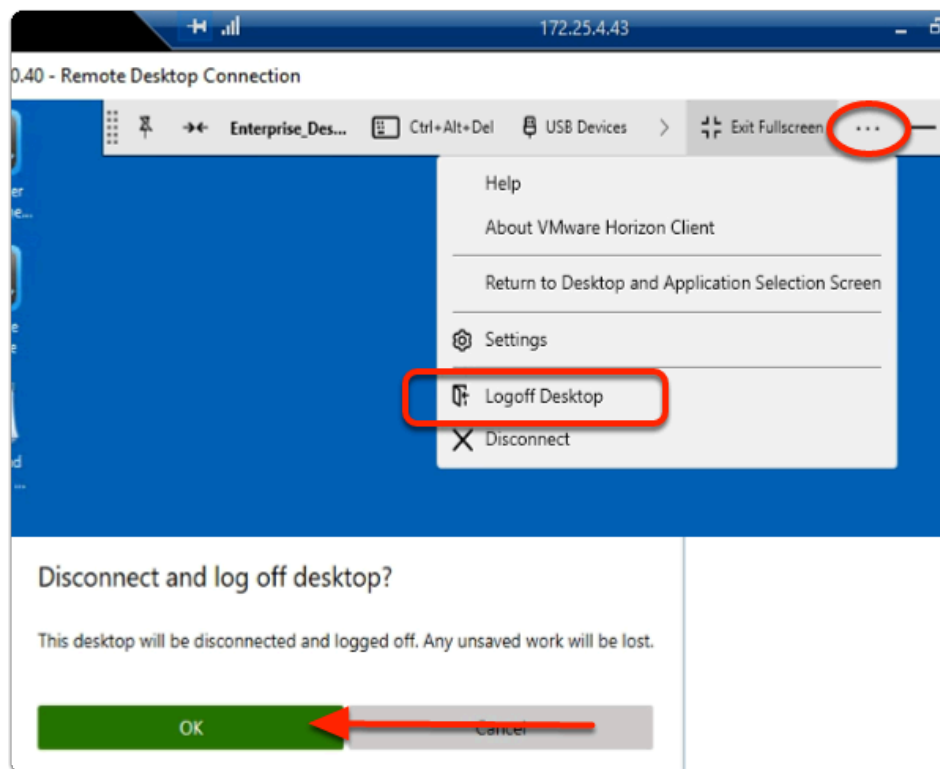
- from the **left Inventory pane**
- select and expand **HKEY\_LOCAL\_MACHINE > SOFTWARE > VMware, Inc. > VMware VDM > SessionData > 1**



12. In the **SessionData \ 1** folder

- Note the registry based **ViewClient\_ parameters** that are available. These can serve as part of a **Conditional Element** in **Horizon Smart Policies**
- Other than **Risk Scoring** functionality, with **DEM Conditions**, Its important to note, these are the only parameters we might consider using to manage and control the endpoint session in Dynamic Environment Manager.

- In the next Parts we will look at example parameters like and evaluate how secure this approach ACTUALLY is
  - **ViewClient\_MDMDeviceID** : enrolled devices
  - **ViewClient\_Broker\_GatewayLocation** or **Client Location**: which has the value of Internal or External
  - Other examples of contributing to endpoints being Secured and Usable when accessing resources using Horizon in an Organization could be
    - **ViewClient\_Machine\_Domain**: the remote **Windows 10/11** clients domain name
    - **ViewClient\_Machine\_Name**: the remote **Windows 10/11** clients PC name



### 13. In the Horizon Client VDI session

- next to **Exit Fullscreen**
  - select the **more options** icon
    - select **Logoff Desktop**
- In the **Disconnect and log off desktop?** window
  - select **OK**

## Part 2: Setting up VMware Horizon Smart Policies with VMware Dynamic Environment Manager

This part is divided up into two sections.

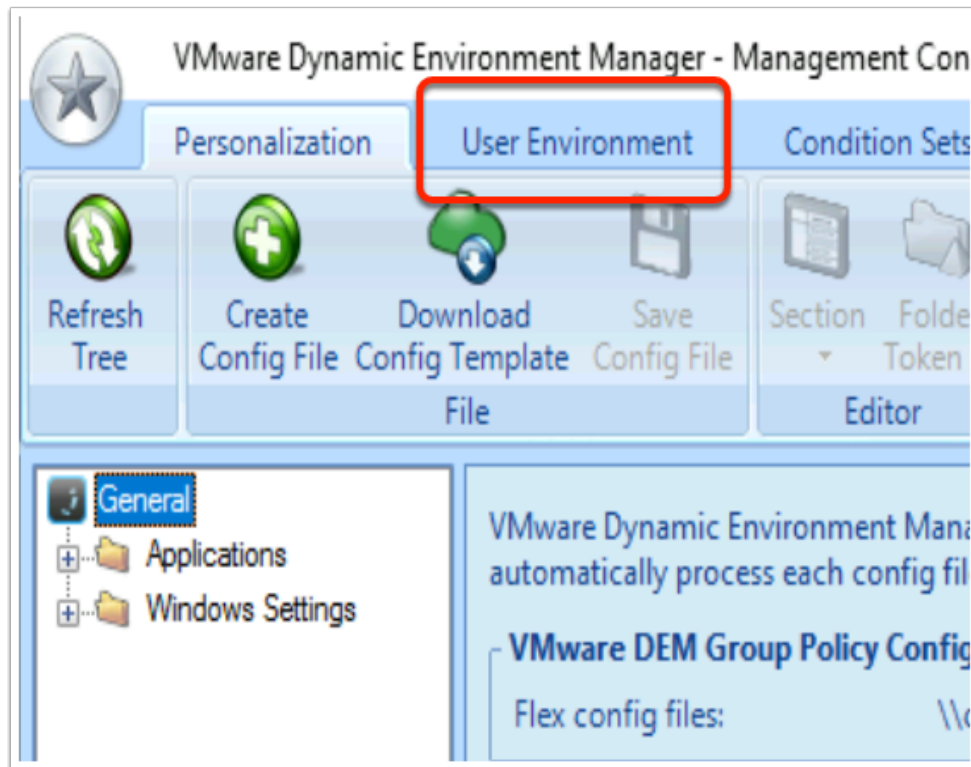
Section 1: We will create a Horizon Smart Policy for external endpoints that are Managed by Workspace ONE UEM

Section 2: We will create a Horizon Smart Policy for external endpoints that are UnManaged by Workspace ONE UEM

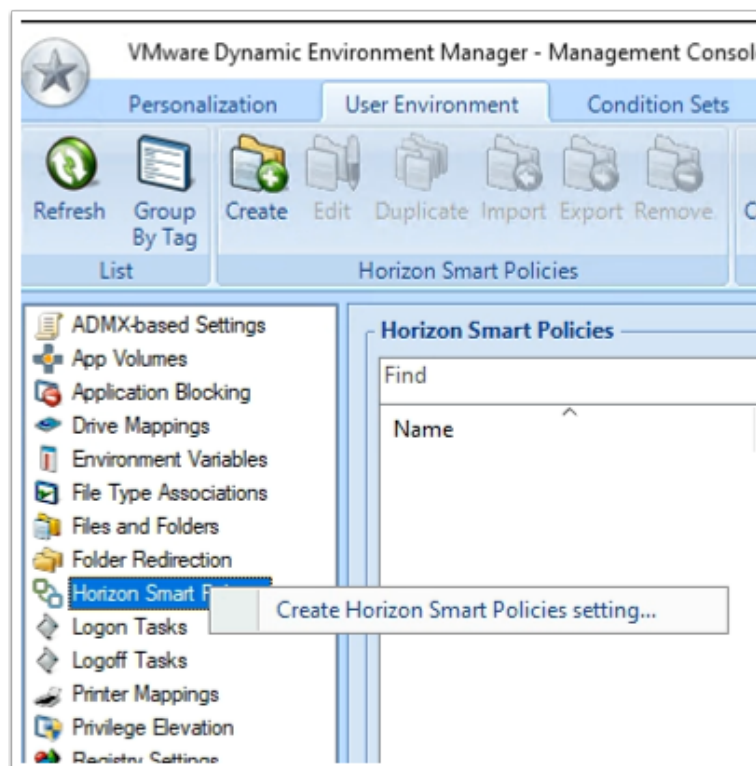
## Section 1: Setting up a Smart Policy for Trusted Devices using the ManagedDevices property



1. On your ControlCenter server Desktop
  - from the **Taskbar**
    - select and launch, the **DEM management Console** shortcut

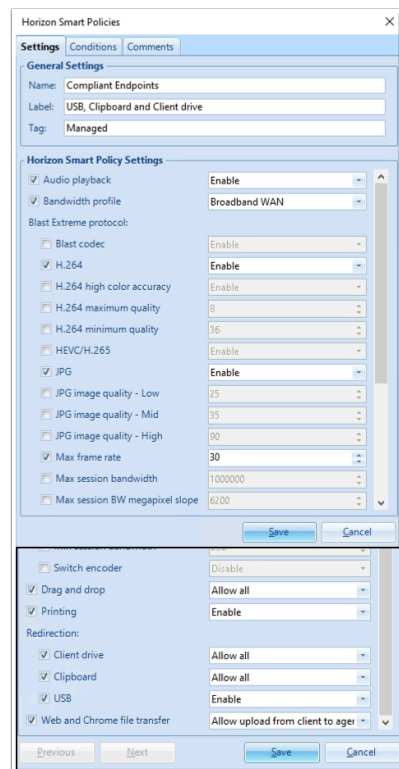


2. In the Dynamic Environment Manager Console
  - Select the **User Environment** tab



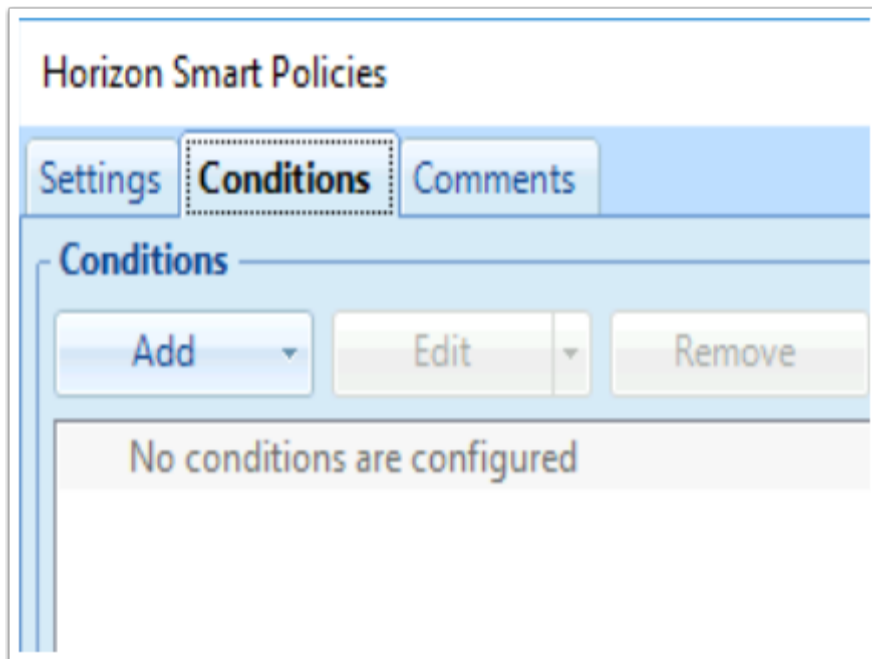
3. In the Dynamic Environment Manager Console
  - In the **User Environment** Inventory
    - Select **Horizon Smart Policies**,

- Right-click and select **Create Horizon Smart Policies setting...**

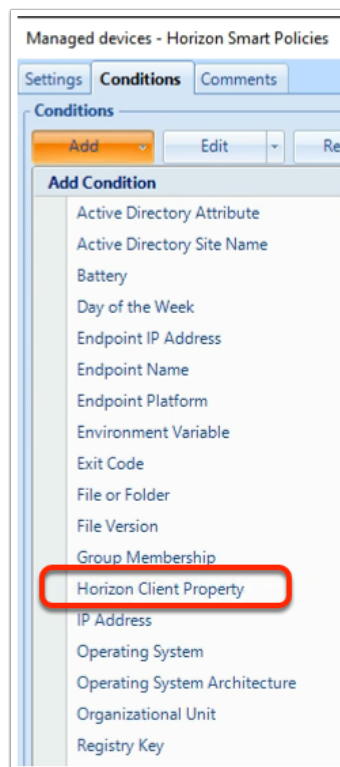


4. In the **Horizon Smart Policies**, window

- Under the **Settings** tab
  - enter the following:-
    - Under **General** Settings, enter the following, next to:
      - **Name:** **Compliant Endpoints**
      - **Label:** **USB, Clipboard and Client drive**
      - **Tag:** **Managed**
    - In the **Horizon Smart Policy Settings**, enable the following checkboxes, next to:
      - **Audio Playback :** **Enable**
      - **Bandwidth Profile :** **Broadband WAN**
      - **Blast Extreme protocol**
        - **H.264:** **Enable**
        - **JPG:** **Enable**
        - **Max frame rate :** **30**
    - **Drag and drop :** **Allow all**
    - **Printing :** **Enable**
    - In the **Redirection** settings, enable the following checkboxes and associated settings, next to:
      - **Client drive :** **Allow all**
      - **Clipboard :** **Allow all**
      - **USB :** **Enable**
    - **Web and Chrome file transfer:** **Allow all**



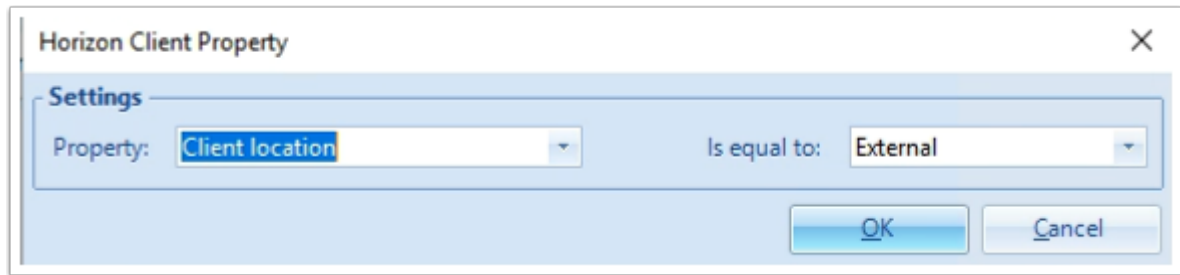
5. In the **Horizon Smart Policies** window
  - Select the **Conditions** tab
  - Under **Conditions**, select the **dropdown** next to **Add**



6. In the **Add Condition** dropdown
  - Select **Horizon Client Property**
  - Note: By default, if you connect directly to a **View Connection Server**,
    - the gateway location is **Internal**

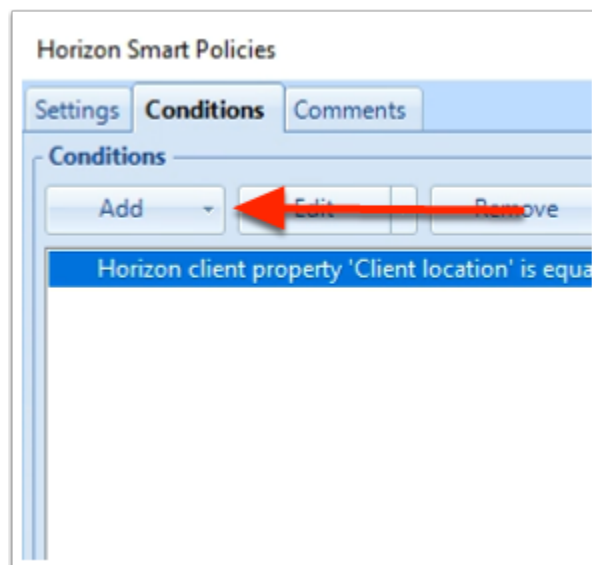


- If you connect to an **Unified Access Gateway Server**,
- the gateway location is **External** by default.



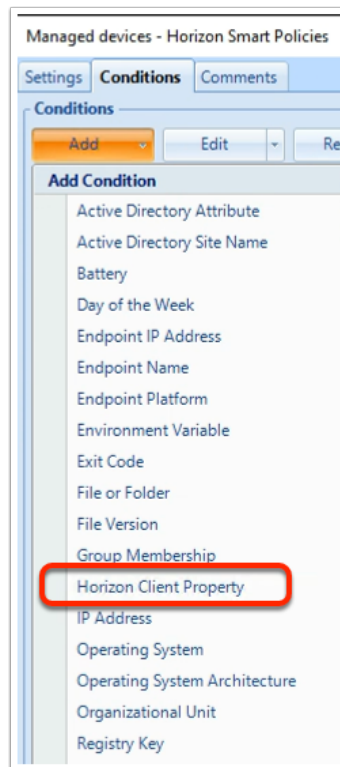
7. In the **Horizon Client Property**, add the following:

- next to **Property**,
  - from the **dropdown**
    - select **Client location**
- next to **Is equal to**,
  - from the **dropdown**
    - select **External**
- To close the **Horizon Client Property**
  - select **OK**

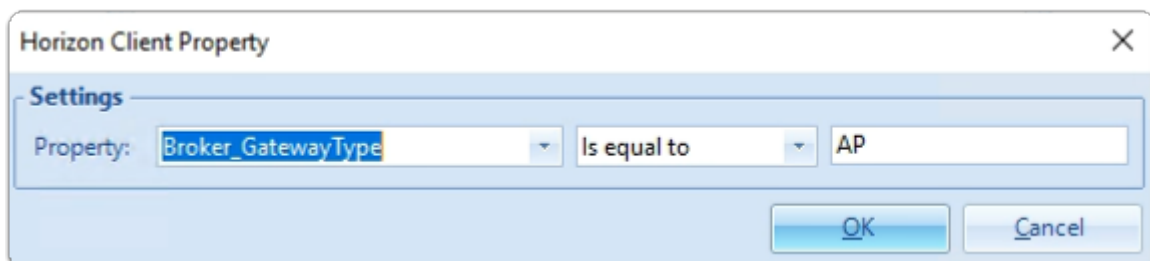


8. In the **Horizon Smart Policies** window

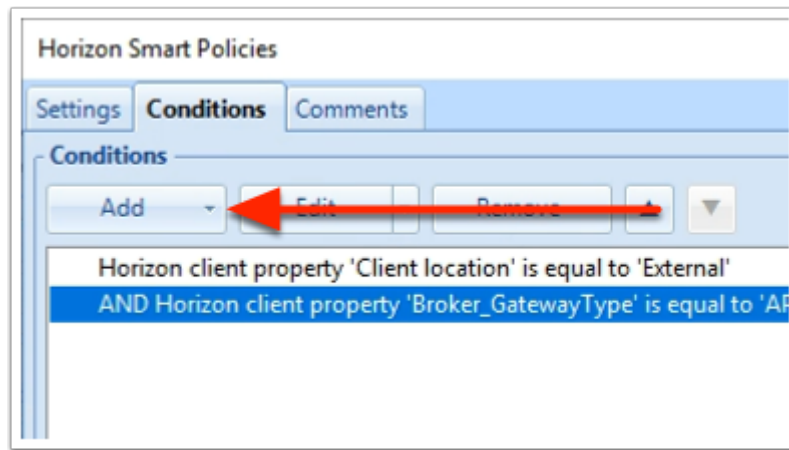
- In the **Conditions** tab
  - next to **Add**
    - select the **dropdown**



