

# EUC: HORIZON INTEGRATIONS 2020



# Table of Contents

|   |     |
|---|-----|
| Day 1 .....   | 3   |
| Getting Started - Workspace ONE Access & Workspace ONE UEM SaaS Instance .....                                    | 4   |
| Configuring the Workspace ONE Access and the AirWatch Cloud Connector .....                                       | 21  |
| Workspace ONE Access and Workspace ONE UEM Integration.....   | 46  |
| Federating a SAML application with Workspace ONE Access .....   | 51  |
| Android emulator setup (Optional).....  | 65  |
| Day 2.....  | 84  |
| WorkspaceOne Hub Enrollment .....   | 85  |
| Federating BambooHR with WorkspaceONE Access.....   | 108 |
| Authentication Method - Android SSO .....   | 119 |
| Day 3.....  | 137 |
| Unified Access Gateway deployment using the PowerShell.....   | 138 |
| Horizon integration into Workspace ONE Access .....   | 154 |
| Horizon Configuration with Workspace ONE Access and the Unified Access Gateway...                                 | 165 |
| Installing and Configuring Horizon TRUESSO .....  | 183 |
| Day 4.....  | 259 |
| VMware App Volumes Operations.....  | 260 |
| Troubleshooting an App Volumes App Stack deployment with Mozilla Firefox .....                                    | 298 |
| Delivering a functional user experience that is consistent with organisational policy for the remote worker ..... | 314 |
| Day 5.....  | 363 |
| Integration of ThinApp Packages with VMware App Volumes and VMware Dynamic Environment Manager.....               | 364 |
| Profiling with mRemoteNG .....  | 416 |



# Day 1

# Getting Started - Workspace ONE Access & Workspace ONE UEM SaaS Instance

## Overview

The scenario you will be working with this week is a company called Euc-Livefire. They are a very dynamic organisation and have traditionally been on-premise but have recently moved into the cloud without truly understanding the challenges and would like a simple solution from an end-user perspective.

The organisation has key drivers around security, availability, mobility, and business continuity. At present all user Accounts and Passwords are managed in Microsoft Active Directory.

The organisation has recently started started using Salesforce and BambooHR as SaaS Applications

End-users require consumption of their applications across all platforms and recently have commented on how difficult it is to remember all the access portals and passwords.

Our objective this week will be to integrate all existing resources both On-premise and SaaS into a singular simple solution for end users.

### Colour Code Conventions

In the Screensteps we have made a lot of effort to colour code our work to facilitate a better user experience

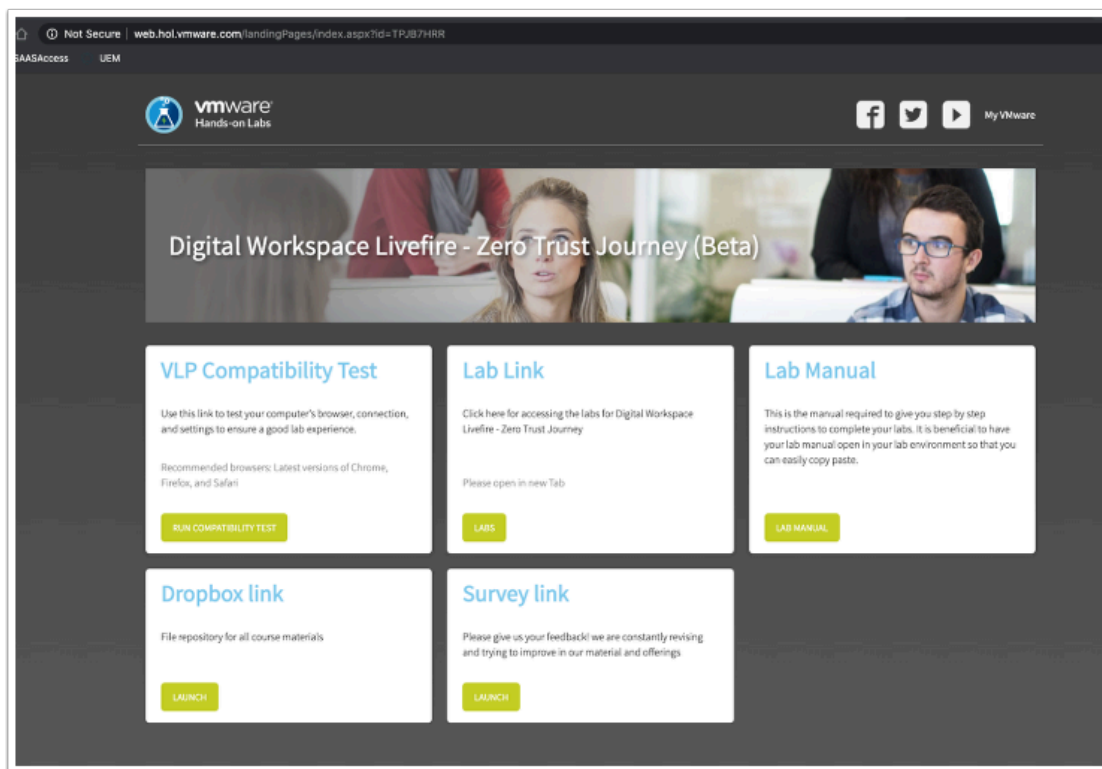
1. There are 3 colours we use as part of the Screensteps convention
  - If the colour is in a **bold Green**. Its something to click or select
  - If the colour is in a **bold Blue**. Its something to type out or enter
  - If the colour is in **BOLD BLACK**. Its something to look our for to assist you in finding the final destination on the page to either **enter** or **select**
2. Overview of our On-premise and SaaS resources
  - The following resources in your lab environment are representative of what the EUC-Livefire organisation "On-premise" resources.
    - Active Directory Domain Controller and DNS services.  
Server Name is **ControlCenter2** and the Active Directory Domain is **EUC-Livefire.com**
    - **Horizon Connection Server**
      - A single Broker called CS1-PD1.euc-livefire.com.
        - 1 Windows 10 Instant Clone Desktop pool
        - 1 RDSH server with published applications
    - **Connector Server**
      - A dedicated Windows server called **ws1.euc-livefire.com**, this is dedicated for the Workspace ONE Access Connector and the Workspace ONE UEM Airwatch Cloud connector.

### 3. Cloud SaaS resources

- A SaaS Instance of Workspace ONE Access (formerly known as VMware Identity Manager)
  - A SaaS Instance of Workspace ONE UEM (formerly known as VMware AirWatch)
  - In a later part of the labs you will register with the following SaaS services with a view to building a complete EUC solution.
    - A Salesforce tenant with Workspace ONE Access
    - BambooHR tenant with Workspace ONE Access
4. Please validate that you have an email registration link sent to you for Workspace ONE Access
5. Please validate that you have your own unique Student Number before starting this session.
6. As a best practice, right from the start
- For all SaaS resources, ensure you document all associated access information in a text editor
    - Admin URL
    - Username
    - Password
  - This will include the following:-
    - Your SaaS instance of Workspace ONE UEM
    - Your SaaS instance of Workspace ONE Access
    - Your SaaS applications:-
      - Salesforce
      - BambooHR
    - Your Access URL's into the VMware Learning Portal, representing your on-premise resources
      - Username
      - Password

Failing to document your online resources properly might cause severe disruption to your overall Lab experience.

# Part 1 : Logging into your "ON-Premise Infrastructure



1. On your laptop / Desktop. Open the following unique lab registration link found on [www.vmware.com/go/euclivefire](http://www.vmware.com/go/euclivefire)
  - Under Lab Link. Click on **LABS**

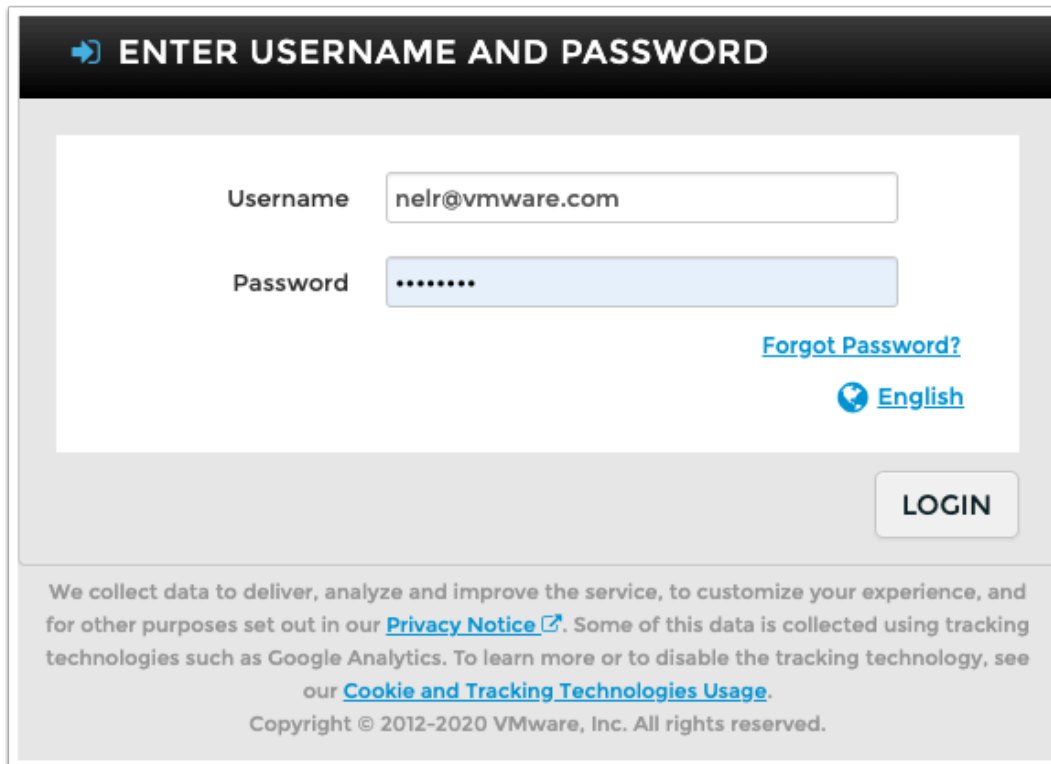
The screenshot shows a login interface with a dark header bar containing a right-pointing arrow icon and the text "ENTER USERNAME AND PASSWORD". Below the header, there are two input fields: "Username" with the value "nelr@vmware.com" and "Password" with masked characters "\*\*\*\*\*". To the right of the password field is a blue link "Forgot Password?". Below that is a language selector showing a globe icon and the text "English". A "LOGIN" button is positioned to the right of the input fields. At the bottom, there is a footer section with a privacy notice: "We collect data to deliver, analyze and improve the service, to customize your experience, and for other purposes set out in our [Privacy Notice](#). Some of this data is collected using tracking technologies such as Google Analytics. To learn more or to disable the tracking technology, see our [Cookie and Tracking Technologies Usage](#)." followed by "Copyright © 2012-2020 VMware, Inc. All rights reserved."

2. Enter your assigned Username.

- This will be the **email address** you were registered with for this training session
- This will be a **Password** you know. Its very likely you will have to select **Forgot Password?** to reset .
  - An email will be sent to

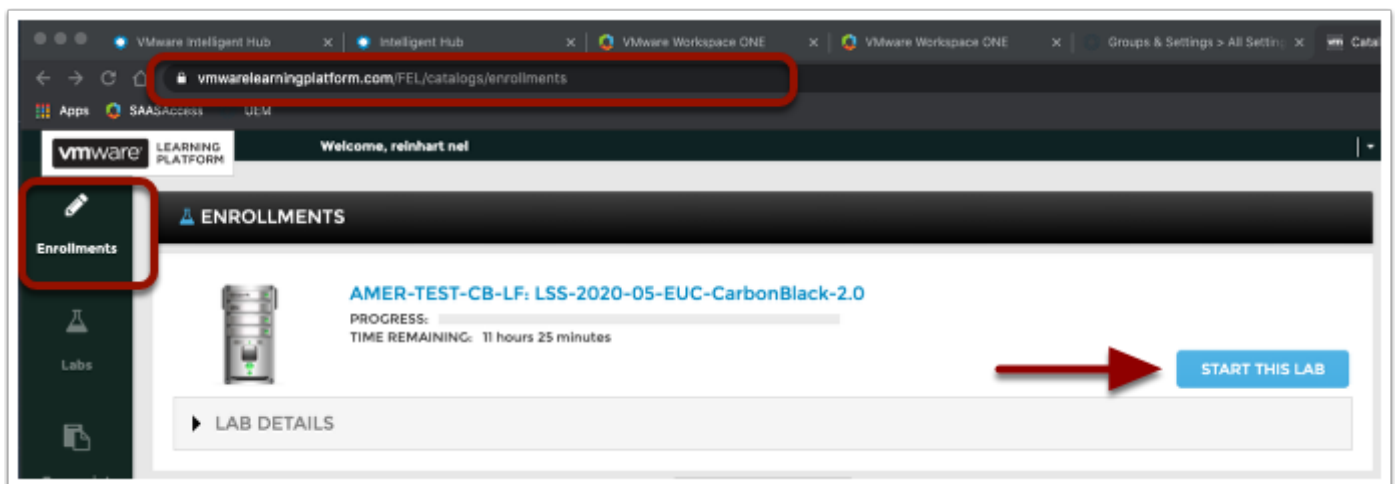
The screenshot shows a "FORGOT PASSWORD?" page with a dark header bar containing a lock icon and the text "FORGOT PASSWORD?". Below the header, there is a message: "You can reset your password by sending a verification email or by answering your security questions". Below this message are two buttons: "SEND EMAIL" and "ANSWER QUESTIONS", and a "Cancel" link. Below these buttons is a privacy notice: "We collect data to deliver, analyze and improve the service, to customize your experience, and for other purposes set out in our [Privacy Notice](#). Some of this data is collected using tracking technologies such as Google Analytics. To learn more or to disable the tracking technology, see our [Cookie and Tracking Technologies Usage](#)." followed by "Copyright © 2012-2020 VMware, Inc. All rights reserved." Below the privacy notice is a section titled "ENTER USERNAME" with a dark header bar containing a lock icon and the text "ENTER USERNAME". Below this header, there is a message: "Enter your username and a link will be sent to your email address to reset your password." Below this message is a "Username" input field with the value "nelr@vmware.com". Below the input field is a "SEND" button and a "Cancel" link. At the bottom, there is another privacy notice: "We collect data to deliver, analyze and improve the service, to customize your experience, and for other purposes set out in our [Privacy Notice](#). Some of this data is collected using tracking technologies such as Google Analytics. To learn more or to disable the tracking technology, see our [Cookie and Tracking Technologies Usage](#)." followed by "Copyright © 2012-2020 VMware, Inc. All rights reserved."

3. On the FORGOT PASSWORD? window select **SEND EMAIL**
  - In the **ENTER USERNAME.** Enter your **registered email** and select **SEND**



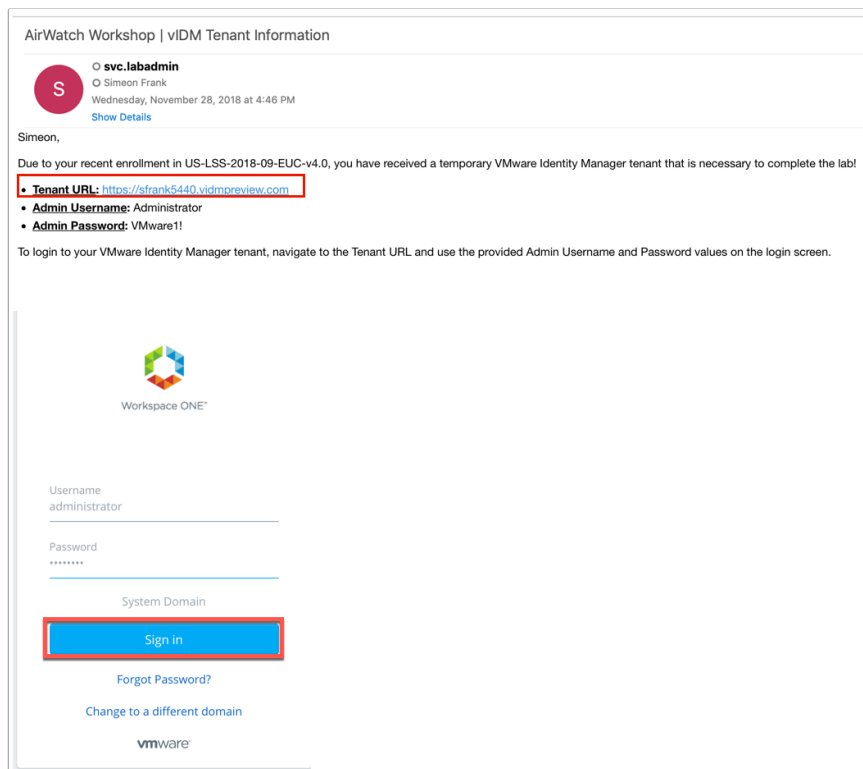
The screenshot shows a login form titled "ENTER USERNAME AND PASSWORD". It has two input fields: "Username" with the value "nelr@vmware.com" and "Password" with masked characters ".....". To the right of the password field are links for "Forgot Password?" and "English". A "LOGIN" button is at the bottom right. Below the form is a privacy notice: "We collect data to deliver, analyze and improve the service, to customize your experience, and for other purposes set out in our [Privacy Notice](#). Some of this data is collected using tracking technologies such as Google Analytics. To learn more or to disable the tracking technology, see our [Cookie and Tracking Technologies Usage](#). Copyright © 2012-2020 VMware, Inc. All rights reserved."

4. Once you have reset your Password, enter your **Password** and select **LOGIN**

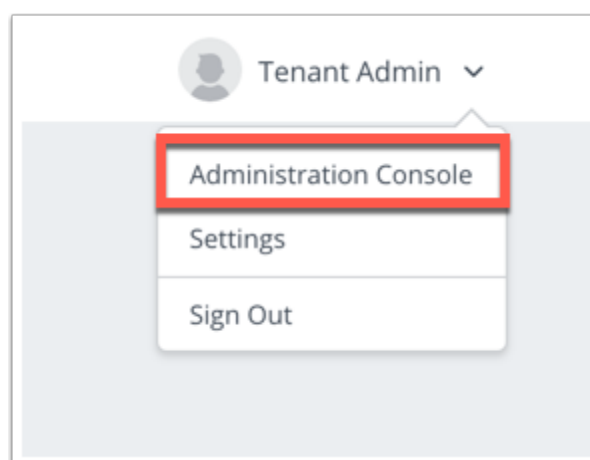


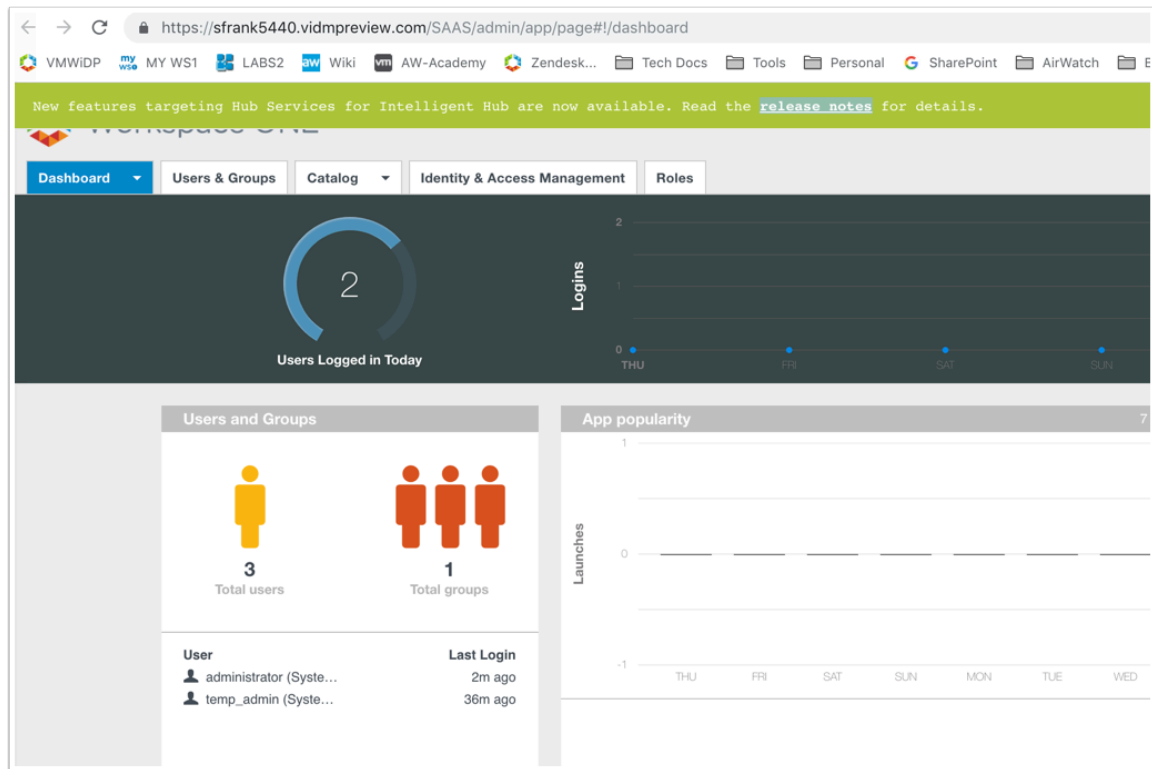
5. Once you have logged in select **Enrollments**
  - Select **START THIS LAB**
    - FYI. The below mentioned Screenshot does not represent your enrollment for this course and is a generic screenshot

## Part 2. Logging into and gaining access to Workspace ONE Access



1. Look in your e-mail and you should also have received an e-mail from **svc.labadmin@vmware.com**.
  - **NOTE:** Check your JUNK folder
  - This e-mail contains the unique tenant for your vIDM SaaS instance. Click on the **TENANT URL** to launch the VIDM Admin Console.
  - Use the credentials provided to login : Username: **Administrator** Password: **VMware1!**

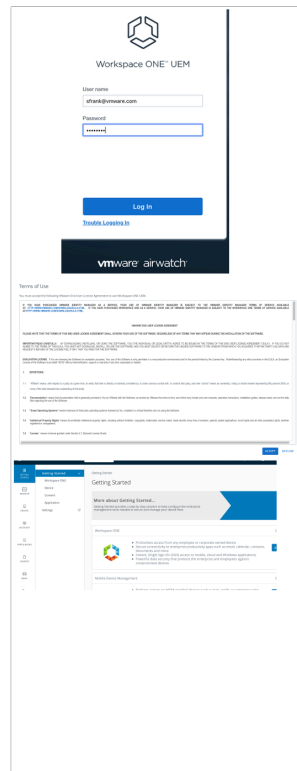




2. Now that you are signed in, change from the catalog view to the admin console by navigating to the top right and clicking on Tenant Admin and selecting Administration Console from the drop-down.
  - You should now see the Workspace ONE Access **Admin Console** to which we will return in a later lab.

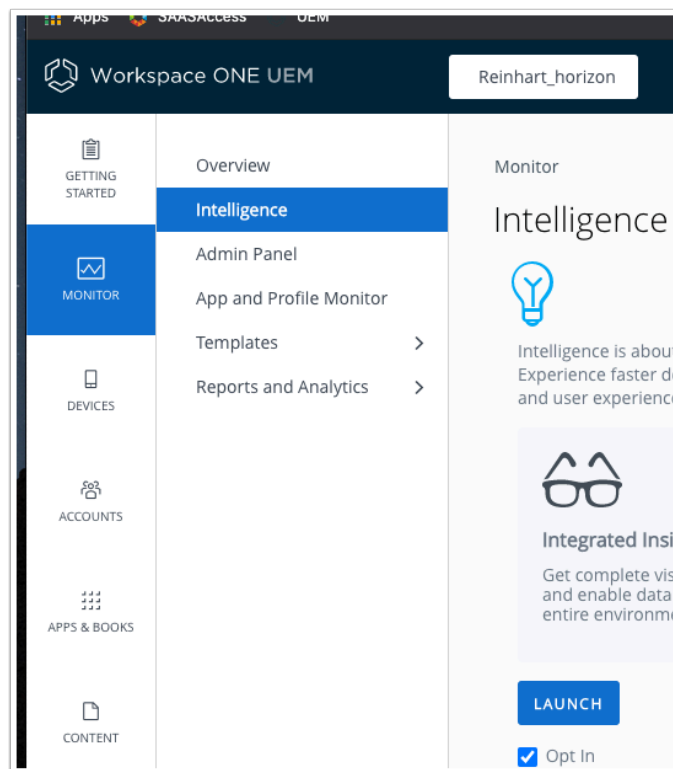


## Part 3. Logging Into Workspace ONE UEM



- **Open** a browser and navigate <https://dw-livefire.awmdm.com>
  - Use the e-mail address you signed up to the course with as the **User Name** (e.g sfrank@vmware.com) and the password: **VMware1!**
  - Click **Log In**
  - In the **Terms of Use** page select **ACCEPT**
  - Now set a security question and answer and a four digit Pin
  - You should now be on the **Getting started** window of the UEM console which is the default landing page.

## Part 4. Integrating with Workspace ONE Intelligence



This part of the lab will take you through how to activate your WorkspaceOne Intelligence Trial environment from the UEM console.

1. In your Workspace ONE UEM Console
  - On your left pane, select **Monitor**
  - Select **Intelligence**
  - Select **LAUNCH**

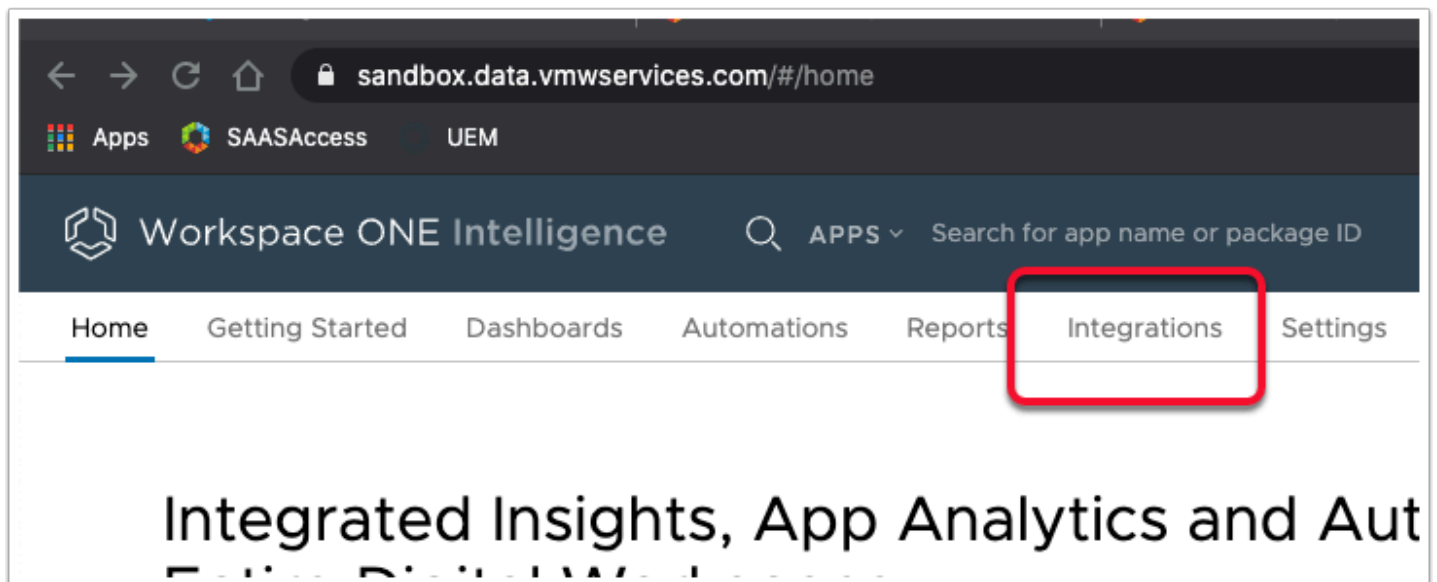
## Terms of Service

You must accept the following terms of service to use Intelligent

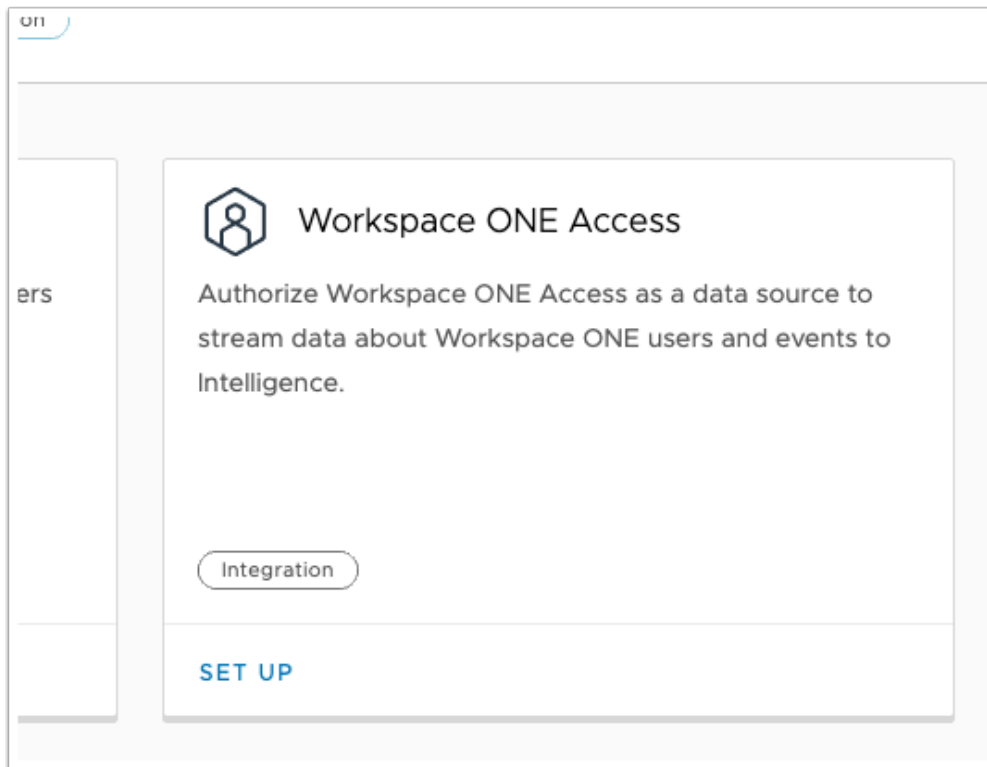
By using a VMware cloud service offering ("**Service Offer Service**"), and by the applicable Service Description, the Agreement. Terms, all of which together constitute the "Ac

|                 |                      |
|-----------------|----------------------|
| Name            | Demal                |
| Email Address   | Demal.Custro@outlook |
| Title           | Solutions Architect  |
| Company Name    | VMware               |
| Company Address | VMware UK            |

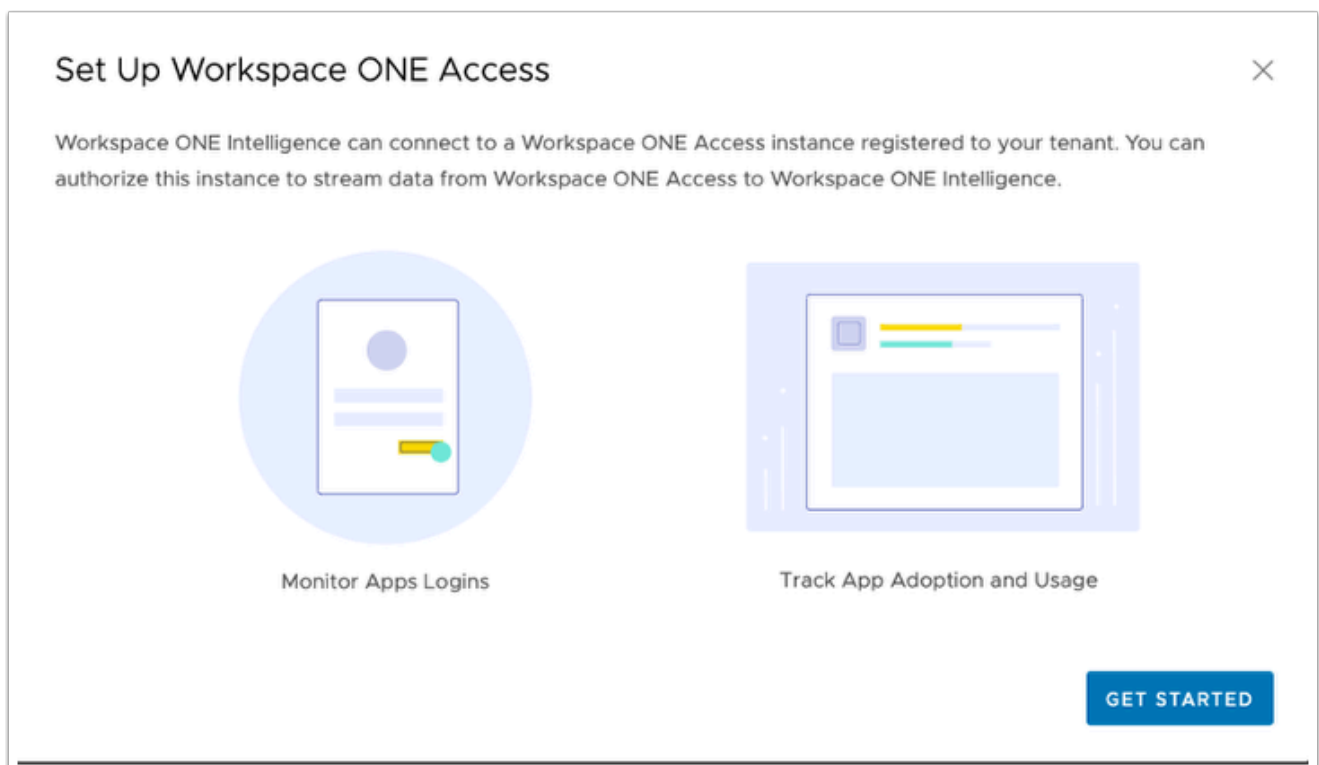
- In the **Terms of Service** page enter your **registered email and details**
  - in the bottom right corner Select **ACCEPT**



- We will setup the integration of WorkspaceOne Intelligence with Workspace ONE Access.
  - This will allow us to begin aggregating information based on logins to Workspace ONE UEM and AppLaunch.
  - At the top of the page select **Integrations**



4. In the **Workspace ONE Access** Box, select **SET UP**



5. In the Set UP Workspace ONE Access window, select **GET STARTED**

Authorize: Workspace ONE Access

Intelligence would like to get access to Workspace ONE Access for the following:


- > Connector Permissions
- ▼ Provide Credentials

Provide your Workspace ONE Access Console URL below.

Tenant Domain

You will be redirected to Workspace ONE Access to authorize.

6. In the **Authorize: Workspace ONE Access** window, expand **Provide Credentials**
- Next to **Tenant Domain** enter the **full FQDN including HTTPS** of your ACCESS Tenant
  - Select **CONNECT TO WORKSPACE ONE ACCESS**



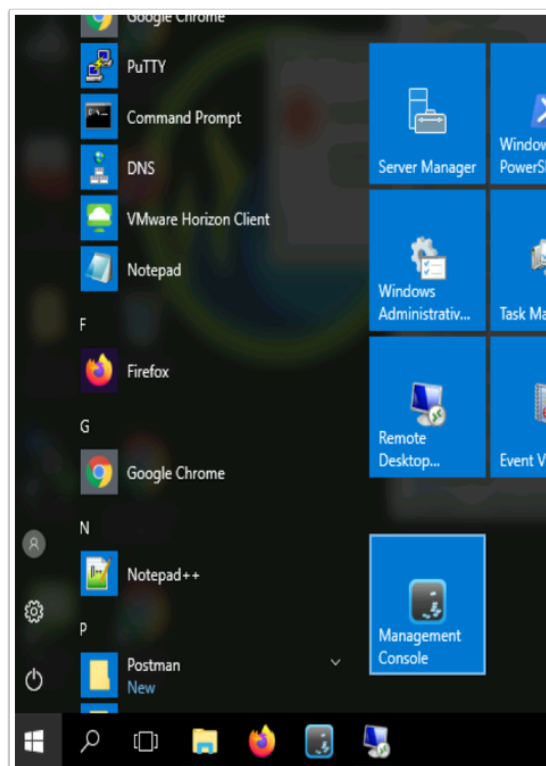
Workspace ONE™

**Workspace ONE Intelligence Integration**

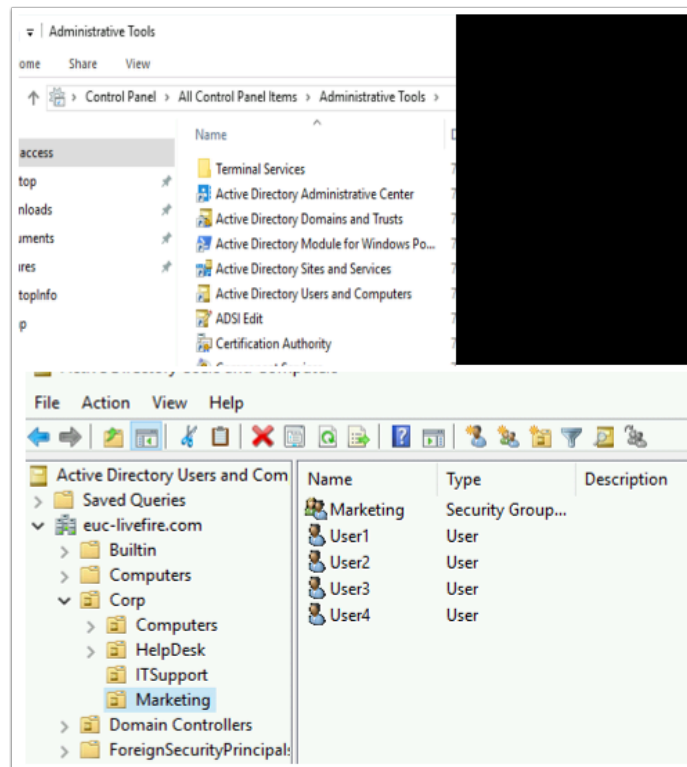
Do you authorize sending user and event data from VMware Workspace ONE Access to Workspace ONE Intelligence?

7. In the **Workspace ONE Intelligence Integration** window, select **Accept**

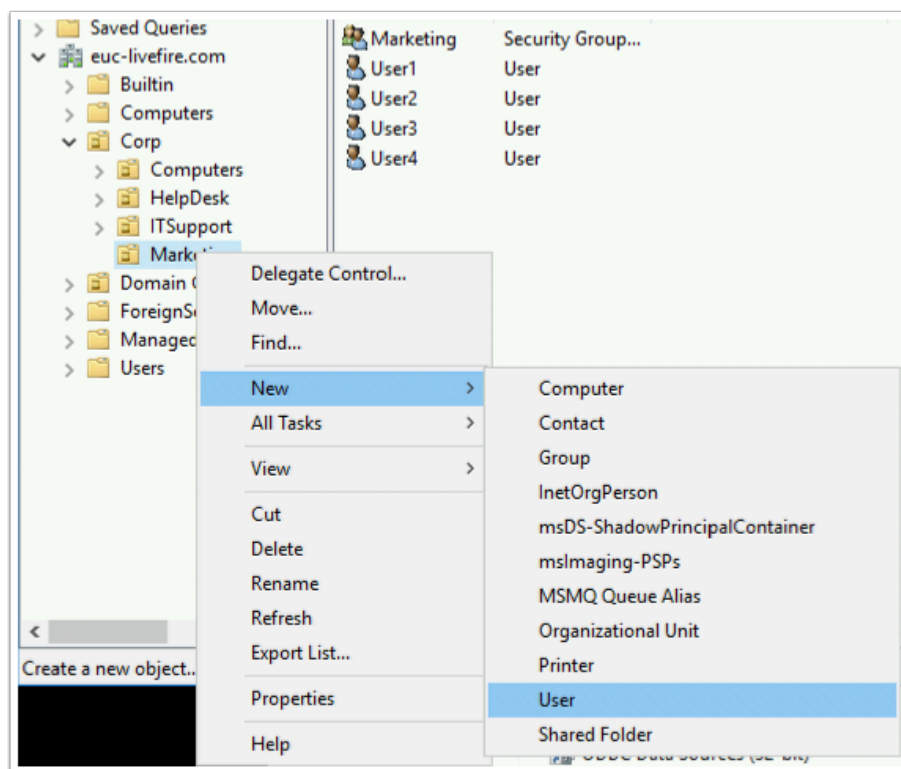
## Part 5. Configuration of a Custom Test Account



1. Revert to your "On-premise" Infrastructure.
  - On the **ControlCenter2** server, select the **Start** button
  - In the **Start Menu**, select **Administrative Tools**

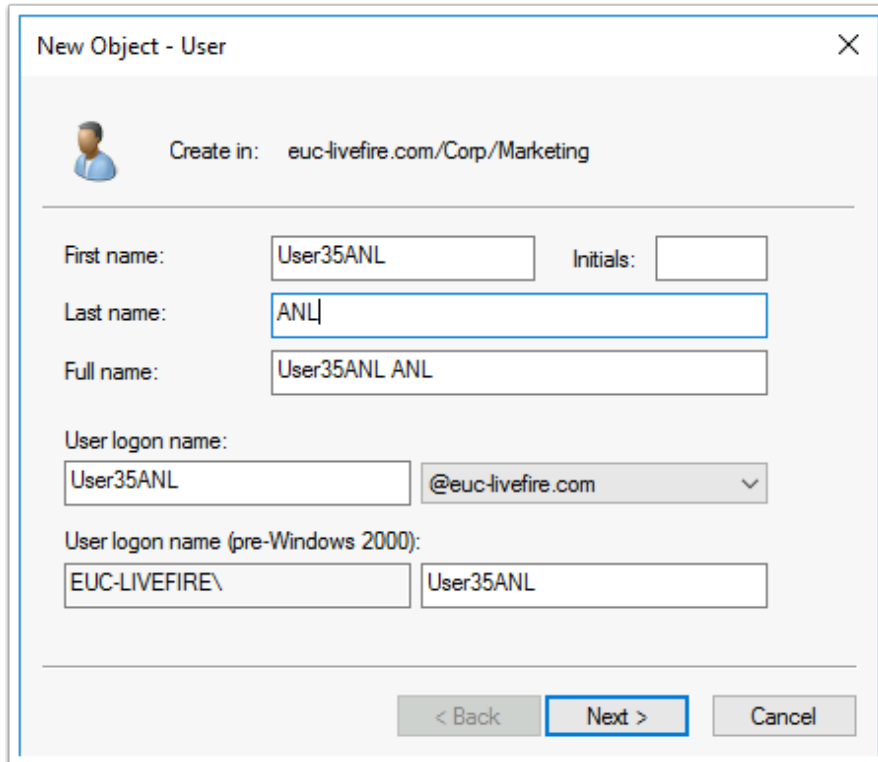


2. Open **Active Directory User & Computers**.
  - Expand the **EUC-livefire.com** domain,
  - Expand the **Corp OU**
  - Expand the **Marketing OU**



3. On the **Marketing OU** select and right-click the **Marketing OU** and select **New > User**,

- For a future Salesforce Lab to work, we need to ensure we create an identical account with all account credentials matching your Salesforce account. Fill in the unique user details,



The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: euc-livefire.com/Corp/Marketing'. Below this, there are several input fields: 'First name' with 'User35ANL', 'Initials' (empty), 'Last name' with 'ANL', and 'Full name' with 'User35ANL ANL'. There are also fields for 'User logon name' (with 'User35ANL' and a dropdown for '@euc-livefire.com') and 'User logon name (pre-Windows 2000)' (with 'EUC-LIVEFIRE\' and 'User35ANL'). At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

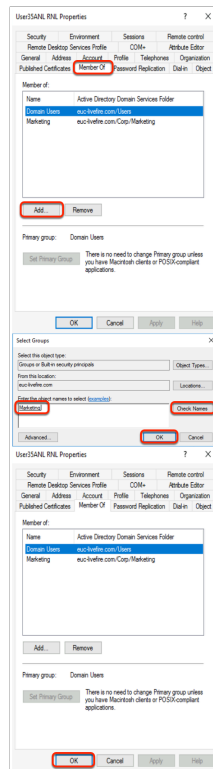
4. Fill in the following details:

- **First Name:** **User xx** {your student number + {the **first letter** of your **city** and country abbreviation}} eg User35ANL
- **Last Name:** the **first letter** of your **city** and country abbreviation eg **ANL**
- **User logon name:** Same as your first name eg **User35ANL**



5. In the **New Object - User**, type and confirm your password **VMware1!**
  - Select the **Password never expires** checkbox, select **Next**, select **Finish**

6. Select your **custom user** and select and go to **Properties**,
  - Select the **General** Tab type in the **email address**, with the user's first name as the user followed by "@euc-livfire.com" eg. **user35ANL@euc-livfire.com**

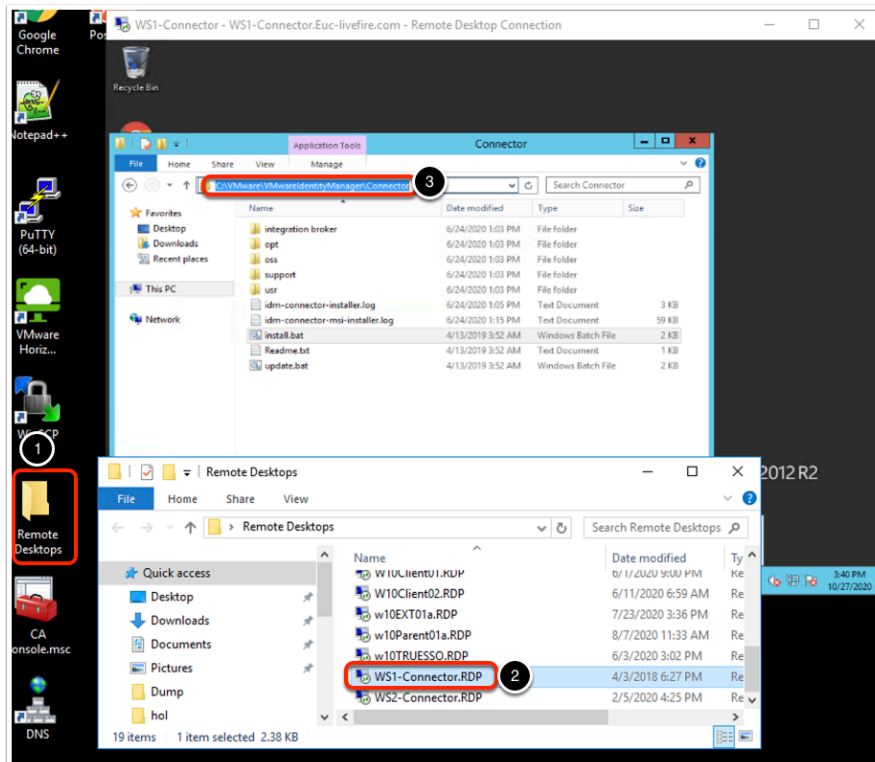


7. Select the **Member Of** tab select **Add**, in the **Enter the object names** box type **Marketing** and select **Check Names**, select **OK**, select **OK**

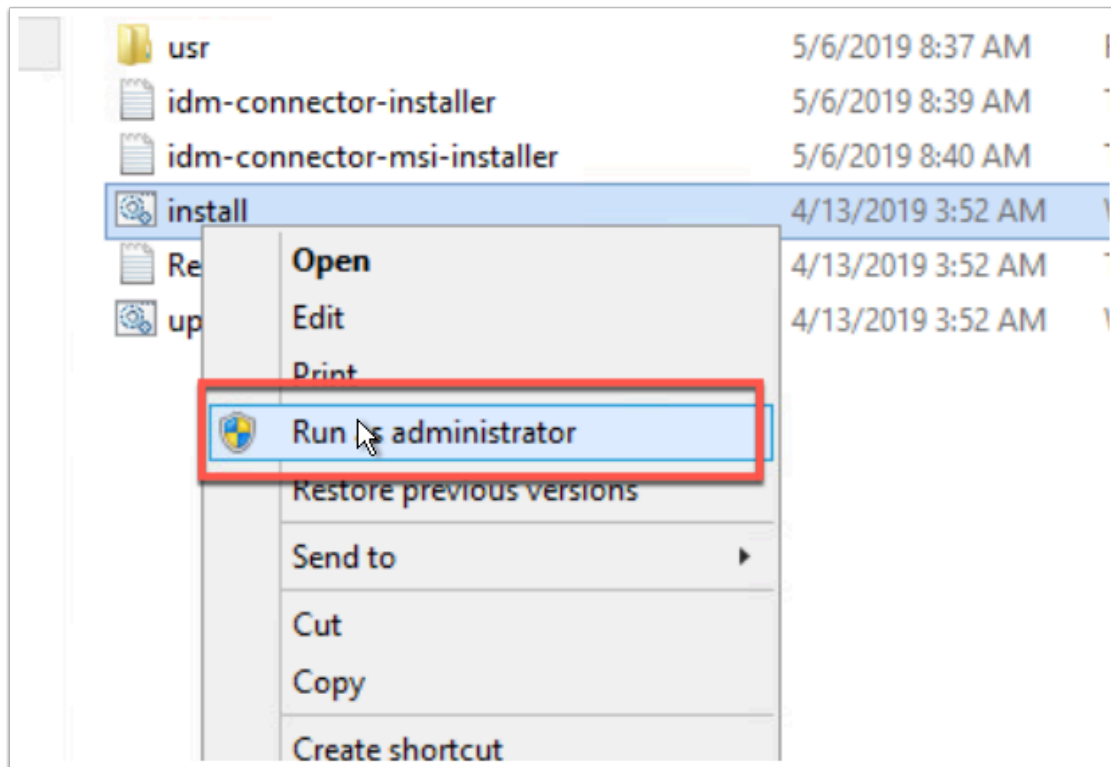
# Configuring the Workspace ONE Access and the AirWatch Cloud Connector

## Part 1. Configuring the Workspace ONE Access Connector

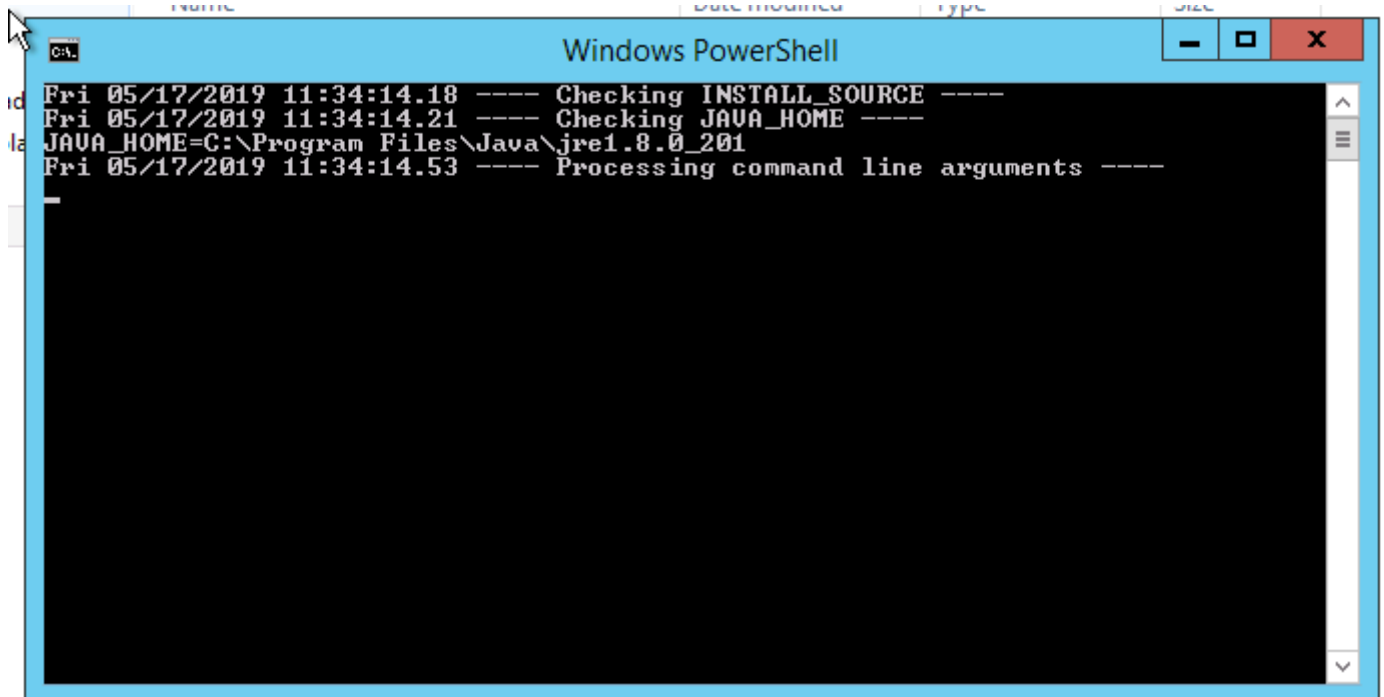
We have pre-installed the Workspace ONE Access Connector for you in the Lab environment. However since we have cloned the machine the connector is in an idle state and needs to be re-initiated.



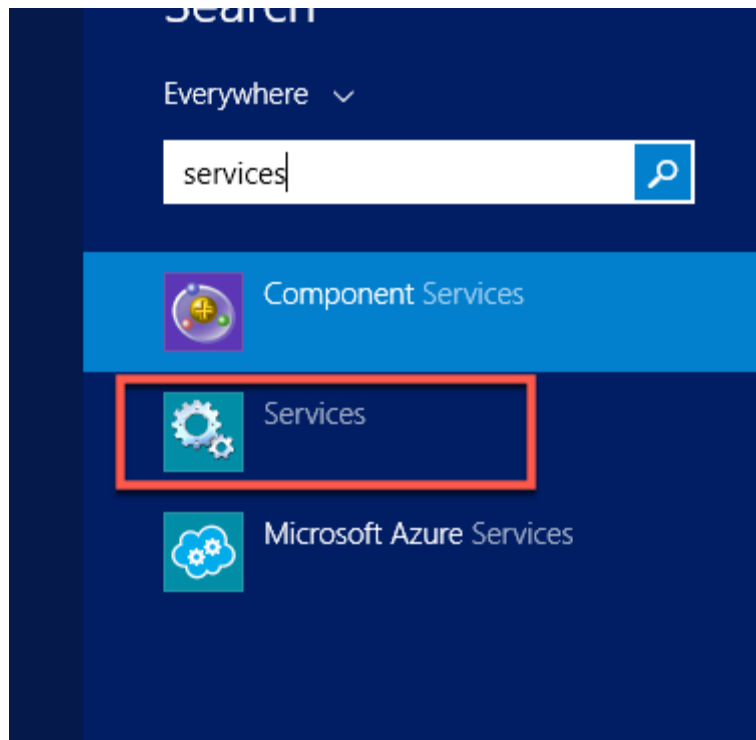
1. Log into your **ControlCenter2** server with username **administrator@euc-livefire.com** and password **VMware1!**
  1. On your **ControlCenter2** server desktop select your **Remote Desktops** folder and select and launch your **WS1-Connector.RDP** shortcut.
  2. When prompted log in as username **administrator@euc-livefire.com** with the password **VMware1!**
  3. On the **WS1-Connector** server open the **File Explorer** to the following path **C:\VMware\VMwareidentityManager\Connector**



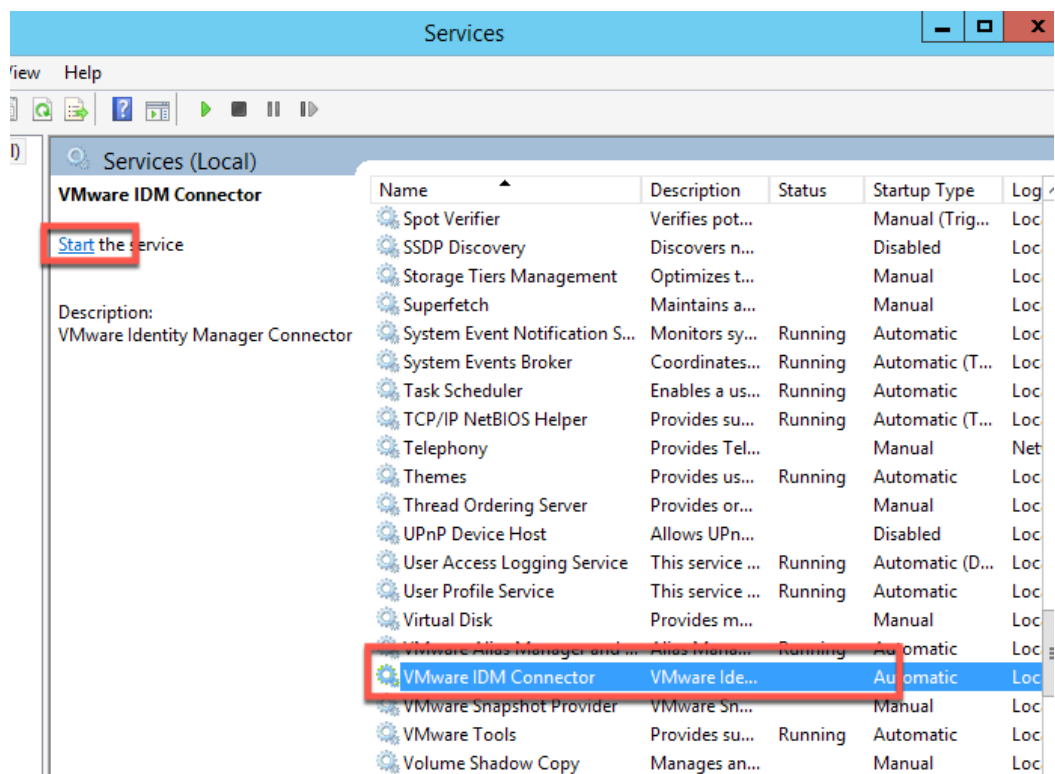
2. Right Click the **install.bat** file and click **Run as Administrator**



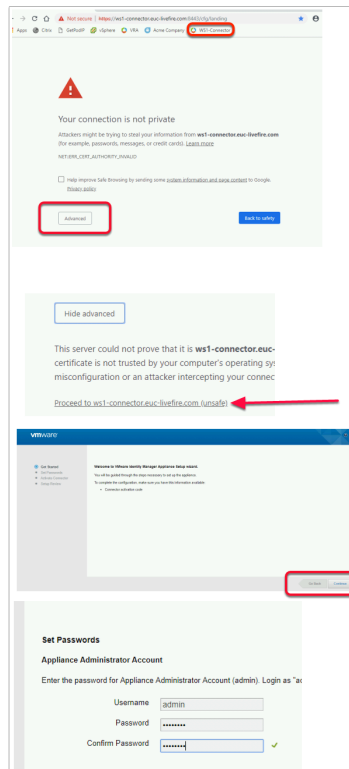
3. This will launch a PowerShell window that will clear out the state of the connector. Wait till the Powershell Window closes which confirms it has run successfully.



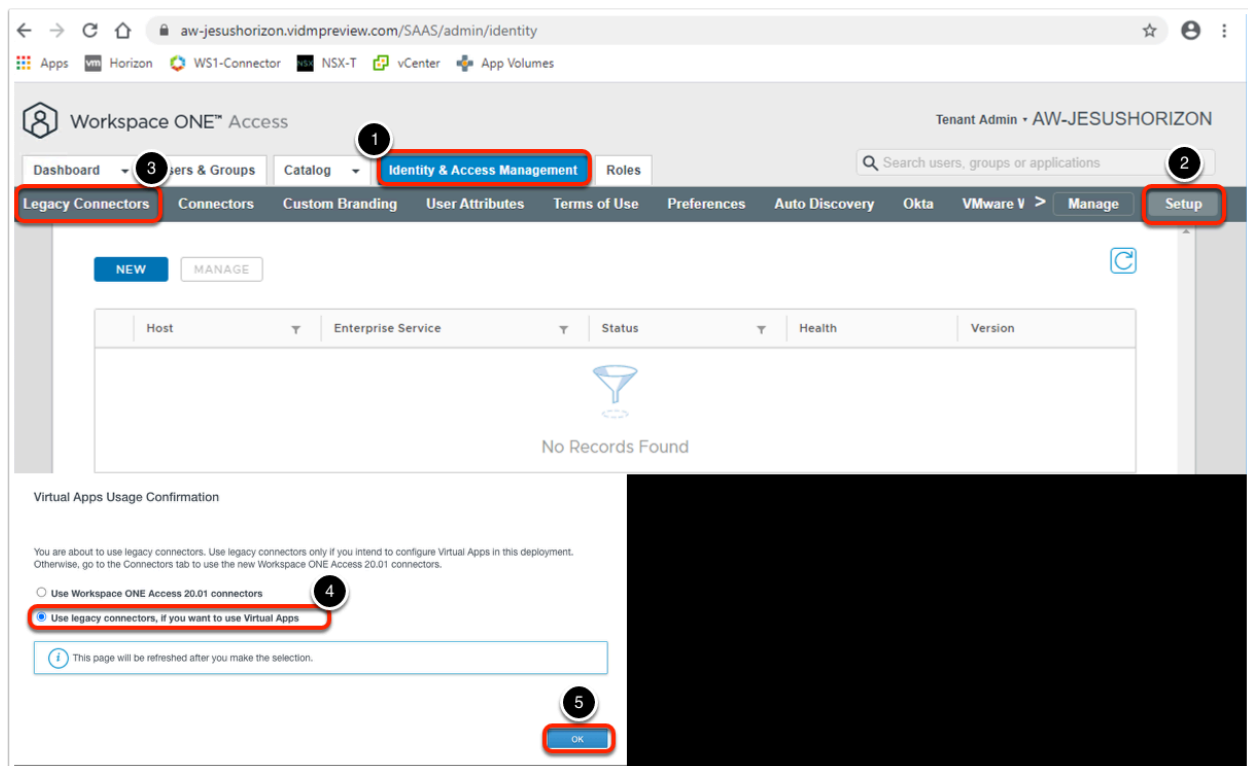
4. Open **services.msc** and **start** the **VMware IDM Connector** service



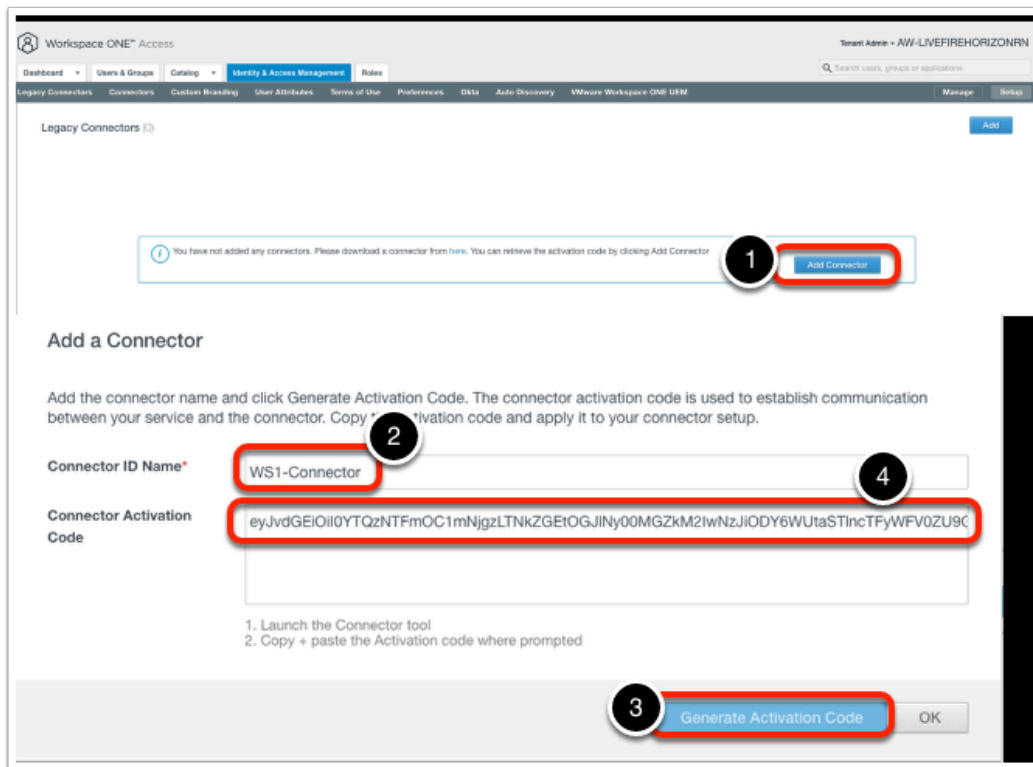
5. Wait for a few minutes till all the services have launched and move on to the next part of the lab.



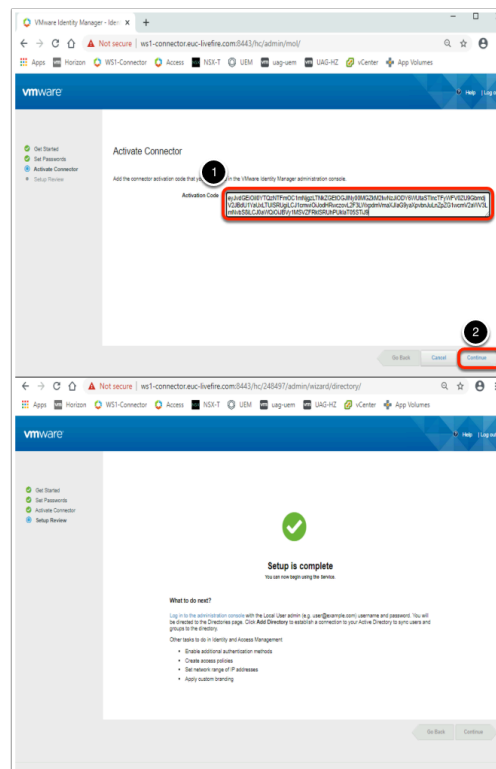
6. Our objective is to associate our on-premise connector instance with our SaaS instance of Workspace ONE Access.
  - On your **Control Center2** server desktop, Open your **Google Chrome browser**.
    1. On your chrome select the **WS1-connector** shortcut or type **https://ws1-connector.euc-livewire.com:8443/cfg** in the address bar
    2. On the Your Connection is not private page, select **Advanced** and select **Proceed to ws1-connector.euc-livewire.comue**.
    3. On the **Get Started** Window select **Continue**
    4. In the **Set Passwords** section next to **Username** type **admin** next to **password** type **VMware1!** next to **Confirm Password** type **VMware1!** select **Continue** at the bottom of the page.



7. On your browser, open up a **second Tab**, navigate to your unique **Workspace ONE Access Tenant** and if you have not done so login as **Administrator** with your **unique password**, that your received in your e-mail login
  - Navigate to **Identity & Access Management > Setup > Legacy Connectors**
  - On the **Virtual Apps Usage Confirmation** window, Select the **radio button** next to **Use legacy connectors, if you want to use Virtual Apps** Select **OK**



- In the **Legacy Connectors** area:
  - select **Add Connector**
  - In the **Add a Connector** window. Next to **Connector ID Name:** type **WS1-Connector**.
  - select **Generate Activation Code**
  - **copy** this code

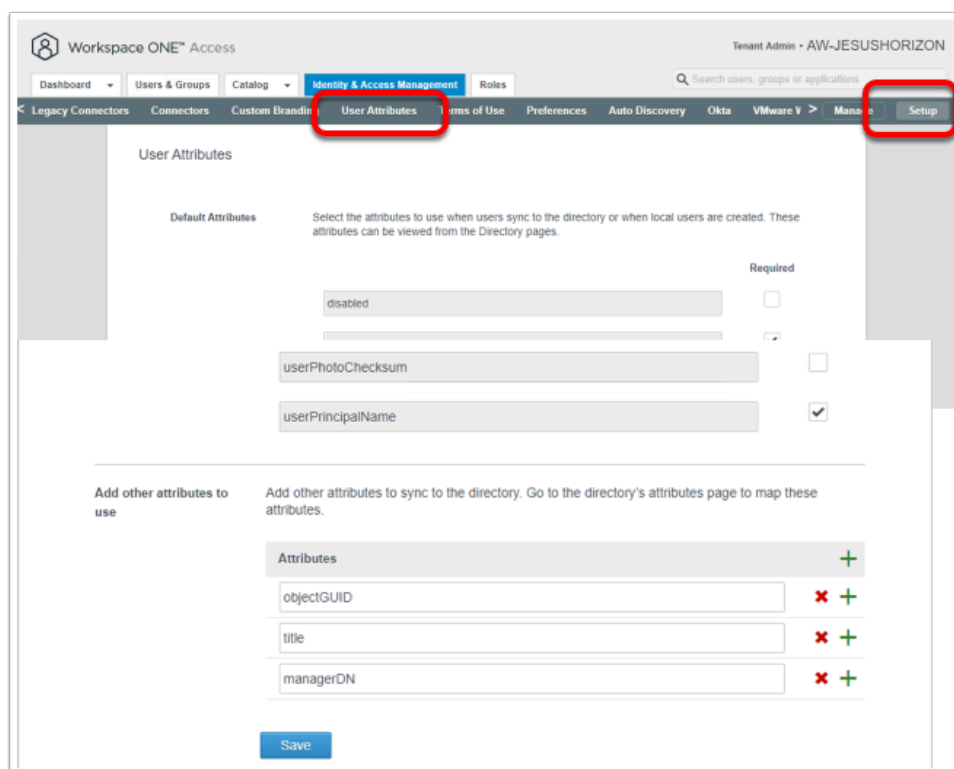




9. **Revert back** to your **WS1-Connector Server** setup: On the **activate connector page** **Paste** this code into the **Activation Code** box of your **Connector configuration** setup, select **Continue**
- You should get a **setup is complete** page inside the Workspace ONE Access Console.

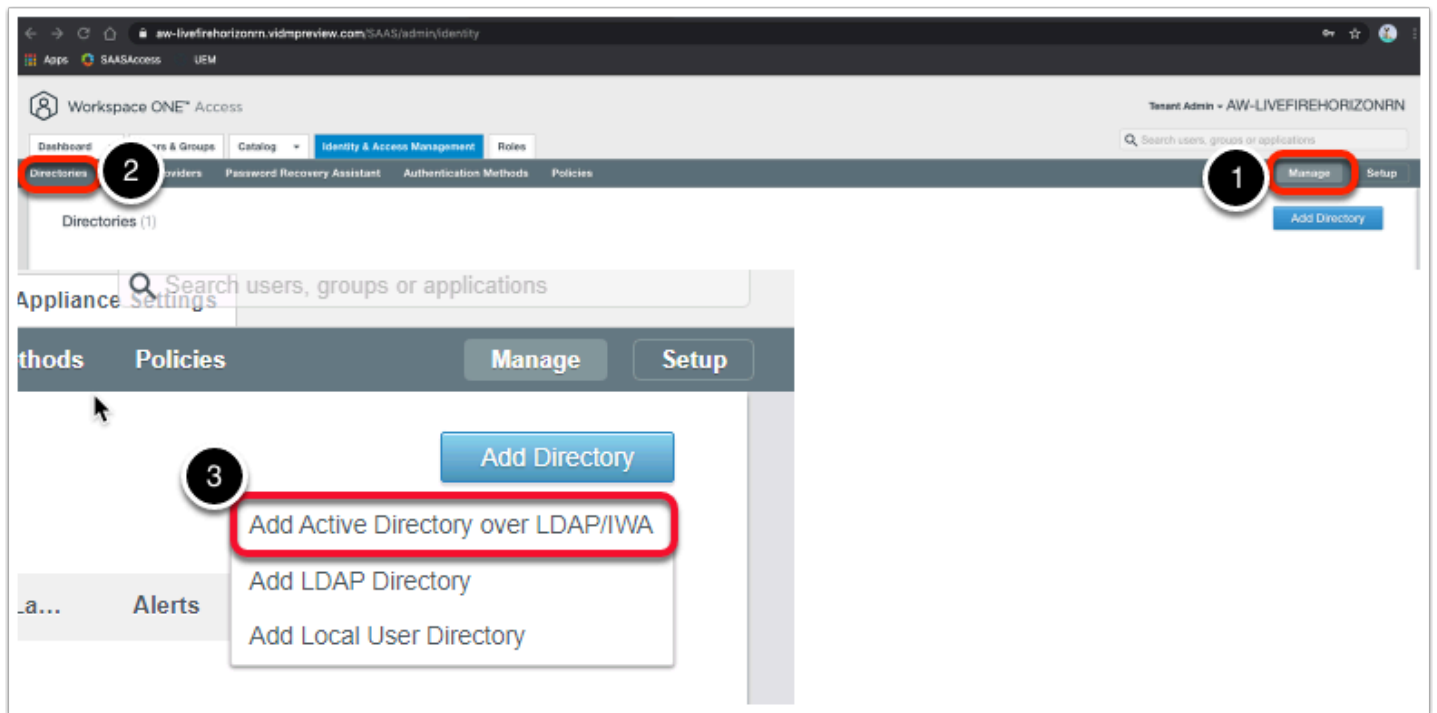
## Part 2 . Configuring Active Directory Sync

We will now configure and synchronise Active Directory to the Workspace ONE Access server using the external connector.



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

1. Navigate to **Identity & Access Management > Setup > User Attributes**  
Notice the attributes that are available and the option available to set these to **Required**.  
**IMPORTANT NOTE:** The attributes set to required **cannot** be changed after a directory sync has taken place.
  - Set the attribute **distinguishedName** and **userPrincipalName** to **Required**
  - Under Attributes to the right select the **Green Plus ( + )** Add the following additional attributes (case sensitive) :
    - **objectGUID**
    - **title**
    - **managerDN**
  - Select **Save**



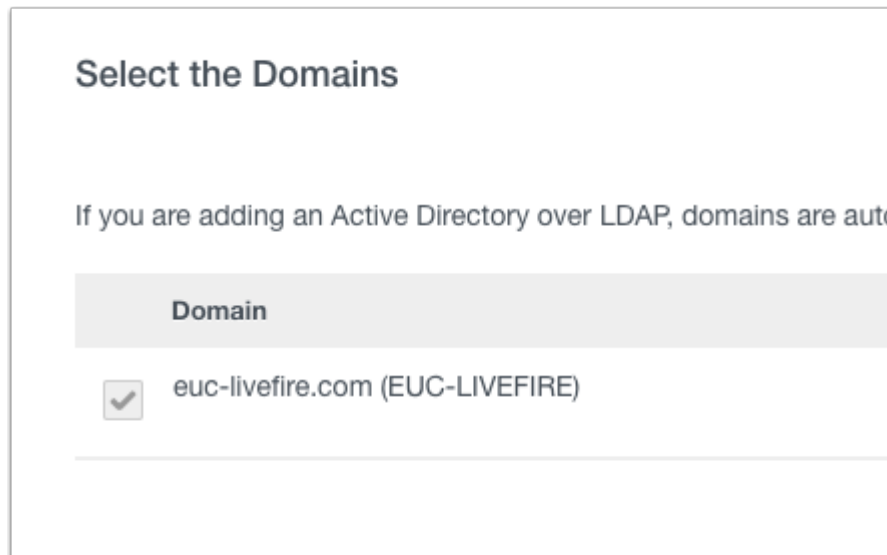
## 2. Configure our AD-sync configuration with Workspace ONE Access.

- To the right of the screen select **Manage**, select **Directories**
- Select **Add Directory** > **Add Active Directory over LDAP/IWA**

## 3. In the **Add Directory** Page, configure the following (please note) The Bind syntax appears to be case sensitive

1. **Directory Name:** **LivefireSync**

2. Ensure the **Active Directory over LDAP** **radio button** is selected
3. The **Sync Connector** select the external connector **ws1-connector.euc-livefire.com**
4. **Directory Search Attribute:** **sAMAccountName**
5. **Base DN:** **dc=EUC-Livefire,dc=com**
6. **Bind DN:** **cn=administrator,ou=corp,dc=EUC-Livefire,dc=com**
7. **Bind DN Password:** **VMware1!**
8. Select **Test Connection**. You will see **Test connection successful**.
9. Select **Save & Next**



Select the Domains

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

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

4. On the **Select the Domains** page, select **Next**. **euc-livefire.com** should be discovered.

**Map User Attributes**

If the attribute in the directory column is mapped to Active Directory attributes, if the directory attribute is not mapped to the correct Active Directory attribute, select the correct attribute from the drop-down menu. To manage the list of required attributes or to add attributes that are not listed, go to the Setup > User Attributes page.

| Attribute Name in VMware Workspace ONE A... | Attribute Name in Active Directory |          |
|---|------------------------------------|----------|
| userPrincipalName                           | userPrincipalName                  | Required |
| userName                                    | sAMAccountName                     | Required |
| lastName                                    | sn                                 | Required |
| firstName                                   | givenName                          | Required |
| email                                       | mail                               | Required |
| distinguishedName                           | distinguishedName                  | Required |
| disabled                                    | userAccountControl                 |          |
| domain                                      | canonicalName                      |          |
| employeeID                                  | employeeID                         |          |
| managerDN                                   | manager                            |          |
| objectGUID                                  | objectGUID                         |          |
| phone                                       | telephoneNumber                    |          |
| sourceAnchor                                | objectGUID                         |          |
| title                                       | title                              |          |

Previous Close **Next**

5. On the **Map User Attribute** page configure the following :

- Scroll down to **objectGuid** and select the **drop down** arrow select **objectGUID**.
- Since this is the attribute we setup earlier in User Attributes we will also need to map it to an AD attribute.
- Next to **managerDN** select **custom input** and type **manager** in the dropdown
- Next to **title** select **title** in the dropdown
- Select **Next**

Select the groups you want to sync

Enter the Group DNs to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, the group names are synced immediately. Memberships of these groups will be synced when the group is entitled to a resource.

☒ Sync nested group members

Specify the group DNs      Select All      Groups to sync      +

dc=euc-livewire,dc=com      Find Groups      x      +

| Group DN               | Mapped Groups |
|------------------------|---------------|
| dc=euc-livewire,dc=com |               |

Cancel      Save & Sync      Save

---

☒ Sync nested group members

Specify the group DNs      Select All      Groups to sync      +

dc=euc-livewire,dc=com      ☒      54 of 54      Select      x      +

| Group DN               | Mapped Groups                      |
|------------------------|------------------------------------|
| dc=euc-livewire,dc=com | All groups in this DN are selected |

6. Configure our AD-sync configuration with Workspace ONE Access....continued

- On the **Select the Groups you want to sync** page, select the green plus (+) to the right of the page,
- Under **Specify the group DNs** type the following **dc=euc-livewire,dc=com** next to the distinguished name you added, select **Find Groups** then the **Select All** check box
- select **Next**.

Select the Users you would like to sync

Enter the User DNs to sync, for example, CN=username,CN=users,DC=example,DC=company,DC=com. All users found under the DN are also synced. To exclude any users from syncing, provide exclusion filters.

Specify the user DNs

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

Add a filter to exclude users

Cancel Save

Review

The groups and users you selected are ready to sync to the directory. You can still make changes before you sync.

|  | Add | Remove | Update |                |
|--|-----|--------|--------|----------------|
|  | 10  | 0      | 0      | Edit User DNs  |
|  | 54  | 0      | 0      | Edit Group DNs |

After the initial sync, the sync is scheduled to run Once per week. You can change the sync frequency now or you can change it later from the Sync Frequency page. [Edit](#)

Cancel Sync Directory

7. Configure our AD-sync configuration with Workspace ONE Access....continued
  1. On the **Select the Users you would like to sync page**, under **specify the user DNs** type **ou=corp,dc=EUC-Livefire,dc=com**
  2. Select **Next**, notice the objects to sync in the Review page.
    - There may be an error, "Missing required attributes email for imaservice" Disregard this error. The sync will stil work.
  3. Select **Sync Directory**

## Part 3: Configuring the Built-in IDP in Workspace ONE Access

Workspace ONE™ Access

Tenant Admin - AW-LIVEFIRE-HORIZON

Dashboard Users & Groups Catalog **Identity & Access Management**

Search users, groups, applications

Directories Identity Providers Password Recovery Assistant Authentication Methods Policies **Manage** Setup

Identity Providers (3)

| Identity Provider Name   | Auth Methods               | Directory        | Network Ranges | Connection(s)                  | Type                 | Status  |
|--------------------------|----------------------------|------------------|----------------|--------------------------------|----------------------|---------|
| System Identity Provider | Password (Local Directory) | System Directory | ALL RANGES     |                                | Built-in             | Enabled |
| Built-in                 |                            |                  |                |                                | Built-in             | Enabled |
| WorkspaceIDP_3123        | Password                   | LivefireSync     | ALL RANGES     | ws1-connector.euc-livefire.com | Workspace ONE Access | Enabled |

1. Navigate to and select **Identity & Access Management** > **Manage**, select **Identity Providers**.

- Notice you now have an additional Identity Provider which is a Workspace IDP called **WorkspaceIDP\_1xxx** which is associated with the LiveFireSync directory we just created above. This is an automatic process whereby when the built in connector is associated with Active Directory this Identity Provider gets created.

Identity Providers (3) [Add Identity Provider](#)

| Identity Provider Name   | Auth Methods               | Directory        | Network Ranges | Connector(s)                  | Type             | Status  |
|--------------------------|----------------------------|------------------|----------------|-------------------------------|------------------|---------|
| System Identity Provider | Password (Local Directory) | System Directory | ALL RANGES     |                               | Built-in         | Enabled |
| <b>Built-In</b>          |                            |                  |                |                               | Built-in         | Enabled |
| WorkspaceIDP_1xxx        | Password                   | LivefireSync     | ALL RANGES     | ws1-connector.euc-livfire.com | Identity Manager | Enabled |

**Configuration for Built-In Identity Provider:**

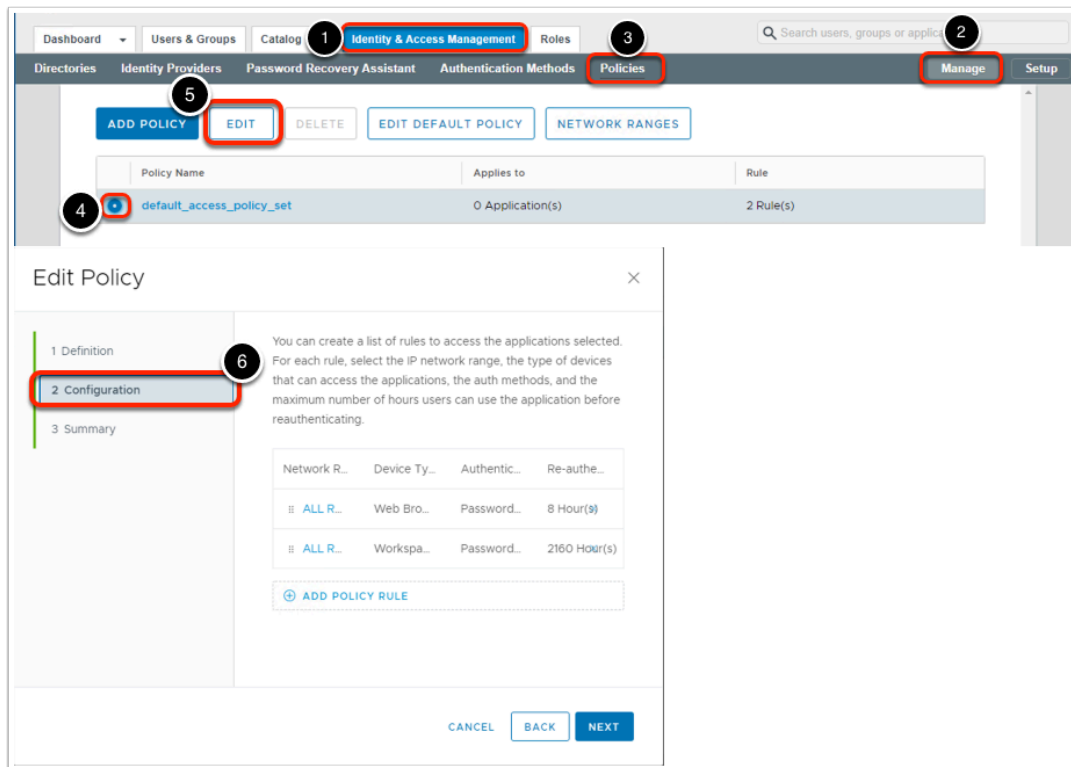
- Directory:** ☒ System Directory, ☒ **LivefireSync**
- Network:** Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below. ☒ **ALL RANGES**
- Authentication Methods:** Select which authentication methods the IdP will use to authenticate users.
  - Authentication Methods: Password (Local Directory)
  - Associate Authentication Method: ☐
- Connector(s):**
  - ☒ **WS1-Connector (ws1-connector.euc-livfire.com)** ✗
  - Add a Connector: You can select additional connectors for high availability (HA). Create the connector activation code from the Add a Connector page and set up the connector, and then select the connector for this IdP. Important: For high availability, each connector must have the same authentication method configuration.
- Connector Authentication Methods:**
  - Authentication Methods: Password (cloud deployment) ☒
  - Associate Authentication Method: ☐

2. We will now associate the **Built-In iDP** with our LivefireSync Directory and the external connector to ensure **Password (Cloud Deployment)** can be used as an authentication method.

1. Select **Built-In**.

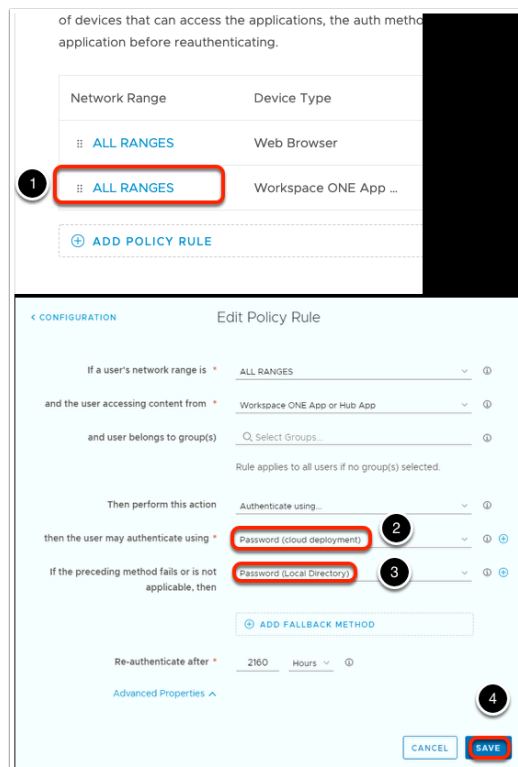
2. In the **Built-in iDP** windows select the following:

- Select **LivefireSync** under **Users**
- **All Ranges** under Network
- **Add** the **WS1-Connector.euc-livfire.com** to the connector section
  - Click **Add Connector** to confirm
- Select **Password (Cloud Deployment)** **checkbox**
- Select **Save** at the bottom of the page.



3. We need to ensure that our default access policy has **Password (Cloud Deployment)** set as the authentication method.

- Navigate to **Identity & Access Management > Manage > Policies**.
- Select the **radio button** next to **default\_access\_policy\_set** and select **EDIT**
- Select **Configuration** on the left navigation





4. Select **ALL RANGES** next to **Workspace One App Policy**
- Next to **then the user may authenticate using \*** and select **Password (Cloud Deployment)** as the first authentication form.
  - Next to **If the preceding method fails or is not applicable, then** select **Password (Local Directory)**
  - Select **SAVE** at the bottom of the page.

**Edit Policy**

1 Definition  
2 Configuration  
3 Summary

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

| Network Range | Device Type           | Authentication           | Re-authenticate |
|---------------|-----------------------|--------------------------|-----------------|
| ALL RANGES    | Web Browser           | Password*                | 8 Hour(s)       |
| ALL RANGES    | Workspace ONE App ... | Password (cloud deplo... | 2160 Hour(s)    |

ADD POLICY RULE

CANCEL BACK NEXT

Then perform this action

Authenticate using...

then the user may authenticate using \*

Password (cloud deployment)

If the preceding method fails or is not applicable, then

Password (Local Directory)

ADD FALLBACK METHOD

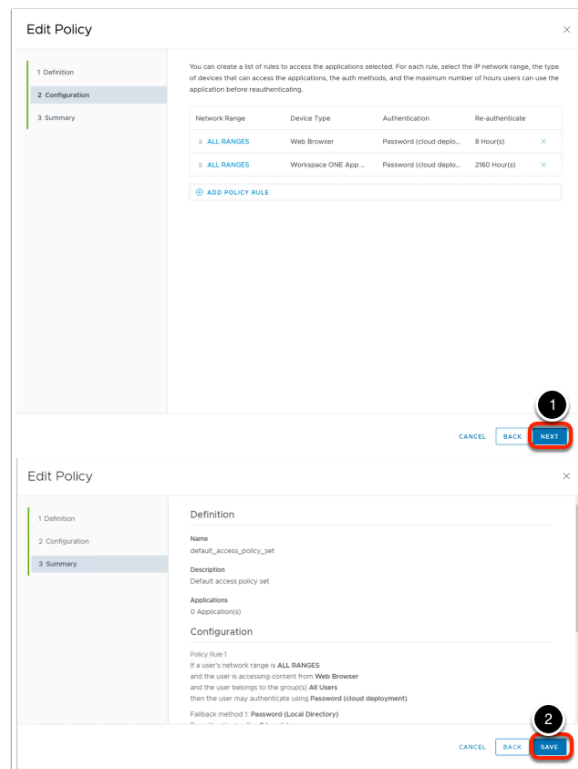
Re-authenticate after \*

8 Hours

Advanced Properties ^

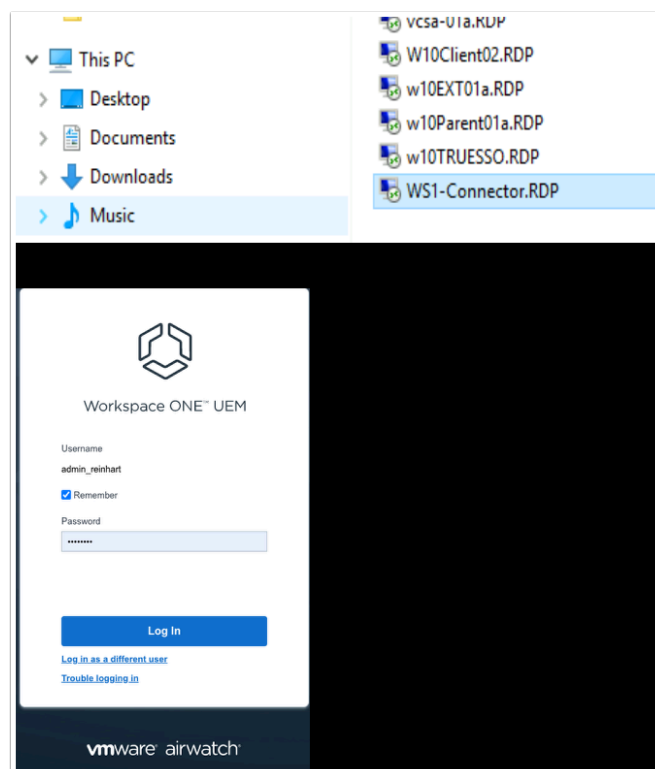
CANCEL SAVE

5. Select **ALL RANGES** next to **Web Browser**
- Next to **then the user may authenticate using \*** and select **Password (Cloud Deployment)** as the first authentication form.
  - Next to **If the preceding method fails or is not applicable, then** select **Password (Local Directory)**
  - Select **SAVE** at the bottom of the page.

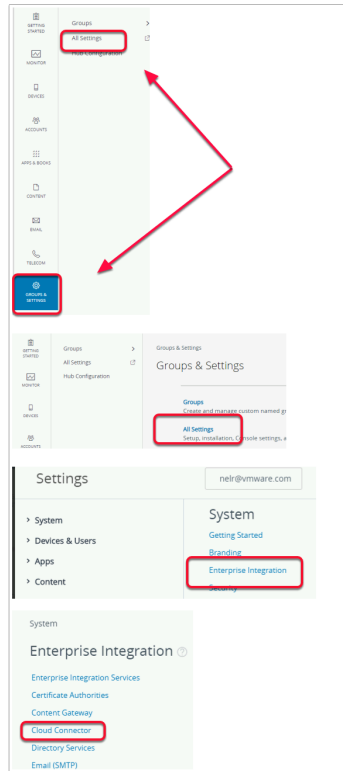


6. On the **Edit Policy** window, select **Next**
  - Select **SAVE**

## Part 4: AirWatch Cloud Connector - Installation



1. On the ControlCenter2 desktop open and locate the **Remote Desktop** Folder. Launch **WS1-Connector.euc-livewire.com RDP shortcut**.
  - Open your **chrome browser** and login to **DW-livewire.awmdm.com**, using your **custom username** and password **VMware1!** (or your custom password if the default needed to be changed)
  - If you get prompted with **Workspace ONE UEM highlights**, **Close** the window.



2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector**

System > Enterprise Integration

## Cloud Connector ?

**General**   Advanced

---

Current Setting   ☐ Inherit   ☒ Override

---

Enable AirWatch Cloud Connector   **ENABLED**   DISABLED

Enables secure connection to enterprise components

Enable Auto Update   **ENABLED**   DISABLED

Enabling Auto Update will seamlessly update the AirWatch Cloud Connector installed on your server after the corresponding AirWatch Cons... [Show More](#)


---

Child Permission \*   ☐ Inherit only   ☐ Override only   ☒ Inherit or Override

**SAVE**

3. Select the **override** radio button and then select **ENABLED** on both toggle options.
  - Select **Save** at the bottom of the page

! The VMware Identity Manager connector is no longer included with the AirWatch Cloud Connector (ACC) installer. If you still need access to the VMware Identity Manager connector, it can be found [here](#).

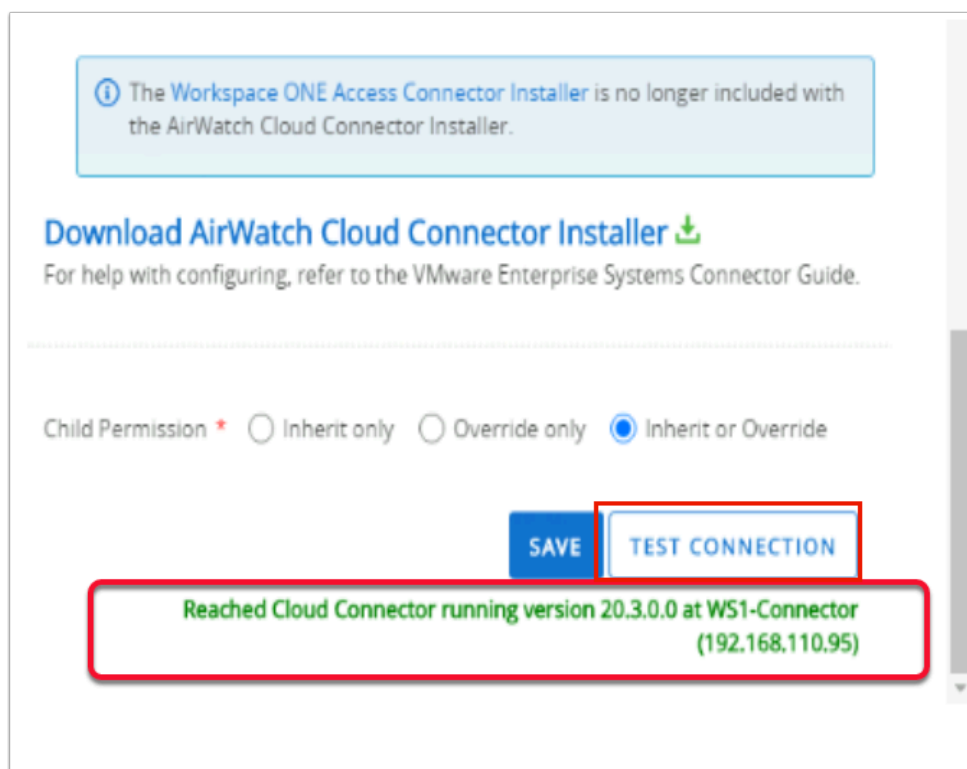
**Download AirWatch Cloud Connector Installer** 

For help with configuring, refer to the AirWatch Cloud Connector Guide.

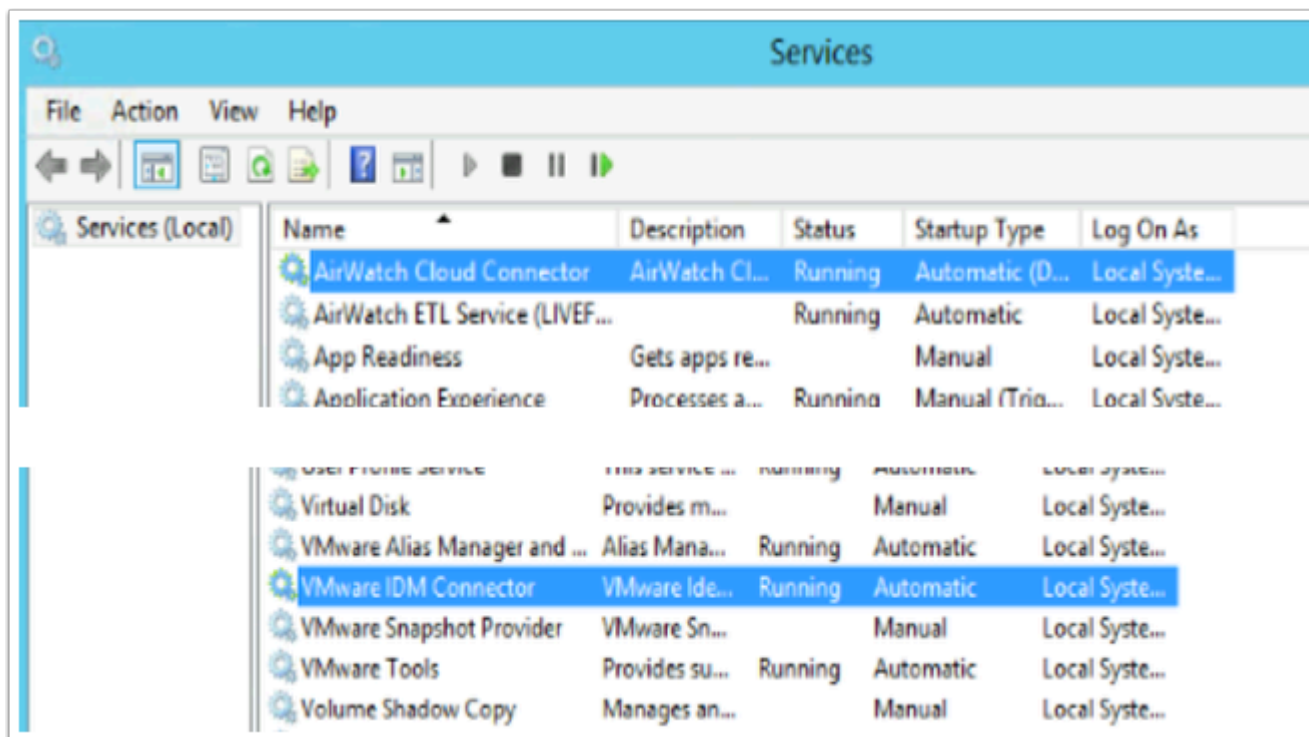
4. Now click the **Download AirWatch Cloud Connector Installer**



6. On the **Ws1-Connector** machine, install the ACC using the installer that you have downloaded. This might require a reboot of the Server.
  1. Select **Airwatch Cloud Connector.exe** and select **open**
  2. Select **Run**
  3. Select **Next**
  4. Select the **licensing to accept terms...** **radio button** , select **Next**
  5. Select **Next**
  6. In the **ACC Certificate Password** window type the password **VMware1!** and select **Next**
  7. Select **Next**
  8. Select **Install**
  9. Select **Finish**

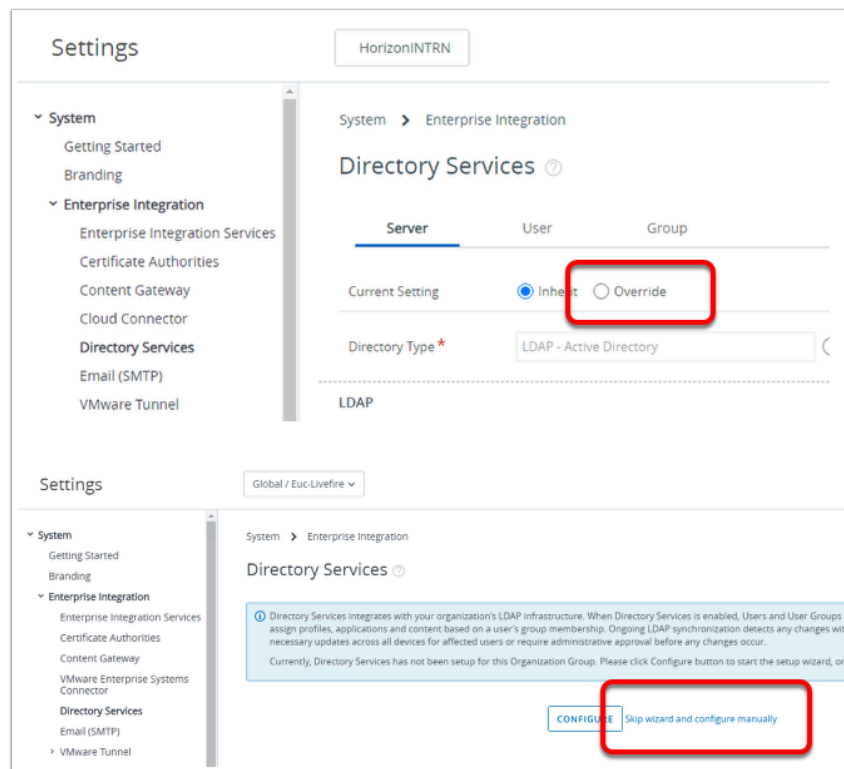


7. Once the ACC is installed you can **test the connection** inside the UEM console.  
You should see **AirWatch Cloud Connector is active**



8. You will now see that there are two services in the **Programs and Features** that are considered "connectors" We have the **AirWatch Cloud Connector** and the **VMware Identity Manager Connector**

## Part 5 Workspace ONE UEM & Active Directory Integration



## 1. In your **Settings** window

- from the left hand navigation pane select **Directory Services** under **Enterprise Integration**
- Select the **Override** radio button
- Select **Skip wizard and configure manually**

The screenshot shows the 'LDAP' configuration section in the Horizon Settings window. The 'Directory Type' is set to 'LDAP - Active Directory'. The 'DNS SRV' is 'ENABLED'. The 'Server' is 'controlcenter2.euc-liveware.com'. The 'Encryption Type' is 'NONE'. The 'Port' is '389'. The 'Protocol Version' is '3'. The 'Use Service Account Credentials' is 'ENABLED'. The 'Bind Authentication Type' is 'GSS-NEGOTIATE'. The 'Bind Username' is 'administrator'. The 'Clear Bind Password' checkbox is unchecked. The 'Bind Password' field is masked with asterisks. The 'Domain' is 'euc-liveware.com' and the 'Server' is 'controlcenter2.euc-liveware.com'. The 'ADD DOMAIN' button is visible at the bottom.



2. From the **Directory Services** Interface, Under the **Server Tab** ensure the following are selected
- Directory: **LDAP-Active Directory**
  - DNS SRV: **Disabled**
  - Server : **ControlCenter2.euc-livefire.com**
  - Encryption Type: **None**
  - Port: **389**
  - Protocol Version: **3**
  - User Service Account Credentials: **Disabled**
  - Bind Authentication Type: **GSS-Negotiate**
  - Bind User Name: **administrator**
  - Bind Password: **VMware1!**
  - Domain: **euc-livefire.com**

The screenshot shows the 'Directory Services' configuration page with the 'User' tab selected. The 'Current Setting' is 'Override'. The 'Domain' is 'euc-livefire.com' and the 'Base DN' is 'DC=euc-livefire,dc=com'. The 'User Object Class' is 'person' and the 'User Search Filter' is '(&(objectCategory=person)(sAMAccountName={EnrollmentUser}))'.

System > Enterprise Integration

### Directory Services ?

Server User Group

Current Setting ☐ Inherit ☒ Override

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

User Object Class\* person ⓘ

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

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

System > Enterprise Integration

## Directory Services

Server User **Group**

✓ Saved Successfully

Current Setting: ☐ Inherit ☒ Override

Domain: euc-livewire.com Base DN: DC=euc-livewire,DC=com

Group Object Class: Available Base DN

Organizational Unit Object Class: DC=euc-livewire,DC=com

> Advanced

Child Permission: ☐ Inherit ☐ Override

**1** SAVE **2** TEST CONNECTION START SETUP WIZARD

Connection successful with the given server name, bind user name, and password.

4. Repeat these steps for the third tab **Group**

- Under Base DN, next to **defaultUserDN** select the **+** icon
- Select the first option which is **DC=euc-livewire,DC=com**, you may be require to manually type this value.
- Scroll to the bottom of the page and select **Save**
- Select **TEST CONNECTION**

## Test Connection

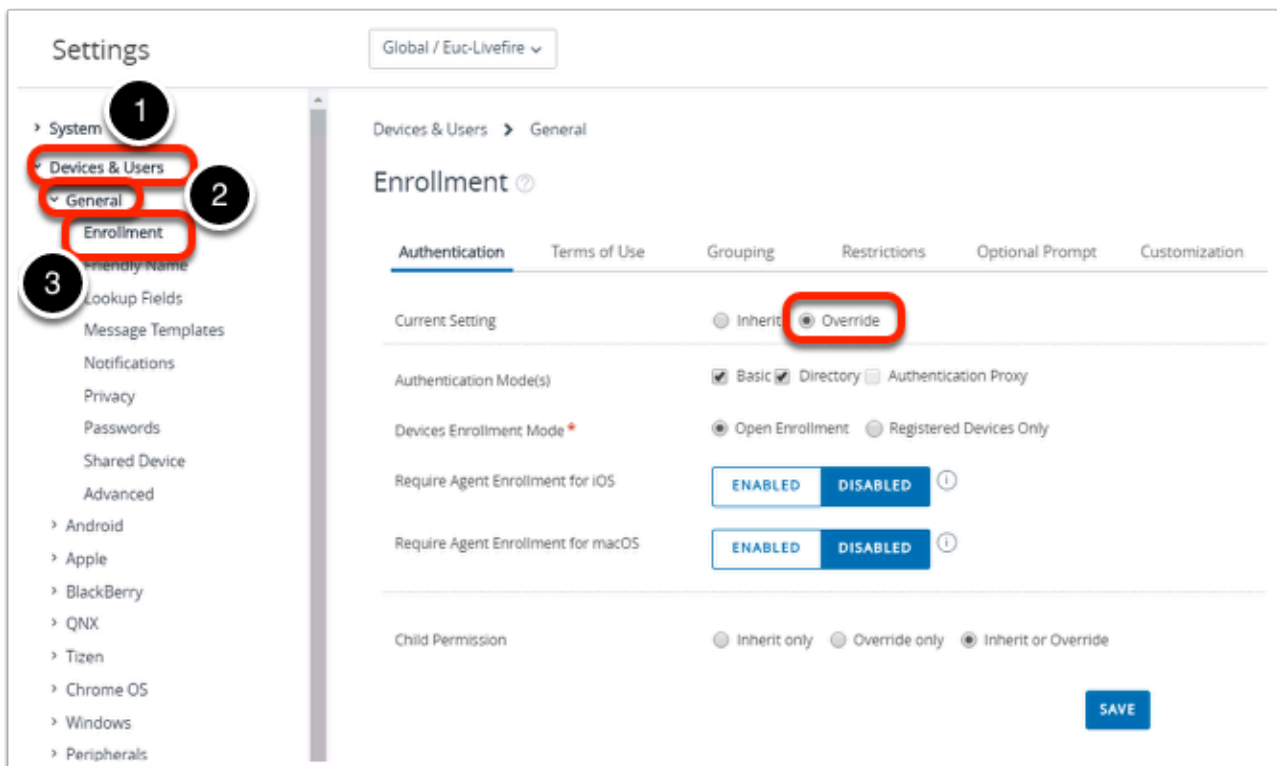
Server

| Domain           | Status   |
|------------------|--|
| euc-livewire.com | Connection successful with the given server name, bind username, and password. |

TEST AGAIN

5. You should have a **Test Connection** window launch saying **Connection successful....**

- Select **CANCEL** to close the window
- **Close** the Enrollment window

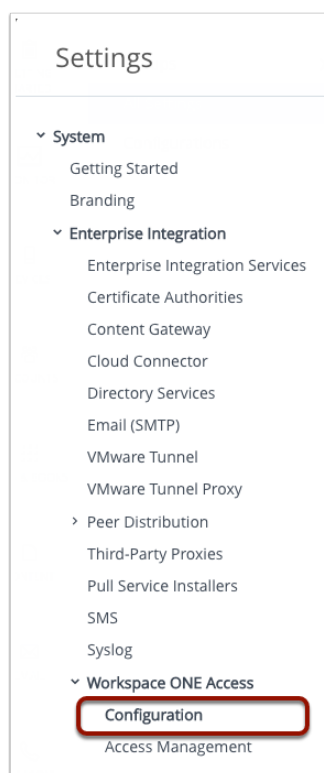


6. Let's ensure users can enroll their devices using Active Directory credentials.
  - Select **Groups & Settings** , > **All Settings** under **Devices & User** > **General** > **Enrollment**
  - Ensure the **Override** radio button is selected.
  - Next to **Authentication Modes(s)** ensure the the **Directory** check box is selected
  - Select **SAVE**
  - Close the **Settings** window, by selecting the **X** on the right of the window.

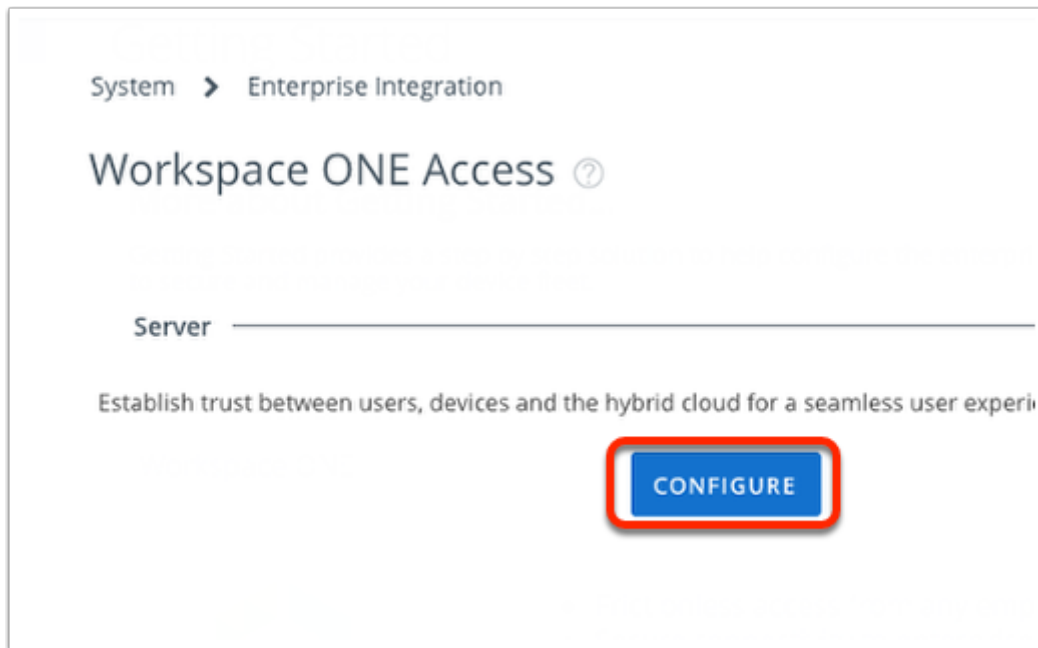
# Workspace ONE Access and Workspace ONE UEM Integration

In this lab we will follow the required steps to configure the Workspace one access and Workspace ONE UEM integration. these steps take place in the Workspace ONE UEM console

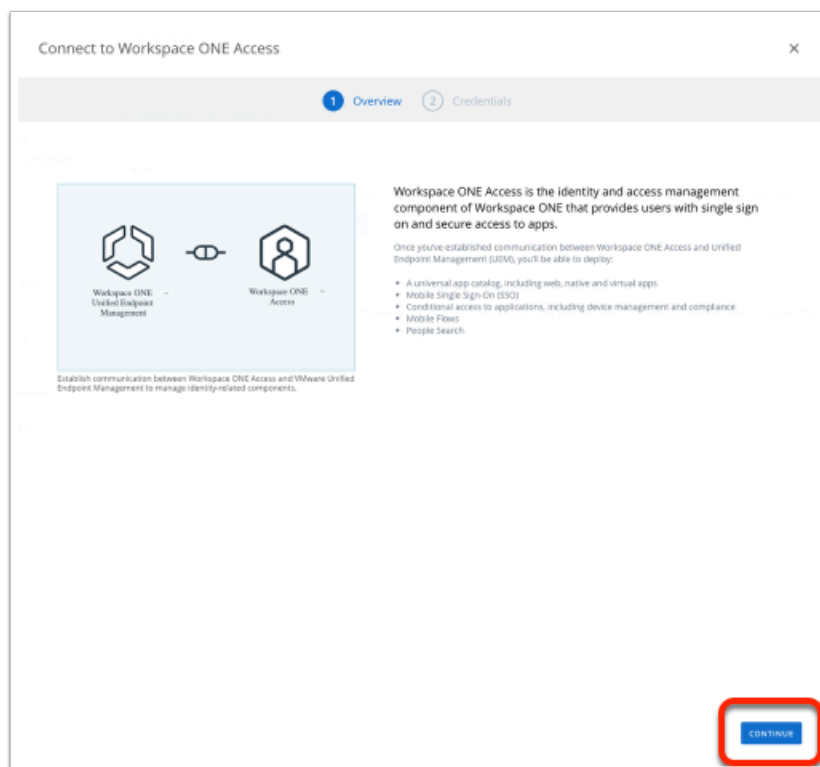
## Part 1: Workspace ONE UEM console configuration.



1. Return to your the Workspace ONE UEM Admin console if its not open already go to <https://dw-livewire.awmdm.com> in your Chrome browser.
  - Navigate to **Groups and Settings > All Settings > System > Enterprise Integration > Workspace ONE Access > Configuration**



2. Under the **Server** area, select **CONFIGURE**



3. On the **Connect to Workspace ONE Access** window, select **CONTINUE**

Connect to Workspace ONE Access

Overview 2 Credentials

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

Tenant URL

Username

Password

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

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

TEST CONNECTION

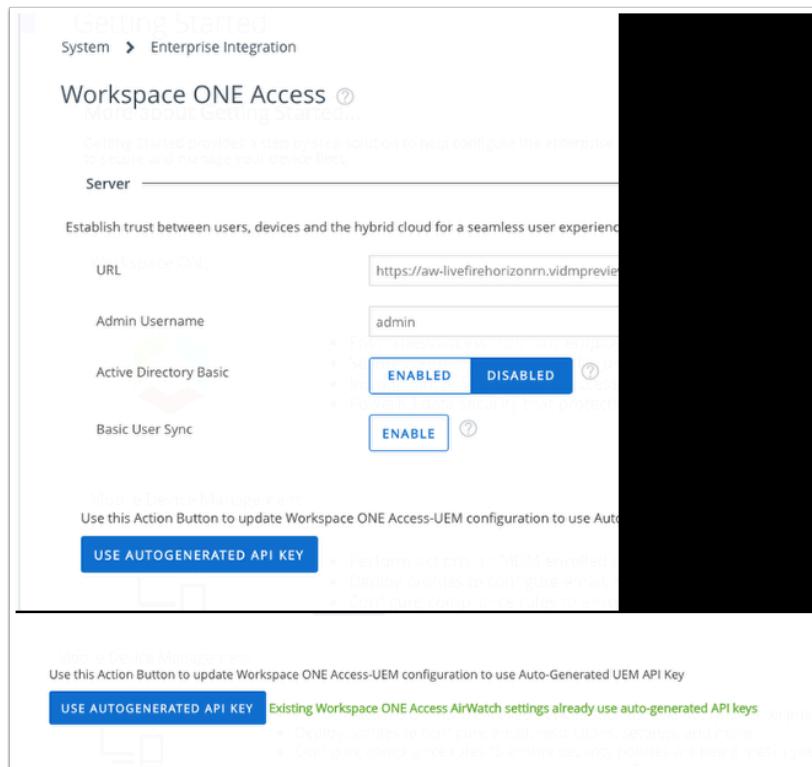
Test to confirm Workspace ONE UEM and Workspace ONE Access are communicating securely.

TEST CONNECTION

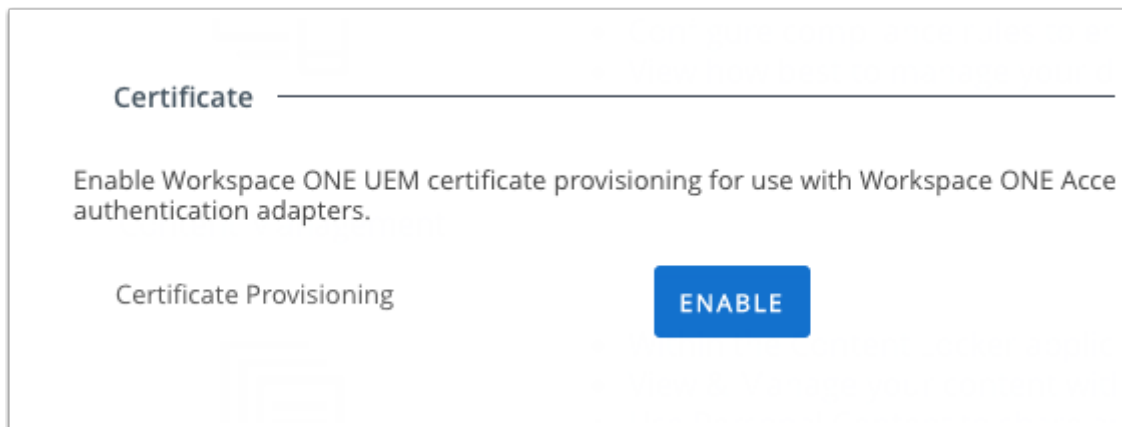
Test connection successful

BACK SAVE

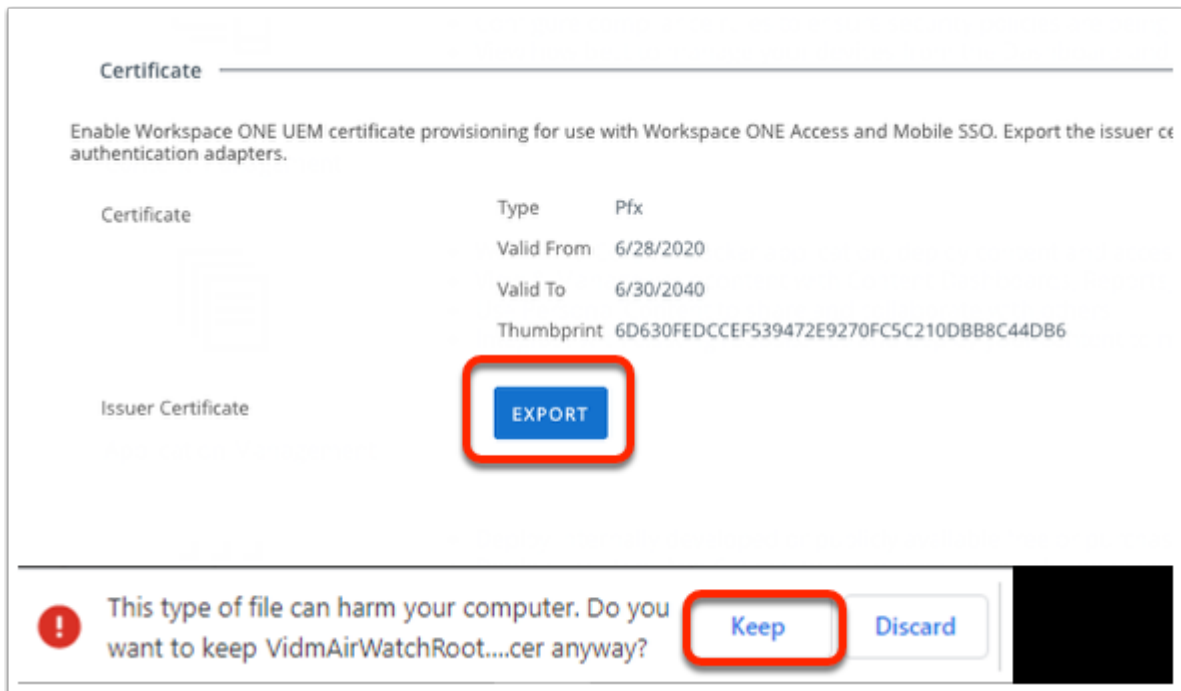
4. On the **Connect to Workspace ONE Access** window enter the following:
  - **Tenant URL:** Your Tenant eg. <https://aw-livefirehorizonrn.vidmpreview.com/>
  - **User Name:** Your Tenant Admin account
  - **Password:** Your Tenant Password
  - Select **TEST CONNECTION** to ensure Tenant configuration has been entered successfully.
  - Select **SAVE** and close the settings window



5. Towards the center of the page select **"USE AUTOGENERATED API KEY"**



6. In the **Certificate** section, next to **Certificate Provisioning** click **ENABLE** - we will use this certificate later for Single-Sign-On with Windows 10



7. Under the Certificate section, you are now able to select **EXPORT**. Select **EXPORT**
- If you get a security warning click **Keep**
  - We will use this certificate in a later exercise, leave this window open for the next part.



# Federating a SAML application with Workspace ONE Access

## Workspace ONE SaaS application deployment number 1

This lab is intended to prepare those federating SaaS applications for authentication via Workspace ONE Access. As SAML is a standard authentication type, this example is just one of many documented integrations.

Please take Note!

For all SaaS resources, ensure you document all associated access information in a text editor

- Admin URL
- Username
- Password

## Part 1. Salesforce Setup

The screenshot shows the Salesforce Lightning Platform Developer Edition sign-up page. The page has a light blue header with the Salesforce logo and the text 'lightning platform'. Below the header, it says 'Get your very own Developer Edition' and 'A full featured copy of Lightning Platform, for FREE'. The main form contains fields for Name (First and Last), Email, Role (dropdown menu), Company, Username, and Password. There are also checkboxes for marketing communications and terms of service. A 'Sign me up' button is at the bottom of the form. Below the form, there is a link for 'Already have a Salesforce Developer Environment? Log In'. At the bottom of the page, it says 'Almost there... Please check your email to confirm your account.' and a link for 'Wondering where to start? Read our Getting Started page.'

## 1. Signing up for a Salesforce developer trial account.

1. Open a **new tab** on your **Browser** on the **ControlCenter2** desktop
2. Navigate to <https://developer.salesforce.com/signup> for a free account.
  - Fill in your details using a personal e-mail address. Please ensure this e-mail address has not previously been used with SFDC.
  - If you have then one option might be to create a dummy email address with Outlook and register this.
  - Be sure to put in **Livefire** as your company
  - When complete select **Sign me up >**

Thanks for signing up with Salesforce!

Click below to verify your account.

[Verify Account](#)

To easily log in later, save this URL:  
<https://verify3-dev-ed.my.salesforce.com>

Username:  
ppgsa.farap@gmail.com

Again, welcome to Salesforce!

© Copyright 2000-2019 Salesforce.com, Inc. All rights reserved. Various trademarks held by their respective owners.

**Change Your Password**

Enter a new password for richardpregan@outlook.com.  
Make sure to include at least:

- 8 characters
- 1 letter
- 1 number

\* New Password Good

\* Confirm New Password Match

Security Question

▼ In what city were you born?

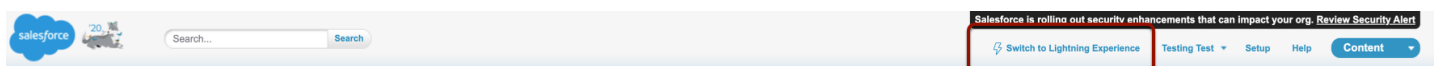
\* Answer  
London

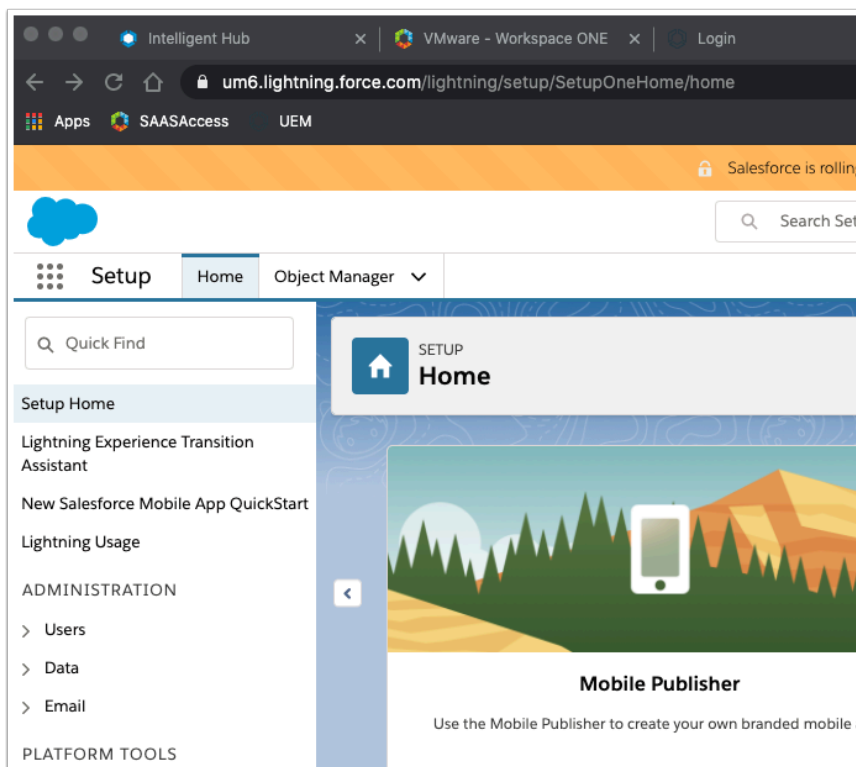
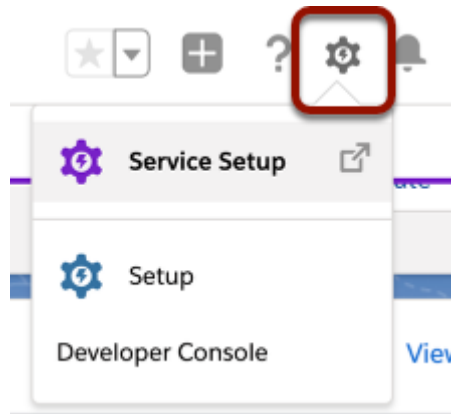
[Change Password](#)

Password was last changed on 30/06/2020, 15:12.

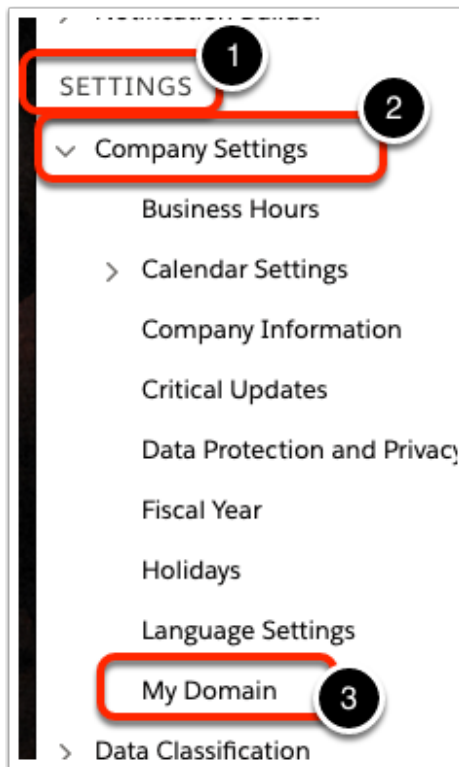
## 2. Go to your **email** and confirm your registration.

- Select **Verify Account**. This will take you to the **Change Your Password** Site.
- **Set a password of your choosing** and provide a security question and answer
- Select **Change Password** to save and you will be redirected automatically to the Setup Home page.

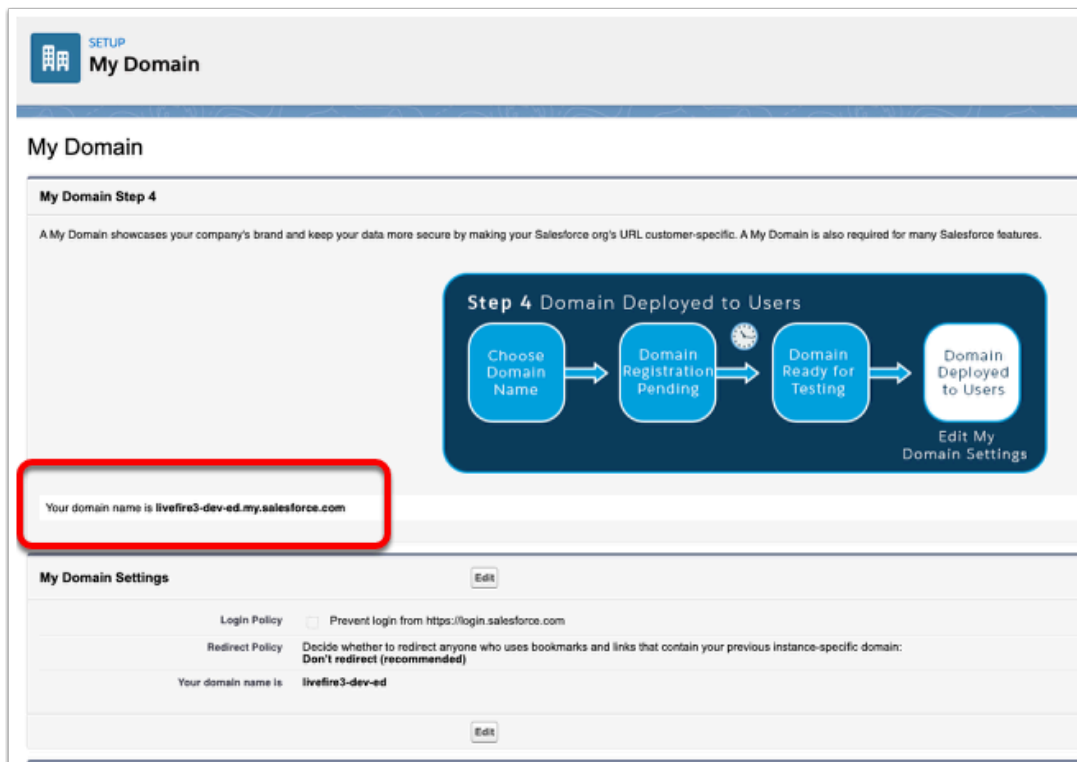




3. You should still be automatically logged in with the user that you have created above, if not navigate to <https://login.salesforce.com> and login with the details for your account.
  - **NOTE:** Salesforce has two Web Interfaces and this can get quite confusing. Please be sure to use the **lightning experience** interface rather than the classic interface. **You will now register a unique domain name for you SFDC dev account.** Click on **Lightning experience**. From the top right, find the settings icon and select **Service Setup** from the dropdown menu.



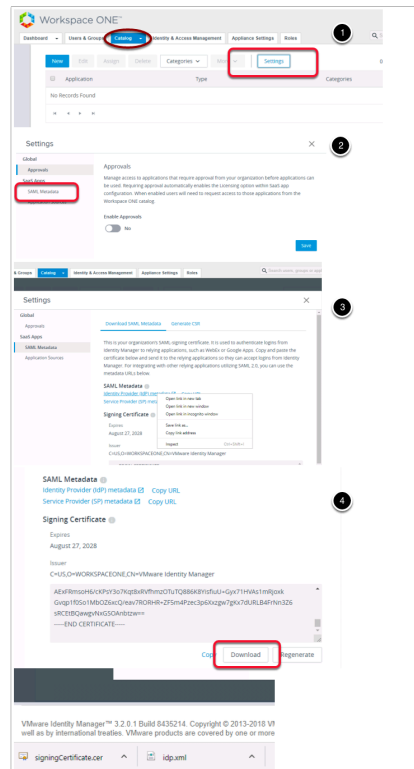
4. On the Left of the Home page **Navigate to** **SETTINGS** > **Company Settings** > **My Domain**



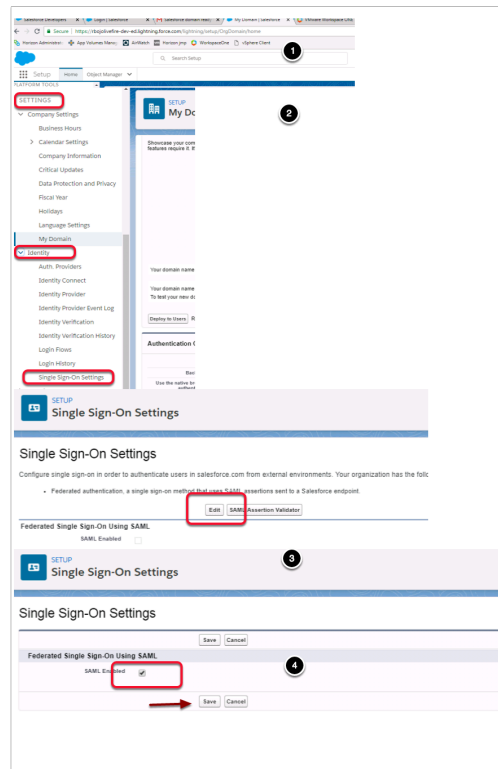
5. In the **My Domain Step 4** area

- Note and document your **custom FQDN**
- eg. <https://livefire3-dev-ed.my.salesforce.com/>

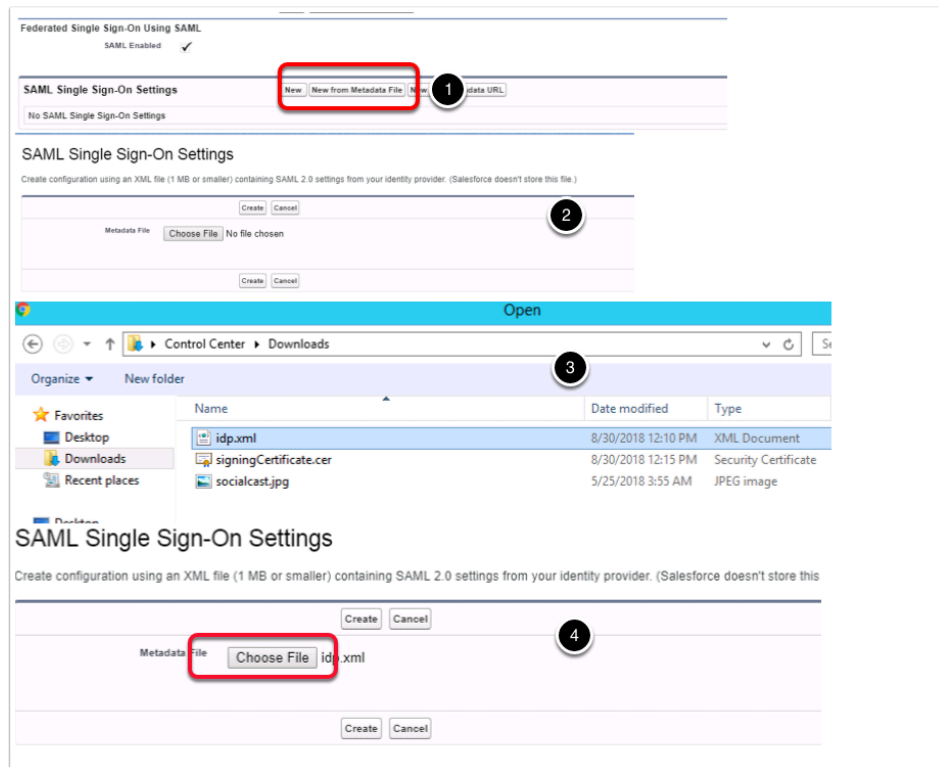
## Part 2. Establishing a SAML Trust



1. Now we will download the identity provider Signing certificate from Workspace ONE Access and upload it into SFDC to create the trust relationship for authentication.
  1. **Login** to your SaaS Workspace ONE Access administrator console as **sysadmin**
  2. Select the **Catalog** tab, in the drop down select **Web Apps**
  3. To the right, select **SETTINGS** select **SAML Metadata**
  4. Right click on **Identity Provider (Idp) metadata** and select **save link as**, this will open your **Save As** window. Leave the **Downloads** folder as default and the name as **idp.xml** and select **Save**
  5. Go to the **Signing Certificate** area and select **Download** , you should now have a **signingCertificate.cer** and a **idp.xml** in the **Downloads** folder



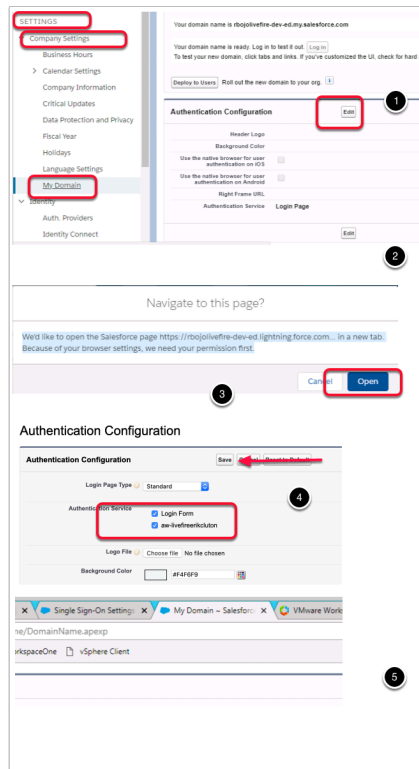
2. **Navigate** back to your SalesForce site where you should now be able to login with your unique registered domain **\*-dev-ed.lightning.force.com**
  - On the home page for the admin user you will find **Settings > Identity > Single Sign-On Settings** **NOTE:** if you can't locate these options on the initials login page select the cog wheel in the top right hand side of the page and select setup and it will take you to the correct configuration page.
  - On the **Single Sign-On Settings** Page next **SAML Assertion Validator** select **Edit**, below **Federated Single Sign-on Using SAML**, select the **SAML Enabled** **checkbox**. Select **Save**.



3. Now select **New From Metadata File** just underneath where the SAML settings have been enabled.
  1. This will take you to the **SAML Single Sign-On Settings** page where it will request the SAML metadata.
  2. Click **Choose File** that you have downloaded into the **Downloads** Folder from Workspace ONE Access named **idp.xml** (created in paragraph 1).
  3. Select the **idp.xml** and select **Open** select **Create**.







5. On the Salesforce admin console

1. Navigate to **Settings > Company Settings > My Domain**
2. In the **Authentication Configuration** section select **edit**, this will open a new tab or navigate you to the edit page depending on the browser you are using. (Ensure that you observe Pop-up Blocker in your browser and select the radio button **to Always allow pop-ups....**)
3. Select **Done**, and then on the **Navigate to this page?** window select **Open**
4. Under **Authentication Configuration** page next to **Authentication Service** select the **check box** that has **"YOUR SaaS Workspace ONE Access"** and select **Save**
  - **NB! Notice that this pop-up window opened up in a new window on a new TAB.**

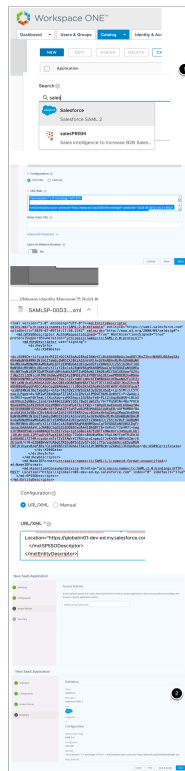
**Revert back by selecting the original window Single Sign-On Settings tab to the left of your current window**

## 6. Creating a unique user for your Salesforce environment.

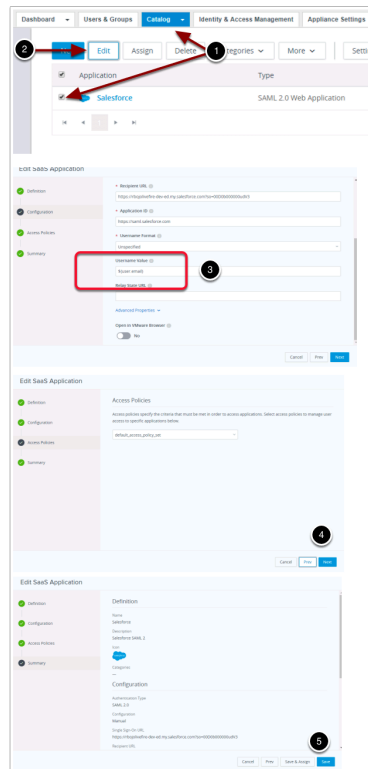
NB! This has to be an Identical account to what you created at the beginning of the course

1. Navigate to **Administration > Users > Users** > click Select **New User**
2. Fill in the unique user details,
  - **First Name:**User xx {your student number + {the first letter of your city and country abbreviation}} eg User35AUK
  - **Last Name:**{the first letter of your city and country abbreviation
  - **Alias:**{same as your username}
  - **Email:**{FirstName@euc-livfire.com (For Example: user35BUK@euc-livfire.com)}
  - **Username:**{FirstName@euc-livfire.com (For Example: user35BUK@euc-livfire.com)}
  - **Nickname:** {same as your FirstName}. In some cases the field is only 8 characters long and you first name should be 9 characters long, dont pay attention to this as if does not break the lab.
  - **Role:** <None Specified >
  - **User License:** Force.com - Free
  - **Profile:**Force.com - Free User
3. Click **Save**

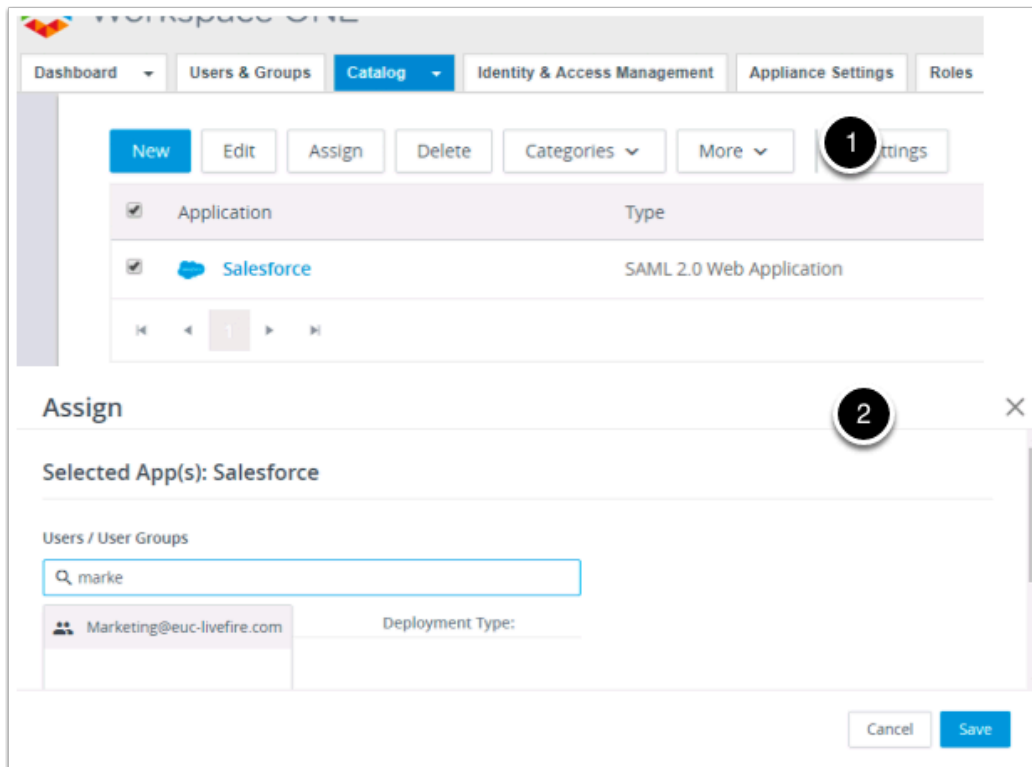
This will be the user we will use to test the authentication



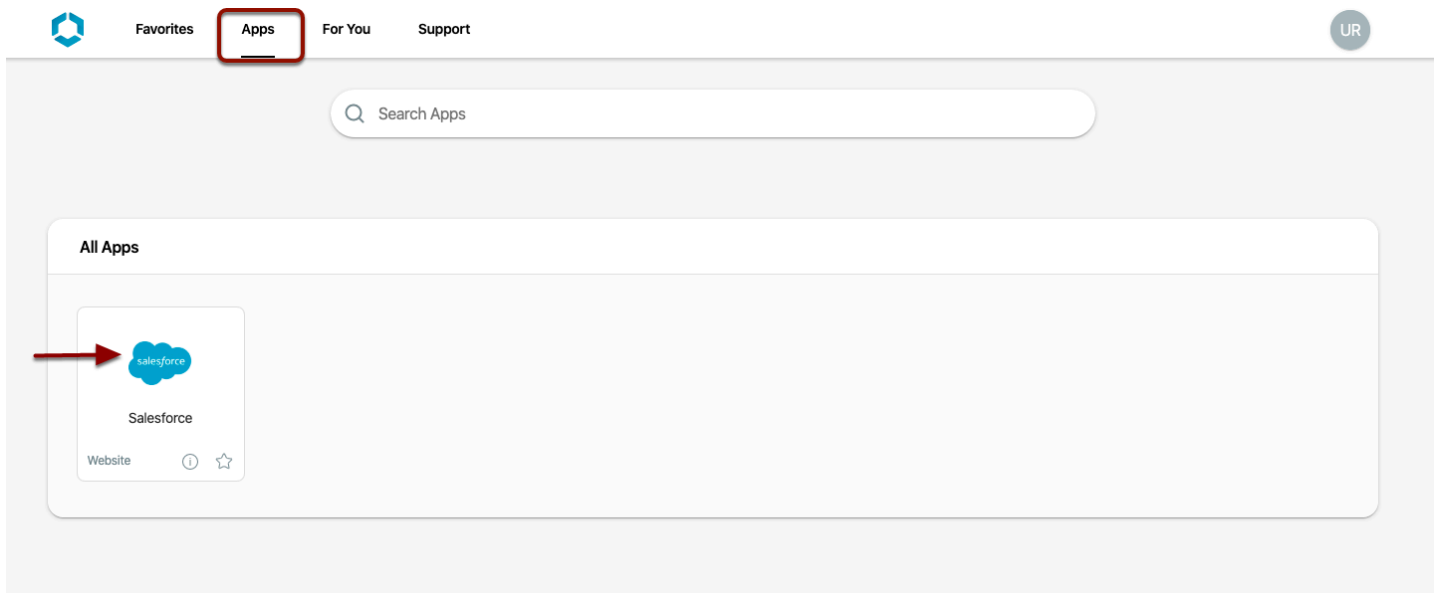
7. Navigate back to your **Workspace ONE Access console**
  1. Select the **Catalog** tab, select **New**
  2. On the **New SaaS Application** window, in the search type **sales** and select **Salesforce**, select **Next**,
  3. Under **Configuration**, under the **Single Sign-On** section, select the **URL/XML** radio button.
  4. On your **Controlcenter2** server Open **file Explorer** window and browse to **Downloads**. Right click and open the **metadata** file you downloaded from **Sales force** that was called **SAMLSP....xml**
  5. Open in **Notepad**. In the Notepad select all or press **CTRL + A** and copy with **CTRL + C**. Now **paste** the **Metadata** in the XML field in **Single Sign-On** page under **URL/XML**.
  6. On the **Single Sign-On** page select **Next**, on the **default Access policies** page accept the default select **Next** and select **Save**

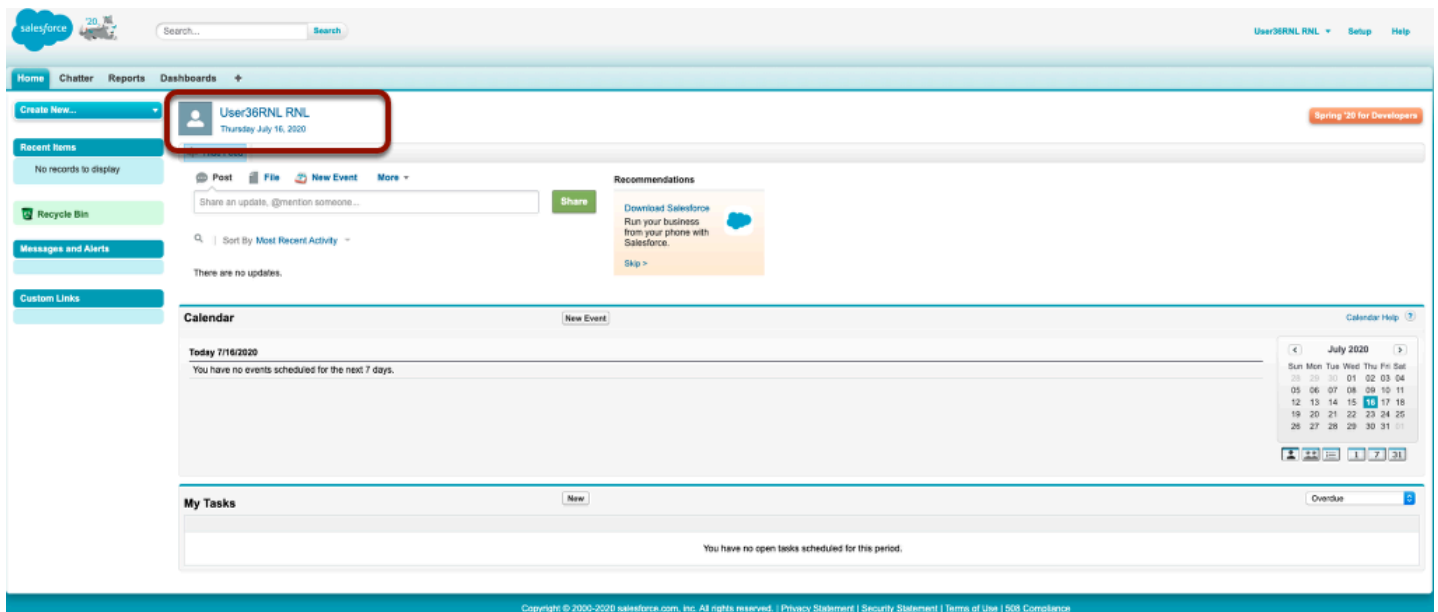


8. On the **Catalog** tab, select **Salesforce** select **Edit**,
  1. Select **Configuration**, to the right of configuration, **scroll down** to **Username Value** and change **\${user.username}** to **\${user.email}**.
  2. Select **Next**, on the **Access Policies** page, select **Next**, on the **definition** page, select **Save**.



