

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 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. The Horizon Enrollment services, integrates with Microsoft Certificate Services to provide a solution to this challenge and we refer to the solution as **Horizon TRUE SSO**

Since December 2019

Caching of Passwords for Horizon has been disabled and a user will always have to re-authenticate when they select their entitlement. <https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/rn/VMware-Workspace-ONE-Access-Cloud-Release-Notes.html>

We have already demonstrated how to facilitate a single-sign on with password based authentication. When authenticating to Workspace ONE Access using a 3rd Party authentication method and wanting to launch a Horizon based resource, one will still be prompted for password based Authentication.

In a Zero-Trust environment, it is critical we secure our Horizon Sessions with authentication methods that are not Password based.

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.

In June 2020, Caching of Passwords was re-introduced as an option to re-enable, to allow Password Single Sign-On based Authentication. Caching of Passwords is disabled by default.

When using Horizon with Workspace ONE Access and a 3rd Party Authentication method, the only way we can get a good user experience with Single Sign-On is to deploy Enrollment Services also known as TRUESSO.

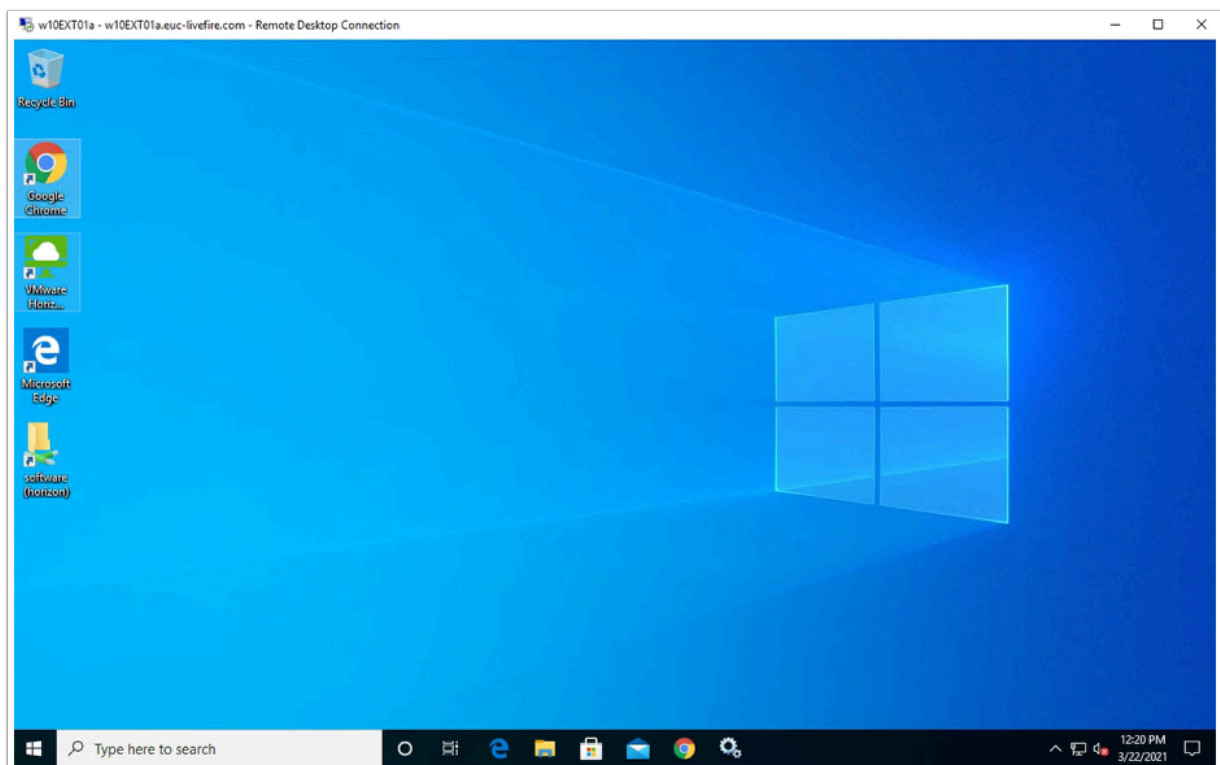
We will start off by doing the following:

1. Log into a Windows 10 Desktop and demonstrate the limitation
2. Deploy and configure TRUE SSO
 - Deploy and configure Horizon Enrollment services
 - Integrate and configure Active Directory Certificate services with Horizon Enrollment services
3. Log into a Windows 10 Desktop and demonstrate the solution

Please Note. This lab is not for the faint-hearted. You will see the implementation process of deploying and configuring Enrolment services in Horizon and integration with Microsoft Active Directory services.

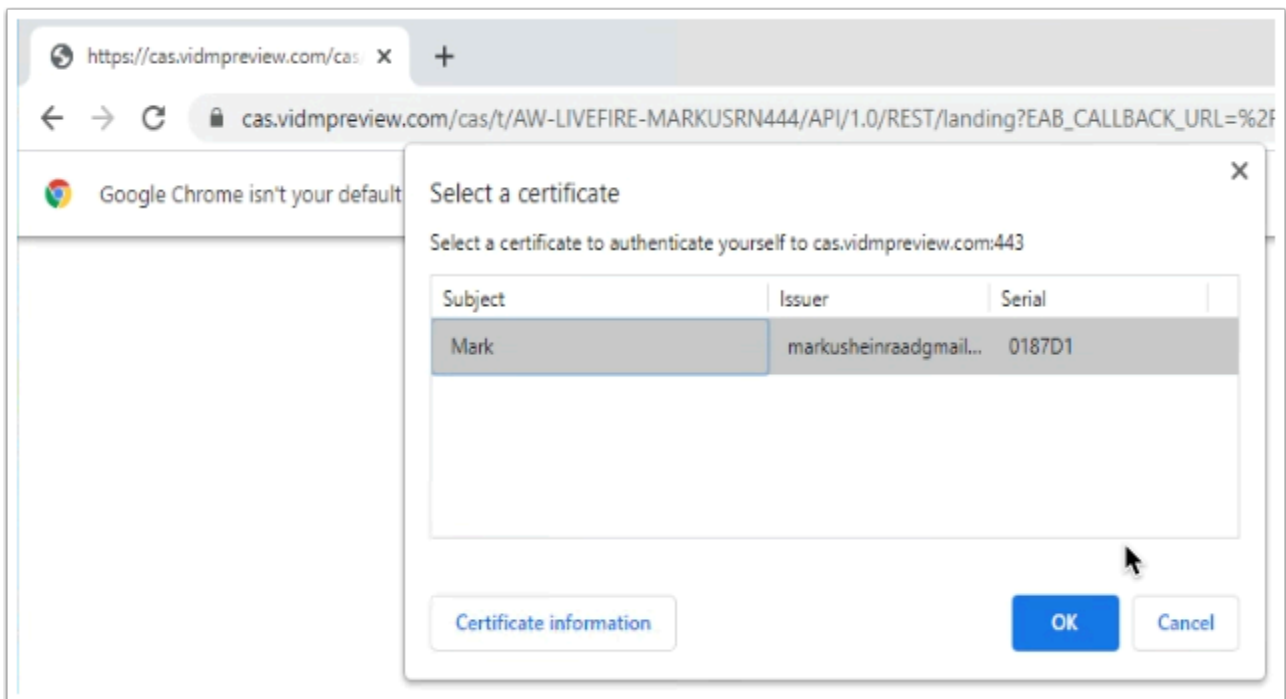
You will also experience first hand how reliant Enrollment services on Microsoft Active Directory Certificate services is.

Part 1: Log into a Windows 10 Desktop and demonstrate the limitation

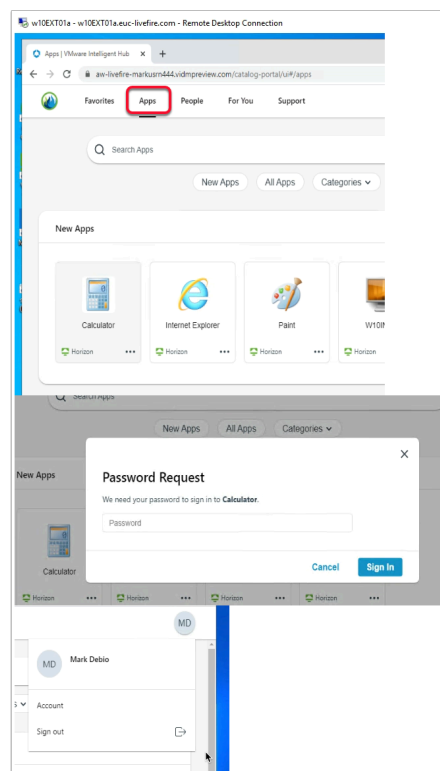


1. On the **ControlCenter** server Desktop,
 - **Switch back** to your the **W10EXT01a.RDP** session
 - **W10EXT01a.RDP** is enrolled into Workspace ONE UEM and has a certificate already deployed

- If necessary login as:
 - Username: **administrator@euc-livefire.com**
 - Password: **VMware1!**



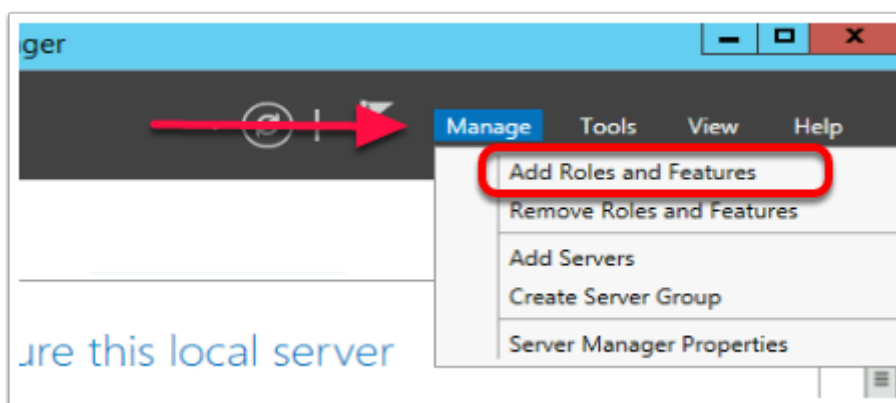
2. Open a **browser** on your windows 10 desktop
 - Enter **your custom Workspace ONE Access URL**
 - On the **Select a certificate** window note the account of the certificate and select **OK**



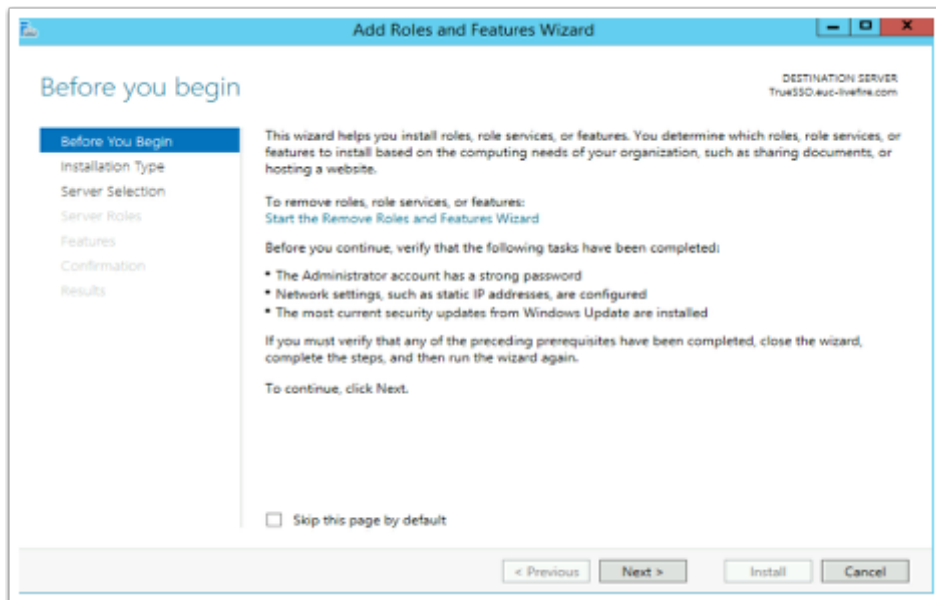
3. On the **Workspace ONE Intelligent Hub** console ,
 - Under **Apps**,
 - Select **Calculator**
- Notice we are getting a Password request.
 - We used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password Auth method, to pass on to the Horizon Agent.
- Select **Cancel** to close the **Password Request** window
- In the top right-hand corner,
 - Select and right-click the **User Icon** ,
 - select **Sign out**
- **Close** your Browser
- **Minimize** your **W10EXT01a.RDP** session

We will now go and configure Horizon Enrollment Services, to be able to facilitate a Single Sign-On experience for 3rd Party Authentication methods

Part 2. Installing a sub-ordinate CA and the Enrollment services

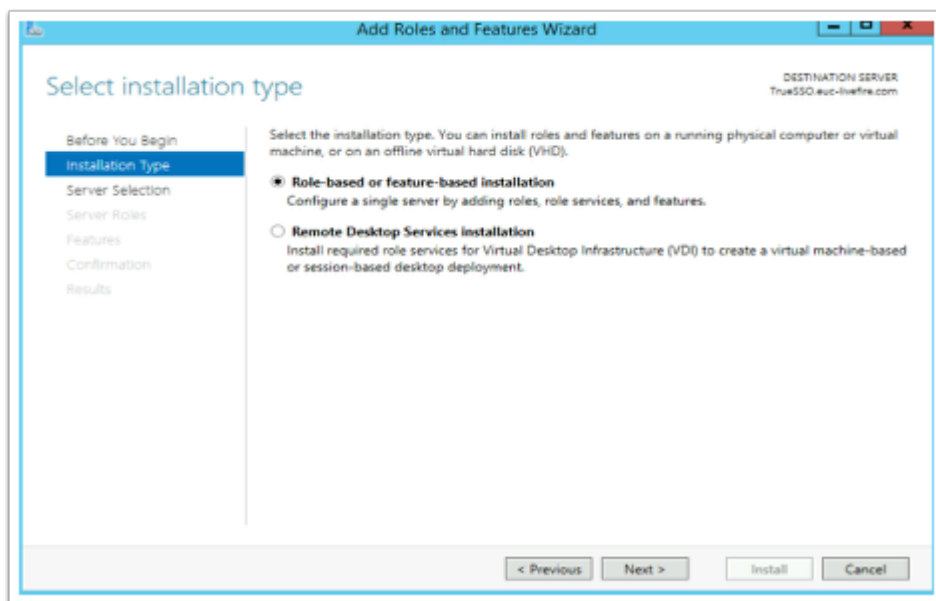


1. On your **ControlCenter** server
 - Open the **Remote Desktop** Folder
 - Launch the **TrueSSO.RDP** shortcut,
 - login as **administrator@euc-livewire.com**.
 - Use the password **VMware1!**
 - **Server Manager** should launch automatically on the **TRUESSO** Server, desktop interface
 - On the **Server Manager** Interface
 - Select **Manage > Add Roles and Features**



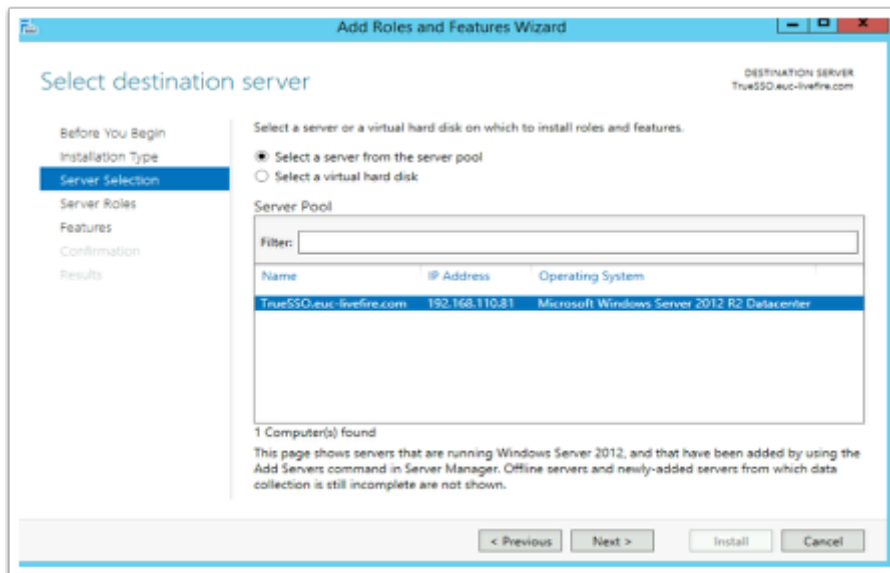
2. On the **Before you begin** window

- Select **Next**



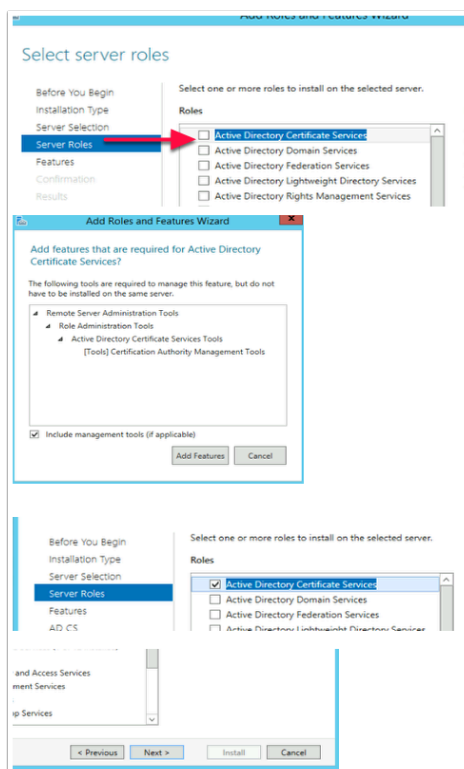
3. On the **Select installation type** window,

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



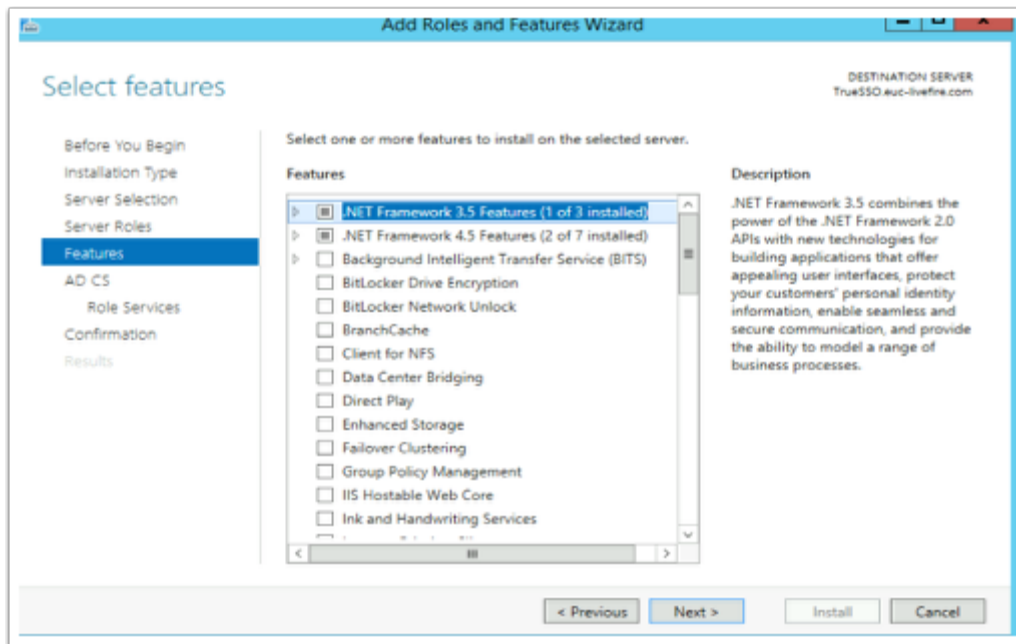
4. On **Select destination server** window (accept the defaults)

- Select **Next**



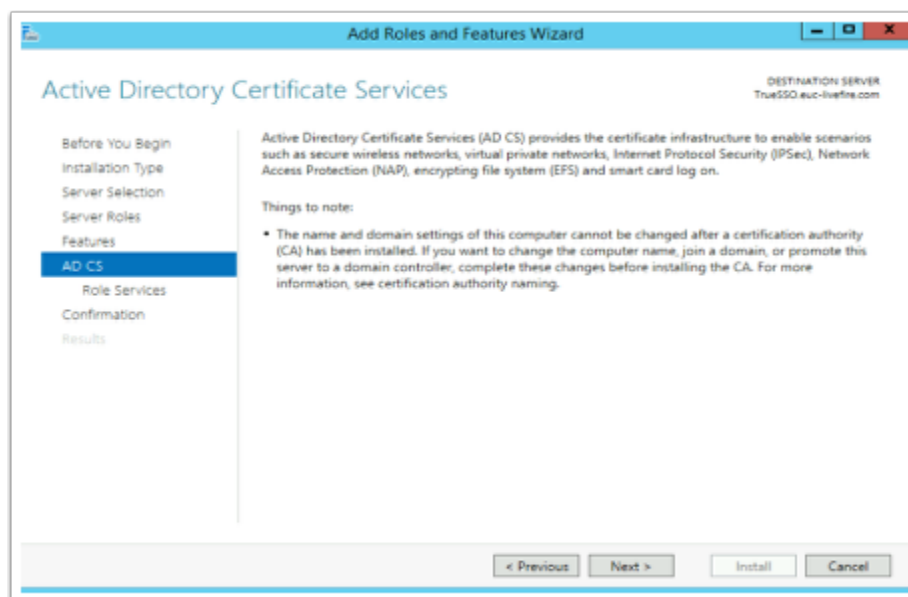
5. On the **Select server roles** window,