9. In the **Add Condition** dropdown
  - Select **Horizon Client Property**

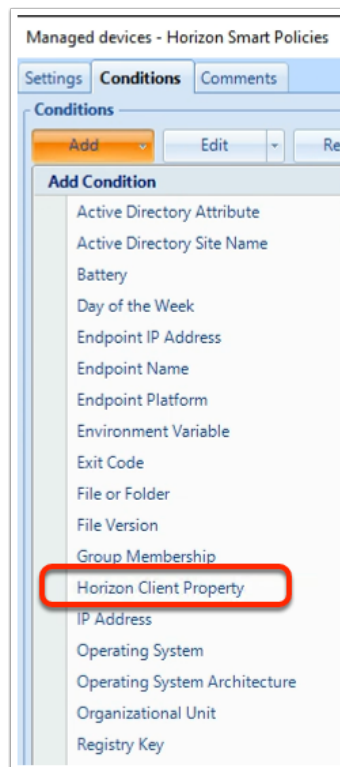


10. In the **Horizon Client Property** window,
  - next to **Property:**
    - enter **Broker\_GatewayType**
  - next to **Broker\_GatewayType**
    - from the **dropdown**
      - select **Is equal to**
  - In the box area, to the right of **Is equal to**
    - enter **AP**
  - select **OK**



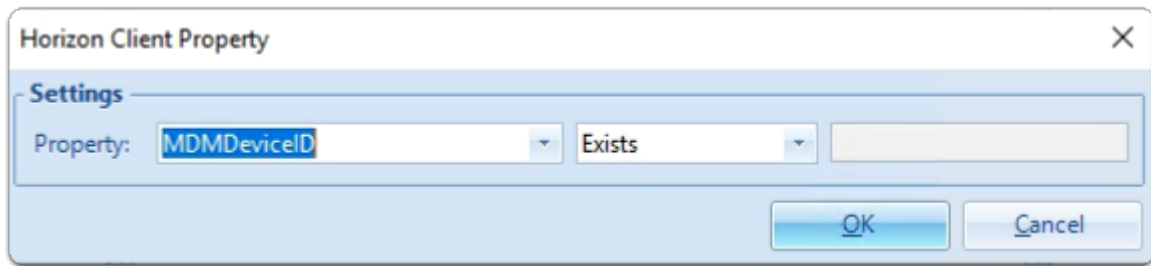
11. In the **Horizon Smart Policies** window

- In the **Conditions** tab
  - next to **Add**
    - select the **dropdown**

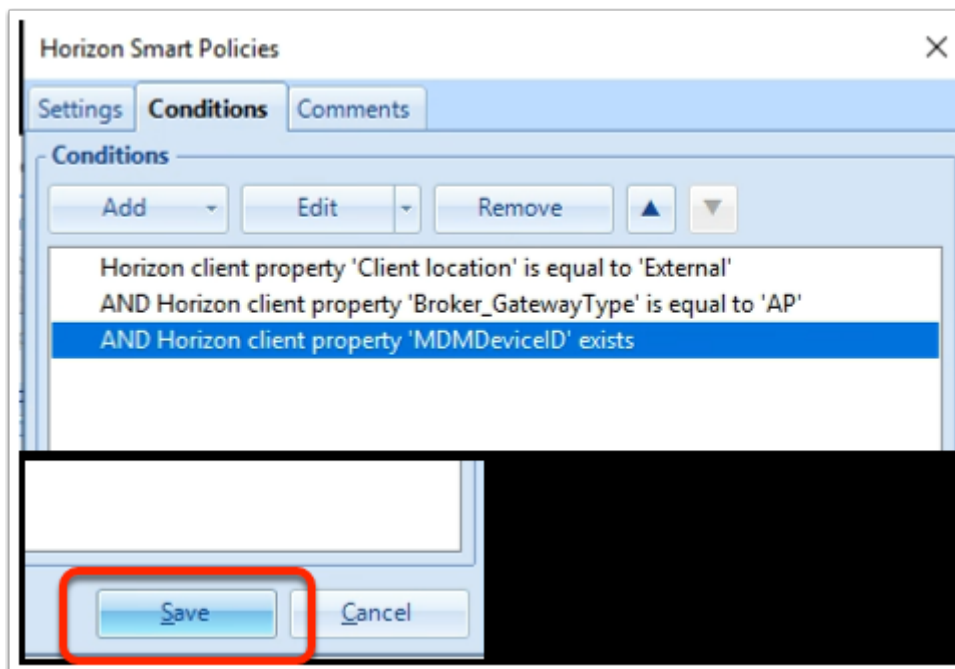


12. In the **Add Condition** dropdown

- Select **Horizon Client Property**

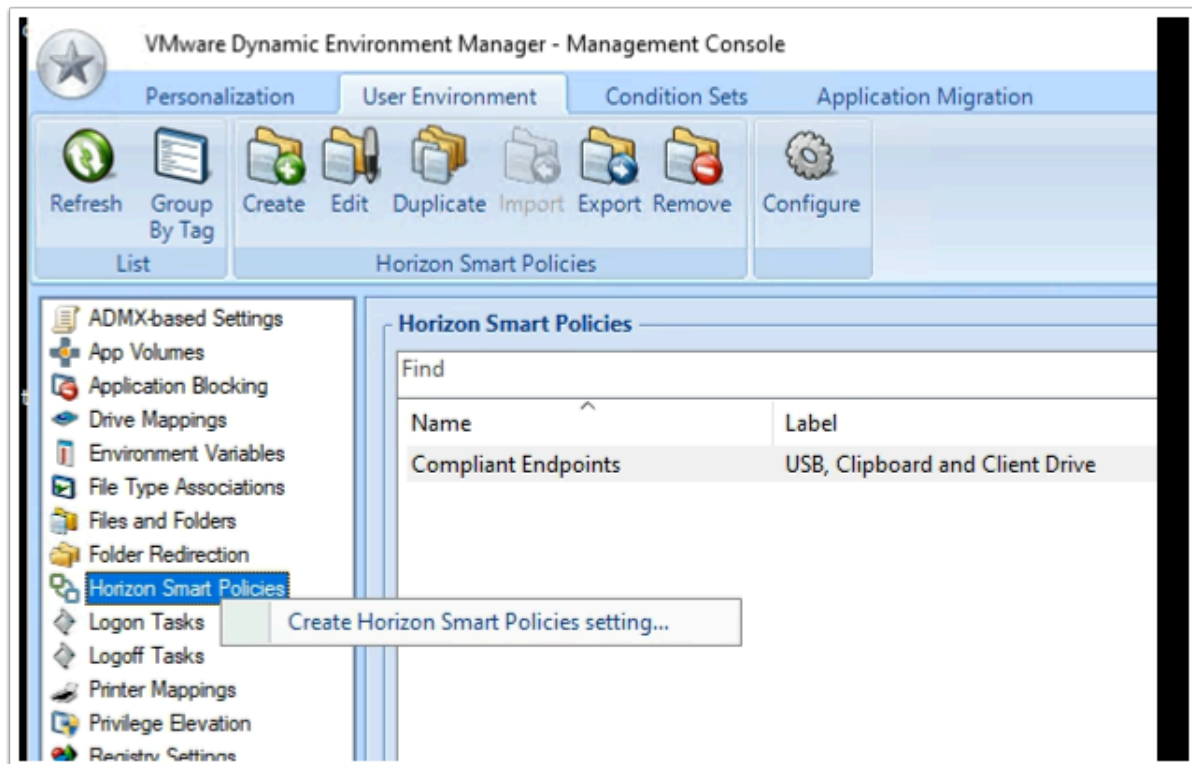


13. In the **Horizon Client Property** window,
  - next to **Property:**
    - enter **MDMDeviceID**
  - next to **MDMDeviceID**
    - ensure **Exists** is selected
  - select **OK**



14. In the **Horizon Smart Policies** window
  - Select **Save**

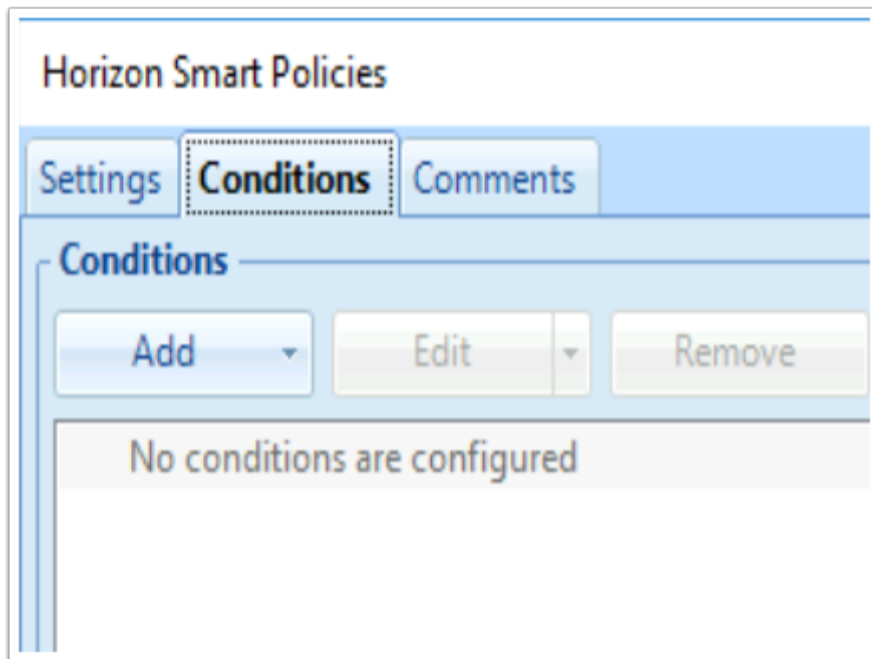
## Section 2: Setting up a Smart Policy for UnTrusted Devices using the ManagedDevices property



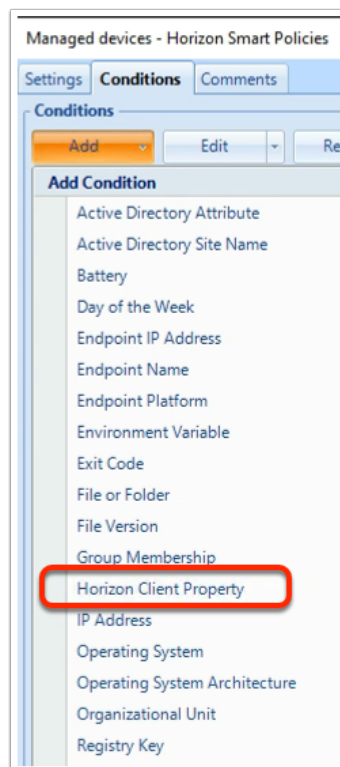
1. In the **User Environment** Inventory
  - Select **Horizon Smart Policies**,
  - Right-click and select **Create Horizon Smart Policies setting...**

The screenshot shows the 'Unmanaged Devices - Horizon Smart Policies' window. The 'Settings' tab is selected. In the 'General Settings' section, the 'Name' is 'Non Compliant Devices', the 'Label' is 'USB, Clipboard and Client drive disabled', and the 'Tag' is 'UnManaged'. The 'Horizon Smart Policy Settings' section contains a list of settings: 'JPG' is checked and set to 'Enable'; 'JPG image quality - Low' is 25, 'JPG image quality - Mid' is 35, and 'JPG image quality - High' is 90; 'Max frame rate' is checked and set to 30; 'Max session bandwidth' is 1000000; 'Max session BW megapixel slope' is 6188; 'Min session bandwidth' is 256; 'Switch encoder' is checked and set to 'Disable'; 'Drag and drop' is checked and set to 'Disable'; 'Printing' is checked and set to 'Enable'. Under the 'Redirection' section, 'Client drive', 'Clipboard', 'USB', and 'Web and Chrome file transfer' are all checked and set to 'Disable'. At the bottom, there are 'Previous', 'Next', 'Save', and 'Cancel' buttons.

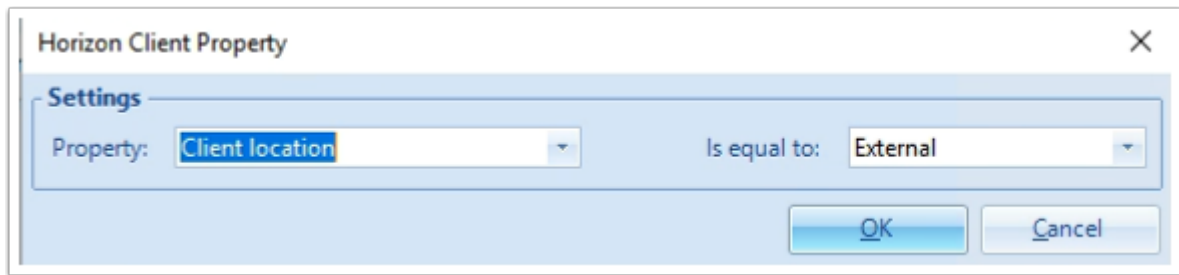
2. In the **Horizon Smart Policies, Settings** tab enter the following:-
  - Under **General** Settings, enter the following, next to:
    - **Name: Non Compliant Endpoints**
    - **Label: USB, Clipboard and Client drive disabled**
    - **Tag: UnManaged**
  - In the **Horizon Smart Policy Settings**, enable the following checkboxes, next to:
    - **Audio Playback : Enable**
    - **Bandwidth Profile : Broadband WAN**
    - **Blast Extreme protocol**
      - **H.264: Enable**
      - **Max frame rate : 30**
    - **Drag and drop : Disable**
  - In the **Redirection** settings, enable the following checkboxes and associated settings, next to:
    - **Client drive : Disable**
    - **Clipboard : Disable**
    - **USB : Disable**
  - **Web and Chrome file transfer: Disable**



3. In the **Horizon Smart Policies** window
  - Select the **Conditions** tab
  - Under **Conditions**, select the **dropdown** next to **Add**

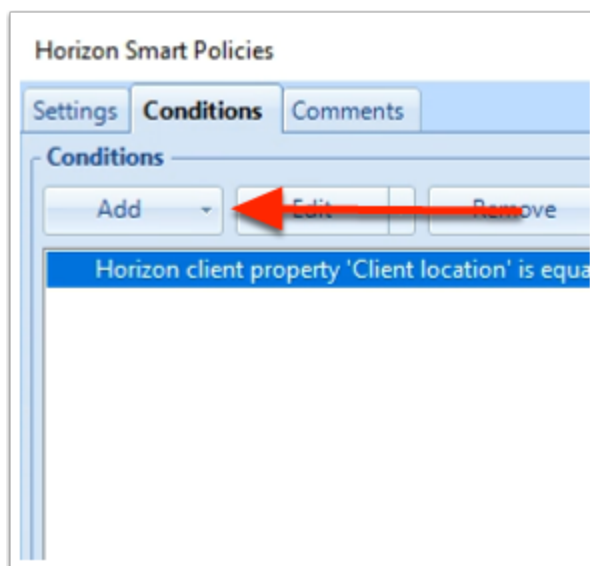


4. In the **Add Condition** dropdown
  - Select **Horizon Client Property**



5. In the **Horizon Client Property**, add the following:

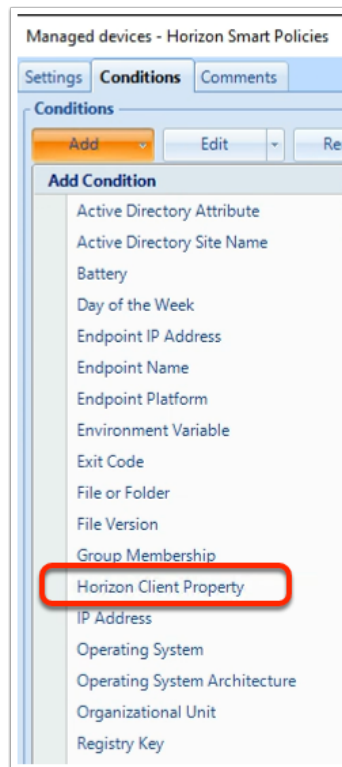
- next to **Property**,
  - from the **dropdown**
    - select **Client location**
- next to **Is equal to**,
  - from the **dropdown**
    - select **External**
- To close the **Horizon Client Property**
  - select **OK**



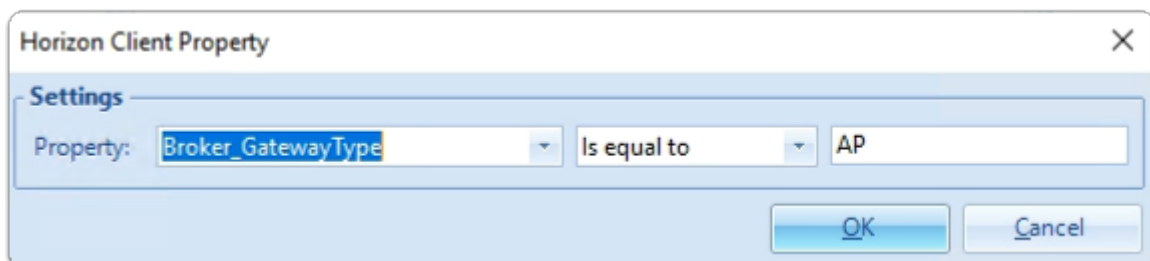
6. In the **Horizon Smart Policies** window

- In the **Conditions** tab
  - next to **Add**
    - select the **dropdown**

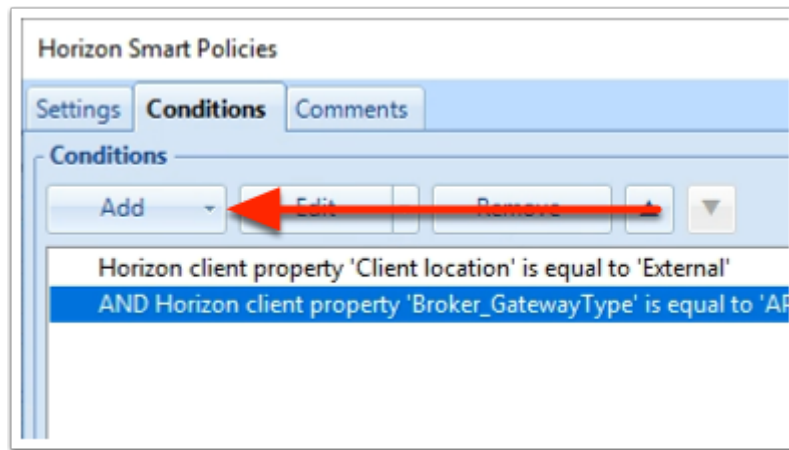




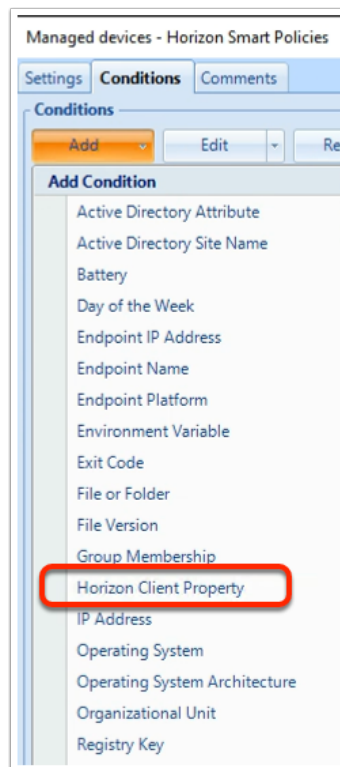
7. In the **Add Condition** dropdown
  - Select **Horizon Client Property**