9. In the **Catalog** area next to Salesforce, select the **check box** and then select **Assign**
- In the **Assign** window under **Users / User Groups** box type **marke** and select **Marketing@euc-livefire.com**.
  - Under **Deployment Type**, change to **Automatic** from User-Activated and select **SAVE**





## 10. Testing your custom account with the Salesforce Federation

- Open up an Incognito window an alternate browser and navigate to your Workspace ONE access URL.
- On **Select your Domain** screen, click on the dropdown and select **euc-livewire.com**.
- Login to your SaaS instance of Workspace ONE Access with your custom user account i.e. UserXXRNL
  - In the Workspace ONE Catalog, from the top menu option, navigate to APPS.
  - Click to **open** your Salesforce Application

If the federation was setup correctly, your custom user UserXXRNL is logged in successfully.

# Android emulator setup (Optional)

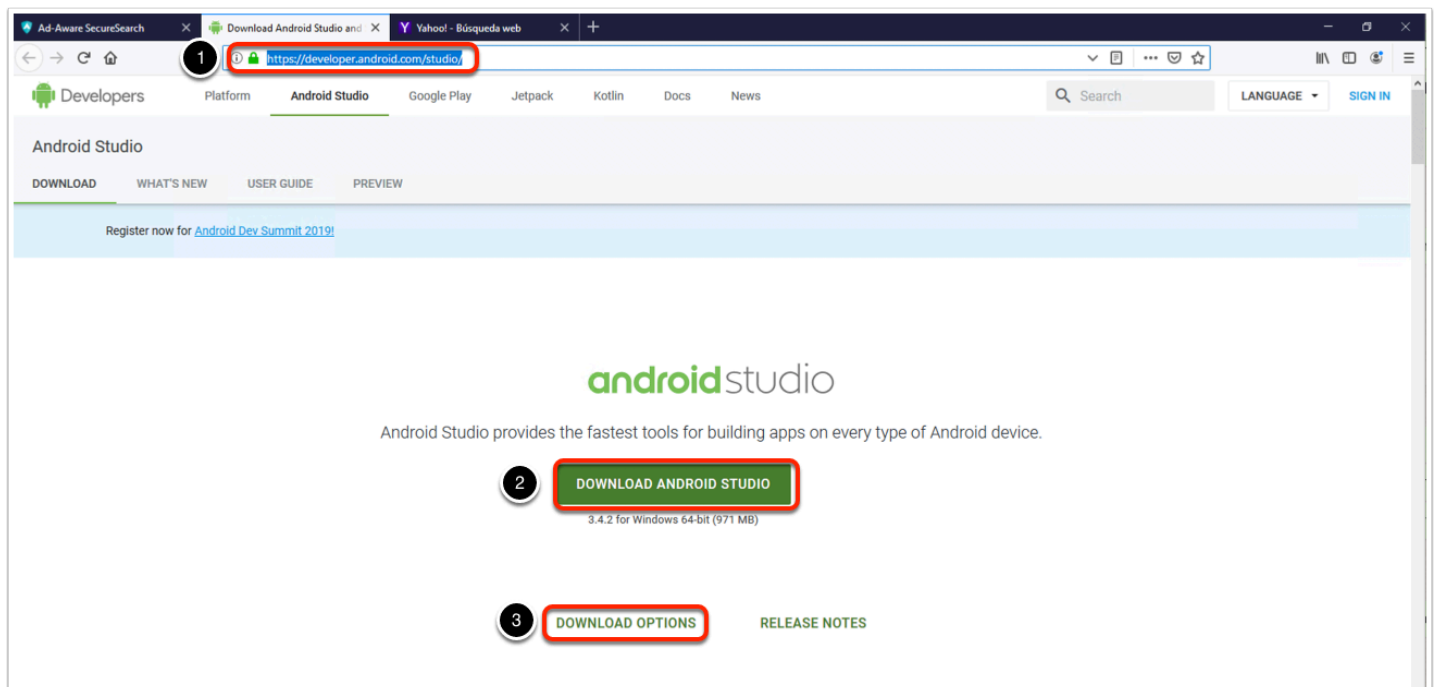
## Introduction

If you don't have an android test device and you want to test the Device enrollment, android single sign on, and other android based labs, theres an emulator you can install in your laptop an follow along with the particular lab manual as you would do on a physical device. What follows is the installation instructions for the installation of such software.

If something goes wrong and you want to start again with a fresh device, instructions are included for redeploying the os image.

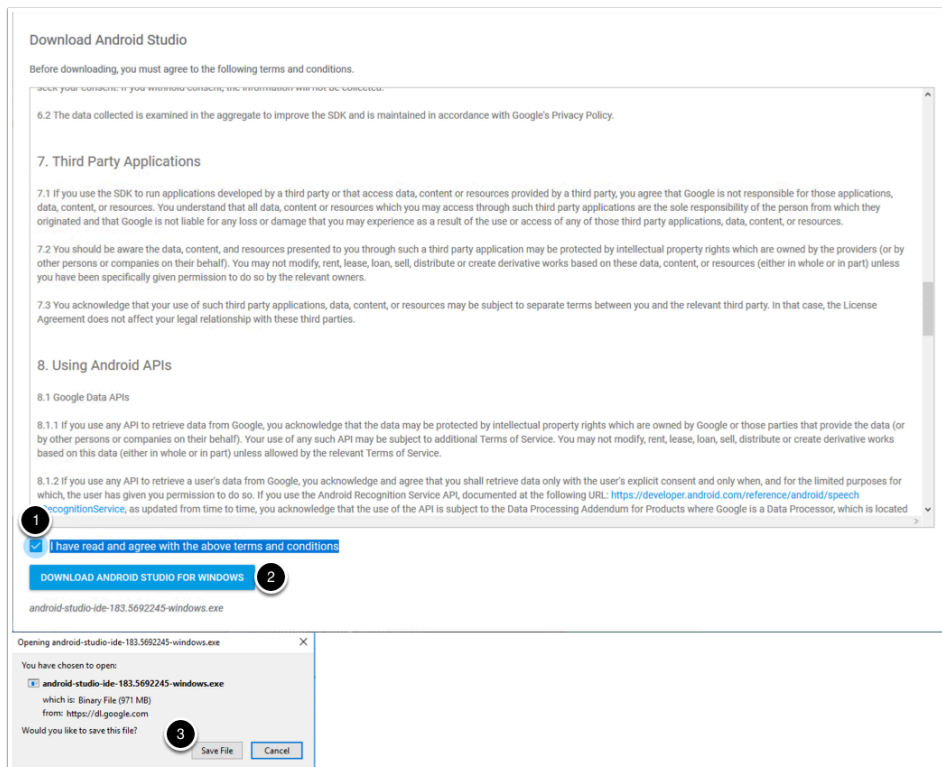
💡 Note: Screenshot precedes the steps in this lab.

## Part 1: Downloading the installer



1. On your laptop, Go to <https://developer.android.com/studio/>
  - Find and click on **Download Android Studio**
  - If the correct os version is not displaying click on **download options** and download the correct one

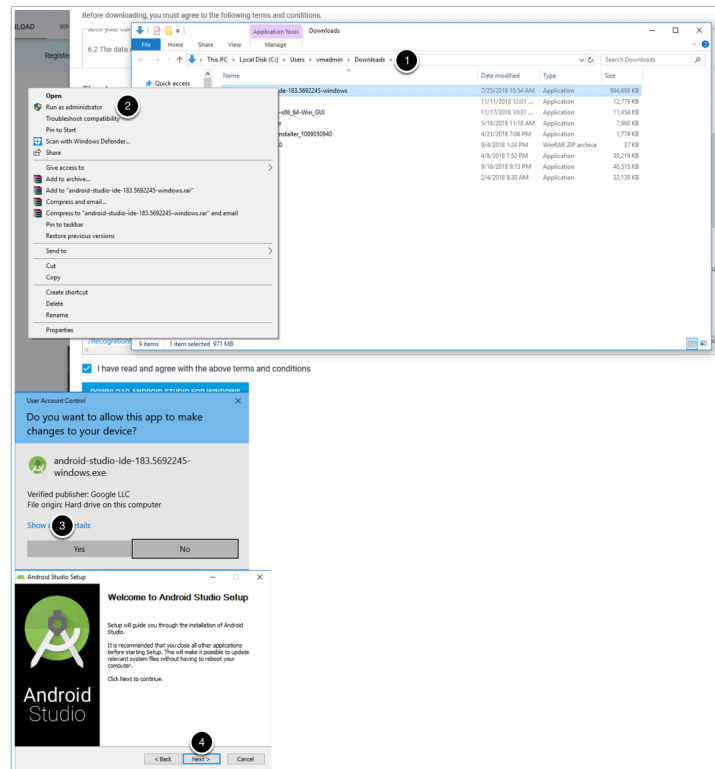
NOTE: Installation of Android Studio should be done on your ControlCenter server.



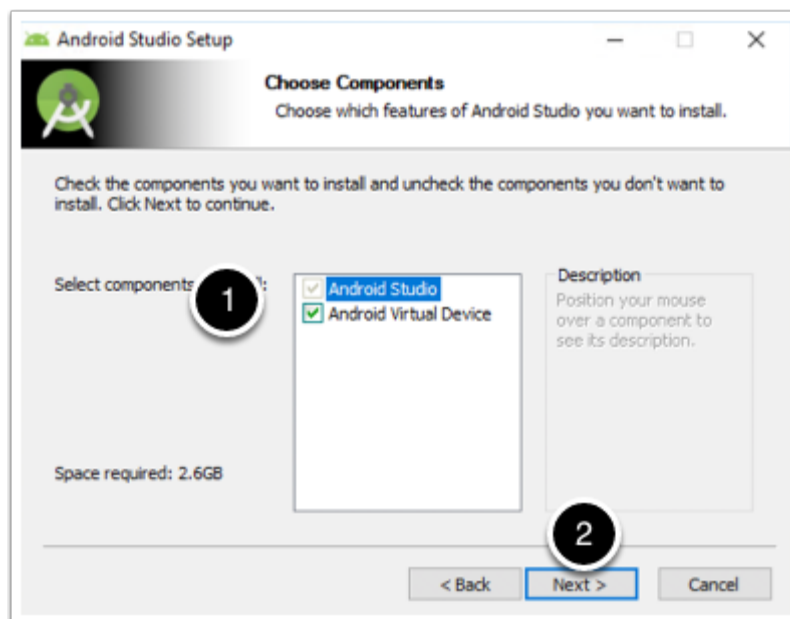
2. Check the box next to **I have read and agree with the above terms and conditions**
  - Click on **Download android Studio for your platform**
  - Click on **save file** when prompted



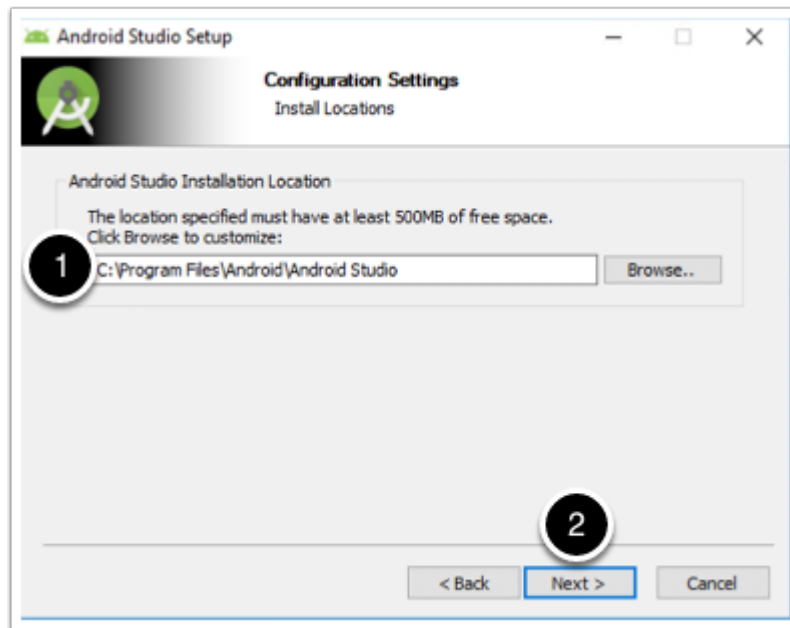
## Part 2 : Windows installation



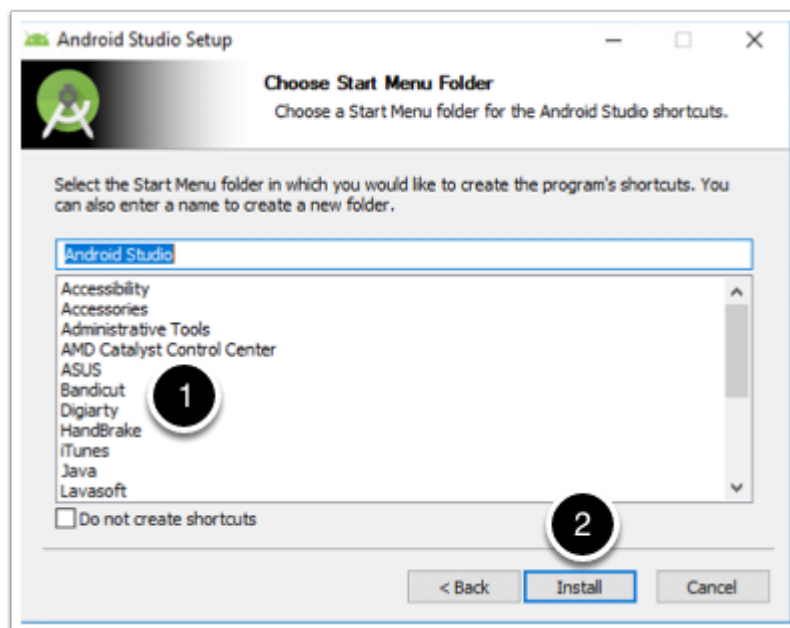
1. Go to your **downloads** folder
  - Right click on your recently downloaded file and click on **run as and administrator**
  - Click on **yes** to allow the installer to make changes to your machine
  - Click next on the welcome to android studio setup window



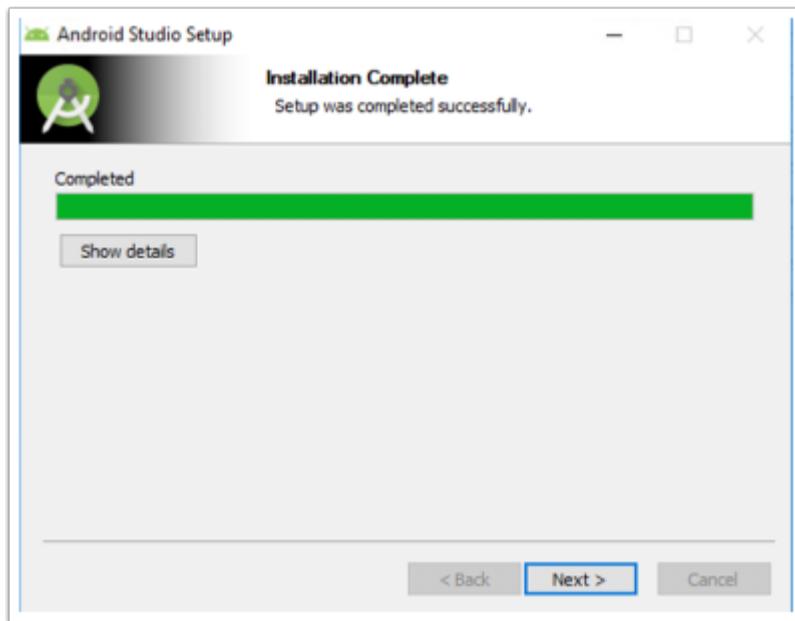
2. Make sure both **Android studio** and **android virtual device** are selected and click **next**



3. Select your installation location and click **Next**



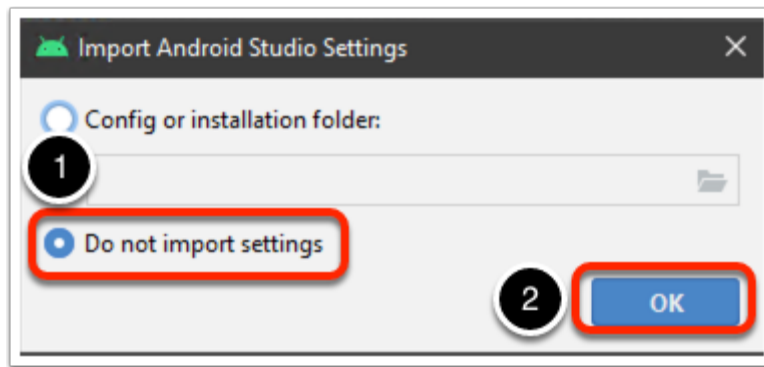
4. Choose your start menu shortcut configuration and click **Install**



5. On the installation complete window click **Next**

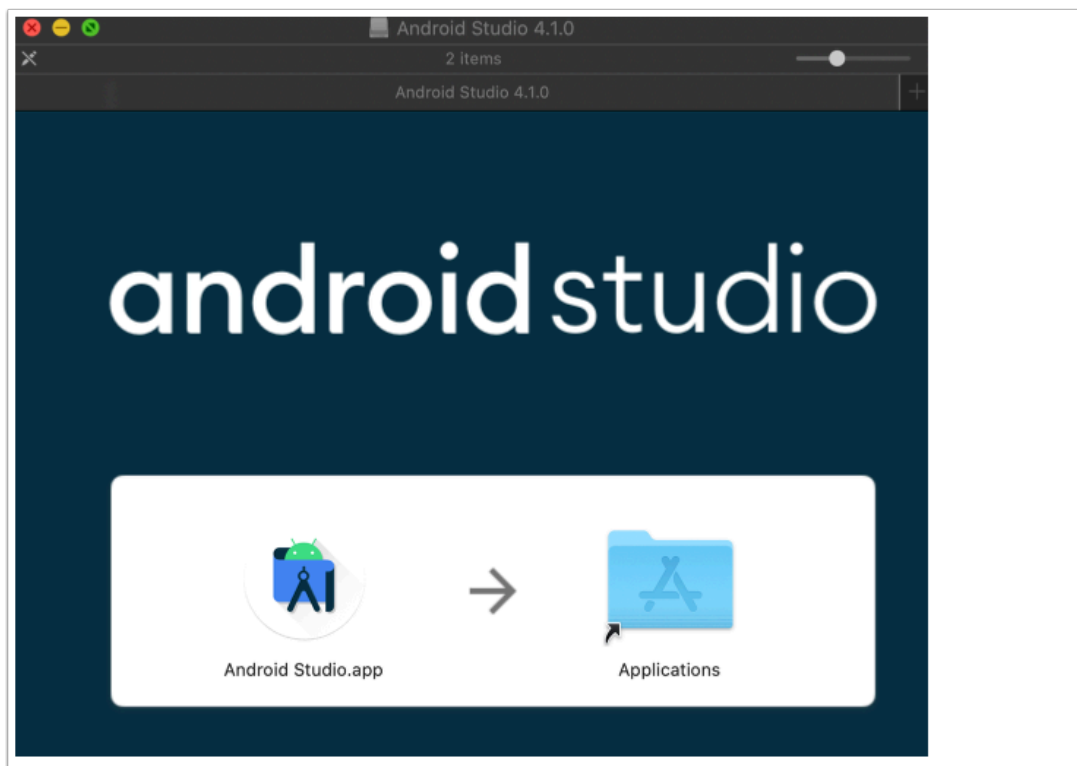


6. In the completing Android Studio Setup window check the **Start Android Studio** checkbox and click **finish**

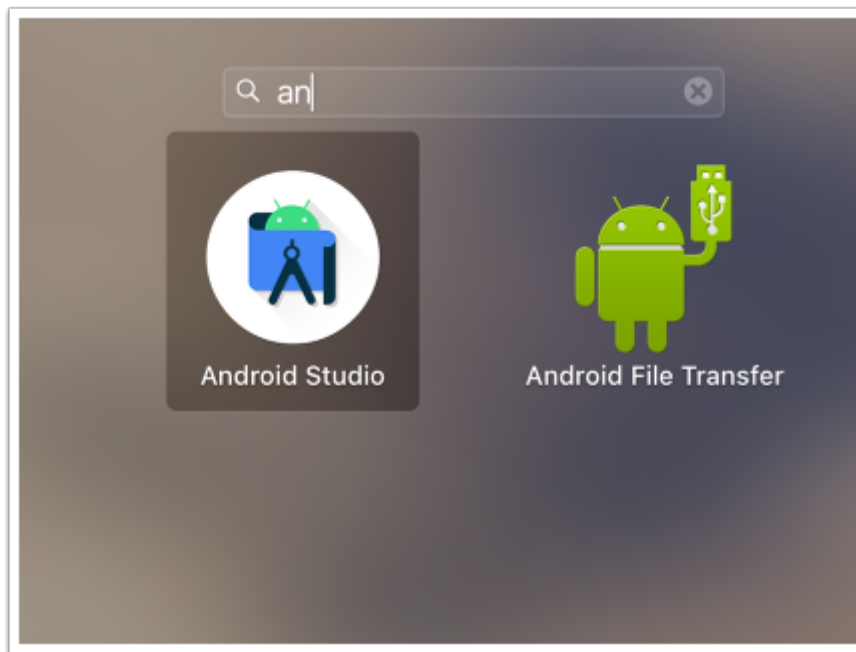


7. In the **Import Android Studio Settings** prompt Select **Do not import settings** radio button and click **OK**

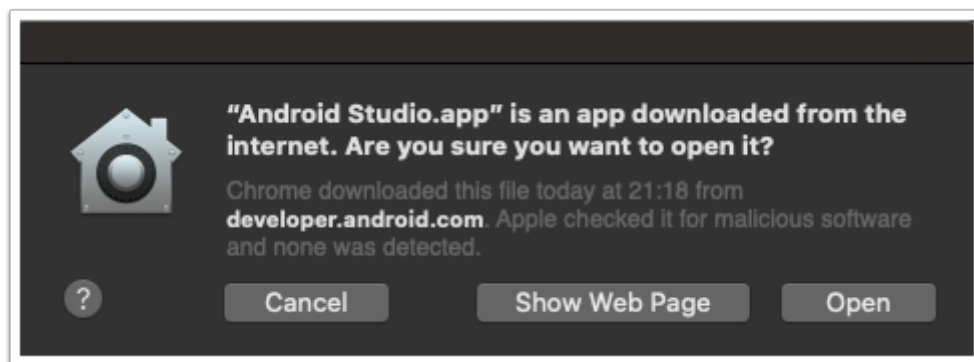
## Part 3 Mac OS installation



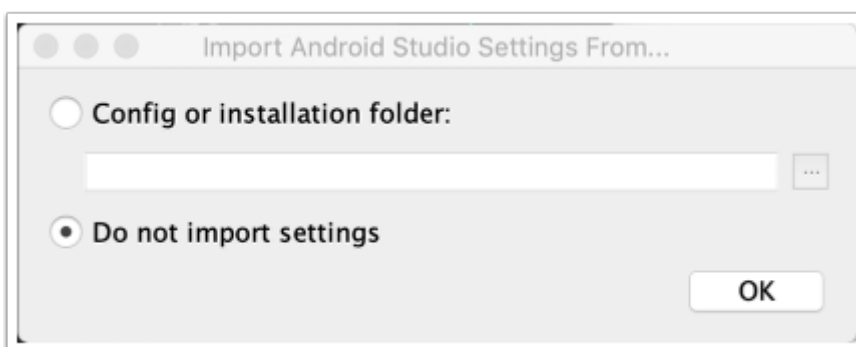
1. Mount and open your downloaded dmg image. Drag the **Android studio** icon into the **Applications** folder.



2. From your applications folder double click your **Android Studio** icon



3. Click on **Open** if you get a security prompt



4. In the Import android Studio settings From.. window select **Do not import settings** and click **ok**

5. On the Android Setup Wizard, in the Welcome window click **Next**. From this point on you can follow the initial configuration steps, please ignore anything regarding the HAXM plugin as this has been already installed for you in the initial installation process.

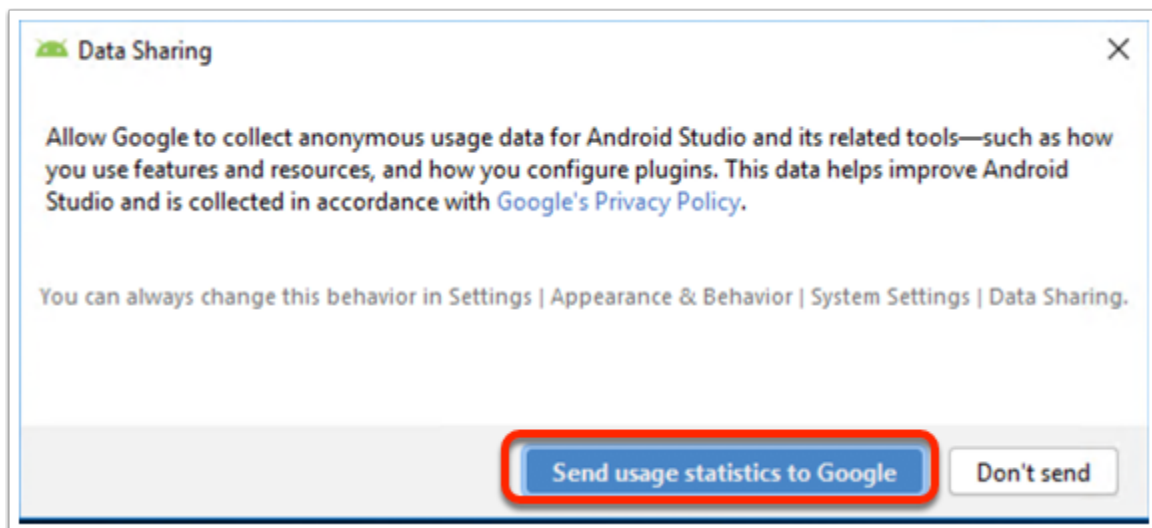
## Part 4: Initial configuration

In this part we are setting up a project and a virtual device with the following settings:

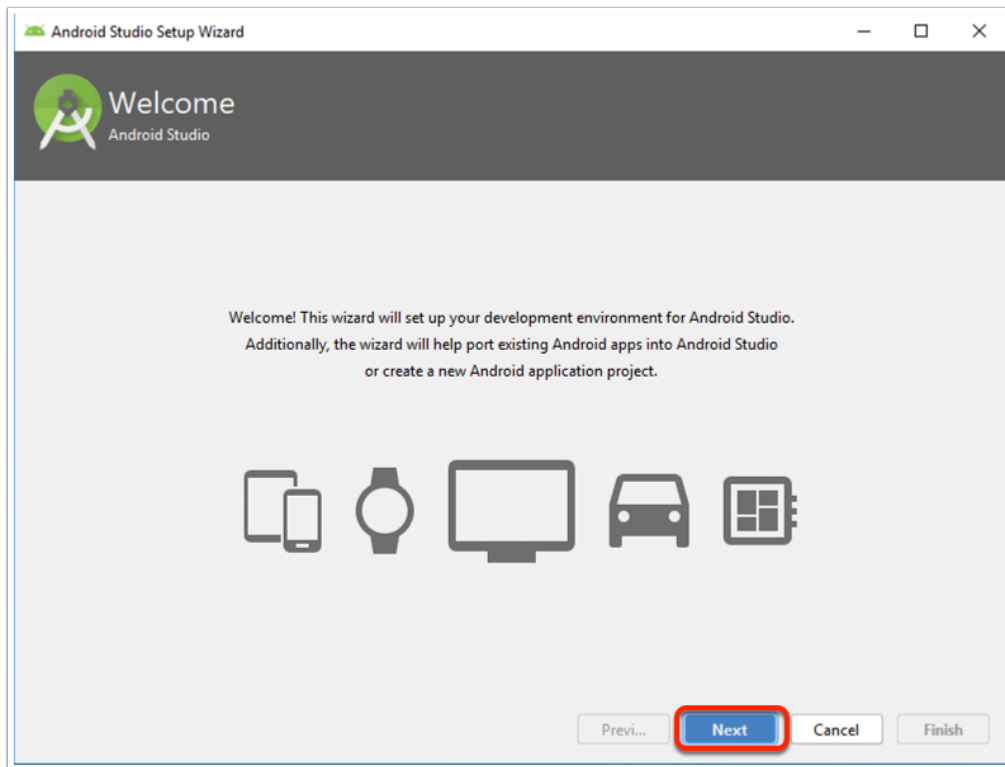
- **API Level:** 29
- **ABI:** x86\_64
- **Target:** Android 10.0 (Google Play)

api level 29 is the project compatible with android 10 onwards.

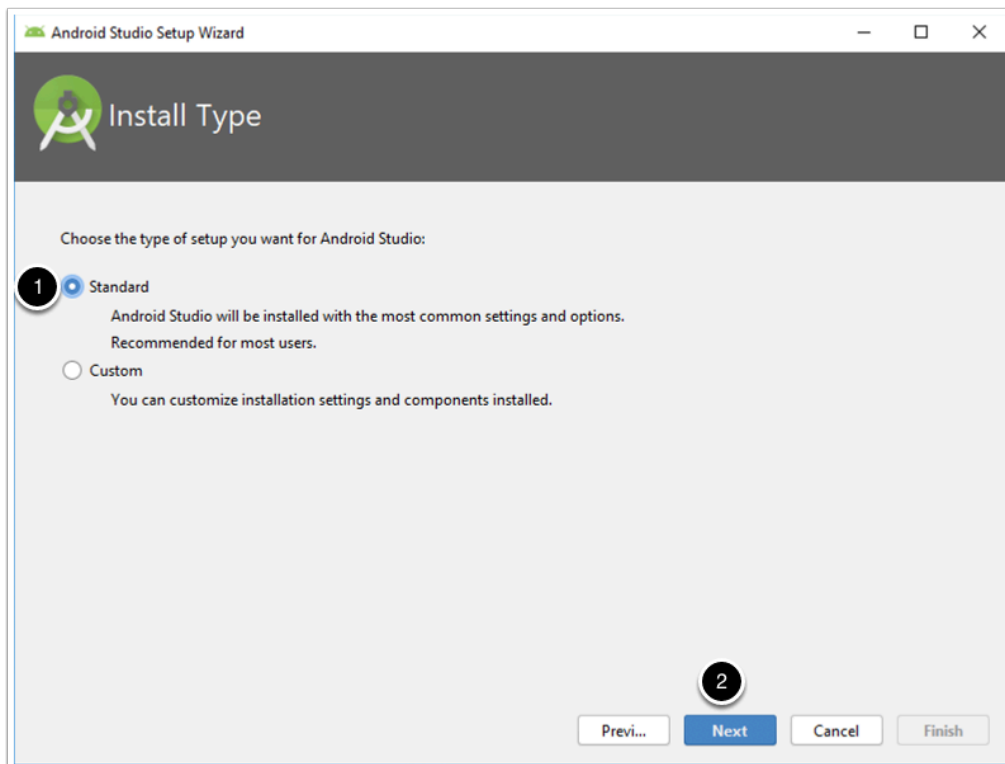
The abi is a image classification for processor command type, in this case for native x86 64 bit, so the commands can be executed in your pc or mac without translation. this is not mandatory but it's important for app compatibility, as these settings are visible to developers and they can choose which image types to make their apps available to. this is the case with the salesforce app that gets used in some of our labs.



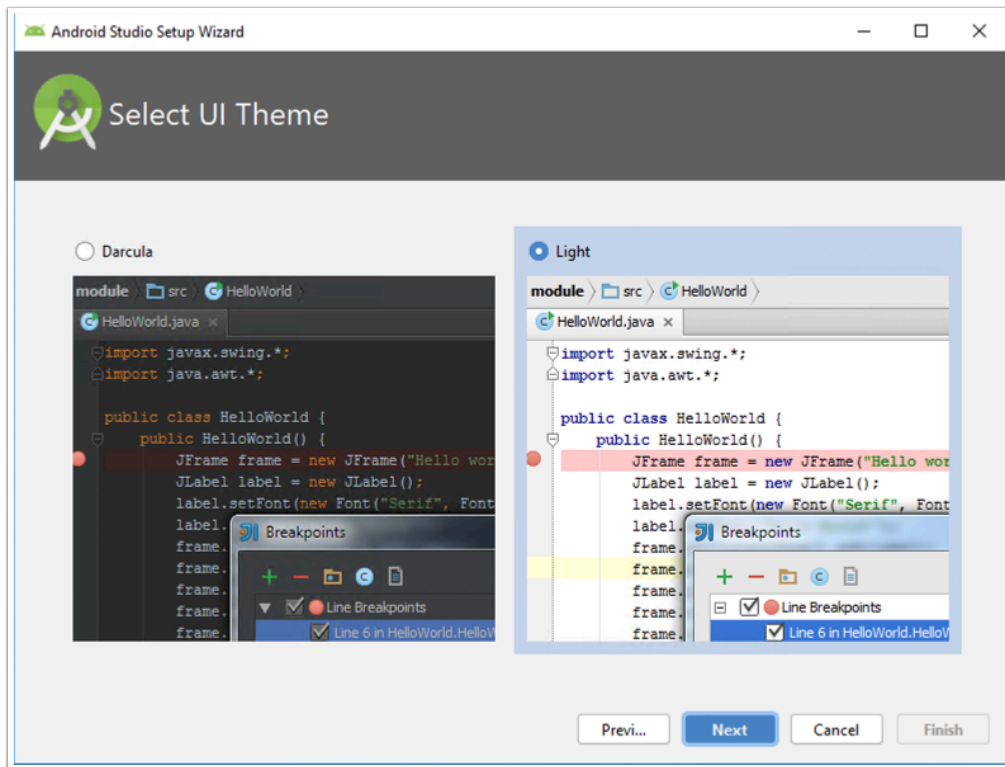
1. If prompted, in the Data Sharing window click on **Send usage statistics to Google**



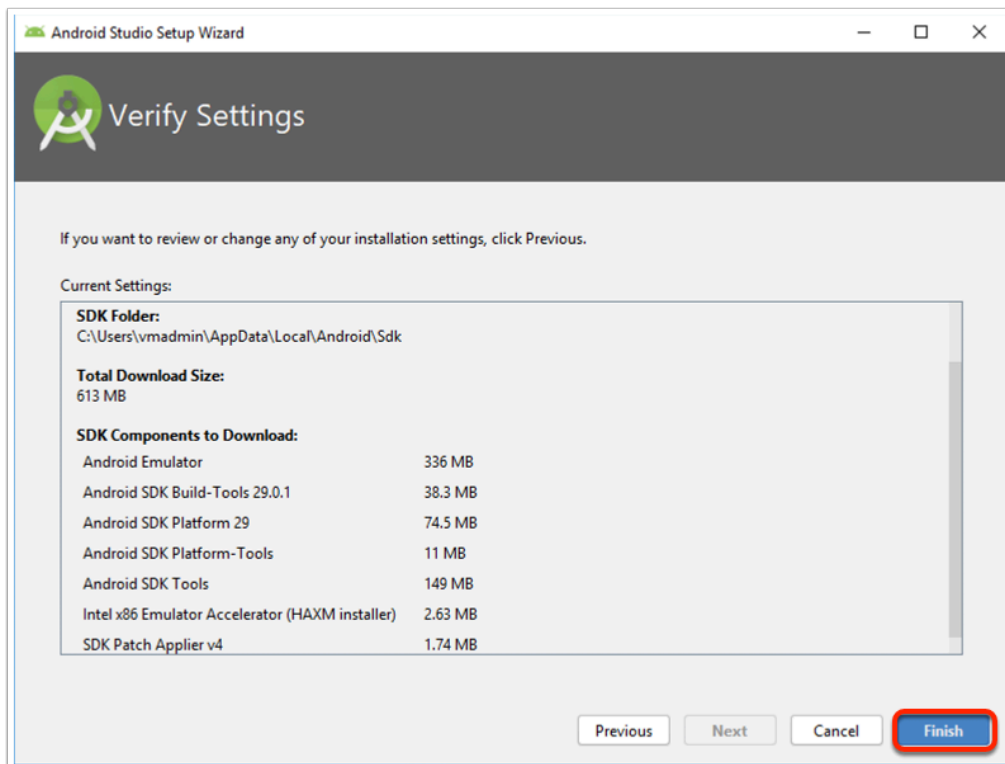
2. In the **Android Studio Setup Wizard**, in the **Welcome** window click **Next**



3. In the Android Studio Setup Wizard in the install type window
  - Make sure **Standard** setup radio button is selected
  - Click **Next**

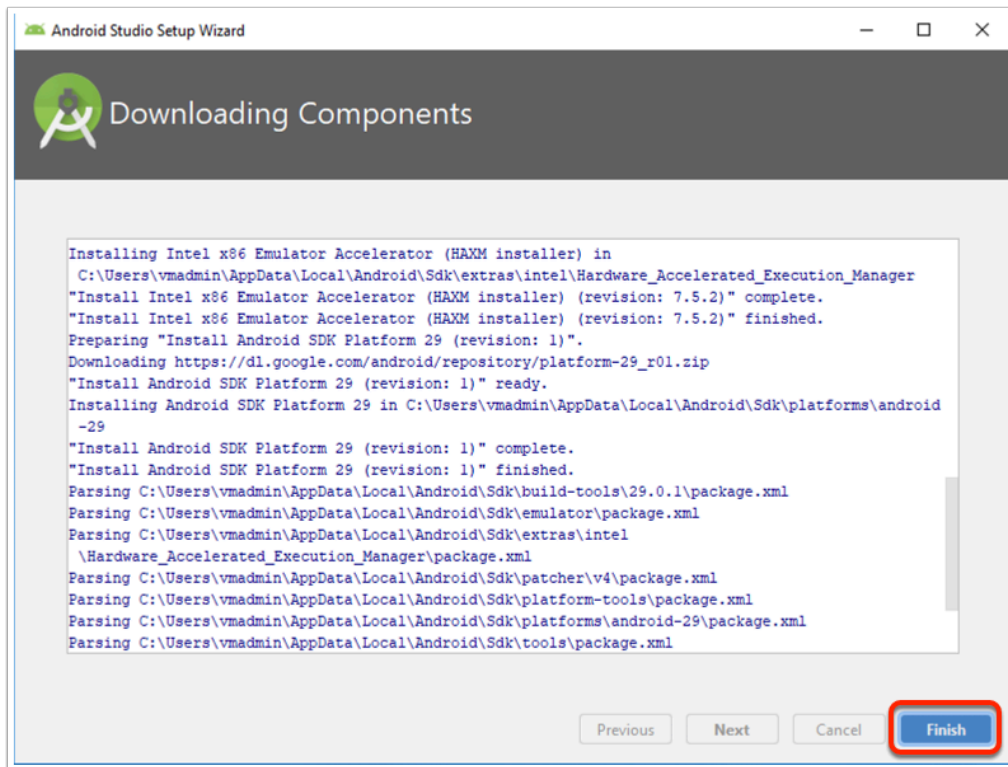


4. Choose your preferred UI theme and click **Next**

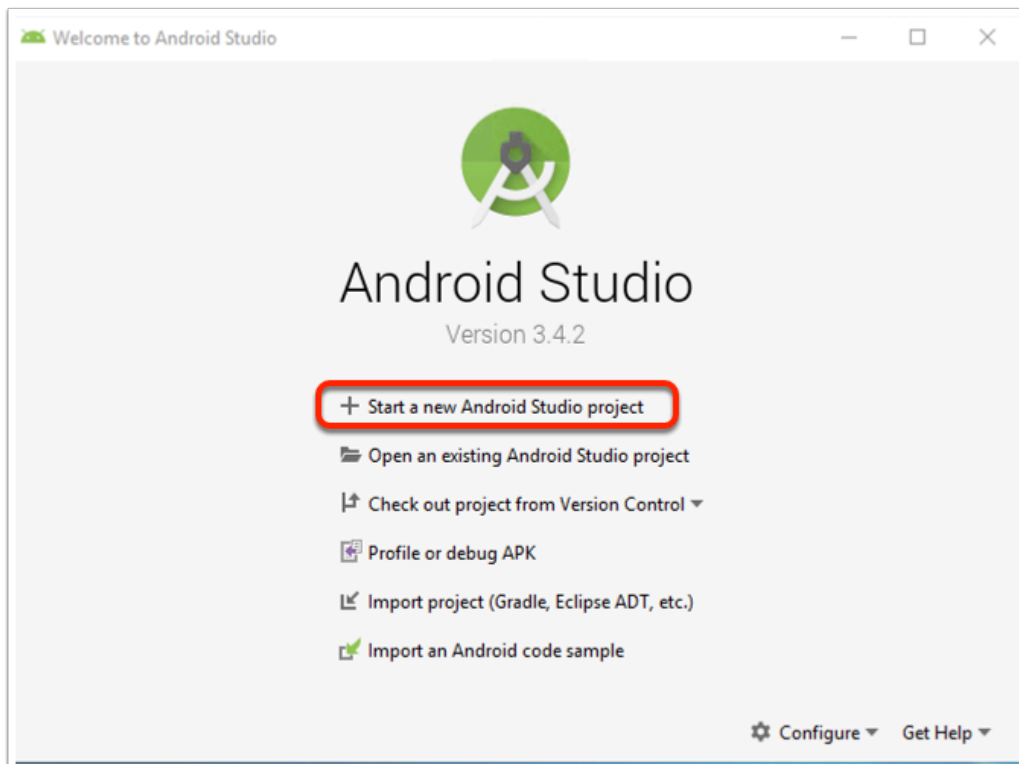


5. On the **Verify Settings** window click **Finish**

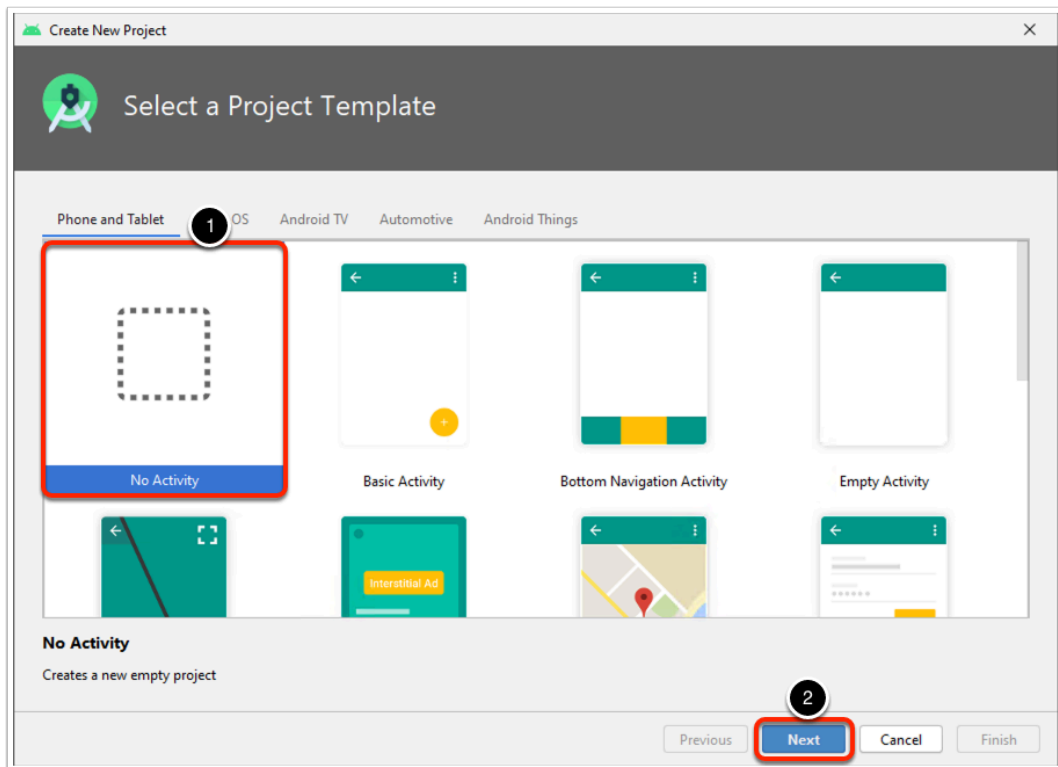




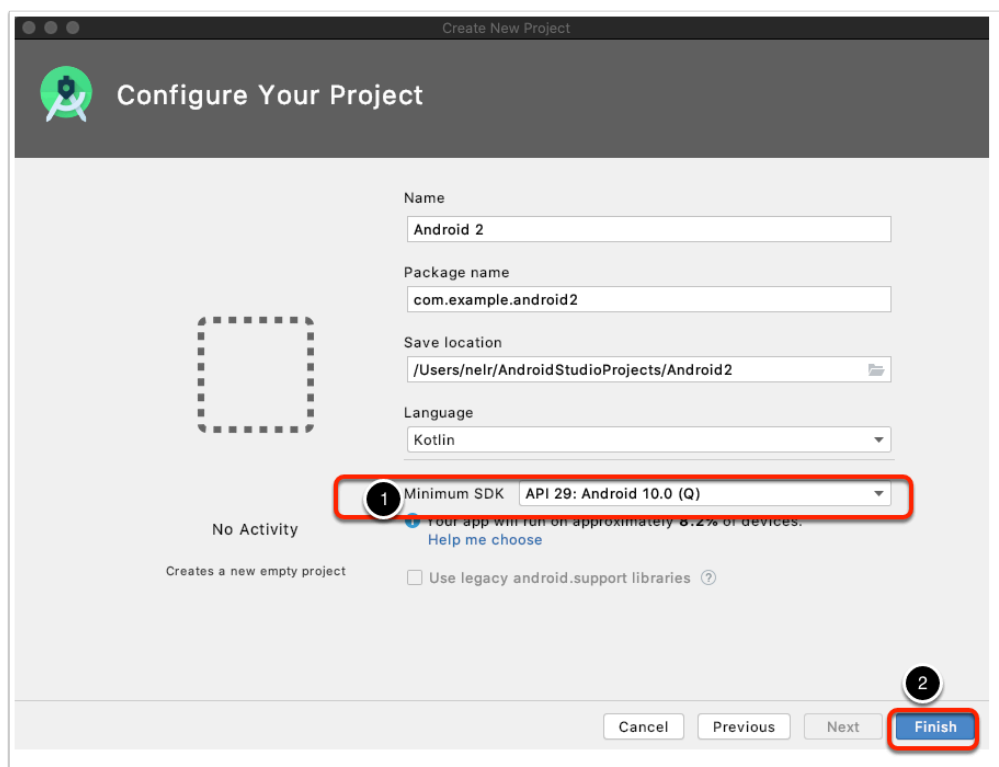
6. In the **Downloading Components** window, when finished click **Finish**



7. In the Welcome to **Android Studio** window click on **Start a new Android project**



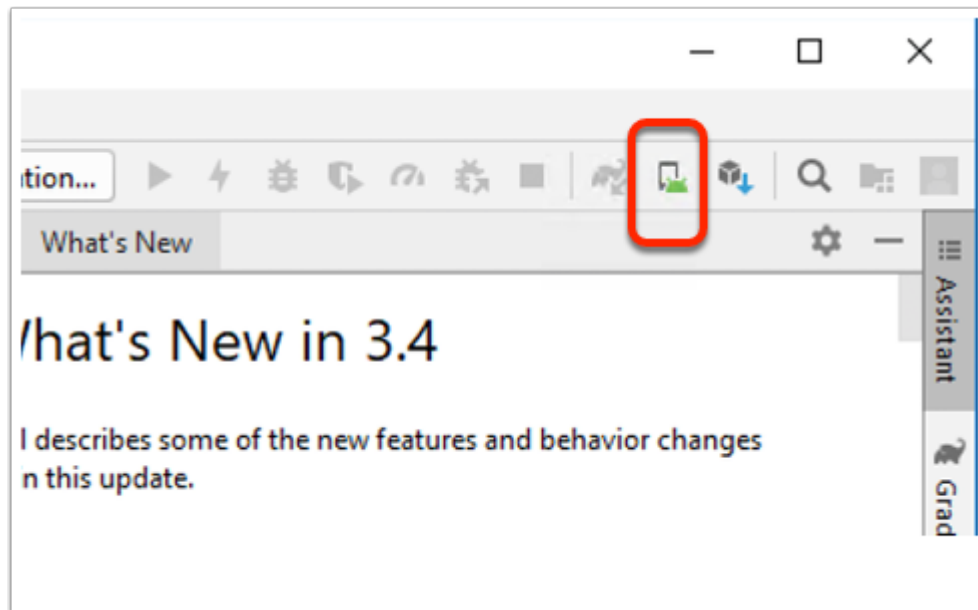
8. In the **Choose your project** window, choose **Add No Activity** and click **Next**



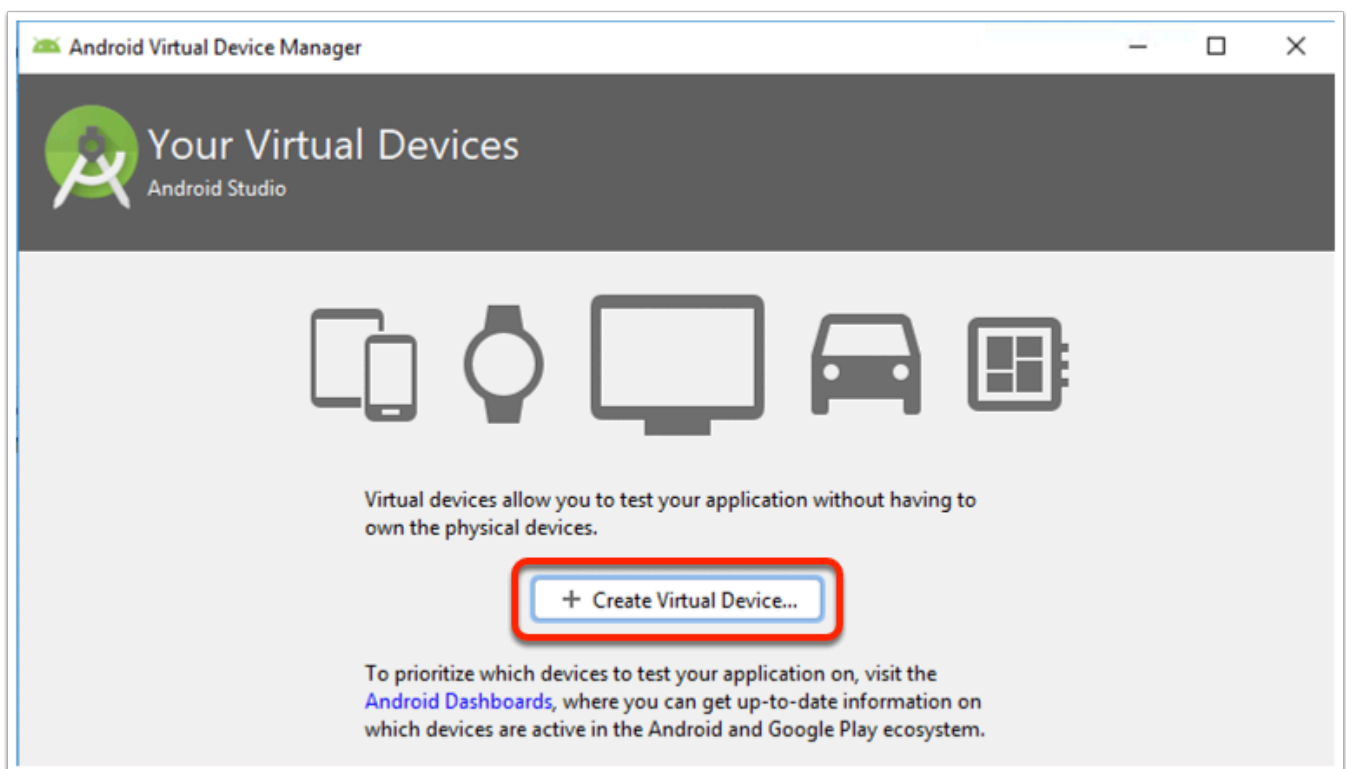
9. In the **Configure your project** window:

- in the **Name** field put something significant i.e. **"Livefire"**
- In the **Minimum SDK** dropdown menu, select API 29: Android 10.0 (Q)

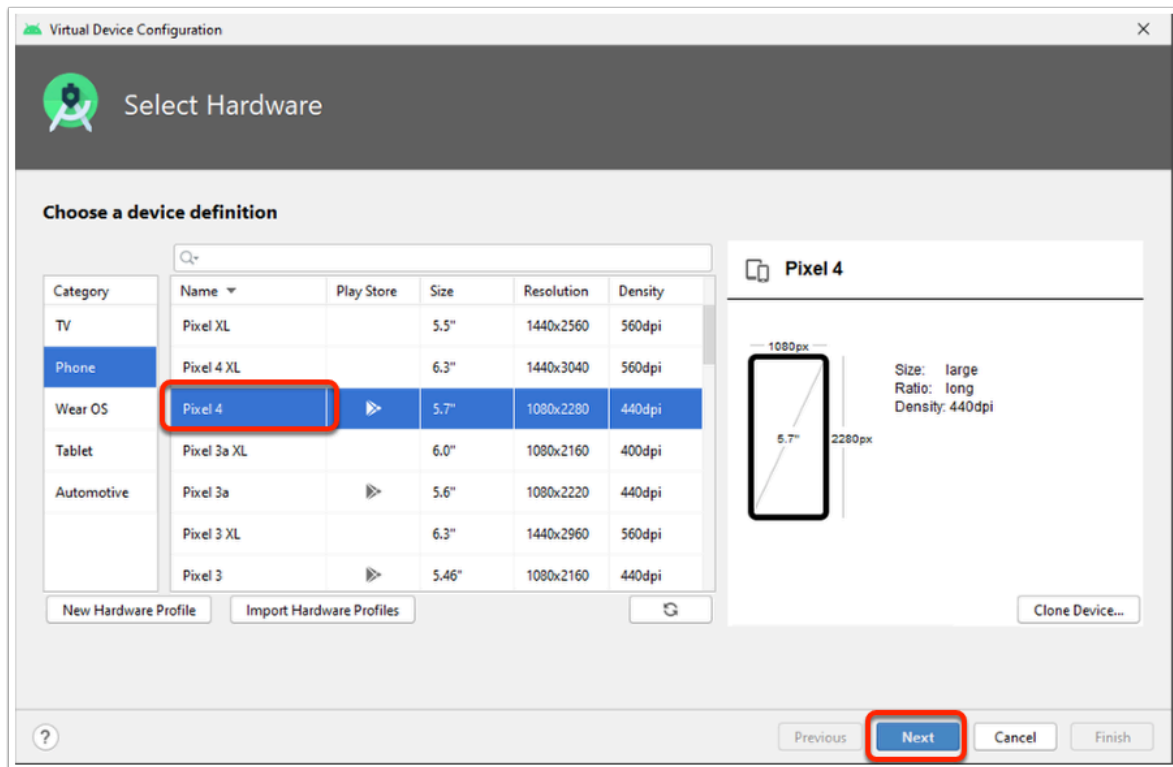
- Click **Finish**



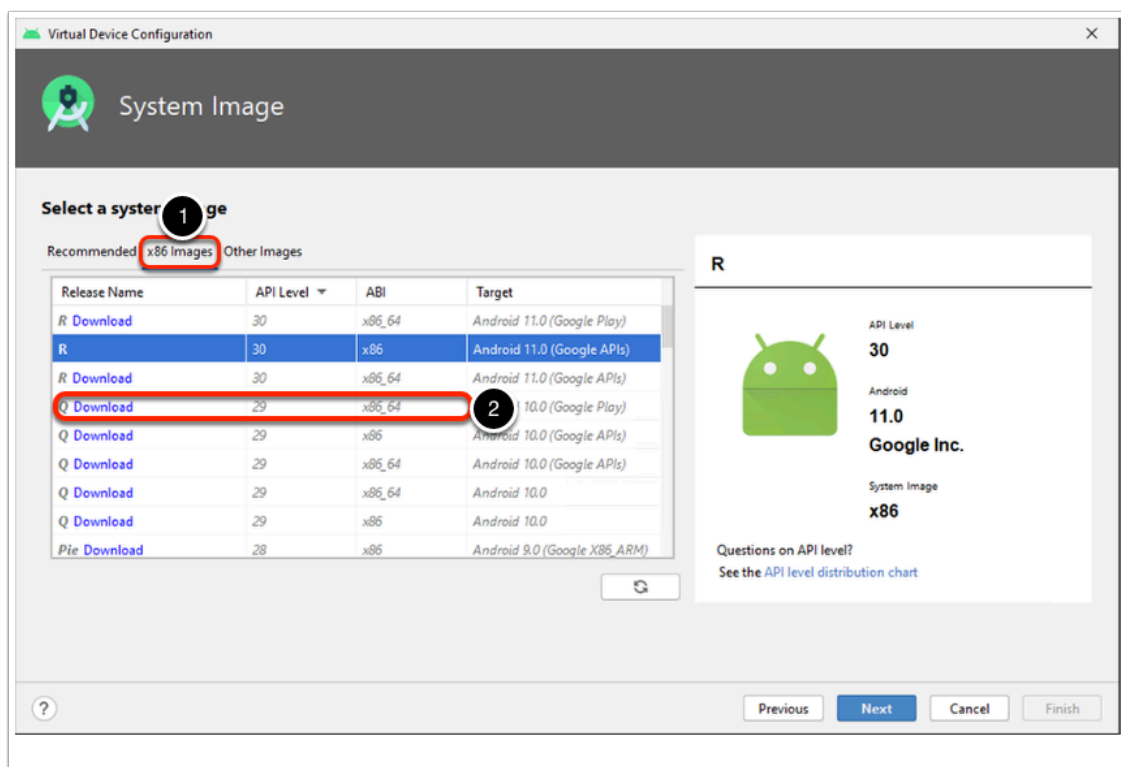
10. Click on the AVD Manager icon on the toolbar



11. Click on **Create Virtual Device**



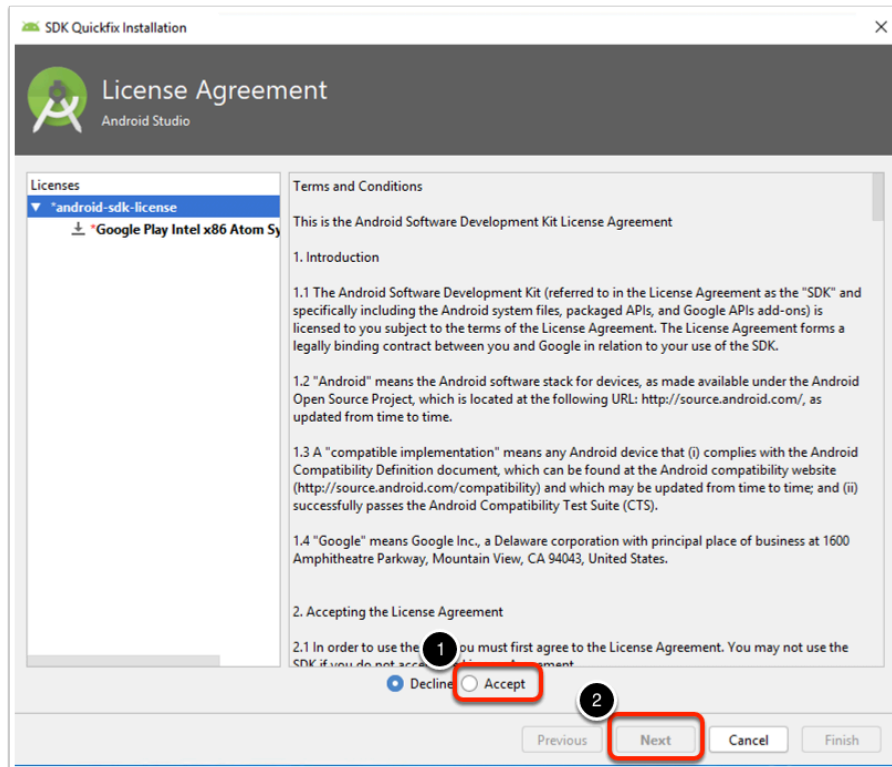
12. Select the **Pixel 4** Image marked with Play Store access and click **Next**



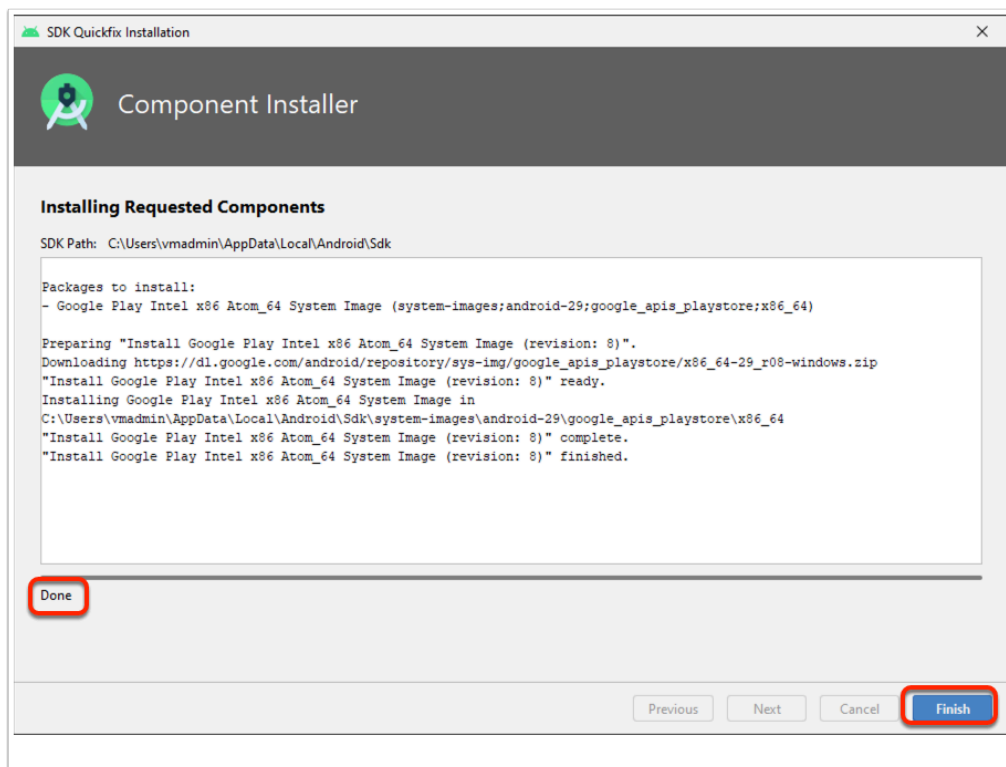
13. In the System image window:

- Select the **x86 Images** tab

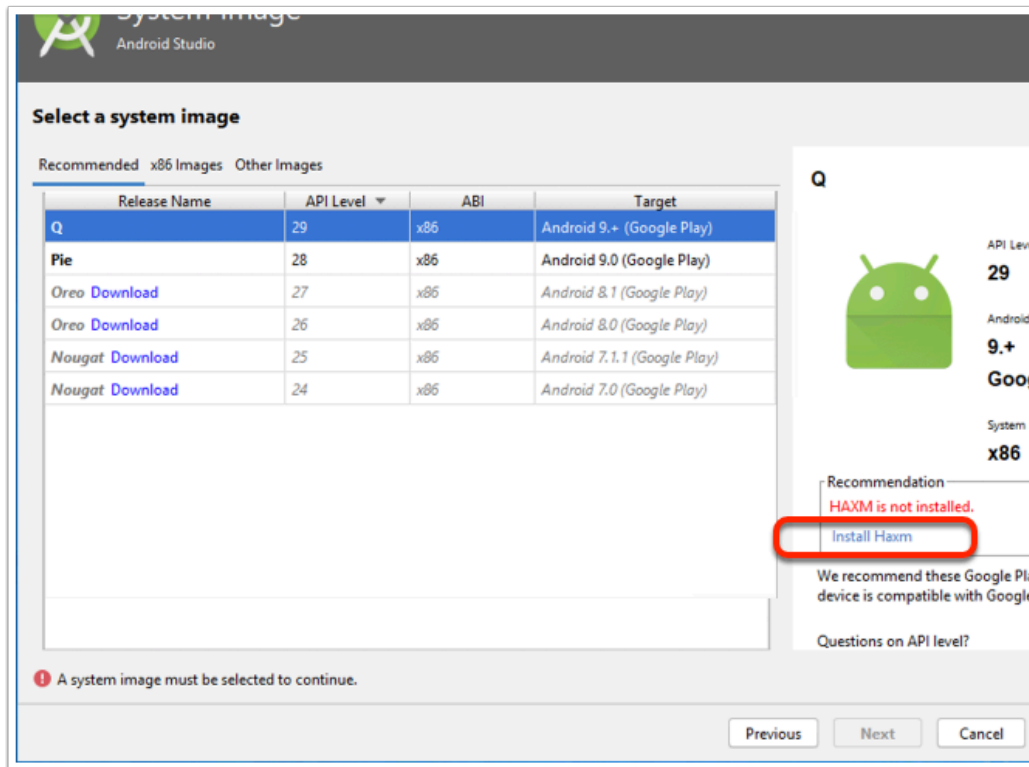
- select the **x86\_64** version of the **Q** image. If you havent used this image before you need click on **Download** first



14. If you clicked on download, in the **License Agreement** window select the radio button next to **I agree** and click **Next**



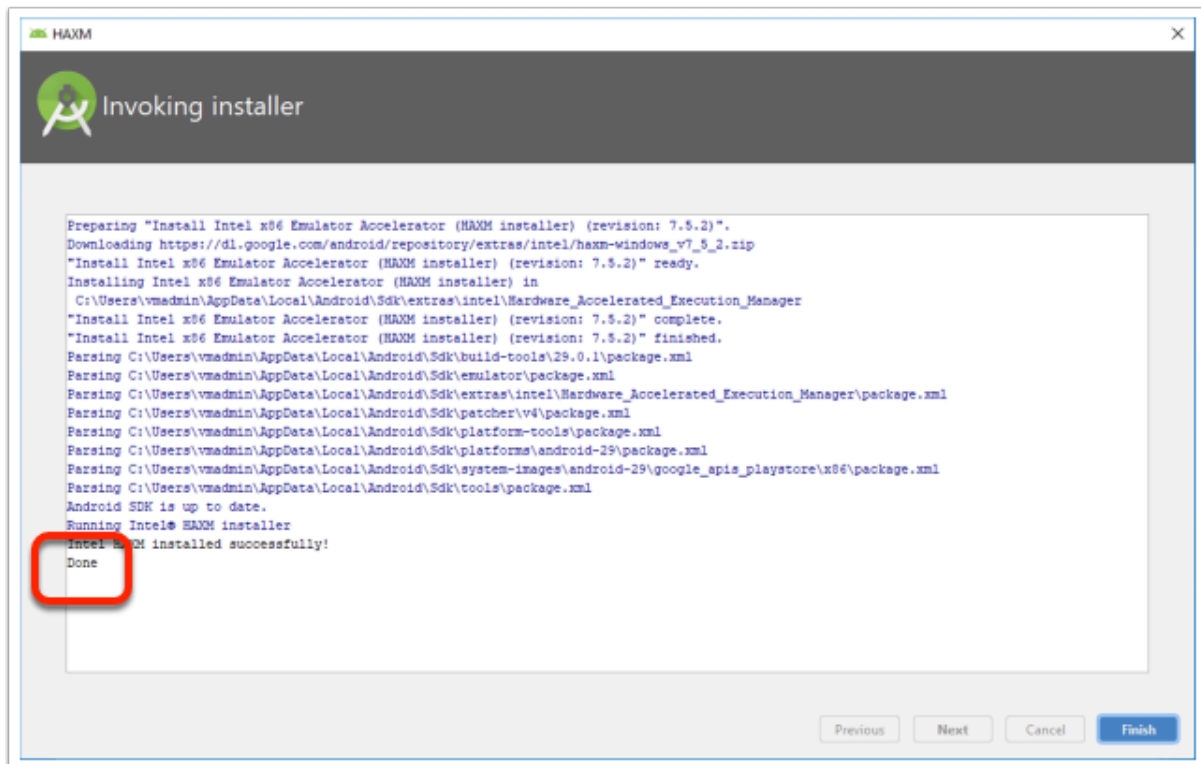
15. In the **Installing Requested Components** window Click **Finish** when the progress bar shows **DONE**



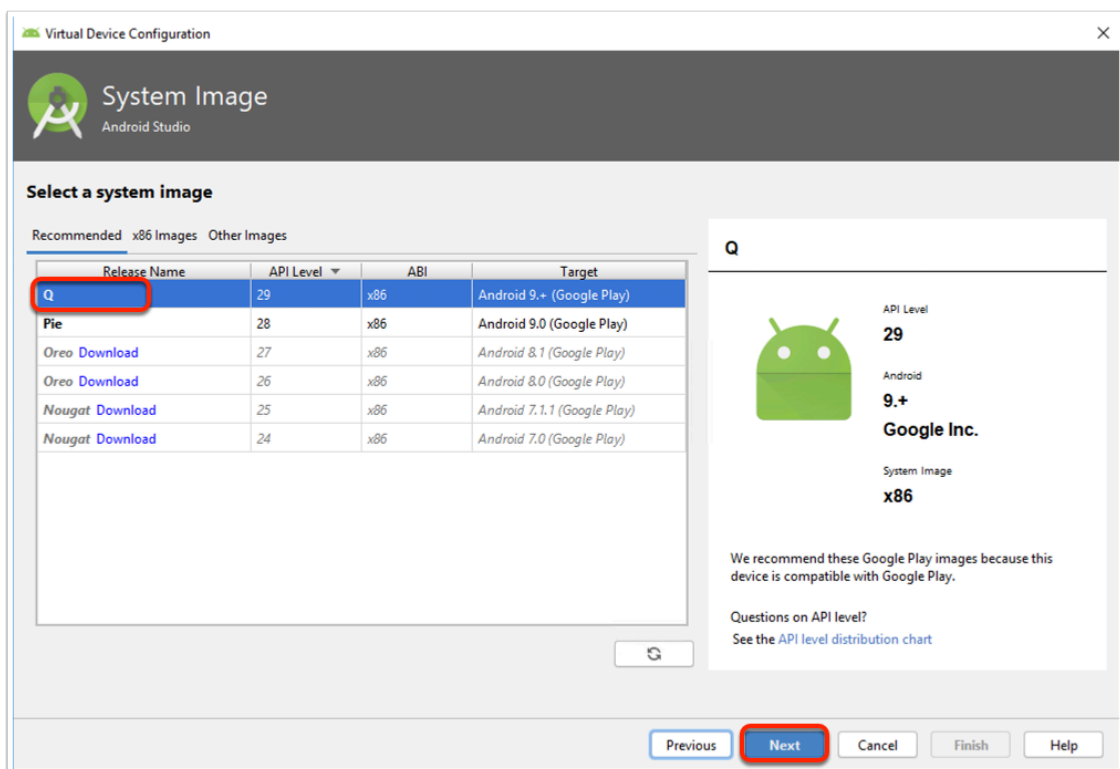
16. In the **Select a system image** window, if recommended **Install Haxm**



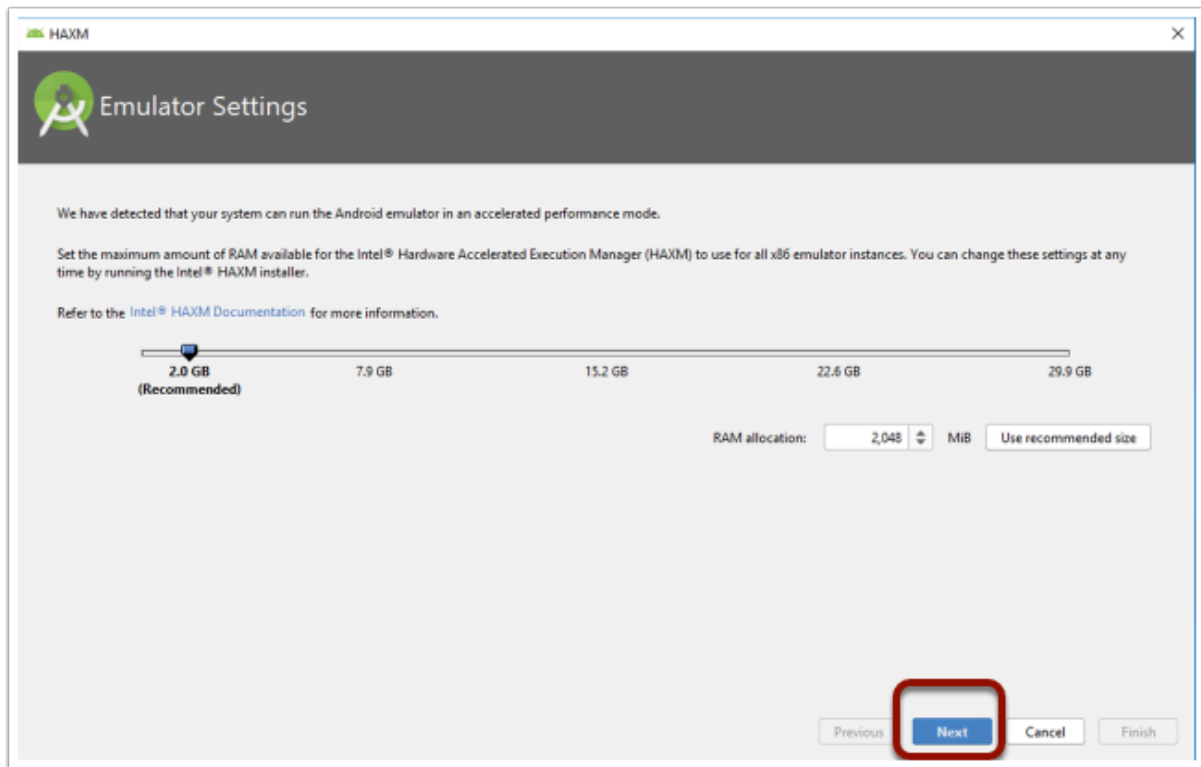
17. Click **Yes** to allow windows command processor to make changes to your device



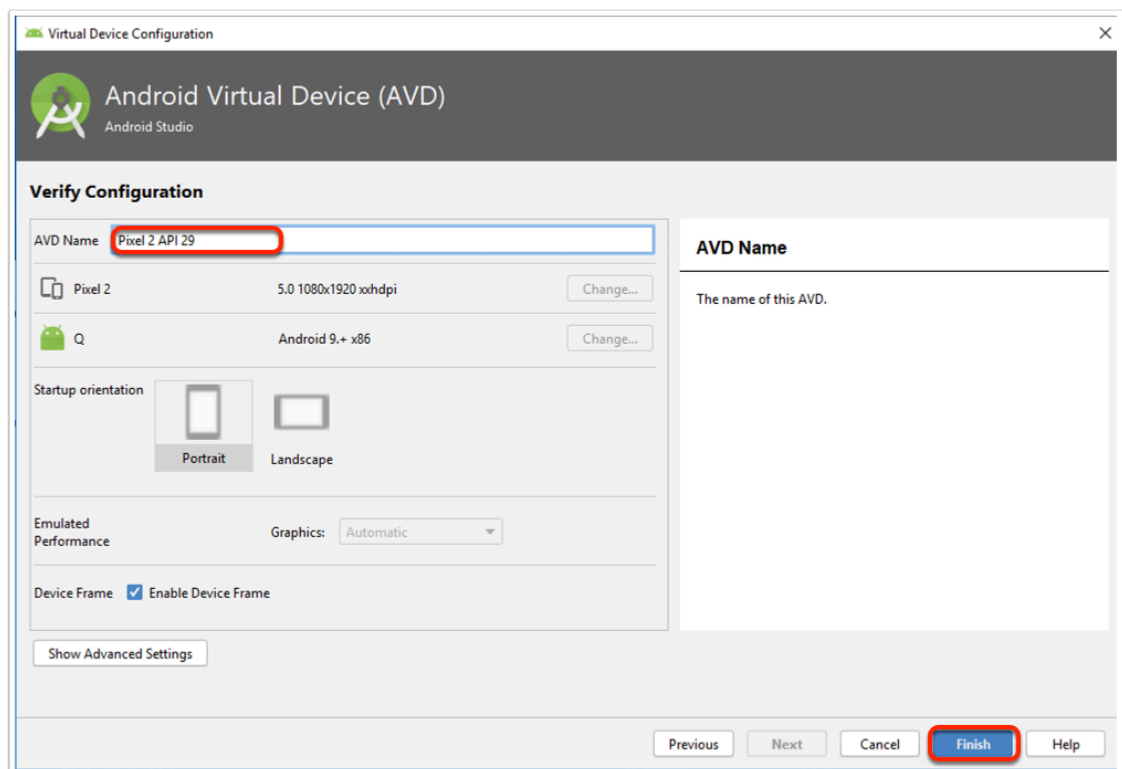
18. When you see **Done**. Select **Finish**.



19. Back in the Select a system image window Select **Q** and click **Next**

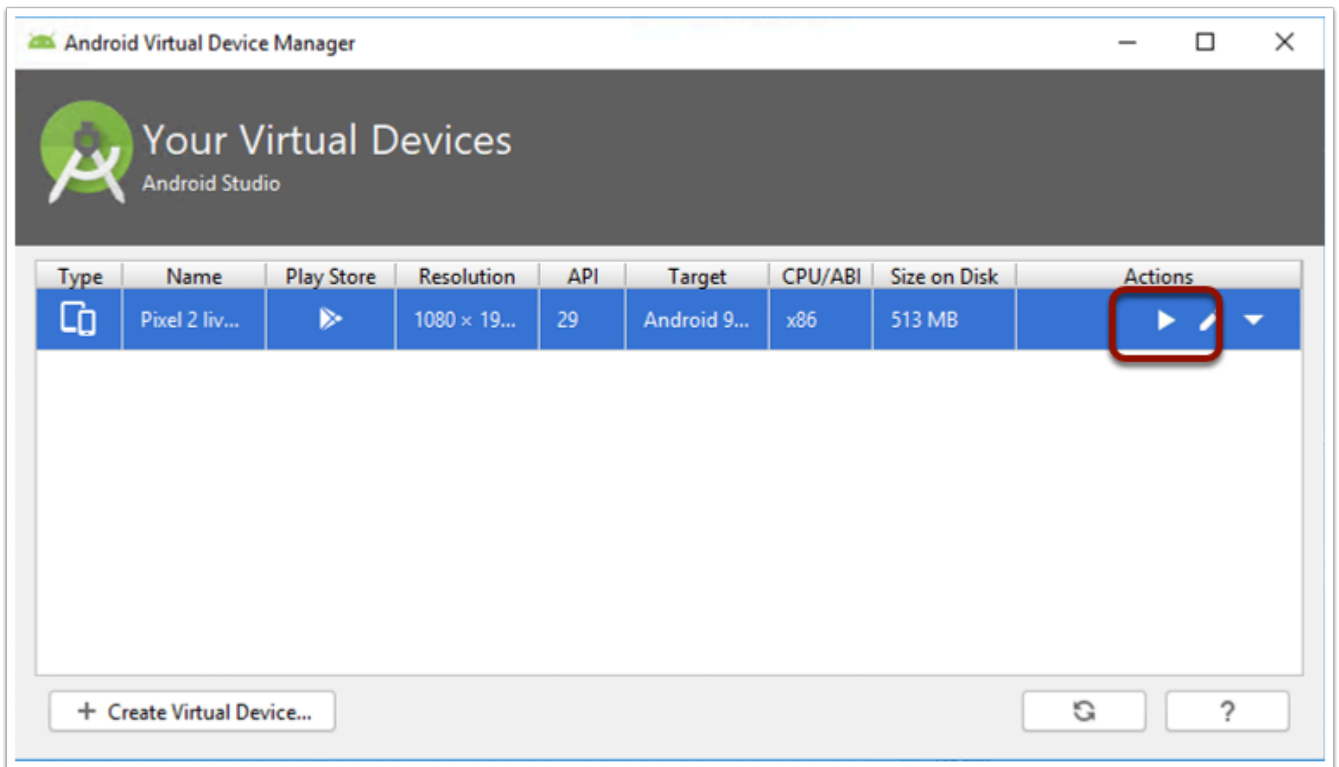


20. If prompted, in the **Emulator Settings** window, Use the recommended memory settings and click **Next**

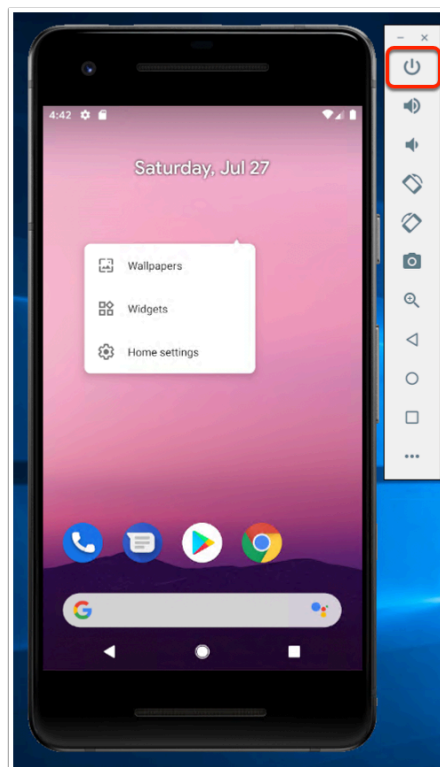


21. Give a name to your virtual device and click **Finish**





22. In your **Android Virtual Device Manager** window, in the actions column click on the "Play" icon to start the emulator



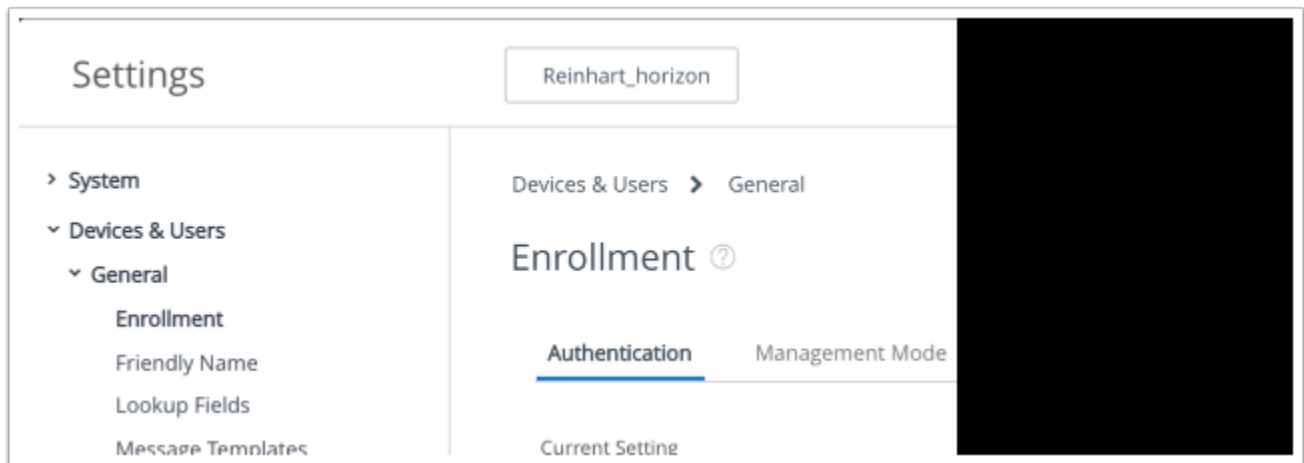
23. Your emulator is ready to use, if you need to restart your device you can hold the power icon to see the power options.

# Day 2

# WorkspaceOne Hub Enrollment

## Part 1: Pre-Requirement for Enrollment

There are some pre-requirements on the Workspace ONE UEM console before you enroll your device. for getting the Intelligence Hub application to work well. VMware is moving away from the **AirWatch Agent** and **Workspace One** application and consolidating under a single application referred to as the **Workspace ONE Hub**. We have to configure Workspace ONE Access and Workspace ONE UEM to provision applications, we will configure the **Hub Services** for additional features.



1. Login to your **WorkspaceOne UEM Admin Console** and select to **Groups & Settings > All Settings > Device & Users > General > Enrollment**

Authentication Mode(s) ☒ Basic ☒ Directory ☐ Authentication Proxy

Source of Authentication for Intelligent Hub WORKSPACE ONE UEM WORKSPACE ONE ACCESS ⓘ

Devices Enrollment Mode\* ☒ Open Enrollment ☐ Registered Devices Only

User Enrollment for iOS 13+ and macOS 10.15+ devices ENABLED DISABLED ⓘ

Require Intelligent Hub Enrollment for iOS ENABLED DISABLED ⓘ

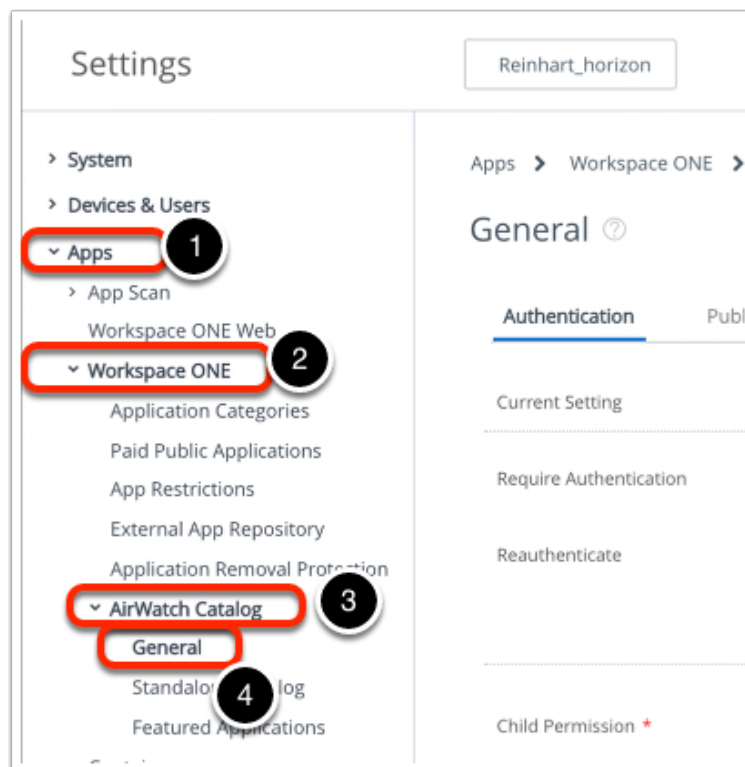
Require Intelligent Hub Enrollment for macOS ENABLED DISABLED ⓘ

---

Child Permission ☐ Inherit only ☐ Override only ☒ Inherit or Override

## 2. Under the Authentication Tab

- Next to **"Source of Authentication for Intelligence Hub"** switch **WORKSPACE ONE UEM** to **Workspace ONE Access**
- Select **ENABLED** next to **"Require Intelligence Hub Enrollment for iOS"**
- Select **SAVE** at the bottom right corner.



## 3. You will now have to enable the catalog service in the Hub application

- Select **All Settings > Apps > WorkspaceOne > AirWatch Catalog > General**

Apps > Workspace ONE > AirWatch Catalog

### General ?

Authentication **Publishing** Customization

Current Setting ☐ Inherit ☒ Override

Catalog Title \*  This corresponds to the catalog title that appears on the home: recommended tha... [Show More](#)

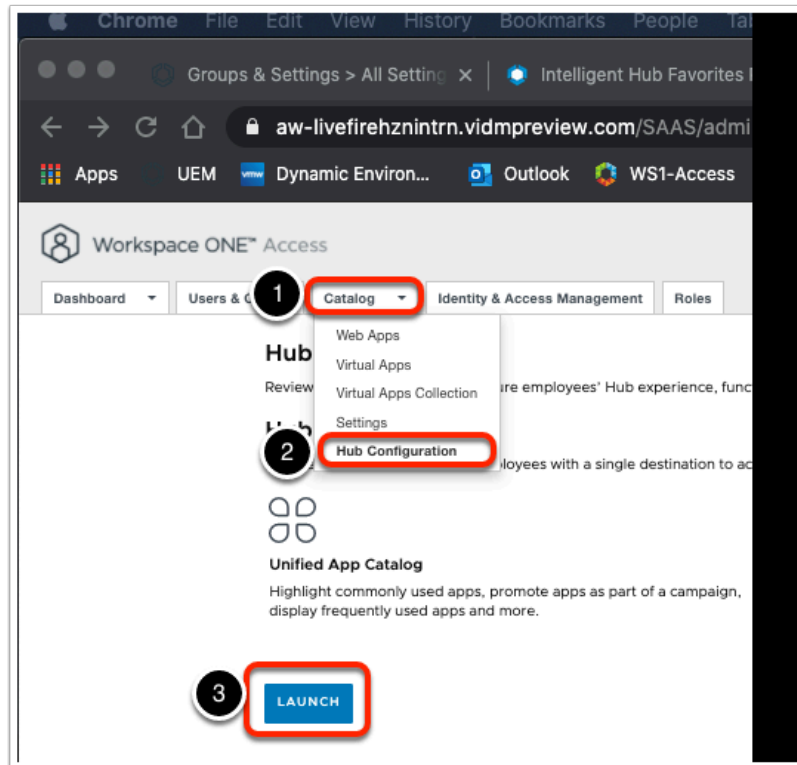
#### Platforms

? Publish the catalog to devices in this Organization Group. Legacy Catalog settings will deliver the catalog as a webclip/shortc

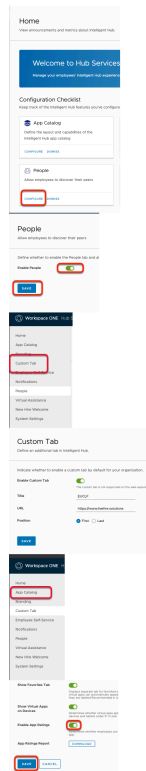
|   |                         |
|---|-------------------------|
| Legacy Catalog (iOS)                      | <b>ENABLED</b> DISABLED |
| Full Screen                               | ENABLED <b>DISABLED</b> |
| Intelligent Hub Catalog (iOS)             | <b>ENABLED</b> DISABLED |
| Legacy Catalog (Android)                  | <b>ENABLED</b> DISABLED |
| Intelligent Hub Catalog (Android)         | <b>ENABLED</b> DISABLED |
| Legacy Catalog (Windows Desktop)          | <b>ENABLED</b> DISABLED |
| Intelligent Hub Catalog (Windows Desktop) | <b>ENABLED</b> DISABLED |
| Legacy Catalog (macOS)                    | <b>ENABLED</b> DISABLED |
| Intelligent Hub Catalog (macOS)           | ENABLED <b>DISABLED</b> |

4. Under the **Publishing** tab select **ENABLED** next to
  - **"Intelligence Hub Catalog (iOS)"**
  - **"Intelligence Hub Catalog (Android)"**
  - **"Intelligent Hub Catalog" (Windows Desktop)**
  - Select **Save** at the bottom right.

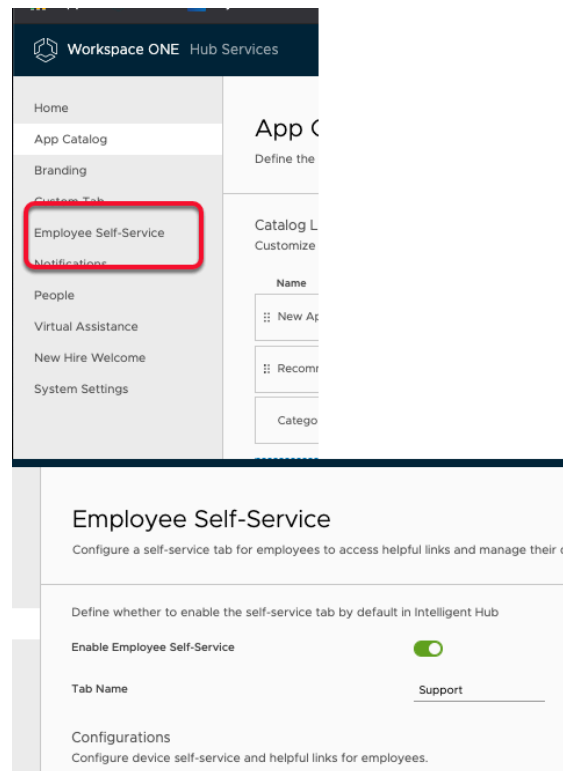
## Part 2: Hub Services & People Search



1. Now we will enable Hub Services and People Search inside of Workspace ONE Access to ensure that we have a connection
  - Navigate to your unique Workspace ONE Access SaaS Tenant Admin Console and authenticate using your **Admin credentials. (Select Domain as System Domain)**
  - On the **Workspace ONE Access** Console,
    - Select the **Catalog** tab
    - From the drop-down, select **Hub Configuration**
    - Select **LAUNCH**

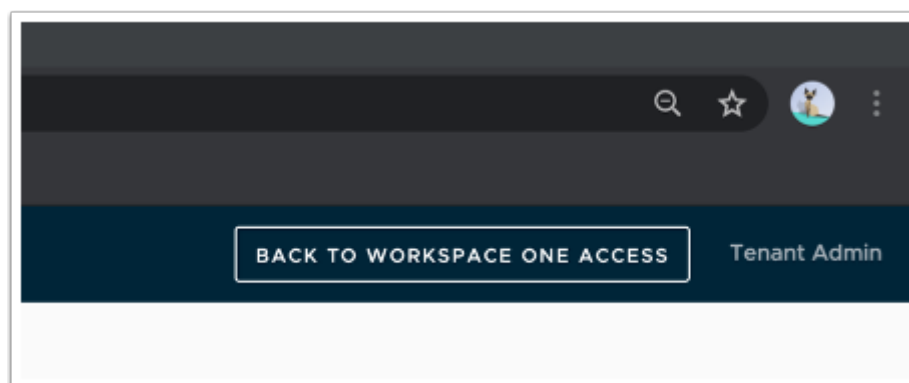


2. On the **Home** page, Under **Configuration Checklist**, configure the following:
  - Click on **CONFIGURE** under **People**,
    - **Enable People** by turning the **toggle** green. Select **SAVE**.
  - On the left menu, select the **Custom** Tab. Enable by turning the toggle green.
    - In the **Title** area type:
      - **EUCLF** (Best practice is not use a label longer than 6 characters).
    - **URL:** <https://www.livefire.solutions>.
    - Next to **Position**, ensure the **First** **radio button** is selected.
  - On the left menu, select **App Catalog**,
    - Ensure **Enable App Ratings** **toggle** is on (default is ON)
    - Leave the rest as default
  - Select **SAVE**



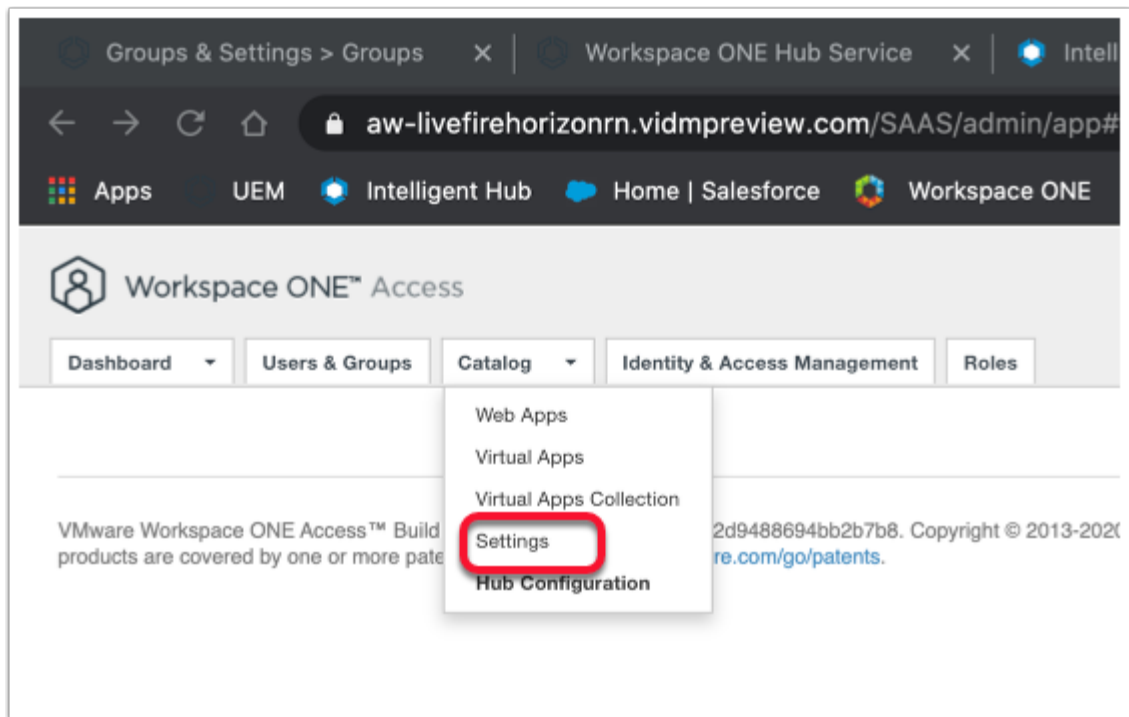
### 3. Enabling Employee Self Service,

- In left navigation pane select **Employee Self-Service** .
- This is enabled by default. No action needed. Take note of the configurable options. For example Helpful Links or how to guides. This might be helpful for onboarding as one example

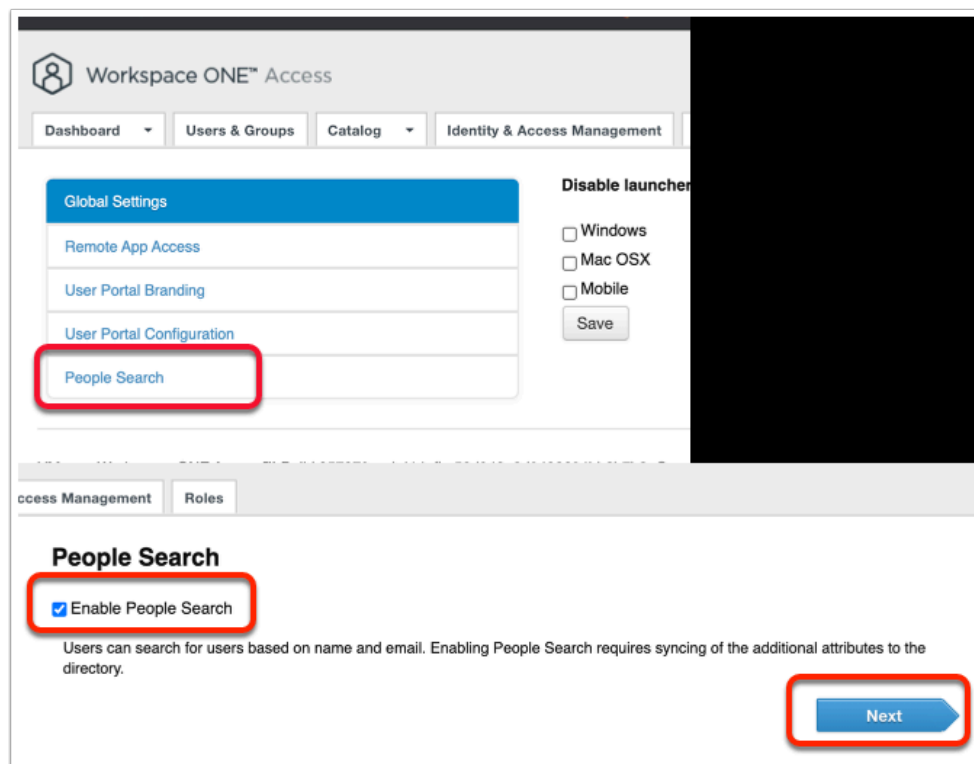


### 4. To the right of the page select **BACK TO WORKSPACE ONE ACCESS**

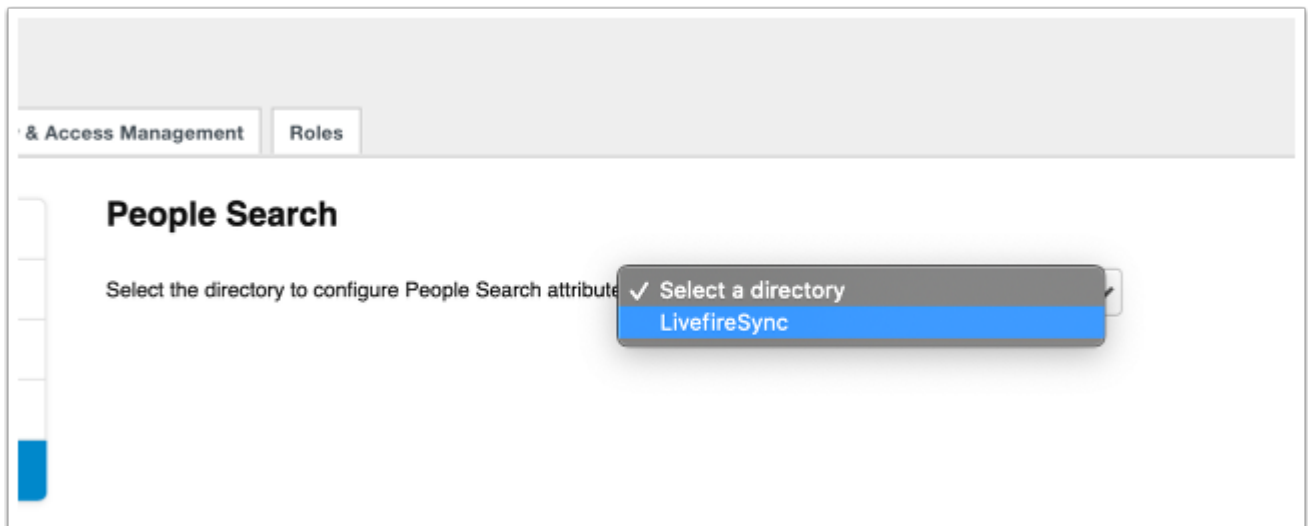




5. Select the **Catalog** tab ,
  - From the dropdown select **Settings**.



6. Select **People Search**
  - Select the **check box** next to **Enable People Search**
  - Select **NEXT**



7. Select the Directory **LivefireSync**

| Attribute Name in VMware Workspaces ONE Access | Attribute Name in Active Directory |
|--|------------------------------------|
| distinguishedName                              | distinguishedName                  |
| managerDN                                      | manager                            |
| title  | title                              |

8. Note the following with the associated dropdown
- **distinguishedName, checkbox** is enabled
  - **managerDN, checkbox** is enabled
  - **title, checkbox** is enabled
  - select **Next**
  - **Validate the associated attributes are associated in the Attribute Name Directory**
    - **distinguishedName = distinguishedName**
    - **managerDN = manager**
    - **title = title**

- Select **Next**

Access Management Roles Search users,...

### People Search

Specify the users that you want to sync.

To use the People Search app successfully, all users should be synced to the directory. If the Workspace ONE Access service is not already configured to sync all users, specify the distinguished name (DN) to sync all users.

Note: This User DN is added to the directory sync profile that is set up in Directory > Sync Setting > Users.

Enter as CN=users,DC=domain,DC=com.

Specify the user DN's

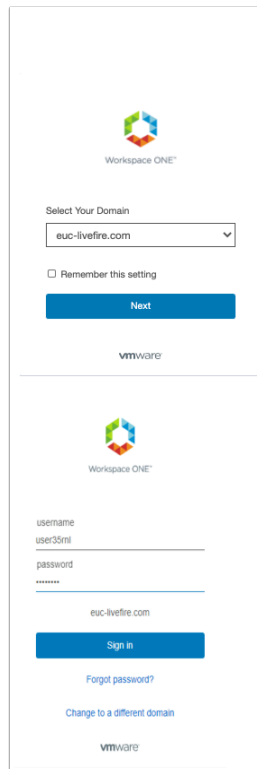
OU=corp,DC=euc-livewire,DC=com

[Back](#) [Save & Sync](#)

[Sync Directory](#)

protected by copyright and intellectual property laws in the United States and other

- On the **People Search** page
  - Under the **Specify the user DN's** edit the default **CN=Users,DC=euc-livewire,DC=com**
    - **OU=Corp,DC=euc-livewire,DC=com**
    - Select **Save & Sync**
    - Select **Sync Directory**



Workspace ONE™

Select Your Domain

euc-livewire.com

☐ Remember this setting

Next

VMware

---

Workspace ONE™

username

user35rnl

password

\*\*\*\*\*

euc-livewire.com

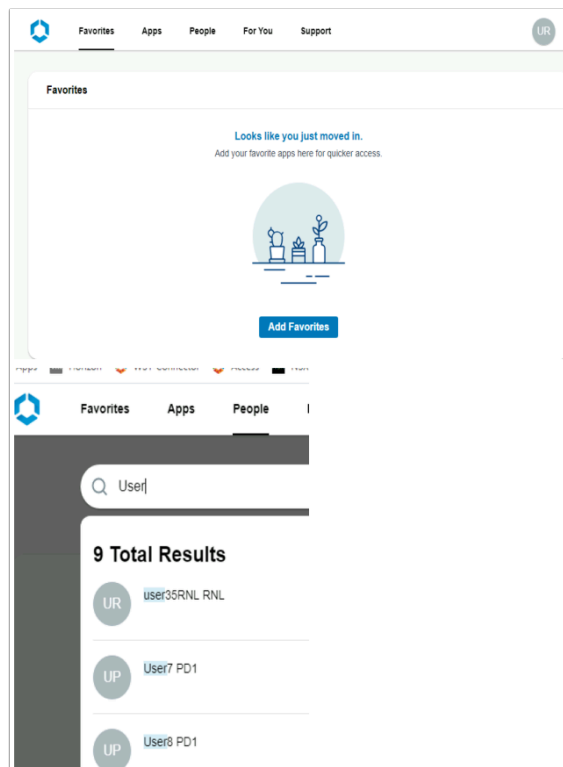
Sign in

[Forgot password?](#)

[Change to a different domain](#)

VMware

10. Open an **Incognito window** on your browser and navigate back to your **Workspace ONE Access** tenant
- Under **Select Your Domain**, select **euc-livewire.com**, select **Next**
  - Login using your custom Active Directory Account **Userx** and **VMware1!** e.g. **user35RNL**
  - Select **Sign in**

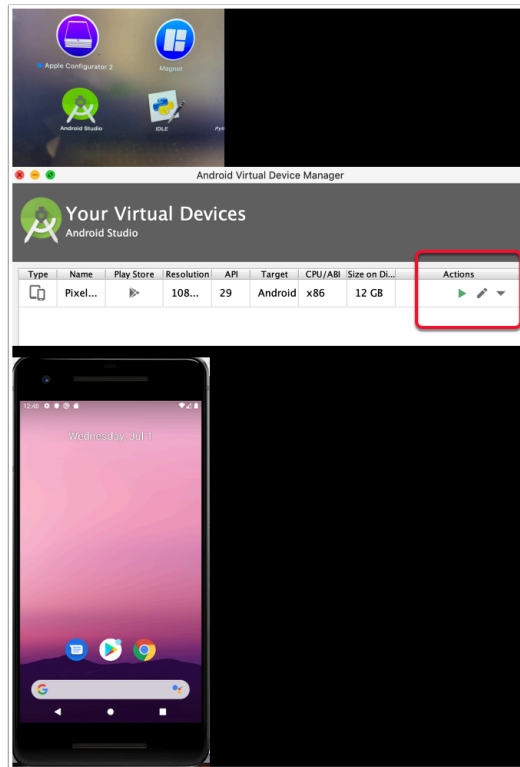


11. Select **People**

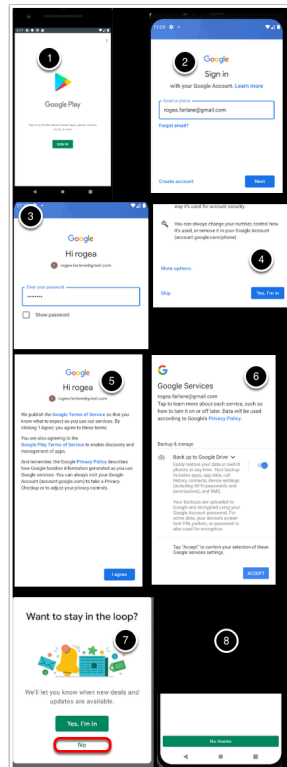
- In the **search interface** type **User**
  - Notice the search results
  - Select an individual user and notice you can see information related to the user.

## Part 3 Intelligence Hub Enrollment

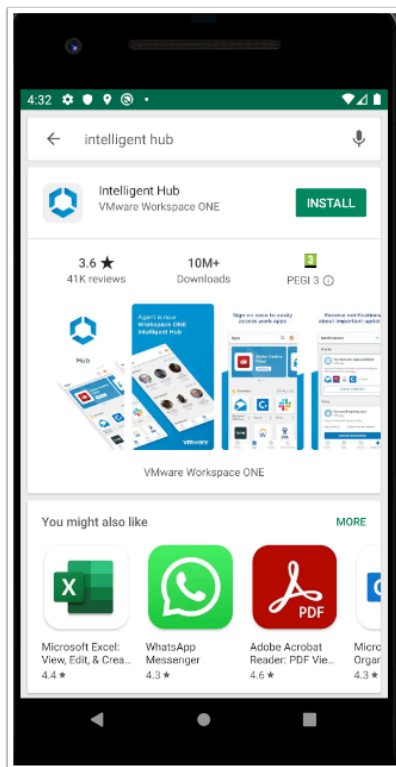
### Section 1. Android - Intelligence Hub Enrollment



1. This lab will walk you through how to enroll an android device in **Device Profile mode** using the WorkspaceOne Intelligence Hub.
  - Launch your Android Studio Emulator configured on Day 1
    - In the **Your Virtual Devices** window under **Actions**, select the **Play** button

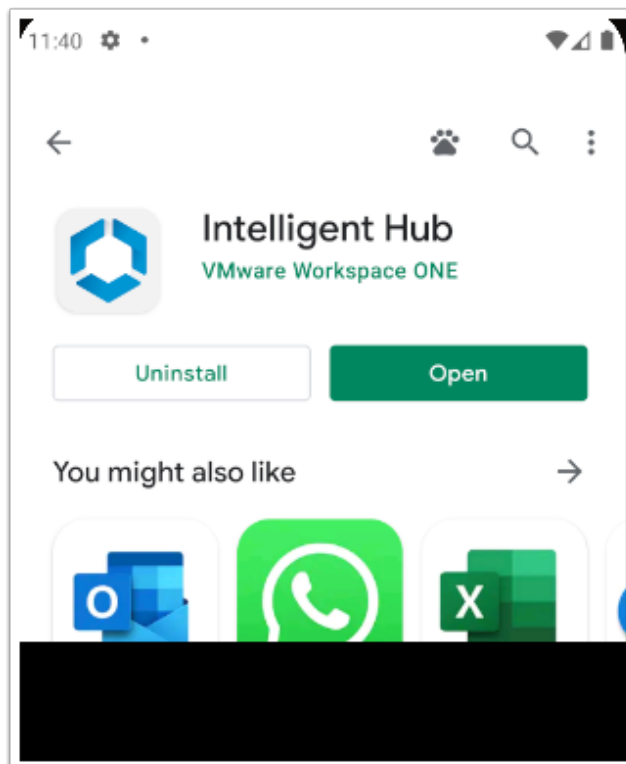


2. Open the **Google Play Store** APP on your android device
  1. Select **SIGN IN**
  2. In the **Sign in** window, **enter your email**, select **NEXT**
  3. Enter your **Password** window, select **NEXT**
  4. On the **Add phone number?** page, **scroll down** and select **Skip**
  5. On the **Terms of Service** page, select **I agree**
  6. On the **Google Services** page select **ACCEPT**
  7. On the **Want to stay in the loop?** select **No**
  8. On the **Google Play** select **No thanks**, twice

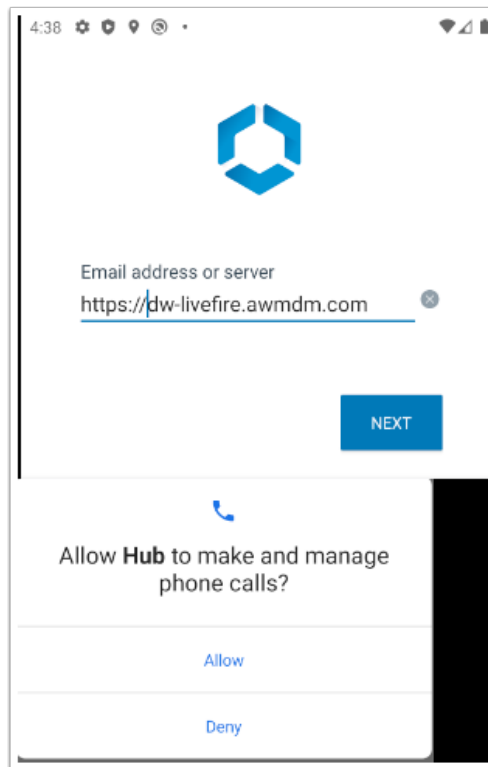


3. Search for **Intelligent Hub**

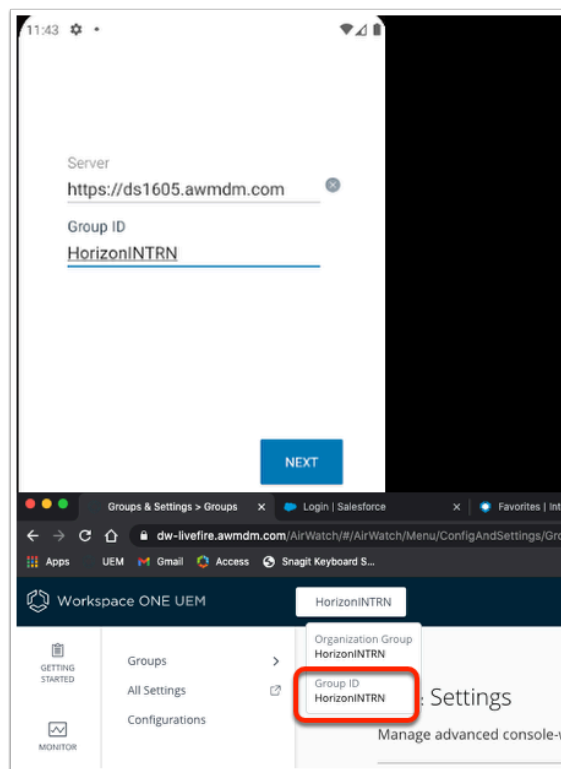
- If you are prompted for payment information, select **SKIP**
- Select **INSTALL**



4. Next to **Intelligent Hub**, select **Open**



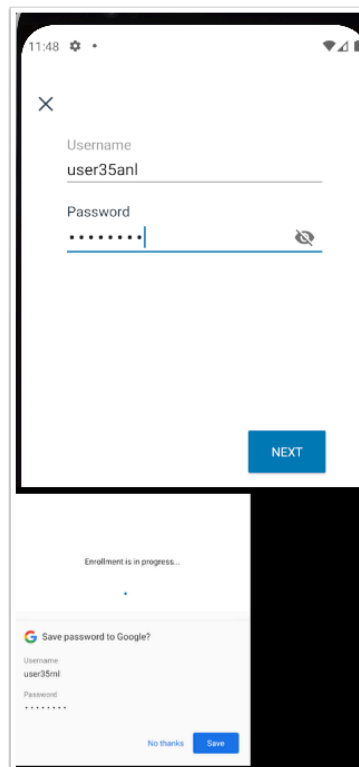
5. Under the **Email address or server** area, type <https://dw-livefire.awmdm.com>
  - Select **NEXT**
  - When prompted select **Allow**



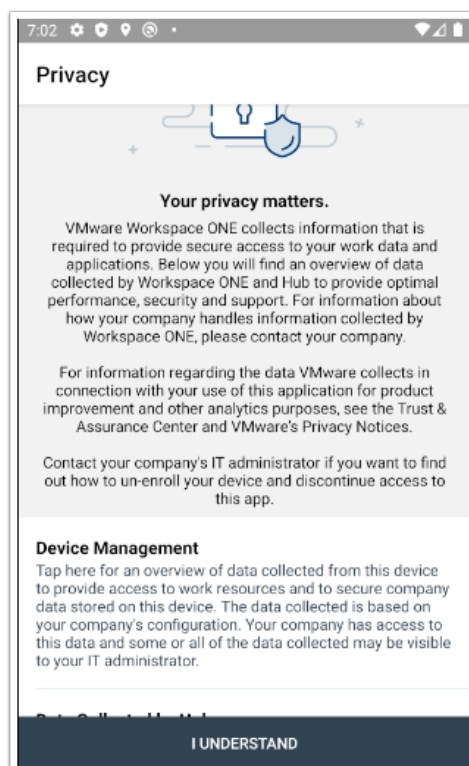
6. Under **Group ID**, enter your **Workspace ONE UEM org Group ID**. If you dont know your Group id hover over the dropdown menu for your organizational unit.



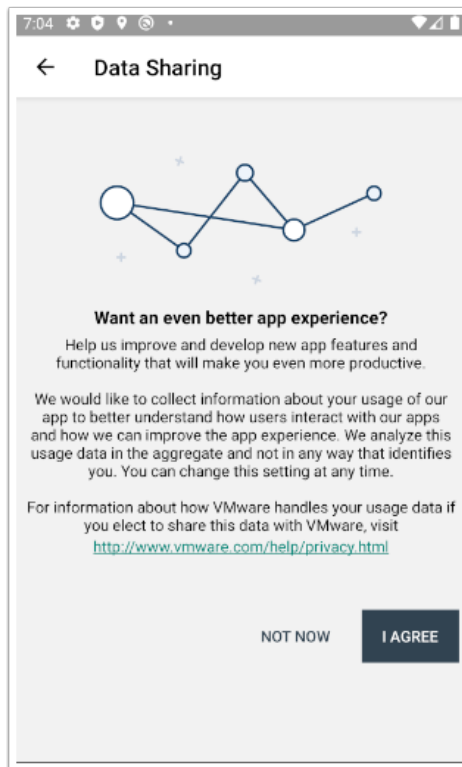
- Select **NEXT**



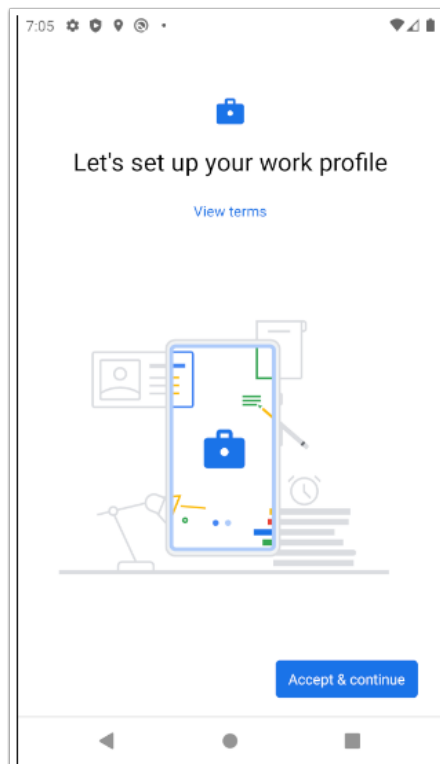
7. Under **Username**, enter your **custom Active Directory Username**. eg User35ANL
  - In the **Password** area, enter **VMware1!**
  - When prompted to **Save password to Google?**, select **No thanks**



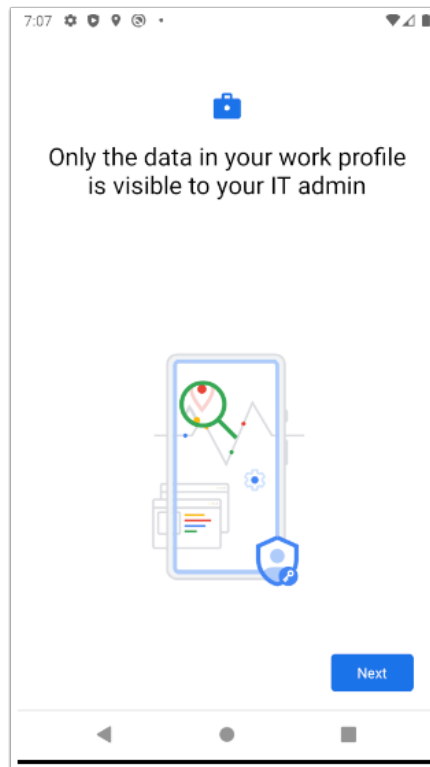
8. On the **Privacy** window, select **I UNDERSTAND**



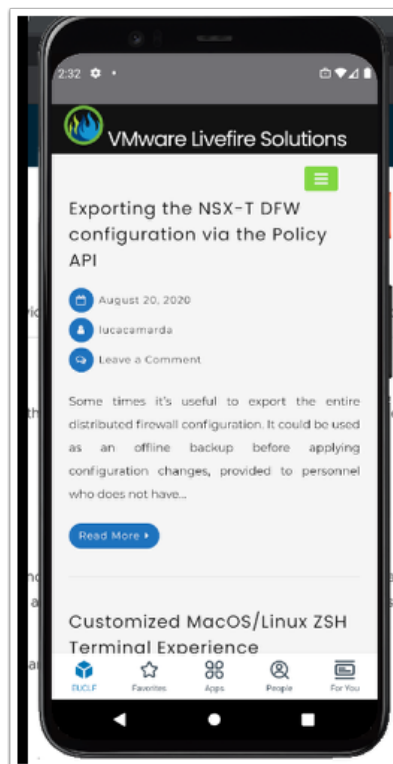
9. On the **Data Sharing** window, select **I AGREE**



10. On the **Let's set up your work profile**, select **Accept & continue**



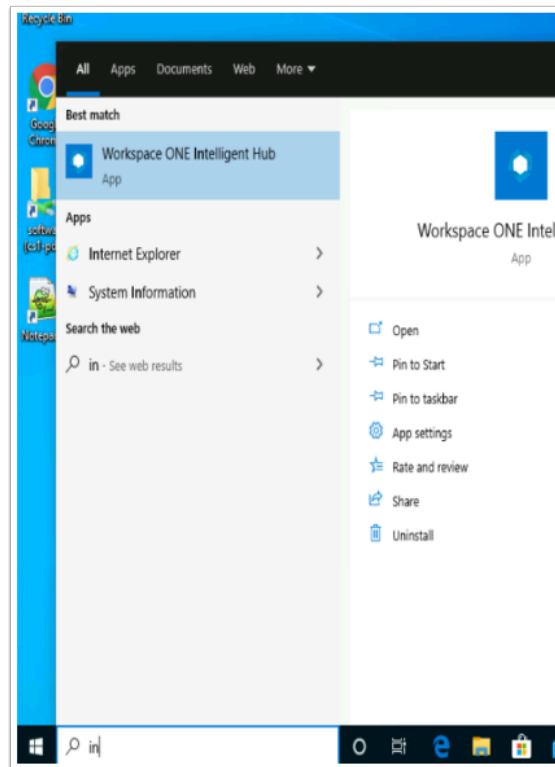
11. On the **Let's set up your work profile** page select **Next**



12. Notice the process in the enrollment phase on Android Enrollment.

- When you see this, you have completed your Android Enrollment with Intelligent Hub

## Section 2. Windows 10 Intelligent Hub Enrollment



In this Lab we will Enroll a Win10 1809 VM using the latest WorkspaceOne Intelligence Hub

1. Log into the **Control Center** and open the **Remote Desktop** folder on the Desktop.
  - Select the **W10Client02 RDP** client and sign-in with **username administrator** and **password VMware1!**
  - To the right of the **Start** button in the search area, start typing **intel**
  - Select the **Workspace ONE Intelligent Hub**

Workspace ONE Intelligent Hub

Email or Server Address

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

Next

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

Groups & Settings > Groups

Workspace ONE UEM

HorizonNTRN

Organization Group: HorizonNTRN

Group ID: HorizonNTRN

Email or Server Address

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

Group ID

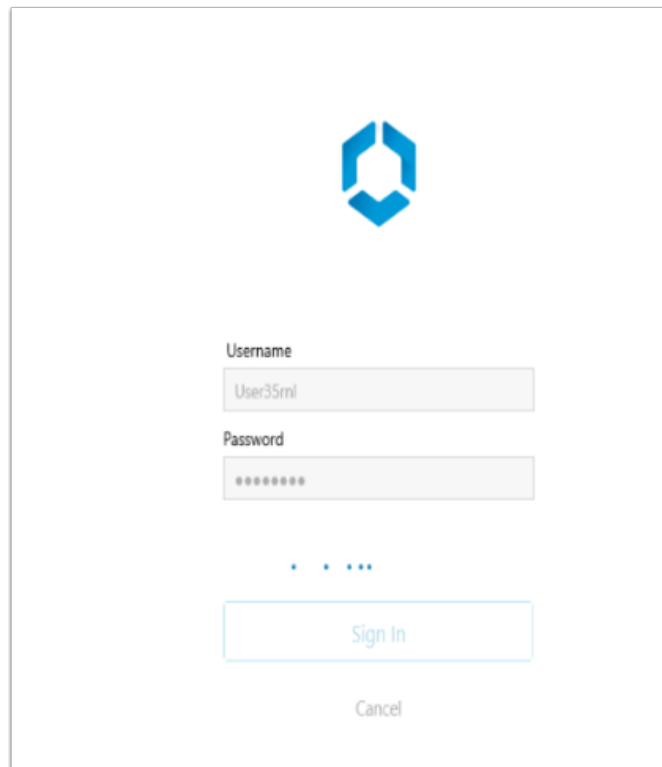
HorizonNTRN

Next

Cancel

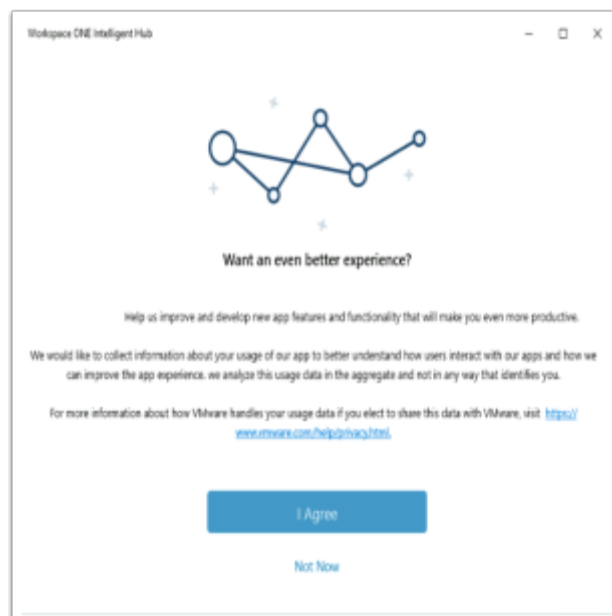
3. Under **Group ID** unique enter your unique your **Workspace ONE UEM** tenant **Group ID**
  - To get your unique *Workspace ONE UEM Group ID*, revert back to your **Workspace ONE UEM** tenant and look for the following next to the **Workspace ONE UEM** logo, select your **Organization Group** and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

- Select **NEXT**



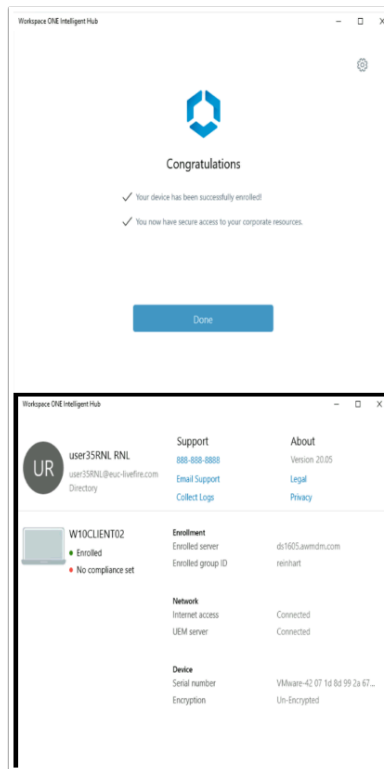
The image shows a login window for Workspace ONE Intelligent Hub. At the top center is a blue hexagonal logo. Below it, there are two input fields: 'Username' with the text 'User35ml' and 'Password' with masked characters '\*\*\*\*\*'. Below the password field are three small blue dots. At the bottom, there are two buttons: 'Sign In' and 'Cancel'.

4. In the **Workspace ONE Intelligent Hub** under
  - **Username** enter your **custom Active Directory Username**
  - **Password** enter **VMware1!**
  - Select **Sign in**



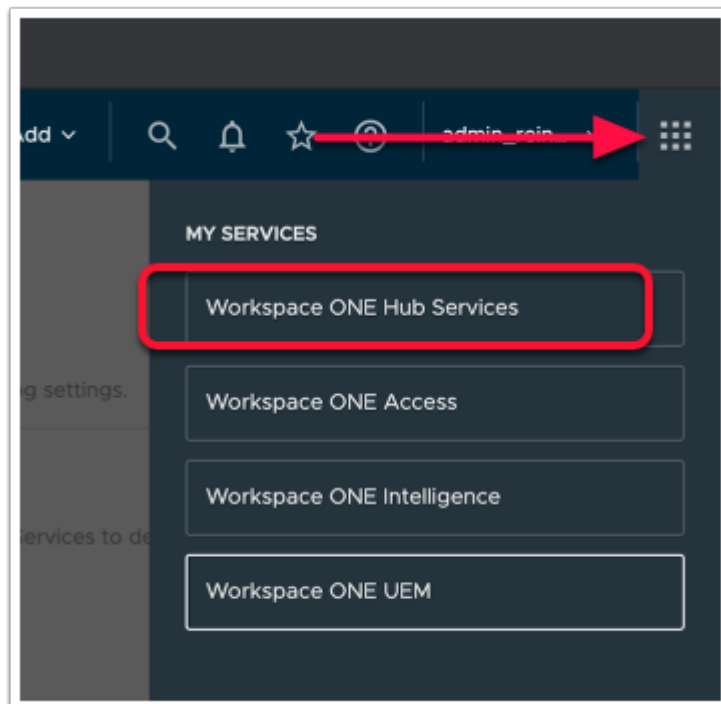
The image shows a privacy notice window titled 'Workspace ONE Intelligent Hub'. It features a blue line-art logo of a network. Below the logo, the text reads: 'Want an even better experience? Help us improve and develop new app features and functionality that will make you even more productive. We would like to collect information about your usage of our app to better understand how users interact with our apps and how we can improve the app experience. we analyze this usage data in the aggregate and not in any way that identifies you. For more information about how VMware handles your usage data if you elect to share this data with VMware, visit <https://www.vmware.com/help/privacy.html>.' At the bottom, there are two buttons: 'I Agree' and 'Not Now'.

5. Select **I Agree**

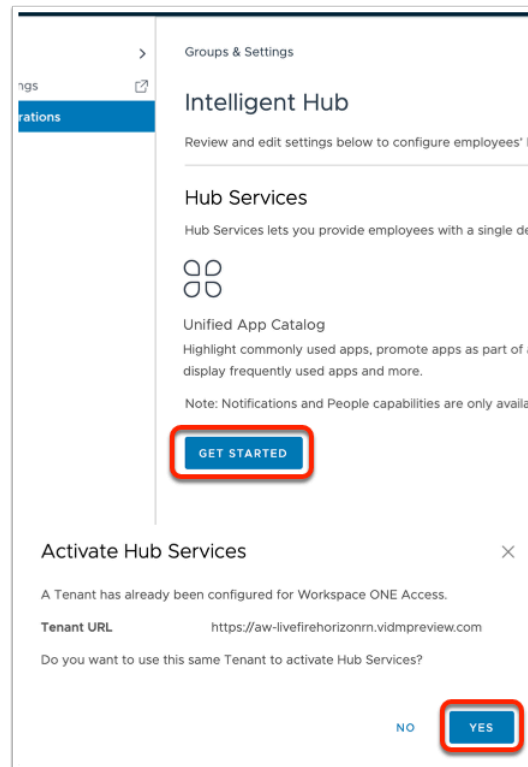


6. On the **Congratulations** window, select **Done**
  - Notice the Enrolled status of **W10Client02**

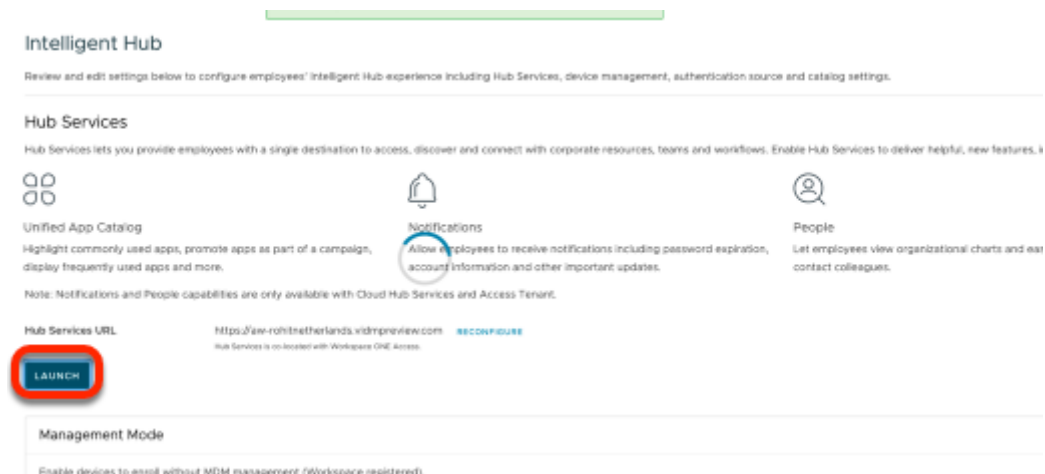
## Part 4. Workspace ONE UEM & Workspace One Hub Services



1. In the **WorkspaceOne UEM** console in the top right corner select the **six square grid**.
  - Select **Workspace ONE Hub Services**

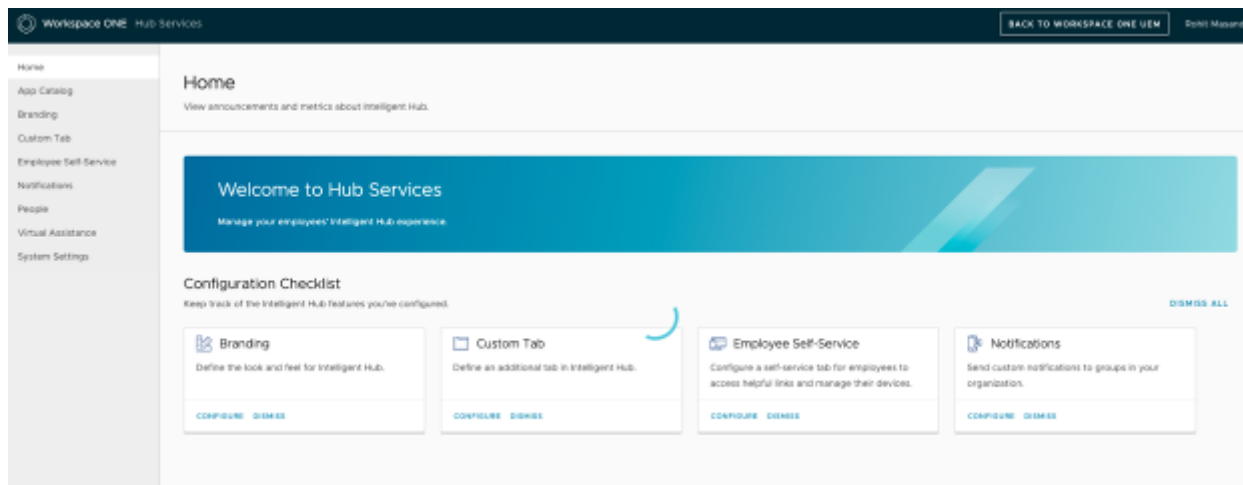


2. In the Intelligent Hub window, select **GET STARTED**.
  - When prompted to **Activate Hub Services**, select **YES**

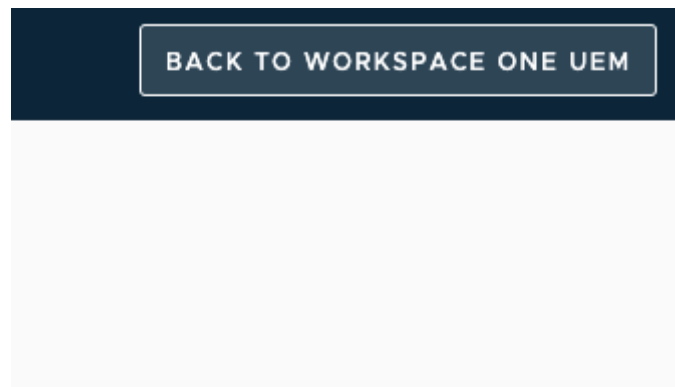


3. Click on **Launch** to open the Workspace ONE Hub Services.





- This page allows you to control the user experience inside the Intelligent HUB application, setup notifications and Self service portal for your users. Feel free to explore individual pages from the left menu panel. No further action needed.



- On top right, click on the **BACK TO WORKSPACE ONE UEM** Console.

# Federating BambooHR with WorkspaceONE Access

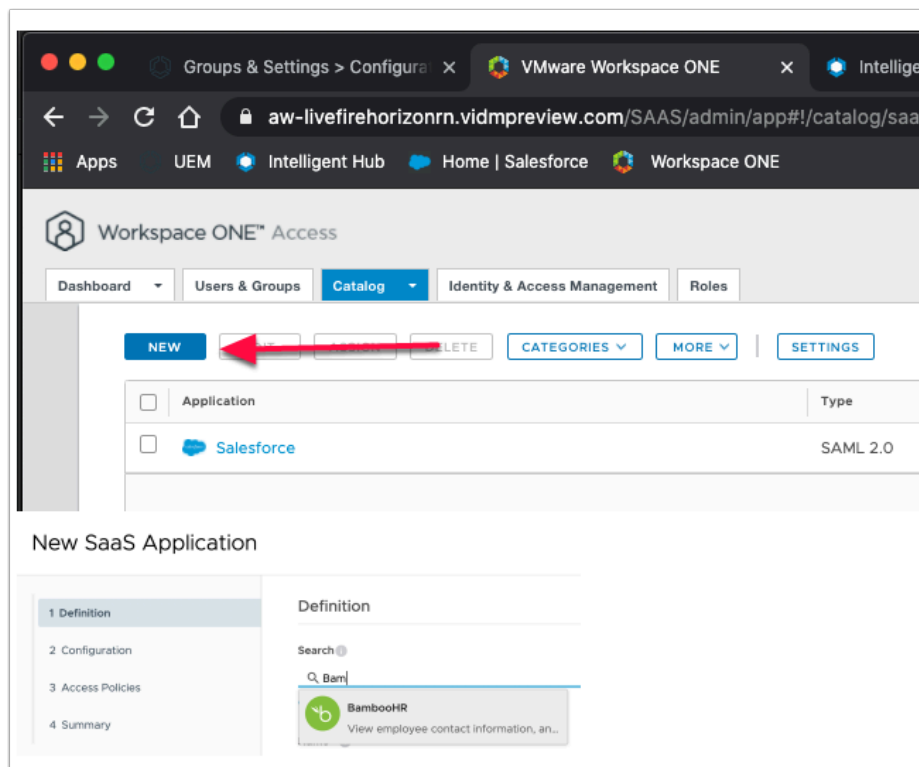
## Overview

In this section, we will be leveraging a public application BambooHR to demonstrate successful Federation of a SaaS application with Workspace ONE Access as an Identity Provider.

Its also comes as a native application for Android and IOS and will be useful when testing Mobile SSO for Android and IOS in later exercises

Note: Images precedes the steps

## Part 1: Adding BambooHR to the Workspace ONE Access Catalog



1. To enable single sign-on to BambooHR on the service, you must configure the application in the catalog and copy the SAML-signing certificate to BambooHR.

- **Add BambooHR to the Catalog**

1. Log in to the **Workspace ONE Access** administration console.
2. In the **Catalog** page, select **NEW**
3. In the **New SaaS Application** wizard under **Search** type **BambooHR**.
4. Select the **BambooHR** icon.
5. Select **NEXT**

**Single Sign-On**

**Authentication Type** \* ⓘ  
SAML 2.0

**Configuration** \* ⓘ  
☐ URL/XML ☒ Manual

**Single Sign-On URL** \* ⓘ  
<https://rnl35.bamboohr.com/saml/consume.php>

**Recipient URL** \* ⓘ  
<https://rnl35.bamboohr.com>

**Application ID** \* ⓘ

2. In the **Configuration** section of the **New SaaS Application** Wizard
  - Under **Single Sign-ON URL** append the first letter of your city and country two letter abbreviation + student number eg. rnl35
    - <https://rnl35.bamboohr.com/saml/consume.php>
  - Under **Recipient URL** append your domain name ie Utrecht35 to the FQDN
    - <https://rnl35.bamboohr.com>
- Please remember to document this in your custom accounts form

1 Definition

2 Configuration

3 Access Policies

4 Summary

Relay State URL ①

Application Parameters ①

| Name       | Description           | Default Value | Value |
|------------|-----------------------|---------------|-------|
| domainName | BambooHR sub domain n |               | rn35  |

Advanced Properties ▾

Assign

Application: 'BambooHR' added successfully.

Selected App(s): BambooHR

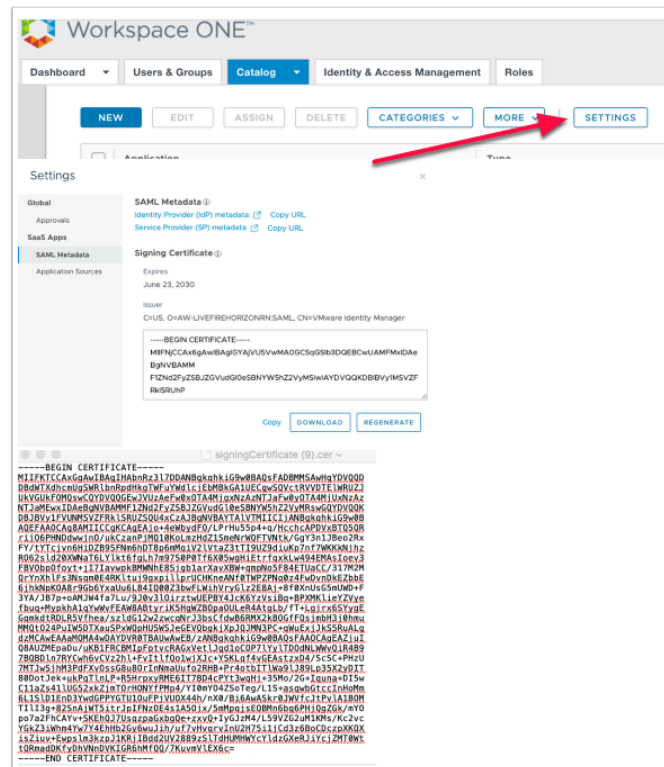
Users / User Groups

Search for Users or Groups

| Selected Users / User Groups | Deployment Type | Entitlement Type |
|------------------------------|-----------------|------------------|
| Marketing@euc-livewire.com   | Automatic       | Include          |

CANCEL SAVE

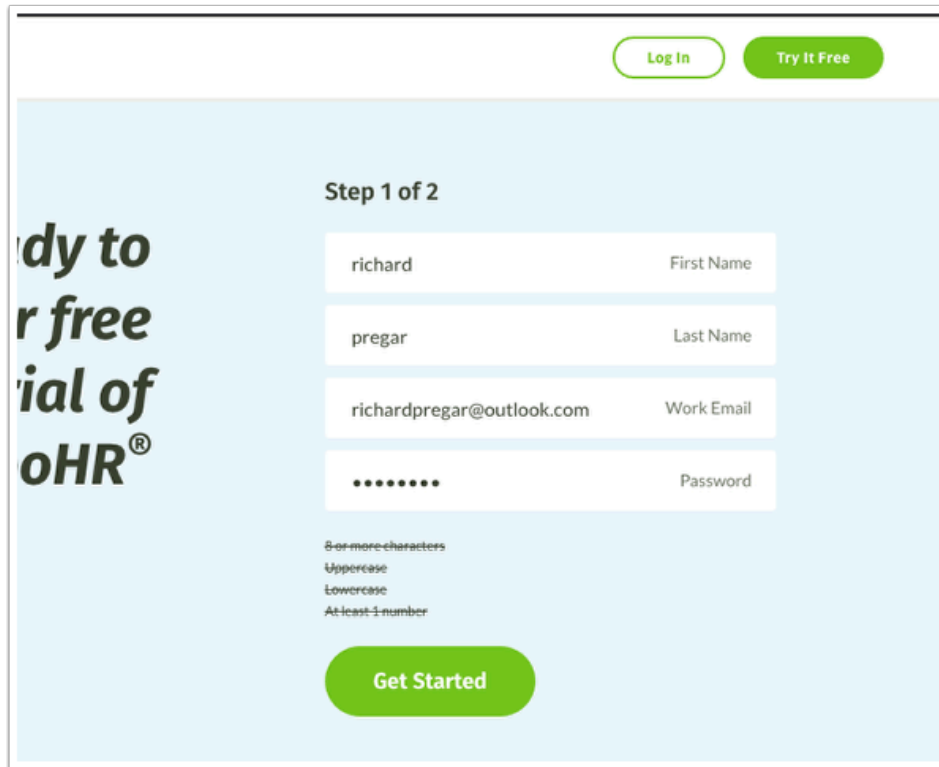
3. Under **Application Parameters** under value type in your Singular domain name
  - If your FQDN is going to be *rn35.bamboohr.com* then under **Value** type **rn35**
- Select **Next**
- On the **Access Policies** page select **NEXT**
- On the **Summary** page select **SAVE & ASSIGN**
- Under **Users / User Groups** type and select **Marketing**
  - Under **Deployment Type**, select **Automatic**
  - Ensure **Include** is selected under **Entitlement Type (Default)**
- Select **SAVE**



#### 4. Download SAML-Signing Certificate

- We need to download the SAML-signing certificate from the Workspace ONE Access service for the BambooHR configuration.
  - In the **Catalog** > **Settings** tab, click **SAML Metadata**.
  - Under **Signing Certificate** text select **download**.
  - Open a .txt editor and **copy** Make sure that you include text from -----BEGIN CERTIFICATE----- through -----END CERTIFICATE-----.

## Part 2. Setting up BambooHR



The image shows the BambooHR registration interface. At the top right, there are two buttons: "Log In" and "Try It Free". The main content area is titled "Step 1 of 2". On the left, there is a large, partially visible text "dy to r free ial of oHR®". The registration form consists of four input fields: "First Name" with the value "richard", "Last Name" with the value "pregar", "Work Email" with the value "richardpregar@outlook.com", and "Password" with masked characters ".....". Below the password field, there are four lines of password requirements: "8 or more characters", "Uppercase", "Lowercase", and "At least 1 number". At the bottom of the form is a green "Get Started" button.

1. We start off by registering a trial account with BambooHR, next we will federate BambooHR with Workspace ONE Access
  - Open up a browser use the following URL <https://www.bamboohr.com/signup.php>
    - As part of **Step 1** fill in your registration information and select **Get Started**

**Step 2 of 2**

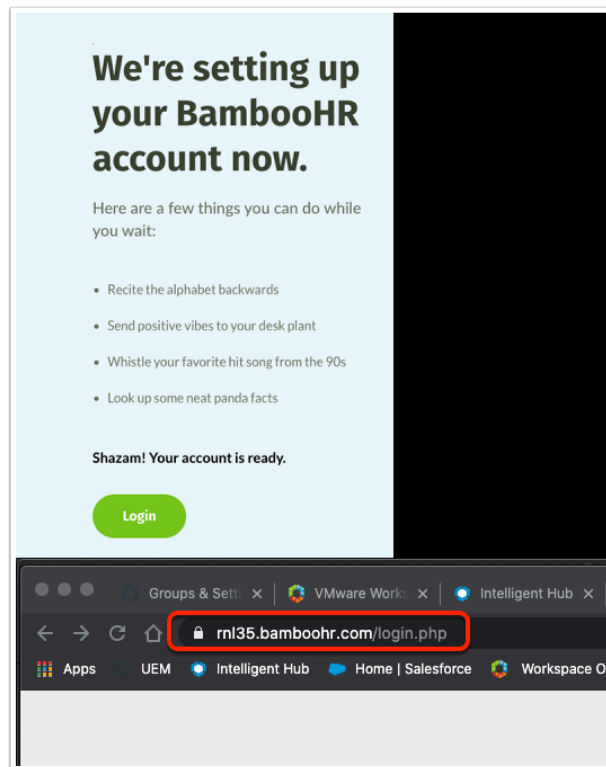
|                  |               |
|------------------|---------------|
| +447920812496    | Work Phone    |
| Livefire         | Company Name  |
| 1 - 10 employees | ▼             |
| United Kingdom   | ▼             |
| ANL36            | .bamboohr.com |

☒ By registering for this content, I am signing up to receive marketing materials (webinar and event invitations, newsletters, eBooks, etc.) from BambooHR. I understand that I can opt out at any time.