- 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**



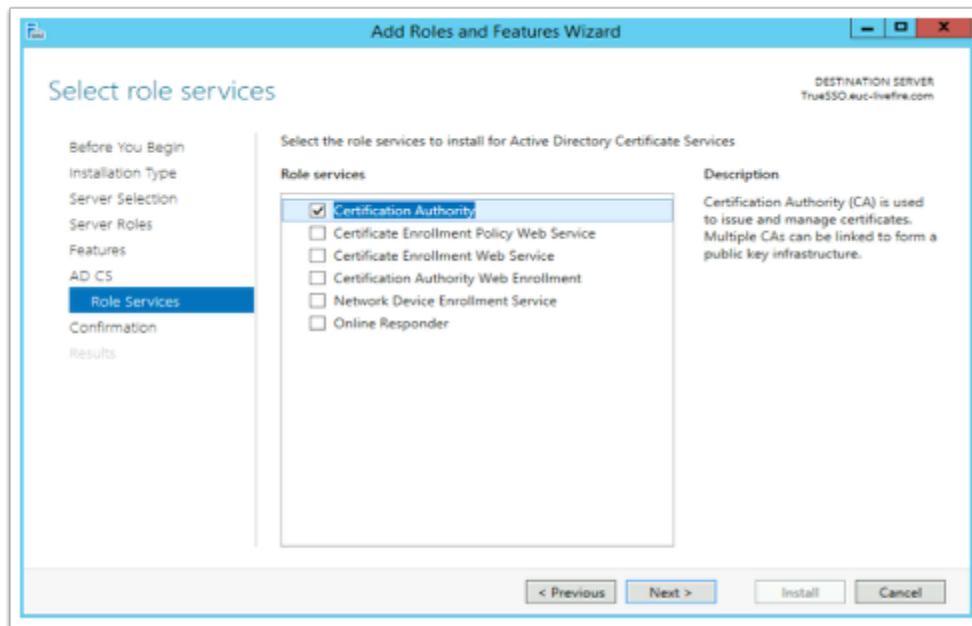
6. On the **Select features** window

- Select **Next**



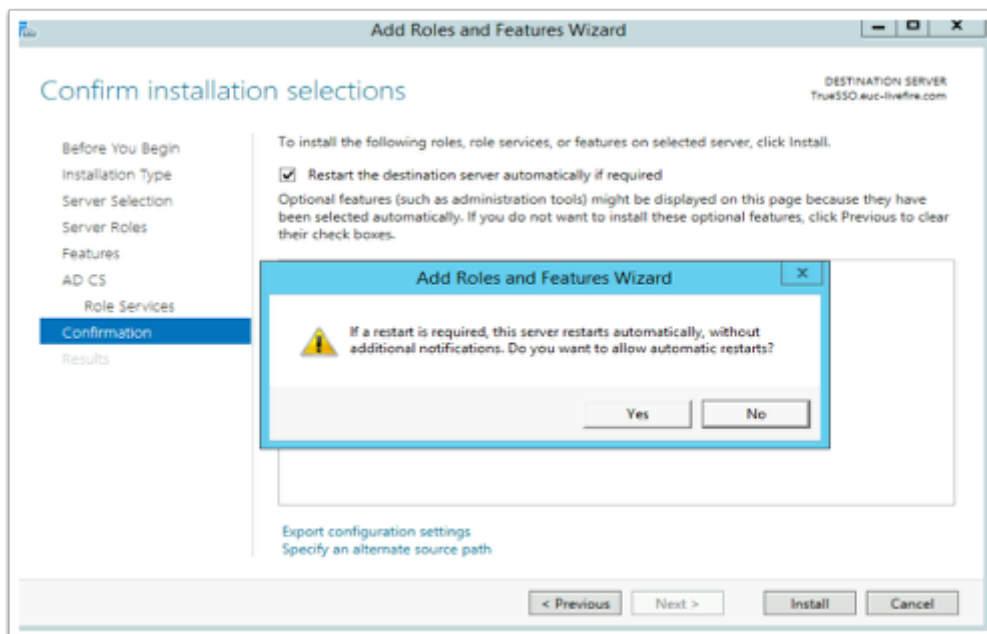
7. On the **Active Directory Certificate Services** window

- Select **Next**



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

- Select **Next**

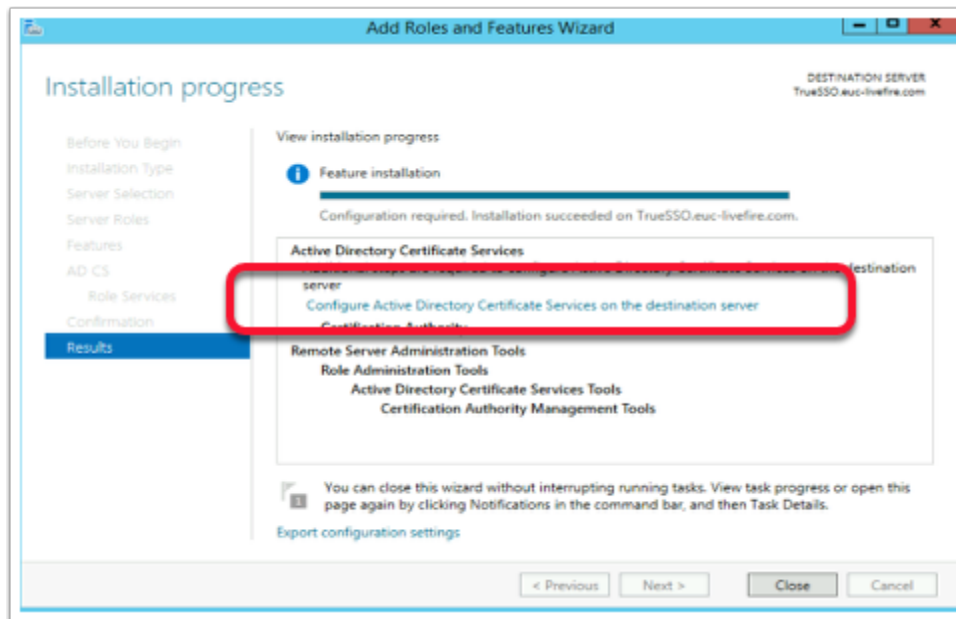


9. On the **Confirm Installation selections** window,

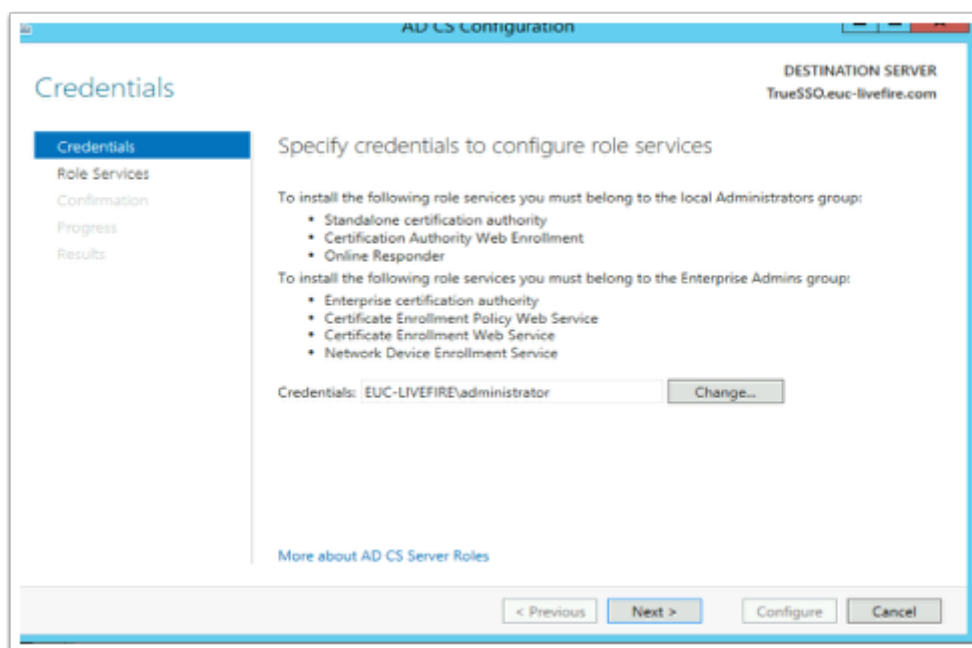
- Select the **checkbox** next to **Restart the destination server automatically if required**,
- On the **Add Roles and Features Wizard** window
 - Select **Yes**

- Select **Install**

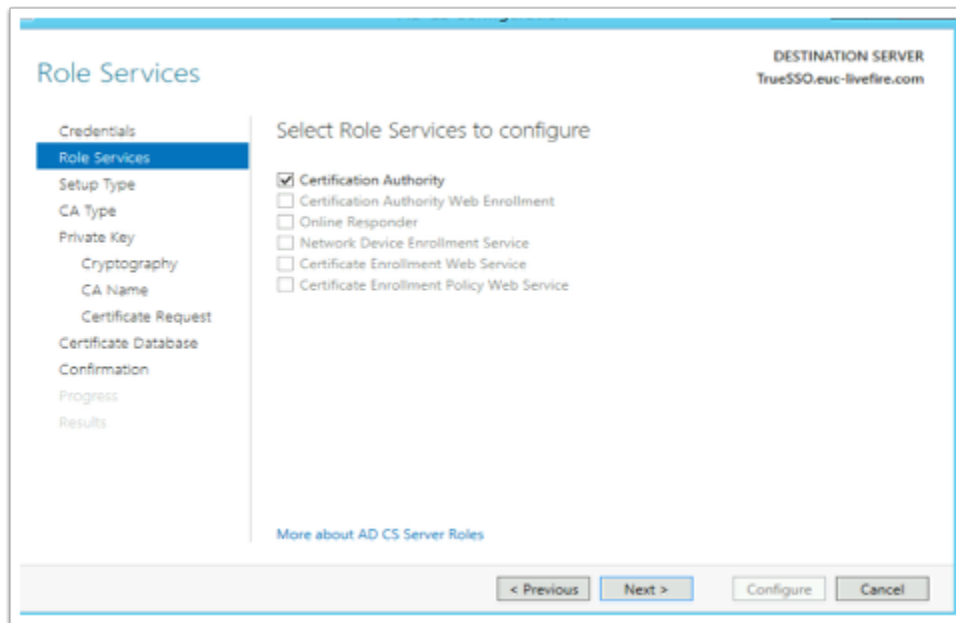
- You will have to wait a short while before moving on to **step 10**



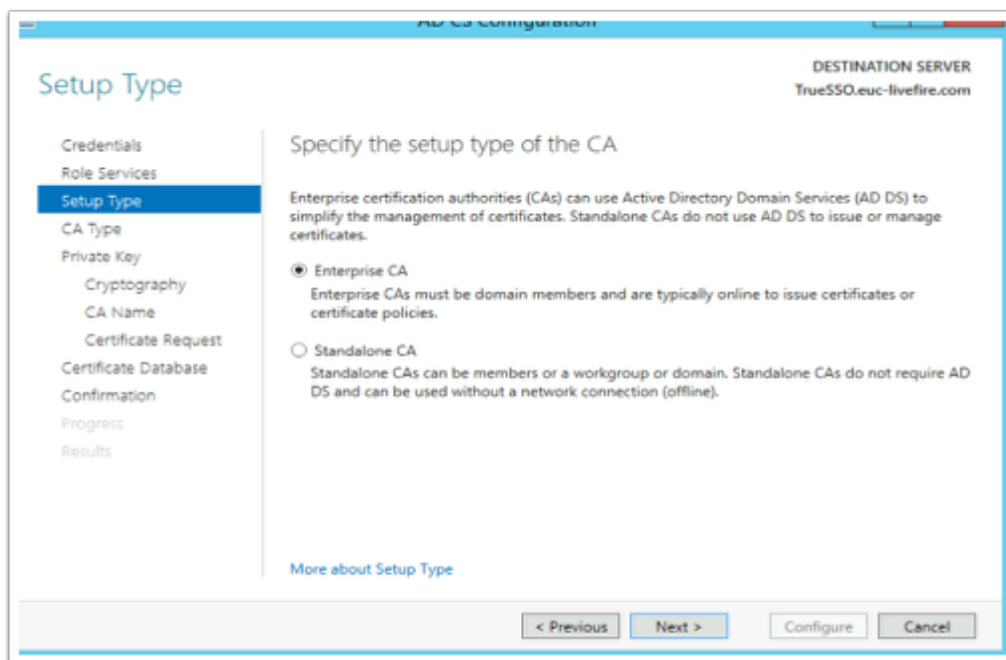
10. On the **Installation progress** page,
 - Select the **Configure Active Directory Certificate Services on the destination server** hyper-link



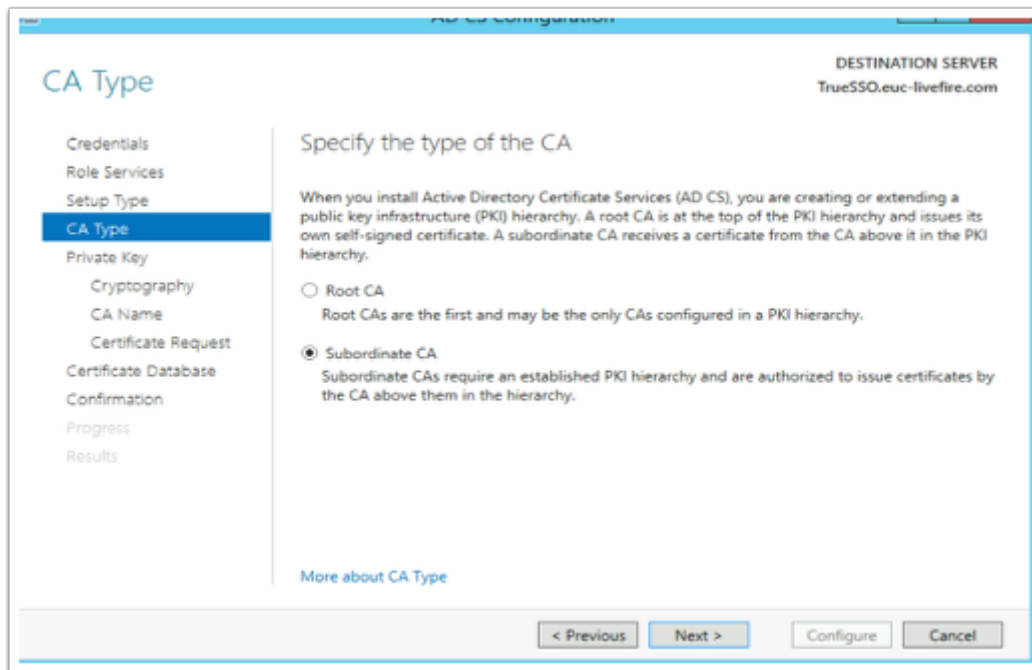
11. On the **Credentials** window
 - Select **Next**



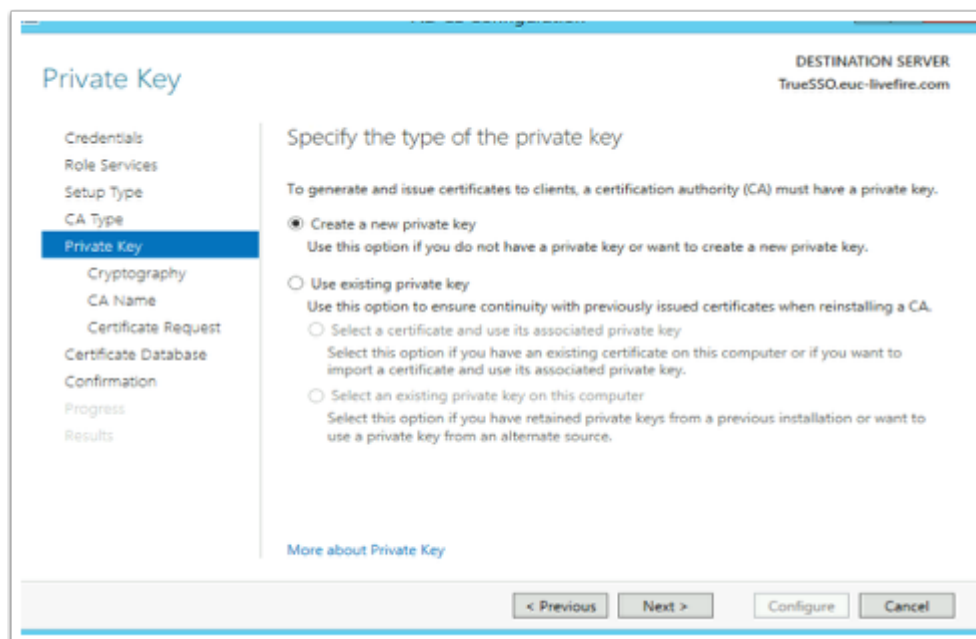
12. On the **Role Services** page,
 - Select the **Certificate Authority** checkbox



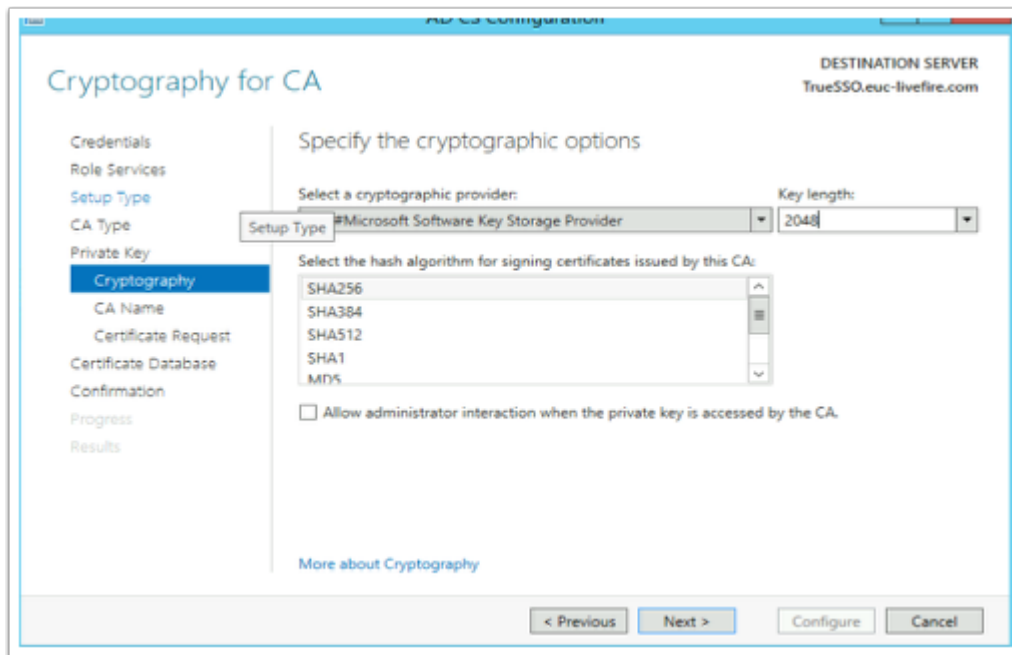
13. On the **Specify the setup type of the CA** window ,
 - Select the radio button next to **Enterprise CA**
 - Select **Next**



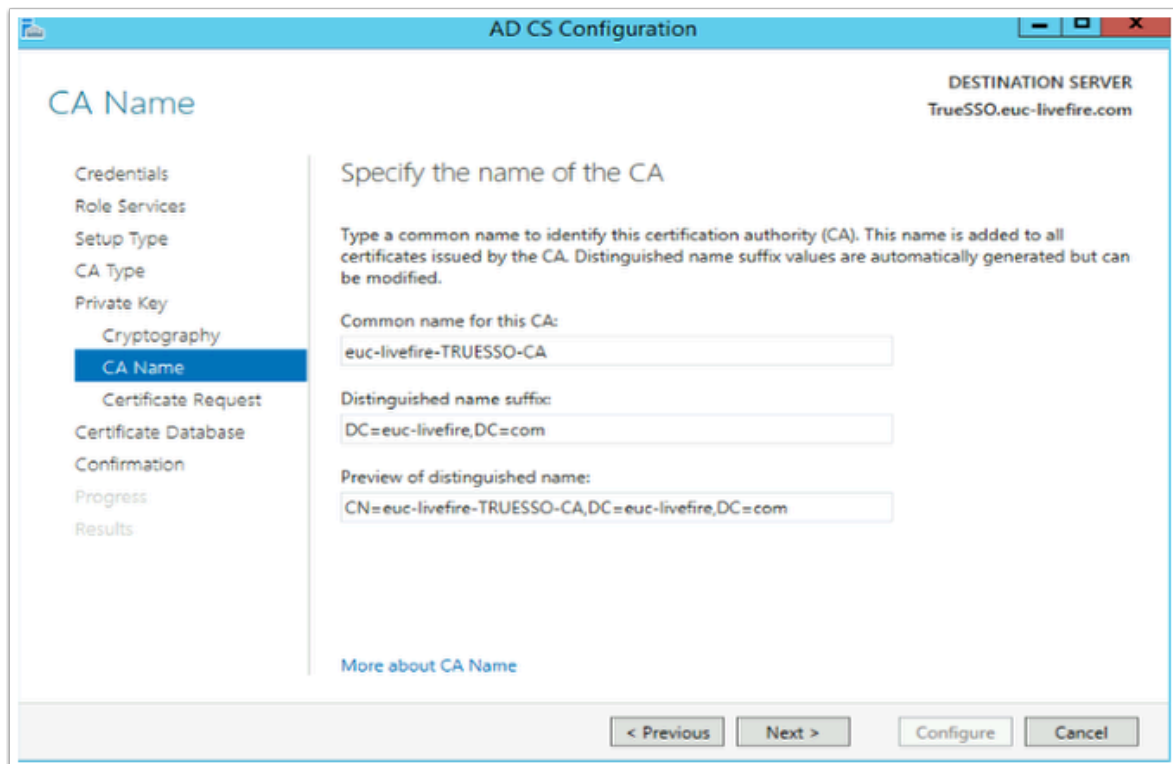
14. On the **CA type** window
 - Ensure the **Subordinate CA radio button** is selected,
 - Select **Next**



15. On the **Private Key** window,
 - Ensure the **radio button** next to **Create a new private key** is selected
 - Select **Next**

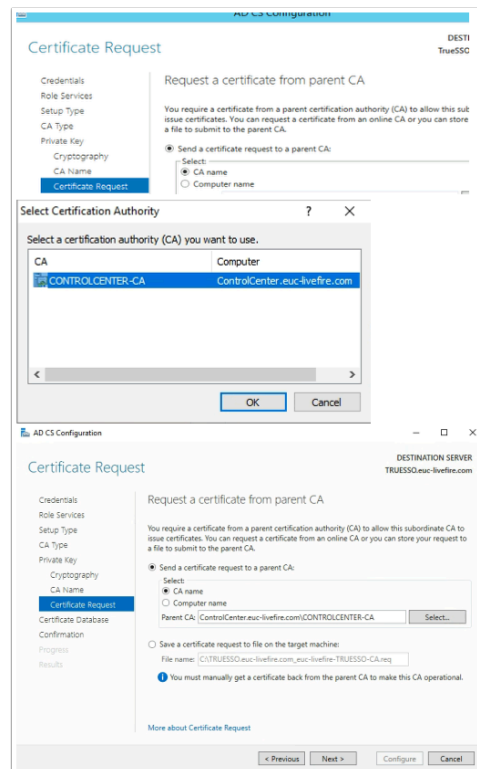


16. On the **Cryptography for CA** window, validate the following is selected
- Under **Cryptographic Provider:** **RSA#Microsoft Software Key Storage Provider**
 - Next to **Key Length:** **2048**
 - **Hash Algorithm:** **SHA256**
 - Select **Next**