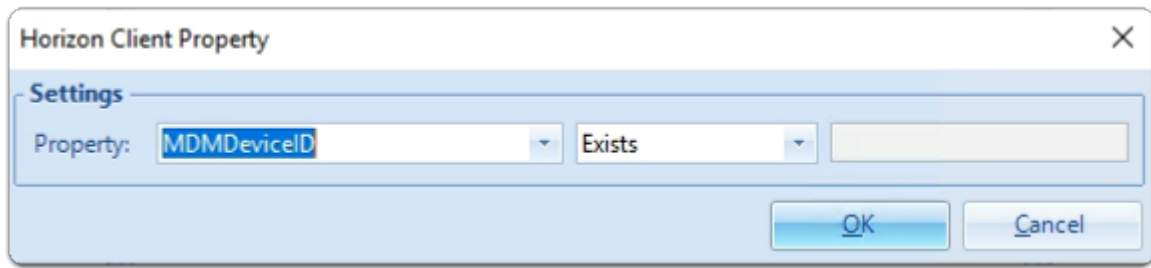
8. In the **Horizon Client Property** window,
  - next to **Property:**
    - enter **Broker\_GatewayType**
  - next to **Broker\_GatewayType**
    - from the **dropdown**
      - select **Is equal to**
  - In the box area, to the right of **Is equal to**
    - enter **AP**
  - select **OK**



9. In the **Horizon Smart Policies** window
  - In the **Conditions** tab
    - next to **Add**
      - select the **dropdown**

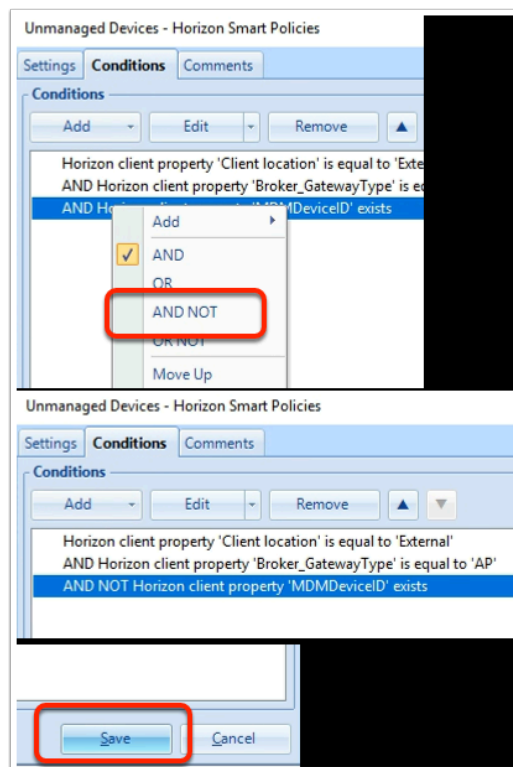


10. In the **Add Condition** dropdown
  - Select **Horizon Client Property**



11. In the **Horizon Client Property** window,

- next to **Property:**
  - enter **MDMDeviceID**
- next to **MDMDeviceID**
  - ensure **Exists** is selected
- select **OK**



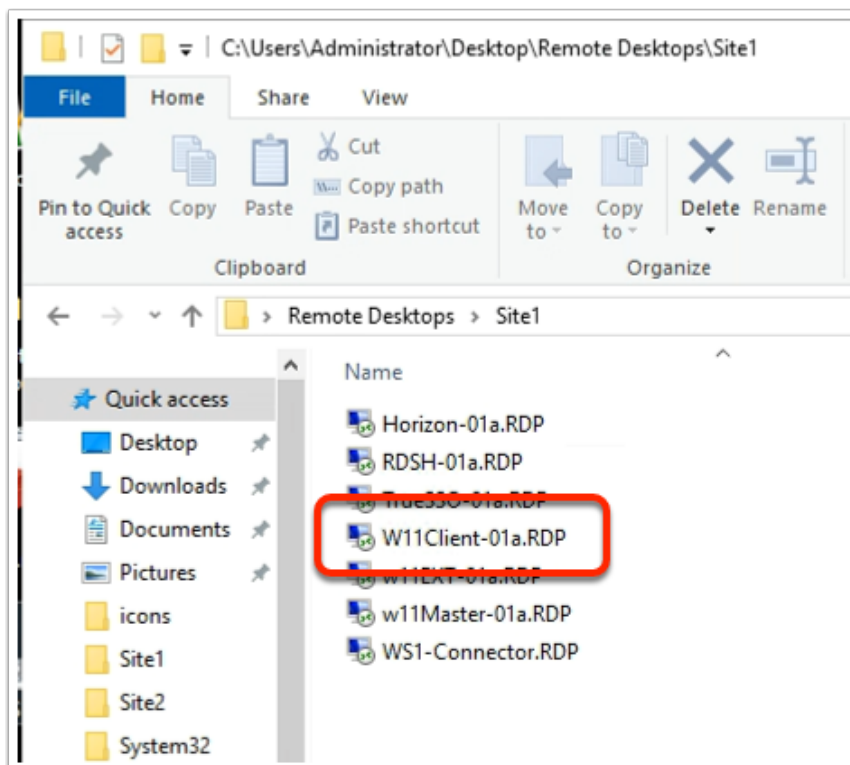
12. In the **Horizon Smart Policies** window

- next to AND Horizon client property 'MDMDeviceID' exists
  - **select & right-click** and **from the dropdown**
    - select **AND NOT**
- Select **Save**

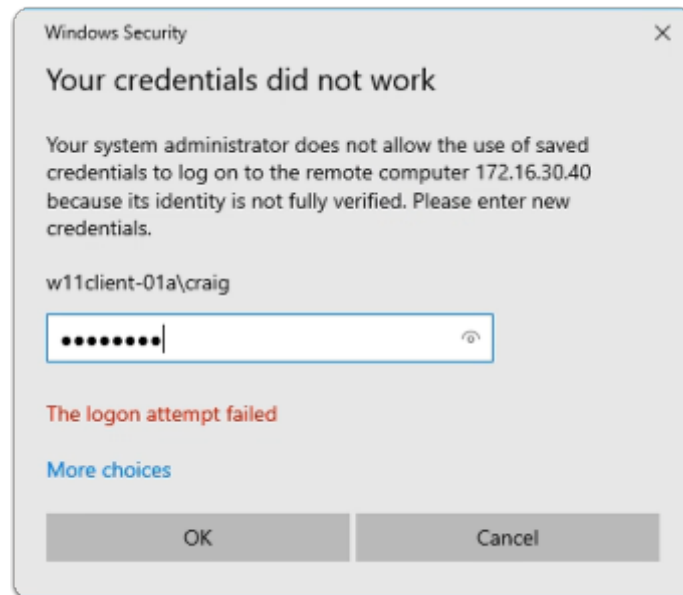
## Part 3 : Testing your Smart Policies.

- We will demonstrate the following in this exercise
  - That being **Drag and Drop** functionality.
  - **USB redirection** (limited functionality here)
  - We will use the Dynamic Environment Manager Logs, to see if the settings are effective.
- We will use a Managed and UnManaged device to test this setup
  - W11Client-01a is our managed device
  - W11EXT-01a is our unmanaged device
- We will use the **Sales User Mark** to test this functionality

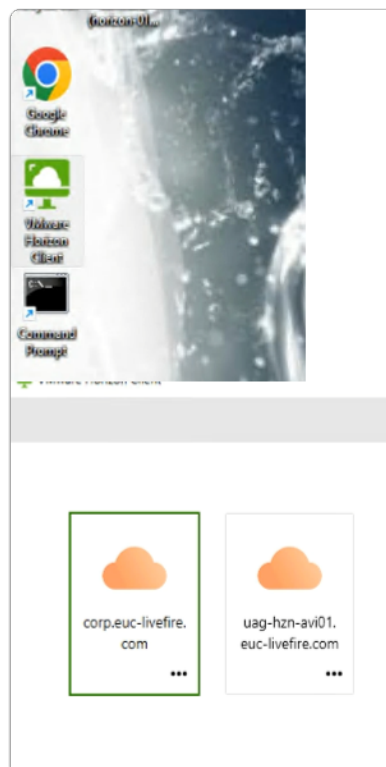
### Step 1: Testing the Smart Policies for a Managed device



1. On your **ControlCenter server desktop**
  - Open the **Remote Desktop \ Site 1** folder
  - launch **W11Client-01a.RDP**

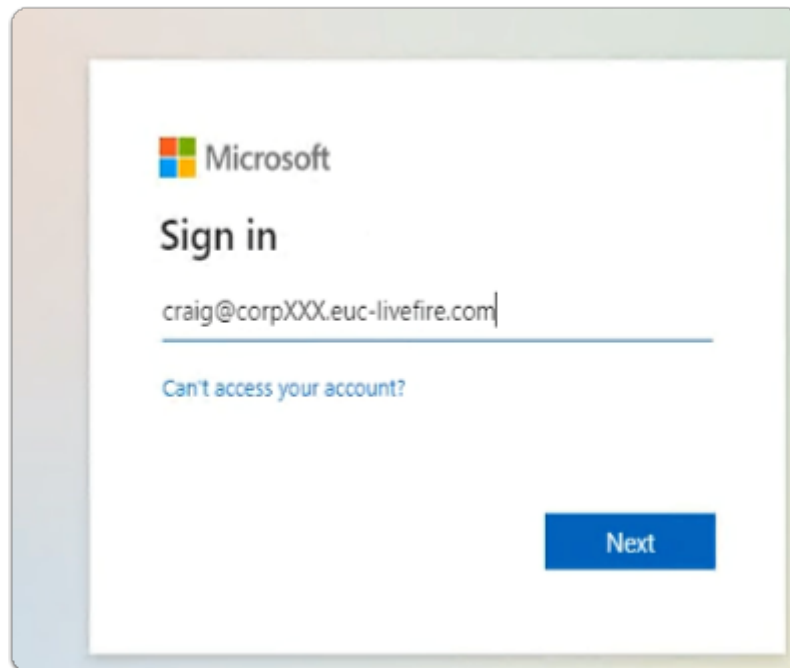


2. In the **Windows Security** page
  - using the **W11client-01a\craig** as username
  - in the **password** area
    - enter **VMware1!**
  - select **OK**

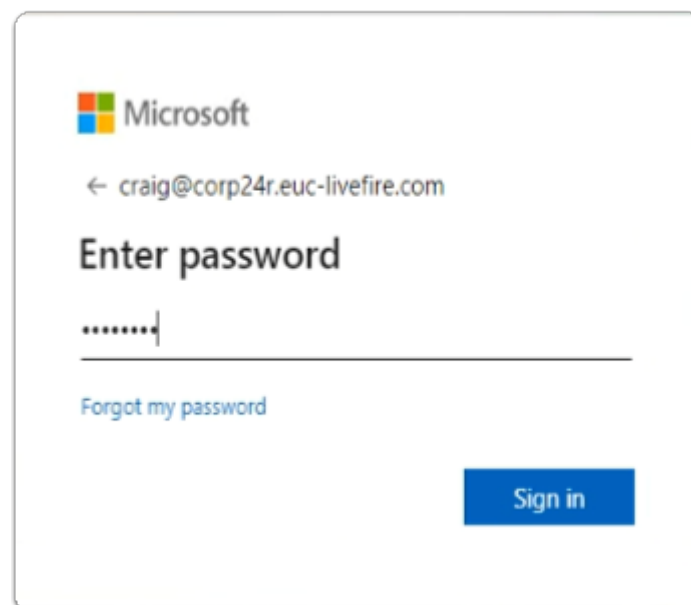


3. On your **W11Client-01a** desktop
  - From the **taskbar** or **Desktop**
    - launch your **VMware Horizon Client**

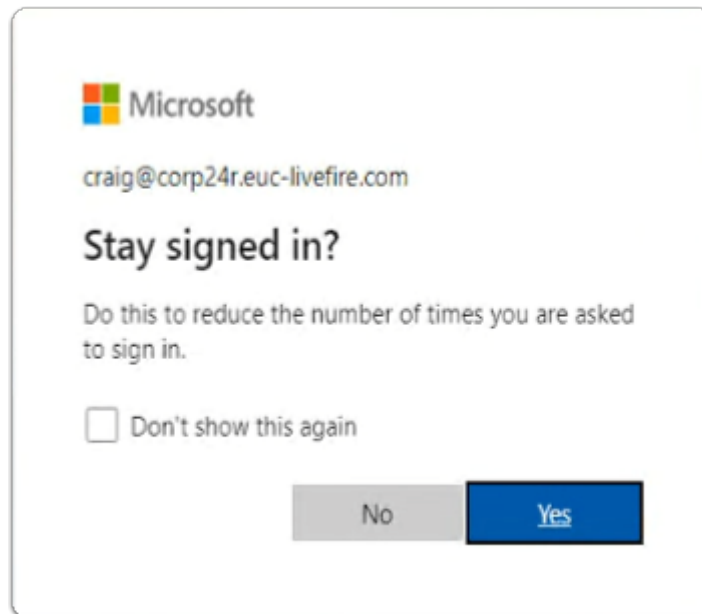
- In the **VMware Horizon Client** window
  - select **corp.euc-livewire.com** broker URL



4. In the **Microsoft Sign in** window
  - enter **Craig@corpXXX.euc-livewire.com**
    - where **XXX** is your assigned Domain identifier
  - select **Next**

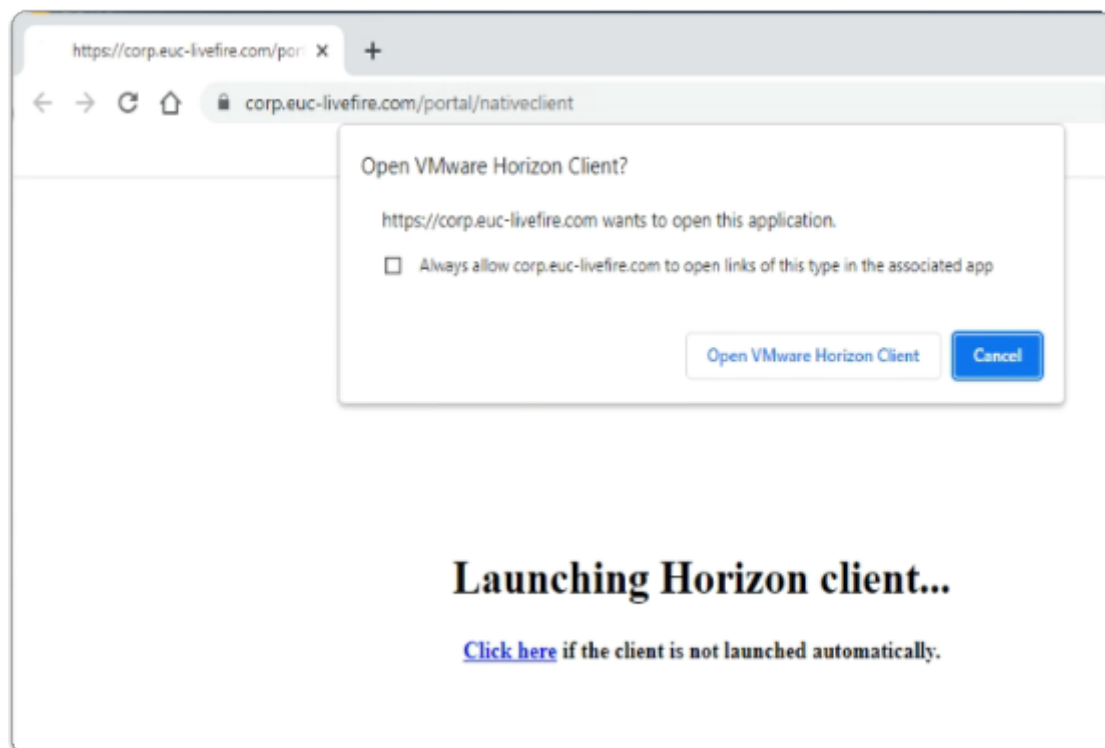


5. In the **Microsoft Enter password** window
  - enter **VMware1!**
  - select **Sign in**



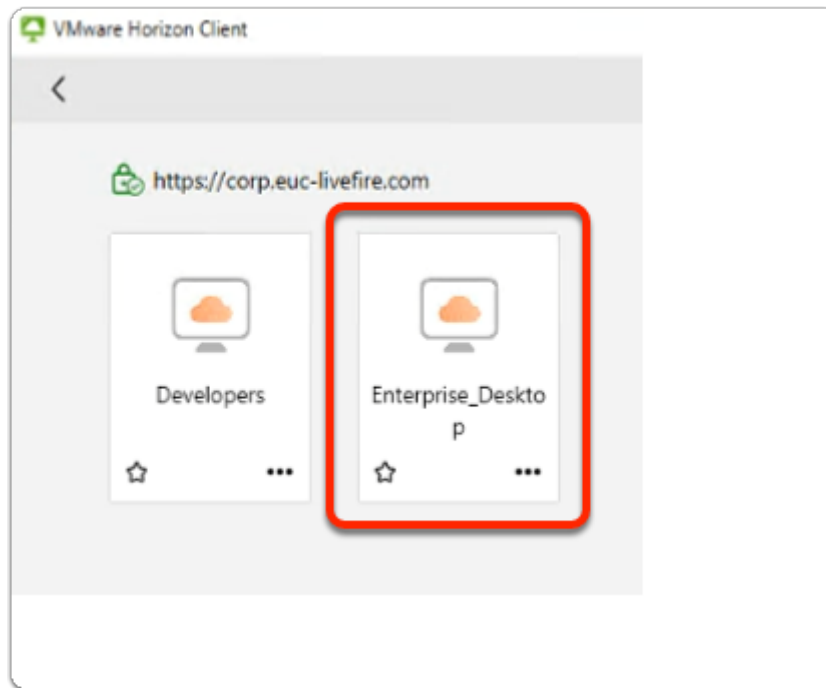
6. In the **Microsoft Stay signed in?**

- select **Yes**

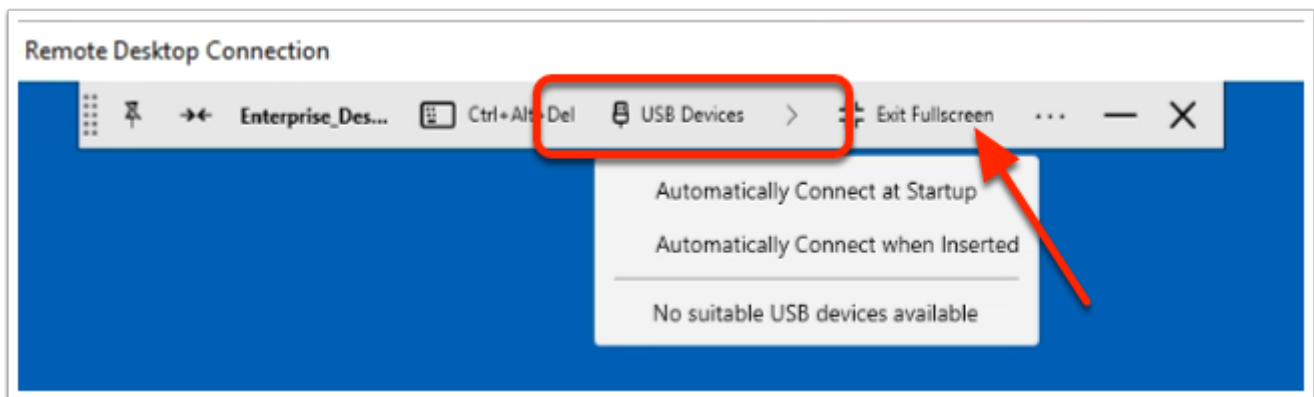


7. On your **W11Client-01a** desktop

- on the **Open VMware Horizon Client?** window
  - select **Open VMware Horizon Client**

