

Horizon Integration with Untrusted Active Directory Forests

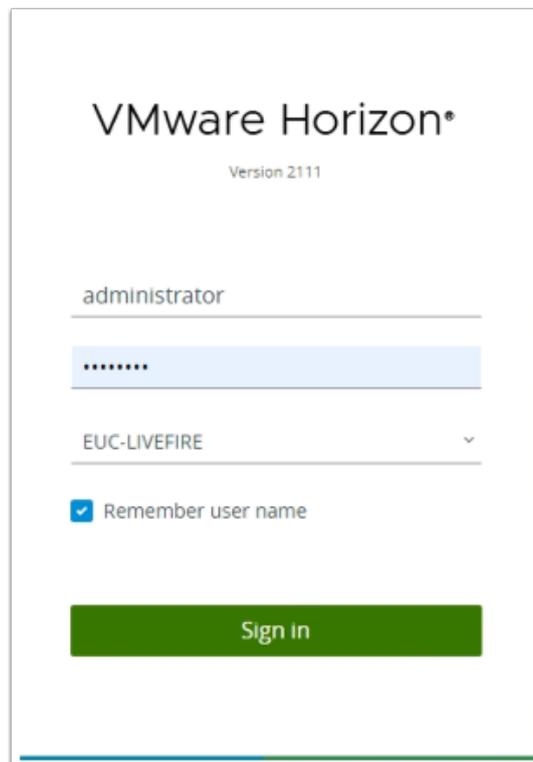
For as long as Horizon and View have existed, if a Horizon Pod needed to give users access to Horizon based resources. All Active Directory domains had to have at least a one-way AD Trust with the Horizon Domain. The Horizon Domain would have to be Trusted to read the Domain objects in the User Domain.

Many organization's setup separate Active Directory Forests for security reasons, yet they want to give users Access through a singular Horizon Pod. In the past this was almost impossible.

Recently with the 2103 release of Horizon a very simple solution has been developed to allow users from Untrusted Active Directory Domains, access to Horizon resources in an alternate untrusted Active Directory Domain Forest .

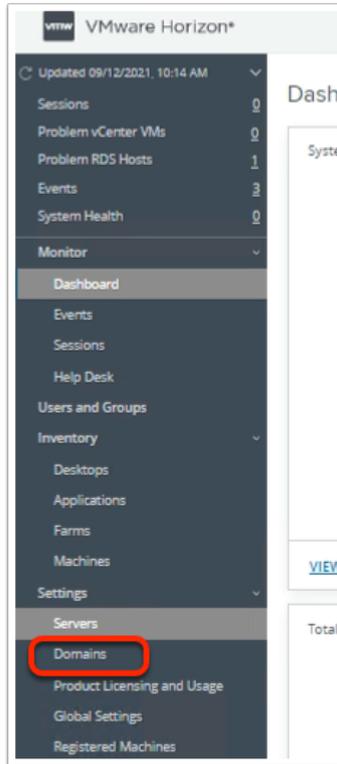
In this session we will walk you through the process of configuring a Domain Bind account and configuring Horizon resources to facilitate this process

Part 1: Configuring Domain Bind and Instant Clone Engine Domain Accounts



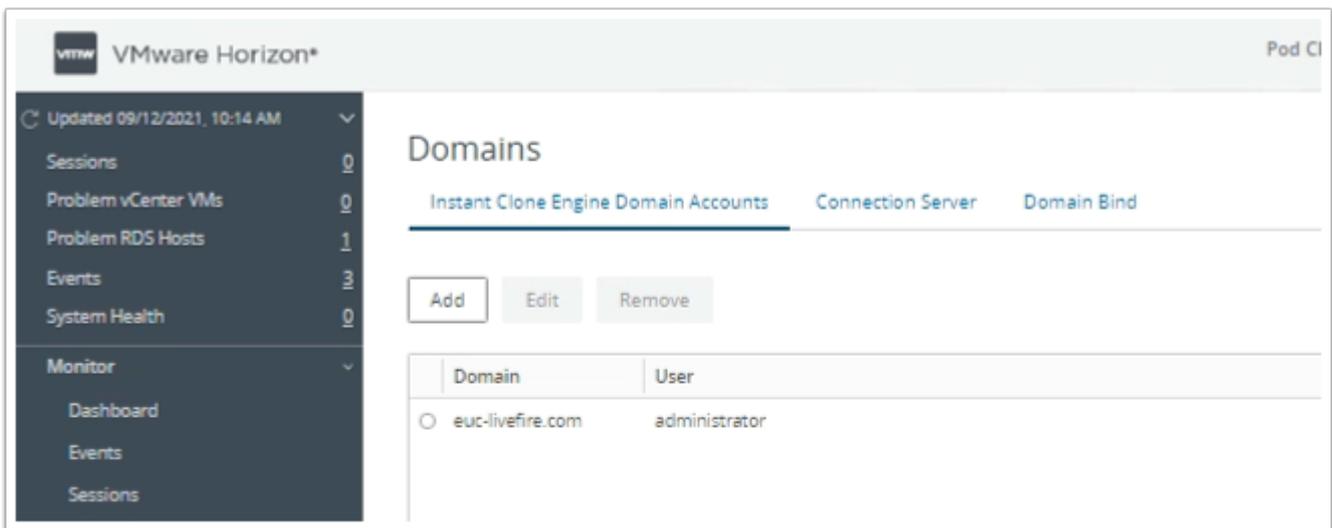
1. On your ControlCenter server
 - Open your **Chrome Browser**
 - In the Favourites Bar, launch the **VMware Horizon** shortcut
 - Login as username **Administrator**

- Login with the password **VMware1!**
- Select **Sign in**



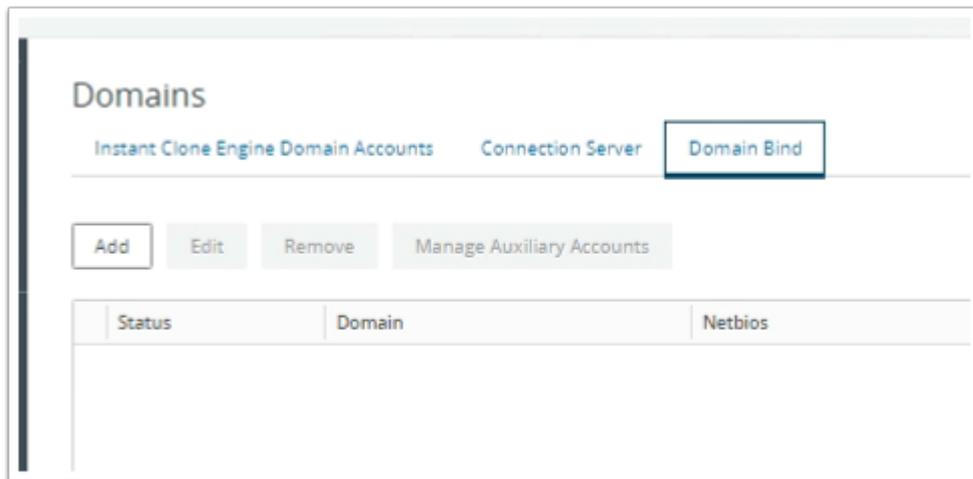
2. In the Horizon Admin Console

- In the left Inventory pane, under **Settings**, select **Domains**

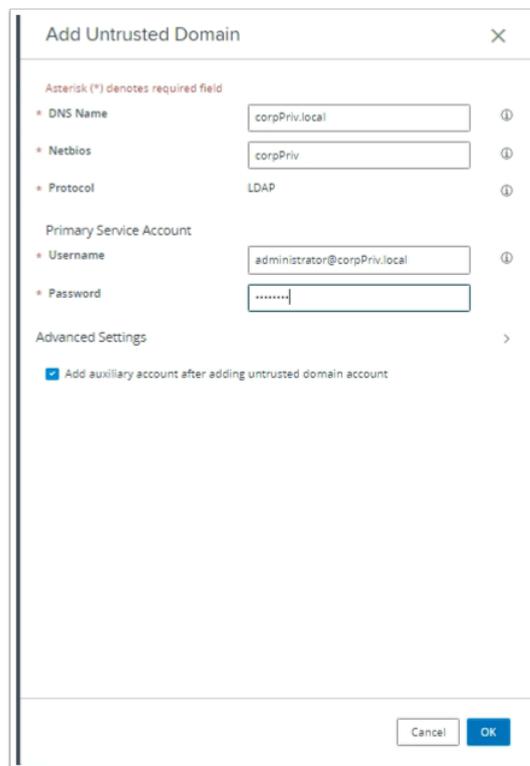


3. In the Horizon Admin Console

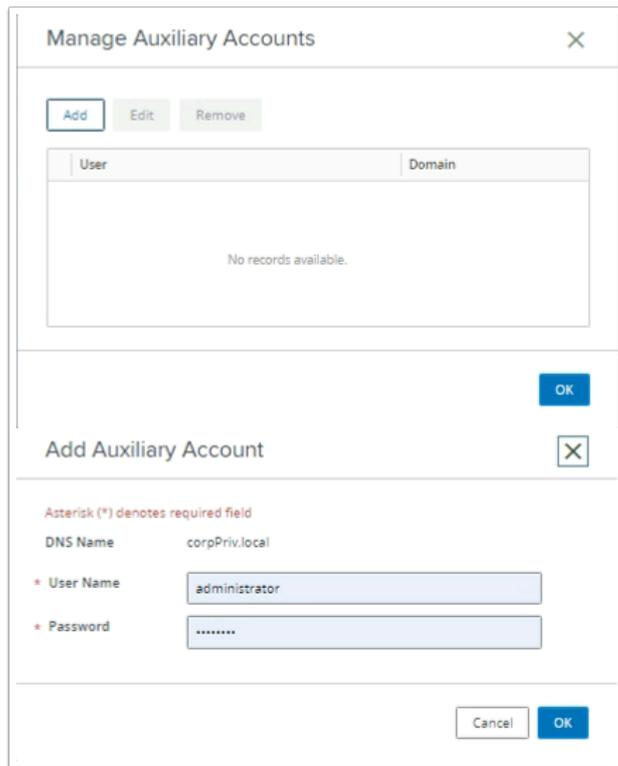
- Under **Domains** area
 - Select the **Domain Bind** tab



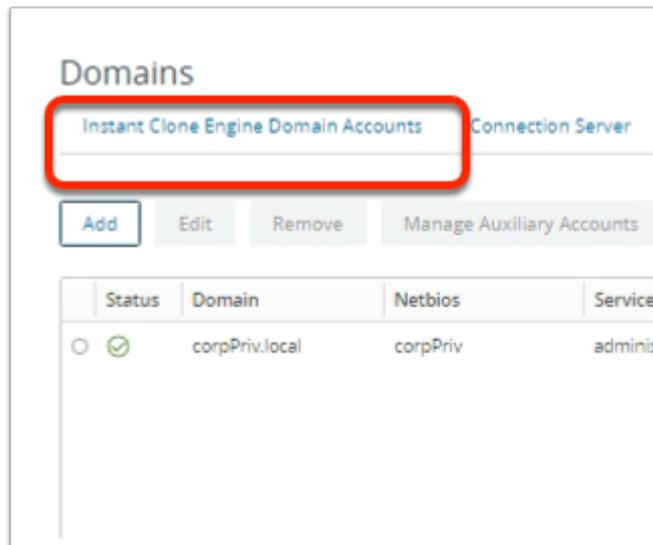
4. In the Horizon Admin Console
 - Under **Domains** area > **Domain Bind**
 - Select **Add**



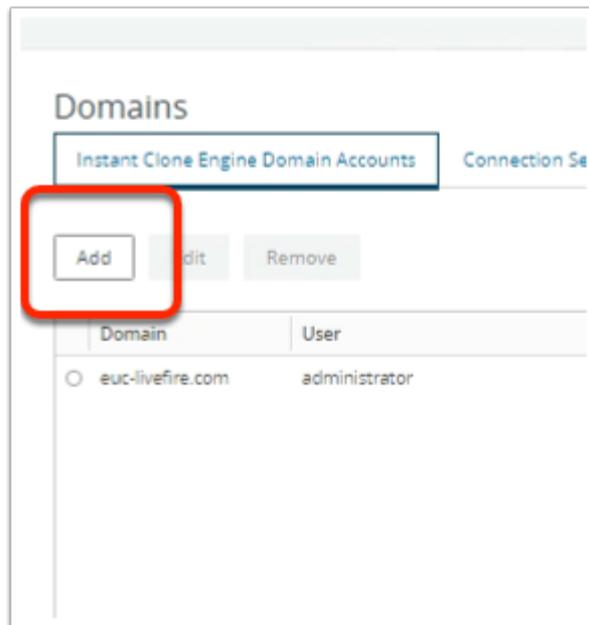
5. In the **Untrusted Domain** window
 - Add the following, next to:-
 - **DNS Name:** corpPriv.local
 - **Netbios:** corpPriv
 - **Username:** administrator@corpPriv.local
 - **Password:** VMware1!
 - Select **OK**



6. In the **Manage Auxiliary Accounts** window
 - Select **Add**
 - In the **Add Auxiliary Account** window
 - Select **OK**
 - Select **OK**, to close the **Manage Auxiliary Accounts** window



7. In the Horizon Admin Console
 - Under **Domains** area
 - Select the **Instant Clone Engine Domain Accounts** tab



8. In Domains Area

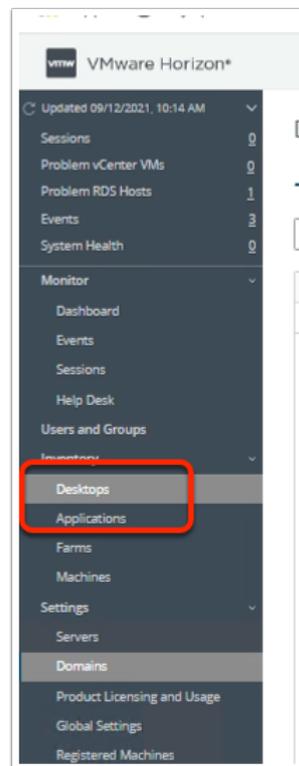
- Select **Add**

The screenshot shows a dialog box titled 'Add Domain Admin'. It has a close button (X) in the top right corner. The dialog contains three input fields: 'Full Domain Name' (a dropdown menu showing 'corpPriv.local'), 'Username' (a text box containing 'administrator'), and 'Password' (a text box with masked characters '.....'). At the bottom right, there are two buttons: 'Cancel' and 'OK'.

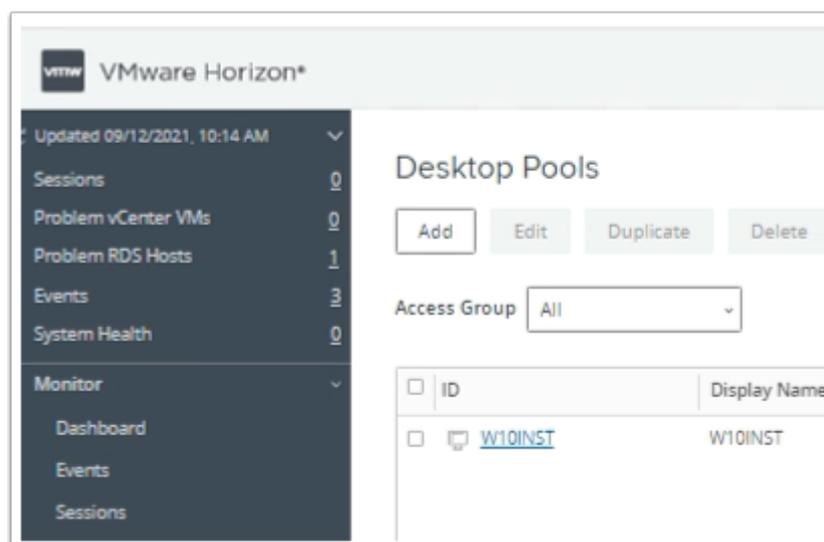
9. In the Add Domain Admin window

- Add the following next to:-
 - **Full Domain Name:** from the dropdown, select **corpPriv.local**
 - **Username:** type **Administrator**
 - **Password:** type **VMware1!**
 - Select **OK**

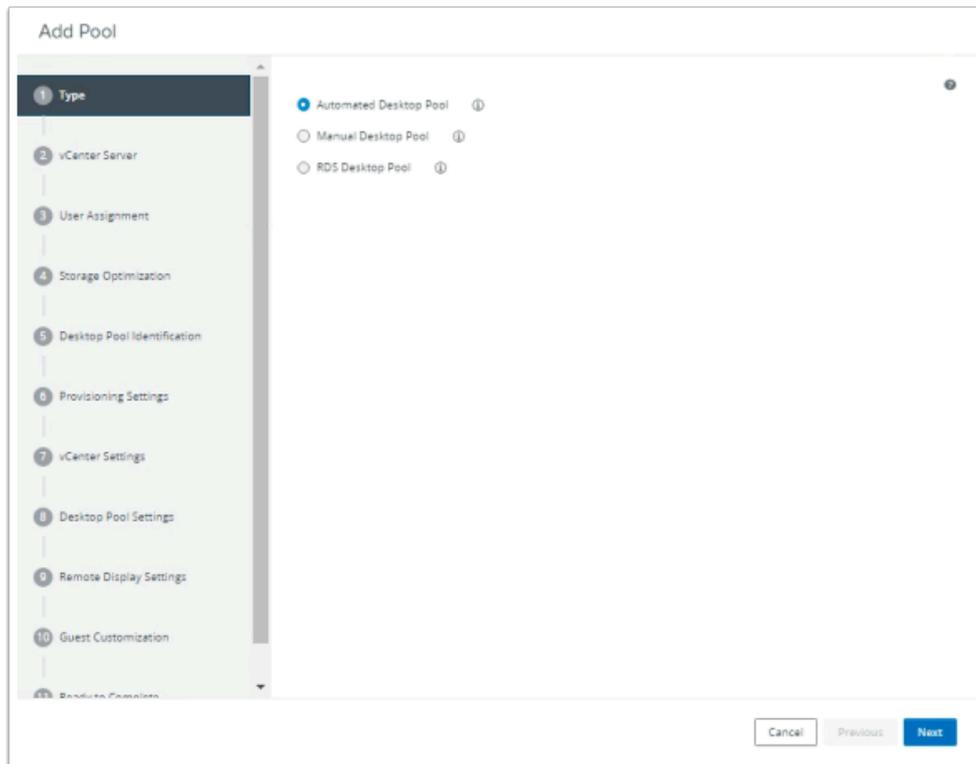
Part 2: Configuring a Desktop Pool Assignment for the Untrusted Active Directory Domain



1. In the **Horizon Admin** Console
 - In the left Inventory pane
 - Under **Inventory**, select **Desktops**

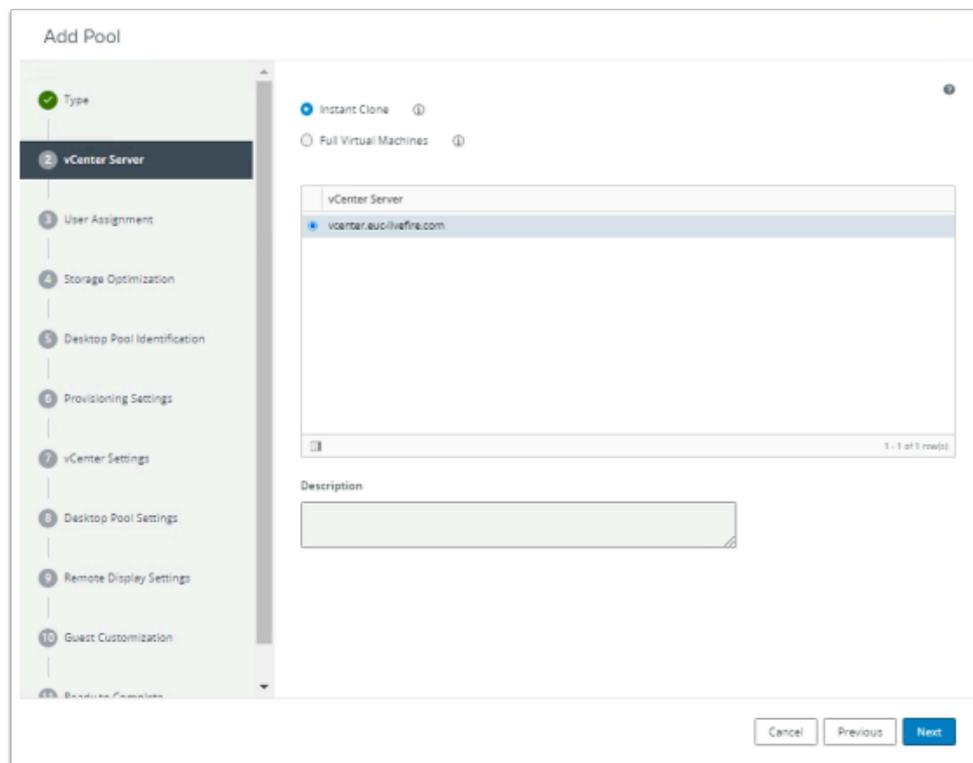


2. In the **Desktop Pools** area
 - Select **Add**



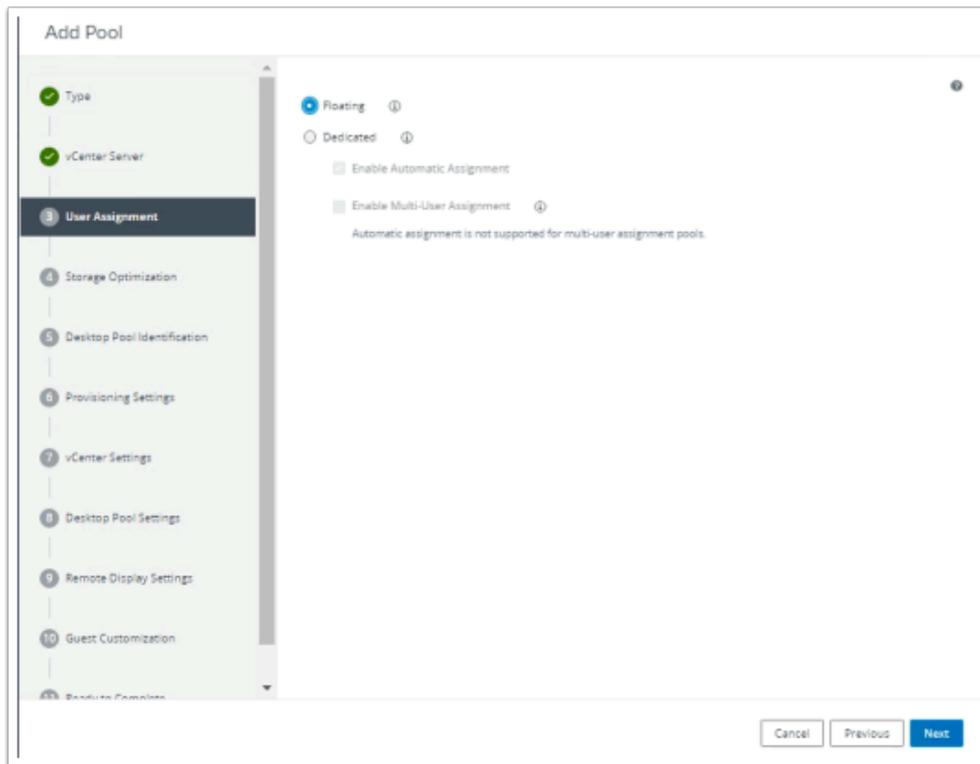
3. In the **Add Pool** wizard

- Select **Next**



4. In the **Add Pool** wizard

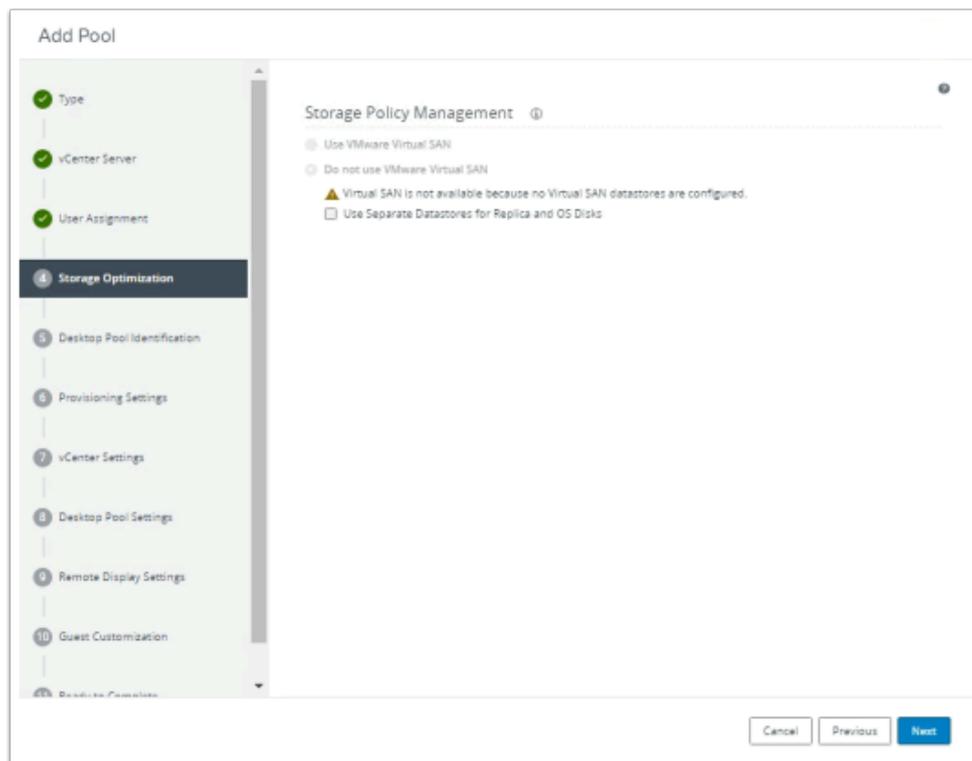
- **vCenter Server**
- Select **Next**



5. In the **Add Pool** wizard

- **User Assignment**

- Select the **radio button** next to **Floating**
- Select **Next**



6. In the **Add Pool** wizard

- **Storage Optimization**
 - Select **Next**

The screenshot shows the 'Add Pool - CorpPrivW10' wizard. The left sidebar indicates the current step is '5 Desktop Pool Identification'. The main form area contains the following fields:

- ID** (required): CorpPrivW10
- Display Name**: W10_CorpPriv
- Access Group**: /
- Description**: (empty text area)

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

7. In the **Add Pool** wizard

- **Desktop Pool Identification**, update the following areas:-
 - Under **ID** enter **CorpPrivW10**
 - Under **Display Name** enter **W10_CorpPriv**
 - Select **Next**

The screenshot shows the 'Add Pool - CorpPrivW10' wizard in the Provisioning Settings step. The left sidebar lists steps 1 through 11, with 'Provisioning Settings' selected. The main content area includes:

- Basic:**
 - Enable Provisioning
 - Stop Provisioning on Error
- Virtual Machine Naming:**
 - Specify Names Manually
 - Use a Naming Pattern
 - Naming Pattern: w10CorpPriv
- Provision Machines:**
 - Machines on Demand
 - All Machines Up-Front
- Desktop Pool Sizing:**
 - Maximum Machines: 2
 - Spare (Powered On) Machines: 1
- Virtual Device:**
 - Add vTPM Device to VMs

Buttons at the bottom: Cancel, Previous, Next.

8. In the **Add Pool - CorpPrivW10** wizard

- **Provisioning Settings**

- Under **Use a Naming Pattern** enter **w10CorpPriv**
- Under **Display Name** enter **W10CorpPriv**
- Under **Desktop Pool sizing > Maximum Machines** enter **2**
- Select **Next**

The screenshot shows the 'Add Pool - CorpPrivW10' wizard in vCenter. The left sidebar lists the steps: Type, vCenter Server, User Assignment, Storage Optimization, Desktop Pool Identification, Provisioning Settings, vCenter Settings (highlighted), Desktop Pool Settings, Remote Display Settings, Guest Customization, and Ready to Complete. The main content area is divided into three sections:

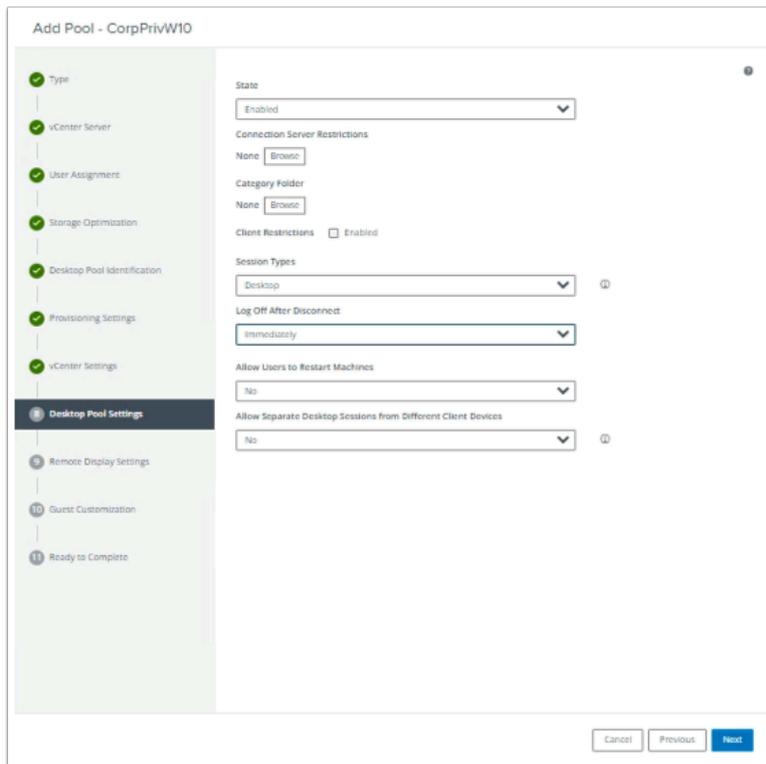
- Default image:** Includes 'Golden image in vCenter' with a text field containing '/RegionA01/vm/Discovered virtual machine/w10Parent01a' and a 'Browse' button. It also includes 'Snapshot' with a text field containing '/Baseline' and a 'Browse' button.
- Virtual Machine Location:** Includes 'VM Folder Location' with a text field containing '/RegionA01/vm' and a 'Browse' button.
- Resource Settings:** Includes 'Cluster' with a text field containing '/RegionA01/host/RegionA01-COMP01' and a 'Browse' button. It also includes 'Resource Pool' with a text field containing '/RegionA01/host/RegionA01-COMP01/Resources' and a 'Browse' button. Below this is 'Datastores' with a dropdown showing '1 selected' and a 'Browse' button. Finally, there is a 'Network' section with the text 'Golden Image network selected' and a 'Browse' button.