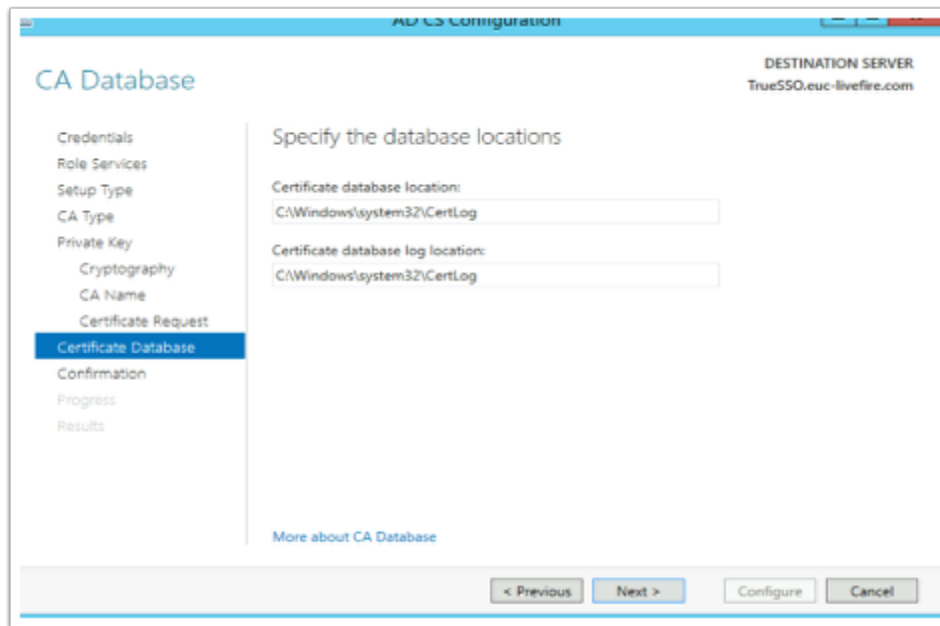


17. On the **CA Name** window
- Observe the CA naming convention

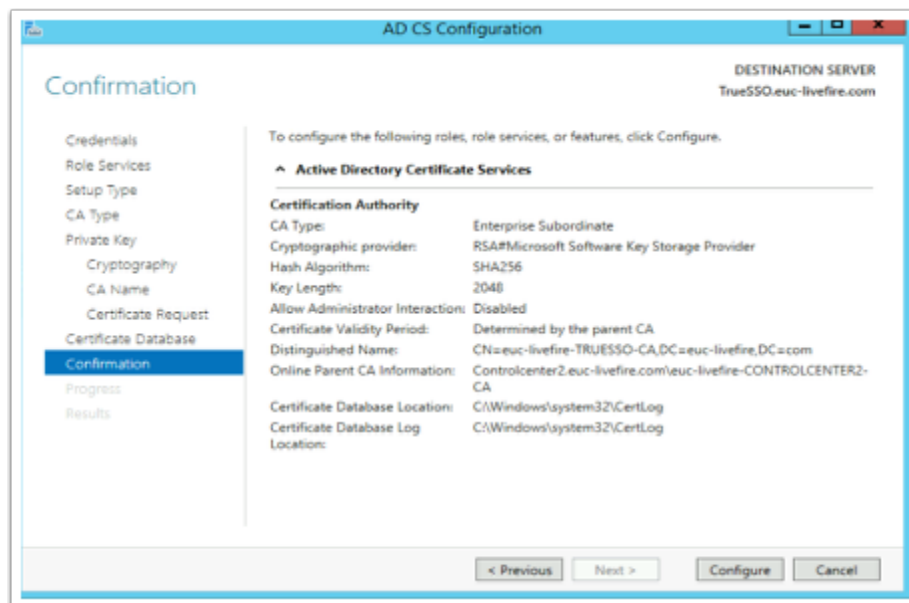
- Select **Next**



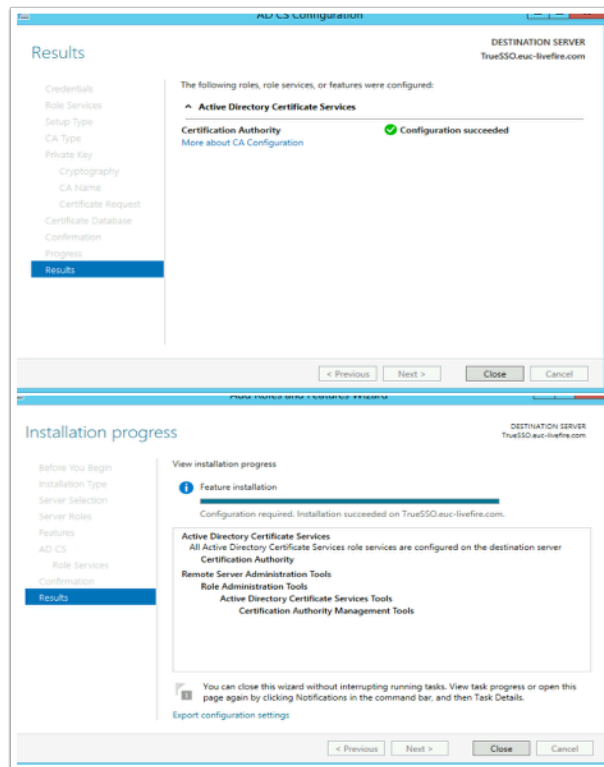
- On the **Request a certificate from parent CA** ,
 - Select the **radio button** next to **Send a certificate request to a parent CA:**
 - In the **Select** box, select the **radio button**, next to **CA name**
 - To the right of the **Parent CA** box click the **Select** button
 - In **Search box**, enter **ControlCenter** and select **Check Names**
 - Select **OK** accept the Defaults
 - Select **Next**



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



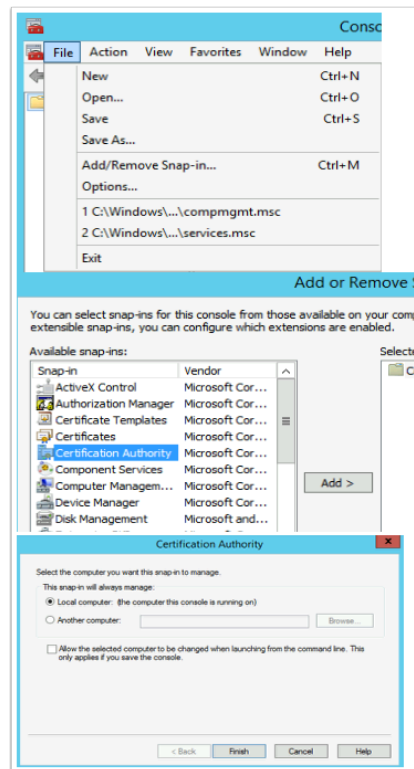
20. On the **Confirmation** window
 - Select **Configure**



21. On the **Results** window

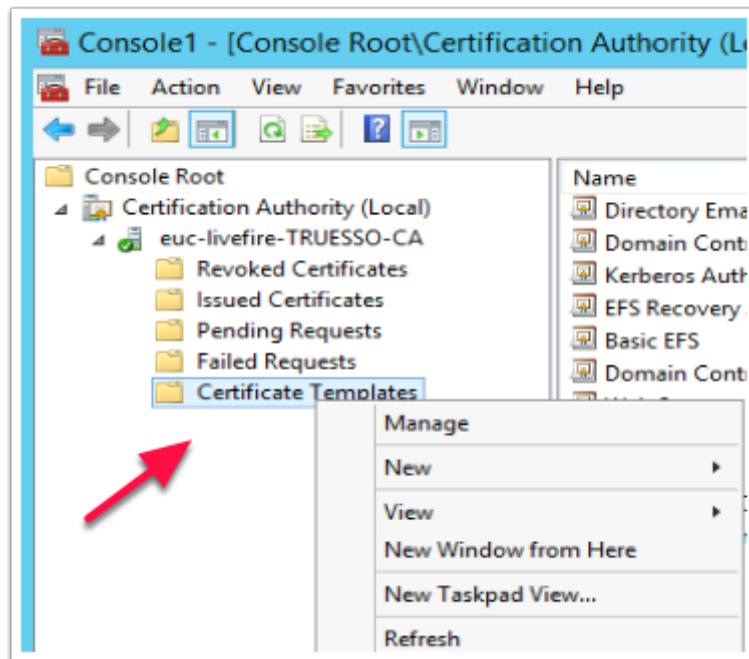
- Select **Close** on the **Installation progress** window,
- Select **Close**, again

Part 3: Deploying and Configuring Horizon TRUE SSO



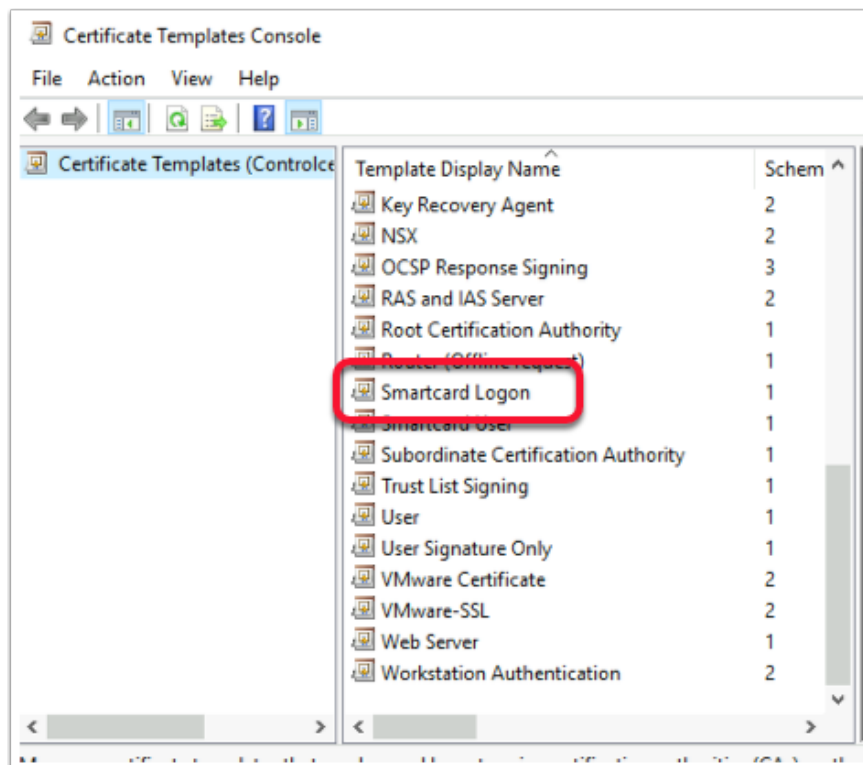
1. In this section we will create a certificate template for Horizon TRUESSO

- On your **TRUESSO** server
- Select **Start** > **Run** > type **mmc**
- Select **File** > **Add/Remove Snap-in...**
- Select the **Certificate Authority** services snap-in, select **Add**
- Ensure the **Local computer** radio button is selected.
- Select **Finish**
- Select **OK** to close the **Snap-ins** window



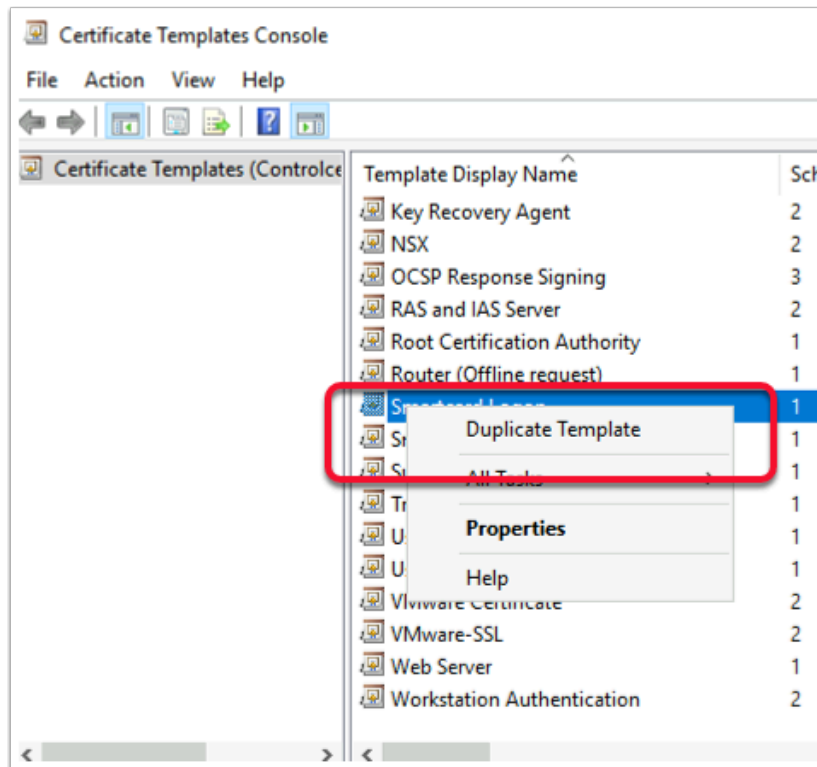
2. Expand the **euc-livewire-TRUESSO-CA** inventory

- Select **Certificate Templates**,
- Right-click and select **Manage**

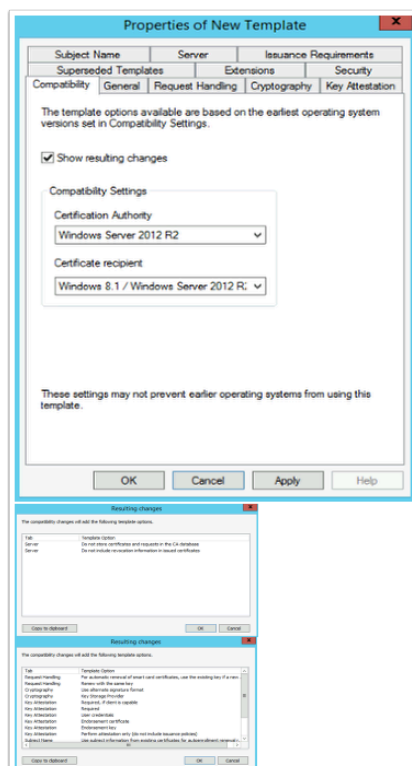


3. In the **Certificate Template** Console

- Select the **Smartcard Logon** template

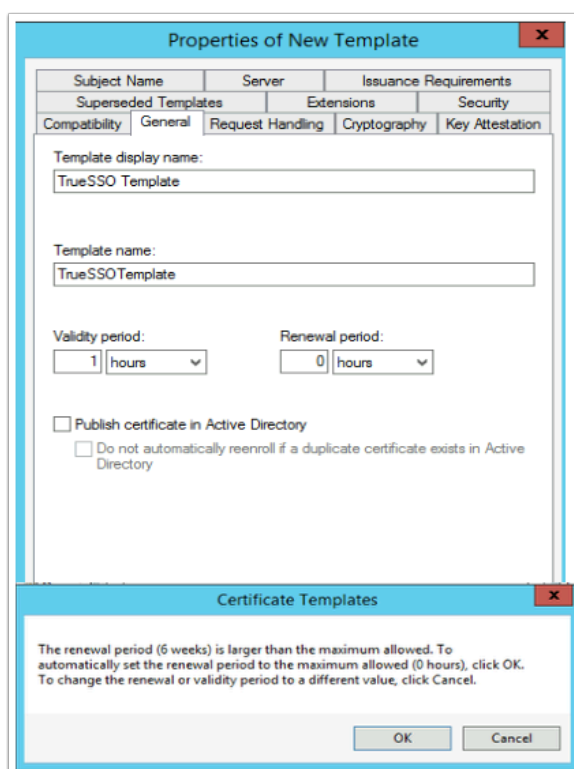


4. Right-click the **Smartcard Logon** template
 - Select **Duplicate Template**

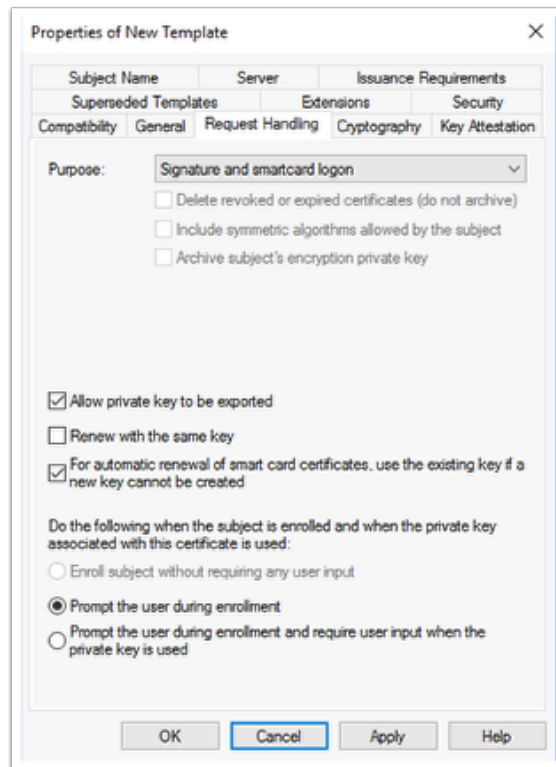


5. In the **Properties of New Template** window in the **Compatibility** tab under **Certificate Authority**
 - Change from **Windows 2003** to **Windows 2012 R2**

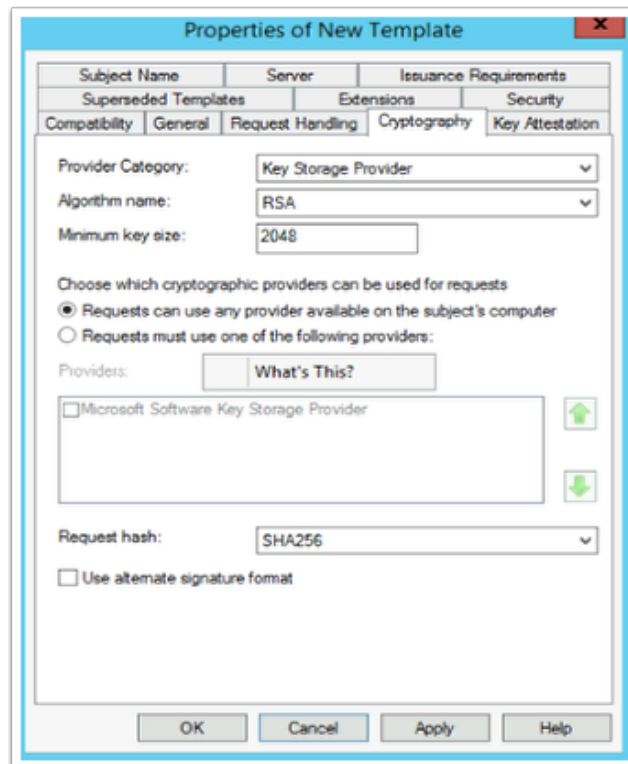
- When prompted for the **Resulting changes** window select **OK**.
- Under **Certificate recipient** change **Windows XP / Server 2003** to **Windows 8.1 / Server 2012 R2**
 - When prompted for the **Resulting changes** window select **OK**.



6. Select the **General** tab,
 - Under **Template display name:** type **TrueSSO Template**,
 - You will notice **Template name** gets filled in automatically
 - **Do NOT edit the Template name**. Leave as is in the screenshot
 - 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**

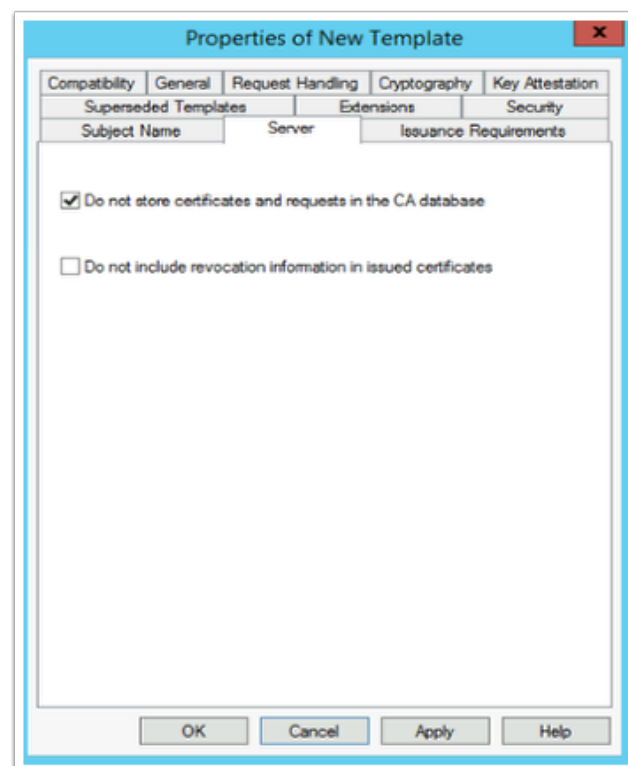


7. Select the **Request Handling** tab change the following next to :-
- **Purpose:** change: **Signature and encryption** to **Signature and smartcard logon**.
 - Select the **checkbox** in front of **Allow private key to be exported**
 - Select the **checkbox** in front of **For automatic renewal of 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

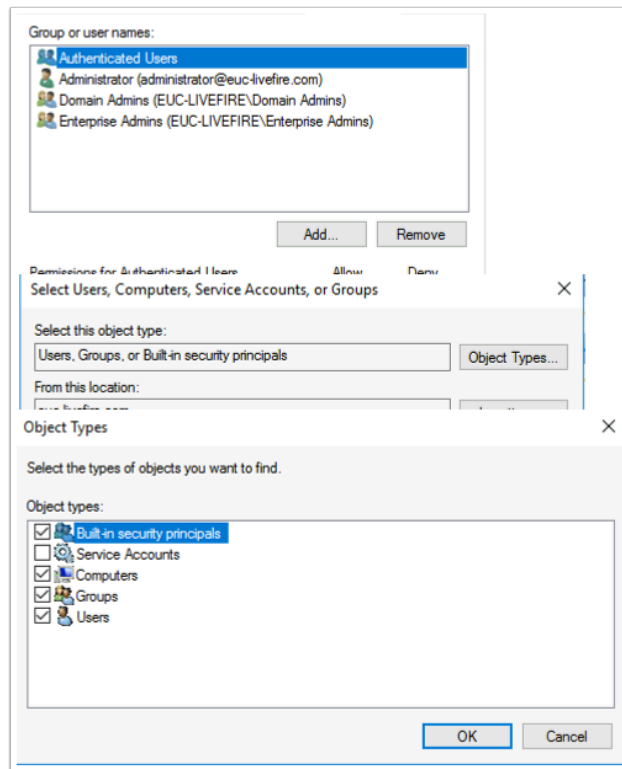


9. Select the **Server** tab,

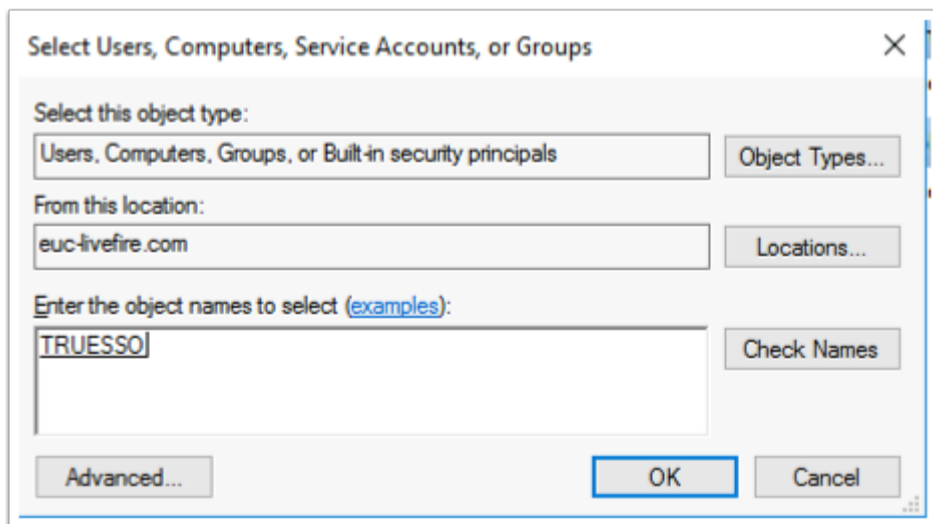
- Select the **checkbox** in front of **Do not store certificates and requests in the CA database**
 - You will notice that **Do not include revocation information in issued certificates** is selected automatically.
- Uncheck the **check box** next to **Do not include revocation information in issued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

The screenshot shows the 'TrueSSO Template Properties' dialog box with the 'Issuance Requirements' tab selected. The 'Subject Name' tab is also visible. The 'Require the following for enrollment' section has the 'CA certificate manager approval' checkbox unchecked and the 'This number of authorized signatures' checkbox checked with a value of 1. The 'Policy type required in signature' dropdown is set to 'Application policy', and the 'Application policy' dropdown is set to 'Certificate Request Agent'. The 'Issuance policies' section is empty. The 'Require the following for reenrollment' section has the 'Valid existing certificate' radio button selected. A note at the bottom states '* Control is disabled due to compatibility settings.' The 'Cancel' button is highlighted with a blue border.