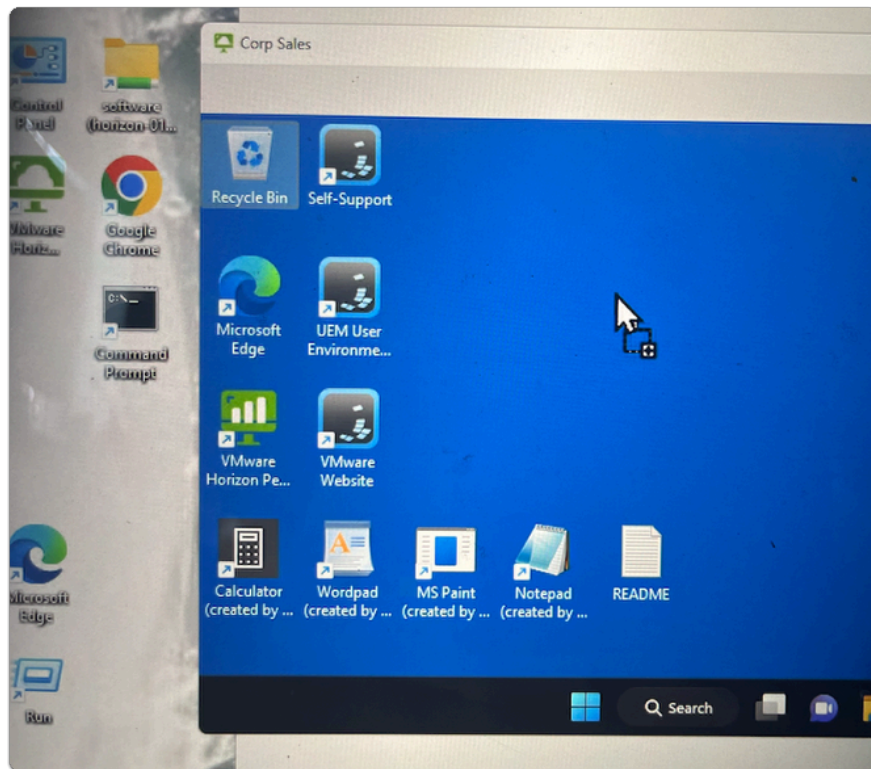


8. In the **VMware Horizon Client** login window
  - select the **Enterprise\_Desktop** entitlement

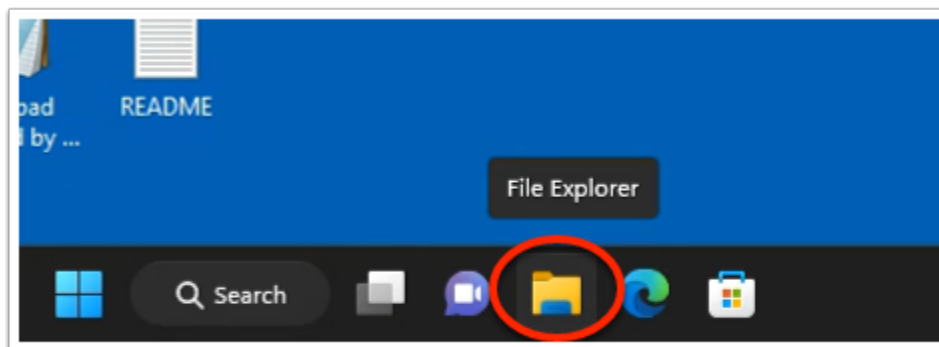


9. In the **VMware Horizon Client**
  - next to **USB Devices**
    - select the **dropdown arrow**,
    - Note, **No suitable USB devices available**, is the message you get.
      - Therefore if there were physical devices connected to the endpoint, its most likely that USB redirection would work
    - select **Exit Fullscreen**

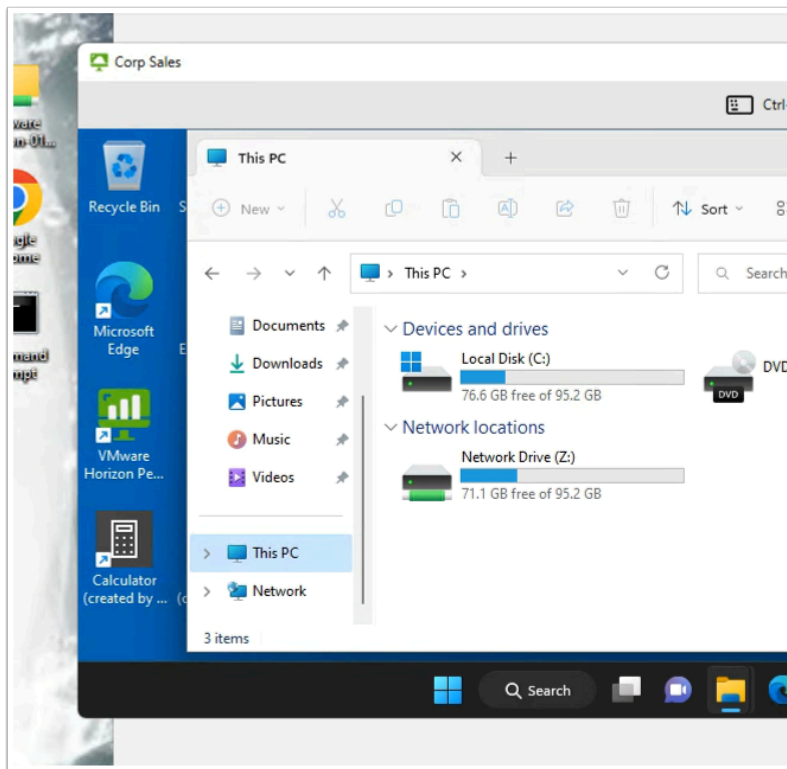




10. From your W11Client-01a desktop
  - With your **mouse, select** the Google Chrome shortcut
    - Drag it over into the Horizon Client session
      - Note that you will get a **+ type Icon** , just below your cursor.
  - Release your mouse button to **Drop the Console** within the Horizon Session

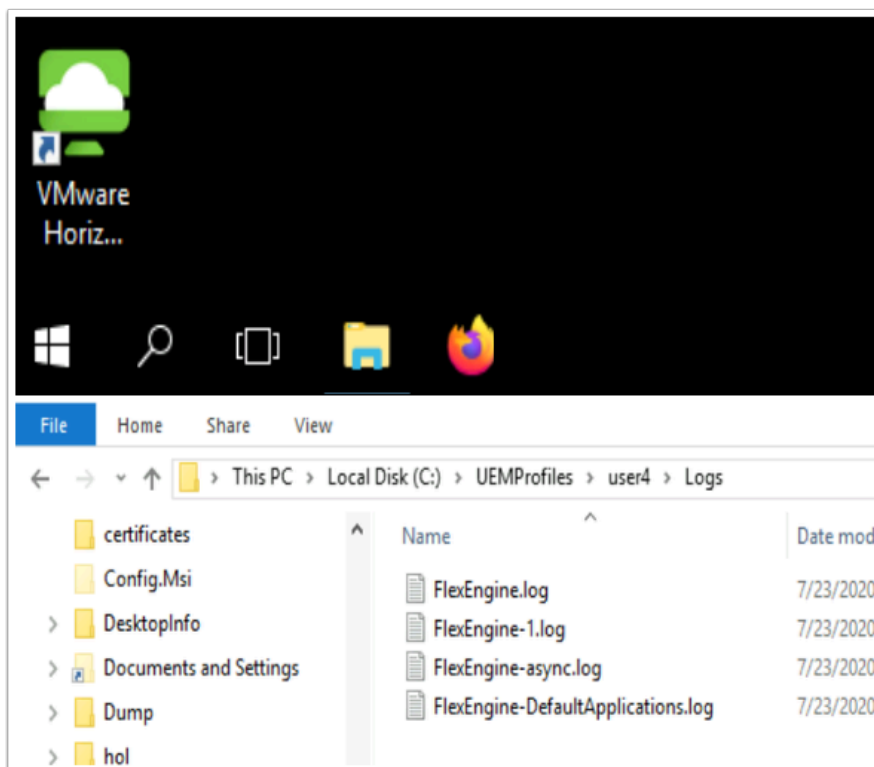


11. In the Horizon Client session
  - From the **Taskbar**,
    - select the **File Explorer** folder shortcut




## 12. In the **File Explorer** Window

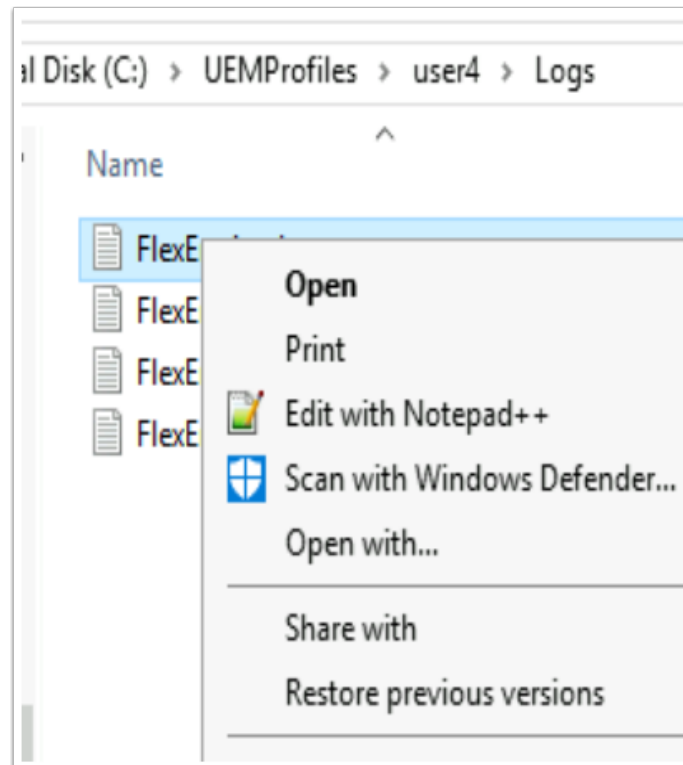
- Select **This PC** in the left Inventory
- To the right, **scroll down** and observe, there are network locations configured. ie the **Z: drive**



## Step 2: Observing the Logs

1. On the **ControlCenter** server
  - Open your **File Explorer** Icon, from the Taskbar
  - On the **C:\**, open your **UEMProfiles\YOUR Custom Test User\Logs** folder

 Click to copy

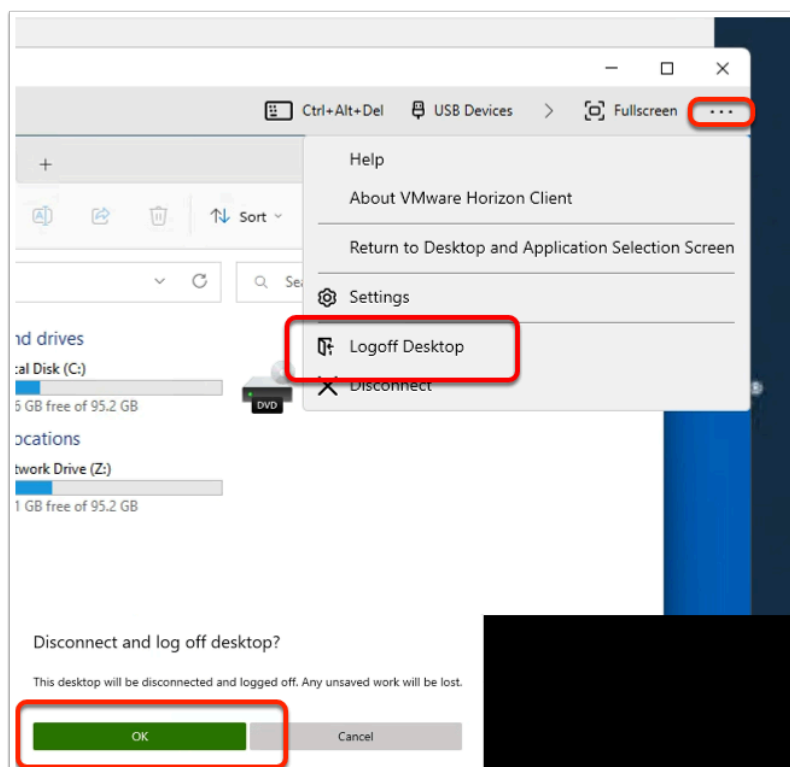


2. In File Explorer **C:\UEMProfiles\user1\Logs**
  - Select and right-click **FlexEngine.log**
  - Select **Edit with Notepad++**

```
845 2023-03-30 16:59:24.641 [INFO ] Processing path-based DEM undo actions and/or creation of
846 2023-03-30 16:59:24.656 [INFO ] Done (480 ms) [<<IFP#2b062380-82a29]
847 2023-03-30 16:59:09.384 [INFO ] Starting FlexEngine v10.8.0.1064 [IFP#31/ab01e-1a2d42>>]
848 2023-03-30 16:59:09.384 [INFO ] Running from service (NoAD)
849 2023-03-30 16:59:09.385 [INFO ] Performing path-based import
850 2023-03-30 16:59:09.424 [INFO ] Skipping Horizon Smart Policies settings due to condition
851 2023-03-30 16:59:09.430 [INFO ] Applied Horizon Smart Policies settings:
852 2023-03-30 16:59:09.430 [INFO ]     Bandwidth profile is set to 'Dedicated WAN'
853 2023-03-30 16:59:09.430 [INFO ]     Audio playback is enabled
854 2023-03-30 16:59:09.430 [INFO ]     Blast Extreme: H.264 is enabled, JPG is enabled, Max
855 2023-03-30 16:59:09.430 [INFO ]     Drag and drop is allowed
856 2023-03-30 16:59:09.430 [INFO ]     Printing is enabled
857 2023-03-30 16:59:09.430 [INFO ]     Client drive redirection is allowed
858 2023-03-30 16:59:09.430 [INFO ]     Clipboard redirection is allowed
859 2023-03-30 16:59:09.430 [INFO ]     USB redirection is enabled
860 2023-03-30 16:59:09.430 [INFO ]     Web and Chrome file transfer is allowed
861 2023-03-30 16:59:09.755 [INFO ] Configured message for trigger 'Workstation unlocked' ('
862 2023-03-30 16:59:09.770 [INFO ] Configured user environment settings refresh for trigger
863 2023-03-30 16:59:09.786 [INFO ] Configured user environment settings refresh for trigger
864 2023-03-30 16:59:11.384 [INFO ] Config file \\centralcenter.sva.lifefire.com\demconf\c
```

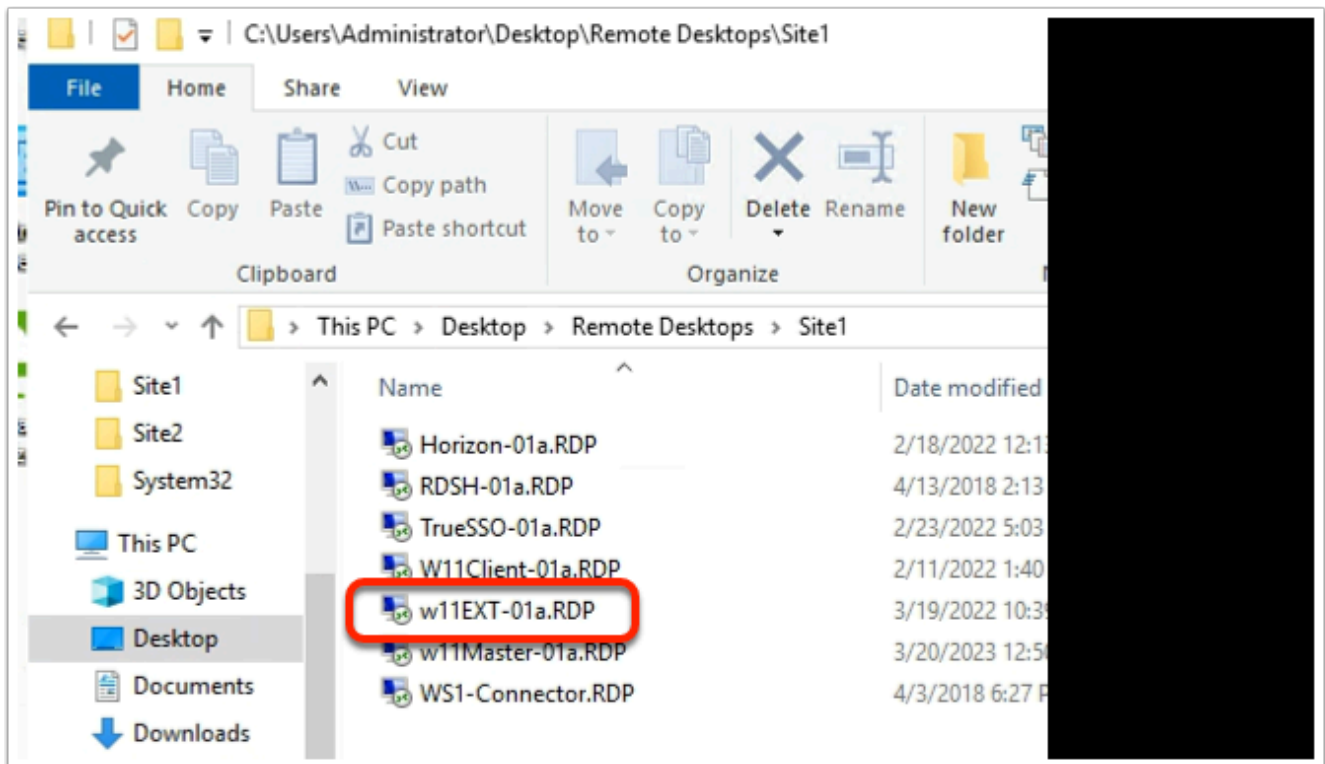
### 3. In the **Notepad++** session

- **Reload your logs**, by selecting **File > Reload from Disk**
- **Scroll down**, right to the bottom of your logs,
  - **Scroll up** until you find the **YOUR Custom Test User** and the **Performing path-based import** logs starting
  - Observe that each configuration is processed and logged as **disabled** / **enabled** or **True** / **False**
  - Note its the **Internal Policy** that is being **applied**
  - Note what features are **allowed** or **enabled**