☒ I agree to the terms and conditions

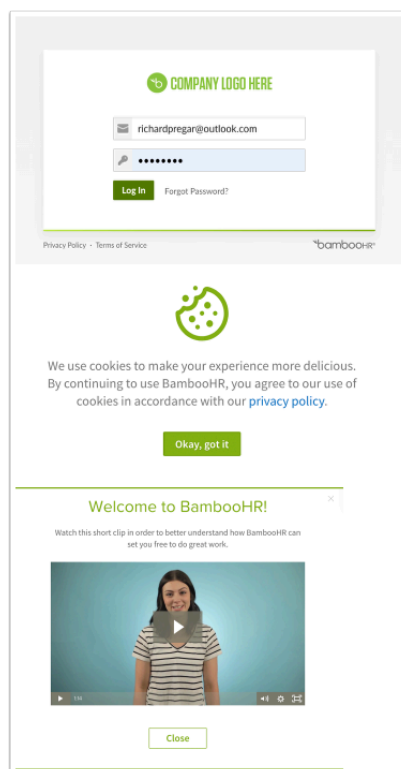
**Create Account**

2. As part of **Step 2** complete your registration information Next to
- **Phone number:** Add a phone number
  - **Company :** Livefire
  - **Number employees :** select a number
  - **Country :** your choice. e.g. Netherlands
  - **UnderFQDN** enter the first letter of your city, then country code + student number  
e.g. ANL35
- Select **Create Account**



### 3. ***Please wait until your account to be created***

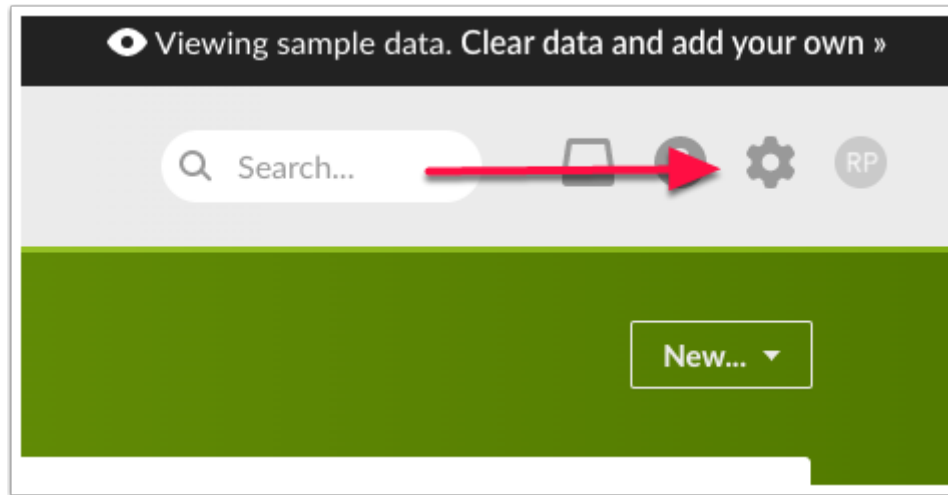
- Once your account is Ready select **Login**
- Document your new admin URL, username, password and email address used to register this account





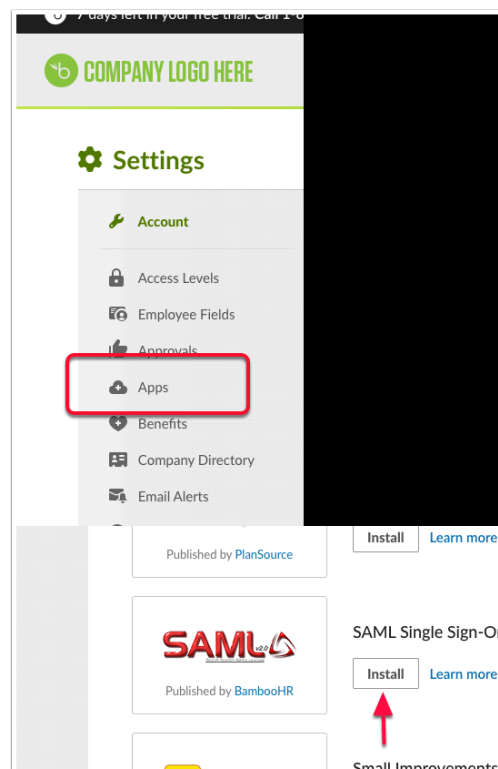
4. In your login page

- Enter your with your **email address** and **password**
- Select **Log In**
- On the Welcome page select **Close**
- Select **Okay, got it** on the Cookie notice page



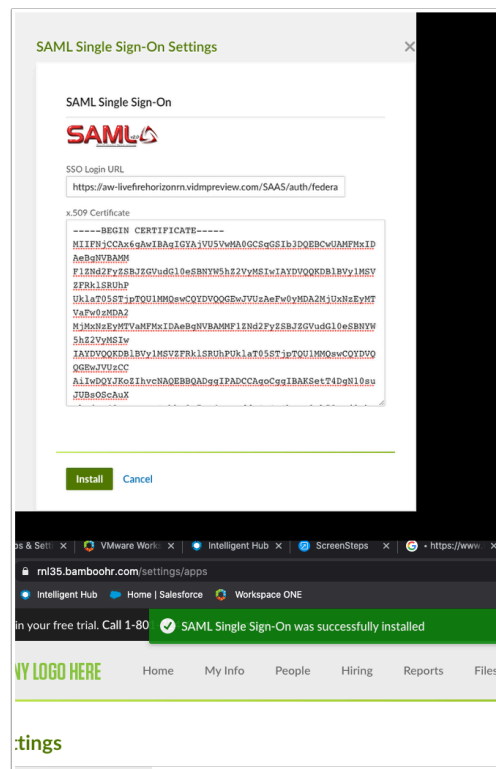
5. Once registered and logged in we will now configure the Single-Sign ON settings in BambooHR for Workspace ONE Access

- On the **Home Page** look to the right and select the **Cog wheel** Icons for **Settings**



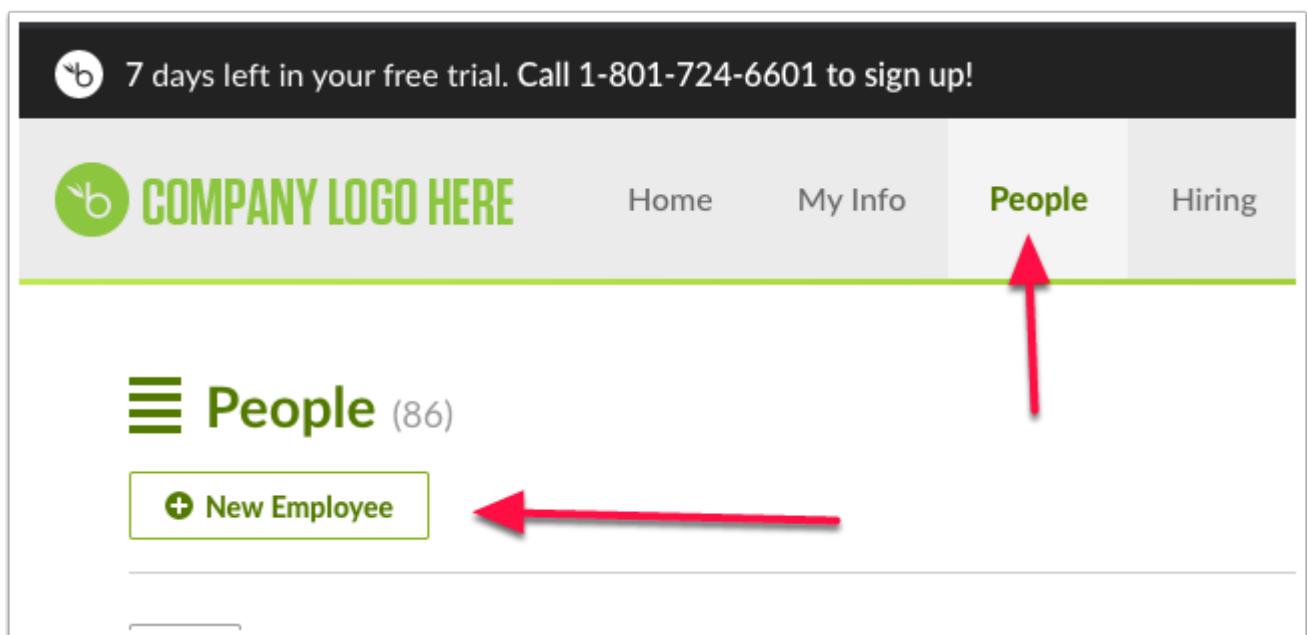
6. Under **Settings** select **Apps**

- In the **Apps Settings** page scroll down until you see the red **SAML** icon
- Select the **install** option next it.



7. In the SAML Single Sign-On window enter the following:-

- Under SSO Login URL\* : enter your Workspace ONE Access URL in the following format <https://myco.vmwareidentity.com/SAAS/auth/federation/sso>
  - e.g. <https://aw-euclivefirefran.vidmpreview.com/SAAS/auth/federation/sso>
- x509 Certificate: copy the entire content of your signing certificate downloaded in Part 1
  - Include text from **-----BEGIN CERTIFICATE-----** through **-----END CERTIFICATE-----**.
  - Select **Install**



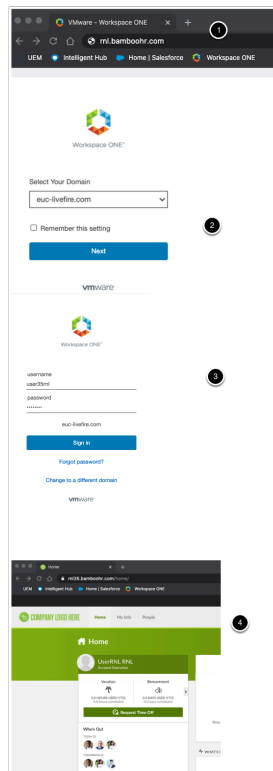
## 8. Setting an Identical custom test User account

- Select the **People** tab.
- Select **New Employee**.

The screenshot shows the 'user@STRL.RSL Properties' dialog box with the 'New Employee' tab selected. The form is divided into several sections: Personal, Address, Information, and Employment Data. The 'Email' field in the Personal section is highlighted with a red arrow. The 'Self-Service Access' radio button in the Employment Data section is also highlighted with a red arrow. The 'Save' button at the bottom of the dialog is highlighted with a red arrow.

## 9. In the Add Employee window add the identical information to what you added at the beginning of the course from your active directory,

- **NB!** Matching **email address** information identical to your Active Directory
  - If necessary double-check your info in Active directory
  - Ensure you have the **Self-Service Access** radio button turned on
- Select **Save**



## 10. Testing with your custom user account

- In Chrome, open up another browser and use the **Incognito mode** option or open an alternate browser like **Mozilla Firefox**
- Type your **domainname.bamboohr.com** e.g. **rnl35.bamboohr.com**
- On the Select your domain, ensure **euc-livewire.com** is selected and select **Next**
- On the **Workspace ONE Access** login type your custom account **username** and **Password** and select **Sign in**
- **Close down** the default access prompts and observe that your custom now has access to BambooHR with password based authentication from a Web Browser

In later exercises will use the Native application to provide a single-sign on experience and understand the specifics related to authentication that might be required to fulfill from a platform but also the application perspective

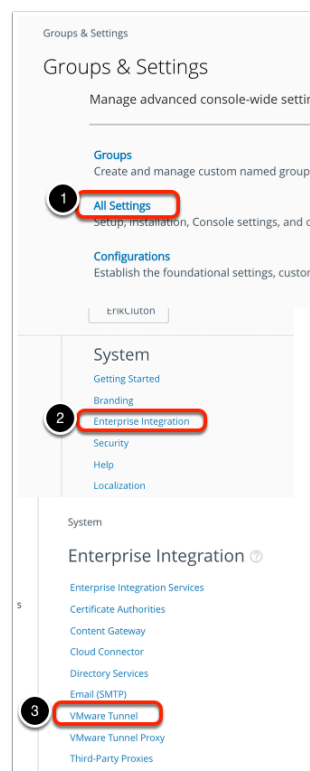
# Authentication Method - Android SSO

## Configure Single-Sign-on for Android Device from the Workspace ONE UEM Admin Console

### Pre-requisites to this lab

- For this lab you will need an Android Device that you are willing to enroll into this lab environment.
- If you do not have an Android test device, please complete Android emulator setup, from Day 1 lab, before proceeding.

## Part 1: Configuring Workspace ONE Access for Android Mobile SSO



1. In this section we will download a certificate from WorkspaceONE UEM and use to configure Android Mobile SSO in Workspace ONE Access. After we will round all the remaining Workspace ONE Access configurations.
  - Login to your Saas **WorkspaceONE UEM** with your custom credentials
  - Select **GROUPS & SETTINGS > All Settings**

- Under **System** select **Enterprise Integration**
- Under **Enterprise Integration** select **VMware Tunnel**

SAVE CANCEL ⓘ

2

Deployment Details

Deployment Type ☒ Basic ☐ Cascade ⓘ

1

Hostname \* Euclivfire

Port \* 444

- On the **Tunnel Configuration** page enter the following
  - Next to **Hostname:** **EUclivfire**
    - Note: This is a dummy value as we only leverage the Device Network traffic rules to send the Authentication request to a cert proxy service and not deploy a Tunnel Server physically.
  - **Port:** **444** (Choose any dummy port number)
  - At the top of the page select **SAVE**

> Server Authentication

Client Authentication

Authentication ☒ AirWatch ☐ Third Party ⓘ

CA Certificate \*

Thumbprint

E81E2A4887C4CF9C6C384DA7CC7FBC1C66FAD81

EXPORT REGENERATE

TunnelDeviceR....cer ^

! This type of file can harm your computer. Do you want to keep TunnelDeviceRoot....cer anyway? Keep Discard

- In the Tunnel Configuration window
  - Expand **Client Authentication**

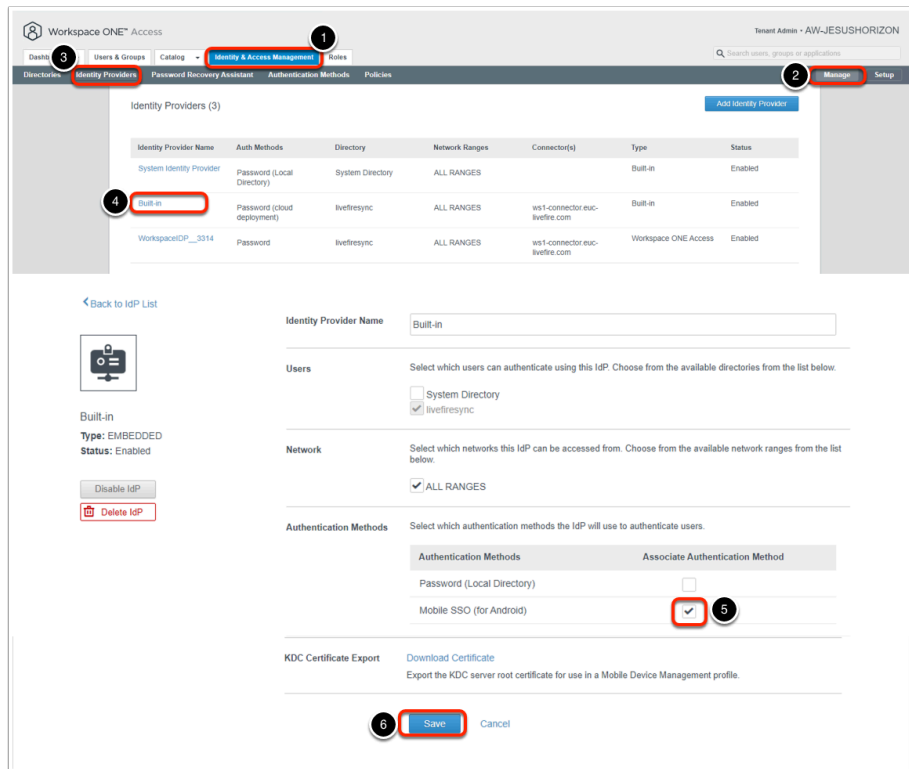
- Below **Thumbprint** select **EXPORT**
- Note the name of the certificate is **TunnelDeviceRootCertificate.cer**
- if you get a security prompt click **Keep**

The screenshot shows the 'Mobile SSO (for Android)' configuration page. At the top, there's a breadcrumb trail: 'Home > Authentication Methods > Mobile SSO (for Android)'. Below this, the title 'Mobile SSO (for Android)' is followed by a pencil icon. The main section is titled 'Mobile SSO (for Android)' and contains several settings:

- Enable Certificate Adapter:** A checkbox that is checked. Below it, a note says 'When enabled, the client cert'.
- Root and Intermediate CA certificates:** A 'Select File' button is highlighted. Below it, a note says 'You can upload multiple DER'.
- Update Auth Adapter:** A dialog box with 'Please click OK to confirm and upload file.' and 'Cancel' and 'OK' buttons. The 'OK' button is highlighted.
- Enable Cert Revocation:** A checkbox that is unchecked. Below it, a note says 'Check box to enable revocation checks'.
- Use CRL from Certificates:** A checkbox that is unchecked. Below it, a note says 'Check box to use the CRL Distribution Points extension of the certifi'.
- CRL Location:** A text input field with a note below it: 'CRL location to use for revocation check (e.g. http://crlurl.crl or file://)'.
- Enable OCSP Revocation:** A checkbox that is unchecked. Below it, a note says 'Check box to use CRL if OCSP fails'.
- Use CRL in case of OCSP failure:** A checkbox that is unchecked. Below it, a note says 'Check box to use CRL if OCSP fails'.
- Enable Cancel Link:** A checkbox that is unchecked. Below it, a note says 'When you enable Cancel, users can click Cancel on the Signing in page to stop Kerberos authentication'.
- Enterprise Device Management Server URL:** A text input field.

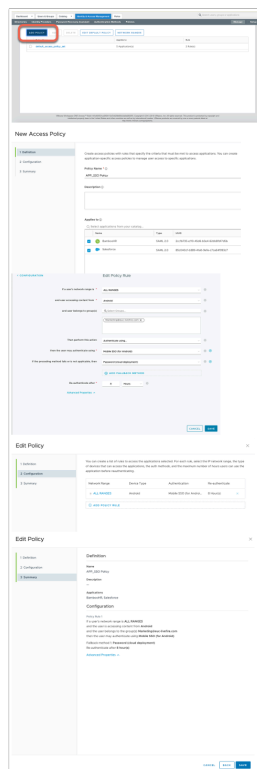
At the bottom right, there are 'Cancel' and 'Save' buttons. The 'Save' button is highlighted with a red box.

- Switch to and if necessary, login to your SaaS instance of **Workspace ONE Access**
  - Select the **Identity & Access Management** tab select **Manage** and then select **Authentication Methods**
  - Under **Authentication methods** select the **Pencil Icon** next to **Mobile SSO (for Android)**
  - On the **Mobile SSO (for Android)** window select the following: Next to
    - **Enable Certificate Adapter:** select the **checkbox**
    - **Root and Intermediate CA certificates** click on the **Select File** button, choose the **TunnelDeviceRootCertificate.cer** file you downloaded earlier and select **Open**.
      - On the **Update Auth adapter** window select **OK**
    - **Use CRL from Certificates :** **Uncheck the checkbox**
    - **Use CRL in case of OCSP failure:** **Uncheck the checkbox**
    - At the bottom of the page select **Save**



## 5. In the Workspace ONE Access Admin Console

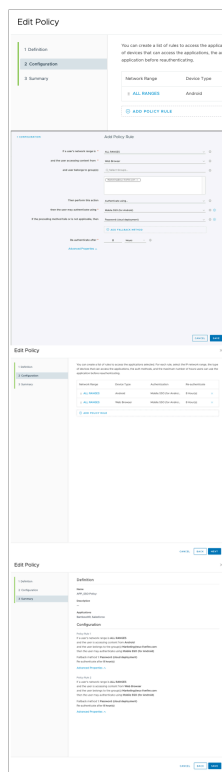
- Select the **Identity & Access Management** tab > **Manage** , select **Identity Providers**
- On the **Identity Providers** window, select **Built-in**
- Under the **Authentication Methods** area select **Mobile SSO (for Android)** checkbox
- Select **Save**





6. In the Workspace ONE Access Admin Console

- On the **Identity & Access Management** tab > **Manage**, select **Policies**
- Select **ADD POLICY**.
- In the **1. Definition** area
  - Enter a policy name: **App\_SSO Policy**
  - Under **Applies to** section, select **Salesforce & BambooHR**.
  - Select **NEXT**,
- In the **2. Configuration** area
  - Select **+ADD POLICY RULE**
    - On the **Add Policy Rule** page add the following, next to:
      - **and user accessing content from \*** : **Android**
      - and user belongs to group(s) : **Marketing@euc-livefire.com**
      - **then the user may authenticate using\*** : **Mobile SSO (for Android)**
      - **if the preceding method fails or is not applicable, then \*** : **Password (cloud deployment)**
    - Select **SAVE**



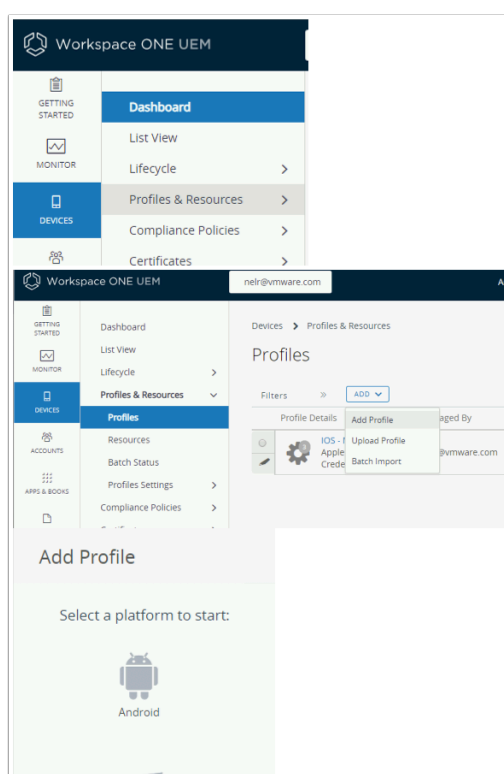
7. In the Workspace ONE Access Admin Console, **Edit Policy** window

- In the **2. Configuration** area
  - Select **+ADD POLICY RULE**
    - On the **Add Policy Rule** page add the following, next to:
      - **and user accessing content from \*** : **Web Browser**
      - and user belongs to group(s) : **Marketing@euc-livefire.com**
      - **then the user may authenticate using\*** : **Mobile SSO (for Android)**

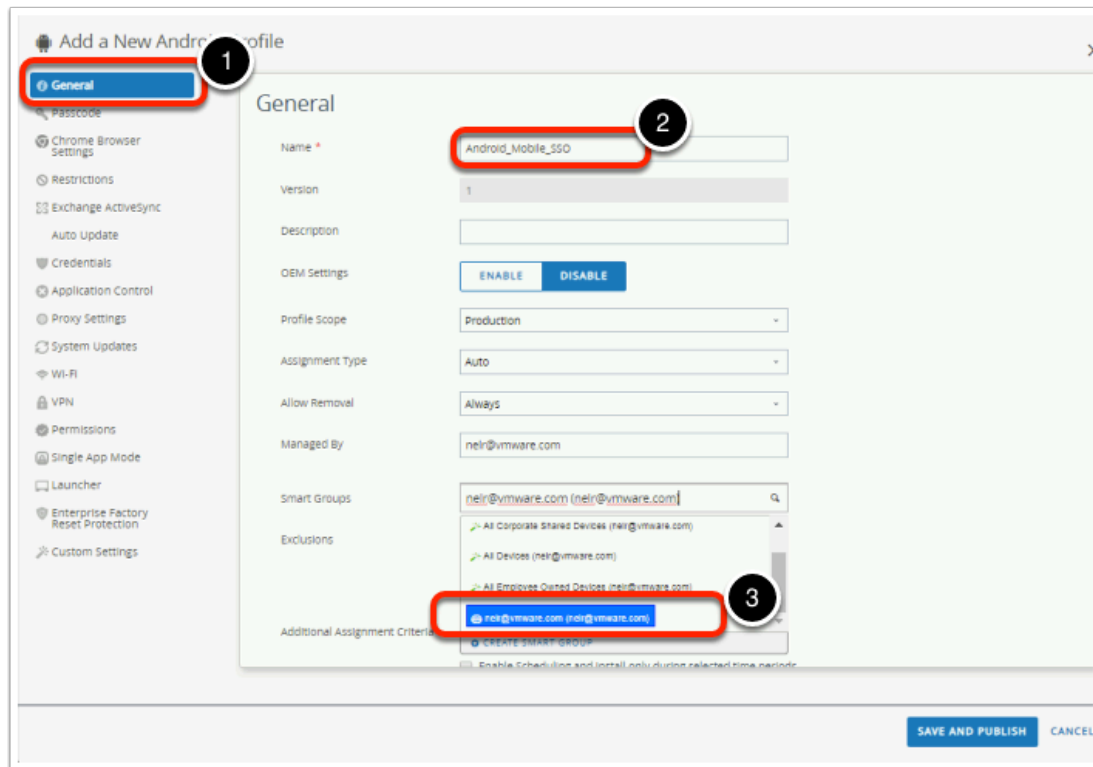
- if the preceding method fails or is not applicable, then \* : Password (cloud deployment)
- Select **SAVE**
- Select **NEXT**
- On the **3. Summary** area, select **SAVE**

## Part 2. Configuring Single-Sign-on for Android: Android VPN Profile

Introduction: We have just configured the Workspace ONE Access Android SSO auth Adaptor, we will now configure the Android VPN profile and add a version to the profile in Workspace ONE UEM.

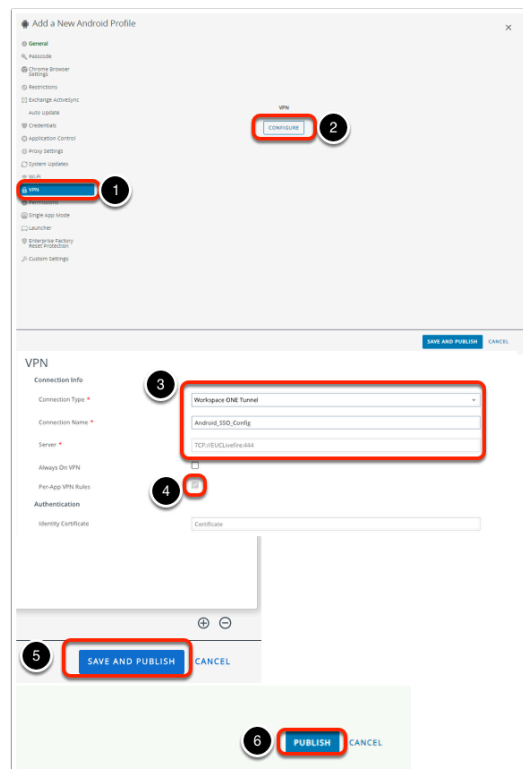


1. **Switch** to your **SaaS Workspace ONE UEM Admin Console**, if necessary **login**
  - Select **Devices** > **Profiles & Resources**
  - Under **Profiles & Resources** select **Profiles** > **ADD** dropdown, then select **Add Profile**
  - On the **Add Profile** window, select **Android**.



## 2. Configuring Single-Sign-on for Android

- In the **Add a New Android Profile** window configure the following...
  - In the left column select **General** and configure only the following: Next to -
    - **Name** type **Android\_Mobile\_SSO**
    - **Smart Groups:** **YOUR ORGANISATIONAL GROUP**. (scroll to the bottom and select the line with the world icon and your OG name)

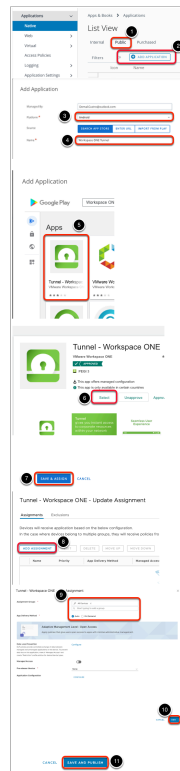


3. In the **Add a New Android Profile** window configure the following...

- In the left column, select **VPN** and select **CONFIGURE**
  - In the **VPN** window configure the following next to:-
    - **Connection Type:** **WorkspaceONE Tunnel**
    - **Connection Name:** **Android\_SSO\_Config**
    - **Server:** (leave default)
    - **Per-App VPN Rules:** **checkbox enabled (default)**
- Select **SAVE AND PUBLISH**
- On **View Device Assignment** window select **PUBLISH**

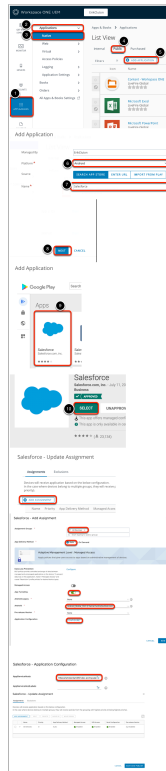
## Part 3: Configuring Android Public applications for a Per App VPN Profile in WorkspaceONE UEM for SSO

This section is dedicated to configuring Workspace ONE UEM to deliver native applications to your Android device



1. In the Workspace ONE UEM Admin Console

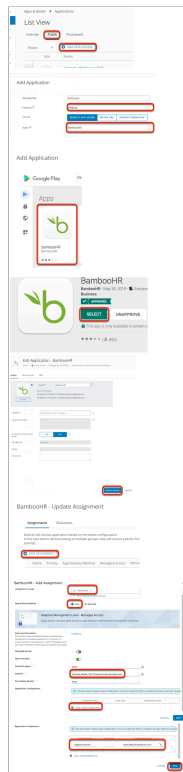
- Select **APPS & BOOKS > Applications > Native > Public** tab
  - Select **+ADD APPLICATION**
    - In the **Add Application** window next to: Select
      - **Platform\***: **Android**
      - **Name\***: **Workspace ONE Tunnel**
      - select **NEXT**
    - In the **Add Application** window select **Tunnel-Workspace ONE**
    - In the **Tunnel - Workspace ONE** section, click the **Select** button
      - Select **SAVE & ASSIGN**
    - On the **Tunnel- Workspace ONE - Update Assignment** window
      - Select **ADD ASSIGNMENT**
    - In the **Tunnel- Workspace ONE - Add Assignment** window next to the following, select:-
      - **Select Assignment Groups:** **All Devices**
      - **App Delivery Method:** **Auto** radio button
      - At the bottom of the page select **ADD**
    - On the **Tunnel- Workspace ONE - Update Assignment** window
      - Select the **radio button** next **All devices**
      - Select **SAVE & PUBLISH**
    - On the **Tunnel- Workspace ONE - Preview Assignment** window
      - Select **PUBLISH**



## 2. Configuring Sales Force for native Android Single Sign-On

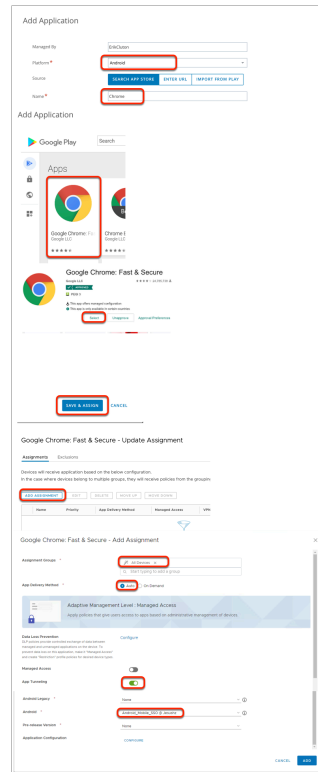
- In the **WorkspaceONE UEM** console, select **APPS & BOOKS** > **Applications** > **Native**
  1. In the **List View** interface select **Public**, select **+ ADD APPLICATION**
  2. In **Add Application** window, select the following, next to:-
    - **Platform\***: **Android**
    - **Name\***: **Salesforce**
  3. At the bottom of the **Add Application** window, select **NEXT**
  4. In the **Add Application** window under **Apps** select **Salesforce**
  5. In the **Add Application** window under **Salesforce** click **Select**
  6. On the **Edit Application - Salesforce** window, select **SAVE & ASSIGN**
  7. On the **Salesforce - Update Assignment** window select **ADD ASSIGNMENT**
  8. On the **Salesforce - Add Assignment** window select and update the following next to:-
    - **Select Assignment Groups**: **All Devices**
    - **App Delivery Method\***: **AUTO**
    - **App Tunneling**: **Enabled**
      - **Android\***: **Android\_Mobile\_SSO**
  9. Next to **Application Configuration** select **CONFIGURE**. You will notice a whole range of additional configurations now become available
  10. Next to **AppServiceHosts**
    - Type in your **custom Salesforce domain**
      - e.g. **https://globalrn01-dev-ed.my.salesforce.com**
    - At the bottom select **SAVE**

11. On the **Salesforce - Add Assignment** window, select **ADD**
12. On the **Salesforce - Update Assignment** window , select **SAVE AND PUBLISH.**
13. On the **Salesforce- Preview Assigned Devices** window select **PUBLISH**



3. Configuring **BAMBOOHR** for native Android Single Sign-On
  1. In the **WorkspaceONE UEM** console, select **APPS & BOOKS > Applications > Native**
    - Under the **Public** select **+ADD APPLICATION**
  2. In **Add Application** window, select the following, next to:-
    - **Platform\*:** **Android**
    - **Name\*:** **BAMBOOHR**
    - Select **NEXT**
  3. In the **Add Application** window under **Apps** select **BambooHR**
  4. In the **Add Application** window under **BambooHR** click **Select**
  5. On the **Edit Application - BambooHR** window, select **SAVE & ASSIGN**
  6. On the **BambooHR - Update Assignment** window select **ADD ASSIGNMENT**
  7. On the **BambooHR - Add Assignment** window select and update the following next to:-
    - **Select Assignment Groups:** **All Devices**
    - **App Delivery Method\*:** **AUTO**
    - **App Tunneling:** **Enabled**
      - **Android\*:** **Android\_Mobile\_SSO**
    - **Under Application Configuration :**select **+ADD CONFIGURATION**
      - Under **Configuration key** type **AppServiceHosts**
      - Under **Value** Type select **String**
      - Under **Configuration Value** type ; **https://customdomain.bamboohr.com .**

- eg. <https://globalrn.bamboohr.com>
  - At the bottom of the **BambooHR - Add Assignment** window select **ADD**
8. On the **BambooHR - Update Assignment** window select **SAVE AND PUBLISH**
  9. On the **Preview Assigned Devices** window select **PUBLISH**
- This application does not support the SDK we will therefore have to manually configure the native application settings on the device



4. Configuring your Chrome Browser for Single-Sign ON
    - Certain Applications like **BambooHR** integrate with your Browser. You will have to configure your browser for single-sign ON as well
1. In the **APPS & BOOKS > Applications > Native > Public** tab continued..
  2. Select **+ADD APPLICATION**
  3. In the **Add Application** window next to: Select
    - **Platform\*** : **Android**
    - **Name\***: **Chrome**
    - select **NEXT**
  4. In the top of the **Add Application** window select **Google Chrome**
  5. In the **Chrome : Fast & Secure**, click on **Select**
  6. In the **Edit Application - Google Chrome**, select **SAVE & ASSIGN**
  7. On the **Google Chrome - Update Assignment** window select **ADD ASSIGNMENT**
  8. In the **Google Chrome - Add Assignment** window next to
    - **Select Assignment Groups:** **All Devices**
    - **App Delivery Method:** **AUTO**
  9. Next to **App Tunneling** select **ENABLED** ( two new sections are added)



- **Android\*** : **Android\_Mobile\_SSO**

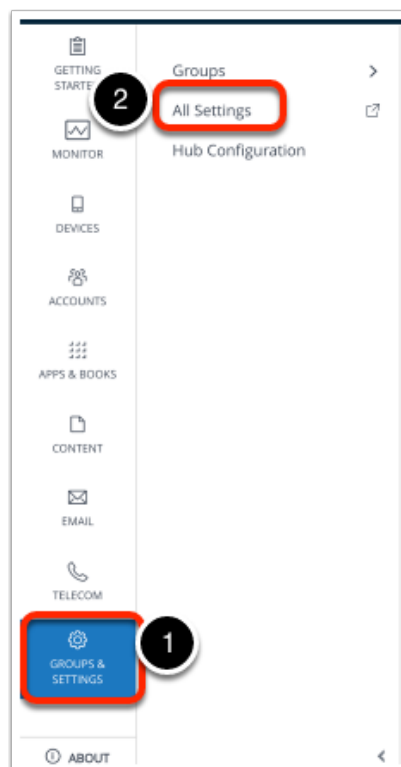
10. At the bottom of the page select **ADD**
11. In the **Google Chrome: Fast & Secure - Update Assignment**, select **SAVE & PUBLISH**
12. In the **Google Chrome: Fast & Secure - Preview Assigned Devices** page, select **PUBLISH**

## Part 4: Configuring VMware Tunnel Component

Configure single sign-on for Android devices to allow users to sign in securely to enterprise apps, without entering their password.

### About this task

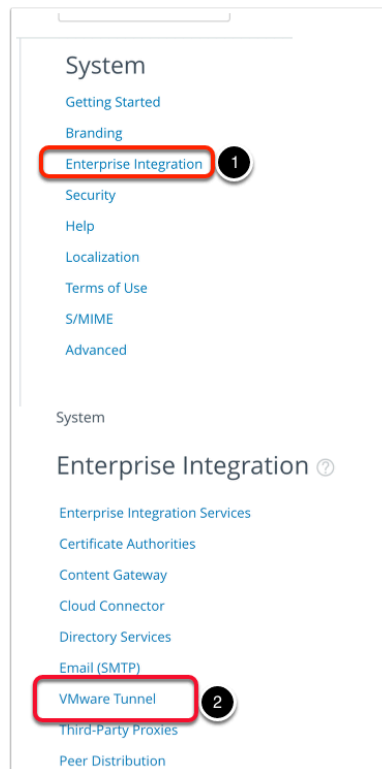
To configure single-sign-on for Android devices, you do not need to configure the VMware Tunnel, but you configure single sign-on using many of the same fields



### 1. Configuring Single-Sign-on for Android

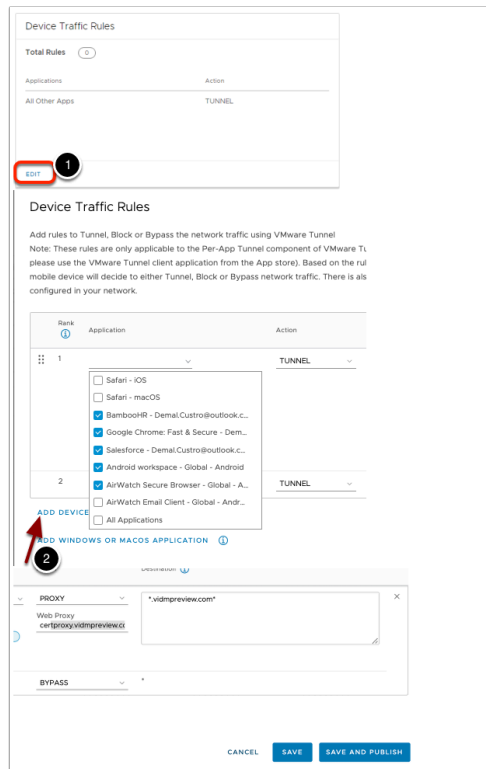
- Ensure you launch your on your Control center desktop and launch your browser to enter <https://dw-livewire.awmdm.com>
- Log into your **Workspace ONE UEM** admin console with your Admin credentials.

- In the **Workspace ONE UEM** admin console, select **GROUPS & SETTINGS**, select **All Settings**



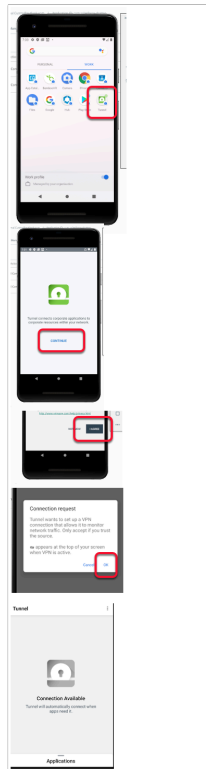
## 2. Configuring VMware Tunnel Component...

- Under **System** select **Enterprise Integration**
- Select **VMware Tunnel**.



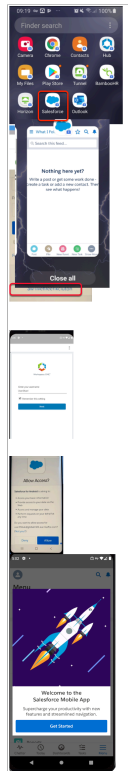
### 3. In the Tunnel Configuration Page

- In the **Device Traffic Rules** section select **EDIT**
  1. To the left of the **Device Traffic Rules** window select **ADD DEVICE TRAFFIC RULE**
  2. Next to **Rank # 1**, under **Application** in the **drop down** select **BambooHR; Chrome ; Salesforce; Android Workspace; Airwatch Secure Browser**
    - Under **Action** from the **dropdown** select **PROXY**
    - Under **Web Proxy** type **certproxy.vidmpreview.com:5262**
    - Under **Destination** type **\*.vidmpreview.com**
  3. Next to **Rank # 2**, under **Application** leave (**all other Apps**) under **Action** select **BYPASS**
  4. Select **SAVE AND PUBLISH**
  5. On the **Are you sure you want to continue?** window select **OK**



4. Switch to your enrolled Android Emulator or physical Android device
  - Wait until all your apps have been deployed on your device. That being **BambooHR; Salesforce & Chrome.**
  - **If you are using the Android Emulator and the salesforce app didnt deploy, your image type may be wrong, go back to the android emulator lab and redeploy your virtual device.** In this article you'll find salesforce official information for android studio [https://developer.salesforce.com/docs/component-library/documentation/en/lwc/lwc.mobile\\_extensions\\_setup\\_android\\_studio](https://developer.salesforce.com/docs/component-library/documentation/en/lwc/lwc.mobile_extensions_setup_android_studio)
  - Select your **WORK** Profile
  - Select your **Tunnel** Application
    - In the Tunnel application, select **CONTINUE**
    - In the **Privacy** window, select **I UNDERSTAND**
    - In **Data Sharing** window, select **I AGREE**
    - On the **Connection request** window, select **OK**
- Wait until all your apps have been deployed on your device. That being **BambooHR; Salesforce & Chrome.**
- Look to be prompted for the following message : **Connection request. Tunnel wants to set up a VPN connection....** You have the option to select **Cancel** and **OK**. Select **OK**

## Part 5: Testing Mobile SSO for Android



### 1. Testing **Mobile SSO for Salesforce**

- On your Android device, choose your **Work** profile
  1. Select the **Salesforce icon**
  2. On the terms and conditions select **I AGREE**
  3. On your login notice you have the option at the bottom **OR Log in using: your custom domain**. Select **your custom domain**
  4. In the Workspace ONE Auth window, under Enter your username type your custom username,
    - Select the **Remember this setting, checkbox**
    - Select **Next**
  5. In the **Salesforce for Android** window select **Allow**
  6. Notice you are now in your Salesforce application for the first time. Close the application and re-open.



## 2. Testing Mobile SSO for BambooHR

- On your **Android** Device select your **BambooHR** application
  1. In the **bambooHR** window type in your **custom domain** in the **yourdomain.boomboohr.com** section
    - eg. **globalrn.bamboohr.com**
    - select **Continue**
  2. Select the **LOG IN** button
  3. On the **Welcome to Chrome** window select **Accept & Continue**
  4. On the **Sign in to Chrome** select **No thanks**
  5. On the **Workspace ONE** console enter your **username** and select **Next**.
  6. Notice you were logged in without a need to provide password. This means Mobile Single Sign on was successful.

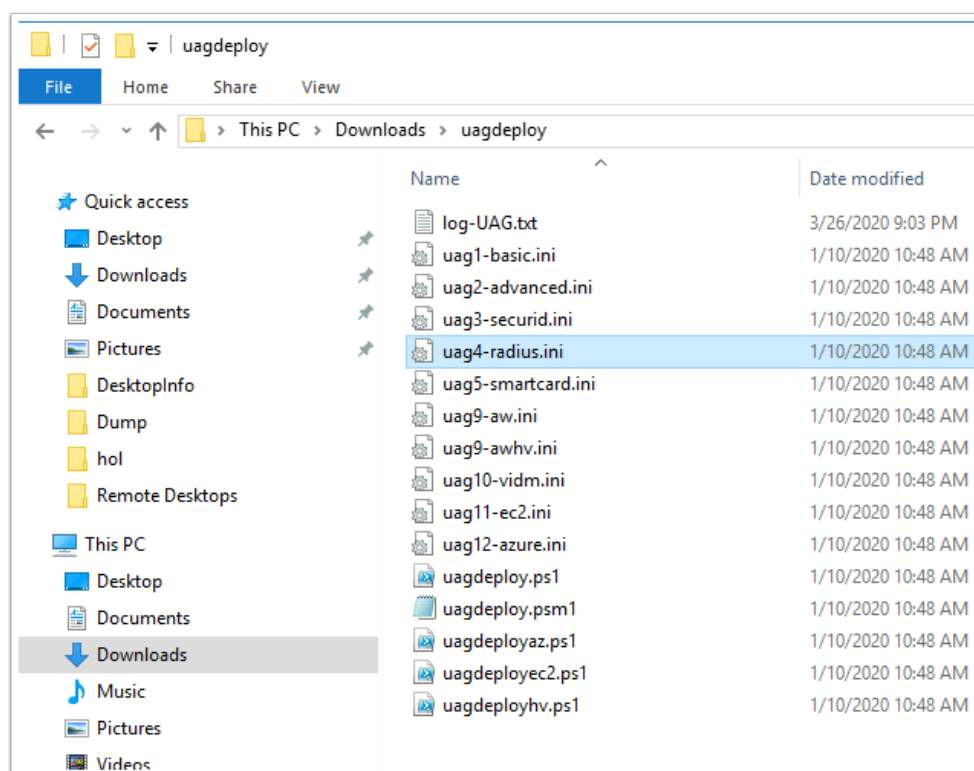
Proceed to the next lab.

# Day 3

# Unified Access Gateway deployment using the PowerShell

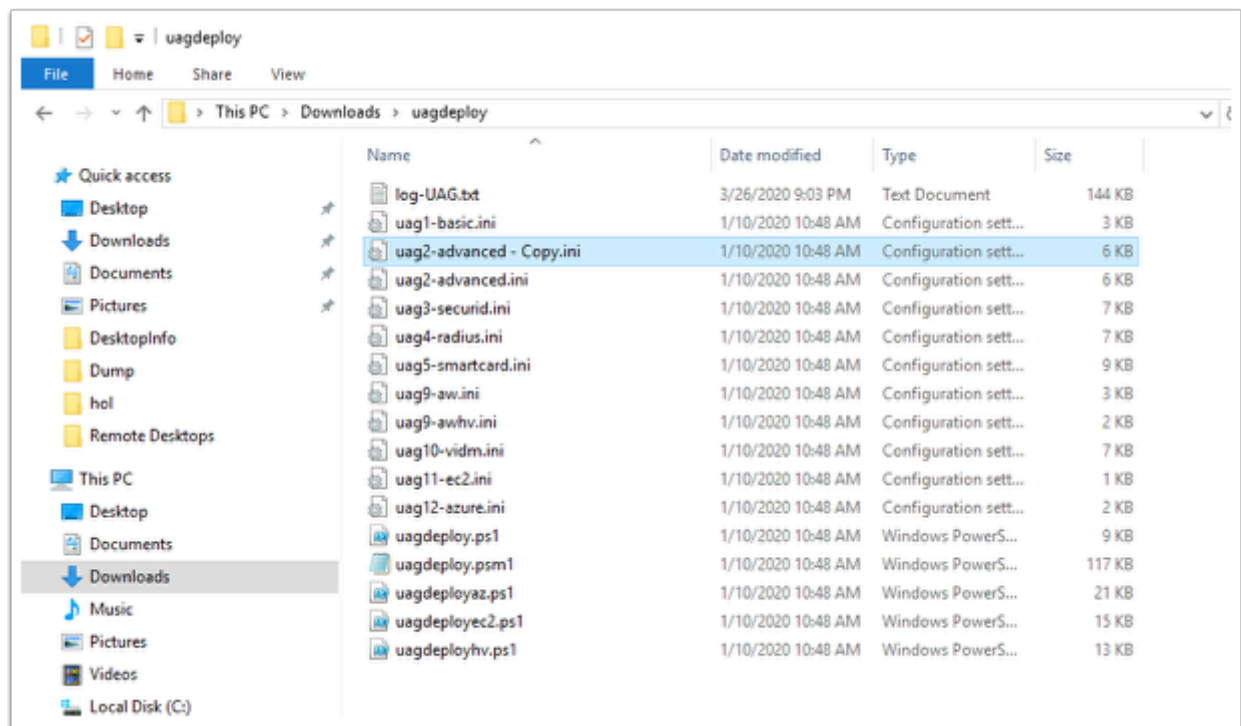
## PART 1

This is an overview of deploying the Unified Access Gateway script for VMware Horizon

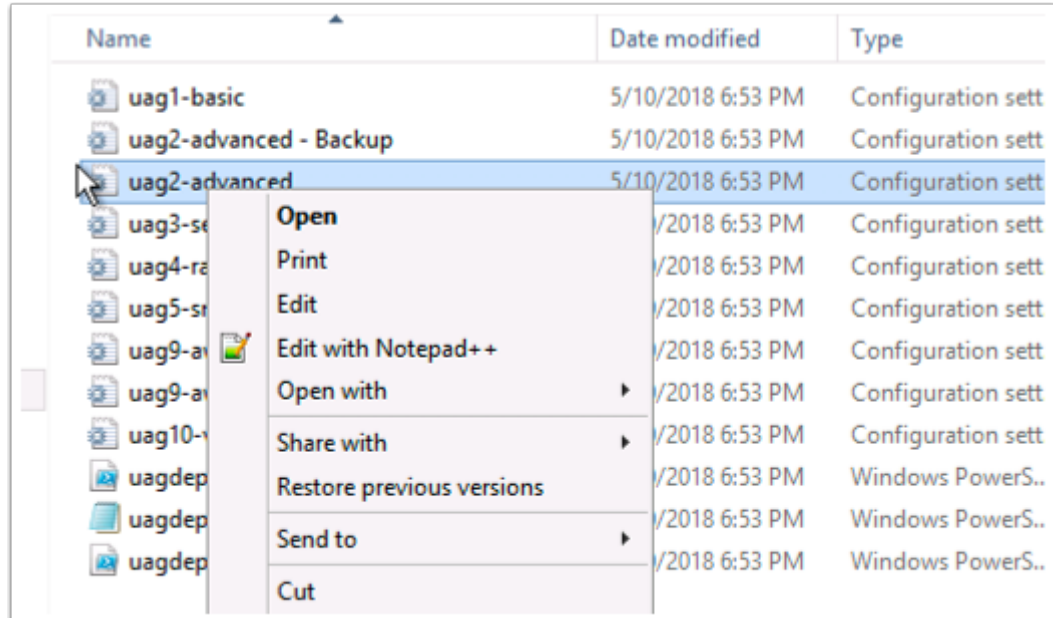


1. On the **ControlCenter2** server, go the **downloads** folder and select the **uagdeploy** folder and observe the contents





2. Select the **uag2-Advanced.ini**,
  - **Copy and Paste** so that you have a backup of the original file .



3. Select **uag2-advanced** and then select **Edit with Notepad++**

```

# UAG virtual appliance unique name (between 1 and 32 characters).
# If name is not specified, the script will prompt for it.
#
name=UAG-HZN
#
# Full path filename of the UAG .ova virtual machine image
# The file can be obtained from VMware
#
source=\\cs1-pd1.euc-livfire.com\\software\\UAG\\euc-unified-access-gateway-20.09.0.0-16926381_OVF10.ova
#
# target refers to the vCenter username and address/hostname and the ESXi host for deployment
# Refer to the ovftool documentation for information about the target syntax.
# See https://www.vmware.com/support/developer/ovf/
# PASSWORD in upper case results in a password prompt during deployment so that passwords do not need
# to specified in this .INI file.
# In this example, the vCenter username is administrator@vsphere.local
# the vCenter server is 192.168.0.21 (this can be a hostname or IP address)
# the ESXi hostname is esxi.myc0.int (this can be a hostname or IP address)
#
target=vi://administrator@euc-livfire.com:PASSWORD@192.168.110.22/RegionA01/host/RegionA01-COMP01/esxi-01a.euc-livfire.com
#

```

#### 4. In the NotePad++ application

- Next to **name** change to **UAG-HZN**
- Next to **source** change

```
source=\\cs1-pd1.euc-livfire.com\\software\\UAG\\euc-unified-access-gateway-20.09.0.0-16926381_OVF10.ova
```

- Next to **target** change it to:

```
target=vi://administrator@euc-livfire.com:PASSWORD@192.168.110.22/RegionA01/host/RegionA01-COMP01/esxi-01a.euc-livfire.com
```

```

33
34 ds=CorpLUN01
35
36 #
37 # Disk provisioning mode. Refer to OVF Tool doc
38 #
39
40 diskMode=thin
41
42 #
43 # vSphere Network names. For pre 3.3 UAG versions
44 # network settings such as IPv4 subnet mask, CIDR
45 # value must be specified for each NIC. Normal
46 #
47
48 netInternet=VL-DMZ
49 netManagementNetwork=VL-DMZ
50 netBackendNetwork=VL-DMZ
51
52 defaultGateway=172.16.20.1
53
54 deploymentOption=onenic
55 ip0=172.16.20.11
56 netmask0=255.255.255.0
57 routes0=172.16.20.0/24 172.16.20.1
58
59 #deploymentOption=twonic
60 #ip0=192.168.0.10

```

5. **Scroll down** in your NotePad++ window

- Next to **ds=Local Disk 1** change to **ds=CorpLUN01**
- Next to **#diskMode=thin** change to **diskMode=thin**
- Change the following network settings to:
  - **netInternet=VL-DMZ**
  - **netManagementNetwork=VL-DMZ**
  - **netBackendNetwork=VL-DMZ**
  - **defaultGateway=172.16.20.1**
  - **deploymentOption=onenic**
  - **ip0=172.16.20.11**
  - **netmask0=255.255.255.0**
  - **routes0=172.16.20.0/24 172.16.20.1**

```
70 #ip1=192.168.0.91
71 #netmask1=255.255.255.0
72 #ip2=192.168.0.92
73 #netmask2=255.255.255.0
74 #routes0=192.168.1.0/24 192
75 #routes1=192.168.3.0/24 192
76 #routes2=192.168.5.0/24 192
77
78 dns=192.168.110.10
79
80 #syslogUrl=syslog://server.
81
82 #
83 # Setting honorCipherOrder 1
84 # UAG 2.7.2 and newer to fo
85 #
```

## 6. Scroll Down

- Change **dns=192.168.0.10** to

```
dns=192.168.110.10
```

```
97
98  [SSLCert]
99
100  #
101  # From UAG 3.0 and newer, you can specify
102  # any required intermediate certificates
103  # associated PEM certificates file and P
104  #
105
106  pfxCerts=C:\certificates\WildCard.pfx
107
108  #
109  # If there are multiple SSL certificates
110  # This is not necessary if there is only
```

7. Under **[SSLCert]** Change **pfxCerts=sslcerts.pfx** to

```
pfxCerts=C:\certificates\WildCard.pfx
```

```
133  #
134
135  [SSLCertAdmin]
136
137  pfxCerts=C:\certificates\WildCard.pfx
138  #pemCerts=sslcerts.pem
139  #pemPrivKey=sslcertsakey.pem
140
141  [Horizon]
142
```

8. In the **[SSLCertAdmin]** section , change **pfxCerts=sslcerts.pfx** to

```
pfxCerts=C:\certificates\WildCard.pfx
```

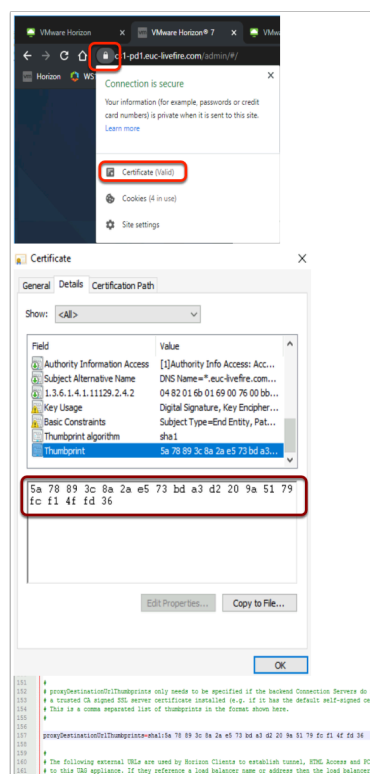
```

141 [Horizon]
142
143 #
144 # proxyDestinationUrl refers to the backend Connection Server
145 # It can either specify the name or IP address of an individual
146 # via a load balancer in front of multiple Connection Servers
147 #
148
149 proxyDestinationUrl=https://cs1-pd1.euc-livefire.com
150
151 #
152 # proxyDestinationUrlThumbprints only needs to be specified
153 # a trusted CA signed SSL server certificate installed (e.g.
154 # This is a comma separated list of thumbprints in the format
155 #

```

9. Under the **[Horizon]** section change **proxyDestinationUrl=https://192.168.0.209** to

**proxyDestinationUrl=https://cs1-pd1.euc-livefire.com**



10. On your **ControlCenter**, open your **Google Chrome Browser**, using **Horizon shortcut** in the address bar launch the **Horizon Administrator admin** console.

- In the Address Bar select and click on the **briefcase icon**.
- Click on **Certificate (Valid)**

- Select the **Details** tab and scroll down and select **Thumbprint**. Use your **keyboard** to copy the thumbprint by selecting **CTRL+C**. Switch back to your **Advanced.ini** file in Notepad++
- Using the thumbprint you have just copied, change the Hash in the **#proxyDestinationUrlThumbprints=sha1:3e ef ed c6 86 75 a6 15 ff c8 96 27 5a 4c ee 8e 16 fd 6e d3,sha1:3e ef ed c6 86 75 a6 15 ff c8 96 27 5a 4c ee 8e 16 fd 6e d3** section to

```
proxyDestinationUrlThumbprints=sha1:5a 78 89 3c 8a 2a e5 73 bd a3 d2 20 9a 51 79 fc f1
4f fd 36
```

```
160 # The following external URLs are used by Horizon Clients
161 # to this UAG appliance. If they reference a load balancer
162 # configured for source IP hash affinity otherwise the con
163 #
164
165 tunnelExternalUrl=https://uag-hzn.euc-livefire.com:443
166 blastExternalUrl=https://uag-hzn.euc-livefire.com:443
167
168 #
169 # pcoipExternalUrl must contain an IPv4 address (not a DNS
170 #
```

## 11. **Scroll down** and Change

- **tunnelExternalUrl=https://uag2.horizon.myco.com:443**
- **blastExternalUrl=https://uag2.horizon.myco.com:443**

To

```
tunnelExternalUrl=https://uag-hzn.euc-livefire.com:443
blastExternalUrl=https://uag-hzn.euc-livefire.com:443
```

```

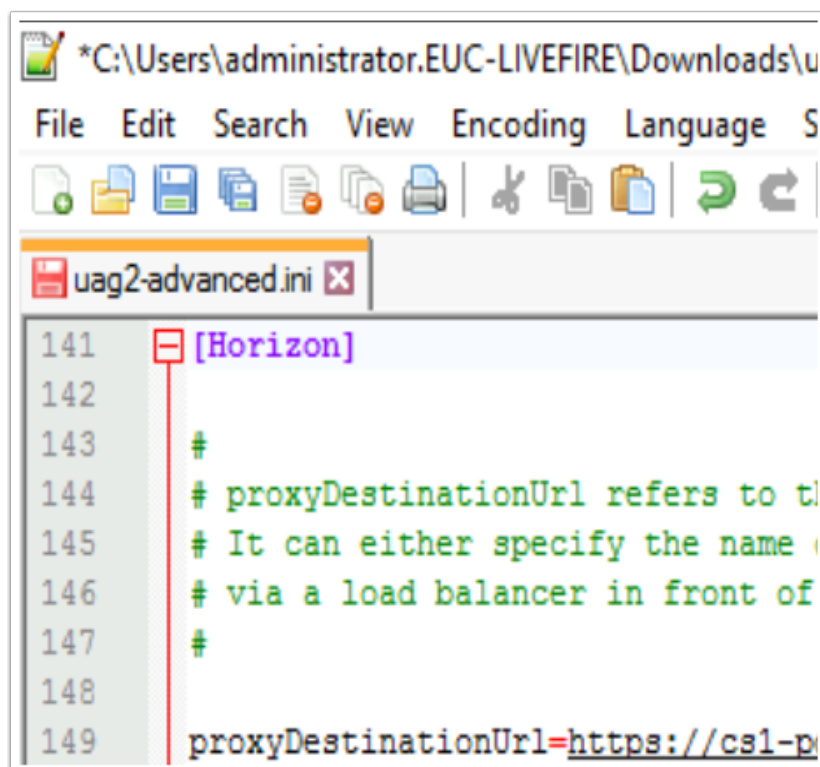
168 #
169 # pcoipExternalUrl must contain an IPv4 address
170 #
171
172 pcoipExternalUrl=172.16.20.11:4172
173 pcoipDisableLegacyCertificate=true
174
175
176

```

# 11. Scroll down and Change

- In the **pcoipExternalUrl** section change **pcoipExternalUrl=10.20.30.90:4172** to:

```
pcoipExternalUrl=172.16.20.11:4172
```

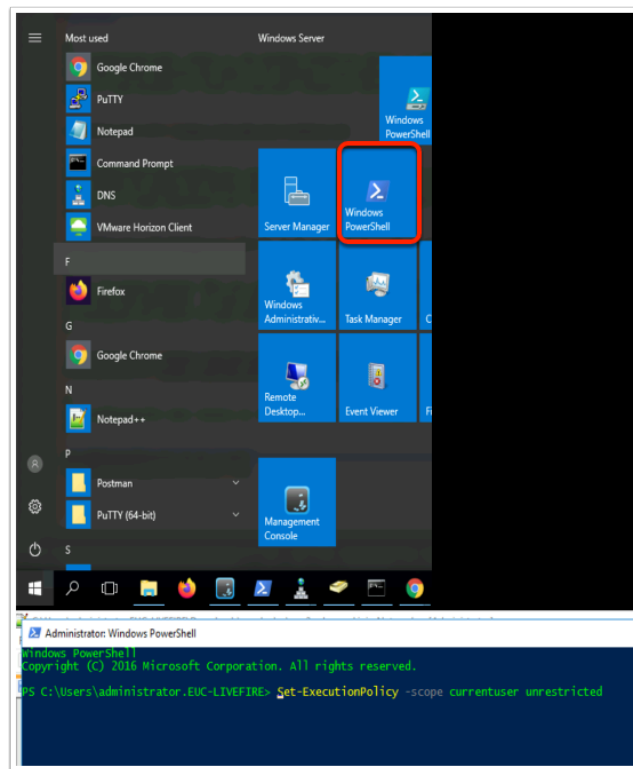


# 12. SAVE THE .ini File before running the powershell command.

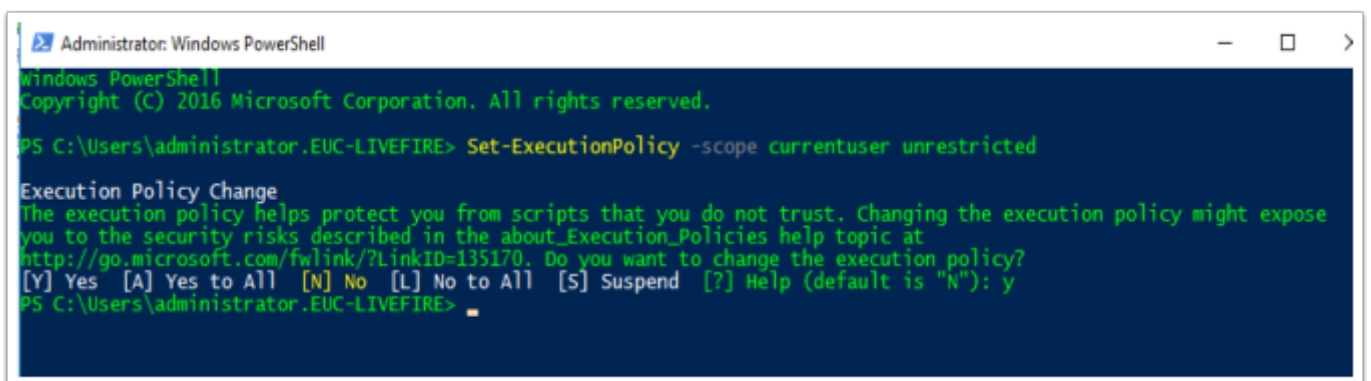


## Part 2

In this section, we will deploy the Unified Access Gateway using a Powershell Script



1. On your **ControlCenter2** server , launch the **powershell** shortcut from the **Start Menu**



2. We will set the script execution is set to unrestricted. Execute the following command.

```
Set-ExecutionPolicy -scope currentuser unrestricted
```

When Prompted select Y

```
PS C:\Users\administrator.EUC-LIVEFIRE> cd downloads\uagdeploy
PS C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy> █
```

3. Within the powershell interface type the following command

```
cd downloads\uagdeploy
```

```
PS C:\Users\administrator.EUC-LIVEFIRE> cd downloads\uagdeploy
PS C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy> .\uagdeploy.ps1 -iniFile uag2-advanced.ini

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy\uagdeploy.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy\uagdeploy.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r
Unified Access Gateway (UAG) virtual appliance deployment script
Enter a root password for UAG-HZN: *****
Re-enter the root password: ***** █
```

4. Execute the following command

```
.\uagdeploy.ps1 -iniFile uag2-advanced.ini
```

- When you get a security warning type: **R**
- When you get a second security warning type: **R**
- When prompted to **enter a root password for UAG-HZN**,
  - type: **VMware1!**
  - when prompted to confirm type **VMware1!**

```

Enter an optional admin password for the Admin UI and REST API management access for UAG-HZN: *****
Re-enter the admin password: *****
Join the VMware Customer Experience Improvement Program?

This setting is supported in UAG versions 3.1 and newer.

VMware's Customer Experience Improvement Program (CEIP) provides VMware with information that enables VMware to
improve its products and services, to fix problems, and to advise you on how best to deploy and use our products.

As part of the CEIP, VMware collects technical information about your organization's use of VMware products and
services on a regular basis in association with your organization's VMware license key(s). This information does
not personally identify any individual.

Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware
is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

If you prefer not to participate in VMware's CEIP for UAG 3.1 and newer, you should enter no.

You may join or leave VMware's CEIP for this product at any time. In the UAG Admin UI in System Configuration,
there is a setting 'Join CEIP' which can be set to yes or no and has immediate effect.

To Join the VMware Customer Experience Improvement Program with Unified Access Gateway version 3.1 and newer,
either enter yes or just hit return as the default for this setting is yes.
Join CEIP for UAG-HZN ? (default is yes for UAG 3.1 and newer): No
Enter the password for the specified [SSLcert] PFX certificate file WildCard.pfx:

```

5. When prompted to

- Enter an optional admin password for the RESP API management access for UAG: type **VMware1!**
- When prompted to **Re-Enter an optional admin password** : type **VMware1!**
- When prompted whether or not to join the customer experience program type **No**

```

Join CEIP for UAG-HZN ? (default is yes for UAG 3.1 and newer): No
Enter the password for the specified [SSLcert] PFX certificate file WildCard.pfx: *****
Enter the password for the specified [SSLcertAdmin] PFX certificate file WildCard.pfx: *****
Opening OVA source: \\cs1-pd1.euc-livfire.com\software\UAG\euc-unified-access-gateway-3.10.0.0-16455273_OVF10.ova
The manifest validates
Source is signed and the certificate validates
Enter login information for target vi://192.168.110.22/
Username: administrator%40euc-livfire.com
Password:
Enter login information for target vi://192.168.110.22/
Username: administrator%40euc-livfire.com
Password: *****
Enter login information for target vi://192.168.110.22/
Username: administrator%40euc-livfire.com
Password: *****
Opening VI target: vi://administrator%40euc-livfire.com@192.168.110.22:443/Livfire/host/RegionA02-COMP02/
livefire.com
Deploying to VI: vi://administrator%40euc-livfire.com@192.168.110.22:443/Livfire/host/RegionA02-COMP02/e
livefire.com
Disk progress: 17%

```

6. When prompted to

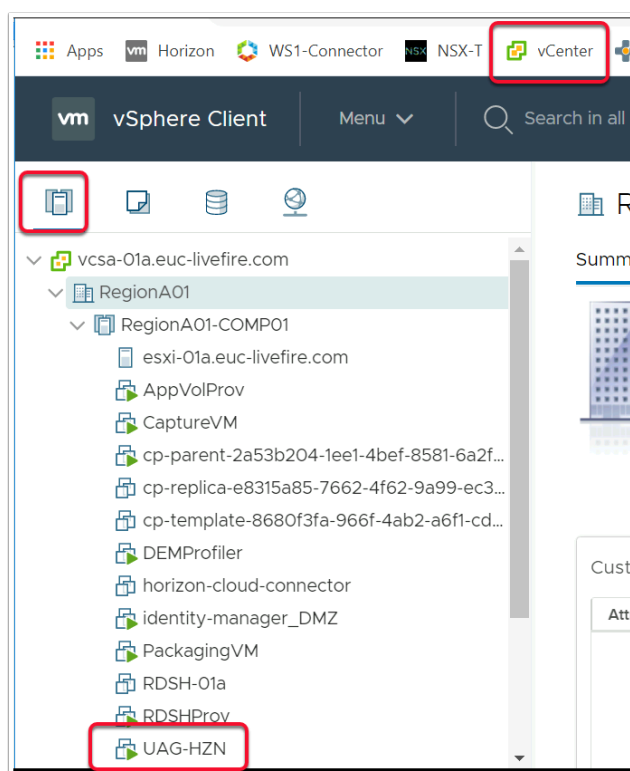
- Enter password for the **.pfx** type: **VMware1!**,
- When prompted to **confirm** type **VMware1!** again.
- When prompted the password for **administrator@euc-livfire.com**
  - Type **VMware1!**
- **Your virtual Appliance deployment will now start , it will take between 5 - 10min to deploy. Proceed to step 8**

```

Deploying to VI: vi://administrator@euc-livefire.com@192.168.110.22:443/RegionA01/host/RegionA01-COMP01/esxi-01a.euc-
livefire.com
Transfer Completed
Powering on VM: UAG-HZN
Task Completed
Received IP address: 172.16.20.11
Completed successfully
Note that the IP addresses will be set to the specified IP addresses for each NIC
UAG virtual appliance UAG-HZN deployed successfully
MPS C:\Users\administrator.EUC-LIVEFIRE\downloads\uagdeploy>

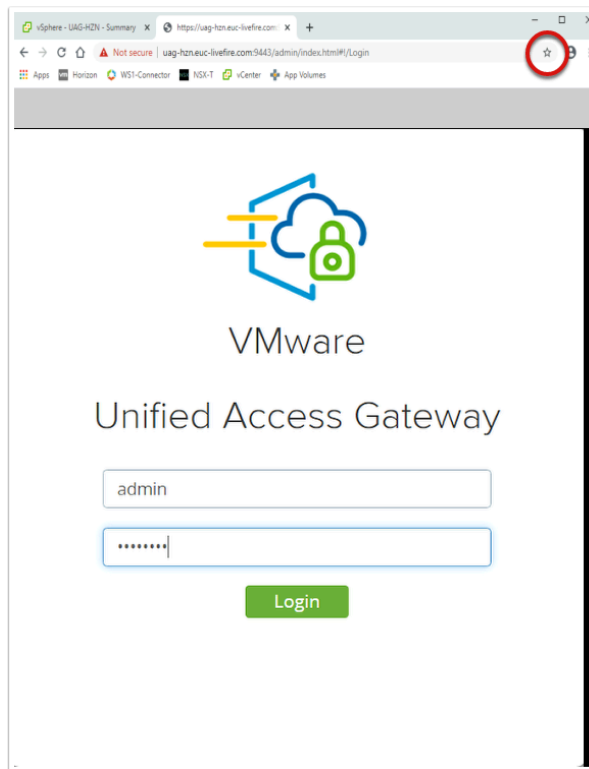
```

## 7. Review the deployment once the setup has completed



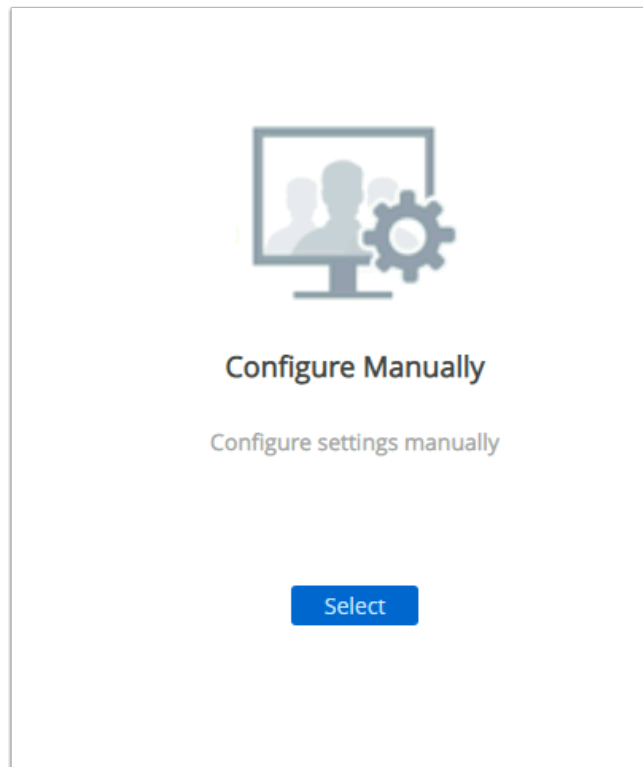
## 8. On your ControlCenter2 server

- Open your **Chrome Browser**. Select the **vCenter** shortcut
  - Login as **administrator** with the password **VMware1!**
  - Select the **Host & Clusters** icon
  - In **Host & Clusters**, expand the **inventory** under **RegionA01-COMP01**
- Switch Back to your Powershell window to check if the deployment has completed.

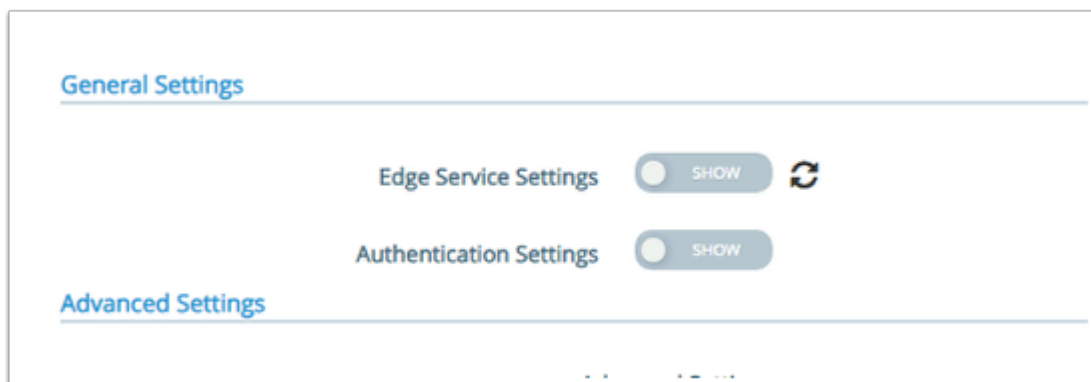


9. On your **Controlcenter2** server

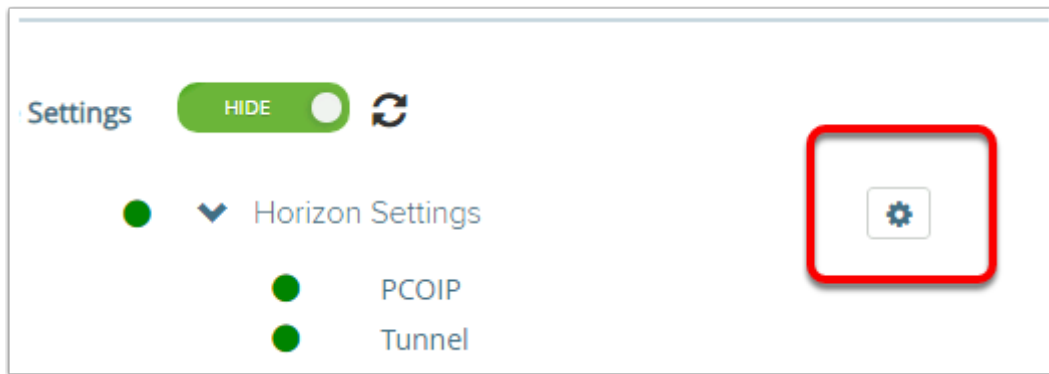
- On your **Chrome Browser** open a **new Tab**
- Enter the following URL into the address bar
  - <https://uag-hzn-euc-livewire.com:9443/admin/index.html#!/Login>
- In the right of your Chrome Browser . Add the following URL as Favourite in your Bookmarks, by selecting the **STAR**.
- Login to your UAG server by entering the following
  - **Admin Username :** [admin](#)
  - **Admin Password:** [VMware1!](#)
  - Select **Login**



10. On your UAG Admin Console
- Click the **Select** button under **Configure Manually**

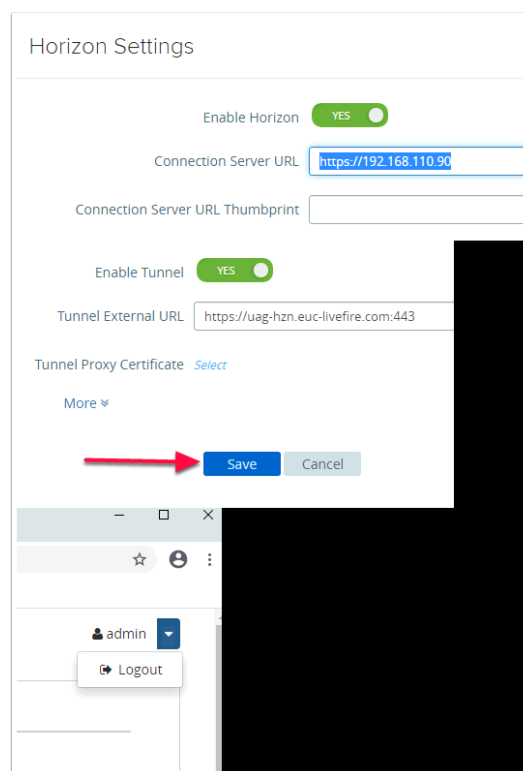


11. On your UAG Admin Console
- Under **General Settings**
    - Next to **Edge Service Settings**, move the **toggle** to the right



12. On your UAG Admin Console

- To the right of **Horizon Settings**, select the **Gearbox**



13. In your UAG Admin Console

- Under **Horizon Settings**
  - Edit the **Connection Server URL**, change **https://192.168.110.90** to
    - **Connection Server URL** : <https://cs1-pd1.euc-livefire.com>
    - Select **Save**
    - **Logout** from the UAG Admin Console

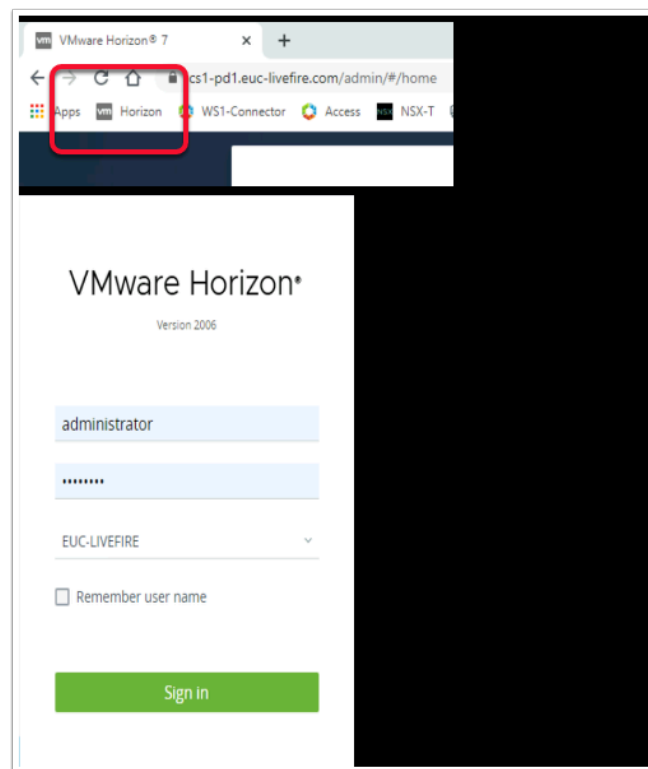
This concludes the deployment of the Unified Access Gateway using a Powershell Script

# Horizon integration into Workspace ONE Access

## Overview

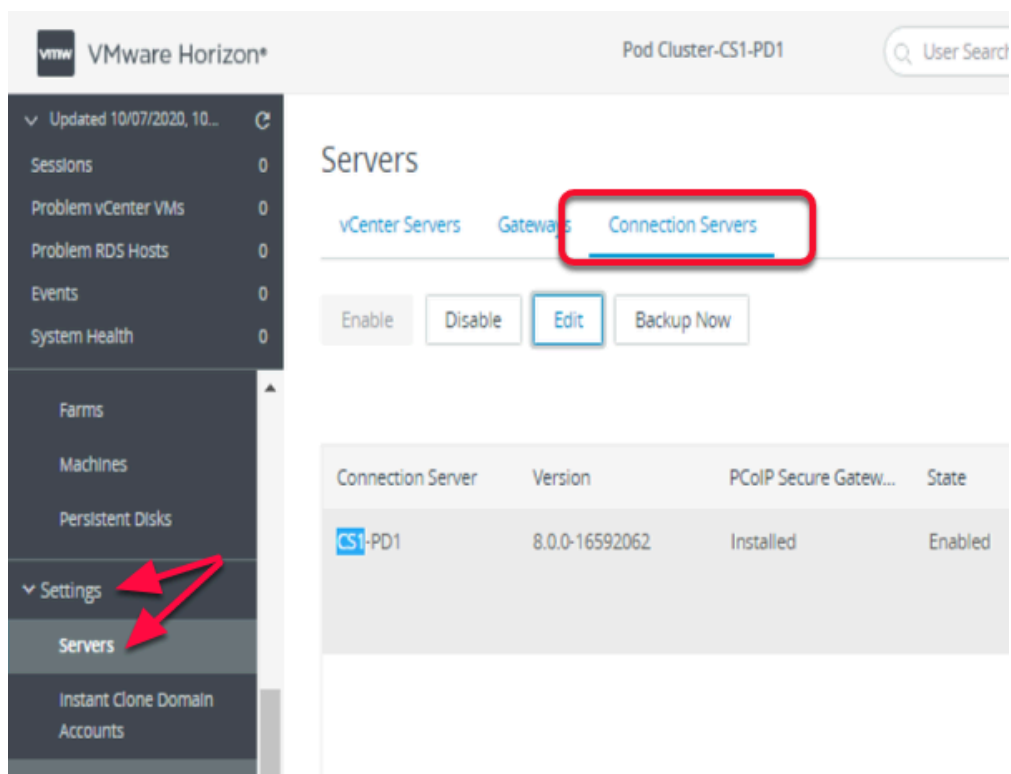
- Federating VMware Horizon with Workspace ONE Access

## Configuring Workspace ONE Access and Horizon Integration

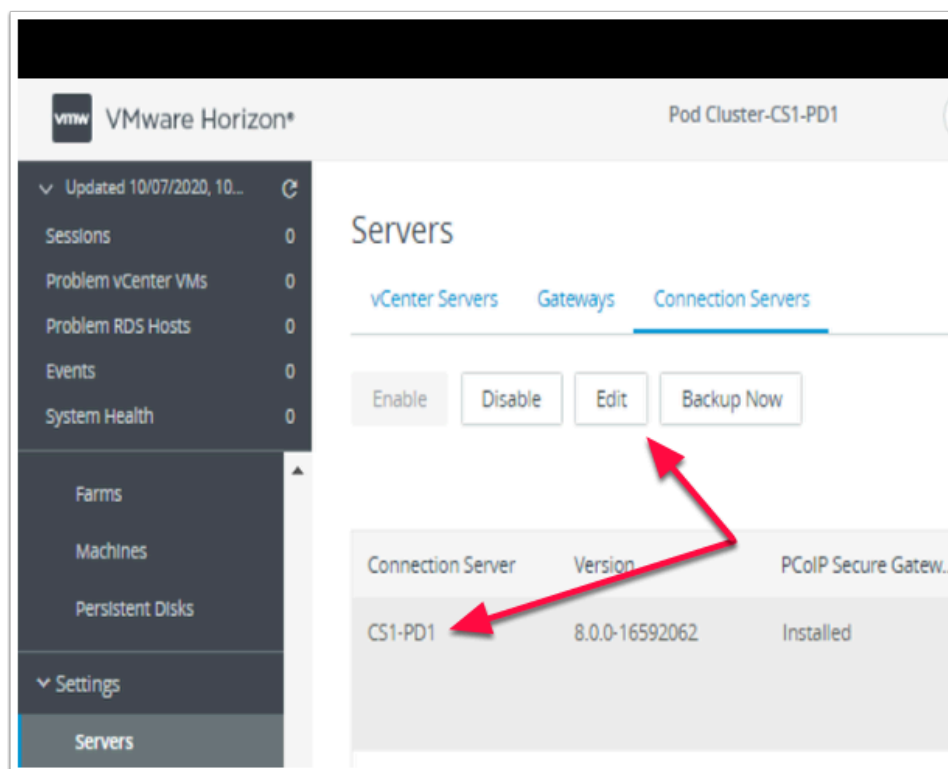


1. On your **ControlCenter2** desktop open your **Google Chrome browser**
  - Select the **Horizon shortcut** for **Horizon administrator**
  - In the **User Name** area login as **administrator**
    - In the **Password** area type **VMware1!**
  - Select **Sign in**





2. Expand **Settings**,
  - Select **Servers**
  - Select the **Connection Servers** Tab



3. Select **CS1-PD1** select **Edit**

## Edit Connection Server Settings

General
Authentication

---

**Tags**

Tags can be used to restrict which desktop pools can be accessed through this Connection Serv

**Tags**

Separate tags with ; or ,

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

## Edit Connection Server Settings

General
Authentication

---

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

Disabled
Disabled
**Allowed**
Required

Manage SAML Authenticators

---

**General**

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

Allowed

SAML Authenticator

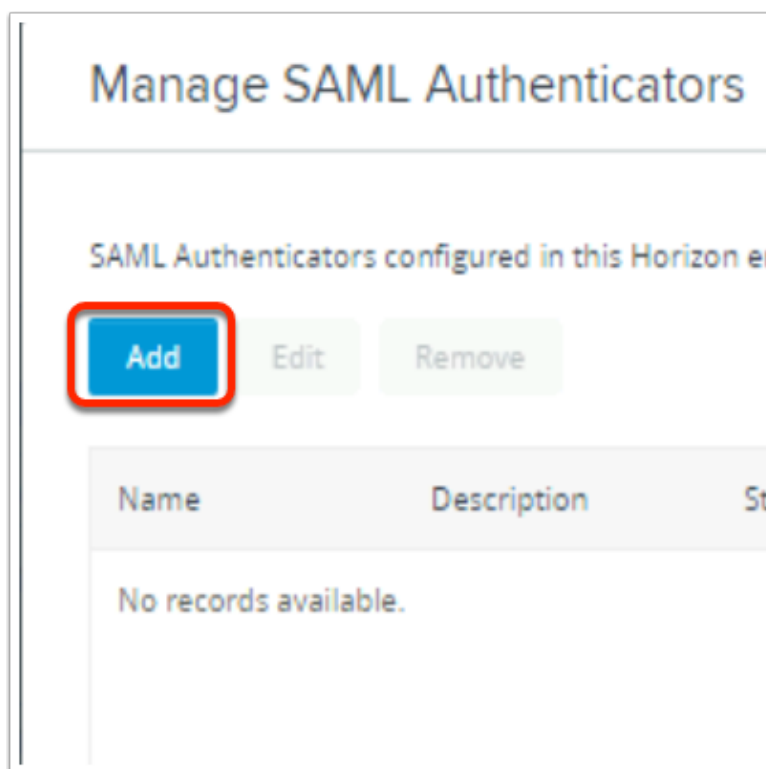
No Enabled Authenticator configured

Manage SAML Authenticators

Create at least one SAML Authenticator and enable it, f

☐ Enable Workspace ONE mode ⓘ

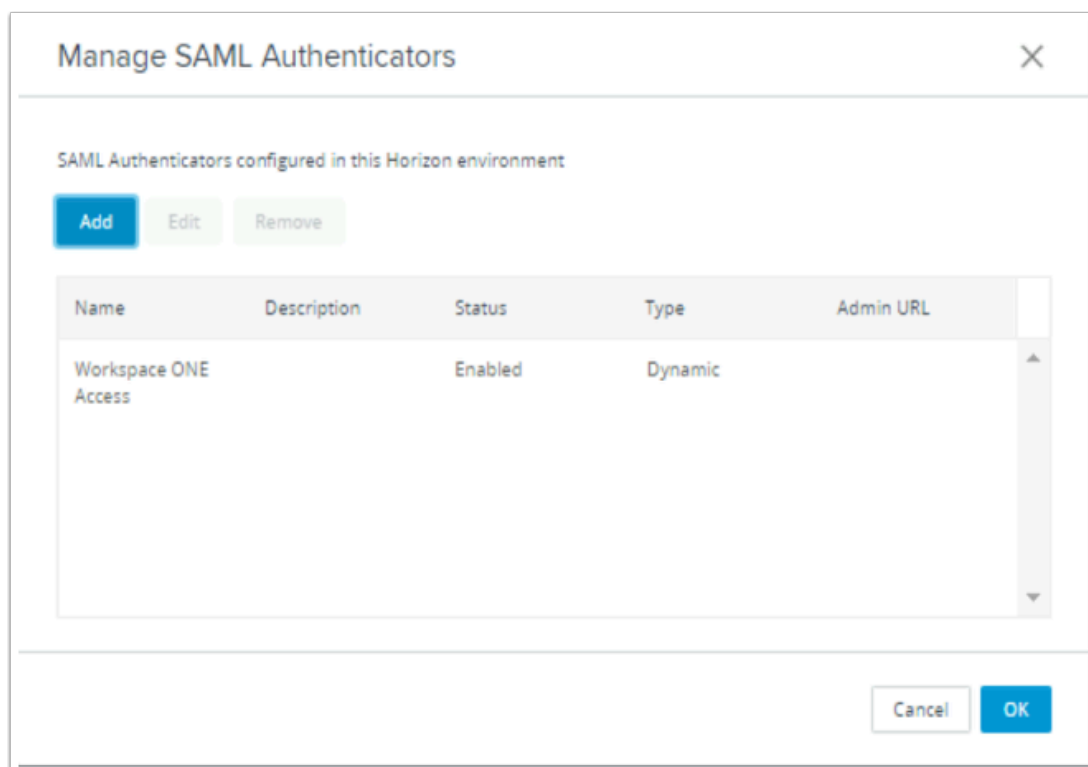
- On the Authentication tab, **Under Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):**
  - On the **Drop down Arrow** Select **Allowed**,
  - Select the **Manage SAML Authenticators** box



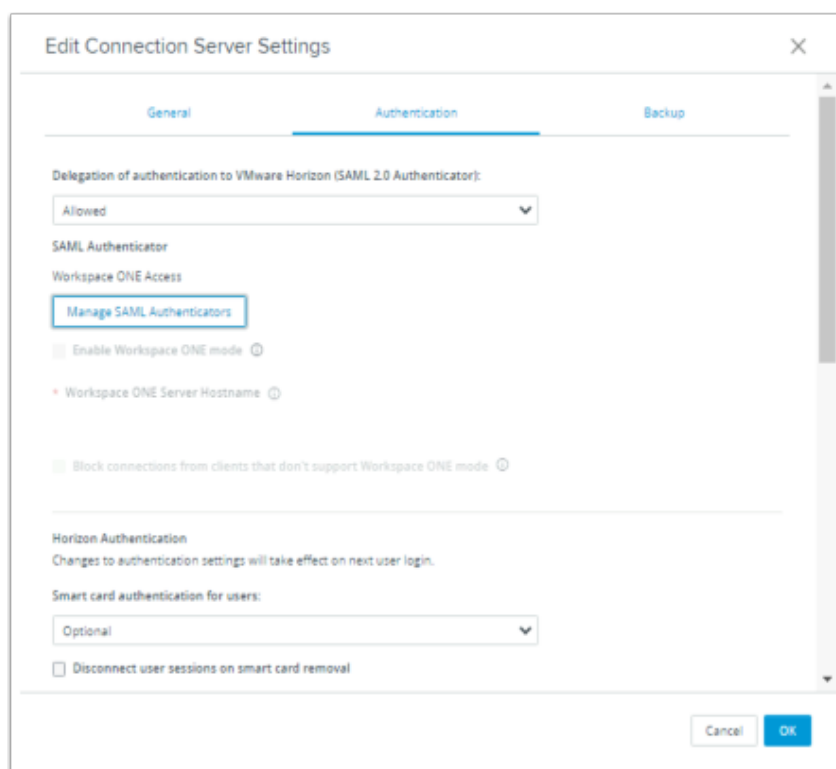
6. On the **Manage SAML Authenticators** box select **Add**

7. In the **Add SAML 2.0 Authenticator** window. Ensure **Dynamic** radio button is selected,
- Enter the following:
    - Under **Label:** type **Workspace ONE Access**

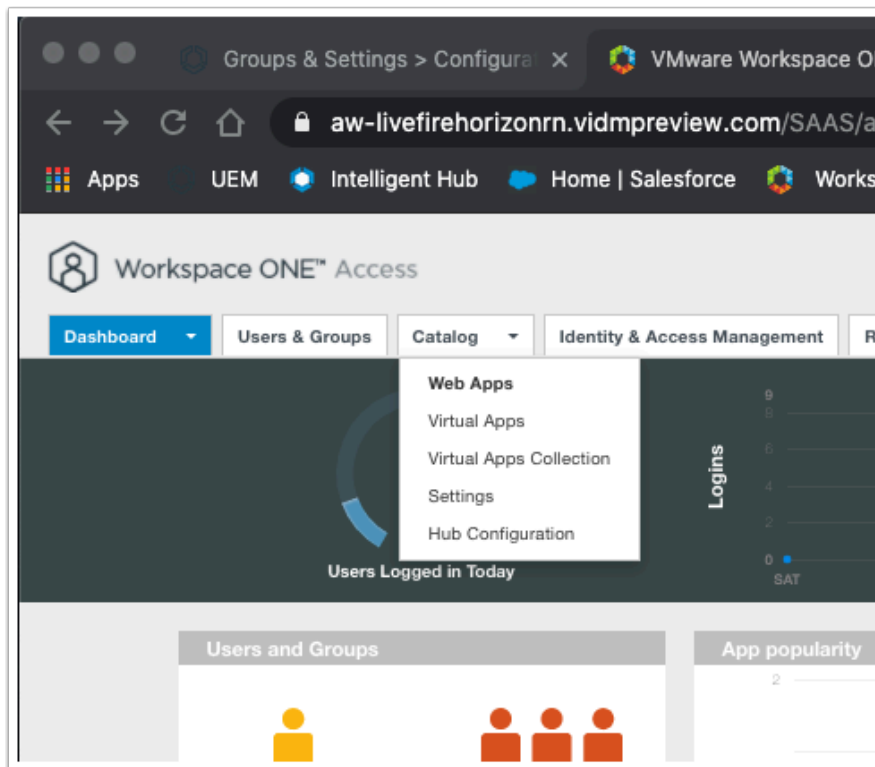
- **Under Metadata URL :** [https://YOUR\\_CUSTOM\\_Access\\_URL/SAAS/API/1.0/GET/metadata/idp.xml](https://YOUR_CUSTOM_Access_URL/SAAS/API/1.0/GET/metadata/idp.xml)
- e.g. <https://aw-euclivefirefran.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml>



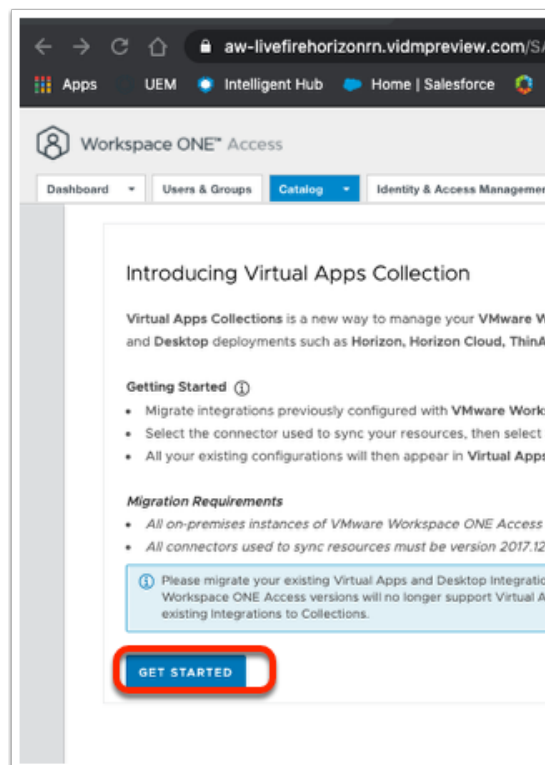
8. Click **OK** to close the **Manage SAML Authenticators** window



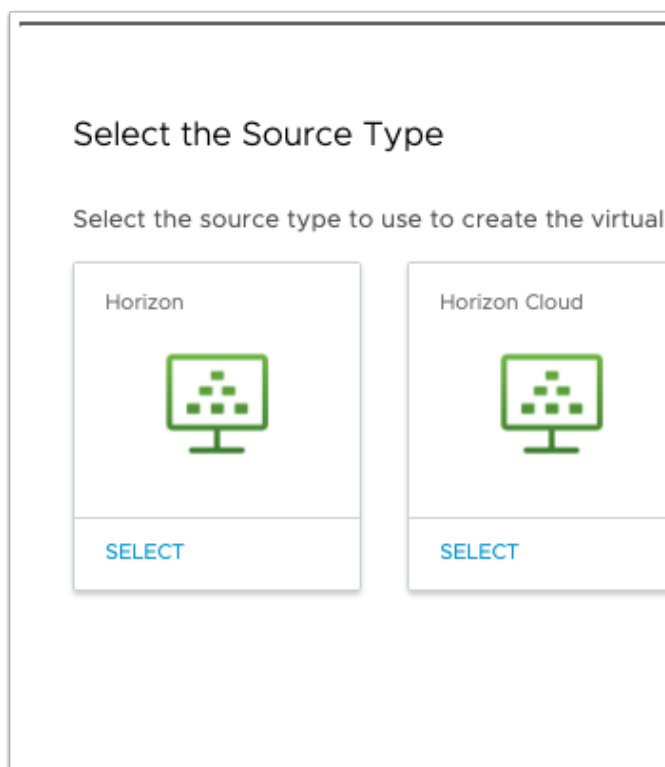
9. Click **OK** to close the **Connection Server Settings**



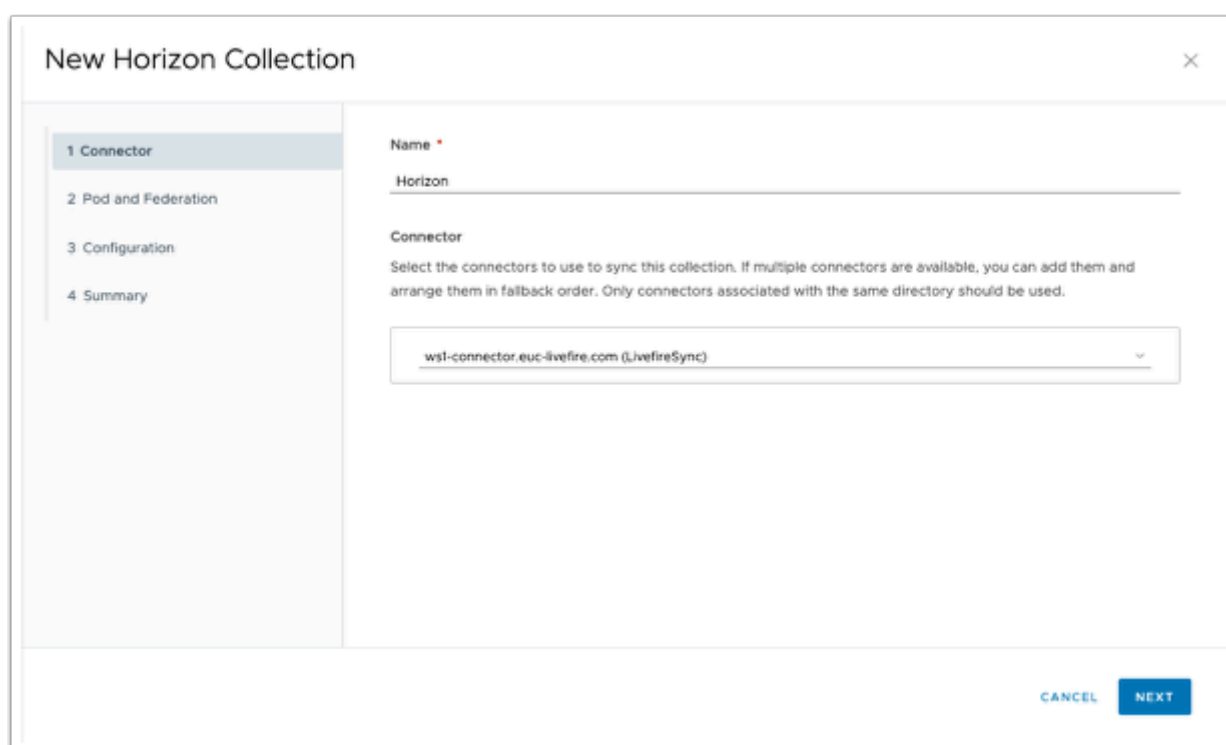
10. On the **ContolCenter2 Server** desktop, launch your **Google Chrome Browser** .
- Login as sysadmin to your **SaaS Instance of Workspace ONE Access** and login as sysadmin
  - On the **Catalog** tab, select **Virtual Apps Collection**



11. On the **Introducing Virtual Apps Collection** Page select **GET STARTED**



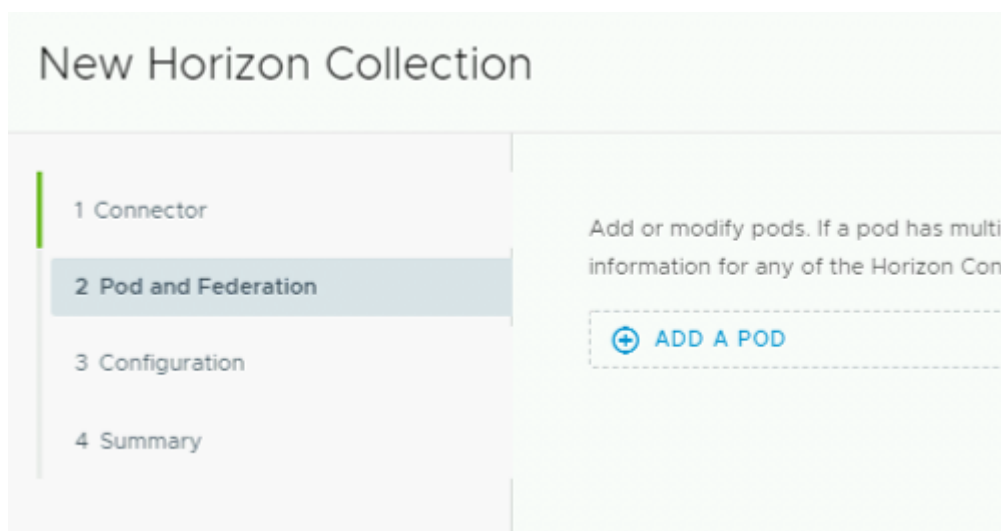
12. In the **Select the Source Type** window, in the **Horizon** box, click the **SELECT** link



13. On the **NEW Horizon Collection** page type the follow next the following headers

- **Name :** **Horizon**

- In the Connector area accept the default **ws1-connector.euc-livefire.com (LivefireSync)**
- Select **NEXT**



14. In the **New Horizon Collection** wizard

- Step **2. Pod and Federation**, select **+ ADD A POD**

15. In the **New Horizon Collection** wizard

- Under **Horizon Connection Server** type : **cs1-pd1.euc-livefire.com**
- Under **Username** type: **administrator@euc-livefire.com**
- Under **Password** type: **VMware1!**
- Select **ADD**
- Select **Next**

**New Horizon Collection**

1 Connector  
2 Pod and Federation  
**3 Configuration**  
4 Summary

**Sync**

Sync Frequency  
Manual

Sync Duplicate Apps ⓘ  
Yes ☒

**Other Configurations**

Activation Policy ⓘ  
Automatic

Default Launch Client ⓘ  
Browser

CANCEL BACK NEXT

16. In the **New Horizon Collection** wizard
- In Step **3 Configuration**
    - On the **Sync** page under **Activation Policy**
    - Change **User Activated** to **Automatic**,
    - Under the **Default Launch Client** select **Browser**
  - Select **Next**

**Pod**

| Horizon Connection Server | Username      | Smart Card Authentication | True SSO | Sync Local Assignments |
|---------------------------|---------------|---------------------------|----------|------------------------|
| csl-pd1.euc-liveline.com  | Administrator | Disabled                  | Disabled | Enabled                |

Cloud Pod Architecture (CPA)  
Disabled

CANCEL BACK SAVE & CONFIGURE NETWORK RANGE

17. In the **New Horizon Collection** wizard
- In Step **4 Summary**
    - Select **SAVE & CONFIGURE NETWORK RANGE**



Network Ranges

Collection 'Horizon' has been added successfully.

Assign pods to the following network ranges. If you cannot find the right network ranges for these pods, create a new one.

| Name       | Description              | IP Address Range          |
|------------|--------------------------|---------------------------|
| ALL RANGES | A network for all ranges | 0.0.0.0 - 255.255.255.255 |

CREATE NETWORK RANGE

FINISH

## 18. On the Network Ranges window

- Select **FINISH**

Virtual Apps Collections

NEW

EDIT

SYNC

DELETE

| Name    | Source Type |
|---------|-------------|
| Horizon | Horizon     |

1 - 1 of 1 items

Calculating Sync Actions

| Applications | Desktops  | Assignments |
|--------------|-----------|-------------|
| 3 added      | 1 added   | 4 added     |
| 0 updated    | 0 updated | 0 updated   |
| 0 deleted    | 0 deleted | 0 deleted   |

OK

SAVE

Virtual Apps

EDIT

ASSIGN

CATEGORIES

SETTINGS

| Application       | Type                |
|-------------------|---------------------|
| Calculator        | Horizon Application |
| Internet Explorer | Horizon Application |
| Paint             | Horizon Application |
| W10INST           | Horizon Desktop     |

## 19. In the Virtual Apps Collections Window

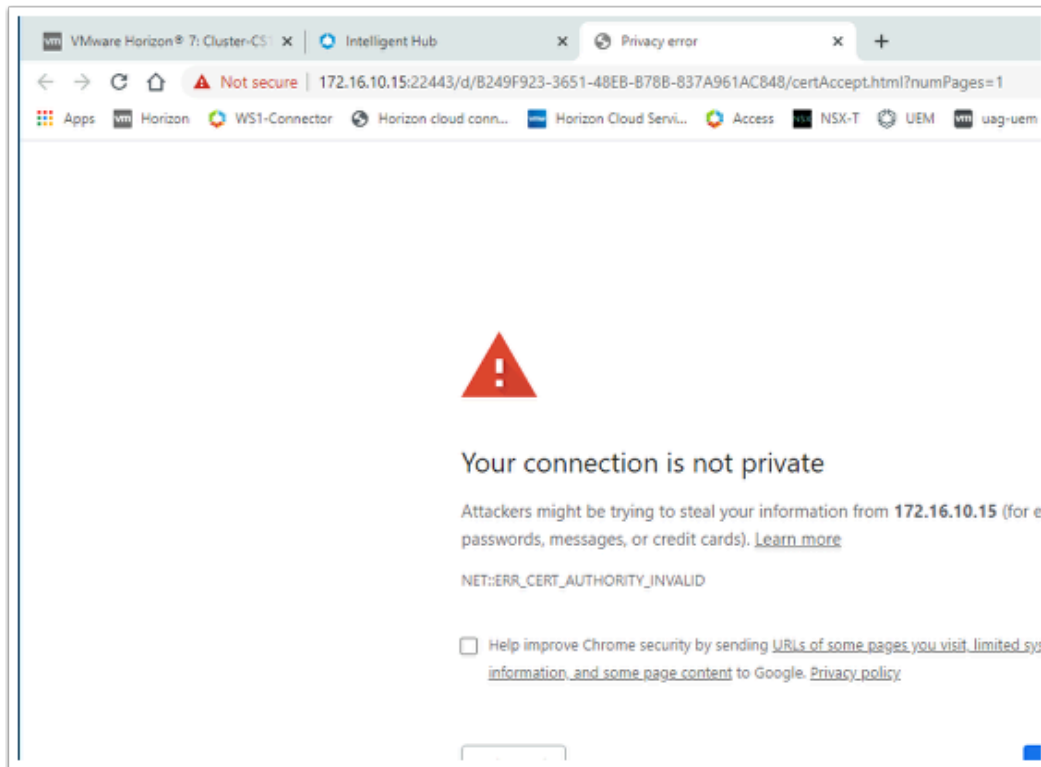
- Select the **radio button** next to **Horizon**
- Select **SYNC**

- On **Calculating Sync Actions** select **SAVE**
- navigate to **catalog \ virtual apps** and notice your new virtual applications

This concludes this exercise. Move onto the next chapter

# Horizon Configuration with Workspace ONE Access and the Unified Access Gateway

## Introduction



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

In this Chapter we will look at what the default configuration of a session is, exactly what happens and how we can make sure our sessions are secure.

## Background

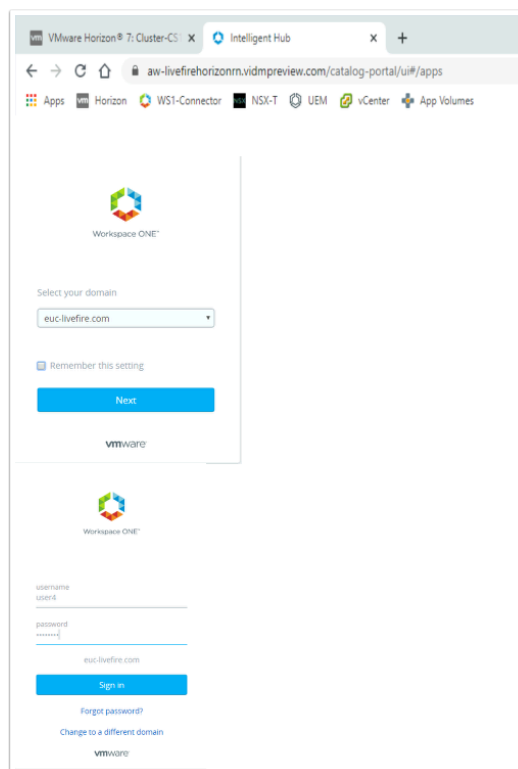
In earlier versions of Horizon, if we wanted to solve this problem we had to perform two primary operations.

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.

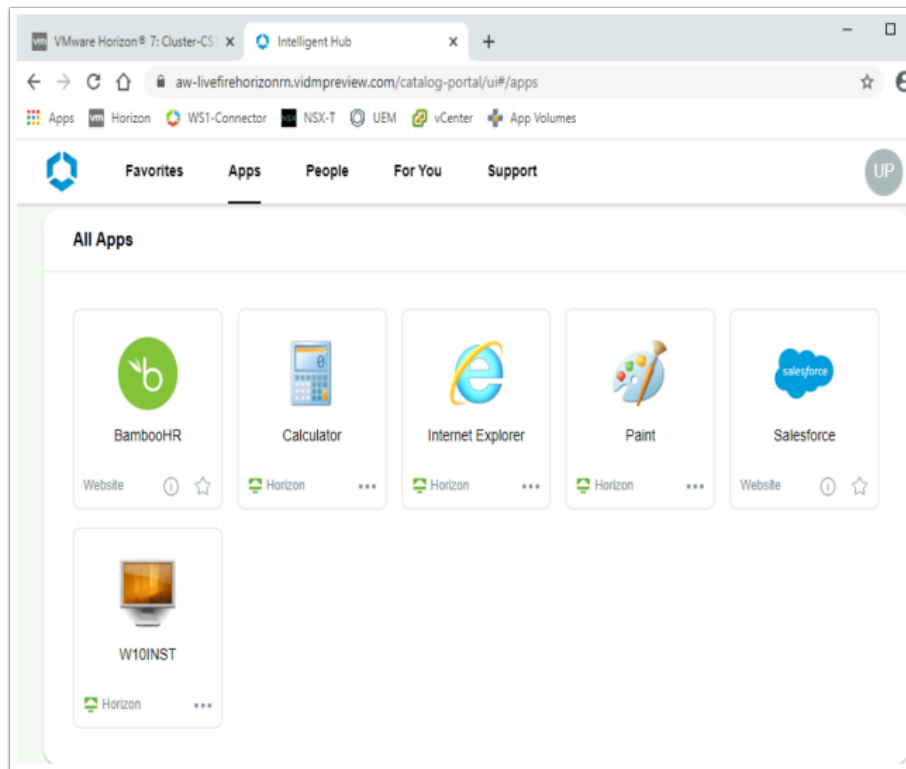
This exercise is divided into two parts.

- 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.

## Part 1. Validating the default configuration on the Blast transport

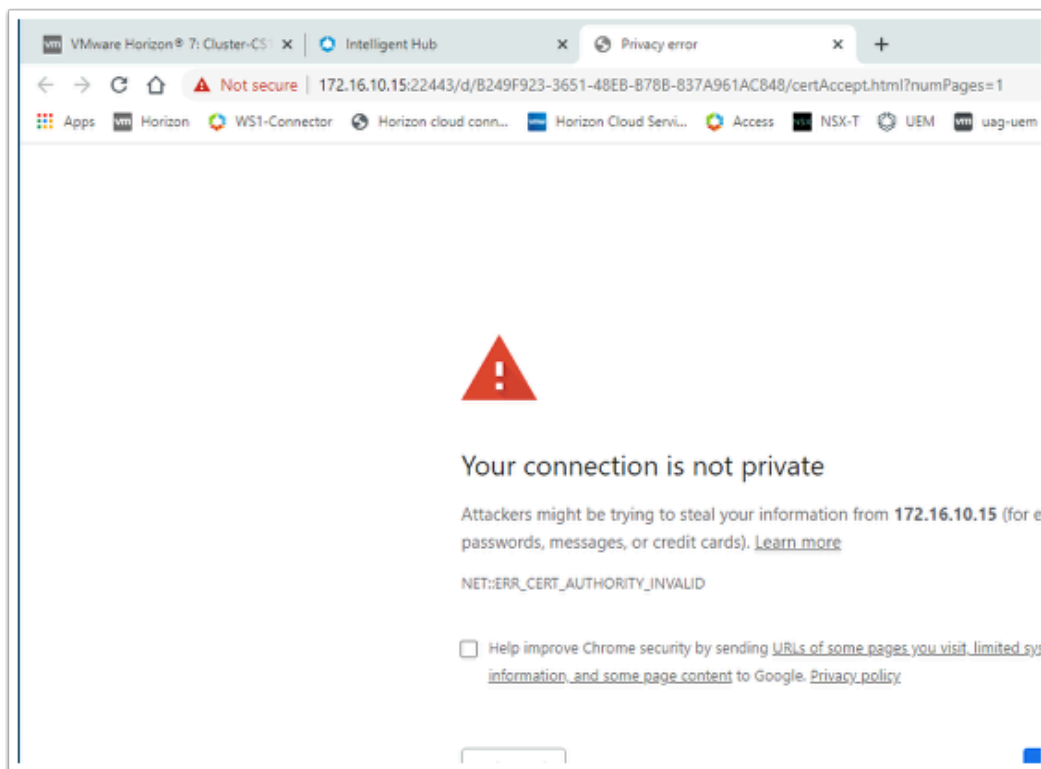


1. On the **ControlCenter** server. Open up your **Chrome browser** session
  - Launch a new session of your cloud **SaaS Workspace ONE Access** select **Next**
  - In the **Select your domain**, ensure **euc-livewire.com** is the selection. Select **Next**
  - Enter the user name **User 4** and the password **VMware1!** Select **Sign in**
  - Select **Apps** in the title bar

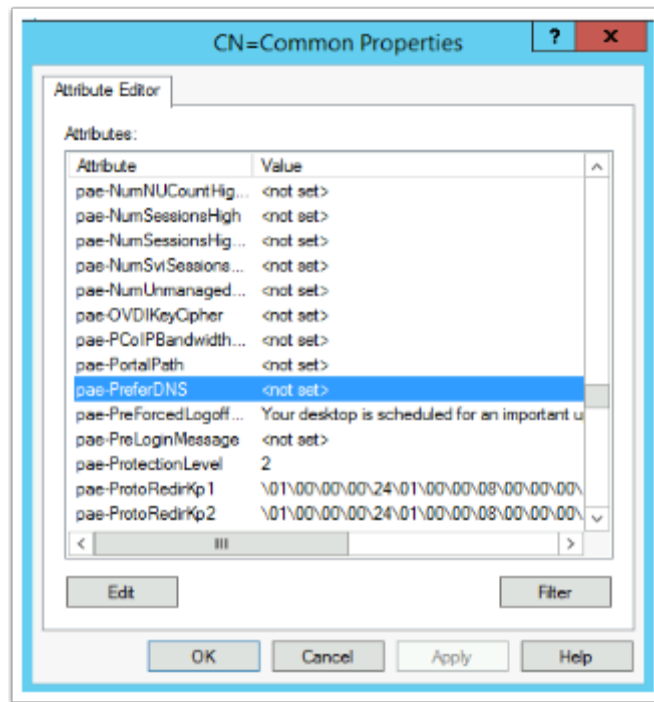


## 2. In the **Workspace ONE Access Console**

- Select **Apps**
- Select and launch, any **one** of the **4 Horizon based entitlements**



3. In the address bar, notice you have an IP address, also you will notice it says the certificate is not Valid.



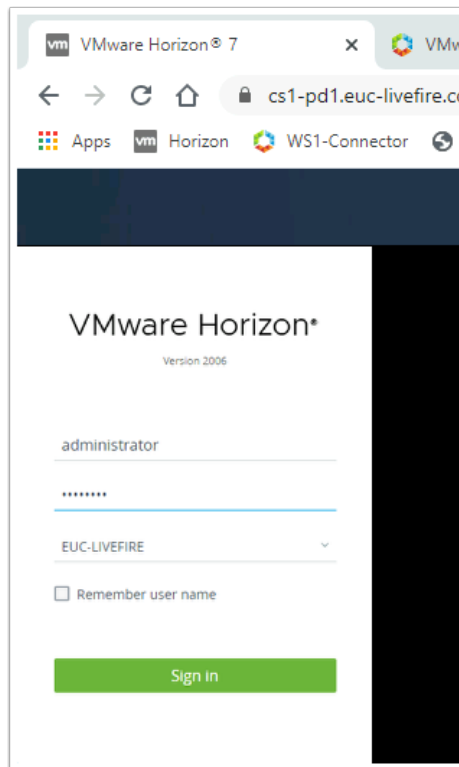
4. So there are two problems here, our Agent is using a self-signed cert, but even if we had a CA signed cert it would not be trusted as by default Horizon prefers to use IP address rather than domain name.
  - In the **past** this was a two part process, where we had to edit the LDS database using ADSIEDIT (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.
  - 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.
  - 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

## Part 2. Securing a Horizon Blast sessions using HTML Access.

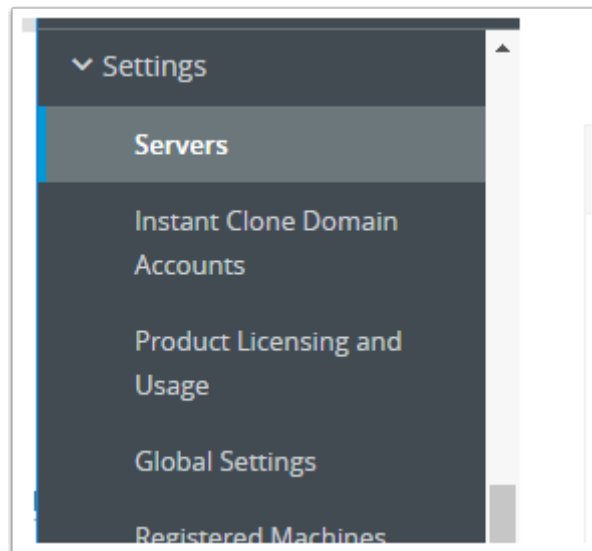
What the Product development team have done is give us the ability to Tunnel HTML Blast traffic through the Broker.

- 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

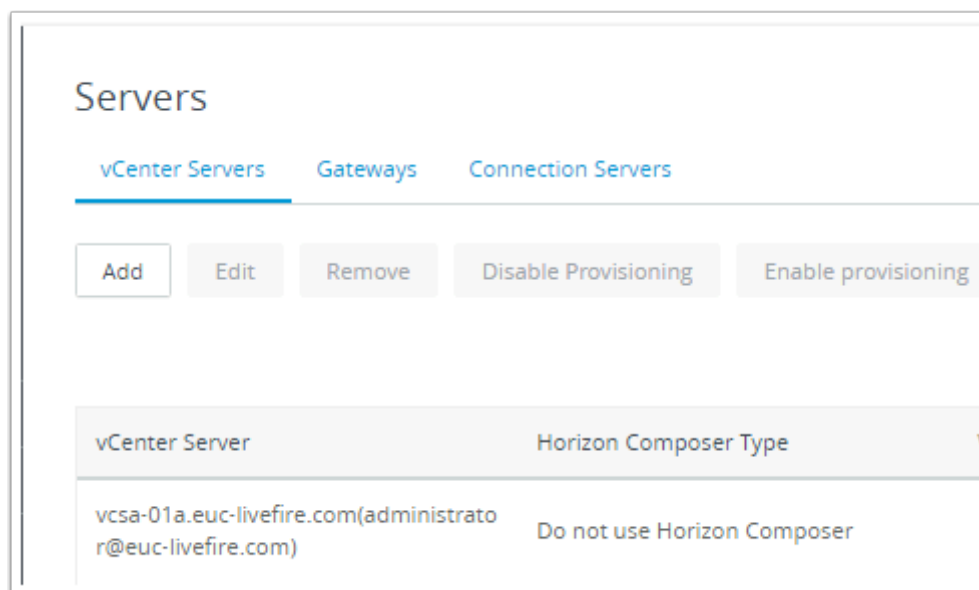


1. On your **ControlCenter** server, launch the **Chrome Browser**, select the **Horizon** shortcut in the **Favourites Bar**
  - Login as **Administrator**
  - For password us **VMware1!**
  - Select **Sign in**



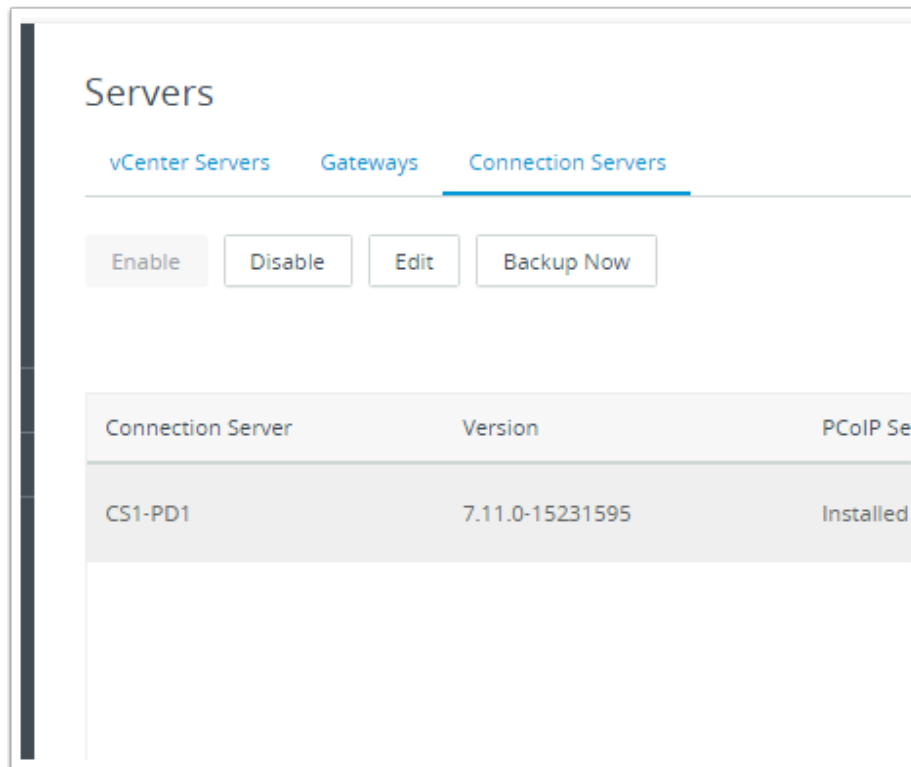
2. In the **Horizon Console**

- **Expand Settings**
- Select **Servers** under **Settings**

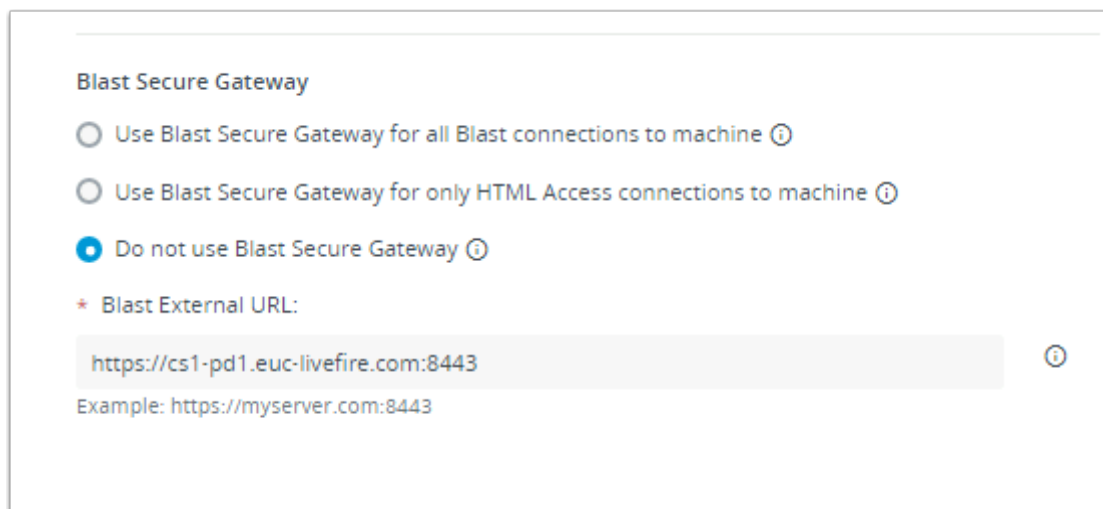


3. Under **Servers**, select the **Connection Servers** tab





4. On the **Connection Servers** tab, select the **CS1-PD1** and select **Edit**



5. Notice the default configuration under Blast Secure Gateway is selected to **Do not use Blast Secure Gateway**

**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:

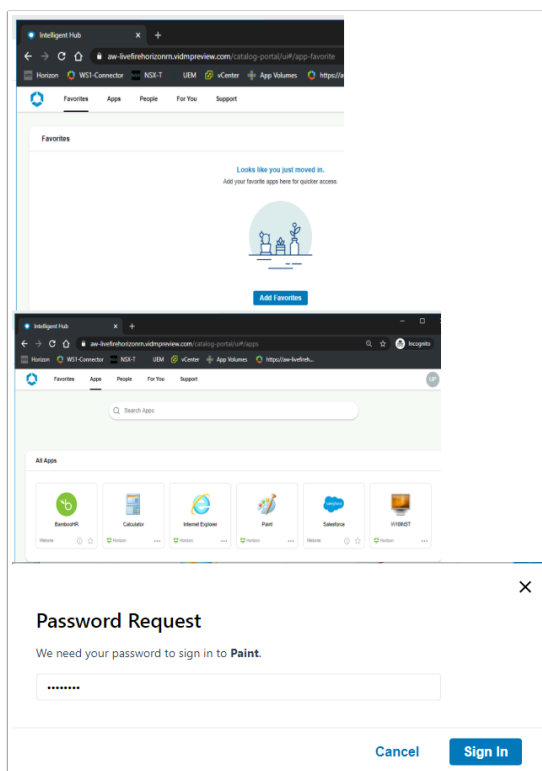
ⓘ  
 Example: https://myserver.com:8443

6. Change the default configuration by selecting 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 3 . Validating our Horizon HTML Blast Configuration

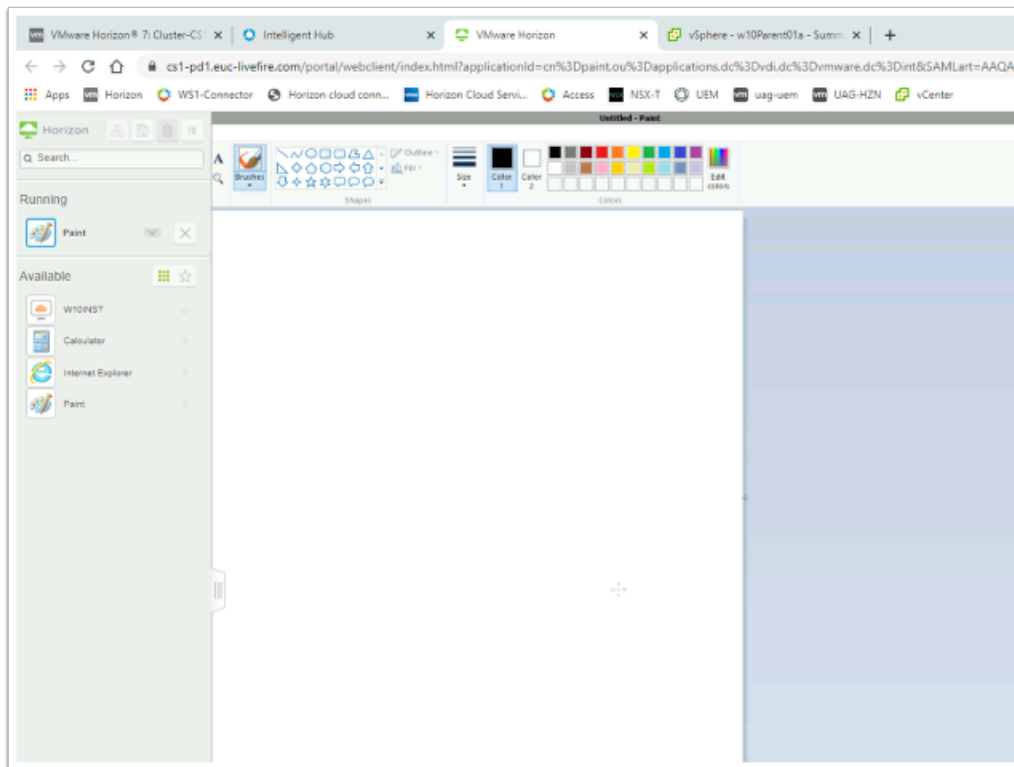
1. On the **ControlCenter2** server. Open up a new incognito **Chrome browser** session
  - Select your **Custom Workspace ONE Access** url select **Next**
  - In the **Select your domain**, ensure **euc-livefire.com** is the selection. Select **Next**

- Enter the user name **User 4** and the password **VMware1!** Select **Sign in**



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

- Select **Apps**
- Select and launch, any **one** of the **4 entitlements**,
  - In the following example we will launch **Paint**
  - In the **Password Request** window, enter **VMware1!**
    - **Select Sign In**
      - *Note! Caching of Passwords is by default disabled by Workspace ONE Access . In the next lab - Horizon TrueSSO we will sort this out*



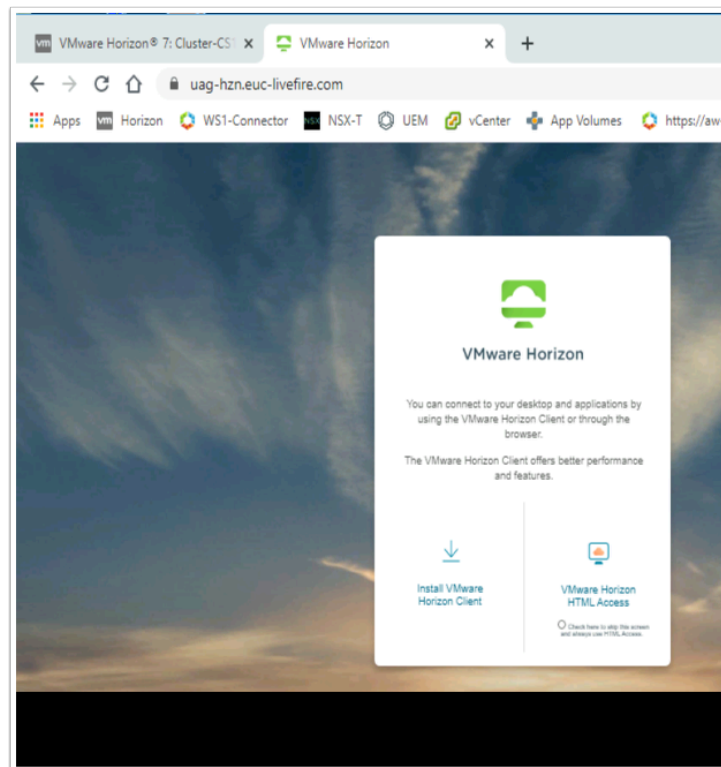
3. Notice there were no hiccups in the launch of your application in your browser and you have a valid certificate in your Browser
  - You are being tunneled via the broker to your Horizon session
  - **Log off** and **close all** windows from this lab.

## Conclusion

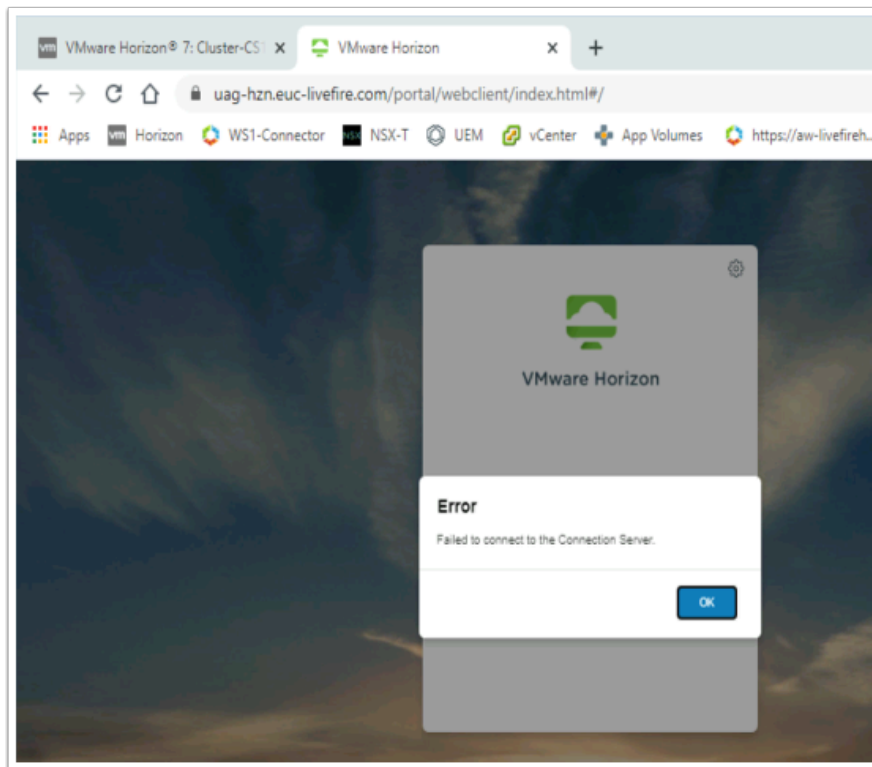
In this session we have seen how we secure internal HTML Blast traffic

- 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.
- The User Experience has been vastly improved as now there are no hiccups when using the HTML Client.

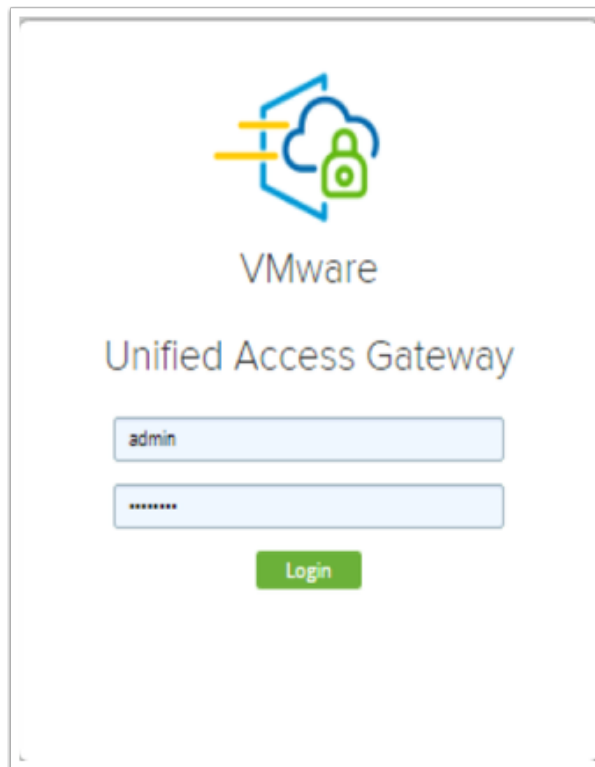
## Part 4: Securing the HTML Blast Transport using the Unified Access Gateway



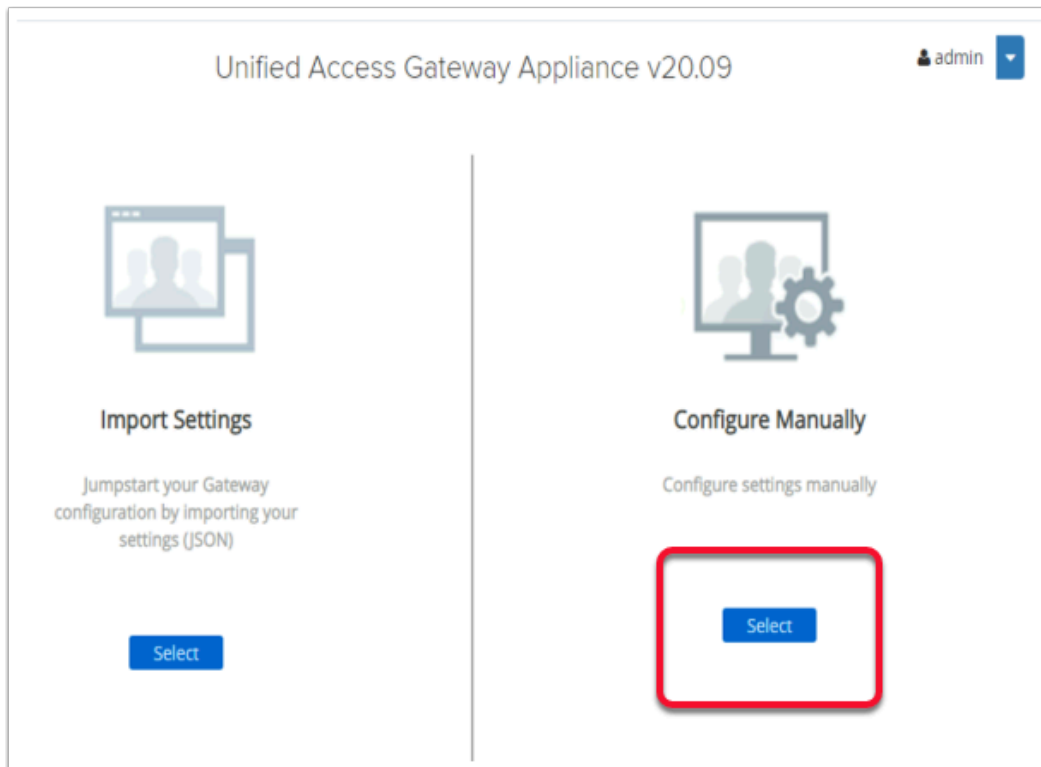
1. On your **ControlCenter2** server,
  - Launch your **Chrome Browser**
  - Enter **UAG-HZN.euc-livefire.com** in the Address **Bar**
  - Select **VMware Horizon HTML Access**



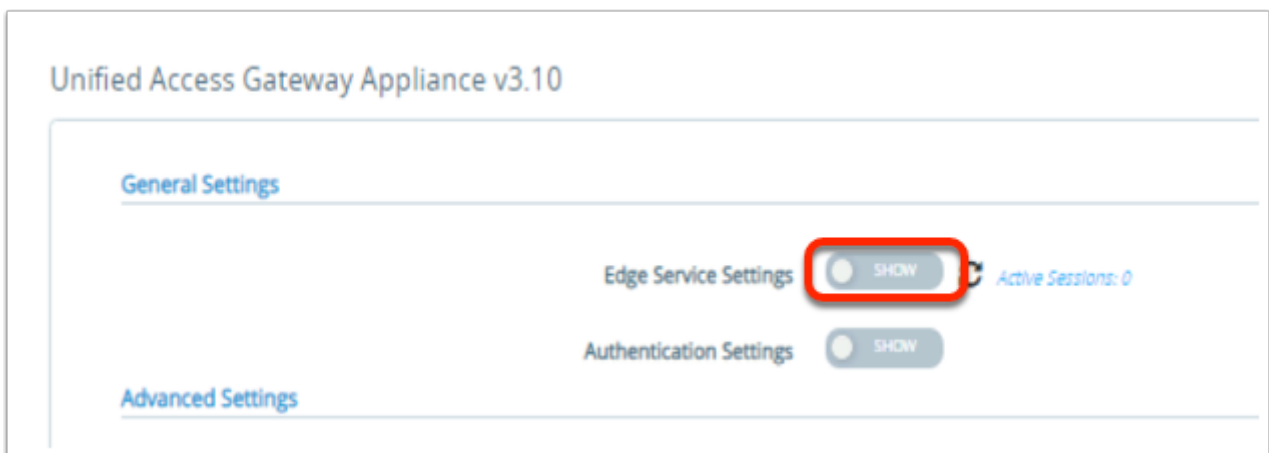
2. Notice you have a **Failed to connect to the Connection Server** issue
  - Select **OK** to close the **Error** message
  - This is not a UAG issue and nothing is broken. This due to a new secure feature that has been enabled in Horizon 7 called **Origin checking** which is enabled by default and 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>



3. On your **ControlCenter2** server Desktop
  - Open your **Browser** and enter the following URL in the address bar. [uag-hzn.euc-livefire.com:9443](https://uag-hzn.euc-livefire.com:9443)
  - In the **username** area enter [admin](#) (case sensitive ) and in the **password** section enter [VMware1!](#)
  - Select **Login**

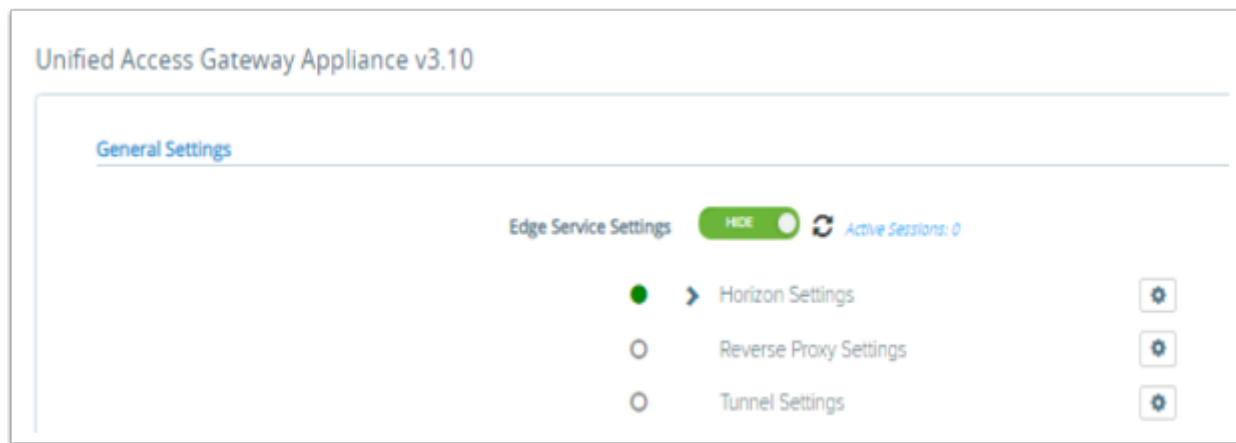


4. In the **Unified Access Gateway Appliance v20.09** window under **Configure Manually** click **Select**

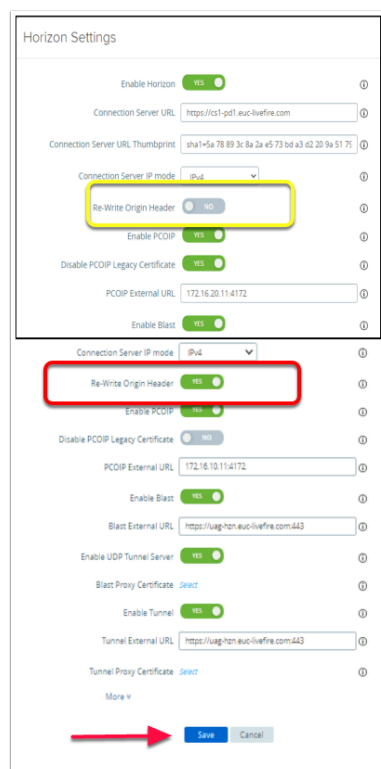


5. Under **General Settings**, move the **toggle** next to **Edge Service Settings** from Left to Right



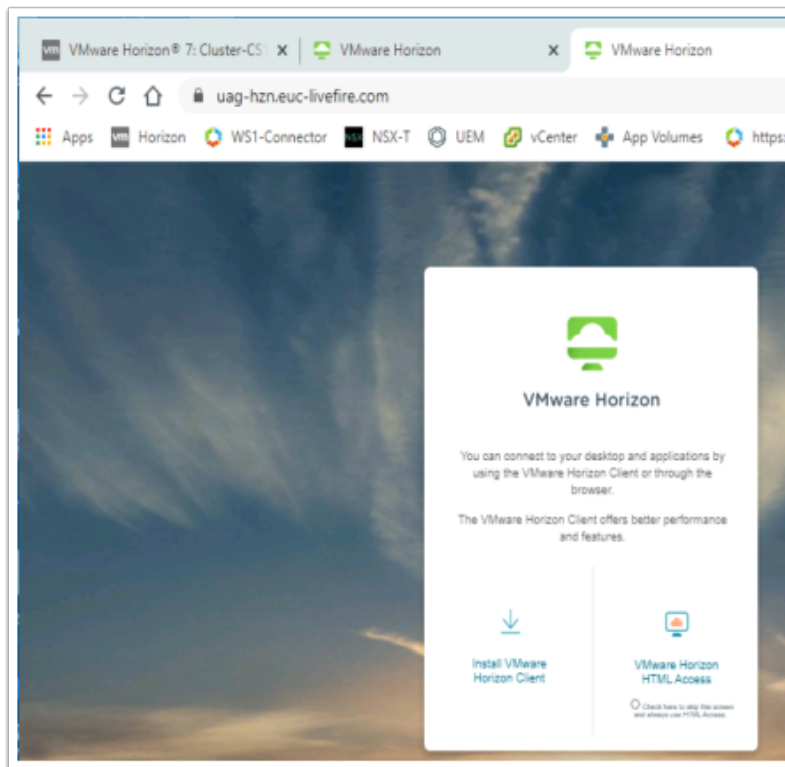


6. To the right of Horizon Settings, select the **gear wheel**



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

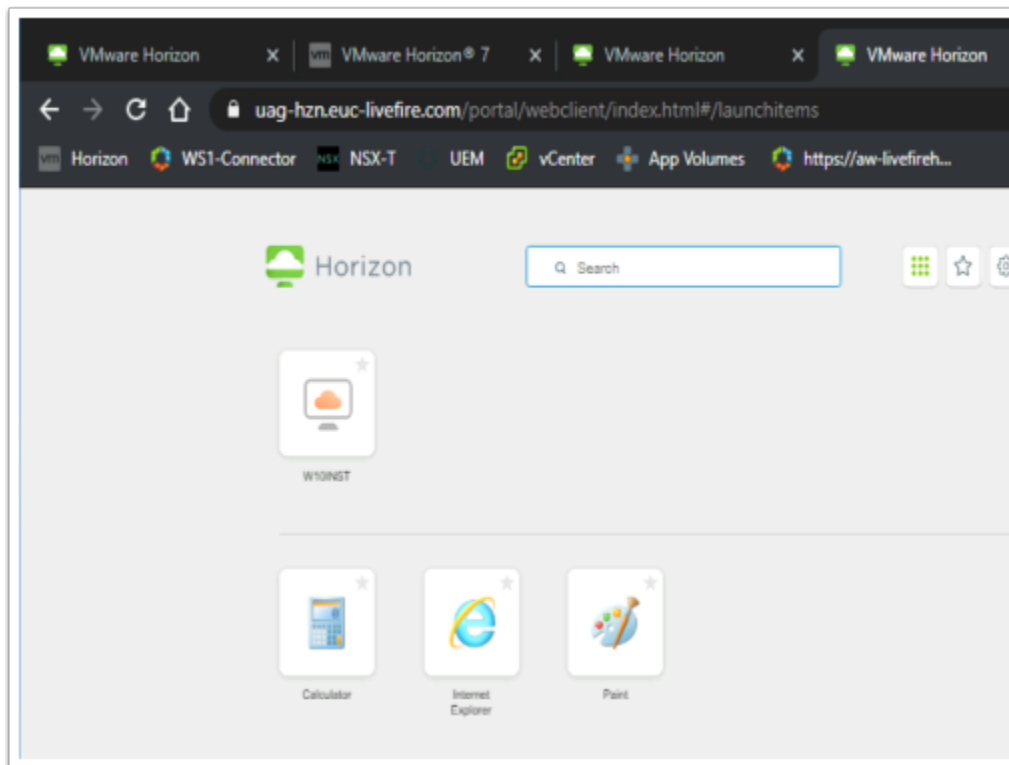
- **Re-write Origin Header**, move the **toggle** from **No** on the left to **Yes** on the right.
- Select **Save** at the bottom of the window.
- Logout from the Admin console



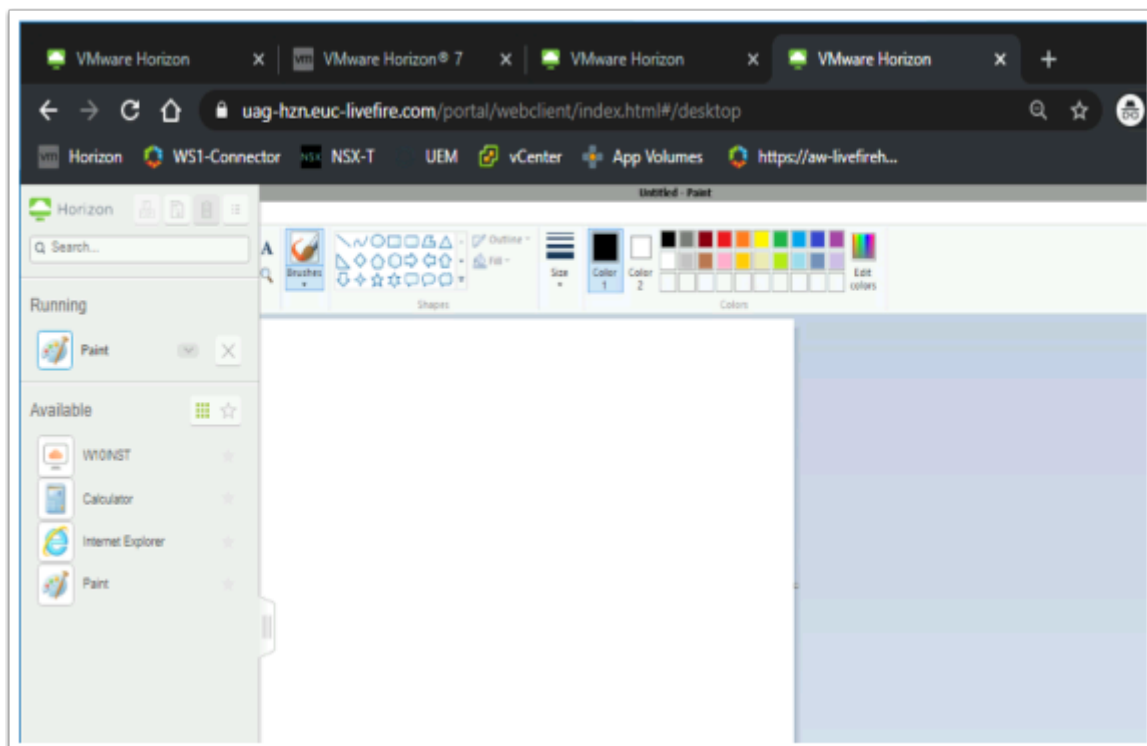
8. On your **ControlCenter2** server,
  - Launch your **Chrome Browser**
  - Enter **UAG-HZN.euc-livewire.com** in the Address Bar
  - Select **VMware Horizon HTML Access**

9. In the Login window type in the following:

- Username: **User4**
- Password: **VMware1!**
- Select **Login**



10. In the Horizon HTML entitlements, launch any of the **4 entitlements**



11. Notice your entitlement launches without any further prompts

- Also notice that you had when you did not login via Workspace ONE Access you had a Single SSO experience with Password based Authentication

## 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 his support in guidance on getting this lab right

Mark Ewert for his guidance and insights on the Horizon Blast Protocol

[https://techzone.vmware.com/resource/understand-and-troubleshoot-horizon-connections#HTML\\_Client\\_Access](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>

## About the Author: Reinhart Nel

<https://www.dropbox.com/s/cf32s1ddeyt5zx4/Reinhart%20Nel.pdf?dl=0>

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

# Installing and Configuring Horizon TRUESSO

## Overview

**i** Traditionally when authenticating to Workspace ONE Access using a 3rd party authentication method, the user will by default, not have a Single-Sign On experience when trying to launch any VMware Horizon based resource through Workspace ONE Access.