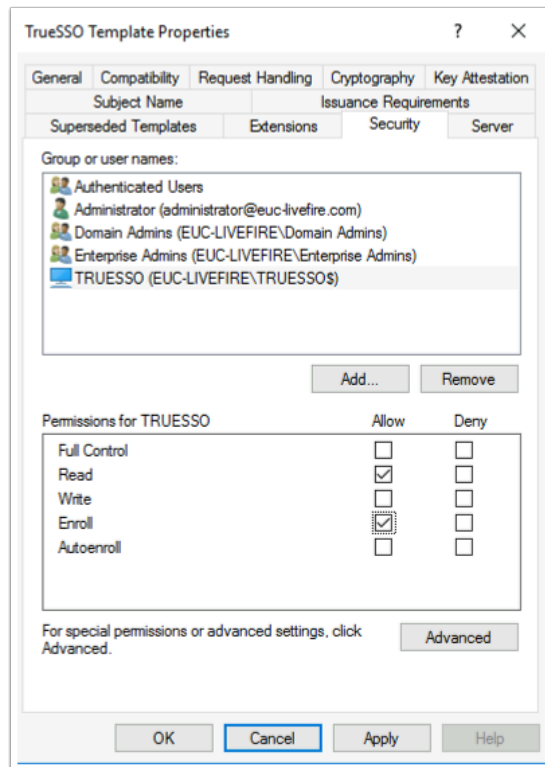
10. Select the **Issuance Requirements** tab, configure the following:
 - Select the **checkbox** : **This number of authorized signatures** and change the value to **1** in the **box**
 - Under **Policy type required in signature**
 - Ensure the **Application policy** is selected (default config)
 - 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**

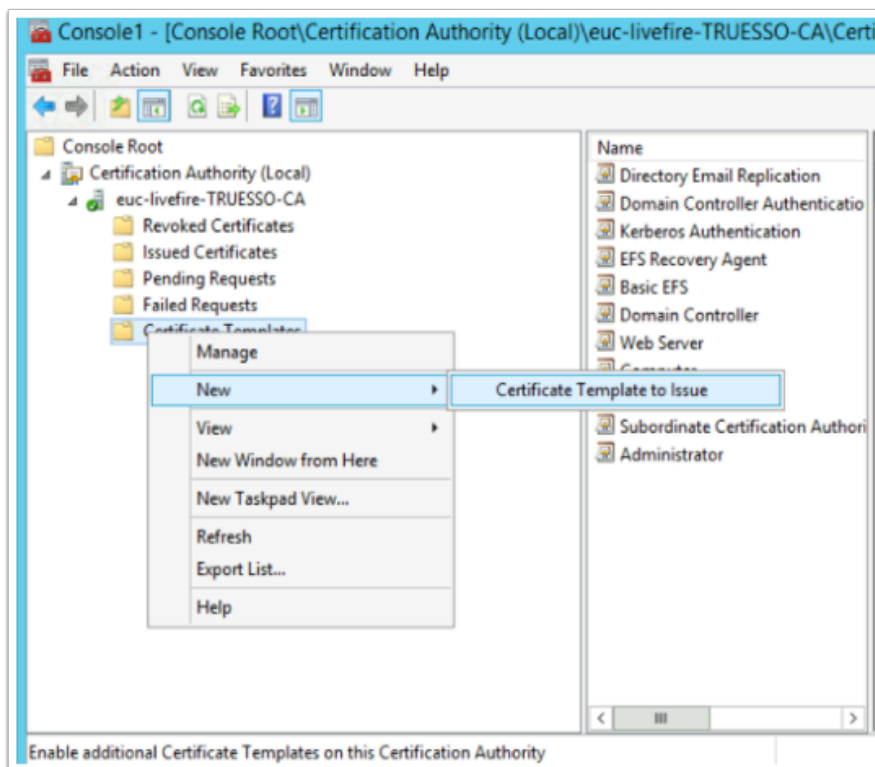


12. In the **Enter the object names area**
 - Type **Truessso**
 - To the right select **Check Names**
 - Select **OK**



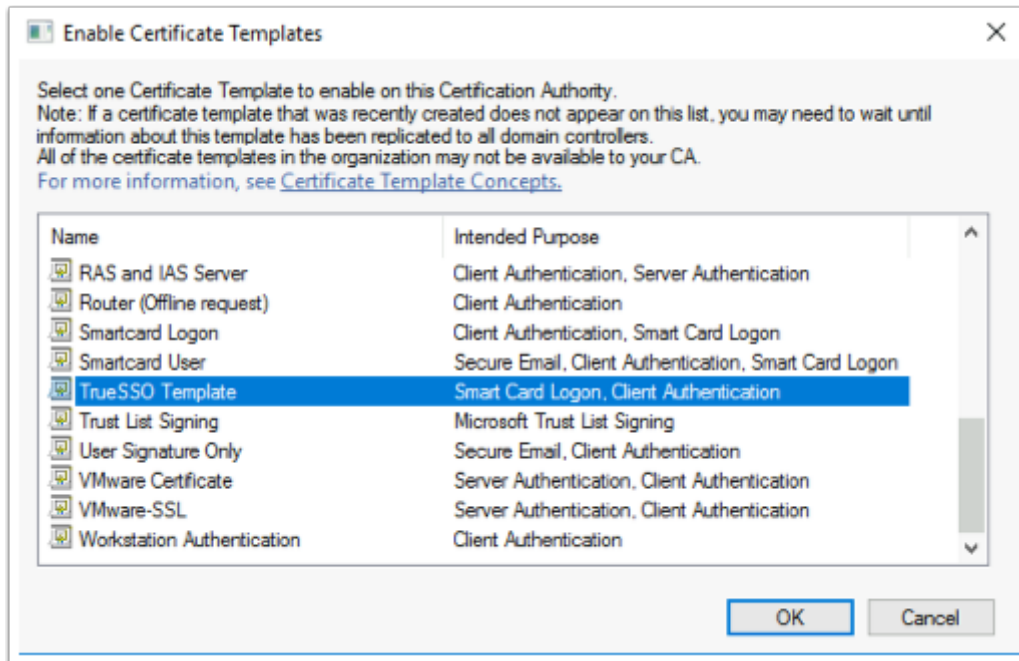
13. For the **Permissions for TRUESSO**

- Select the **Security** tab
- Select the **Read** and **Enroll** checkboxes
- Select **OK** to close the **TrueSSO Template Properties**,

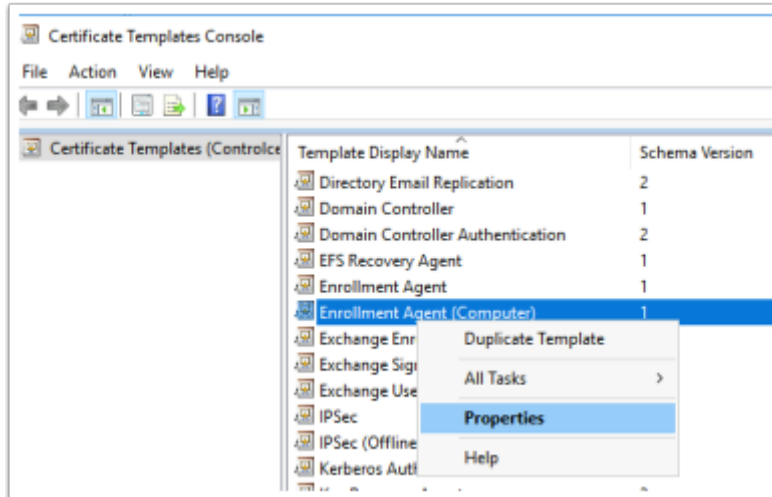


14. Switch to the **Certificate Authority Console**

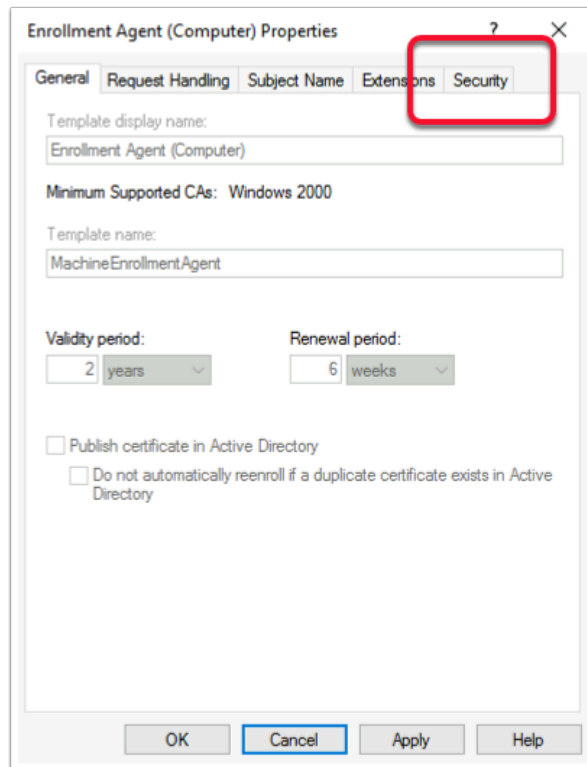
- Select and right-click the **Certificate Templates** container,
- Select **New > Certificate Template to Issue**



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

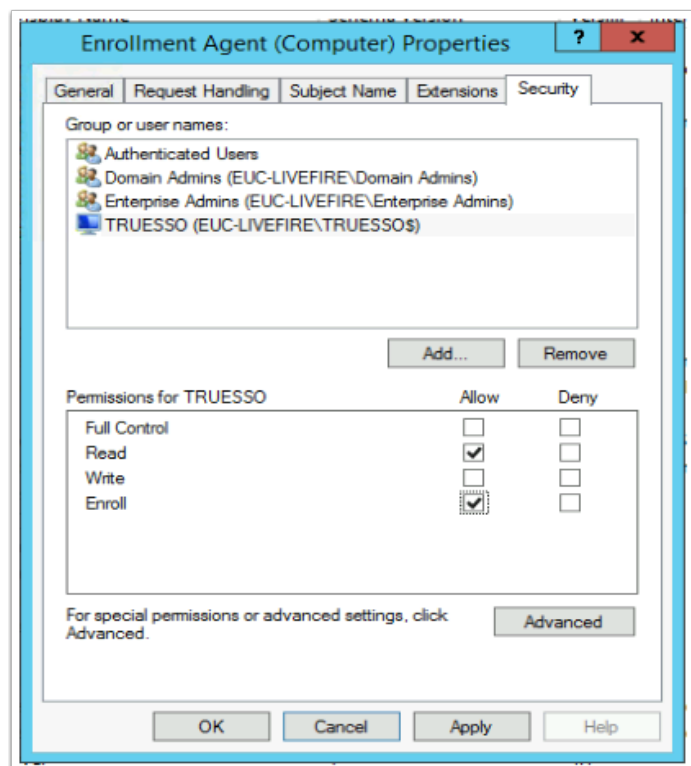


16. Switch back to the **Certificate Templates** Console
 - Select and right-click the **Enrollment Agent (computer)** template
 - Select **Properties**



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

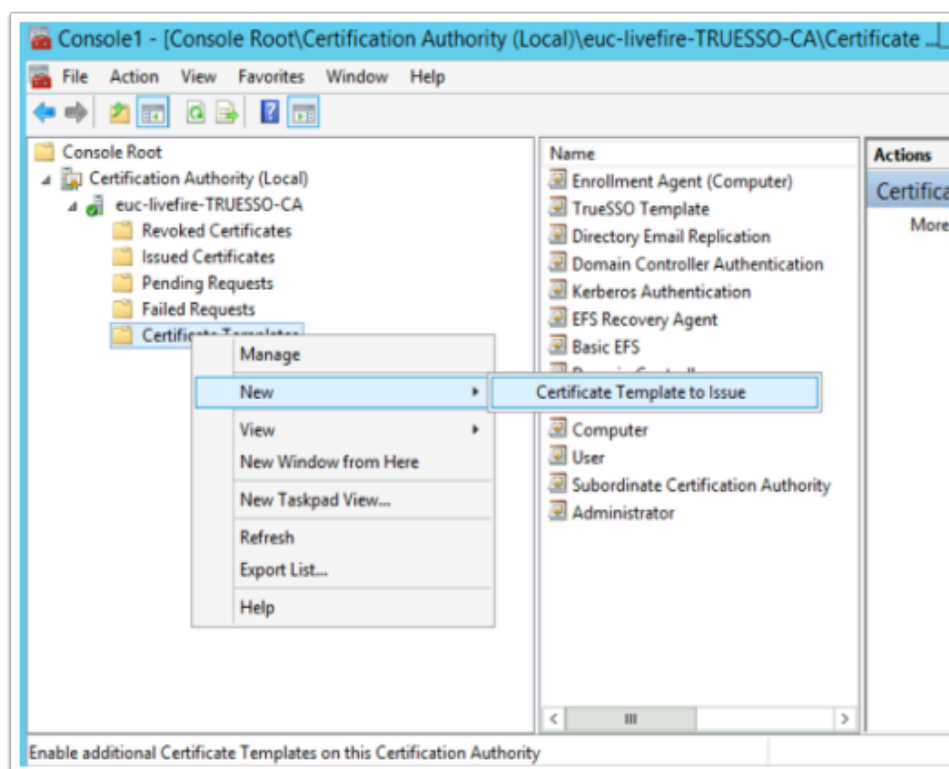
- Select the **Security** tab



18. In the **Enrollment Agent Properties** window (Security Tab)

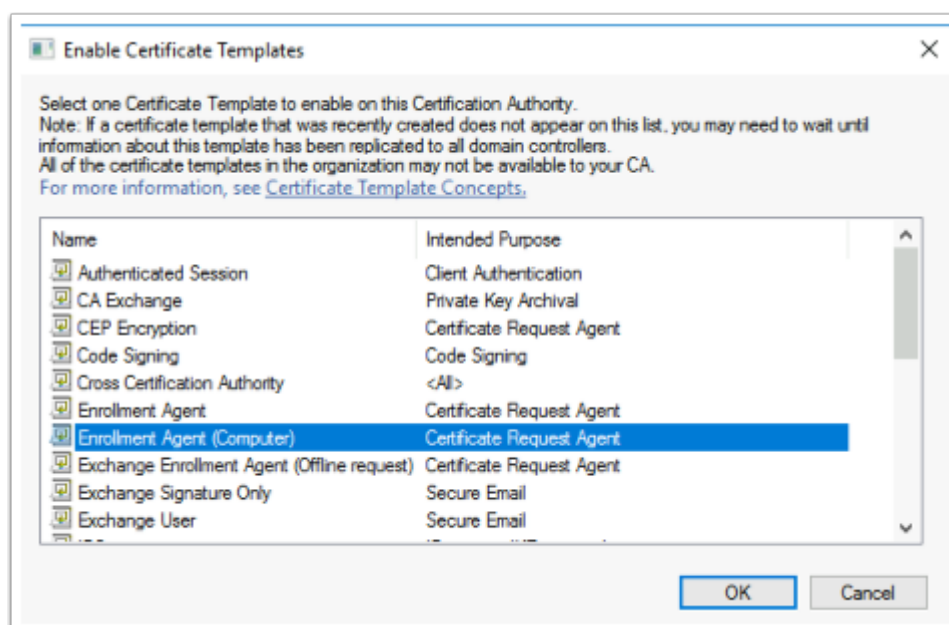
- Select **Add** and add the **TRUESSO** Computer account
- Ensure **Read** and **Enroll** permissions are selected

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



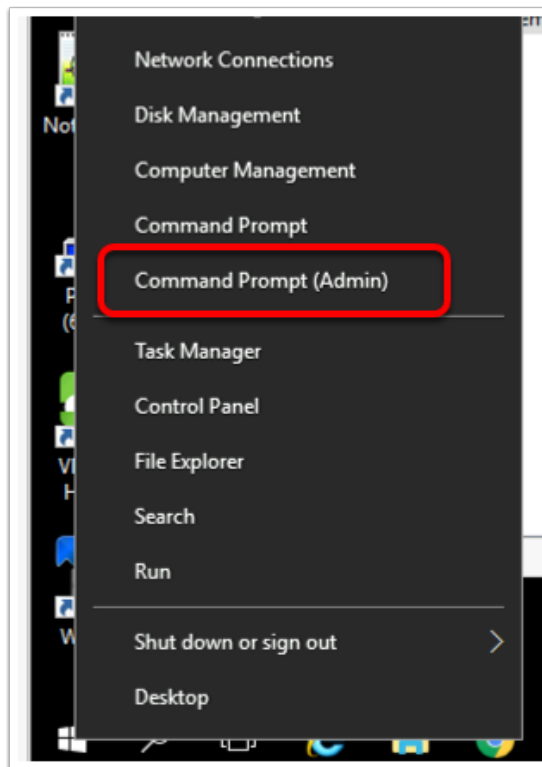
19. Switch back to the **Certificate Authority Console**

- 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
- Select **OK**



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

- On your existing **TrueSSO** 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_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`

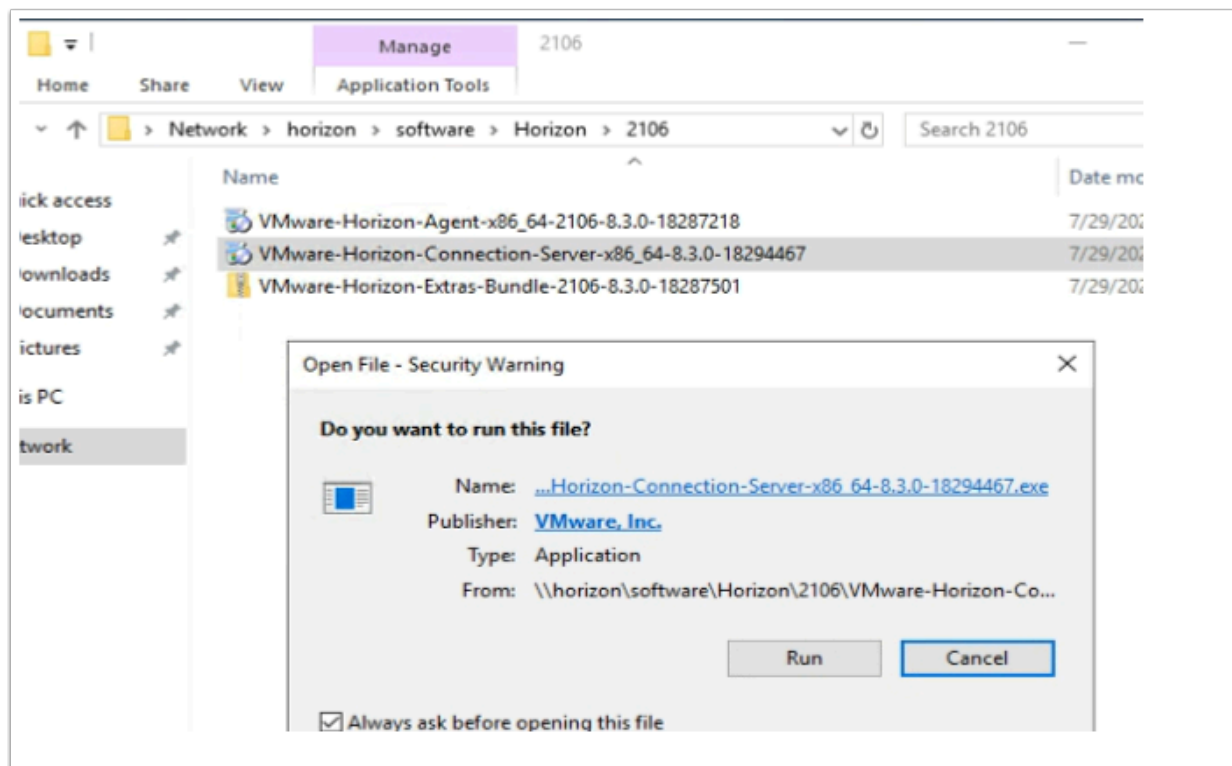
```
C:\Windows\system32>net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.

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

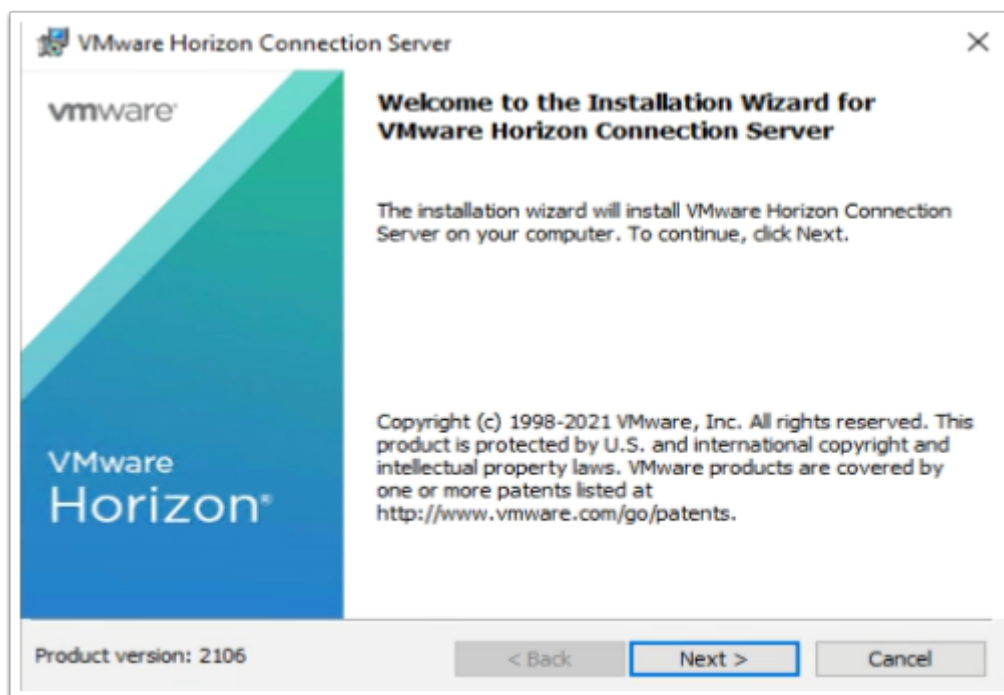
C:\Windows\system32>
```