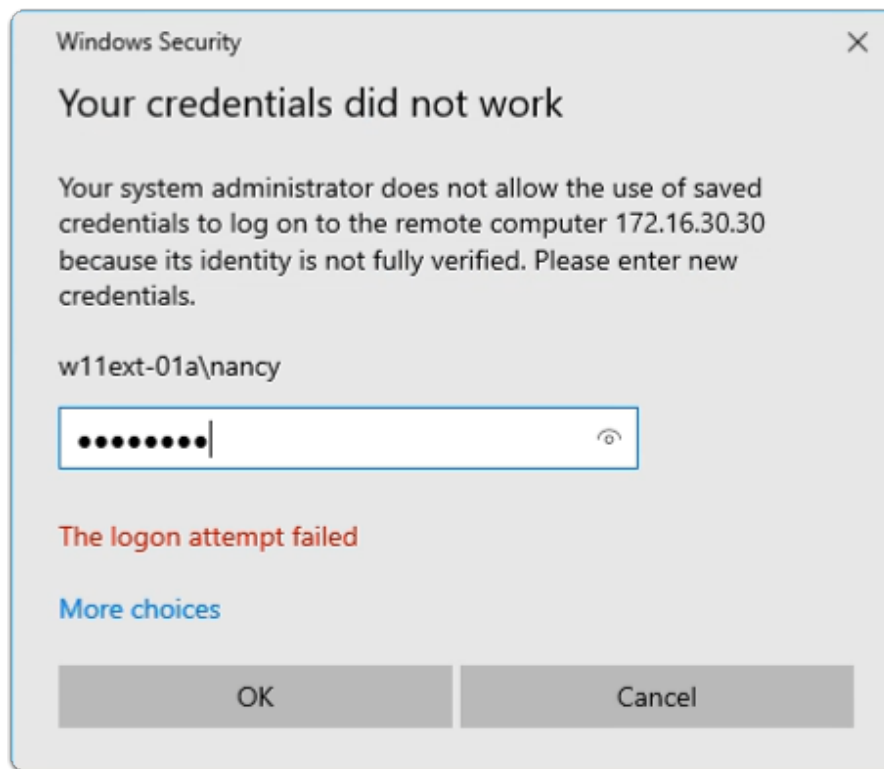


4. On the **ControlCenter** server
  - switch back to your **Horizon Client** session
  - next to Fullscreen,
    - next to **Options**,
      - select the **See more (3 buttons)**,
  - select **Log Off Desktop**
    - On the **Disconnect and log off desktop?** window
  - select **OK**

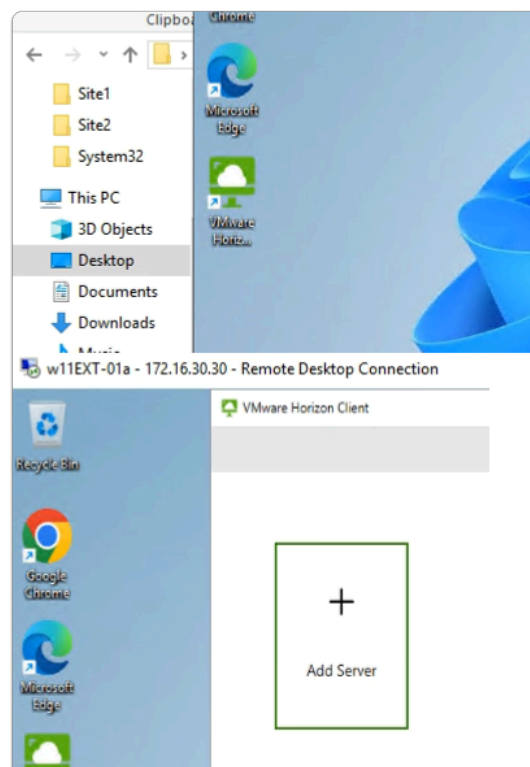
## Step 3: Testing the Smart Policies for an UnManaged device



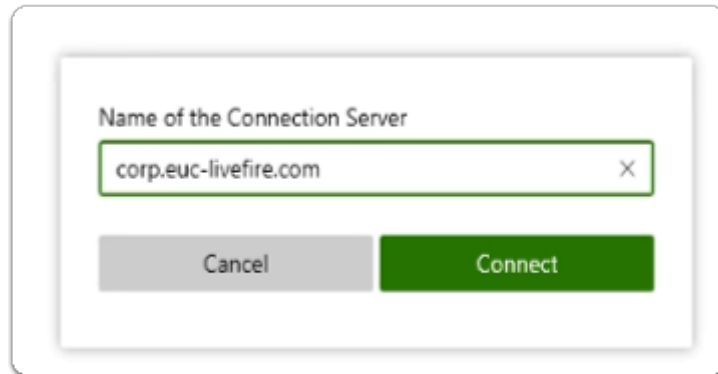
1. On the **ControlCenter** server
  - Open the **Remote Desktops \ Site1** folder
  - Open **w11EXT-01a.RDP**



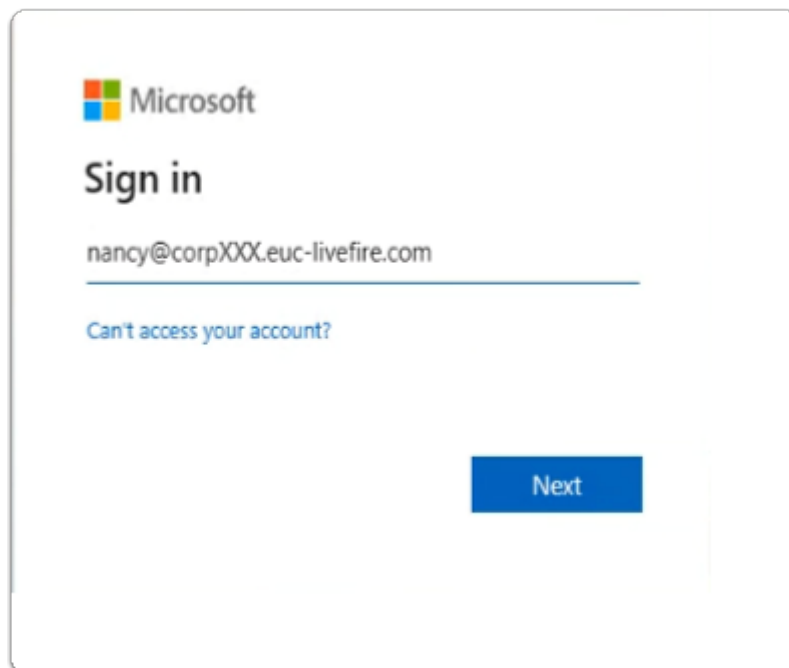
2. On the **Windows Security** window
  - Ensure **w11ext-01a\nancy** is the username
  - In the **password** area
    - enter **VMware1!**
  - select **OK**



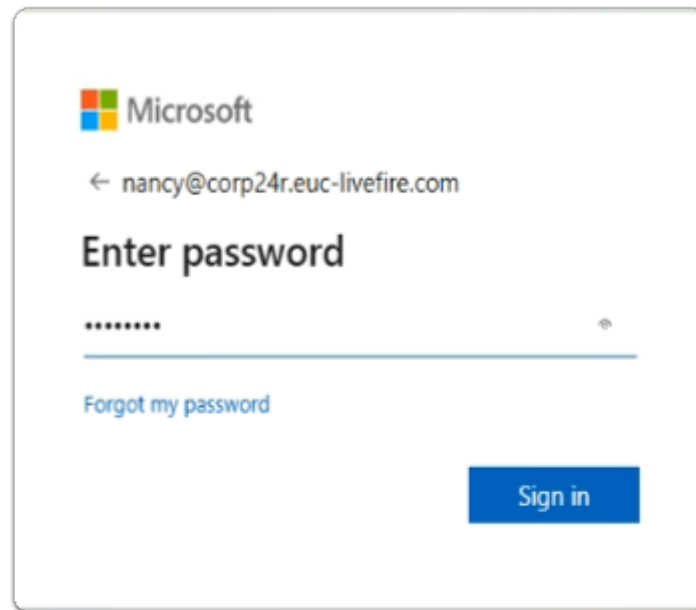
3. On the **W11Ext-01a** desktop
  - Launch the **VMware Horizon Client** shortcut
  - In the **VMware Horizon Client**
    - select **+ Add Server**



4. On the **W11Ext-01a** desktop
  - In the **Name of the Connection Server** window
    - enter **corp.euc-livefire.com**
    - select **Connect**



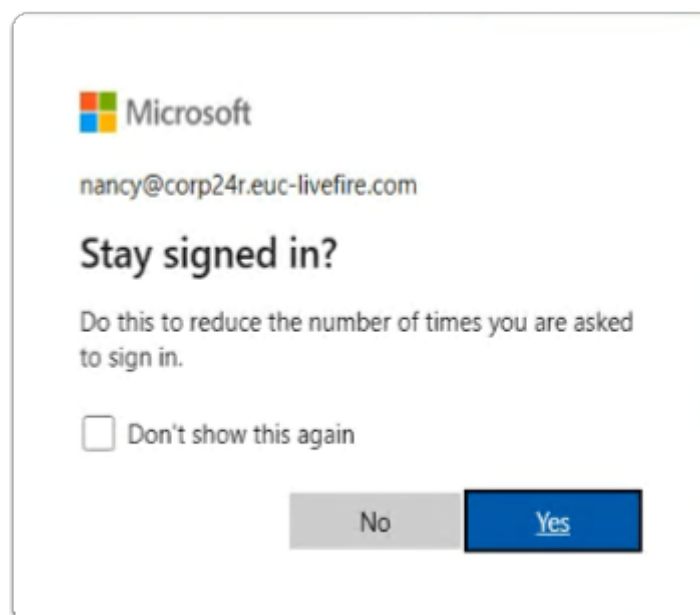
5. In the **Microsoft Sign in** window
  - enter **nancy@corpXXX.euc-livefire.com**
    - where **XXX** is your assigned Domain identifier
  - select **Next**



A screenshot of a Microsoft login window. At the top is the Microsoft logo. Below it is the email address 'nancy@corp24r.euc-liveware.com' with a back arrow to its left. The main heading is 'Enter password'. Below this is a password input field with a masked password '\*\*\*\*\*' and a toggle icon on the right. A link 'Forgot my password' is positioned below the input field. At the bottom right is a blue 'Sign in' button.

5. In the **Microsoft Enter password** window

- enter **VMware1!**
- select **Sign in**

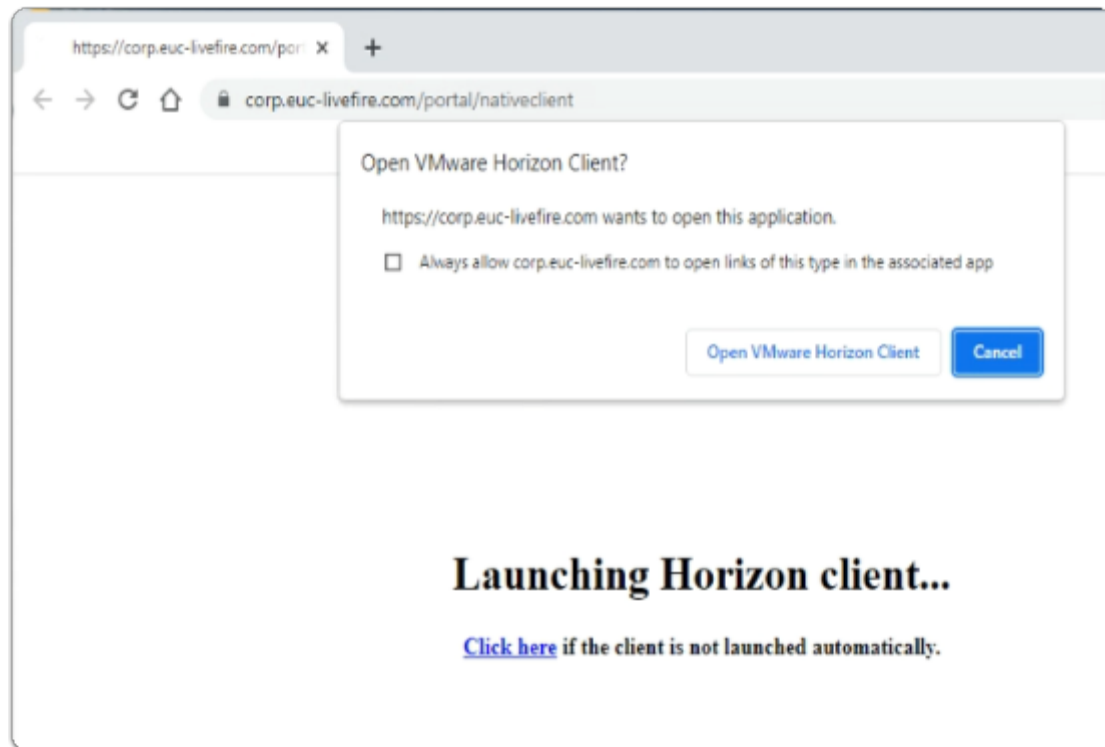


A screenshot of a Microsoft 'Stay signed in?' window. At the top is the Microsoft logo. Below it is the email address 'nancy@corp24r.euc-liveware.com'. The main heading is 'Stay signed in?'. Below this is the text 'Do this to reduce the number of times you are asked to sign in.' followed by a checkbox and the text 'Don't show this again'. At the bottom are two buttons: a grey 'No' button and a blue 'Yes' button.

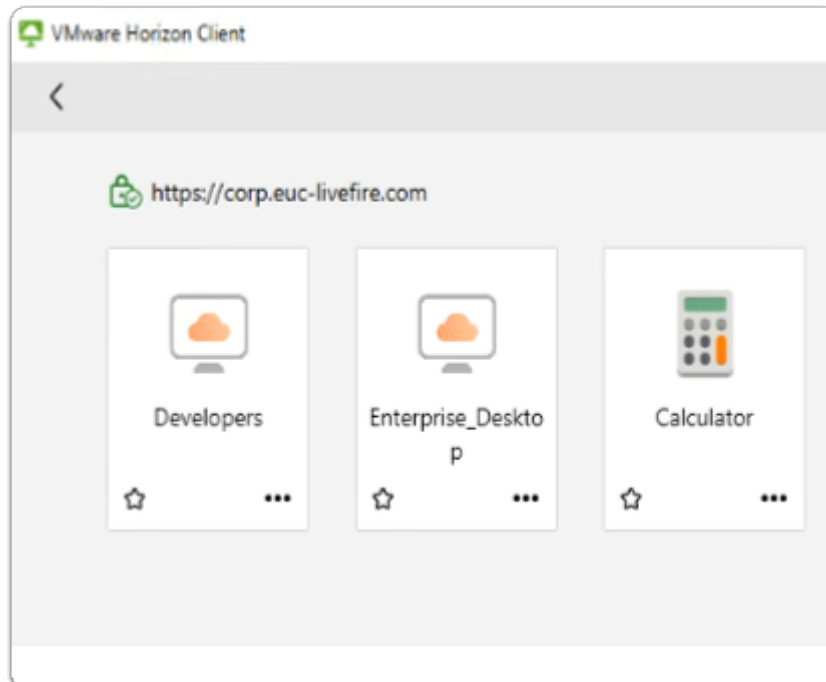
6. In the **Microsoft Stay signed in?**

- select **Yes**

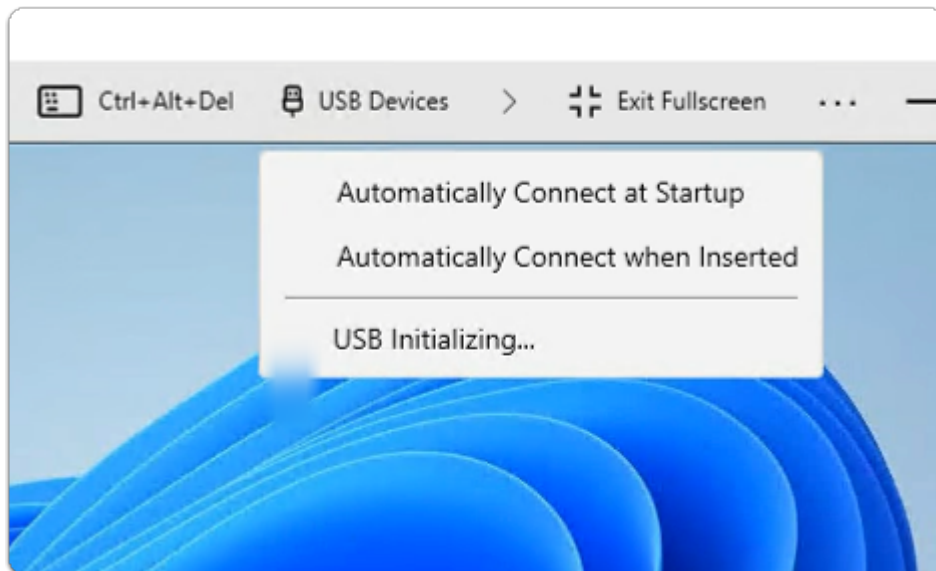




7. On your **W11Client-01a** desktop
  - on the **Open VMware Horizon Client?** window
    - select **Open VMware Horizon Client**