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

9. In the **Add Pool - CorpPrivW10** wizard

- **vCenter Settings**

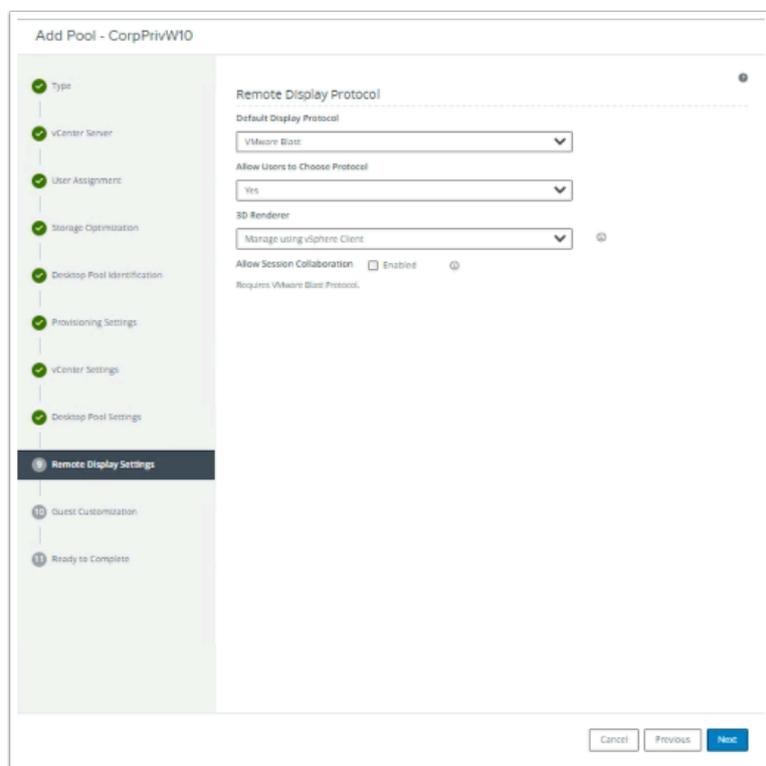
- **Browse** and **submit** to the following:- Under:-
 - Under **Golden Image in vCenter:** **Browse** to **W10Parent01a** and **Submit**
 - Under **Snapshot** **Browse** to **/Baseline** and **Submit**
 - Under **VM Folder Location** **Browse** to **RegionA01** and **Submit**
 - Under **Resource Settings > Cluster** **Browse** to **RegionA01-COMP01** and **Submit**
 - Under **Resource Settings > Resource Pool** **Browse** to **RegionA01-COMP01** and **Submit**
 - Under **Resource Settings > Datastores** **Browse** to **CorpLUN2** and **Submit**
 - In the **Warning** window select **OK**
- Select **Next**



10. In the **Add Pool - CorpPrivW10** wizard

- **Desktop Pool Settings**

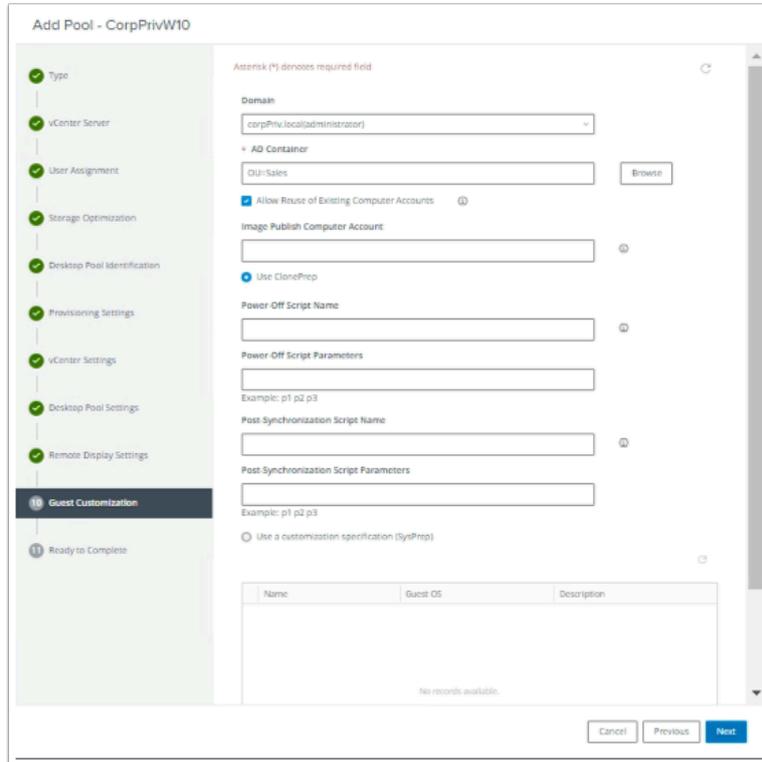
- Under **Log off After Disconnect:** from the dropdown select **Immediately**
- Select **Next**



11. In the **Add Pool - CorpPrivW10** wizard

- **Remote Display Settings**

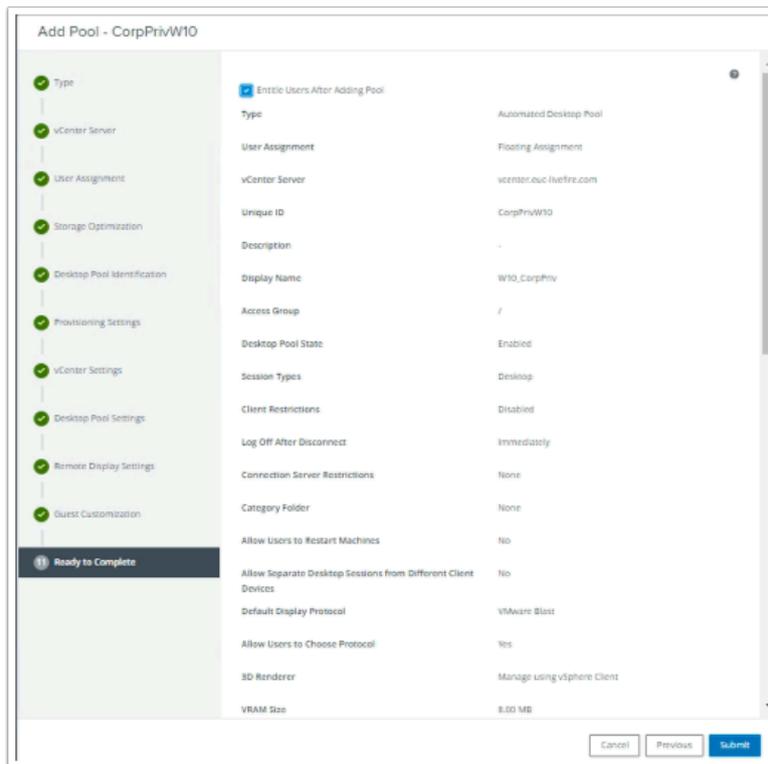
- Select **Next**



12. In the **Add Pool - CorpPrivW10** wizard

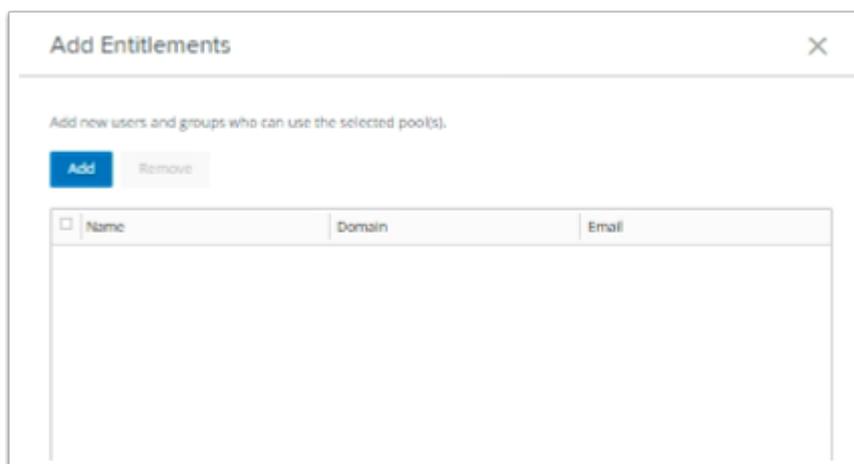
- **Guest Customization**

- **Browse** and **submit** to the following:- Under:-
 - Under **AD Container:** **Browse** to **OU=Sales** and **Submit**
 - Select the **checkbox** next to **Allow Reuse of Existing Computer Accounts**
- Select **Next**



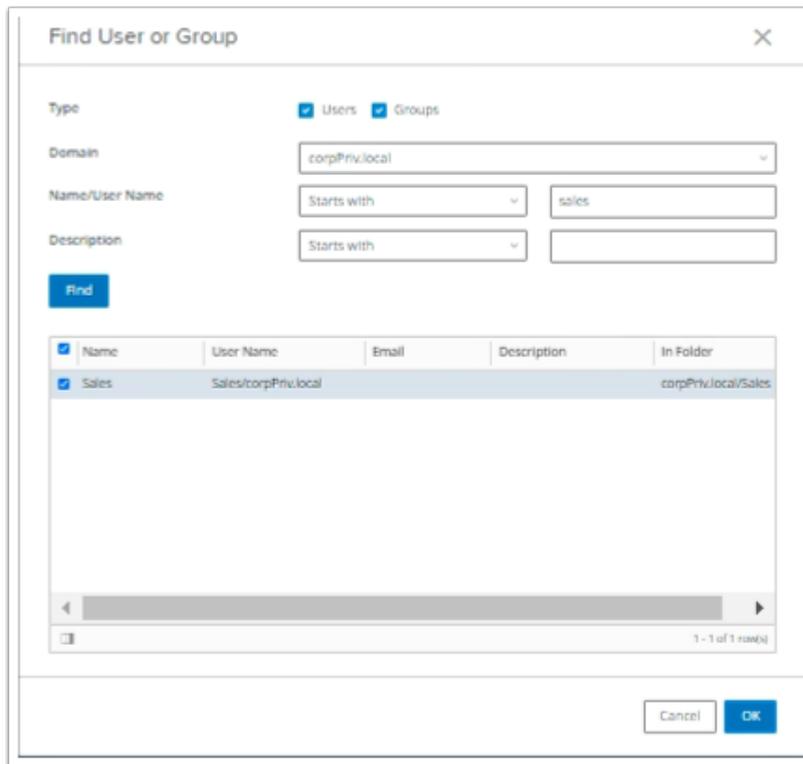
13. In the **Add Pool - CorpPrivW10** wizard

- **Ready to Complete**
 - Select the **checkbox** next to **Entitle Users After Adding Pool**
 - Select **Submit**



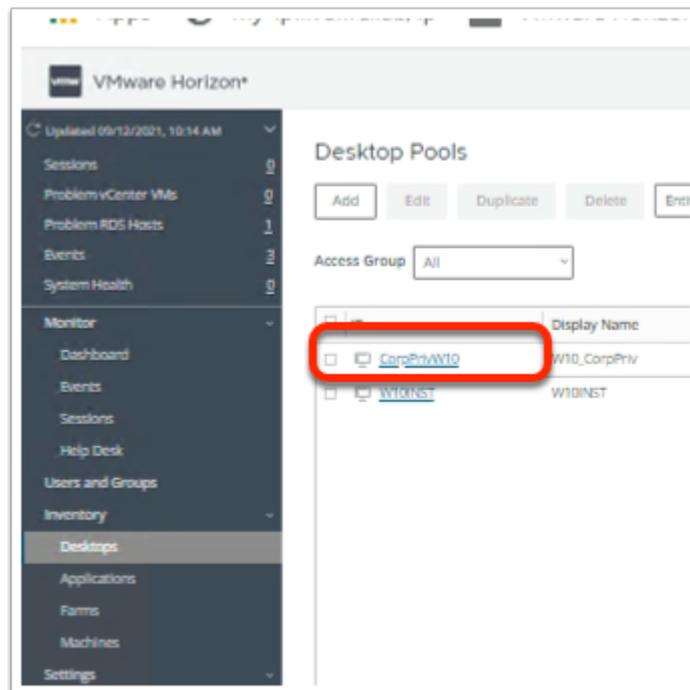
14. In the **Add Entitlements** window

- Select **Add**



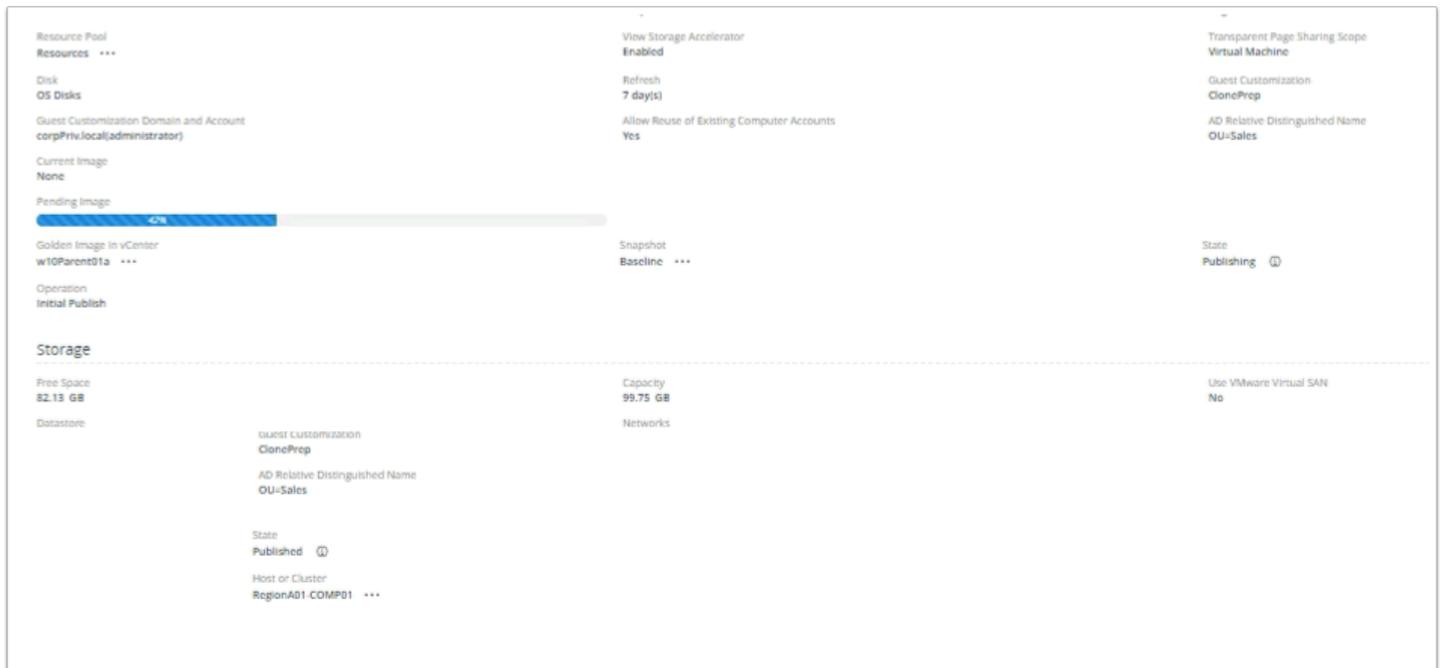
15. In the **Find User or Group** window

- Next to **Domain**, from the dropdown, select **corpPriv.local**
- Next to **Name/User Name**, to the right of **Starts with**, enter **sales**
 - Select **Find**
 - Under **Find** select **Sales**
- Select **OK**
- Select **OK**



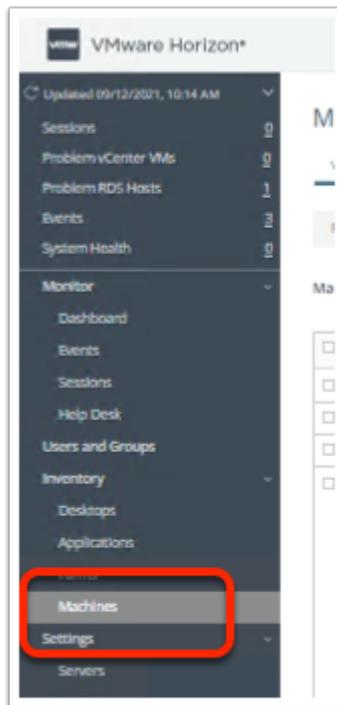
16. In the Desktop Pools area

- Select **CorpPrivW10**



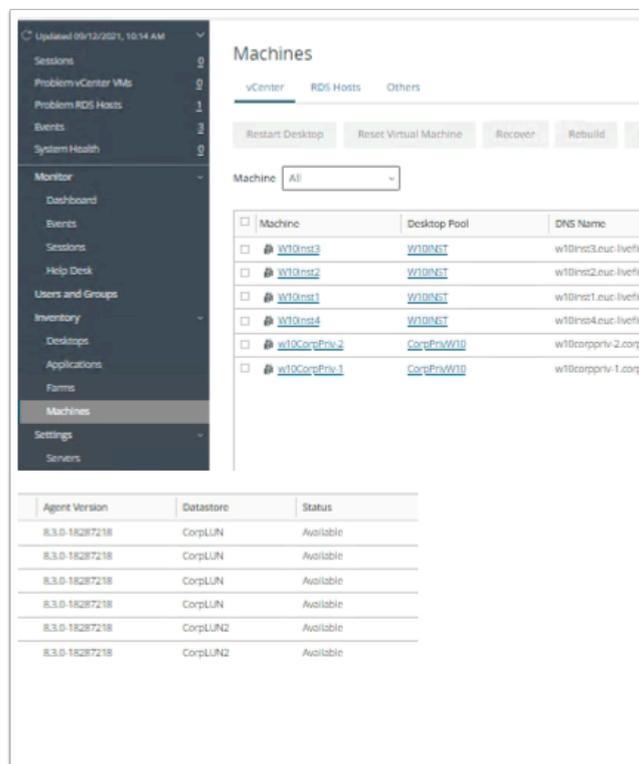
17. In the **CorpPrivW10** area

- Under the **Summary** tab,
 - Scroll down to **Pending Image**
 - View the progress of the pool being Provisioned
 - To the right notice the **State** is **Publishing**
 - When complete this will report as **Published**
 - The page does not dynamically update. You will have to refresh periodically.
 - This can be done by selecting the **Refresh icon** in the top right-corner of the **Summary** page
 - You will need to have to wait until the Pool is **Published**



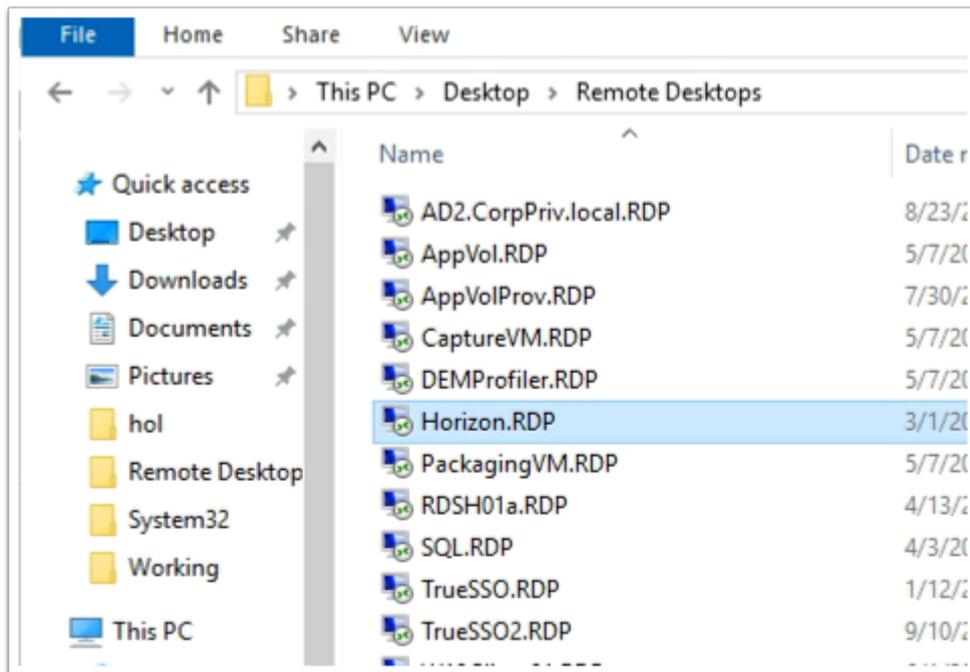
18. In the Horizon Admin Console

- Under **Inventory**
 - Select **Machines**



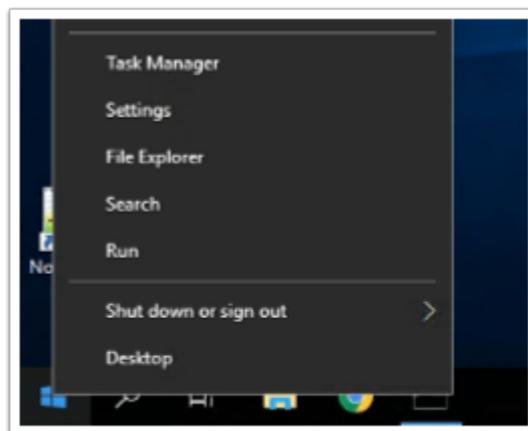
19. In **Machines** area

- Look for your **CorpPrivW10** virtual Machines
- Wait until the **Status** is **Available**



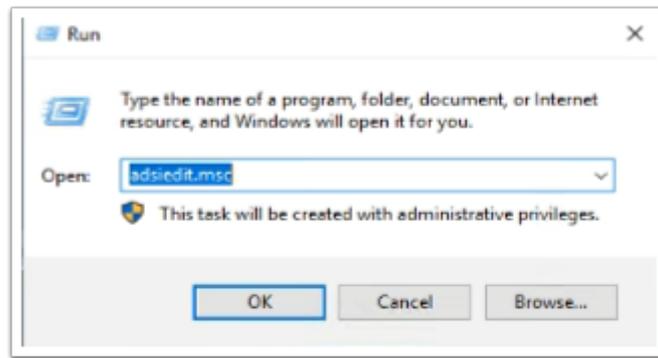
20. On your Controlcenter server

- Open the **Remote Desktops** Folder
- Launch the **Horizon.RDP** shortcut
 - Note. you should automatically be authenticated with the account Administrator@euc-livewire.com



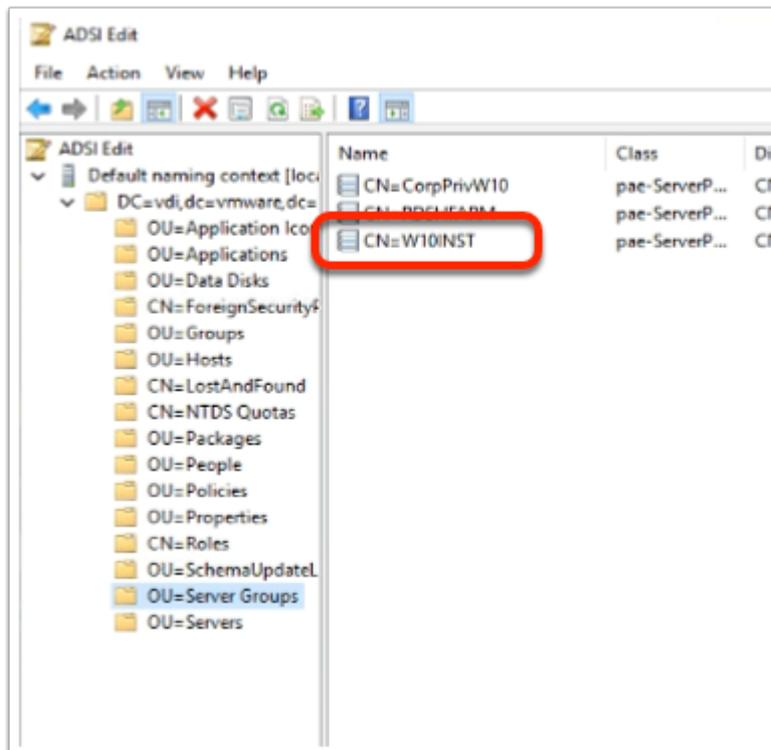
21. On the **Horizon Desktop**

- Select and right-click the **Start** button
- Select **Run**



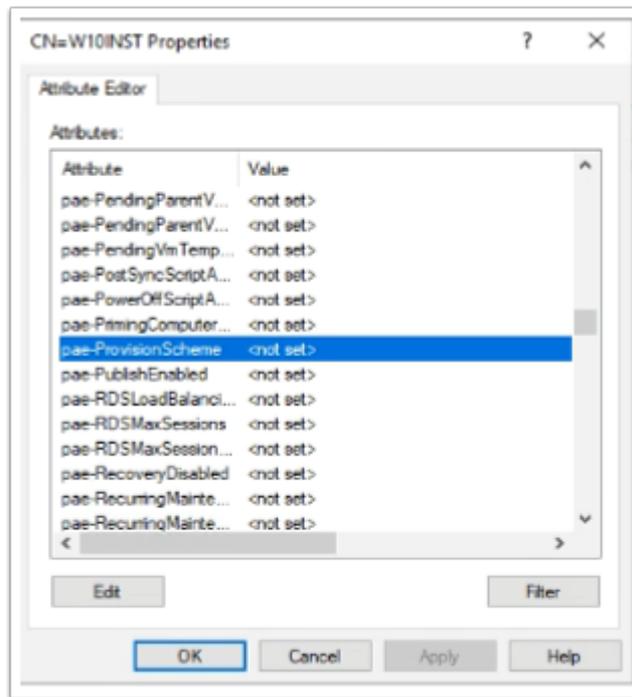
22. In the **Run** window

- Next to **Open:** enter **adsiedit.msc**
- Select **OK**
 - If you were to open adsiedit for the first time you would have to follow the guides in the below Knowledge Base
 - <https://kb.vmware.com/s/article/2012377>



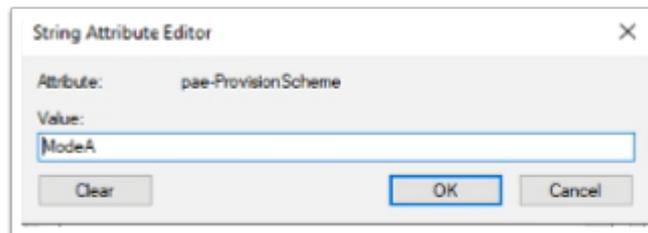
23. In the **ADSI Edit** window

- **Expand** the inventory
- Select **OU=Server Groups**
- Select and right-click **CN=W10INST**



24. In the **CN=W10INST Properties** window

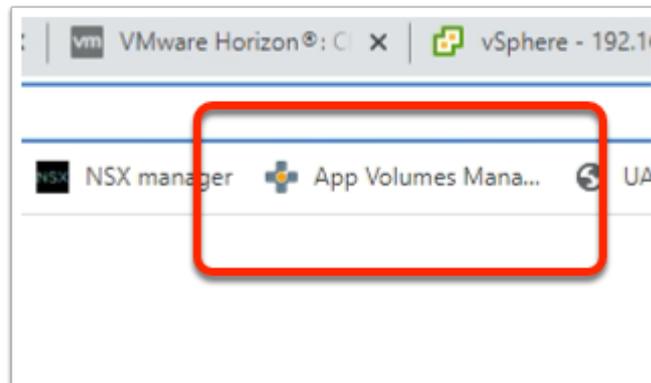
- Scroll down until you find the **pae-ProvisionScheme** attribute
- Select the **pae-ProvisionScheme** attribute
 - Select **Edit**



25. In the **String Attribute Editor** window

- In the **Value** area, type **ModeA**
- Select **OK**, to close the window
- Select **OK**, to close the **CN=W10INST Properties** window
- **Close** the **ADSI Edit** window

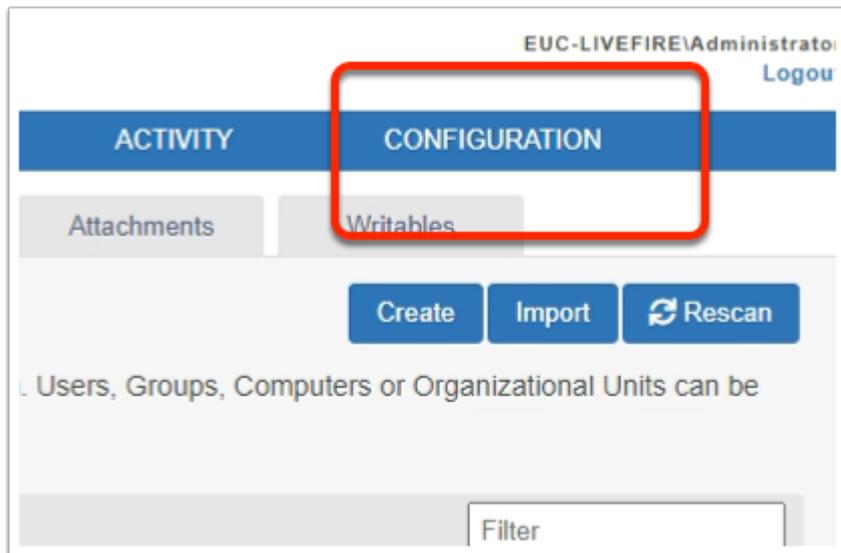
Part 3. Configuring VMware App Volumes for the Untrusted Active Directory Domain



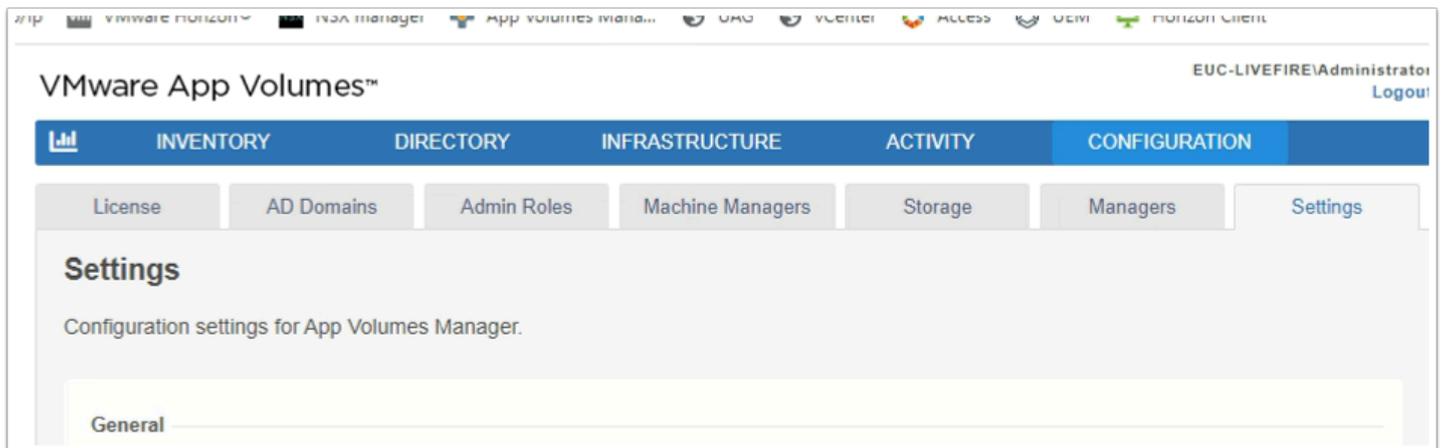
1. On the ControlCenter Server
 - Open your **Chrome** browser
 - From the **Favourites** bar, select the **App Volumes Manager** shortcut

A screenshot of the VMware App Volumes login page. The page title is 'VMware App Volumes™'. There are three input fields: 'Username:' with the value 'administrator', 'Password:' with a masked password '*****', and 'Domain:' with a dropdown menu showing 'EUC-LIVEFIRE'. Below these fields is a blue 'Login' button. At the bottom of the page, there is a grey banner for the 'Customer Experience Improvement Program (CEIP)' with a blue 'OK' button.

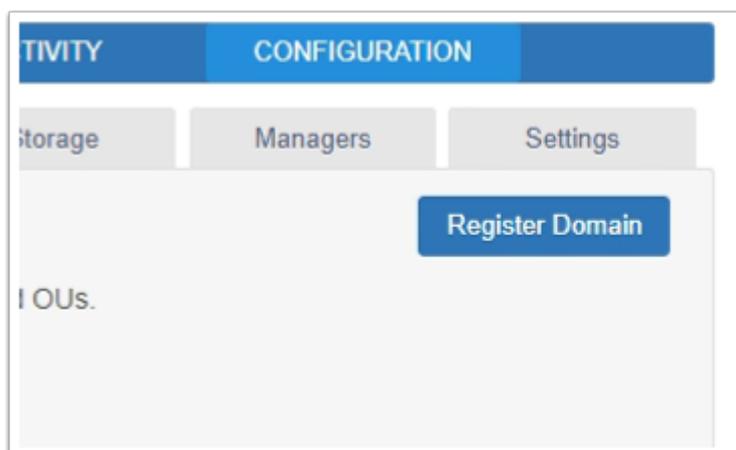
2. In the **App Volumes Manager login** page
 - Next to **Username:** enter **Administrator**
 - Next to **Password:** enter **VMware1!**
 - Select **Login**
 - Select **OK** to close the **Customer Experience Improvement Program(CEIP)** window



3. In the **App Volumes Manager Admin** console
 - Select the **Configuration** Tab



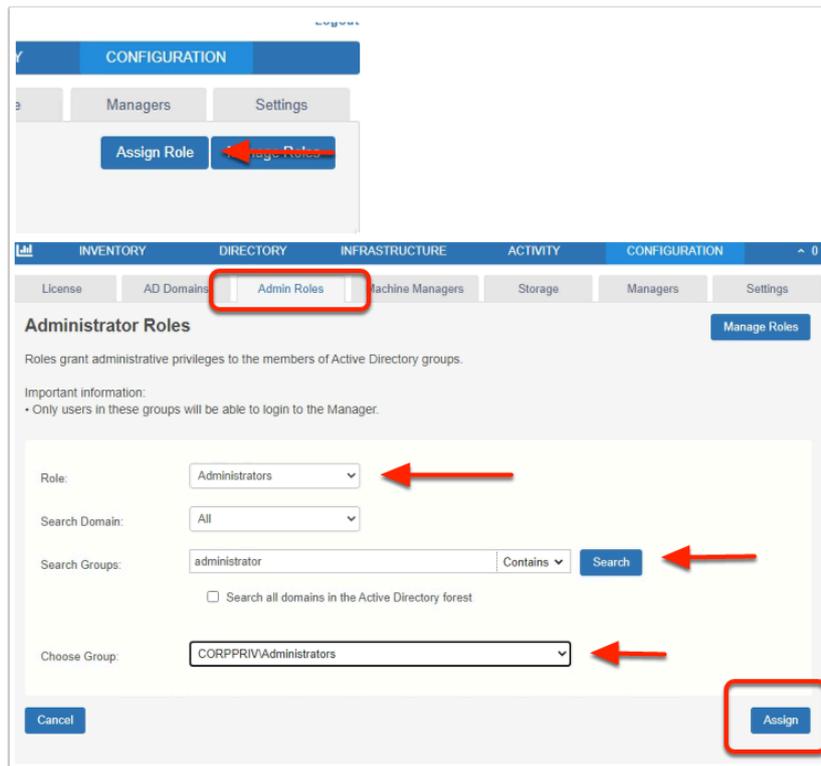
4. In the **App Volumes Manager Admin** console
 - In the **Configuration** Area
 - Select the **AD Domains** Tab



5. In the **AD Domains** area
 - Select **Register Domain**

The screenshot shows the 'Register Active Directory Domain' form in a VMware Horizon console. The form is titled 'Register Active Directory Domain' and is part of the 'AD Domains' configuration section. It contains several input fields and a dropdown menu, each with a corresponding help text. The fields are: 'Active Directory Domain Name' (corpPriv.local), 'Domain Controller Hosts' (empty), 'LDAP Base' (empty), 'Username' (Administrator), 'Password' (masked with asterisks), 'Security' (LDAP (insecure)), and 'Port' (389). The 'Security' field is a dropdown menu. At the bottom, there are 'Cancel' and 'Register' buttons.