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

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



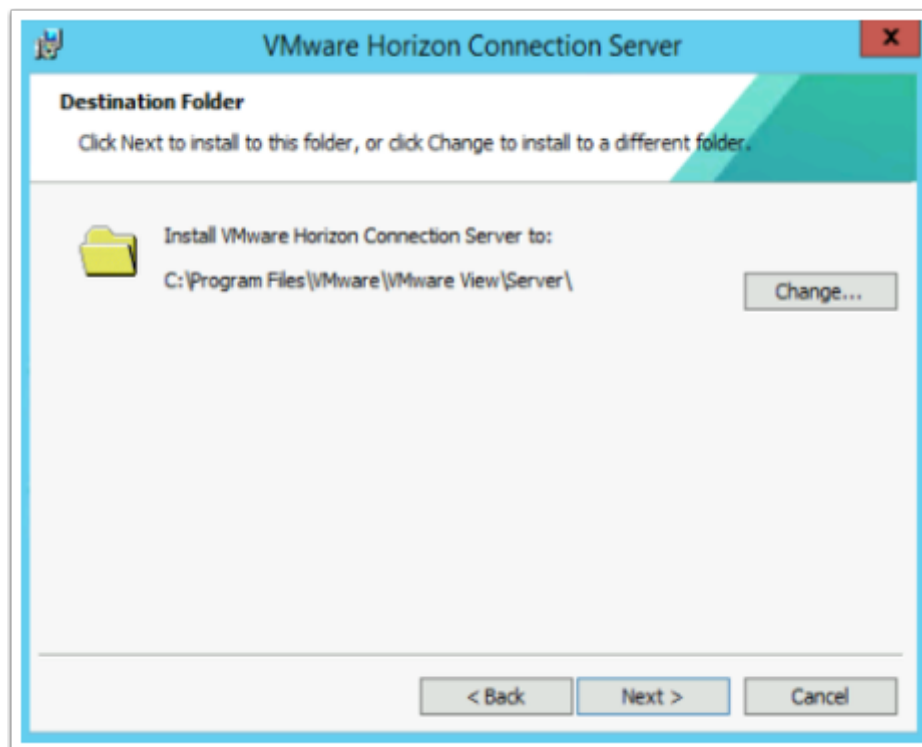
25. On the **TrueSSO** server desktop
- Launch the **software** shortcut and open the **Horizon\2106** folder.
 - Select the installer, **VMware-Horizon-Connection-Server-x86_64-8.3.0-18294467**
 - Select **Run**



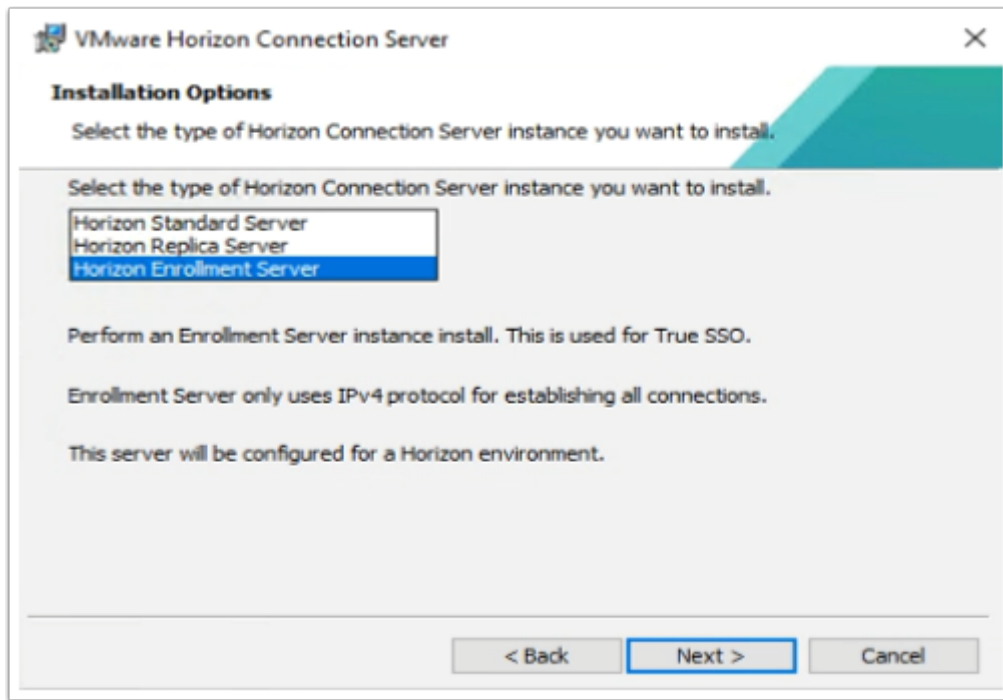
26. On the **Welcome** window
- Select **Next**



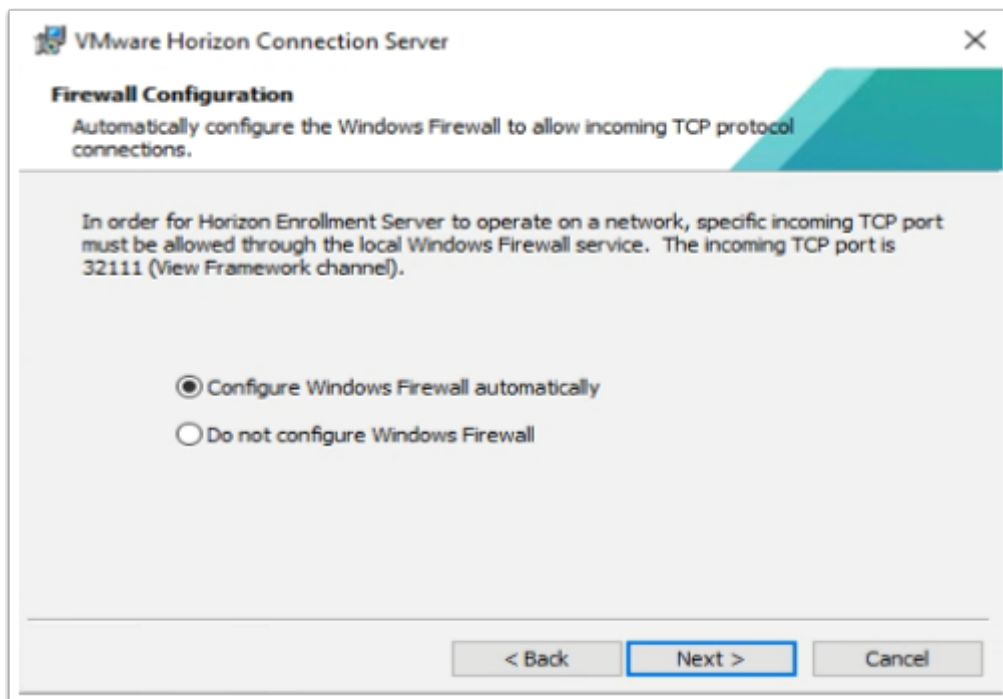
27. On the **License agreement** window
- Select the **radio button** next **I accept the terms in the license agreement**,
 - Select **Next**



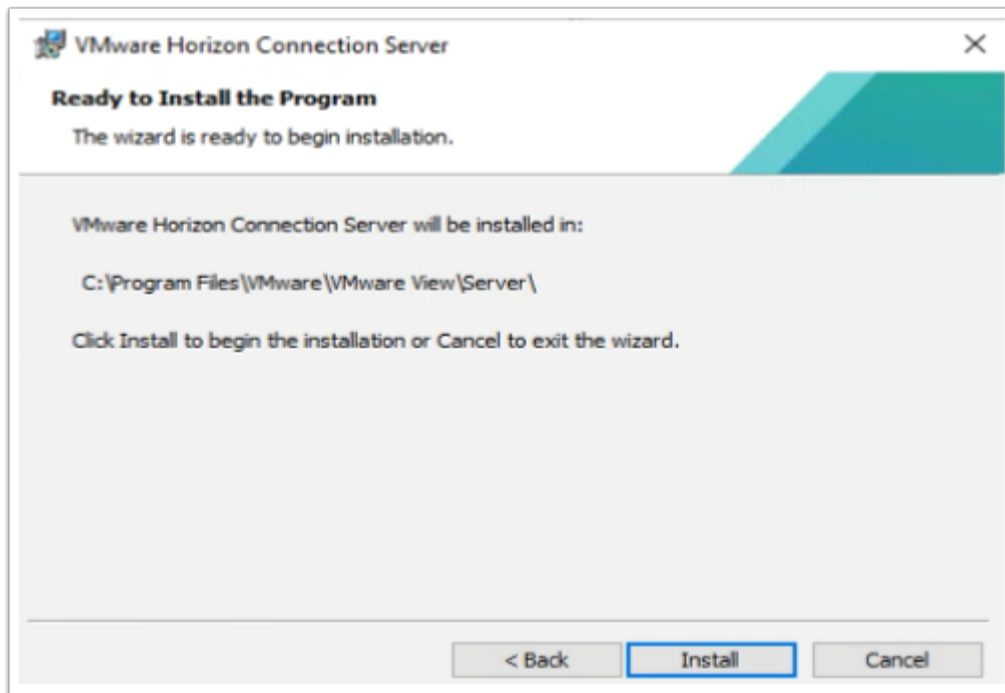
28. On **Destination Folder** window
- Select **Next**



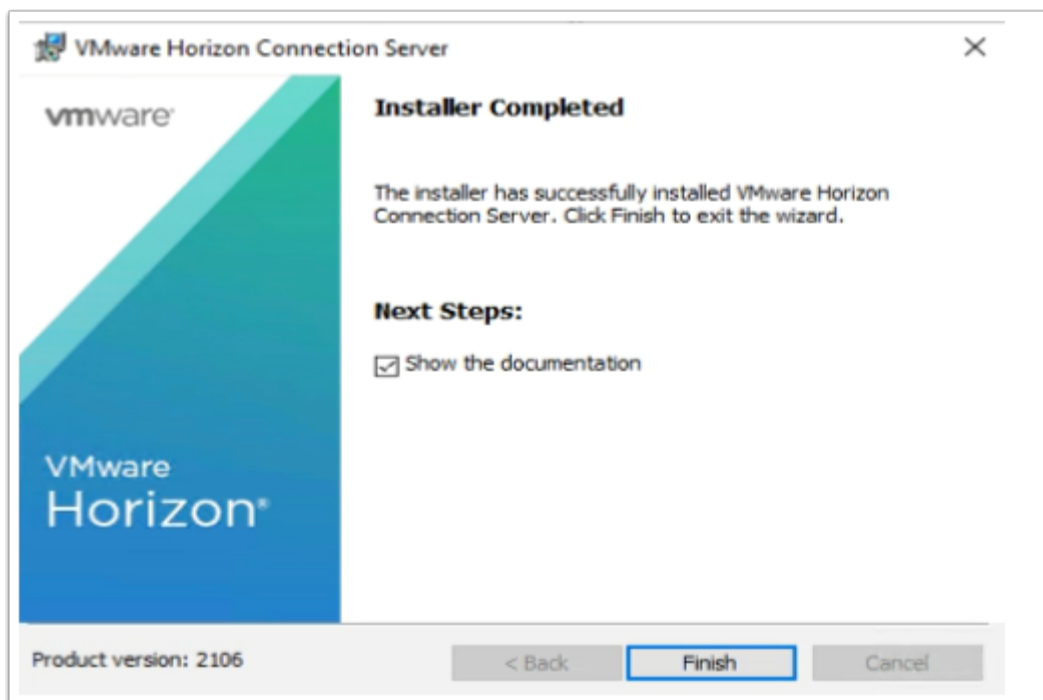
29. On the **Installation Options** window
- Select **Horizon Enrollment Server**
 - Select **Next**



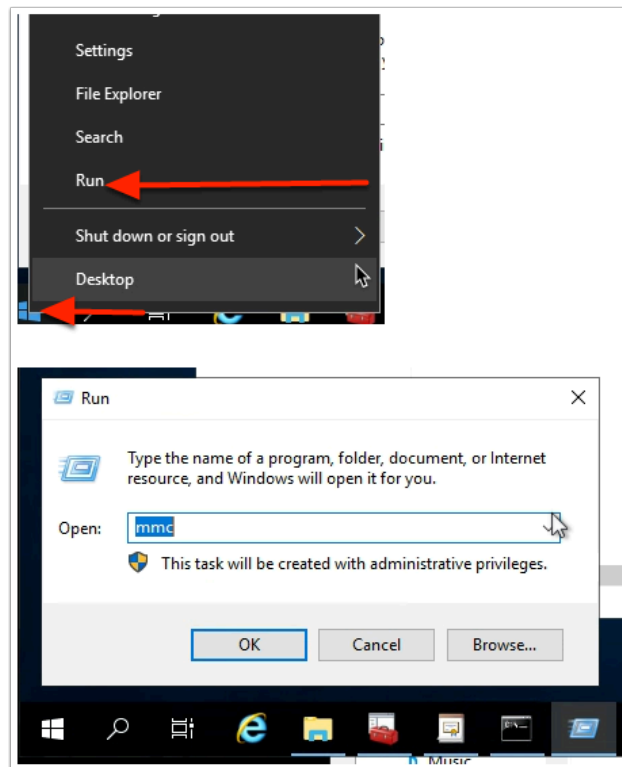
30. On **Firewall configuration** window
- Select **Next**



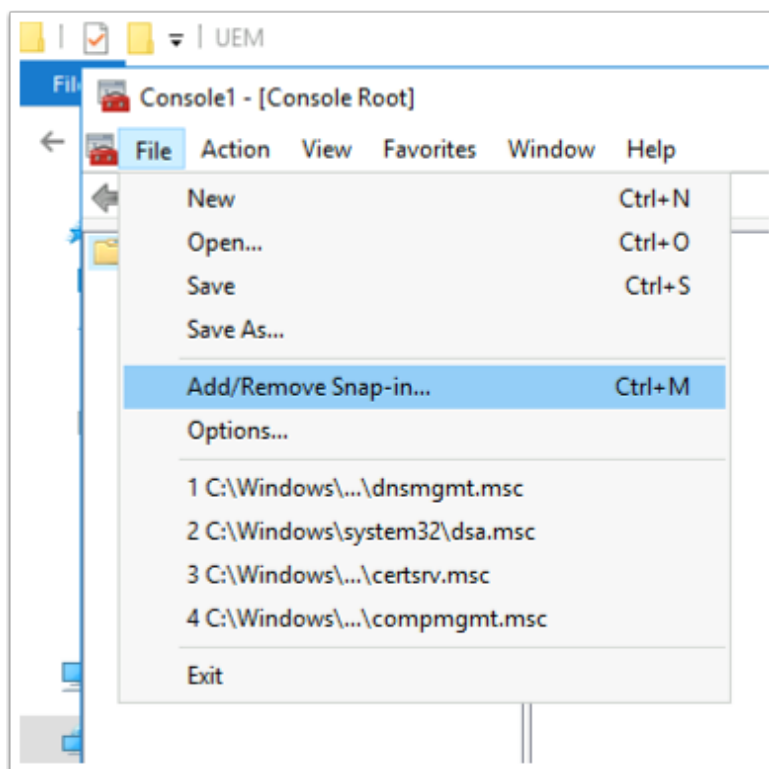
31. On the **Ready to Install the Program** window
- Select **Install**



32. On the **Installer Completed** Window
- Select **Finish**

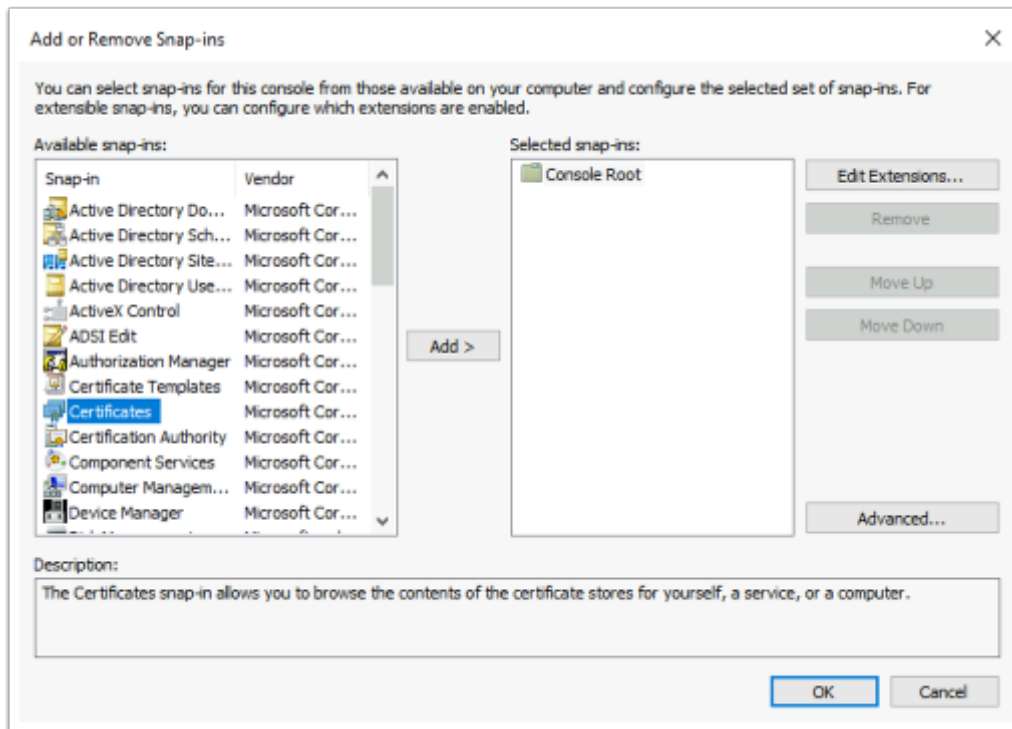


33. On the **TrueSSO** server
- Select and right-click the **Start Button**,
 - Select **Run**, type **MMC**,
 - Select **OK**



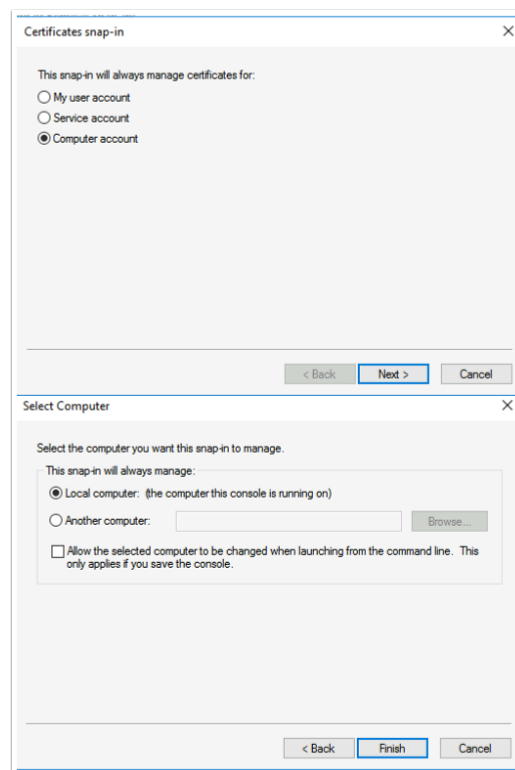
34. In the **Console** window,

- Select **File** > **Add/Remove Snap-in..**



35. In the **Add or Remove Snap-ins** window,

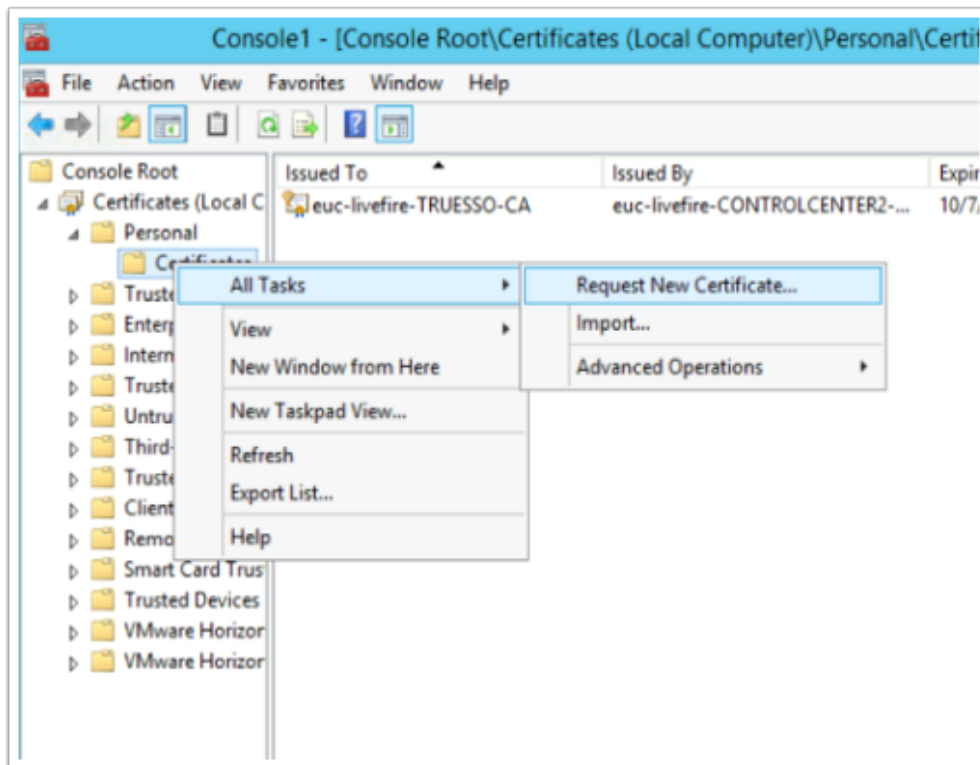
- Select **Certificates**
- Select **Add**