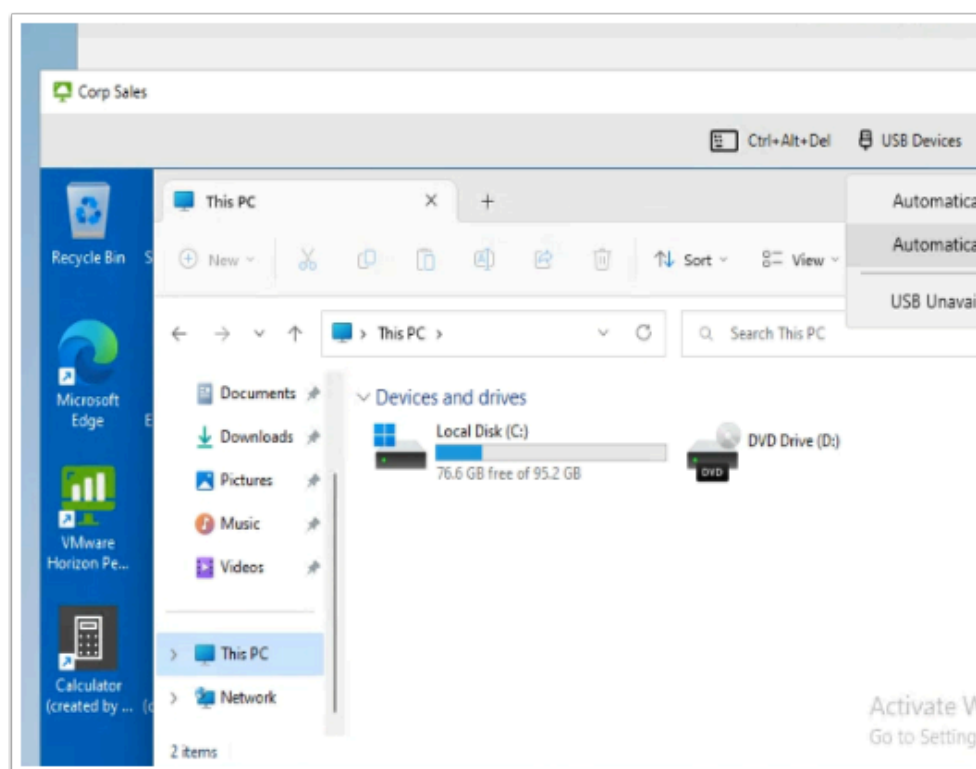


8. In the **VMware Horizon Client** login window
  - select the **Enterprise\_Desktop** entitlement



## 9. In the **Horizon Client**

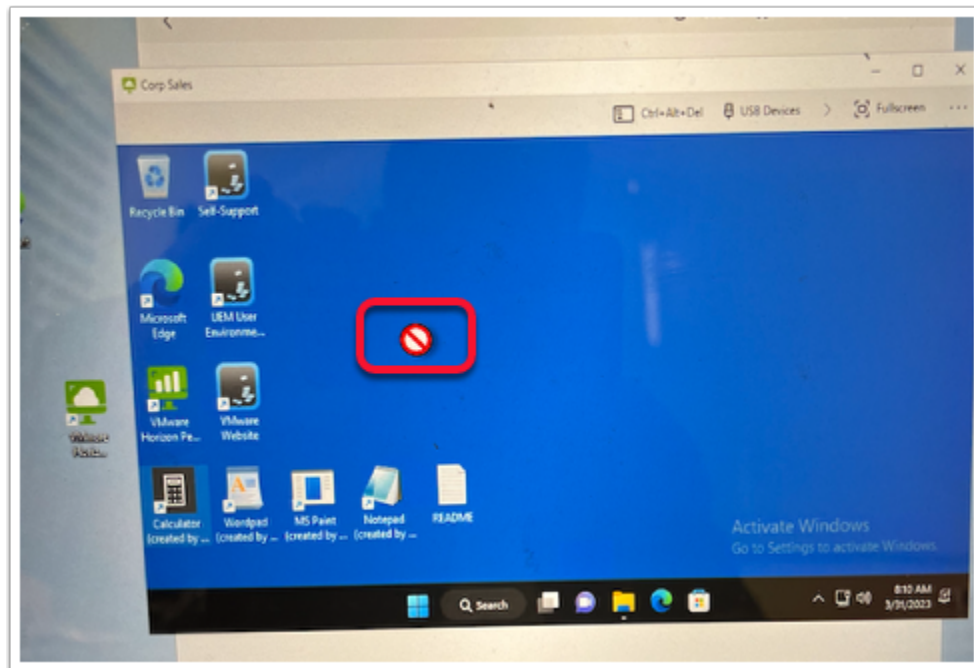
- In the top bar, next to **Connect USB Device**, select the **drop-down**
  - Notice that **USB is "Initializing"** is the state of USB ( a change of state)
    - We will read the logs to validate



## 10. In the **Horizon Client Desktop**

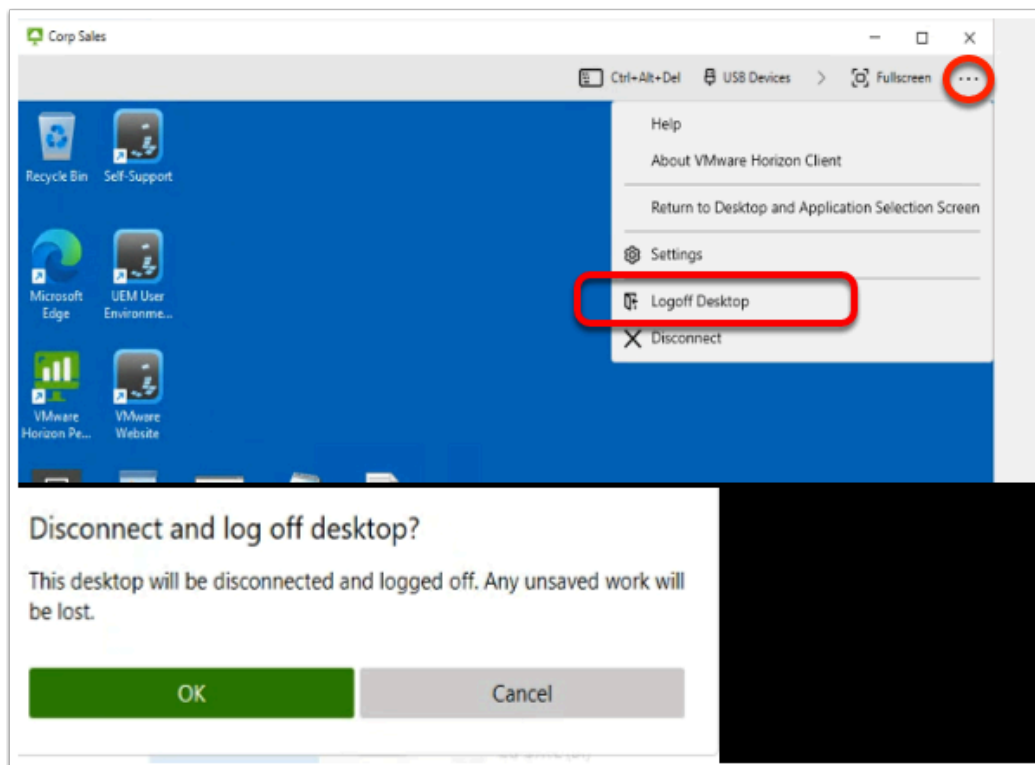
- On the title bar,
  - select the **File Explorer Icon**
- Ensure **This PC** is selected in the left inventory
  - **Scroll down** on the right side to the bottom of the window.

- Notice that you have **no Network drive Mappings**
- In the **Horizon W11 desktop session**
  - **Close all** windows



# 11. In the **W11EXT-01a** Desktop

- Attempt to drag the **VMware Horizon shortcut** into the **Horizon Desktop** session.
- From the **Horizon Desktop** session
  - attempt to drag the **Google** shortcut to the **W11EXT-01a** desktop

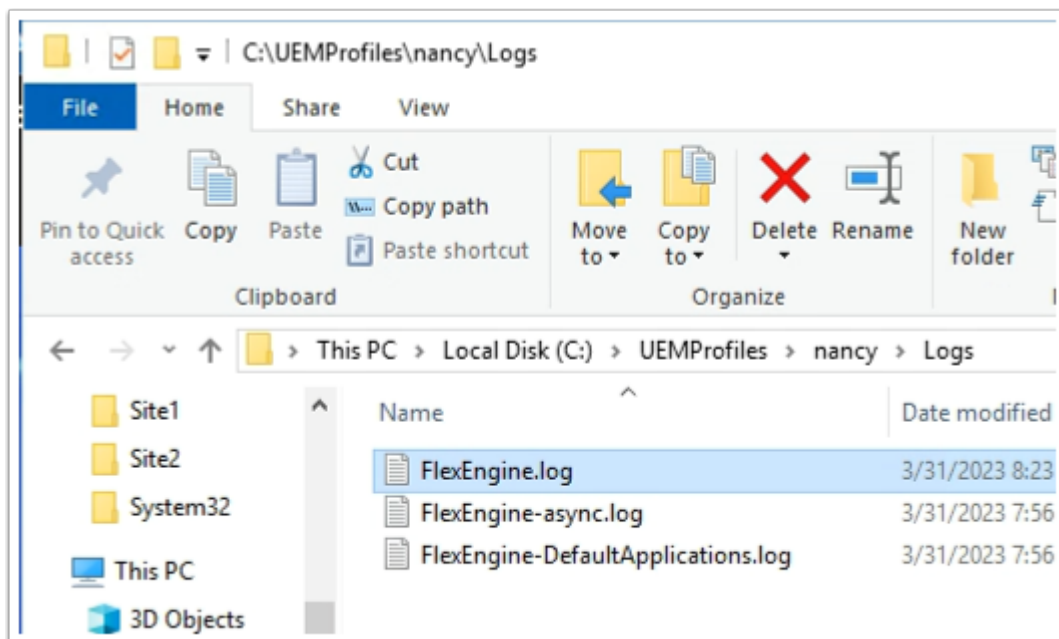


12. On the **W11EXT-01a** desktop
  - Switch back to your **Horizon Client** session
    - to the right of **FullScreen**
      - select ... (see more)
      - select the drop down,
      - select **Log Off Desktop**
    - In the **Disconnect and log off desktop?** window
      - Select **OK**

## Step 4: Observing the Logs

1. On the **ControlCenter** server
  - From the Taskbar
    - open your **File Explorer** Icon,
  - On the **C:\**
    - Browse to **UEMProfiles > nancy > Logs** folder

Click to copy



2. In File Explorer **C:\UEMProfiles\nancy\Log**
  - select and right-click **FlexEngine.log**
  - select **Edit with Notepad++**

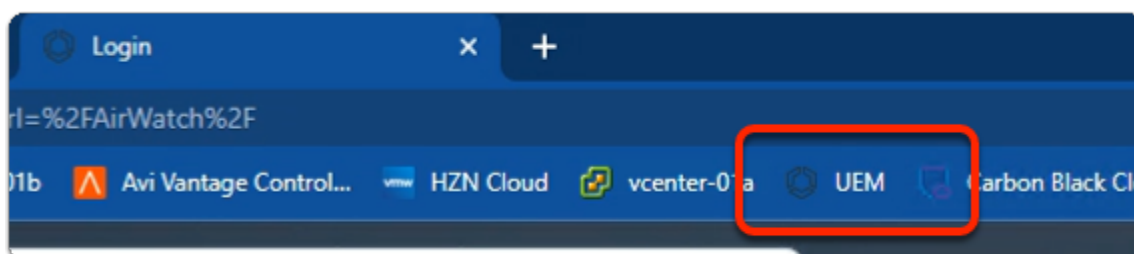
```
[INFO ] Done (589 ms) [<<IFP#05alceb5-4c86bf]
[INFO ] Starting FlexEngine v10.8.0.1064 [IFP#2c57349d-531ae2>>]
[INFO ] Running from service (NoAD)
[INFO ] Performing path-based import
[INFO ] Skipping Horizon Smart Policies settings due to conditions ('Compliant Endpoints.xml')
[INFO ] Applied Horizon Smart Policies settings:
[INFO ]   Bandwidth profile is set to 'Dedicated WAN'
[INFO ]   Blast Extreme: Max frame rate is set to 30
[INFO ]   Drag and drop is disabled
[INFO ]   Client drive redirection is disabled
[INFO ]   Clipboard redirection is disabled
[INFO ]   USB redirection is disabled
[INFO ]   Web and Chrome file transfer is disabled
[INFO ] Configured message for trigger 'Workstation unlocked' ('Message at unlock.xml')
[INFO ] Configured user environment settings refresh for trigger 'Workstation unlocked' ('Refresh A:
[INFO ] Configured user environment settings refresh for trigger 'Session reconnected' ('Refresh Pr:
[INFO ] Config file '\\controlcenter.euc-livewire.com\UemConfig\General\Applications\Acrobat Reader
[INFO ] No profile archive to import for config file '\\controlcenter.euc-livewire.com\UemConfig\Ge:
[INFO ] Config file '\\controlcenter.euc-livewire.com\UemConfig\General\Applications\Chrome.INI' ad
```

3. In the **Notepad++** session

- **Reload your logs**, by selecting **File > Reload from Disk**
- **Scroll down**, right to the bottom of your logs,
  - **Scroll up** until you find the **Performing path-based import** logs starting
  - Note the **Compliant Endpoints.xml** is skipped due to conditions
  - Note the **Applied Horizon Smart Policies**
    - Drag and drop is disabled
    - **Client drive redirection is disabled**
    - **Clipboard redirection is disabled**
    - **USB redirection is disabled**
    - **Web and Chrome file transfer is disabled**
  - Note what features are **allowed** or **enabled**

## Step 5 : The Unvarnished Truth

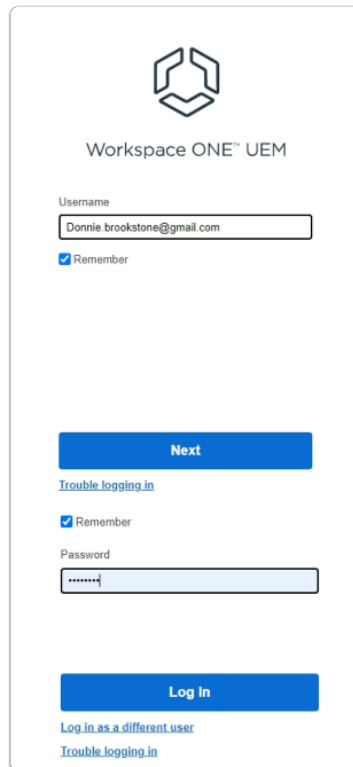
**i** So far everything looks amazing. However we have discovered the following regarding this configuration



1. On your ControlCenter desktop

- switch to your **Chrome Browser**
- open a **new tab**

- from the **Favourites** bar
  - launch the Workspace ONE **UEM** shortcut



Workspace ONE™ UEM

Username

Donnie.brookstone@gmail.com

☒ Remember

Next

[Trouble logging in](#)

☒ Remember

Password

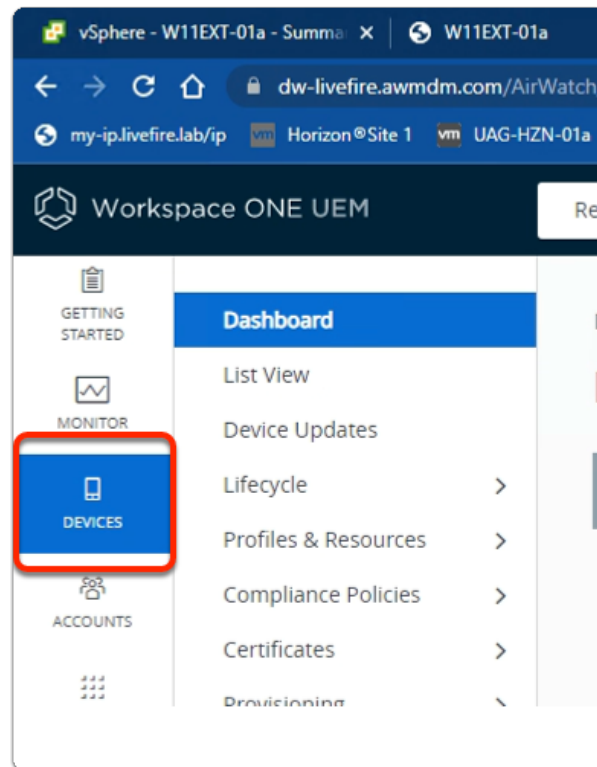
\*\*\*\*\*

Log in

[Log in as a different user](#)

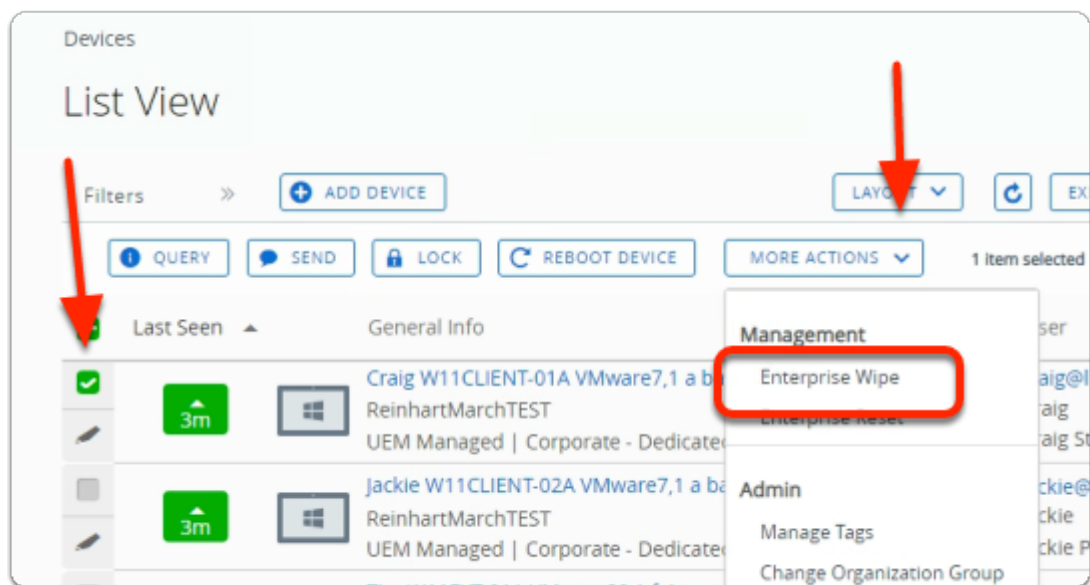
[Trouble logging in](#)

2. In the Workspace ONE UEM login
  - under **Username**
    - enter your **Registered course Username**
    - select **Next**
  - under **Password**
    - enter **VMware1!**
  - select **Log In**



3. In the Workspace ONE UEM Admin console

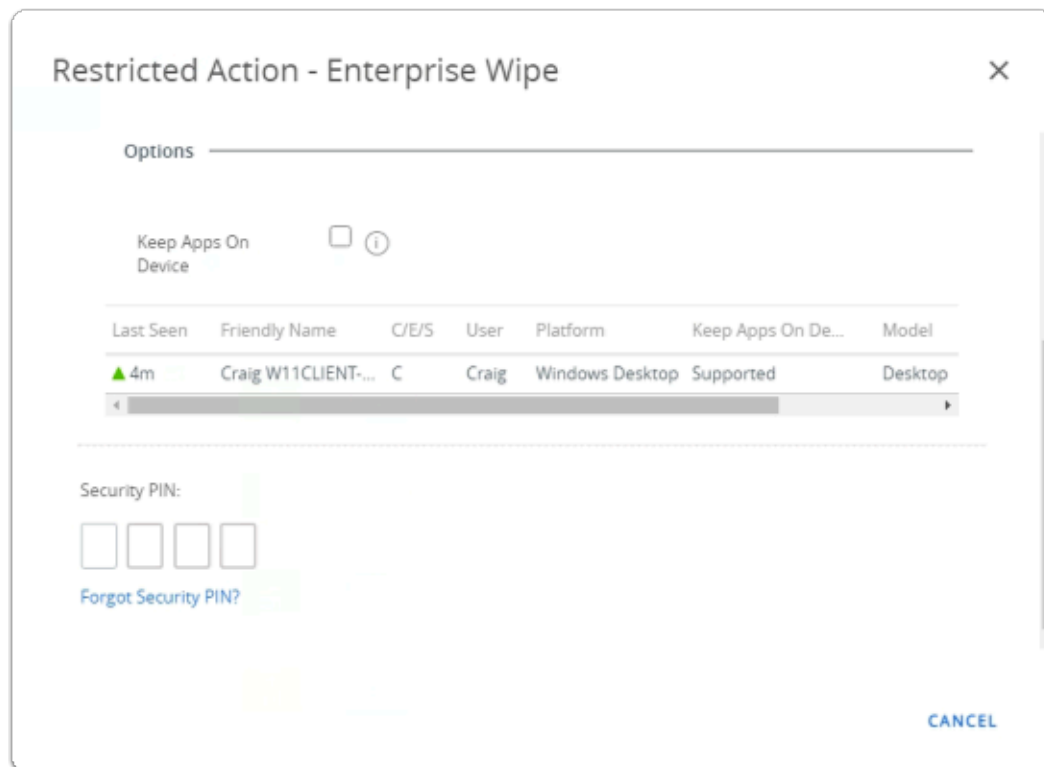
- select **DEVICES**
- under **Dashboard**
  - select **List View**