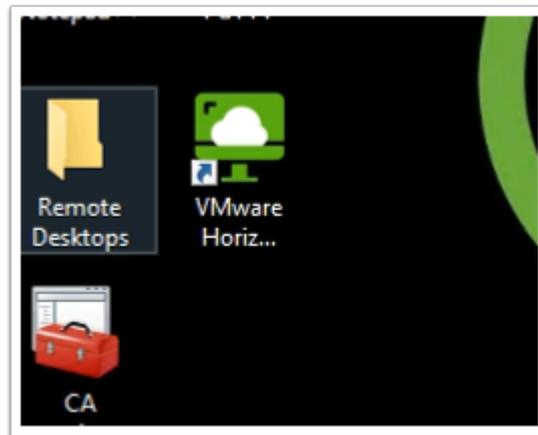
6. In the AD Domains area
 - Enter the following next to:
 - **Active Directory Domain Name:** corpPriv.local
 - **Username:** Administrator
 - **Password:** VMware1!
 - **Security:** LDAP(insecure)
 - **Port:** 389
 - Select **Register**



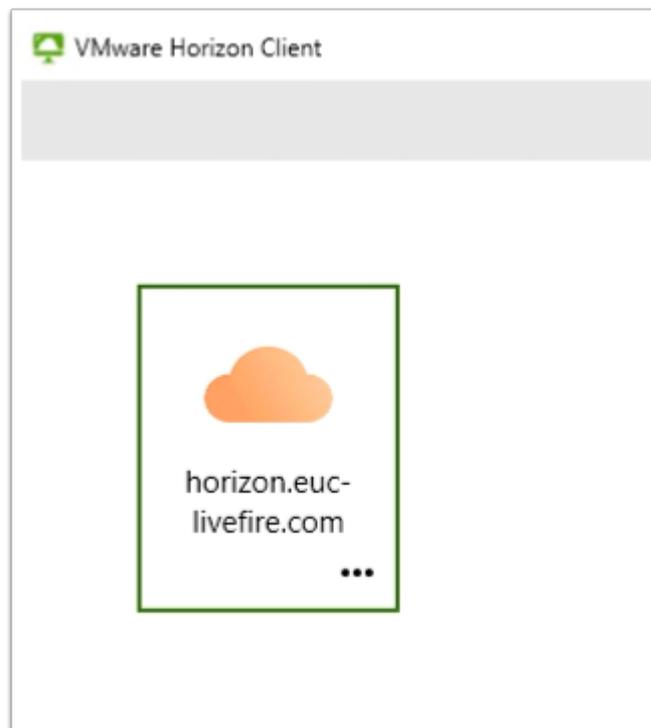
7. In the **App Volumes Manager** consoles

- Select the **Admin Roles** tab
 - Select **Assign Role**
 - Enter and select the following next to:
 - **Role:** from the dropdown select **Administrators**
 - **Search Groups:** **Administrator**
 - **Select :** **Search**
 - **Choose Group:** from the dropdown select **CORPPRIV\Administrators**
- Select **Assign**

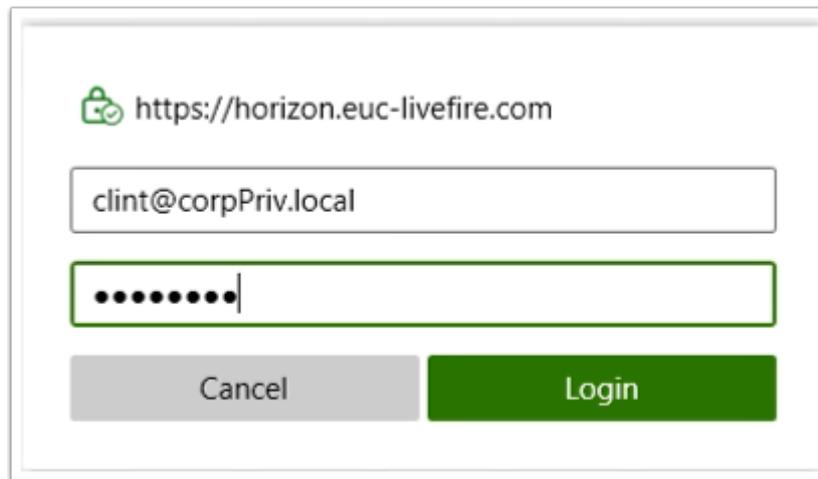
Part 4 Testing the Desktop Pool of users from an Untrusted Domain



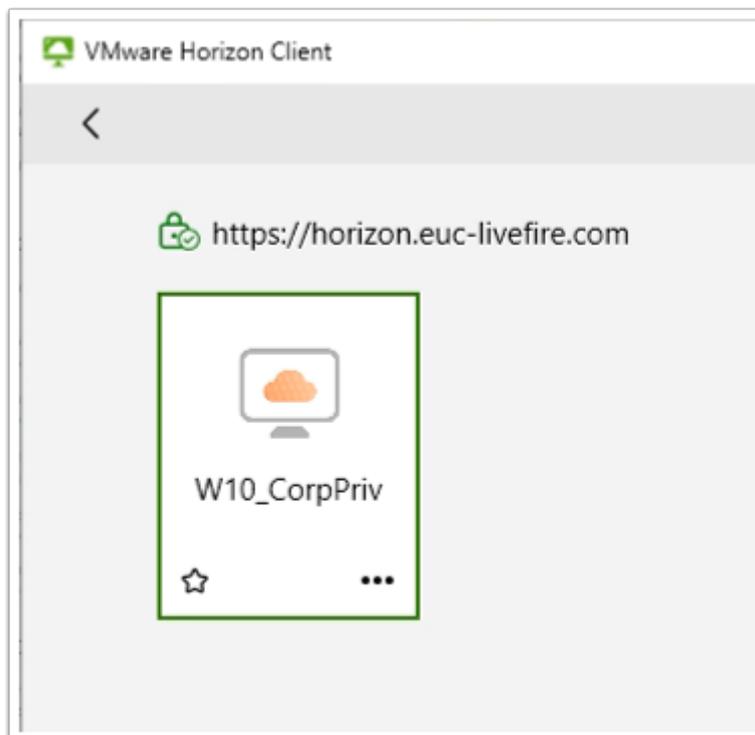
1. On your ControlCenter Server
 - Launch your **Horizon Client**



2. From your Horizon Client
 - Select the **horizon.euc-livefire.com** POD

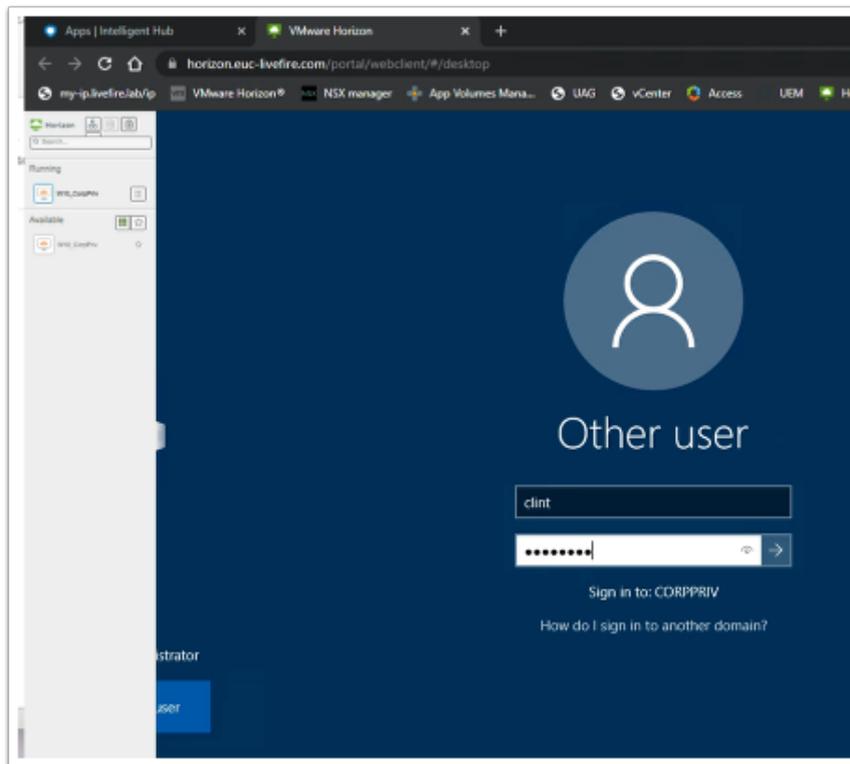


3. In the **Horizon Client Login** window
 - In the **Username** area
 - Enter **clint@corpPriv.local**
 - In the **Password** area
 - Enter **VMware1!**
 - Select **Login**



4. In the Horizon Client login
 - Select the **W10_CorpPriv** entitlement

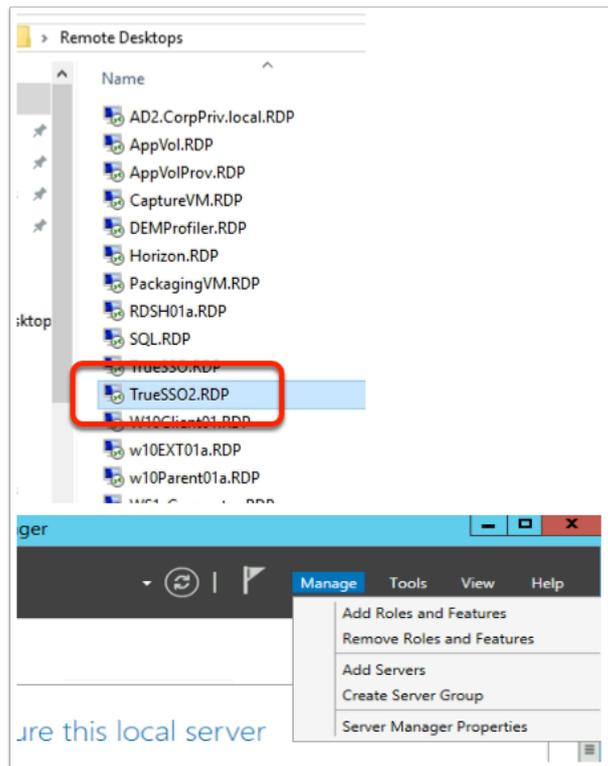
Part 5: Deploying Horizon Enrollment services to facilitate Single Sign-On with Workspace ONE Access



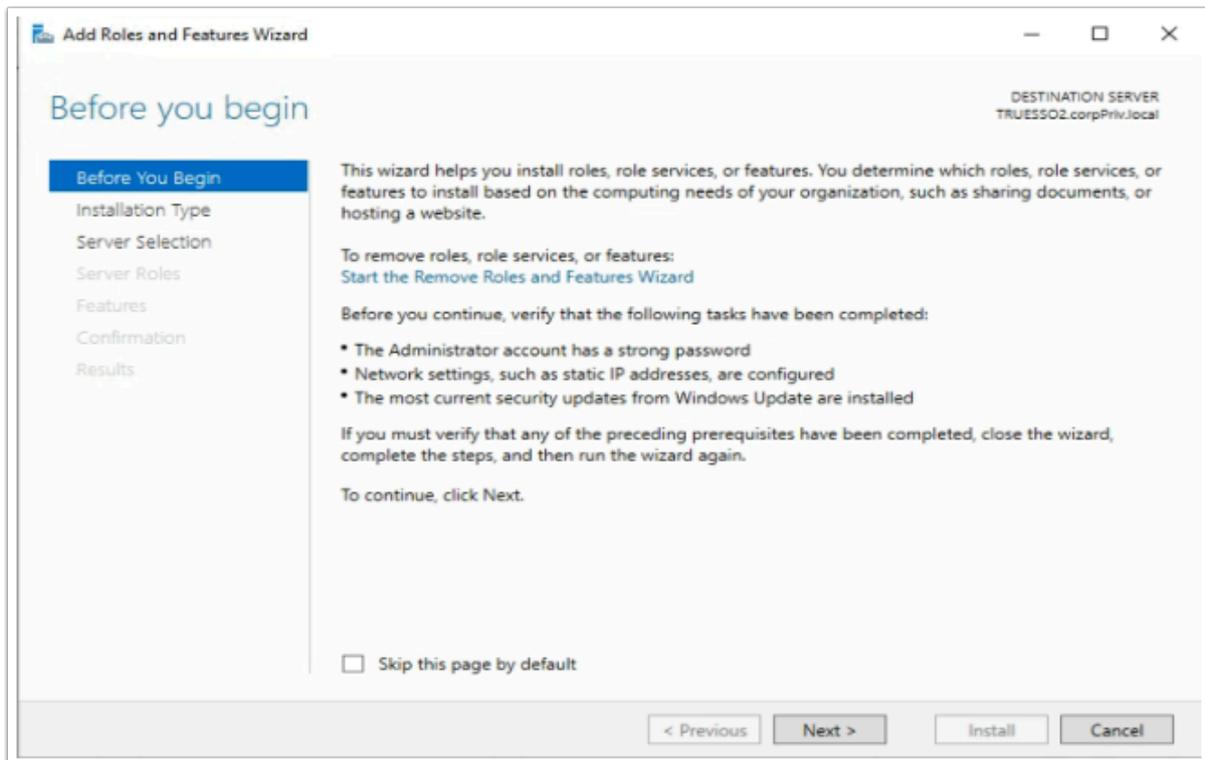
Introduction:

When logging in through Workspace ONE Access to a Horizon Desktop the user does not have a single sign on experience .

We will now configure Horizon Enrollment services in the Untrusted Domain

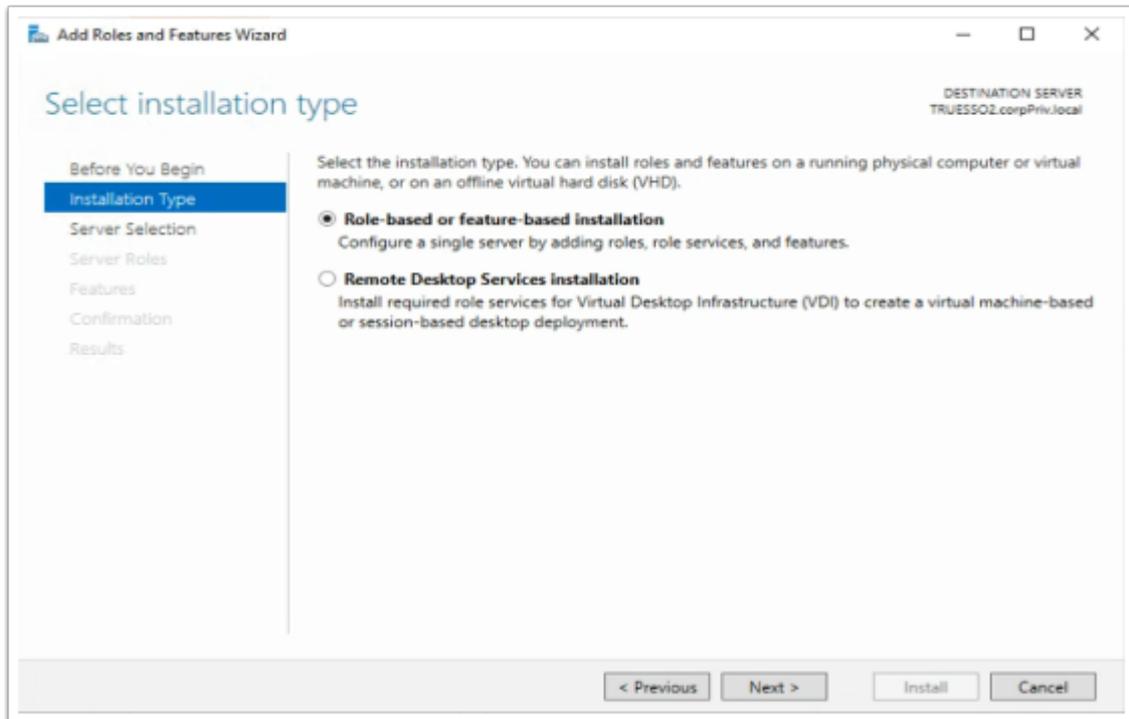


1. On your **ControlCenter** server
 - Open the **Remote Desktops** Folder
 - Launch **TrueSSO2.RDP** shortcut
 - Login as **corpPriv\administrator** and enter the password **VMware1!**
 - On the **Server Manager** Interface select **Manage > Add Roles and Features**



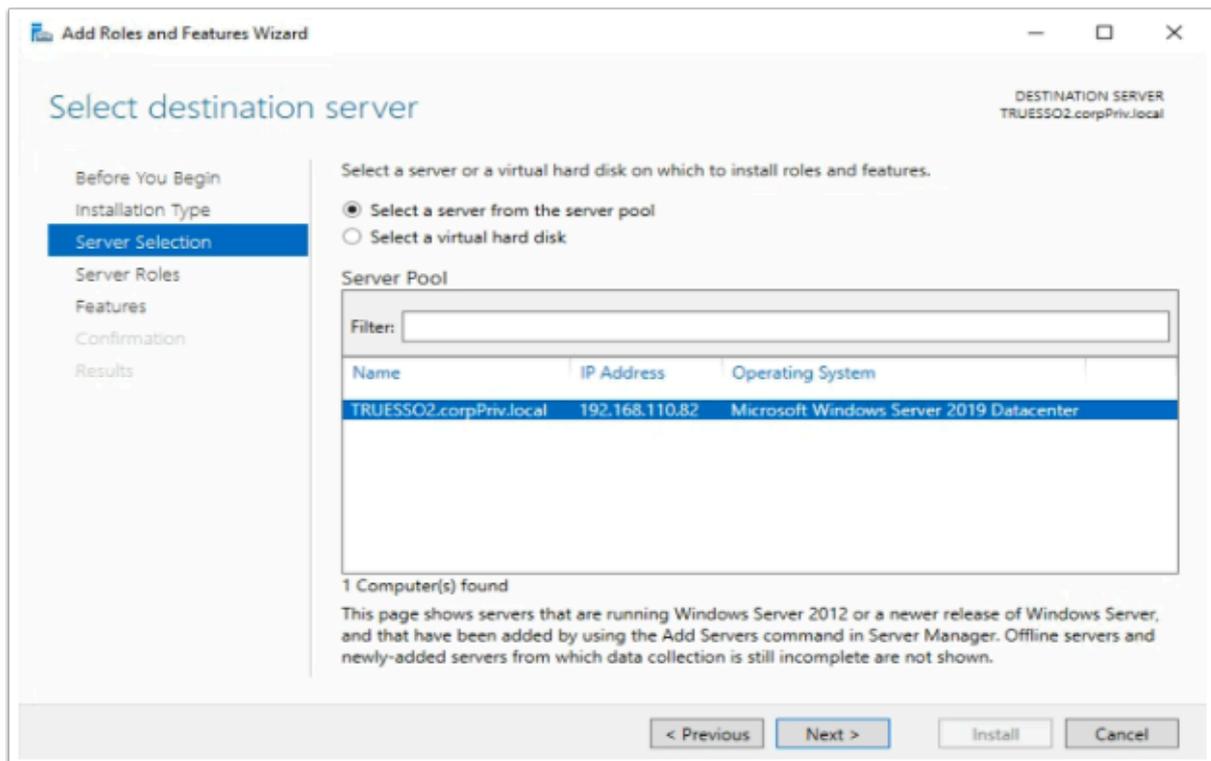
2. On the **Before you begin** window

- Select **Next**



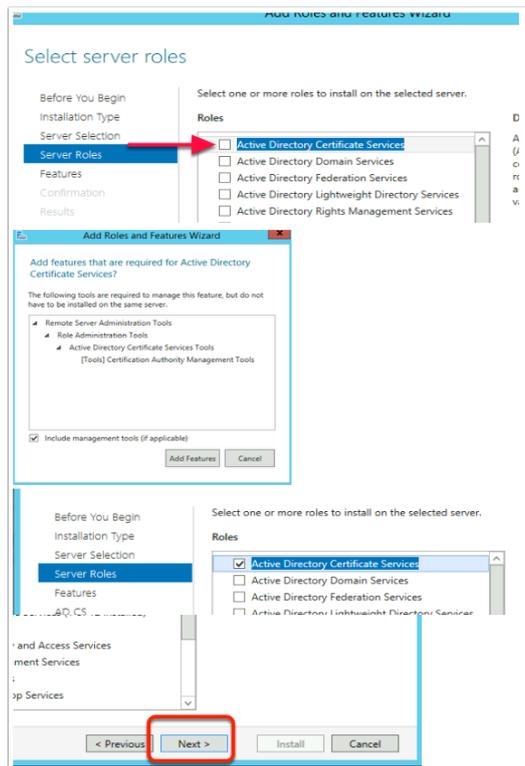
3. On the **Select installation type** window,

- Ensure the **radio button** in front of **Role-based or feature-based installation** is selected
- Select **Next**



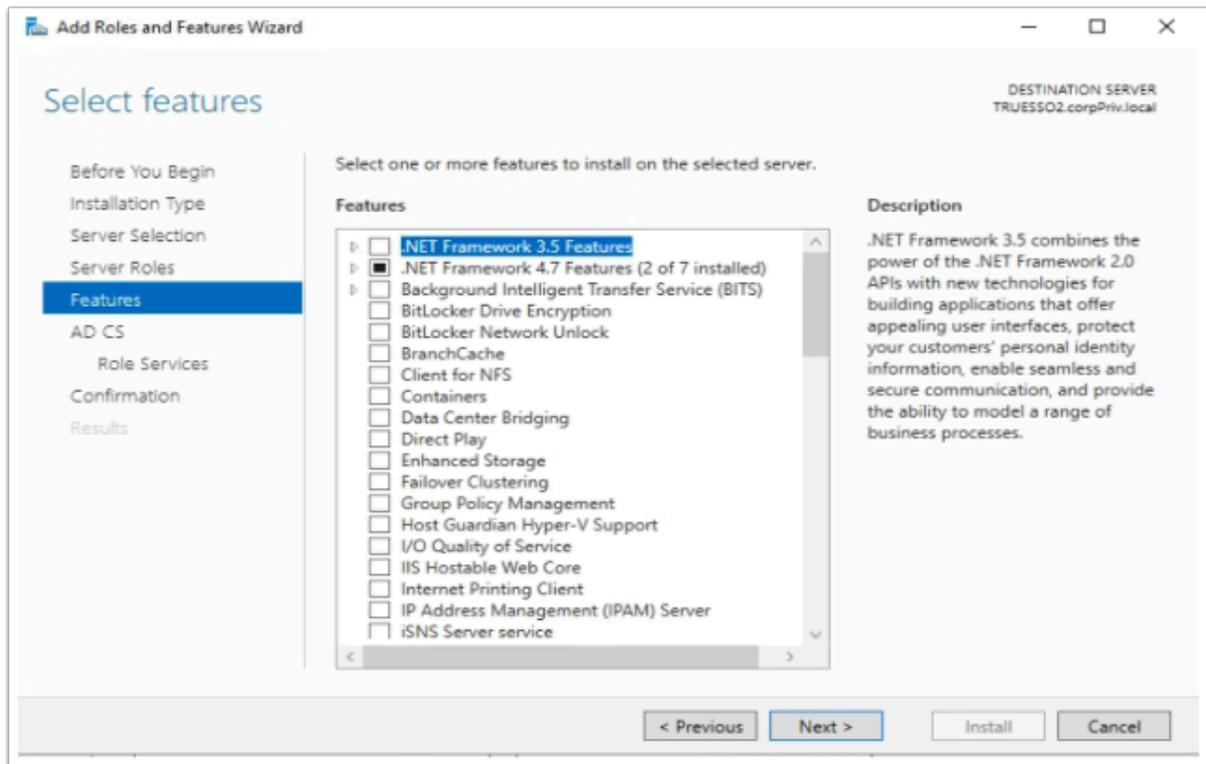
4. On **Select destination server** window (accept the defaults)

- Select **Next**



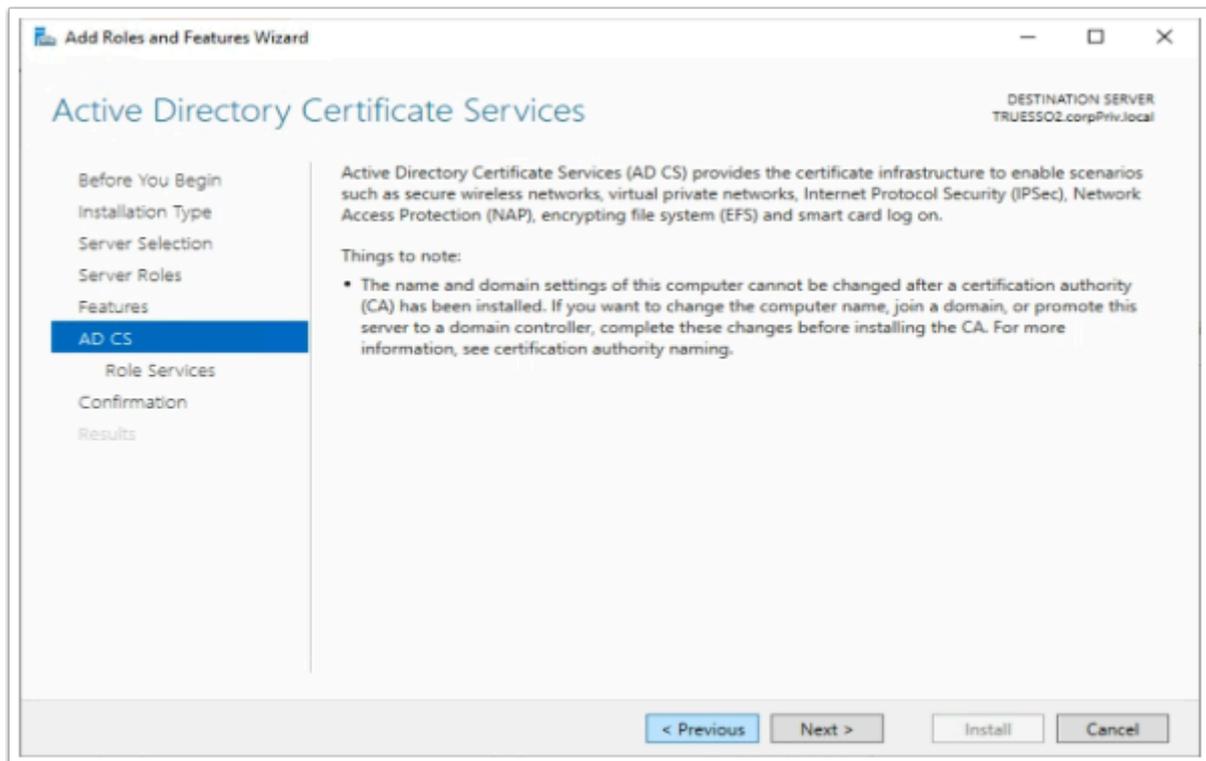
5. On the **Select server roles** window,

- 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**



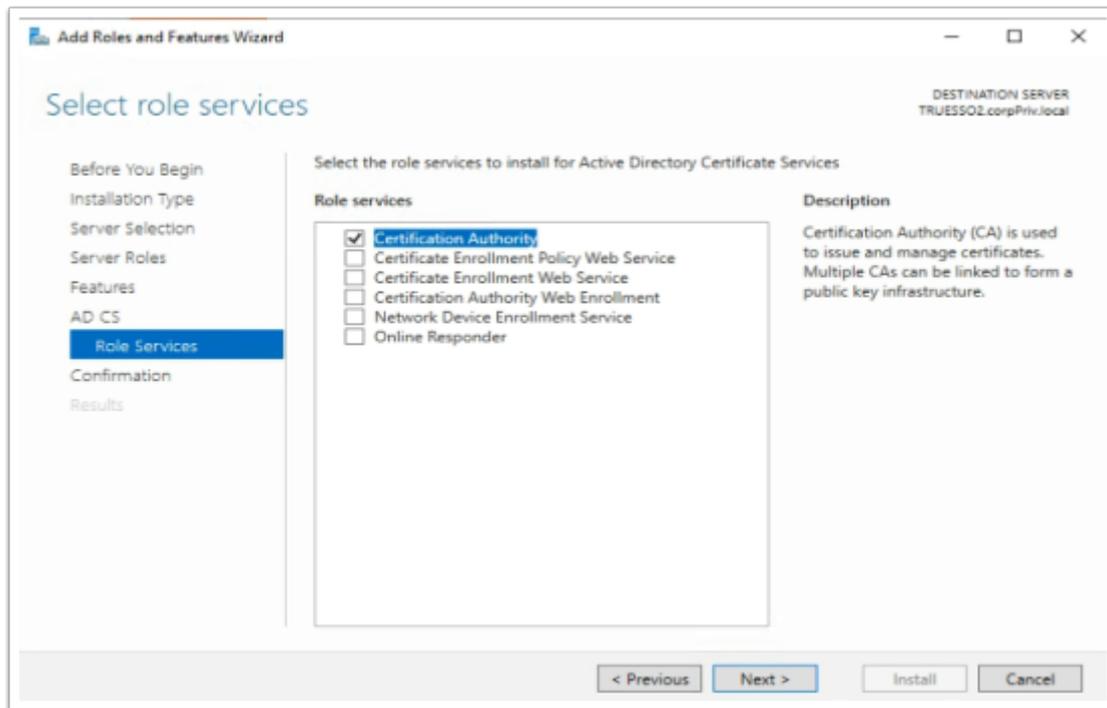
6. On the **Select features** window

- Select **Next**

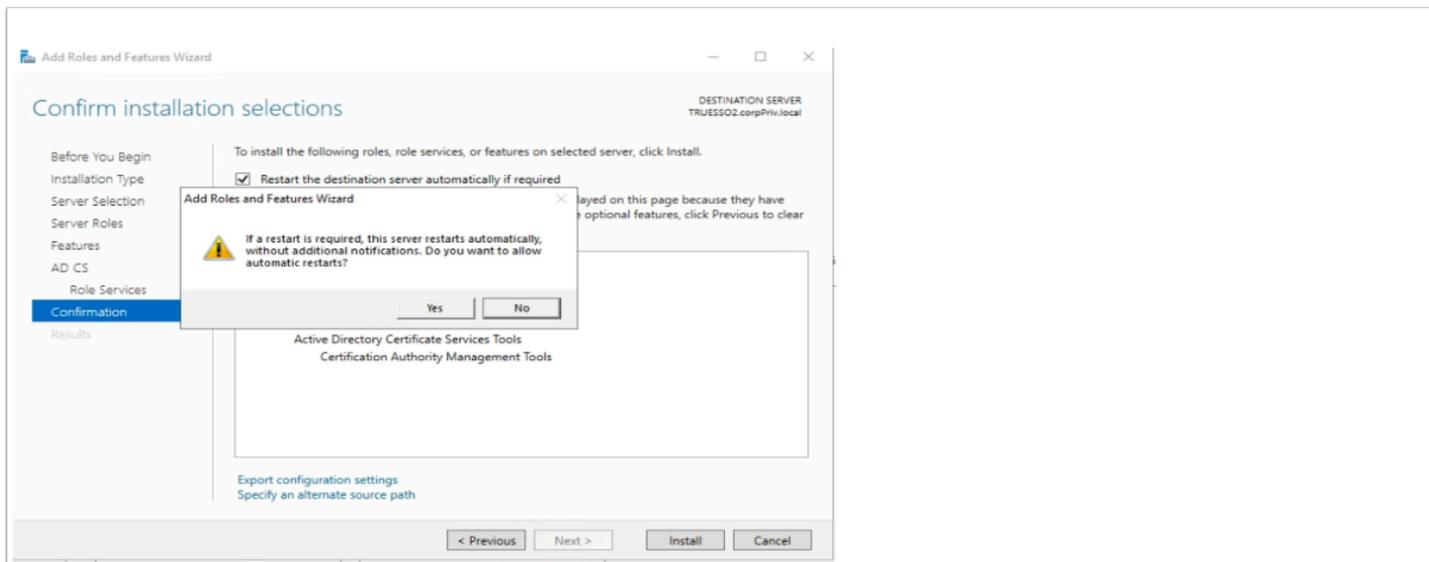


7. On the **Active Directory Certificate Services** window

- Select **Next**

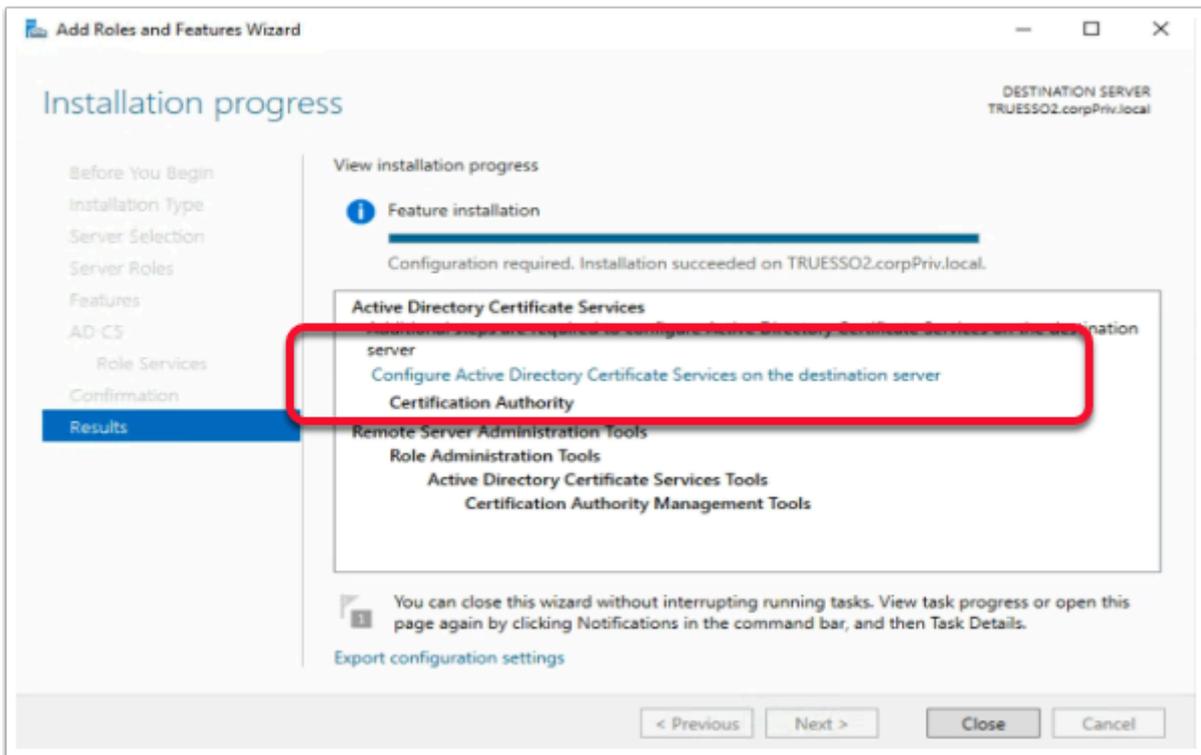


8. On the **Select role services** window
- Select **Next**



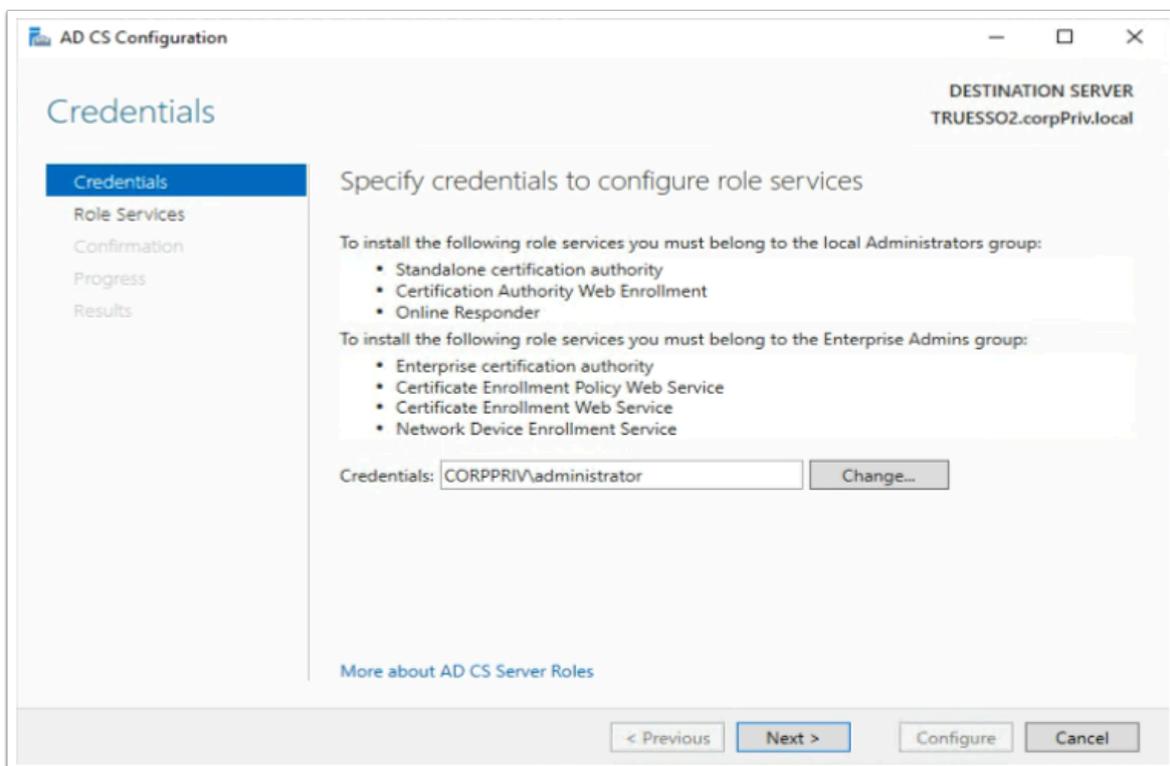
9. On the **Confirm Installation selections** window,
- Select the **checkbox** next to **Restart the destination server automatically if required**,
 - On the **Add Roles and Features Wizard** window select **Yes**
 - Select **Install**