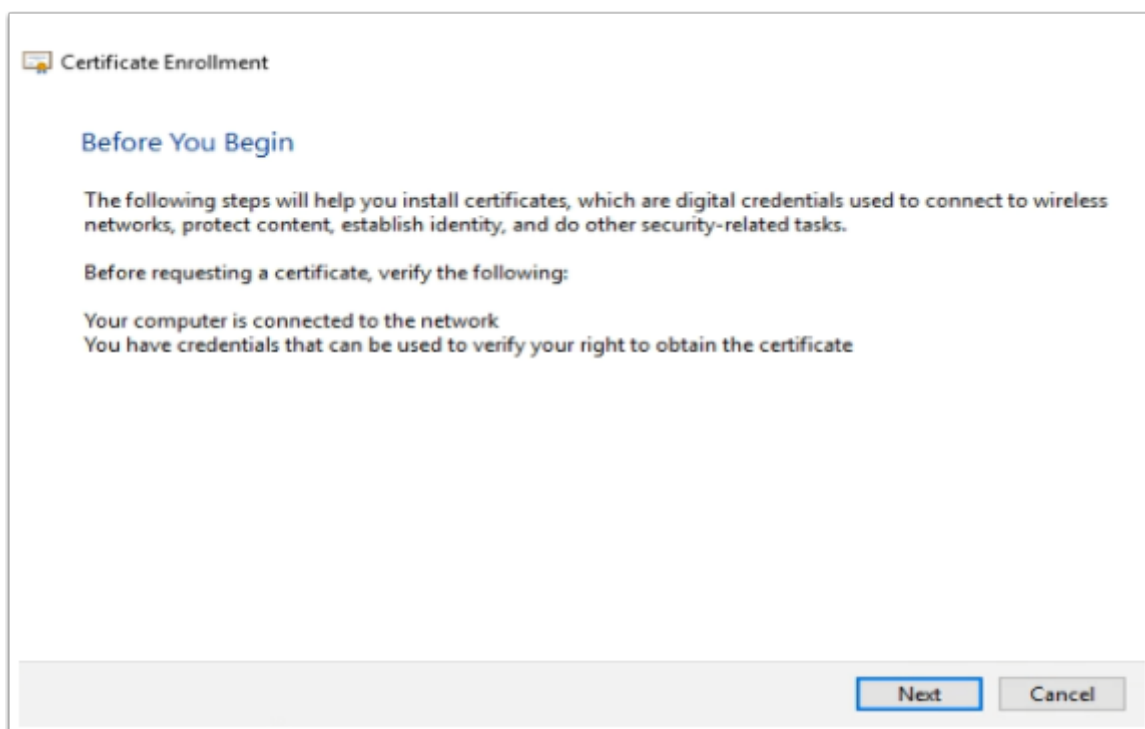
36. On the **Certificates Snap-in**

- Select **Computer account** **radio button**

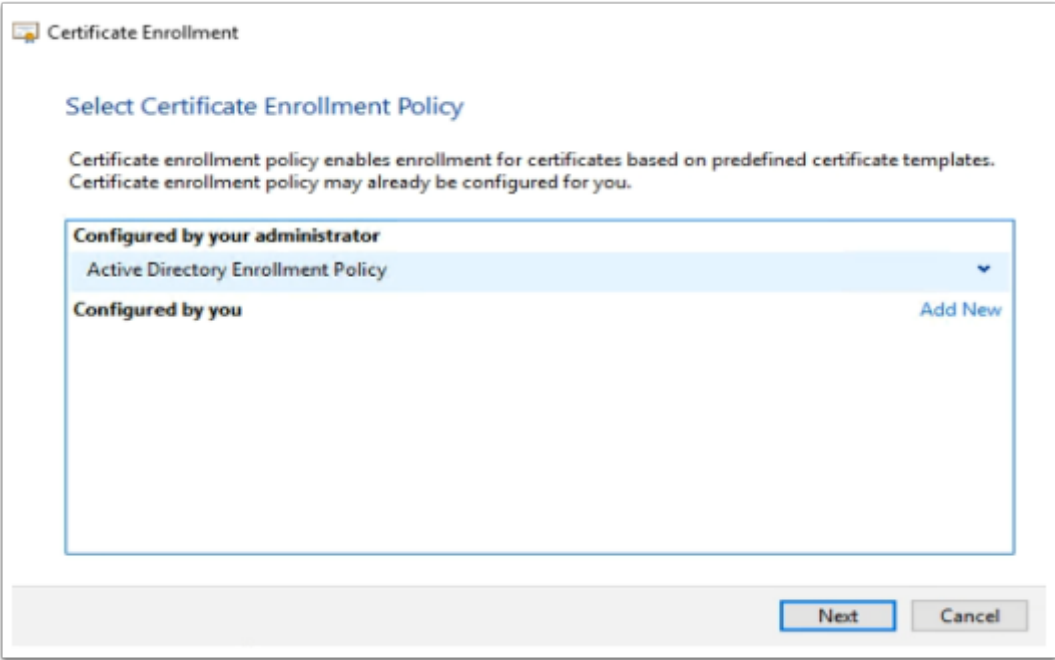
- Select **Next**
- On the **Select Computer** (accept defaults) and select **Finish**
- Select **OK**



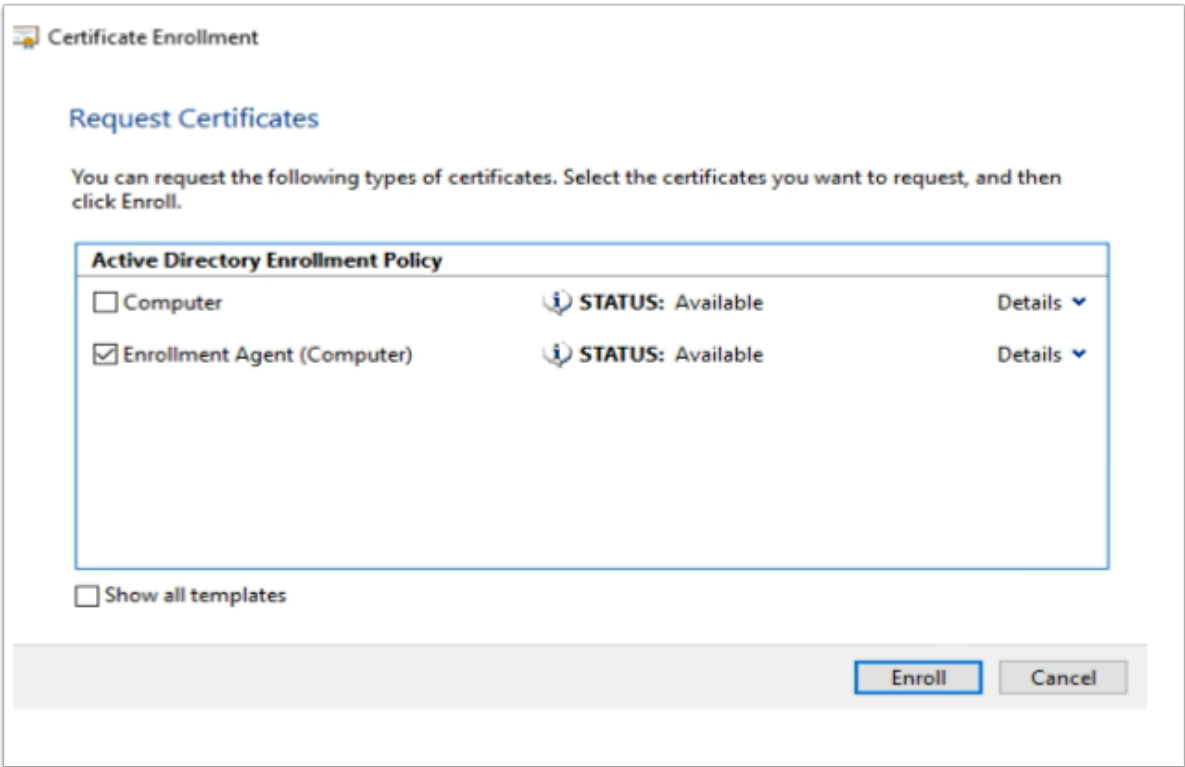
37. Expand the **Certificates** console inventory
- Select and right-click the **Personal** container.
 - Select **All Tasks** > **Request New Certificate**



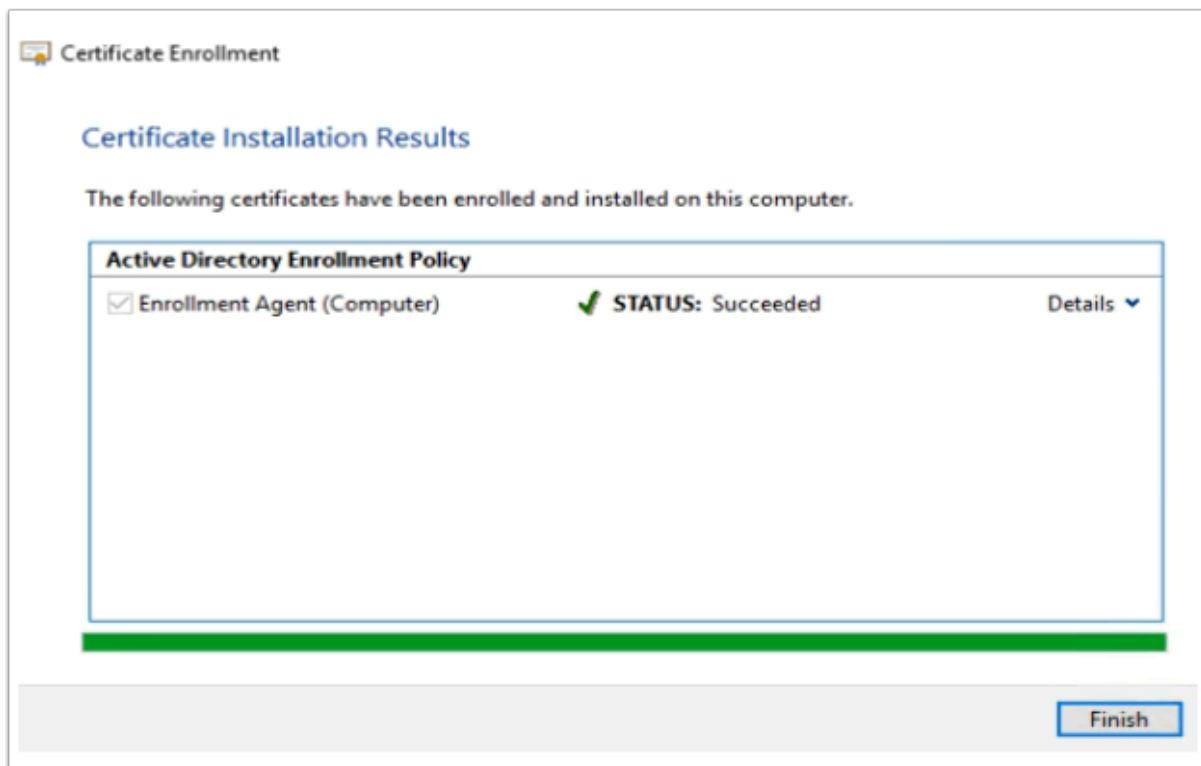
38. On the **Certificate Enrollment > Before you Begin** window
- Select **Next**



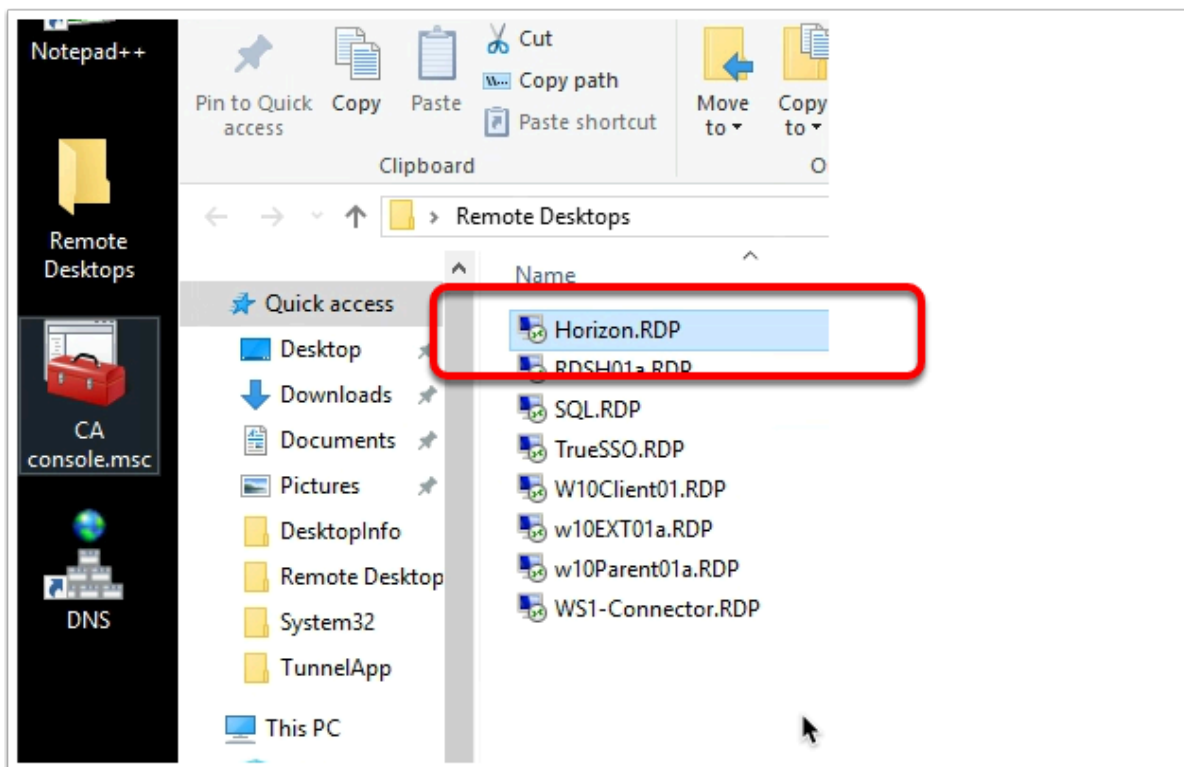
39. On the **Select Certificate Enrollment Policy** window
- Select **Next**



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

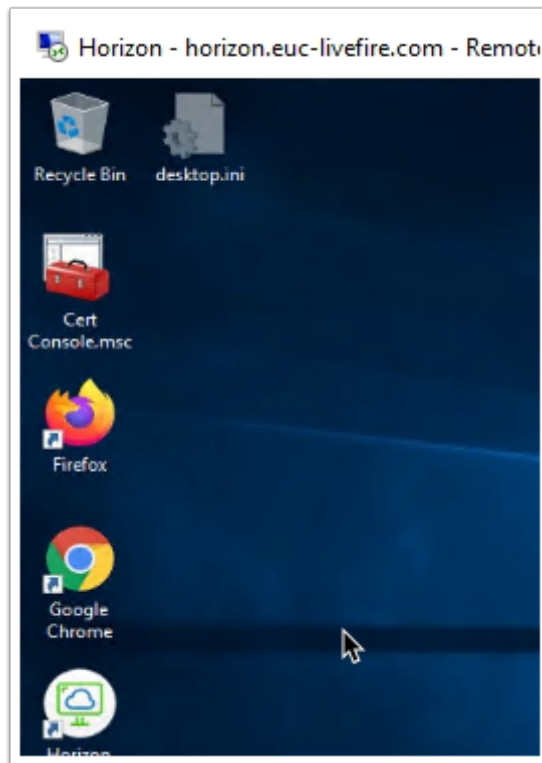


41. On the **Certificate Installation Results** window,
- Ensure the enrollment was successful
 - Select **Finish**.



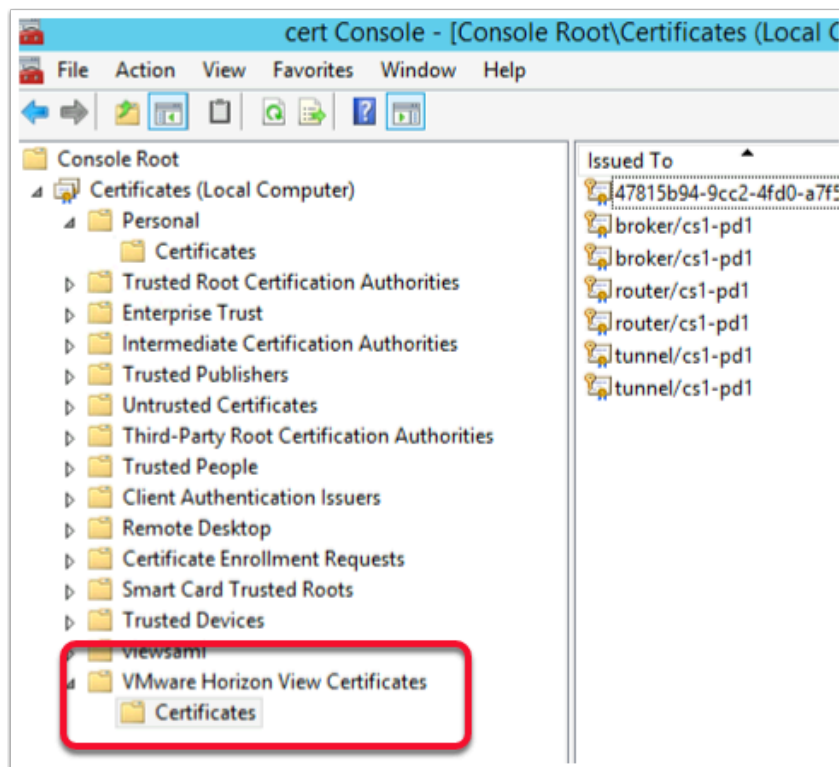
42. On your **ControlCenter** server,
- Open your **Remote Desktops** folder

- Launch the **Horizon.RDP** session



43. On the **Horizon server** desktop

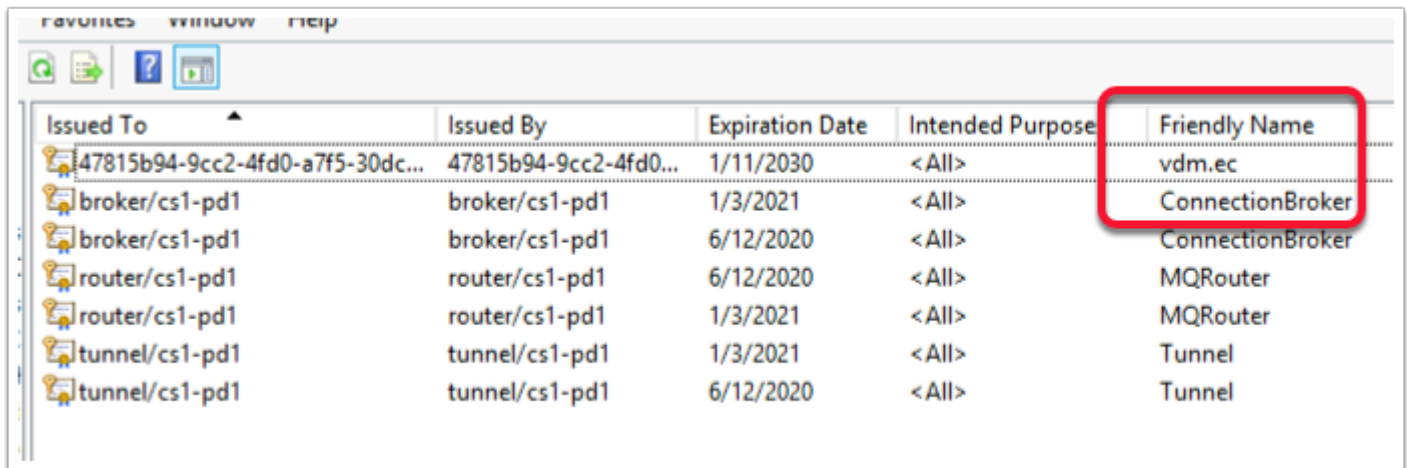
- Select and open your **Cert Console.mmc**



44. In the **Certificates** Console

- **Expand** the inventory

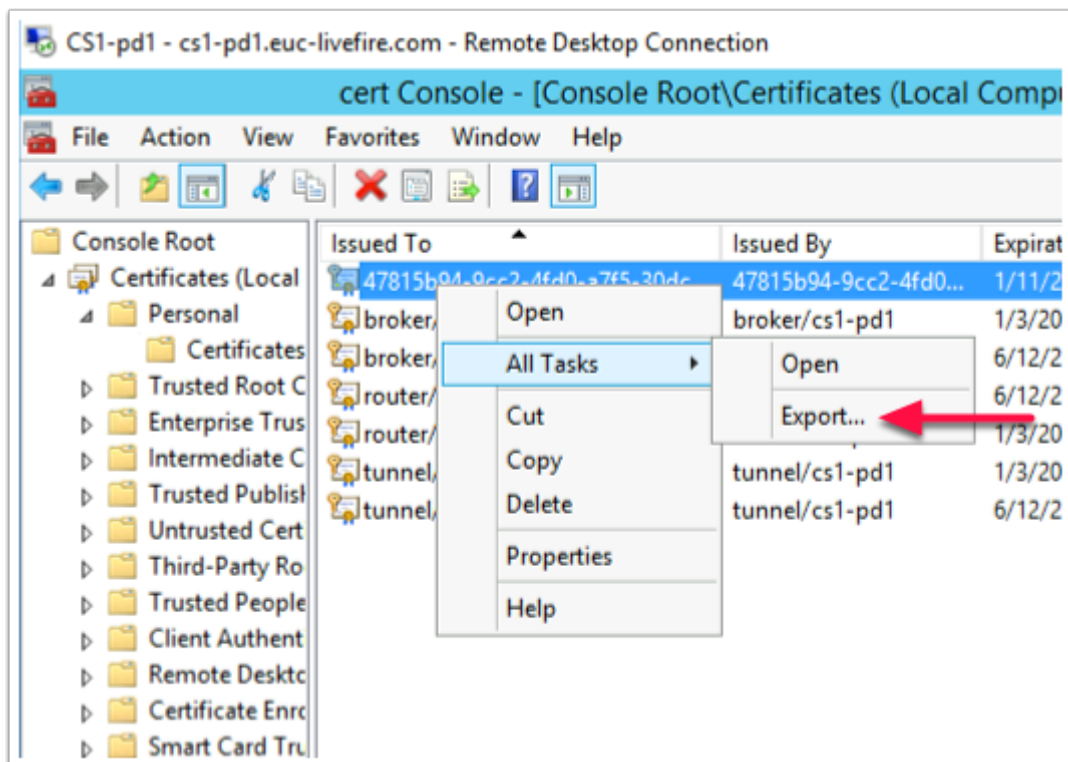
- Browse down to **VMware Horizon View Certificates > Certificates**