4. In the **Workspace ONE UEM Admin** console

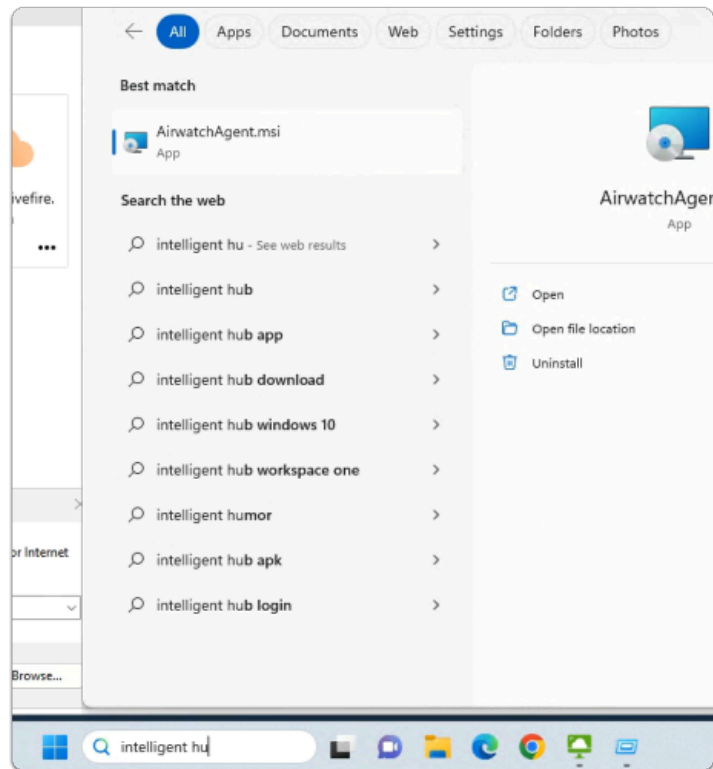
- **List View** console
  - Next to **Craig W11CLIENT-01A**
    - select the **checkbox**
  - In the **middle of the pane**

- **MORE ACTIONS**
  - select the **dropdown**
- In the **dropdown**
  - select **Enterprise Wipe**

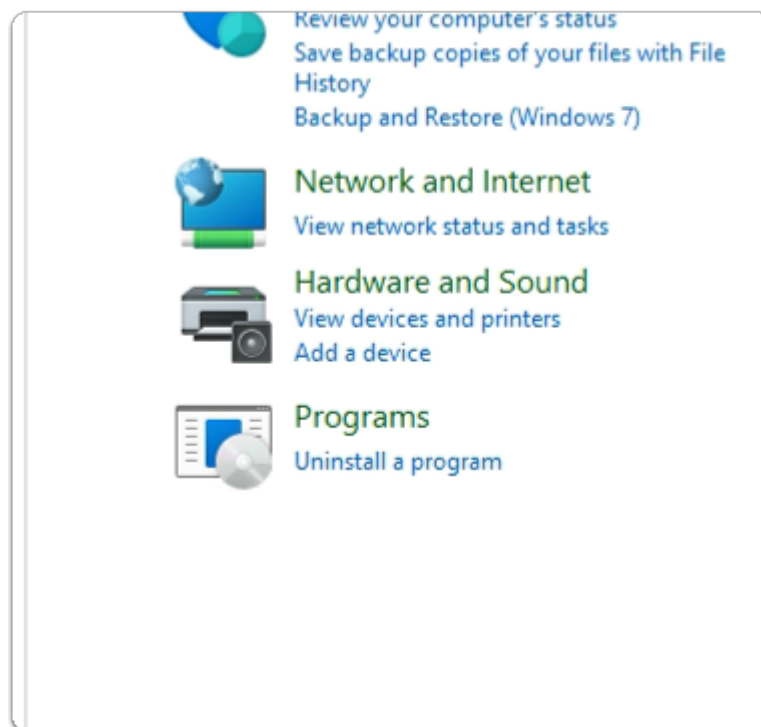


5. In the **Restricted Action - Enterprise Wipe** window
  - below **Security Pin**
    - enter **your PIN**
  - **switch back** to your **W11Client-01a** session



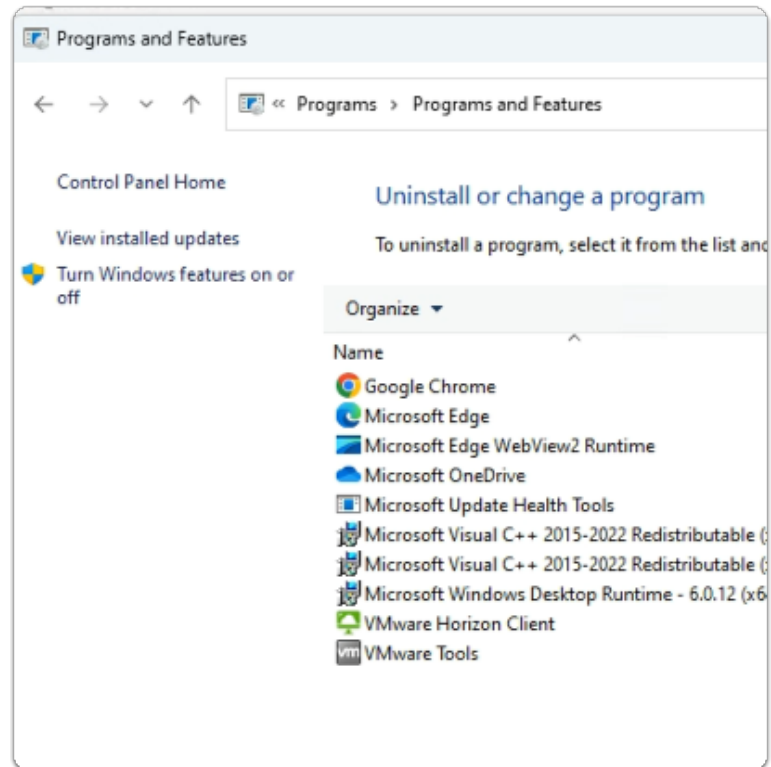


6. On your **W11Client-01a** desktop
  - On **Taskbar / Search** box
    - enter **intelligent hub**
    - notice that all you see is **AirwatchAgent.msi**

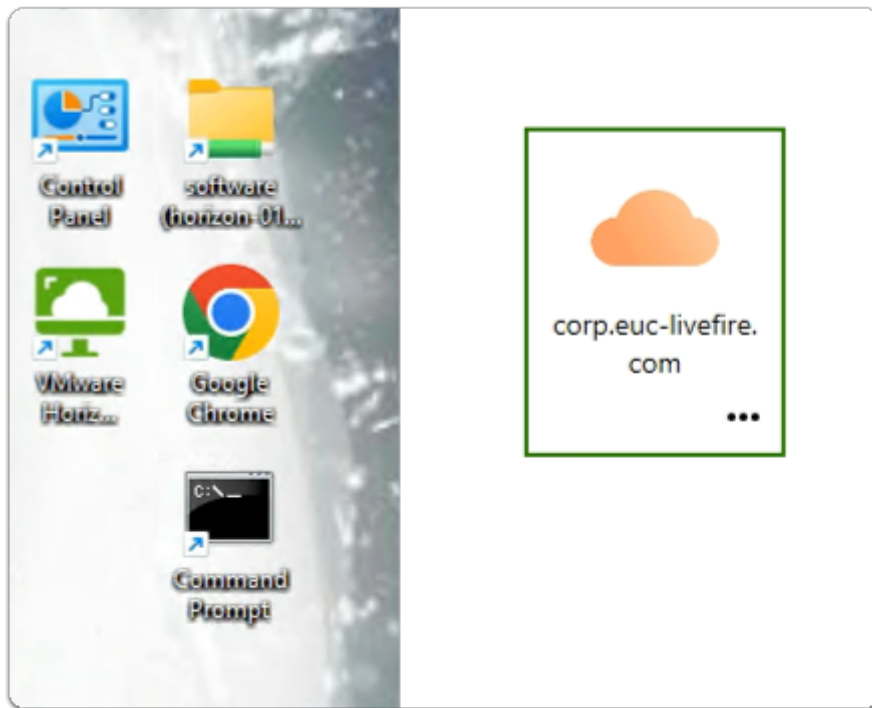


7. On your **W11Client-01a** desktop
  - On **Taskbar / Search** box

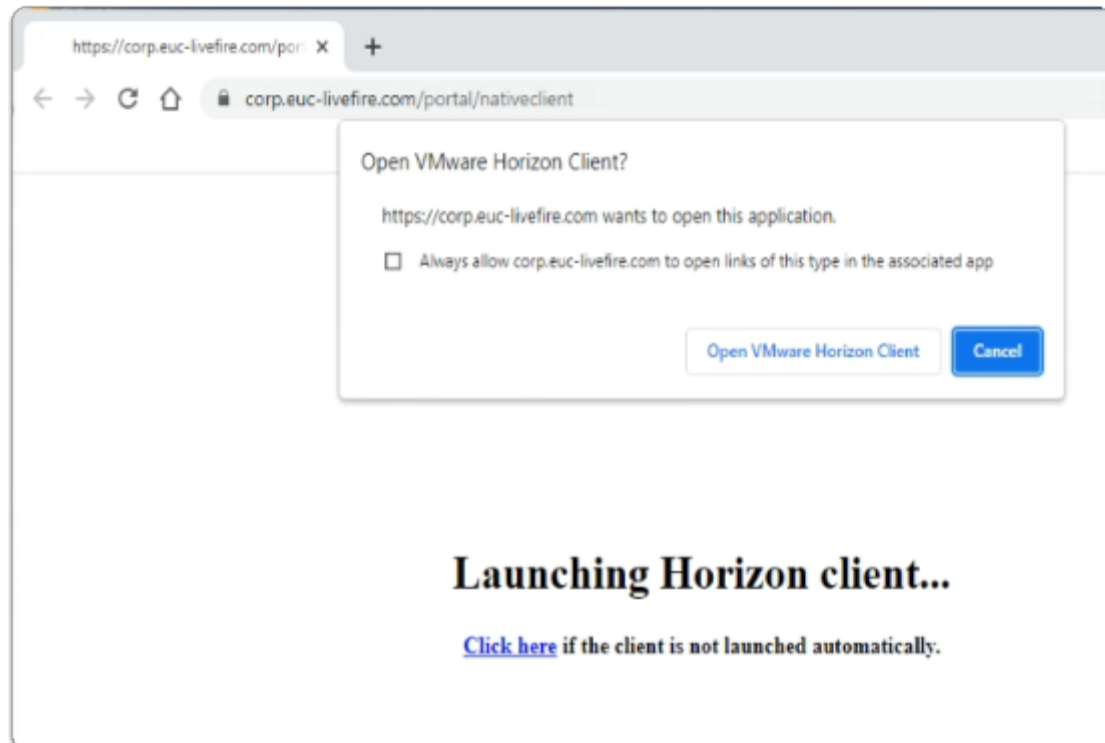
- enter **Control Panel**
- from the **Best Match**
  - select **Control Panel**
- In the **Control Panel** app
  - under **Programs**
    - select **Uninstall a program**



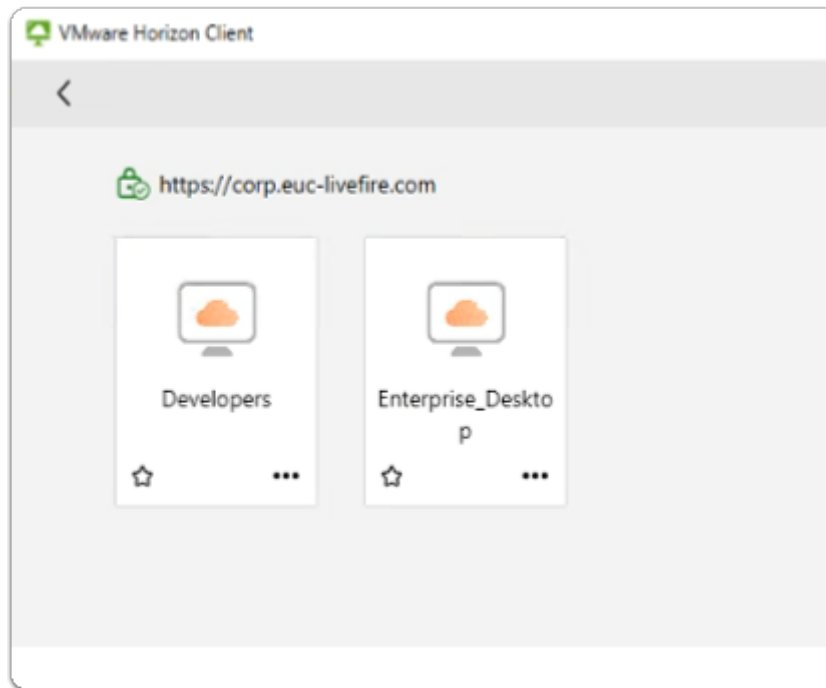
8. In the Programs and Features section
  - Note there is no **Workspace ONE Intelligent HUB** on this endpoint



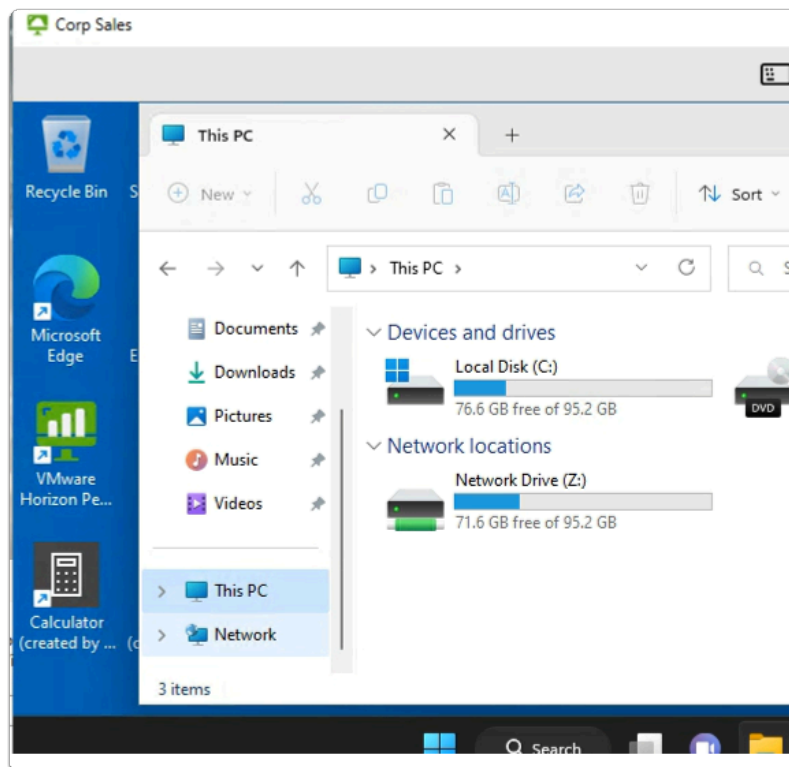
9. On your **W11Client-01a** desktop
  - launch the **VMware Horizon client** shortcut
  - In the **VMware Horizon Client**
    - select the **corp.euc-livefire.com** broker url



10. On your **W11Client-01a** desktop
  - on the **Open VMware Horizon Client?** window
    - select **Open VMware Horizon Client**

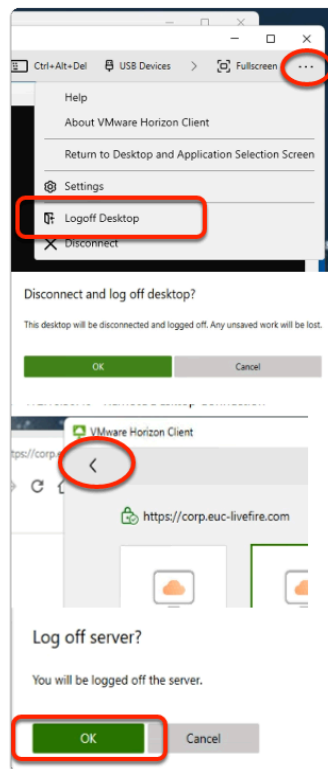


11. In the **VMware Horizon Client** login window
  - select the **Enterprise\_Desktop** entitlement



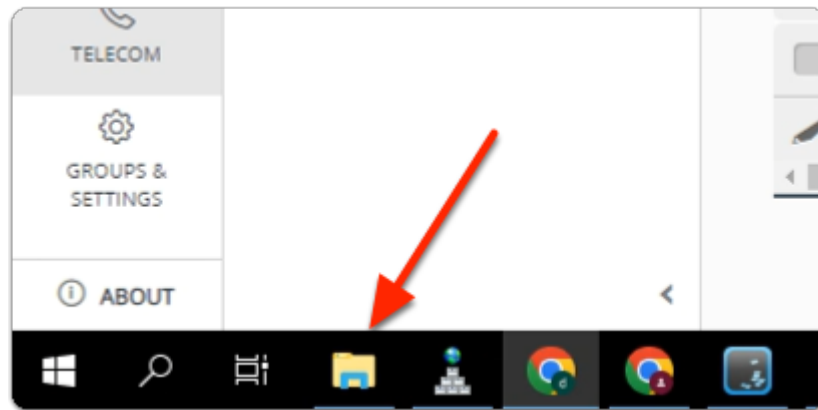
12. In the **VMware Horizon Client** session
  - from the **taskbar**
    - select the **Folder** icon
    - In the **Quick Access** pane
      - select **This PC**

- In **This PC** area
  - Note you have a drive mapping
- Feel free to attempt to drag and drop