You will have to wait a short while before moving on to step 10



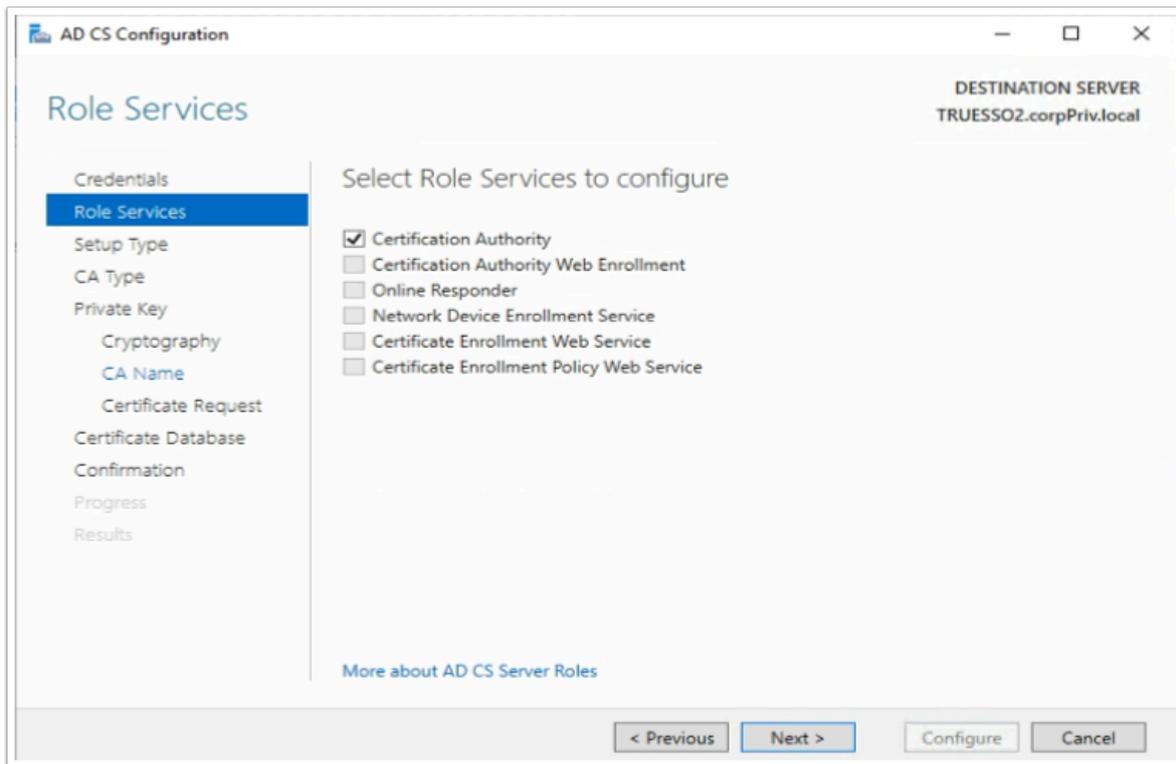
10. On the **Installation progress** page,

- Select the **Configure Active Directory Certificate Services on the destination server** hyper-link

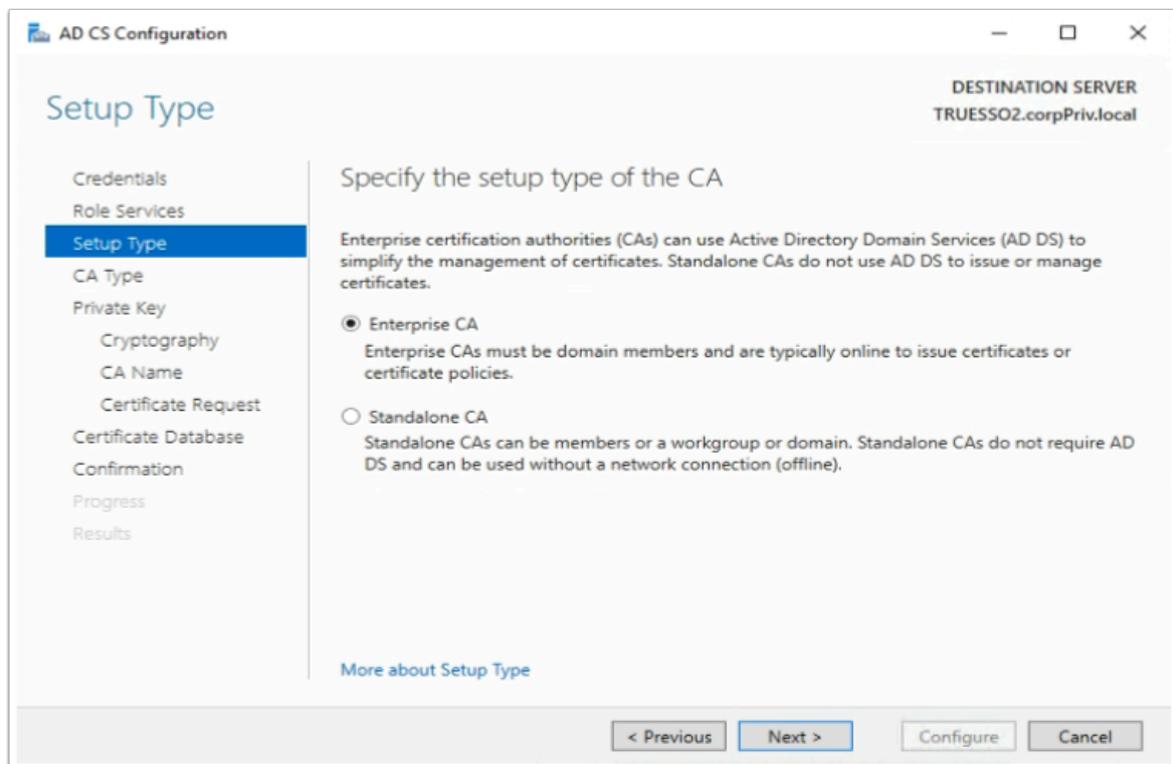


11. On the **Credentials** window

- Select **Next**

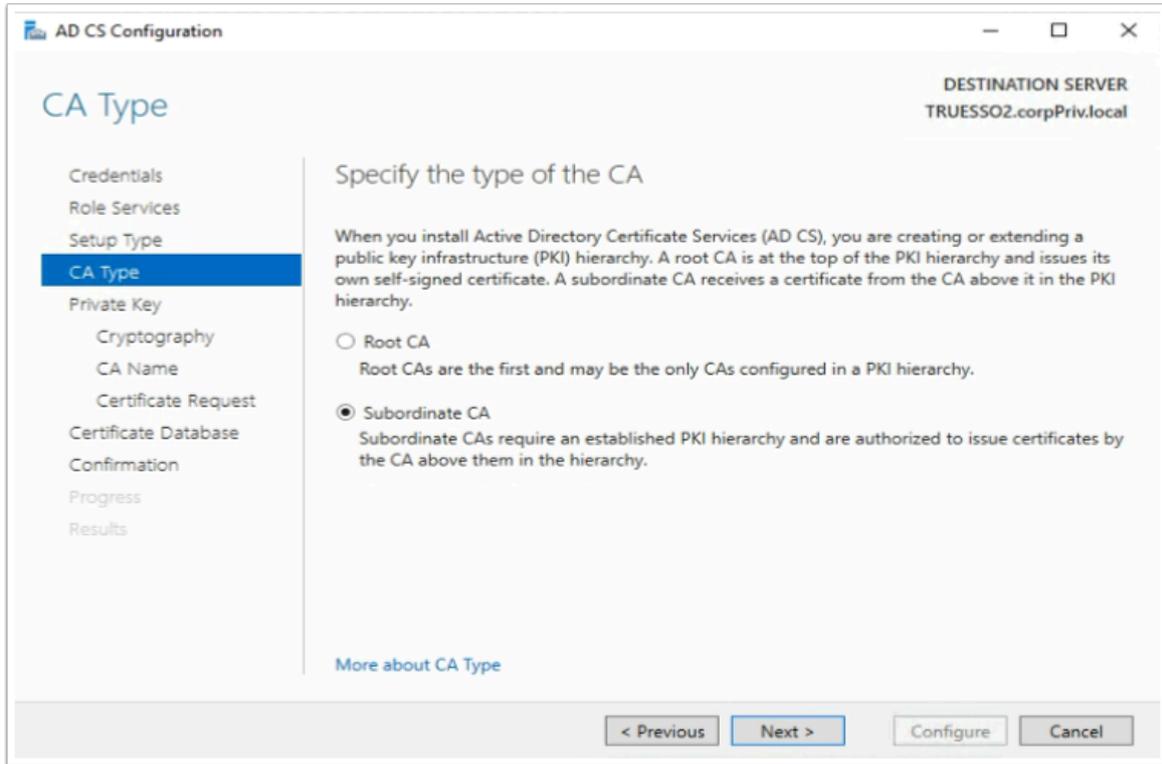


12. On the **Role Services** page,
- Select the **Certification Authority** checkbox
 - Select **Next**



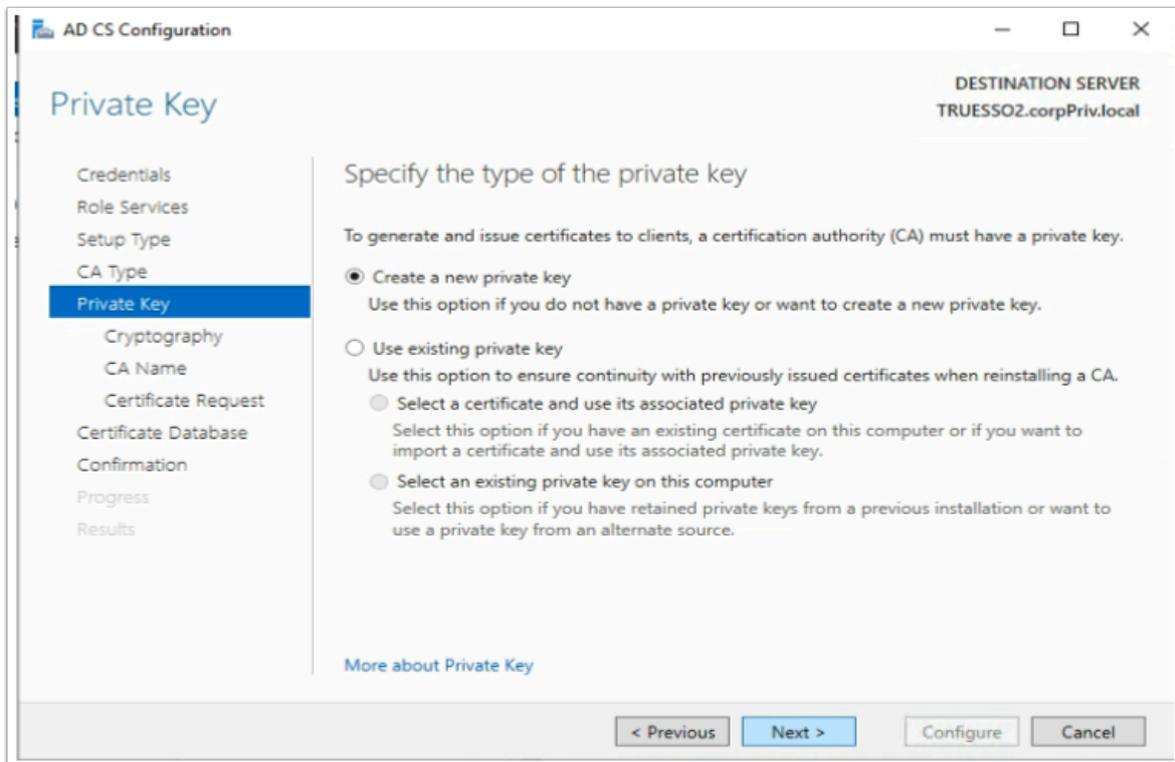
13. On the **Specify the setup type of the CA** window ,
- Select the **radio button** next to **Enterprise CA**

- Select **Next**



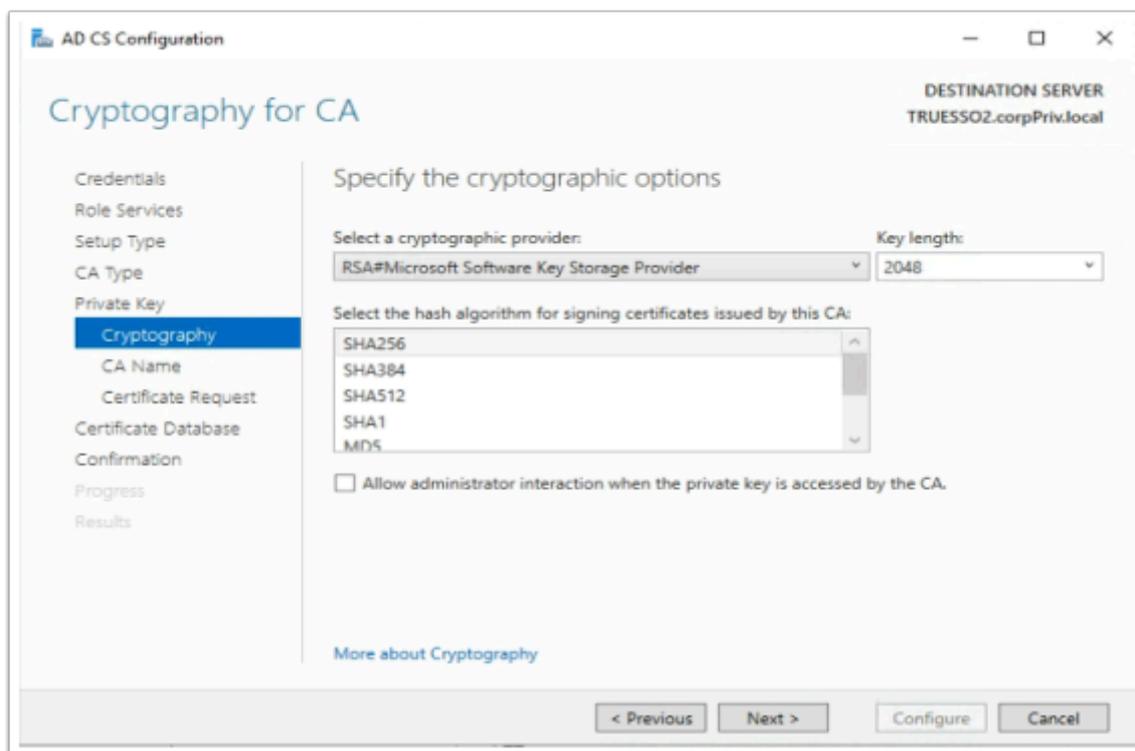
14. On the **CA type** window

- Ensure the **Subordinate CA radio button** is selected,
- Select **Next**

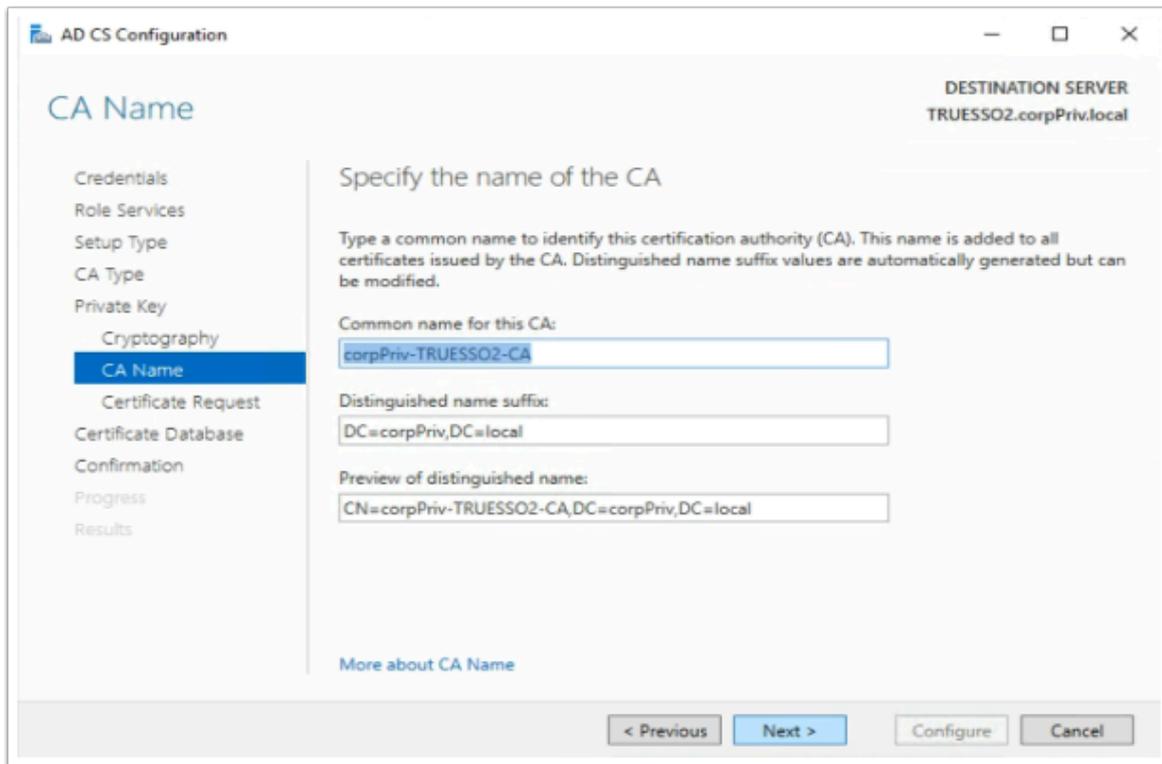


15. On the **Private Key** window,

- Ensure the **radio button** next to **Create a new private key** is selected
- Select **Next**

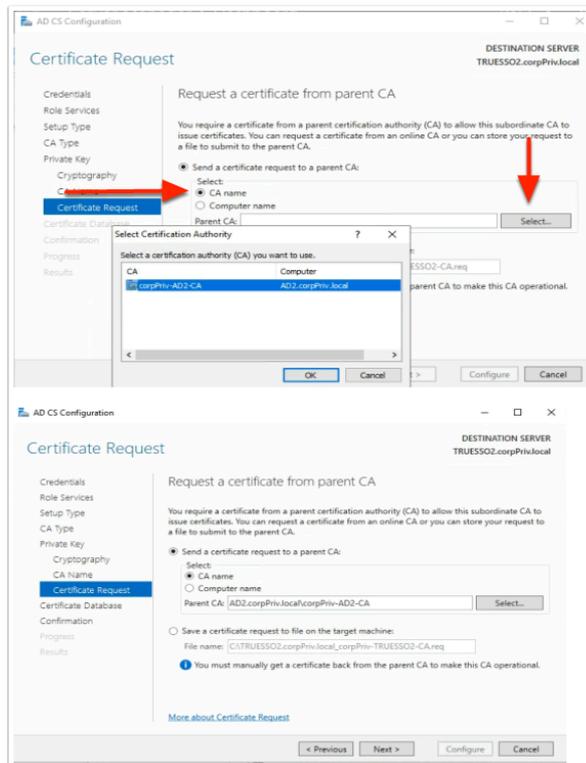


16. On the Cryptography for CA window select the following
- Under **Cryptographic Provider:** **RSA#Microsoft Software Key Storage Provider**
 - Next to **Key Length:** **2048**
 - **Hash Algorithm:** **SHA256**
- Select **Next**

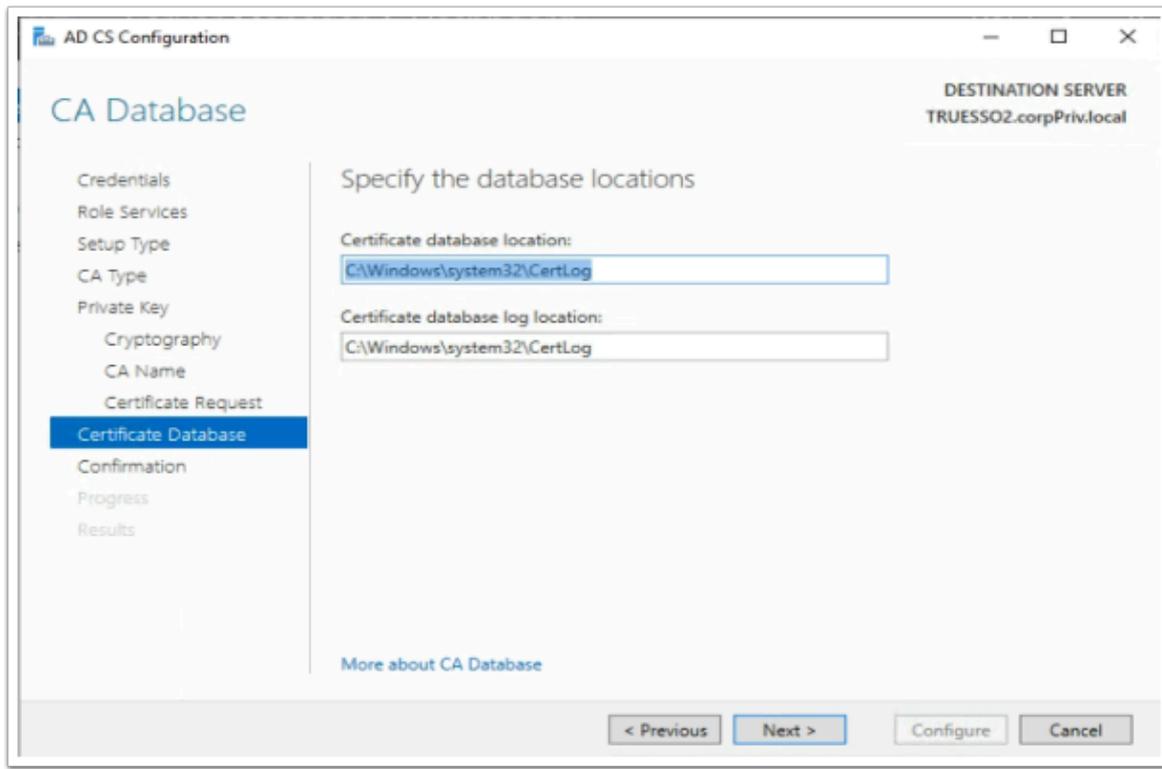


17. On the **Specify the Name of the CA** window

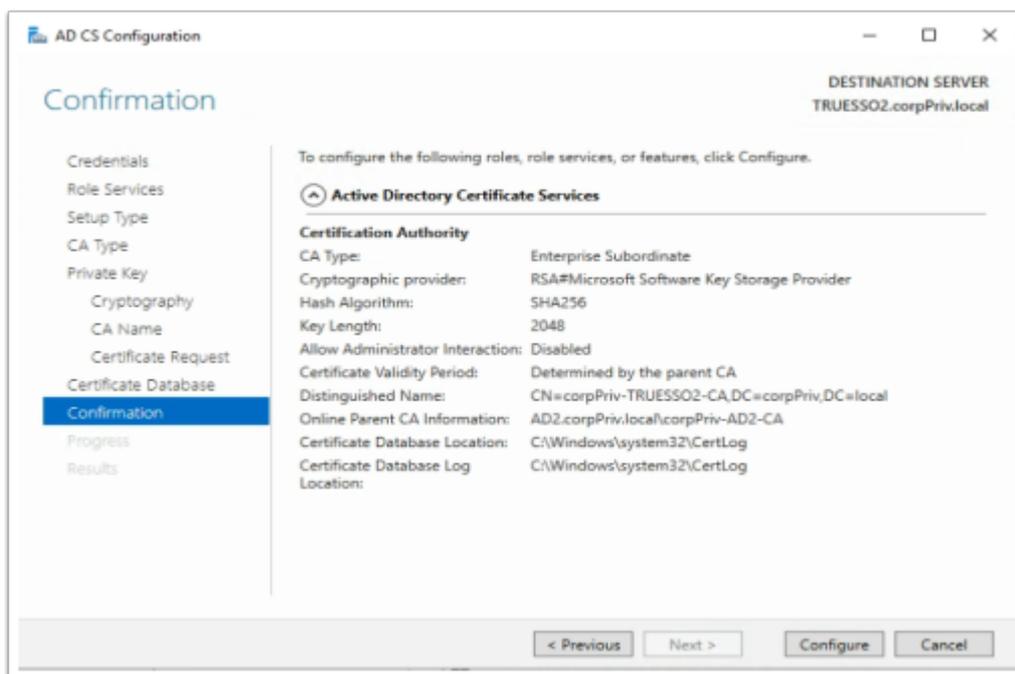
- Observe the CA naming convention
- Select **Next**



18. 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
 - Select **Next**

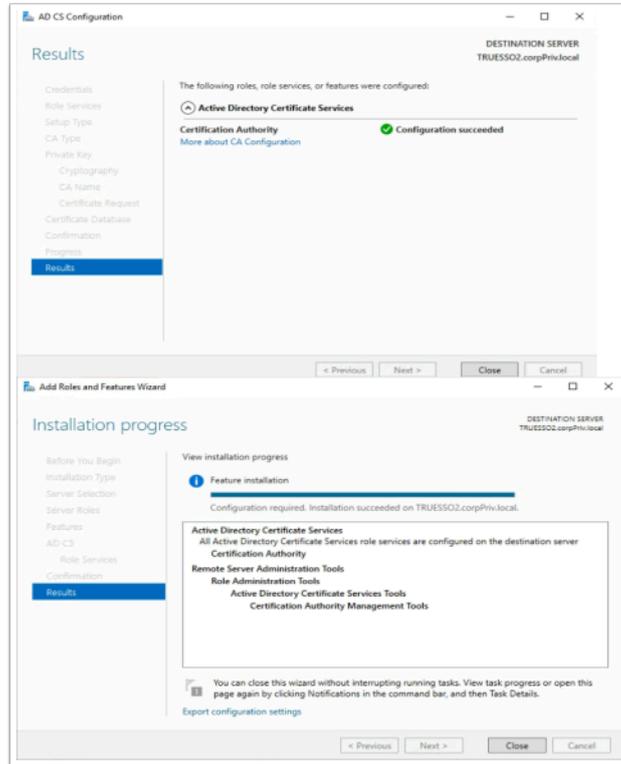


19. On the **CA Database** window,
- Select **Next**



20. On the **Confirmation** window

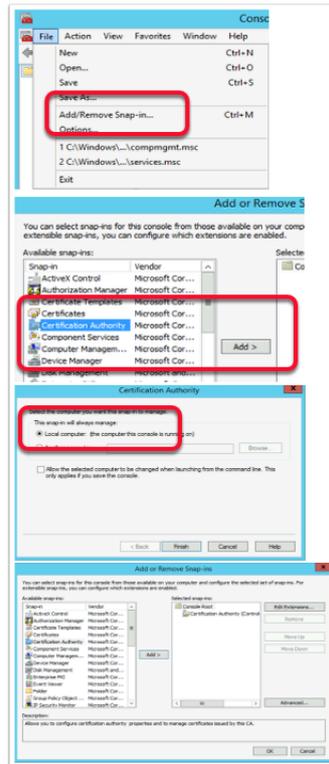
- Select **Configure**



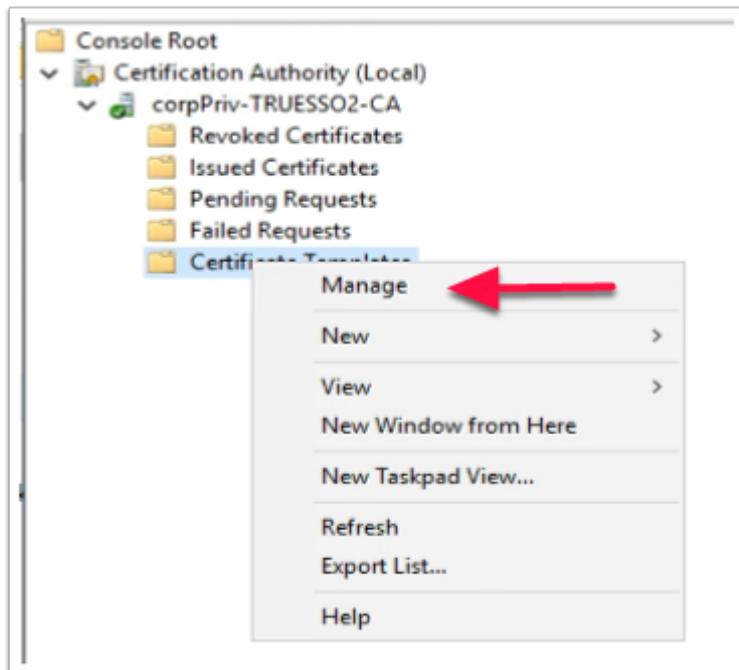
21. On the **Results** window

- Select **Close**
 - On the **Installation progress** window,
 - Select **Close**

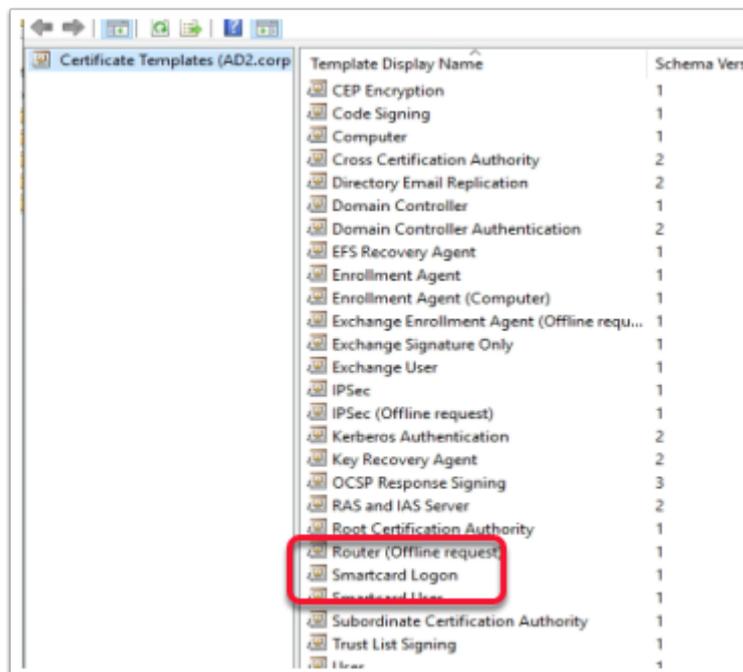
Part 6: Deploying and Configuring Horizon TRUE SSO



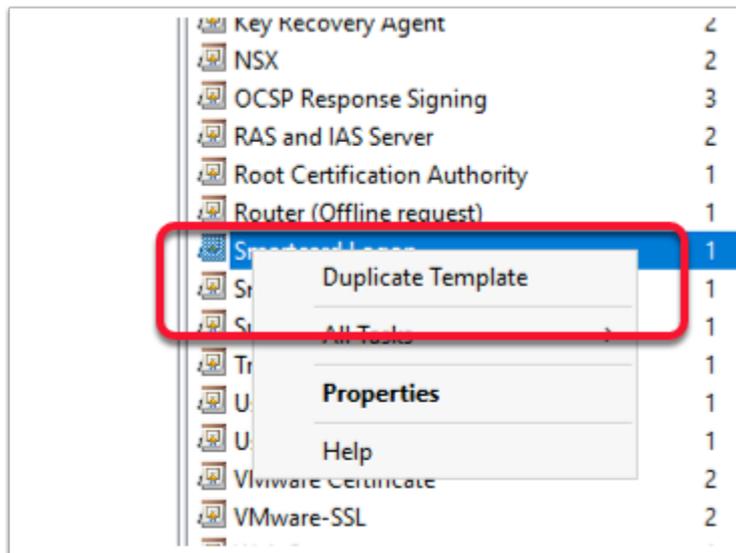
1. In this section we will create a certificate template for **Horizon TRUESSO**
 - On your **TRUESSO2** server select **Start > Run >** type **mmc**
 - Select **File > Add/Remove Snap-in...**
 - Select the **Certificate Authority** services snap-in, select **Add**
 - In the Certificate Authority window,
 - Select the **Local computer** radio button
 - Select **Finish**
 - Select **OK** to close the **Snap-ins** window



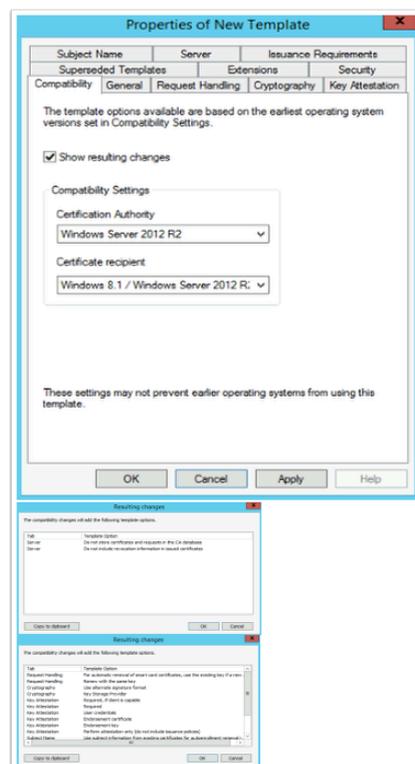
2. Expand the **corpPriv-TRUESSO2-CA** inventory
 - Select **Certificate Templates**,
 - right-click and select **Manage**



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



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

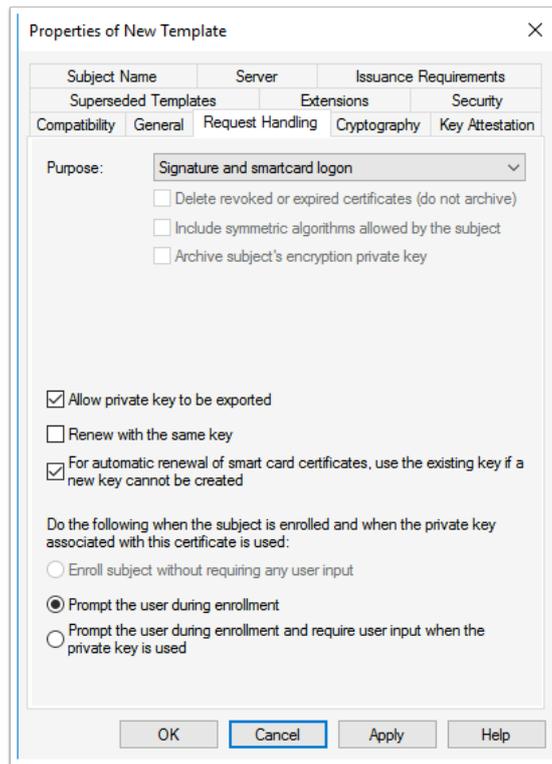


5. In the **Properties of New Template** window in the **Compatibility** tab under **Certificate Authority**
 - Change from **Windows 2003** to **Windows 2012 R2**
 - When prompted for the **Resulting changes** window
 - Select **OK**.
 - Under **Certificate recipient** change **Windows XP / Server 2003** to **Windows 8.1 / Server 2012 R2**

- When prompted for the **Resulting changes** window
 - Select **OK**.