Traditionally when using a password based authentication method Workspace ONE Access would cache the original authentication against Access and then pass this on when required to the Broker.

Traditionally Single-Sign On would only be an issue when using a 3rd Party authentication method. To solve this problem we would deploy what is known as the Horizon Enrollment services to facilitate a single-sign on experience. We integrate with Microsoft Certificate Services to provide a solution to this challenge and we refer to the solution as **Horizon TRUE SSO**

### Since December 2019

When connecting to Horizon Resources via Workspace ONE Access. Caching of Passwords for Horizon has been disabled by default for SAAS, and a user will have to re-authenticate when they select their entitlement. Whilst the session is open we can choose to Cache the users credentials provided the Authentication method is password based.

<https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/rn/VMware-Workspace-ONE-Access-Cloud-Release-Notes.html>

To continue offering users a seamless single-sign On experience, Enrollment services has now become a critical service with the integration with Workspace ONE Access

In this lab scenario the 3rd party authentication method we use to login into Workspace ONE Access will be a certificate based method of authentication.

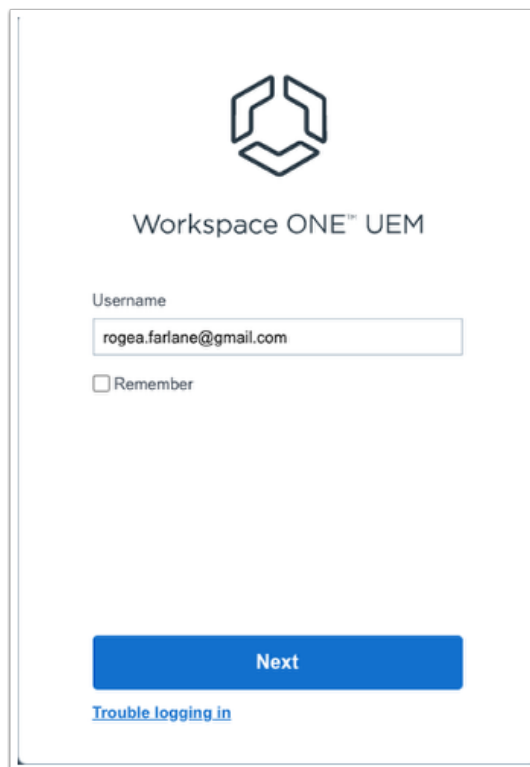
We will start off by doing the following:

1. Configure Windows 10 for Certificate Based Authentication using Workspace ONE UEM
2. Configure Workspace ONE Access for Certificate based Authentication
3. Log into a Windows 10 Desktop and demonstrate the limitation
4. Deploy and configure TRUE SSO

- Deploy and configure Horizon Enrollment services
- Integrate and configure Active Directory Certificate services with Horizon Enrollment services

5. Log into a Windows 10 Desktop and demonstrate the solution

## Part 1: WorkspaceOne UEM - Certificate Profile



Workspace ONE™ UEM

Username

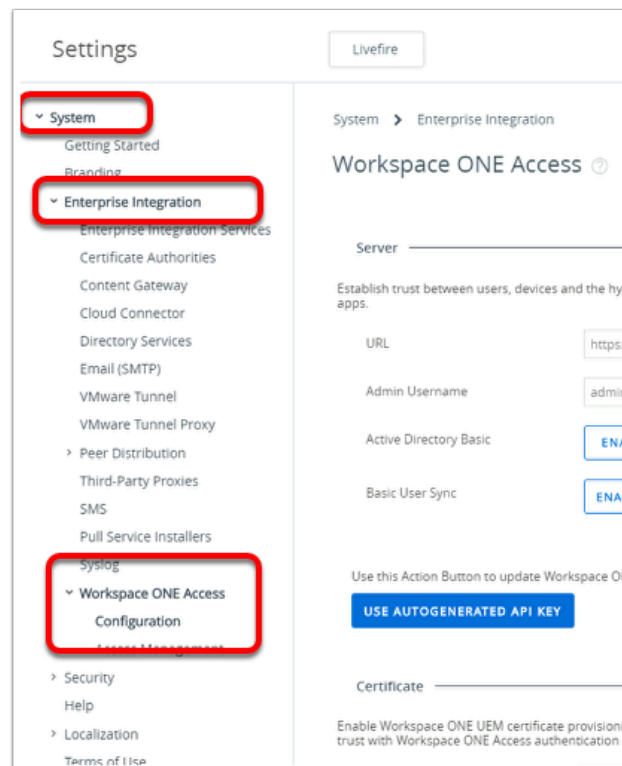
rogea.farlane@gmail.com

☐ Remember

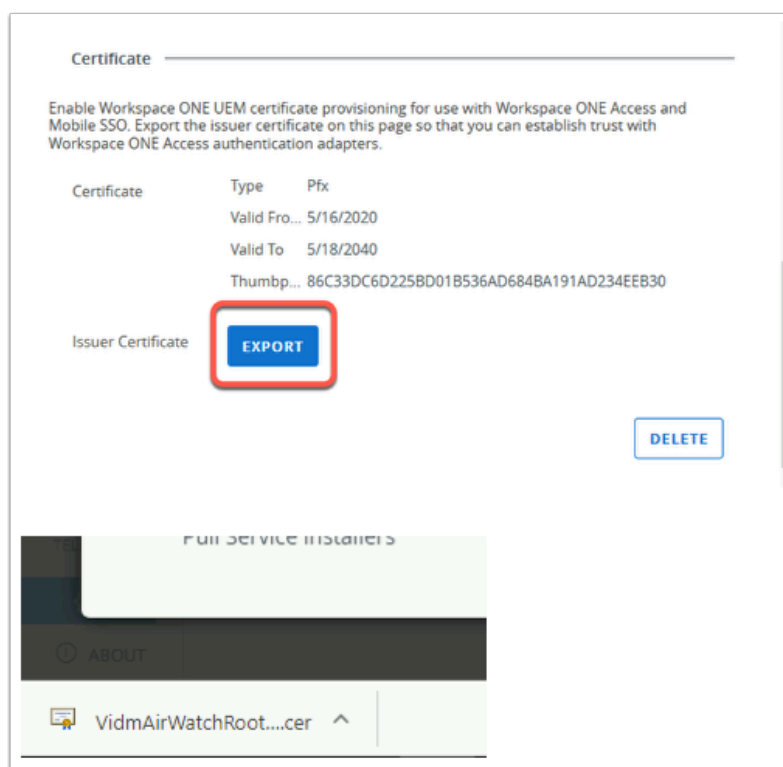
Next

[Trouble logging in](#)

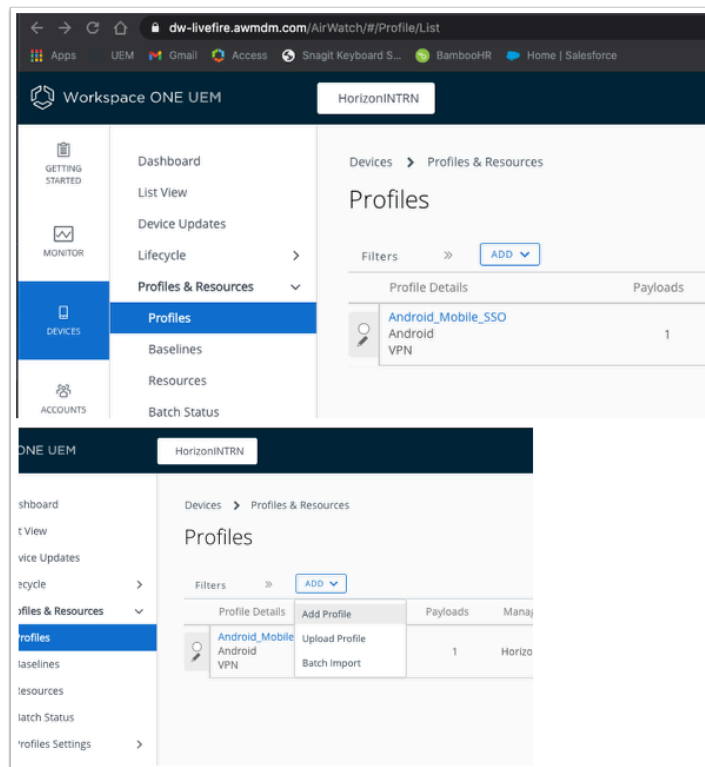
1. Navigate to your **custom UEM SaaS Tenant**
  - If necessary, authenticate using your SaaS Admin credentials



2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Workspace ONE Access > Configuration**

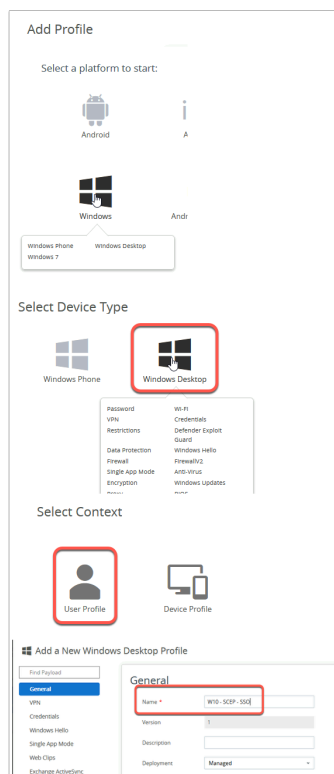


3. Click **EXPORT** in the **Certificates** section on the **Workspace ONE Access** page
  - Note this will download a .cer file (**VidmAirWatchRootCertificate.cer**)
  - Click to **close** the **Settings** window



#### 4. From the UEM Console

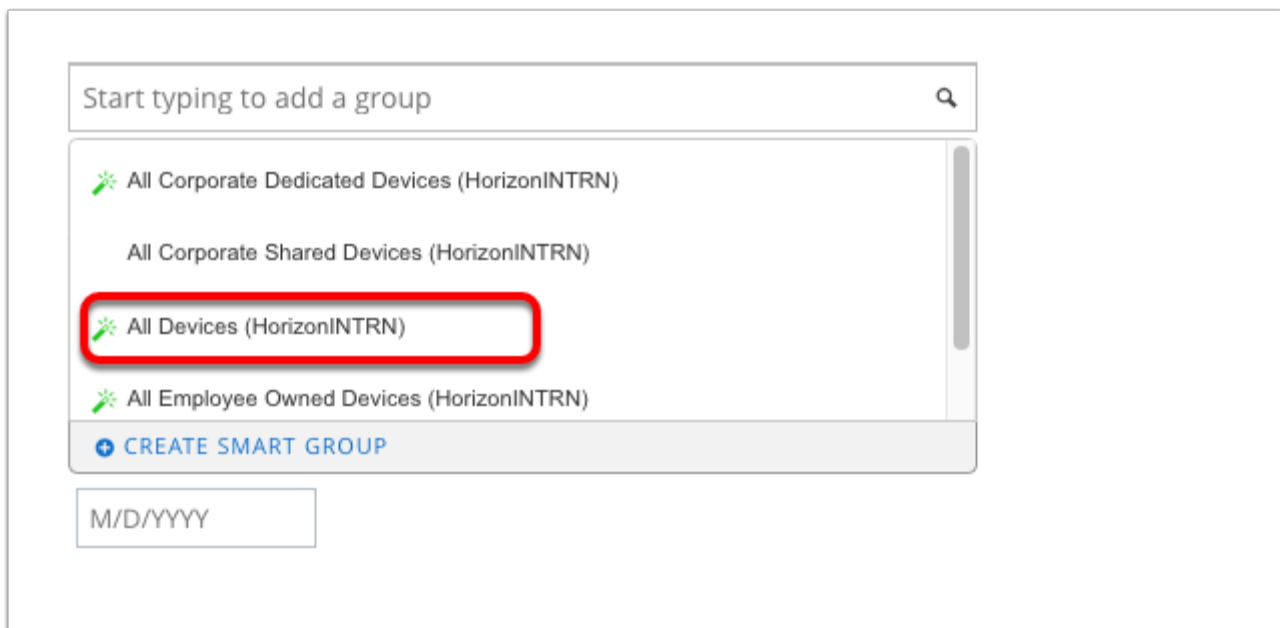
- Navigate to **Devices > Profiles & Resources > Profiles**
- Select > **ADD > Add Profile**



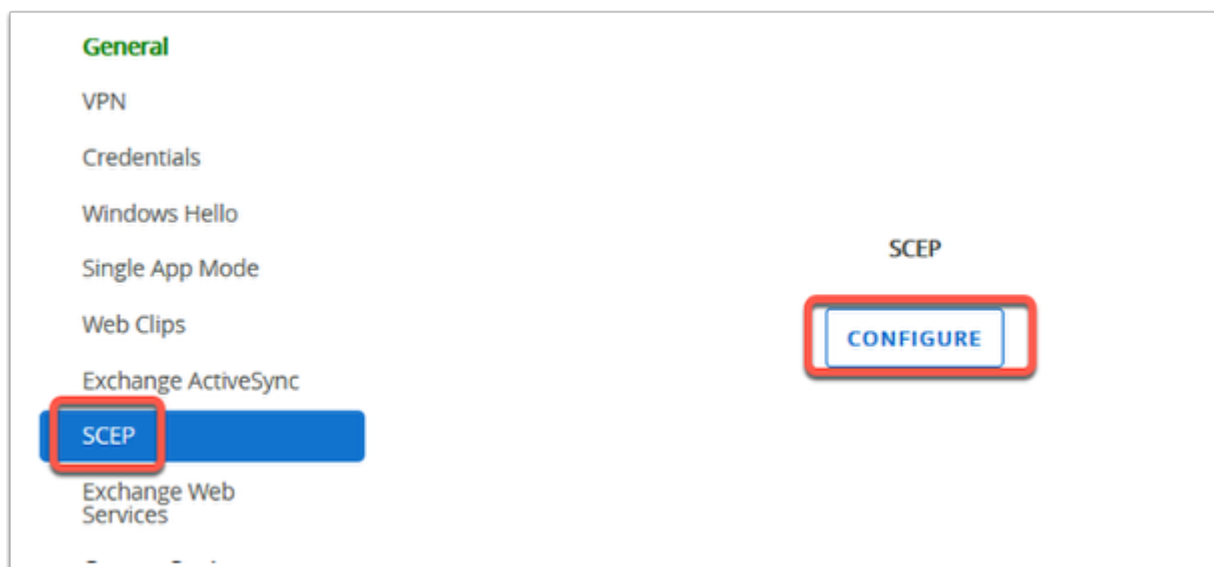
#### 5. In the Add Profile window select **Windows > Windows Desktop > User Profile**

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





6. Still in the **General** tab,
- Scroll down to **Smart Groups** and select **All Devices(YOUR SAAS Tenant)**



7. Now navigate to the **SCEP** tab on the left menu and select **CONFIGURE**

**SCEP**

Credential Source: AirWatch Certificate Authority

Certificate Authority \*: AirWatch Certificate Authority

Certificate Template \*: Single Sign-On

Issuer \*: LiveFire

Key Location: Software

10

⊕ ⊖

**SAVE AND PUBLISH** CANCEL

8. Set the following:

- Credential Source: **AirWatch Certificate Authority**
- Certificate Template: **Certificate (Cloud Deployment)**
- Issuer: **LiveFire**
- Key Location: **Software**
- Click **SAVE AND PUBLISH** at the bottom right of the window

View Device Assignment

Assignment Status: All Filter Grid

| Assignment Status | Friendly Name                          | User      | Platform/OS/Model                            | Phone Number | Organization Group |
|-------------------|--|-----------|--|--------------|--------------------|
| Added             | User36ARL Desktop Windows Desktop 1... | User36ARL | Windows Desktop / Windows 10 (10.0.18363)... |              | HorizonNTRN        |

Items: 1 of 1 Page Size: 20

PUBLISH CANCEL

9. Confirm your device is shown in the **View Device Assignment** page and select **PUBLISH**

## Part 2 : Configure Workspace ONE Access

Workspace ONE

Select Your Domain

System Domain

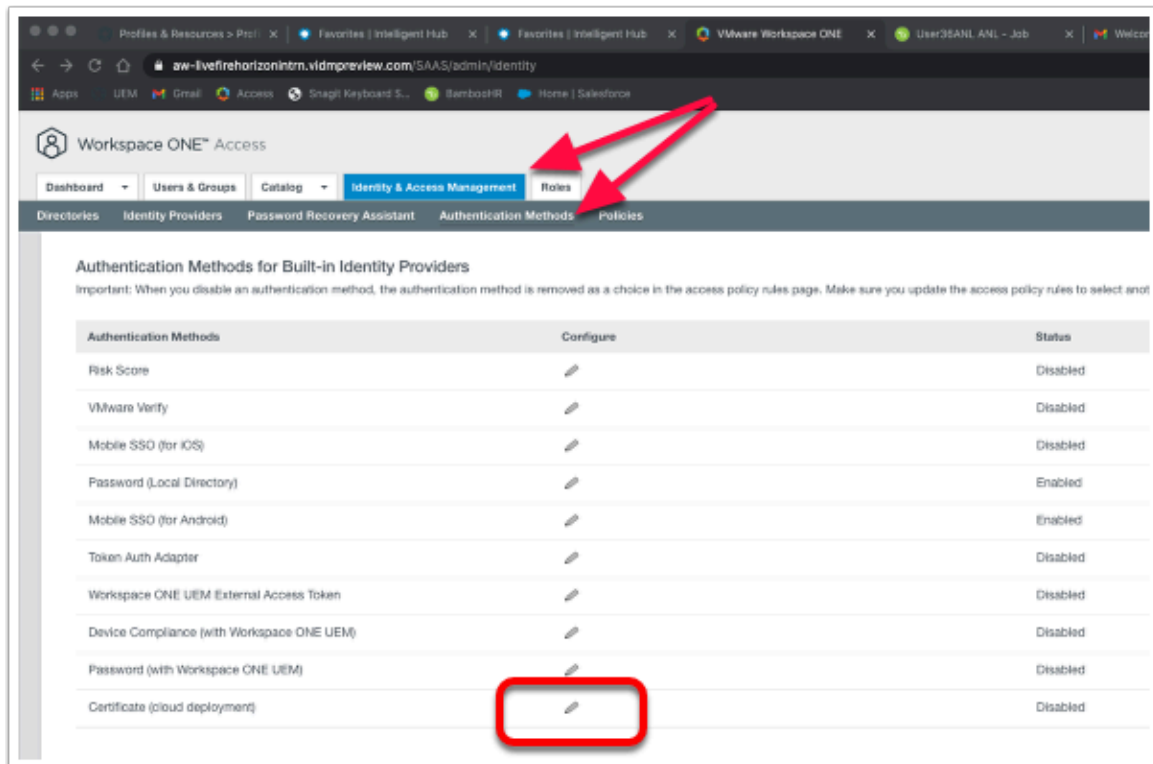
☐ Remember this setting

Next

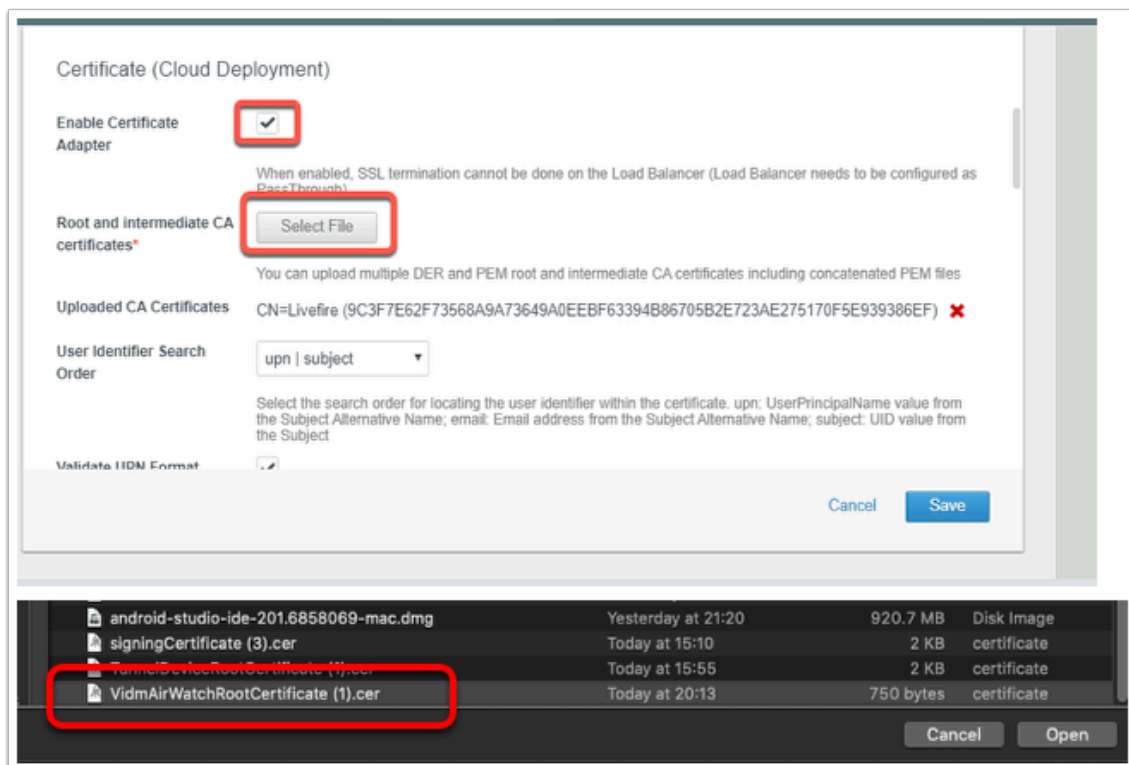
vmware

1. Switch to your custom Access tenant

- If necessary, authenticate as **System Domain**, select **Next**
- Sign in with your Admin credentials for your SaaS Tenant



2. In the Access admin console navigate to **Identity & Access Management** > **Authentication Methods**.
  - Select the **pencil icon** next to **Certificate (Cloud Deployment)**



3. In the **Certificate (Cloud Deployment)** page click the **tickbox** to **Enable Certificate Adapter**
- Click **Select File** for the **Root and Intermediate CA Certificates**
  - Select the **certificate** (VIDMAirWatchRootCertificate.Cer) we have downloaded from the UEM console earlier and
  - Select **Open**

Update Auth Adapter  
Please click OK to confirm and upload file.

Cancel OK

Certificate (Cloud Deployment)

certificates\* **Select File**

You can upload multiple DER and PEM root and intermediate CA certificates including concatenated PEM files

Uploaded CA Certificates CN=Livefire (9C3F7E62F73568A9A73649A0EEBF63394B86705B2E723AE275170F5E939386EF) ✖

User Identifier Search Order upn | subject ▼

Select the search order for locating the user identifier within the certificate. upn: UserPrincipalName value from the Subject Alternative Name; email: Email address from the Subject Alternative Name; subject: UID value from the Subject

Validate UPN Format ☒

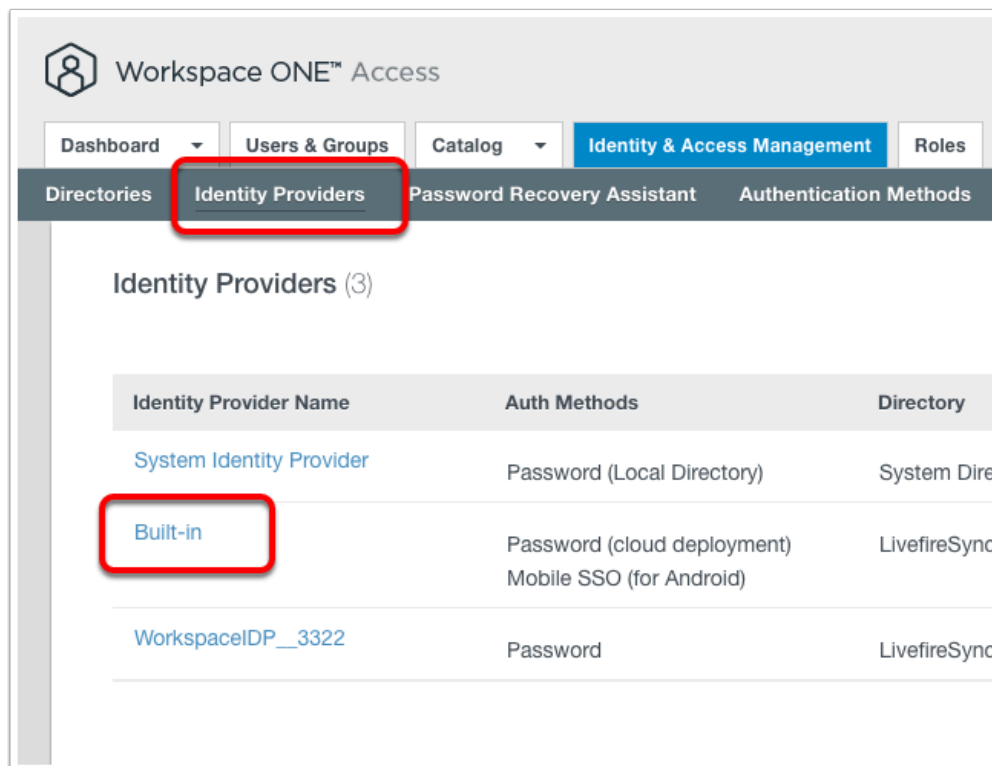
Validate the format of the UserPrincipalName field

Request Timeout 0

Timeout in seconds to wait for a response. A value of zero will wait indefinitely.

Cancel Save

4. Once the certificate has uploaded select **OK**.
- Keep the remaining settings as default and click **Save** at the bottom of the page



5. Navigate **Identity Providers** under **Identity & Access Management** click on **Built-in**

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

| Authentication Methods         | Associate Authentication Method     |
|--------------------------------|-------------------------------------|
| Password (Local Directory)     | <input type="checkbox"/>            |
| Mobile SSO (for Android)       | <input checked="" type="checkbox"/> |
| Certificate (cloud deployment) | <input checked="" type="checkbox"/> |

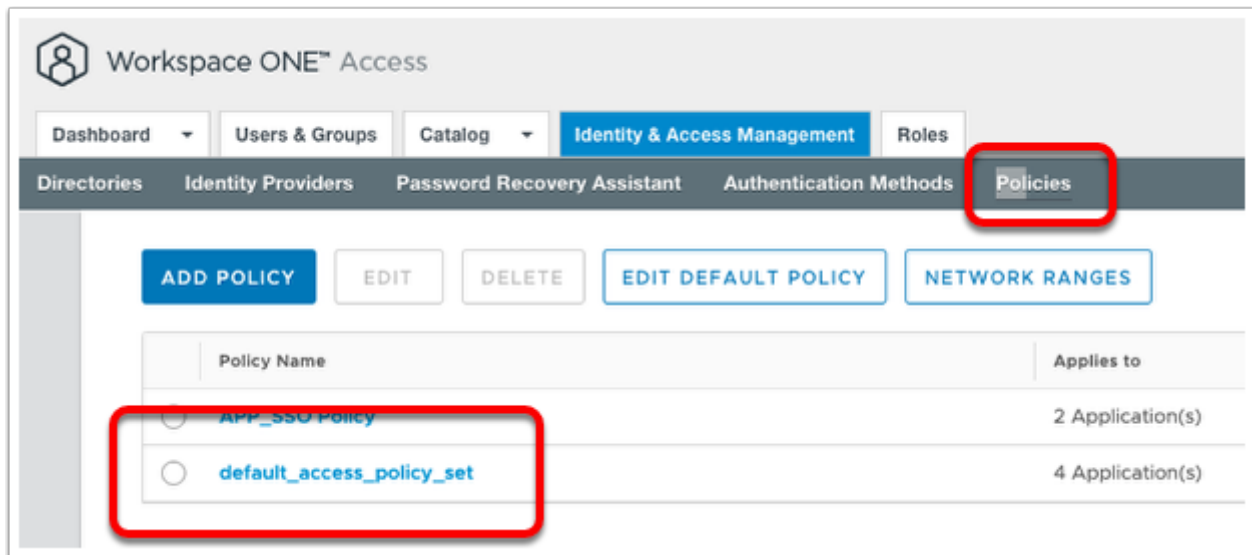
---

**KDC Certificate Export** [Download Certificate](#)  
Export the KDC server root certificate fo

---

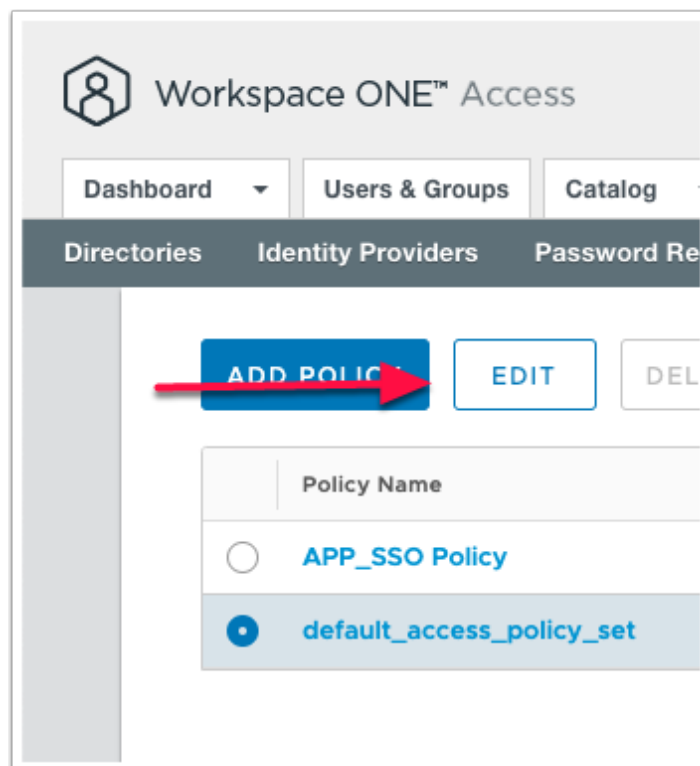
[Save](#) [Cancel](#)

6. Navigate to the **Authentication Methods** area
- Select the **check box** next to **Certificate (Cloud Deployment)**
  - Select **Save** at the bottom of the page.



7. In the Access Admin console

- Navigate to **Identity & Access Management > Policies**
- Select the **default\_access\_policy\_set**



8. Click **EDIT**

## Edit Policy

1 Definition
2 Configuration
3 Summary

You can create a list of rules to access the applications selected by devices that can access the applications, the authentication method before reauthenticating.

| Network Range | Device Type           |
|---------------|-----------------------|
| ⌵ ALL RANGES  | Web Browser           |
| ⌵ ALL RANGES  | Workspace ONE App ... |

+ ADD POLICY RULE

9. In the **Edit Policy** window, select, the second header, from the left column **Configuration**
- Select **All Ranges** next to **Web Browser**, under **Device Type**

### Edit Policy Rule

< CONFIGURATION

If a user's network range is \*

and the user accessing content from \*

and user belongs to group(s)

Then perform this action

then the user may authenticate using \*

If the preceding method fails or is not applicable, then

If the preceding method fails or is not applicable, then

ALL RANGES

Web Browser

Q Select Groups...

Rule applies to all users if no group(s) selected.

Authenticate using...

Certificate (cloud deployment)

Password (cloud deployment)

Password (Local Directory)

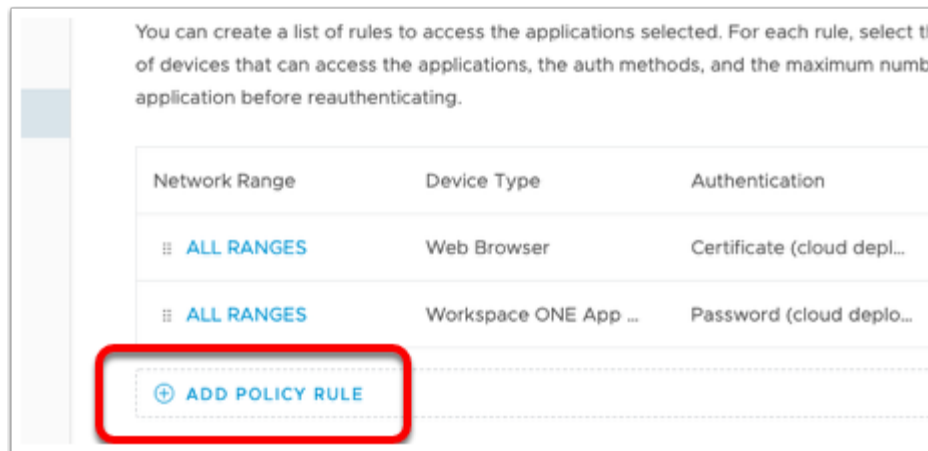
+ ADD FALLBACK METHOD

CANCEL
SAVE

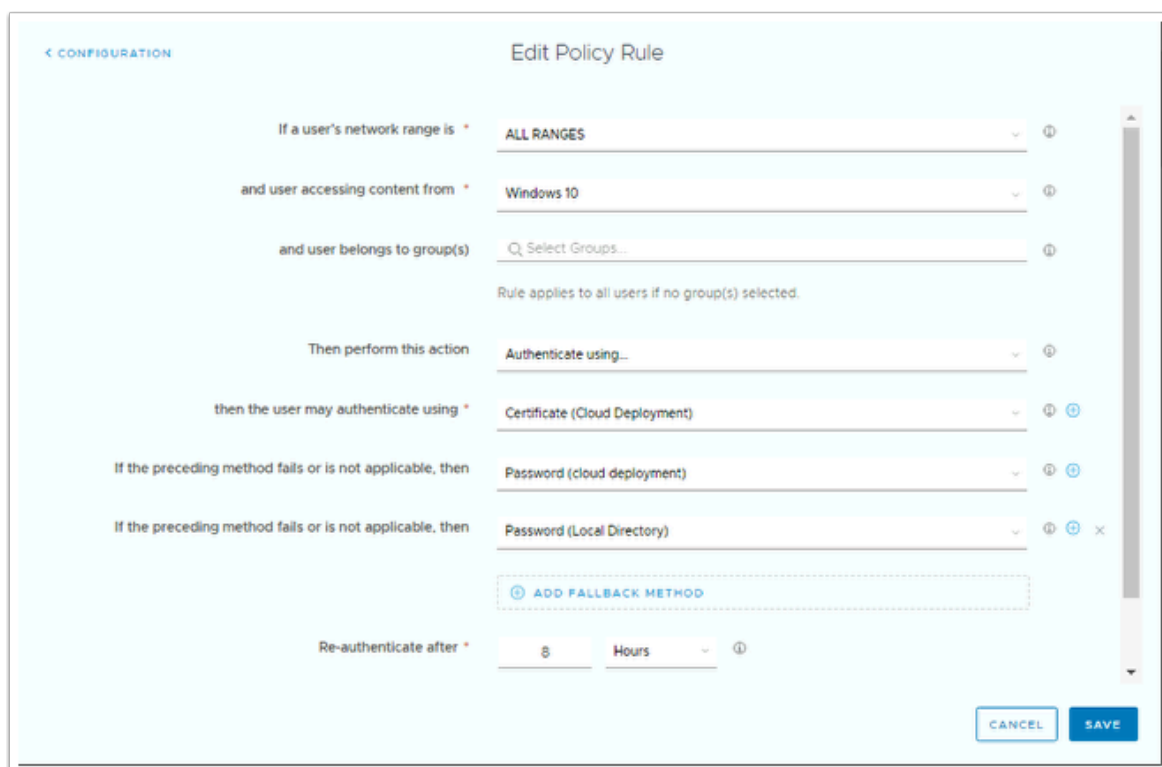
10. In the **Edit Policy Rule** window
- Next to **then the user may authenticate using \*** to select **Certificate (Cloud Deployment)**
  - Next to **if preceding method fails or is not applicable, then \*** select **Password (Cloud Deployment)**,



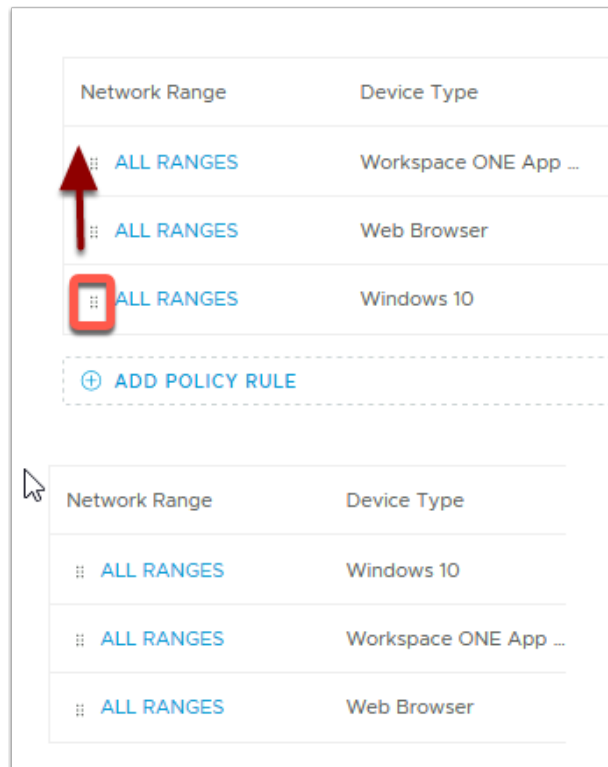
- Select **ADD FALLBACK METHOD**
- Next to **if preceding method fails or is not applicable, then \*** select **Password (Local Directory)**
- Click **SAVE** at the bottom of the window



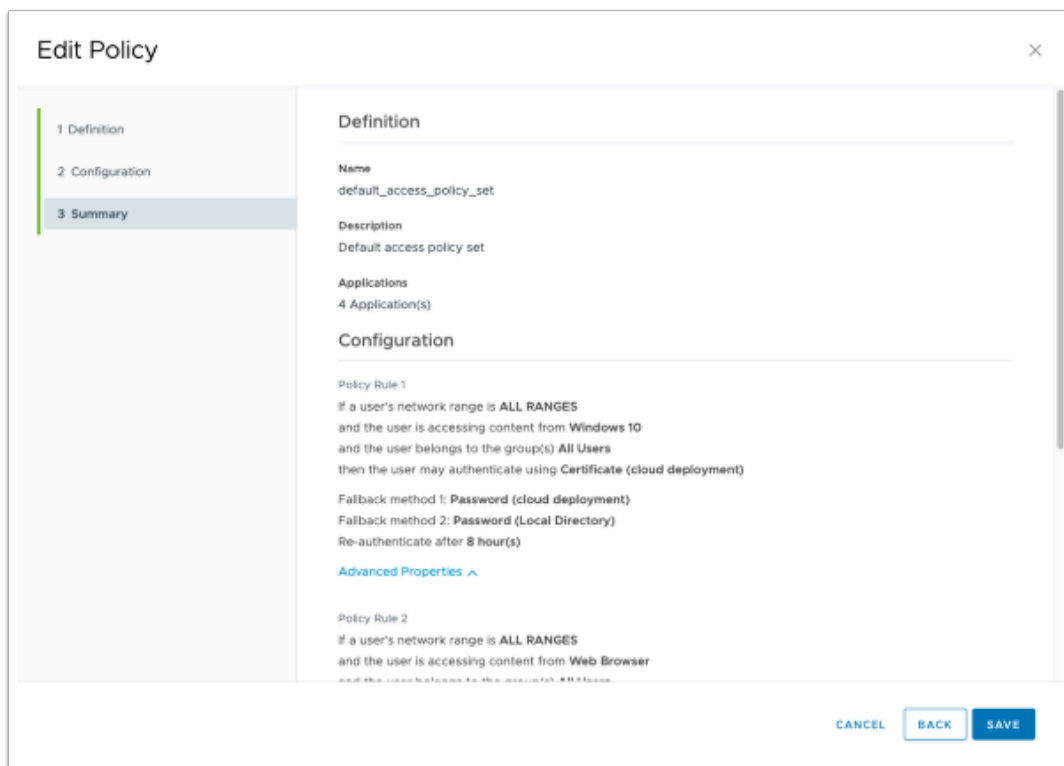
11. Click **ADD POLICY RULE** in the **Configuration** tab of **Edit Policy** page.



12. Select **Windows 10** from the **user accessing content** from drop down.
- Select **Certificate (Cloud Deployment)** for the first authentication method
  - Select **Password (cloud deployment)** for **if the preceding method fails ...**
  - Select **Password (Local Directory)** for **if the preceding method fails ...**
  - Click **SAVE** at the bottom right hand side of the page



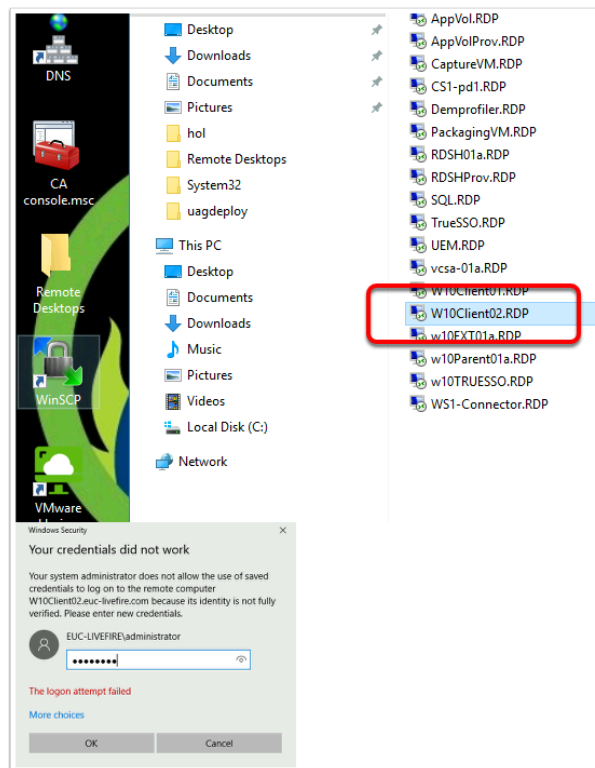
13. Next to **ALL RANGES for Windows 10** on the left select the **6 DOTS** and drag to the top
  - Select **NEXT** on the **Edit Policy Page**



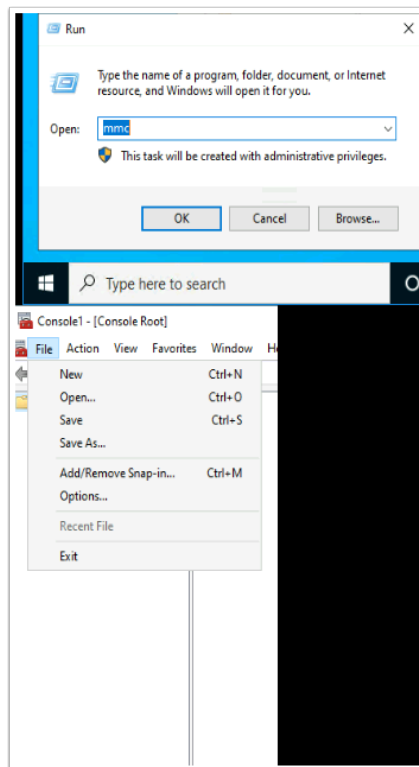
14. Select **SAVE** on the Summary tab of the **Edit Policy** Page.
  - You have now enabled Certificate (Cloud Deployment) as an authentication method on the default access policy.

- Our next step is to ensure this implementation is working.

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

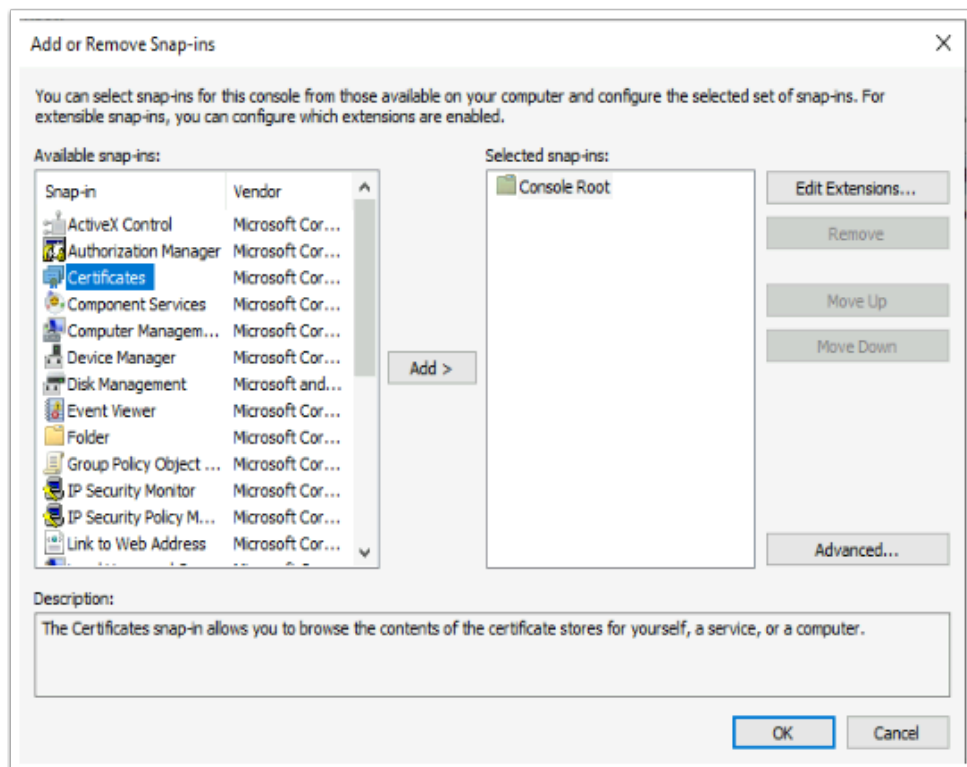


1. On the **ControlCenter2** server Desktop,
  - Open the **Remote Desktops** folder, select the **W10Client02.RDP** session
  - Log in as **EUC-Livefire\administrator**, enter the password **VMware1!**, select **OK**



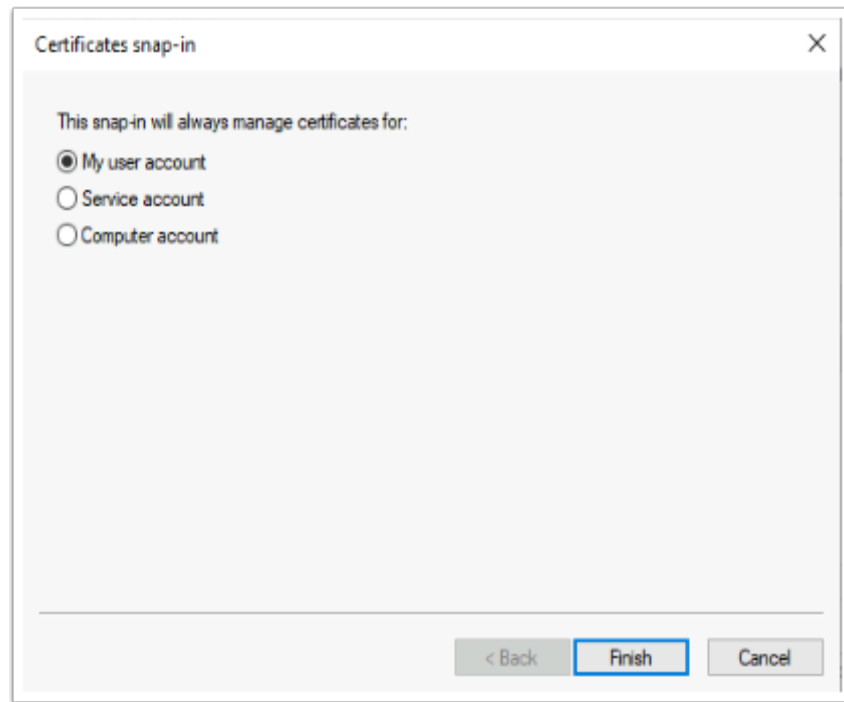
## 2. On **W10Client02** desktop

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

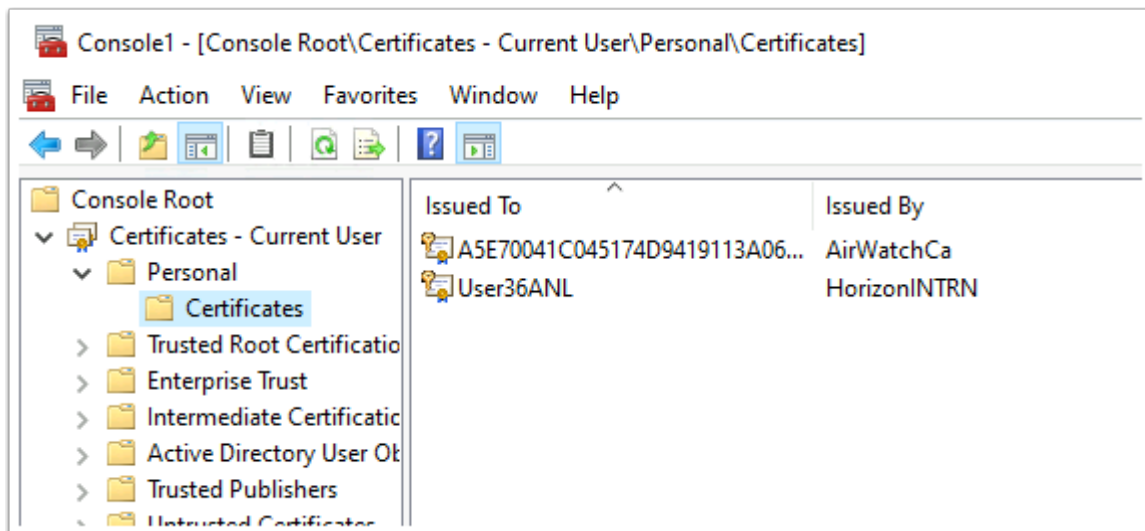


## 3. In the **Add or Remove Snap-ins** window

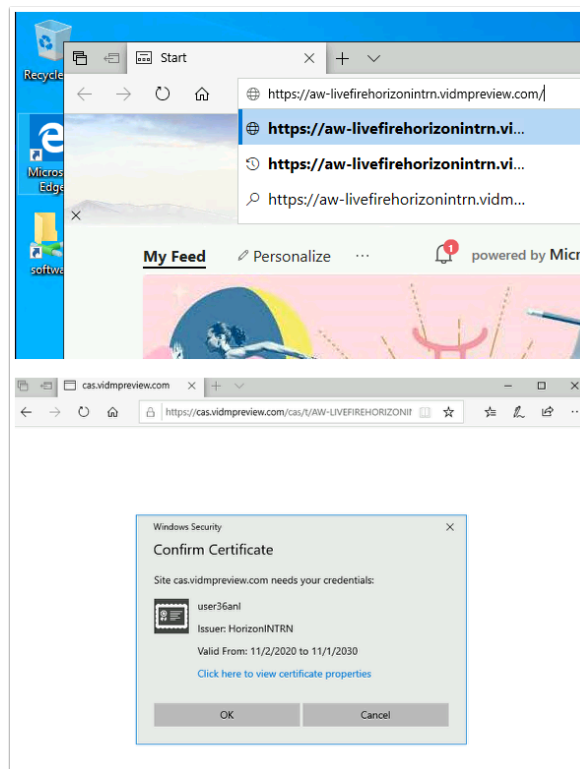
- Select **Certificates**, select **Add**



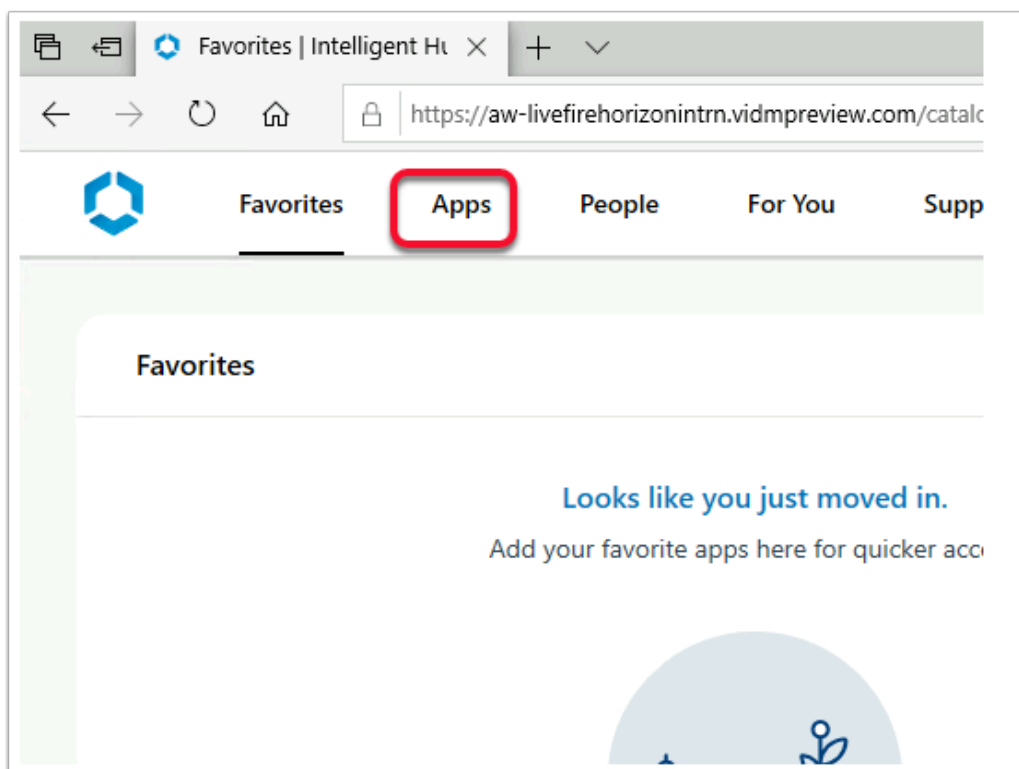
4. In the **Certificates snap-in**, accept the Defaults, select **Finish**
  - Select **OK**



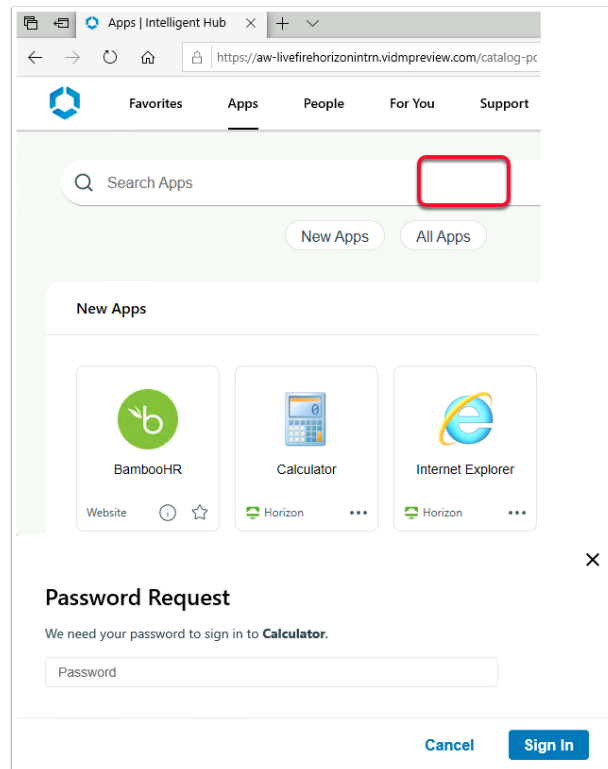
5. **Expand Certificates - Current User**
  - **Expand Personal**
  - Select **Certificates**
    - Note you have an enrolled certificate. If you dont have a certificate, reach out for support.



6. On your **W10Client02** Desktop
  - Open a **browser** on your windows 10 desktop and enter the **URL of your SaaS Access Tenant**
  - On the **Select a certificate** window note the account of the certificate and select **OK**



7. On the **Workspace ONE** console , Select the **Apps** tab

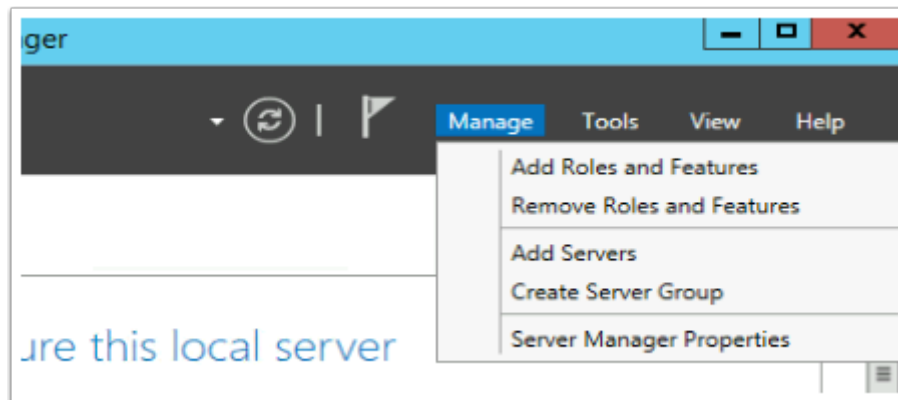


## 8. Select **Calculator**,

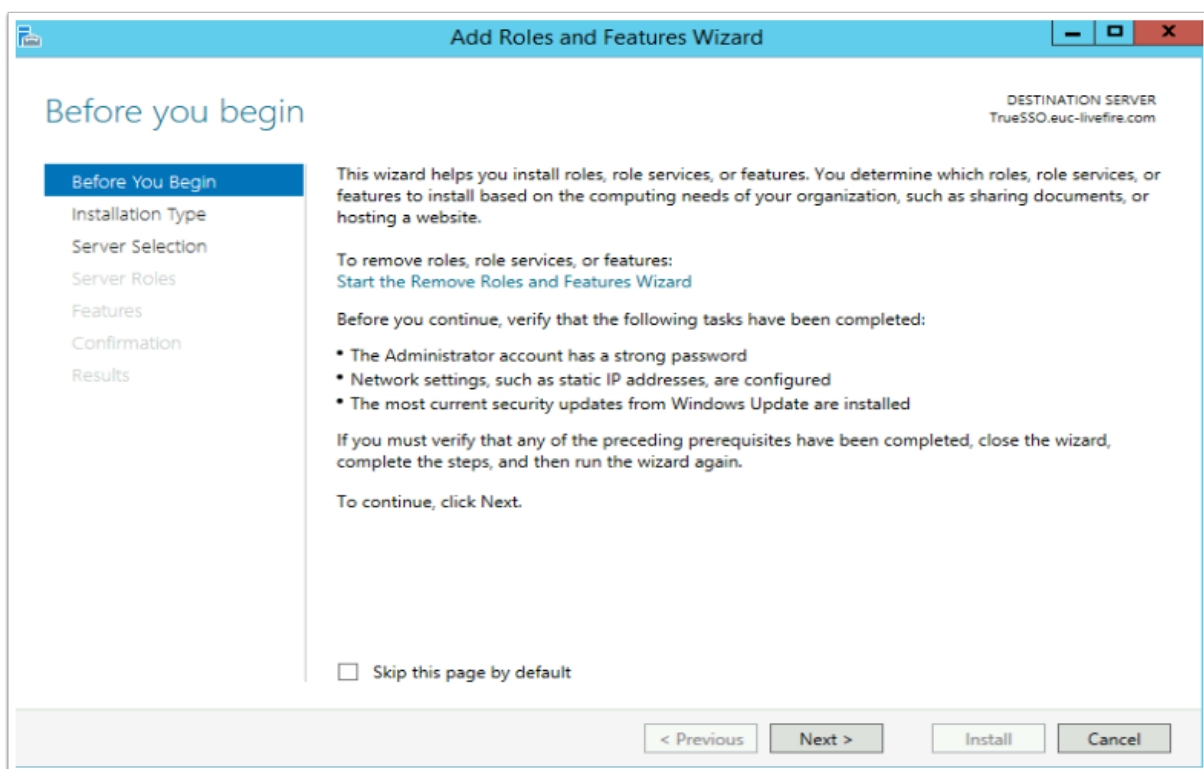
- Notice we are getting a Password request.
  - The 1st reason is, we used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password Auth method, to pass on to the Horizon Agent.
  - Up to version 1903, Workspace ONE Access would CACHE the credential when a password method of Authentication was used to login to the Console. Prior to version 20.01 or up to version 1903, when a user logged into Workspace ONE Access with a password method of authentication, the user would enjoy a Single-Sign on experience. It was therefore only necessary to Deploy TRUESSO if the users were authenticating with an Auth method that was NOT password based.
  - From version 20.01 SaaS onwards, the automatic CACHING of password credentials is no longer a feature in Workspace ONE Access. This is an enhancement of Workspace ONE Access security.
  - In June this year a feature was re-introduced to allow Automatic Caching of Passwords on the SaaS Instance of Access
  - We however still need Enrollment services when authenticating with 3rd party auth methods
- In the next Part, we will proceed with the deployment of TRUESSO to solve this challenge.
- Select **Cancel** to close the **Password Request** window.
- **Logout** and **close** all windows on **W10Client02**

## Part 4. Installing a sub-ordinate CA and the Enrollment

## services

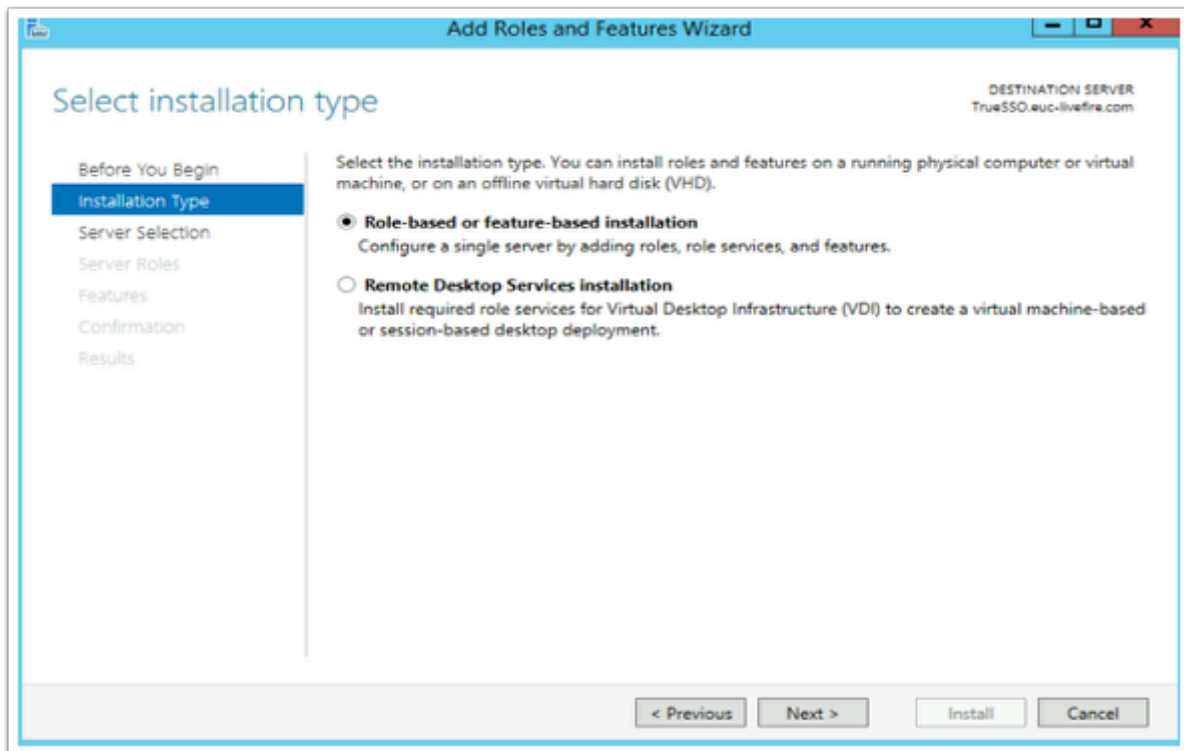


1. On your **ControlCenter2** server
  - Open the **Remote Desktop** Folder and launch **TrueSSO.RDP** shortcut
  - On the **Server Manager** Interface select **Manage > Add Roles and Features**

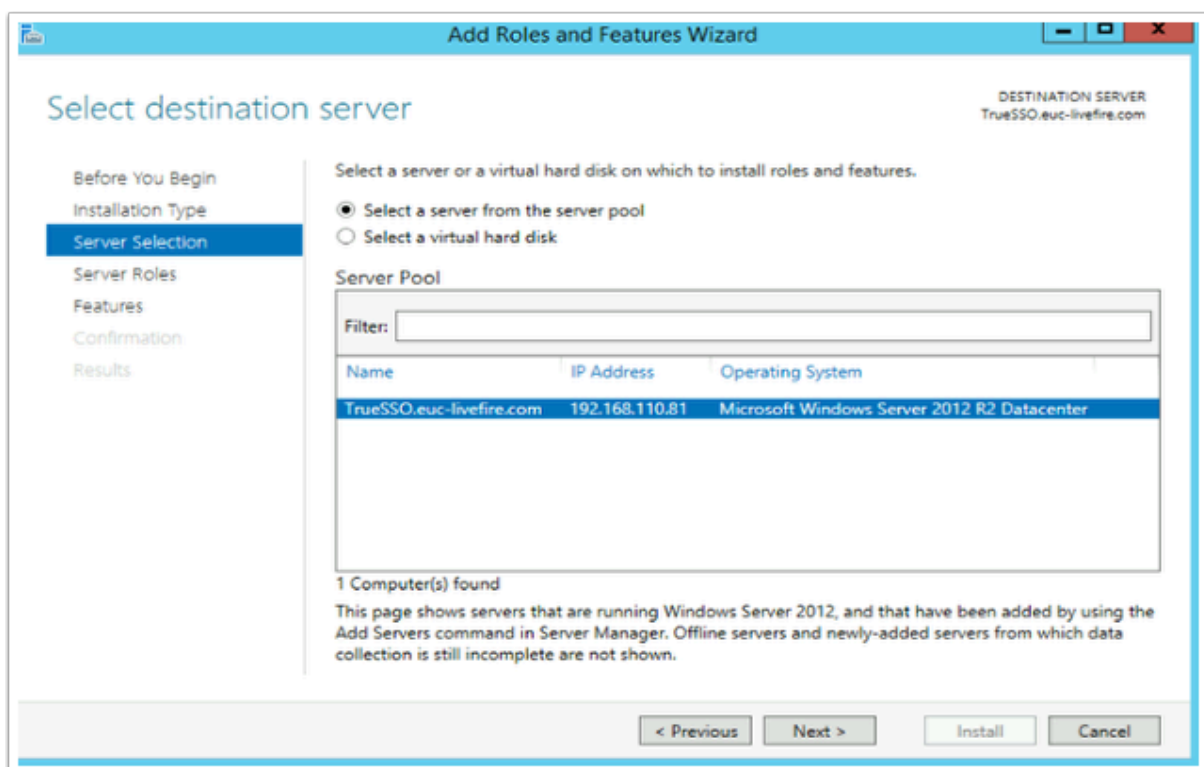


2. On the **Before you begin** window select **Next**

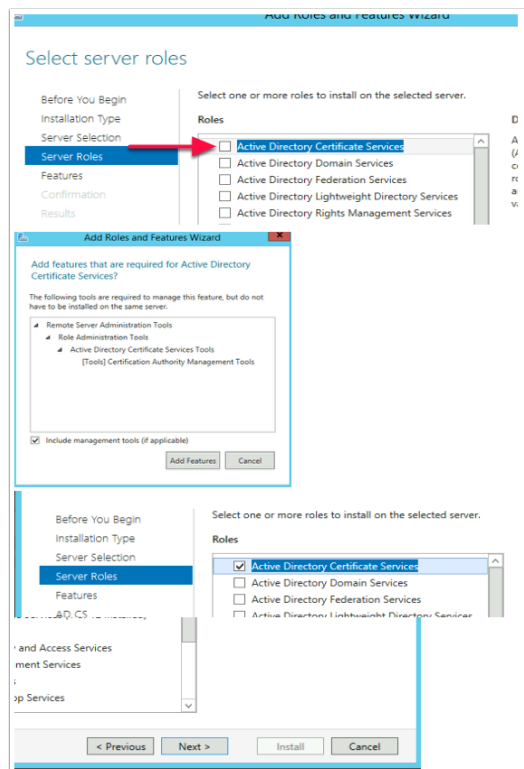




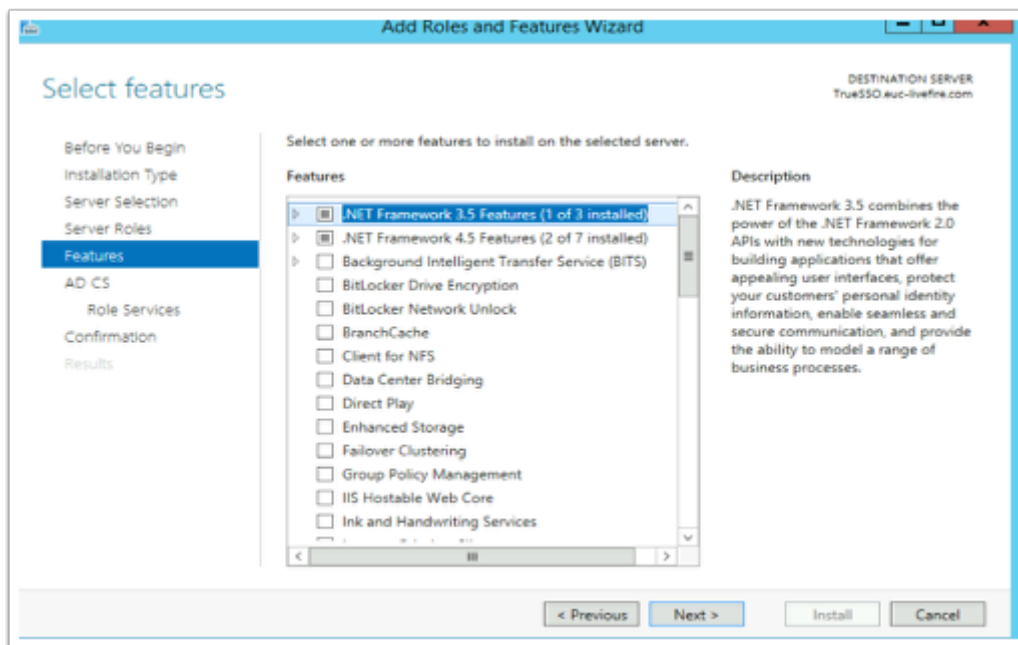
3. On the **Select installation type** window, ensure the **radio button** in front of **Role-based or feature-based installation** is selected select **Next**



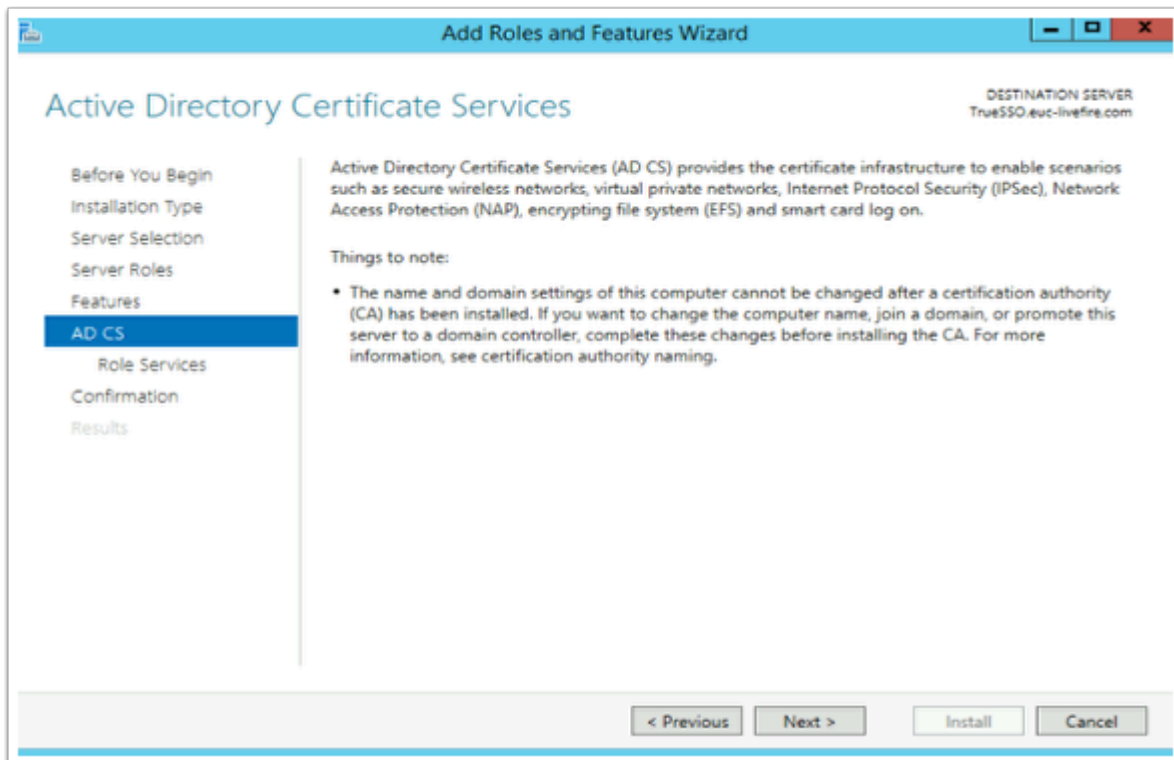
4. On **Select destination server** window (accept the defaults) select **Next**



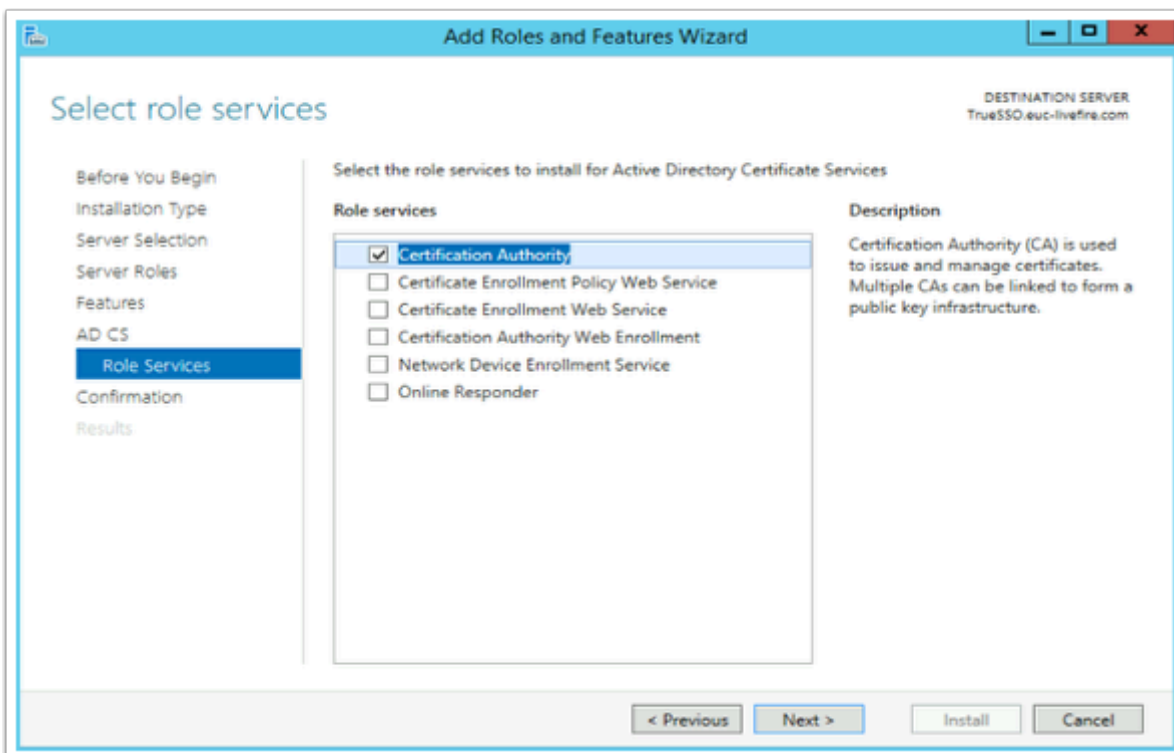
- On the **Select server roles** window, select the **check box** in front of **Active Directory Certificate Services**, when prompted for the **Add Features** window, select **Add Features** box, then select **Next**



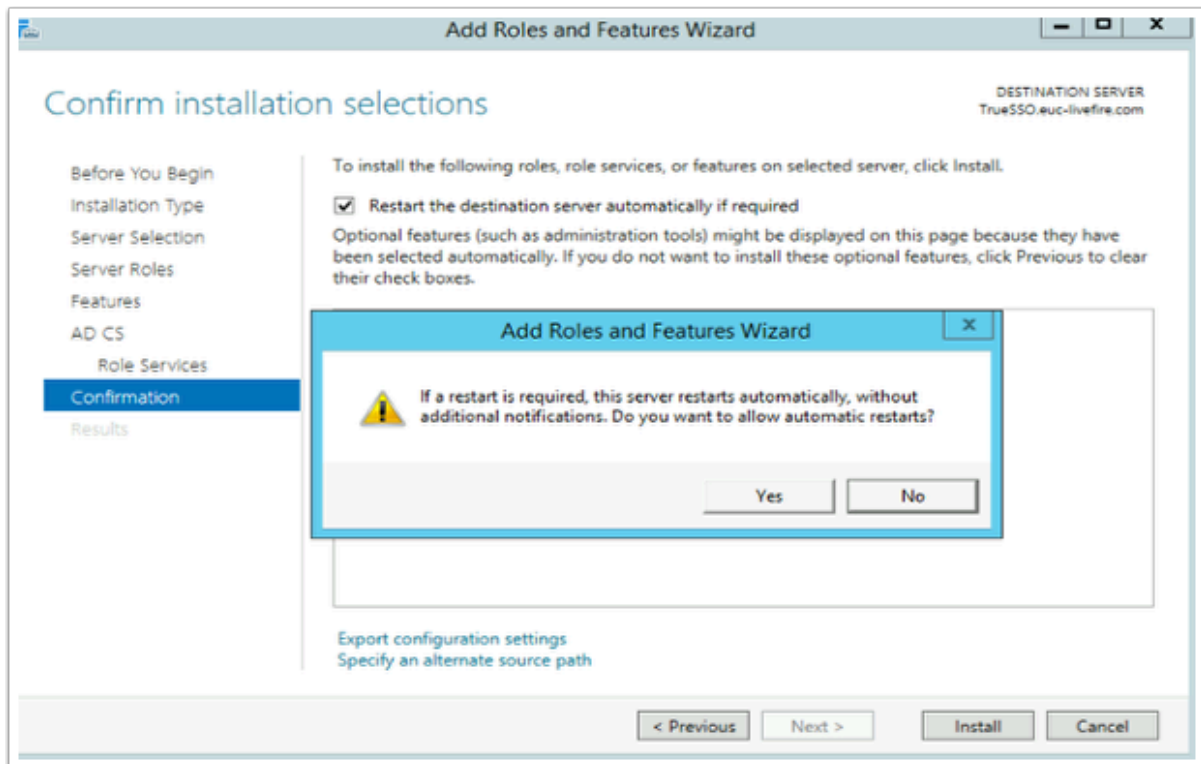
- On the **Select features** window select **Next**



7. On the **Active Directory Certificate Services** window select **Next**

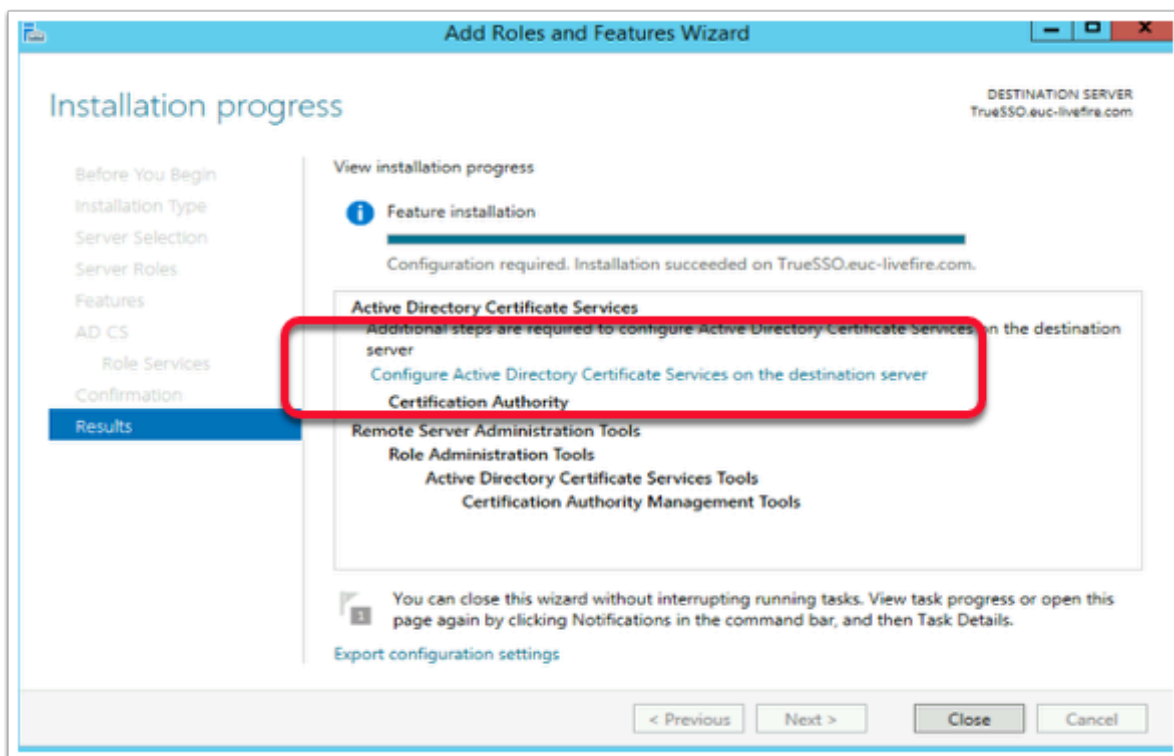


8. On the **Select role services** window select **Next**

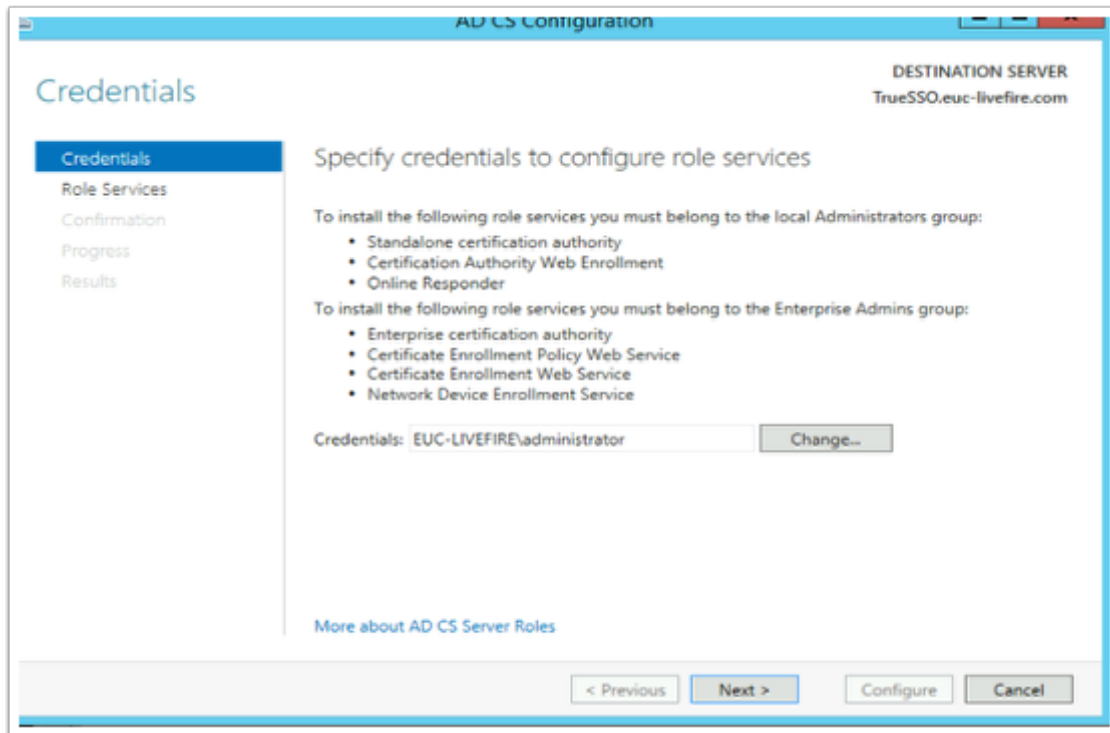


9. On the **Confirm Installation selections** window, select the **checkbox** next to **Restart the destination server automatically if required**, on the **Add Roles and Features Wizard** window select **Yes** and then select **Install**

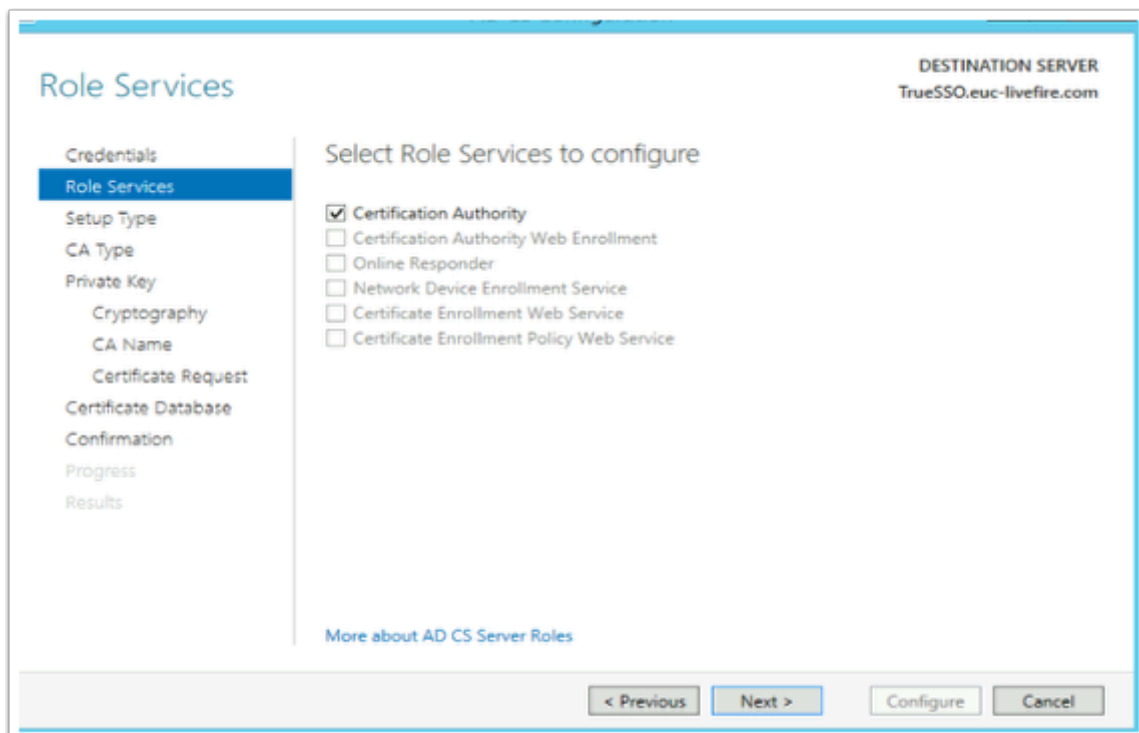
You will have to wait a short while before moving on to step 11.



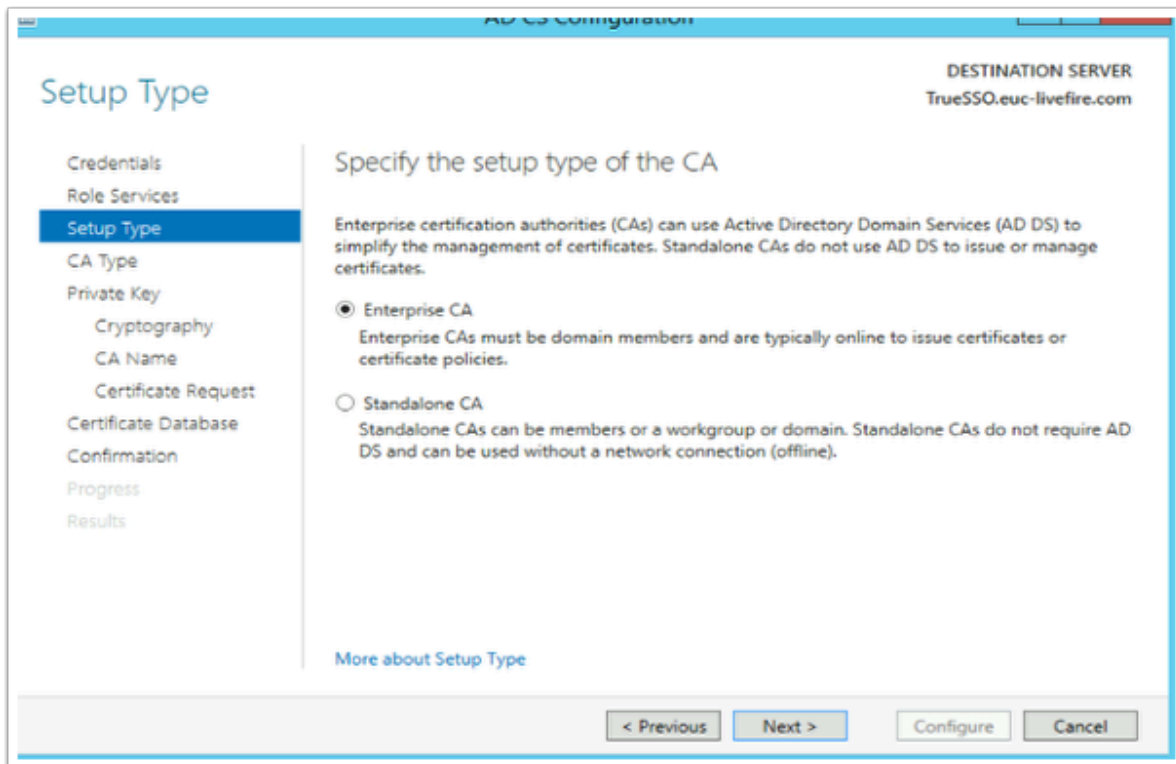
10. On the **Installation progress** page, select the **Configure Active Directory Certificate Services on the destination server** hyper-link



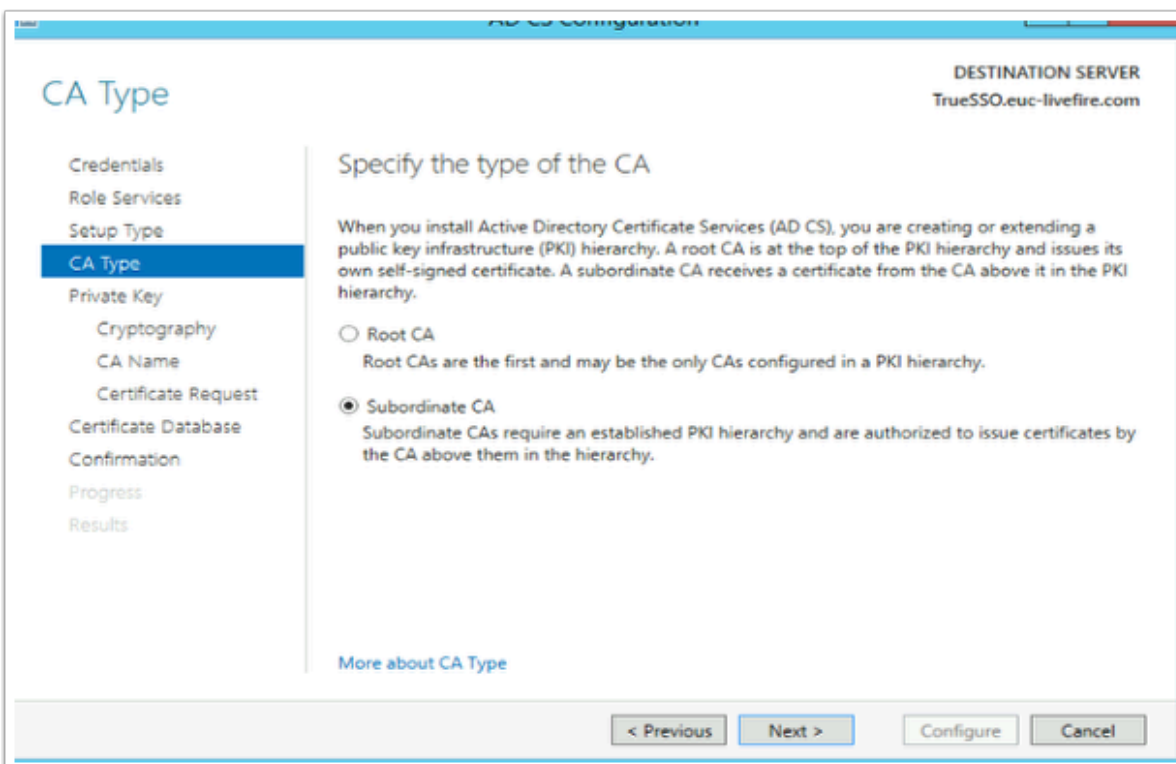
11. On the **Credentials** window select **Next**



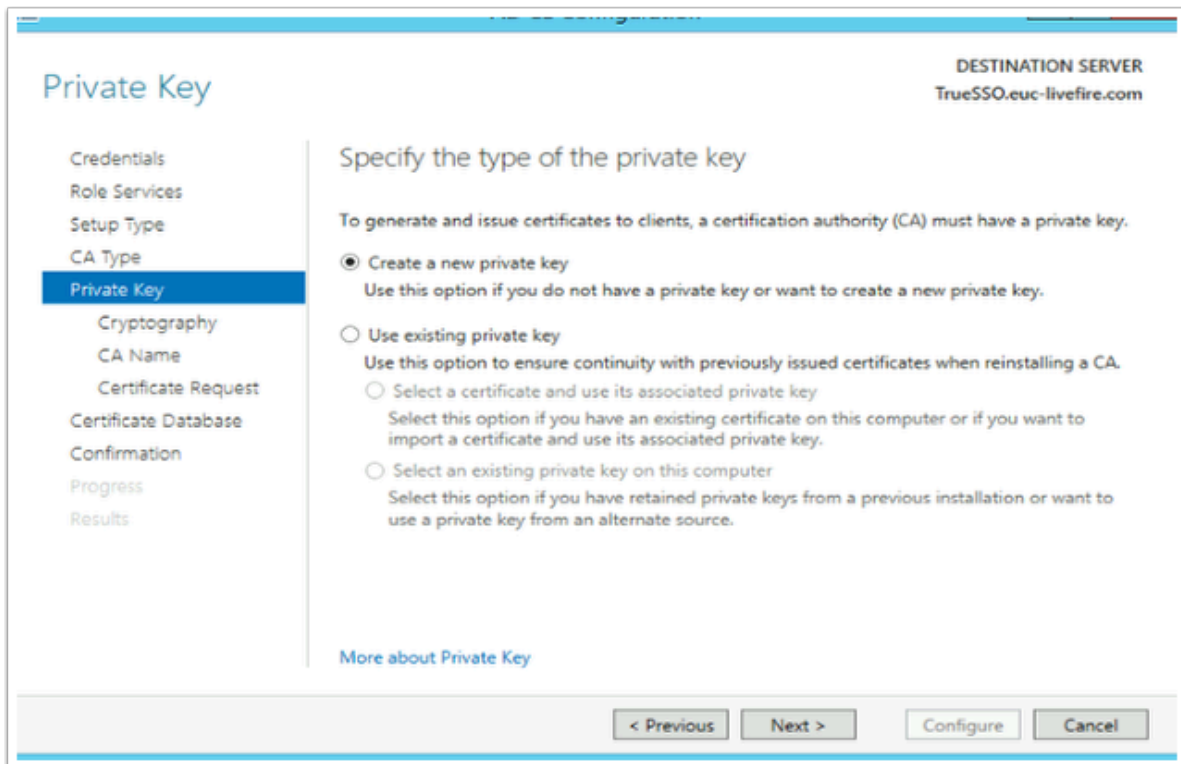
12. On the **Role Services** page, select the **Certificate Authority** checkbox



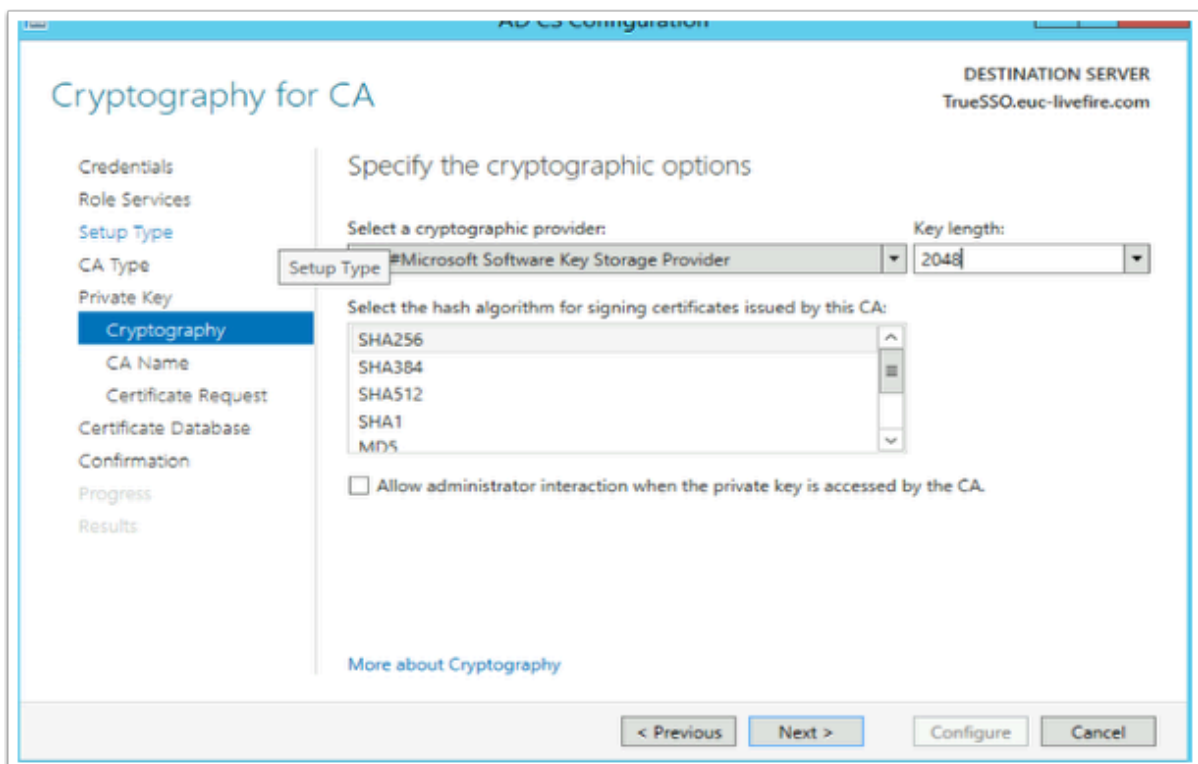
13. On the **Specify the setup type of the CA** window , select the **radio button** next to **Enterprise CA** and select **Next**



14. On the **CA type** window ensure the **Subordinate CA** **radio button** is selected, select **Next**



16. On the **Private Key** window, ensure the **radio button** next to **Create a new private key** is selected and select **Next**



17. On the Cryptography for CA window select the following
  - Under **Cryptographic Provider:** **RSA#Microsoft Software Key Storage Provider**
  - Next to **Key Length:** **2048**



- Hash Algorithm: **SHA256**
- Select **Next**

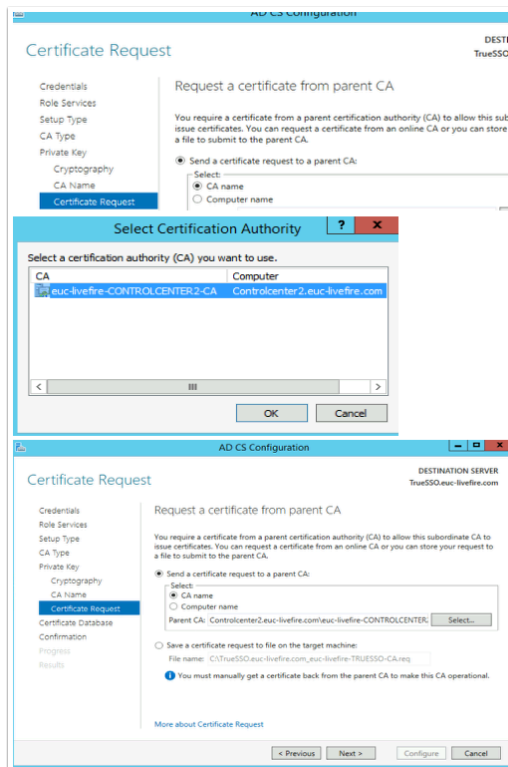
The screenshot shows the 'AD CS Configuration' window with the 'CA Name' step selected in the left-hand navigation pane. The main area is titled 'Specify the name of the CA'. It contains a text box for 'Common name for this CA:' with the value 'euc-livefire-TRUESSO-CA'. Below it is a text box for 'Distinguished name suffix:' with the value 'DC=euc-livefire,DC=com'. A 'Preview of distinguished name:' text box shows 'CN=euc-livefire-TRUESSO-CA,DC=euc-livefire,DC=com'. At the bottom right, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'TrueSSO.euc-livefire.com'.

18. On the **CA Name** window observe the CA naming convention and select **Next**

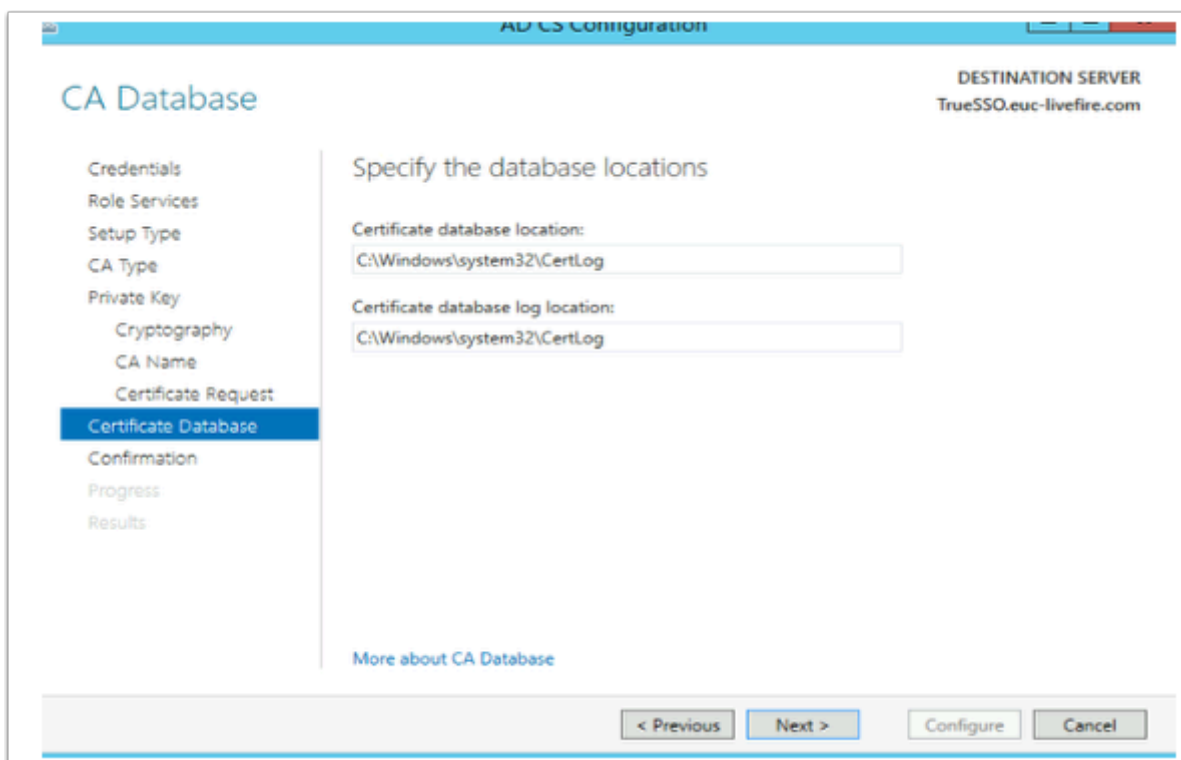
This screenshot is identical to the one above, showing the 'AD CS Configuration' window at the 'CA Name' step. The 'Common name for this CA:' is 'euc-livefire-TRUESSO-CA', the 'Distinguished name suffix:' is 'DC=euc-livefire,DC=com', and the 'Preview of distinguished name:' is 'CN=euc-livefire-TRUESSO-CA,DC=euc-livefire,DC=com'. The 'Next >' button is highlighted, indicating the next step in the process.

19. On the **Specify the name of the CA** window select **Next**

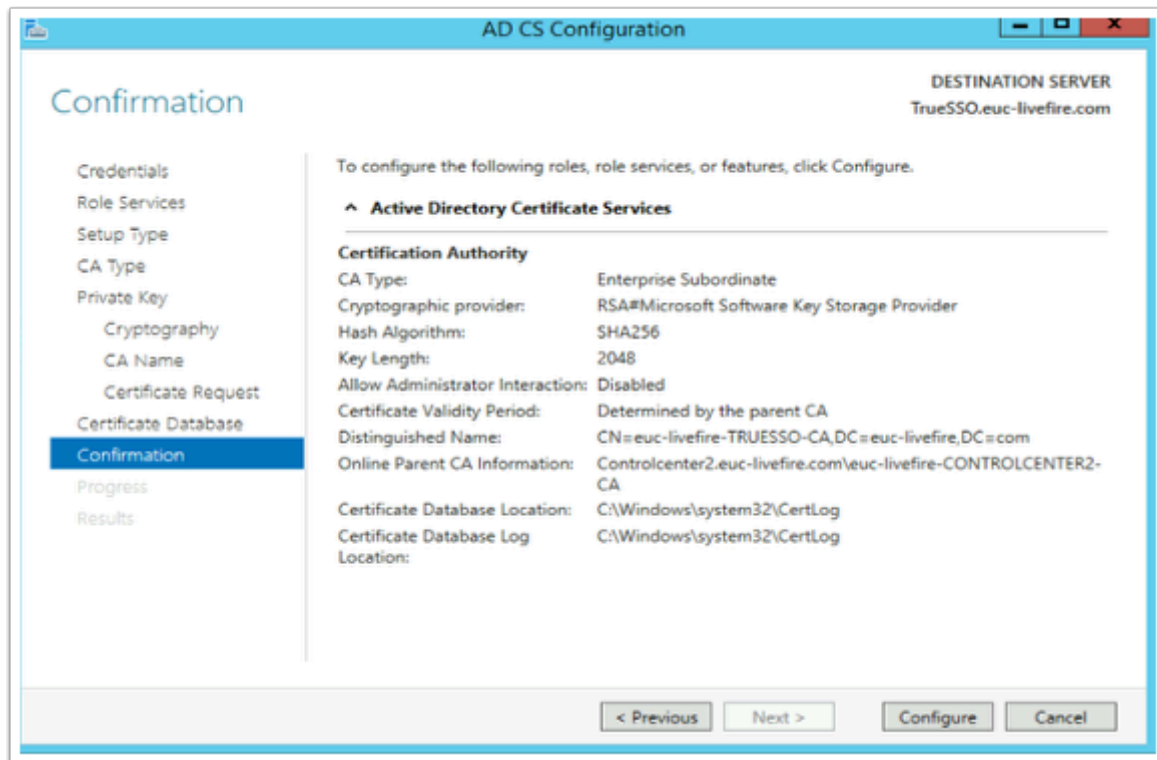




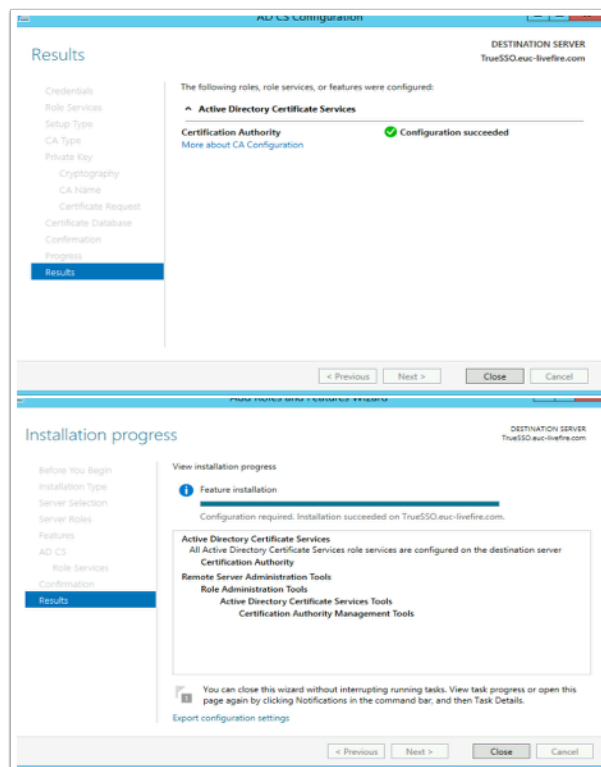
20. On the **Request a certificate from parent CA**, select the **radio button** next to **Send a certificate request to a parent CA**:
- To the right of the **Parent CA** box click the **Select** button
  - Select **OK** accept the Default and select **Next**



21. On the **CA Database** window, select **Next**

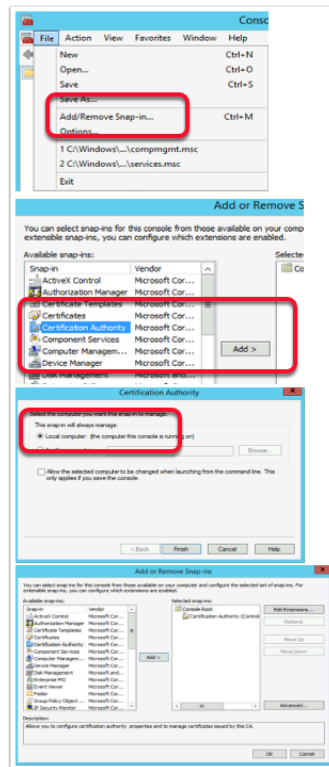


22. On the **Confirmation** window select **Configure**

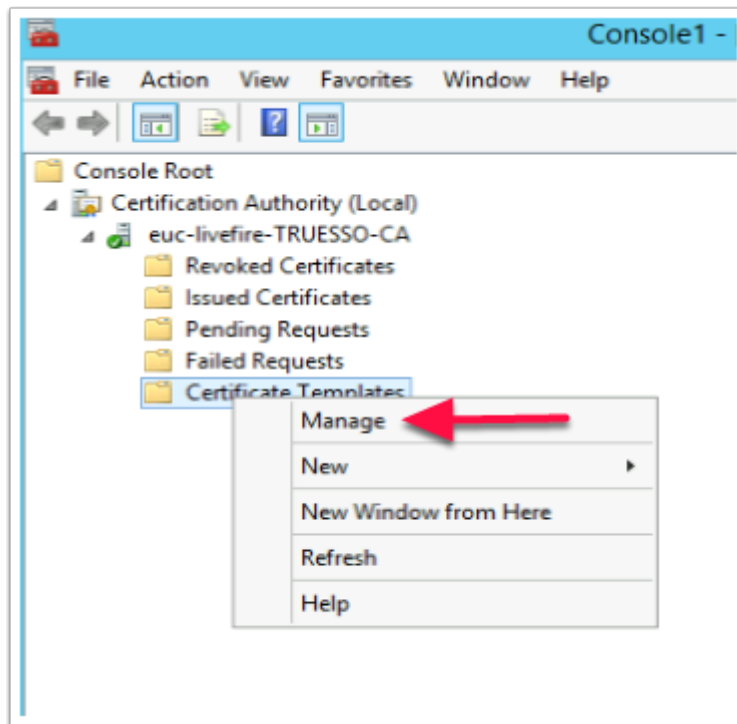


23. On the **Results** window select **Close** on the **Installation progress** window, select **Close**

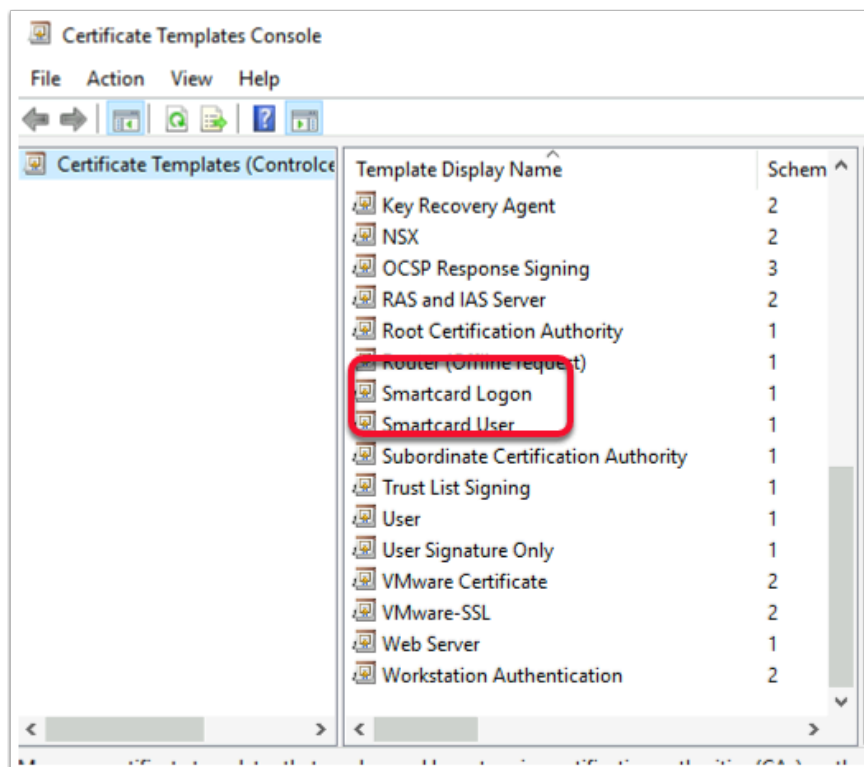
## Part 5: Deploying and Configuring Horizon TRUE SSO



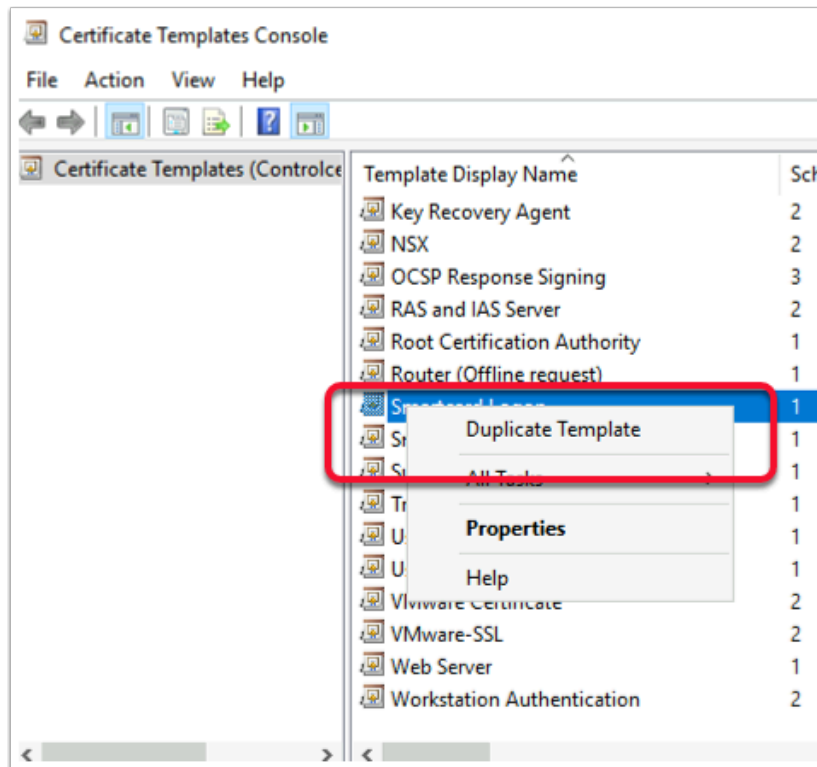
1. In this section we will create a certificate template for Horizon TRUE SSO
  - On your **TRUESSO** server select **Start** > **Run** > type **mmc**
  - Select **File** > **Add/Remove Snap-in...**
  - Select the **Certificate Authority** services snap-in, select **Add**
  - In the Certificate Authority window,
    - Select the **Local computer** radio button
    - Select **Finish**
  - Select **OK** to close the **Snap-ins** window



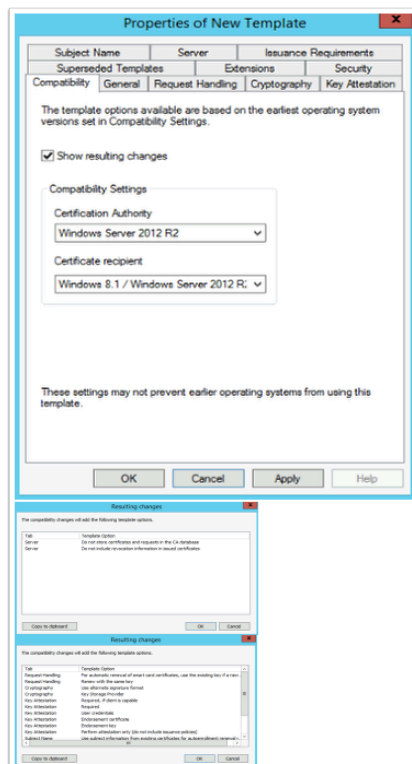
2. Expand the **euc-livewire-TRUESSO-CA** inventory
  - Select **Certificate Templates**, right-click and select **Manage**



3. In the **Certificate Template** Console find and select the **Smartcard Logon** template

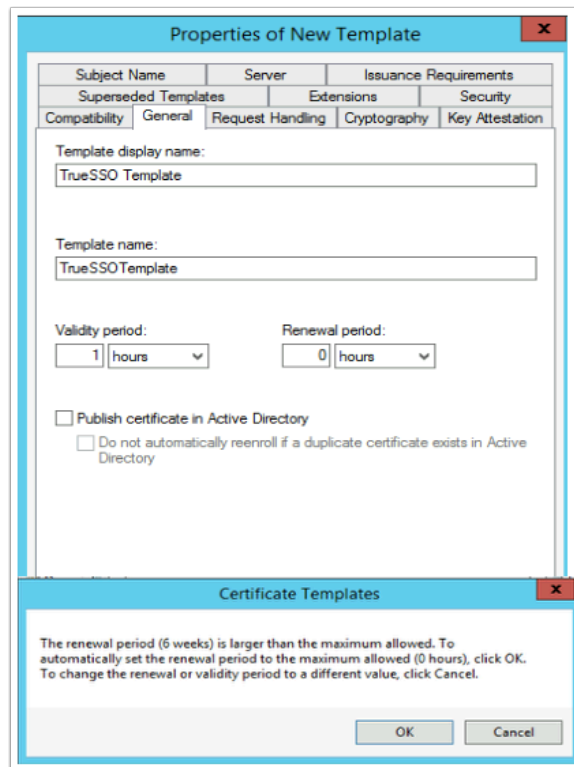


4. Right-click the **Smartcard Logon** template and select **Duplicate Template**



5. In the **Properties of New Template** window in the **Compatibility** tab under **Certificate Authority**
- Change from **Windows 2003** to **Windows 2012 R2**
  - When prompted for the **Resulting changes** window select **OK**.

- Under **Certificate recipient** change **Windows XP / Server 2003** to **Windows 8.1 / Server 2012 R2**
  - When prompted for the **Resulting changes** window select **OK**.



6. Select the **General** tab,
  - Under **Template display name:** type **TrueSSO Template**, you will notice Template name gets filled in automatically.
  - Under **Validity period** change the period from **1 years** to **1 hours**
    - When prompted by **the Certificate Templates Box** select **OK**
  - The **Renewal period** will automatically change from **6 weeks** to **0 hours**

The screenshot shows the 'Properties of New Template' dialog box with the 'Request Handling' tab selected. The 'Purpose' dropdown is set to 'Signature and smartcard logon'. Three checkboxes are present: 'Delete revoked or expired certificates (do not archive)' (unchecked), 'Include symmetric algorithms allowed by the subject' (unchecked), and 'Archive subject's encryption private key' (unchecked). Below these, 'Allow private key to be exported' is checked, 'Renew with the same key' is unchecked, and 'For automatic renewal of smart card certificates, use the existing key if a new key cannot be created' is checked. At the bottom, under the heading 'Do the following when the subject is enrolled and when the private key associated with this certificate is used:', the 'Prompt the user during enrollment' radio button is selected. The 'Cancel' button is highlighted with a blue border.

7. Select the **Request Handling** tab change the following next to :-
- **Purpose:** change: **Signature and encryption** to **Signature and smartcard logon**.
  - Select the **checkbox** in front of **Allow private key to be exported**
  - Select the **checkbox** in front of **For automatic renewal of smartcard certificates, use the existing key if a new key cannot be created**
  - Select the **radio button** in front of **Prompt the user during enrollment**

**Properties of New Template**

|                      |            |                       |
|----------------------|------------|-----------------------|
| Subject Name         | Server     | Issuance Requirements |
| Superseded Templates | Extensions | Security              |
| Compatibility        | General    | Request Handling      |
| Cryptography         |            | Key Attestation       |

Provider Category:

Algorithm name:

Minimum key size:

Choose which cryptographic providers can be used for requests

☒ Requests can use any provider available on the subject's computer

☐ Requests must use one of the following providers:

Providers:

☐ Microsoft Software Key Storage Provider

Request hash:

☐ Use alternate signature format

OK Cancel Apply Help

8. Select the Cryptography tab change the following next to

- **Provider Category:** Key Storage Provider
- **Minimum key size:** 2048
- **Request hash:** SHA256

**Properties of New Template**

|                      |            |                       |              |                 |
|----------------------|------------|-----------------------|--------------|-----------------|
| Compatibility        | General    | Request Handling      | Cryptography | Key Attestation |
| Superseded Templates | Extensions | Security              |              |                 |
| Subject Name         | Server     | Issuance Requirements |              |                 |

☒ Do not store certificates and requests in the CA database

☐ Do not include revocation information in issued certificates

OK Cancel Apply Help



9. Select the **Server** tab,
  - Select the **checkbox** in front of **Do not store certificates and requests in the CA database**
    - You will notice that **Do not include revocation information in issued certificates** is selected automatically.
  - Uncheck the **checkbox** next to **Do not include revocation information in issued certificates**

TrueSSO Template Properties

General Compatibility Request Handling Cryptography Key Attestation  
Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

Require the following for enrollment:

☐ CA certificate manager approval

☒ This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:  
Application policy

Application policy:  
Certificate Request Agent

Issuance policies:

Add... Remove

Require the following for reenrollment:

☐ Same criteria as for enrollment

☒ Valid existing certificate

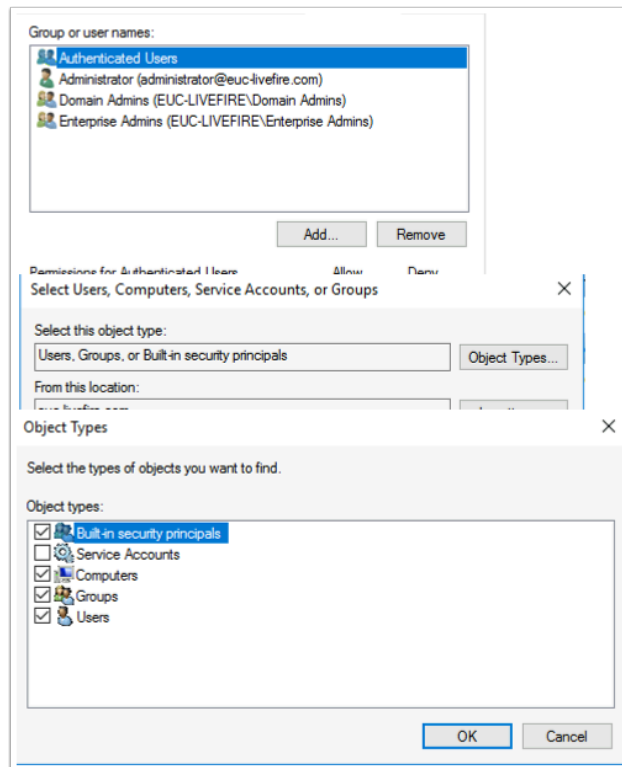
☐ Allow key based renewal (\*)

Requires subject information to be provided within the certificate request.

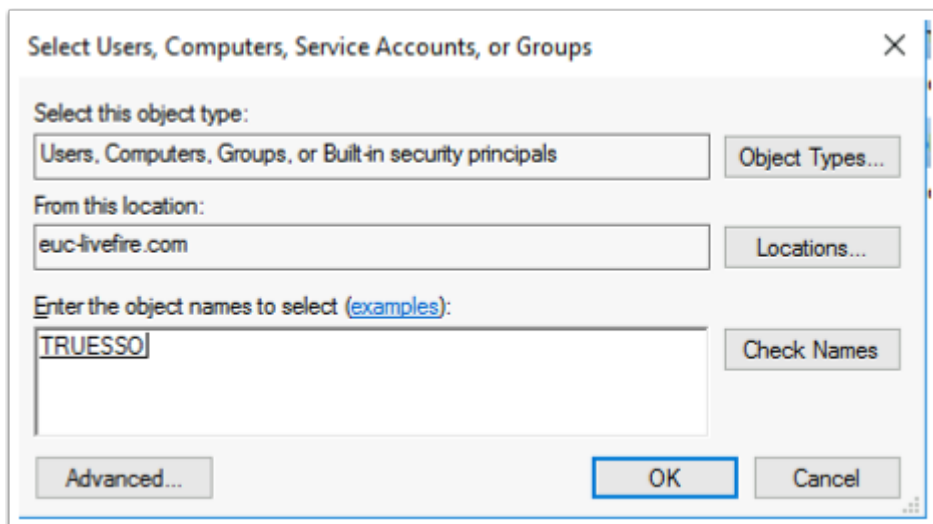
\* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

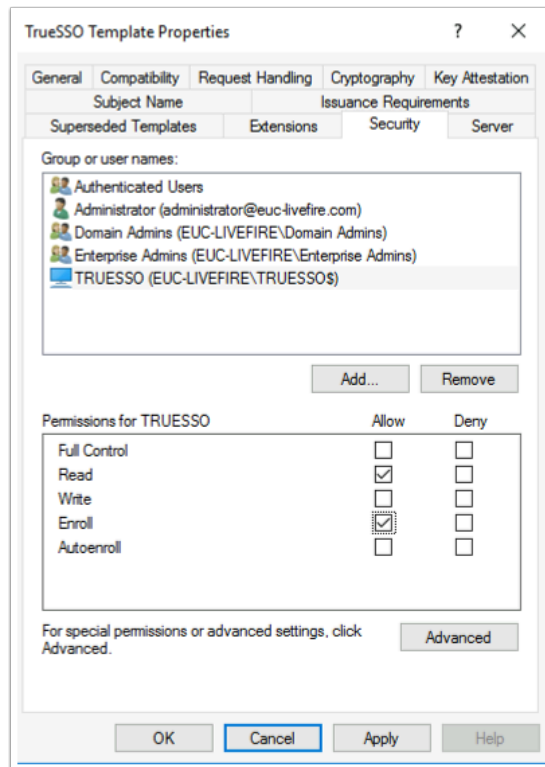
10. Select the **Issuance Requirements** tab, configure the following:
  - Select the **checkbox** : **This number of authorized signatures** and change the value to **1** in the **box**
  - Under **Policy type required in signature**
    - Ensure the **Application policy** is selected (default config)
  - Under **Application Policy**
    - Select **Certificate Request Agent** from the dropdown
  - Under the **Require the following for reenrollment**
    - Select the **Valid existing certificate radio button**



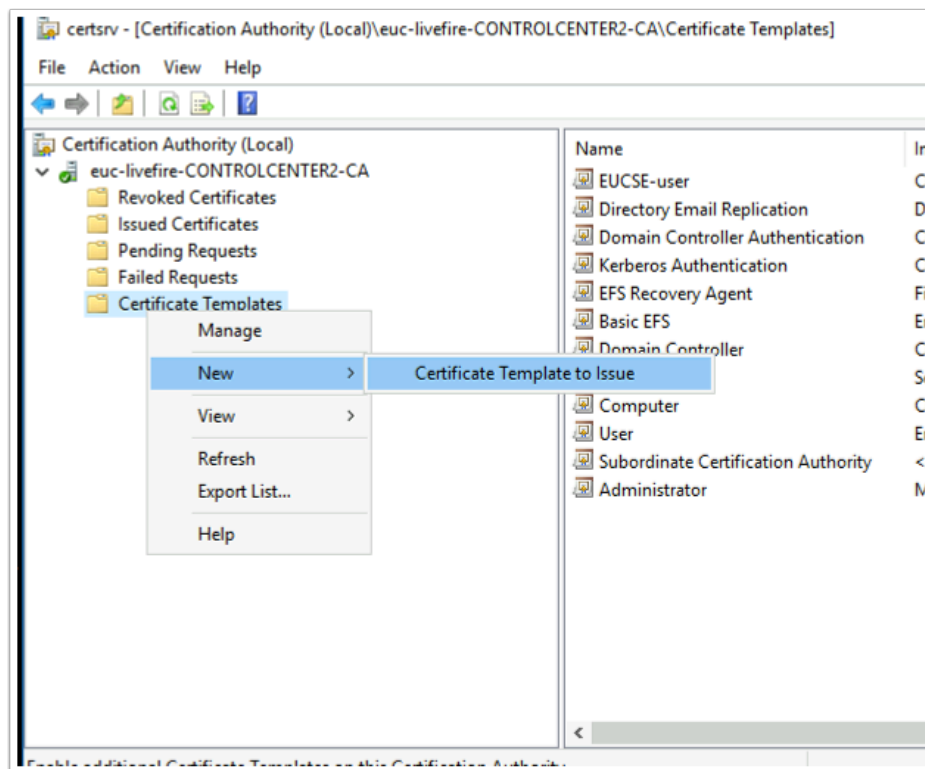
11. On the **Security** tab in the **Group or user names:** area select **Add**
  - To the right of the **Select this object type:** box select the **Object types** button
  - Select the **checkbox** next to **Computers**, select **OK**



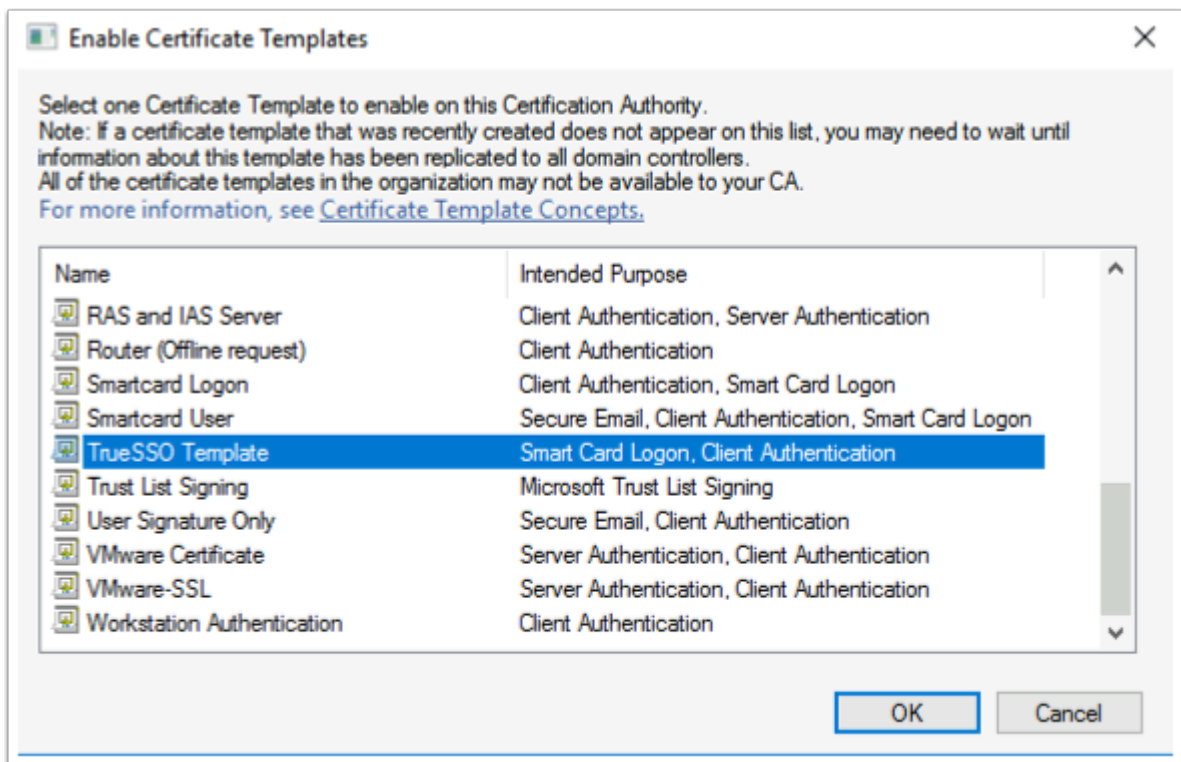
12. In the **Enter the object names to select** type **Truesso** and to the right select **Check Names** select **OK**



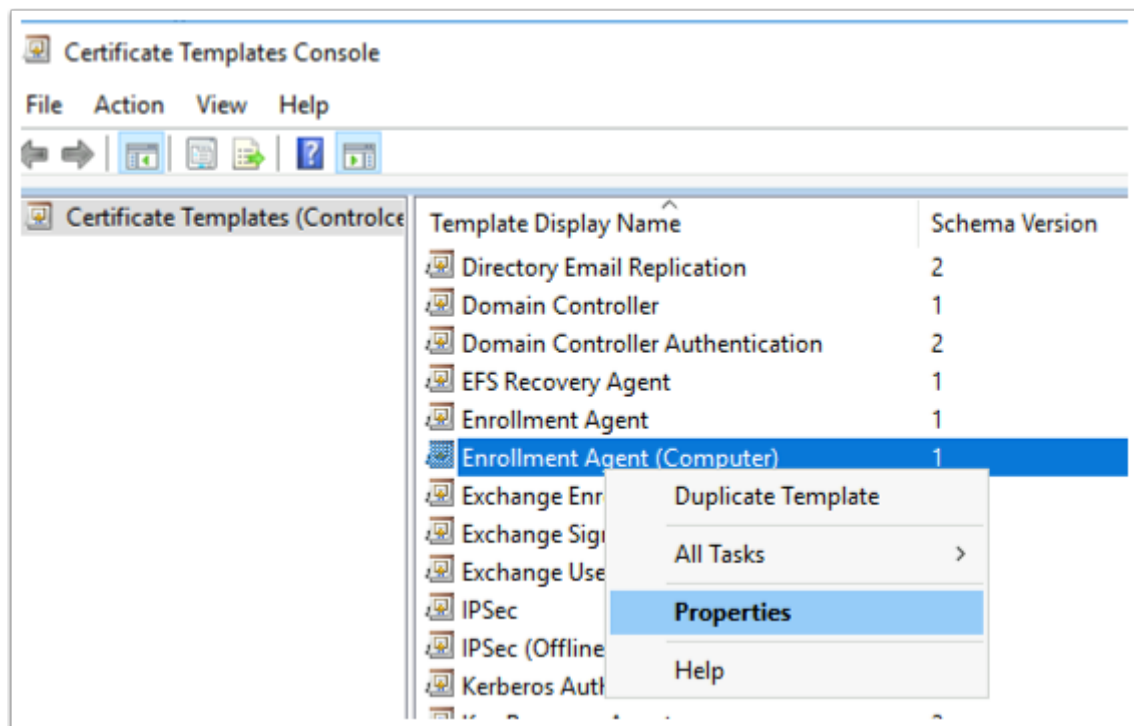
13. For the **Permissions for TRUESSO** ensure that the permission **Read** and **Enroll** checkboxes are selected.
  - Select **OK** to close the **TrueSSO Template Properties**,



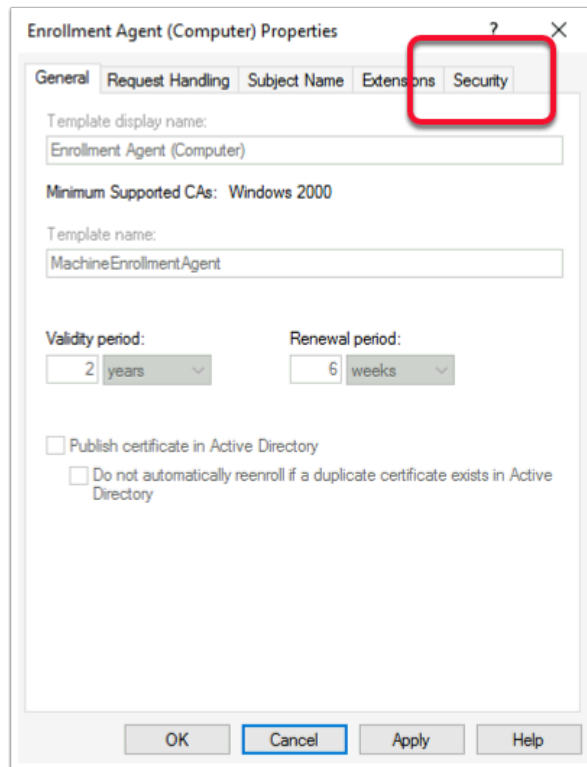
14. Switch to the **Certificate Authority Console** select and right-click the **Certificate Templates** container, select **New > Certificate Template** to Issue



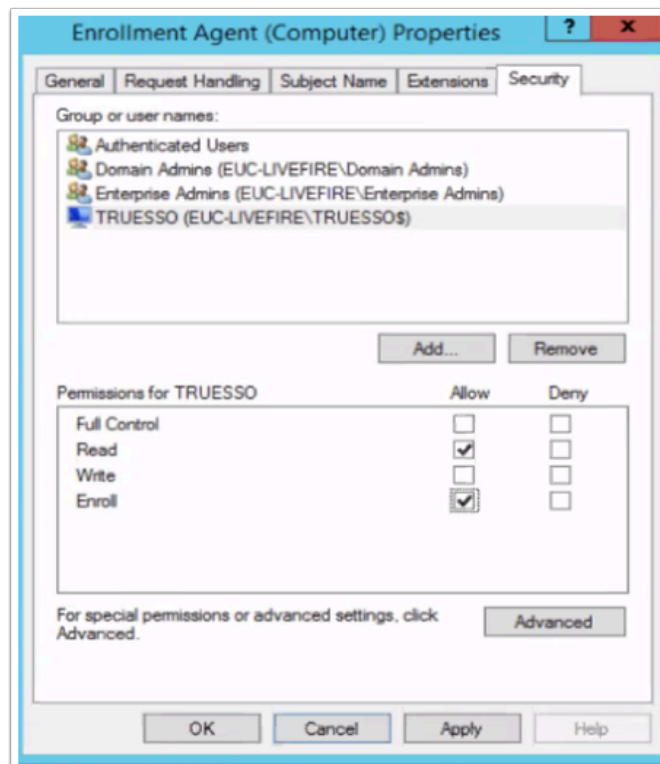
15. In the **Enable Certificate Templates** window, select your **TrueSSO Template** and select **OK**



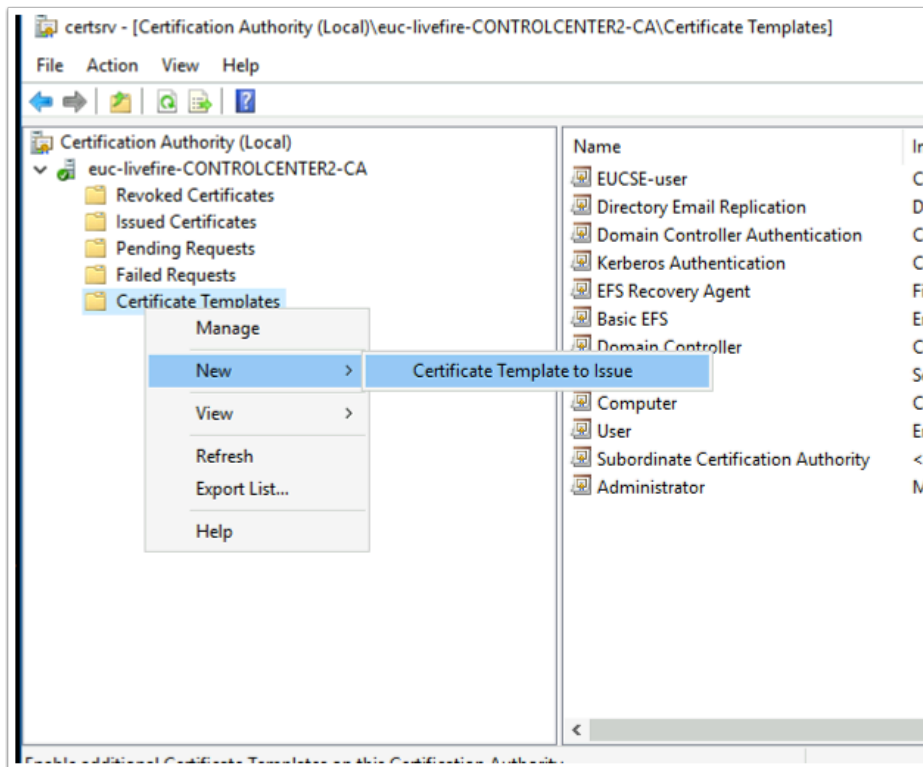
16. Switch back to the **Certificate Templates** Console select and right-click the **Enrollment Agent (computer)** template and select **Properties**



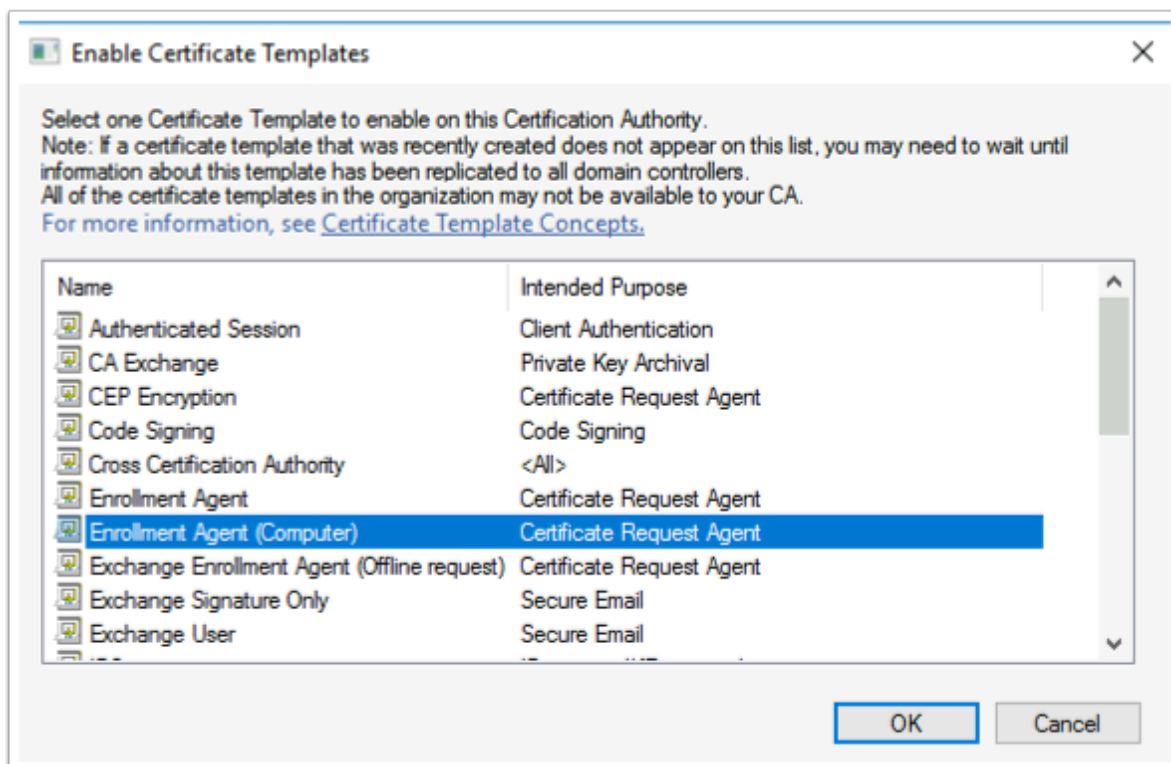
17. In the **Enrollment Agent Properties** window select the **Security** tab



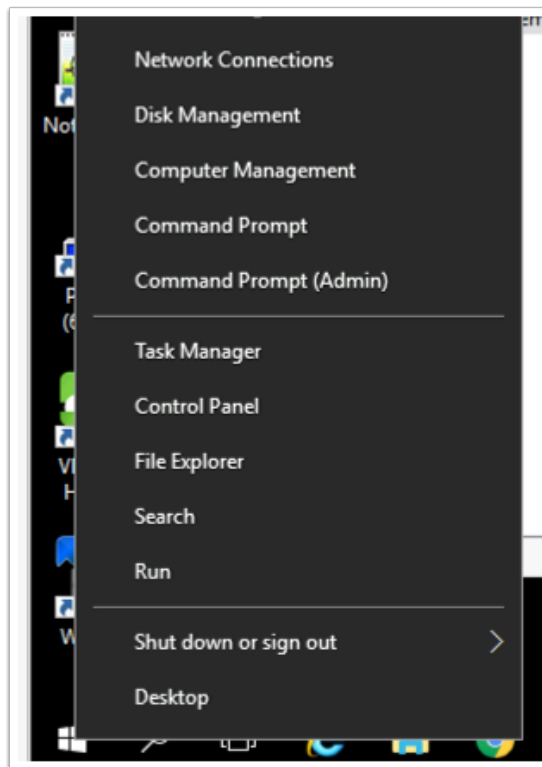
18. Select **Add** and add the **TRUESSO** Computer account with Read and **Enroll** permissions .  
Select **OK** to close the **Enrollment agent** properties



19. Switch back to the **Certificate Authority Console** select and right-click the **Certificate Templates** container, select **New > Certificate Template to Issue**



20. In the **Enable Certificate Templates** window select the **Enrollment Agent (Computer)** template and select **OK**



21. We will now configure the CA for non-persistent certificate processing

- On the **TrueSSO** server select and right-click the **Start** button and select **Command Prompt (Admin)**

```
Administrator: Command Prompt

C:\Windows\system32>certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DBFlags:

Old Value:
DBFlags REG_DWORD = b0 (176)
  DBFLAGS_MAXCACHESIZE100 -- 10 (16)
  DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
  DBFLAGS_LOGBUFFERSHUGE -- 80 (128)

New Value:
DBFlags REG_DWORD = 8b0 (2224)
  DBFLAGS_MAXCACHESIZE100 -- 10 (16)
  DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
  DBFLAGS_LOGBUFFERSHUGE -- 80 (128)
  DBFLAGS_ENABLEVOLATILEREQUESTS -- 800 (2048)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>
```

22. In the Administrator: Command Prompt enter the following commands

- `certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS`

```
C:\Windows\system32>certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\euclivefire-CONTROLCENTE
R2-CA\CRLFlags:

Old Value:
  CRLFlags REG_DWORD = 2
  CRLF_DELETE_EXPIRED_CRLS -- 2

New Value:
  CRLFlags REG_DWORD = a (10)
  CRLF_DELETE_EXPIRED_CRLS -- 2
  CRLF_REVCHECK_IGNORE_OFFLINE -- 8
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>
```

## 23. Configure CA to ignore offline CRL errors

- `certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE`

```
C:\Windows\system32>net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.

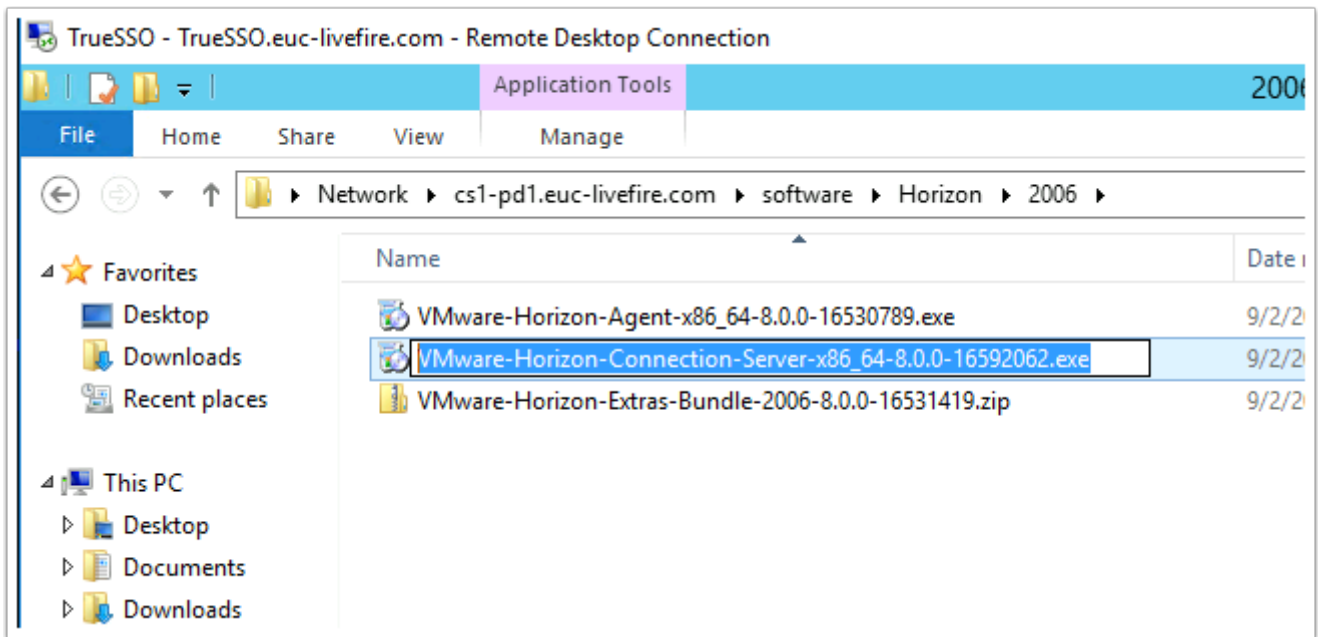
C:\Windows\system32>net start certsvc
The Active Directory Certificate Services service is starting.
The Active Directory Certificate Services service was started successfully.

C:\Windows\system32>
```