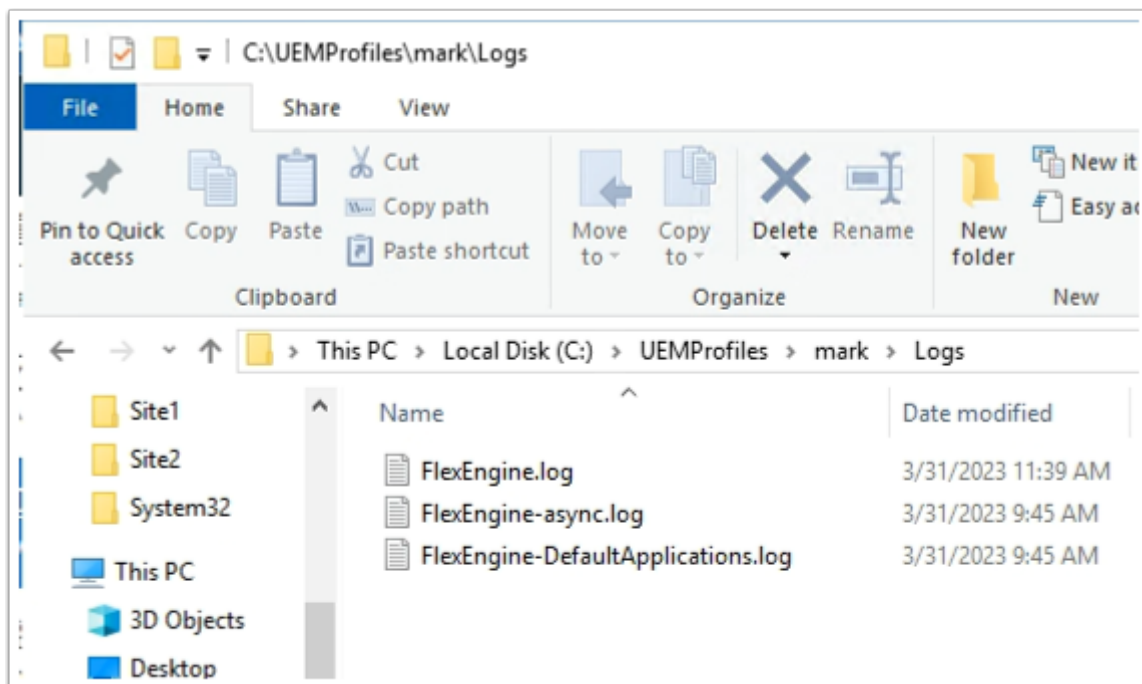
### 13. In the **Horizon Client** session

- next to **Fullscreen**
  - select the **dropdown**
    - select **Logoff Desktop**
- In the **Disconnect and log off desktop?**
  - select **OK**
- In the VMware Horizon Client
  - top left corner
    - select the **back arrow**
  - In the **Log off server?** window
    - select **OK**
- **minimize** the **w11Client-01a** session



14. On the **ControlCenter** server
  - From the **Taskbar**
    - open your **File Explorer** Icon,
  - On the **C:\**
    - Browse to **UEMProfiles** > **mark** > **Logs** folder

Click to copy



15. In File Explorer **C:\UEMProfiles\mark\Log**
  - select and right-click **FlexEngine.log**
  - select **Edit with Notepad++**

```

0 [INFO ] Processing path-based DEM undo actions and/or creation of 'run once' flag files
7 [INFO ] Done (764 ms) [<<IFP#317a99cd-1a2d42]
1 [INFO ] Starting FlexEngine v10.8.0.1064 [IFP#39f6elc9-23ee30>>]
2 [INFO ] Running from service (NoAD)
2 [INFO ] Performing path-based import
4 [INFO ] Skipping Horizon Smart Policies settings due to conditions ('Non Compliant Devices.xml')
1 [INFO ] Applied Horizon Smart Policies settings:
1 [INFO ]   Bandwidth profile is set to 'Dedicated WAN'
1 [INFO ]   Audio playback is enabled
1 [INFO ]   Blast Extreme: H.264 is enabled, JPG is enabled, Max frame rate is set to 30
1 [INFO ]   Drag and drop is allowed
1 [INFO ]   Printing is enabled
1 [INFO ]   Client drive redirection is allowed
1 [INFO ]   Clipboard redirection is allowed
1 [INFO ]   USB redirection is enabled
1 [INFO ]   Web and Chrome file transfer is allowed
7 [INFO ] Configured message for trigger 'Workstation unlocked' ('Message at unlock.xml')
1 [INFO ] Configured user environment settings refresh for trigger 'Workstation unlocked' ('Refresh P
3 [INFO ] Configured user environment settings refresh for trigger 'Session reconnected' ('Refresh P

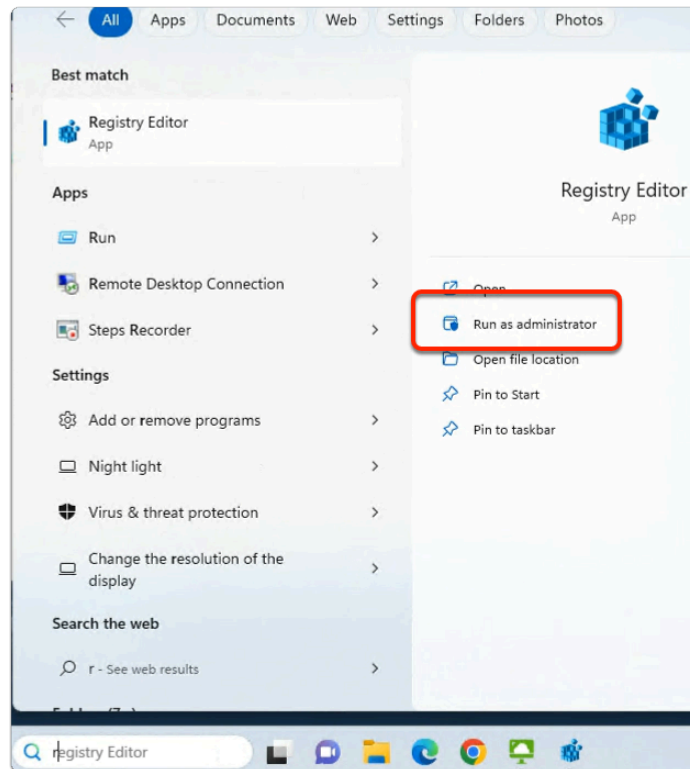
```

16. In the **Notepad++** session

- **Reload your logs**, by selecting **File > Reload from Disk**
- **Scroll down**, right to the bottom of your logs,
  - **Scroll up** until you find the **Performing path-based import** logs starting
  - Note the **Non Compliant Endpoints.xml** is skipped due to conditions
  - Note the **Applied Horizon Smart Policies**
    - **Drag and drop is allowed**
    - **Client drive redirection is allowed**
    - **Clipboard redirection is allowed**
    - **USB redirection is allowed**
    - **Web and Chrome file transfer is allowed**

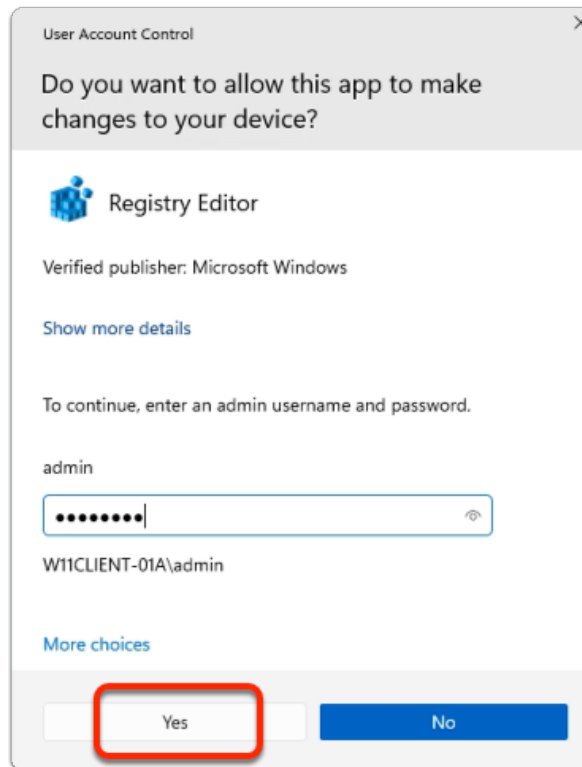
**i** We will now investigate why this is happening

- **Switch back** to your W11Client-01a RDP session

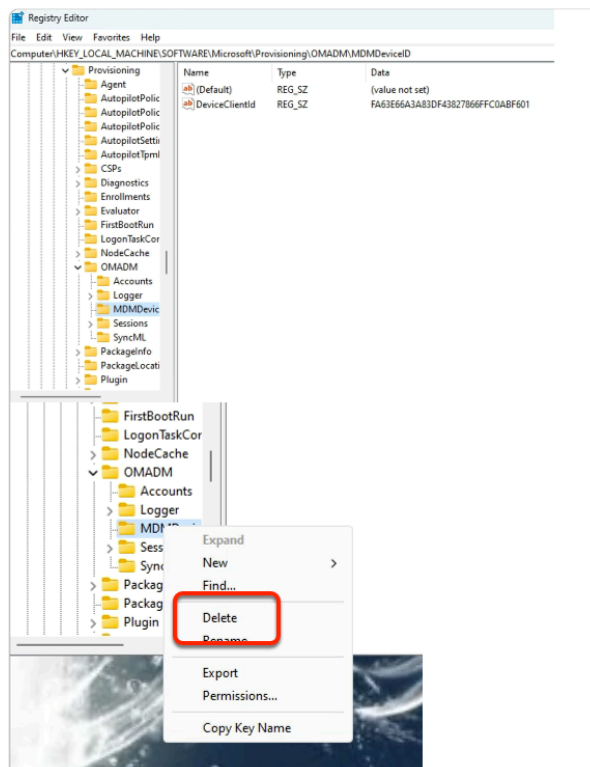


17. On the **W11Client-01a** desktop session
  - From the **taskbar**
    - In the **Search** area
      - enter **registry Editor**
    - In the **Best Match** area
      - select **Run as administrator**



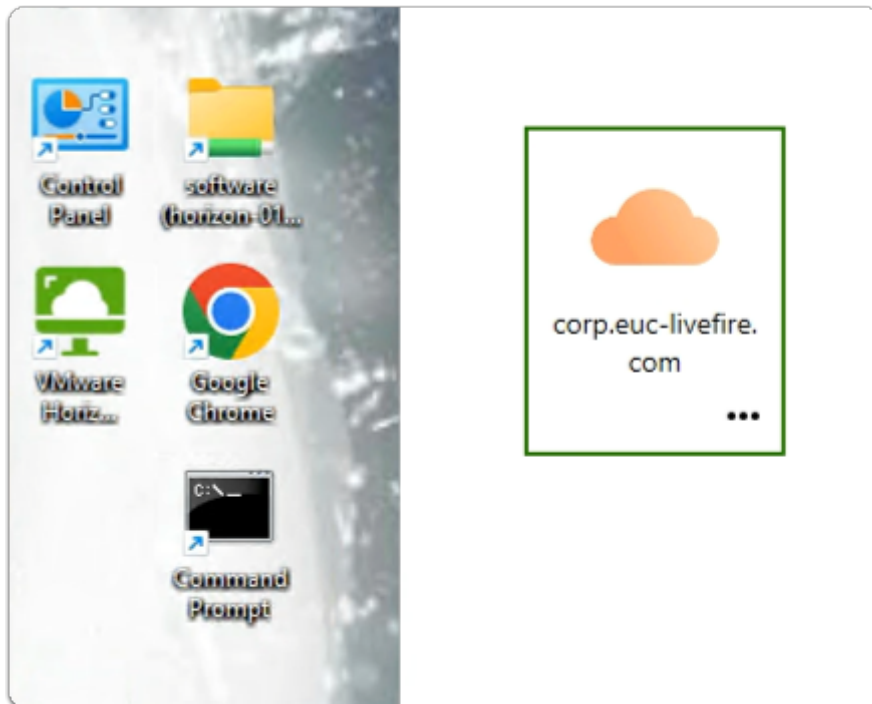


18. In **User Account Control** window
- Below **admin**
    - enter **VMware1!** as the *password*
  - select **Yes**



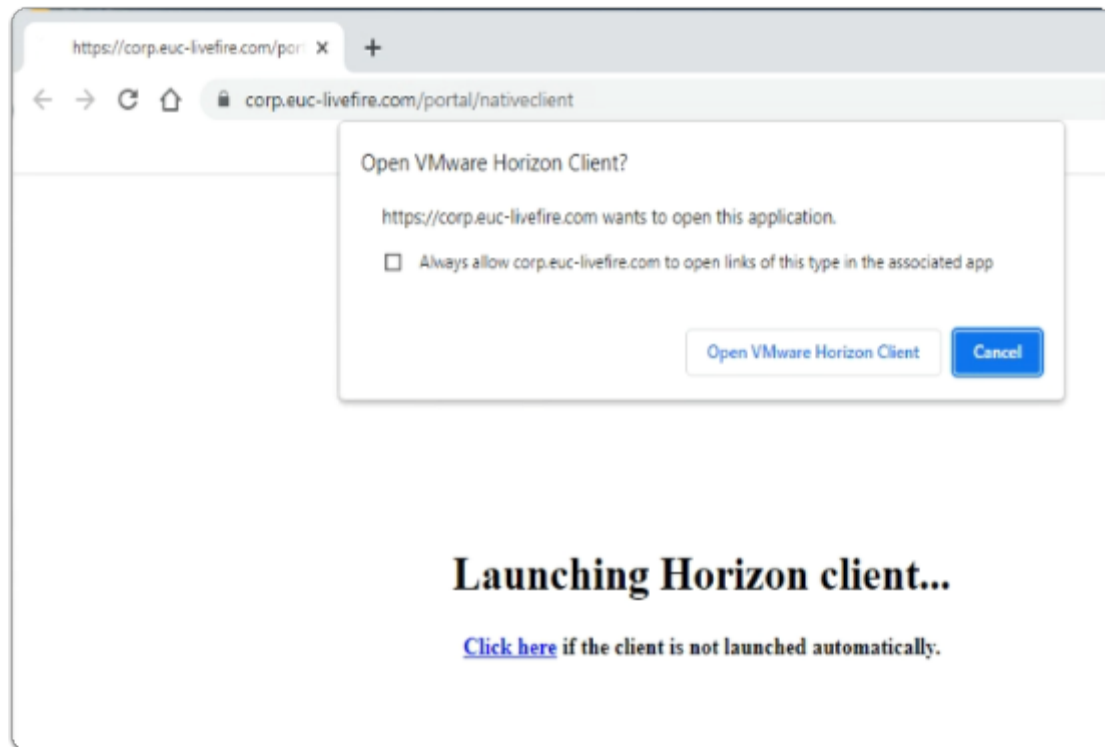
19. In the **Registry editor**

- In the **Inventory**
  - browse to
    - **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Provisioning > OMADM > MDMDeviceID**
  - Notice that you still have a **DeviceClientId** value in the registry
- In the **Inventory**
  - select & right-click the **MDMDeviceID** folder
    - select **Delete**

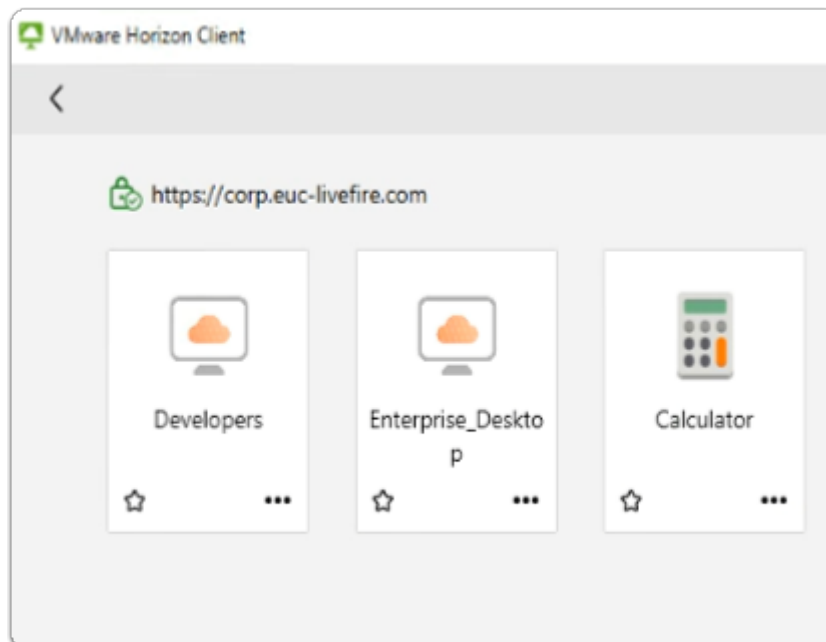


20. On your **W11Client-01a** desktop

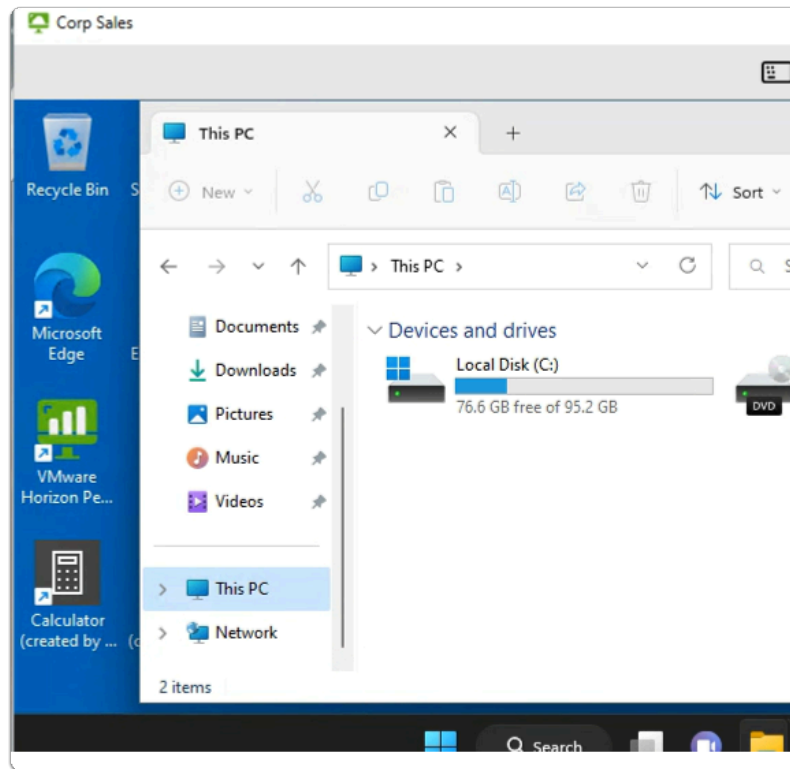
- launch the **VMware Horizon client** shortcut
- In the **VMware Horizon Client**
  - select the **corp.euc-livfire.com** broker url



21. On your **W11Client-01a** desktop
  - on the **Open VMware Horizon Client?** window
    - select **Open VMware Horizon Client**



22. In the **VMware Horizon Client** login window
  - select the **Enterprise\_Desktop** entitlement



## 23. In the **VMware Horizon Client** session

- from the **taskbar**
  - select the **Folder** icon
  - In the **Quick Access** pane
    - select **This PC**
    - In **This PC** area
      - Note that you now dont have a drive mapping
- Feel free to attempt to drag and drop

### In Summary

Using the registry element for Conditions within Dynamic Environment Manager is more a usability solution than a security solution and we are not able to rely on this alone.

Other Client System Information that is registry based that we might consider for Conditions might be

- Machine\_Domain: the remote Windows 10 clients domain name
- Machine\_Name: the remote Windows 10 clients PC name
- Broker\_GatewayLocation or Client Location which has the value of Internal or External

In a later lab we will look at a 3rd Party solution called OPSWAT that will allow us to provide a broad range of rules to ensure compliant