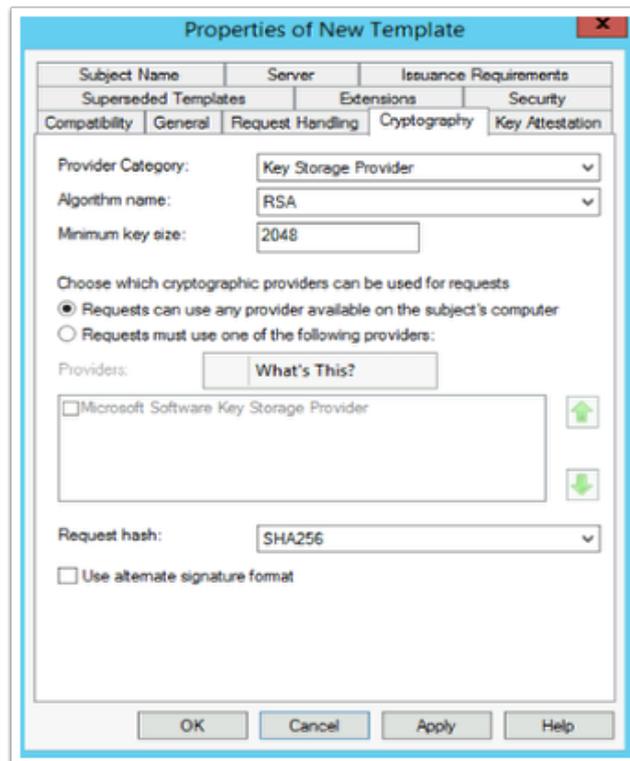


6. Select the **General** tab,
 - Under **Template display name:** type **TrueSSO Template**,
 - You will notice Template name gets filled in automatically.
 - **(Don't edit the TemplateName)**
 - Under **Validity period** change the period from **1 years** to **1 hours**
 - When prompted by **the Certificate Templates Box**
 - Select **OK**
 - The **Renewal period** will automatically change from **6 weeks** to **0 hours**

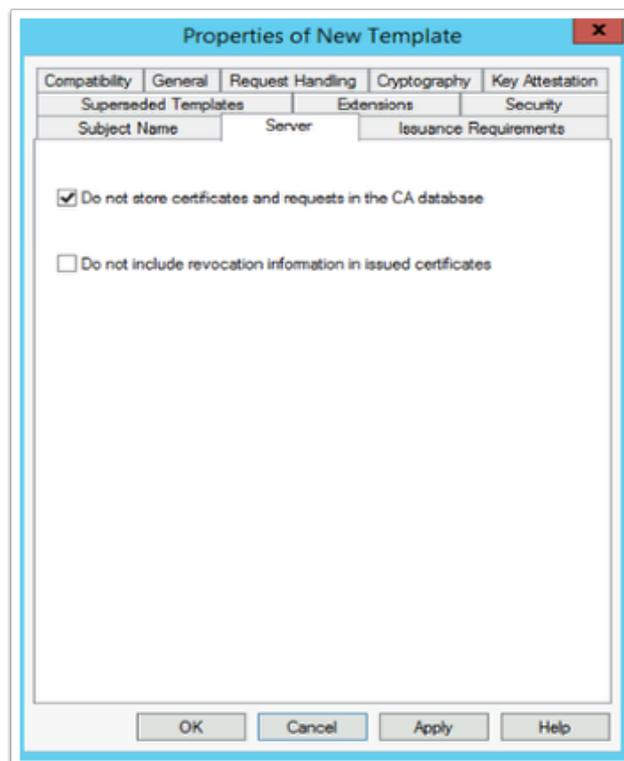


7. Select the **Request Handling** tab change the following next to :-

- **Purpose:** change: **Signature and encryption** to **Signature and smartcard logon**.
 - When prompted, select **Yes**
- 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**

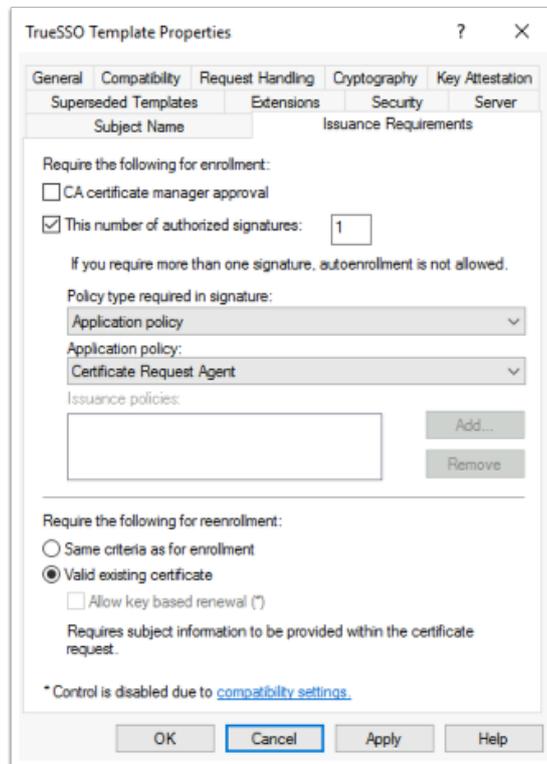


8. Select the **Cryptography** tab change the following next to
- **Provider Category:** **Key Storage Provider**
 - **Minimum key size:** **2048**
 - **Request hash:** **SHA256**

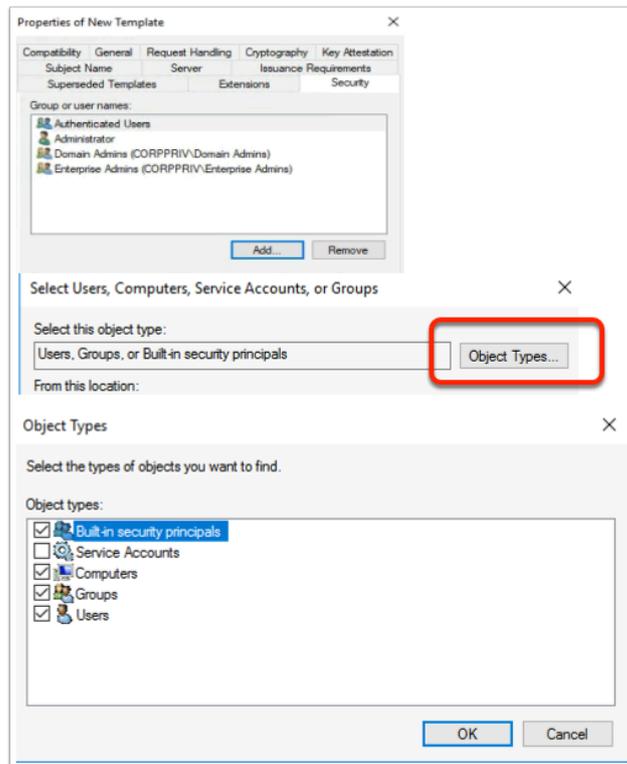


9. Select the **Server** tab,

- 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 **check box** next to **Do not include revocation information in issued certificates**

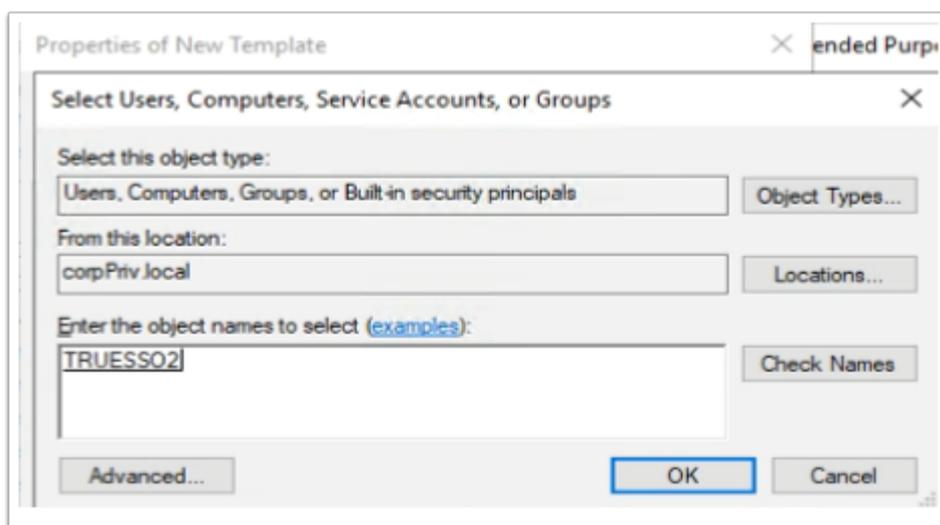


10. Select the **Issuance Requirements** tab, configure the following:
 - Select the **checkbox** : **This number of authorized signatures** and change the value to **1** in the **box**
 - Under **Policy type required in signature**
 - Ensure the **Application policy** is selected (default config)
 -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



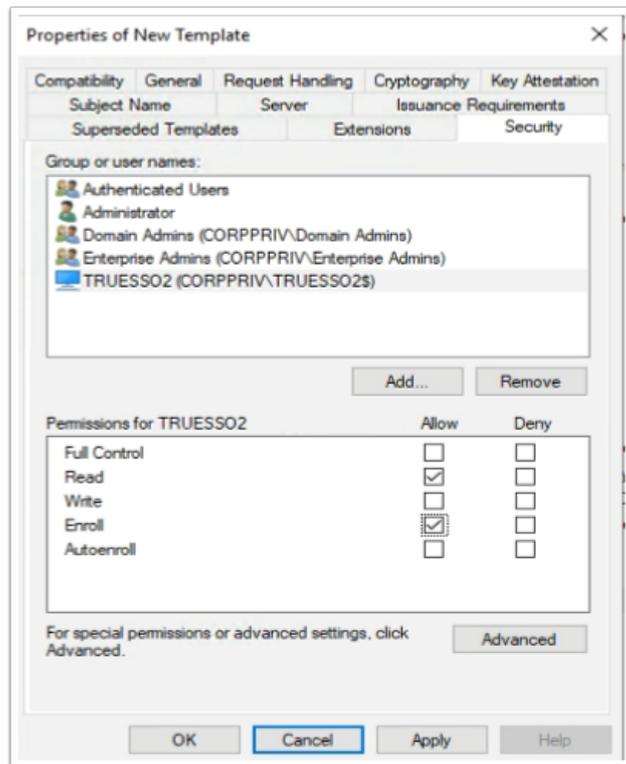
11. On the **Security** tab in the **Group or user names:** area

- 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**



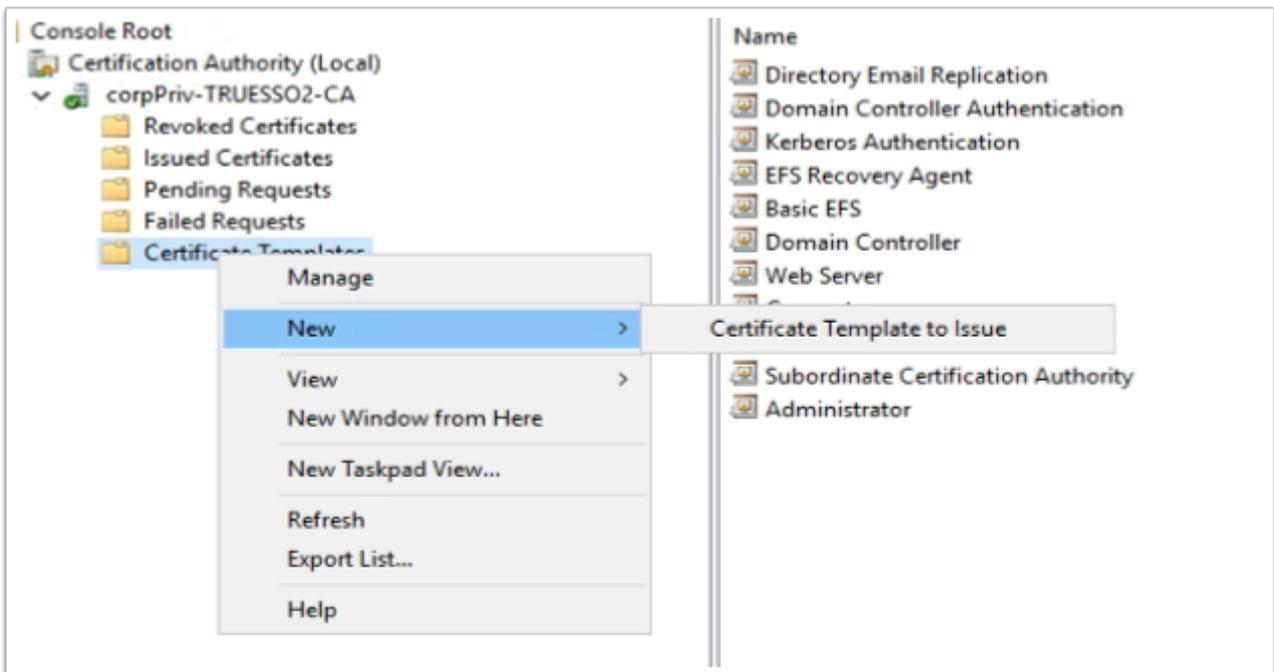
12. In the **Enter the object names to select**

- Type **TRUESSO2**
- To the right select **Check Names**
- Select **OK**



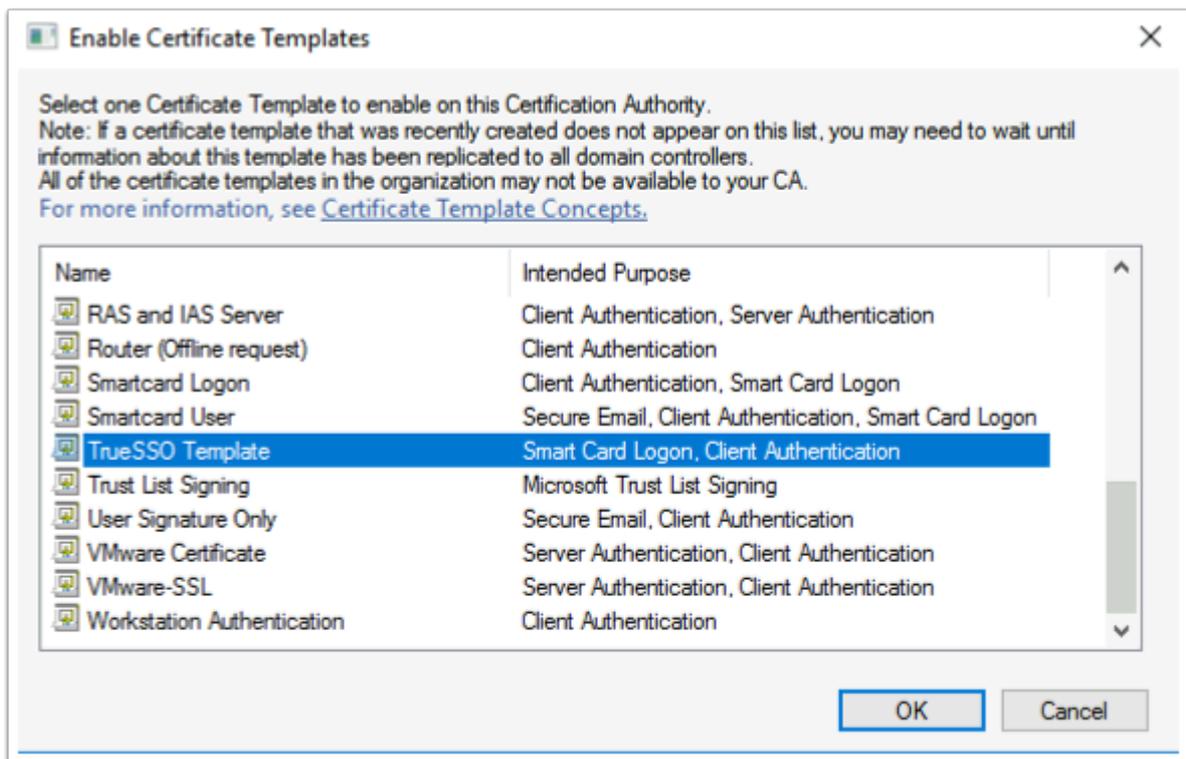
13. For the **Permissions for TRUESSO2**

- Ensure that the permission **Read** and **Enroll** checkboxes are selected.
- Select **OK** to close the **TrueSSO Template Properties**,

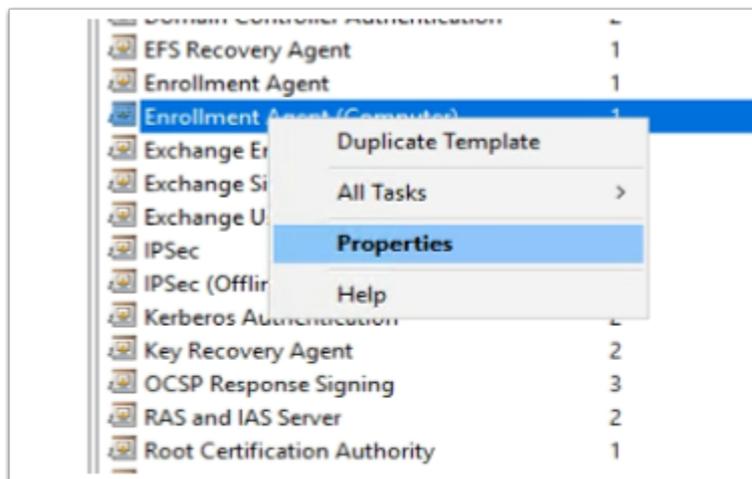


14. Switch to the **Certificate Authority Console**

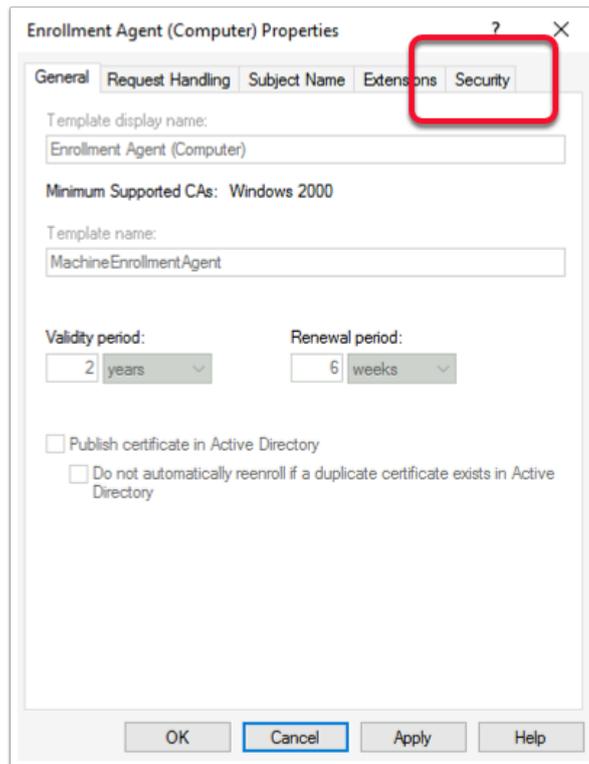
- Select and right-click the **Certificate Templates** container,
- Select **New** > **Certificate Template** to Issue



- In the **Enable Certificate Templates** window,
 - Select your **TrueSSO Template**
 - Select **OK**

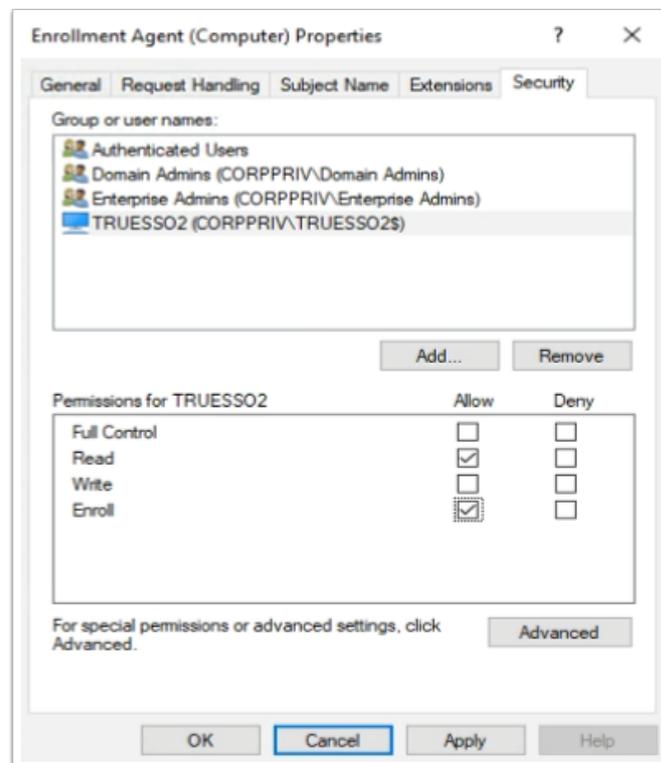


- Switch back to the **Certificate Templates** Console
 - Select and right-click the **Enrollment Agent (computer)** template
 - Select **Properties**



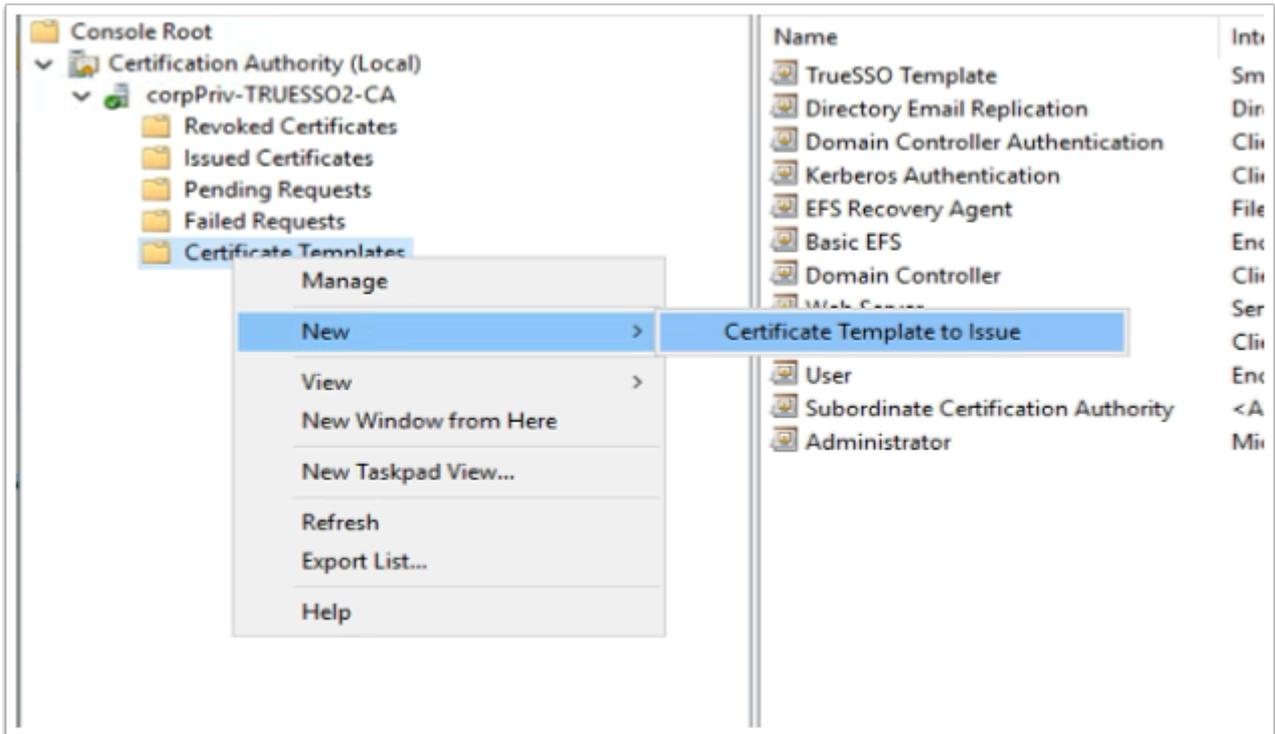
17. In the **Enrollment Agent Properties** window

- Select the **Security** tab

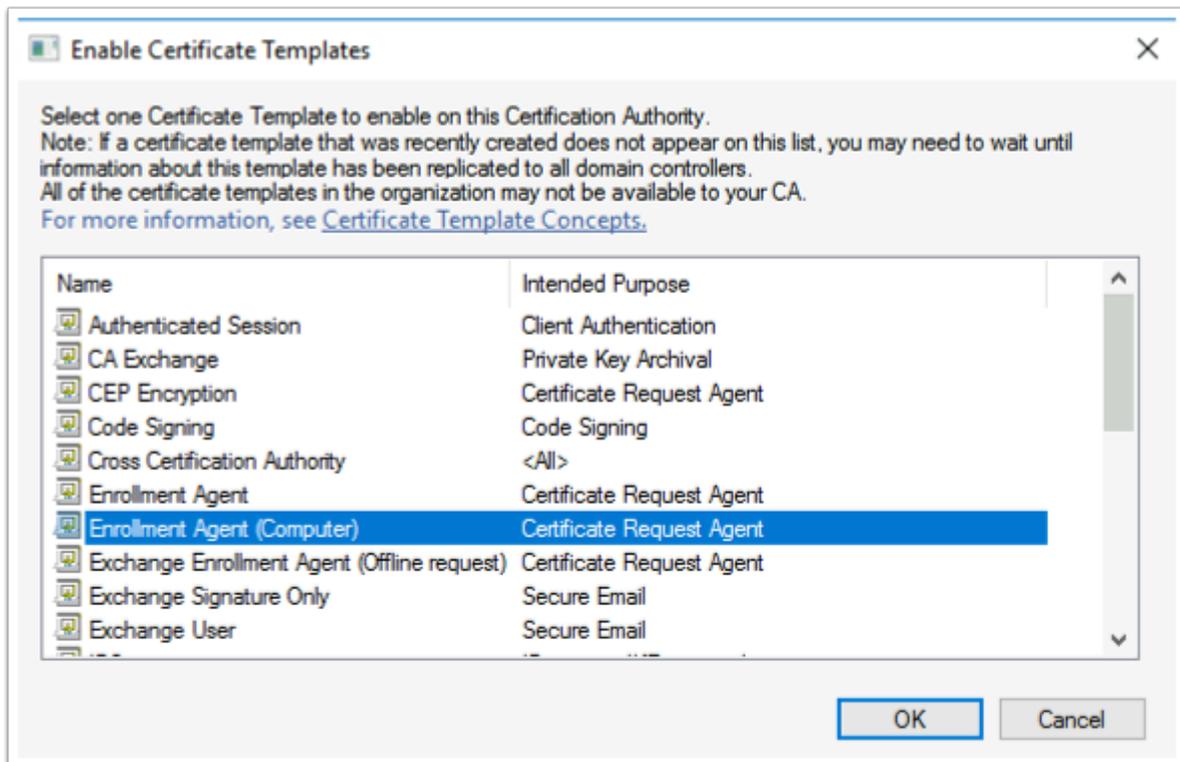


18. Select **Add** and add the **TRUOSSO** Computer account with Read and **Enroll** permissions .

- Select **OK** to close the **Enrollment agent** properties

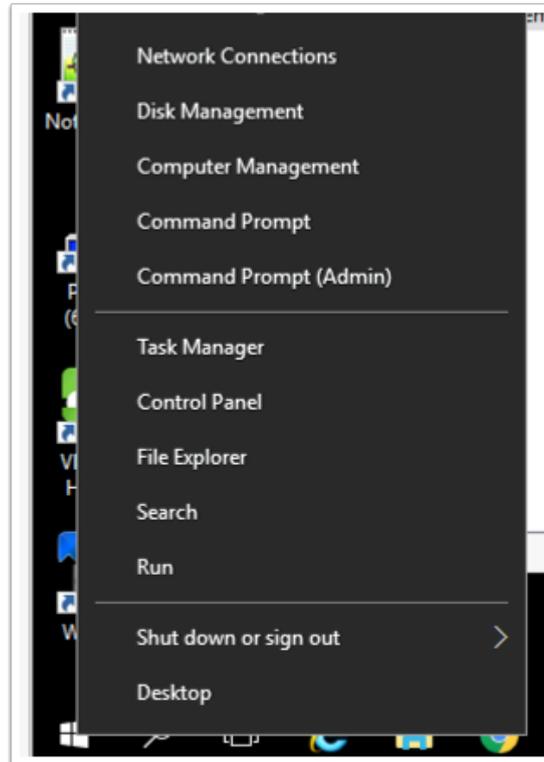


19. Switch back to the **Certificate Authority Console** select
- Right-click the **Certificate Templates** container,
 - Select **New > Certificate Template to Issue**



20. In the **Enable Certificate Templates** window

- Select the **Enrollment Agent (Computer)** template
- Select **OK**



21. We will now configure the CA for non-persistent certificate processing
- On the **TrueSSO2** server
 - Select and right-click the **Start** button
 - Select **Command Prompt (Admin)**

```
Administrator: Command Prompt

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

Old Value:
  DBFlags REG_DWORD = b0 (176)
  DBFLAGS_MAXCACHESIZEX100 -- 10 (16)
  DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
  DBFLAGS_LOGBUFFERSHUGE -- 80 (128)

New Value:
  DBFlags REG_DWORD = 8b0 (2224)
  DBFLAGS_MAXCACHESIZEX100 -- 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`

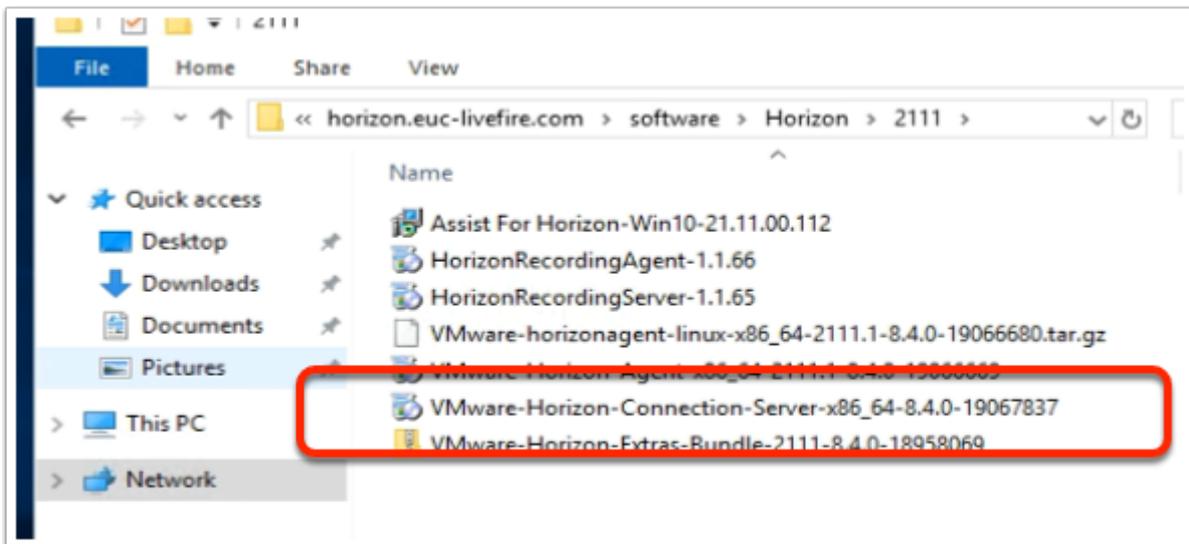
```
C:\Windows\system32>net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.