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

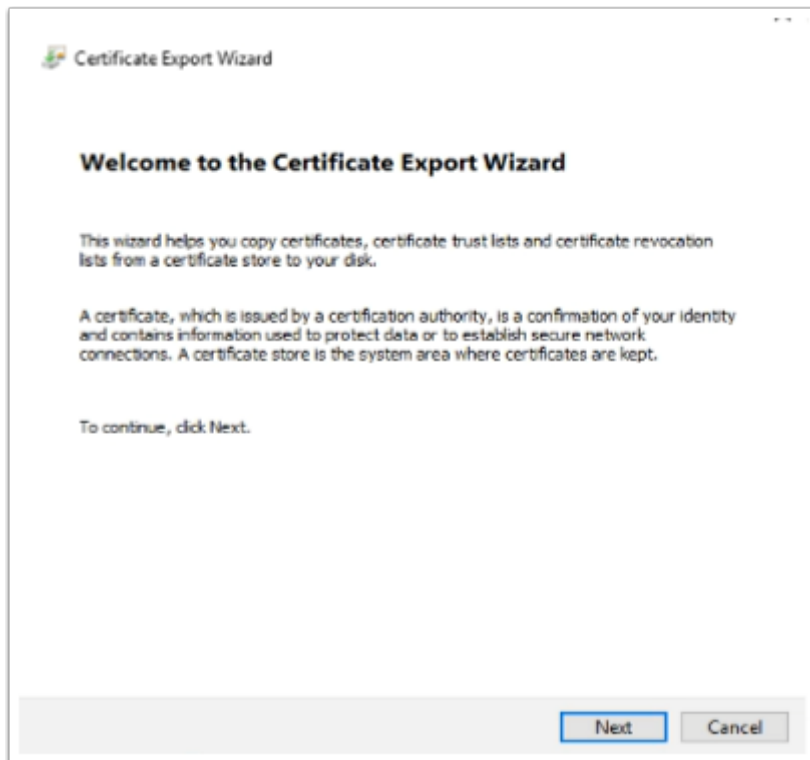
45. In the Certificates Console

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



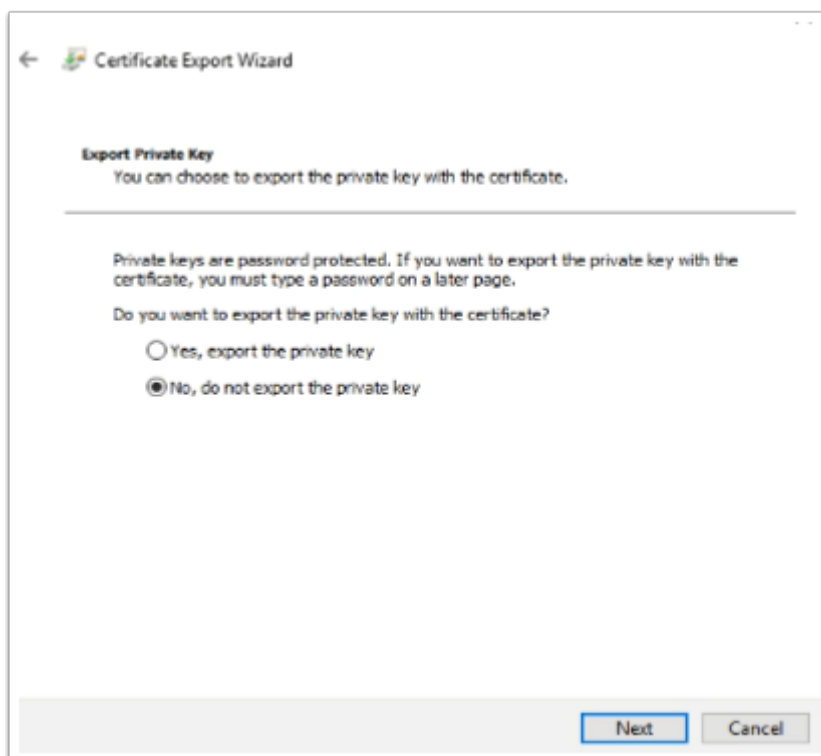
46. In the Certificates Console

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



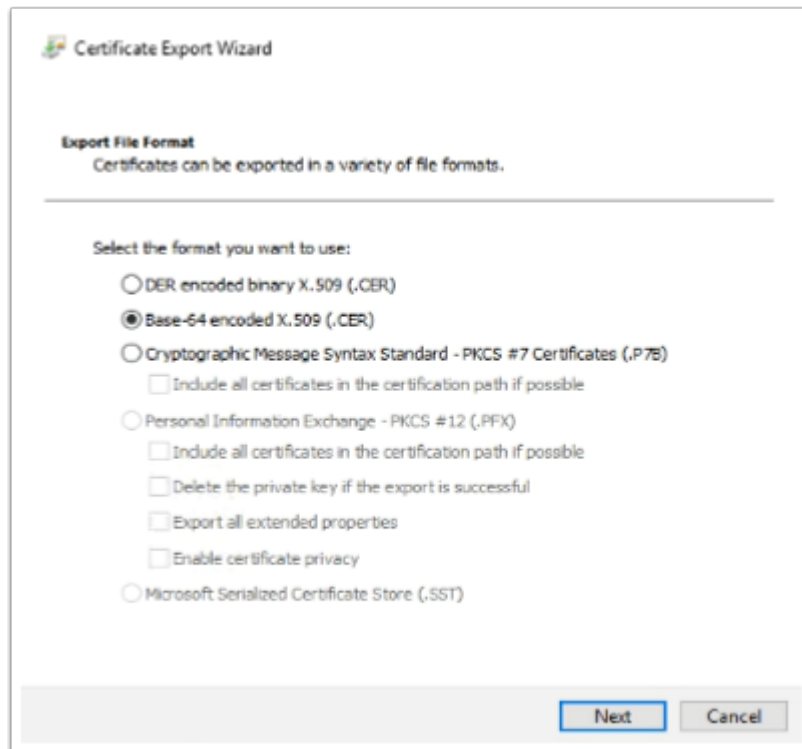
47. On the **Welcome** window

- Select **Next**

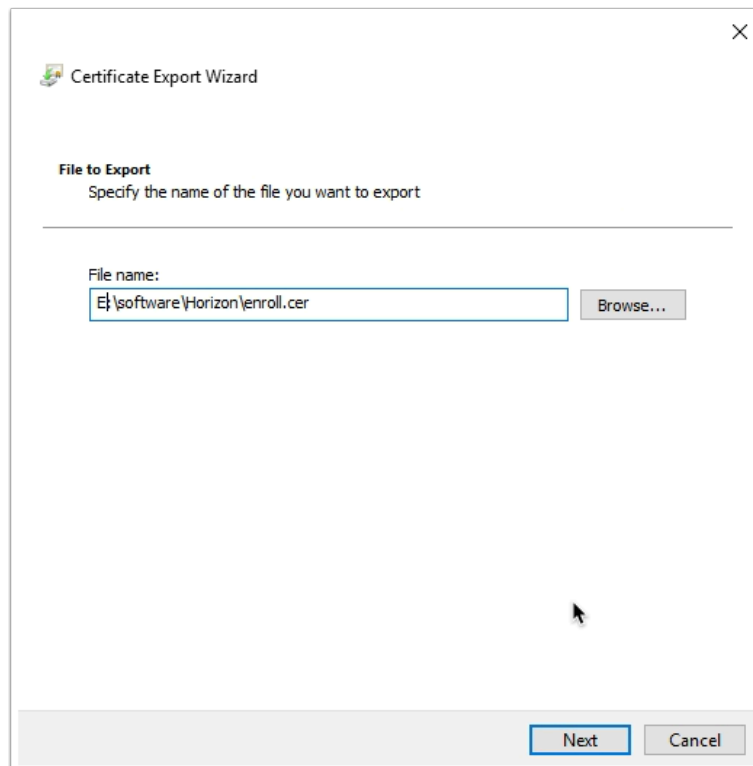


48. On the **Export Private Key** page

- Select the **radio button** next to **No, do not export the private key**
- Select **Next**

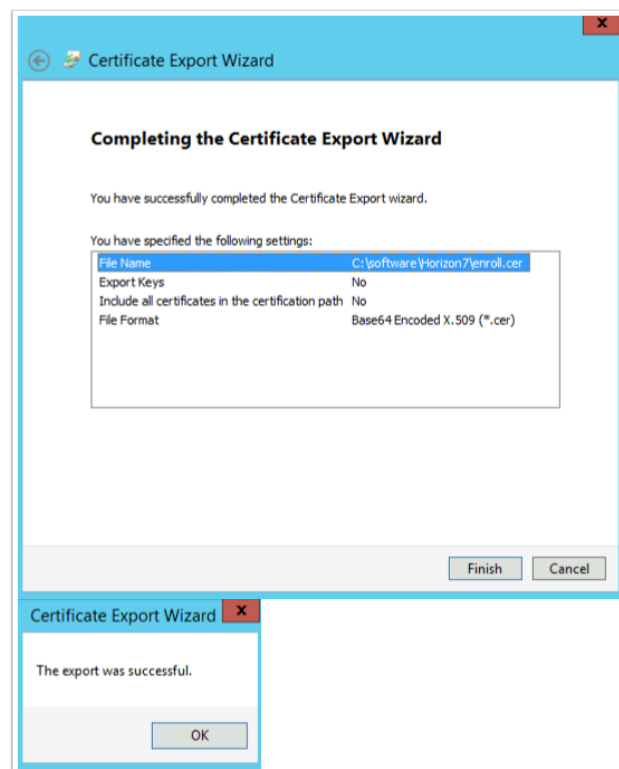


49. On the **Export File Format** window
- Select the **radio button** next to **Base-64 encoded X.509**
 - Select **Next**

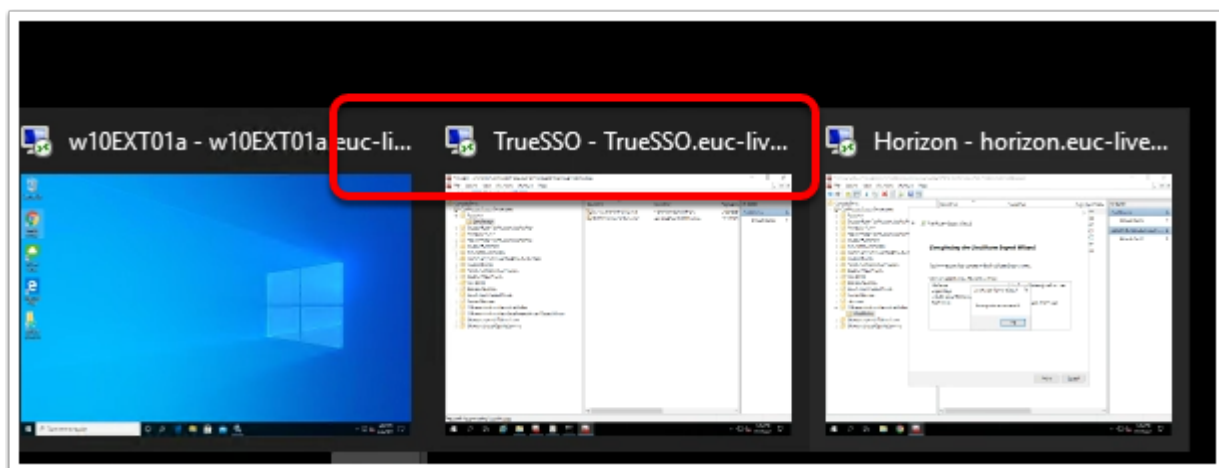


50. In the **File to Export** window
- In the **File name** area type the following **E:\software\Horizon\enroll.cer**

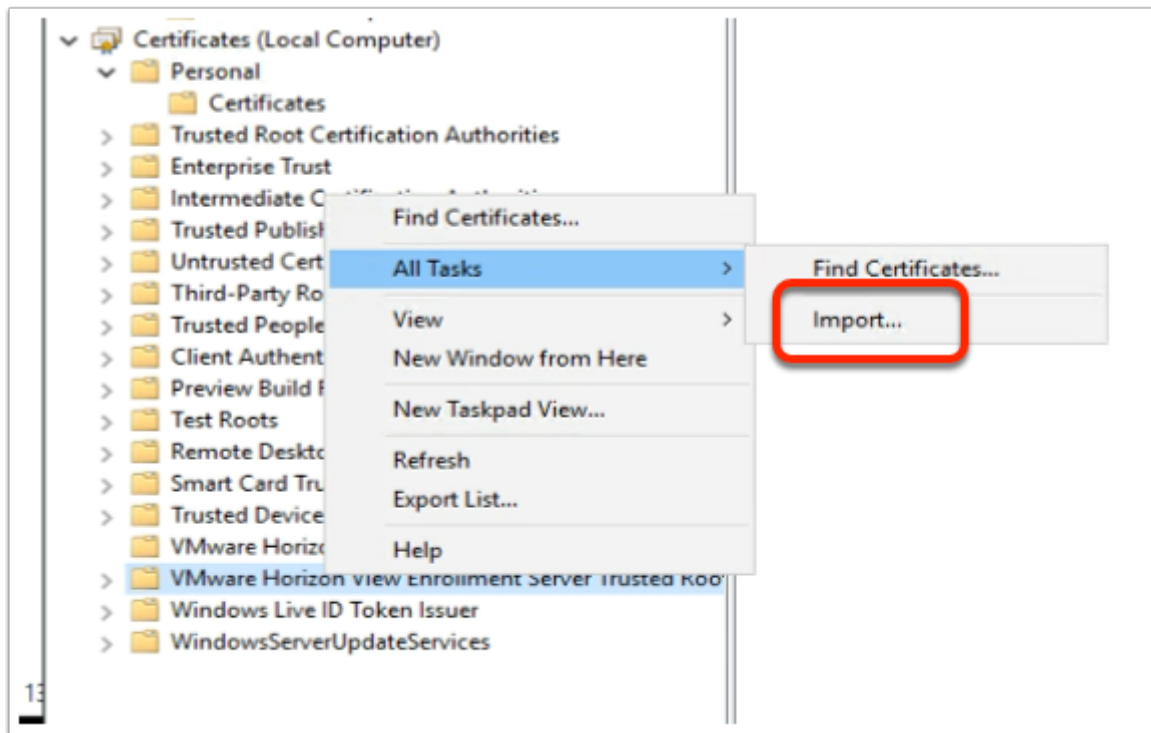
- Select **Next**



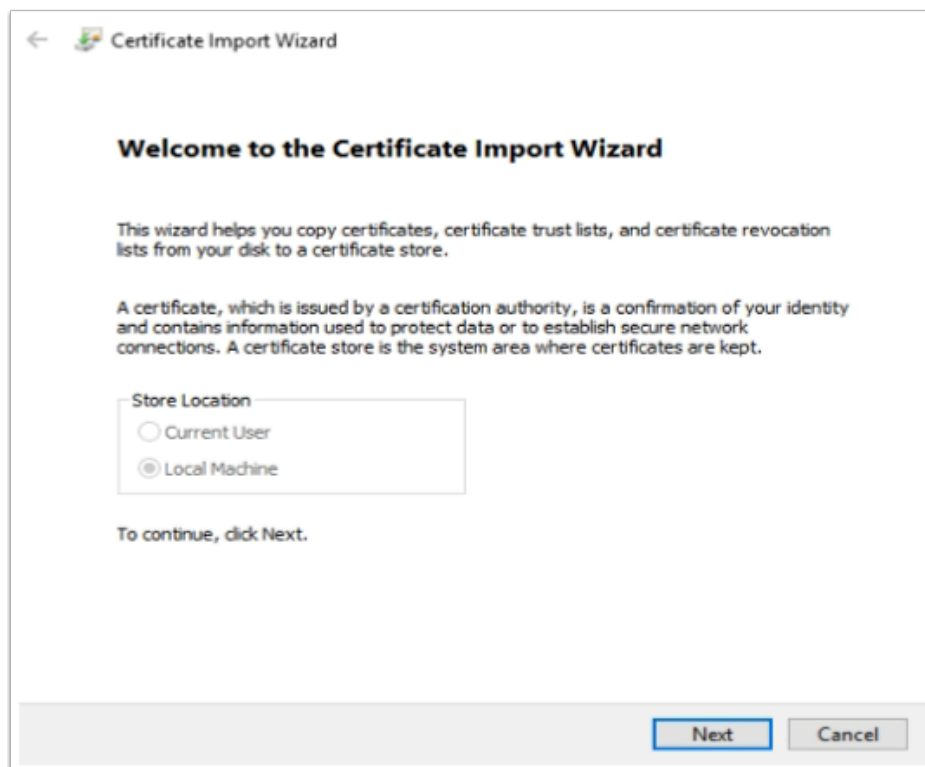
- On the **Completing the Certificate Export Wizard** window
 - Select **Finish**.
 - When prompted that **The export was successful**,
 - Select **OK**



- On your **ControlCenter** server desktop
 - Switch from your **Horizon** RDP session to your **TrueSSO** RDP session

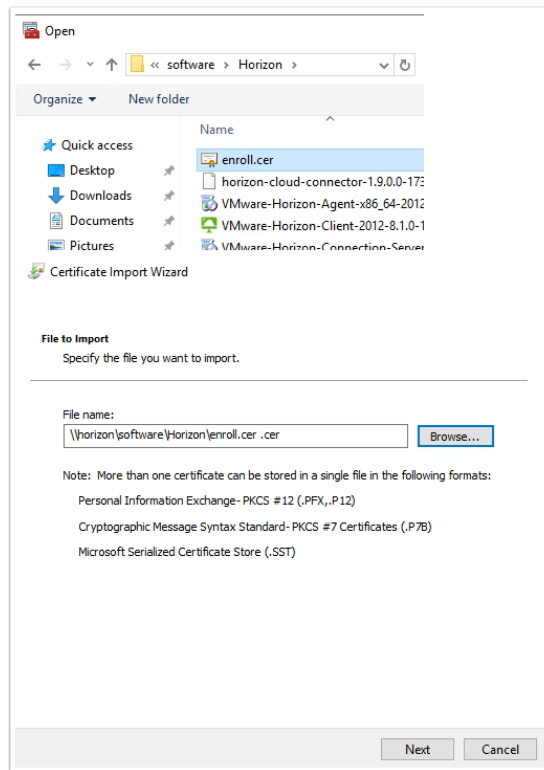


53. On your **TRUESSO** server
- Open your **Certificate services** Snap-in,
 - Select and right-click the last container in the inventory **VMware Horizon View Enrollment Server Trusted Roots**,
 - Select **All Tasks** > **Import**



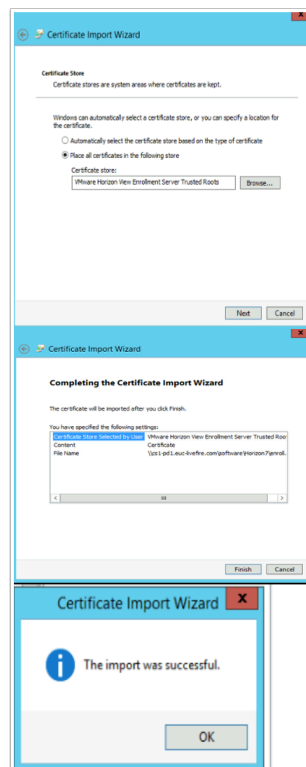
54. On the **Welcome** window

- Select **Next**



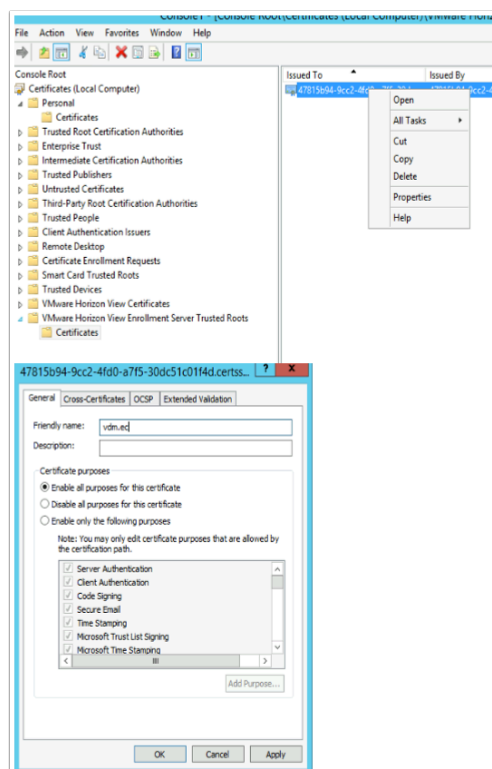
55. In the **File to import** window

- Type the following **\\horizon\software\Horizon\enroll.cer**
- Select **Next**



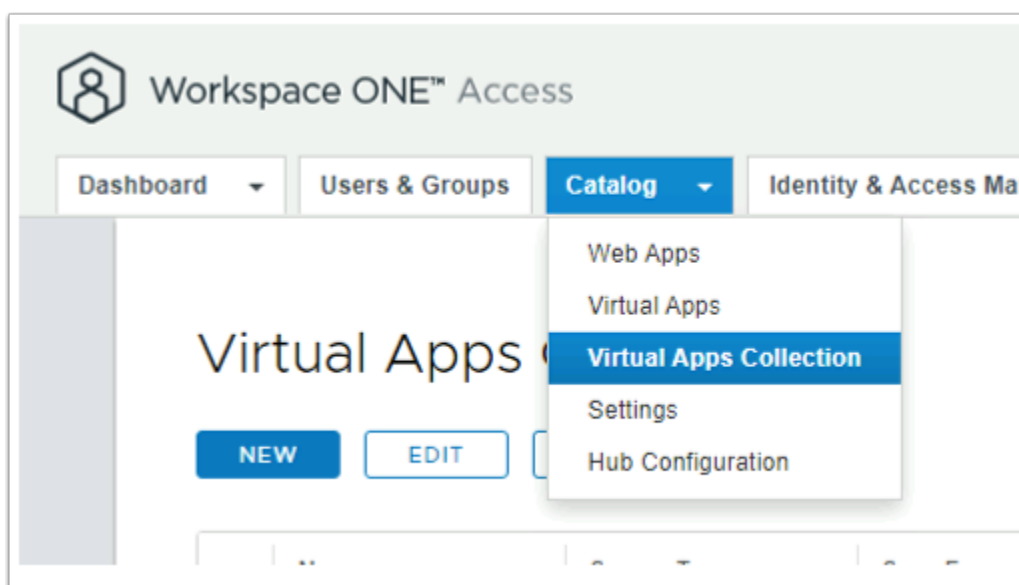
56. In the **Certificate Store** window accept the defaults and select **Next**.