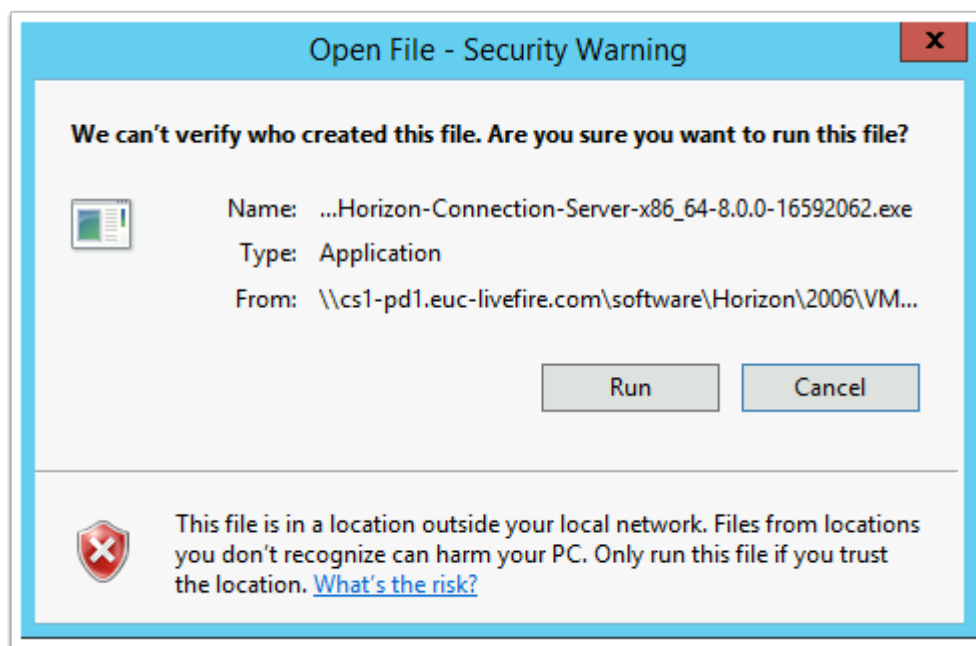
## 24. Restart the CA service. From the command prompt run:

- `net stop certsvc`
- `net start certsvc`





25. On the **TrueSSO** server desktop launch the **software** shortcut and open the **Horizon\2006\** folder.
- Select and launch the **VMware-Horizon-Connection-Server-x86\_64-8.0.0-16592062.exe**



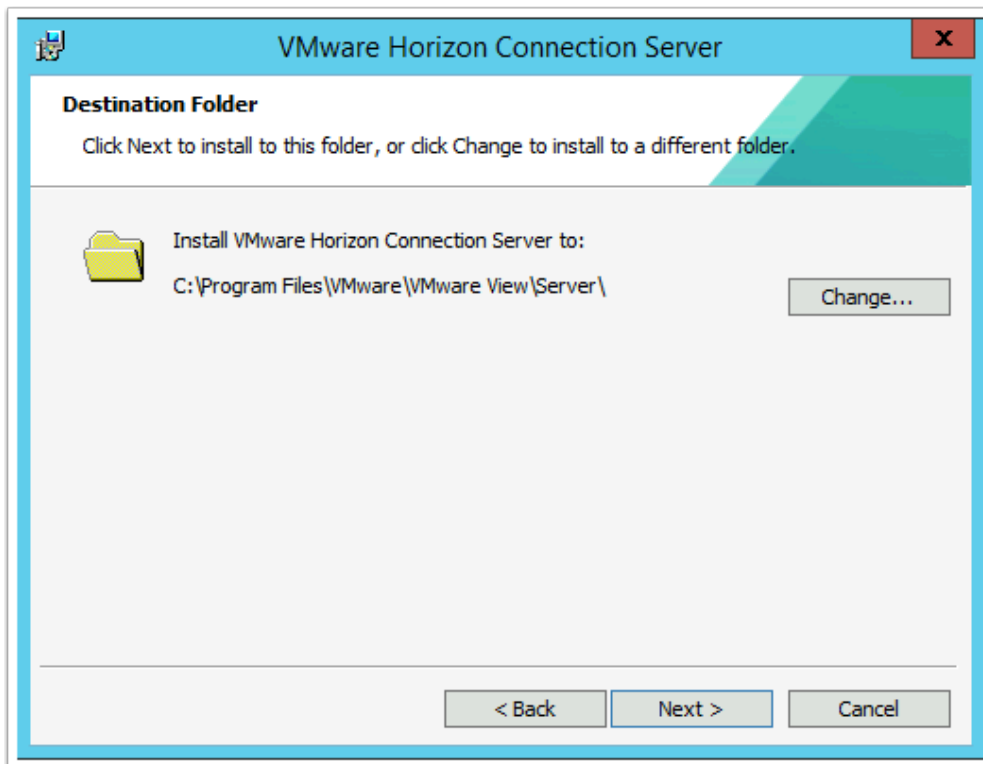
26. On the **Open File - Security Warning** window select **Run**



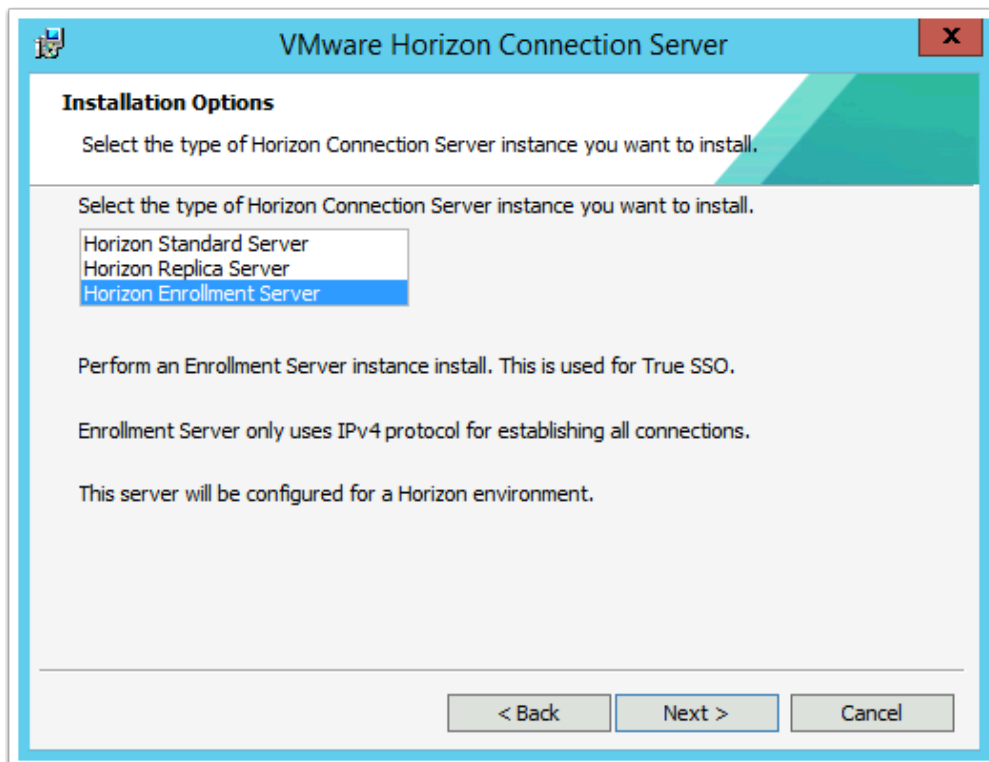
27. On the **Welcome** window select **Next**



28. On the **License agreement** window select the **radio button** next **I accept the terms in the license agreement**, select **Next**

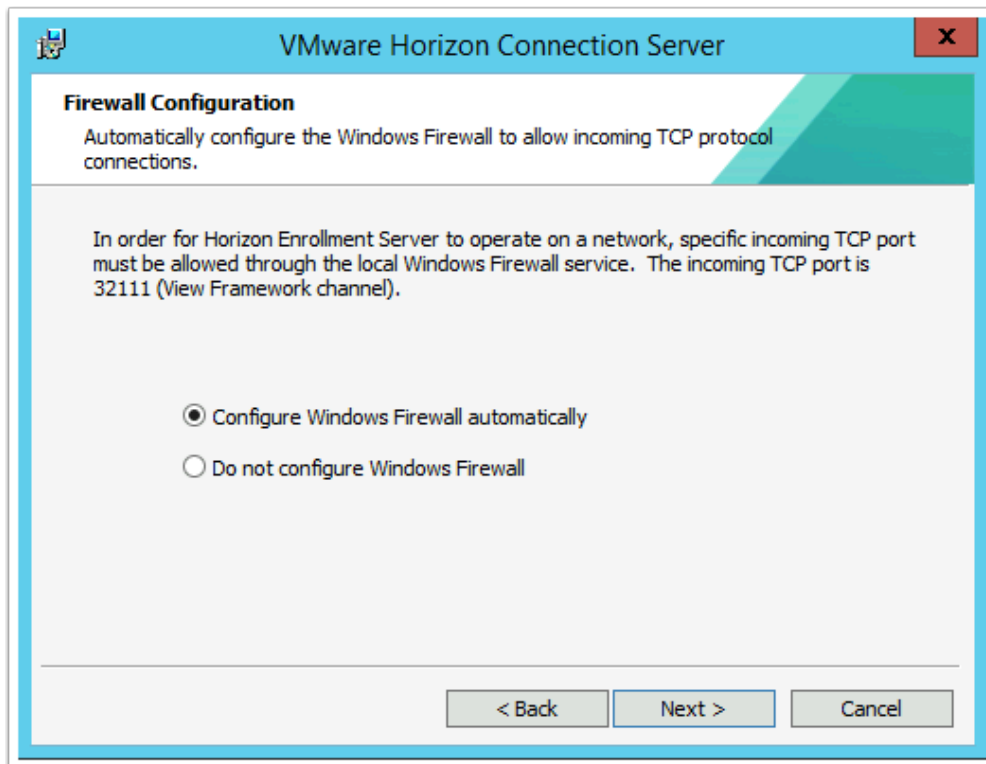


29. On **Destination Folder** window select **Next**

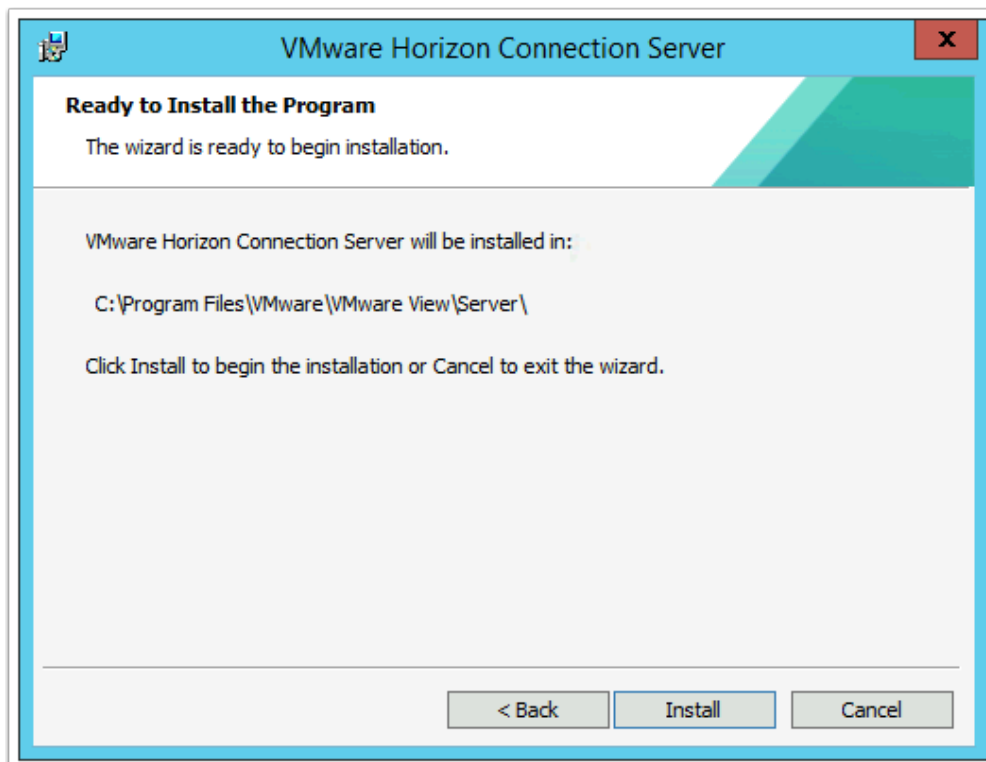


30. On the **Installation Options** window select **Horizon Enrollment Server**

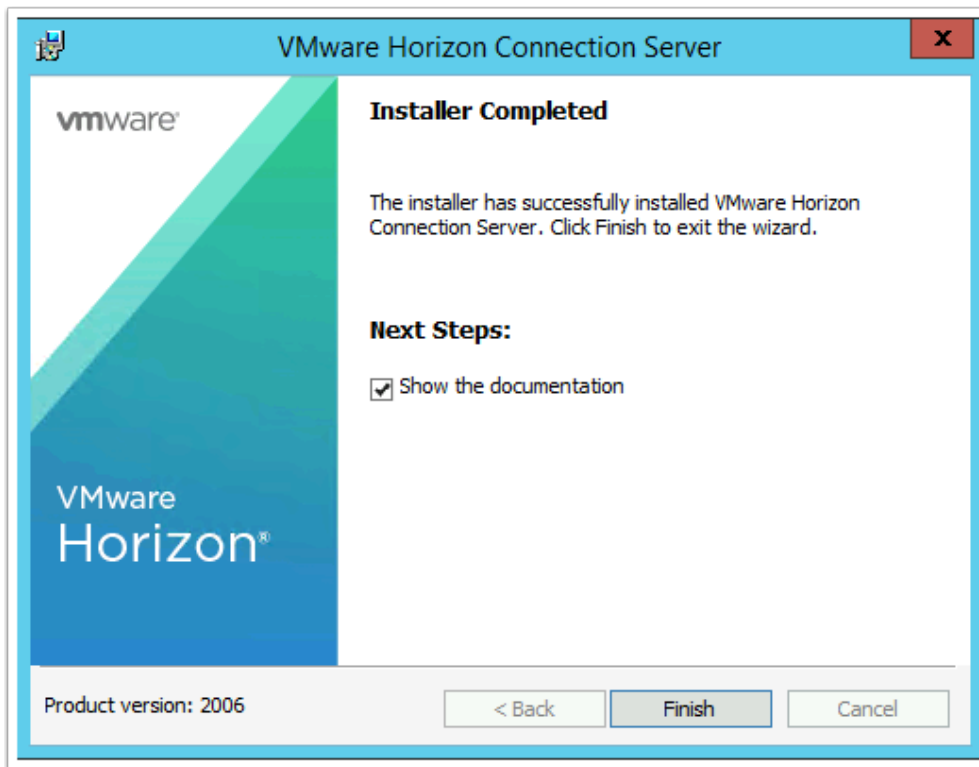
- Select **Next**



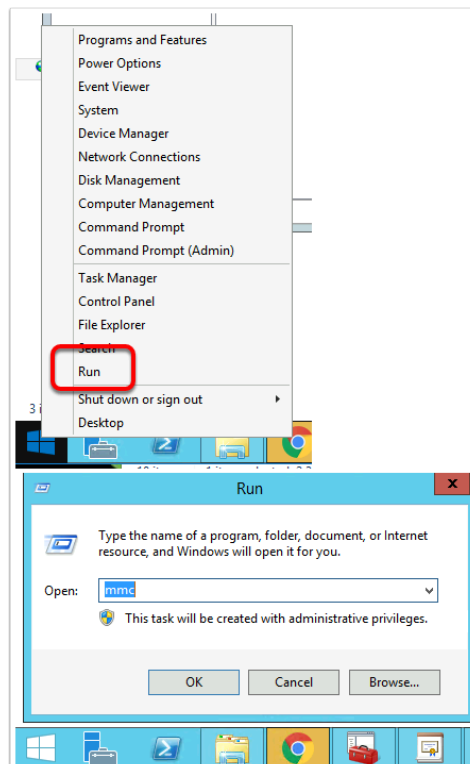
31. On **Firewall configuration** window select **Next**



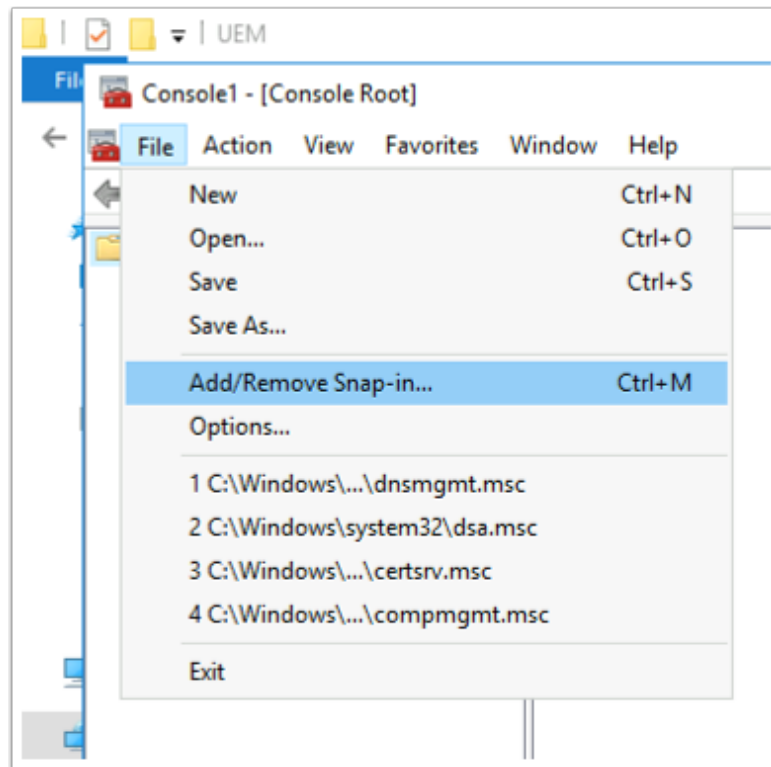
32. Select **Install**



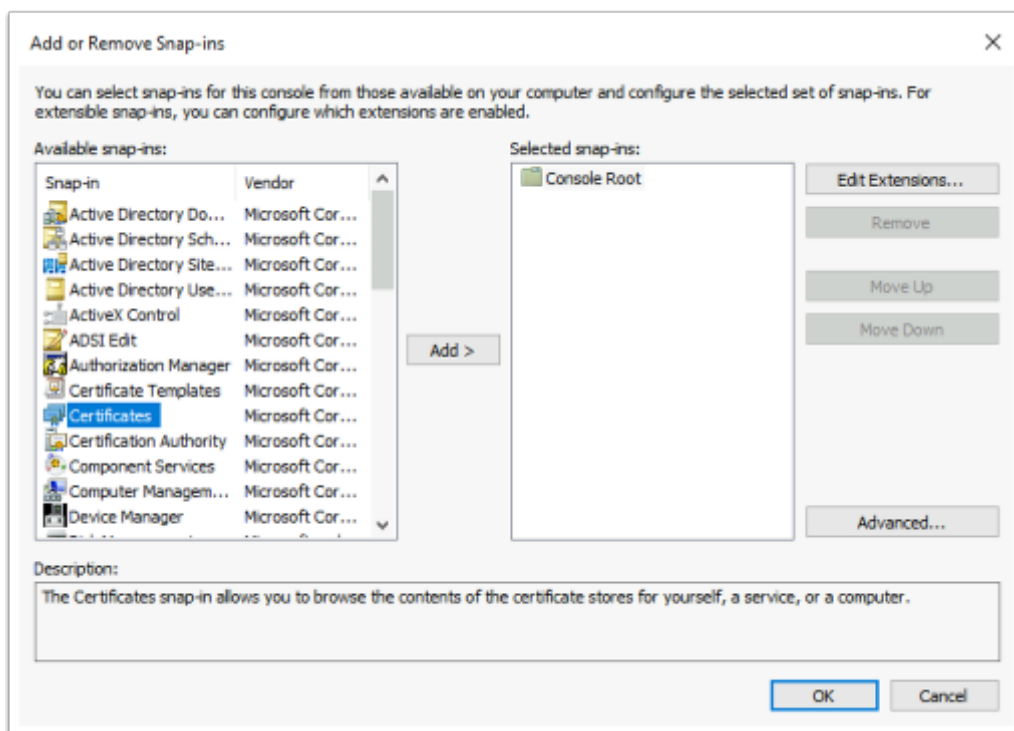
33. On the **Installer Completed** Window select **Finish**



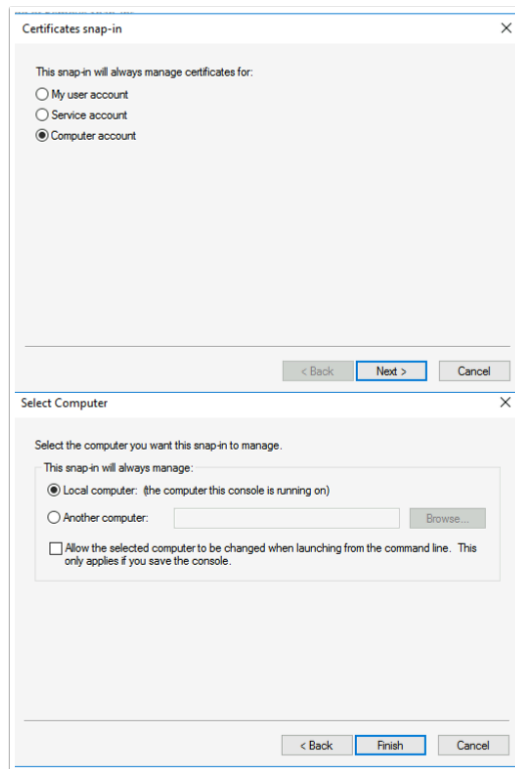
34. On the **TrueSSO** server select and right-click the **Start Button**, select **Run**, type **MMC**, select **OK**



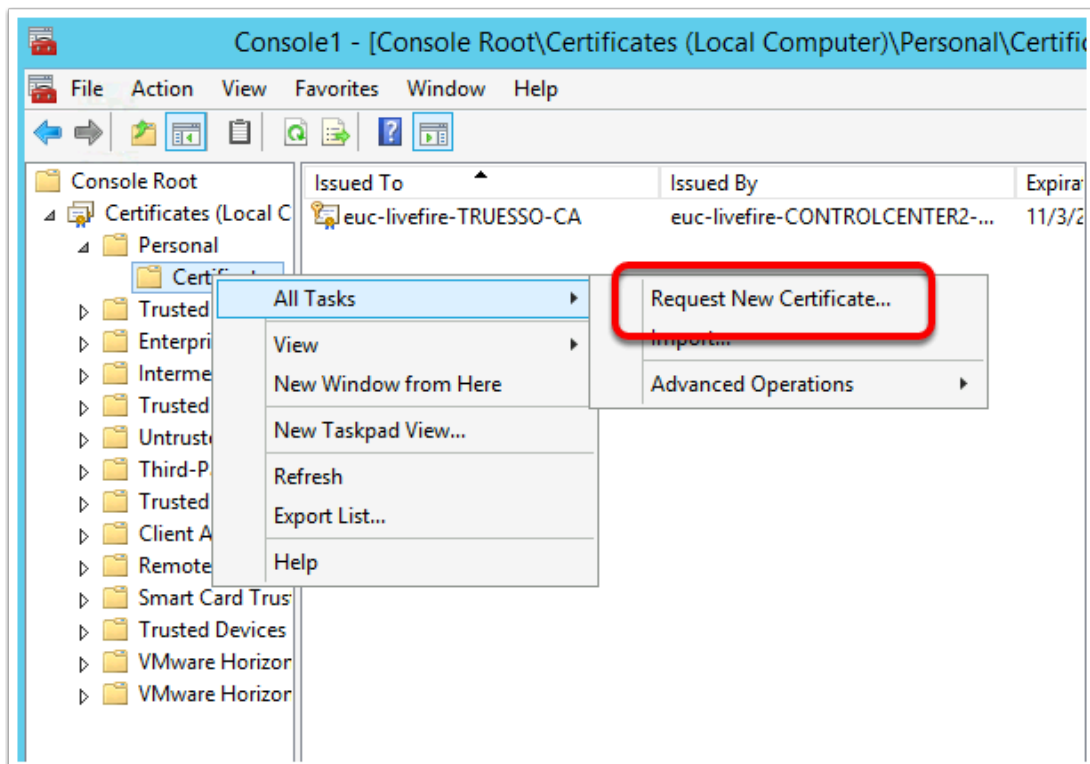
35. In the **Console** window select **File** > **Add/Remove Snap-in..**



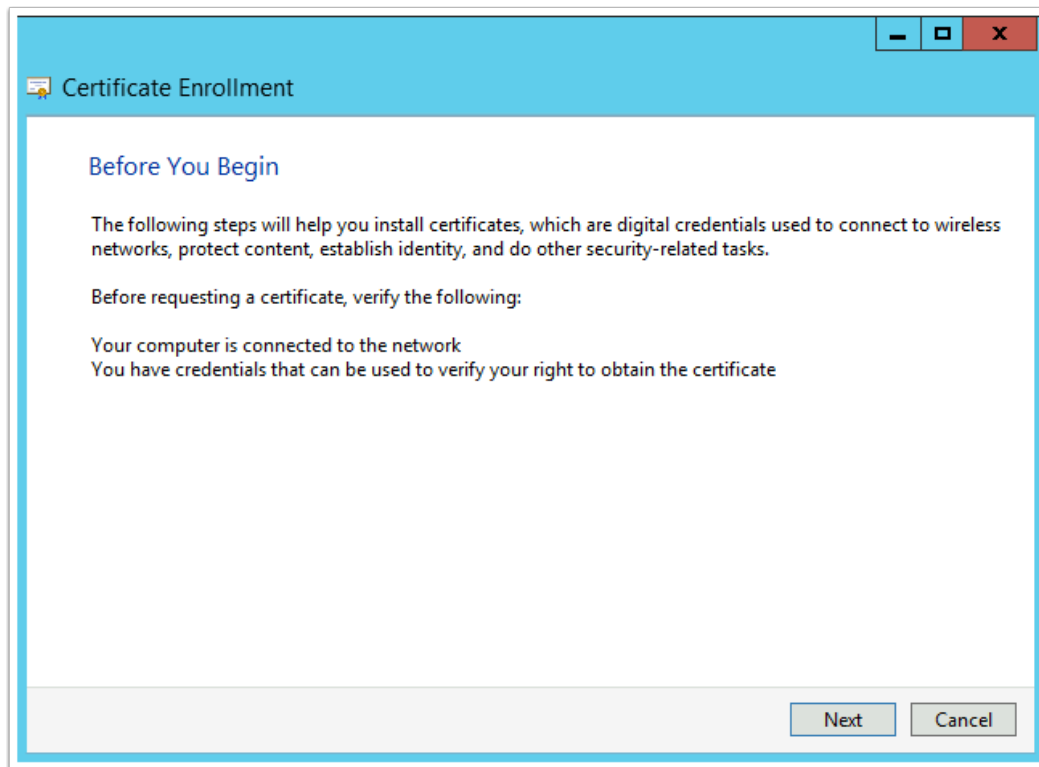
36. In the **Add or Remove Snap-ins** window, select **Certificates** and select **Add**



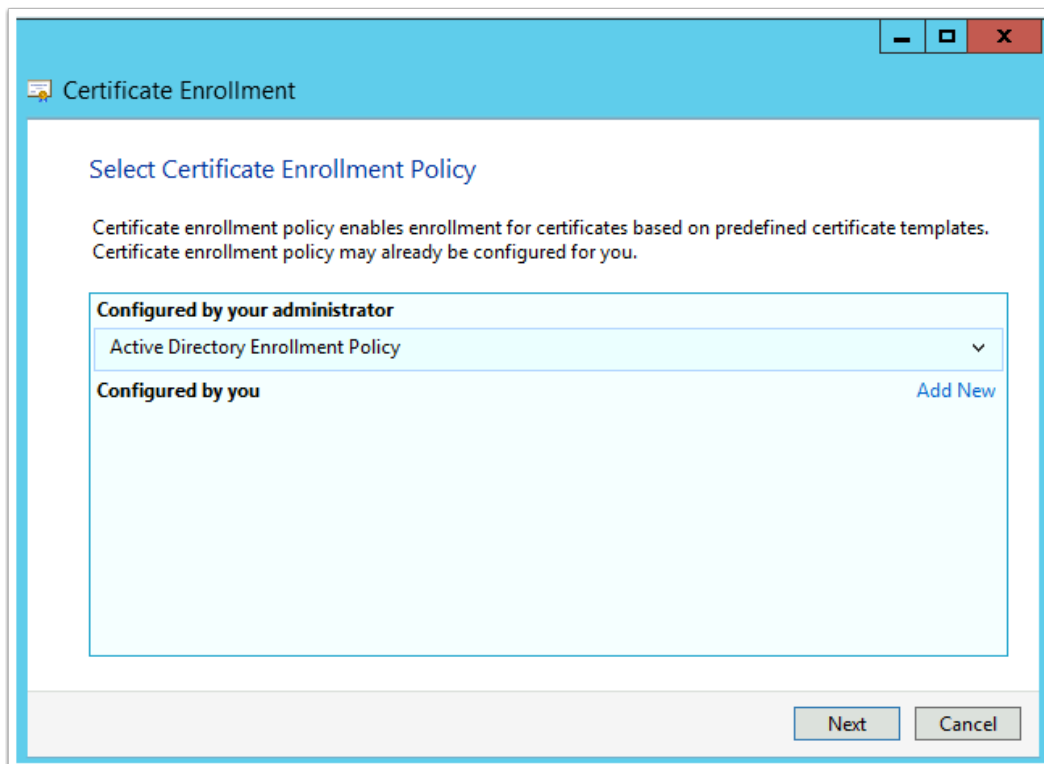
37. Select **Computer account** radio button select **Next** and select **Finish** select **OK**



38. Expand the **Certificates** console inventory and select and right-click the **Personal** container. Select **All Tasks** > **Request New Certificate**

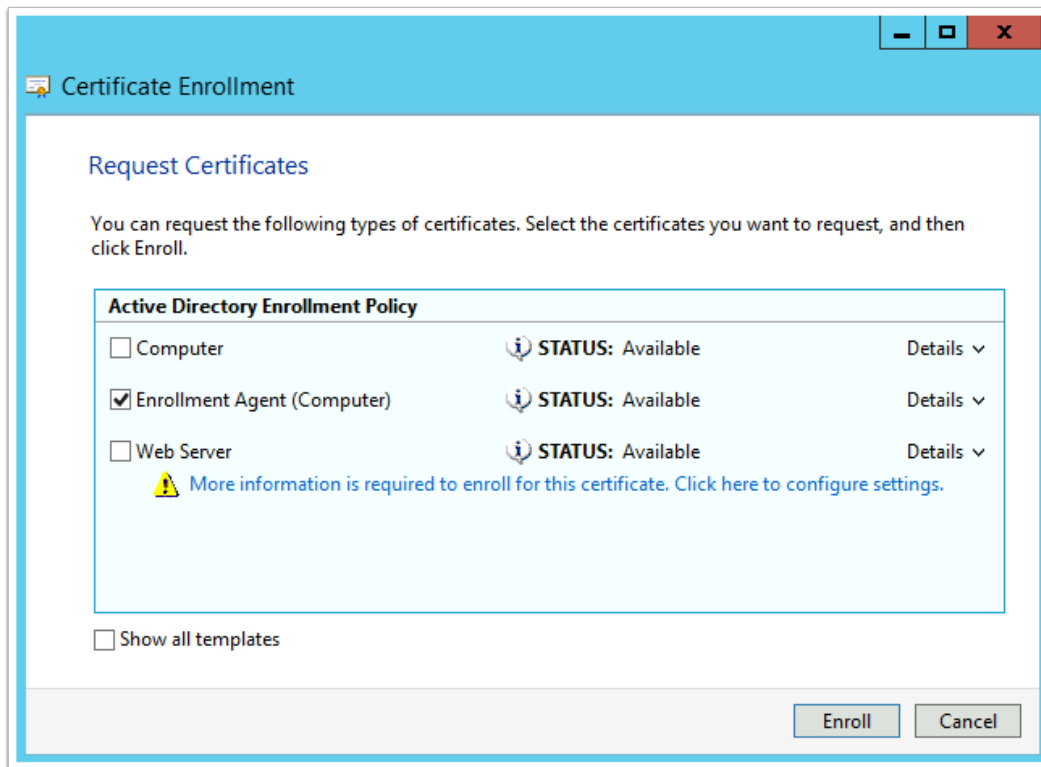


39. On the **Certificate Enrollment > Before you Begin** window select **Next**

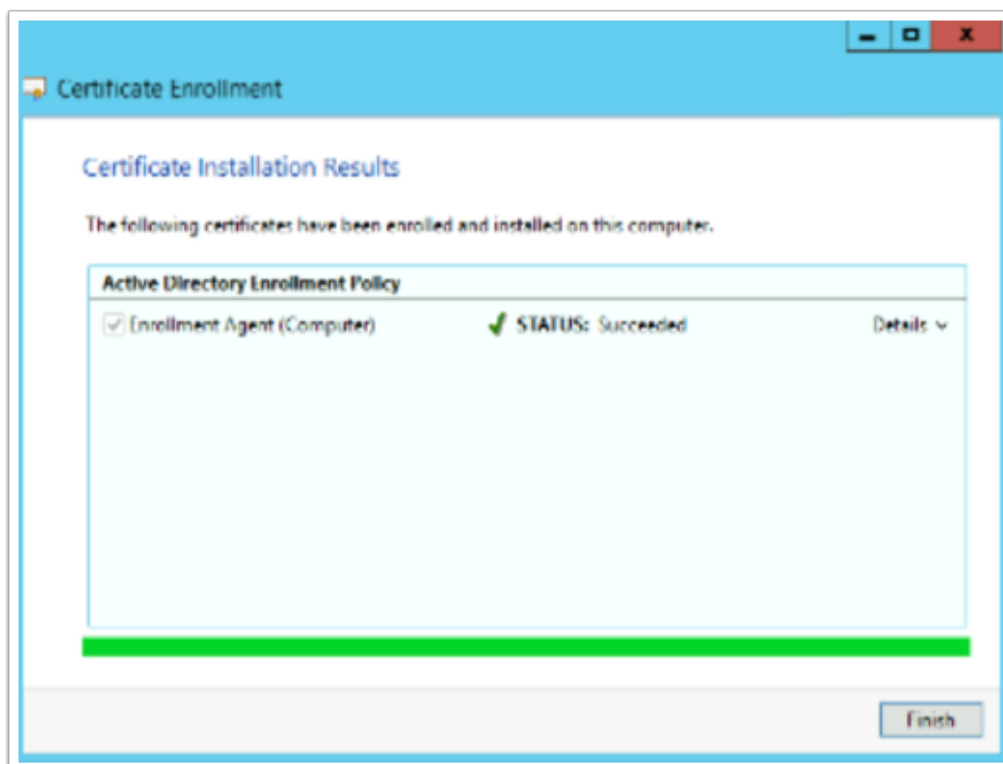


40. On the **Select Certificate Enrollment Policy** window select **Next**

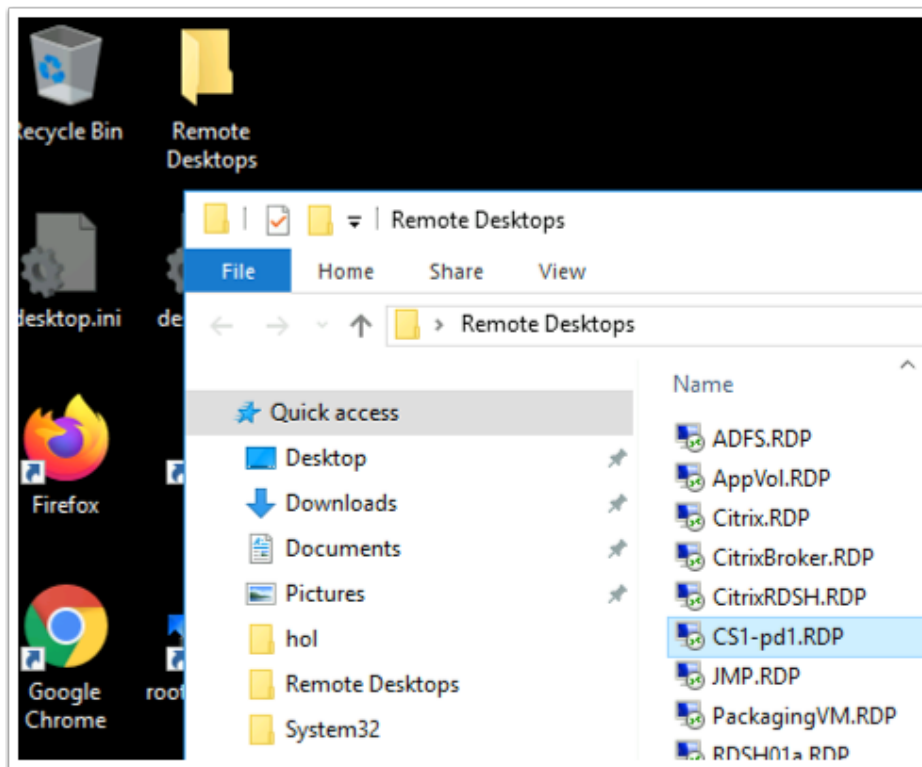




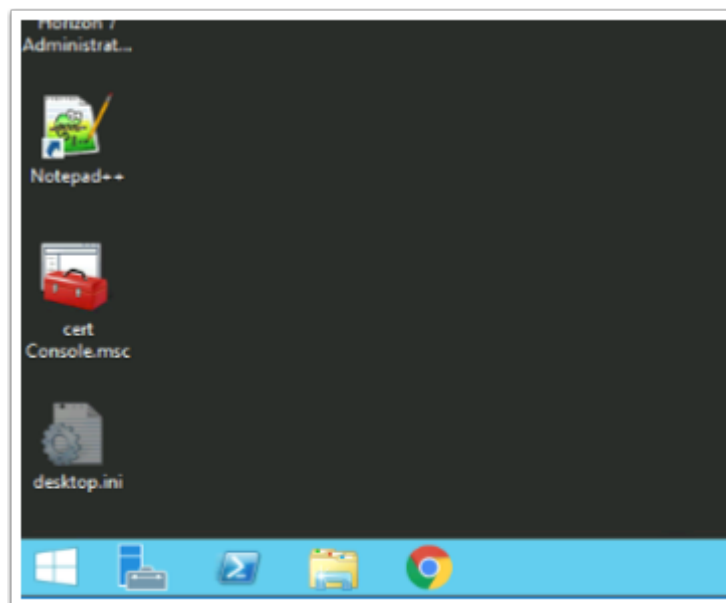
41. On the **Request Certificates** windows select the **checkbox** in front of **Enrollment Agent (Computer)** and select **Enroll**



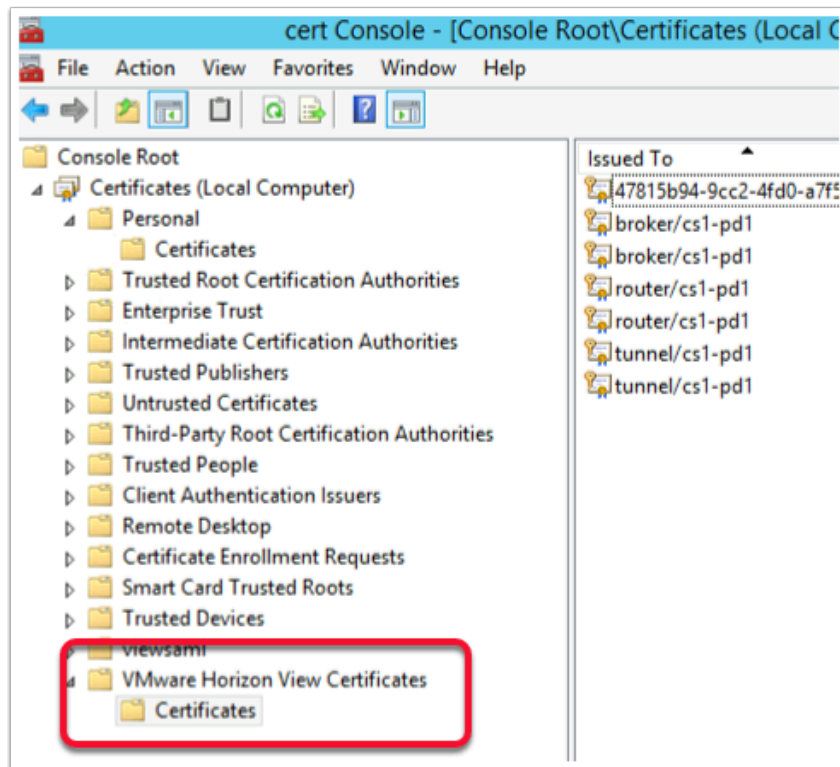
42. On the **Certificate Installation Results** window, ensure the enrollment was successful and select **Finish**.



43. On your **ControlCenter2** server,
- Open up your **Remote Desktop** folder and **RDP** to **CS1-PD1**
  - With username **euc-livefire\administrator** and password **VMware1!**



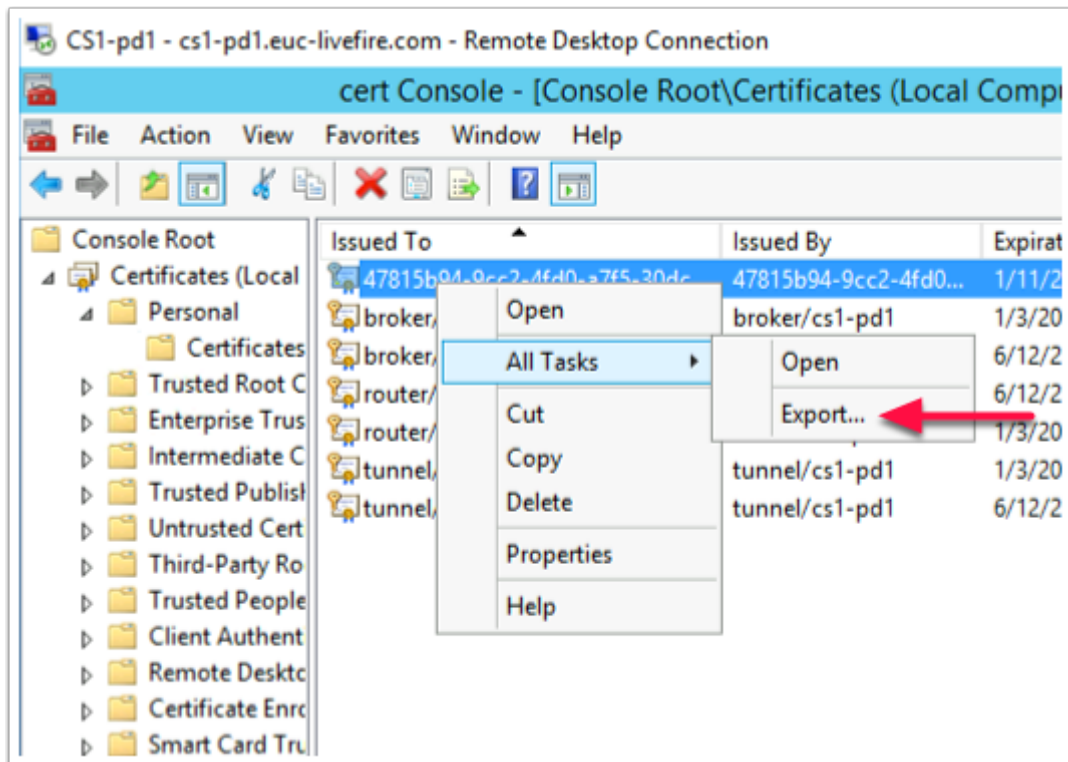
44. On the **CS1-PD1** desktop select and open your **Cert Console.mmc**



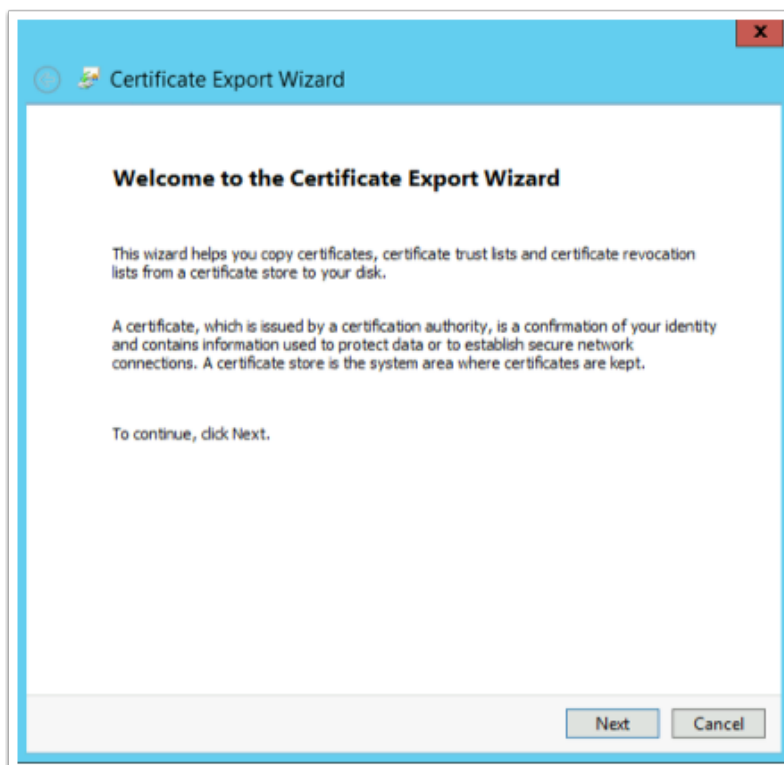
45. In the **Certificates** Console **expand** the inventory and browse down to **VMware Horizon View Certificates > Certificates**

| Issued To                       | Issued By             | Expiration Date | Intended Purpose | friendly name    |
|---------------------------------|-----------------------|-----------------|------------------|------------------|
| 47815b94-9cc2-4fd0-a7f5-30dc... | 47815b94-9cc2-4fd0... | 1/11/2030       | <All>            | vdm.ec           |
| broker/cs1-pd1                  | broker/cs1-pd1        | 1/3/2021        | <All>            | ConnectionBroker |
| broker/cs1-pd1                  | broker/cs1-pd1        | 6/12/2020       | <All>            | ConnectionBroker |
| router/cs1-pd1                  | router/cs1-pd1        | 6/12/2020       | <All>            | MQRouter         |
| router/cs1-pd1                  | router/cs1-pd1        | 1/3/2021        | <All>            | MQRouter         |
| tunnel/cs1-pd1                  | tunnel/cs1-pd1        | 1/3/2021        | <All>            | Tunnel           |
| tunnel/cs1-pd1                  | tunnel/cs1-pd1        | 6/12/2020       | <All>            | Tunnel           |

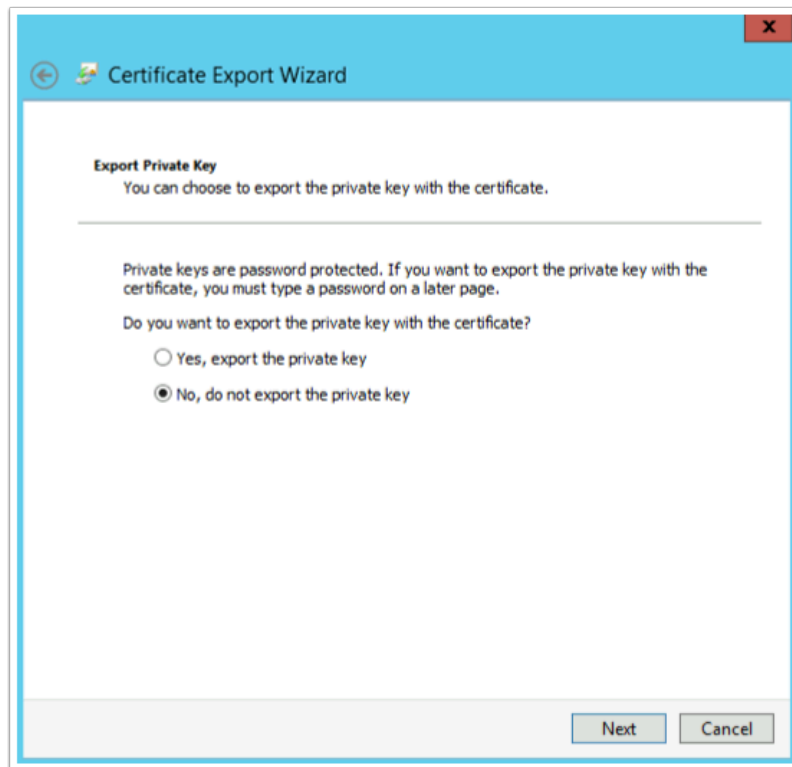
46. Expand the console or **scroll** across the console and notice the **guid** based certificate has a friendly name of **vdm.ec**



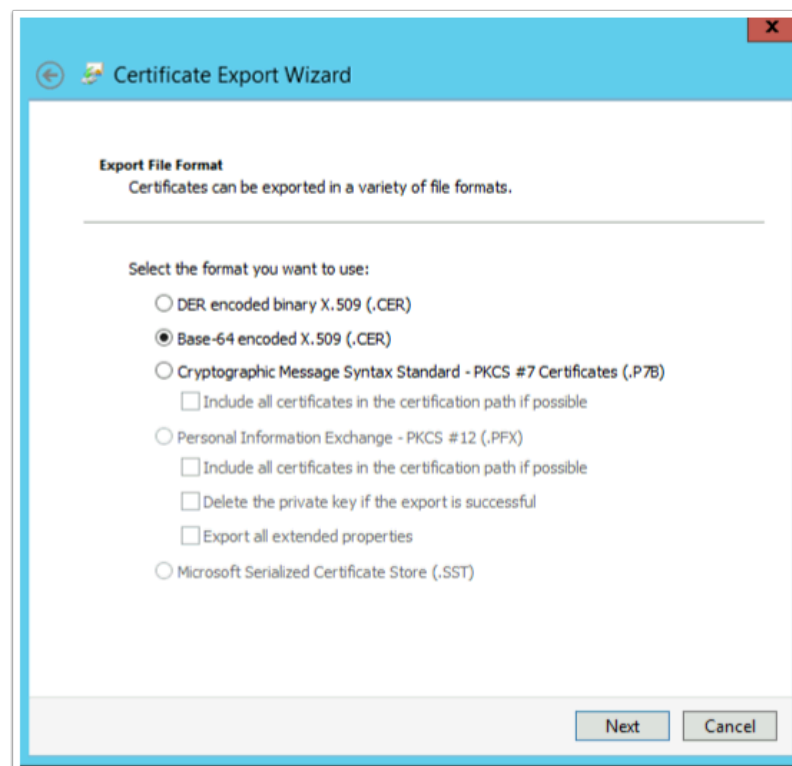
47. Select your **GUID certificate** with the friendly name of **vdm.ec**. Right-Click select **All Tasks** and select **Export**



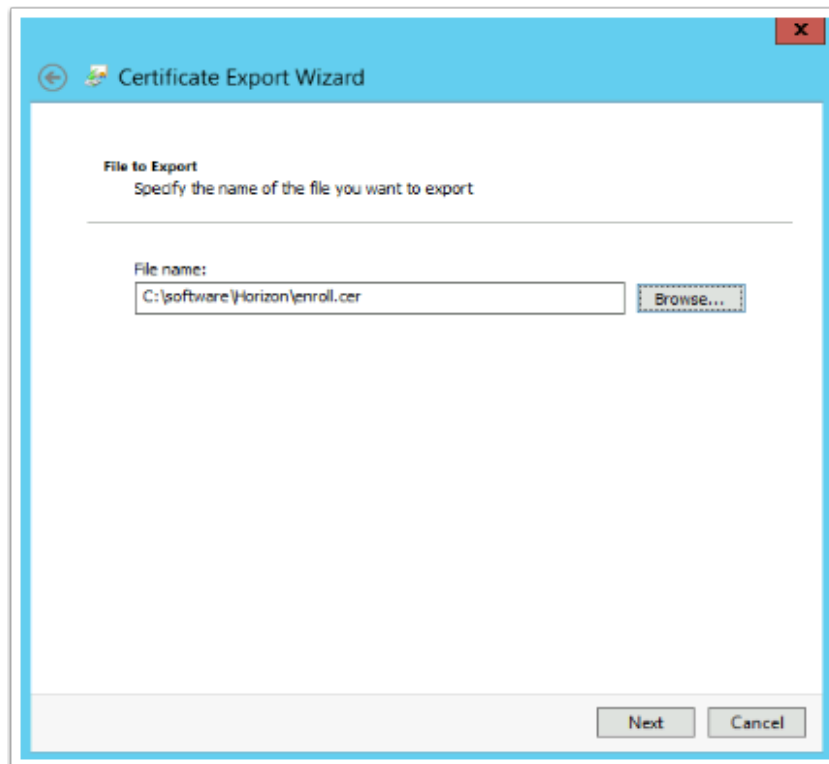
48. On the **Welcome** window select **Next**



49. On the **Export Private Key** page select the **radio button** next to **No, do not export the private key** select **Next**

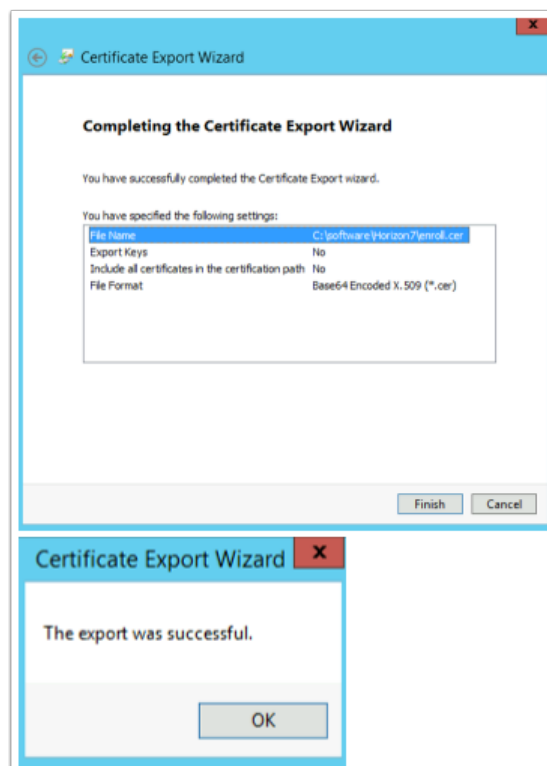


50. On the **Export File Format** window select the **radio button** next to **Base-64 encoded X.509** select **Next**

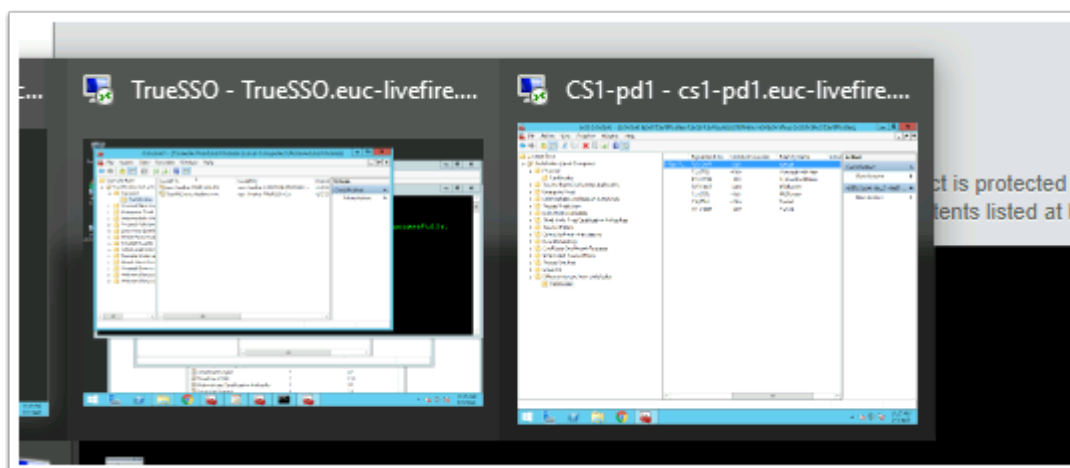


51. In the **File to Export** window in the **File name** area type the following **C:\software\Horizon\enroll.cer** and select **Next**

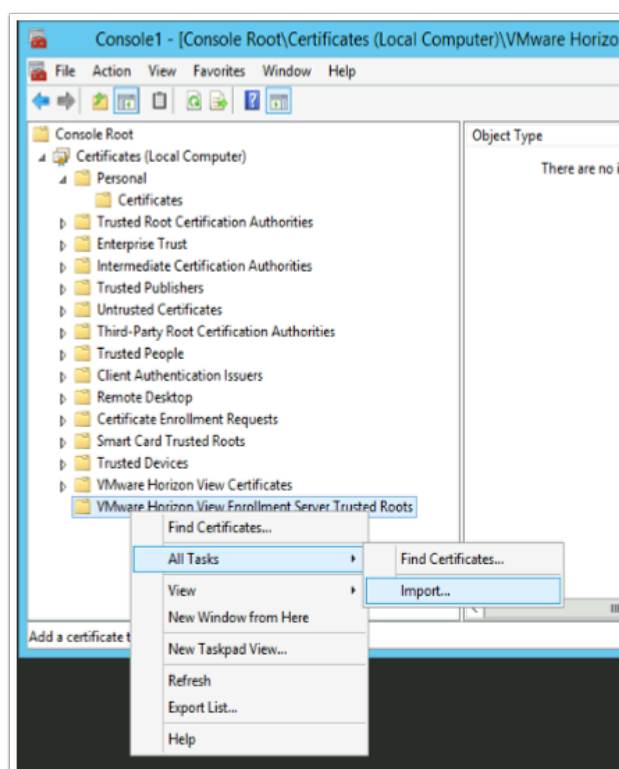
(**Software** is a shared folder which we will use to copy from on the TrueSSO server)



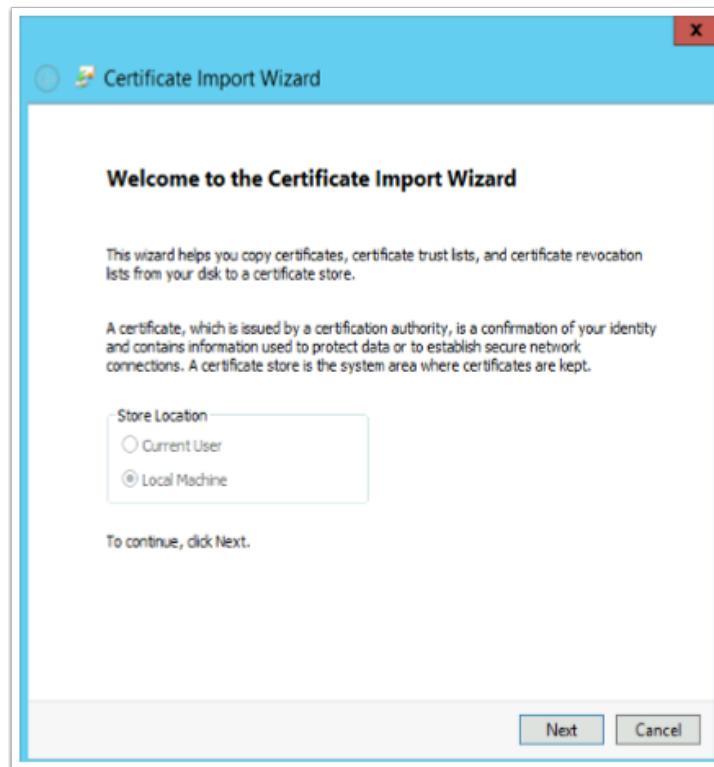
52. On the **Completing the Certificate Export Wizard** window select **Finish**. When prompted that **The export was successful**, select **OK**



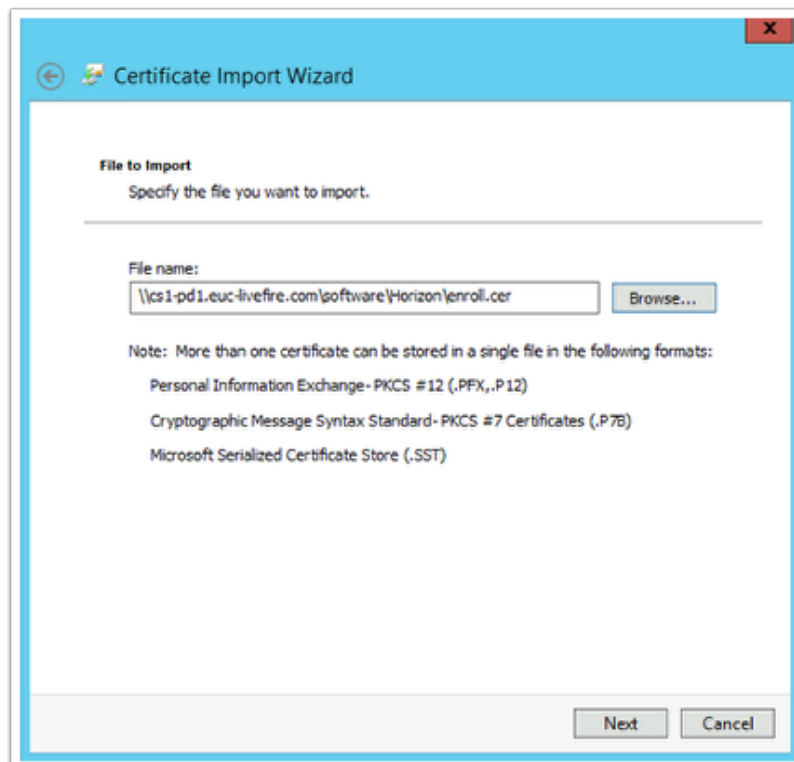
53. On your **ControlCenter2** server desktop switch from your **CS1-pd1** session to your **TrueSSO** session



54. Open your **Certificate services** Snap-in, select and right-click the last container in the inventory **VMware Horizon View Enrollment Server Trusted Roots**, select **All Tasks > Import**

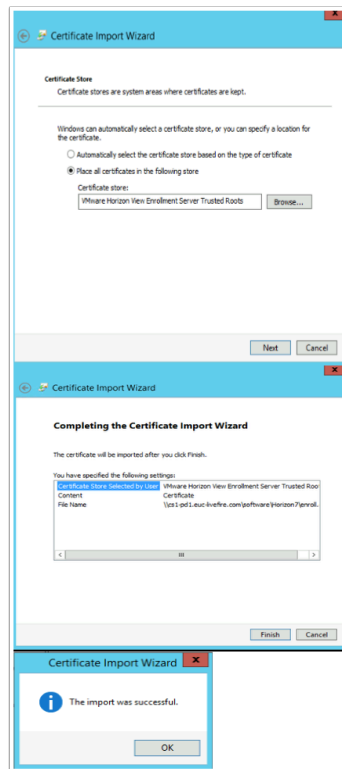


55. On the **Welcome** window select **Next**

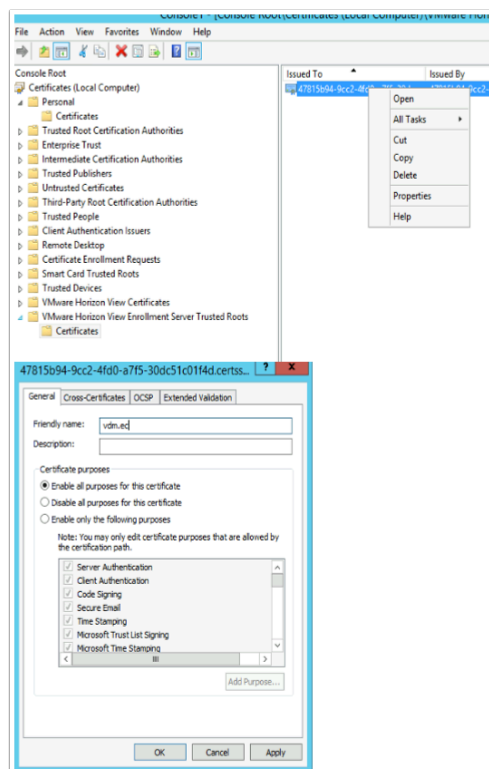


56. In the **File to import** window type the following **\\cs1-pd1.euc-livefire.com\\software\\Horizon\\enroll.cer** and select **Next**

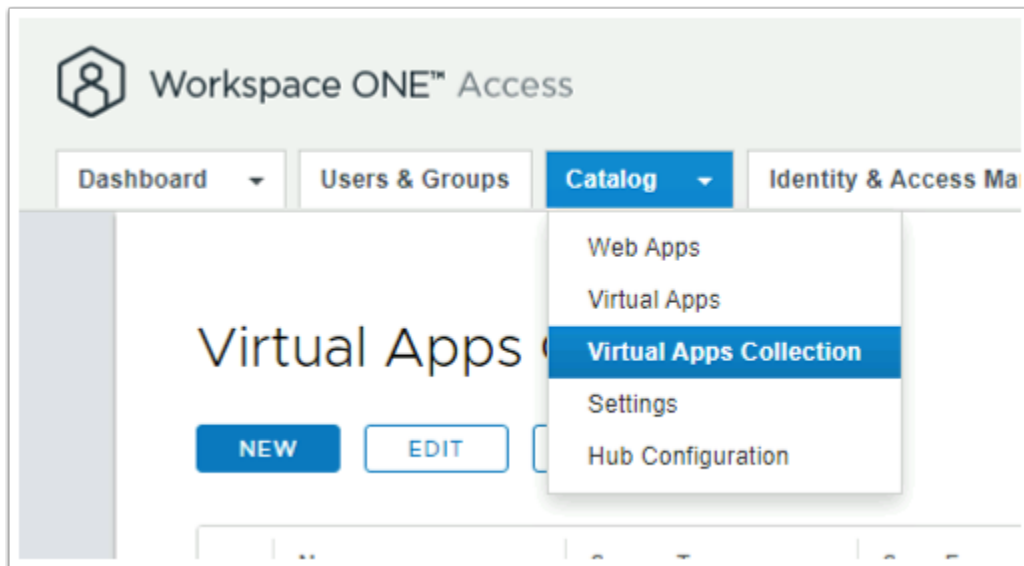




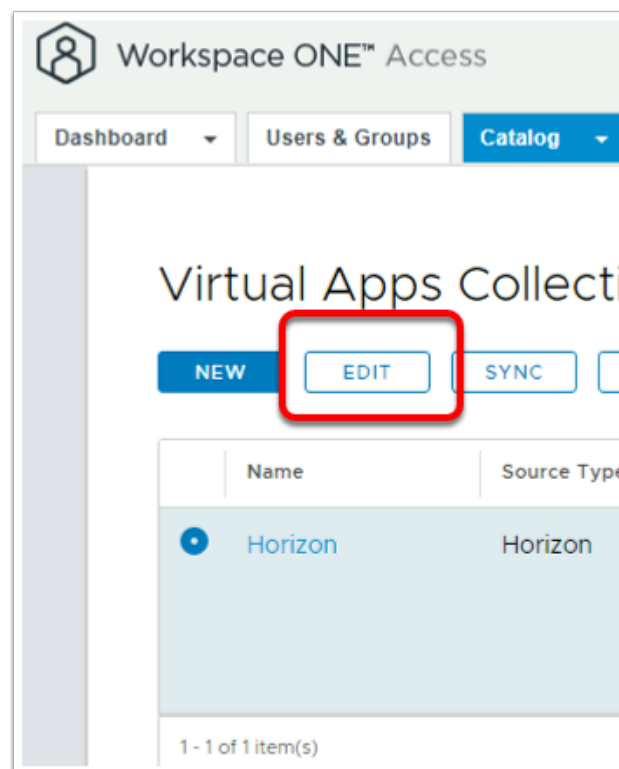
57. In the **Certificate Store** window accept the defaults and select **Next**. On the **Summary** page select **Finish**. When Prompted that **The Import was succesful** select **OK**



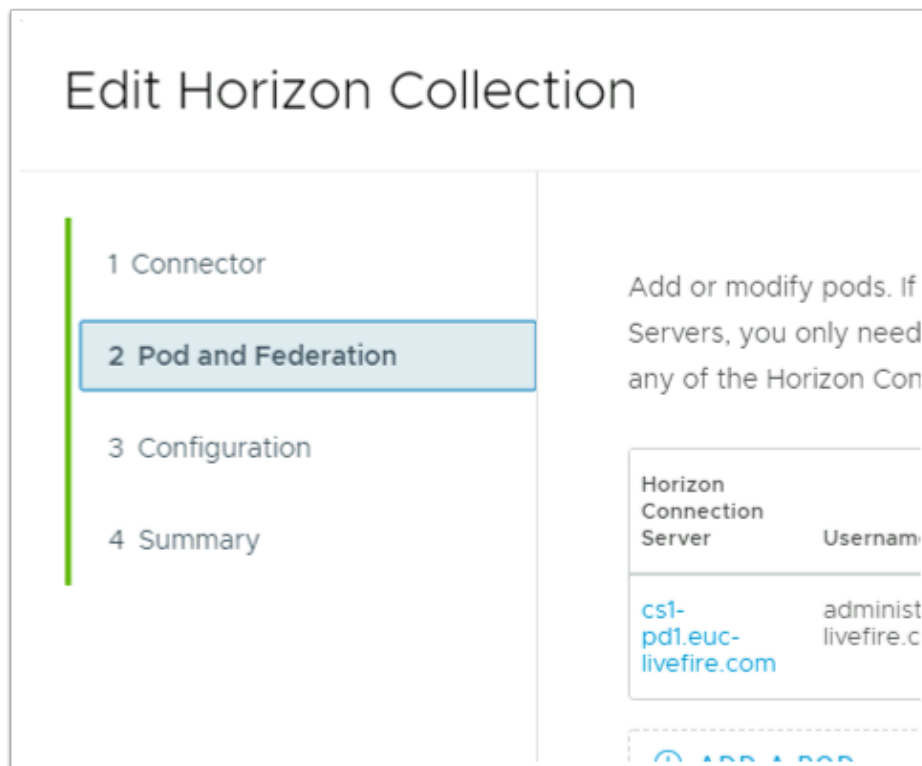
58. Right-click the **imported certificate** and select **Properties**. In the **Friendly name:** section type **vdm.ec** and select **OK**



59. Switch to your **browser, Workspace ONE Access SaaS** session,
- Select the **Catalog** tab > **Virtual Apps Collection**



60. Select the **radio button** next **Horizon** and select **EDIT** next to **NEW**



61. In the **Edit Horizon Collection** window, select **2 Pod and Federation**, under **Horizon Connection Server** select **cs1-pd1.euc-livefire.com**

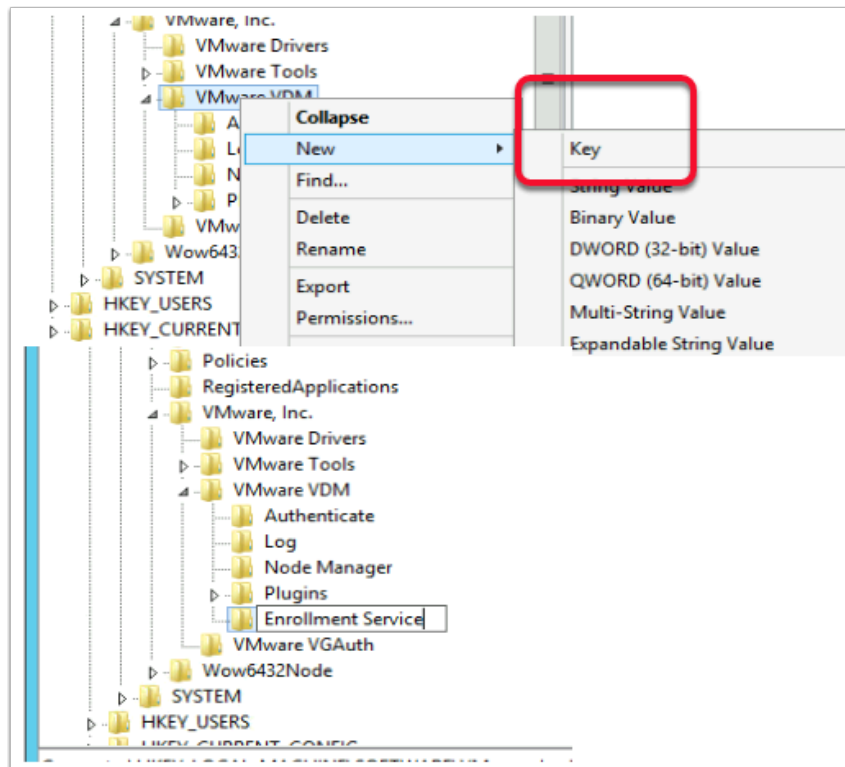
62. In the **Edit Pod** window under **True SSO**, change the **toggle** from **Disabled** to **Enabled**

- Select **SAVE** , select **NEXT**, select **NEXT**, select **SAVE**

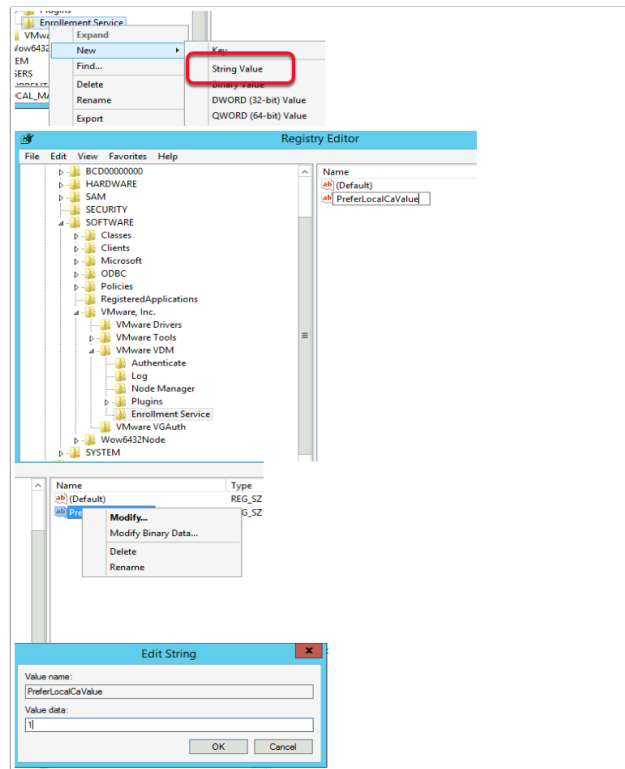
EUC: Horizon Integrations 2020

Manual Export Date: 2020-12-03 07:22:31 +0000

Page 245

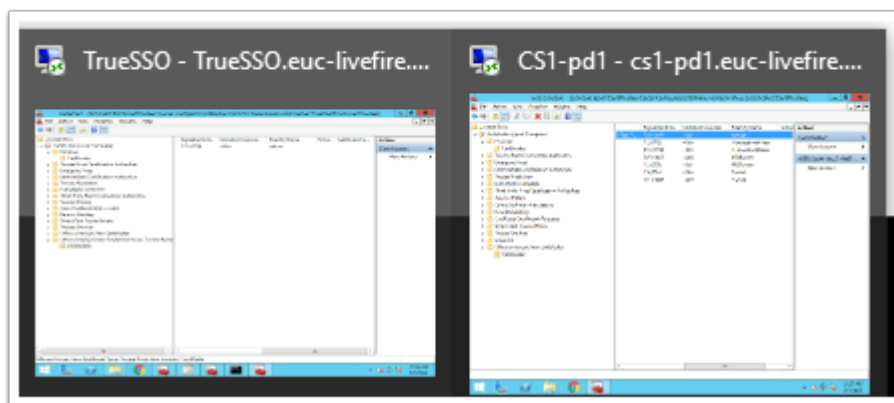


63. On the **ControlCenter2** server, switch back to your **TrueSSO.RDP** session
  1. Select the **Start button** > **RUN** and type **regedit.exe**
  2. In the regedit inventory, browse to the following location, browse to
    - **HKLM\SOFTWARE\VMware, Inc.\VMware VDM\**
    - What we should see is an **Enrollment Service** Key
      - **HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service.**
      - You will notice there is no **Enrollment Service** key, we need to create one. In our case we have to
  3. Create the **Enrollment Service** key
    - Right-click **VMware VDM** > **New** > **Key** and type **Enrollment Service** as a name

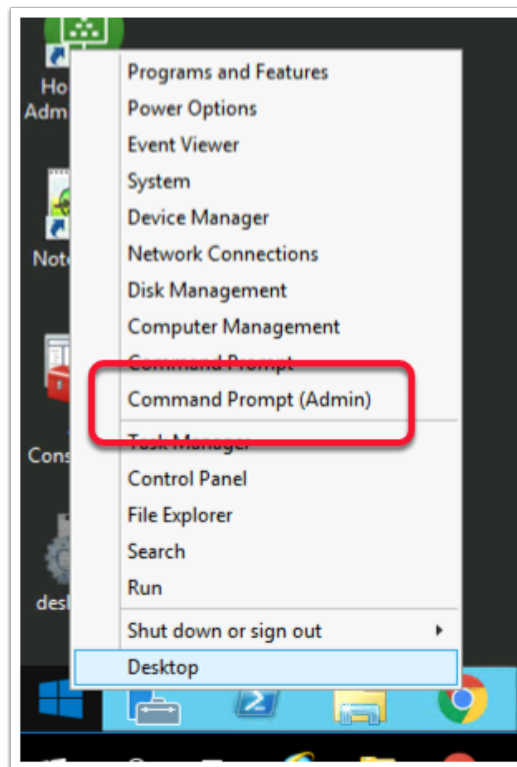


64. Configure the enrollment service to give preference to the local certificate authority when they are co-located:

- Add a new **String Value**
  - Right-click the **Enrollment Service** key > **New** > **String Value** and type the name **PreferLocalCaValue**
  - Right-click the **PreferLocalCaValue** String value and select **Modify** and in the **Value data:** field enter **1**
  - Select **OK** to close the window.
  - Click to **close RegEdit**



65. On your **ControlCenter2** server switch to your **CS1-PD1.RDP** session



66. Select and right-click the **Start** button and select **Command Prompt (Admin)**

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd \
C:\>cd Program Files\VMware\VMware View\Server\tools\bin_
```

67. In the **Administrator: Command Prompt** type the following:-

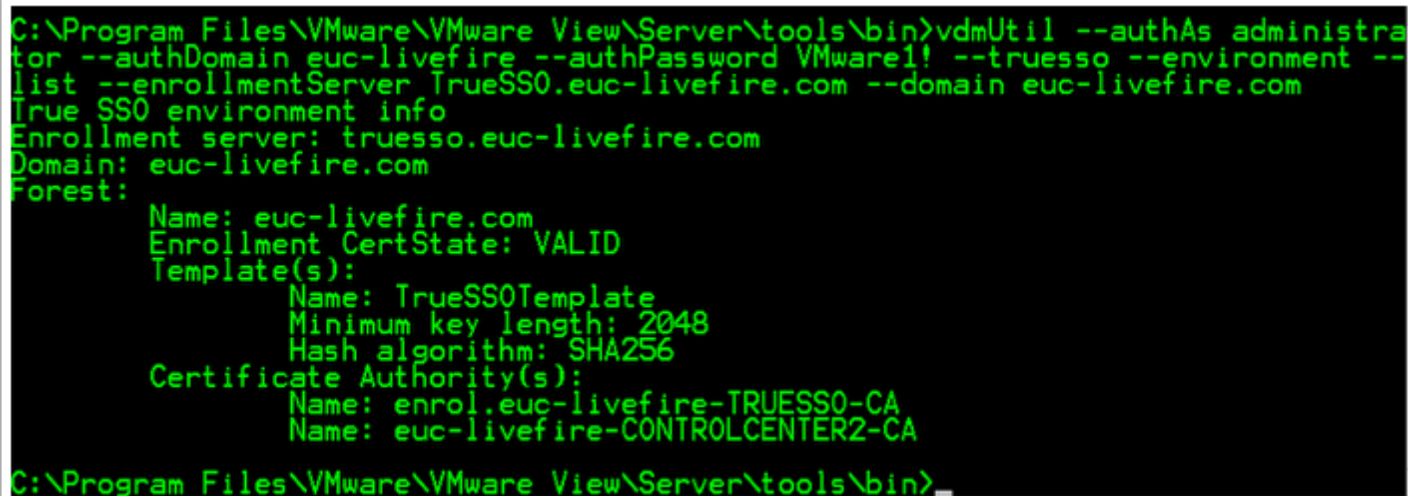
- `cd \`
- `cd Program Files\VMware\VMware View\Server\tools\bin`

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware! --truesso --environment --add --enrollmentServer TrueSSO.euc-livefire.com
Enrollment server(s) added to the environment
C:\Program Files\VMware\VMware View\Server\tools\bin>_
```

68. In the **Administrator: Command Prompt** type the following:-

The enrollment server is added to the global list.

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truessso --environment --add --enrollmentServer TrueSSO.euc-livefire.com
```



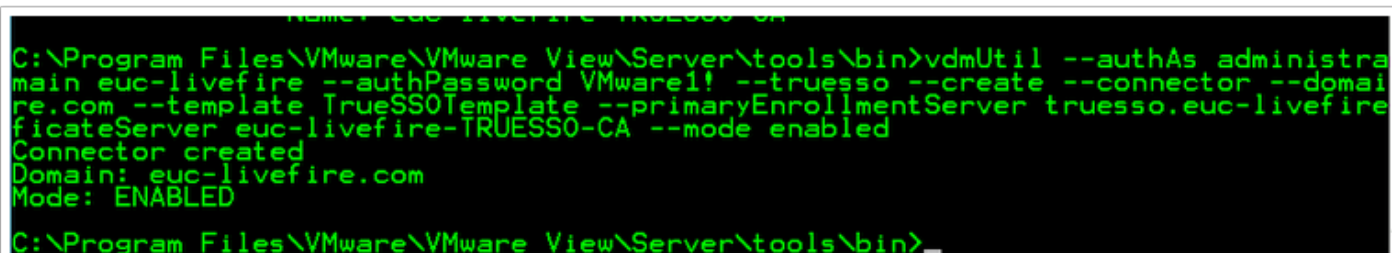
```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truessso --environment --list --enrollmentServer TrueSSO.euc-livefire.com --domain euc-livefire.com
True SSO environment info
Enrollment server: truessso.euc-livefire.com
Domain: euc-livefire.com
Forest:
  Name: euc-livefire.com
  Enrollment CertState: VALID
  Template(s):
    Name: TrueSSOTemplate
    Minimum key length: 2048
    Hash algorithm: SHA256
  Certificate Authority(s):
    Name: enrol.euc-livefire-TRUESSO-CA
    Name: euc-livefire-CONTROLCENTER2-CA
C:\Program Files\VMware\VMware View\Server\tools\bin>
```

69. **Wait 1 min** before doing the next command

In the **Administrator: Command Prompt** type the following:-

The output shows the **forest name**, whether the **certificate for the enrollment server is valid**, the name and **details of the certificate template** you can use, and the **common name** of the certificate authority.

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truessso --environment --list --enrollmentServer TrueSSO.euc-livefire.com --domain euc-livefire.com
```



```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truessso --create --connector --domain euc-livefire.com --template TrueSSOTemplate --primaryEnrollmentServer truessso.euc-livefire.com --certificateServer euc-livefire-TRUESSO-CA --mode enabled
Connector created
Domain: euc-livefire.com
Mode: ENABLED
C:\Program Files\VMware\VMware View\Server\tools\bin>
```

70. Enter the command to create a True SSO connector, which will hold the configuration information, and enable the connector.

```
vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truessso --create --connector --domain euc-livefire.com --template TrueSSOTemplate --primaryEnrollmentServer truessso.euc-livefire.com --certificateServer euc-livefire-TRUESSO-CA --mode enabled
```

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livewire --authPassword VMware1! --truesso --list --authenticator
Authenticator(s) found: 1
Name: Workspace ONE Access
True SSO mode: DISABLED
C:\Program Files\VMware\VMware View\Server\tools\bin>_
```

## 71. Enter the command to discover which SAML authenticators are available

Authenticators are created when you configure SAML authentication between Workspace ONE Access and a connection server, using Horizon Administrator.

The output shows the name of the authenticator and shows whether True SSO is enabled

```
vdmUtil --authAs administrator --authDomain euc-livewire --authPassword VMware1! --truesso --list --authenticator
```

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livewire --authPassword VMware1! --truesso --authenticator --edit --name "Workspace ONE Access" --truessoMode ENABLED
Authenticator updated
Name: Workspace ONE Access
True SSO mode: ENABLE_IF_NO_PASSWORD
C:\Program Files\VMware\VMware View\Server\tools\bin>_
```

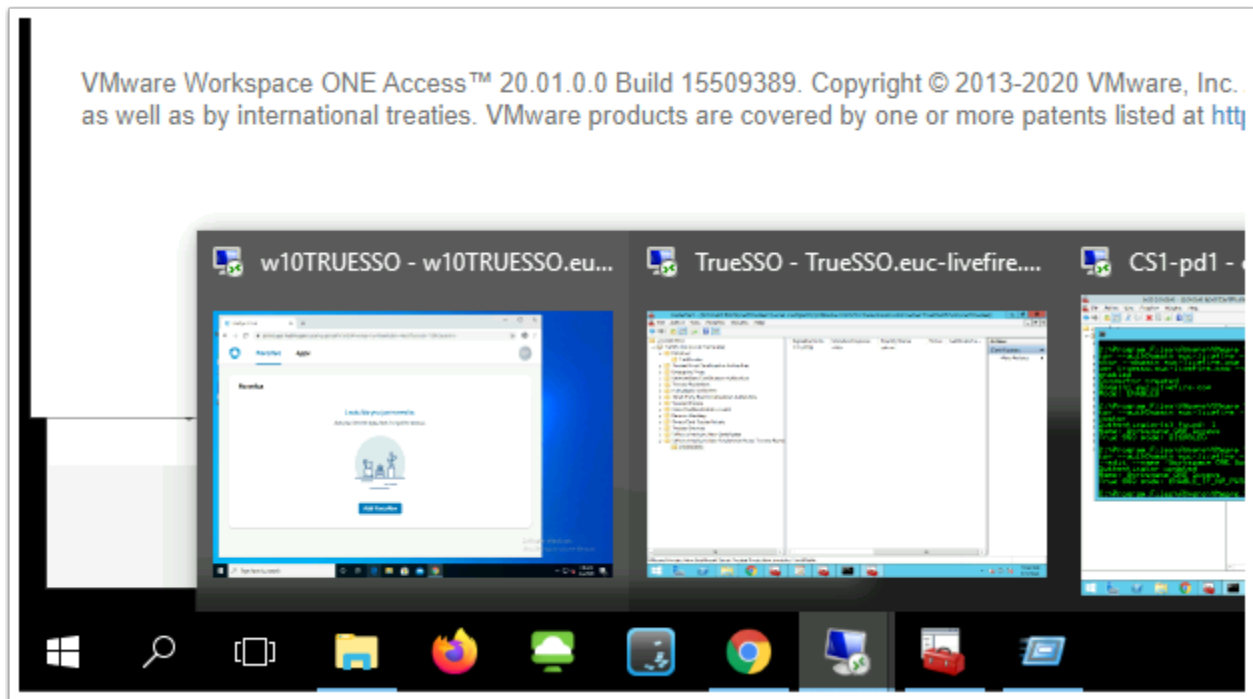
## 72. You will notice True SSO mode is Disabled. Enter the command to enable the authenticator to use True SSO mode

```
vdmUtil --authAs administrator --authDomain euc-livewire --authPassword VMware1! --truesso --authenticator --edit --name "Workspace ONE Access" --truessoMode ENABLED
```

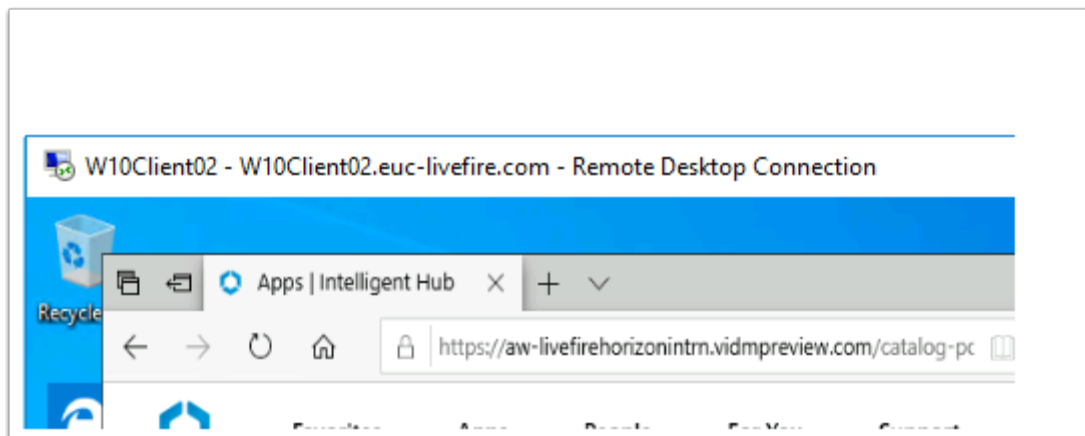
For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to VMware Identity Manager. In this case if a password was used and cached, the system will use the password. Set --truessoMode to ALWAYS if you want True SSO to be used even if a password was supplied when the user logged in to VMware Identity Manager



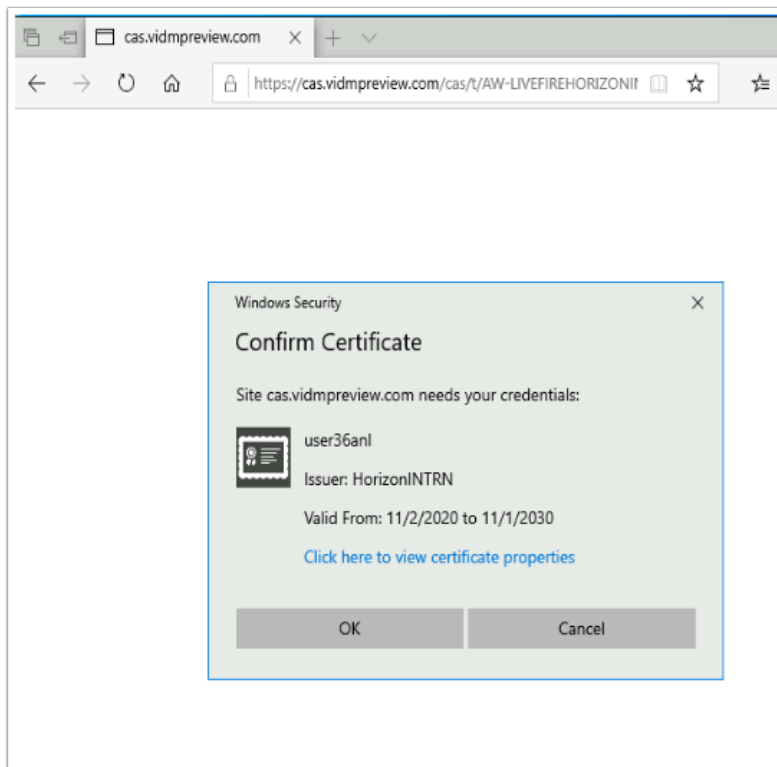
## Part 5: Testing to see if TrueSSO works



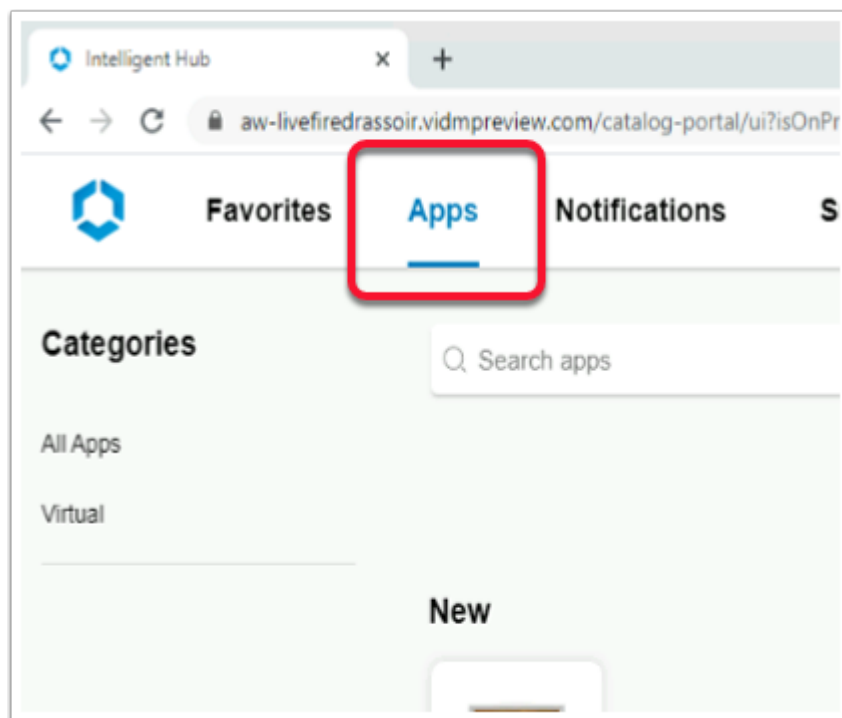
1. On your **ControlCenter2** server, switch your **Remote Desktops** session for **W10Client02.RDP**.



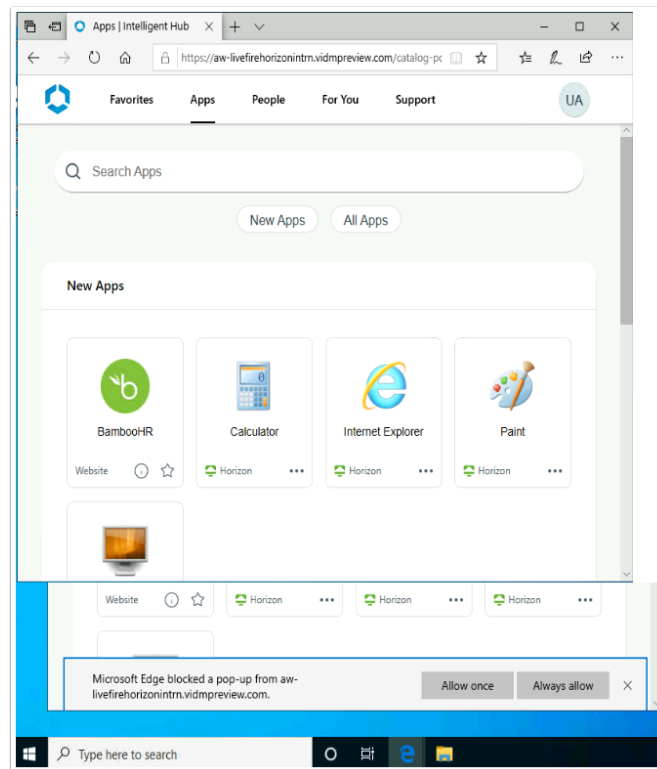
2. On your **W10Client02** desktop, ensure that any existing browser session is **CLOSED**
  - **Open** your browser and type enter your custom **Access Tenant URL**



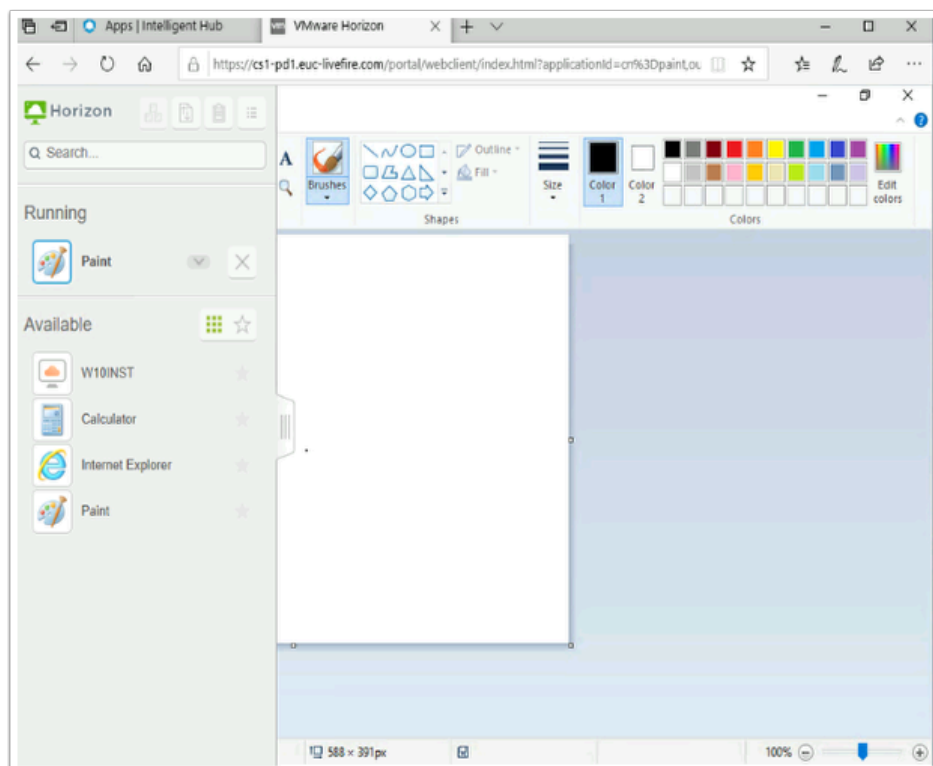
3. On the **Confirm Certificate** window, select **OK**



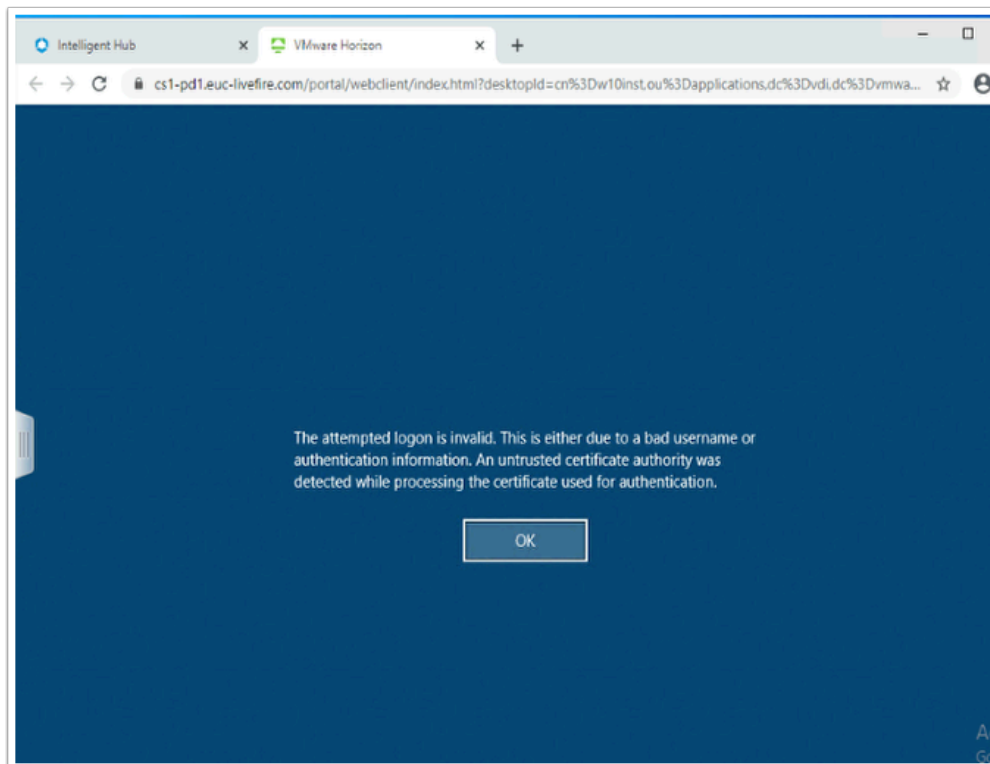
4. Select **Apps** tab in the Console



5. In the **Apps** area, under **New Apps** select **Paint**
  - Select **Always allow**

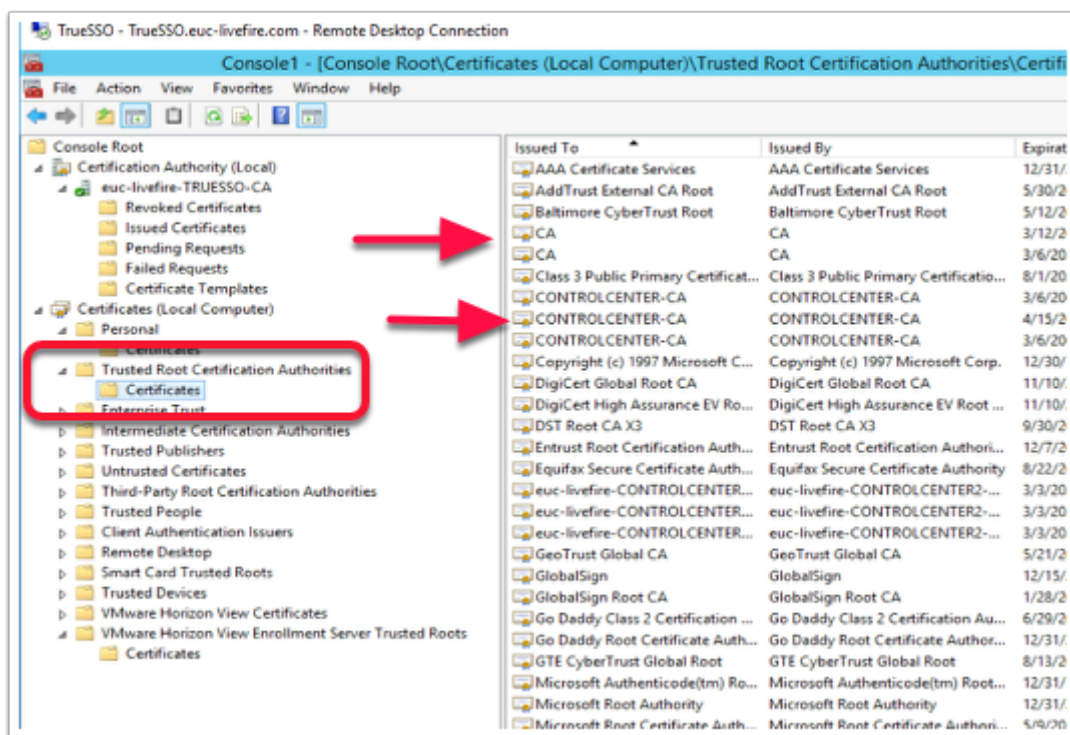


6. On the W10Client02
  - Note your Paint session launch
  - Launch the **W10INST** desktop pool



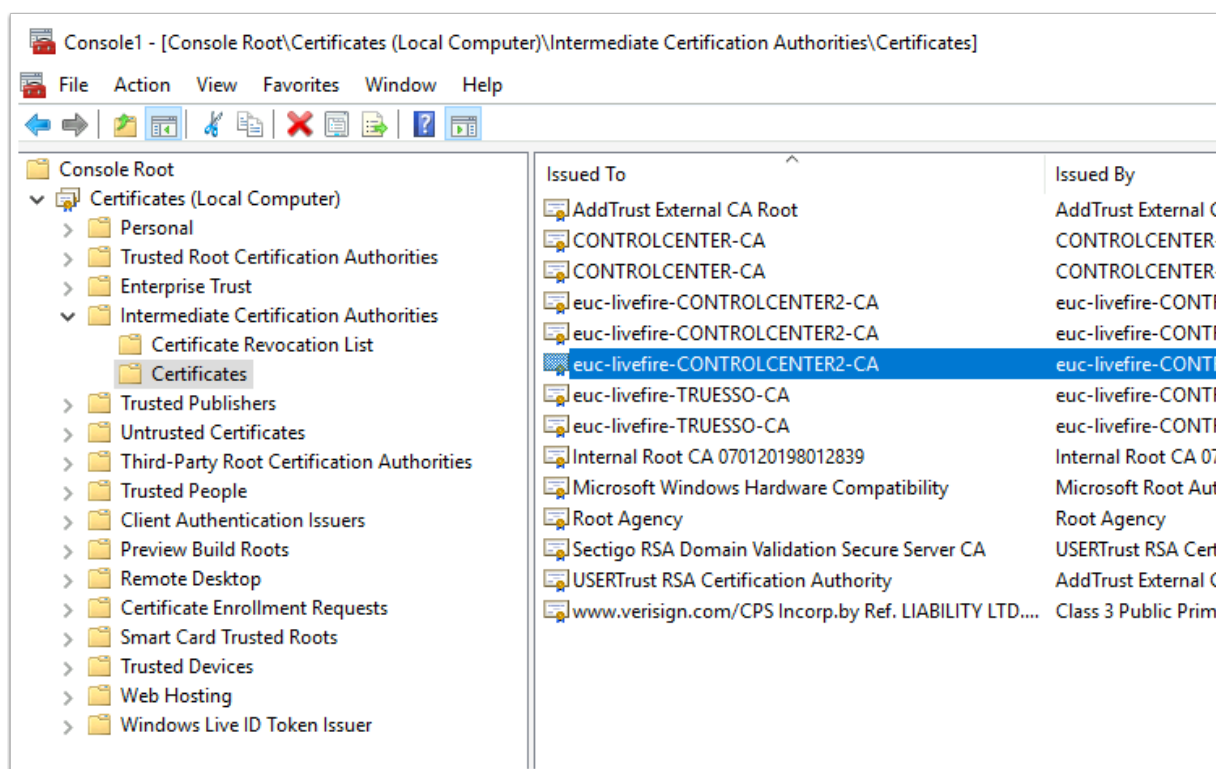
7. This might be the result. If it is not move on to **Step 10**

- As we mentioned early, for VMware Horizon Enrolment services to work, it critical we have a Healthy Certificate Services environment.
- Move on to the following step to clean out your **Microsoft Certificate Services**

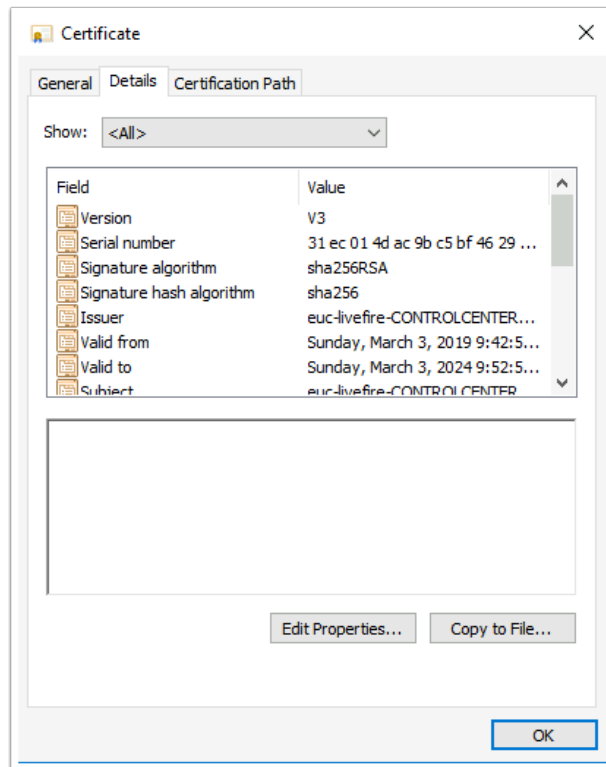


8. Perform the following steps on the following stakeholder platforms:-

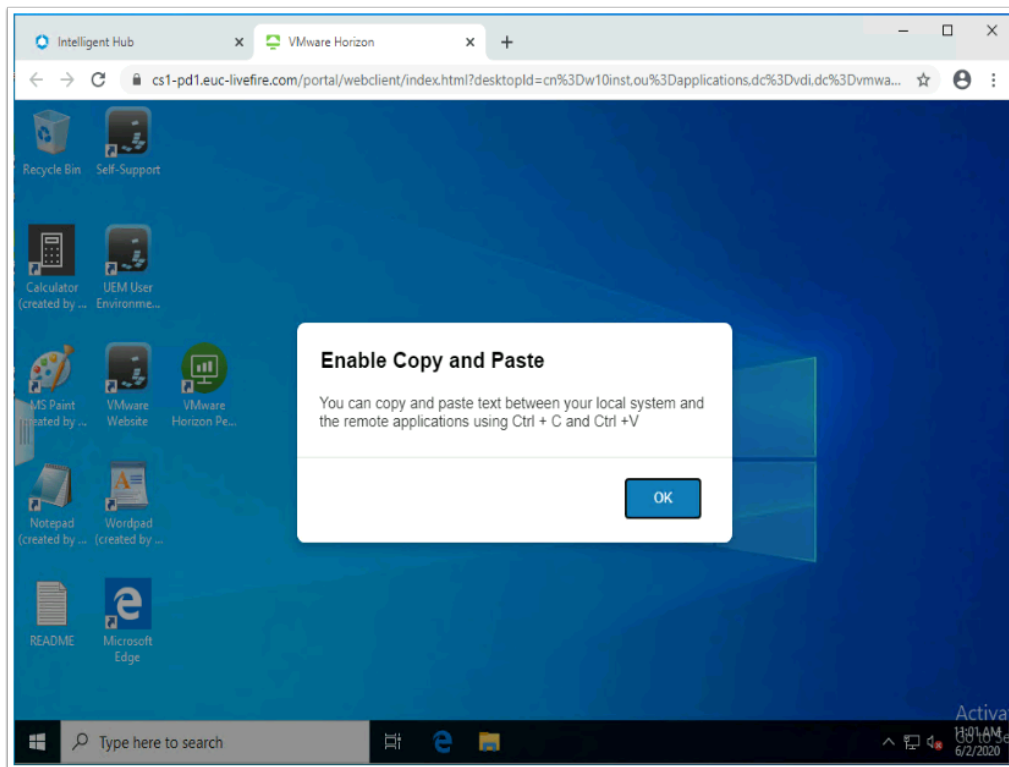
- The **TRUESSO** (Enrolment server), **CS1-PD1** (Horizon Connection server ) and your **ControlCenter2** (Certificate Authority) servers
  - Repeat these task on the **W10TRUESSO** desktop
    - When you open the Certificates Snap-In for Local Computer we will go to two areas:
      - **Trusted Root Certificate Authorities > Certificates**
      - **Intermediate Certificate Authorities > Certificates**
  - On all stakeholder platforms **Delete** the following:-
    - The Certificates starting with **CA**
    - The Certificates starting with **CONTROLCENTER-CA**
      - On some of the stakeholder platforms there might be 3 and others 2



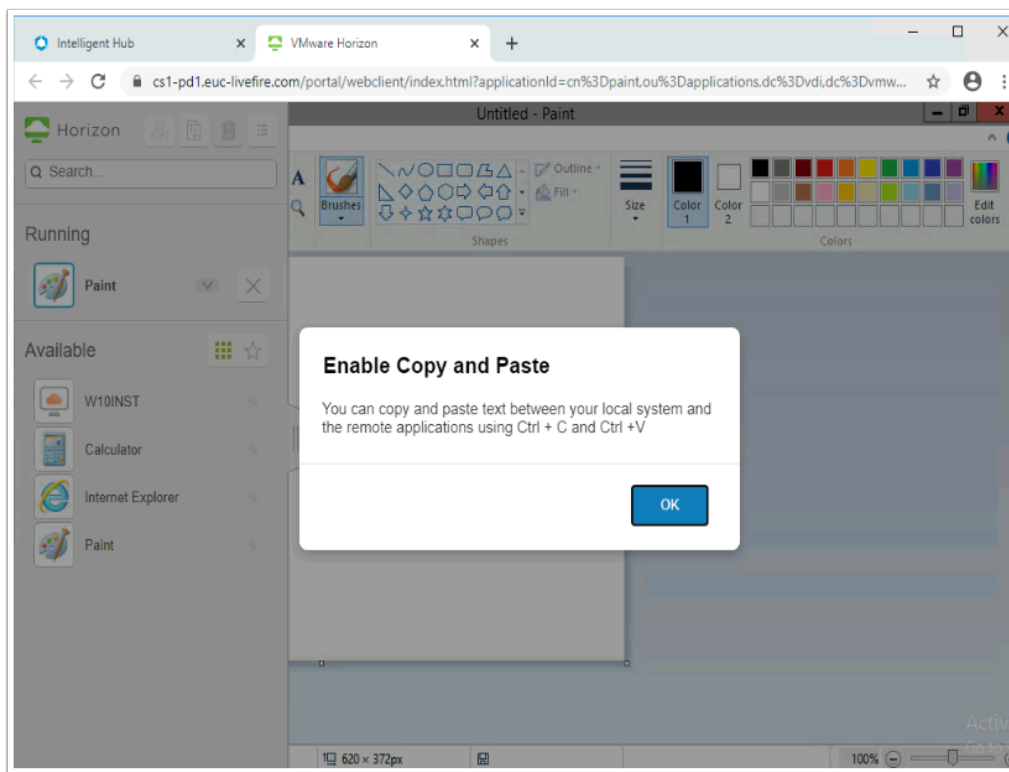
9. Perform the following steps on the following stakeholder platforms:-
- The **TRUESSO** (Enrolment server), **CS1-PD1** (Horizon Connection server ) and your **ControlCenter2** (Certificate Authority) servers
    - Repeat these task on the **W10TRUESSO** desktop
      - When you open the Certificates Snap-In for Local Computer we will go to two areas:
        - **Trusted Root Certificate Authorities > Certificates**
        - **Intermediate Certificate Authorities > Certificates**
    - On all stakeholder platforms **Delete** the following:-
      - You will notice there are certificates starting with **euc-livewire-CONTROLCENTER2-CA**
      - Always start by selecting the bottom of either a set of two or three certificates
        - Select the **certificate** and select **Open**



10. On the Certificate, select the **Details**. You will notice the certificate starts with a **Serial number** of **31 ec 01....**
  - PLEASE NOTE: If the certificate **Serial number** starts with **29 03 ...** This is a valid cert and should be left alone.
  - Select **OK** to close the **Certificate** window and then **delete** this certificate
    - Perform this task on all Stakeholder Platforms
  - Open the **Command Prompt** on all **stakeholder platforms** and type the command **GPUPDATE /Force**
  - You are now ready to again test your login through **Workspace ONE Access**. If necessary go back to Paragraph1 and repeat the login process



11. Launch another session from the **Workspace ONE** portal and launch your **Desktop** entitlement.
  - This should be the result



12. Launch another session from the **Workspace ONE** portal and launch an **Application** entitlement.

- This could be the result, I have just launched Paint

## Acknowledgments

A Huge thank you to

- Rahul Jha from Global Support Services in Bangalore India for his support in development of this content
- Spas Kalarov from the Hybrid Cloud Team at Livefire for help in Troubleshooting Certificate Services
- Graeme Gordon from Tech Marketing for their guidance on Tech Zone

## References

<https://docs.vmware.com/en/VMware-Horizon-7/7.12/horizon-administration/GUID-7314E2AF-2DA0-4BD0-939D-F5F352B3EEE0.html>

<https://techzone.vmware.com/resource/workspace-one-and-horizon-reference-architecture#Setting-truesso>

## About the Author: Reinhart Nel

<https://www.dropbox.com/s/cf32s1ddeyt5zx4/Reinhart%20Nel.pdf?dl=0>

Any questions related to this session, email Reinhart at Livefire@vmware.com

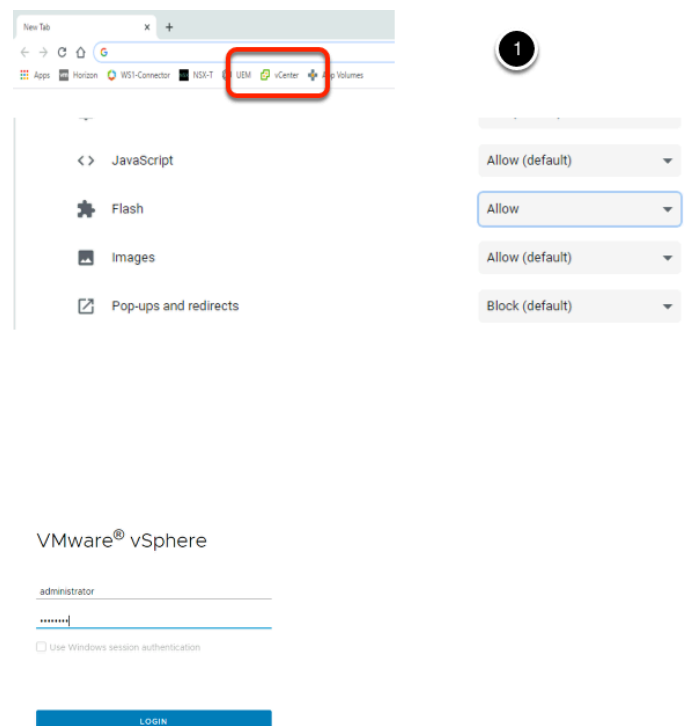


# Day 4

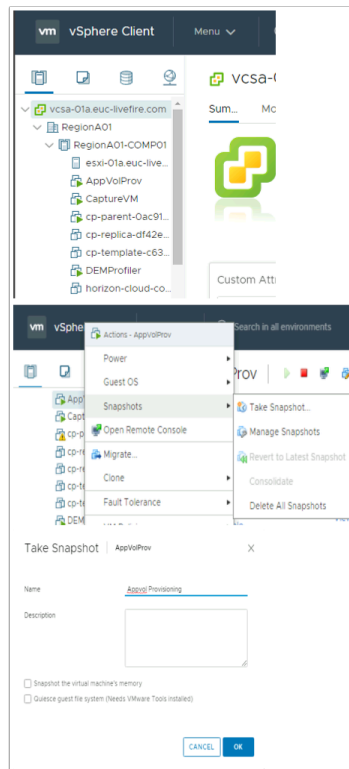
# VMware App Volumes Operations

VMware App Volumes 4.x has been re-engineered completely. The objective of these exercises is to take you through some of the most basic concepts and understand how they relate.

## Part 1. Packaging Creation

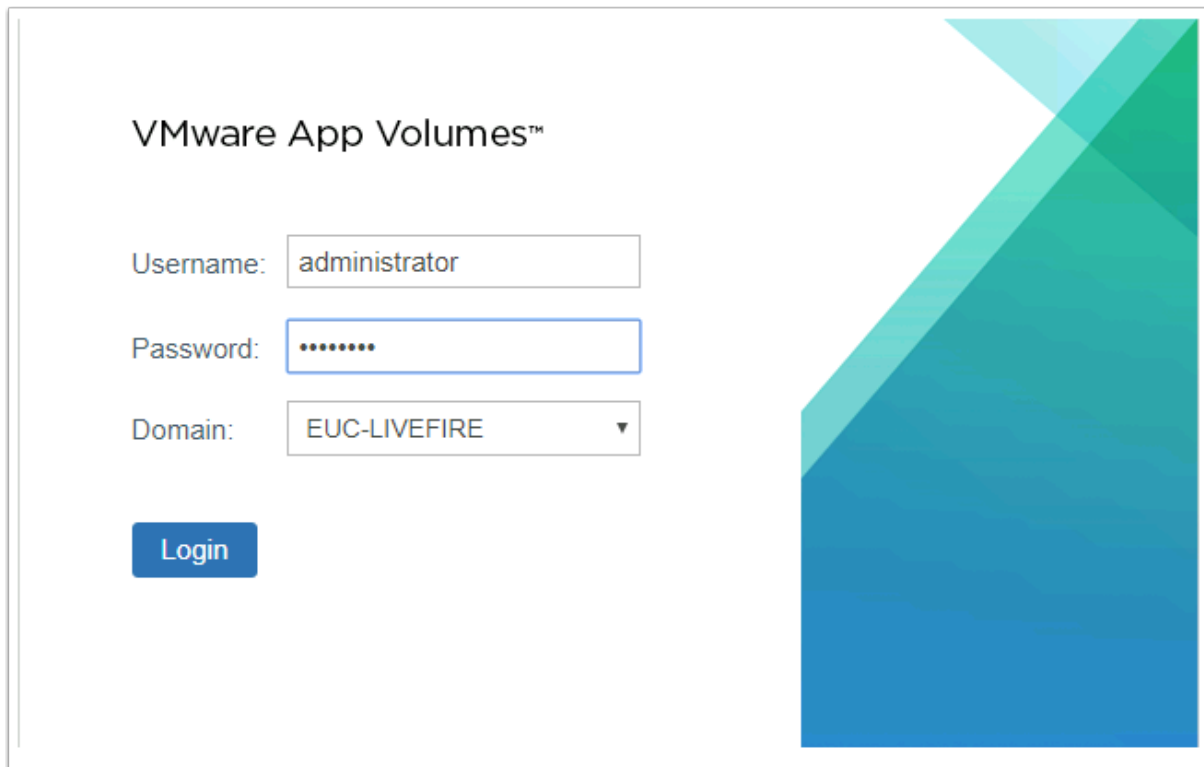


1. On your **ControlCenter2 Desktop** open your **Chrome Browser** and select the the **vCenter** shortcut on the favourites bar.
  - In the "Your connection is not private" window click on **advanced** and then **proceed to site**.
  - Right-click the **Not Secure** and select **Flash to Allow**
  - Select **Reload** under the address bar
  - Enter your User **Administrator** with the password **VMware1!** ,
  - Select **Login**



## 2. Under **Hosts and Clusters** in the Inventory

- Select and expand the **RegionA01-COMP01** cluster
- Select and right-click the **AppVolProv** VM,
- Select **Snapshots > Take Snapshot**
- In the **Take Snapshot** window next to
  - In the **Name** section call the snapshot **Appvol provisioning**
  - Uncheck the **checkbox**, next to **Snapshot the virtual Machine's memory**
  - Select **OK**



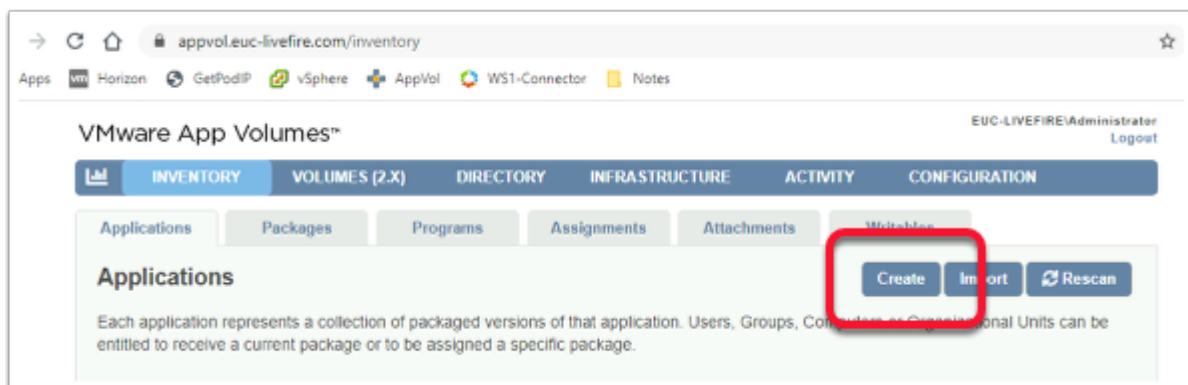
VMware App Volumes™

Username:

Password:

Domain:

- On your browser, open a **new tab** select the **AppVol** shortcut on the favourites bar  
**Username** is **Administrator** and password is **VMware1!** and select **Login**



- In the top menu bar, select the **INVENTORY** tab is selected by default. In the **INVENTORY** area we have sub-category tabs called **Applications**, **Packages**, **Programs**, **Assignments**, **Attachments** and **Writables**. These are the terms and functionality that is current with version 4.x of App Volumes.
  - In the **INVENTORY > Applications** area, select **Create**

VMware App Volumes™

appvol.euc-livefire.com/inventory#/Applications/Create

INVENTORY VOLUMES (2,3) DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

Applications Packages Programs Assignments Attachments Writables

### Create Application

An Application will provide an Application Owner the ability to manage the lifecycle of its Packages.

Name:

Description:

Owner: EUC-LIVEFIRE\Administrator

Package: ☒ Create a Package

Create

Confirm Create Application

Create Application Mozilla Firefox?

Create

3. In the **Creat Application** window

- Next to **Name** type **Mozilla Firefox**, keep all the other settings default
- Select **Create**
- In the **Confirm Create Application** window select **Create**

VMware App Volumes™

appvol.euc-livefire.com/inventory#/Applications/Create

INVENTORY VOLUMES (2,3) DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

Applications Packages Programs Assignments Attachments Writables

### Create Package for Mozilla Firefox

Provides an Application Owner the ability to create a Package for the Application

Name:

Base Package:

Storage:

Path:

Template:

Stage:

Description:

Create

Confirm Create Package

Create Package Firefox 25 for Mozilla Firefox on datastore CorpLun at path appvolumes4/packages?

\* Perform in the background  
☐ Wait for completion

Create

Packages

Each package stores one or more programs required for the application to run. A single package can be delivered to multiple computers, and one of many users.

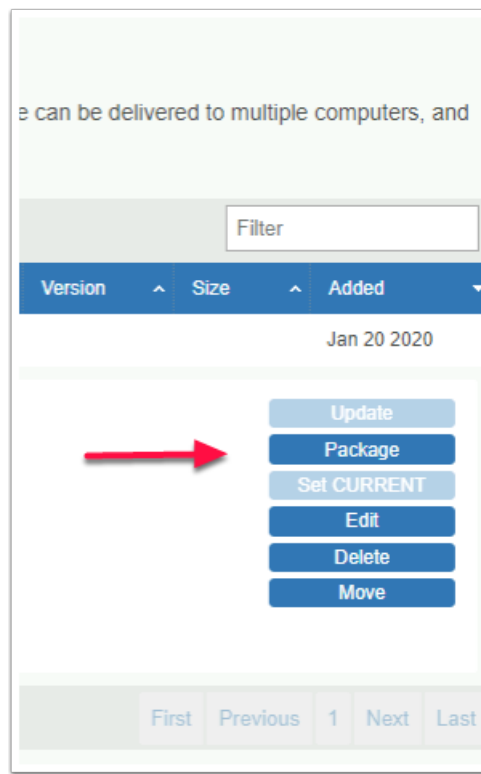
| Name       | Application     | Stage | Status     | Version | Size | Added       |
|------------|-----------------|-------|------------|---------|------|-------------|
| Firefox 25 | Mozilla Firefox | New   | Unpackaged |         |      | Jan 29 2020 |

Next step: Select Packaging VM

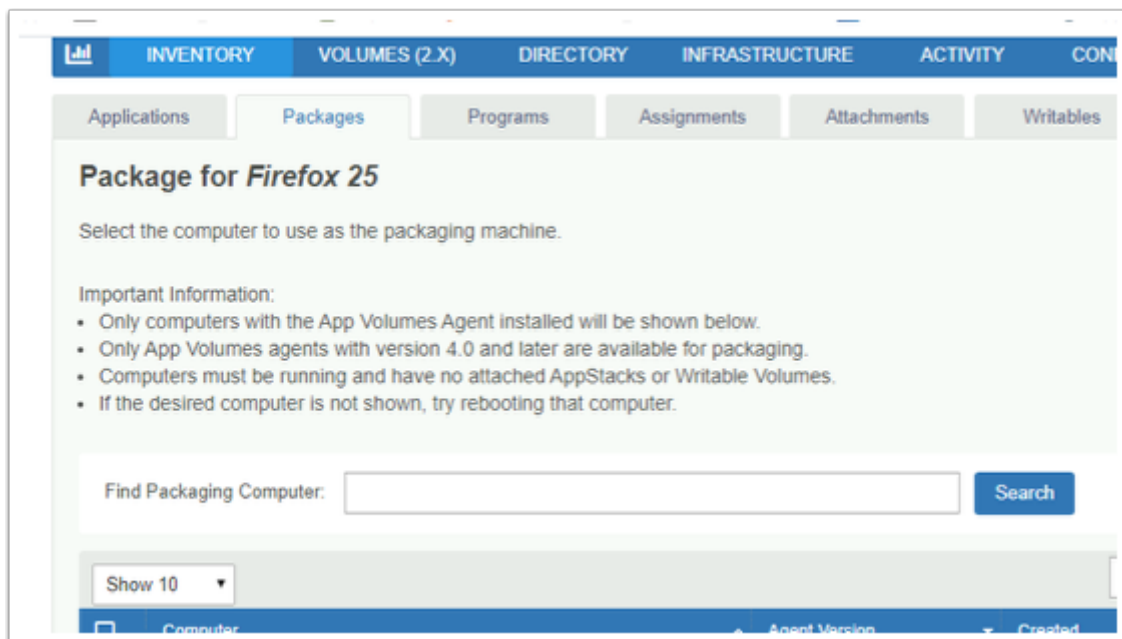
Showing 1 to 1 of 1 Packages

4. In the **Create Package for Mozilla Firefox** window, next to **Name** type **Firefox 25**

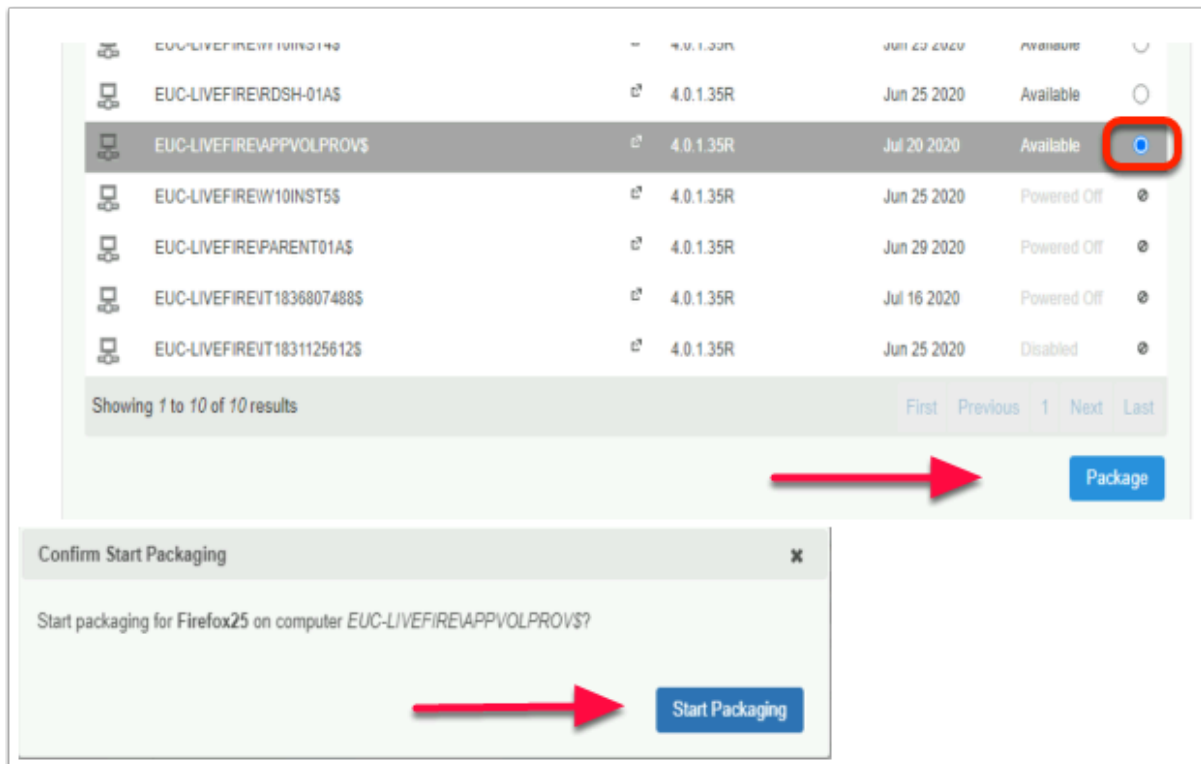
- Make a mental note of the following **Base Package, Storage, Path, Template** and **Stage**
- Select **Create**
- On the **Confirm Create Package** window select **Create**
- Select the **Packages** tab, notice that once the Application and Package has been created, the Package itself has a status of **Unpackaged**



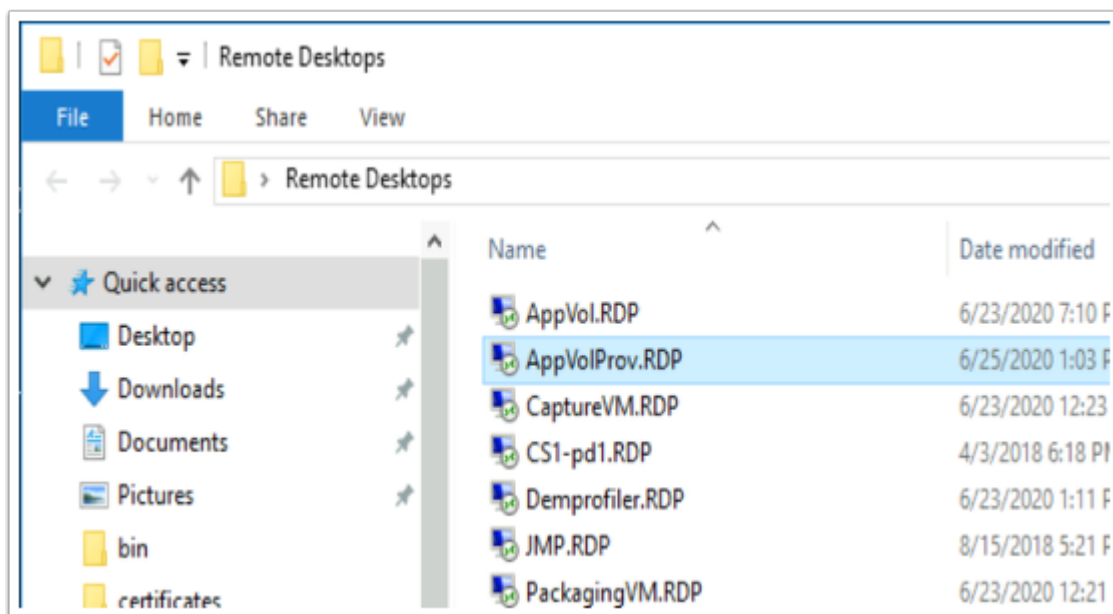
5. Expand the Firefox 25 package and select the **Package** button



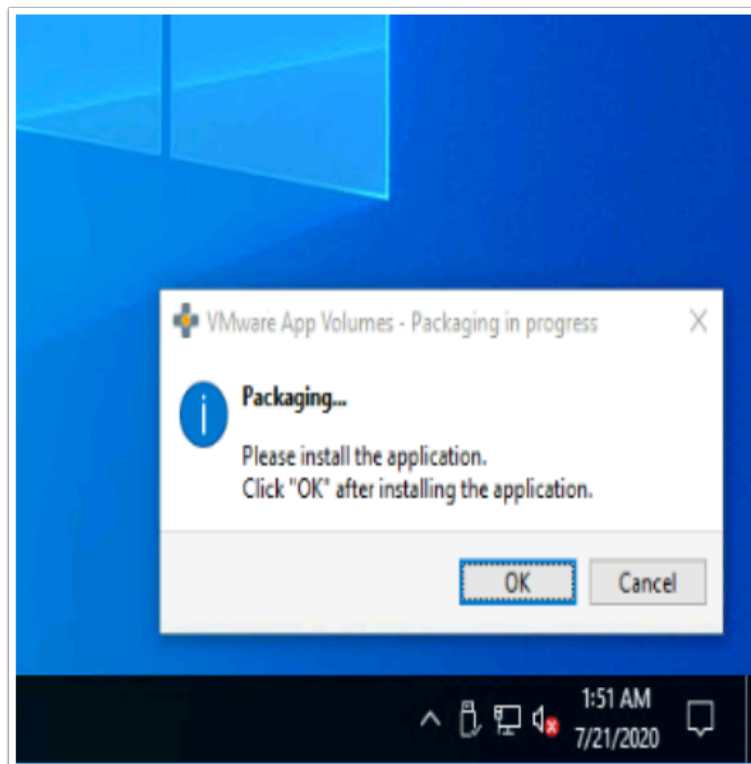
6. In the **Package for Firefox25** next to **Find Packaging Computer** select **Search**



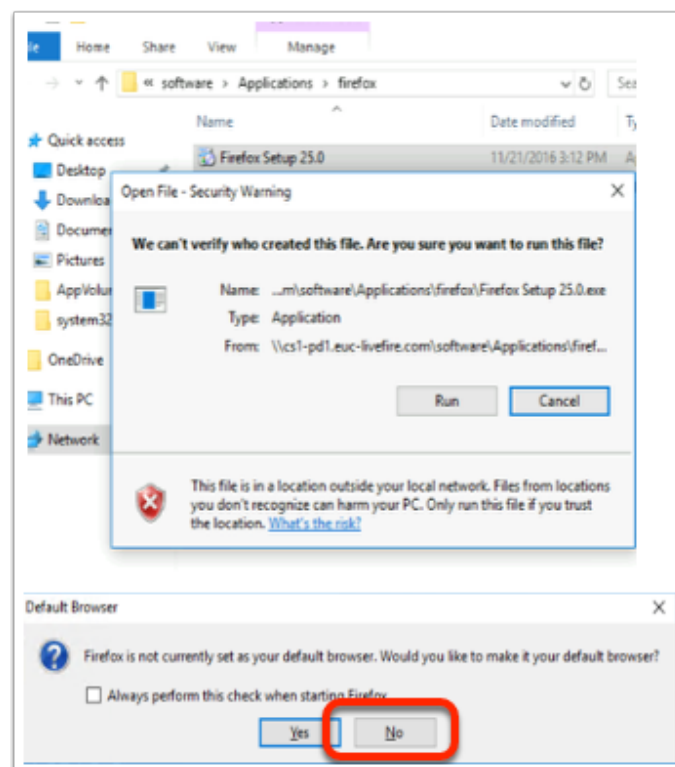
7. Select **EUC-LIVEFIRE\APPVOLPROV\$** radio button and select **Package**
  - On the **Confirm Start Packaging** window select **Start Packaging**



8. On the **Controlcenter2** server Desktop,
  - Open the **Remote Desktops** folder
  - Launch the **AppVolProv.RDP** shortcut
    - You should be automatically logged in as **EUC-Livefire\Administrator** with the password **VMware1!**



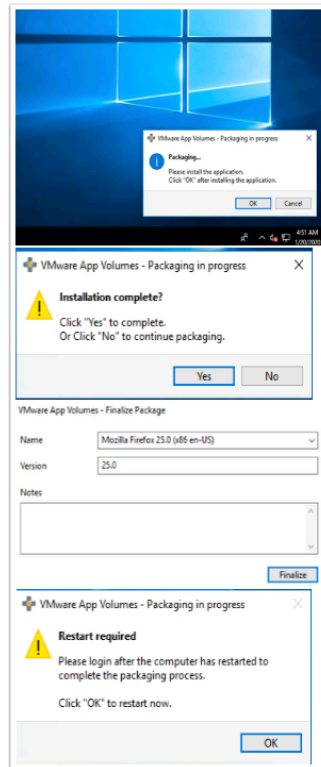
9. In the Right - Hand corner notice you have a **VMware App Volumes** window open.
- If nothing shows, restart your virtual machine and reconnect using your RDP session.
  - **DO NOT** click OK until we have finished all installation and configuration



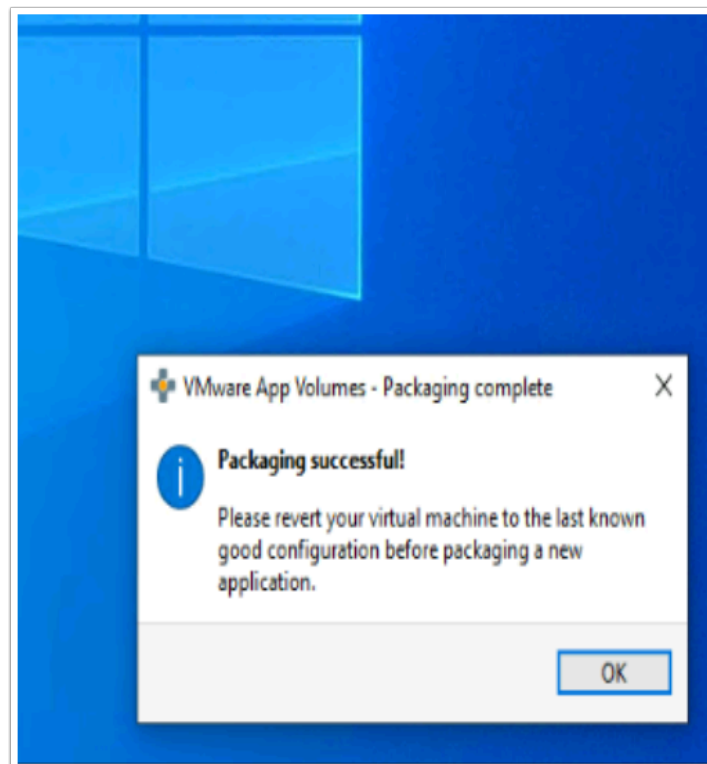
10. On your **Windows 10 Desktop** open the **software shortcut** and browse to **software\Applications\firefox**



- Double-click on **Firefox Setup 25.0** and select **Run**
- Select **Next > Next > Install > Finish**
  - The browser should launch automatically.
- On the **Import Wizard** select the **radio button** next to **Dont import anything** and select **Next**
- In the default browser window click **NO**
- **Close** the browser

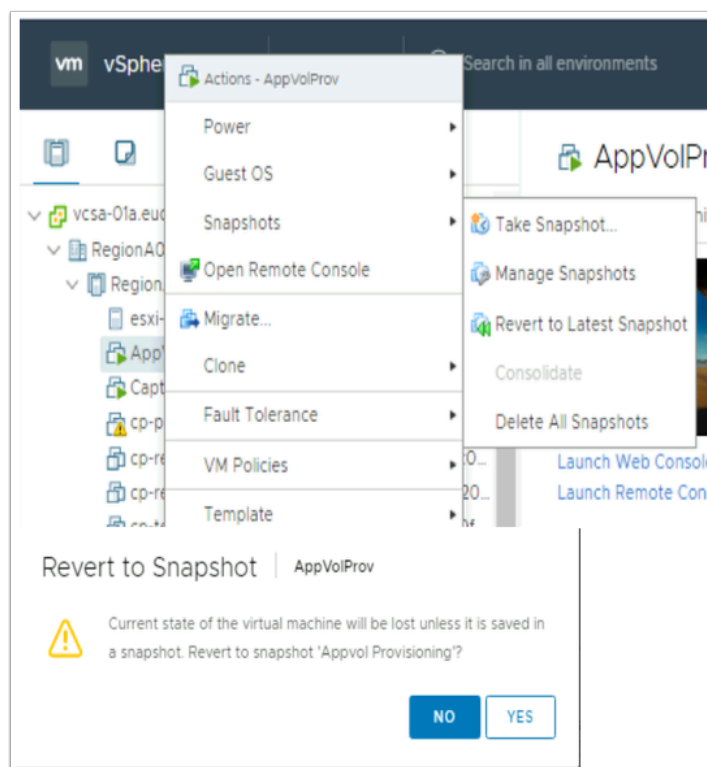


- On the **AppVolProv virtual** machine,
  - On the **VMware App Volumes - Packaging in progress** window select **OK**
  - On the **Installation complete?** window select **Yes**
  - On the **VMware App Volumes - Finalize Package** select **Finalize**
  - On the **Restart required** window select **OK**
  - Give the virtual machine at least 2 minutes to reboot



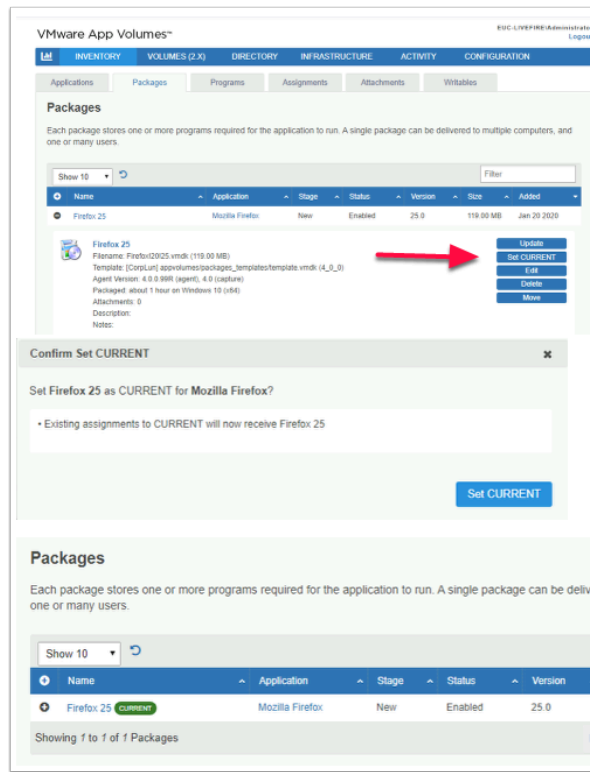
## 12. Reconnect to your **AppVolProv.RDP**

- Notice there is now a Packaging succesful message
- Select **OK**
- **Close** your AppVolProv RDP session



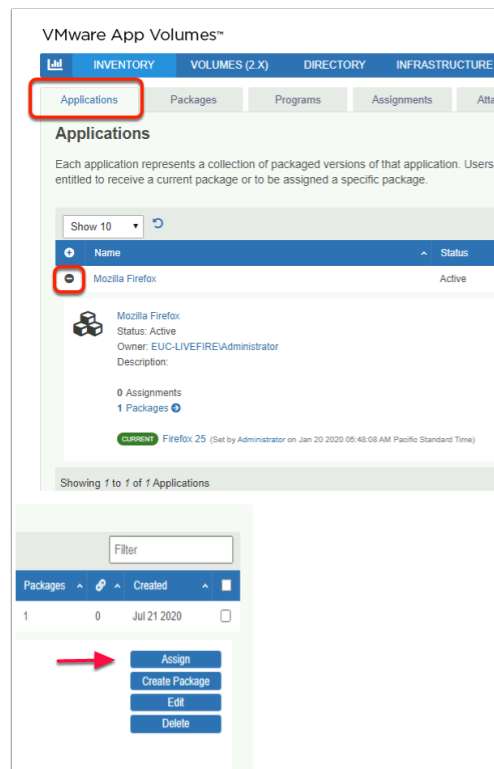
13. On your **ControlCenter2** server desktop

- Open your **Chrome** browser, select your **vSphere web client**,
- Select and right-click your **AppVolProv** machine and select **Revert to latest Snapshot**
- On the **Revert to Snapshot window** select **Yes**
- Select and right click your **AppVolProv VM** and **Power on**



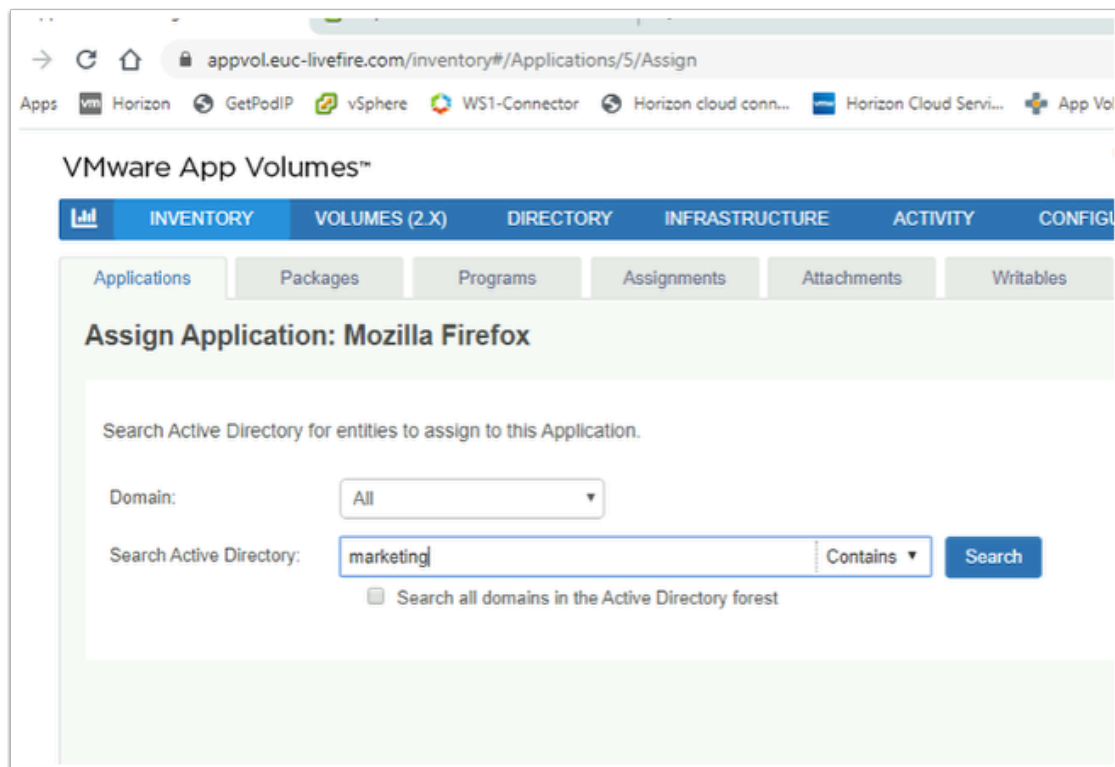
14. Revert back to your App Volumes Admin Console

- Select **Inventory > Packages** area and expand **Firefox25**.
- Select the **Set CURRENT** box
- On the **Confirm Set CURRENT** window select **Set CURRENT** box



15. Go **INVENTORY** > **Applications**

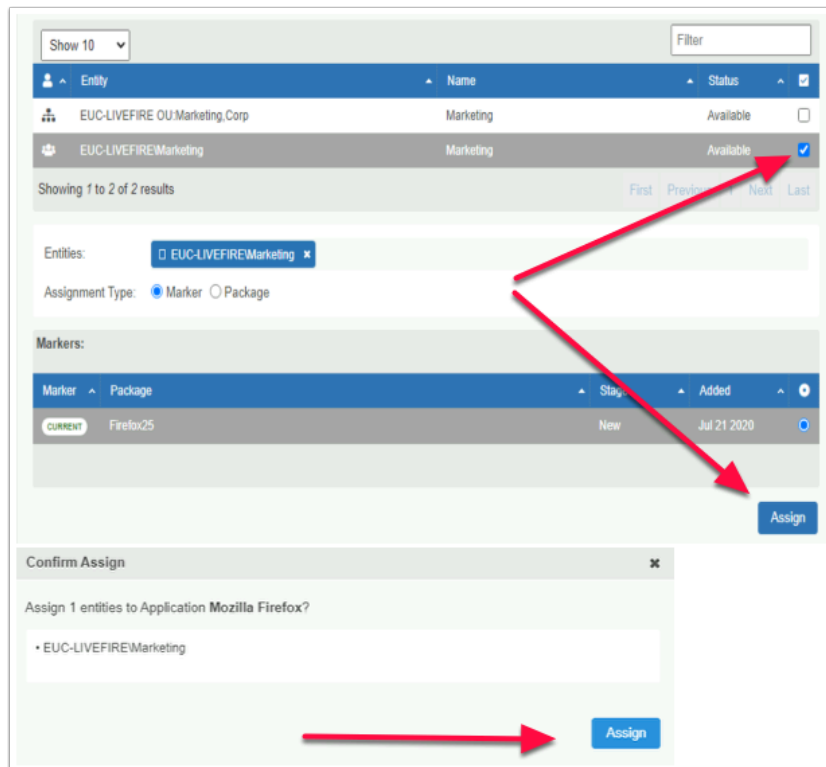
- Expand **Mozilla Firefox**
- Select **Assign**



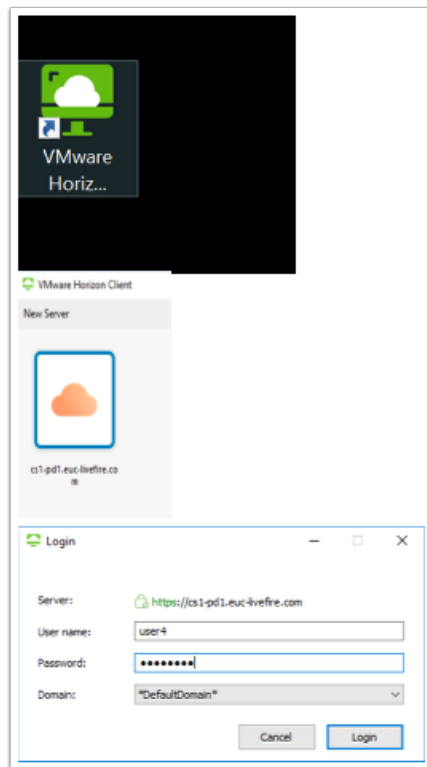
16. In the **Assign Application: Mozilla Firefox** window

- Next to **Search Active Directory** type **Marketing**

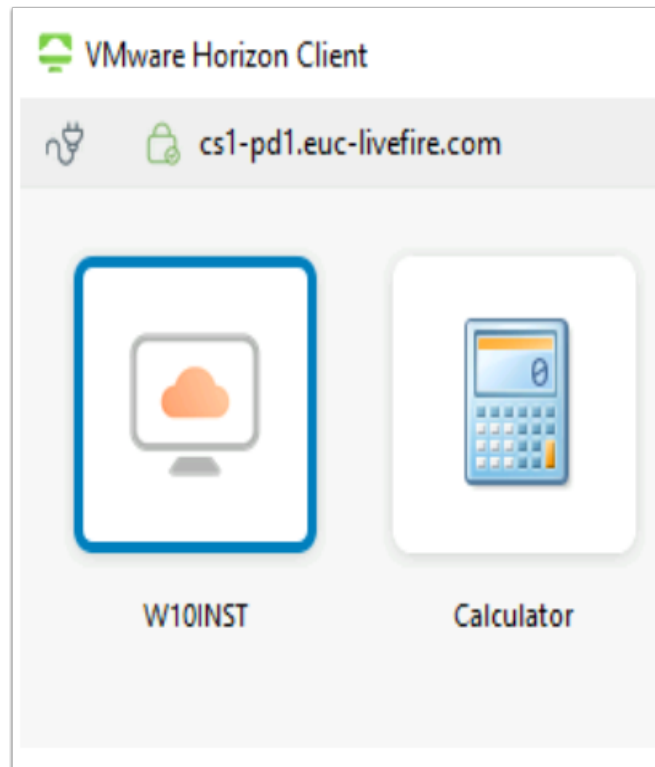
- Select **Search**



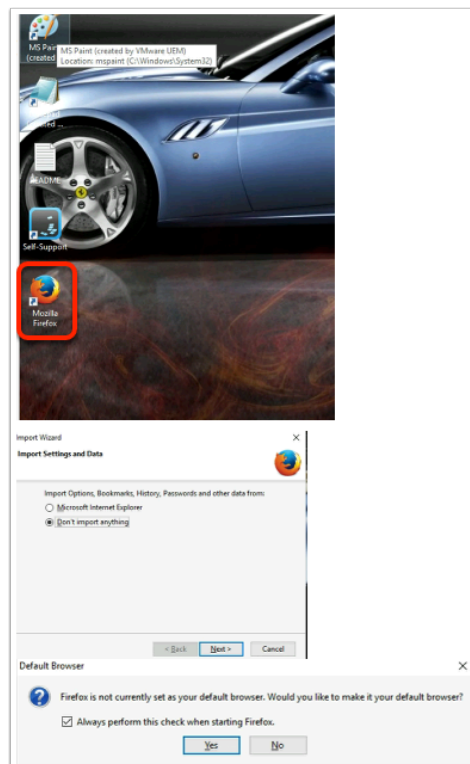
- Take a look at what options are available to you. Notice an Assignment can either be **Marker** or **Package** based. Also the stage is **New**
  - Select the checkbox next to **EUC-LIVEFIRE\Marketing**
  - Select **Assign**
  - In the **Confirm Assign**, select **Assign**



18. On your **ControlCenter2** Desktop
- Launch your **Horizon Client**
  - Select the **CS1-PD1.euc-livfire.com** ICON
  - On the **Login** window
    - Next to **User name** type **user4**
    - Next to **Password** type **VMware1!**
    - Select **Login**

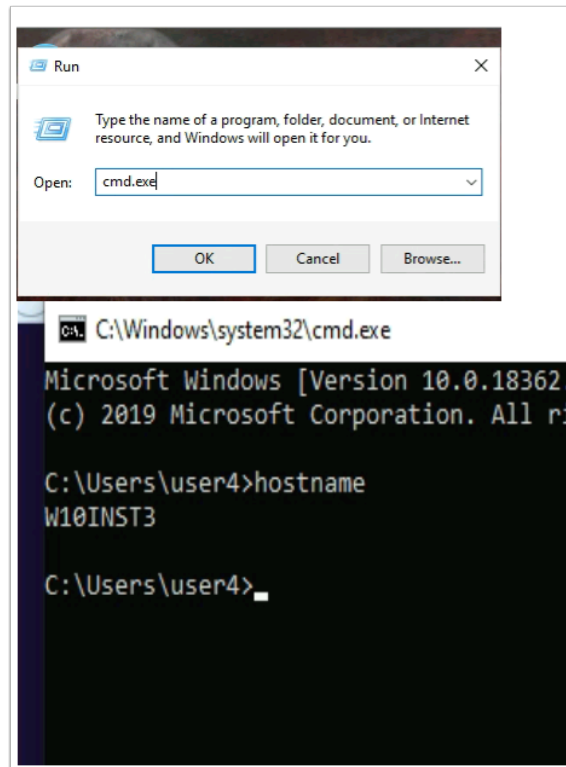


19. On the **Horizon Client** select your **W10INST** desktop entitlement



20. On the W10 virtual desktop select the **Mozilla Firefox** shortcut to launch Firefox
- On the **Import Settings and Data** window, select the **radio button** next to **Don't import anything** and select **Next**
  - On the **Default Browser** window select **No** to close the window

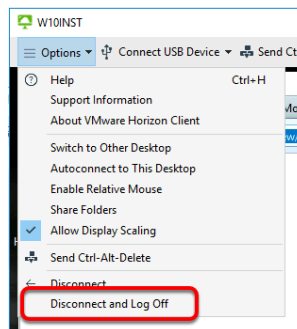
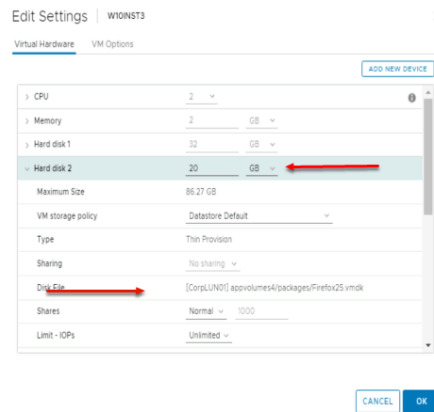
(In a later exercise we will use Dynamic Environment Manager to manage the Application settings)



21. From your **Horizon virtual desktop**

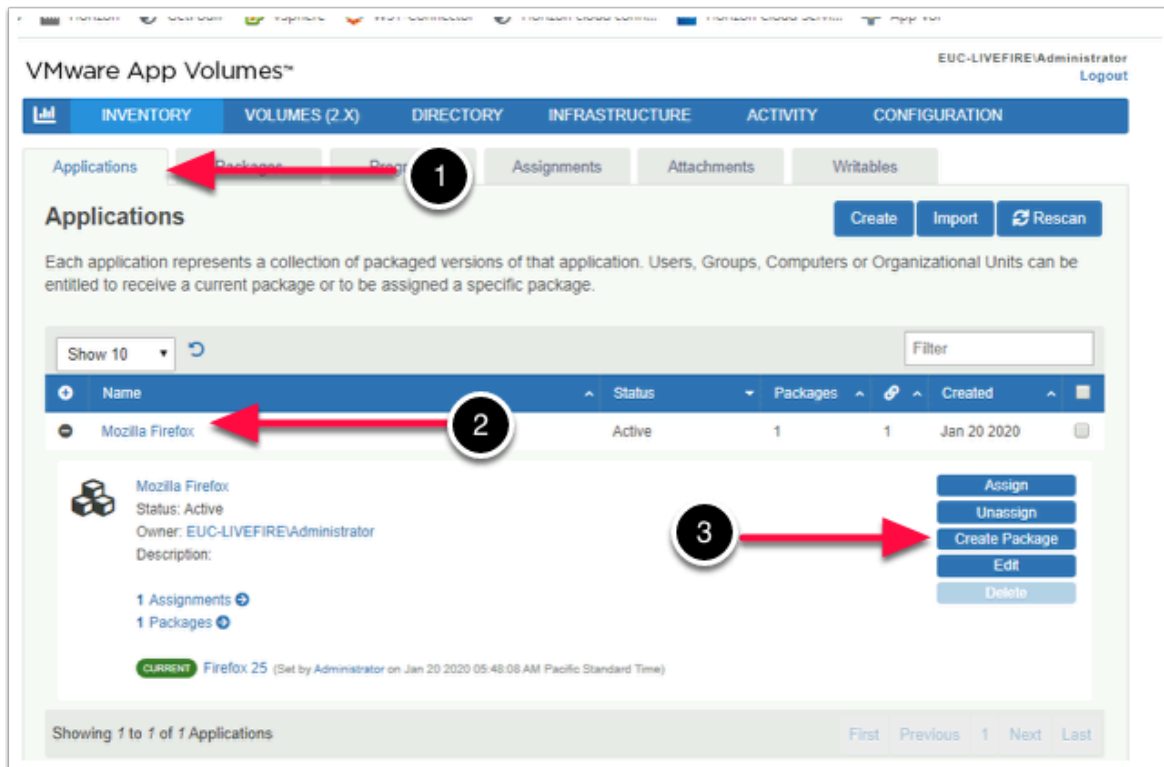
- Right click the **Start** button > **Run** > type **cmd.exe**
- In the **Command prompt** window, type **Hostname** .
  - Take note of your assigned virtual machine



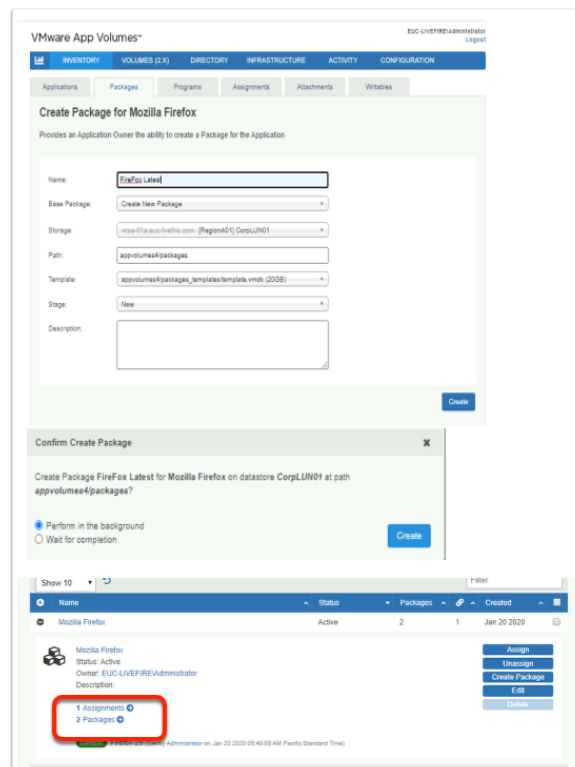


22. On your **ControlCenter2** server Desktop

- Revert back to the **vSphere Web Client**,
  - If necessary login as **administrator** with password **VMware1!**
- Select your **noted virtual desktop** (example = W10INST).
- Select **Edit settings**, notice you now have an AppStack attached to the App Volumes provisioning virtual machine.
- Ensure you **disconnect and log off** from your Horizon session.