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>
```

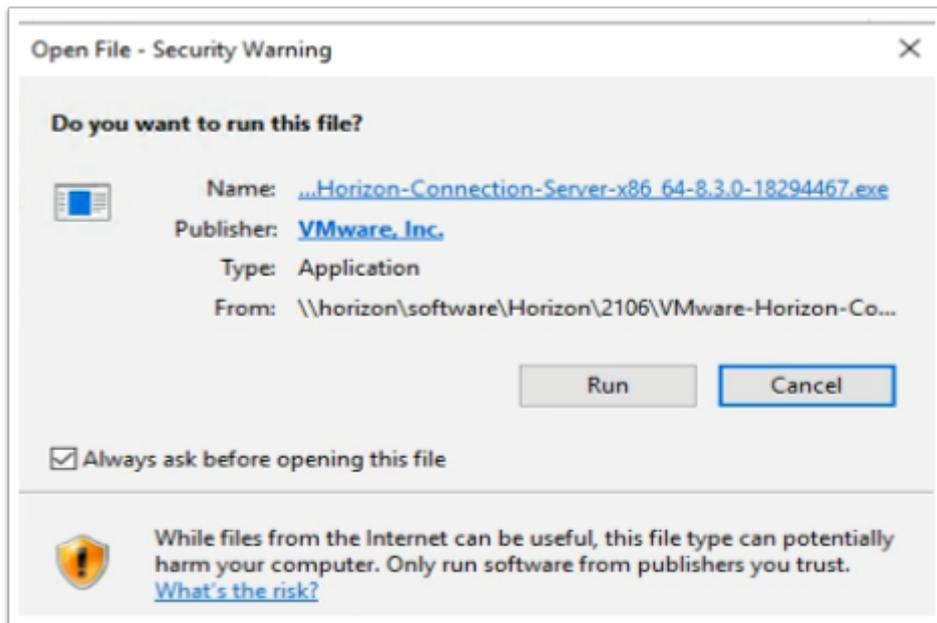
24. Restart the CA service. From the command prompt run:

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

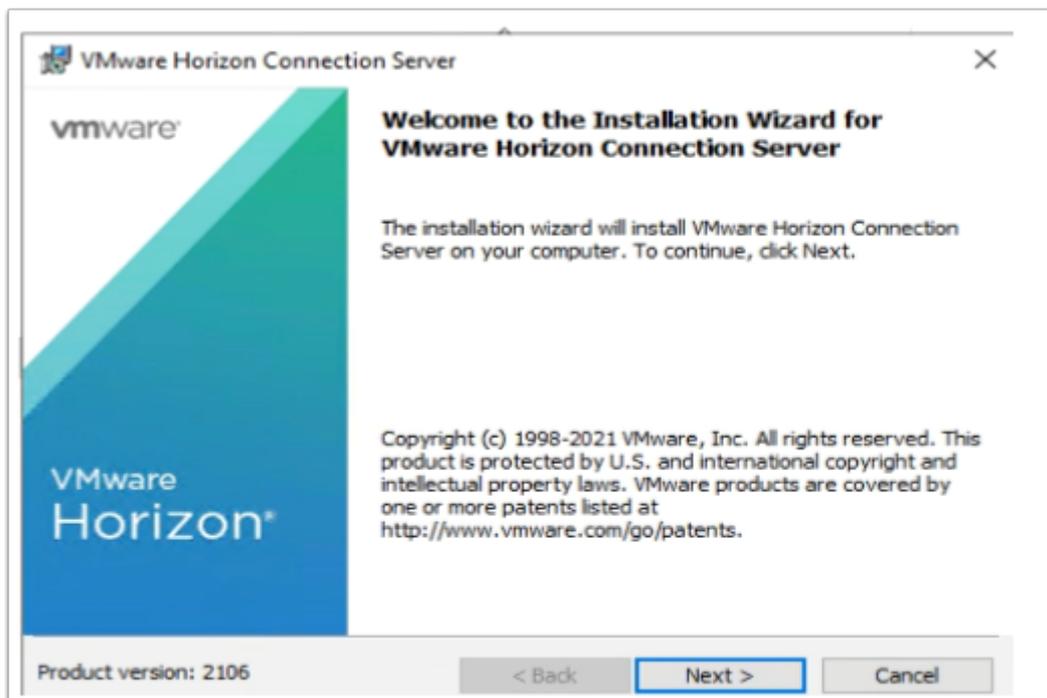


25. On the **TrueSSO2** server desktop

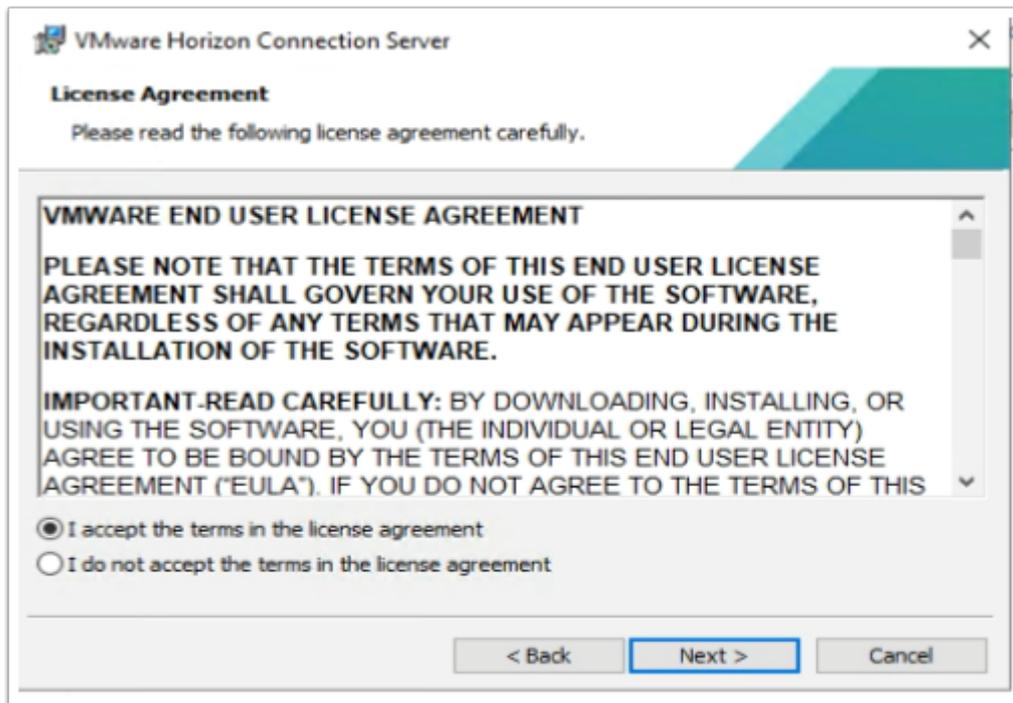
- Launch the **software** shortcut
- In the Software folder, open the **Horizon\2106** folder.
- Select and launch the **VMware-Horizon-Connection-Server-x86_64-8.4.0-19067837.exe**



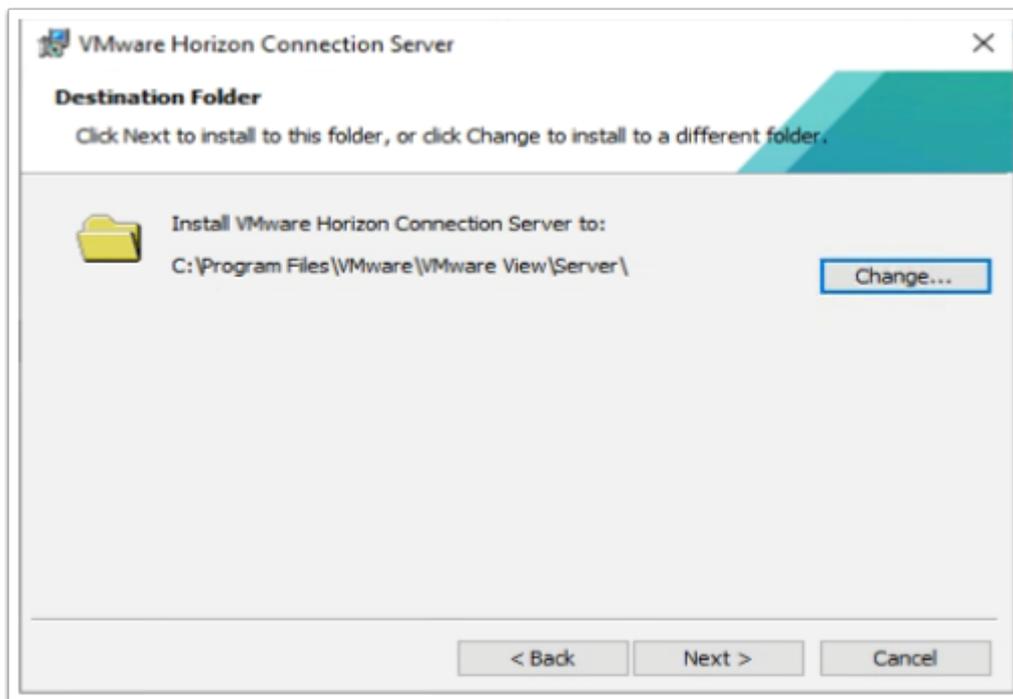
26. On the **Open File - Security Warning** window
- Select **Run**



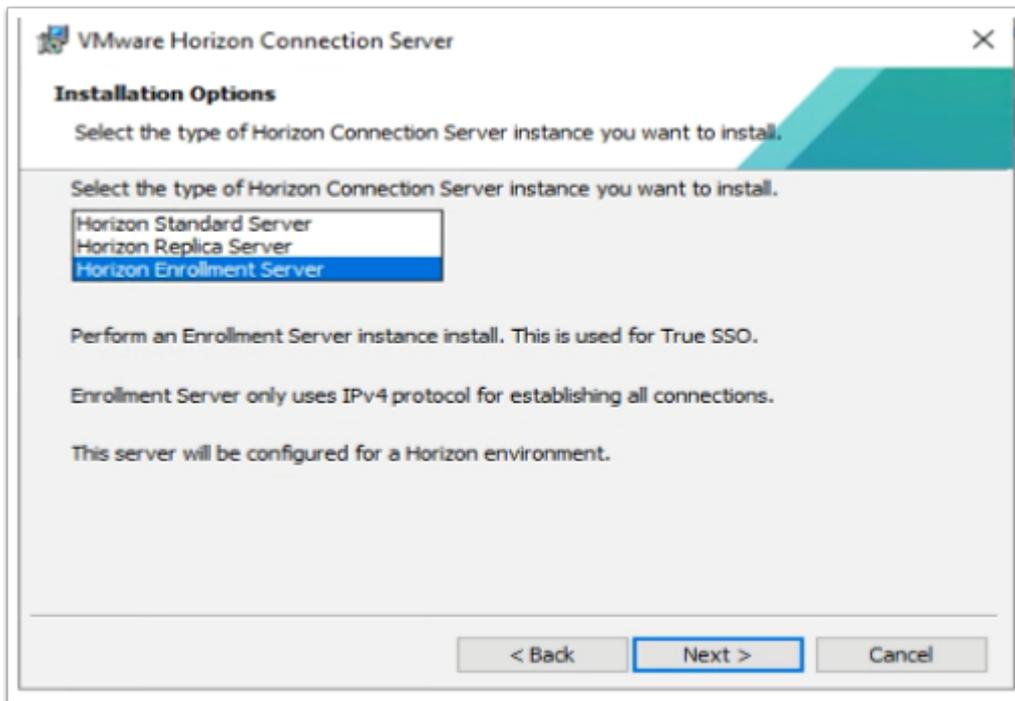
27. On the **Welcome** window
- Select **Next**



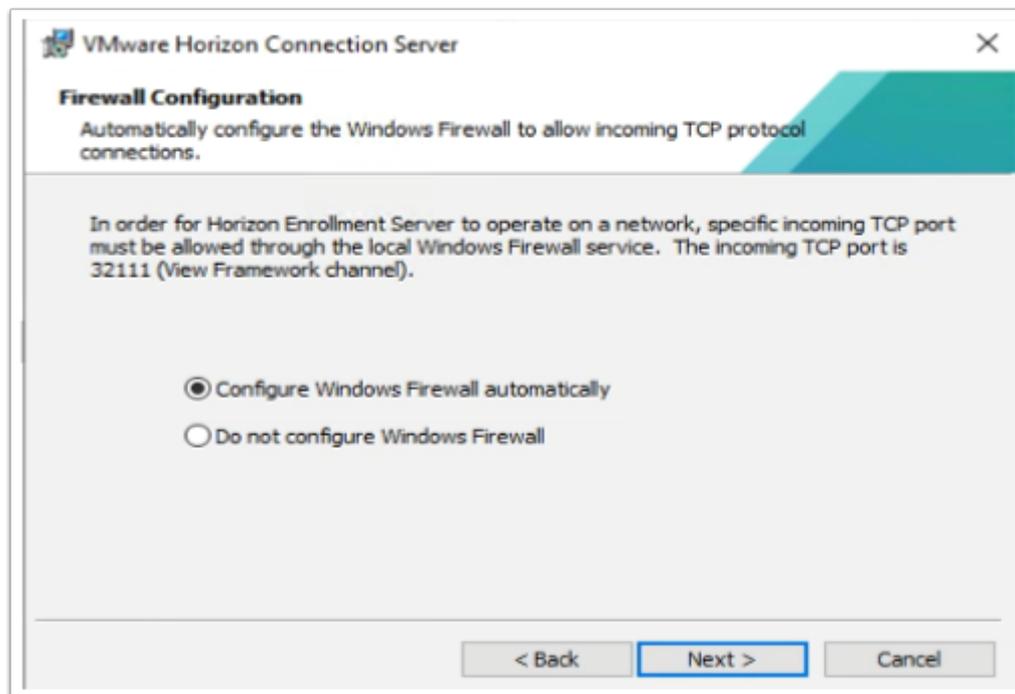
28. On the **License agreement** window
- Select the **radio button** next **I accept the terms in the license agreement**,
 - Select **Next**



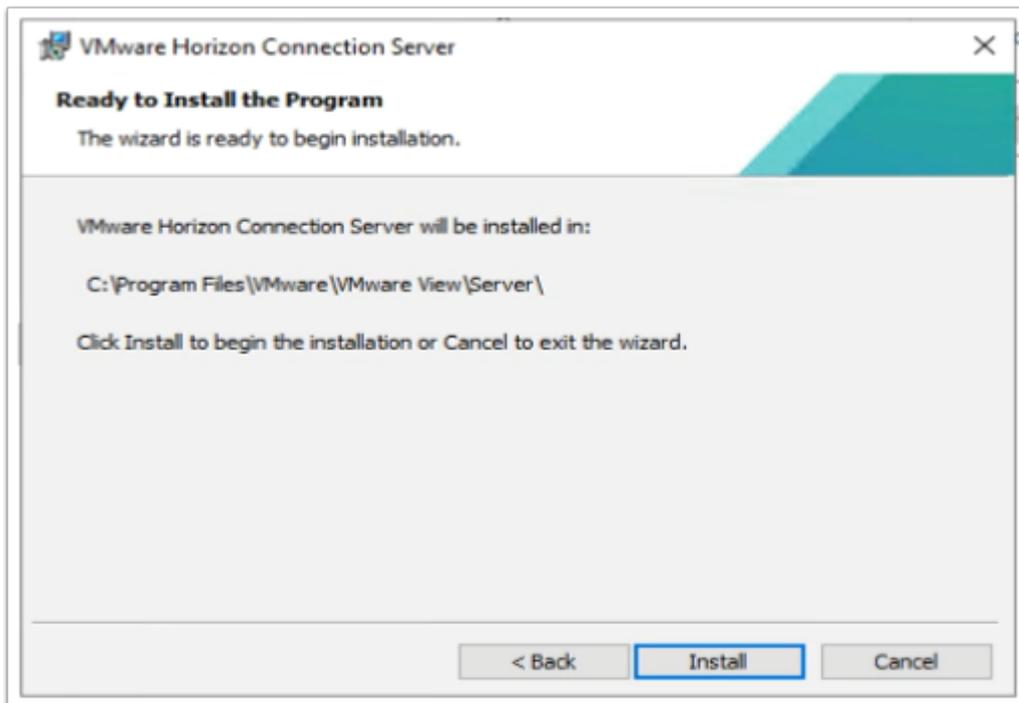
29. On **Destination Folder** window
- Select **Next**



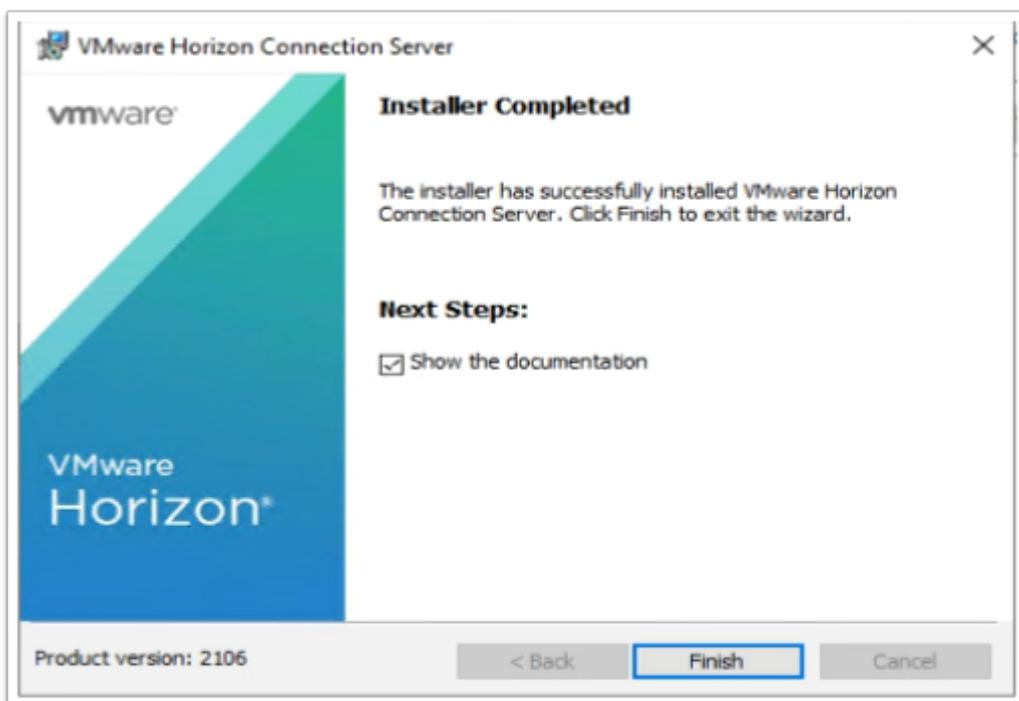
30. On the **Installation Options** window select **Horizon Enrollment Server**
- Select **Next**



31. On **Firewall configuration** window
- Select **Next**

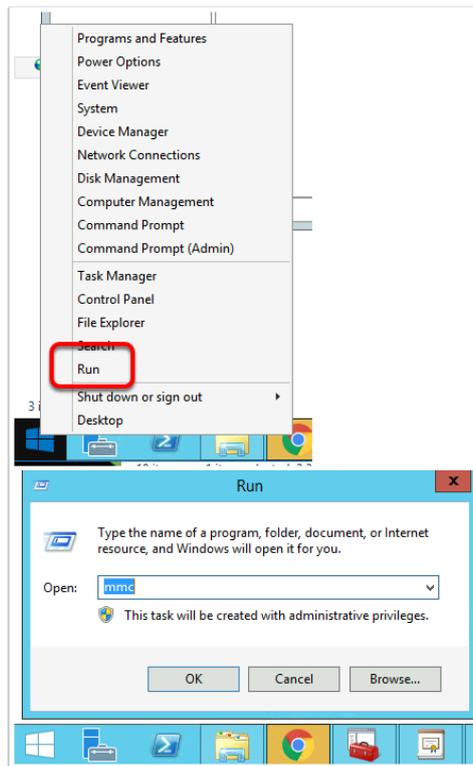


32. Select **Install**

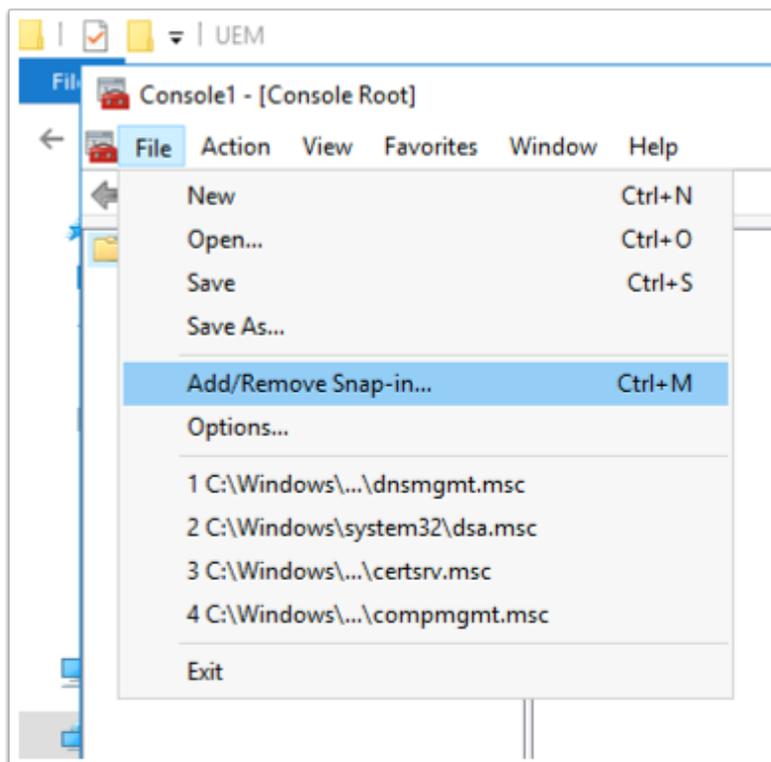


33. On the **Installer Completed** Window

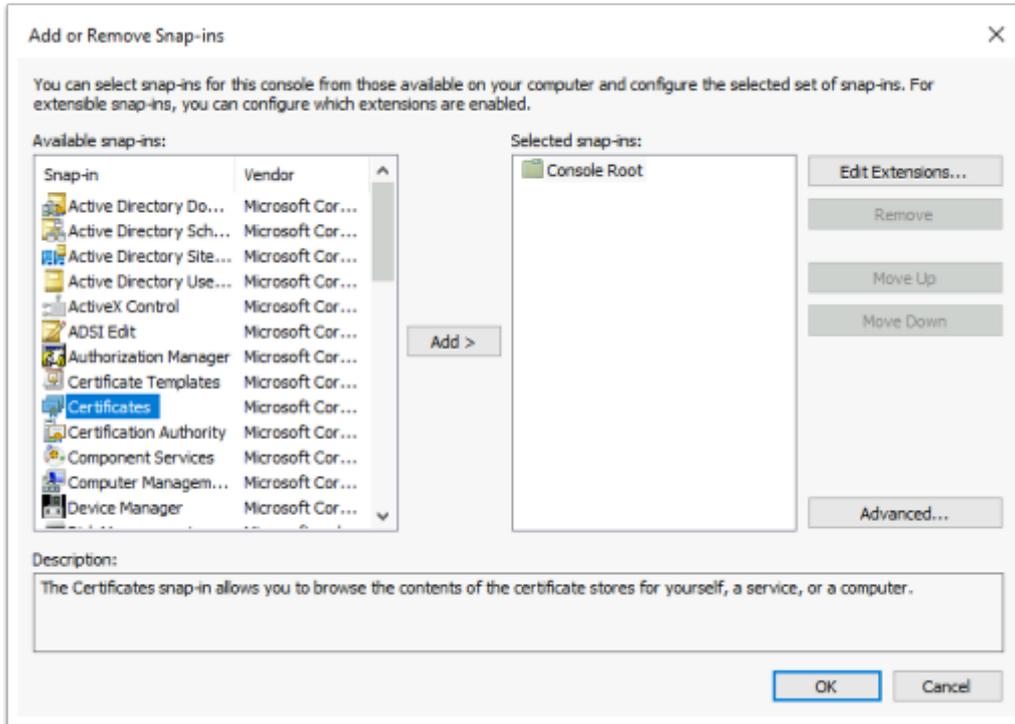
- Select **Finish**



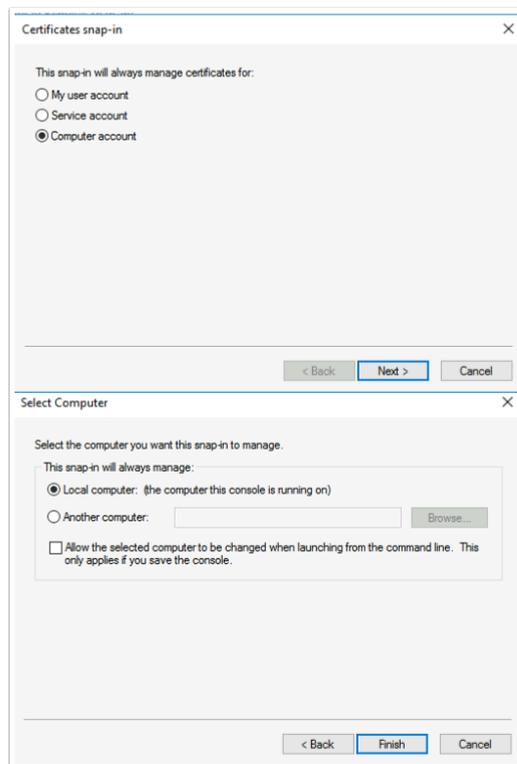
34. On the **TrueSSO2** server
- Select and right-click the **Start Button**,
 - Select **Run**,
 - Type **MMC**,
 - Select **OK**



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

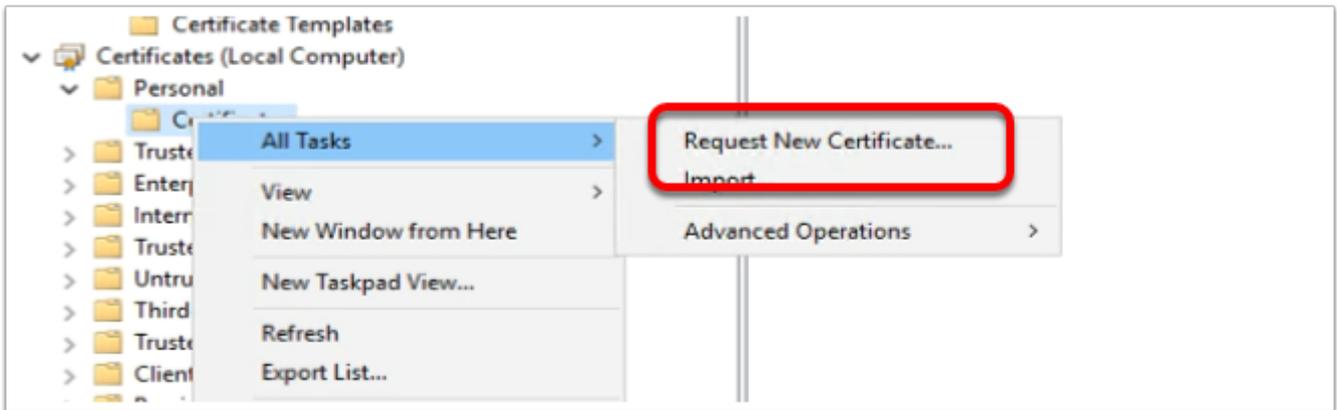


36. In the **Add or Remove Snap-ins** window,
- Select **Certificates**
 - Select **Add**

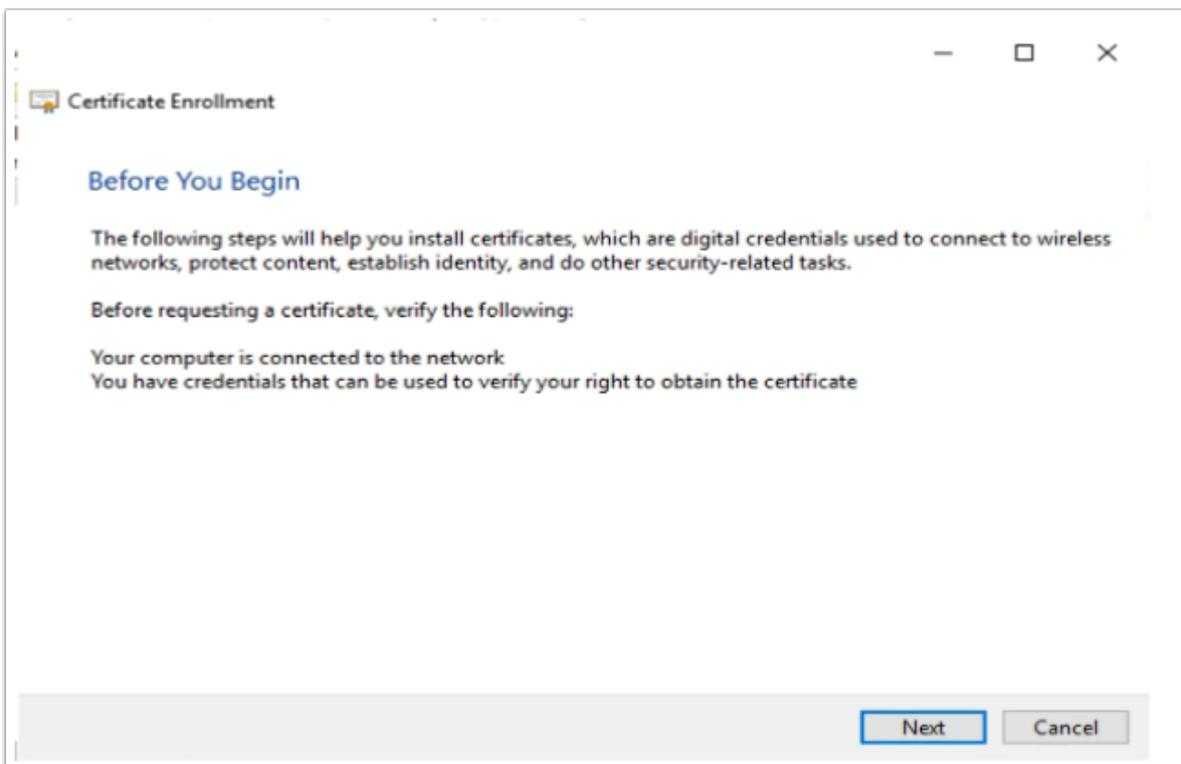


37. Select **Computer account radio button**

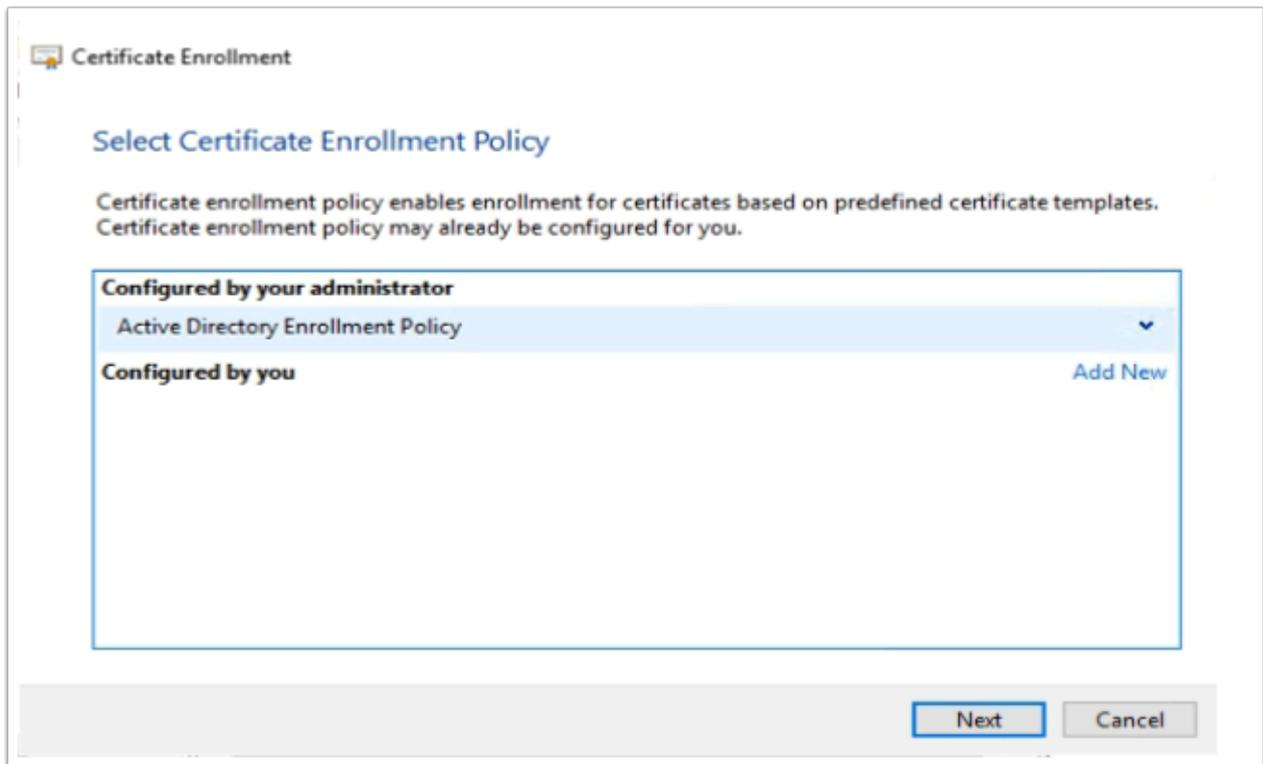
- Select **Next**
- Select **Finish**
- Select **OK**



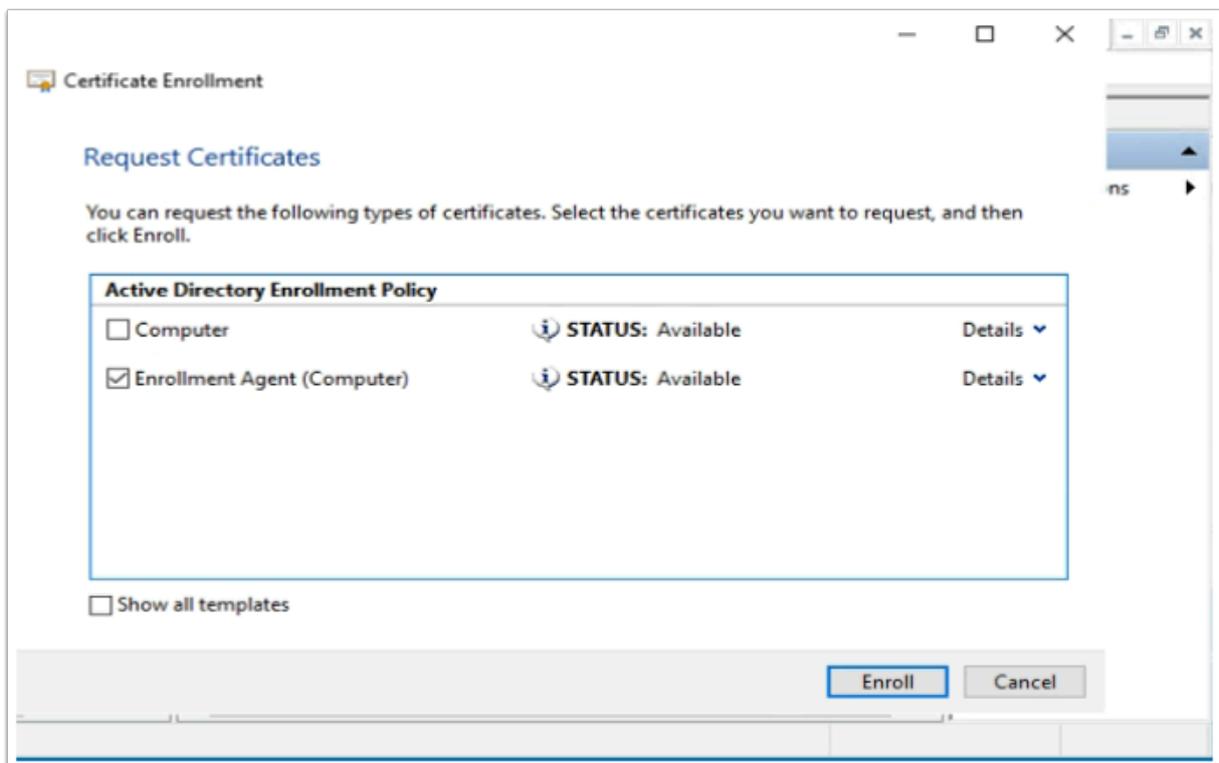
38. Expand the **Certificates** console inventory
- Select and right-click the **Personal** container.
 - Select **All Tasks** > **Request New Certificate**



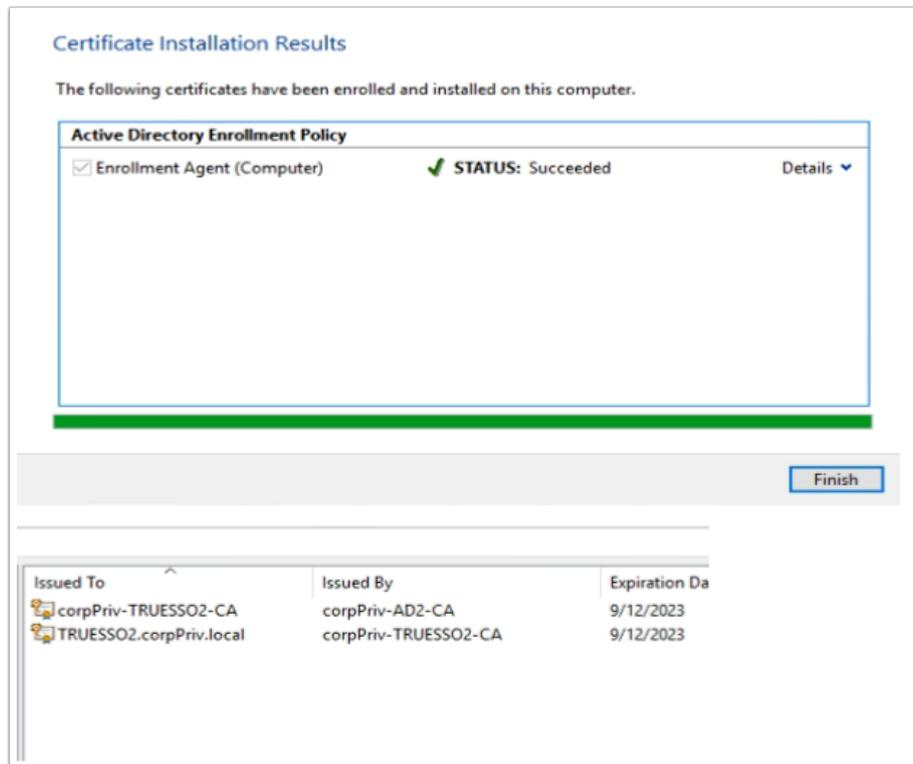
39. On the **Certificate Enrollment** > **Before you Begin** window
- Select **Next**



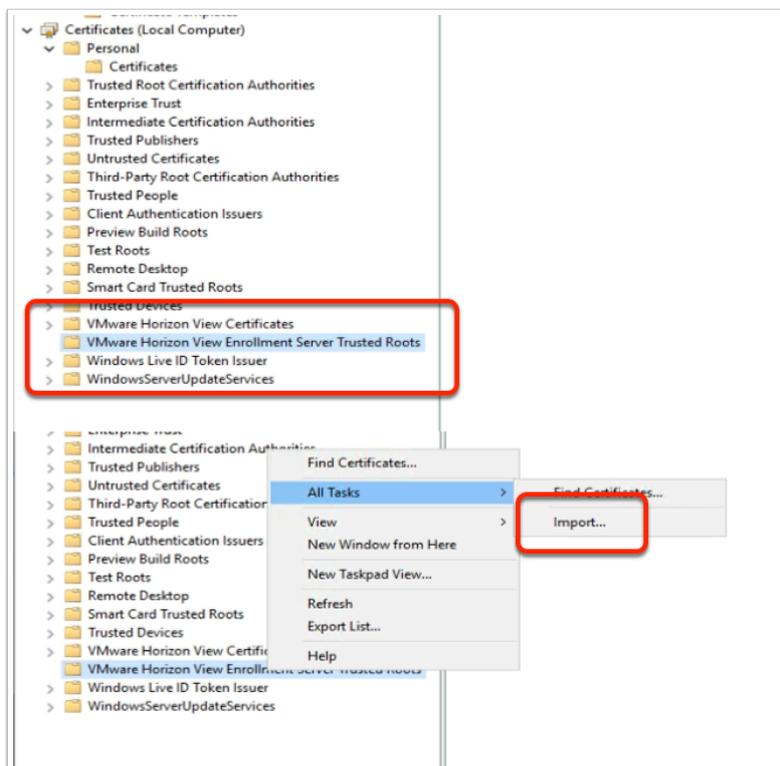
40. On the **Select Certificate Enrollment Policy** window
- Select **Next**



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

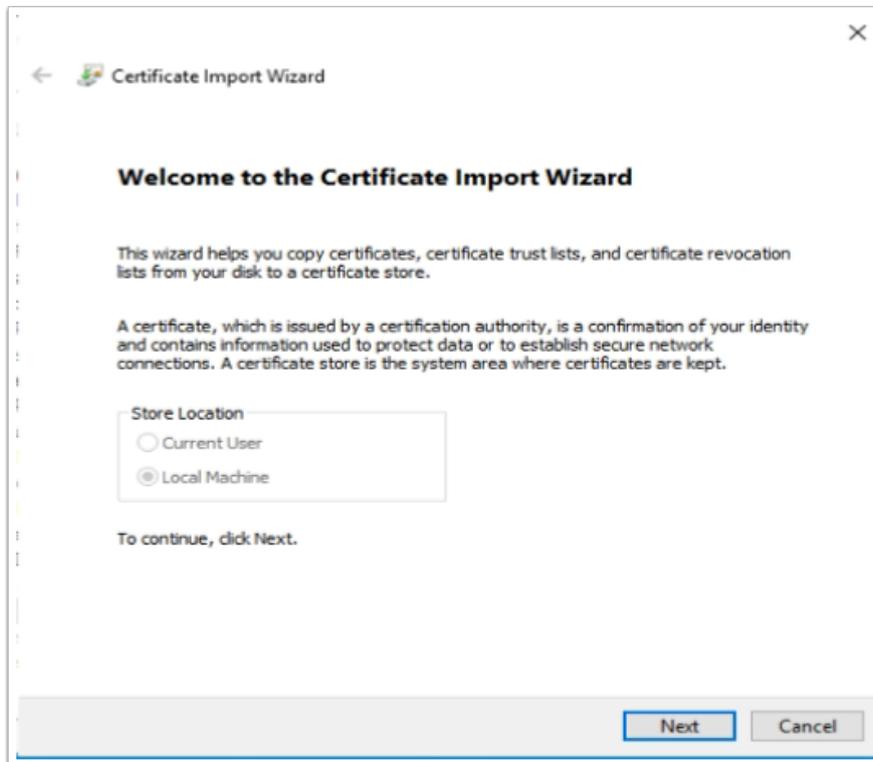


42. On the **Certificate Installation Results** window,
- Ensure the enrollment was successful
 - Select **Finish**.

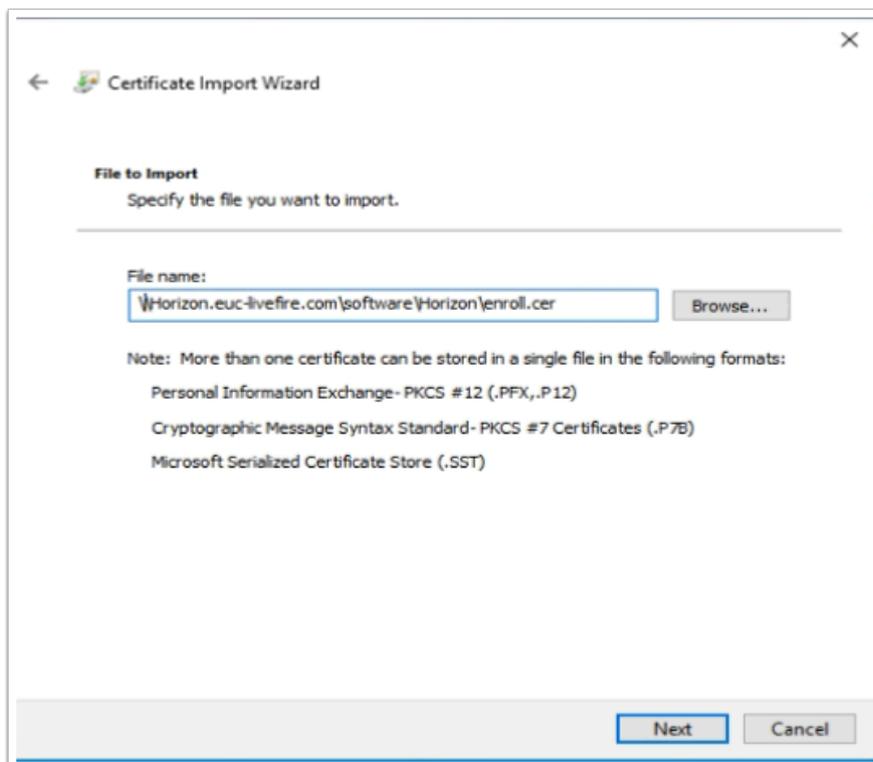


43. On your **TrueSSO2** server
- Select your **Certificate services** Snap-in,

- Select and right-click the last container in the inventory **VMware Horizon View Enrollment Server Trusted Roots**,
- Select **All Tasks > Import**

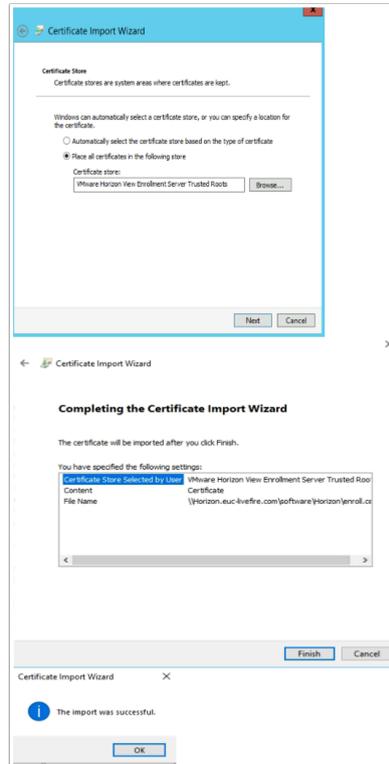


44. On the **Welcome** window
- select **Next**



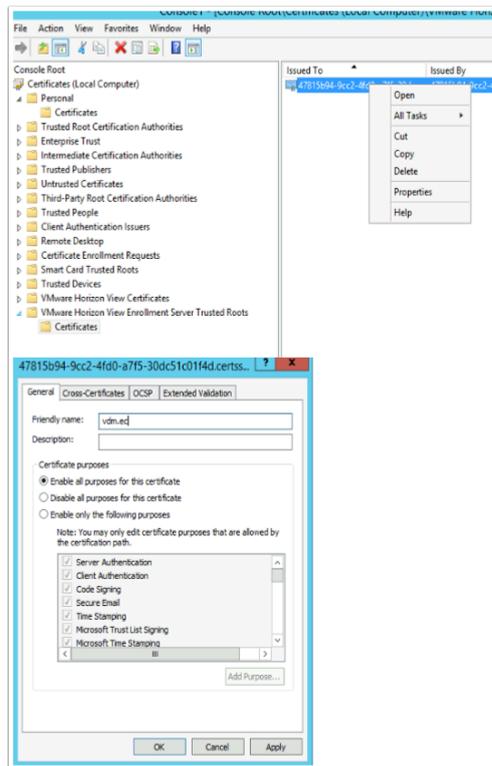
45. In the **File to import** window

- Under **File name**, type the following `\\Horizon.euc-livefire.com\software\Horizon\enroll.cer`
- Select **Next**



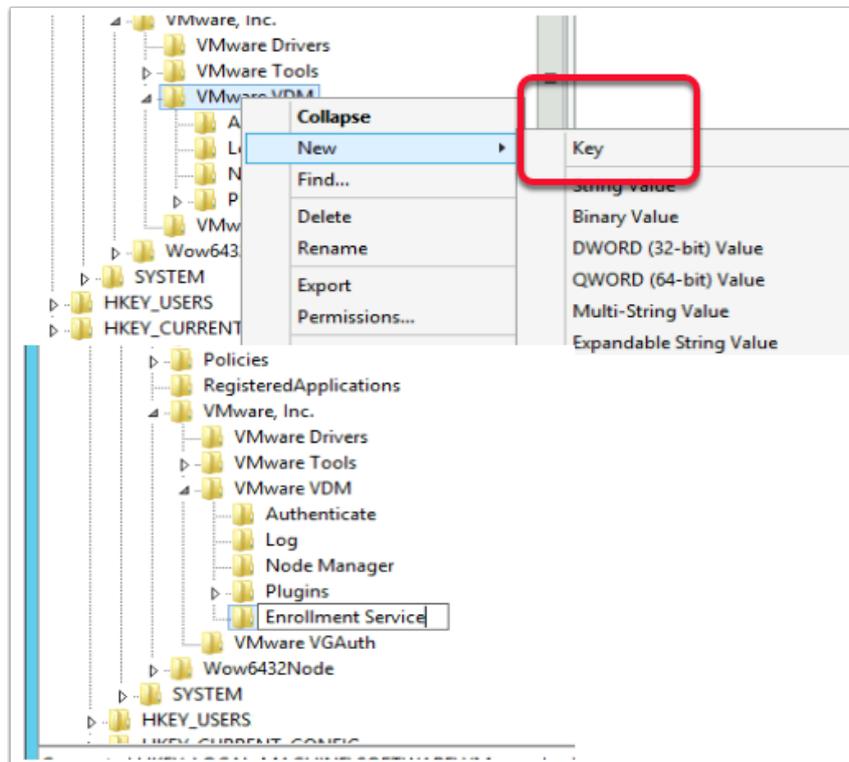
46. In the **Certificate Store** window accept the defaults and

- Select **Next**.
- On the **Summary** page select **Finish**.
- When Prompted that **The Import was succesful** select **OK**



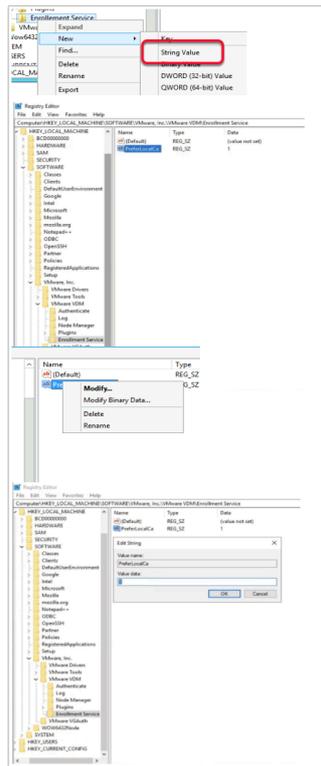
47. In the **Certificates** Folder

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



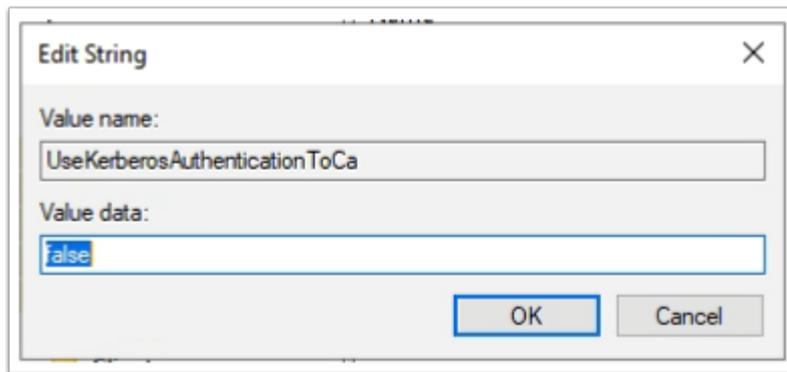
48. On your TrueSSO2 server

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



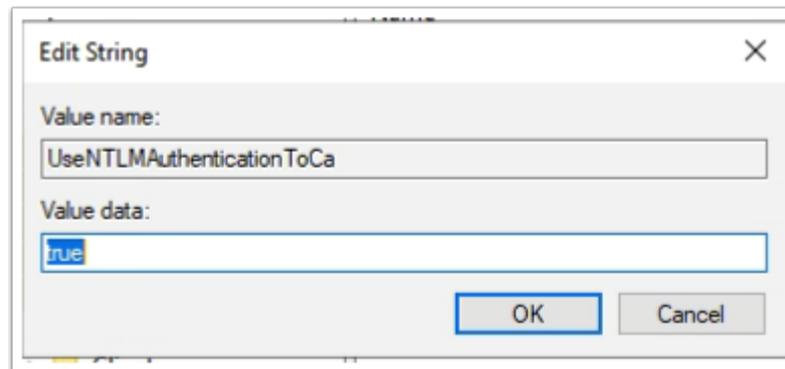
49. Configure the enrollment service to give preference to the local certificate authority when they are co-located:

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



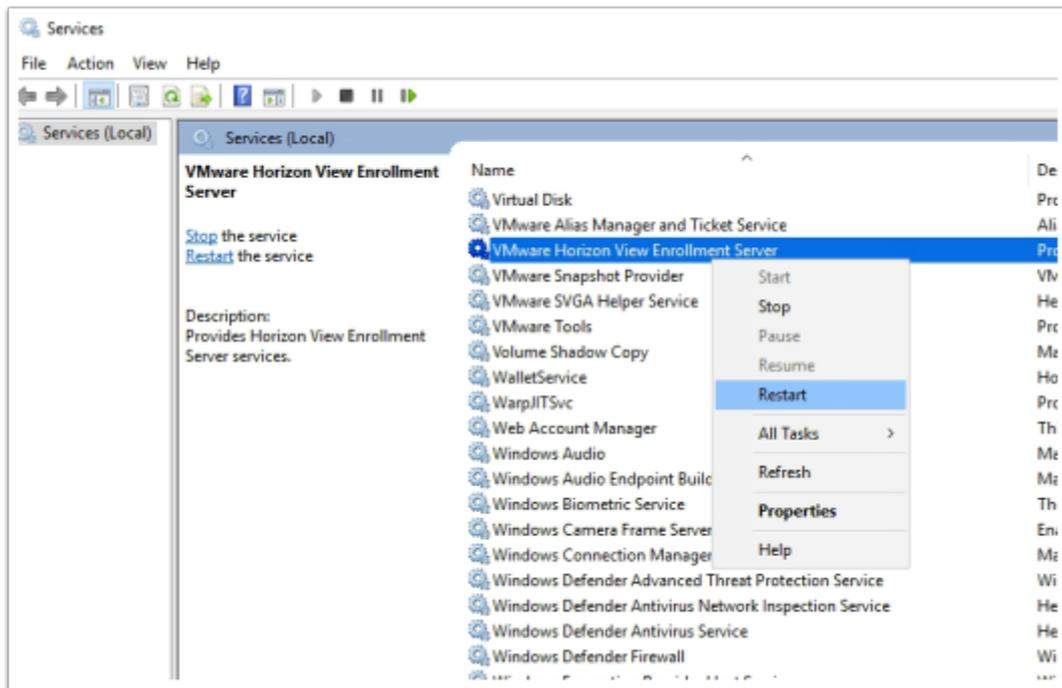
50. Add a new **String Value (this is to rectify a bug in 2111)**

- Right-click the **Enrollment Service** key > **New** > **String Value** and type the name **UseKerberosAuthenticationToCa**
- Right-click the **UseKerberosAuthenticationToCa** String value and select **Modify** and in the **Value data:** field enter **false**
- Select **OK** to close the window.

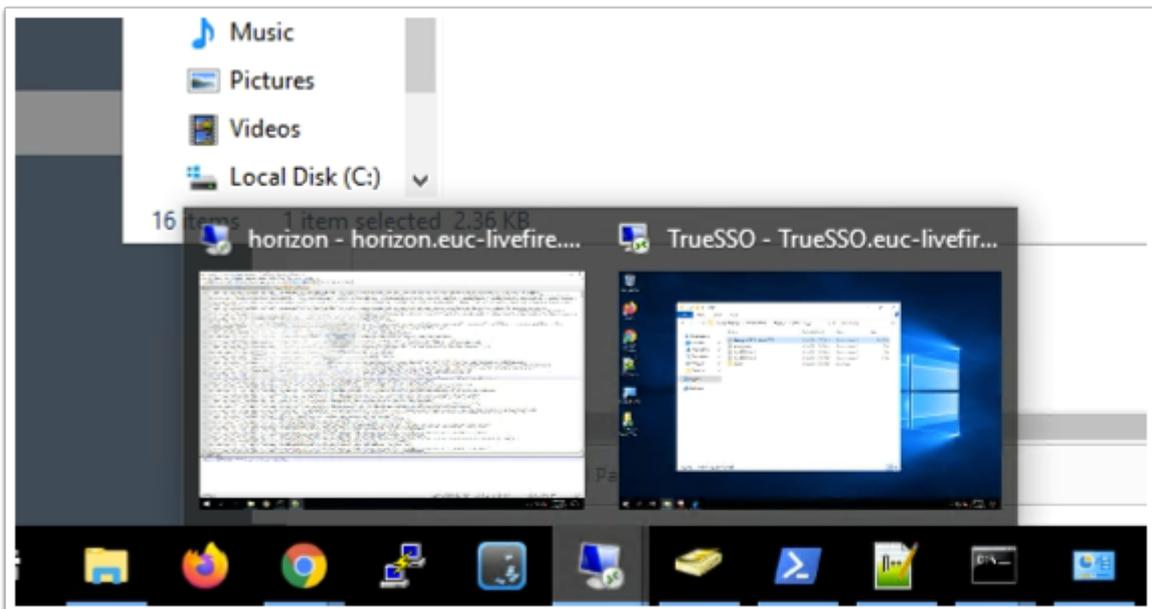


51. Add a new **String Value (this is to rectify a bug in 2111)**

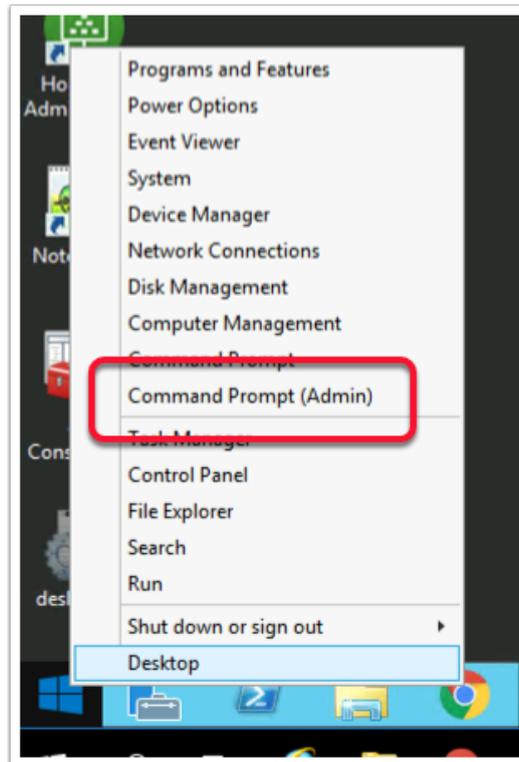
- Right-click the **Enrollment Service** key > **New** > **String Value** and type the name **UseNTLMAuthenticationToCa**
- Right-click the **UseNTLMAuthenticationToCa** String value and select **Modify** and in the **Value data:** field enter **true**
- Select **OK** to close the window.



52. On your TrueSSO2 server
- From the **Start** button, select **Run**
 - Type **services.msc** and select **OK**
 - Scroll down to **VMware Horizon View Enrollment Server service** in services menu
 - Select and right-click the **VMware Horizon View Enrollment Server service**
 - Select **Restart**
 - **Close** the **Services** mmc



53. On your **ControlCenter** server
- Switch to your **HORIZON.RDP** session



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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "\Program Files\VMware\VMware View\Server\tools\bin"
C:\Program Files\VMware\VMware View\Server\tools\bin>
```

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

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

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administra
tor --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>
```

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

The enrollment server is added to the global list.

```
vdmUtil --authAs administrator --authDomain euc-livefire.com --authPassword VMware1! --truesso --environment --add --enrollmentServer TrueSSO2.corpPriv.local
```



```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire.com --authPassword VMware1! --truesso --environment --list --enrollmentServer TrueSSO2.corpPriv.local --domain corpPriv.local
True SSO environment info
Enrollment server: truesso2.corppriv.local
Domain: corppriv.local
Forest:
  Name: corpPriv.local
  Enrollment CertState: VALID
  Template(s):
    Name: TrueSSOTemplate
    Minimum key length: 2048
    Hash algorithm: SHA256
  Certificate Authority(s):
    Name: corpPriv-AD2-CA
    Name: corpPriv-TRUESSO2-CA
C:\Program Files\VMware\VMware View\Server\tools\bin>
```

57. **Wait 2 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! --truesso --environment --list --enrollmentServer TrueSSO2.corpPriv.local --domain corpPriv.local
```



```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire.com --authPassword VMware1! --truesso --create --connector --domain corpPriv.local --template TrueSSOTemplate --primaryEnrollmentServer truesso2.corpPriv.local --certificateServer corpPriv-TRUESSO2-CA --mode enabled
Connector created
Domain: corpPriv.local
Mode: ENABLED
C:\Program Files\VMware\VMware View\Server\tools\bin>
```

58. 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! --truesso --create --connector --domain corpPriv.local --template TrueSSOTemplate --primaryEnrollmentServer truesso2.corpPriv.local --certificateServer corpPriv-TRUESSO2-CA --mode enabled
```

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

59. 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-livefire --authPassword VMware1! --
truesso --list --authenticator
```

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire
--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>
```

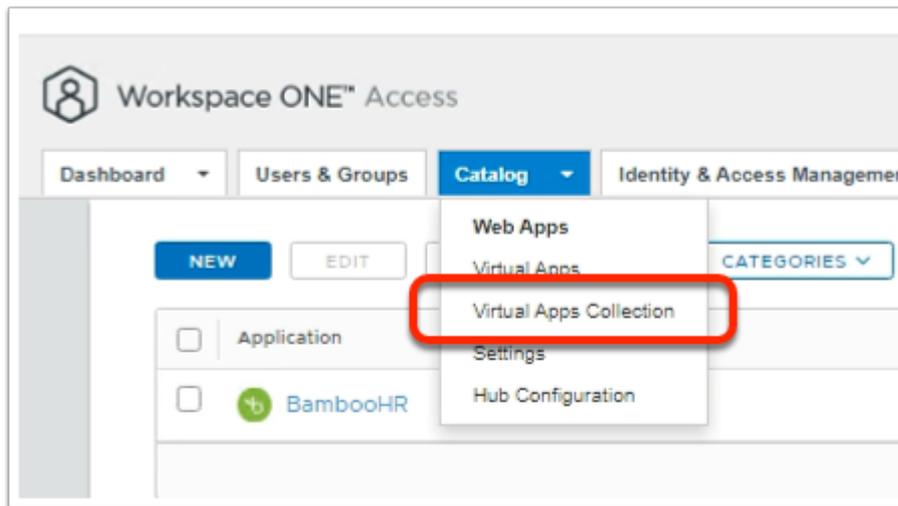
60. You will notice True SSO mode is Disabled. Enter the command to enable the authenticator to use True SSO mode

```
vdmUtil --authAs administrator --authDomain euc-livefire --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

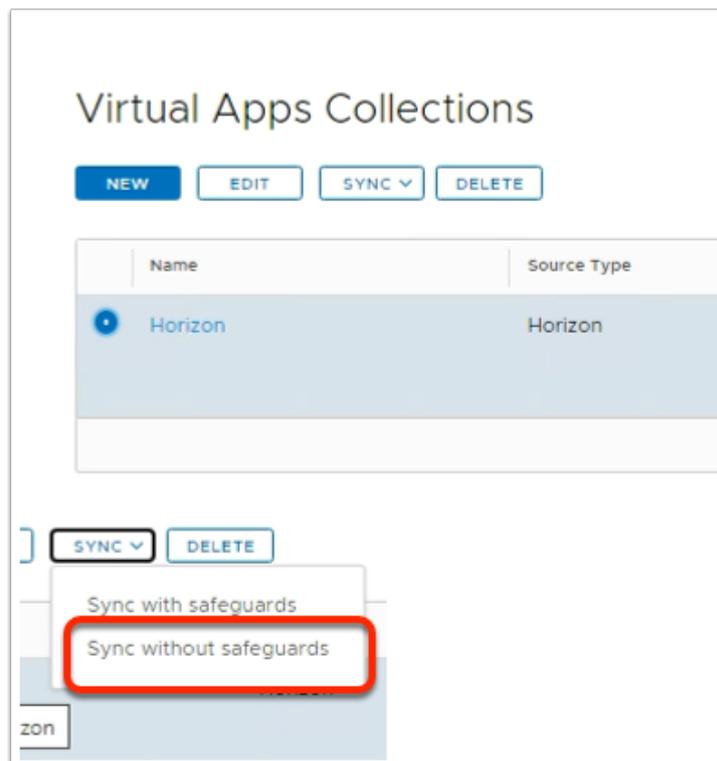
Part 7: Validating Workspace ONE Access User and Group Entitlements.

We will be validating an undocumented issue we have come across in the latest 2108 Connector version of Workspace ONE Access



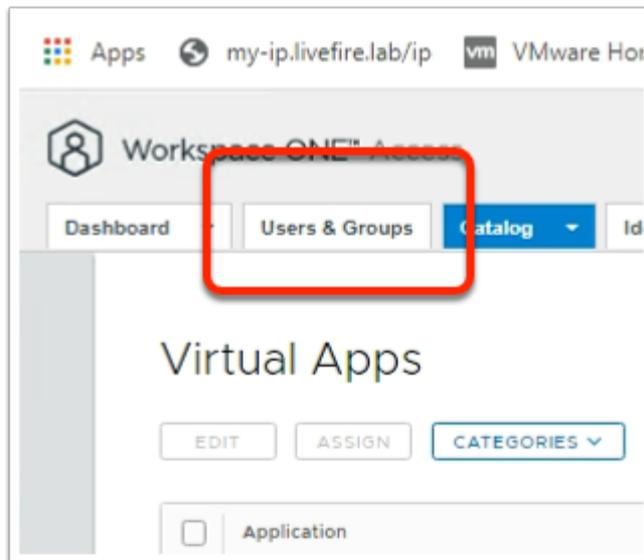
1. In the Workspace ONE Access Console

- Select the **Catalog** tab
- From the dropdown, select **Virtual Apps Collection**



2. In the **Virtual Apps Collections** window

- Select the **radio button** next to **Horizon**
- Select the **dropdown** next to **SYNC**
- Select **Sync without safeguards**

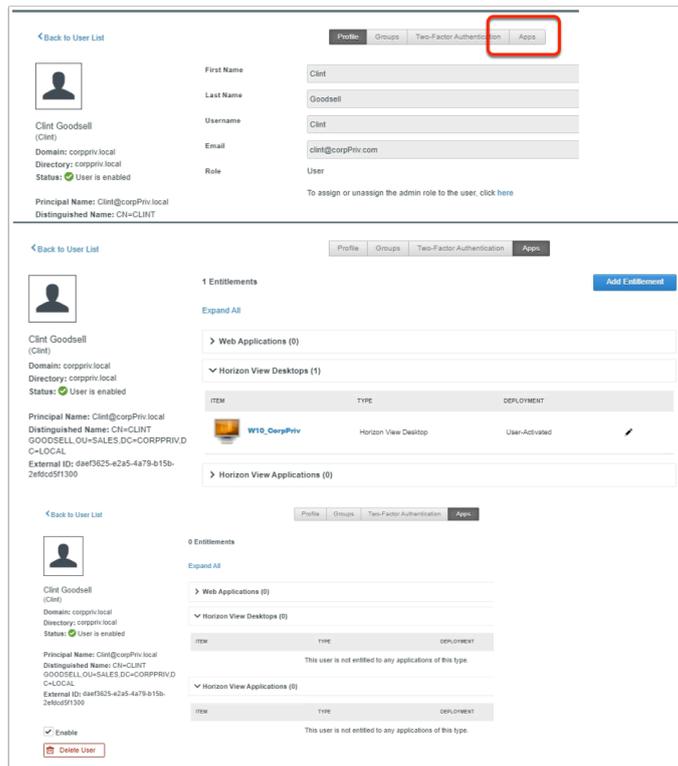


1. In the Workspace ONE Access console
 - Select the **Users & Groups** tab

Users (10)

User Name	User ID	Domain	Directory
Admin, Tenant	administrator	System Domain	System Directory
Debio, Mark	Mark	euc-livefire.com	LivefireSync
Dusello, Fernando	Fernando	euc-livefire.com	LivefireSync
Goodsell, Clint	Clint	corpriv.local	corpriv.local
Ikin, Kevin	Kevin	euc-livefire.com	LivefireSync

2. In the **Users** Interface
 - Select **Goodsell, Clint**

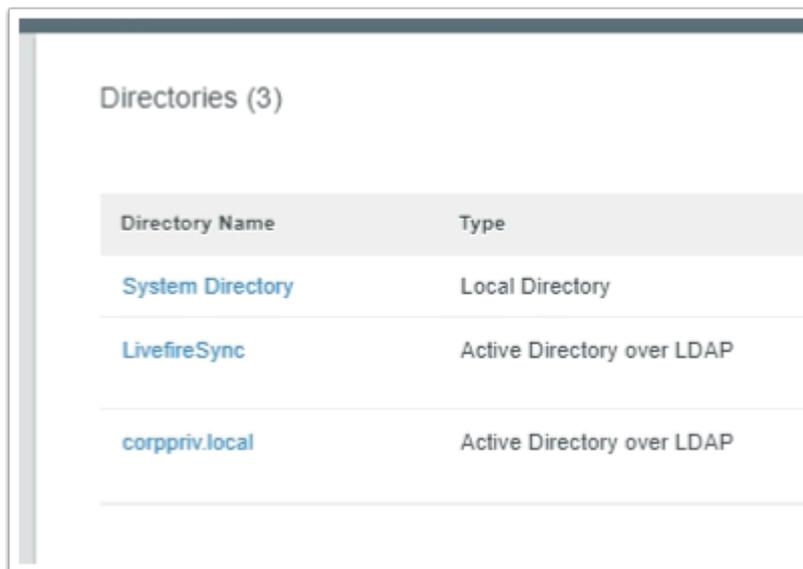


3. In the **Clint Goodsell** interface

- Select **Apps** tab

4. In the **Apps** tab

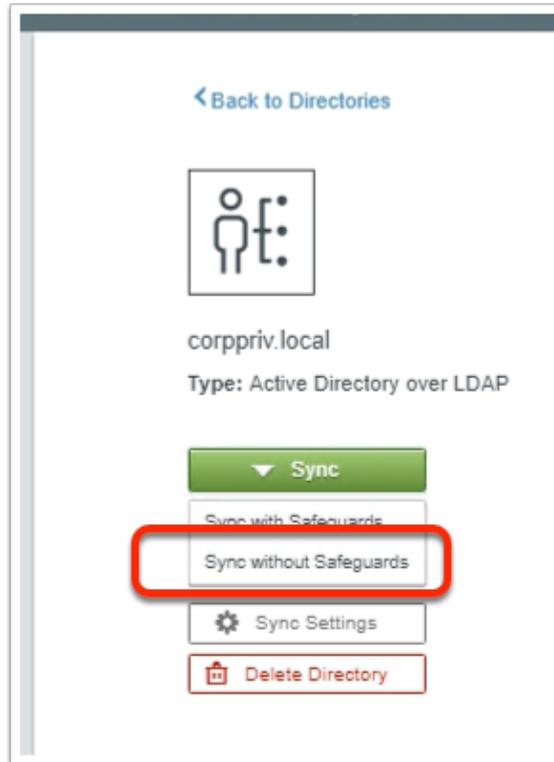
- Expand **Horizon View Desktops** and **Horizon Applications**
 - There should be associated virtual desktops and virtual applications
 - If there are not move on to **step 5**, everything fine in your environment, move on to **Part 8**



26. In the Workspace ONE Access Admin console

- Select the **Identity & Access Management** tab

- In **Directories** area
 - Select **corppriv.local**



27. In the **corppriv.local** interface

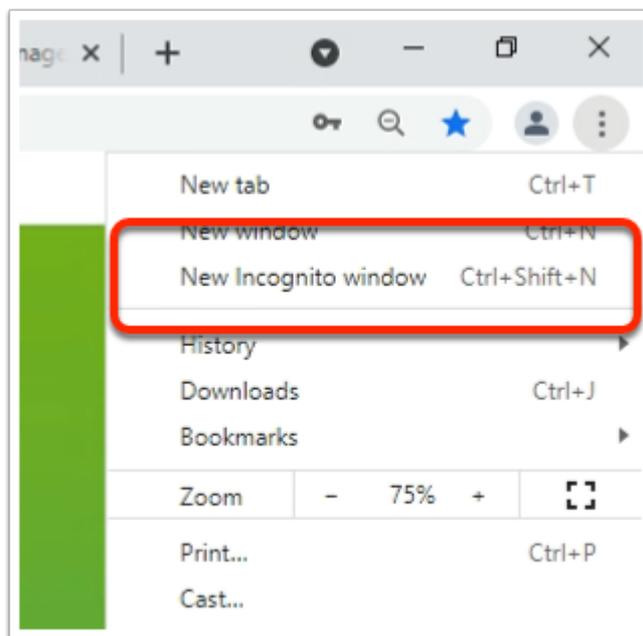
- Select **Sync**,
 - From the dropdown, select **Sync without Safeguards**
- Once the sync has completed
 - Select the **User & Groups** tab
 - Select **Debio Mark**
 - Select the **Apps** tab
 - Expand **Horizon View Desktops** and **Horizon View Applications**
 - You should now have your Virtual Desktops and Virtual Applications
 - Note this is an undocumented feature we have discovered with regard to the 2108 connector version of Workspace ONE Access

Workspace ONE Access user profile for Clint Goodsell. The page includes a navigation bar with tabs for Profile, Groups, Two-Factor Authentication, and Apps. The user's profile information is displayed on the left, and the entitlements are listed on the right. The entitlements are categorized into Web Applications (0), Horizon View Desktops (1), and Horizon View Applications (0). The Horizon View Desktops table shows one item: W10_CorpPriv, which is a Horizon View Desktop with a User-Activated deployment.