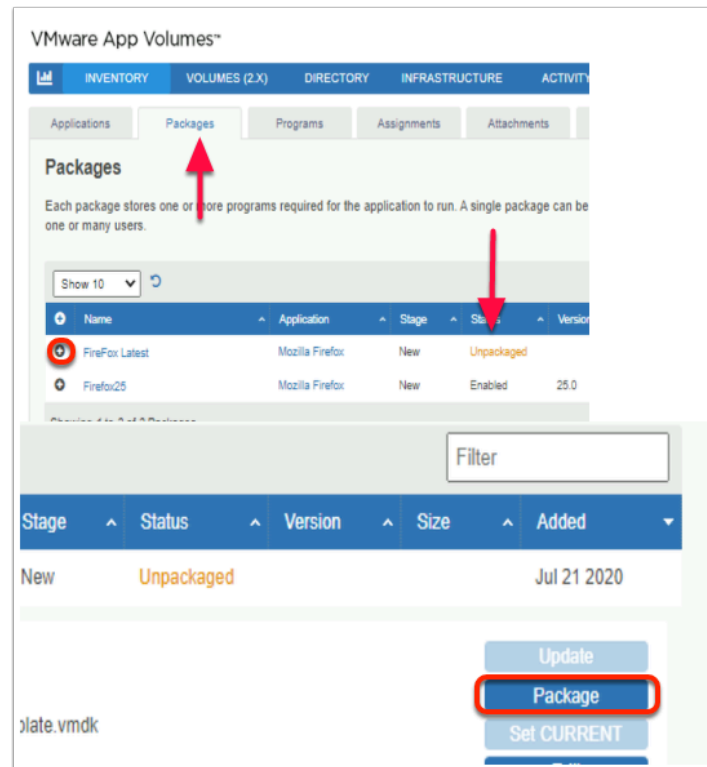


23. Revert to the **App Volumes** Tab in your Chrome browser
- In **INVENTORY > Applications**.
  - **Expand Mozilla Firefox**
  - Select **Create Package**

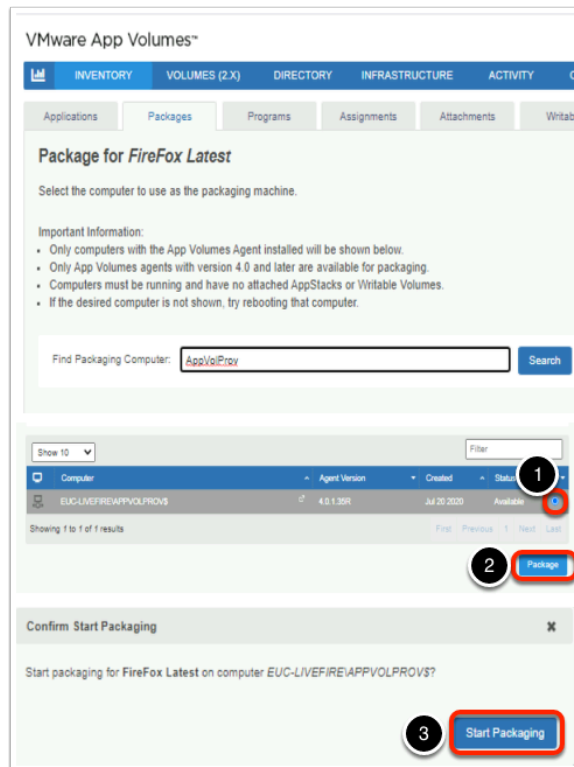


24. In the **Create Package for Mozilla Firefox** window

- Next to **Name:** type **Firefox Latest** and select **Create**
- On the **Confirm Create Package** window select **Create**
  - Notice you now have **2 Packages** under Mozilla Firefox

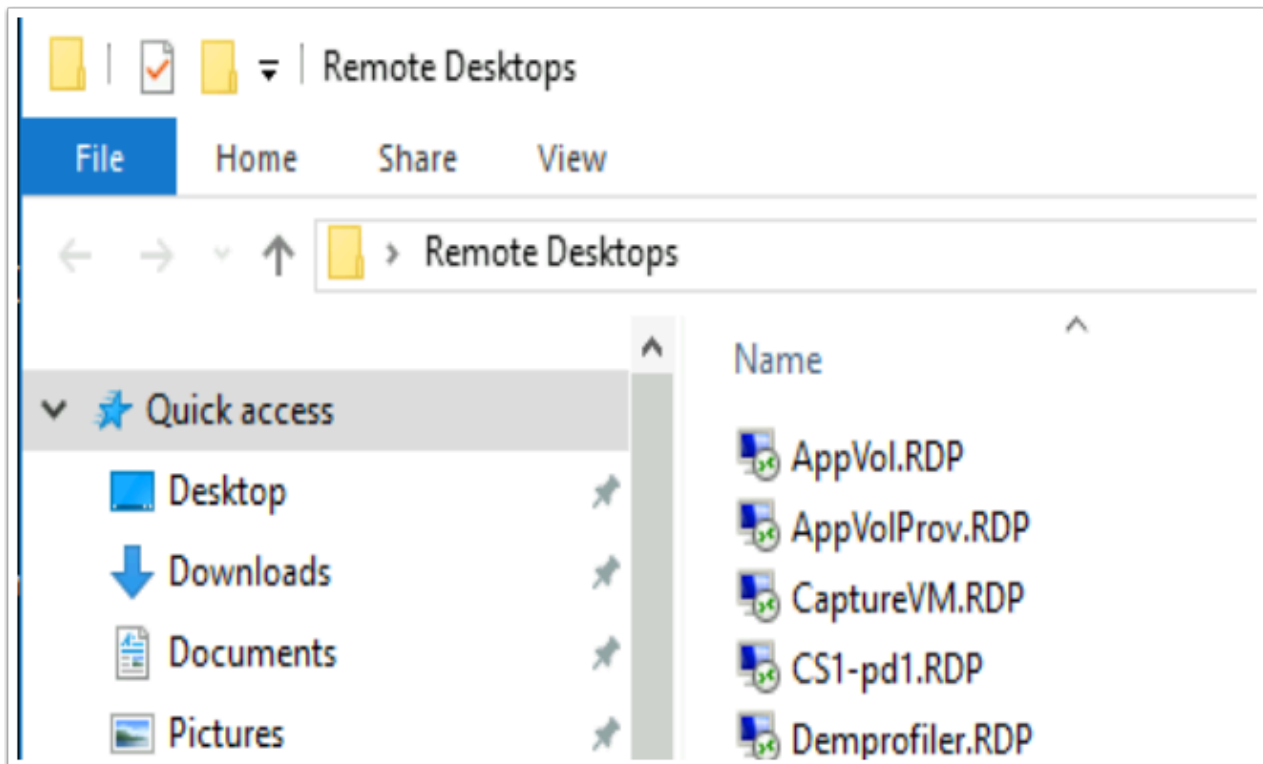


25. In the **VMware App Volumes Manager**, select the **Packages** tab
- Select and expand **Firefox Latest**
  - Select **Package**

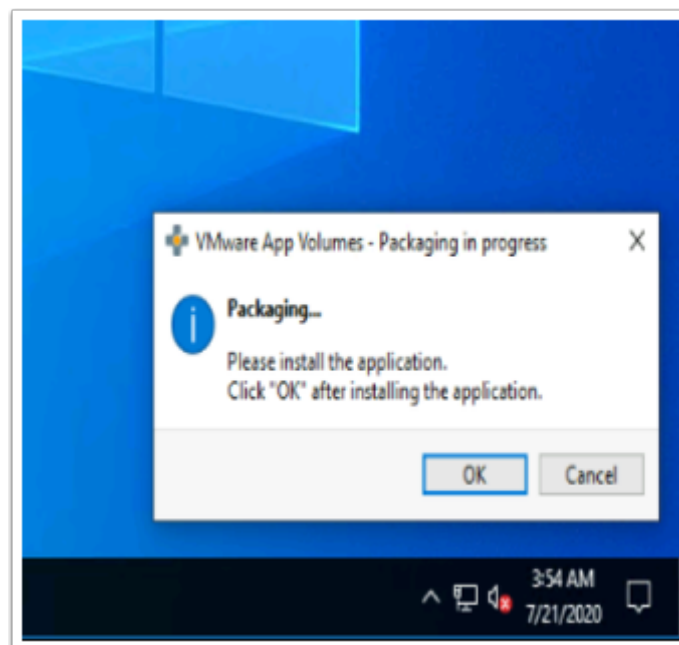


26. In the **Package for Firefox Latest** window

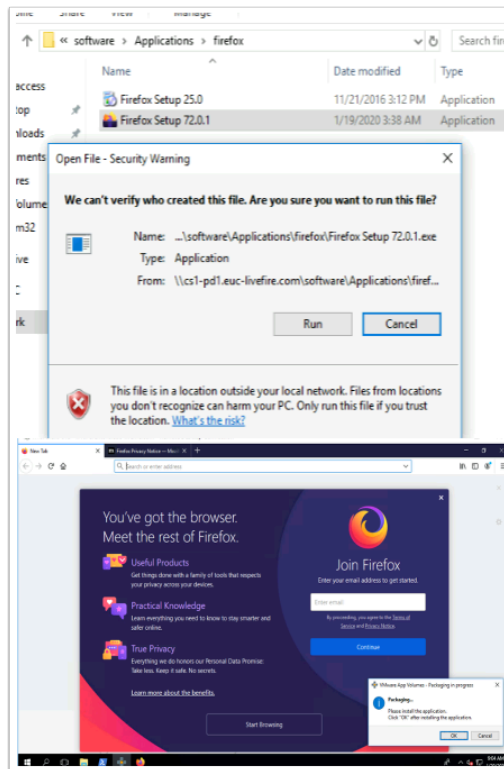
- Next to **Find Packaging Computer** type **wAppVolProv**
  - Select **Search**
- In the below search area select the **radio button** next to **Available**
  - Select **Package**
- On the **Confirm Start Packaging** window select **Start Packaging**



27. On the **Controlcenter2** server Desktop,
- Open the **Remote Desktops** folder and launch the **AppVolProv.RDP** shortcut
    - You should be automatically be logged in as
      - Username: **EUC-Livefire\Administrator**
      - Password: **VMware1!**

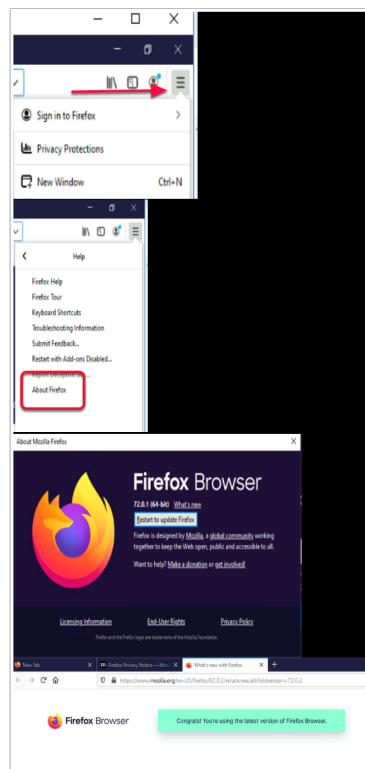


28. On your **AppVolProv** Desktop
- In the Right - Hand corner notice you have a **VMware App Volumes** window open. **DO NOT** click OK until we have finished all installation and configuration



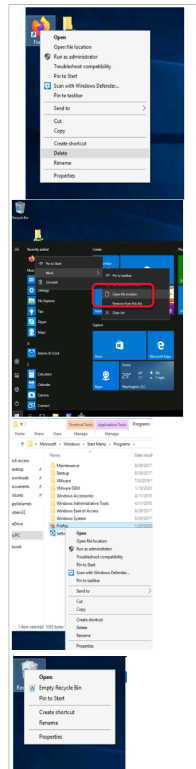
29. On your **AppVolProv** Desktop

- Open the **software shortcut** and browse to **\\software\\Applications\\firefox**
- Double-click on **Firefox Setup 72.0.1** and select **Run**
- Select **Next > Next > Install > Finish**
  - The browser should launch automatically.



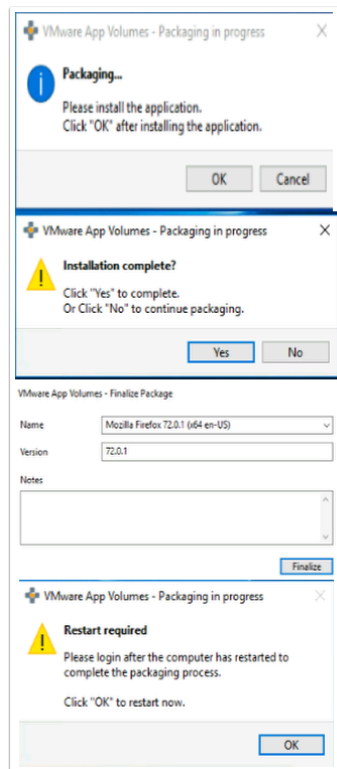
30. In your **Firefox Browser**

- Select the **3 slats** in the top right-hand corner
- Select **Help > About Firefox**
- Select **Restart to update Firefox**
- **REPEAT** these steps until Firefox is up to date
- You should get a notice, **Congrats! You're using the latest version of Firefox Browser**
- **Close** Mozilla Firefox



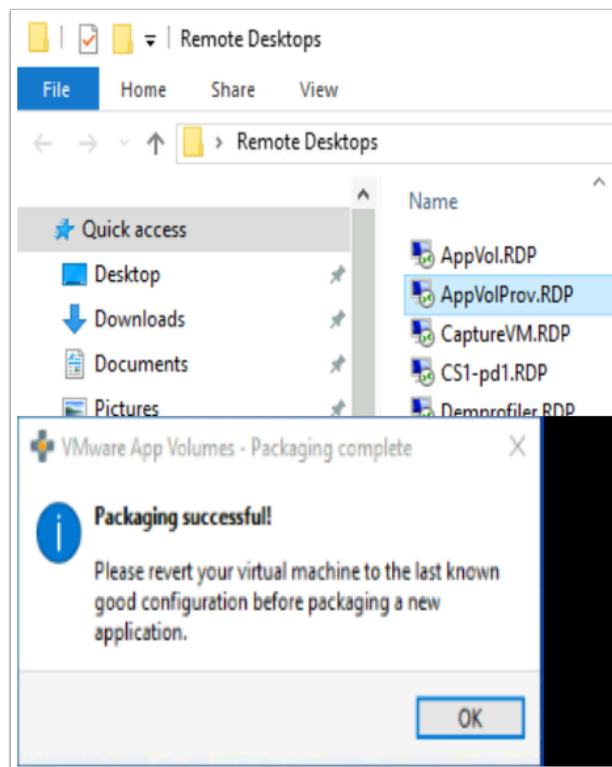
31. On the AppVolProv Desktop

- We will start removing all references to Firefox. ie shortcuts from the Desktop. In a later lab, will manage these functions, using Dynamic Environment Manager.
- Select the **shortcut on the Desktop** and **Delete**
- On the **AppVolProv** desktop
- Select **Start** button and launch the **Start Menu**,
- Select > right click the **Mozilla Firefox** icon > **More > Open file location**
- Delete **the Firefox** Shortcut
- **Empty** the Recycle Bin on the Desktop



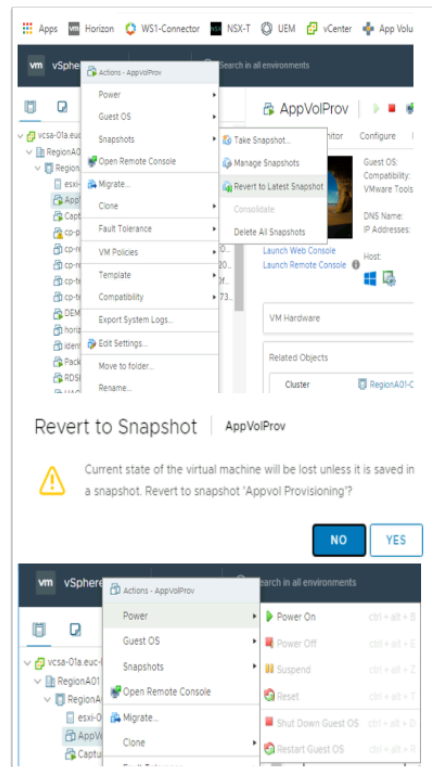
32. On the **AppVolProv** desktop,

- On the **VMware App Volumes - Packaging in progress** window select **OK**
- On the **Installation complete?** window select **Yes**
- On the **VMware App Volumes - Finalize Package** select **Finalize**
- On the **Restart required** window select **OK**

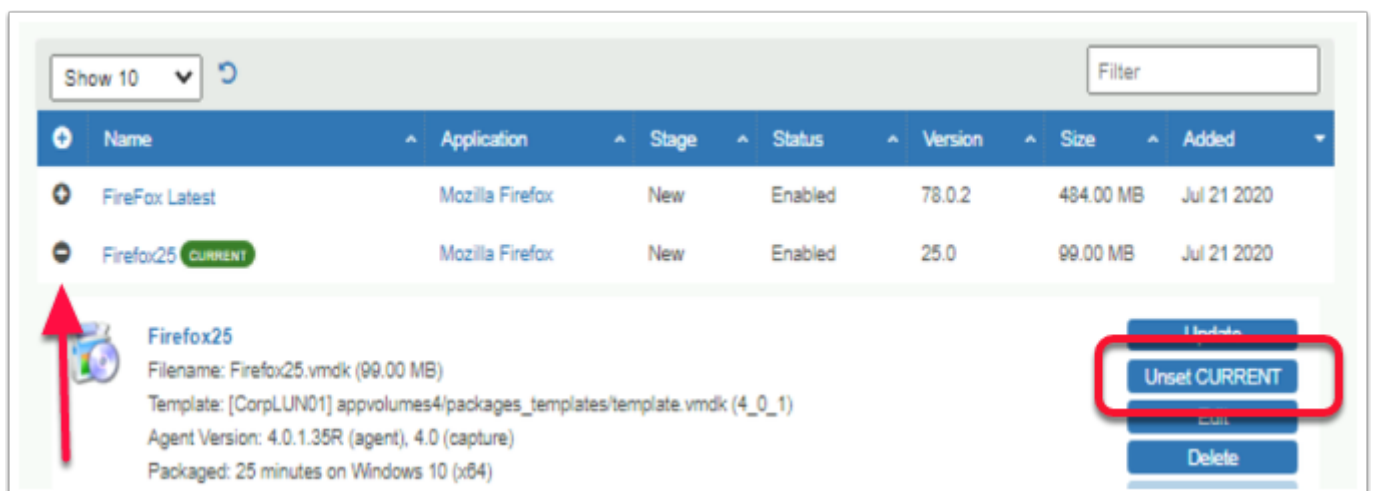




33. On your **ControlCenter2** server
- From the **Remote Desktops** Folder. Launch your **AppVolProv.RDP**
  - Notice there is now a **Packaging successful** message
  - Select **OK**



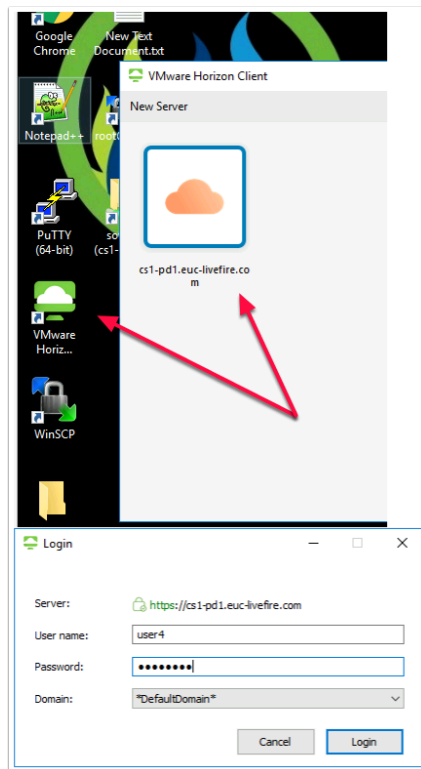
34. On your **ControlCenter2** server
- Go to your **vSphere web** client,
  - Select your **AppVolProv** machine and select **Revert to latest Snapshot** select **Yes**
  - Select and right click your **AppVolProv** VM and **Power on**



35. On your **ControlCenter2** server. **APP Volumes Manager**,
- In **INVENTORY > Packages** expand **Firefox25** and select **Unset CURRENT**
    - Notice that that the green **CURRENT** marker is no longer next to **Firefox 25**

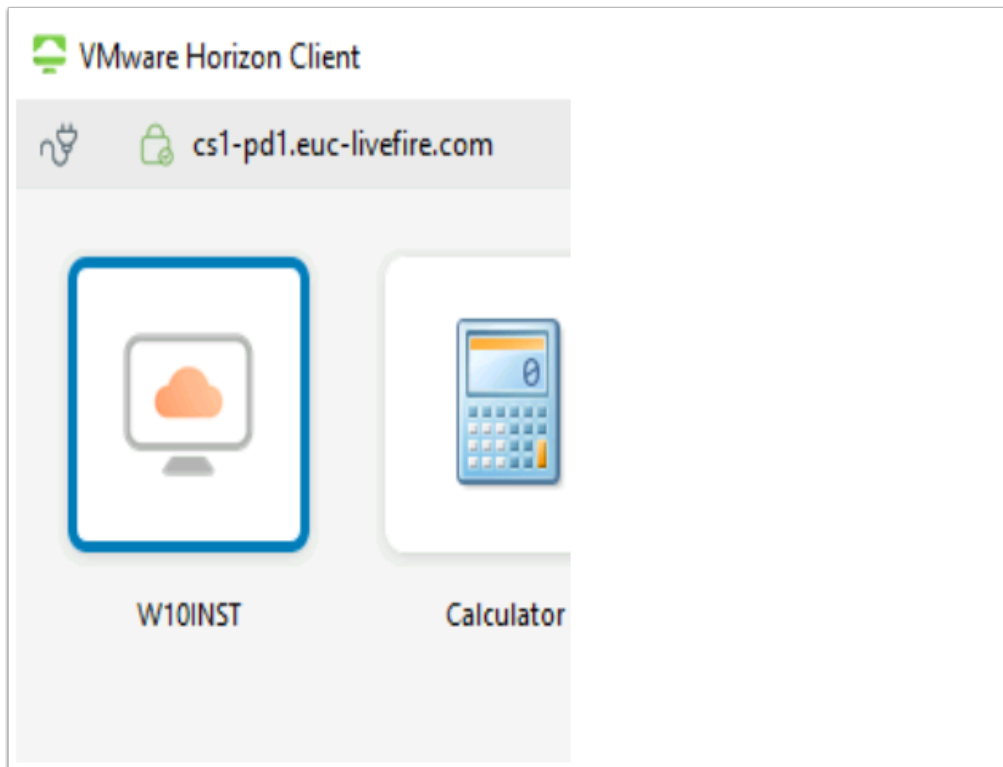


36. In **APP Volumes Manager**, under **Packages**
- Expand **Firefox Latest** and select **Set CURRENT**
  - In **Confirm Set CURRENT** window select the **Set CURRENT** box
    - Notice that the **CURRENT** marker is now next to **Firefox Latest**
      - Note! It does appear, that one can go and select **Set CURRENT** without having to **Unset Current** on another Package

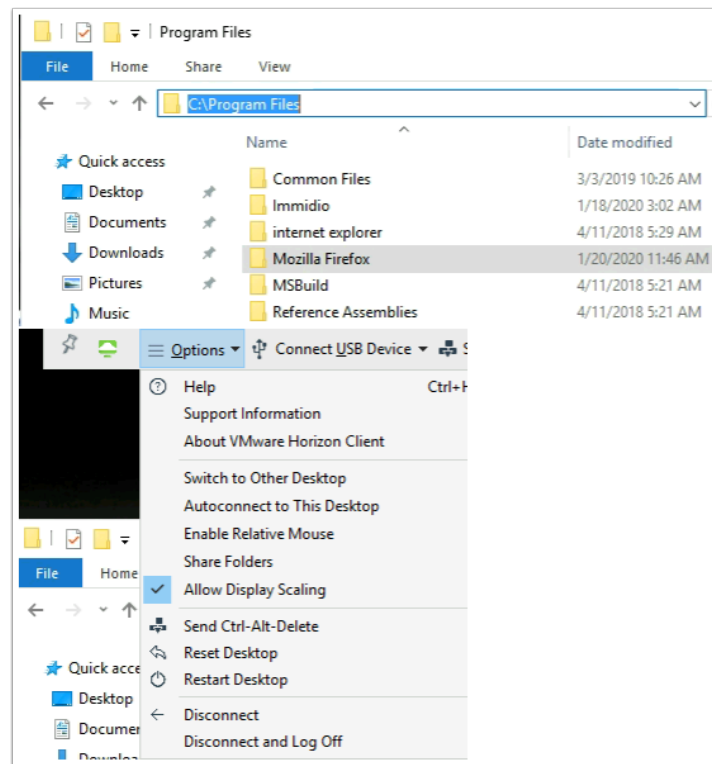


37. On your **ControlCenter2** Desktop

- Launch your **Horizon Client**
- Select and click the **CS1-PD1.euc-liveware.com** ICON
- On the **Login** window
  - Next to **Username** type **user4**
  - Next to **Password** type **VMware1!**
- Select **Login**



38. On the **Horizon Desktop Client** select your **W10INST** desktop entitlement



39. On the Windows 10 virtual desktop session
- Select the **File Explorer** folder and browse to **c:\Program Files**
  - Notice the **Mozilla Firefox** folder
  - Also notice there are no **Mozilla Firefox** icons

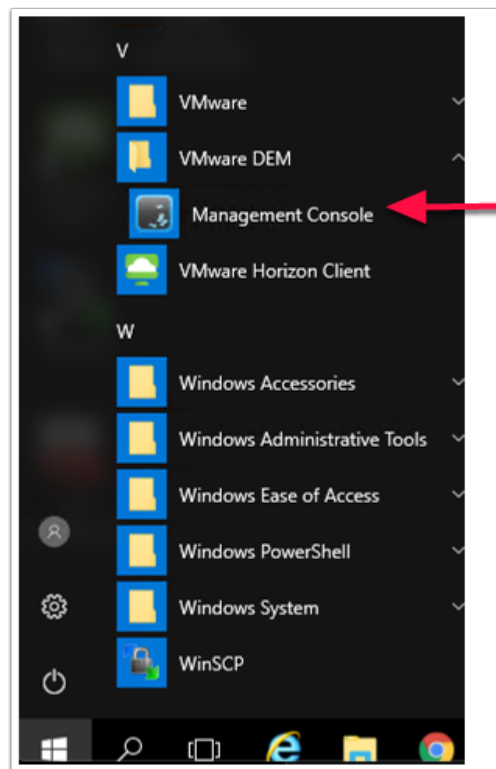
(In a later exercise we will use **Dynamic Environment Manager** to manage the Application short-cuts)

- **Disconnect and logoff** from your Horizon session

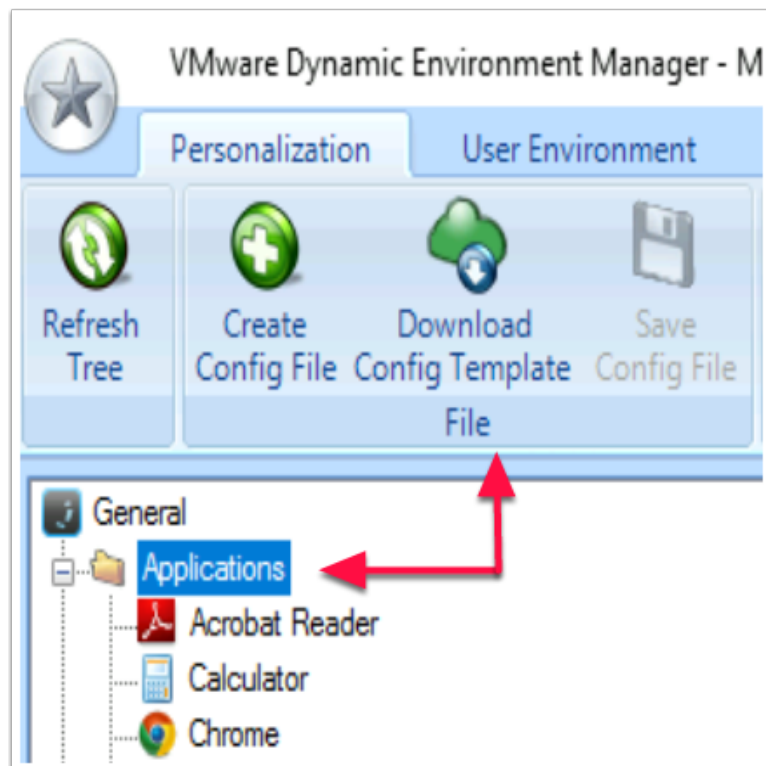
## Part 2: Using Dynamic ENVIRONMENT MANAGER to assign and manage applications delivered using App Volumes AppStacks

When we launched Firefox application any settings we would make to the App Volumes Package would be lost. The package itself is a Read Only container.

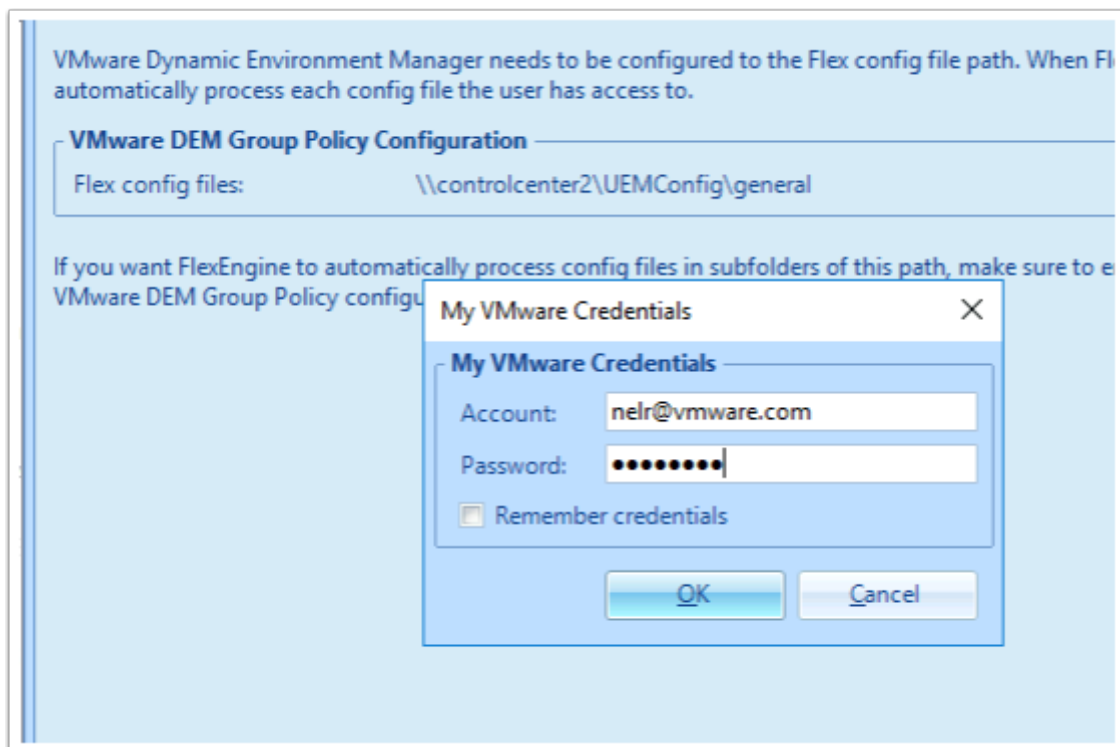
We will now see how we can manage application settings using Dynamic Environment Manager. We can also manage shortcuts for applications using Dynamic Environment Manager



1. On your **ControlCenter2** server
  - On the windows **Start Menu** navigate to **VMware DEM** folder
  - Launch the **Management Console** shortcut

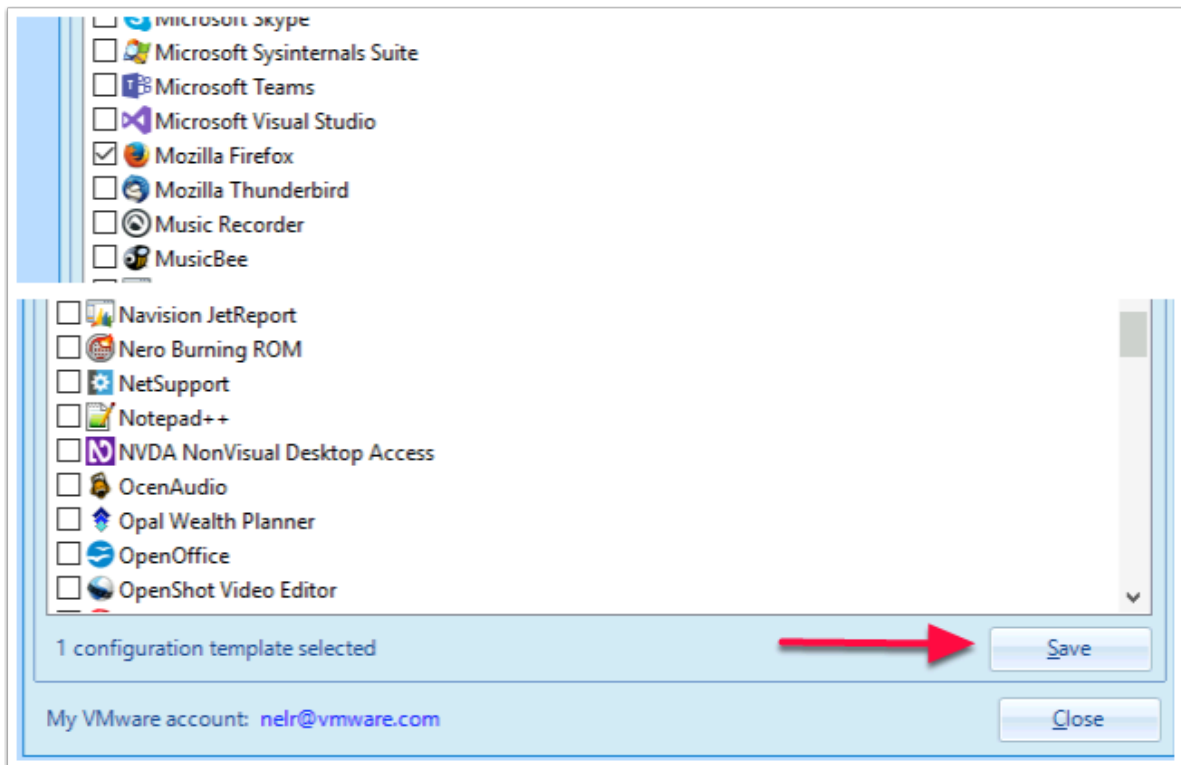


2. Select the **Personalization** tab
  - In the Inventory, under **General**, select **Applications**
  - In the **menu bar** select the **Download Config Template File**

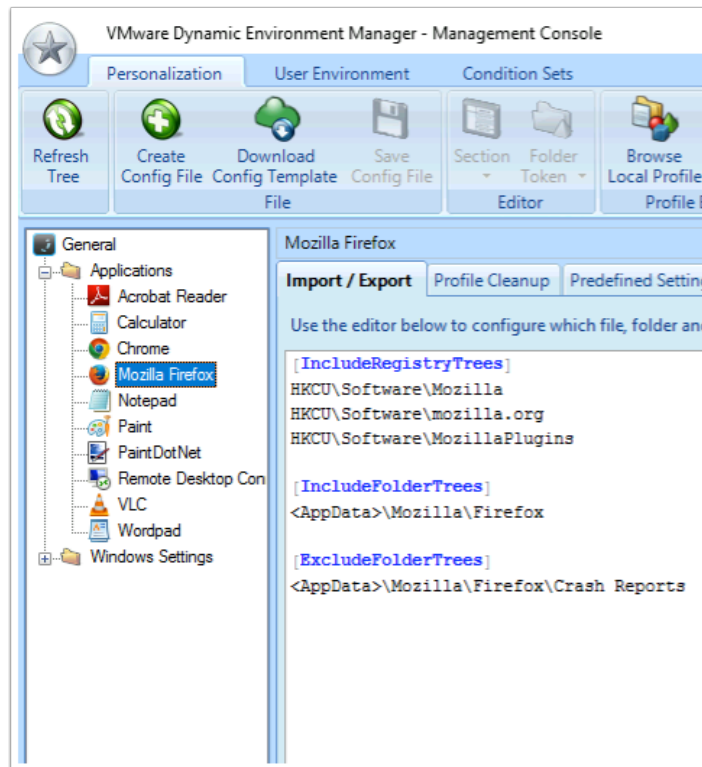


3. In the **My VMware Credentials** you'll need **MYVMware** account details, If you dont have your own credential contact your instructor.

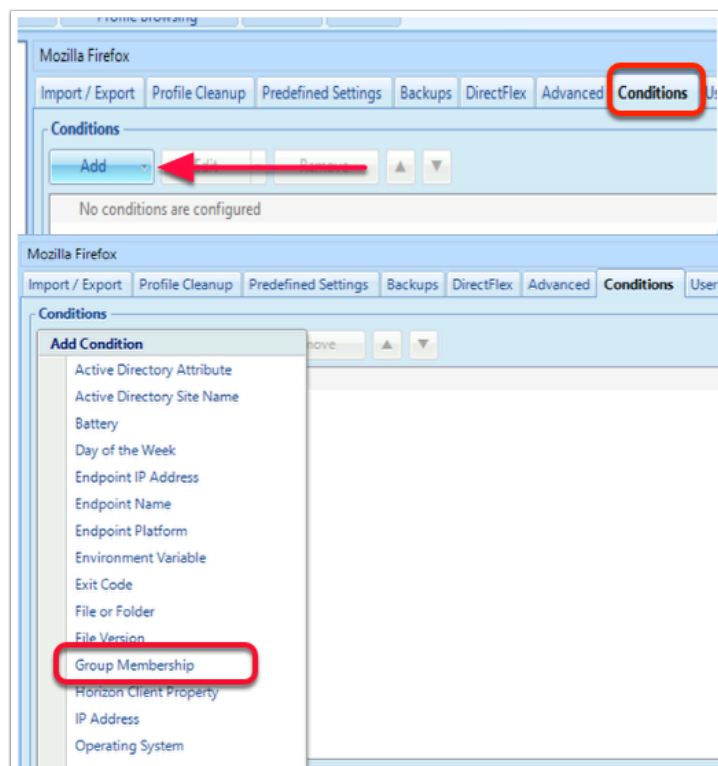
- Next to **Account** enter your **username**
- Next to **Password** enter your **password**
- Select **OK**



4. Scroll down until you get to the **Mozilla Firefox** template,
  - Select **Save**
  - Select **Close**

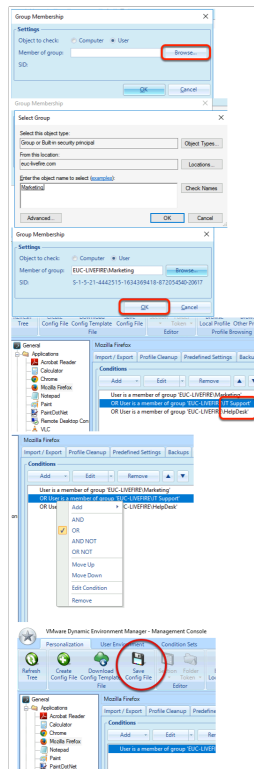


- Notice you now have a Configuration template for **Mozilla Firefox** in your Inventory.
  - Notice the **Import / Export** registry and application folder structure this application uses.



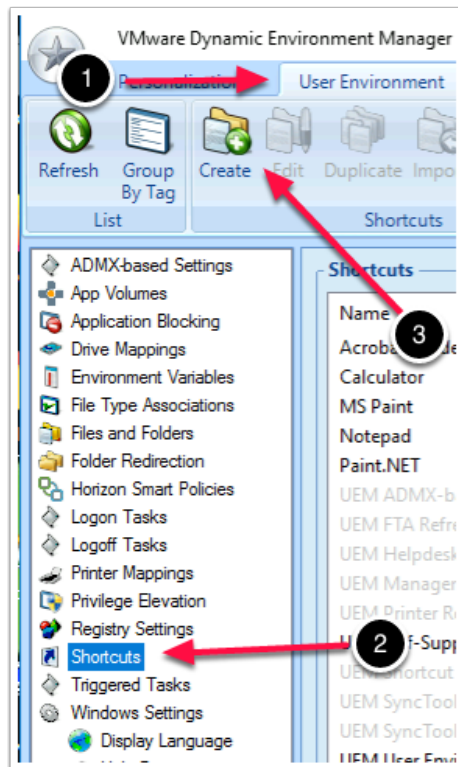
- Select the **Conditions** tab for **Mozilla Firefox**
  - Select **Add**
  - Select **Group Membership**





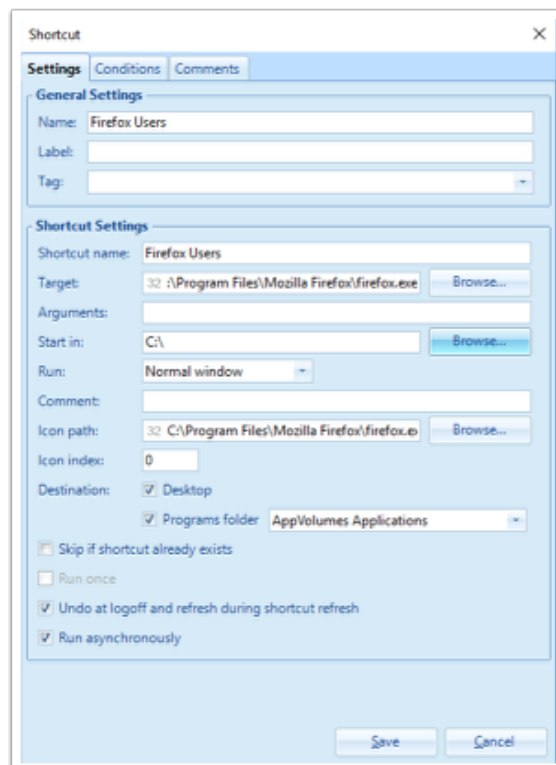
## 7. In the **Group Membership** window

- Select **Browse** and enter **Marketing** and select **Check Names** after entering one at a time, select **OK**
- Repeat the same procedure for the **HelpDesk; IT Support;** next and ensure that between your **Conditions** we change **AND** to **OR**
- Select **Save Config File**



8. Select the **User Environment** Tab

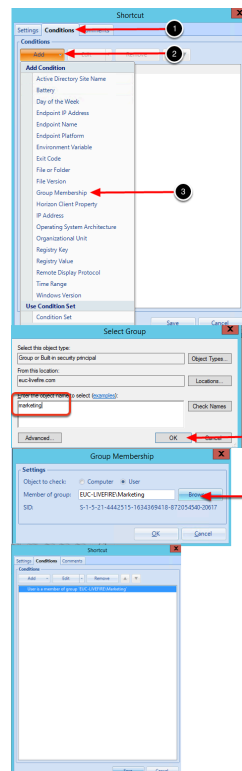
- Select **Shortcuts**,
- Select **Create** in the taskbar



9. In the **Shortcut** Window replace and fill in with the following:

- **Name:** **Firefox Users**

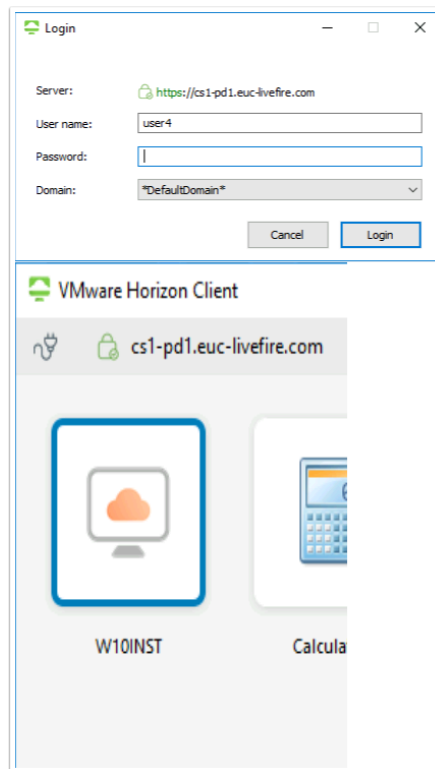
- **Shortcut name:** Firefox
- **Target:** C:\Program Files\Mozilla Firefox\firefox.exe
- **Start in:** C:\
- **Icon path:** C:\Program Files\Mozilla Firefox\firefox.exe
- Check the **checkbox** "Skip if shortcut already exists: check"
- **Icon index:** 0
- **Destination:** Check the **Desktop checkbox**,
- **Programs folder**, Type "AppVolumes Applications"
- Check the **checkbox** "Skip if shortcut already exists"
- Check the **checkbox** "Undo at logoff and refresh during shortcut refresh"
- Check the **checkbox** "Run asynchronously"



#### 10. In the **Shortcut** Window

- Select the **Conditions Tab**,
- Select **Add**, select **Group Membership**,
- In the **Group Membership** interface
  - Select **Browse**, type **Marketing**, in the object name to select,
  - Select **Check Names** and select **Ok**
- Select **Save**

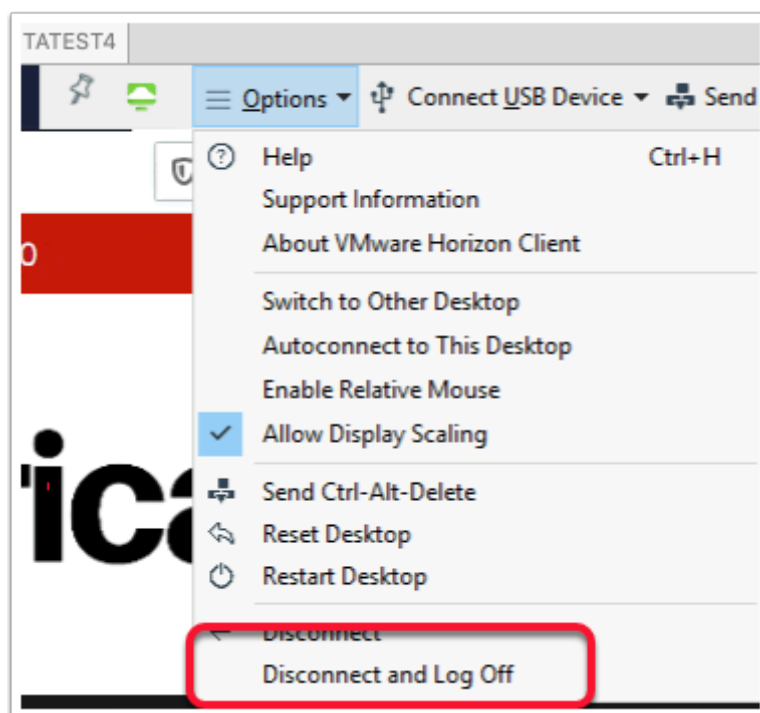
## Part 3: Testing Dynamic Environment Manager with App Volumes in a Horizon Desktop Session



1. On your **ControlCenter2** server Desktop
  - Launch your **Horizon client** shortcut,
  - Select your **CS1-PD1.euc-livewire.com** Horizon URL
  - In the **Login** window
    - Next to **User Name** enter **user4**
    - Next to **Password** enter **VMware1!**
    - Select **Login**
    - Select the **W10INST** desktop entitlement



- in the **Home** section, next to **Homepage and new windows** select **Custom URLs...** and in the box below type in a custom site like [www.iafrica.com](http://www.iafrica.com)
- Next to **New tabs** select **Firefox Home (Default)**
- Select the General section, scroll to the bottom and next to Network Settings select **Settings**, change the Proxy configuration to **No Proxy**
- Select **OK**
- Select **Home**



2. Ensure you **logoff** from your Horizon desktop session.

We will be testing the Dynamic Environment Manager to see if the Chrome configuration settings are exported at logoff .

We are using Instant clones in our lab environment. The instant clone pool has been configured to log off the session immediately. When the session logs off, the virtual desktop is deleted. That way we are guaranteed to get a fresh virtual desktop everytime we login

- From your ControlCenter2 Desktop, using your Horizon client, login as [euc-livewire\User4](#) with password **VMware1!** select the **W10-INST** pool
3. When you re-login you will notice your Mozilla Firefox settings do not work. We will have an interactive session on Day 3 and we will look at Dynamic Environment Manager Troubleshooting.
- We will use this as a base example and exercise to troubleshoot later in the course.
  - Having a base understanding of concepts in troubleshooting will ensure you are successful in getting Mozilla Firefox settings to work.

## Conclusion

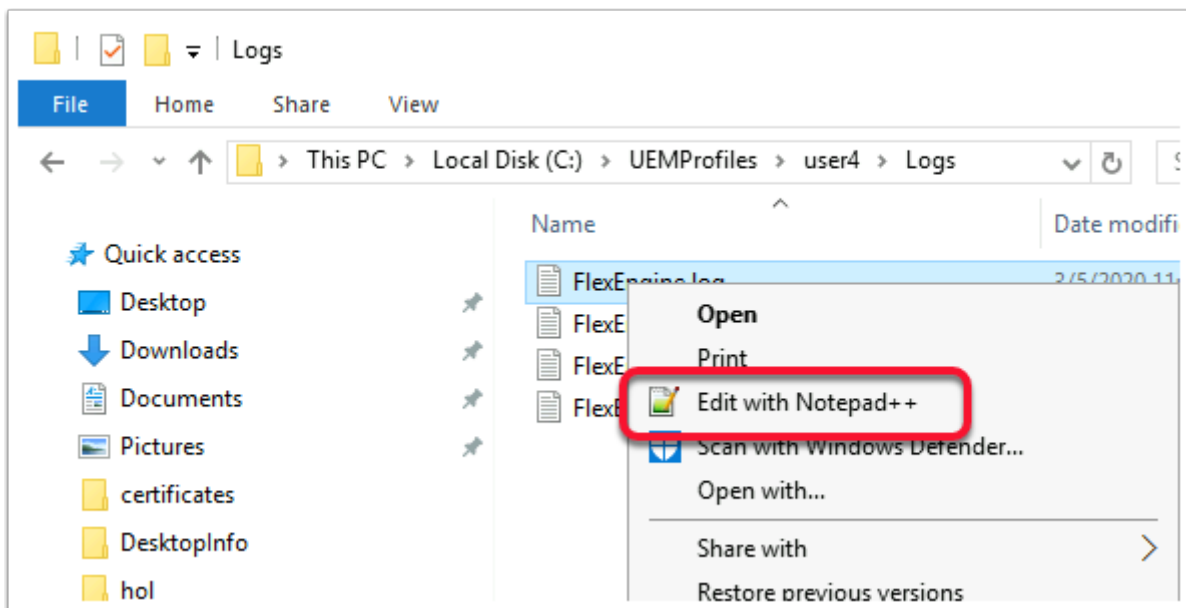
This concludes this section of the VMware Horizon, App Volumes, Dynamic Environment Manager integrations. We will now look at troubleshooting and fixing the issue with regard to Dynamic Environment Manager and take it as an opportunity to understand How Dynamic Environment Manager Logging works

# Troubleshooting an App Volumes App Stack deployment with Mozilla Firefox

## Part 1 : Troubleshooting the issue

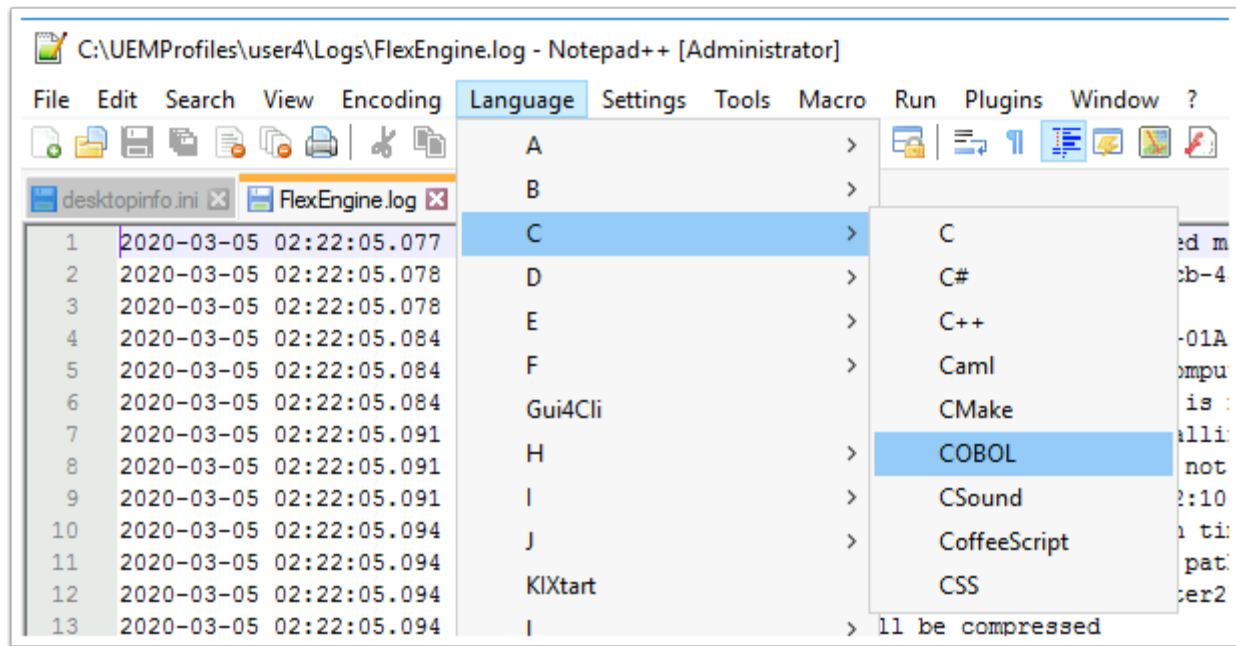
### Opening your logs

As part of the process we need to establish where the problem is. It could be a problem with Dynamic Environment Manager configuration, or it could be a problem specific to this application configuration. We need to isolate the issue. It is helpful if you have worked in the organization and you know where Dynamic Environment Manager is at. But if you were called into an organization and you were not involved in the setup yourself. You would need to validate everything. The challenge is, in many cases the symptoms are the same. The configurations do not work. Therefore isolating the issue is important.



1. Open **File Explorer**. Go to the **C:** Drive of your **ControlCenter2** server and open the **UEMProfiles** folder
  - Open **user4 > Logs**
  - Select **FlexEngine.log**, right-click and select **Edit with Notepad++**
  - If you get prompted to **update Notepad++** select **No**



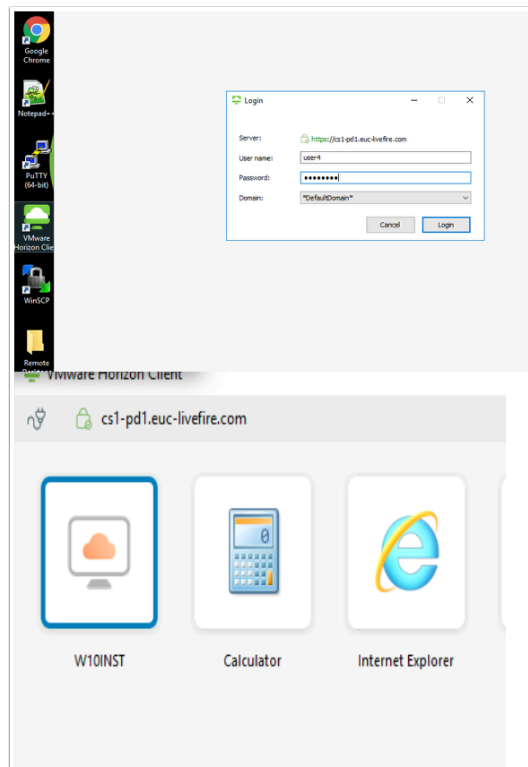


2. When using **Notepad++**, it might be helpful to colour code your settings. If this something you want to do, perform the following steps
- Select **Language** in the menu bar,
  - Select **C > COBOL**
  - **Scroll down** to the bottom of **Notepad++**

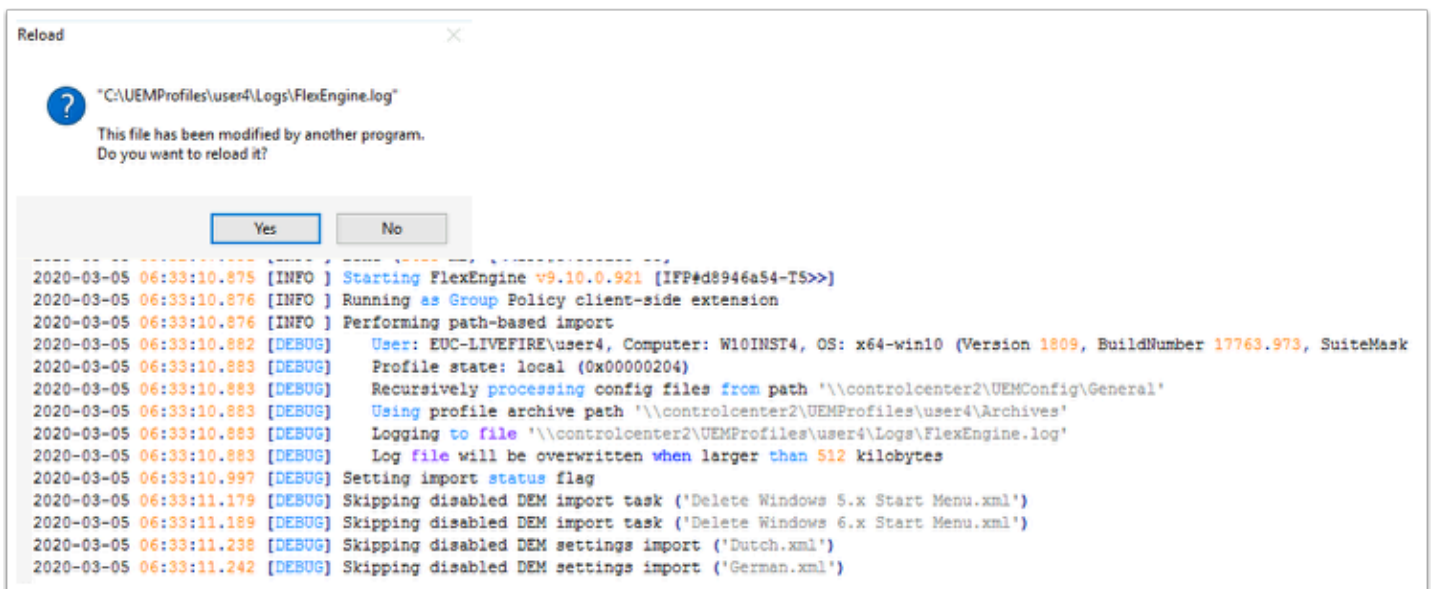
## Part 2: Isolating the issue

### Isolating the issue

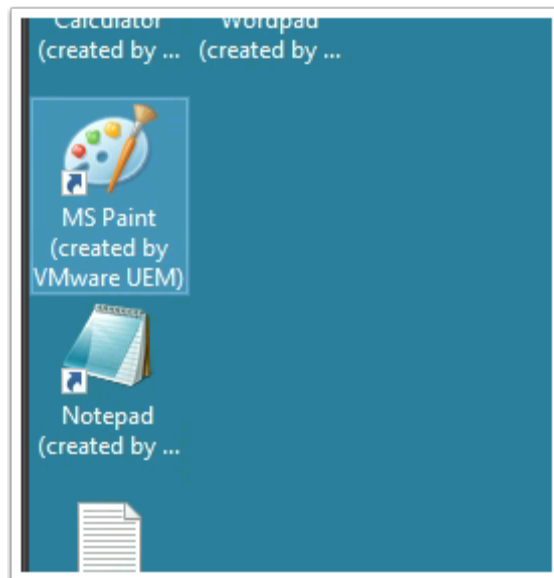
We will follow a methodical approach to isolating the issue. We will observe the FlexEngine logs to identify the source of the issue.



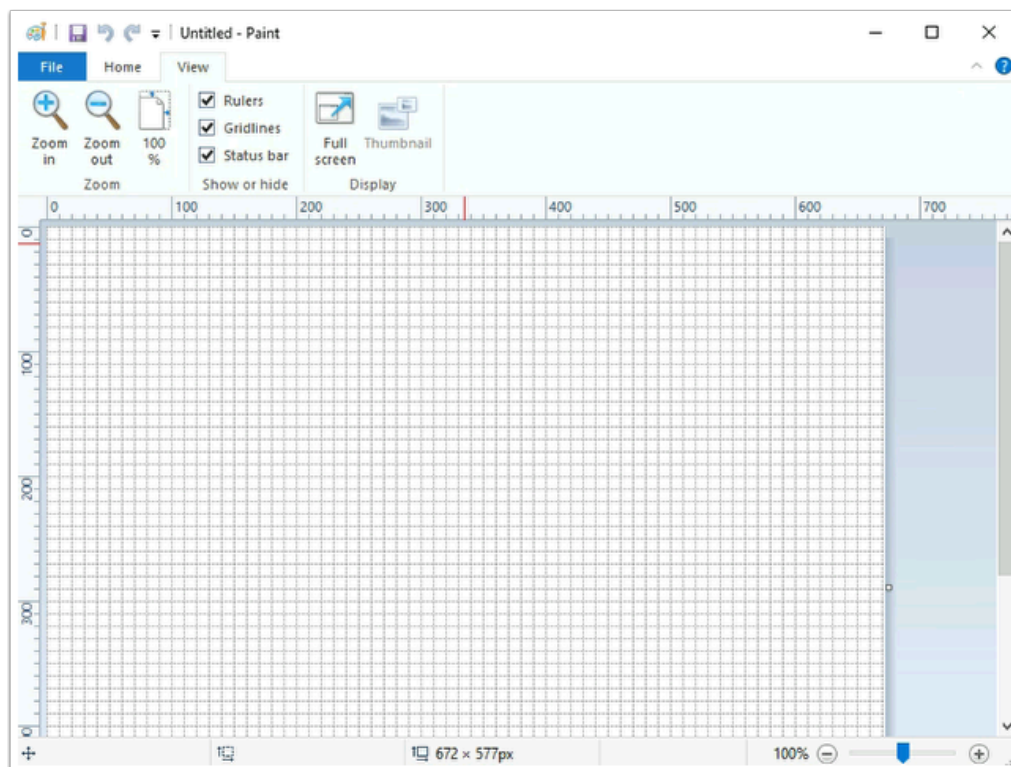
1. Re-login to your **Horizon Client**
  - As **User4** with the password **VMware1!**
  - Select the **W10INST** desktop entitlement



2. On your **ControlCenter2** server, switch back to your logs and notice you have to accept a **Reload**, select **Yes**
  - Scroll right down and notice you have a path-based import that has occurred of Windows settings and many other configurations at logon.
  - Scroll down till the end of the Log



3. To validate that all logs are captured properly, we need to complete a full logon and logoff cycle. Between the logon and logoff we would open and close applications to generate IMPORT and EXPORT requests from the FlexEngine. We can also leverage the DirectFlex feature in Dynamic Environment Manager.
  - On the Desktop launch the **MS Paint** shortcut



4. In MS Paint select the **View** tab
  - Enable **Rulers**, **Gridlines** and **Status bar** checkboxes
  - Close the application
  - Re-Open the application

```

2020-03-05 12:12:19.743 [INFO] Performing DirectFlex import for config file '\\controlcenter2\UEMConfig\General\Applications\Paint.INI' [IFF#
2020-03-05 12:12:19.747 [DEBUG] User: EUC-LIVEFIRE\user4, Computer: W10INST1, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask
2020-03-05 12:12:19.747 [DEBUG] Using profile archive '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip'
2020-03-05 12:12:19.747 [DEBUG] Triggered by 'C:\Windows\System32\mspaint.exe'
2020-03-05 12:12:19.786 [INFO] Importing profile archive 'Paint.zip' (\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip)
2020-03-05 12:12:19.793 [DEBUG] ImportRegistry::Import: Calling '"C:\Windows\REGEDIT.EXE" /S "C:\Users\user4\AppData\Local\Temp\FLX271B.tmp"' (
2020-03-05 12:12:19.995 [DEBUG] Read 1 entry from profile archive (size: 4500; compressed: 935; took 205 ms)
2020-03-05 12:12:20.000 [INFO] Completed DirectFlex import (257 ms) [<<IFF#ac7dee3b-f2ec9d]
2020-03-05 12:13:10.560 [INFO] Performing DirectFlex export for config file '\\controlcenter2\UEMConfig\General\Applications\Paint.INI' [IFF#
2020-03-05 12:13:10.563 [DEBUG] User: EUC-LIVEFIRE\user4, Computer: W10INST1, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask
2020-03-05 12:13:10.563 [DEBUG] Using profile archive '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip'
2020-03-05 12:13:10.563 [DEBUG] Triggered by 'C:\Windows\System32\mspaint.exe'
2020-03-05 12:13:10.579 [INFO] Exporting profile using config file 'Paint.INI' (\\controlcenter2\UEMConfig\General\Applications\Paint.INI)
2020-03-05 12:13:10.579 [INFO] Binary Settings: Applied Application Template 'Microsoft Paint'
2020-03-05 12:13:10.585 [INFO] Exporting Registry information
2020-03-05 12:13:10.585 [DEBUG] ExportRegistry: Exporting tree 'HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Paint'
2020-03-05 12:13:10.589 [INFO] Exported Registry information successfully
2020-03-05 12:13:10.602 [DEBUG] Stored 1 entry in profile archive (size: 4500; compressed: 928)
2020-03-05 12:13:10.605 [DEBUG] Backing up '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip' to '\\controlcenter2\UEMProfile
2020-03-05 12:13:10.627 [INFO] Completed DirectFlex export (67 ms) [<<IFF#8b0ef97-f2ec9d]

```

## 5. On Notepad++

- Look for a DEBUG log with an outdent starting with User: EUC-LIVEFIRE\user4
- Notice the DEBUG log has user information, Computer and build information
- Notice an Import occurs of the Profile archive
- Also take note where it says its a DirectFlex import

```

2020-03-05 12:12:19.743 [INFO] Performing DirectFlex import for config file '\\controlcenter2\UEMConfig\General\Applications\Paint.INI' [IFF#
2020-03-05 12:12:19.747 [DEBUG] User: EUC-LIVEFIRE\user4, Computer: W10INST1, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask
2020-03-05 12:12:19.747 [DEBUG] Using profile archive '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip'
2020-03-05 12:12:19.747 [DEBUG] Triggered by 'C:\Windows\System32\mspaint.exe'
2020-03-05 12:12:19.786 [INFO] Importing profile archive 'Paint.zip' (\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip)
2020-03-05 12:12:19.995 [DEBUG] Read 1 entry from profile archive (size: 4500; compressed: 935; took 205 ms)
2020-03-05 12:12:20.000 [INFO] Completed DirectFlex import (257 ms) [<<IFF#ac7dee3b-f2ec9d]
2020-03-05 12:13:10.560 [INFO] Performing DirectFlex export for config file '\\controlcenter2\UEMConfig\General\Applications\Paint.INI' [IFF#
2020-03-05 12:13:10.563 [DEBUG] User: EUC-LIVEFIRE\user4, Computer: W10INST1, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask
2020-03-05 12:13:10.563 [DEBUG] Using profile archive '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip'
2020-03-05 12:13:10.563 [DEBUG] Triggered by 'C:\Windows\System32\mspaint.exe'
2020-03-05 12:13:10.579 [INFO] Exporting profile using config file 'Paint.INI' (\\controlcenter2\UEMConfig\General\Applications\Paint.INI)
2020-03-05 12:13:10.579 [INFO] Binary Settings: Applied Application Template 'Microsoft Paint'
2020-03-05 12:13:10.585 [INFO] Exporting Registry information
2020-03-05 12:13:10.585 [DEBUG] ExportRegistry: Exporting tree 'HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Paint'
2020-03-05 12:13:10.589 [INFO] Exported Registry information successfully
2020-03-05 12:13:10.602 [DEBUG] Stored 1 entry in profile archive (size: 4500; compressed: 928)
2020-03-05 12:13:10.605 [DEBUG] Backing up '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Paint.zip' to '\\controlcenter2\UEMProfile

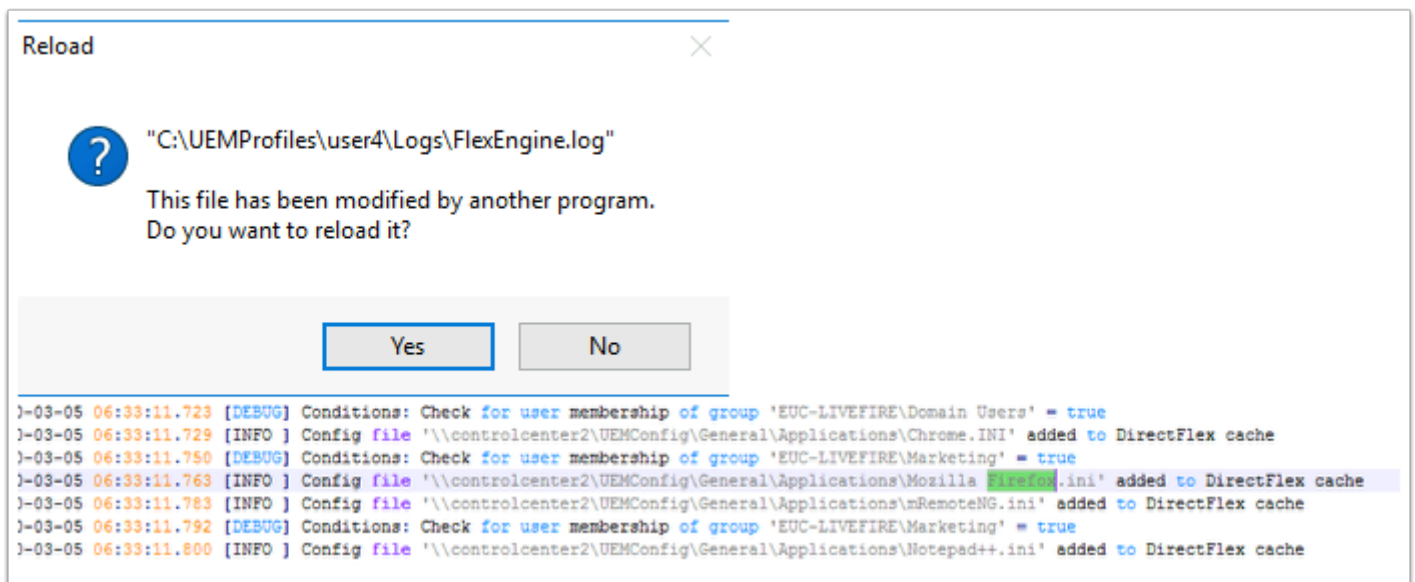
```

## 6. On Notepad++

- Notice a bit later an **Export** process is triggered and the **User** and **Computer** information is logged
- We can also see that a DirectFlex export was triggered in the INFO logs

## 7. In your Horizon client session

- **Open** MSPaint again. Do you notice your settings have been saved? **Close** your **MSPaint** session again
  - What we are seeing here is the **DirectFlex** Component of **Dynamic Environment Manager** is working fine.
  - It might now be safe to conclude that the problem might be specific to the **Mozilla Firefox** configuration

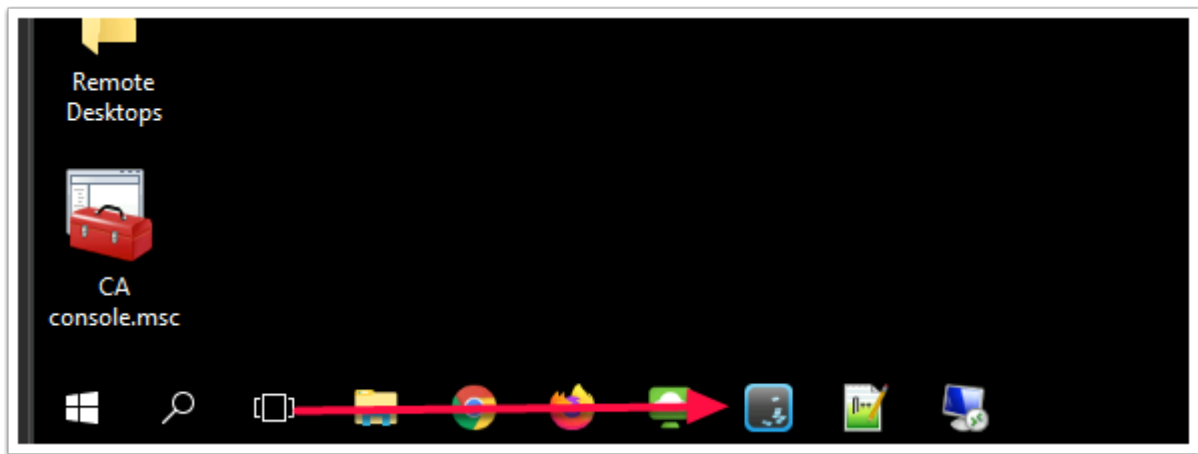


## 8. Open Mozilla Firefox.

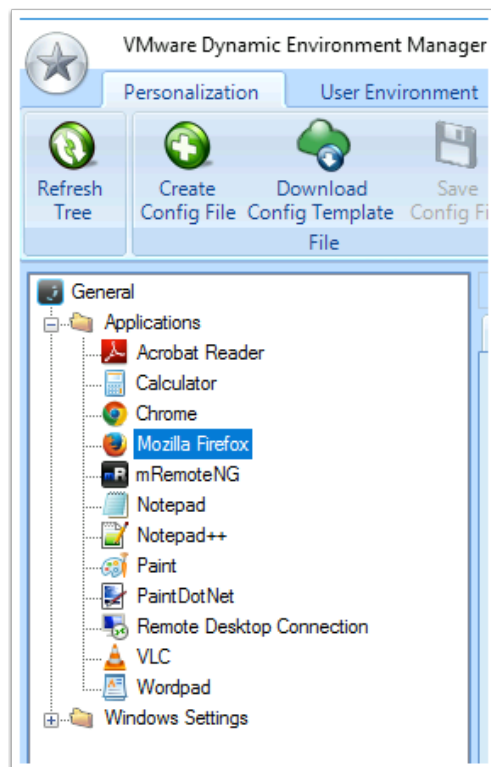
- Go to **Options** and change some configuration to trigger a potential Export. an example might set the homepage again
- **Close** Mozilla Firefox (ensure you close all tabs)
  - Did you notice any update in the LOGS, was there any export or import in the logs related to **Mozilla Firefox**?
    - The answer is no.
  - I only get a **Reload** when I open and close my **MSPaint**.
  - If we do a Firefox search upwards we will see the Mozilla Firefox shortcuts are created
    - We also Mozilla Firefox.ini is added to the DirectFlex cache
  - I do not get any logs related DirectFlex related imports or export to **Mozilla Firefox** the way I did for **Paint**



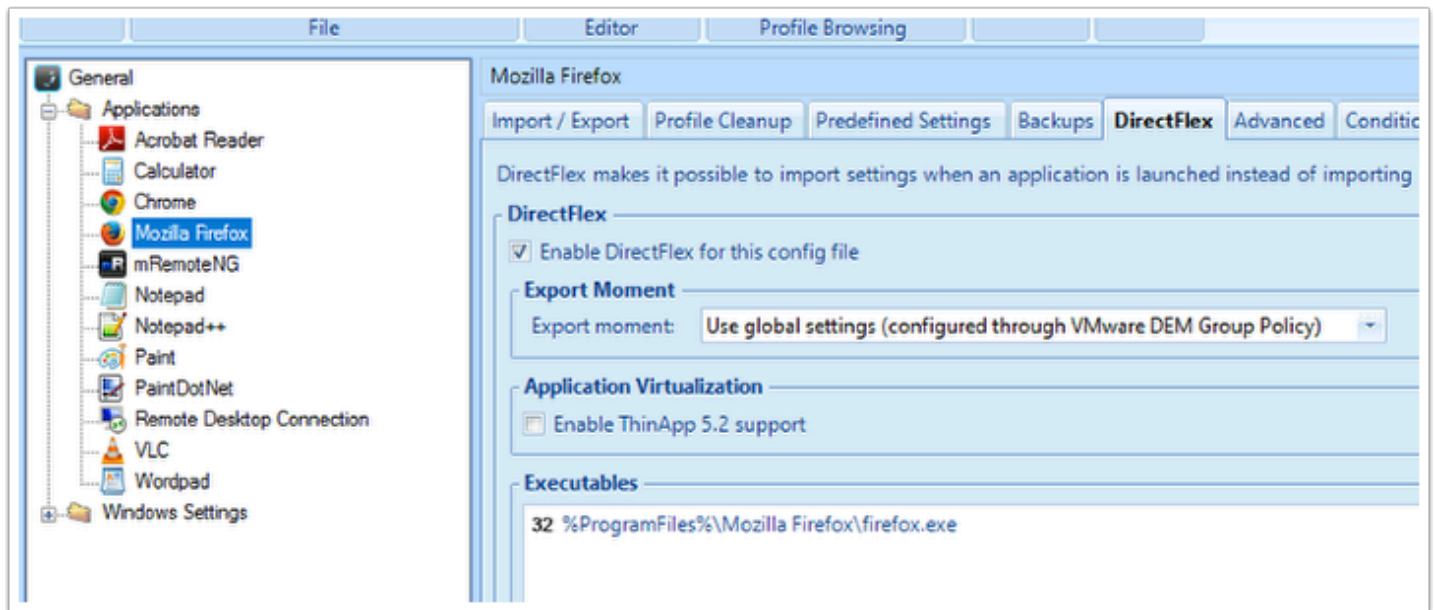




11. On the **ControlCenter2** server open your Management Console for Dynamic Environment Manager. Select the **DEM shortcut** on the Taskbar



12. Expand the **Applications** Folder and select **Mozilla Firefox**



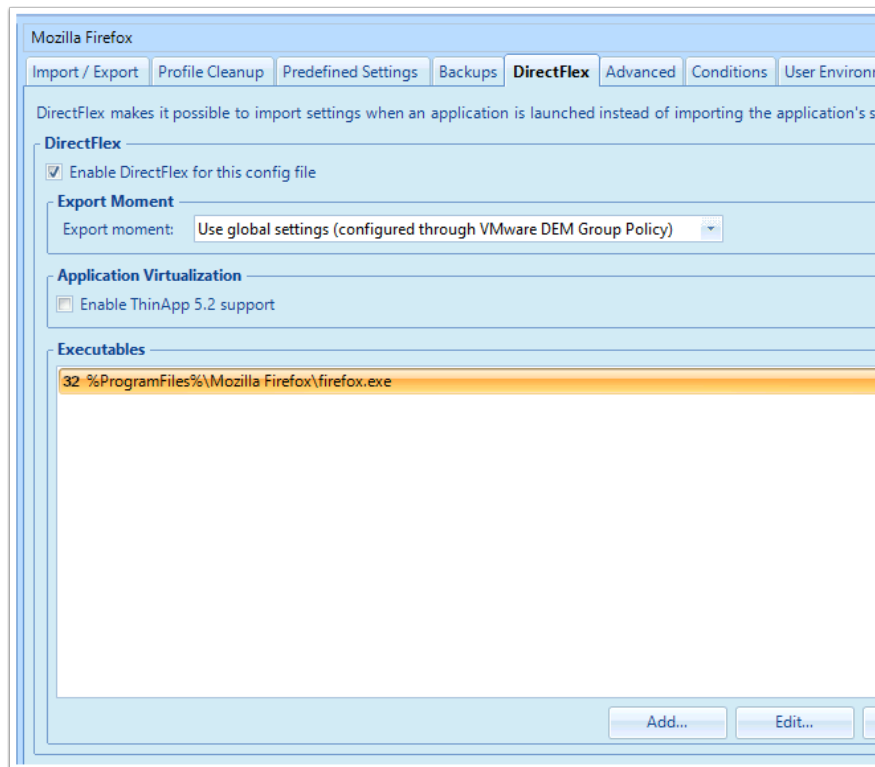
13. On the configuration of **Mozilla Firefox**, select the **DirectFlex** tab
  - Notice for the **Executables**, the path is explicitly configured
  - Switch to **Notepad** and **Notepad++**. Look at **Acrobat Reader**, **VLC** and **WordPad** configurations and notice the on the **DirectFlex** path the executable is not directly configured.
  - As we mentioned previously, the origin of this template is the **VMware** website. When use **Application Profiler** and we save configuration for an application the path is also configured explicitly.

What we might want to try now, is as the other application configurations on the **DirectFlex** tab > **Executables** path is not explicitly configured. Only the executable, we might want to do this as well.

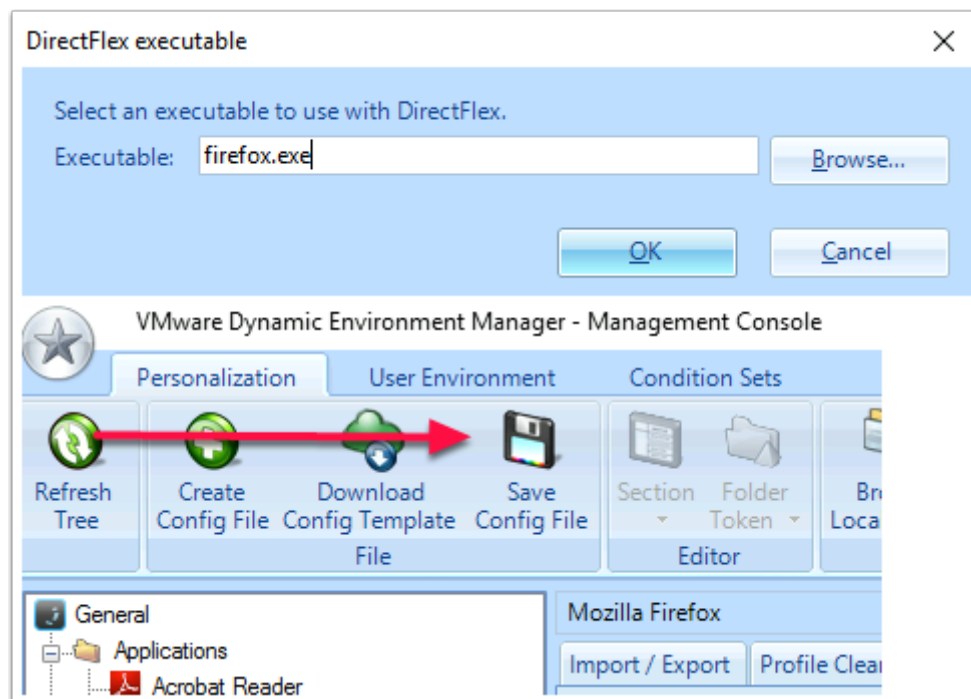
## Part 3: Finding a fix for the problem

- We will start by testing configuration changes until we get the Mozilla Firefox configuration to work.

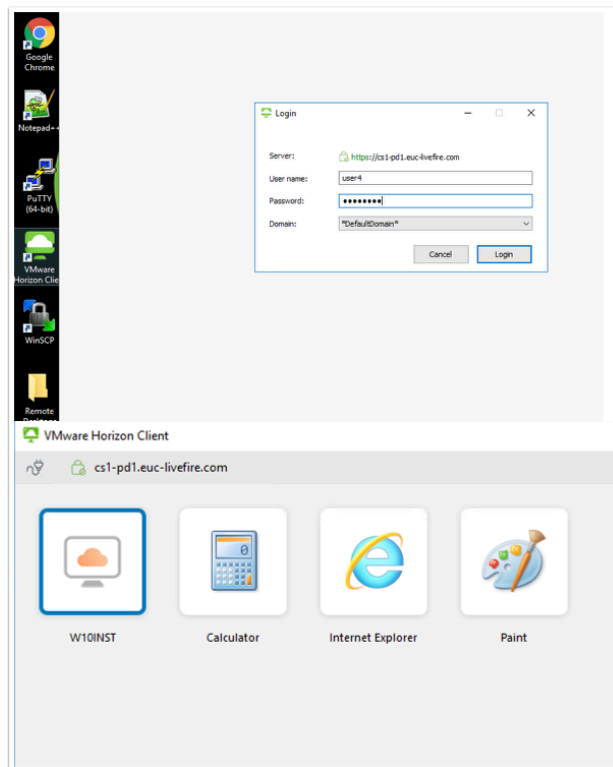




1. In the **Dynamic Environment Manager** Management Console, select **Mozilla Firefox**,
  - Select the **DirectFlex** tab , select the **explicit Path** under **Executables** and select **Edit**

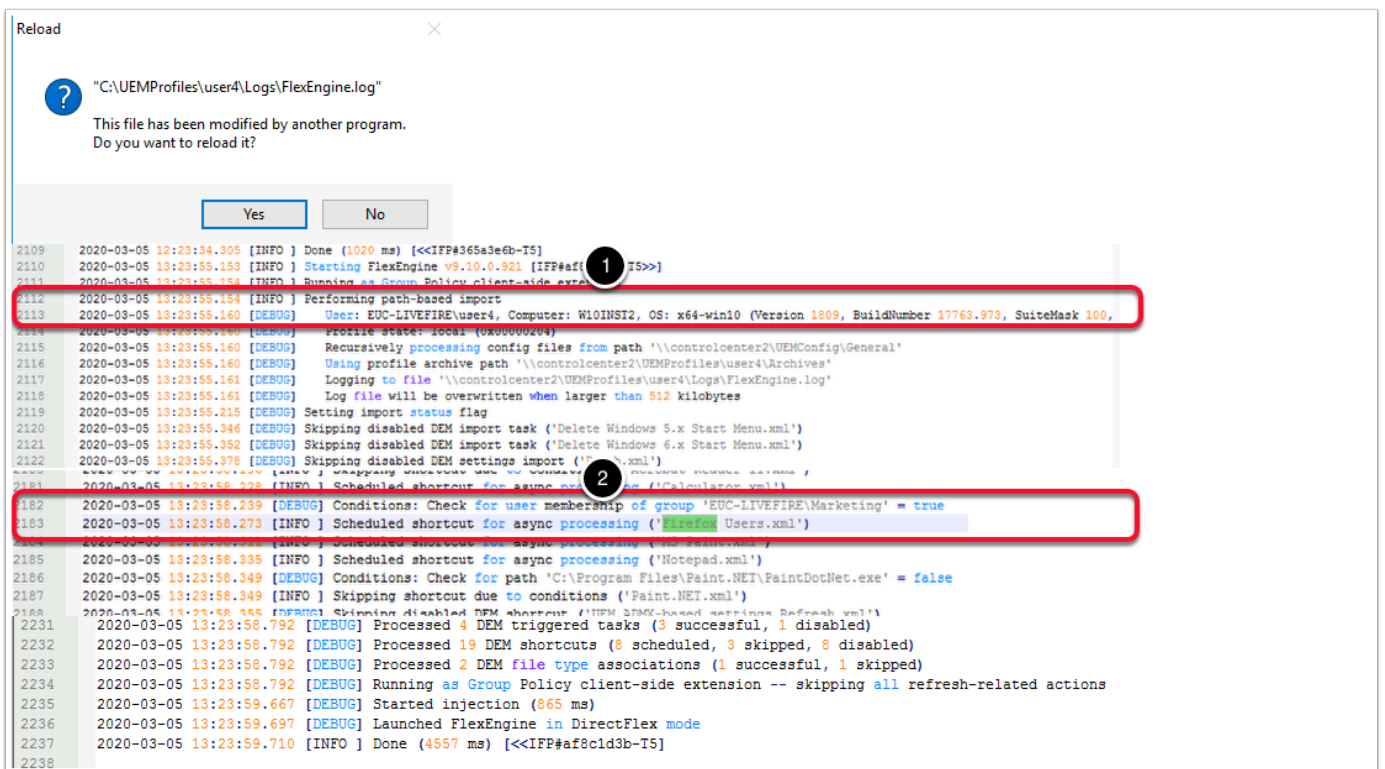


2. In the **DirectFlex executable** window next to **Executable**, **delete everything in the path** with the exception of **firefox.exe**
  - When complete select **OK**
  - In the **Taskbar** at the top of the Console select **Save Config File**



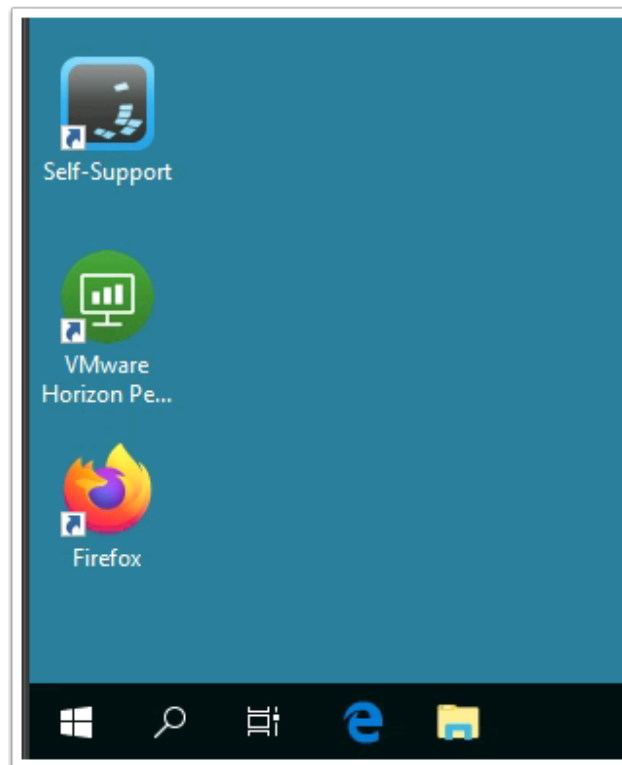
### 3. Re-login to your **Horizon Client**

- As **User4** with the password **VMware1!**
- Select the **W10INST** desktop entitlement



### 4. Revert back to your **Controlcenter2** desktop and revert back to your **Notepad++** session for User 4 FlexEngine.log

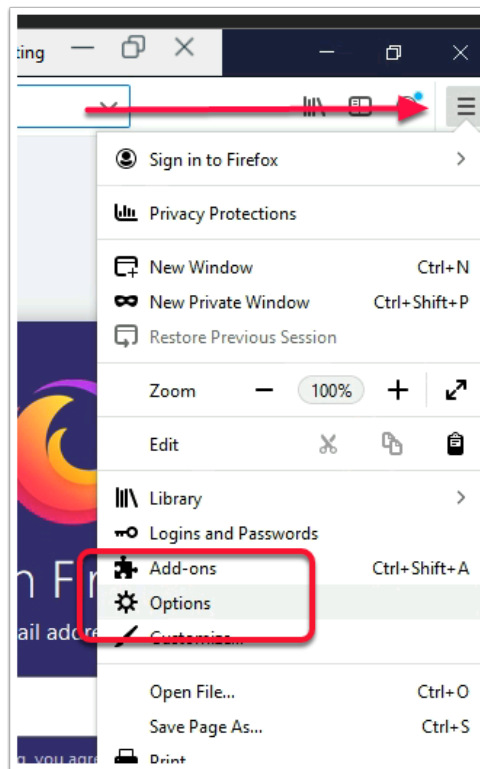
- Select **Yes**, when prompted to **Reload**
  1. Notice in your logs there is a **path-based import**
  2. Notice the **Scheduled shortcut** for Firefox is processed



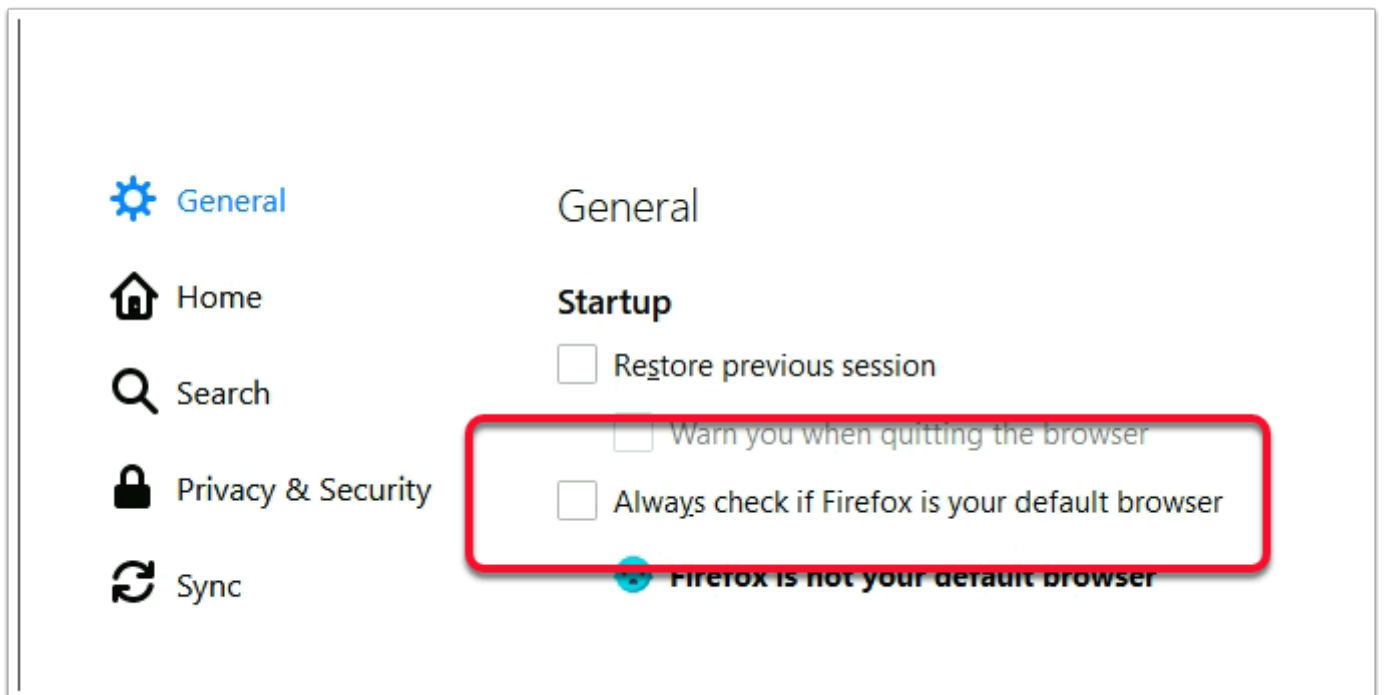
5. On the Horizon Instant Clone Desktop.
  - Launch the **Mozilla Firefox** shortcut.



6. Switch back to your **FlexEngine.log** in **Notepad++**
  - Select **Yes** to reload.
  - Notice **DirectFlex** is performing a path based import for the config file for **Mozilla Firefox.ini**



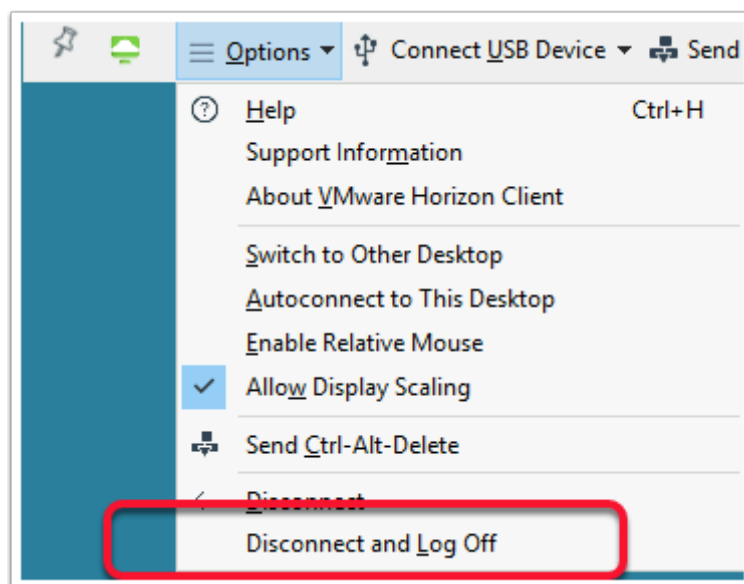
7. Select the **Open Menu** link and select **Options**



8. In the **General** area **uncheck** the **Always check if Firefox is your default browser**



9. Select **Home** and configure a **new custom URL** for example **www.news24.com**
  - Select the **Home** button. Ensure that your **new custom URL** is working
  - **Close Mozilla Firefox**



10. Switch back to your **FlexEngine.log** session with **Notepad++** on **ControlCenter2**.
  - Notice that your logs are not reloading (This is not necessarily bad. Some applications will only perform a path based export at logoff)
  - Switch back to your **Horizon Client**, **Relaunch** your **Mozilla Firefox** browser and you will see that your homepage settings are still saved.

- On an Instant Clone desktop this will need to be saved externally to save these settings

- **Disconnect and Log Off**

11. Switch back to your **FlexEngine.log** session with **Notepad++** on **ControlCenter2**.

- When prompted to **Reload**, select **Yes**
- Notice that a DirectFlex Export is being Triggered at Logoff

```

2465 2020-03-05 22:16:12.405 [INFO ] Starting FlexEngine v9.10.0.921 [IFF#26e766d9-21b67a>>]
2466 2020-03-05 22:16:12.405 [INFO ] Performing path-based export
2467 2020-03-05 22:16:12.405 [DEBUG] User: EUC-LIVEFIRE\User4, Computer: W10INST2, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask :
2468 2020-03-05 22:16:12.409 [DEBUG] Policy "Always wait for the network at computer startup and logon" is enabled
2469 2020-03-05 22:16:12.410 [DEBUG] Policy "Auto-logon scripts synchronization" is not configured
2470 2020-03-05 22:16:12.481 [DEBUG] Policy "Point and Print Restrictions" is not configured
2471 2020-03-05 22:16:12.482 [DEBUG] User policy last applied at 2020-03-05 22:07:00.816 (took 0.995 s)
2472 2020-03-05 22:16:12.488 [DEBUG] Boot time: 2020-03-05 18:05:25.671, Logon time: 2020-03-05 20:24:00.413

2674 2020-03-05 22:16:13.569 [DEBUG] Stored 1 entry in profile archive (size: 55954; compressed: 6507)
2675 2020-03-05 22:16:13.573 [DEBUG] Backing up '\\controlcenter2\UEMProfiles\user4\Archives\Windows Settings\Windows Explorer.zip' to '\\controlcenter2\UEMProfiles\user4\Archives\Windows Settings\Windows Explorer.zip'
2676 2020-03-05 22:16:13.587 [WARN ] Triggering DirectFlex export for config file 'Applications\Mozilla\Firefox\Firefox.ini' due to 11 unprocessed PIDs (<C:\SnapVolumesTemp\MountPointa\{00002760-0000-0000-0000-100000000000}\{1cb506a8-2573-40c8-b6d6-ae43795a_74_04_59-12-14_94}>)
2677 2020-03-05 22:16:13.587 [WARN ] Triggering DirectFlex export for config file 'Applications\Mozilla\Firefox\Firefox.ini' due to 11 unprocessed PIDs (<C:\SnapVolumesTemp\MountPointa\{00002760-0000-0000-0000-100000000000}\{1cb506a8-2573-40c8-b6d6-ae43795a_74_04_59-12-14_94}>)
2678 2020-03-05 22:16:13.608 [DEBUG] Triggering DirectFlex export for config file 'Applications\Mozilla\Firefox\Firefox.ini' due to 11 unprocessed PIDs (<C:\SnapVolumesTemp\MountPointa\{00002760-0000-0000-0000-100000000000}\{1cb506a8-2573-40c8-b6d6-ae43795a_74_04_59-12-14_94}>)
2679 2020-03-05 22:16:13.610 [INFO ] Performing DirectFlex export for config file '\\controlcenter2\UEMConfig\General\Applications\Mozilla\Firefox\Firefox.ini'
2680 2020-03-05 22:16:13.610 [DEBUG] User: EUC-LIVEFIRE\User4, Computer: W10INST2, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask 100,
2681 2020-03-05 22:16:13.613 [DEBUG] Using profile archive '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Mozilla\Firefox\Firefox.zip'
2682 2020-03-05 22:16:13.613 [DEBUG] Triggered by 'C:\SnapVolumesTemp\MountPointa\{00002760-0000-0000-0000-100000000000}\{1cb506a8-2573-40c8-b6d6-ae43795a_74_04_59-12-14_94}>'
2683 2020-03-05 22:16:13.619 [INFO ] Exporting profile using config file 'Mozilla\Firefox\Firefox.ini' (\\controlcenter2\UEMConfig\General\Applications\Mozilla\Firefox\Firefox.ini)
2684 2020-03-05 22:16:13.622 [INFO ] Exporting Registry information
2685 2020-03-05 22:16:13.622 [DEBUG] ExportRegistry: Exporting tree 'HKCU\Software\Mozilla'
2686 2020-03-05 22:16:13.624 [DEBUG] ExportRegistry: Exporting tree 'HKCU\Software\Mozilla.org'
2687 2020-03-05 22:16:13.624 [DEBUG] ExportRegistry:ExportKey: Key 'HKEY_CURRENT_USER\Software\mozilla.org' does not exist
2688 2020-03-05 22:16:13.624 [DEBUG] ExportRegistry: Exporting tree 'HKCU\Software\MozillaPlugins'
2689 2020-03-05 22:16:13.624 [DEBUG] ExportRegistry:ExportKey: Key 'HKEY_CURRENT_USER\Software\MozillaPlugins' does not exist
2690 2020-03-05 22:16:13.625 [INFO ] Exported Registry information successfully
2691 2020-03-05 22:16:13.625 [INFO ] Exporting file information
2692 2020-03-05 22:16:13.625 [DEBUG] ExcludeFolderTrees: Adding exclusion for '<AppData>\Mozilla\Firefox\Crash Reports'
2693 2020-03-05 22:16:13.625 [DEBUG] ExportFiles: Recursively processing folder '<AppData>\Mozilla\Firefox'
2694 2020-03-05 22:16:13.199 [INFO ] Exported file information successfully
2695 2020-03-05 22:16:15.217 [DEBUG] Stored 80 entries in profile archive (size: 28282689; compressed: 7611524)
2696 2020-03-05 22:16:15.219 [DEBUG] Backing up '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Mozilla\Firefox\Firefox.zip' to '\\controlcenter2\UEMProfiles\user4\Archives\Applications\Mozilla\Firefox\Firefox.zip'
2697 2020-03-05 22:16:15.224 [INFO ] Completed DirectFlex export (1626 ms) [<IFF#68b63a6a-21b67a>]
2698 2020-03-05 22:16:15.261 [INFO ] Performing DirectFlex export for config file '\\controlcenter2\UEMConfig\General\Windows Settings\Microsoft Edge\IE
2699 2020-03-05 22:16:15.261 [DEBUG] User: EUC-LIVEFIRE\User4, Computer: W10INST2, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask 100,
2700 2020-03-05 22:16:15.261 [DEBUG] User: EUC-LIVEFIRE\User4, Computer: W10INST2, OS: x64-win10 (Version 1809, BuildNumber 17763.973, SuiteMask 100,

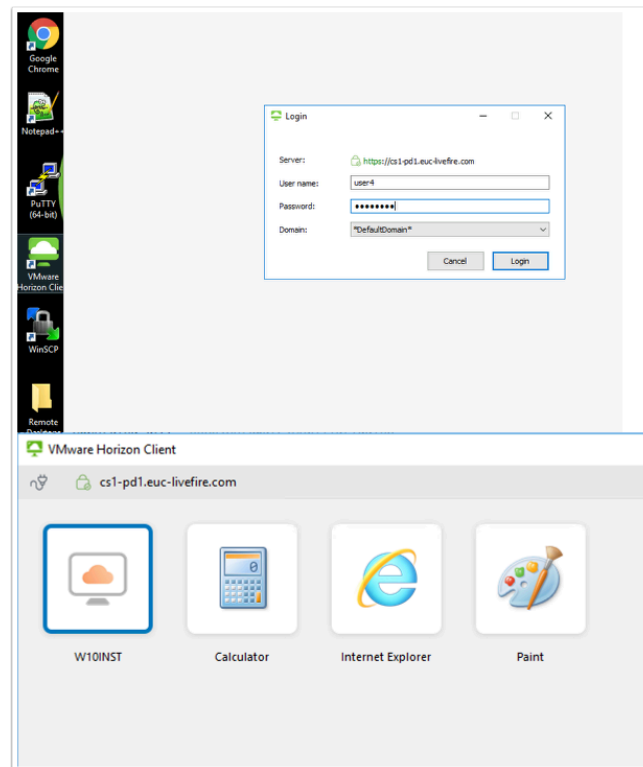
```

**i** If you configured FlexEngine to start as a Group Policy client-side extension, but you did not configure the GPO setting, **Always wait for the network at computer startup and logon**, Dynamic Environment Manager cannot run at login, or it may run every second login.

The important thing to note here from a logs perspective is in Dynamic Environment Manager, this configuration is only logged as enabled when Dynamic Environment Manager performs a path-bath export.

So when troubleshooting, perform a complete cycle of a log in and a log off. Notice Firefox configuration is now exported with directflex





12. Re-login to your **Horizon Client**
  - As **User4** with the password **VMware1!**
  - Select the **W10INST** desktop entitlement



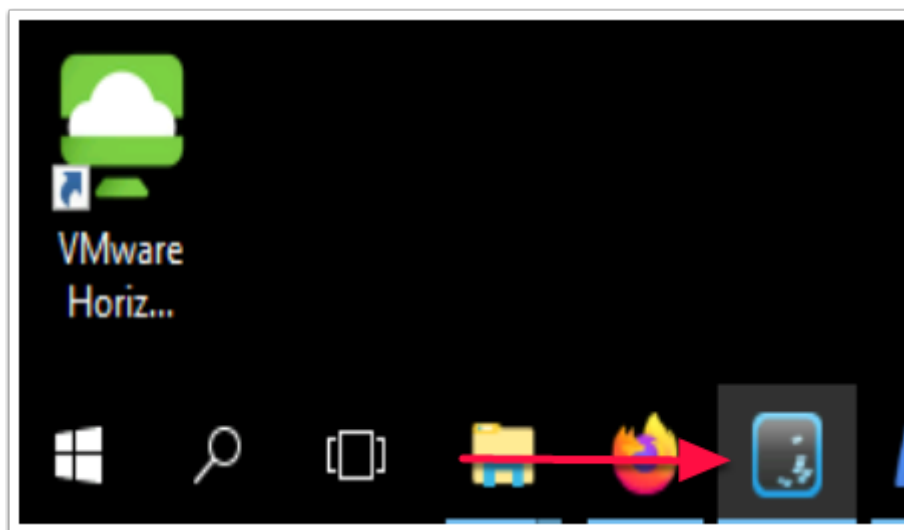
13. Open your **Mozilla Firefox Browser**. Notice your changes persisted.

# Delivering a functional user experience that is consistent with organisational policy for the remote worker

Delivering a consistent yet secure user experiencing can be very challenging in a mobile use case. The remote might sometimes work from home and again in the office. The user might be working from their hotel or out of an Airport.

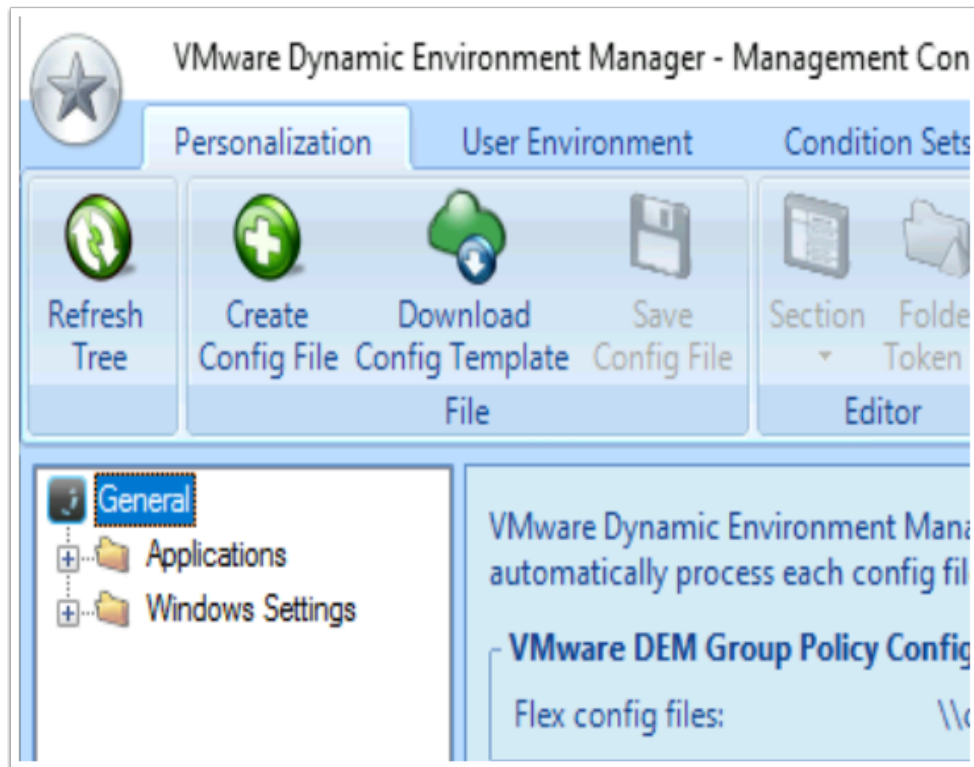
The Objective of this session is help anyone wanting to do this what configurations one would use to get started. We will use a scenario where a user connects from a remote device into their Horizon environment and would potentially be on an untrusted network, versus connecting to the same infrastructure on a trusted network

## PART 1: Setting up VMware Horizon Smart Policies with VMware Dynamic Environment Manager for Trusted Networks

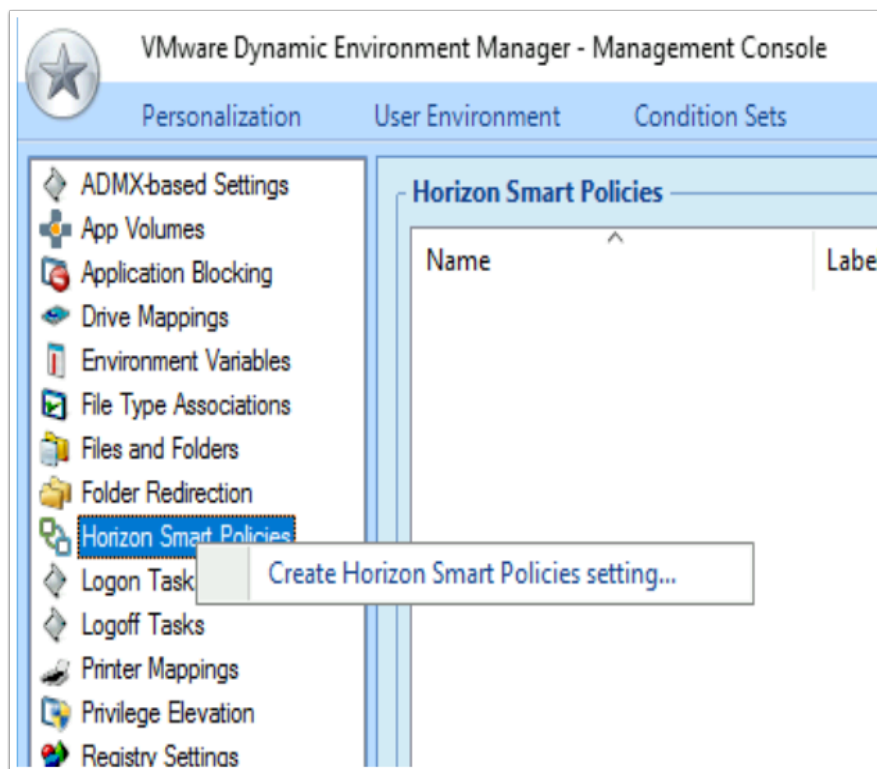


1. On your ControlCenter2 server Desktop
  - Select and Launch, the **DEM management Console** shortcut from your start menu

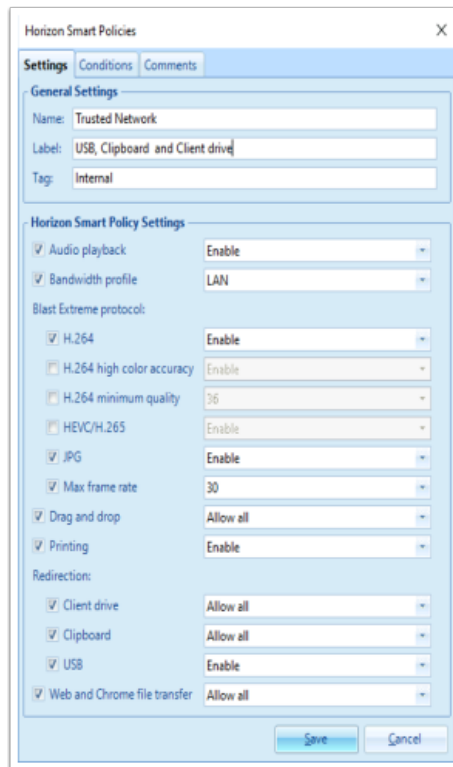




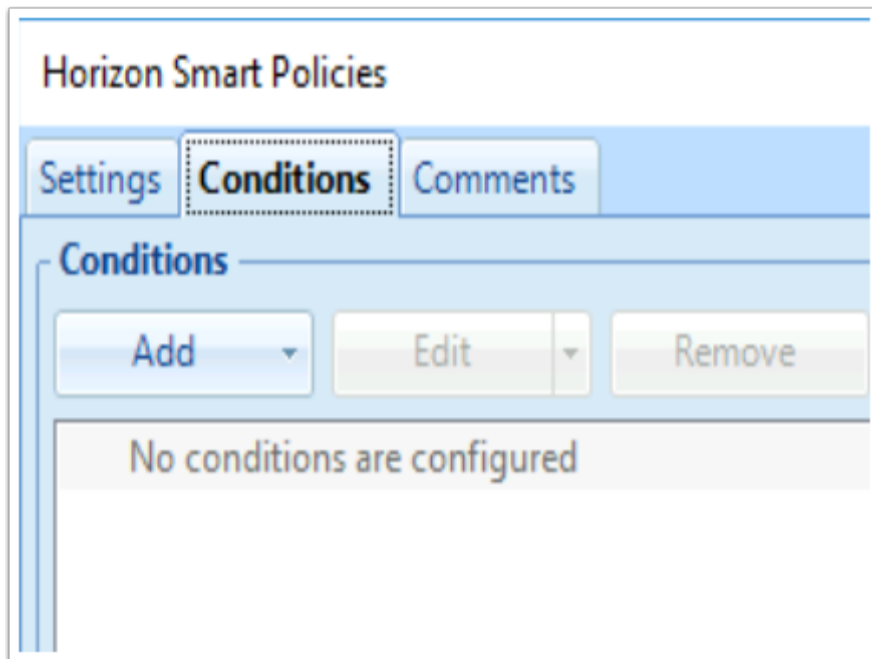
2. In the Dynamic Environment Manager Console
  - Select the **User Environment** tab



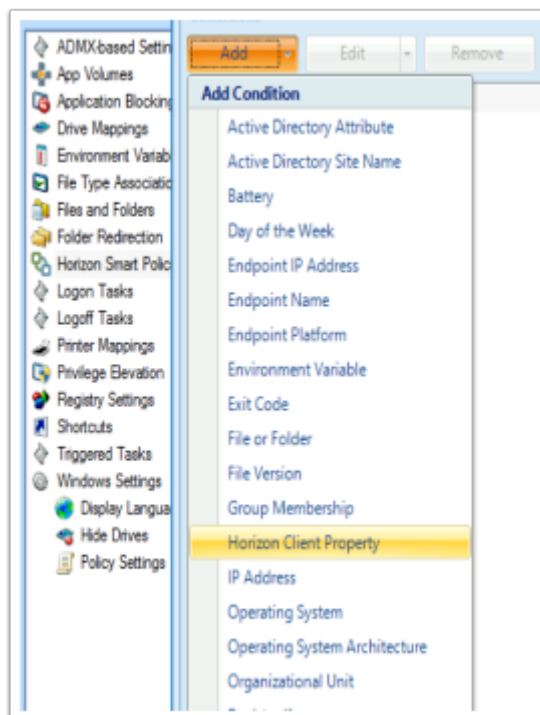
3. In the **User Environment** Inventory
  - Select **Horizon Smart Policies**, right-click and select **Create Horizon Smart Policies setting...**



4. In the **Horizon Smart Policies, Settings** tab enter the following:-
  - Under **General** Settings, enter the following, next to:
    - **Name:** **Trusted Network**
    - **Label:** **USB, Clipboard and Client drive**
    - **Tag:** **Internal**
  - In the **Horizon Smart Policy Settings**, enable the following checkboxes, next to:
    - **Audio Playback :** **Enable**
    - **Bandwidth Profile :** **LAN**
    - **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**

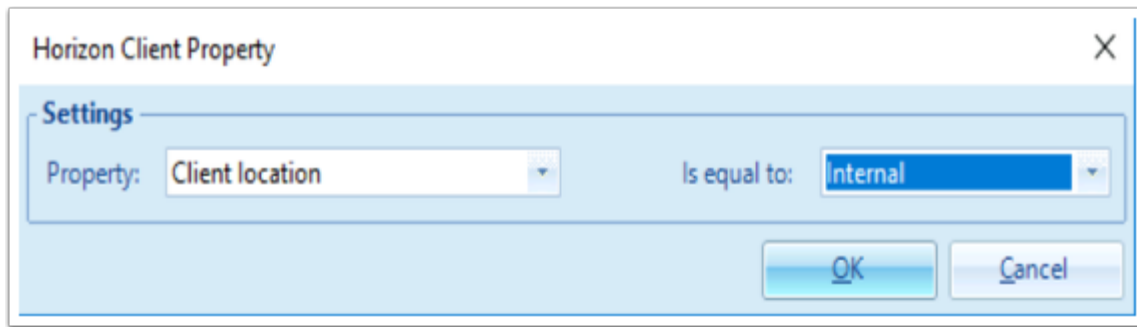


5. In the **Horizon Smart Policies** window
  - Select the **Conditions** tab
  - Under **Conditions**, select the **dropdown** next to **Add**

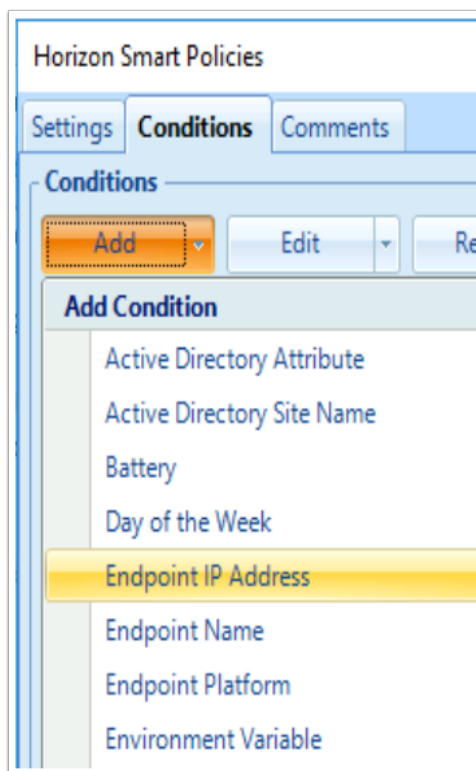


6. In the **Add Condition** dropdown
  - Select **Horizon Client Property**

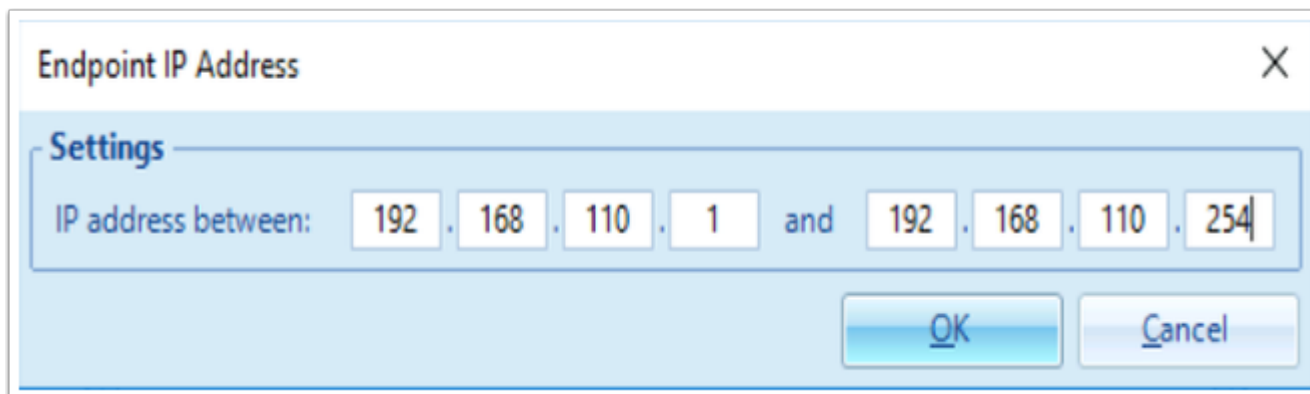
Note: By default, if you connect directly to a View Connection Server, the gateway location is Internal. If you connect to an Unified Access Gateway Server, the gateway location is External by default.



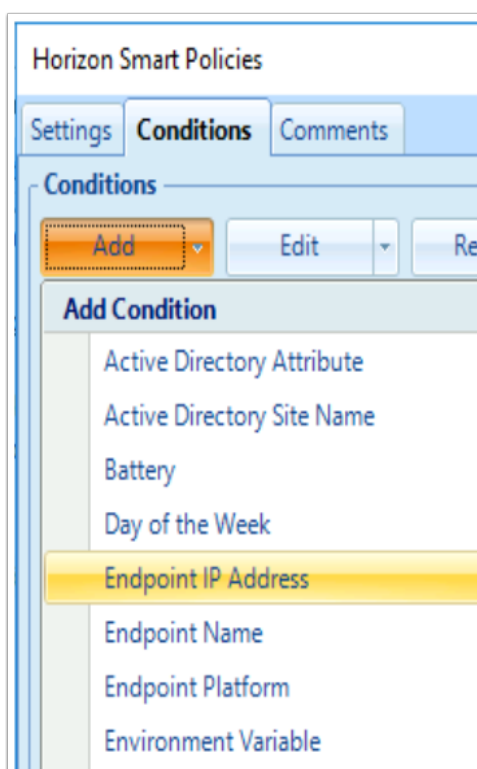
7. In the **Horizon Client Property**, add the following:
- Next to **Property**, select **Client location** from the dropdown
  - Next to **Is equal to**, select **Internal** from the dropdown
  - Select **OK**, to close the **Horizon Client Property**



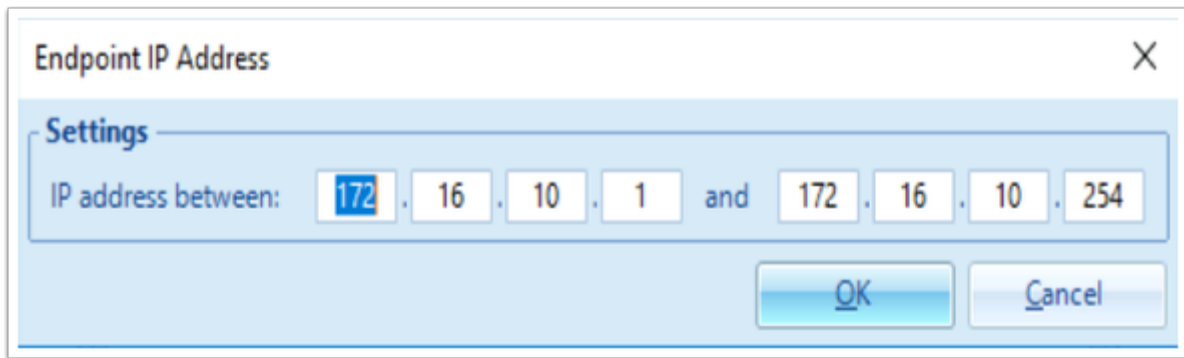
8. In the **Horizon Smart Policies** window, **Conditions** tab
- Select **Add**
  - Select **Endpoint IP Address**



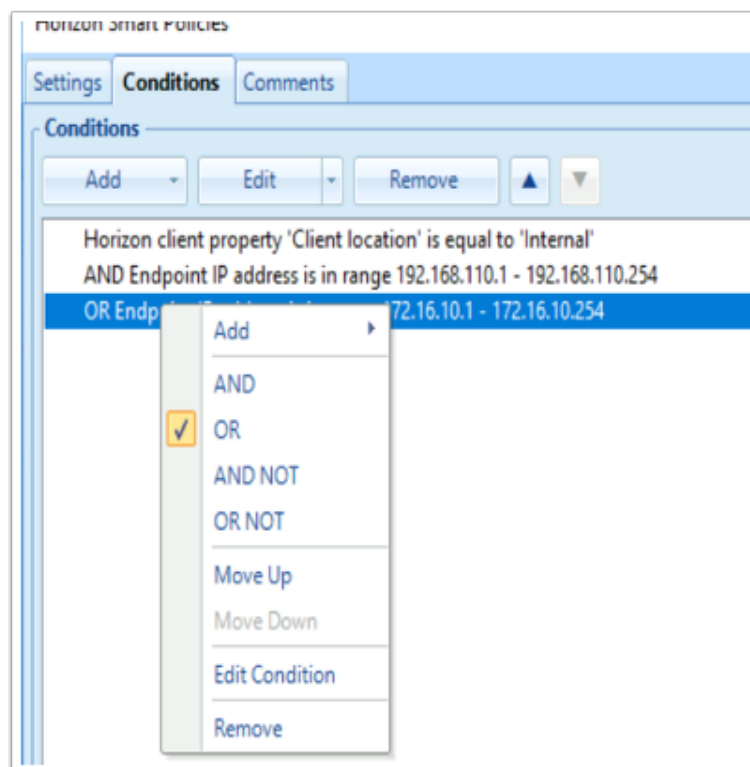
9. In the **Endpoint IP Address** window, enter the following
  - Under **Settings**, next to **IP address between:** **192.168.110.1**
    - next to **and** enter: **192.168.110.254**
  - Select **OK** to close the window



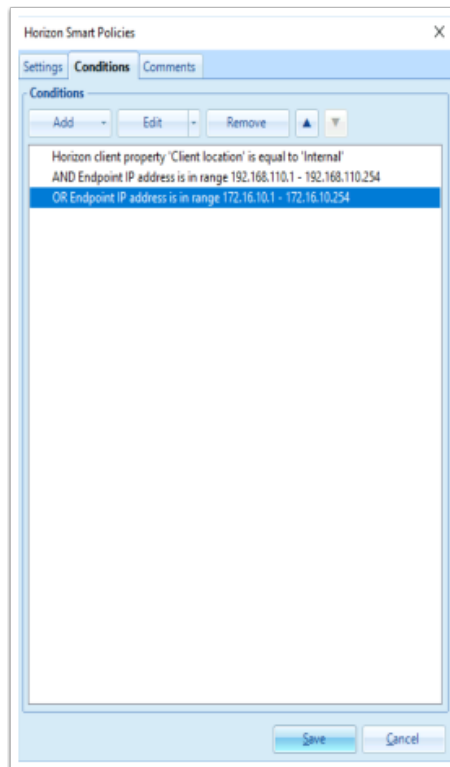
10. In the **Horizon Smart Policies** window, **Conditions** tab
  - Select **Add**
  - Select **Endpoint IP Address**



11. In the **Endpoint IP Address** window, enter the following
  - Under **Settings**, next to **IP address between:** **172.16.10.1**
    - next to **and** enter: **172.16.10.254**
  - Select **OK** to close the window

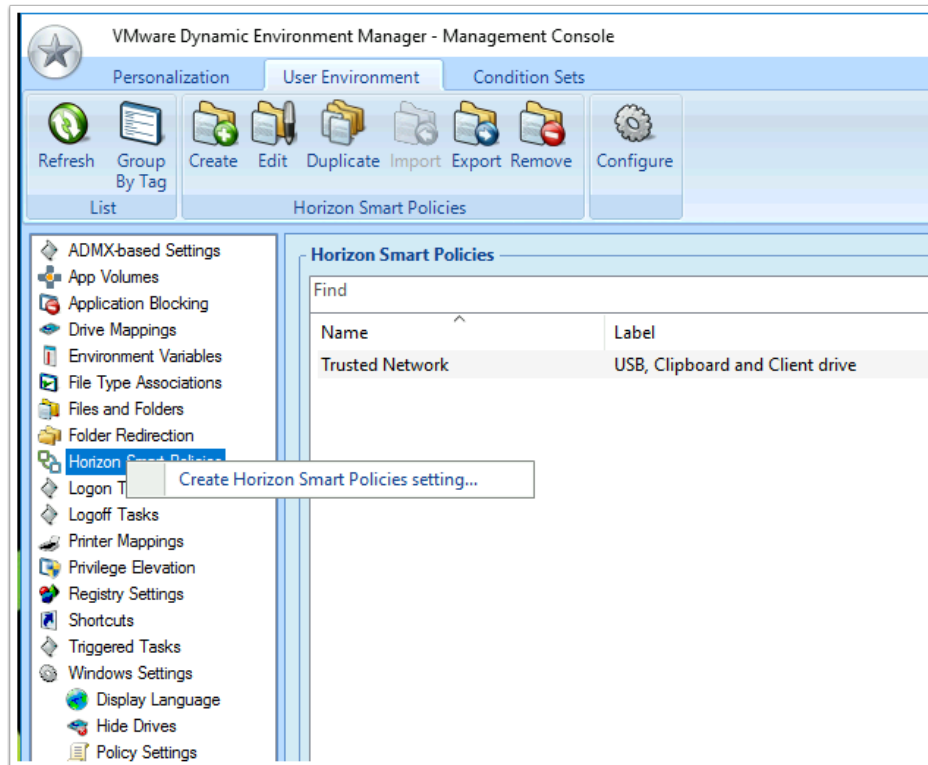


12. In the **Conditions** tab
  - Select your **last entry** and right-click and change the AND to **OR**



13. In the **Horizon Smart Policies** window
- Confirm your configuration with the Screenshot
  - Select **Save**

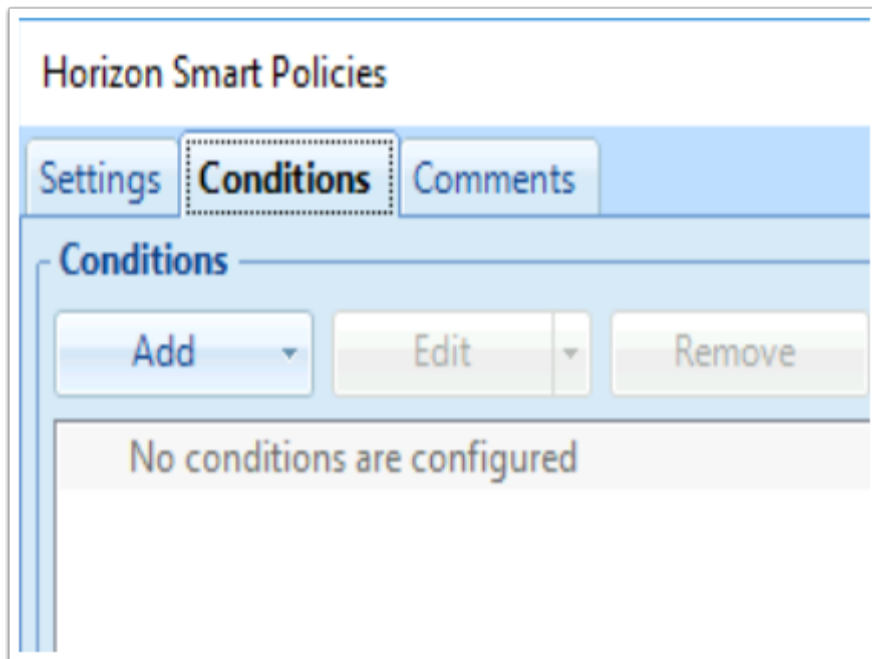
## PART 2: Setting up VMware Horizon Smart Policies with VMware Dynamic Environment Manager for Untrusted Networks



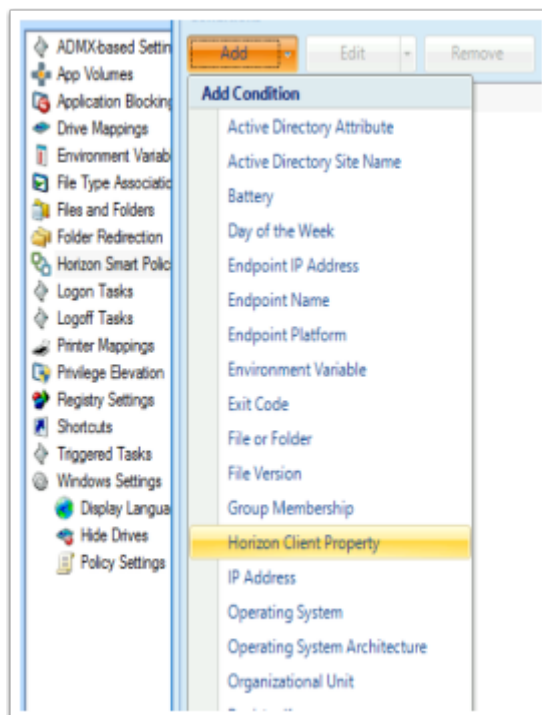
1. In the **User Environment** Inventory
  - Select **Horizon Smart Policies**, right-click and select **Create Horizon Smart Policies setting...**



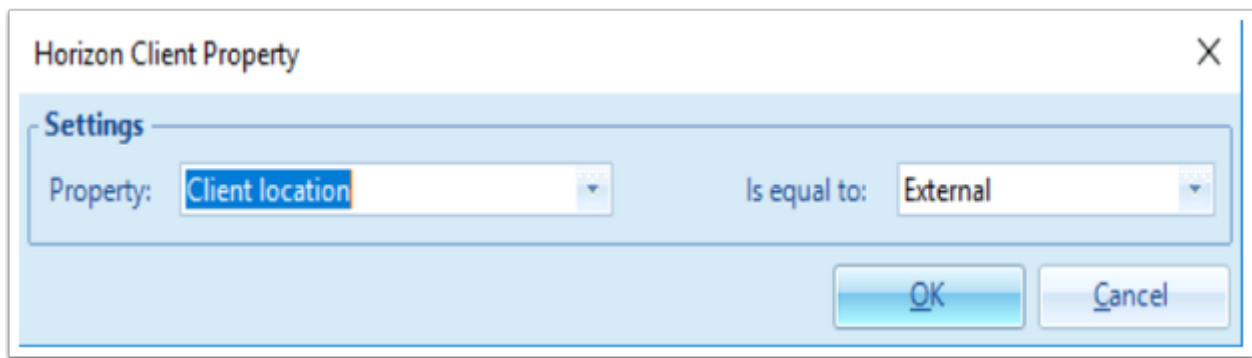
2. In the **Horizon Smart Policies, Settings** tab enter the following:-
  - Under **General** Settings, enter the following, next to:
    - **Name:** **Untrusted Networks**
    - **Label:** **USB, Clipboard and Client drive disabled**
    - **Tag:** **External**
  - In the **Horizon Smart Policy Settings**, 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 :** **Allow drag and drop from client to agent**
  - 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:** **Allow upload from client to agent**



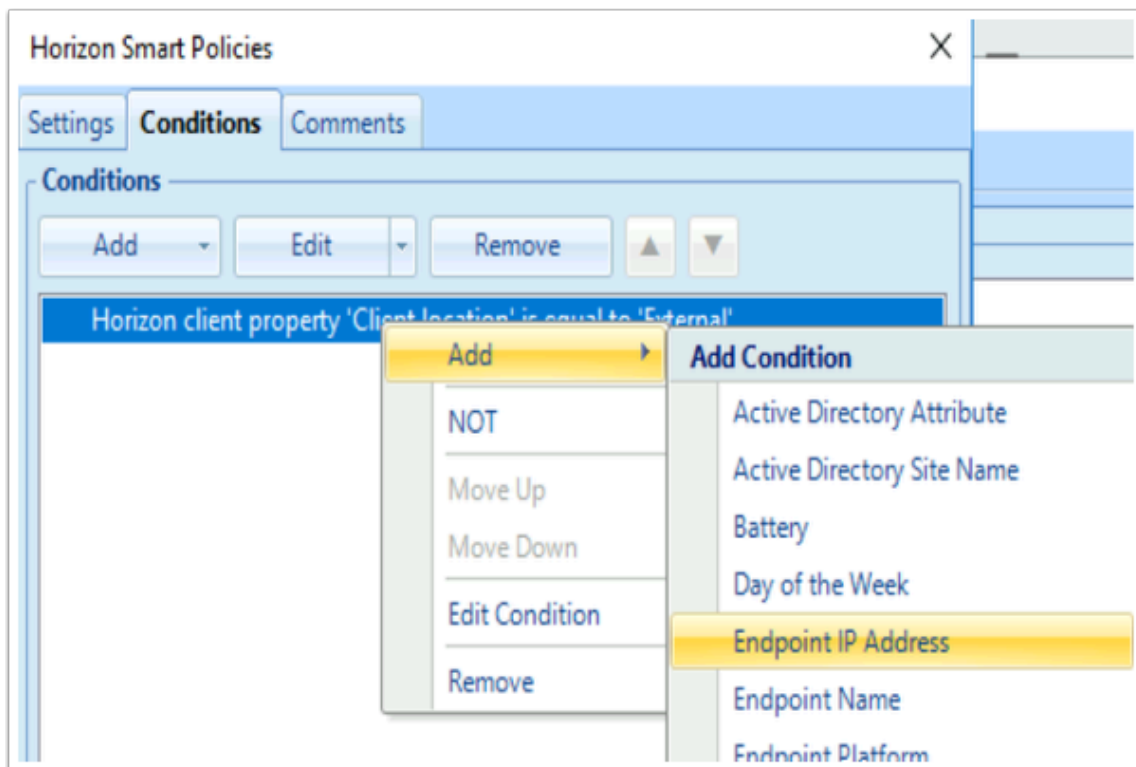
3. In the **Horizon Smart Policies** window
  - Select the **Conditions** tab
  - Under **Conditions**, select the **dropdown** next to **Add**



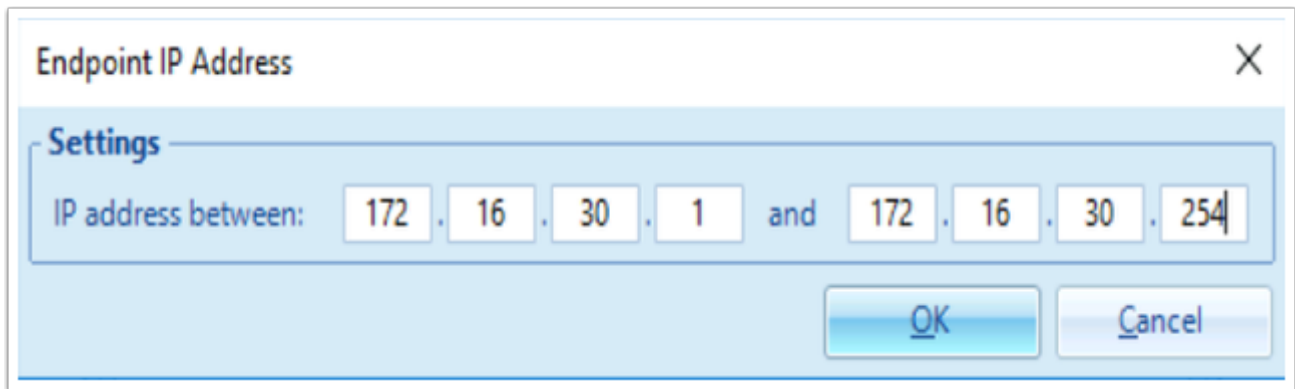
4. In the **Add Condition** dropdown
  - Select **Horizon Client Property**



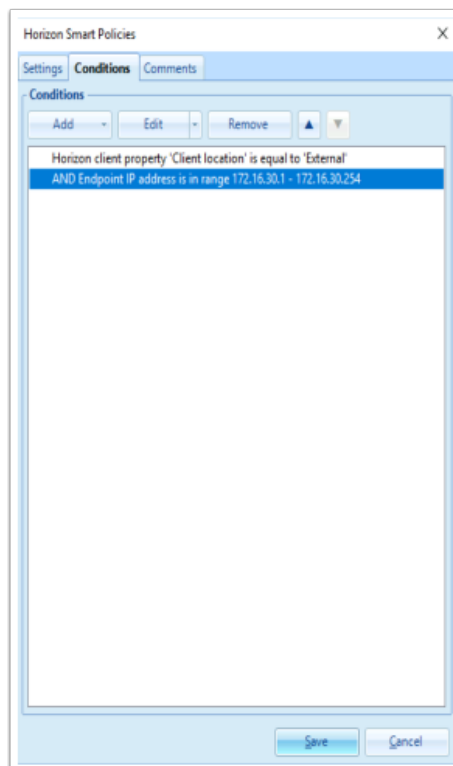
5. In the **Horizon Client Property**, add the following:
  - Next to **Property**, select **Client location** from the dropdown
  - Next to **Is equal to**, select **External** from the dropdown
  - Select **OK**, to close the **Horizon Client Property**



6. In the **Horizon Smart Policies** window, In the **Conditions area**
  - Select and right-click **the the existing client property**
    - Select **Add >**
    - Select **Endpoint IP Address**



7. In the **Endpoint IP Address** window, enter the following
  - Under **Settings**, next to **IP address between:** **172.16.30.1**
    - next to **and** enter: **172.16.30.254**
  - Select **OK** to close the window

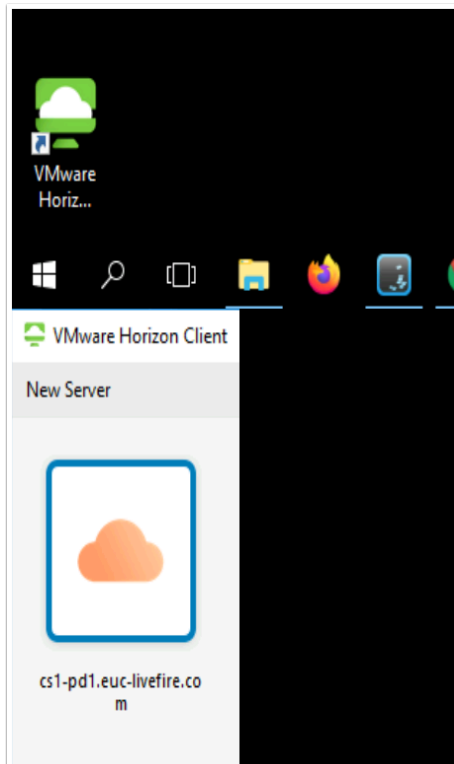


8. In the **Horizon Smart Policies** window
  - Confirm your configuration with the Screenshot
  - Select **Save**

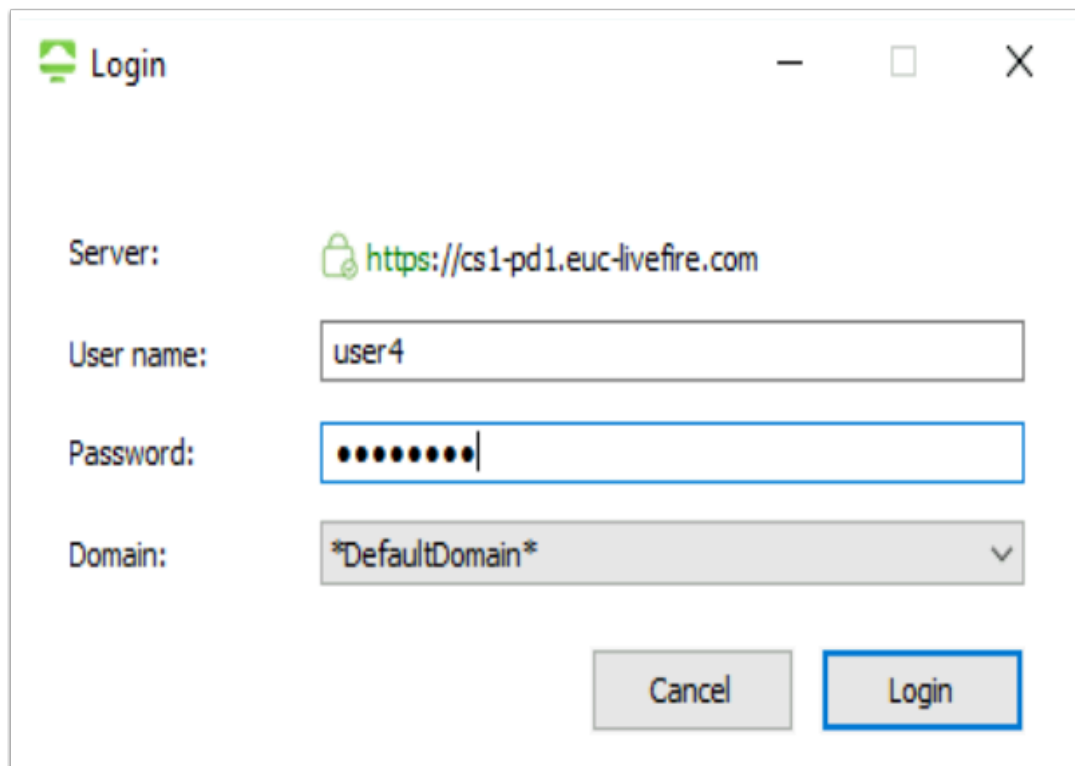
## PART 3 : Testing your Smart Policies.