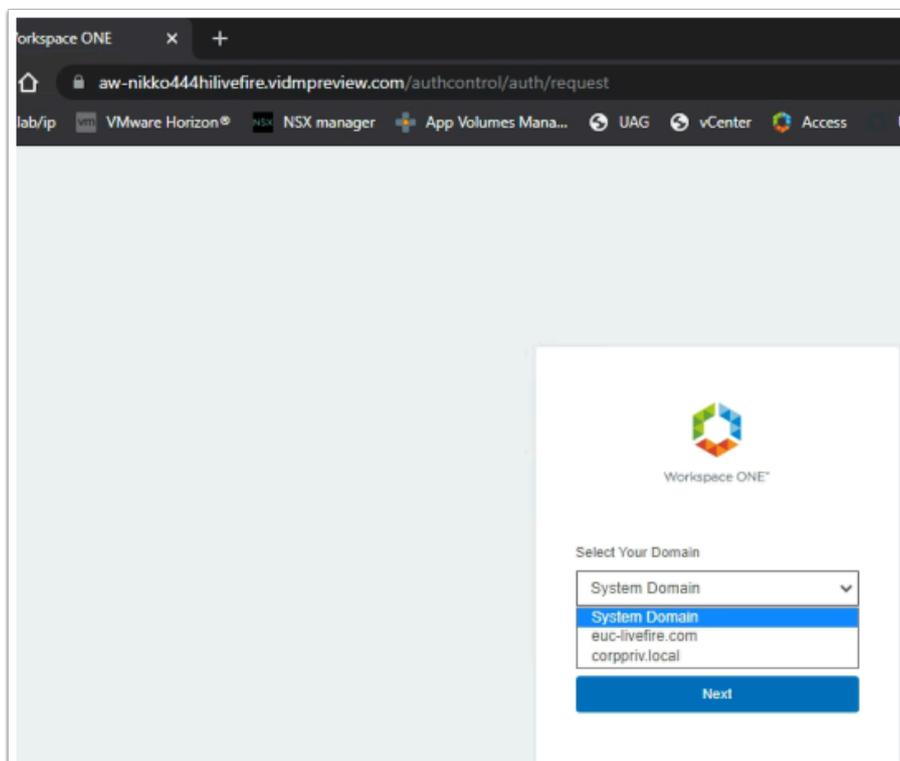
ITEM	TYPE	DEPLOYMENT
W10_CorpPriv	Horizon View Desktop	User-Activated

28. Once the sync has completed
- Select the **User & Groups** tab
 - Select **eGoodselbio Mark**
 - Select the **Apps** tab
 - Expand **Horizon View Desktops** and **Horizon View Applications**
 - You should now have your Virtual Desktops and Virtual Applications
 - Note this is an undocumented feature we have discovered with regard to the 2108 connector version of Workspace ONE Access
 - In the authoring of this lab there were a lot more attempts made. On a first test and write, its not possible to validate the scope of this issue.
 - It might be necessary to reach out to your instructor for further assistance

Part 8: Testing Untrusted Domain Integration with Workspace ONE Access

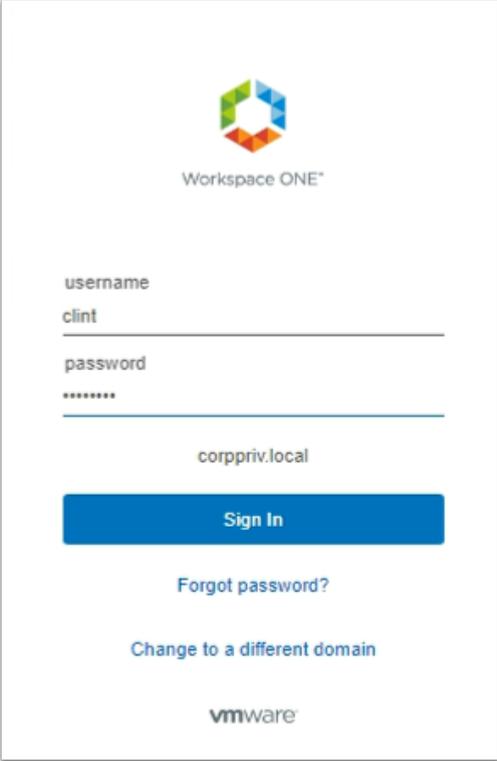


1. On your ControlCenter Server
 - Open a **New Incognito mode window** session with your Chrome browser



2. In the Chrome browser

- Using **your custom Access URL**, launch your Workspace ONE Access porta
- In the **Select your Domain** area
 - Select **corpPriv.local**
 - Select **Next**



Workspace ONE*

username
clint

password

corppriv.local

Sign In

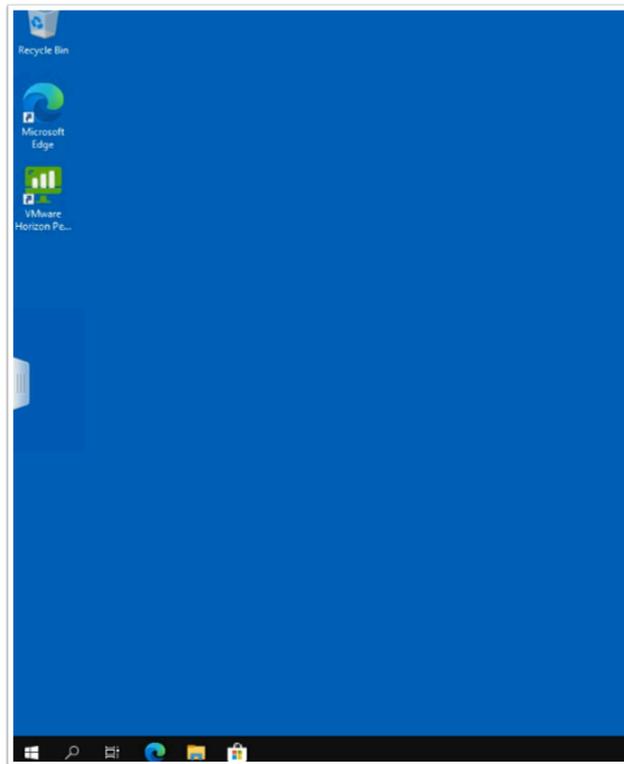
Forgot password?

Change to a different domain

vmware

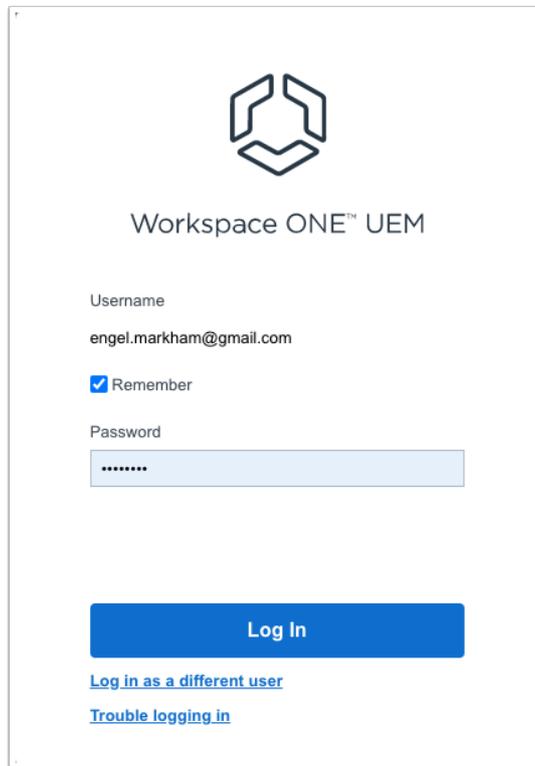
3. In the Workspace ONE Access login

- Under **username**
 - enter **clint**
- Under **password**
 - enter **VMware1!**
- Select **Sign In**



6. On your Horizon web client
 - Note that you had a single sign-on experience
 - **Log off** when done

Part 9: Unified EndPoint Integration with the Active Directory Untrusted Domain



Workspace ONE™ UEM

Username
engel.markham@gmail.com

Remember

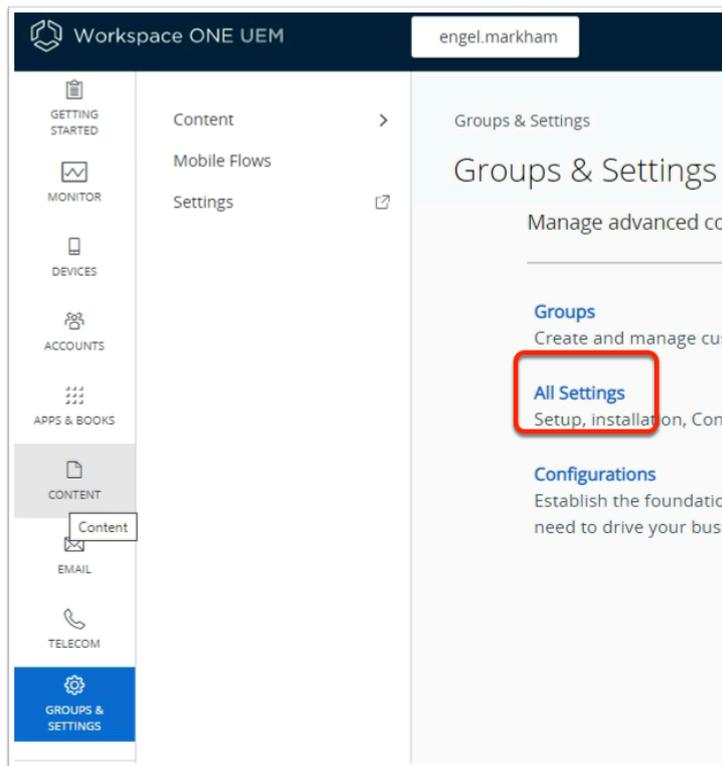
Password

[Log In](#)

[Log in as a different user](#)

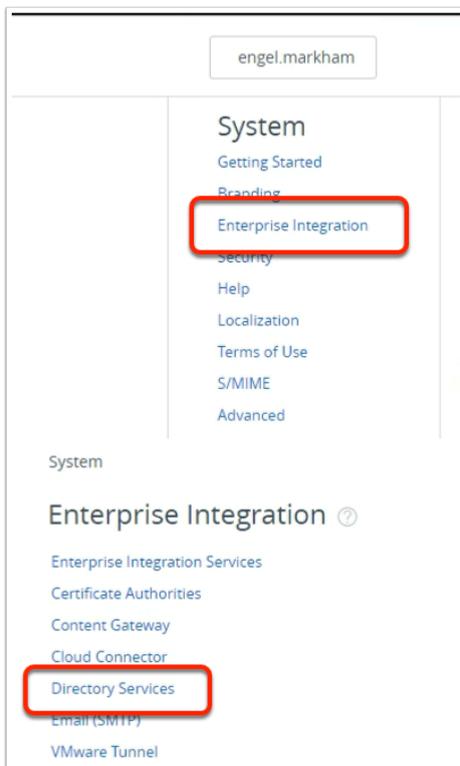
[Trouble logging in](#)

1. On your laptop / Desktop
 - login with your Custom Workspace ONE UEM Credentials



2. In the **Workspace ONE UEM Admin Console**

- Go to **GROUPS & SETTINGS > All Settings**



3. In the **Workspace ONE UEM Admin Console**

- Under **System**, select **Enterprise Integration**
- Under **Enterprise Integration**, select **Directory Services**

Bind Password CHANGE

Domain	Server
euc-livfire.com	ControlCenter.euc-live

+ ADD DOMAIN

[> Advanced](#)

4. In the **Workspace ONE UEM Admin** Console
 - In the **Directory Services** window > **Server** Tab
 - **Scroll down** and select **+ ADD DOMAIN**

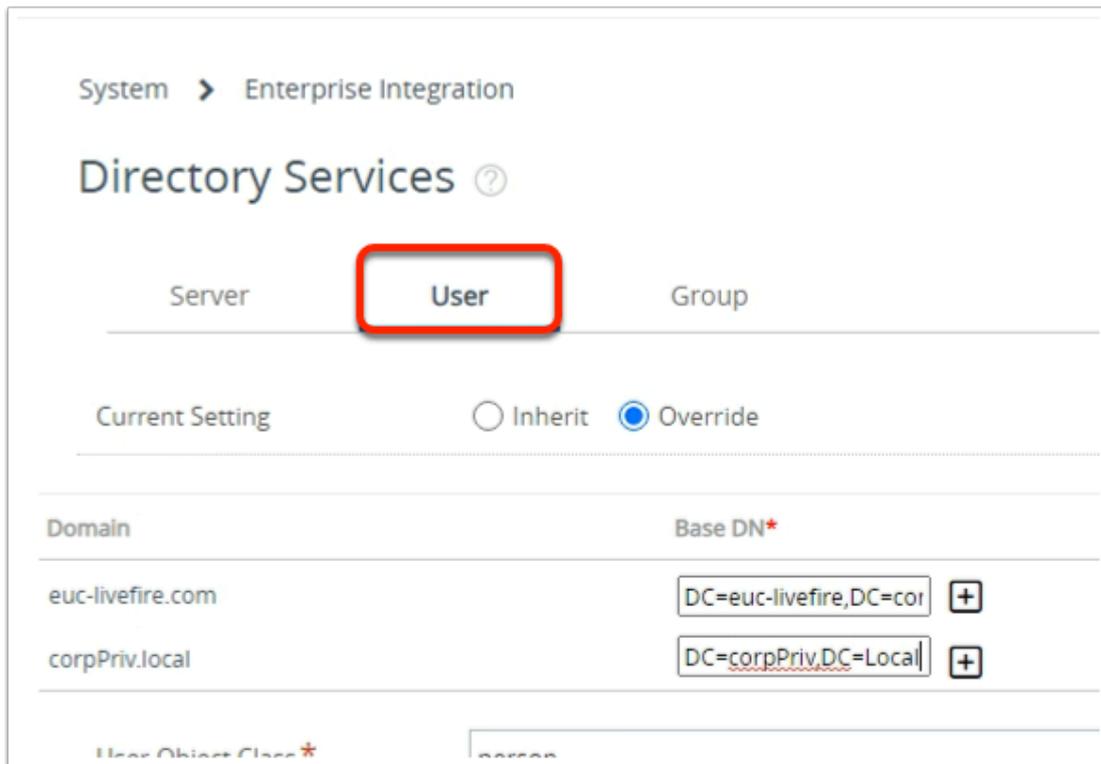
ird CHA

Domain	Server
euc-livfire.com	ControlCenter.euc-live
corpPriv.local	ad2.corpPriv.local ✘

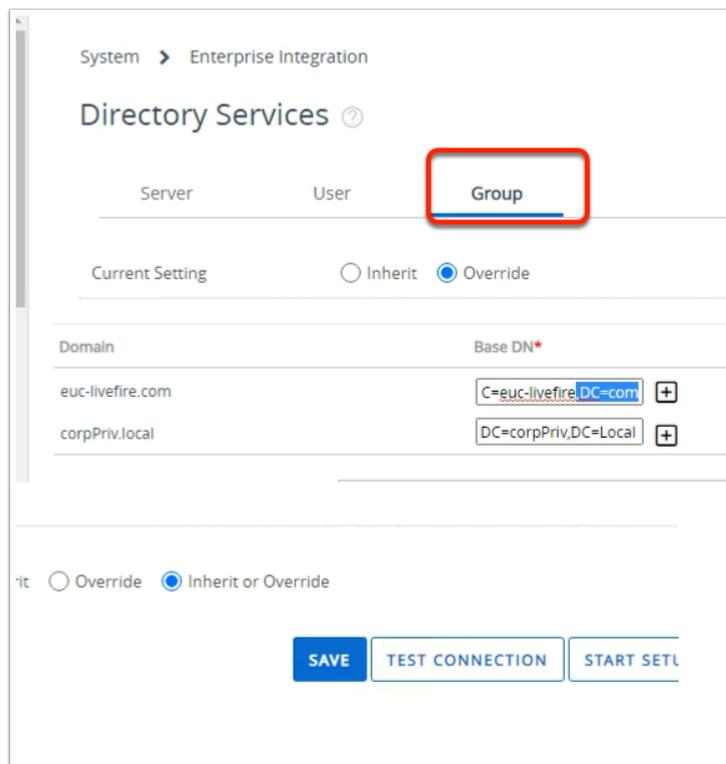
+ ADD DOMAIN

ist relationship the specified YES NO i

5. In the **Workspace ONE UEM Admin** Console
 - Under the **Domain** area : enter **corpPriv.local**
 - Under the **Server** area : enter **ad2.corpPriv.local**



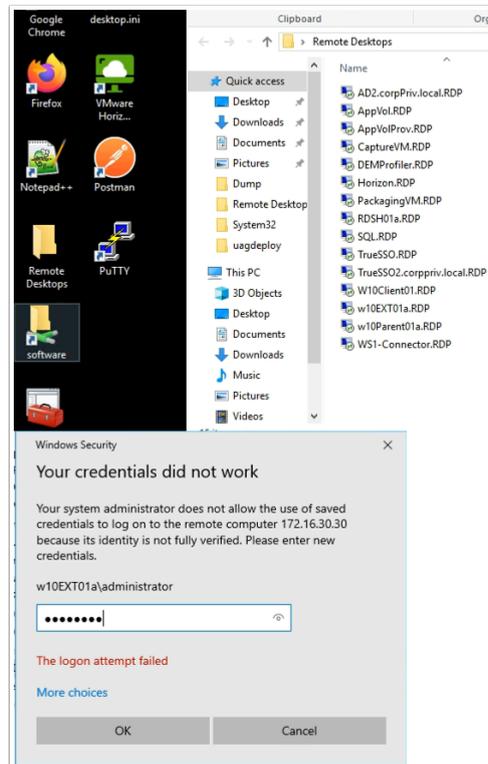
6. In the **Workspace ONE UEM Admin Console**
 - In the **Directory Services** window > **User** Tab
 - Next to **corpPriv.local**
 - Enter **DC=corpPriv,DC=Local**



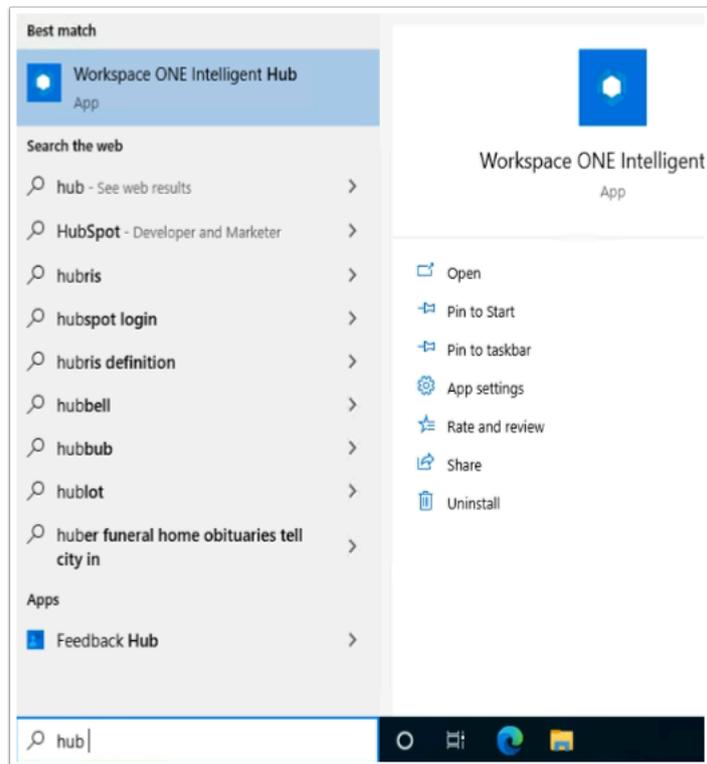
7. In the **Workspace ONE UEM Admin Console**

- In the **Directory Services** window > **Group** Tab
- Next to **corpPriv.local**
 - Enter **DC=corpPriv,DC=Local**
 - **Scroll down**
 - select **SAVE**

Part 10: Enrolling the EndPoint and testing the Integration

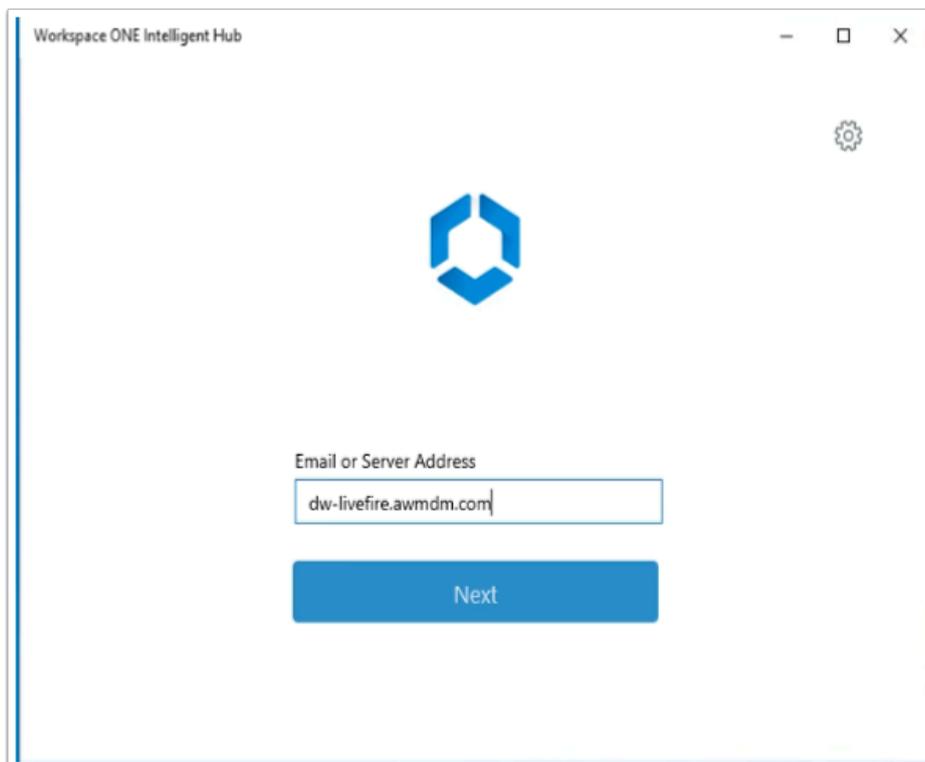


1. On your **ControlCenter** server
 - Open the **Remote Desktops** folder
 - Select and launch the **W10EXT01a.RDP** shortcut
 - Login with the **username: W10EXT01a\administrator**
 - Login with the **password: VMware1!**
 - Select **OK**

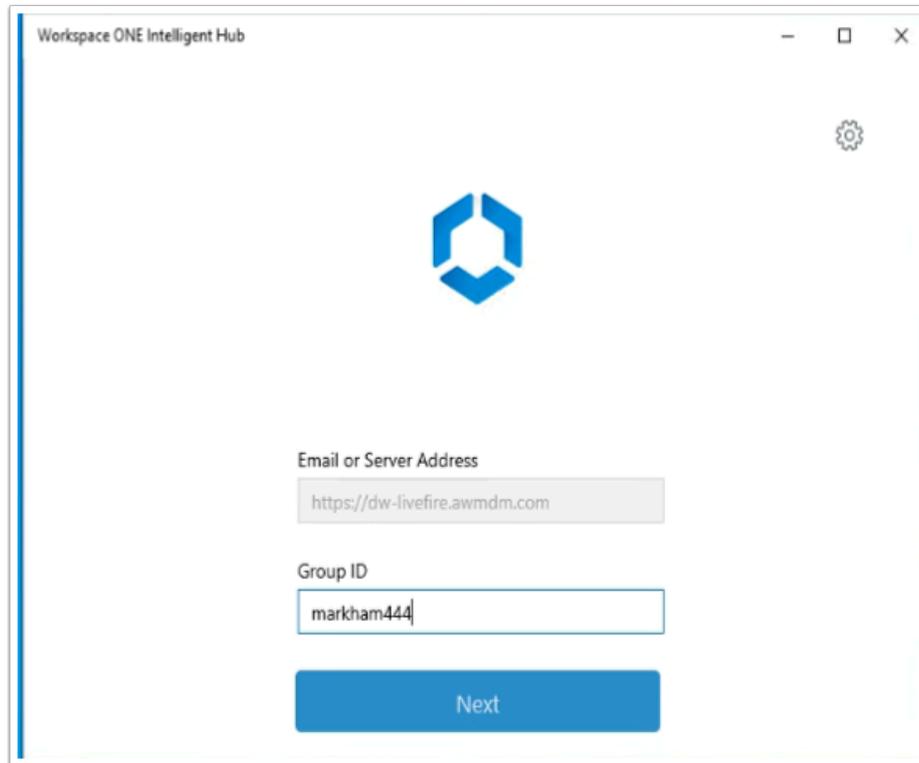


2. On the **W10EXT01a** Desktop

- In the **Type here to search** area , type **hub**
- When the **Workspace ONE Intelligent Hub** is found, select **Open**
 - If your **Workspace ONE Intelligent Hub** does not load properly, go services and start the **Airwatch** service

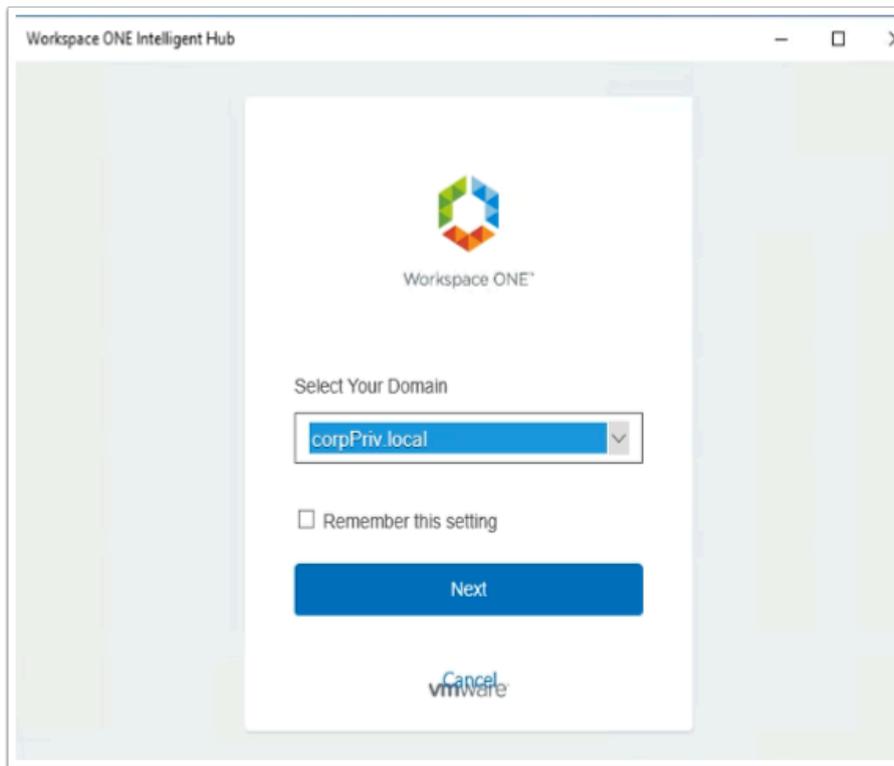


3. In the Workspace ONE Intelligent Hub console
 - Under **Email or Server Address**
 - type dw-livefire.awmdm.com
 - Select **Next**



The screenshot shows the Workspace ONE Intelligent Hub console interface. At the top, the title bar reads "Workspace ONE Intelligent Hub". Below the title bar is a blue hexagonal logo. Underneath the logo, there are two input fields. The first field is labeled "Email or Server Address" and contains the text "https://dw-livefire.awmdm.com". The second field is labeled "Group ID" and contains the text "markham444". Below these fields is a blue button labeled "Next".

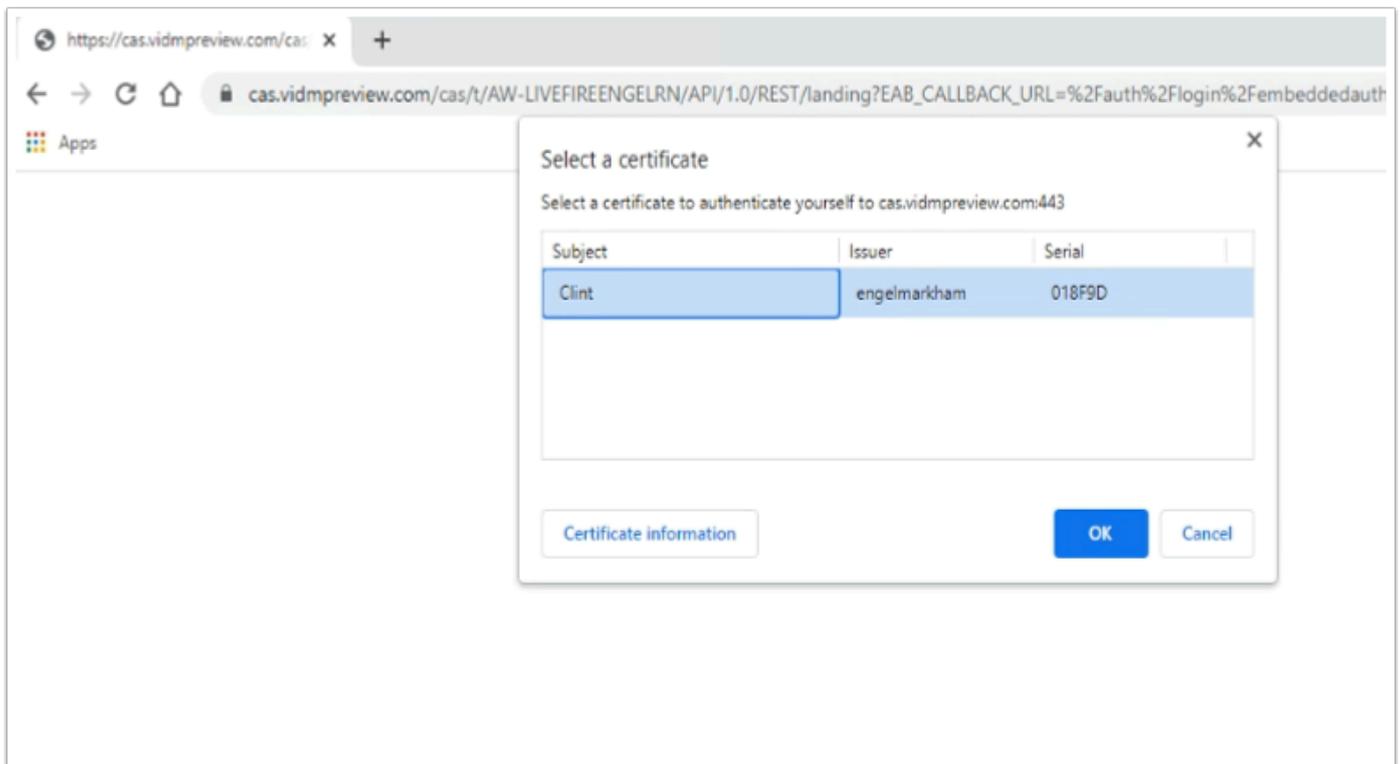
4. In the Workspace ONE Intelligent Hub console
 - Under **Group ID**
 - type **your UEM Tenant Group ID**
 - Select **Next**



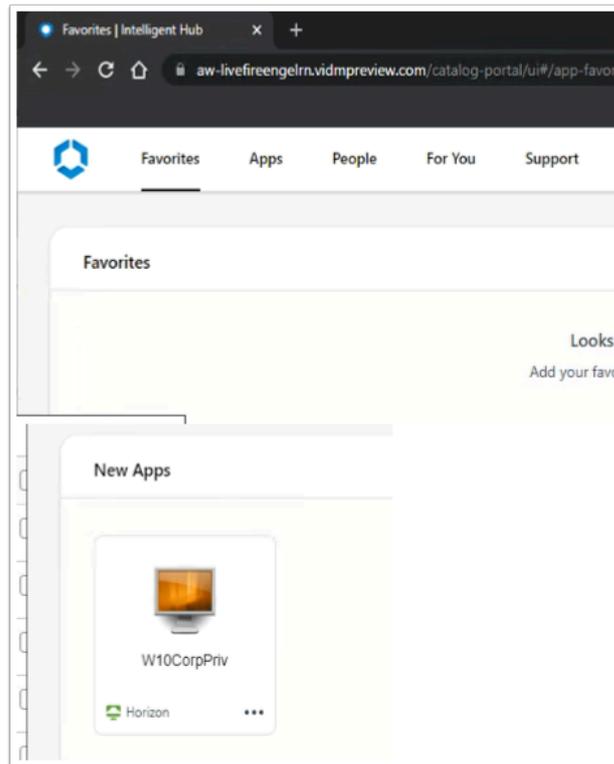
5. In the Workspace ONE Intelligent Hub console
 - Under **Select Your Domain**
 - From the dropdown select **corpPriv.local**
 - Select **Next**



6. In the Workspace ONE Intelligent Hub console
 - Under **username**
 - enter **Clint**
 - Under **password**
 - enter **VMware1!**
 - Select **Sign in**
 - Note you will get a **Enrolling your device this will take several minutes** window
 - When prompted, select **I Agree**
 - On the Congratulations window, select **Done**
 - On the Hello, Clint window, select **Get Started**



7. In the W10EXT01a desktop
 - Launch your **browser**
 - Enter **your custom Workspace ONE Access URL**
 - At the Domain Login, from the dropdown, select **CorpPriv.local**
 - Select **Next**
 - In the Select a certificate,
 - Select **OK**



6. In the Workspace ONE Access Intelligent Web Hub

- Select the **Apps tab**
- Enter **your custom Workspace ONE Access URL**
 - Launch your **W10CorpPriv** entitlement
- You should now have a complete Single Sign-on experience with Workspace ONE

About the Author: Reinhart Nel

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

Any questions related to this session, email Reinhart at RACE-Livefire-EUC <RACE-Livefire-EUC@vmware.com>