Due to constraints in our virtual environment with external access, we will demonstrate only one of the features in Horizon Smart Policies

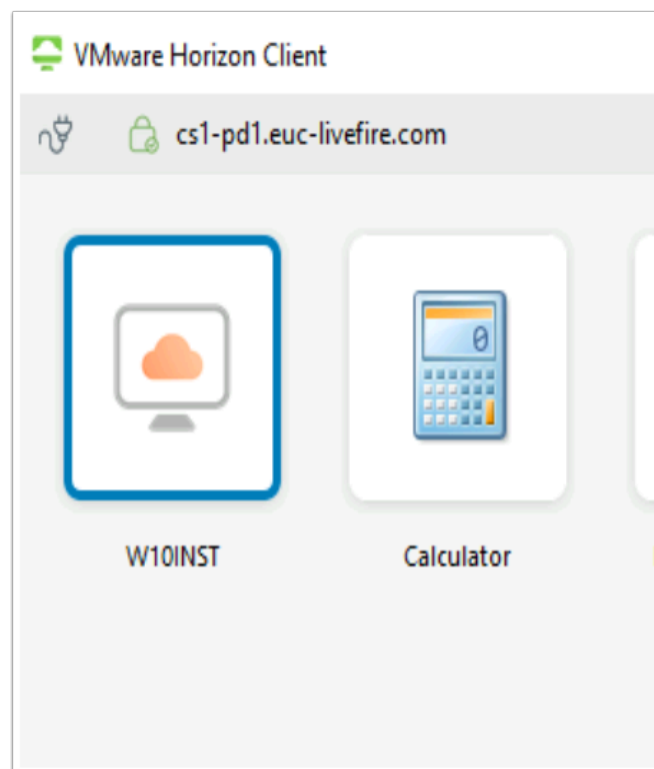
- That being Drag and Drop functionality.
- We have limitations in terms of what we can demonstrate with USB redirection
- We will use the Dynamic Environment Manager Logs, to see if the settings are effective.



1. On your **ControlCenter2** server desktop
  - Launch your **Horizon Client**
  - Select your Horizon POD **cs1-pd1.euc-livewire.com**

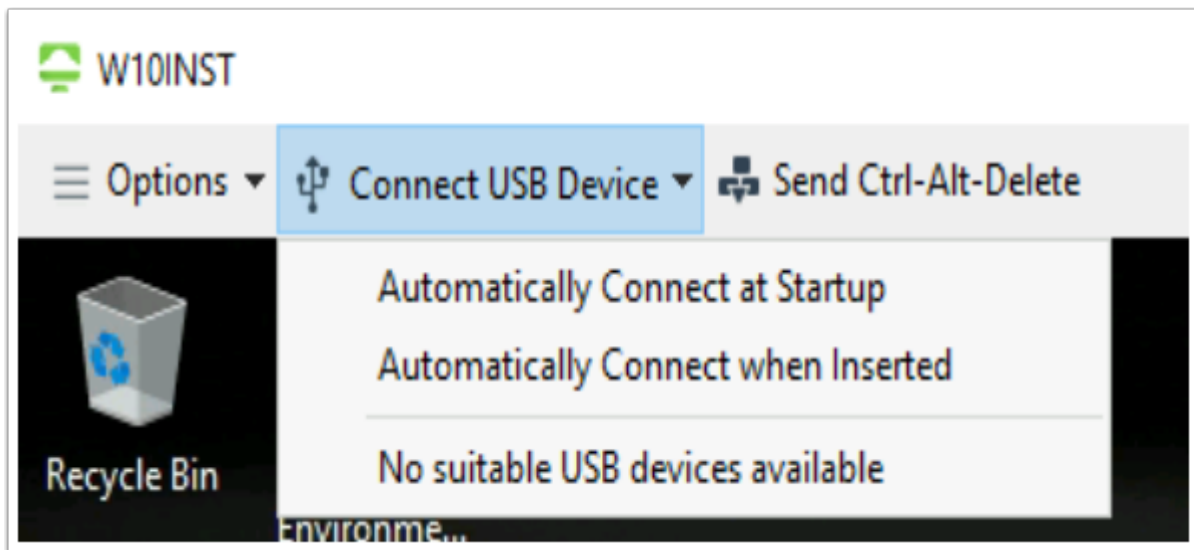


2. In the Horizon Client login window
  - Next to **User name:** login as **user4**
  - Next to **Password:** **VMware1!**
  - Select **Login**

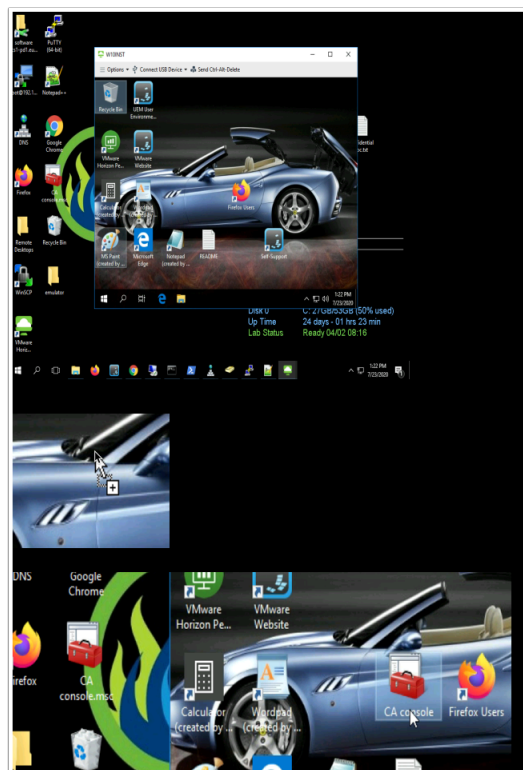


3. In the VMware Horizon Client

- Select your **W10INST** desktop entitlement
- Wait for the Desktop session to load

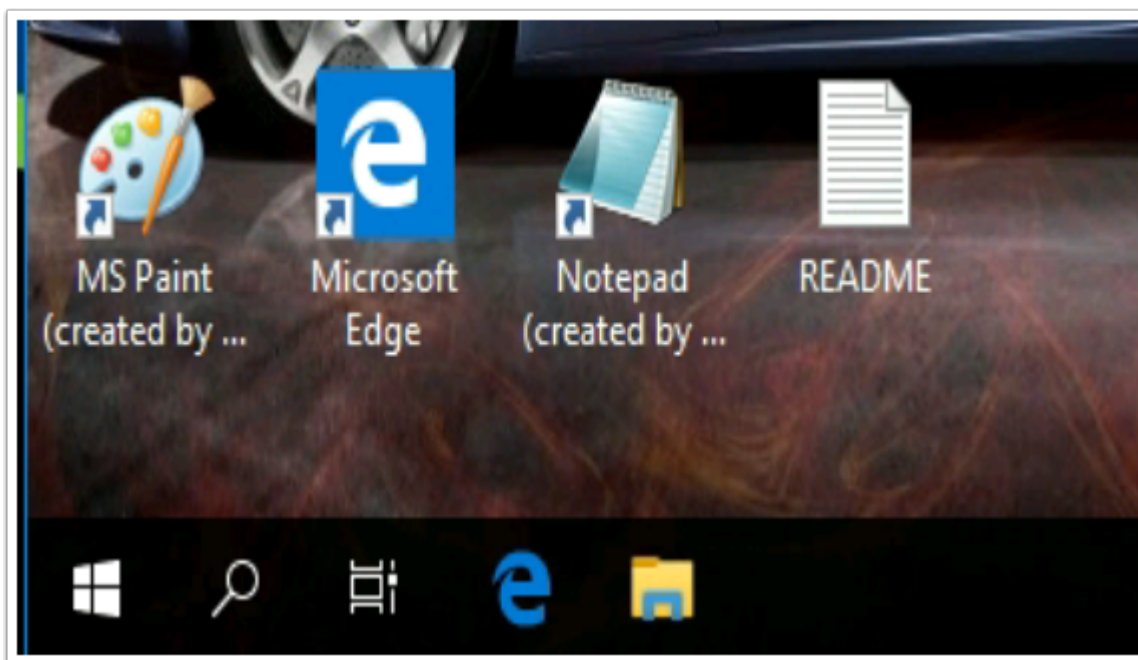


4. In the VMware Horizon Client
  - Select the **dropdown arrow**, next to **Connect USB Device**
  - Note, **No suitable USB devices available**, is the message you get.



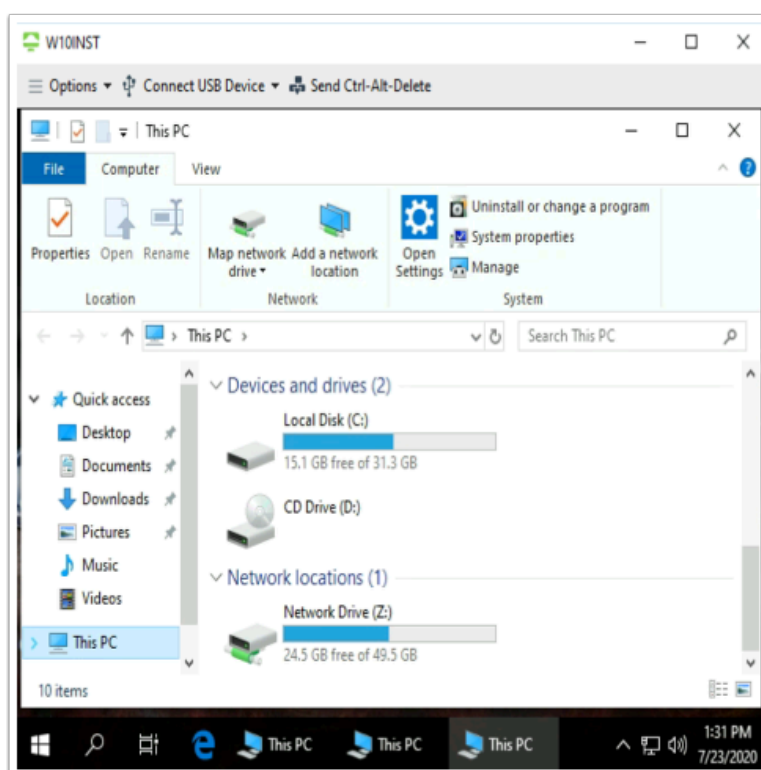
5. Starting from your ControlCenter2 server desktop
  - First, ensure that you are not in full-screen with the **Horizon Client**
  - With your **mouse, select** the **CA Console.msc icon** on the ControlCenter2 server desktop and Drag over into the Horizon Client session
    - Note that you will get a **+ type Icon** , just below your cursor.

- Release your mouse button to Drop the Console within the Horizon Session



6. In the Horizon Client session

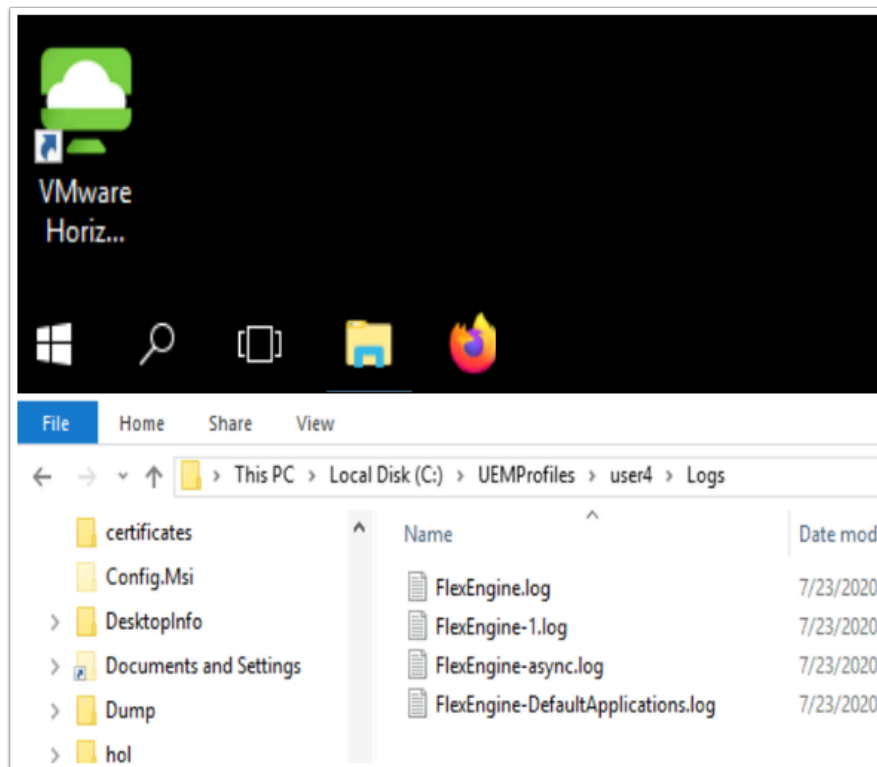
- From the Taskbar, select the **File Explorer** folder shortcut



7. In the File Explorer Window

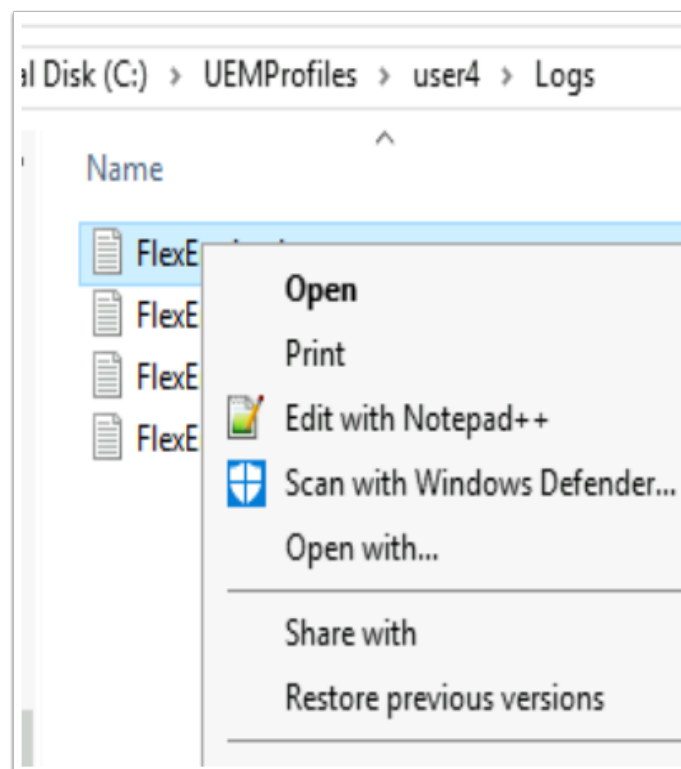
- Select **This PC** in the left Inventory
- To the right, **scroll down** and observe, there are network locations configured. ie the **Z: drive**





8. On the Controlcenter2 server

- Open your **File Explorer** Icon, from the Taskbar
- On the **C:\**, open your **UEMProfiles\user4\Logs** folder



9. In File Explorer C:\UEMProfiles\user1\Logs

- Select and right-click **FlexEngine.log**

- Select **Edit with Notepad++**

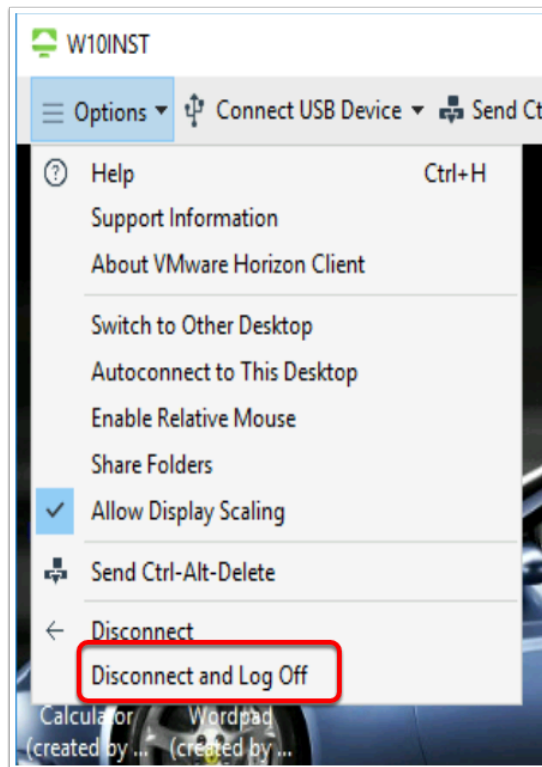
```

7:30:37.426 [INFO ] Performing path-based import
7:30:37.429 [DEBUG] User: EUC-LIVEFIRE\user4, Computer: W10INST2, OS: x64-win10 (Version 1903, BuildNumber 18362.296, SuiteMask 100, Product
7:30:37.429 [DEBUG] Profile name: local (0x00000004)
7:30:37.429 [DEBUG] Recursively processing config files from path '\\controlcenter2\UEMConfig\General'
7:30:37.429 [DEBUG] Using profile archive path '\\controlcenter2\UEMProfiles\user4\Archives'
7:30:37.429 [DEBUG] Logging to file '\\controlcenter2\UEMProfiles\user4\Logs\FlexEngine.log'
7:30:37.429 [DEBUG] Log file will be overwritten when larger than 512 kilobytes
7:30:37.543 [DEBUG] Setting import status flag
7:30:37.618 [DEBUG] Running on Horizon (session 1) [S]
7:30:37.618 [DEBUG] Conditions: Check for Horizon client property 'Broker_GatewayLocation' = true ('Internal' is equal to 'Internal')
7:30:37.620 [DEBUG] Conditions: Check for endpoint IP address = true (192.168.110.10 matches 192.168.110.1 - 192.168.110.254)
7:30:37.624 [DEBUG] Collected Horizon Smart Policies settings for audio playback ('Trusted Network.xml')
7:30:37.626 [DEBUG] Collected Horizon Smart Policies settings for bandwidth profile ('Trusted Network.xml')
7:30:37.626 [DEBUG] Collected Horizon Smart Policies settings for Elast Extreme (H.264) ('Trusted Network.xml')
7:30:37.626 [DEBUG] Collected Horizon Smart Policies settings for Elast Extreme (JPG) ('Trusted Network.xml')
7:30:37.626 [DEBUG] Collected Horizon Smart Policies settings for Elast Extreme (max frame rate) ('Trusted Network.xml')
7:30:37.631 [DEBUG] Collected Horizon Smart Policies settings for drag and drop ('Trusted Network.xml')
7:30:37.631 [DEBUG] Collected Horizon Smart Policies settings for printing ('Trusted Network.xml')
7:30:37.631 [DEBUG] Collected Horizon Smart Policies settings for client drive redirection ('Trusted Network.xml')
7:30:37.631 [DEBUG] Collected Horizon Smart Policies settings for clipboard ('Trusted Network.xml')
7:30:37.631 [DEBUG] Collected Horizon Smart Policies settings for USB redirection ('Trusted Network.xml')
7:30:37.631 [DEBUG] Collected Horizon Smart Policies settings for Web and Chrome file transfer ('Trusted Network.xml')
7:30:37.640 [DEBUG] Conditions: Check for Horizon client property 'Broker_GatewayLocation' = false ('Internal' is not equal to 'External')
7:30:37.640 [INFO ] Skipping Horizon Smart Policies settings due to conditions ('Untrusted Networks.xml')
7:30:37.674 [INFO ] Applied Horizon Smart Policies settings:
7:30:37.674 [INFO ] Bandwidth profile is set to 'LAN'
7:30:37.674 [INFO ] Audio playback is enabled
7:30:37.674 [INFO ] Elast Extreme: H.264 is enabled, JPG is enabled, Max frame rate is set to 30
7:30:37.674 [INFO ] Drag and drop is allowed
7:30:37.674 [INFO ] Printing is enabled
7:30:37.674 [INFO ] Client drive redirection is allowed
7:30:37.674 [INFO ] Clipboard redirection is allowed
7:30:37.674 [INFO ] USB redirection is enabled
7:30:37.674 [INFO ] Web and Chrome file transfer is allowed
7:30:37.718 [DEBUG] Skipping disabled DEM import task ('Delete Windows 5.x Start Menu.xml')
7:30:37.722 [DEBUG] Skipping disabled DEM import task ('Delete Windows 6.x Start Menu.xml')

```

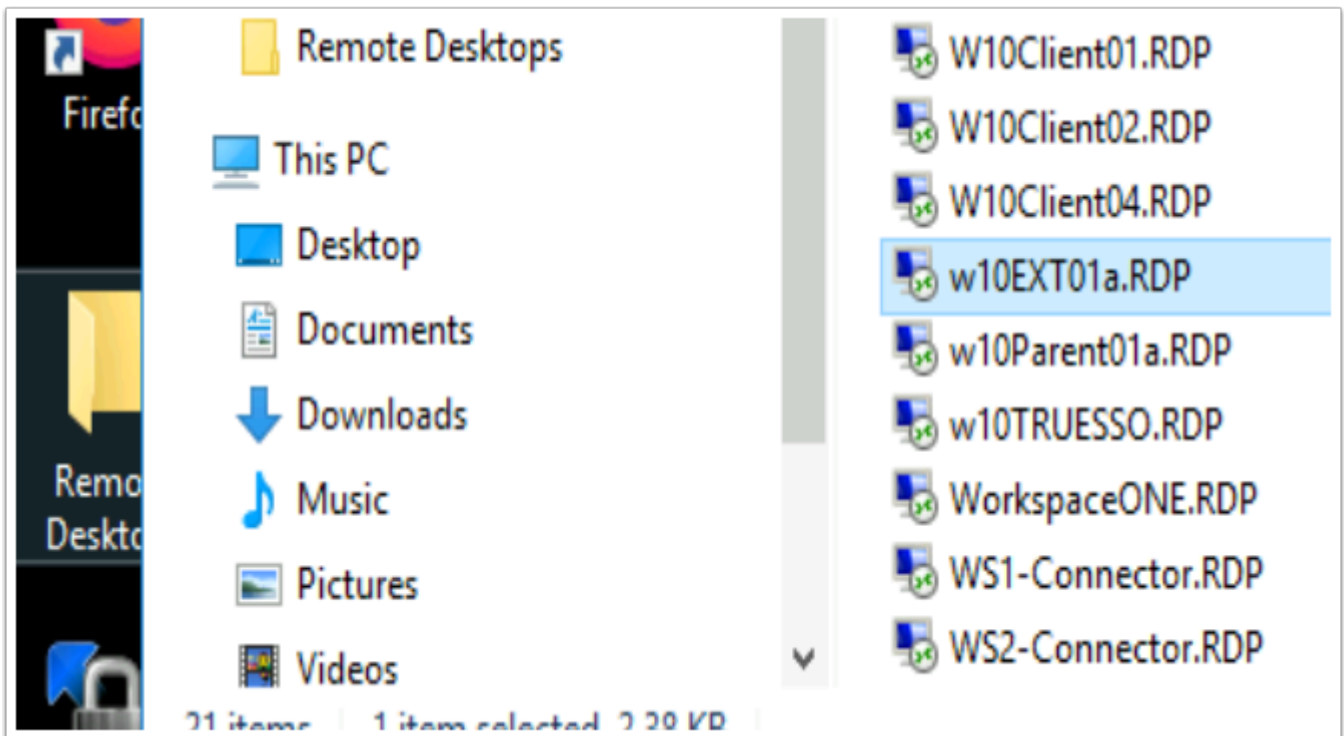
10. In the Notepad++ session

- **Reload your logs**, by selecting **File > Reload from Disk**
- **Scroll down**, right to the bottom of your logs,
  - **Scroll up** until you find the **User4** 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**



11. On the ControlCenter2 server

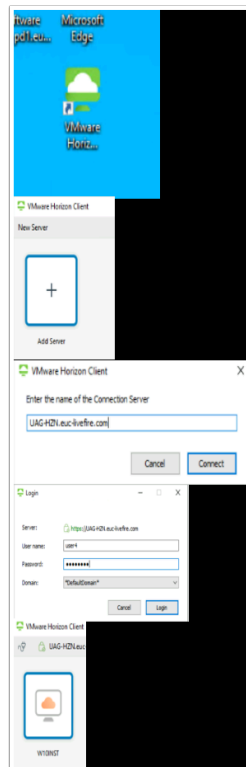
- Switch back to your **Horizon Client** session
- Select the **drop down**, next to **Options**, Ensure you select **Disconnect and Log Off**



12. On the ControlCenter2 server

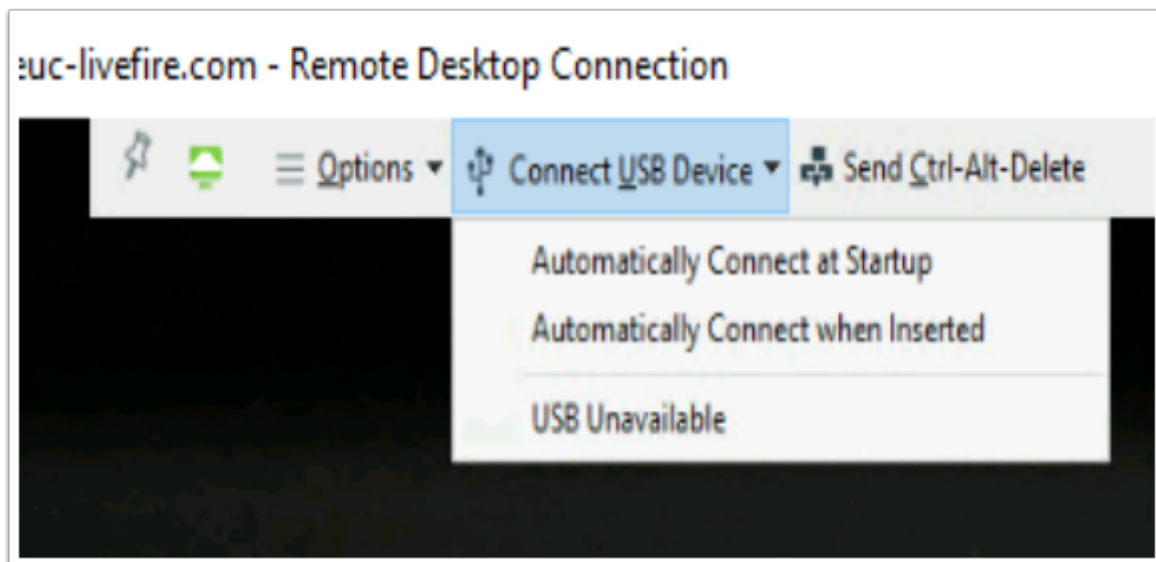
- Open the **Remote Desktops** folder
- Open **w10EXT01a.RDP (Note!)**

- Login with the **username** **w10ext01a\administrator**
- Login with the **password** **VMware1!**



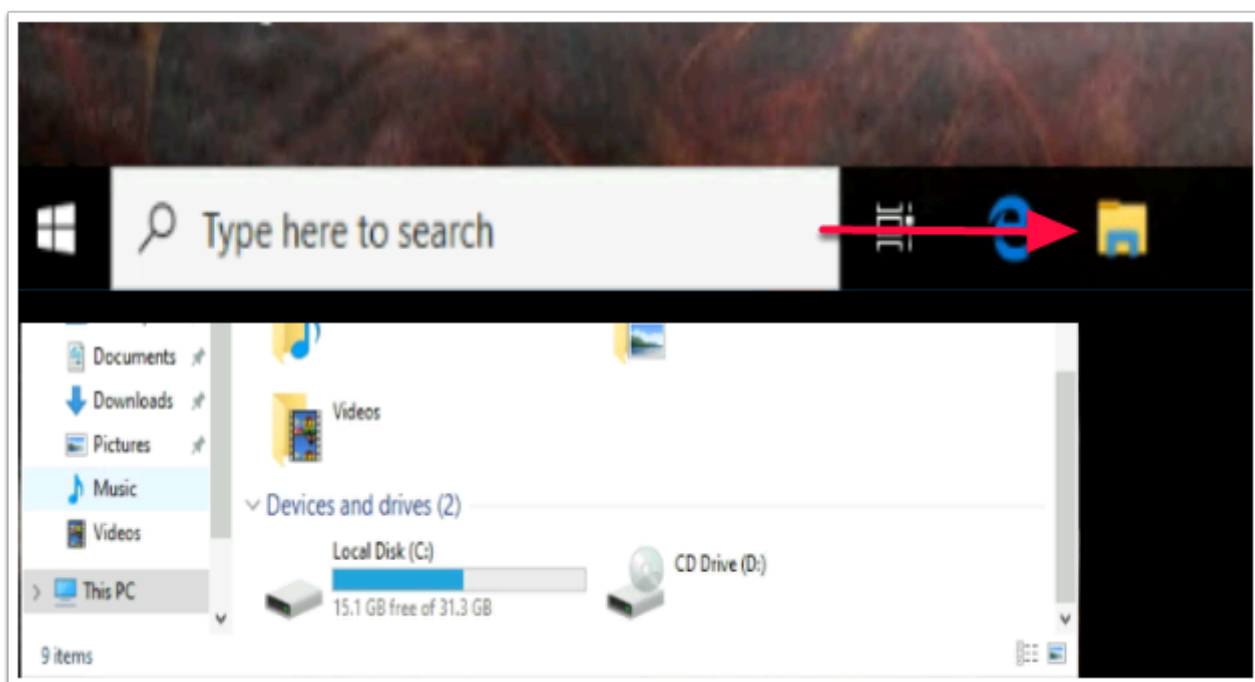
### 13. On the **W10Ext01a** desktop

- Please Note. **W10Ext01a** desktop is on a network which we have configured as external. That being the 172.16.30.x network
- We will also be connecting via the Unified Access Gateway in this exercise
- Launch the **VMware Horizon Client**
- In the **VMware Horizon Client**
  - Select **Add Server**
  - Under **Enter the name of the Connection Server**,
    - Type : **UAG-HZN.EUC-Livefire.com**
  - Select **Connect**
- In the **Login** window
  - Next to **User name:** enter :- **User4**
  - Next to **Password:** enter:- **VMware1!**
  - Select **Login**
- In the **VMware Horizon Client**
  - Select the **W10INST** desktop entitlement



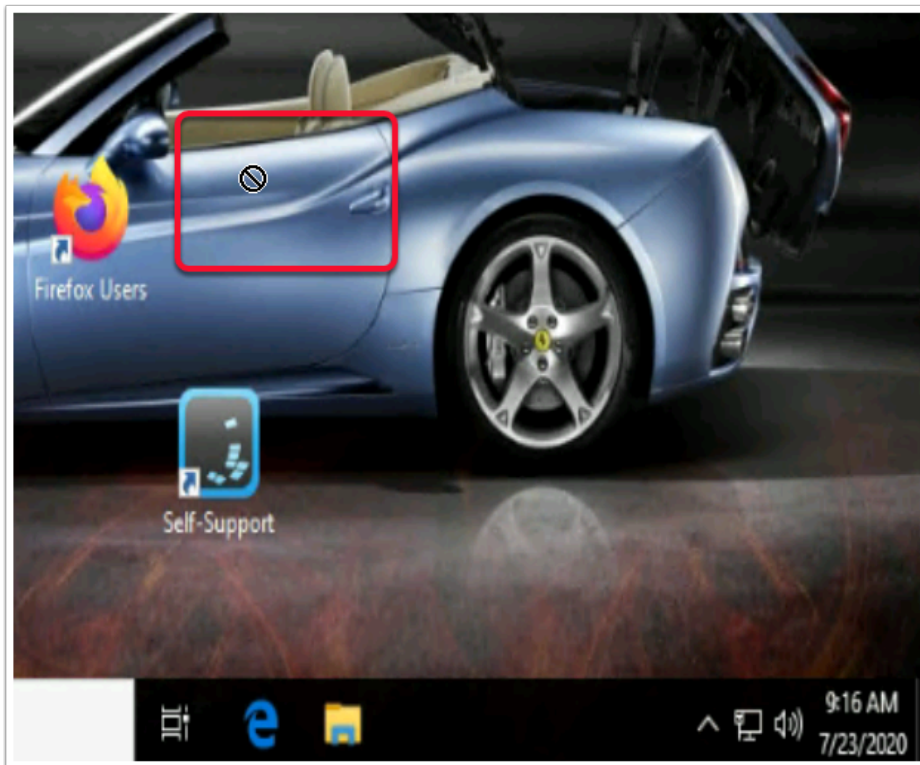
#### 14. In the **Horizon Client**

- In the top bar, next to **Connect USB Device**, select the **drop-down**
- Notice that **USB Unavailable** is the state of USB



#### 15. 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**
  - **Close all** windows in the **Horizon W10 desktop session**



## 16. In the **W10EXT01a** Desktop

- Attempt to drag the **Software Shortcut** on the **W10Ext01a Desktop** into the **Horizon Desktop** session.
- Attempt to drag the **README** file from the **Horizon Desktop** session to the **W10EXT01a Desktop**

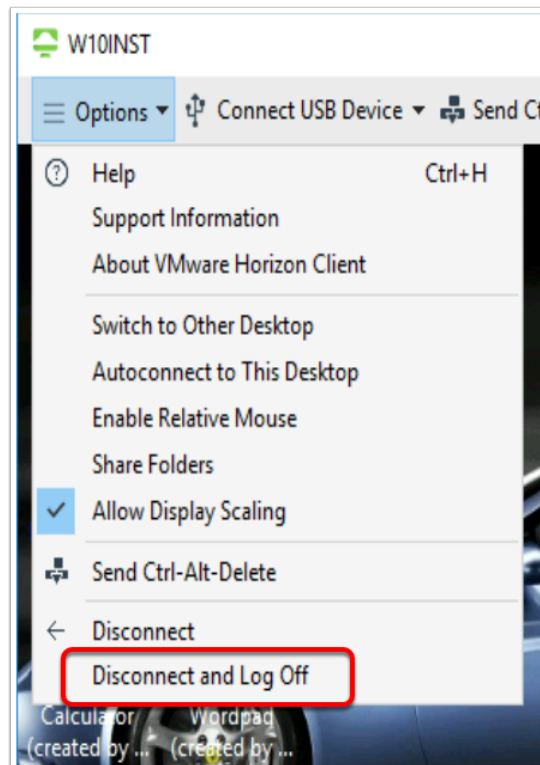
```

0018 2020-07-23 09:01:10.002 [INFO ] Performing path-based import
0019 2020-07-23 09:01:10.004 [DEBUG] User: EUC-LIVEFIRE\user4, Computer: W10INST2, OS: x64-Win10 (Version 1904, BuildNumber 18962.295, SuiteMask 100, Produ
0020 2020-07-23 09:01:10.005 [DEBUG] Profile state: local (0x00000204)
0021 2020-07-23 09:01:10.005 [DEBUG] Recursively processing config files from path '\\controlcenter2\UEMConfig\General'
0022 2020-07-23 09:01:10.005 [DEBUG] Using profile archive path '\\controlcenter2\UEMProfiles\user4\Archives'
0023 2020-07-23 09:01:10.005 [DEBUG] Logging to file '\\controlcenter2\UEMProfiles\user4\Logs\FlexEngine.log'
0024 2020-07-23 09:01:10.005 [DEBUG] Log file will be overwritten when larger than 512 kilobytes
0025 2020-07-23 09:01:10.159 [DEBUG] Setting import status flag
0026 2020-07-23 09:01:10.232 [DEBUG] Running on Horizon (session 1) [3]
0027 2020-07-23 09:01:10.232 [DEBUG] Conditions: Check for Horizon client property 'Broker_GatewayLocation' = false ('External' is not equal to 'Internal')
0028 2020-07-23 09:01:10.236 [INFO ] Skipping Horizon Smart Policies settings due to conditions ('Trusted Networks.xml')
0029 2020-07-23 09:01:10.247 [DEBUG] Conditions: Check for Horizon client property 'Broker_GatewayLocation' = true ('External' is equal to 'External')
0030 2020-07-23 09:01:10.250 [DEBUG] Conditions: Check for endpoint IP address = true (172.16.30.30 matches 172.16.30.1 - 172.16.30.254)
0031 2020-07-23 09:01:10.250 [DEBUG] Collected Horizon Smart Policies settings for audio playback ('Untrusted Networks.xml')
0032 2020-07-23 09:01:10.251 [DEBUG] Collected Horizon Smart Policies settings for bandwidth profile ('Untrusted Networks.xml')
0033 2020-07-23 09:01:10.251 [DEBUG] Collected Horizon Smart Policies settings for Blast Extreme (H.264) ('Untrusted Networks.xml')
0034 2020-07-23 09:01:10.265 [DEBUG] Collected Horizon Smart Policies settings for Blast Extreme (max frame rate) ('Untrusted Networks.xml')
0035 2020-07-23 09:01:10.265 [DEBUG] Collected Horizon Smart Policies settings for drag and drop ('Untrusted Networks.xml')
0036 2020-07-23 09:01:10.265 [DEBUG] Collected Horizon Smart Policies settings for client drive redirection ('Untrusted Networks.xml')
0037 2020-07-23 09:01:10.265 [DEBUG] Collected Horizon Smart Policies settings for clipboard ('Untrusted Networks.xml')
0038 2020-07-23 09:01:10.265 [DEBUG] Collected Horizon Smart Policies settings for USB redirection ('Untrusted Networks.xml')
0039 2020-07-23 09:01:10.265 [DEBUG] Collected Horizon Smart Policies settings for Web and Chrome file transfer ('Untrusted Networks.xml')
0040 2020-07-23 09:01:10.292 [INFO ] Applied Horizon Smart Policies settings:
0041 2020-07-23 09:01:10.292 [INFO ] Bandwidth profile is set to 'Broadband WAN'
0042 2020-07-23 09:01:10.292 [INFO ] Audio playback is enabled
0043 2020-07-23 09:01:10.292 [INFO ] Blast Extreme: H.264 is enabled, Max frame rate is set to 30
0044 2020-07-23 09:01:10.292 [INFO ] Drag and drop is allowed from client to agent
0045 2020-07-23 09:01:10.292 [INFO ] Client drive redirection is disabled
0046 2020-07-23 09:01:10.292 [INFO ] Clipboard redirection is disabled
0047 2020-07-23 09:01:10.292 [INFO ] USB redirection is disabled
0048 2020-07-23 09:01:10.293 [INFO ] Web and Chrome file transfer allows upload from client to agent
0049 2020-07-23 09:01:10.335 [DEBUG] Skipping disabled DEM import task ('Delete Windows 5.x Start Menu.xml')
0050 2020-07-23 09:01:10.340 [DEBUG] Skipping disabled DEM import task ('Delete Windows 6.x Start Menu.xml')
0051 2020-07-23 09:01:10.372 [DEBUG] Skipping disabled DEM settings import ('Dutch.xml')

```

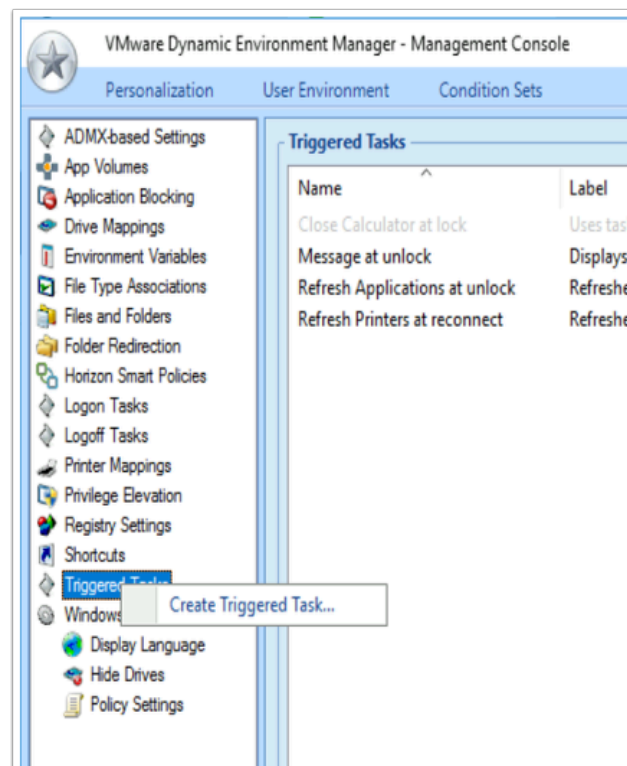


17. On the **ControlCenter2** server Desktop
- Revert back to your **Notepad++** application
  - When prompted to **Reload**, select **Yes**
  - **Scroll right to the bottom** of Notepad ++
  - Slowly scroll up searching for the **User4 path based import**
    - When authoring this material, I had to scroll up about 300 lines
  - Note the following:
    - That the **External** Smart Policy is **applied**
    - **Broadband band-width** profile is being **applied**
    - **Client drive, USB and Clipboard redirection** are **disabled**



11. On the **W10EXT01a** desktop
- Switch back to your **Horizon Client** session
  - Select the **drop down**, next to **Options**, select **Disconnect and Log Off**

## PART 4: Using Triggered Tasks to enforce Horizon Smart Policies



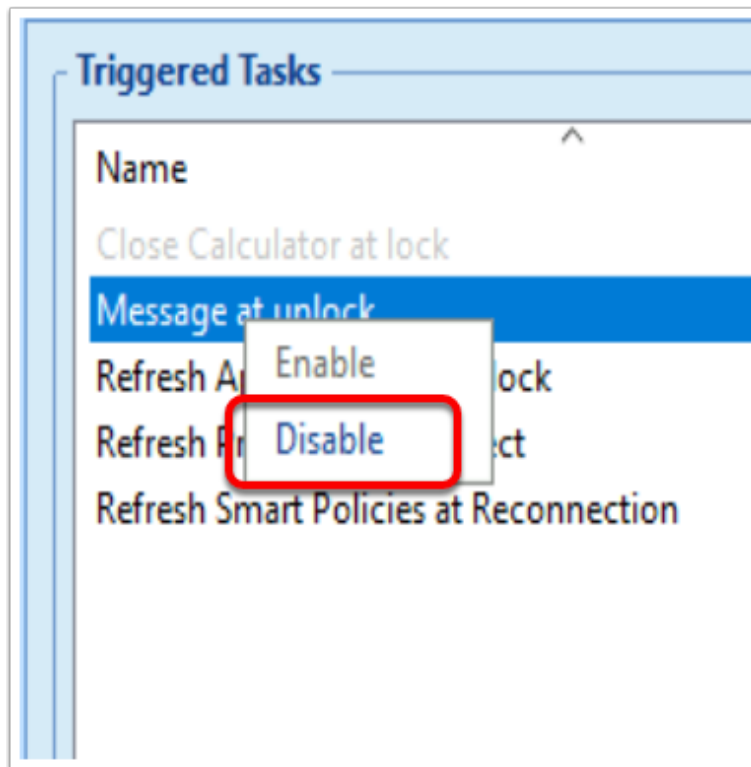
1. In the **Dynamic Environment Manager** Console, under **User Environment**
  - Select **Triggered Tasks**
  - Select **Create Triggered Task...**



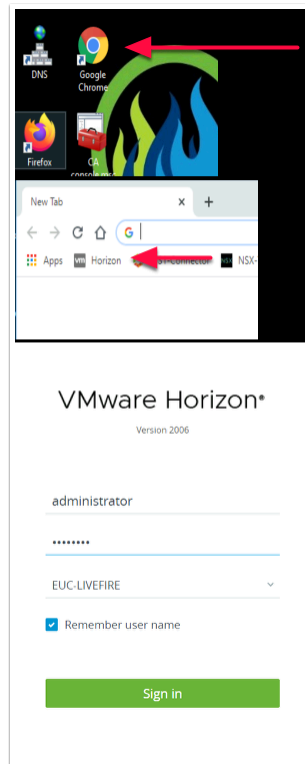
The screenshot shows the 'Triggered Task' window with the following configuration:

- General Settings:**
  - Name: Refresh Smart Policies at Reconnection
  - Label: (empty)
  - Tag: (empty)
- Triggered Task Settings:**
  - Trigger: Session reconnected
  - ☐ Only applies if endpoint IP has changed since session was disconnected
  - Action: User Environment refresh
  - Refresh:
    - ☐ ADMX-based Settings
    - ☒ Application Blocking Settings
    - ☐ Drive Mappings
    - ☐ Environment Variables
    - ☐ File Type Associations
    - ☒ Horizon Smart Policies
    - ☐ Printer Mappings
    - ☐ Privilege Elevation Settings
    - ☐ Shortcuts
    - ☐ Triggered Task Settings
  - ☒ Show message
    - Caption: Your Livefire Configurations have been Updated
    - Message: This is Corp IT Livefire. We have re-evaluated and updated your Desktop settings
  - ☒ Close automatically after 10 seconds
  - ☐ Also allow user to dismiss message

2. In the **Triggered Task** window, configure the following:
  - In the **General Settings** area, add the following
    - Next to **Name:** type **Refresh Smart Policies at Reconnection**
  - In the **Triggered Tasks** area, configure the following next to:
    - **Trigger:** **Session reconnected**
    - **Refresh:** enable the
      - **Horizon Smart Policies** **checkbox**
      - **Application Blocking Settings** **checkbox**
  - Enable the **Check box** next to **Show message**
    - Enter the following:-
      - Next to **Caption:** **Your Livefire Configurations have been Updated**
      - In the **Message Box:** **This is Corp IT Livefire. We have re-evaluated and updated your Desktop settings**
      - Enable the **checkbox** next to **Close automatically after** and type **10** in front of seconds
  - Select **Save** to close the window

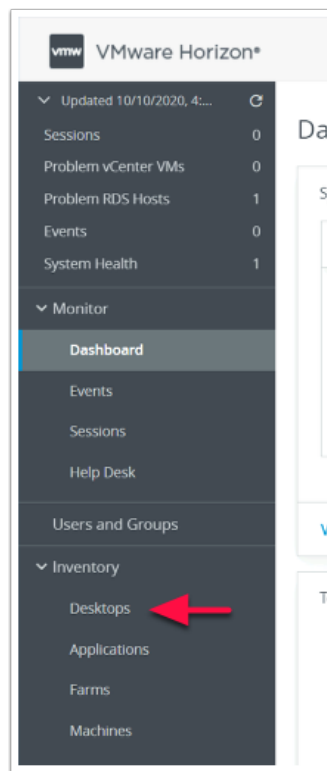


3. In the **Triggered Tasks** area
  - Select and right-click, **Message at unlock**
  - Select **Disable**

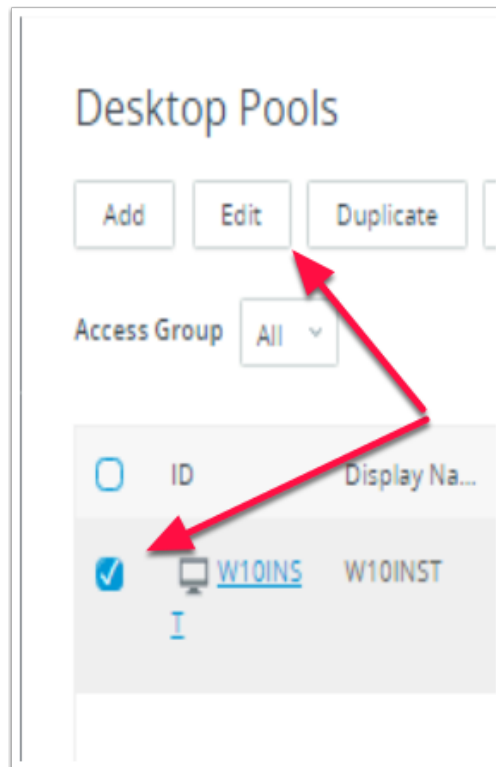


4. On your ControlCenter2 Desktop
  - Open your **Google Chrome Browser**

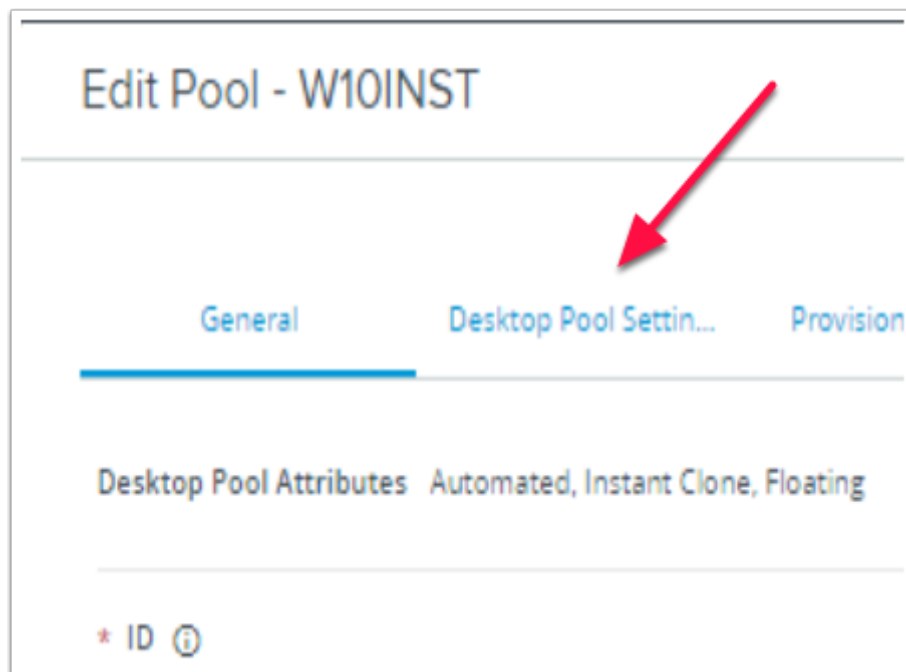
- Select the **Horizon** shortcut in the **Titlebar**
- In the **VMware Horizon** login, enter the following:-
  - **User name** area : - enter **Administrator**
  - **Password** area:- enter **VMware1!**
  - Select **Sign in**



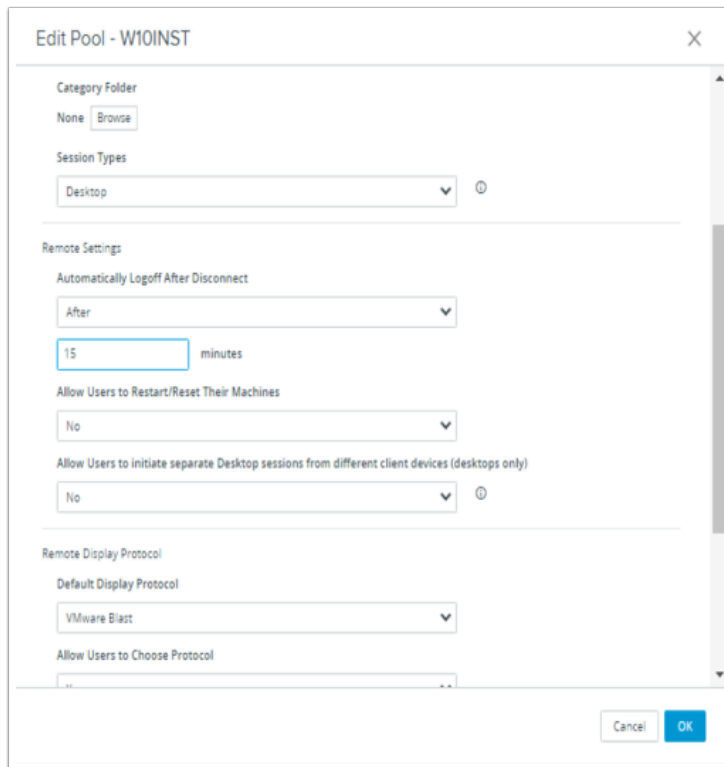
5. In the VMware Horizon Admin console
- Expand **Inventory** and select **Desktops**



6. In the **Desktop Pools** area
- Select the **checkbox** next **W10INST**
  - Select **Edit**



7. In the **Edit Pool - W10INST** window
- Select the **Desktop Pool Settings** tab

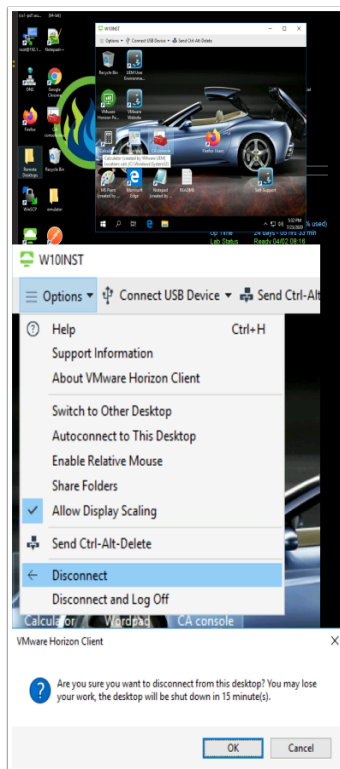


8. In the **Edit Pool - W10INST** window

- Under **Remote Settings** > **Automatically Logoff After Disconnect**
  - From the **dropdown** , Change from **Immediately** to **After**
  - Under **After** change **120 minutes** to **15 minutes**
  - Select **OK**

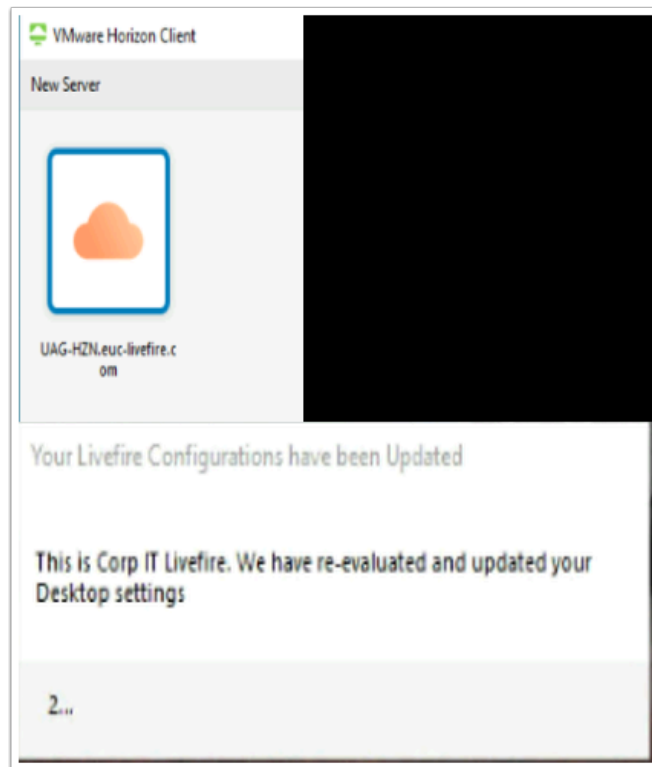
We will now move forward and do two simple tests

- We will log in to VMware Horizon from a Trusted Network. We will NOT log off , we will disconnect
- We will then log back in to the same VMware Horizon session session from an Untrusted Network source.



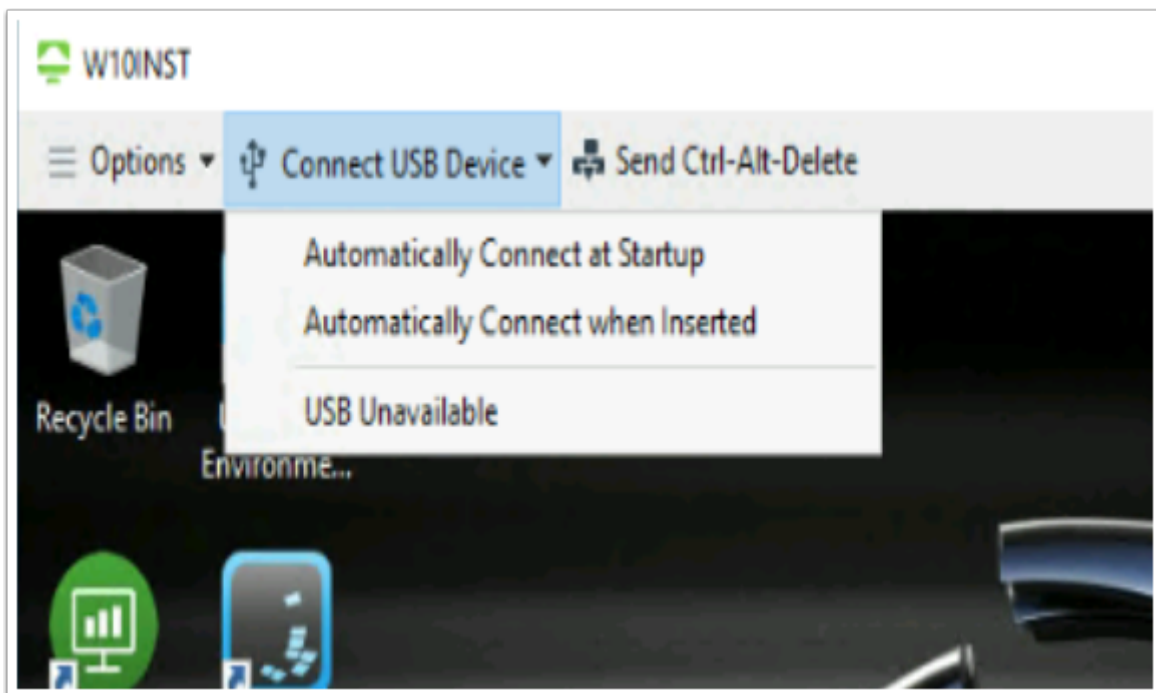
9. On your **Controlcenter2** server desktop

- Launch your **Horizon client** > Login as **User 4** > Select your **W10INST** entitlement
  - Notice you still have all your configurations for a Trusted Network environment. Test some of your configurations
- In the **Horizon Client**, next to **Options**, select the **dropdown**
- Select **Disconnect**
  - When prompted to disconnect for 15 minutes select **OK**
    - ( you have 15 minutes to login to your existing session)

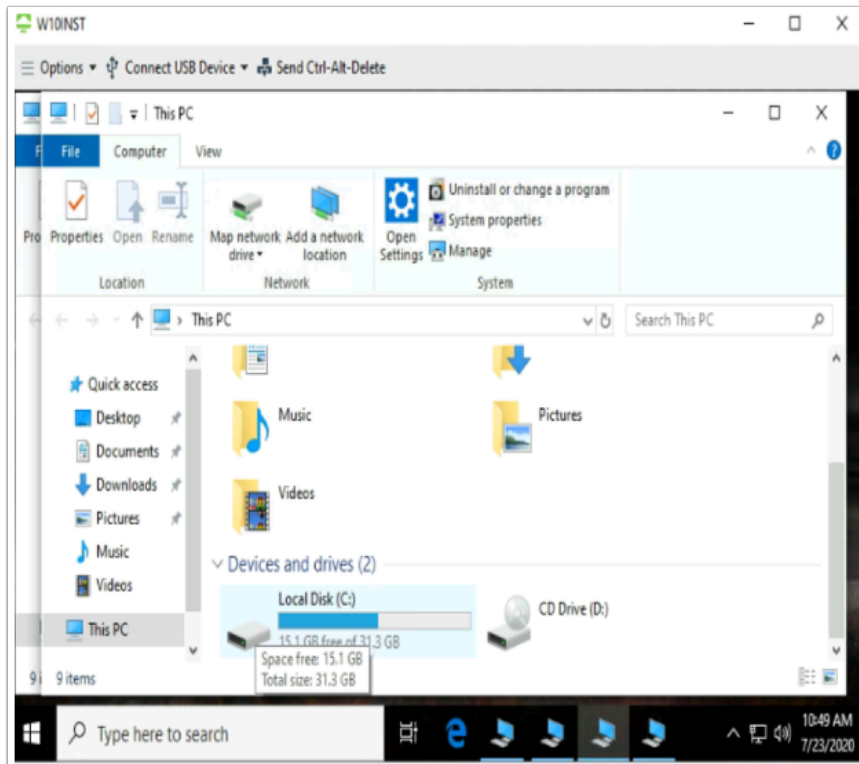


10. On your **W10Ext01a.RDP session**

- Launch your **Horizon Client**
  - Connect via your external Gateway, **UAG-HZN.euc-livfire.com**
    - Login as **User4**
    - Password **VMware1!**
    - Select your **W10INST** desktop Entitlement
    - Notice the prompt that your **Desktop settings** have been **re-evaluated**



11. In the W10INST Horizon client session on W10EXT01a
- Notice that USB is Unavailable



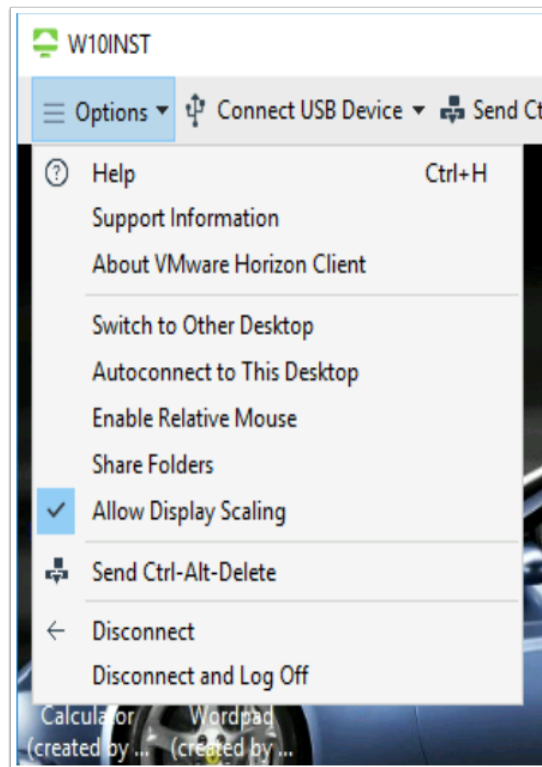
12. In the W10INST Horizon client session on W10EXT01a
- There is no Network Drive Mapping



13. In the W10INST Horizon client session on W10EXT01a



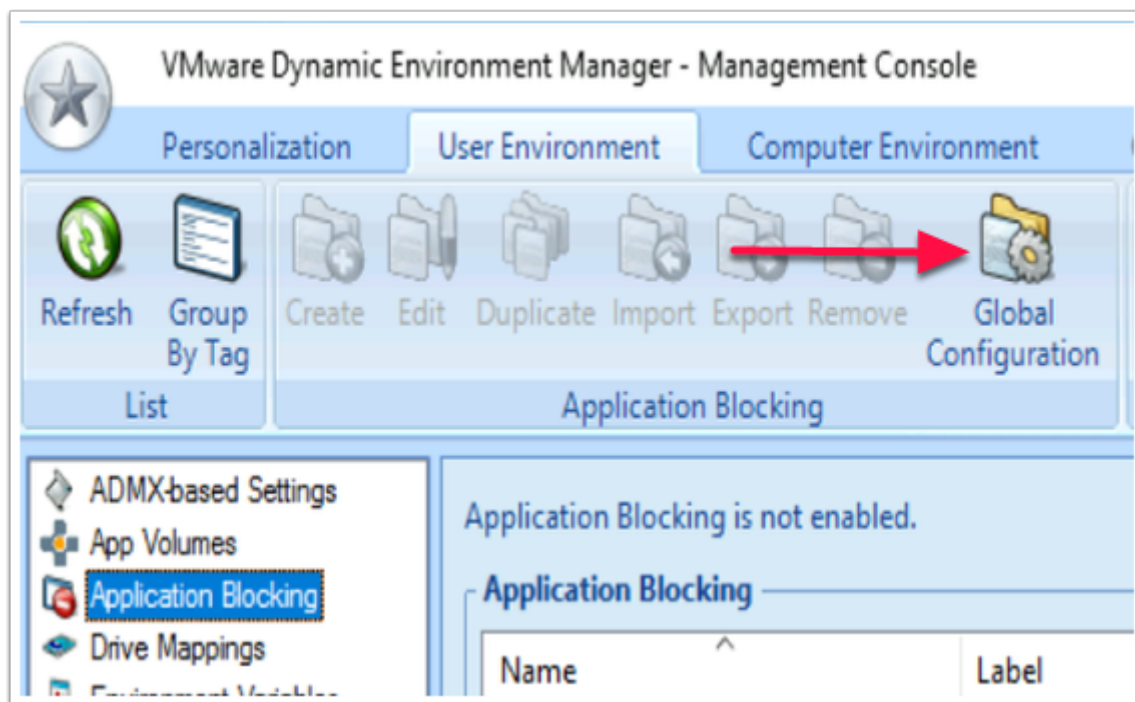
- Note that you still have the file dragged on to the desktop when you were on your Trusted network.
- However, we are unable to drag and drop in and out of this desktop session



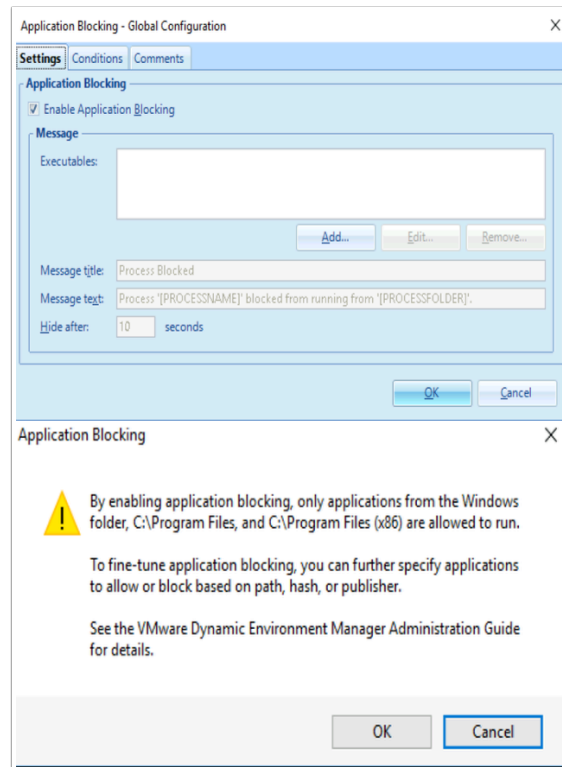
14. On the **W10EXT01a** desktop

- Switch back to your **Horizon Client** session
- Select the **drop down**, next to **Options**, select **Disconnect and Log Off**

## PART 5: Configuring Application Block and integrating with Horizon Smart Policies

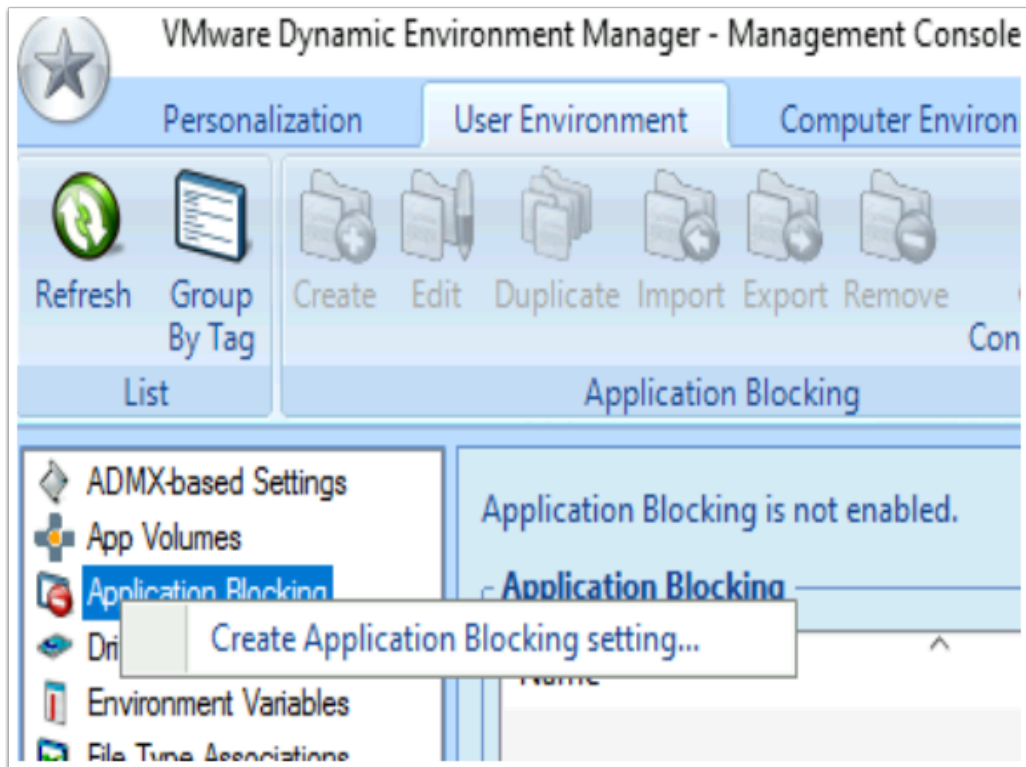


1. On your **ControlCenter2** server desktop
  - In the DEM Console select the **User Environment** tab
  - Select **Application Blocking**
  - In the title bar, select **Global Configuration**

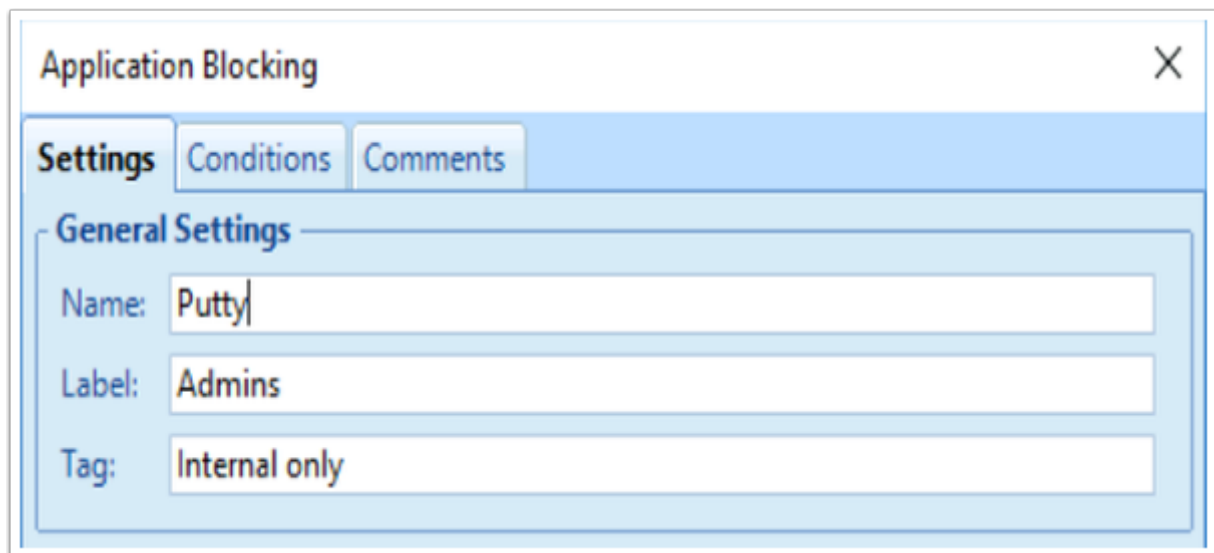


2. In the **Application Blocking - Global Configuration** window
  - Select the **Checkbox** next to **Enable Application Blocking**
  - Select **OK**
  - In the **Application Blocking** window,
    - Before we select **OK** , **read the note**
    - Select **OK**

We will now go and configure further.

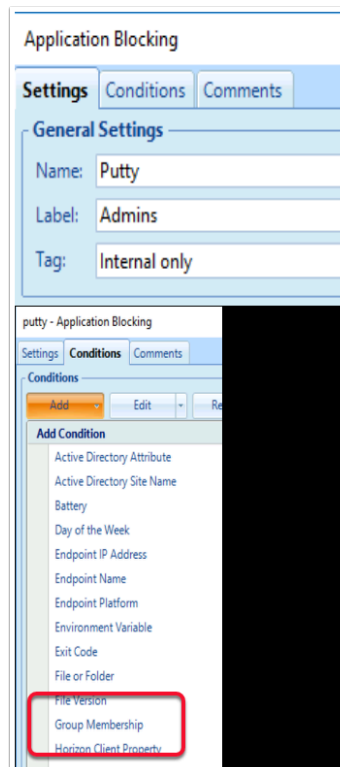


3. On the **User Environment** tab, of the DEM Console
  - Select and right-click **Application Blocking**
  - Then select **Create Application Blocking setting....**

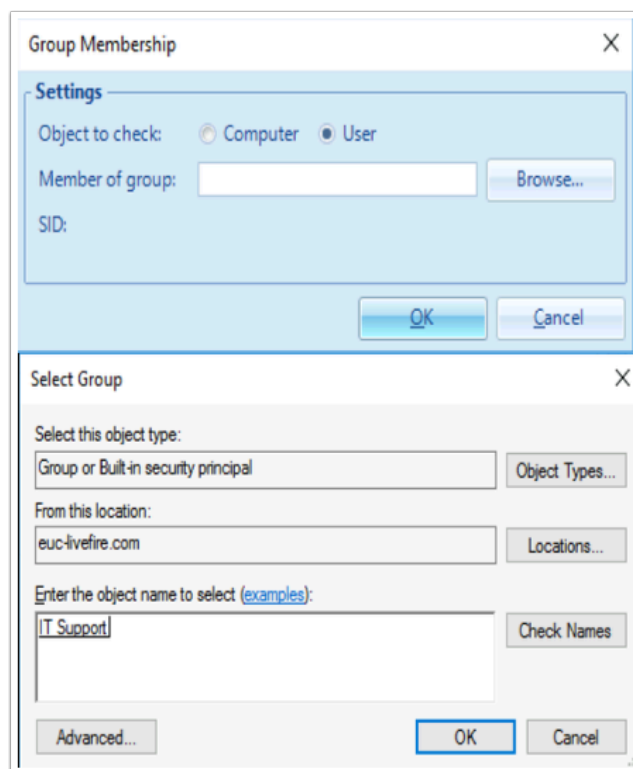


4. In the **Application Blocking** window
  - In the **General Settings** area, add the following next to:
    - **Name:** **Putty**
    - **Label:** **Admins**
    - **Tag:** **Internal only**



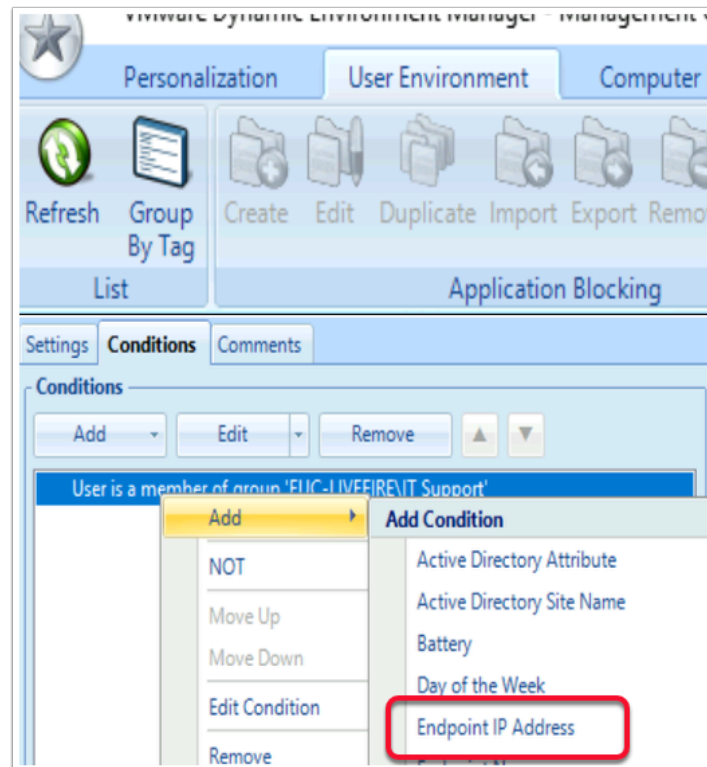


6. In the **Application Blocking** window
  - Select the **Conditions** tab.
  - Under **Conditions**, select the **dropdown** next to **Add**
  - Select **Group Membership**

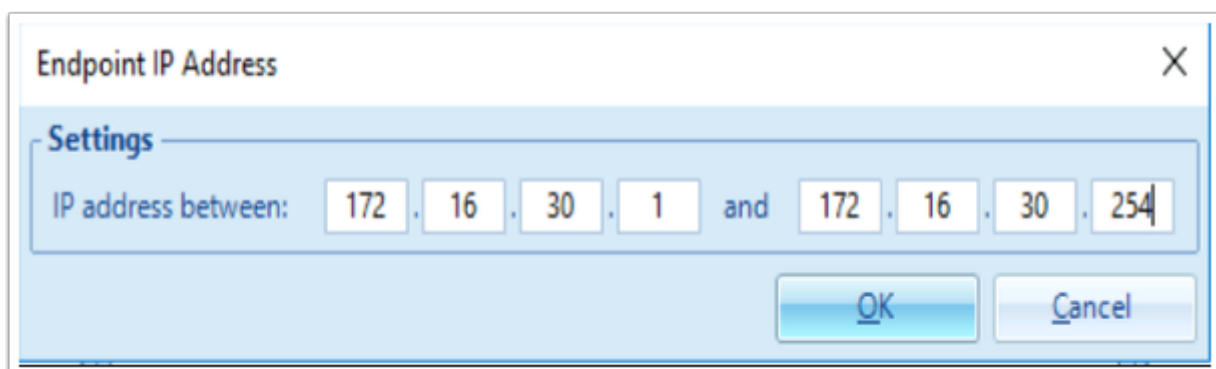


7. In the **Group Membership** window

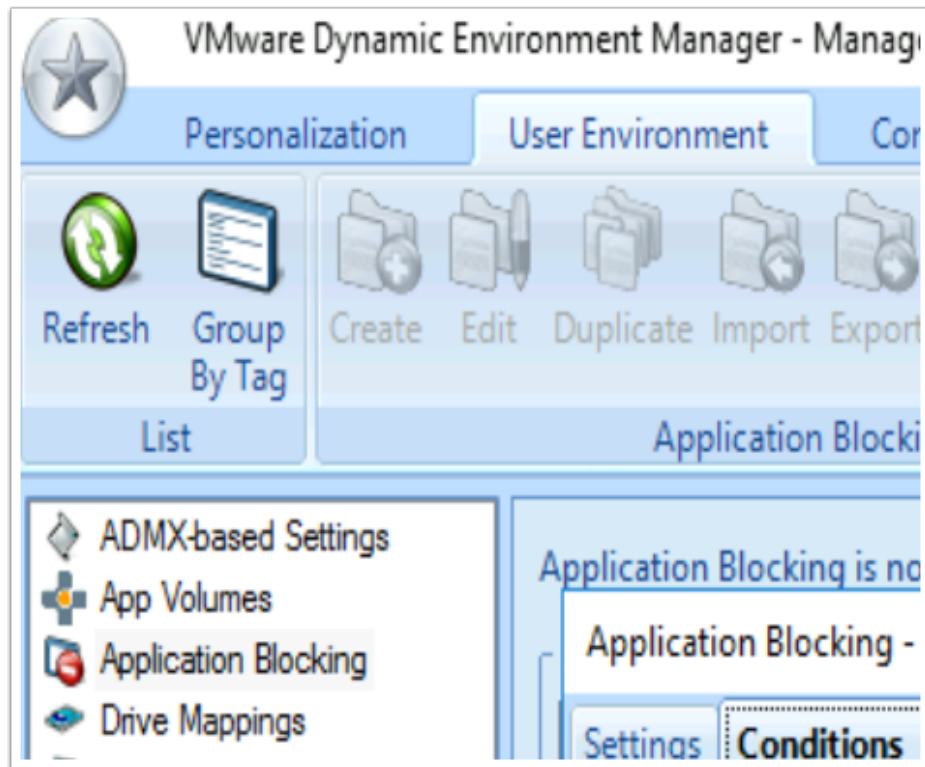
- Select **Browse**
- In the **Select Group** window, under **Enter the object name to select** type **IT** and then select **Check Names**
  - **IT Support** should show
- Select **OK** to close **Select Group**
- Select **OK** to close the **Group Membership** window



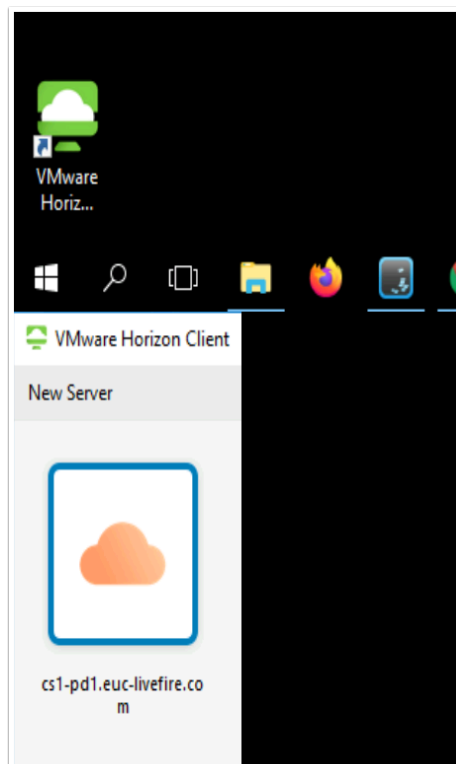
8. In the **Conditions** Tab for Application Blocking
  - Select and right-click the **condition you have just added for IT support**
  - Select **Add >**
  - In the **Add Condition** dropdown select **Endpoint IP Address**



9. In the **Endpoint IP Address** window
  - Under **Settings**, next to **IP address between:** **172.16.30.1** and **172.16.30.254**
  - Select **OK**
  - Select **Save** to close the **Application Blocking** window



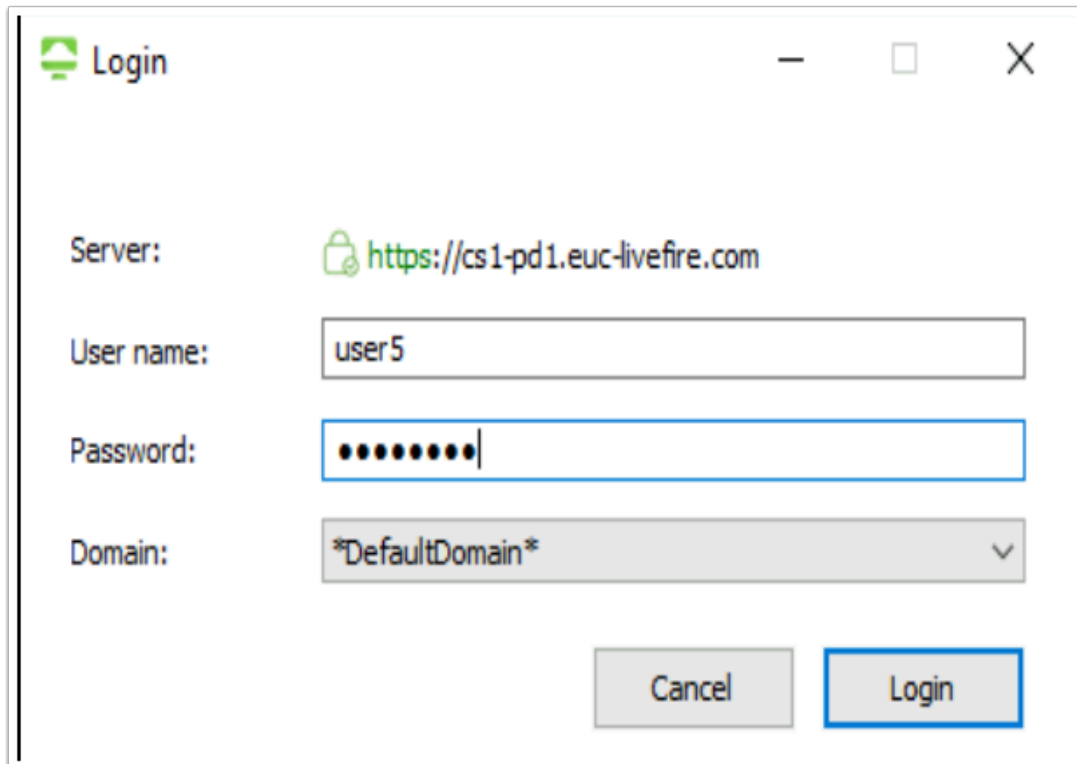
## PART 6: Testing Application Block with VMware Dynamic Environment Manager




1. On your **ControlCenter2** server desktop



- Launch your **Horizon Client**
- Select your Horizon POD **cs1-pd1.euc-livefire.com**



Login

Server:  <https://cs1-pd1.euc-livefire.com>

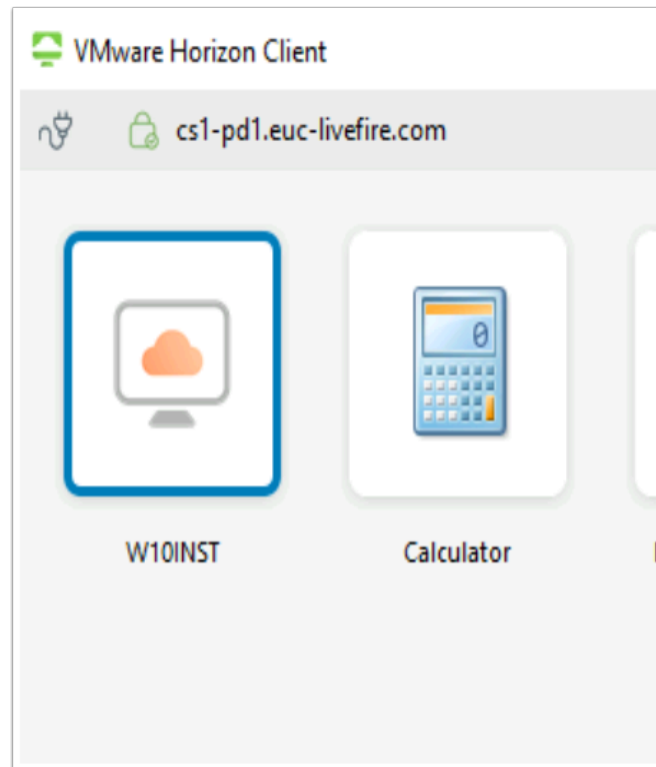
User name:

Password:

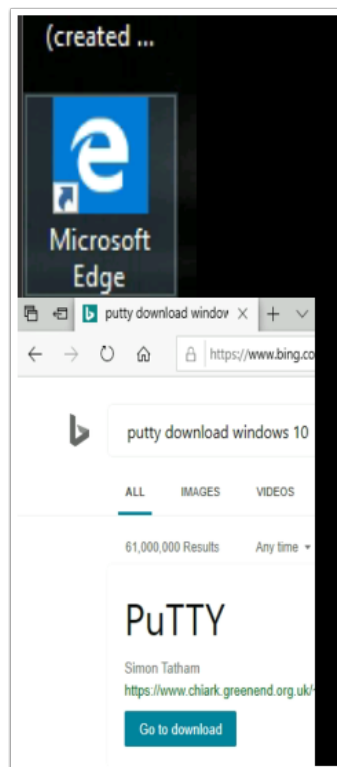
Domain:

Cancel Login

2. In the Horizon Client login window
  - Next to **User name:** login as **user5**
  - Next to **Password:** **VMware1!**
  - Select **Login**

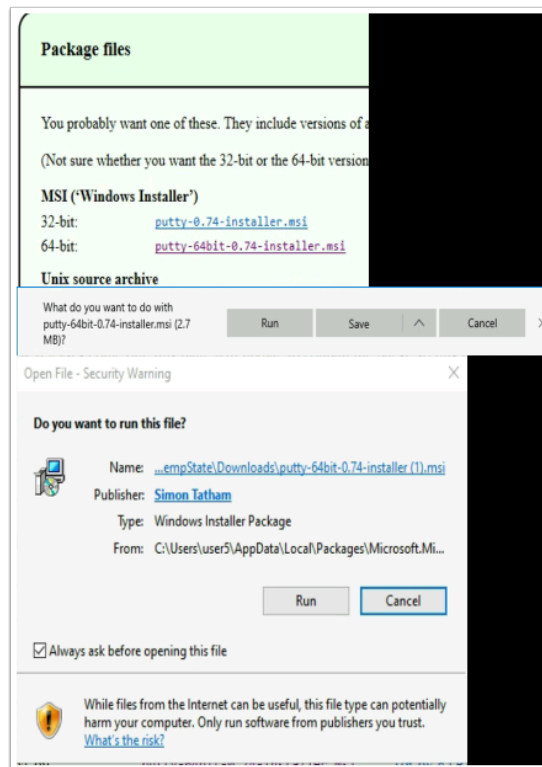


3. In the VMware Horizon Client
  - Select your **W10INST** desktop entitlement
  - Wait for the Desktop session to load

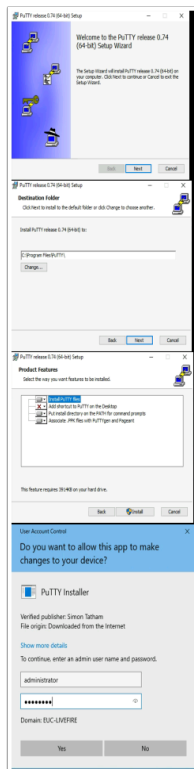


4. On your **VMware Horizon Client** session

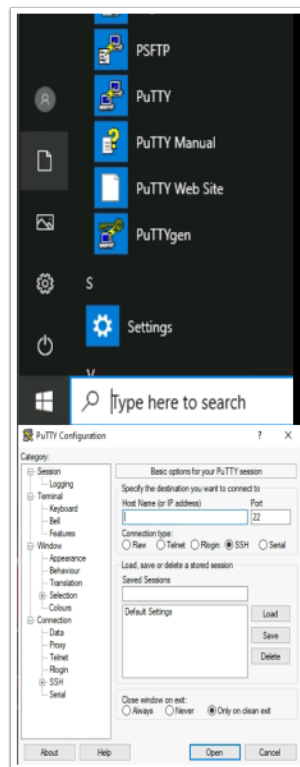
- On your Desktop, launch the **Microsoft Edge Browser**
- Type **Putty download windows 10**
  - In the search results select **Go to download**



5. On your **VMware Horizon Client** session
  - Next to **64bit** , select the **putty-64bit-xxxx-installer.msi**
  - When prompted, **what do you want to do...** select **Run >**

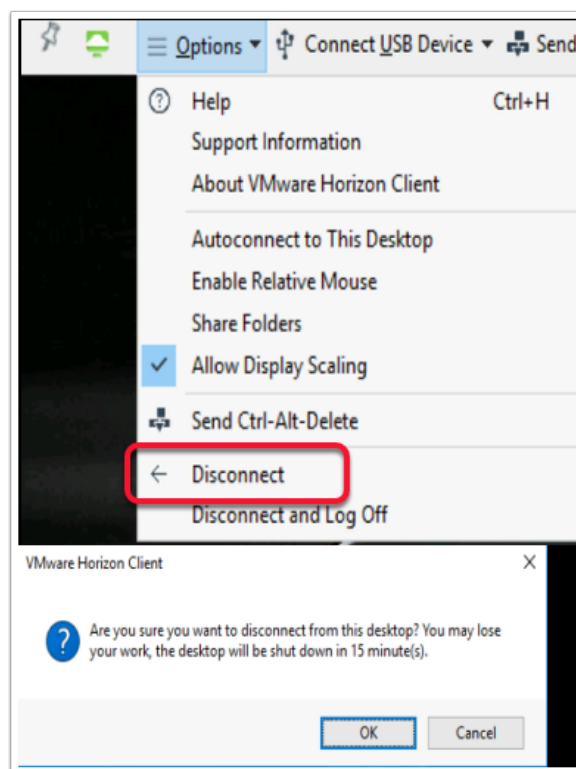


6. On your **VMware Horizon Client** session
  - In the **PuTTY** setup window
    - Select **Next** > **Next** > **Install**
    - When prompted in **User Account Control**
      - In **User name** type **Administrator**
      - In the **Password** type **VMware1!**
      - Select **Yes**
  - Select **Finish**



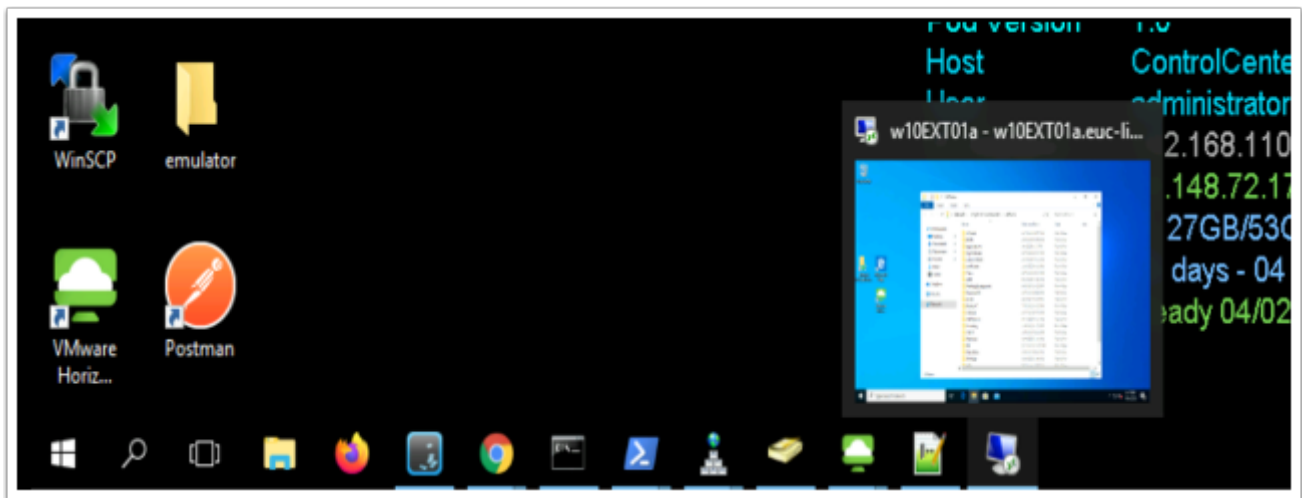
7. On your **VMware Horizon Client** session

- Select the **START** button > **scroll to P** > Expand the **Putty Folder** > Launch **Putty**
- Notice you have your **PuTTY Configuration** window
- Click **Cancel** to close the window **(very important)**



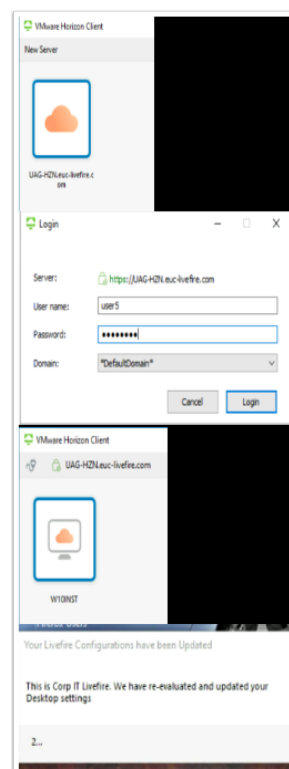
8. On your **VMware Horizon Client** session

- Next to **Options**, select the **dropdown**
- Select **Disconnect**
- Select **OK** to close the **VMware Horizon Client** window



9. On your ControlCenter2 Desktop

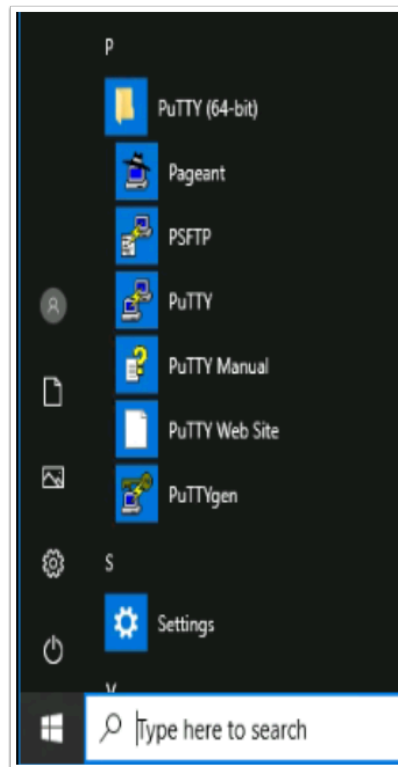
- Select your your **W10EXT01a.rdp** session
  - (If this session has closed, go to your Remote Desktop folder and launch the W10Ext01a.rdp and login as Administrator and password VMware1!)



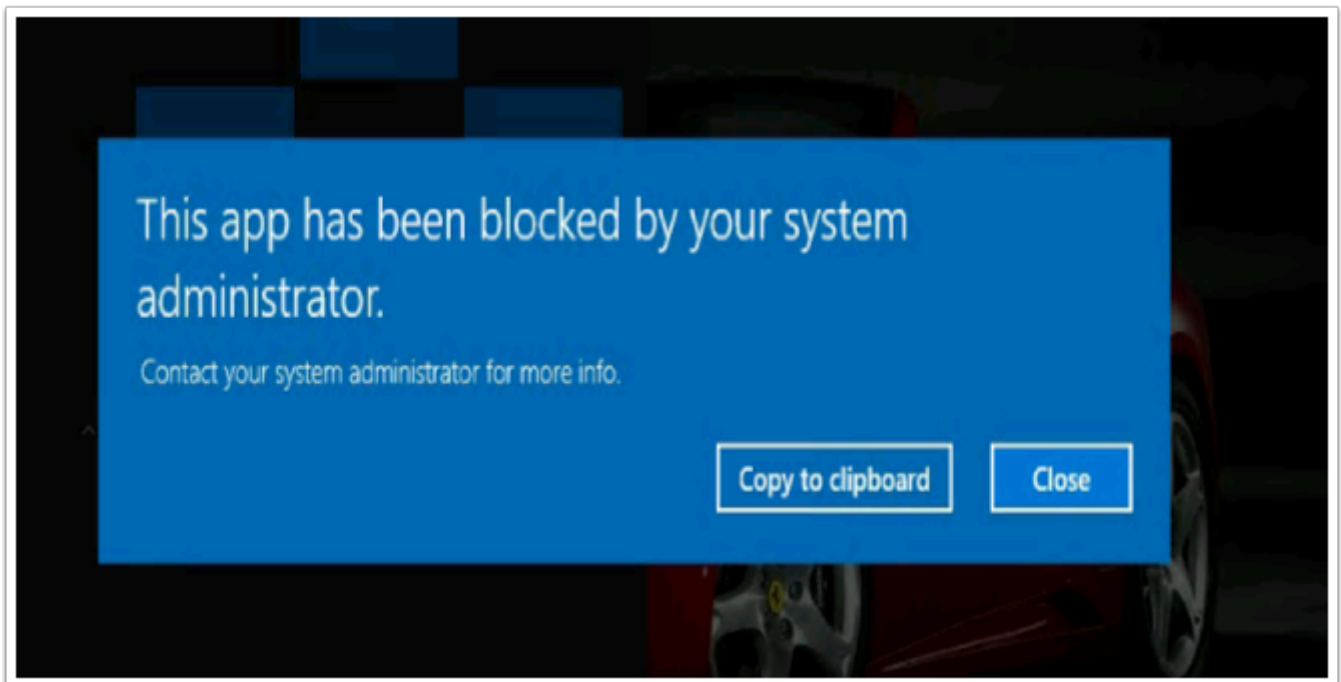
10. On your **W10Ext01a.RDP** session

- Launch your **Horizon Client**
  - Connect via your external Gateway, **UAG-HZN.euc-livefire.com**
  - Login as **User5**

- Password **VMware1!**
- Select your **W10INST** desktop Entitlement
  - Notice the prompt that your **Desktop settings** have been **re-evaluated**

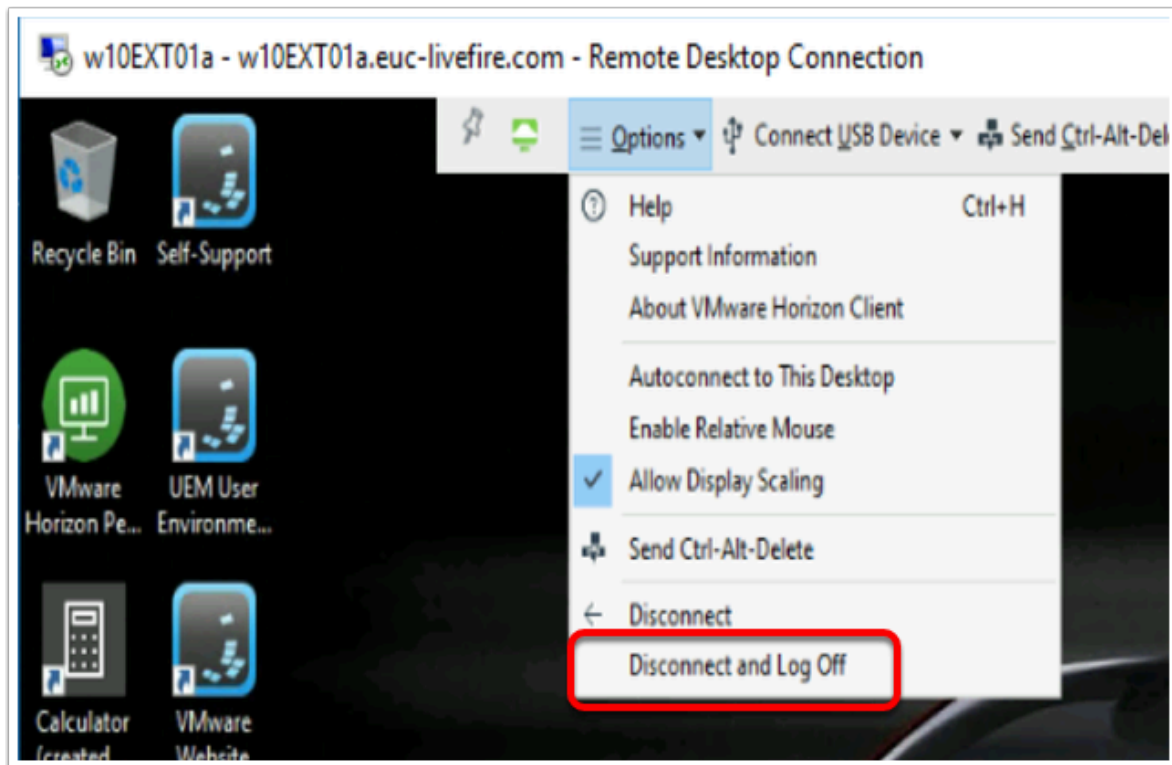


11. In the W10INST Horizon client session on W10EXT01a
  - Select your **START Menu** > Expand the **Putty folder** > Select **Putty**



12. In the W10INST Horizon client session on W10EXT01a

- Notice your App has been blocked, using a combination of App Blocking and Horizon Smart Policies
- Select **Close** to close the App Block message window



13. On the **W10EXT01a** desktop

- Switch back to your **Horizon Client** session
- Select the **drop down**, next to **Options**, select **Disconnect and Log Off**



# Day 5

# Integration of ThinApp Packages with VMware App Volumes and VMware Dynamic Environment Manager

## Overview

- The following are tasks you will have to complete to ensure you understand the base platform and requirements to be in place to perform successful ThinAPP captures.

## Pre-lab tasks (to validate)

Accounts for all resources are administrator for local access and **administrator@euc-livefire.com** for domain access

Password for ALL accounts is **VMware1!**

## Virtual Machine roles

### 1. On the ControlCenter2 server,

- Open your **Chrome Browser** and select the **vCenter** icon.
  - Log in as **Administrator**
  - Password **VMware1!**

### 2. For VMware ThinAPP

- **PackagingVM**. This the VM we use to do our install **VMware Thinapp**
- **CaptureVM**. This the VM we refer to as a **Clean VM**. We perform our ThinApp captures on this VM
- **W10Parent01a**. This VM will be our TEST best for validating the package Capture.

### 3. For VMware Dynamic Environment Manager

- **ControlCenter2**
  - Location of the Configuration and Profile shares
  - Domain Controller configured AD templates on the Corp OU
- **DemProfiler** -
  - Application Profiler captures on this machine

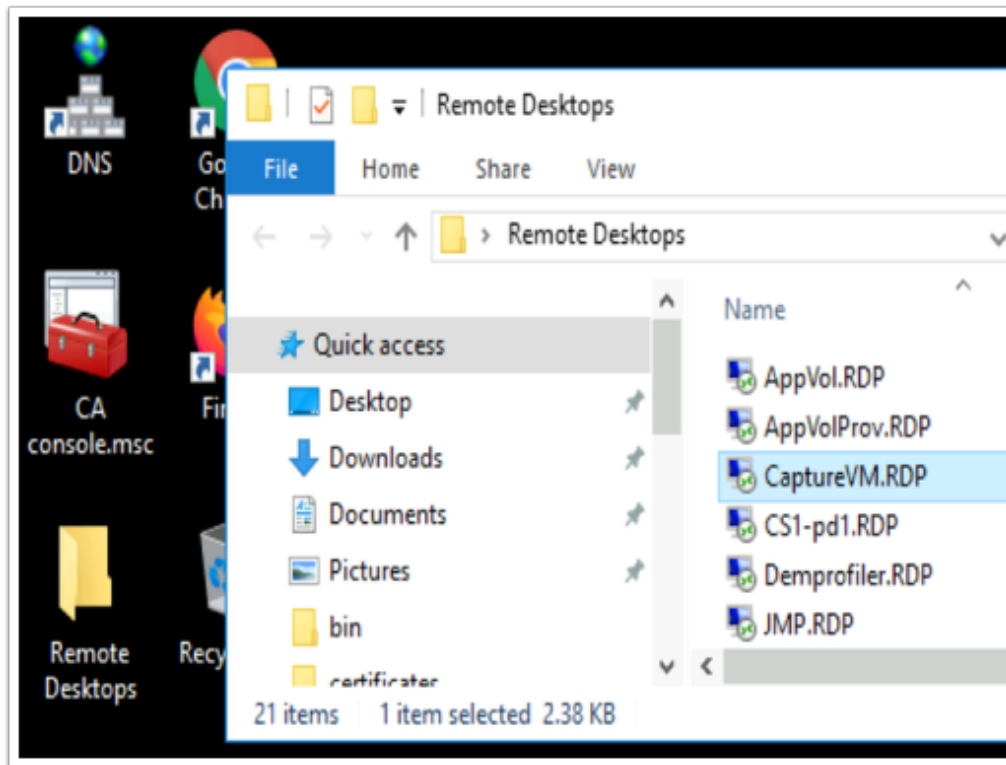
### 4. For VMware App Volumes

- **AppVol.euc-livefire.com**.
  - App Volumes Manager Sever
- **AppVolProv**

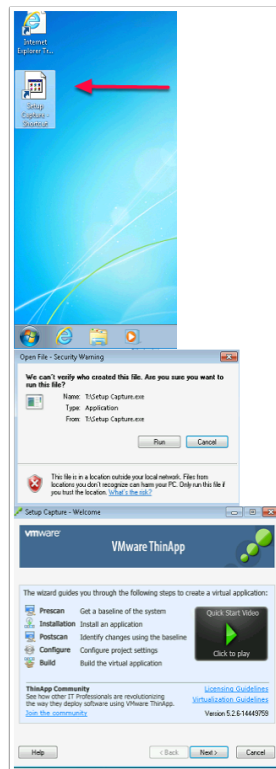
- App Volumes Provisioning Machine

5. Ensure that your **W10Parent-01a** and **AppVolProv** have been **reverted to Snapshot**
  - After revert to current snapshot has completed, **Power on** both your VM's

## Part 1. Deploying VMware ThinApp

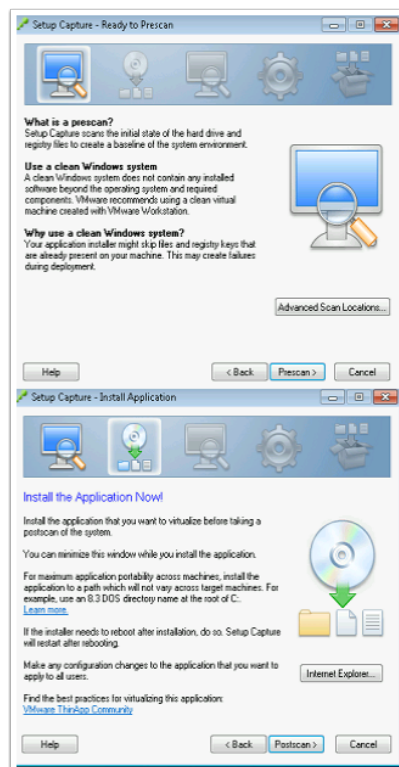


1. On your ControlCenter2 Desktop
  - Open your **Remote desktops** folder
  - Launch the **CaptureVM.RDP** shortcut



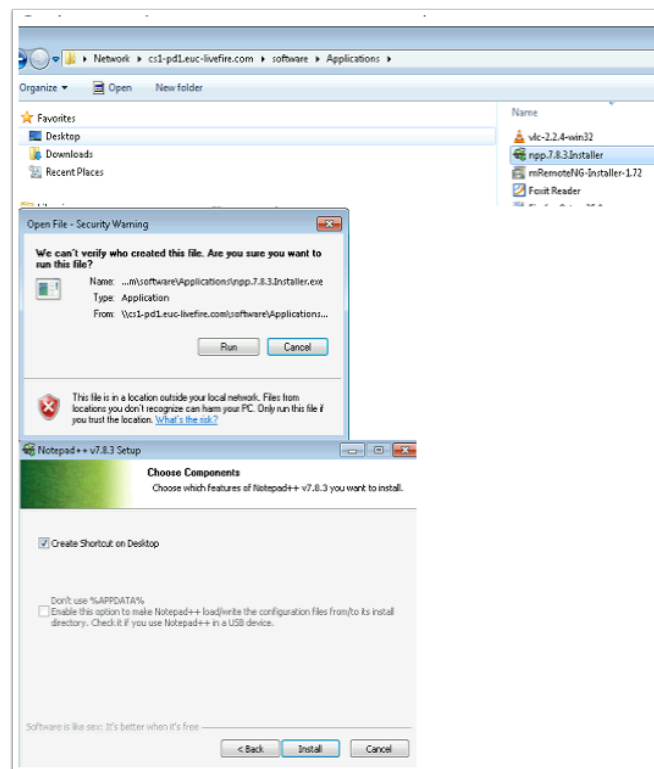
## 2. On the CaptureVM Desktop

- Double-click the short-cut to **SetupCapture.exe**
- Select **Run**
- On the **Setup Capture - Welcome** select **Next**

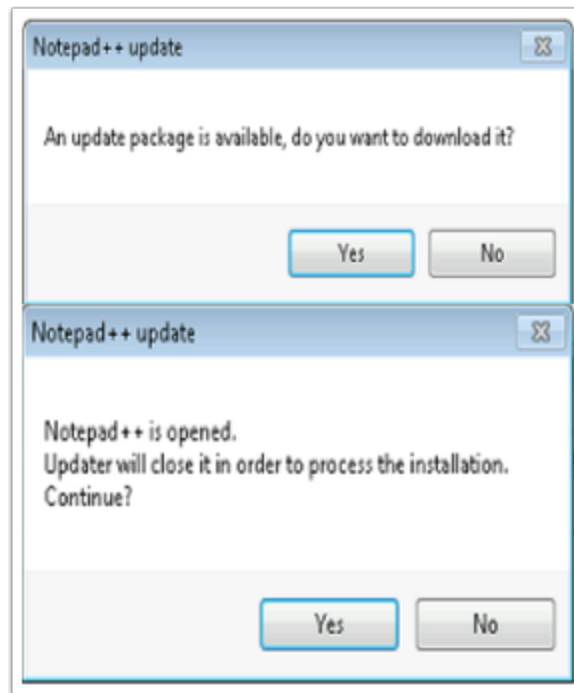


## 3. On the **Setup Capture - Ready to Prescan**

- Select **Prescan** (wait for Pre-Scan to complete)
- On the **Setup Capture - Install Application** window
  - Select the **Software** shortcut on your Desktop and go to **Applications**

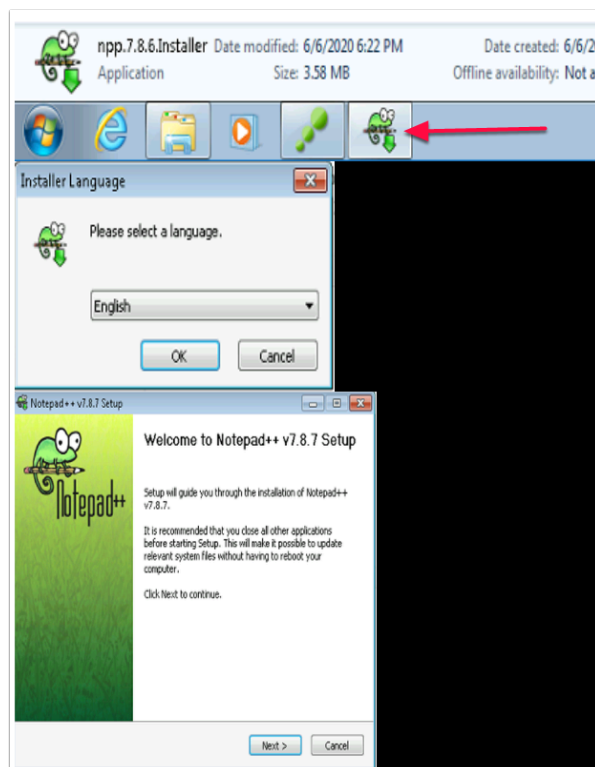


4. Select your **Notepad++ installer** and **Open**
  - Select **Run**
  - Select **Ok > Next > I Agree > Next > Next >**
  - Select the **Create Shortcut on Desktop** checkbox select **Install**
  - Select **Finish**
  - Close the **Notepad++** application and **File Explorer** window



5. On the Notepad++ Update window

- Select **Yes**
- Select **Yes**, to close the existing session of Notepad++



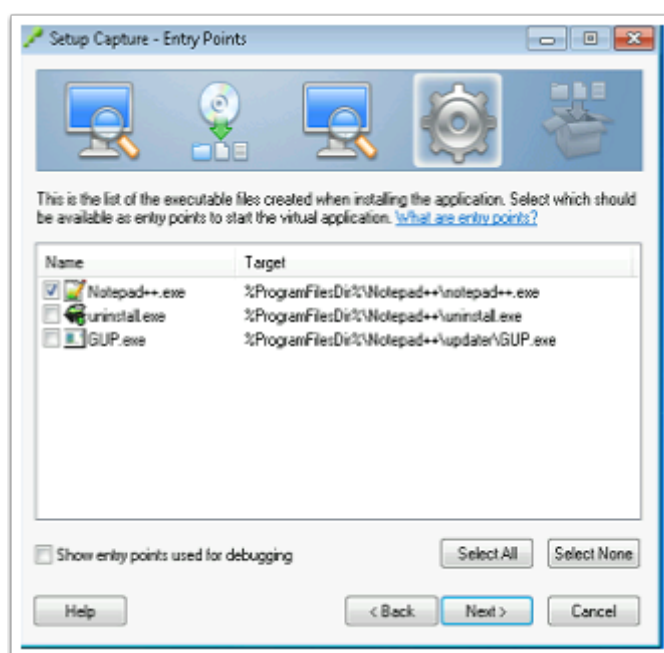
6. On your CaptureVM

- Select the **Frog icon** on the **Taskbar**
- On the **Installer Language** window, Select OK

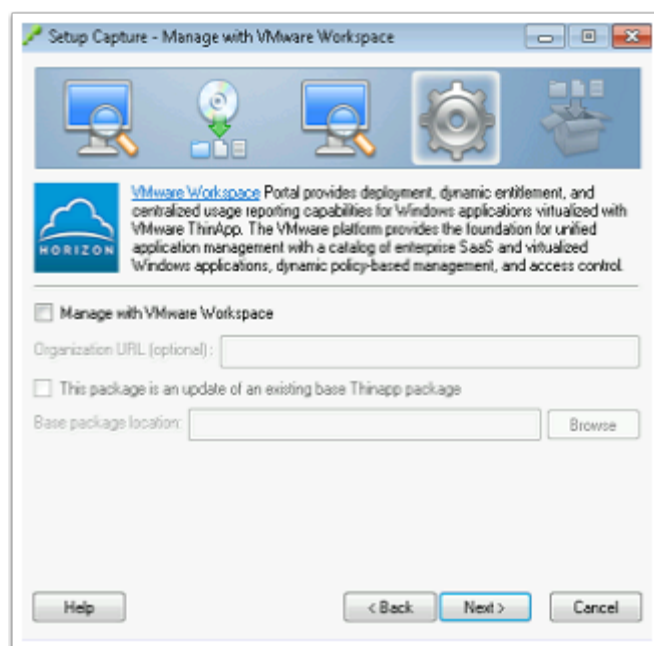
- On the Welcome to **Notepad++ v7.x.x Setup**, select **Next** > **I Agree** > **Next** > **Next** > **Install** > **Finish**
- With the exception of the **Setup Capture - Installation** window.
  - **Close all Windows** including the **Notepad++** window.



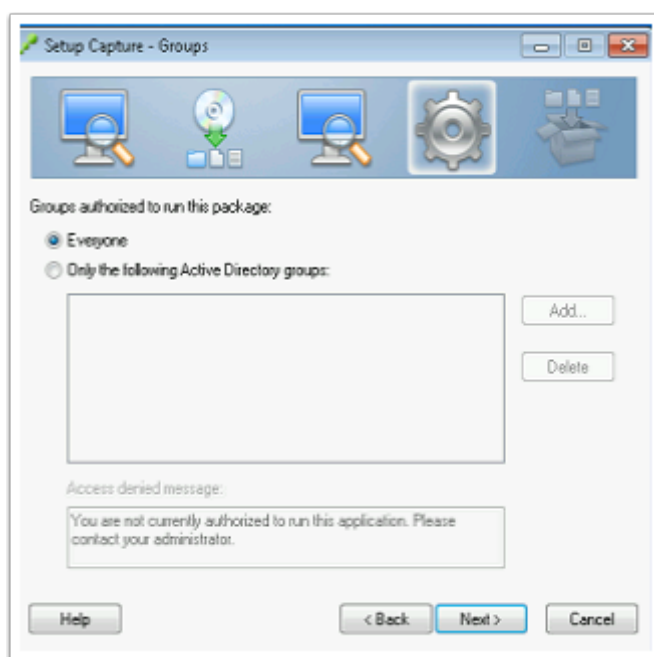
7. On the **Setup Capture - Installation** window.
  - Select **Postscan** select **OK**



8. On the **Setup Capture - Entry Points** window
  - Select **Next**

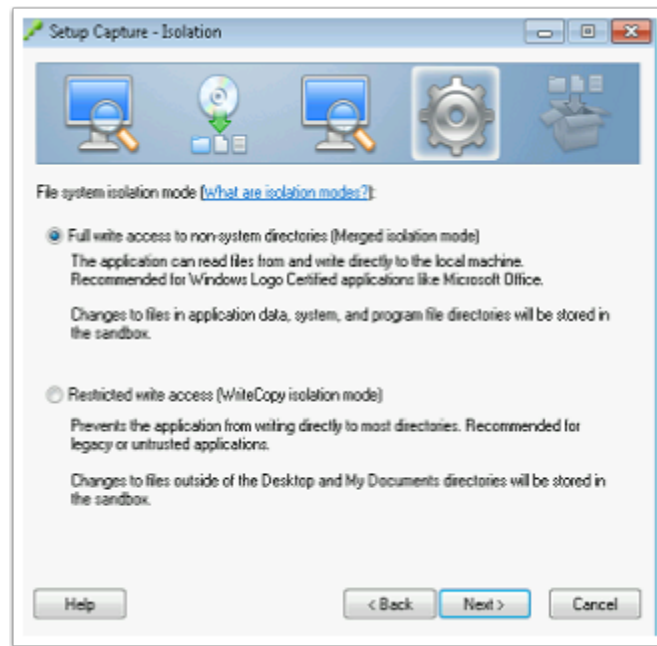


9. On the **Setup Capture - Manage with Workspace** window
  - Select **Next**

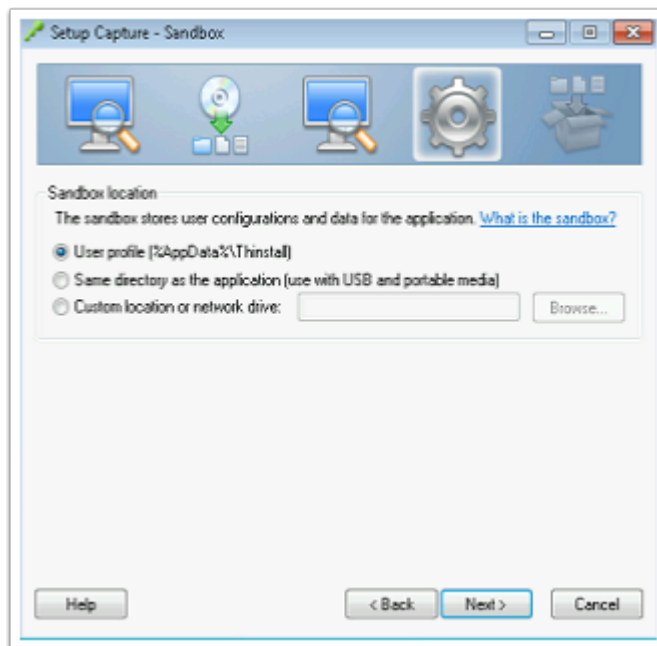


10. On the **Setup Capture - Groups** window
  - Select **Next**

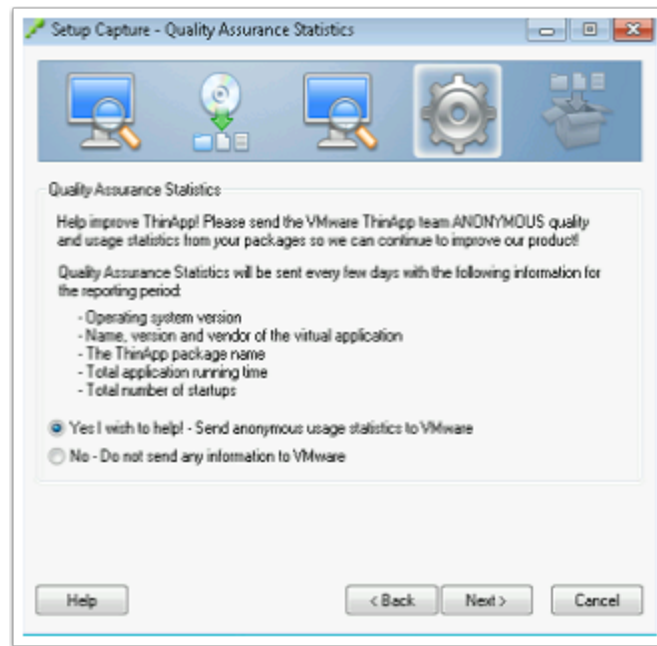




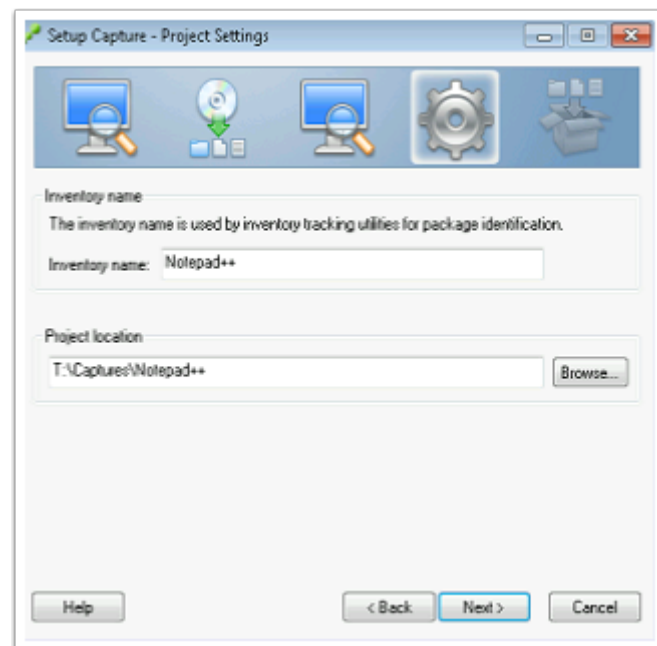
11. On the **Setup Capture - Isolation** window
- Select **Next**



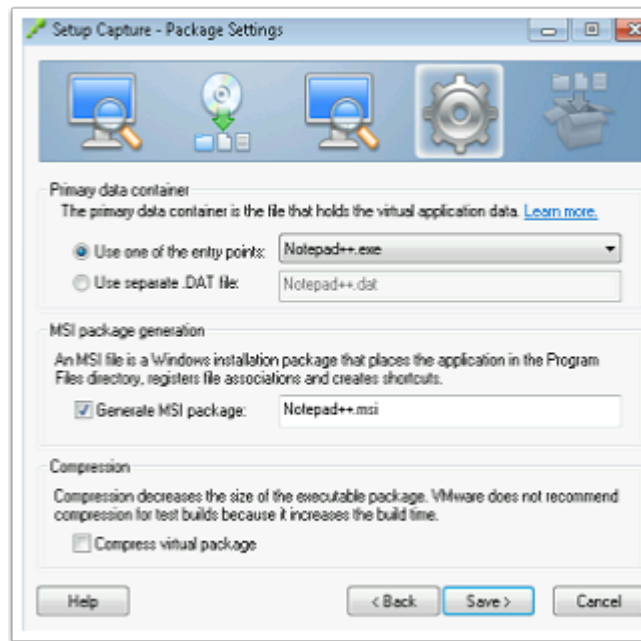
12. On the **Setup Capture - Sandbox** window
- Select **Next**



13. On the **Setup Capture - Quality Assurance Statistics** window
- Select **Next**

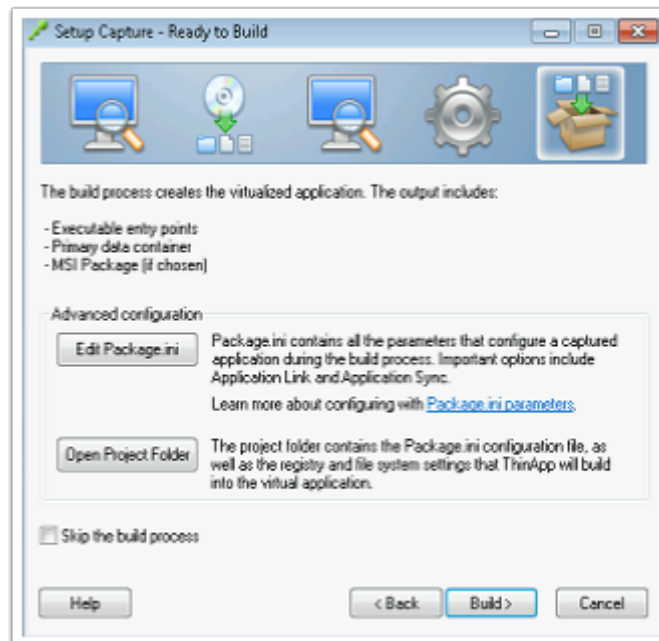


14. On the **Setup Capture - Project Settings** window
- Select **Next**



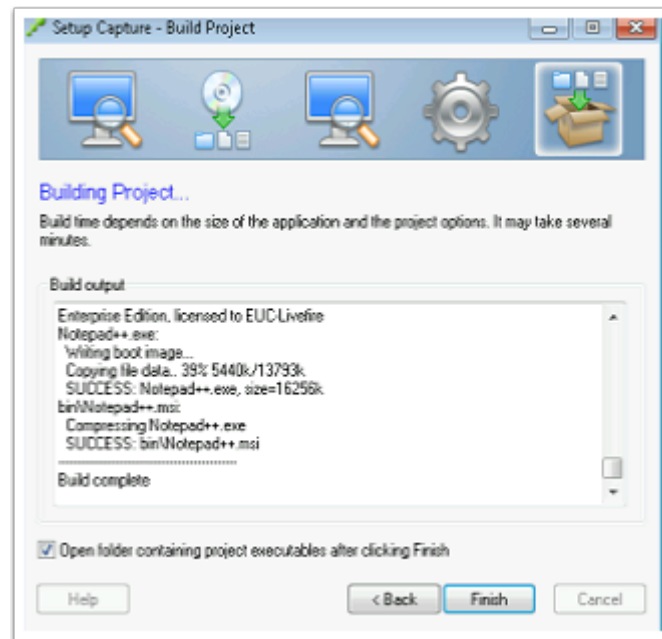
15. On the **Setup Capture - Package Settings** window

- Select the **Generate MSI package** check box
- Select **Save**



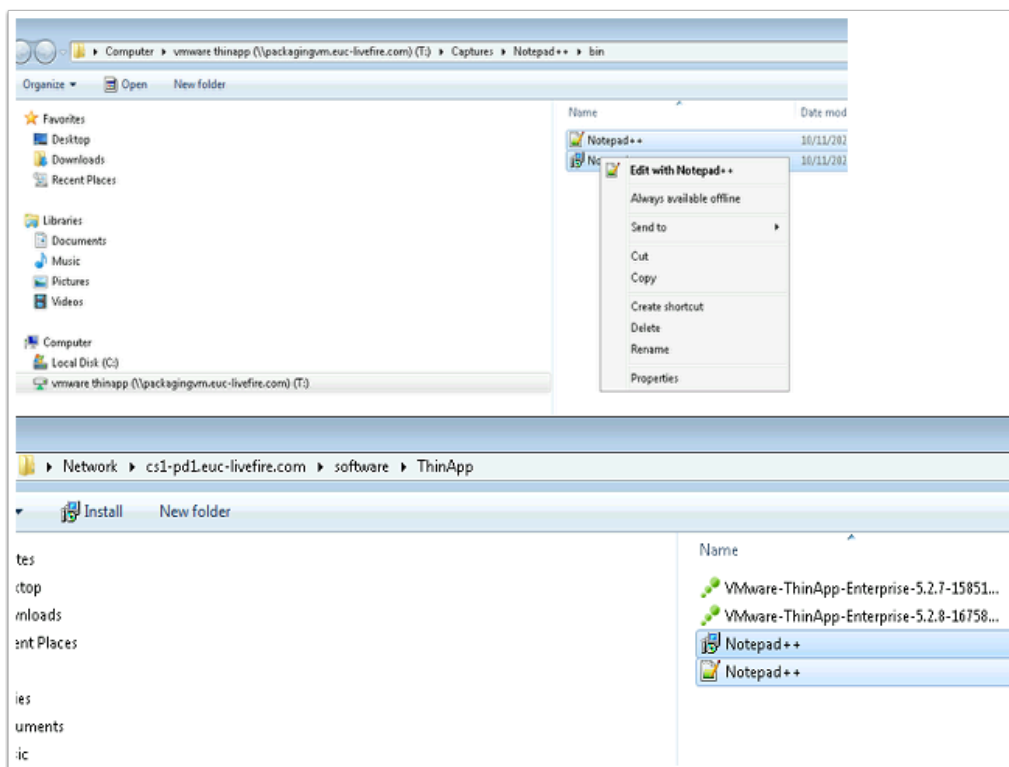
16. On the **Setup Capture - Ready to Build** window

- Select **Build**



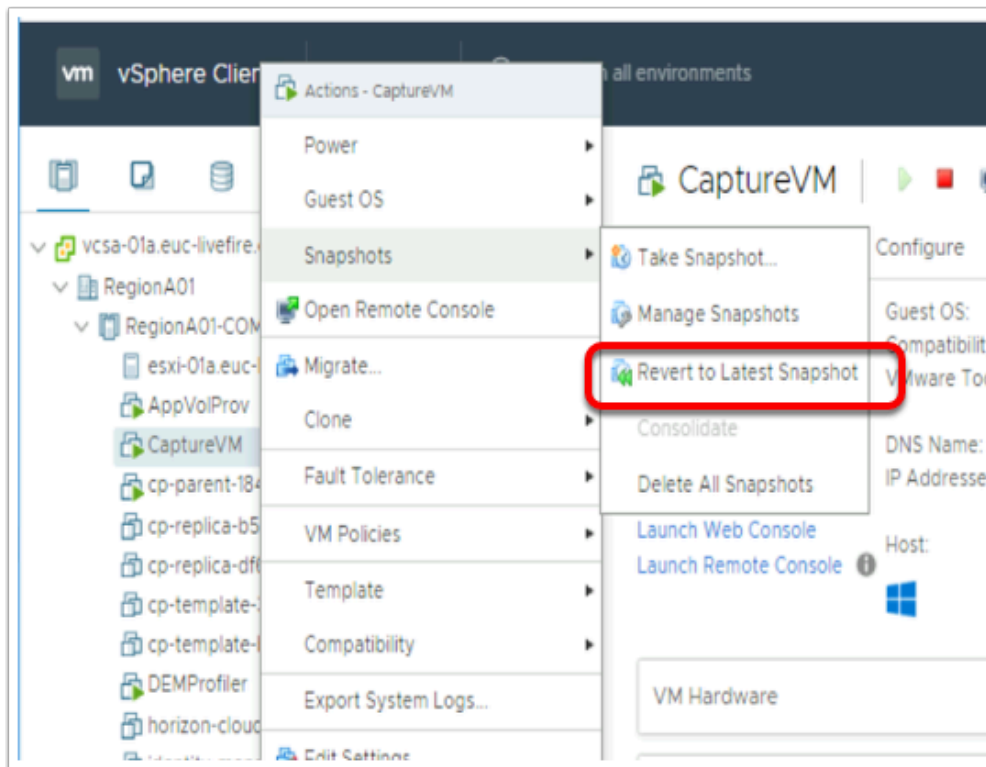
17. On the **Setup Capture - Build Project** window

- Select **Finish**



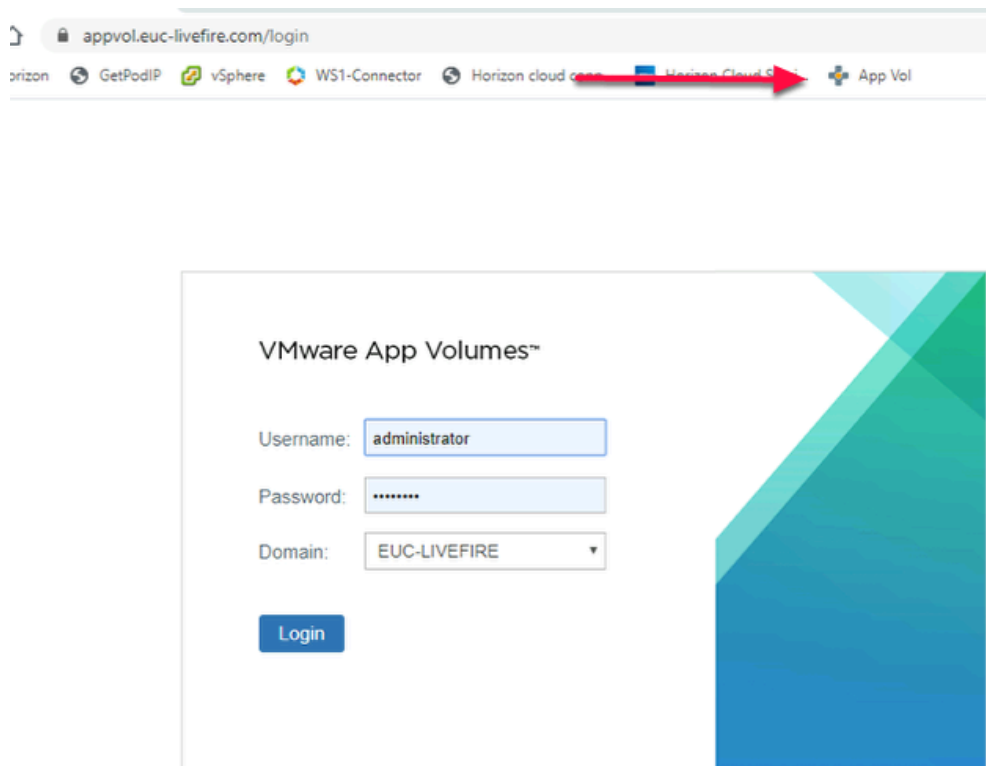
18. Notice your File Explorer window has automatically launched

- Observe where the **.msi** and **.exe** have been saved
- Notice that the UNC path points to the **BIN** folder on your **Packaging** machine
- **Copy** the **Notepad++ msi** and **.exe**
- Select and open the **software** folder on the **Capture VM Desktop**
- Save the Files to the **ThinApp** folder



19. On the Controlcenter2 server Desktop
  - Revert to your **Chrome browser, vCenter** server session.
  - In the **Hosts and Clusters** Inventory
    - Select your **CaptureVM**
    - Right-Click the **CaptureVM** > select **Snapshots** > **Revert to Latest Snapshot**

## Part 2. Integration of Horizon with ThinApp and App Volumes



1. On your **ControlCenter2** desktop
  - Open the **Chrome browser** in Favourites, select the **App Vol** shortcut,
  - **Login** as **Administrator** with password **VMware1!**



2. Select **INVENTORY** > **Applications** select **Create**

VMware App Volumes™ EUC-LIVEFIRE\Administrator Login

INVENTORY VOLUMES (2.X) DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

Applications Packages Programs Assignments Attachments Writables

### Create Application

An Application will provide an Application Owner the ability to manage the lifecycle of its Packages.

Name:

Description:

Owner: EUC-LIVEFIRE\Administrator

Package: ☒ Create a Package

Confirm Create Application

Create Application NotePad++?

3. On the **Create Application** page,
  - In the **Name** section type **NotePad++** , select **Create**
  - In the **Confirm Create Application** window, accept the default and select **Create**

INVENTORY DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

Applications Packages Programs Assignments Attachments Writables

### Create Package for notepad++

Provides an Application Owner the ability to create a Package for the Application

Name:

Base Package:

Storage:

Path:

Template:

Stage:

Description:

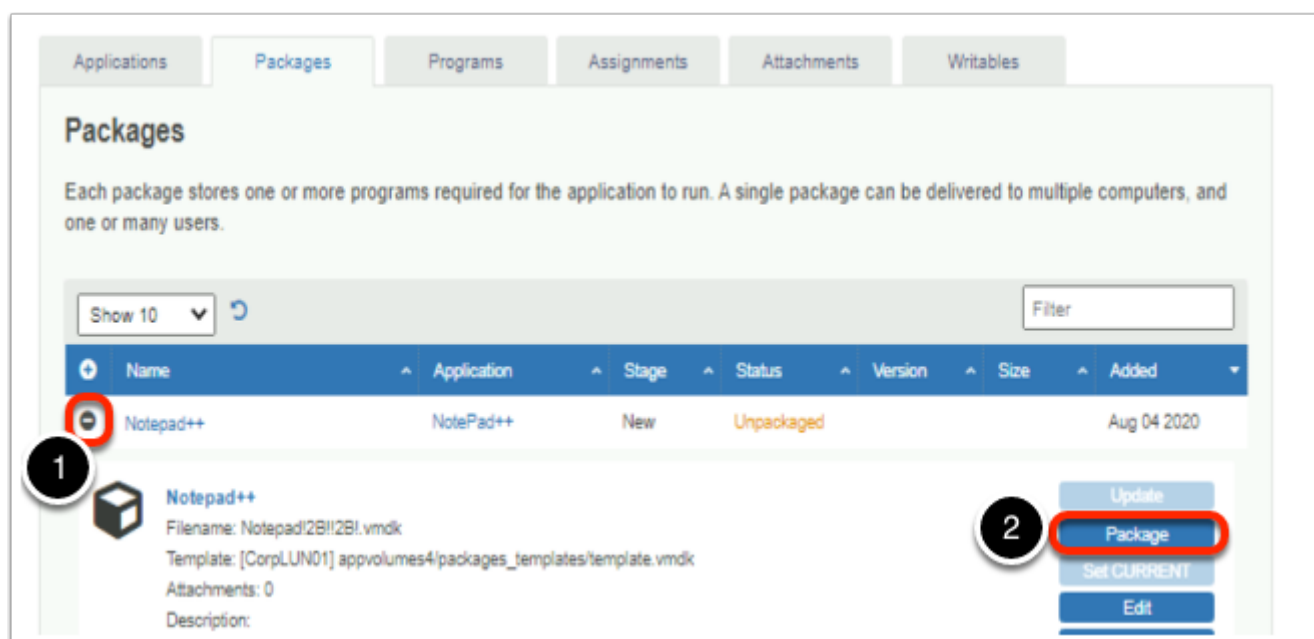
Confirm Create Package

Create Package notepad++ for notepad++ on datastore CorpLUN01 at path appvolumes4/packages?

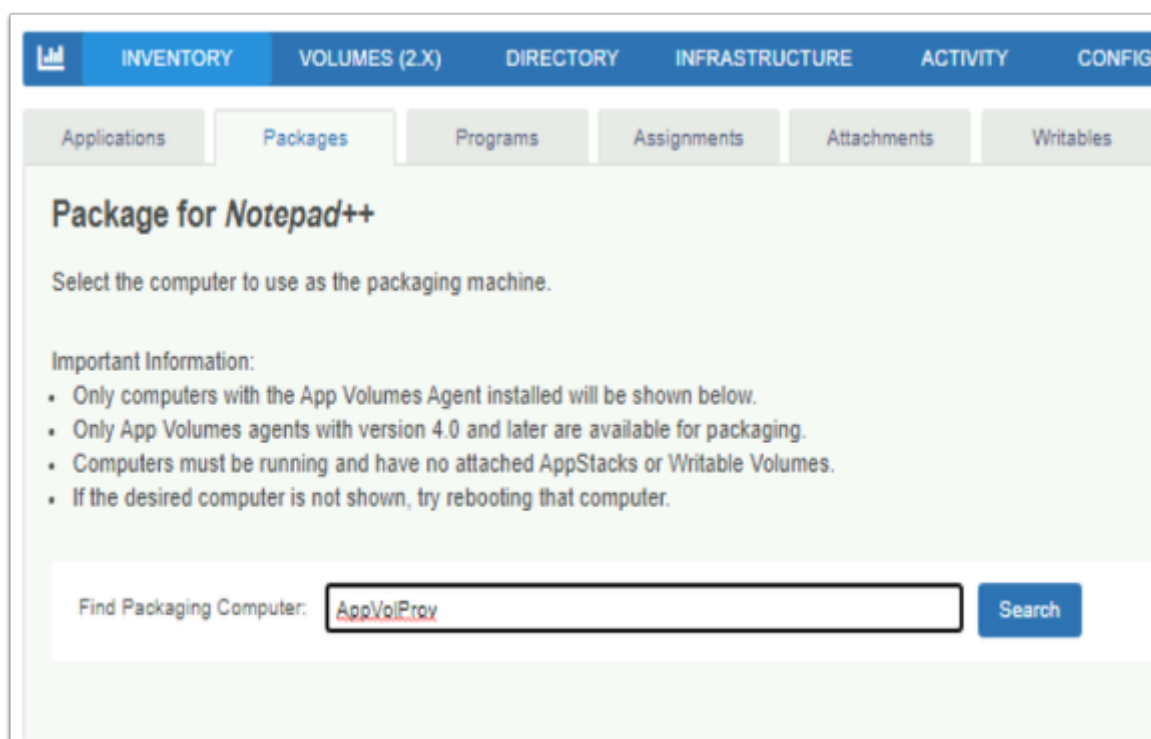
☒ Perform in the background  
☐ Wait for completion

4. The packages tab has automatically opened, for you to create a package for your application.

- in the Name field type **Notepad ++**
- Click **Create**
- On the **Confirm Create package** click **Create**

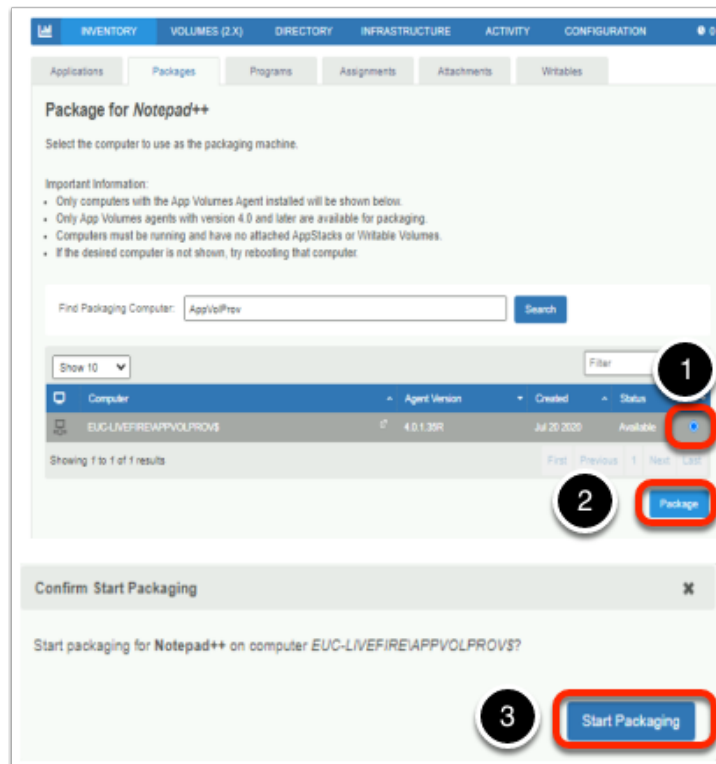


5. Select the **Packages** Tab
  - Expand the + next to **Notepad++**
  - Select **Package**

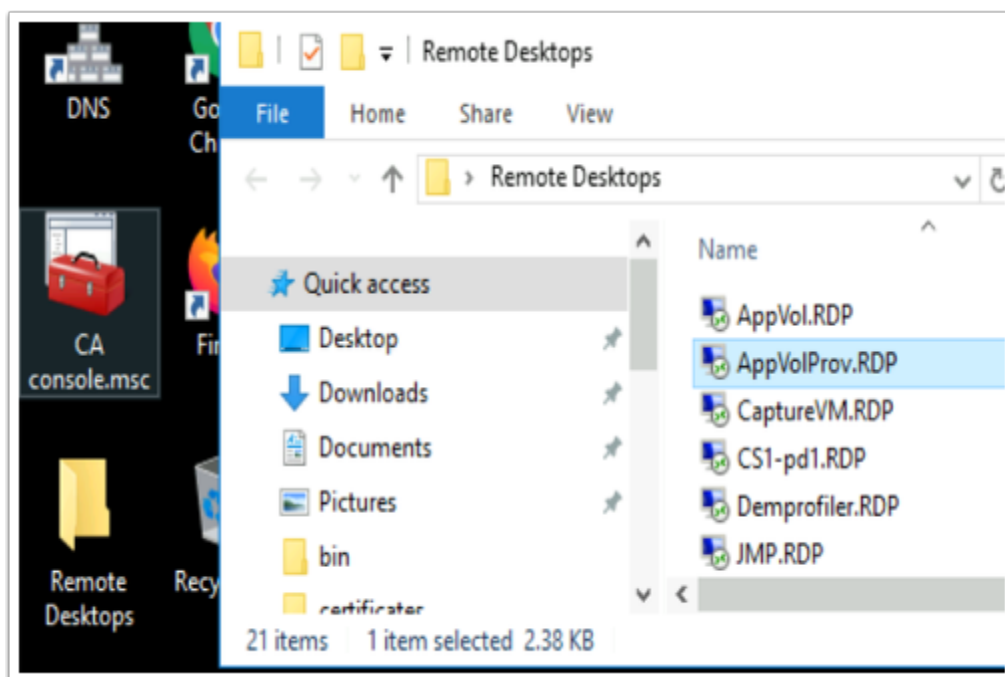


6. On the **Package for Notepad++** window
  - Next to **Find Packaging Computer:** type **AppVolProv**
  - Select **Search**



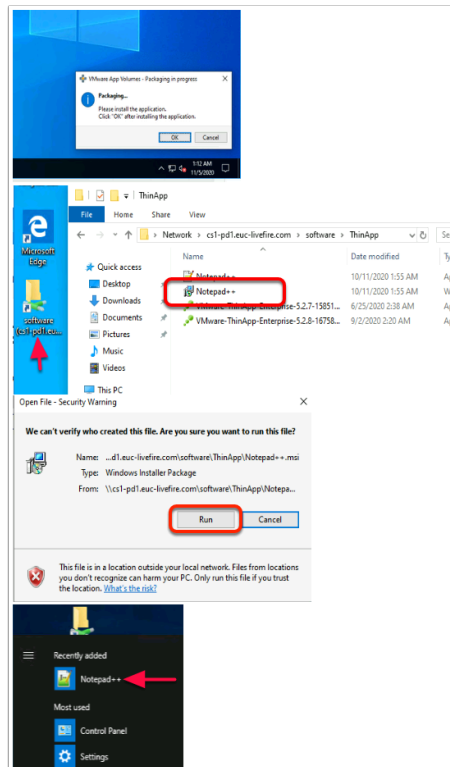


7. On the **Package for Notepad++** window
  - Select **radio button** next to **EUC-Livefire\AppVolProv**
  - Select **Package**
  - On the **Confirm Start Packaging**, select **Start Packaging**



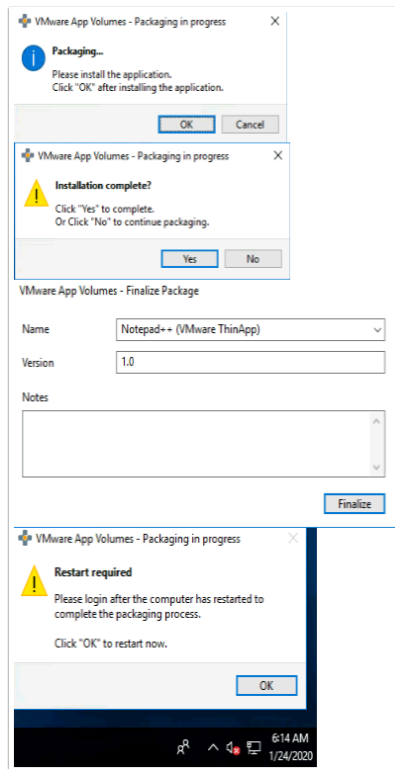
8. On your **ControlCenter2** Desktop
  - Open the **Remote Desktops** folder and launch the **AppVolprov.RDP** shortcut
  - You should automatically be logged in

- Username **administrator@euc-livewire.com**
- Password **VMware1!**



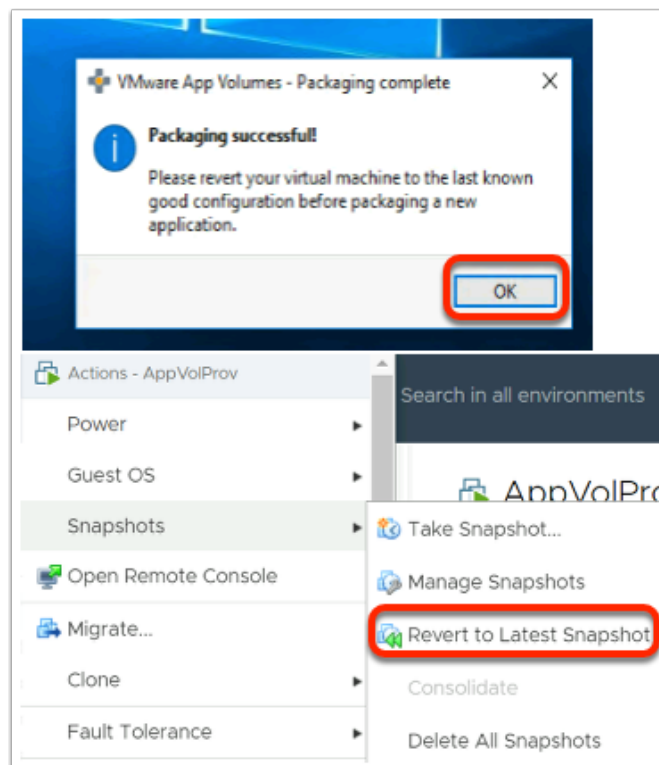
#### 9. On the **AppVolProv** desktop

- Notice you have a prompt, on the Taskbar, **VMware App Volumes - Packaging in Progress**
- Select the **Software** folder, Select open the **ThinApp** folder.
- Select and right-click the **Notepad++ .msi** installer and select **Run**
- Select **Start** and right at the top of Application menu next to **Recently added** select **Notepad++**
- Launch **Notepad++** , **Close Notepad++**
- **Reopen** and **Close Notepad++**
- **Close** the **File Explorer** window

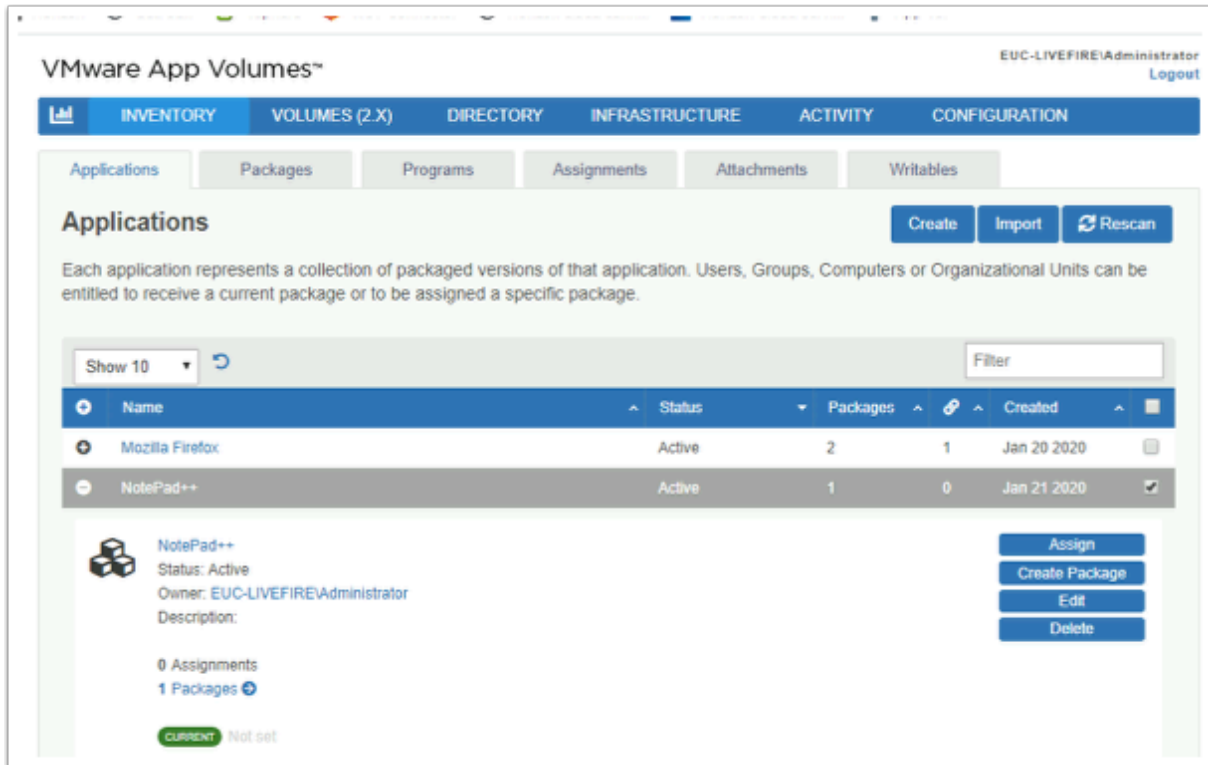


10. On the **AppVolProv** machine

- On the **VMware App Volumes- Packaging in progress** window select **OK**
- On **Installation Complete?** select **Yes**
- On the **Finalize Package** window select **Finalize**
- On the **Restart Required** window select **OK**



11. From the ControlCenter2 server desktop
  - Launch your **APPVolProv.RDP** virtual machine session
  - On the **Packaging** successful window select **OK**
  - In vCenter **Revert** your AppVolProv virtual machine Snapshot



12. From the ControlCenter2 server desktop
  - Go to your **Chrome Browser**, and select your **App Volumes Manager Admin** console session
  - In the **INVENTORY** > **Applications** expand **Notepad++**
  - Select **Assign**

Search Active Directory for entities to assign to this Application.

Domain:

Search Active Directory:

☐ Search all domains in the Active Directory forest

Show 10

| Entity                         | Name      | Status    |                                     |
|--------------------------------|-----------|-----------|-------------------------------------|
| EUC-LIVEFIRE OU-Marketing.Corp | Marketing | Available | <input type="checkbox"/>            |
| EUC-LIVEFIRE\Marketing         | Marketing | Available | <input checked="" type="checkbox"/> |

Showing 1 to 2 of 2 results [First](#) [Previous](#) [1](#) [Next](#) [Last](#)

Entities:

Assignment Type: ☒ Marker ☐ Package

Markers:

| Marker  | Package                                 | Stage | Added |                          |
|---------|---|-------|-------|--------------------------|
| Current | Marker is inactive until package is set |       |       | <input type="checkbox"/> |

- On the **Assign Application: Notepad++** window
  - Next to **Search Active Directory** type **Marketing**
  - Select **Search**
  - Select the **radio button** for **EUC-Livefire\Marketing**
  - Select **Assign**

Confirm Assign

Assign 1 entities to Application NotePad++?

• EUC-LIVEFIRE\Marketing

Show 10

| Name            | Status | Packages | Created |             |
|-----------------|--------|----------|---------|-------------|
| Mozilla Firefox | Active | 2        | 1       | Jan 20 2020 |
| NotePad++       | Active | 1        | 1       | Jan 21 2020 |

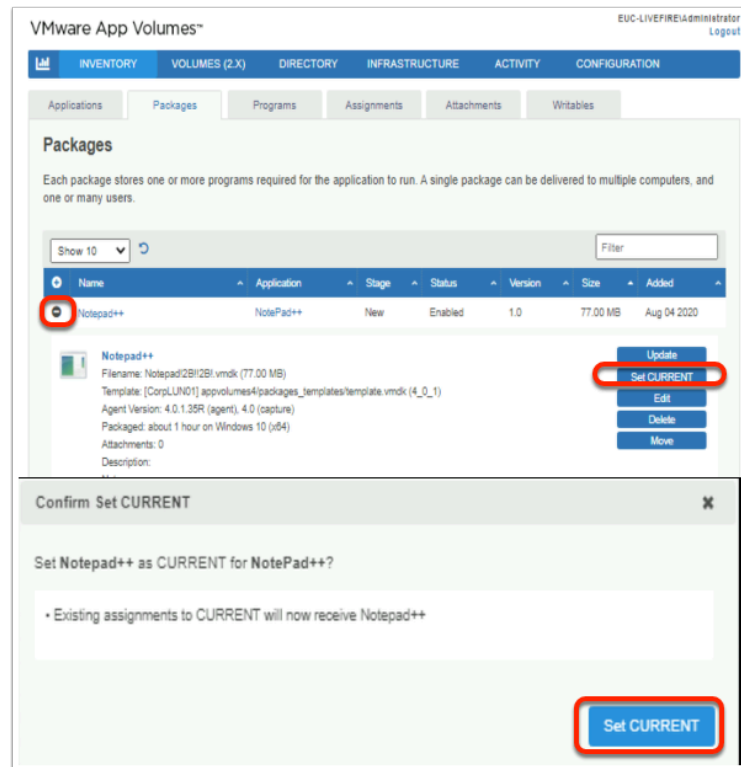
NotePad++  
Status: Active  
Owner: EUC-LIVEFIRE\Administrator  
Description:

1 Assignments [+](#)  
1 Packages [+](#)

**CURRENT** Not set

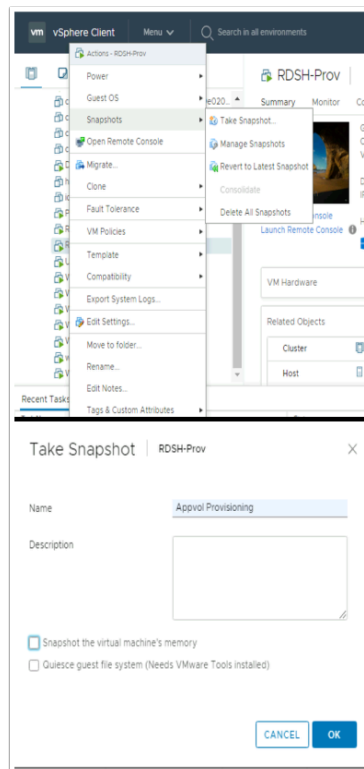
Showing 1 to 2 of 2 Applications [First](#) [Previous](#) [1](#) [Next](#) [Last](#)

14. On the **Assign Application: Notepad++** window
- On **Confirm Assign** select **Assign**
  - Review your Assignment for **NotePad++**

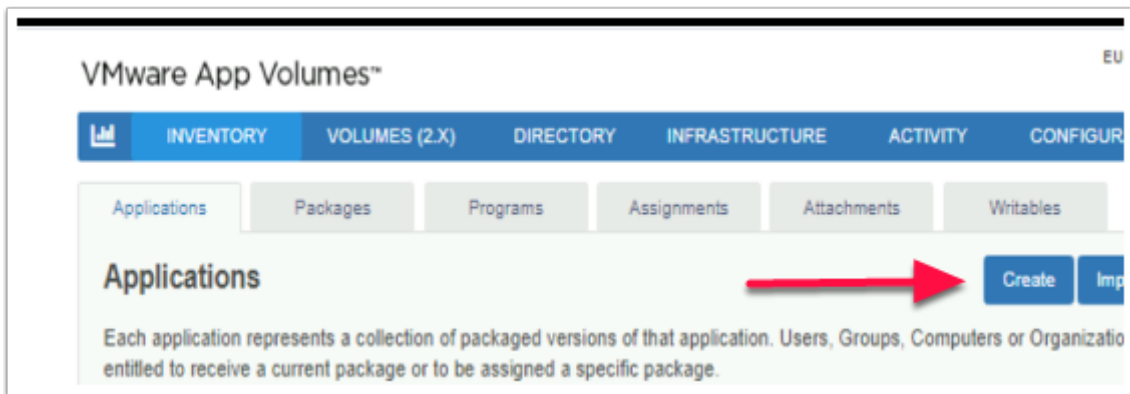


15. In the AppVolumes Manager Admin Console
- Select the **Packages** tab
  - Expand **Notepad++**
  - Select **Set CURRENT**

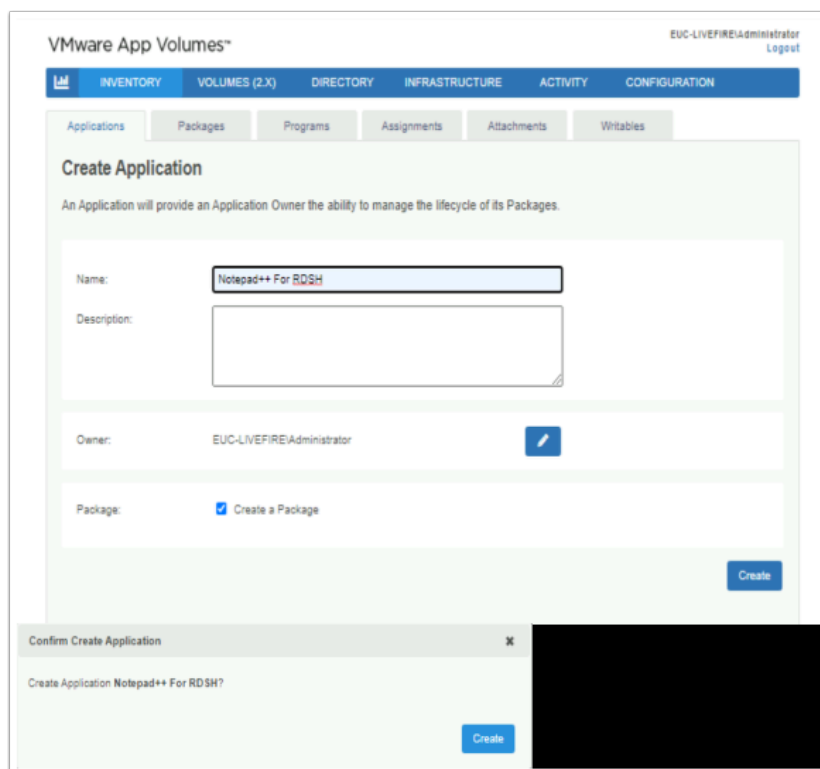
## Part 3 . Integrating and Configuring RDSH, with App Volumes in VMware Horizon



1. On your **ControlCenter2** server
  - Revert to your **vSphere client** session
    - If necessary, login with the following credentials
      - Username - **administrator**
      - Password - **VMware1!**
  - Select **RDSH-Prov** in the **Host and Clusters** Inventory
    - Right-Click **RDSH-Prov** and select **Snapshots** > **Take Snapshot**
  - In the **Take Snapshot** window
    - Next to **Name**, type **Appvol Provisioning**
    - Uncheck the **Snapshot the virtual Machine's memory**, **checkbox**
    - Select **OK**



2. On your App Volumes Manager Console
  - In Inventory Applications, select **Create**



3. In the **Create Application** window
  - Next to Name: , type **Notepad++ for RDSH**
  - Select **Create**
  - On the **Confirm Create Application** window, select **Create**



VMware App Volumes™ EUC-LIVEFIREAdministrator Logout

INVENTORY VOLUMES (2.X) DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

Applications Packages Programs Assignments Attachments Writables

### Create Package for Notepad++ For RDSH

Provides an Application Owner the ability to create a Package for the Application

Name:

Base Package:

Storage:

Path:

Template:

Stage:

Description:

---

**Confirm Create Package** ✕

Create Package Notepad++ For RDSH for Notepad++ For RDSH on datastore CorpLUN01 at path appvolumes4/packages?

☒ Perform in the background  
☐ Wait for completion

4. In the **Create Package for Notepad++ for RDSH** window
  - Next to Name: type **Notepad++ for RDSH**
  - Select **Create**
  - On the **Confirm Create Package** window, select **Create**

VMware App Volumes™

INVENTORY VOLUMES (2.X) DIRECTORY INFRASTRUCTURE ACTIVITY

Applications Packages Programs Assignments Attachments

## Packages

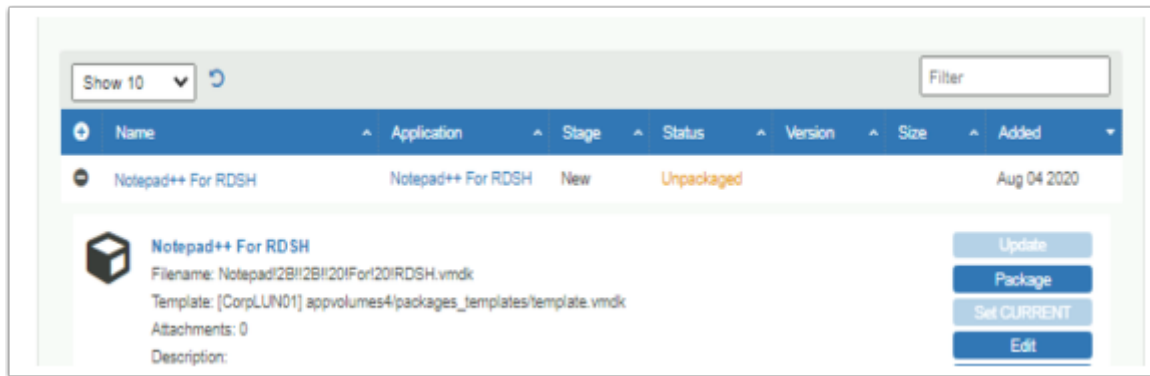
Each package stores one or more programs required for the application to run. A single package can one or many users.

Show 10

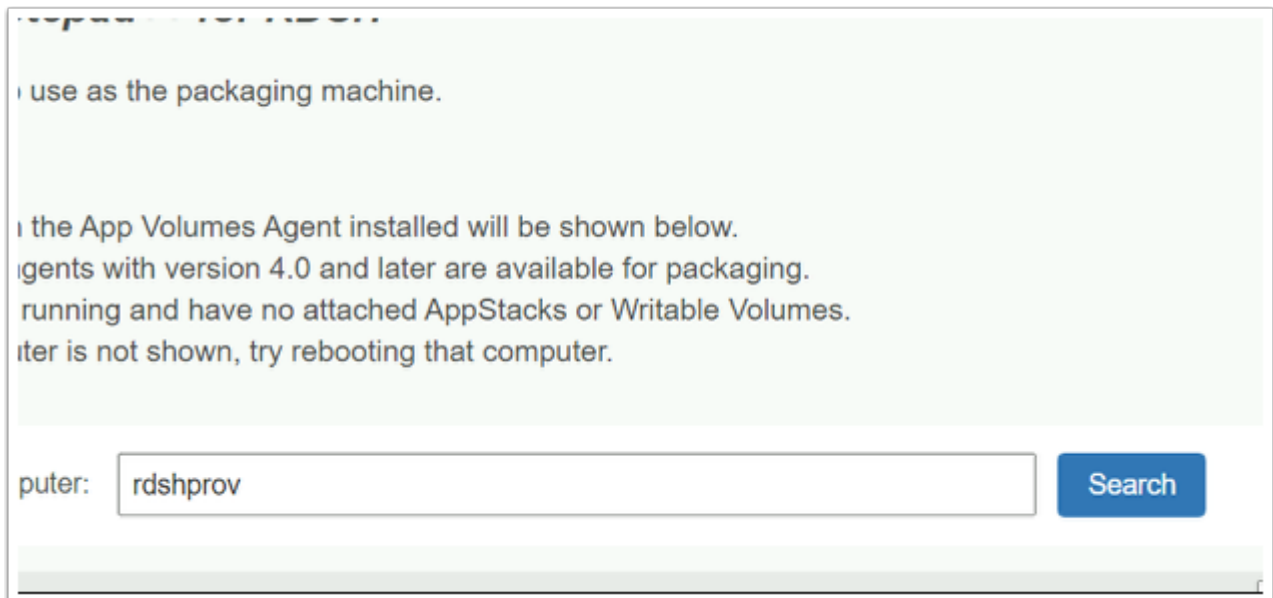
|   | Name                          | Application        | Stage | Status     | Ver  |
|---|-------------------------------|--------------------|-------|------------|------|
| + | Notepad++ For RDSH            | Notepad++ For RDSH | New   | Unpackaged |      |
| + | Notepad++ <b>CURRENT</b>      | NotePad++          | New   | Enabled    | 1.0  |
| + | FireFox Latest <b>CURRENT</b> | Mozilla Firefox    | New   | Enabled    | 78.1 |

5. On the App Volumes Manager Console

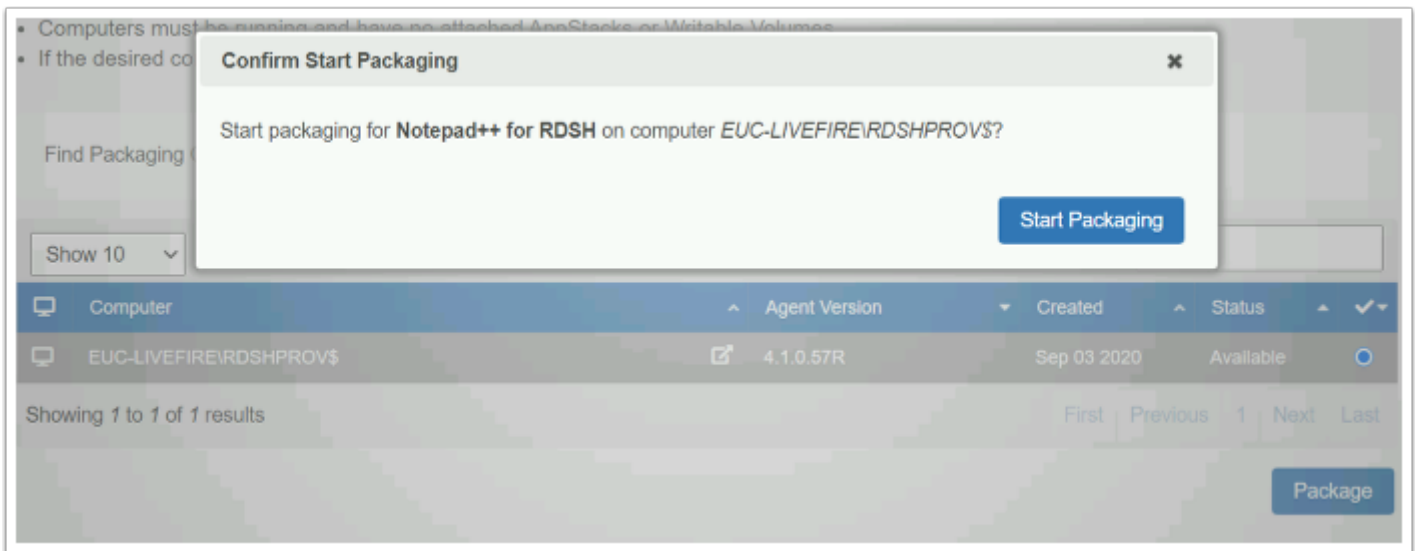
- Select the **Packages** tab
- **Expand Notepad++ For RDSH**



6. In the **Packages** tab
  - In the **Notepad++ For RDSH** to the right select **Package**



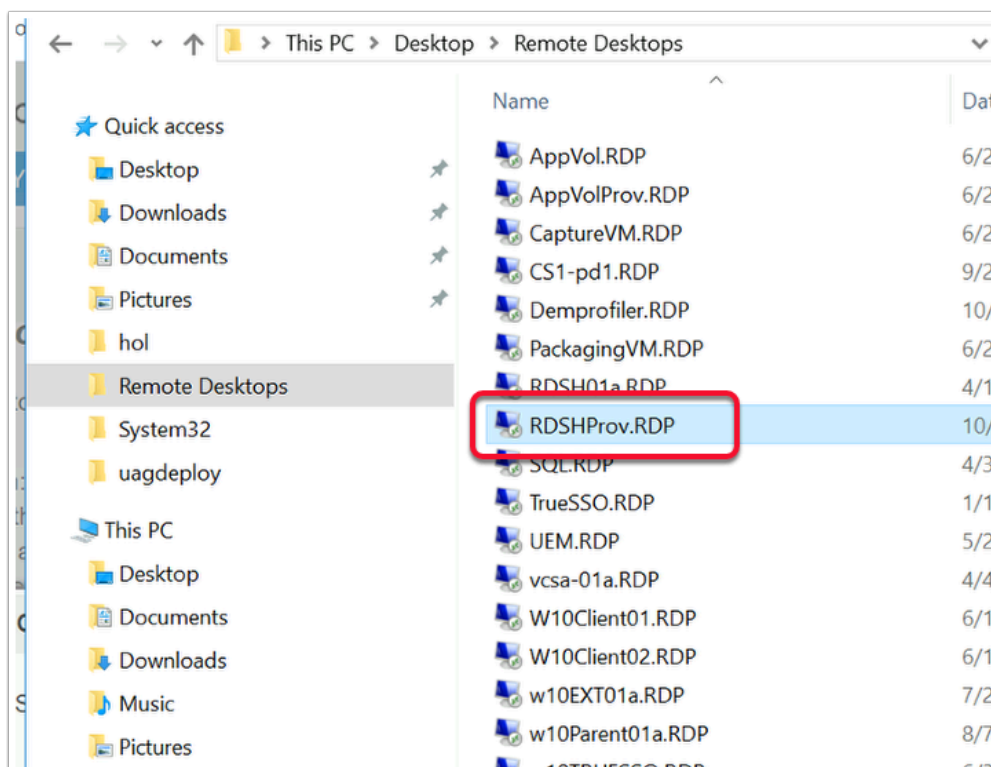
7. In the **Package for Notepad++ For RDSH** window
  1. Next to find **Packaging Computer** type **rdshprov**
  2. Select **Search**



8. In the **Package for Notepad++ For RDSH** window

- Select the **EUC-LIVEFIRE\RDSHPROV\$** radio button
- Select **Package**
- In the **Confirm Start Packaging** window, select **Start Packaging**

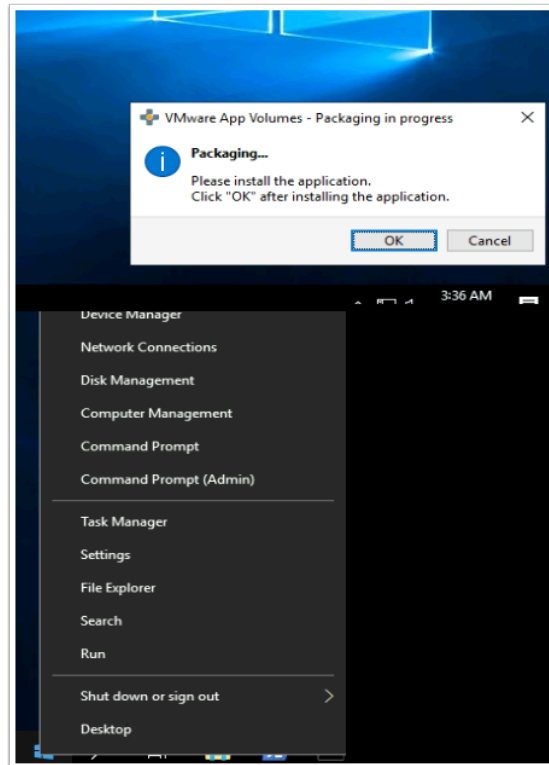
NOTE. If the RDSHPROV shows as unavailable , login to your RDSHPROV server and restart the APP Volumes services



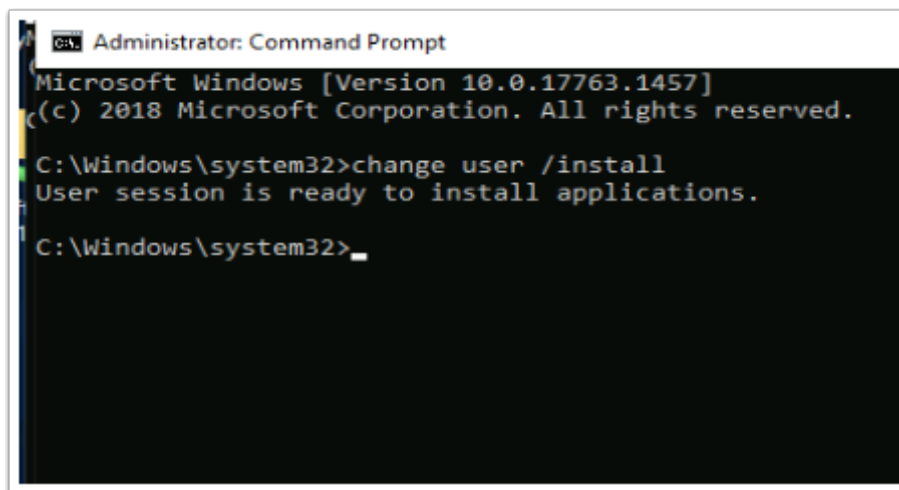
9. On the Controlcenter2 desktop

- Open the **Remote Desktops** folder and launch **RDSHProv.RDP**
  - login with

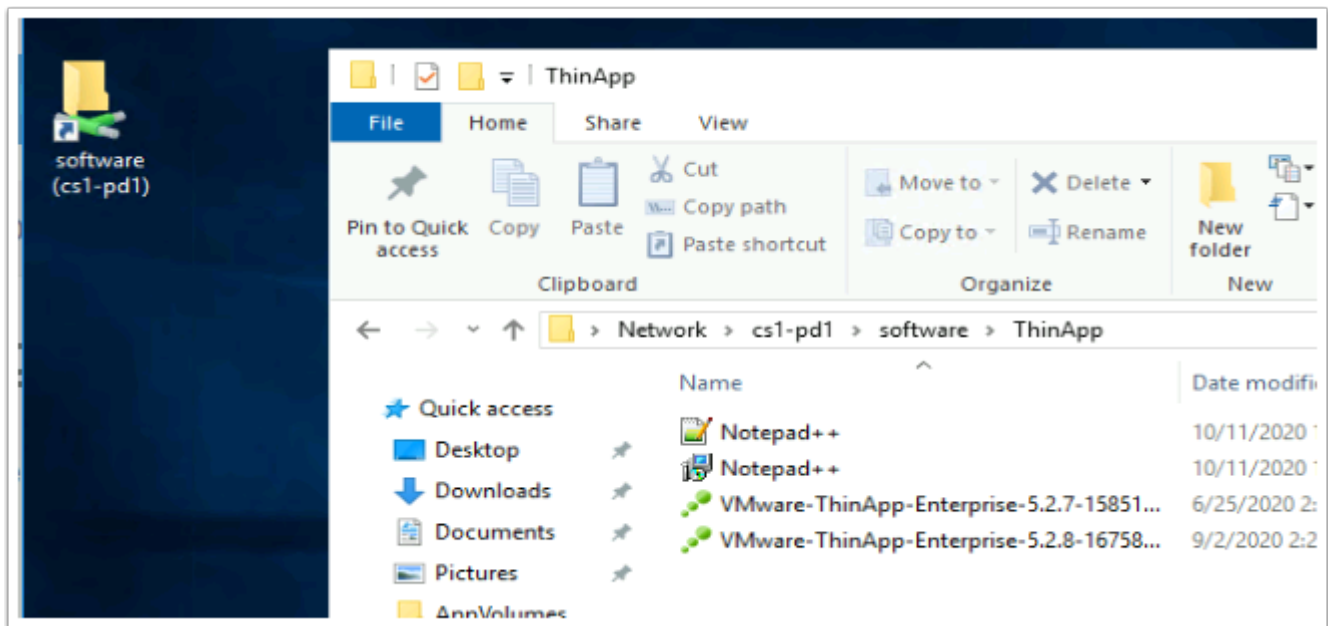
- Username **Administrator@euc-livewire.com**
- Password : **VMware1!**



- On the RDSHPProv desktop
  - Observe the **Packaging in Progress** window
  - Select and right click to the **Start** button
  - Select the **Command Prompt (Admin)** button

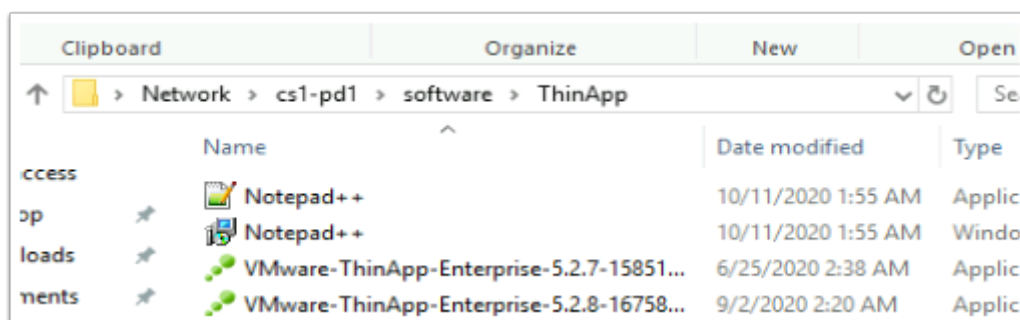


- In the Command Prompt On the RDSH-Prov desktop
  - Type **change user /install** select **ENTER**
  - Notice the message, after you have entered, Keep your **Command Prompt** window Open



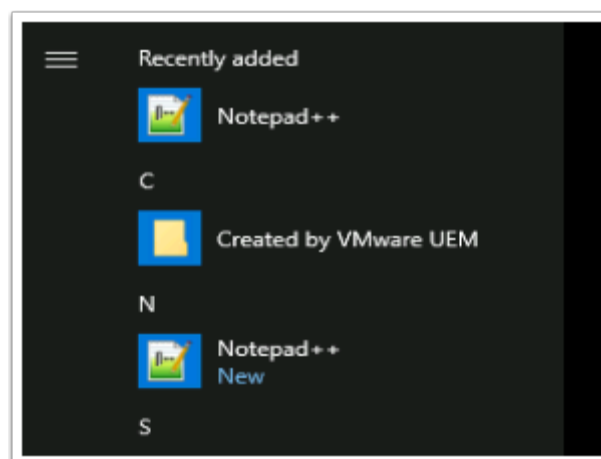
## 12. On the RDSH-Prov Desktop

- Select the **Software** shortcut and open the **ThinApp** folder



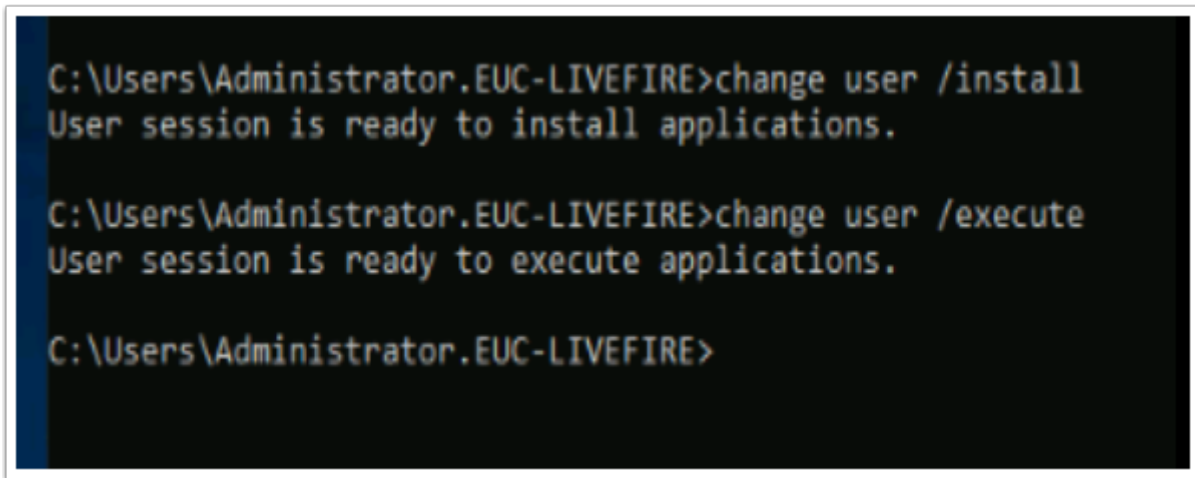
## 13. In the **File Explorer** Window

- Select and double-click **Notepad++.msi** >
- You will notice, it installs automatically



14. On the RDSH-Prov Desktop

- Click the **Start** button, and note the Recently added shortcut, Double-click **Notepad++**
  - Observe the **Thinapp Notepad++ package** launch,
  - **Close** Notepad++



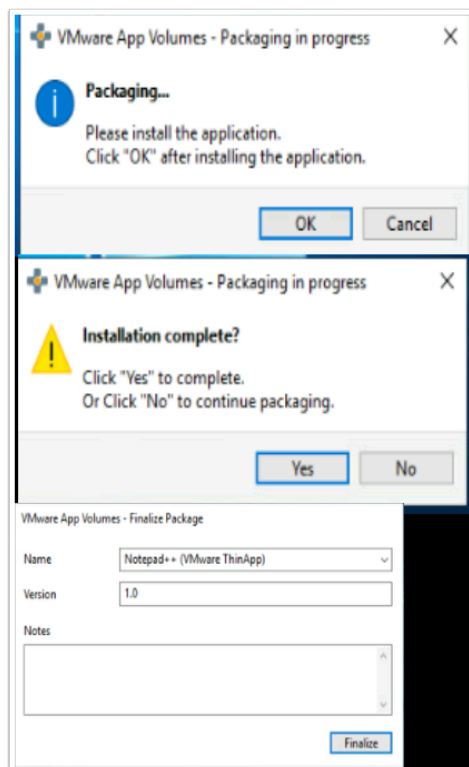
```
C:\Users\Administrator.EUC-LIVEFIRE>change user /install
User session is ready to install applications.

C:\Users\Administrator.EUC-LIVEFIRE>change user /execute
User session is ready to execute applications.

C:\Users\Administrator.EUC-LIVEFIRE>
```

15. On the RDSH-Prov Desktop:

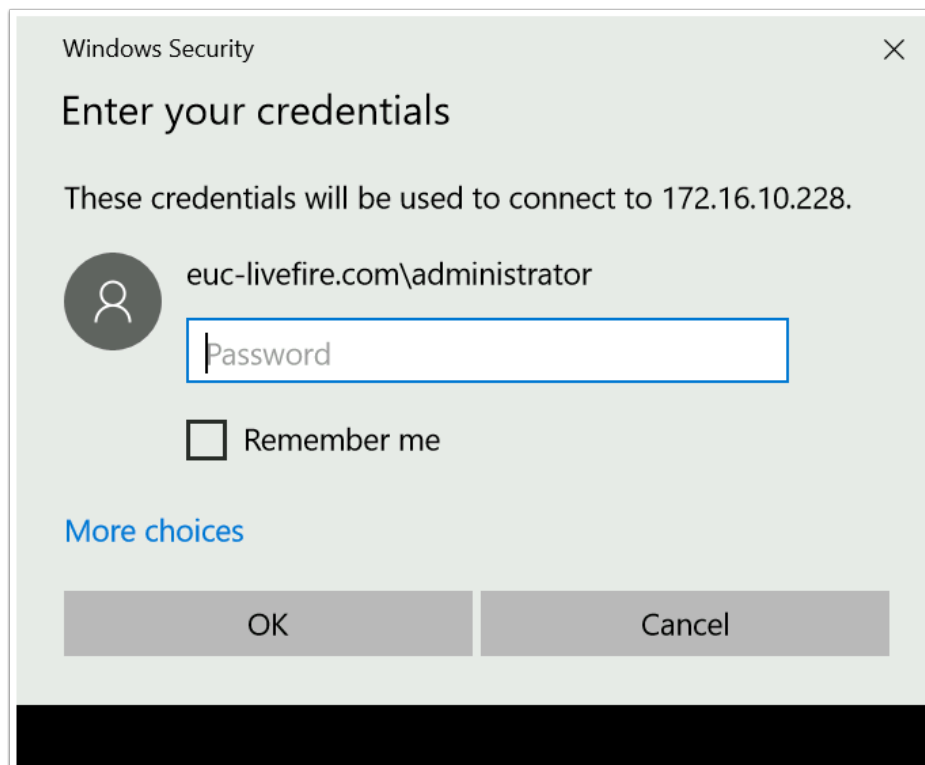
- Revert to the **Command Prompt** window and type the following:
  - **Change user /execute**
- Press **Enter** on your keyboard
  - Notice the message.



16. On the RDSH-Prov Desktop

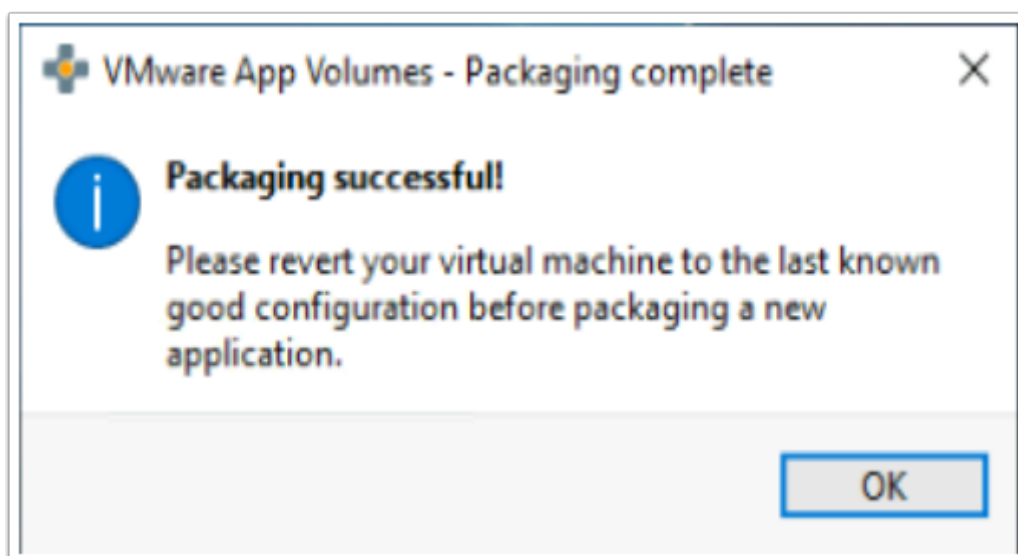
- In the **VMware APP Volumes - Packaging in progress** window,

- Select **OK**
- Select **Yes**
- Select **Finalize**
- Select **OK**



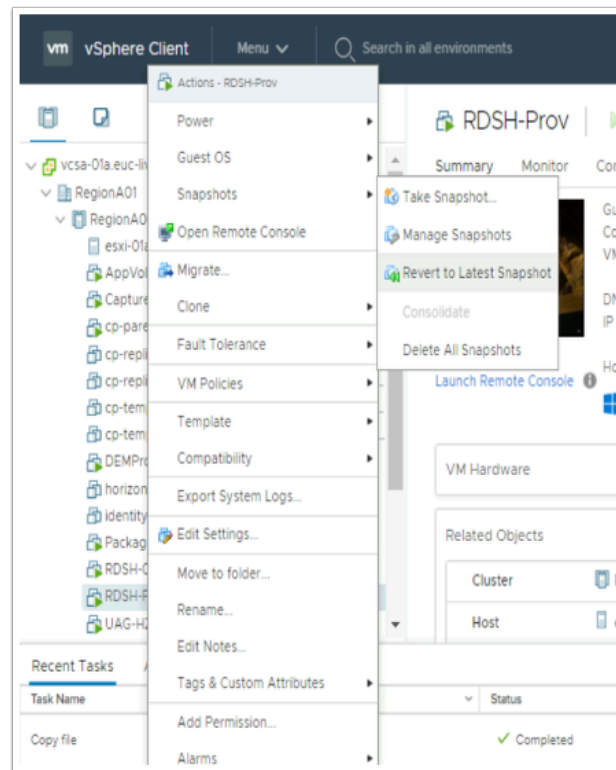
17. On the ControlCenter2 server Desktop

- From the **Remote Desktops** folder, launch **RDSHProv.RDP**
  - Login as **Administrator@euc-livefire.com**
  - Password is **VMware1!**



18. On RDSH-Prov Desktop

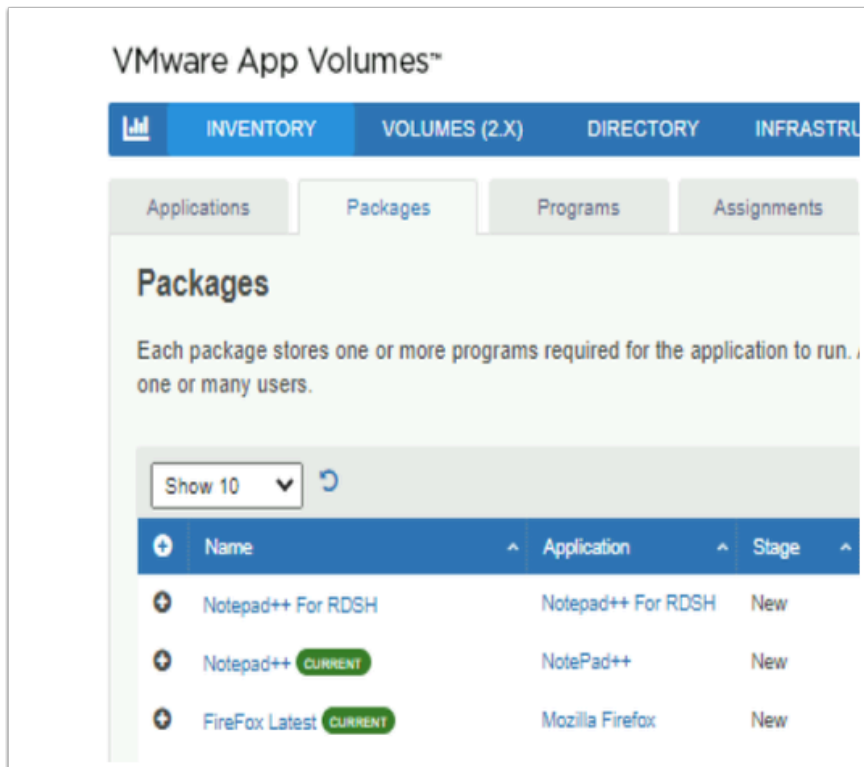
- Select **OK** to close the **VMware App Volumes - Packaging complete** window



19. On the ControlCenter2 desktop

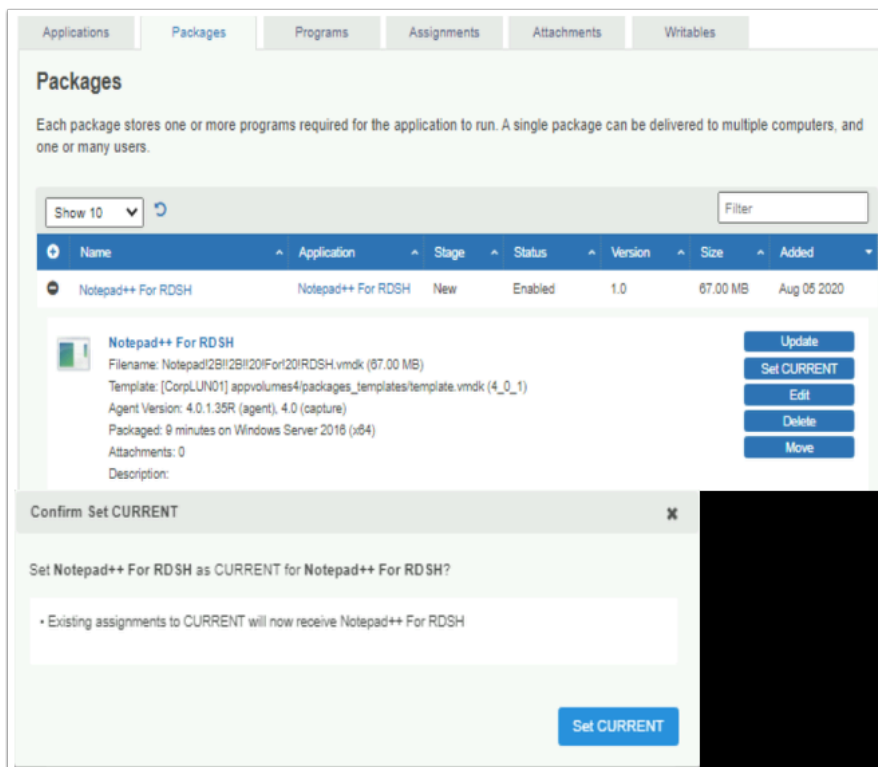
- In the **vCenter admin console**,
  - Select **RDSH-Prov** and **right-click**
  - Select **Snapshots** > **Revert to Latest Snapshot**
  - On the **Revert to Snapshot** window, select **YES**





20. In the App Volumes Admin Console

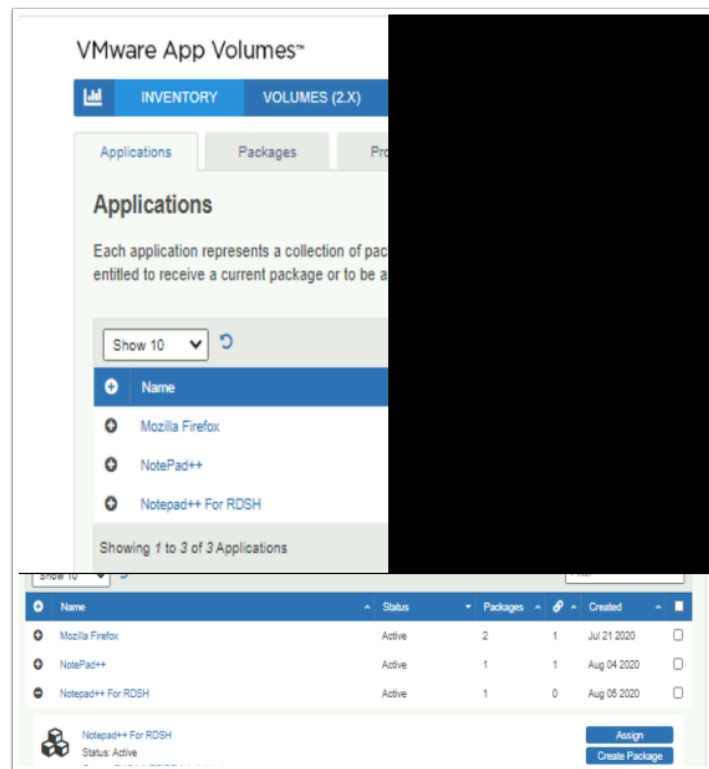
- Select the **Packages** tab
- Expand **Notepad++ For RDSH**



22. In the App Volumes Manager console **Package** tab

- In the **Notepad++ for RDSH** area

- Select **Set CURRENT**
- In the **Confirm Set Current** window
  - Select **Set CURRENT**



23. From your **App Volumes Manager Admin** console session
- Select **INVENTORY > Applications** tab
  - Expand **Notepad++ For RDSH**
  - Select **Assign**

VMware App Volumes™

INVENTORY VOLUMES (2X) DIRECTORY INFRASTRUCTURE ACTIVITY CONFIGURATION

Applications Packages Programs Assignments Attachments Writables

### Assign Application: Notepad++ For RDSH

Search Active Directory for entities to assign to this Application.

Domain:

Search Active Directory:

☐ Search all domains in the Active Directory forest

24. In the **Assign Application: Notepad++ For RDSH** window

- Next to **Search Active Directory**, Type **RDSH**
- Select **Search**

Show 10

| Entity                    | Name       | Status    |                                     |
|---------------------------|------------|-----------|-------------------------------------|
| EUC-LIVEFIRE\CITRIXRDSH\$ | CITRIXRDSH | Available | <input type="checkbox"/>            |
| EUC-LIVEFIRE\RDSH-01A\$   | RDSH-01A   | Available | <input checked="" type="checkbox"/> |
| EUC-LIVEFIRE\RDSH-INS1\$  | RDSH-INS1  | Available | <input type="checkbox"/>            |
| EUC-LIVEFIRE\RDSH-INS2\$  | RDSH-INS2  | Available | <input type="checkbox"/>            |
| EUC-LIVEFIRE\RDSHPARENT\$ | RDSHPARENT | Available | <input type="checkbox"/>            |
| EUC-LIVEFIRE\RDSHPROV\$   | RDSHPROV   | Available | <input type="checkbox"/>            |

Showing 1 to 6 of 6 results [First](#) [Previous](#) [1](#) [Next](#) [Last](#)

Entities:

Assignment Type: ☒ Marker ☐ Package

Markers:

| Marker  | Package        | Stage | Added       |                          |
|---------|----------------|-------|-------------|--------------------------|
| CURRENT | Firefox Latest | New   | Jul 21 2020 | <input type="checkbox"/> |

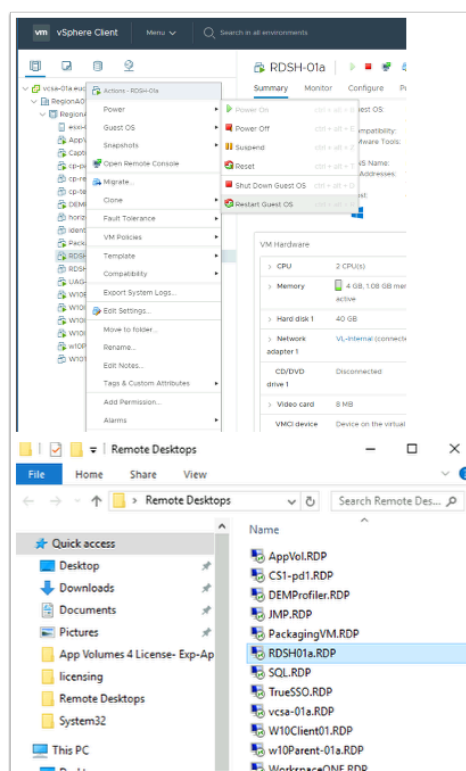
25. In the **Assign Application: Notepad++ For RDSH** window

- Next **EUC-Livefire\RDSH-01a\$**, select the **checkbox** next to **Available**
- Select **Assign**



26. In the **Confirm Assign** window

- Select **Assign**

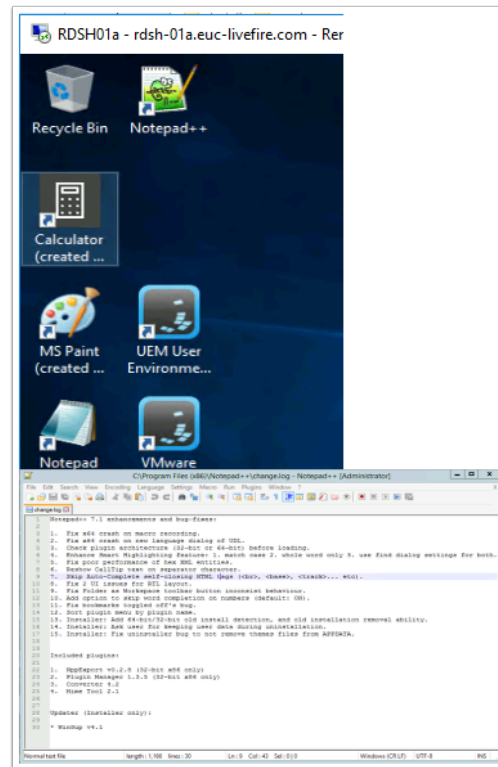


27. On the **ControlCenter2** server,

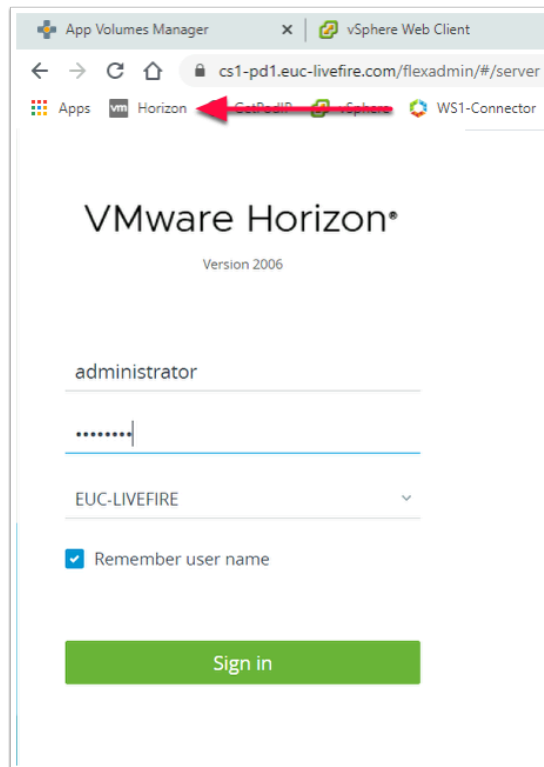
- Switch to your vCenter Admin console
  - Select the **RDSH01a**
    - Select **Power > Restart Guest OS**,
    - On the **Confirm Guest Restart** window, select **YES**
      - Give the reboot about a minute
- Open the **Remote Desktop** folder and launch the **RDSH01a.RDP** shortcut
  - You should automatically be logged in as
    - **Username: Administrator**

- Password: **VMware1!**

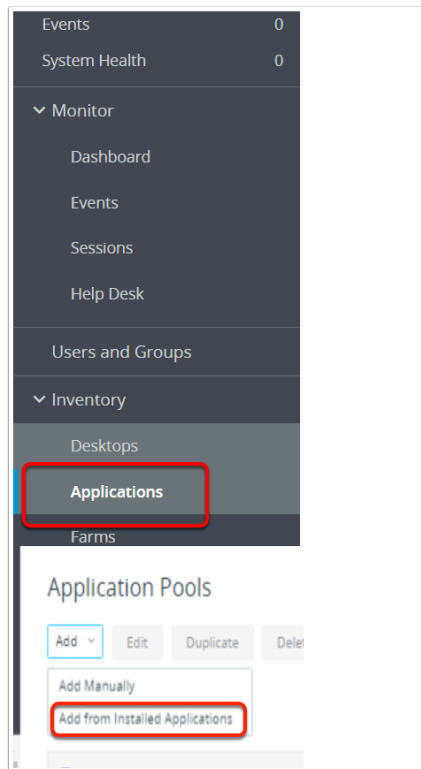
- Restart your **RDSH** server
- From the **Remote Desktops** folder launch the **RDSH01a.RDP** shortcut



- **Close** the application when done
- Disconnect the **RDSH RDP** session



29. On your **ControlCenter2** server,
- Launch Horizon Administrator Console from the **Horizon** Shortcut on the **Favourites bar** on your Chrome browser.
  - Select **LAUNCH** the **Horizon Console (HTML)** Console .
    - In the **Username** are type **Administrator**
    - In the **Password** area type **VMware1!**
    - Select **Sign In**



30. In the Horizon Admin Console,
- Expand **Inventory** and select **Applications**
  - In the **Application Pools** area
    - Select **Add**
    - Select **Add from Installed Applications**

## Add Application Pool

1 Select Applications

2 Edit Applications

**Application Pool Type**

☐ Desktop Pool ☒ RDS Farm

**Select installed applications**

☐ Name

☒ Notepad++

31. In **Add Application Pools** wizard

- Select the **Notepad++** and select the **check box**.
- Select **Next**

**Add Application Pool**

✓ Select Applications

2 Edit Applications

Edit the ID and display name for selected applications.

| ID              | Display Name | Path   |
|-----------------|--------------|--|
| NotepadPlusPlus | Notepad++    | C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Notepad++.lnk |

Cancel Previous Submit

32. In the **Add Application Pools** window

- Under **ID**, change **NotePad** to **NotePadPlusPlus**
- Select **Submit**



The image shows two overlapping windows from the VMware Horizon console. The top window, titled 'Add Entitlements', has a close button (X) and a subtitle 'Add new users and groups who can use the selected pool(s)'. It contains 'Add' and 'Remove' buttons and a table with columns 'Name', 'Domains', and 'Email'. The table is empty with the text 'No records available'. The bottom window, titled 'Find User or Group', also has a close button (X). It features a 'Type' section with 'Users' selected, and a 'Domain' dropdown set to 'Entire Directory'. The 'Name/User Name' and 'Description' fields both have 'Contains' selected from a dropdown. A 'Find' button is present. Below is a table with columns 'Name', 'User Name', 'Email', 'Description', and 'In Folder'. One record is shown: 'Marketing' with 'Marketing@livefire.com' as the email and 'Marketing' as the description. 'Cancel' and 'OK' buttons are at the bottom.

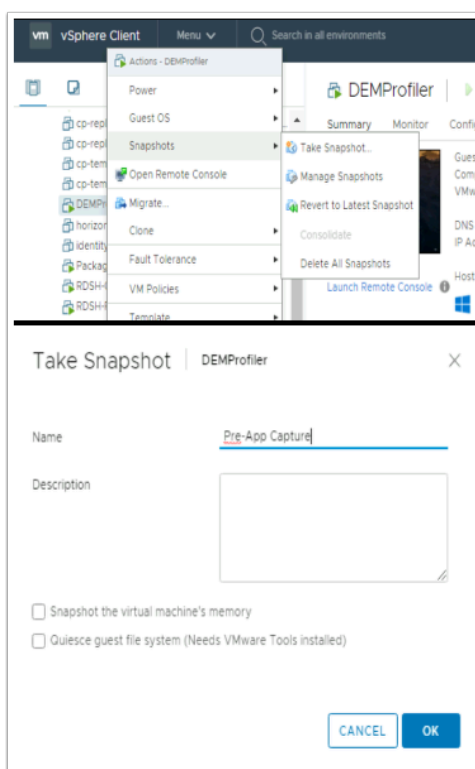
33. In the **Add Entitlements** window select **Add**
- In the **Find User or Group** next **Name/User name: Contains** box type **Marketing**
  - Select **Find**
  - Under **Name** select **Marketing checkbox** and select **OK**
  - Select **OK**

The image shows the VMware Horizon Client interface. At the top is a 'Login' window with fields for 'Server' (https://cs1-pd1.euc-livefire.com), 'User name' (user1), 'Password' (masked with dots), and 'Domain' (DefaultDomain\*). 'Cancel' and 'Login' buttons are at the bottom. Below the login window is the 'VMware Horizon Client' main area, showing a list of applications: 'WorkSpace', 'Calculator', 'Internet Explorer', 'Notepad++' (highlighted with a red rectangle), and 'Paint'. At the bottom, a Notepad++ window is open, displaying a list of tasks and updates.

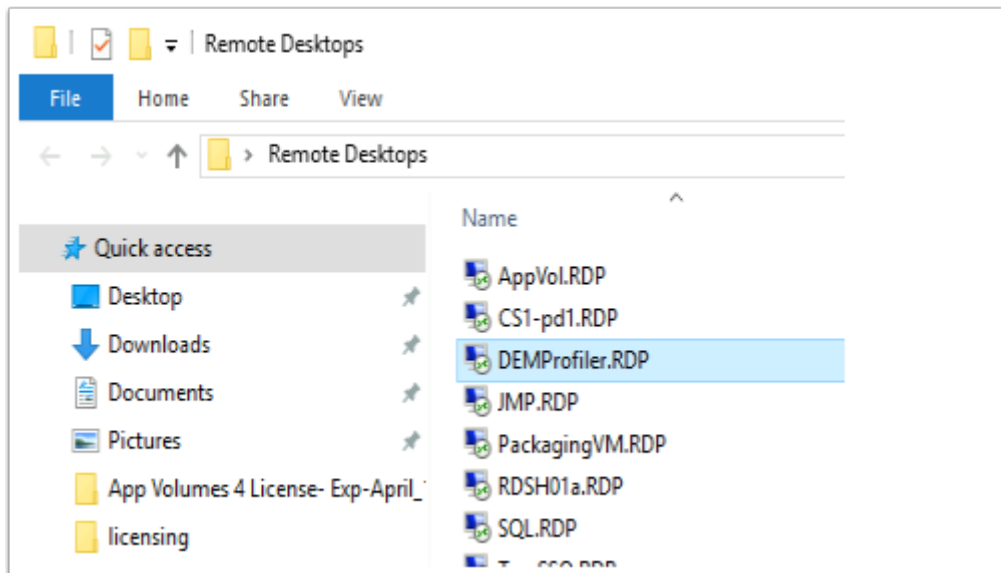
34. On your Controlcenter server desktop
- Launch your Horizon client with the following Credentials
    - Username is **User1**
    - Password is **VMware1!**
  - Select **Log in**
  - Launch **Notepad++**.
  - On the **Notepad++ Plugin Manager** window close **Notepad++**
  - On the Horizon client select **Log off**

## Part 4. Building a custom configuration for Dynamic Environment Manager to work with a ThinApp Application

### Section 1: Capturing a Notepad++ ThinApp configuration DEM Application Profiler

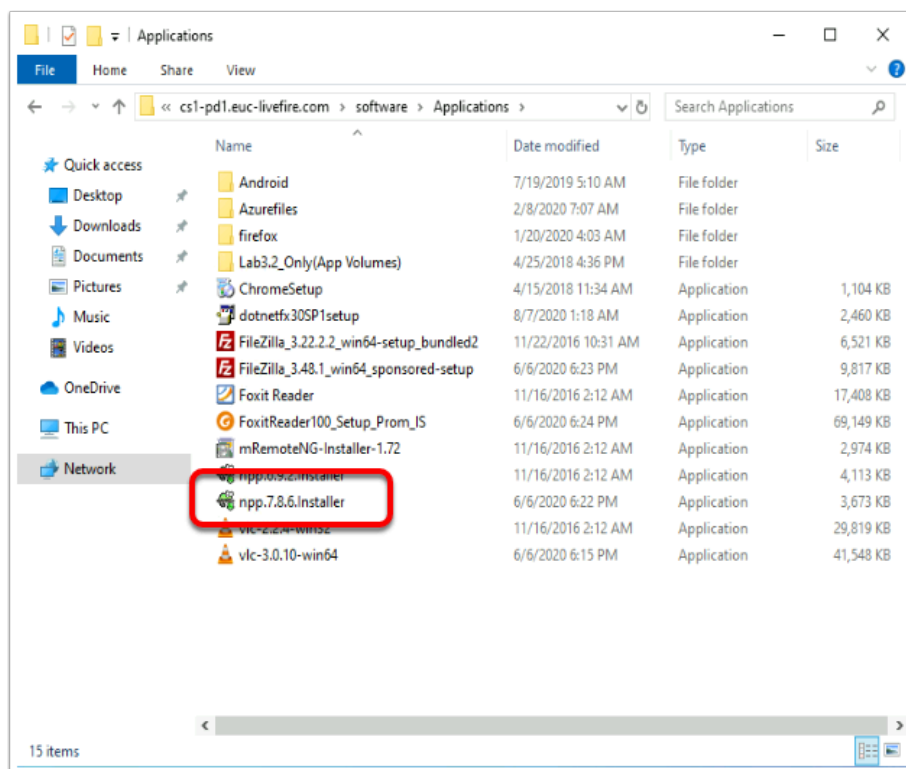


1. On your **ControlCenter2** Desktop,
- Open your **Chrome** browser. Select the **vCenter** shortcut.
  - Login as **Administrator** and the password **VMware1!**
  - Select **DEM-Profiler** > **right click**, select **Snapshots** and **Take Snapshot**
  - In the **Take VM Snapshot for DEMProfiler** window next to **Name** type **Pre-App Capture**
  - Select **OK**



2. From your ControlCenter2 server

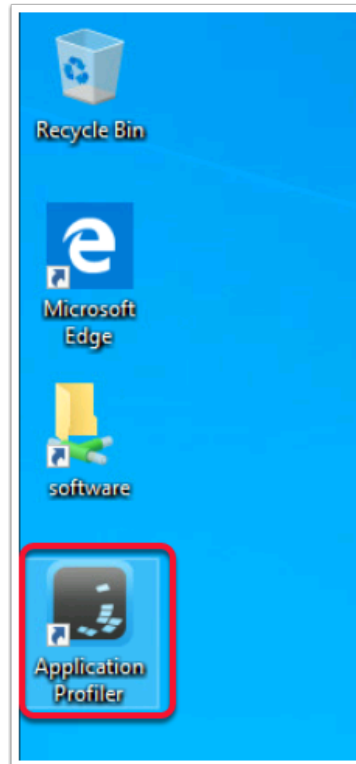
- Open the **Remote Desktops** folder and launch the **DEMProfiler.RDP**
  - Login as **administrator@euc-livefire.com** with the password **VMware1!**



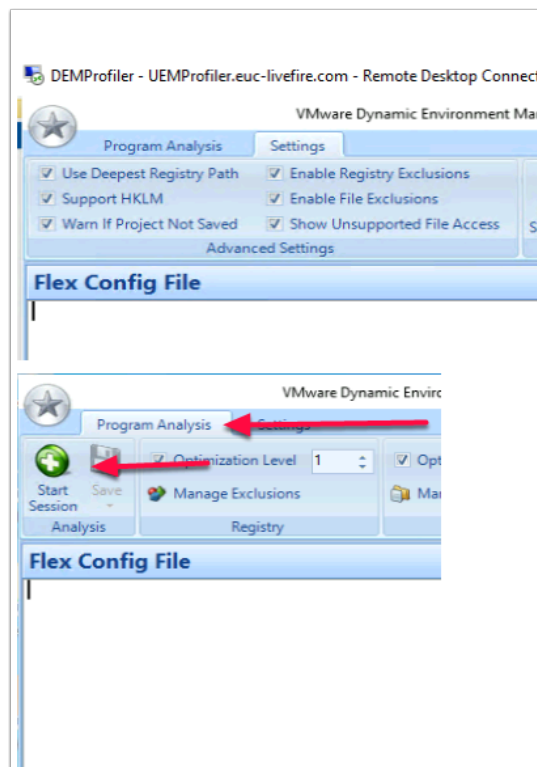
3. On the DEMProfiler desktop

- Open the **software** shortcut, open the **Applications\** folder
- **Install** the **native Notepad++** application you downloaded at the beginning of this lab by selecting the **npp.7.8.6.installer** ,
  - When you are prompted to update, download and install the application is update

- Once **Notepad++** has been installed. **Close All windows**

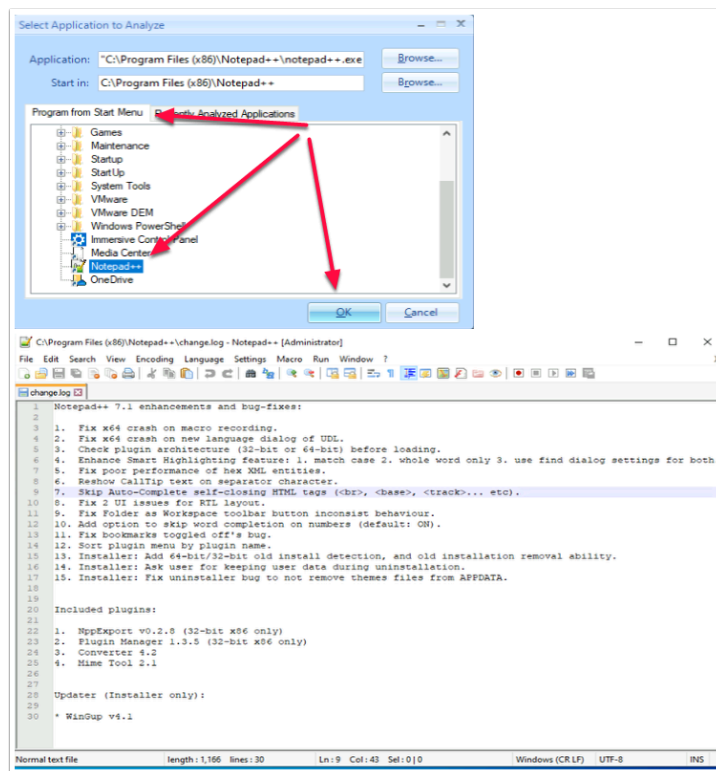


4. From the **DEMPProfiler** Desktop
  - Open the **DEM Application Profiler** Console

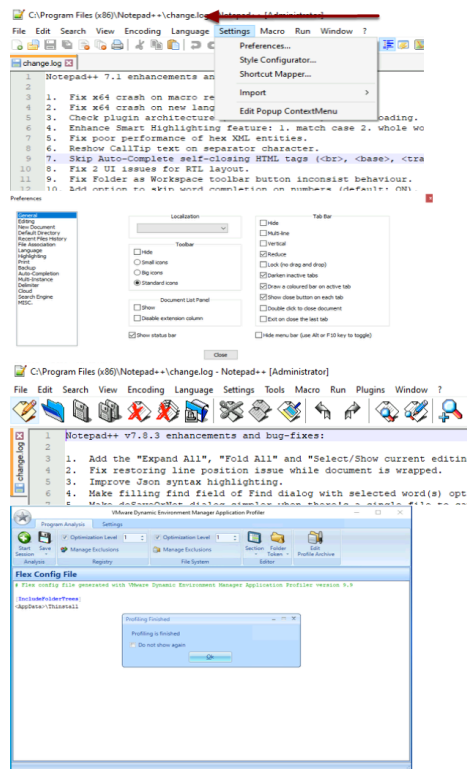


5. In The DEMProfiler Console
  - Select the **Settings** tab, enable the following

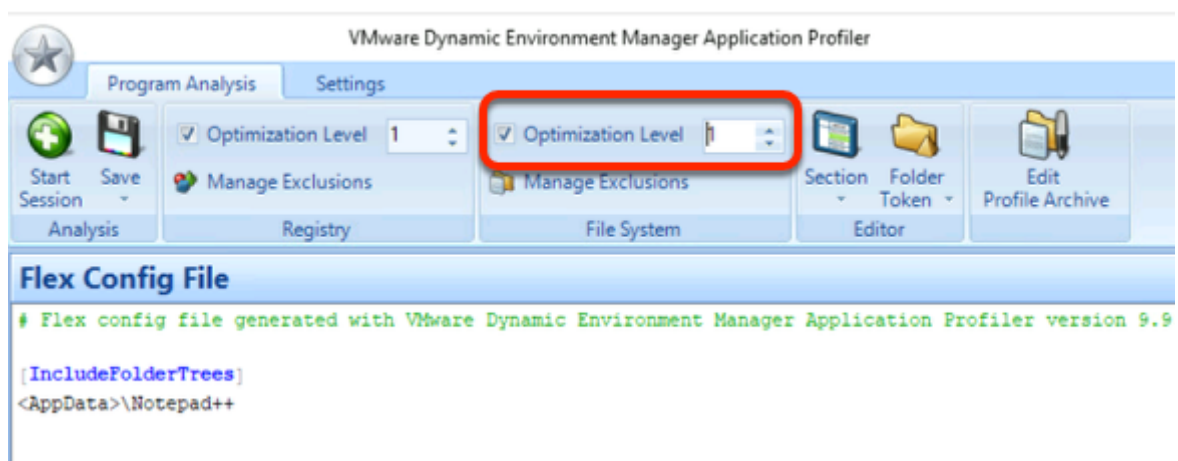
- **Check box** in front of **Support HKLM**
- **Check box** in front of **Warn if Project Not Saved**
- **Check Box** in front of **Show Unsupported File Access**
- Select the **Program Analysis** tab
- Select **Start Session**



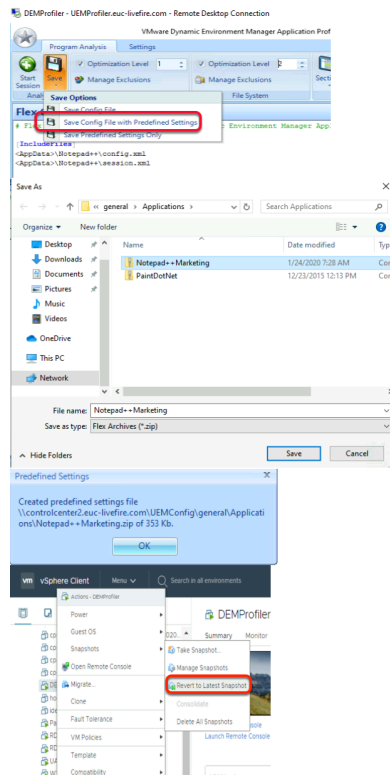
6. In the **Start Application to Analyze** window under **Program from Start Menu**
  - Expand the inventory under **Programs** expand and select the **Notepad++** shortcut
  - Select **OK** to Start New Analysis.
  - You will notice **Notepad++** launching in the Background,



7. In **Notepad++**, select the **Settings > Preferences**,
  - In the **General** area
    - Change from **Standard Icons** radio button to **Big Icons** radio button
    - Under the **Tab Bar** enable **Multi-line** and **Vertical** checkboxes
  - Select the **Close** button to close **Preferences**. Close **Notepad++**
  - Click **OK** to close the **Profiling Finished** window

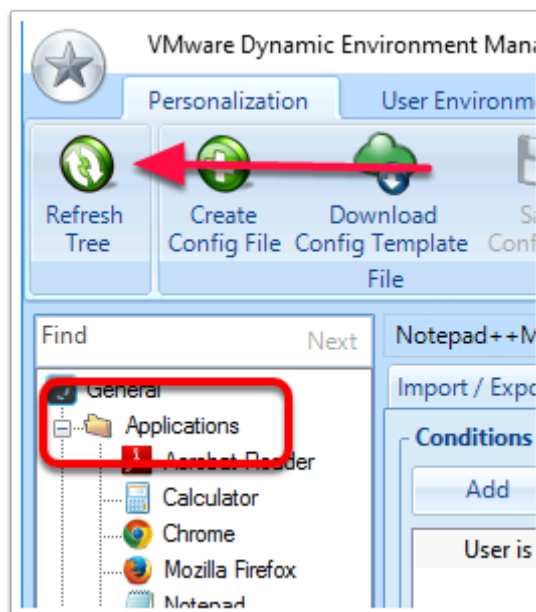


8. To right of the page, make sure the **Optimization level** for this exercise is **1**,



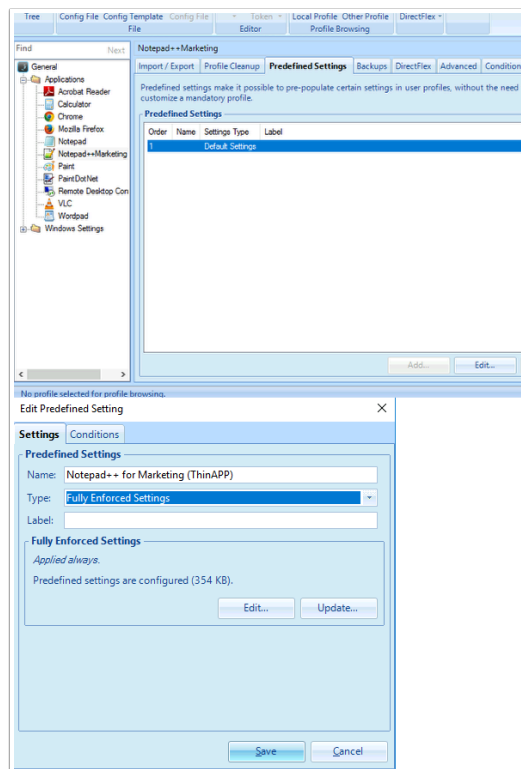
9. Select **Save > Save Config File with Predefined Settings**
  - When prompted to save the configuration, enter **Notepad++Marketing**
  - Select **Save**, select **OK** to close the **Predefined Settings** window
  - Go to your **vSphere client**, select **DEMPProfiler**, **right click** > select **Snapshot > revert to current Snapshot**

## Section 2. Performing DEM based configuration



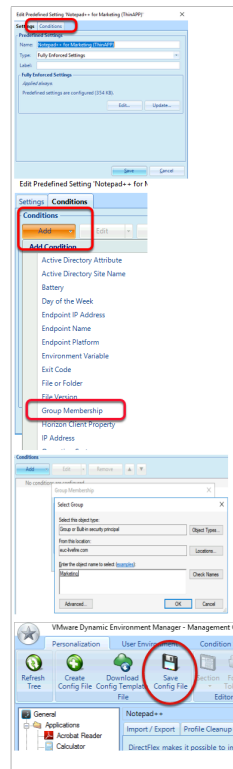
1. On your ControlCenter2 server

- Launch your DEM mmc shortcut
- Under **General**, select the **Applications** folder,
- Select **Refresh Tree** in top left-corner



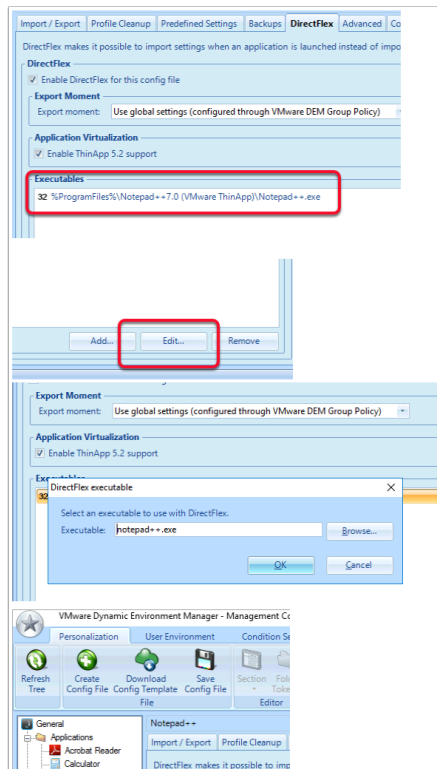
2. On the Dynamic Environment Manager MMC
  - Under **Applications**, select the **Notepad++Marketing** configuration
  - Select the **Predefined Settings** tab
    - Select **Default Settings**, select **Edit**
      - Enter and configuring the following:
        - Name: **Notepad++ for Marketing (ThinAPP)**
        - Type: **Fully Enforced**





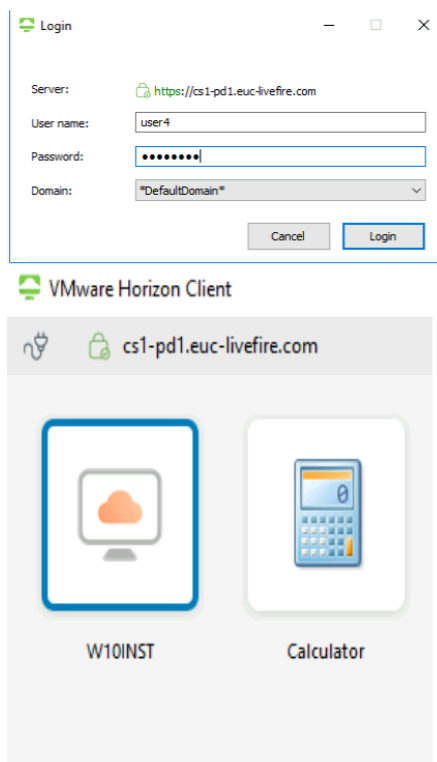
## 5. On **Edit Predefined Setting** window

- Select the **Conditions** Tab select **Add** select **Group Membership**
- Next to **Member of Group** select **Browse**
  - In the **Select Group** window, type **Marketing** and select **Check Names**
- Select **OK twice** >
- In the Tool bar at the top, select **Save Config File**

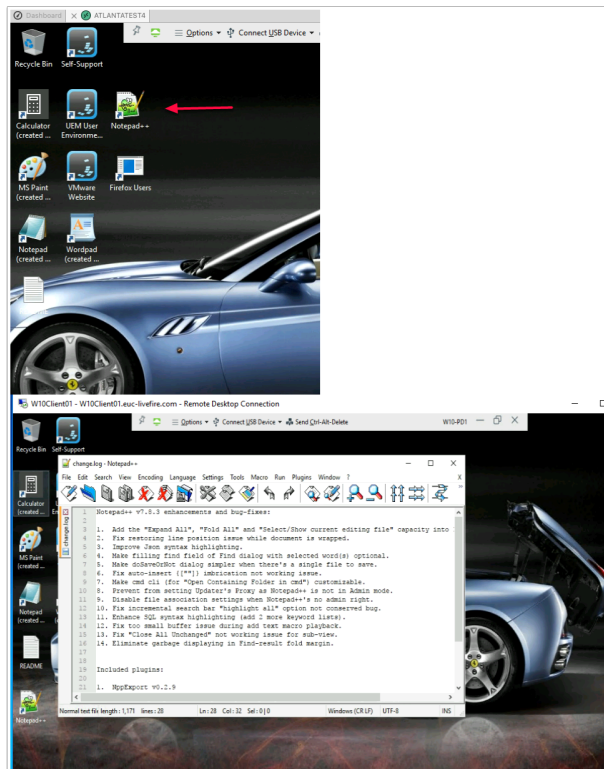


6. Select the **DirectFlex** tab,
  - Select and **enable ThinApp 5.2 support checkbox**
  - Select the Executables path and select Edit
  - **Remove the entire path** with the exception of **notepad++.exe**
  - Select **OK**
  - Select **Save Config file**

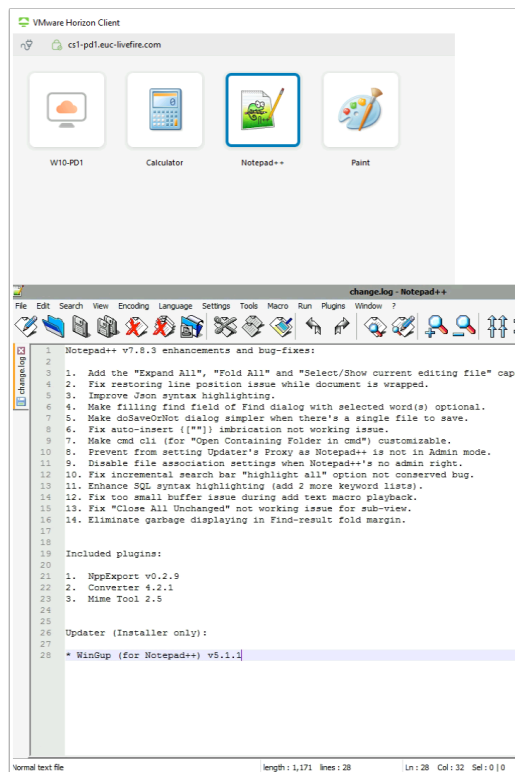
## Part 5. Testing our Notepad++ ThinApp / App Volumes / Dynamic Environment Manager Integration with Horizon Published Apps and Desktops



1. On the **Controlcenter2** desktop,
  - Launch your **Horizon client** shortcut,
  - login as **user4** with the password **VMware1!**
  - Select the **W10INST** desktop entitlement

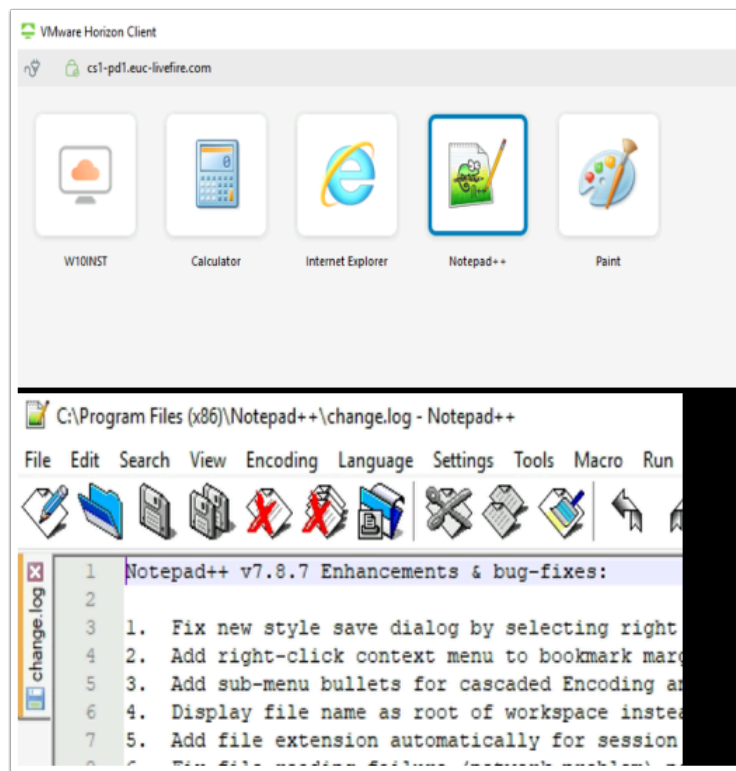


2. On the Windows 10 desktop session
  - Launch the **Notepad++** shortcut
  - Notice your enforced configurations are being applied



3. Revert back to your **Horizon client**, to observe your Entitlements

- Launch the **Notepad++** entitlement
- Try changing your **Big Icons** to **Small Icons** and then **close** the session. **Re-open** the session. Notice that you have **Big Icons** again. This is because we created **Pre-defined settings** and these were enforced.
- **Log off and disconnect** from all sessions



4. On the ControlCenter2 Desktop
  - Select your **Notepad++** Virtual Application, in the Horizon Client
  - Notice your settings are still being enforced

## Conclusion

In this session we covered the integration of VMware ThinAPP being an application Isolation solution and using VMware App Volumes as a Delivery solution to Horizon Desktop and Application Pools.

Finally we covered the management of the application settings using DEM Profiler and Dynamic Environment Manager

# Profiling with mRemoteNG

## Overview

In this module, we will continue look at example related to individual Application Settings in VMware Dynamic Environment Manager.

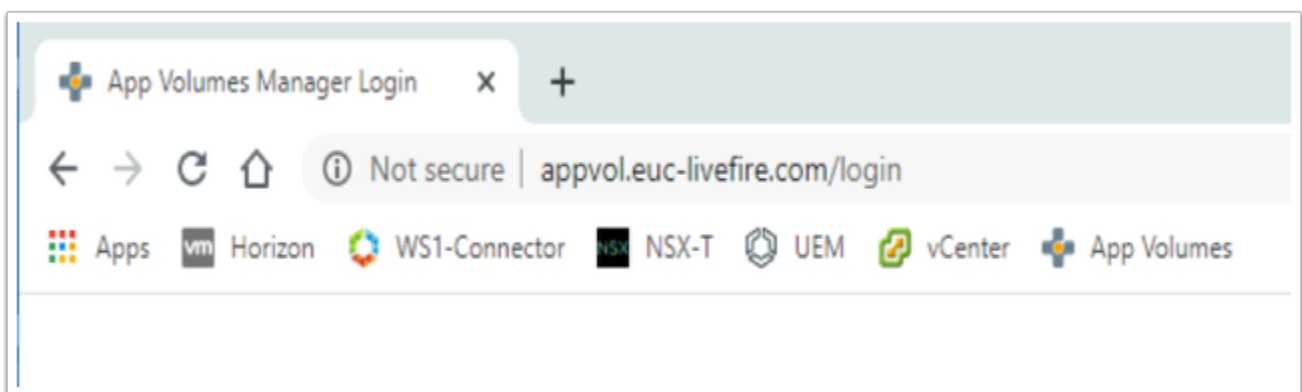
Applications can have pre-defined settings, but you will encounter scenarios where it makes sense to allow users to customize their applications after receiving some initial Application Configuration setting.

The examples we will use here will further help us to understand the challenges we might be faced with with individual applications

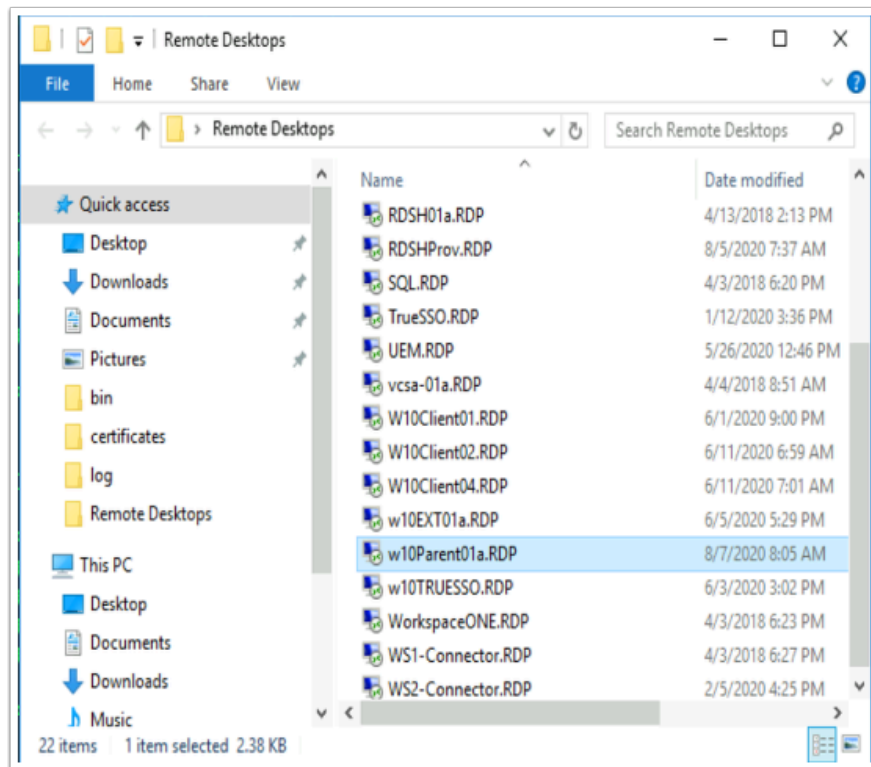
We will start off by

- Deploying the RemoteNG Application on our Horizon Desktop
- Profiling the Application
- Testing to see if the Profiling works
- Update the existing profile to get it to work
- Re-test the application

## PART 1: Deploying mRemoteNG

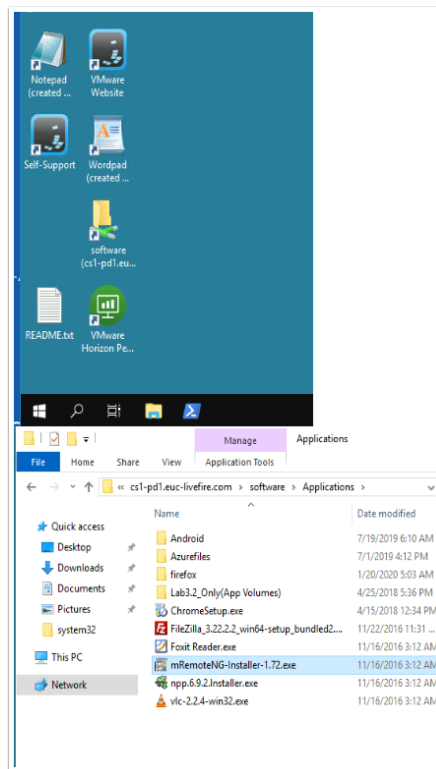


1. On your **ControlCenter2** Server.
  - Open your **Chrome** browser.
  - Select the **vCenter** shortcut in your **Bookmarks**
  - Login as **administrator** with the password **VMware1!**

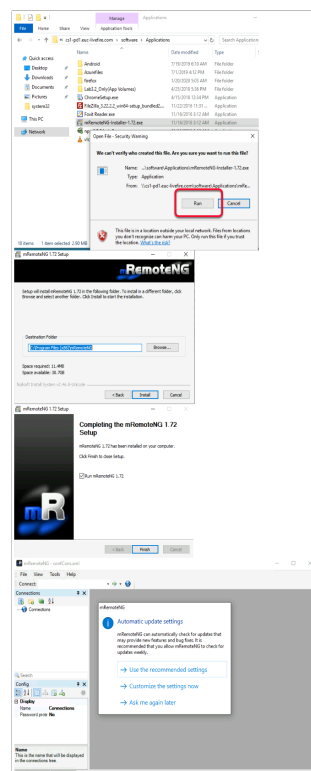


2. On ControlCenter2 desktop

- Open the **RemoteDesktop** folder and launch **W10parent01a.RDP** shortcut
  - Login with the local administrator account
    - **Username** area **Parent01a\administrator**
    - **Password** area enter **VMware1!**
- Select **OK**



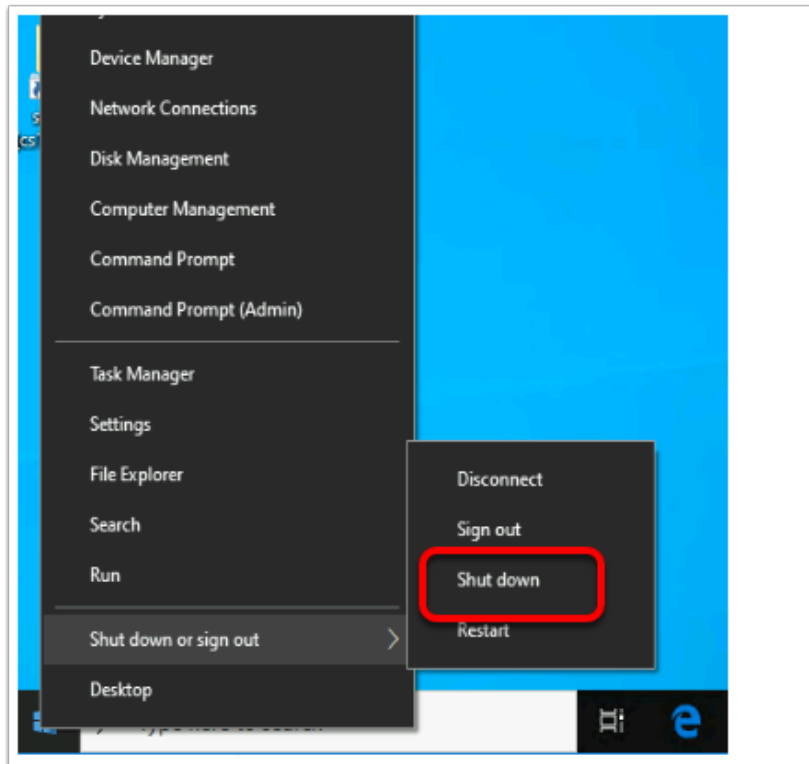
3. On the **W10Parent01a** desktop
  - Open the **Software** folder
  - Open the **Applications** folder
  - Launch **mRemoteNG-Installer-1.72.exe**



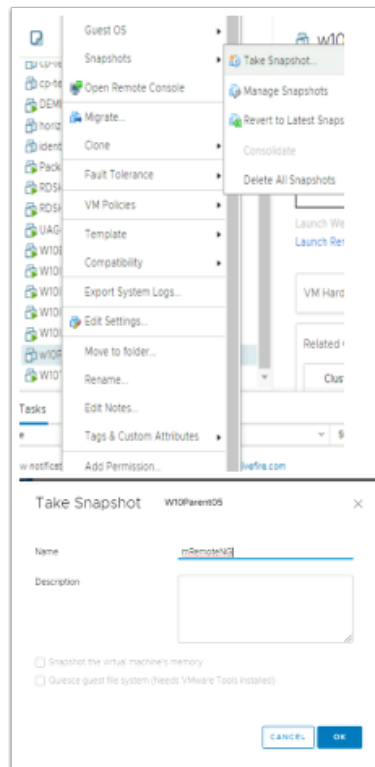
4. On the **W10Parent01a** desktop



- Double-click **mRemoteNG-Installer-1.72.exe** to install
- Select **Run**
- On the **Installer Language** window, select **OK**
- On the **licensing** window select **I Agree**
- Select **Install**
- On the **Completed** window, select **Next**,
- On the **Completing the mRemoteNG 1.72 Setup** select the **Run mRemoteNG checkbox**
- Select **Finish**
- Close the **Automatic update settings** window by selecting **Ask me again later**

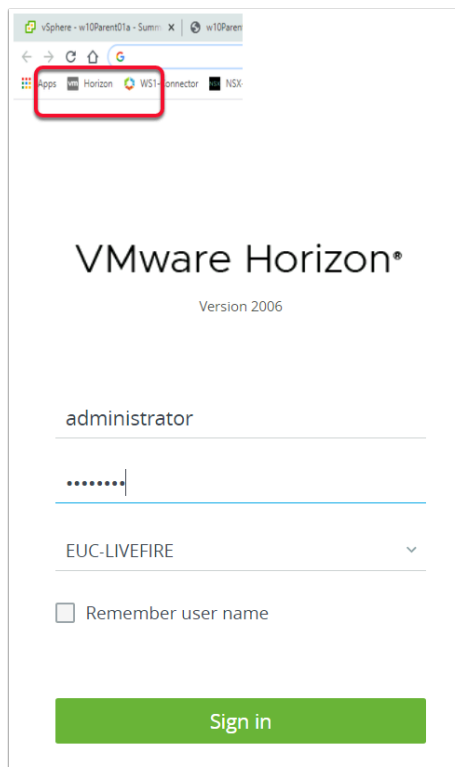


5. On your **w10Parent01a** machine
  - **Close** the application
  - **Close** all windows
  - **Shutdown** your **w10Parent01a** virtual machine

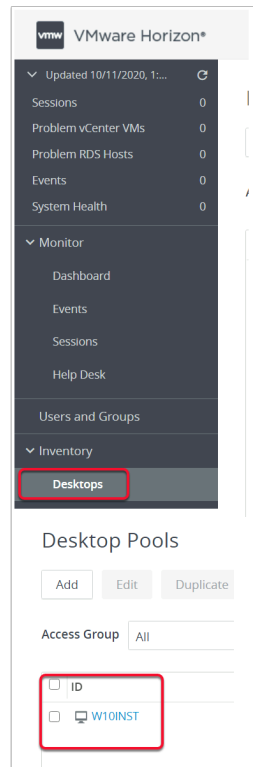


6. On your **Controlcenter2** server desktop

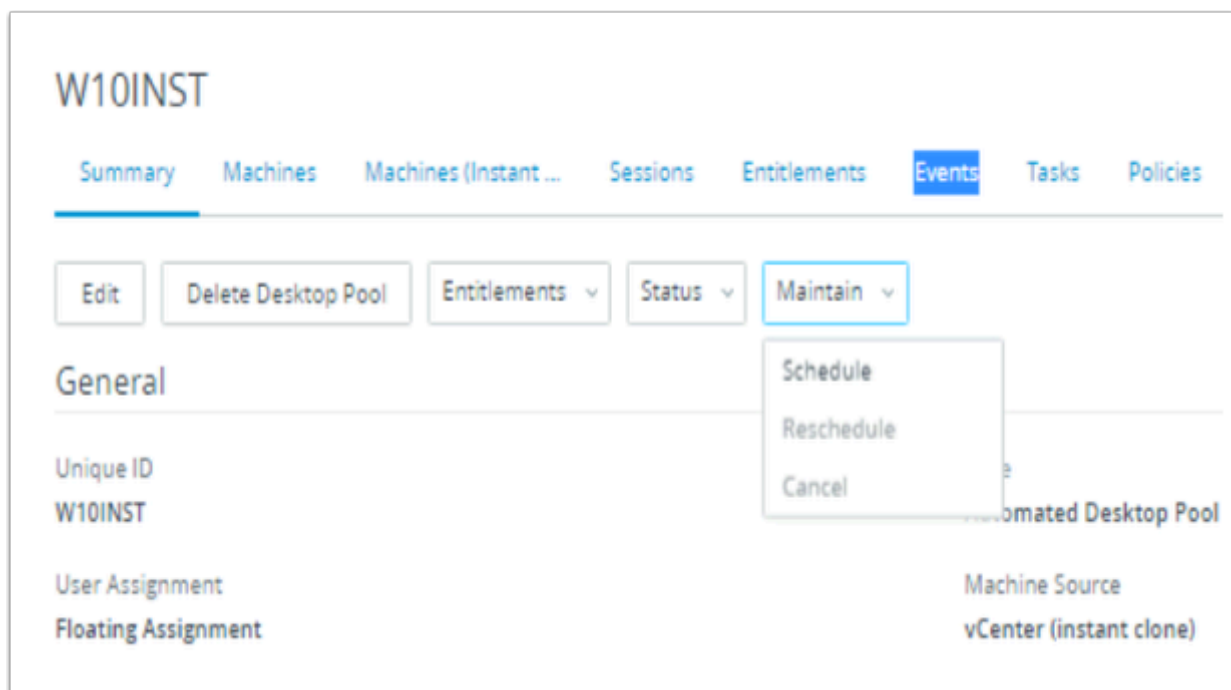
- Revert to your **vCenter server** session in your Chrome browser
- Select the **W10Parent01a** virtual machine
- Select **Snapshots > Take Snapshot**
- Next to **Name** type **mRemoteNG** and select **OK**



8. On your **ControlCenter2** server desktop
- On the **Chrome** browser, open a **new tab**, in the favourites bar, select the **Horizon** shortcut
  - Login as **Administrator** and the password is **VMware1!**



9. In the Horizon Admin Console
- **Expand Inventory** area, select **Desktops**
  - Under Desktop Pools, double-click **W10INST**



10. In the Horizon Admin Console
- Select **Maintain**, select **Schedule**

**Schedule Push Image**

1 Image

2 Schedule

3 Ready to Complete

**Image**

Select the snapshot that will be used as the image. This snapshot can be on the current parent VM or a different one.

The machines created in this desktop pool will use the information in the image as their baseline system configuration.

**Parent VM in vCenter**

/RegionA01/vm/Discovered virtual machine/w10Parent01a Change...

**Snapshot**

Snapshot Details

| Snapshot  | Time Created         | Description | Path  |
|-----------|----------------------|-------------|---|
| mRemoteNG | 08/07/2020, 11:52 AM |             | /Agents installed/certs/test horizon agent/Agent update/mRemoteNG |

**SVGA settings for Instant Clone Pool (Inherited from Master VM)**

| Number of Monitors | VRAM Size | Resolution | 3D Renderer |
|--------------------|-----------|------------|-------------|
| 1                  | 8.00 MB   | 1600x1200  | Disabled    |

Next Cancel

11. In the **Schedule Push Image** window,
- Ensure **mRemoteNG** is selected and select **Next**

**Schedule Push Image**

1 Image

2 Schedule

3 Ready to Complete

**Scheduling**

Specify when you want this task to start

Start at: 2020-08-07 12:38 Web browser local time

☐ Wait for users to log off  
Wait for connected users to disconnect before the task starts. The task starts immediately on machines without active sessions.

☒ Force users to log off  
Users will be forced to log off when the system is ready to operate on their virtual machines. Before being forcibly logged off, users may have a grace period in which to save their work (Global Settings).

☒ Stop at first error

The warning and grace period can be edited in global settings:

☐ Display warning before forced logoff

Logoff Time: 5 minutes

Logoff Message: Your desktop is scheduled for an important update and will shut down in 5 minutes. Please save any unsaved work now.

Back Next Cancel

**Schedule Push Image**

1 Image

2 Schedule

3 Ready to Complete

**Ready to Complete**

Review the options and click Finish

Forced logoff global settings:

Logoff Message: Your desktop is scheduled for an important update and will shut down in 5 minutes. Please save any unsaved work now.

Logoff Time: 5 minutes

| Affected Virtual Machines | Start Time           | User Logoff            | Stop at first error | Parent VM in vCenter                                  | Image   |
|---------------------------|----------------------|------------------------|---------------------|---|---|
| 4                         | 08/07/2020, 12:38 PM | Force users to log off | No                  | /RegionA01/vm/Discovered virtual machine/w10Parent01a | /Agents installed/certs/test horizon agent/Agent update/mRemoteNG |

Add a Trusted Platform Module (TPM) Device to the VMs: No

Show Details

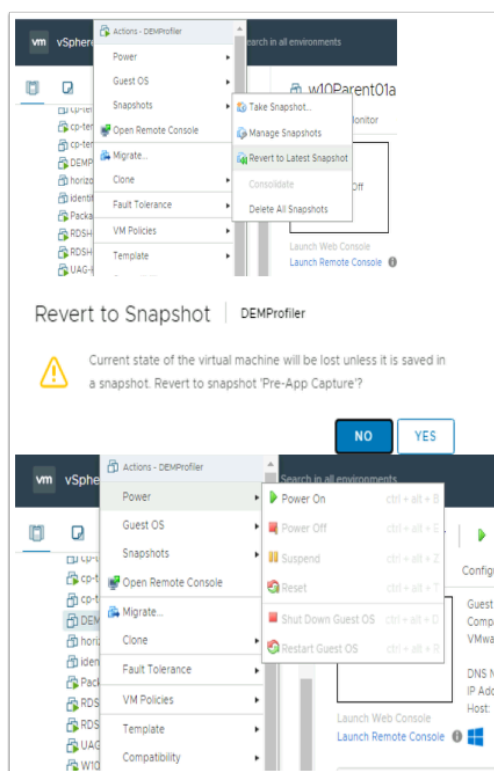
Back Finish Cancel

12. In the **Schedule Push Image** window,

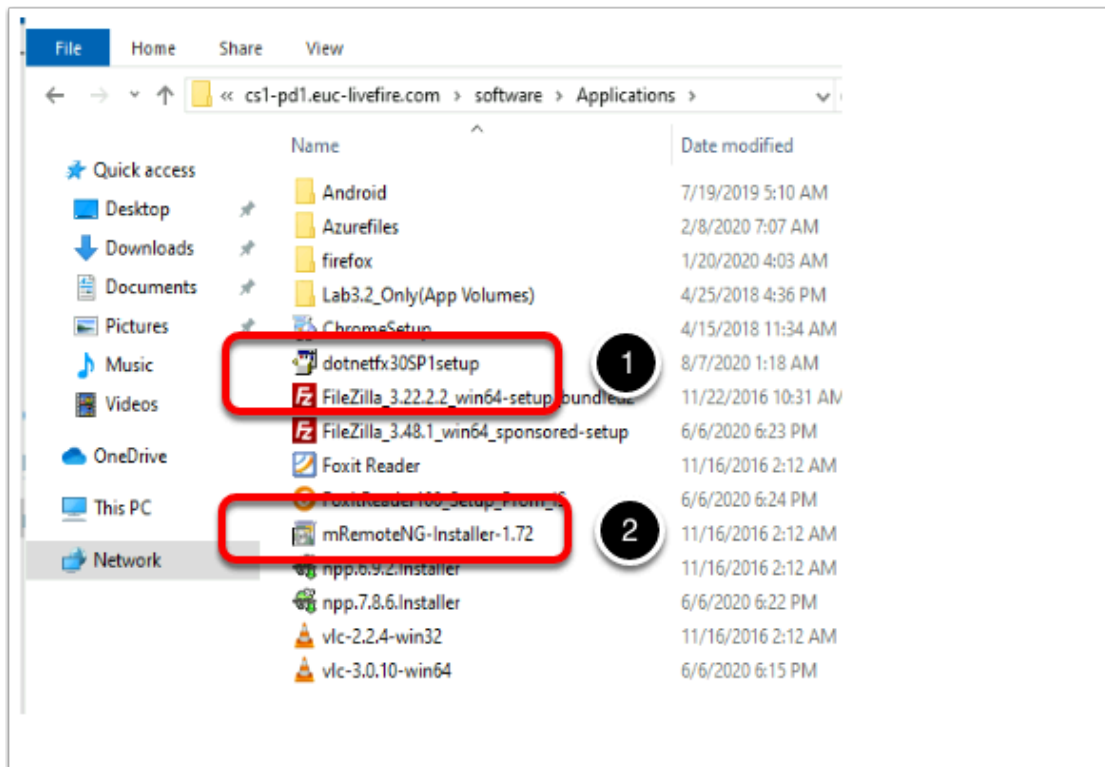
- Select the **Force users to log off** **radio button**,
- **Un-check** the **Stop at first error** checkbox
- Select **Next**
- Select **Finish**

## PART 2: Profiling mRemoteNG

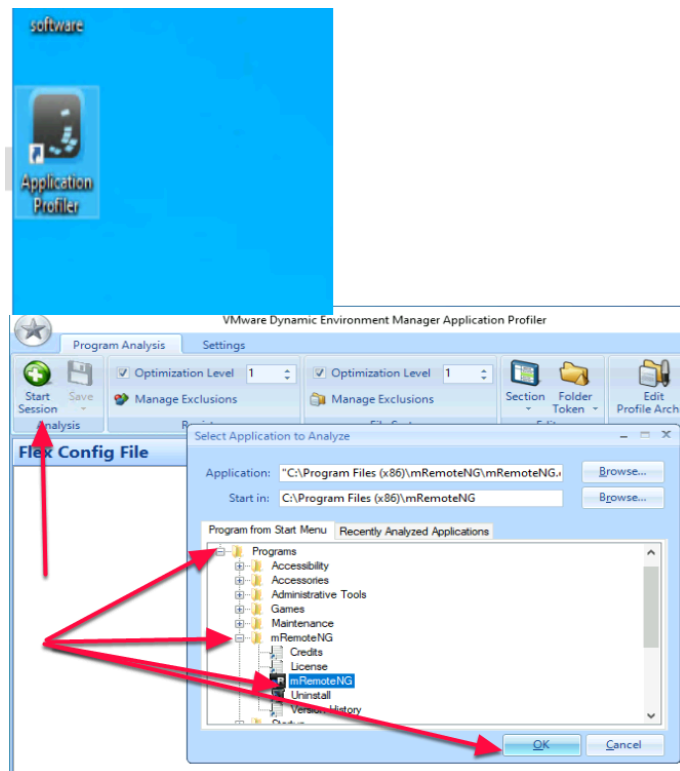
mRemoteNG is a remote desktop utility that can be used by IT administrators. We will build a custom configuration using DEM Application Profiler



1. On your **ControlCenter2** server.
  - In your **Chrome Browser**, select the **vSphere client** tab
  - In the **Hosts & Clusters** inventory select **DEMProfiler** and right-click
    - Select **Snapshots > Revert to Latest Snapshot**
    - In the **Revert to Snapshot** window, select **YES**
    - Select **DEMProfiler**, select **Power > Power On**
      - You might have wait a minute or two for DEMProfiler to **PowerON**

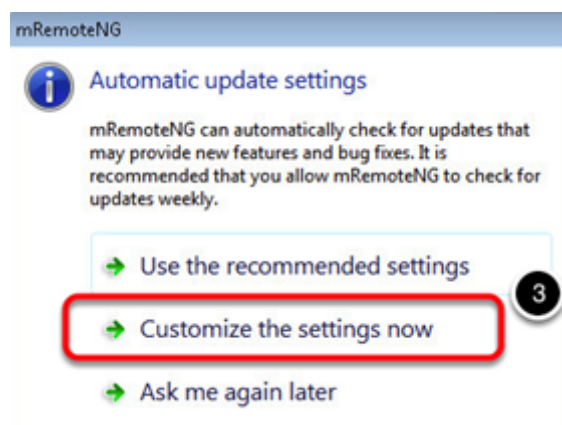


2. On the **ControlCenter2** server desktop
  - Open your **RemoteDesktops** folder and select **DEMPProfiler.RDP** shortcut
- On the **DEMPProfiler** desktop, select the **software** folder
  - Select **Applications**
  - Install the **dotnetfx30sp1setup.exe**
  - Select and double-click the **mRemoteNG-Installer-1.72.exe** application
  - Select **Run** > **OK** > **I Agree** > **Install** > **Next** > **Finish**



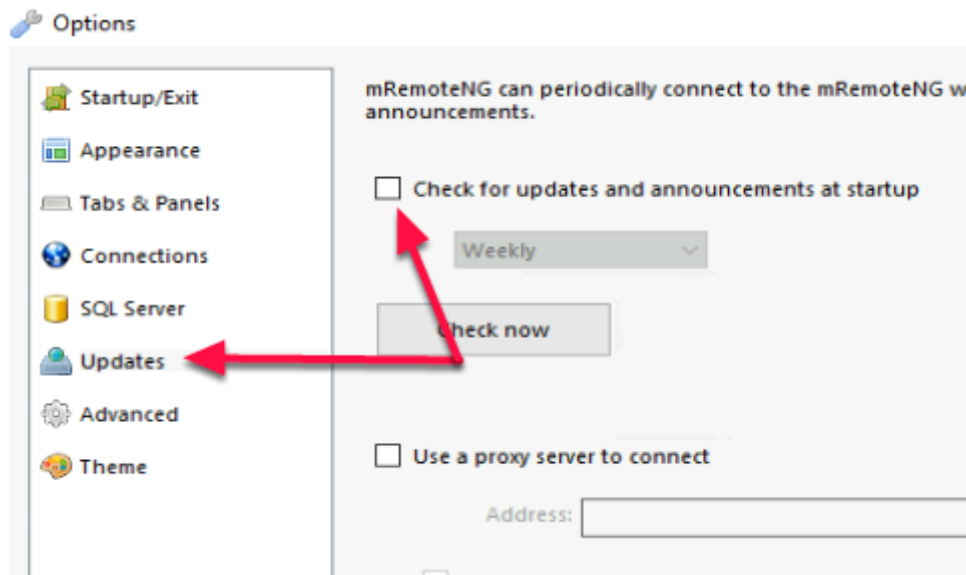
3. On the **DEMProfiler** desktop

- Select the **Application Profiler** shortcut from the Desktop
- Click on **Start Session**. Start a new Analysis by expanding "**Programs**" folder, then "**mRemoteNG**" and choosing the "**mRemoteNG**" application. Click on **OK**



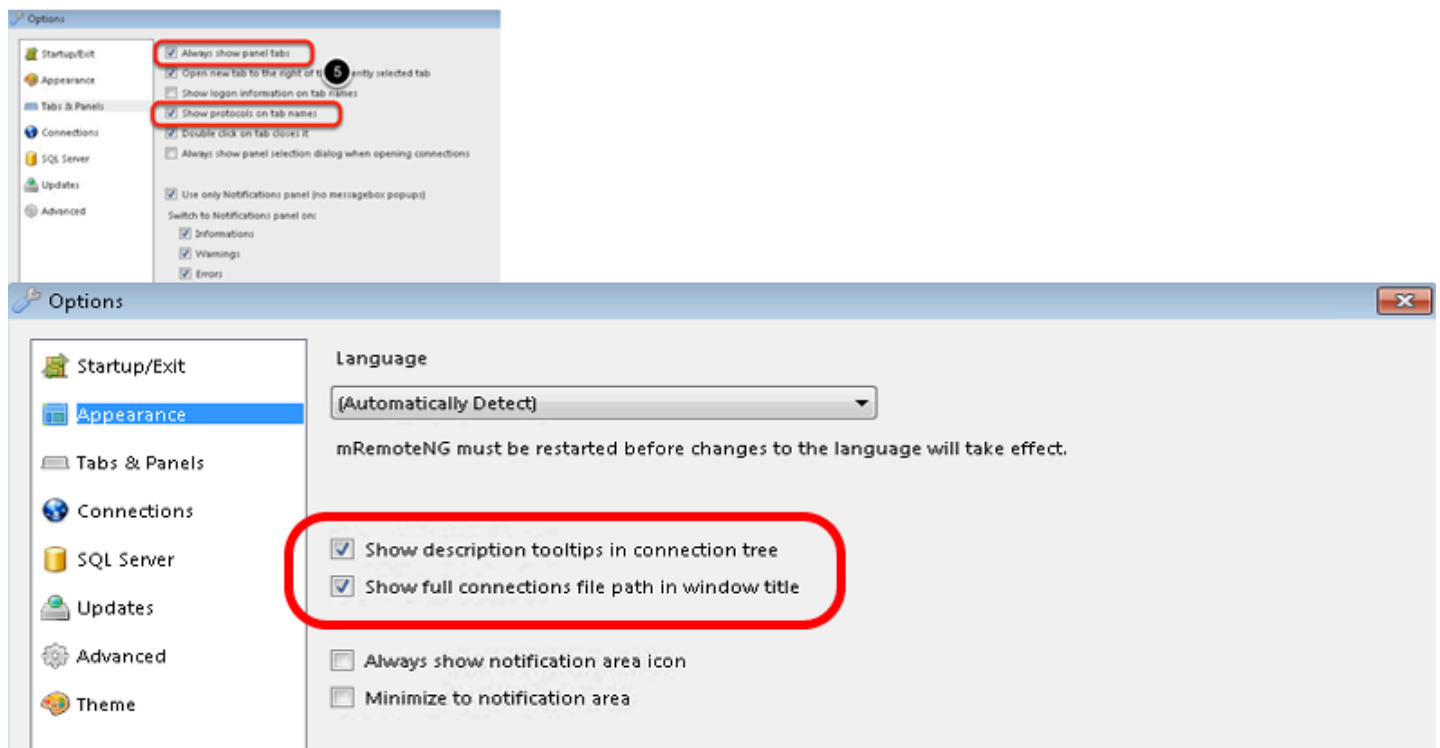
4. On the **DEMProfiler** desktop

- After selecting **OK** you might have to wait up to 30 seconds before the **mRemoteNG** launches
- Since this is the first time opening **mRemoteNG**, choose "**Customize the settings now**".



5. In MRemoteNG Options window

- Uncheck the "**Check for updates and announcement at startup**" checkbox.

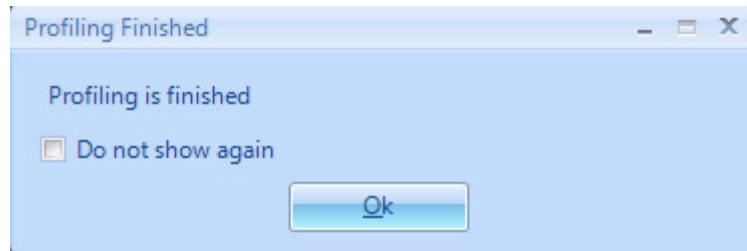


6. In **MRemoteNG Options** window

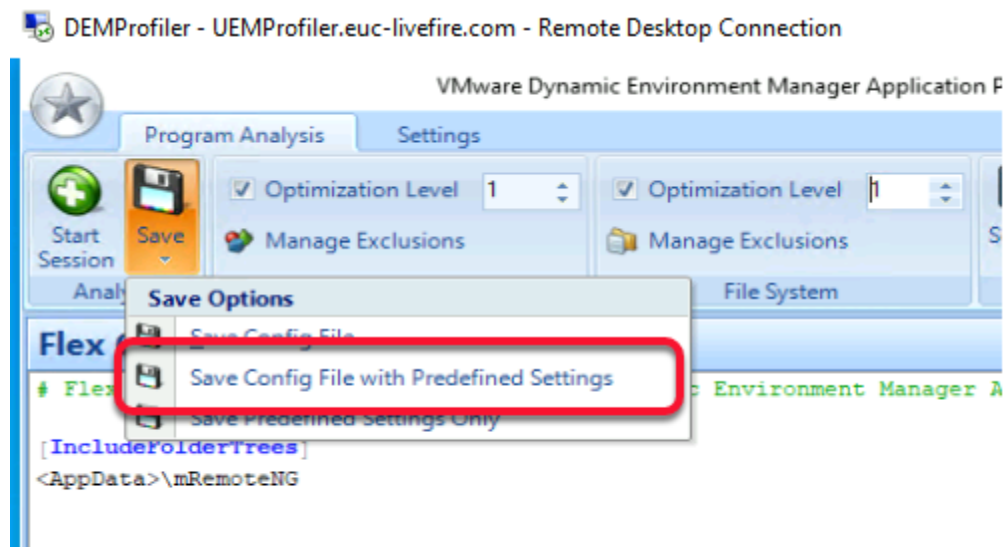
- Select **Tabs & Panels**
  - Check the "**Always show panel tabs**" and "**Show protocols on tab names**".
- Select **Appearance**
  - In the Appearance section select **checkboxes** for
    - **Show description tooltips in connection tree**
    - **Show full connections file path in window title**



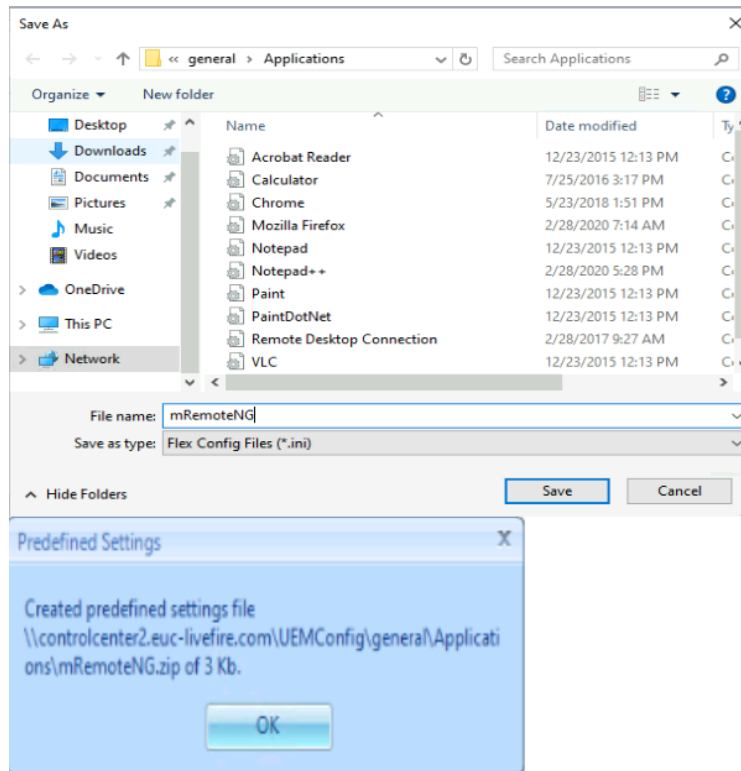
- Close the **Options** window by clicking **OK**
- Close **mRemoteNG**.



7. On the **Profiling finished** window select **Ok**.

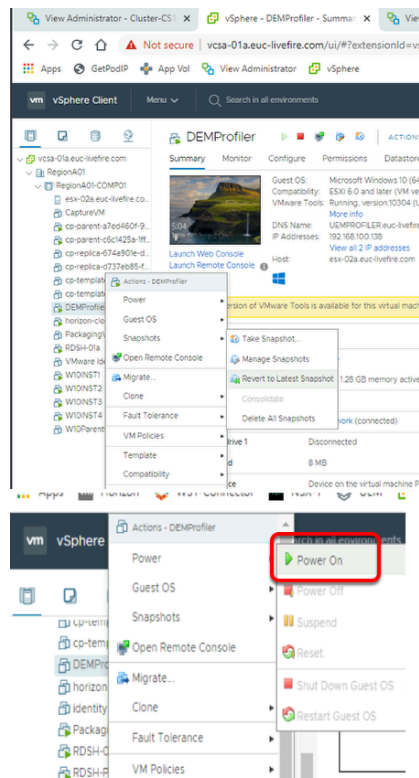


8. On the DEMProfiler application
  - Select **Save**
  - Click on **Save Config File with Predefined Settings**



9. On the DEMProfiler application **Save As** window

- Leave the default chosen directory. Call this file "**mRemoteNG**" and click **Save**,
- Select **OK** to close **Predefined Settings**

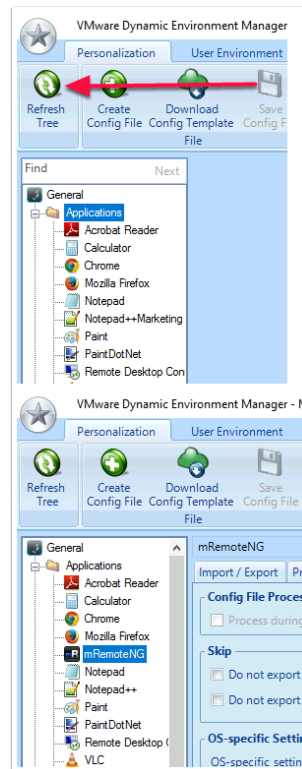


10. Using the vSphere Web client,

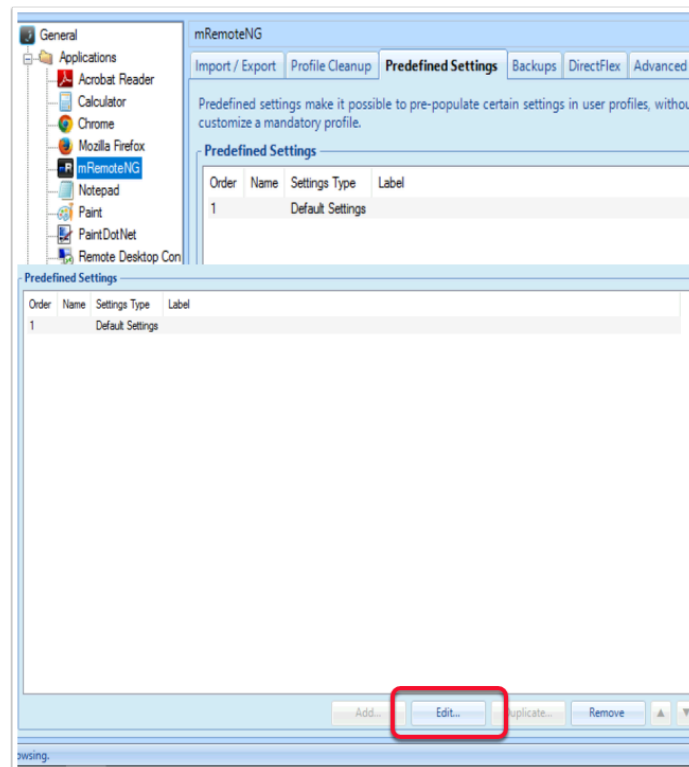
- Select the **DEMProfiler** virtual machine,

- Right click the virtual machine
- Select **Snapshots > Revert to Latest Snapshot**, when prompted, select **YES**
- Select **DEMPProfiler**, right-click, select **Power > Power On**

## PART 3: Application Assignment based on Group Membership

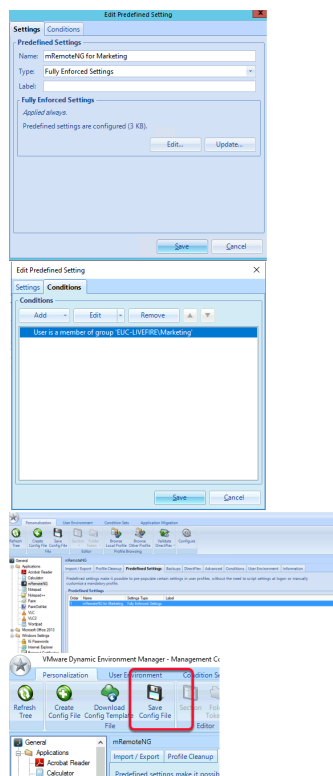


1. On the **ControlCenter2** server
  - From the taskbar, launch the **Dynamic Environment Manager** Console
  - Under **General**, select **Applications**,
  - Select **Refresh Tree**
  - Expand **Applications**
  - Select **mRemoteNG**



## 2. In the Dynamic Environment Manager Console

- After selecting MRemoteNG, select the **Predefined Settings** tab.
- Under **Predefined Settings** select **Default Settings** and select **Edit**



## 3. In the Dynamic Environment Manager Console

- Next to **Name** type "**mRemoteNG for Marketing**"

- Next to **Type:** select **Fully Enforced Settings**
- Select the **Conditions** tab, select **Add**, select **Group Membership** and assign to **Marketing**
- Select **Save** to close the **Edit Predefined Settings** window
- Select **Save Config File**

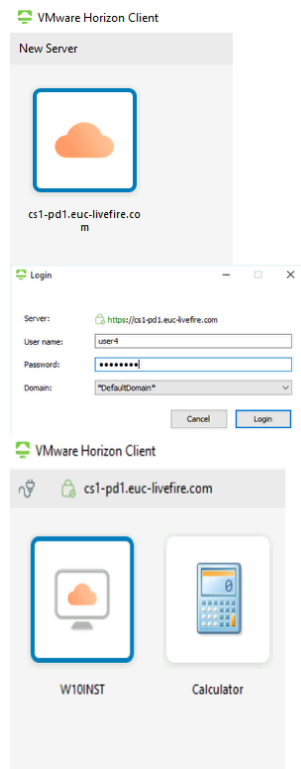
### In Summary:

- We have deployed mRemoteNG in Horizon.
- We are now going to test the Application Configuration we created in Application Profiler.
  - It is very likely the test will fail.
- We will then go and see what we need to do to edit the Configuration to ensure Application settings are captured.
- We will then re-test the application.

## PART 4: Testing application Conditions

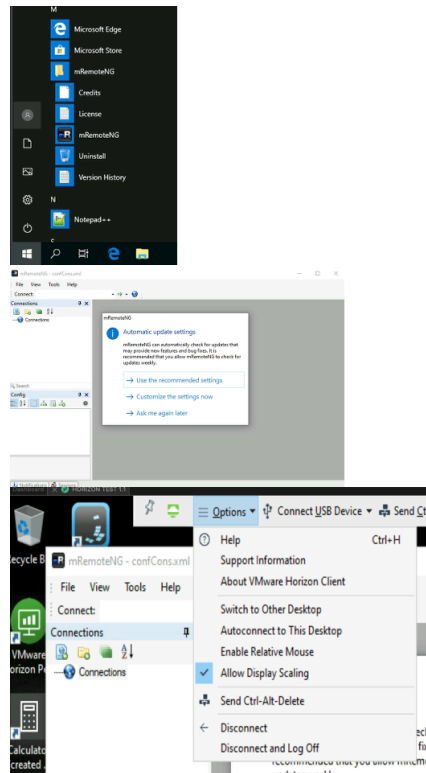


1. From your **ControlCenter2** server desktop,
  - Select the **VMware Horizon Client**



## 2. In the Horizon Client Console

- Select your **CS1-PD1.euc-livewire.com** entitlement and login with the following user credentials
  - **Username:** User4
  - **Password:** VMware1!
- Select **Login**
- Select your **W10INST** entitlement



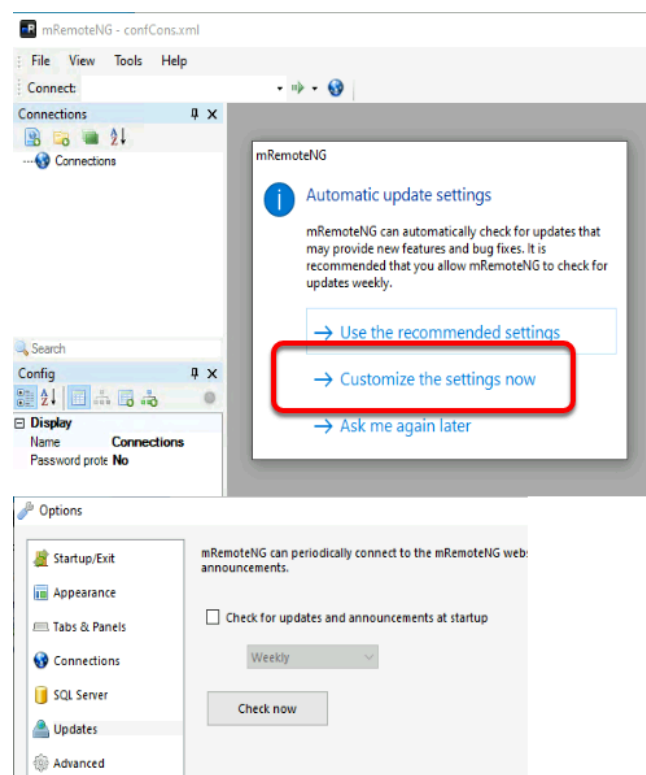
### 3. On your **Windows 10 vDI** session

- Select your **START** menu
- Launch your **mRemoteNG** application
  - Notice your application settings have not been saved
    - If we select **Customize the Settings Now**,
    - In the **Options** window select **Updates**.
      - Notice the **Check for updates and announcements at startup checkbox** is still enabled
      - It therefore means something did not work with DEM Application Profiler tool
      - We will therefore go and see what the issue is.
- **Disconnect and Logoff** from the Windows 10 instant-clone desktop

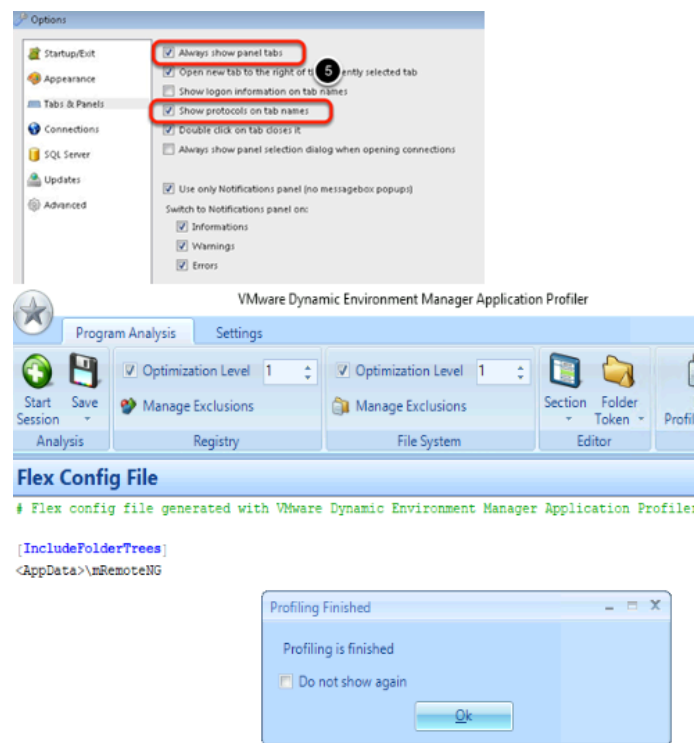




4. From your **ControlCenter2** Desktop.
  - From the **RemoteDesktops** folder.
  - Launch the **DEMProfiler.RDP** shortcut,
    - login with the password **VMware1!**
- On the **DEMProfiler** desktop,
  - Select the **Software** shortcut and install the **dotnetfx30SP1setup.exe** and **RemoteNG** from the **Applications** folder.
  - From the **DEMProfiler** desktop, launch the Application Profiler shortcut
  - Click on **Start Session**. Start a new Analysis by expanding "**Programs**" folder, then "**mRemoteNG**" and choosing the "**mRemoteNG**" application.
  - Click on **OK**.
  - After selecting **OK** you might have to wait a few moments before the **mRemoteNG** launches

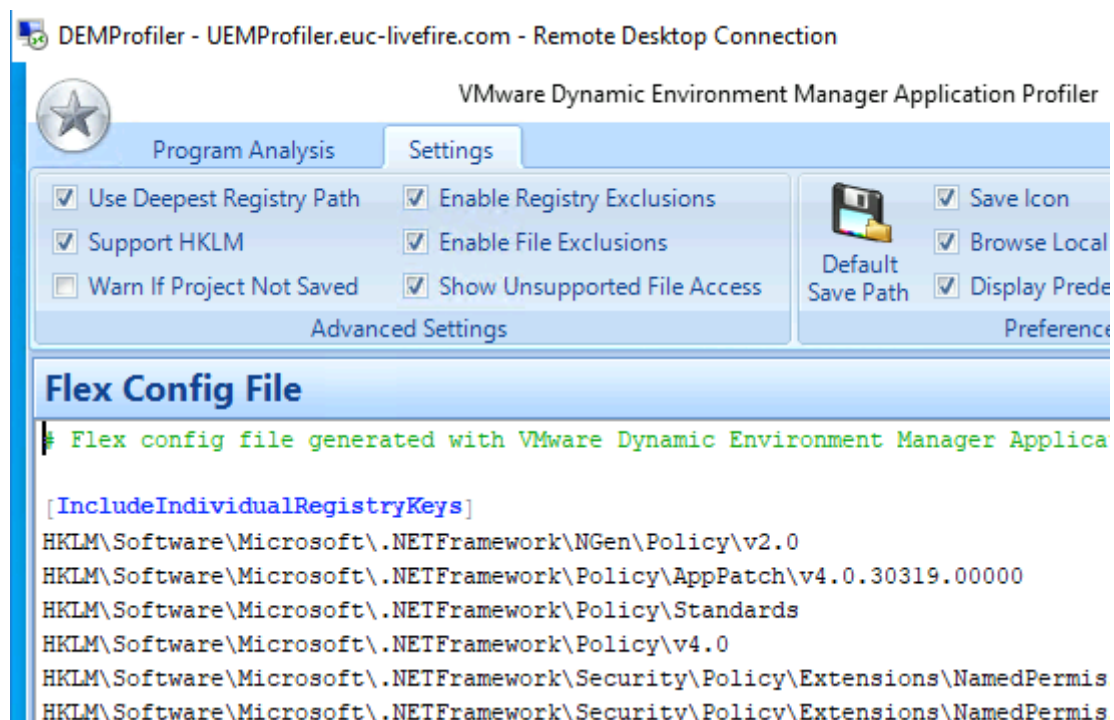


5. Since this is the first time opening **mRemoteNG**, choose "**Customize the settings now**".
  - The first section we will configure is the **Updates** section. **Uncheck** the "**Check for updates and announcement at startup**" checkbox.

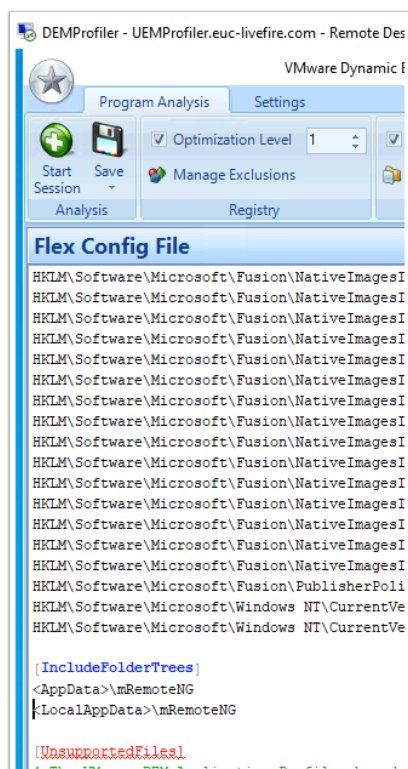


6. Second, let's change some configuration in the **Tabs & Panels** section.

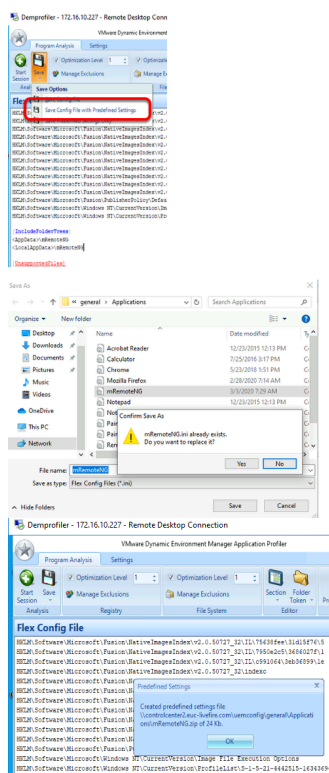
- Check the "**Always show panel tabs**" and "**Show protocols on tab names**".
- Close the **Options** window by clicking **OK** and then close **mRemoteNG**. Application Profiler will re-open.
- Click **OK** to close the **Profiling Finished** window



7. Go to **Settings** and select the **Support HKLM** check box and **Show Unsupported File Access**

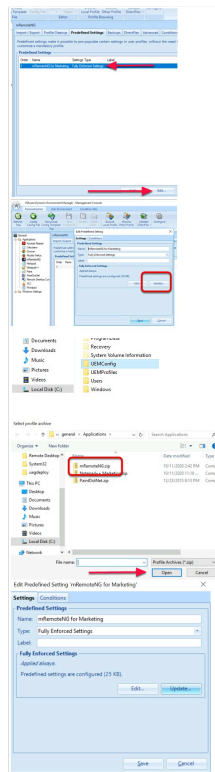


8. Scroll down and find Under **[IncludeFolderTrees]**, type in the following line  
**<LocalAppData>\mRemoteNG**



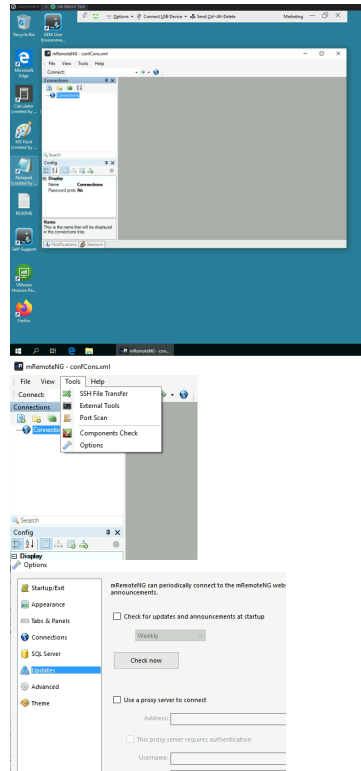
9. In the Application Profiler console

- Select the **Program Analysis** Tab
- Select **Save** and select **Save Config File with Predefined Settings**,
- Select the existing **mRemoteNG** file > When prompted **to Replace**, select **Yes** , select **Save**
- Click **Ok** when to complete the capture process



- On your **ControlCenter2** desktop,
  - Switch back to the **VMware Dynamic Environment Manager** Console
  - Select the **mRemoteNG** application configuration,
    - Select the **Predefined Settings** tab,
    - Select **mRemoteNG for Marketing**
    - Select **Edit**
  - In the Edit Predefined Setting mRemoteNG for Marketing select **Update...**
  - Browse to **C:\UEMConfig\General\Applications**
  - Select **mRemoteNG.zip** and select **Open**
  - Select **Save**
  - On top of the DEM console select **Save Config File**

## PART 5: Re-Testing Application Configuration



1. On your ControlCenter2 desktop,
  - Re-launch your **Horizon** Client shortcut
  - Login as **user4** with the password **VMware1!**
  - Launch You will now notice that when **mRemoteNG** launches it retains its settings, the user is not prompted to do customizations like they had done previously.
  - On the mRemoteNG application, select **Tools > Options**, on the **Startup/Exit**, select **all check boxes** and select **Ok** and **close** mRemoteNG
  - Relaunch mRemoteNG and notice that all configurations are lost
  - When you are complete **Logoff** from your desktop.