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



57. In the Certificates Snap-In

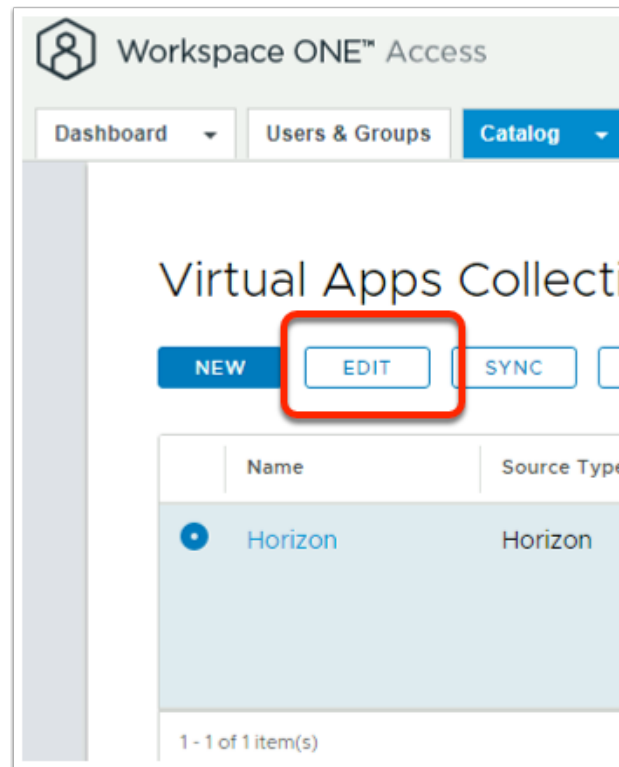
- Right-click the **imported certificate**
- Select **Properties**.
- In the **Friendly name:** section type **vdm.ec**
- Select **OK**



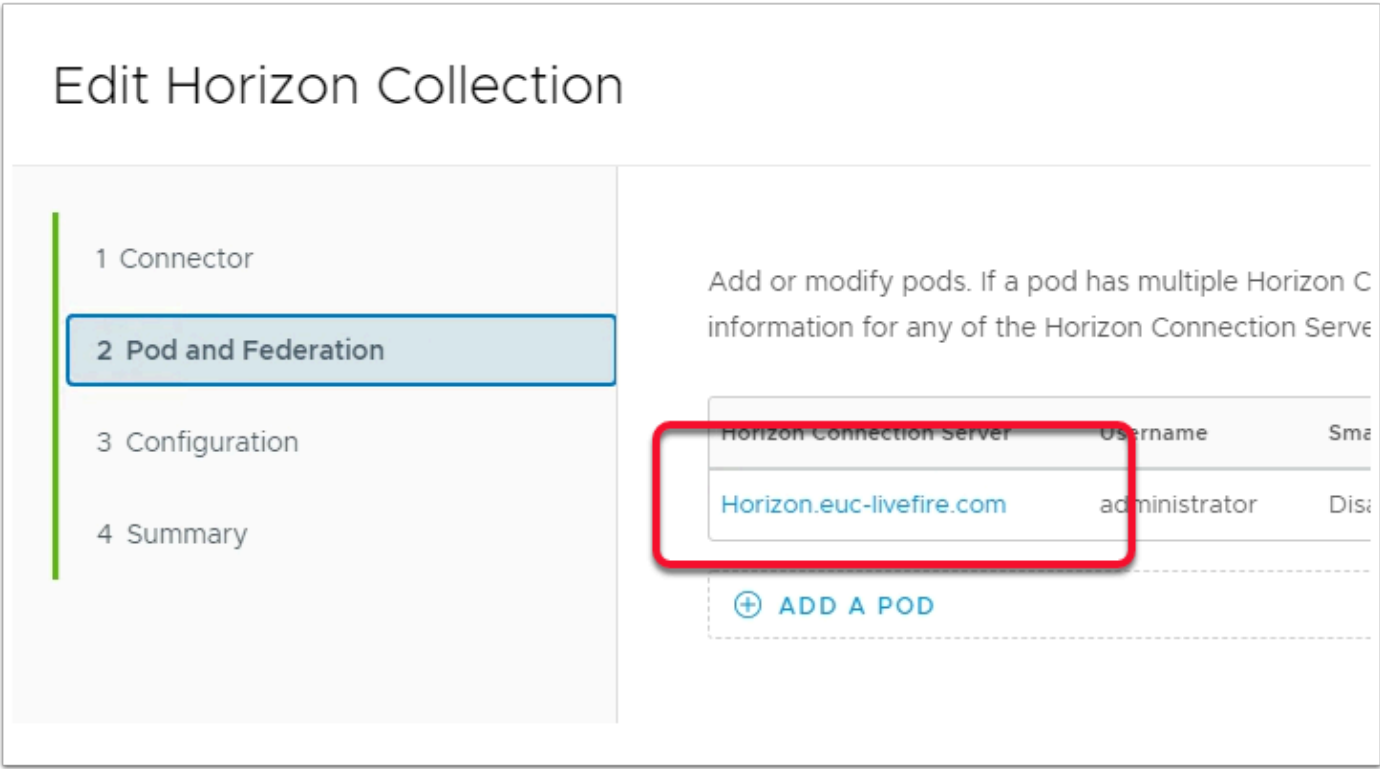
58. On your **ControlCenter** server,

- Switch to your **Chrome browser**,

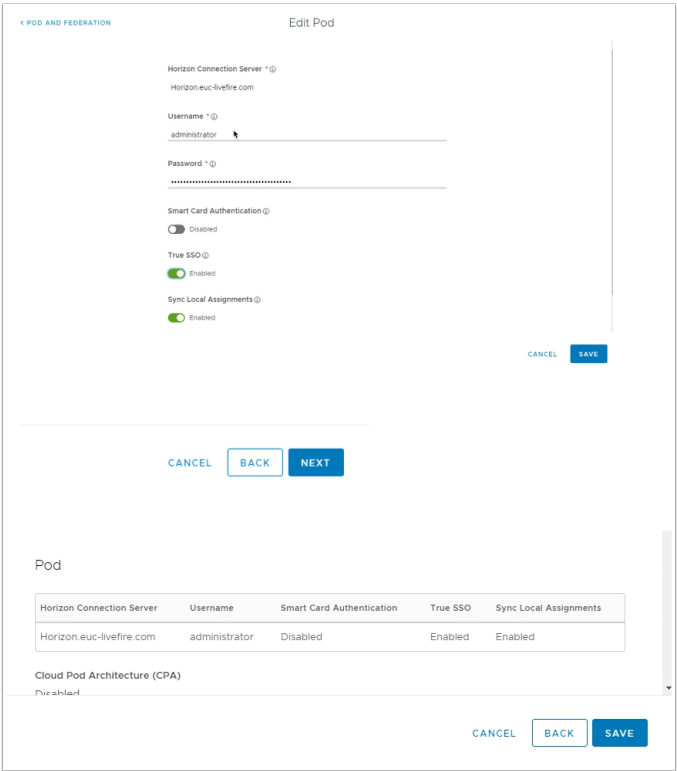
- Open a **new tab**,
- Using your **custom Workspace ONE Access Url**,
 - Log in as **System admin** with your **custom credentials**
- Select the **Catalog** tab > **Virtual Apps Collection**



59. In the **Virtual Apps Collection** window
- Select the **radio button** next **Horizon**
 - Select **EDIT** next to **NEW**

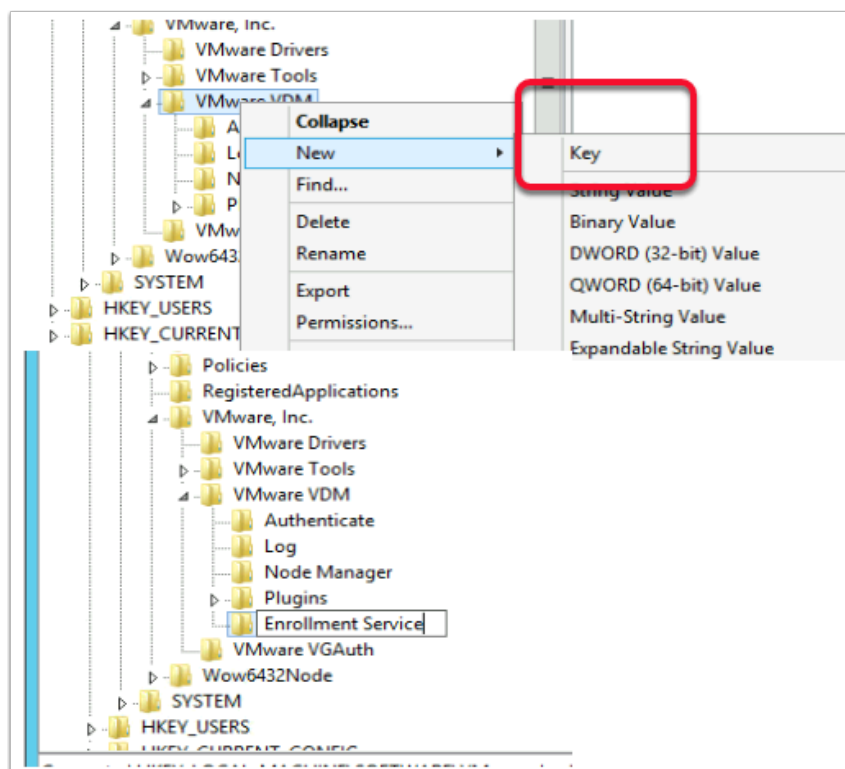


60. In the **Edit Horizon Collection** window,
- Select **2 Pod and Federation**,
 - To the right, select **horizon.euc-livewire.com**



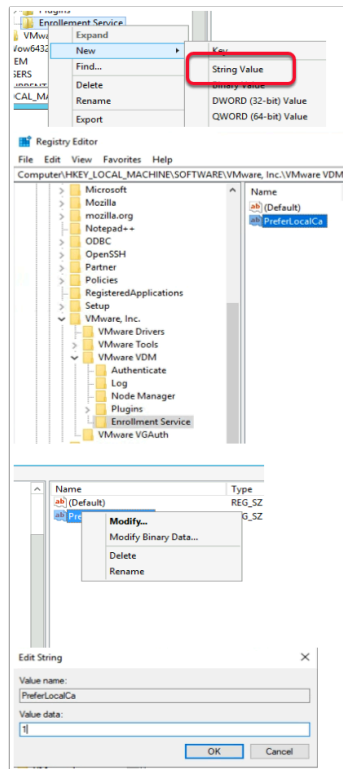
61. In the **Edit Pod** window
- Under **True SSO**, change the **toggle** from **Disabled** to **Enabled**

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



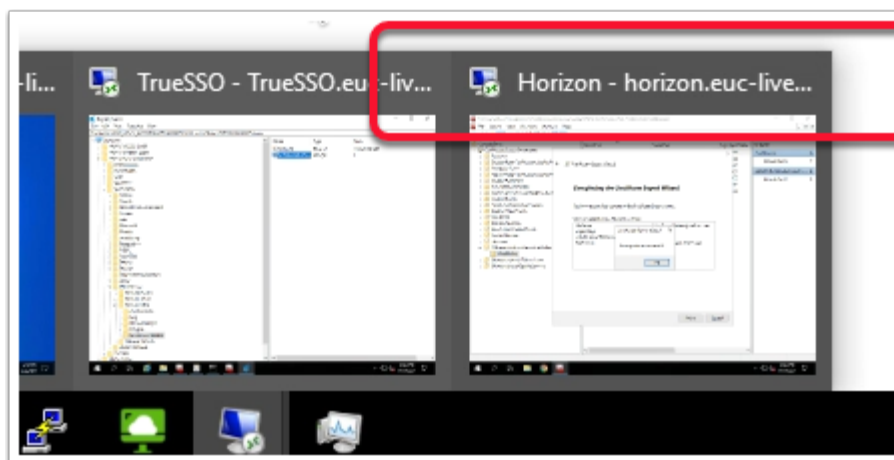
62. From the **ControlCenter** server, switch back to your **TrueSSO.RDP** session

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



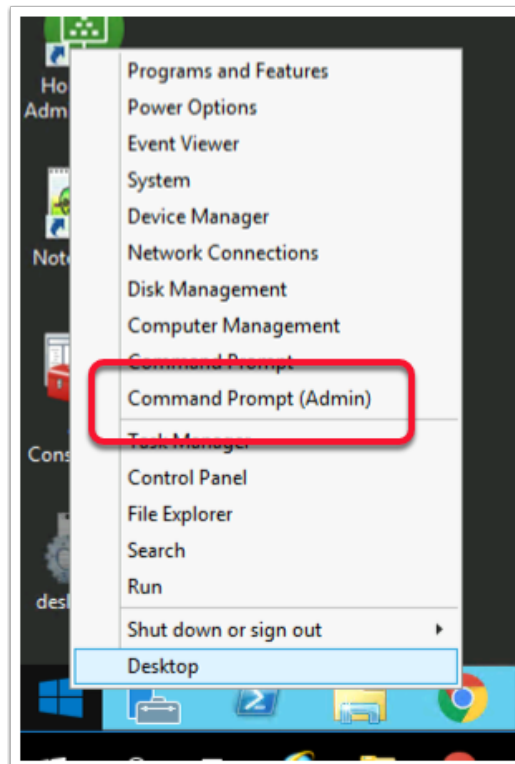
63. Configure the enrollment service to give preference to the local certificate authority when they are co-located:

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

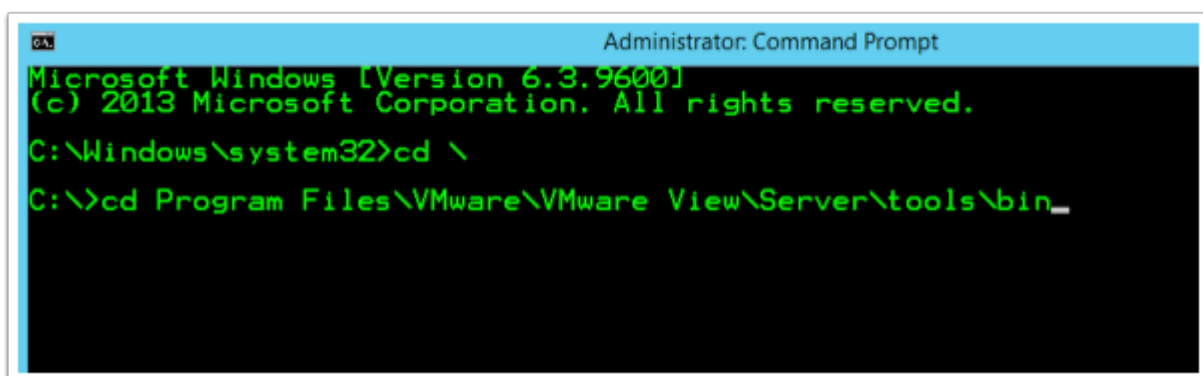


64. On your **ControlCenter** server

- Switch to your **Horizon.RDP** session
- NOTE. At this point, to get the maximum benefit with the following steps, it would be advisable to go Full Screen with your RDP session.



65. On your Horizon server
- Select and right-click the **Start** button
 - Select **Command Prompt (Admin)**
 - **Maximise** your **Command Prompt** window



66. 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 VMware1! --truesso --environment --add --enrollmentServer TrueSSO.euc-livefire.com
Enrollment server(s) added to the environment
C:\Program Files\VMware\VMware View\Server\tools\bin>_
```

67. 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! --truesso --environment --add --enrollmentServer TrueSSO.euc-livefire.com
```

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truesso --environment --list --enrollmentServer TrueSSO.euc-livefire.com --domain euc-livefire.com
Failed to list True SSO environment info
Cannot fetch enrollment servers list ①

C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livefire --authPassword VMware1! --truesso --environment --list --enrollmentServer TrueSSO.euc-livefire.com --domain euc-livefire.com
True SSO environment info
Enrollment server: truesso.euc-livefire.com
Domain: euc-livefire.com
Forest:
  Name: euc-livefire.com
  Enrollment CertState: VALID ②
  Template(s):
    Name: TrueSSOTemplate
    Minimum key length: 2048
    Hash algorithm: SHA256
  Certificate Authority(s):
    Name: CONTROLCENTER-CA
    Name: euc-livefire-TRUESSO-CA

C:\Program Files\VMware\VMware View\Server\tools\bin>_
```

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

1. If one executes too quick, you will get the following error message
 - In the **Administrator: Command Prompt** type the following:-
2. 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 TrueSSO.euc-livefire.com --domain euc-livefire.com
```

```

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

```

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

```

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

```

```

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

```

70. 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-livfire --authPassword VMware1! --truesso --list --authenticator

```

```

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

```

71. 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-livfire --authPassword VMware1! --

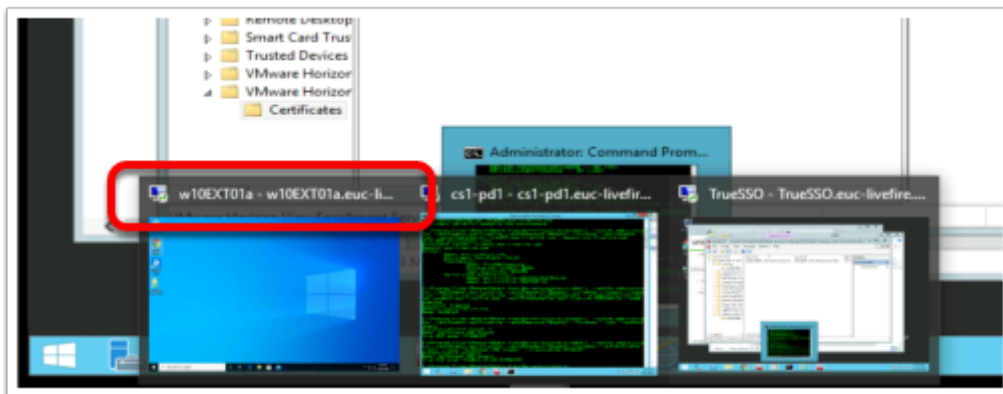
```

```
truesso --authenticator --edit --name "Workspace ONE Access" --truessoMode ENABLED
```

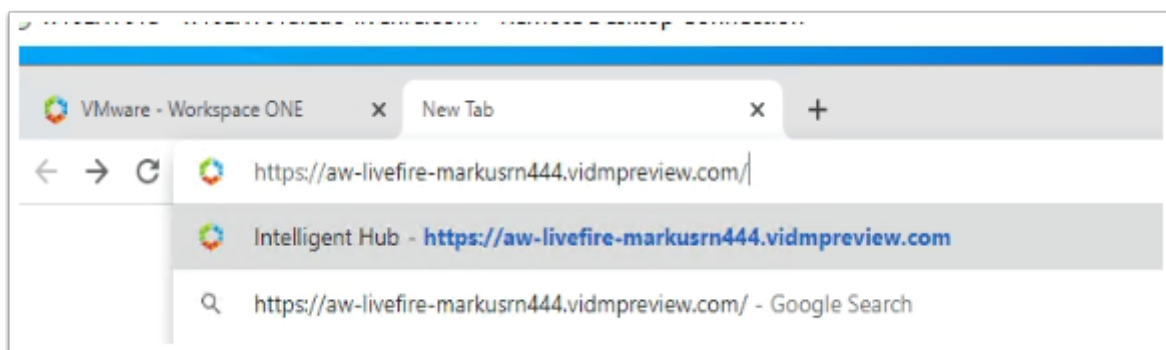
For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to Workspace ONE Access. In this case if a password was used and cached, the system will use the password. Set --truessoMode to ALWAYS if you want True SSO to be used even if a password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

73. On your ControlCenter server
 - Minimise your **Horizon.RDP** Session

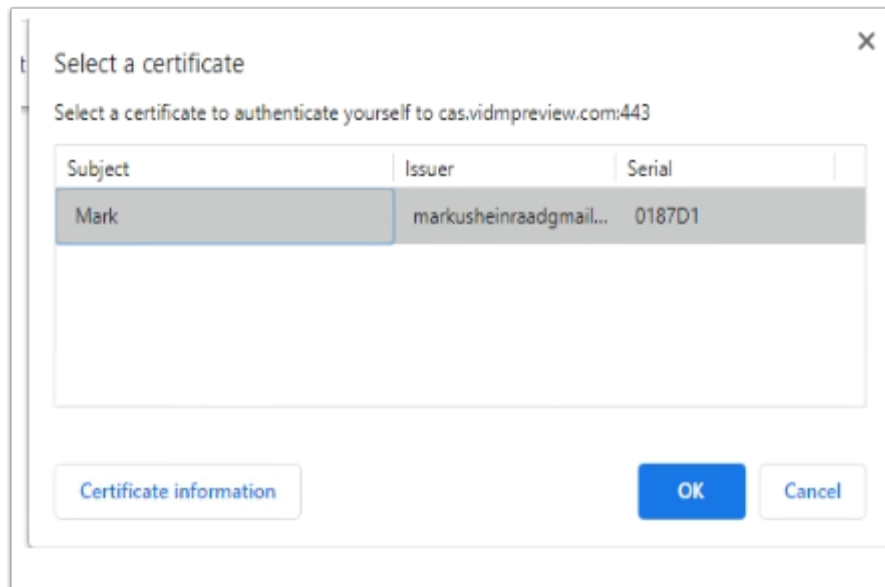
Part 4: Testing to see if TrueSSO works



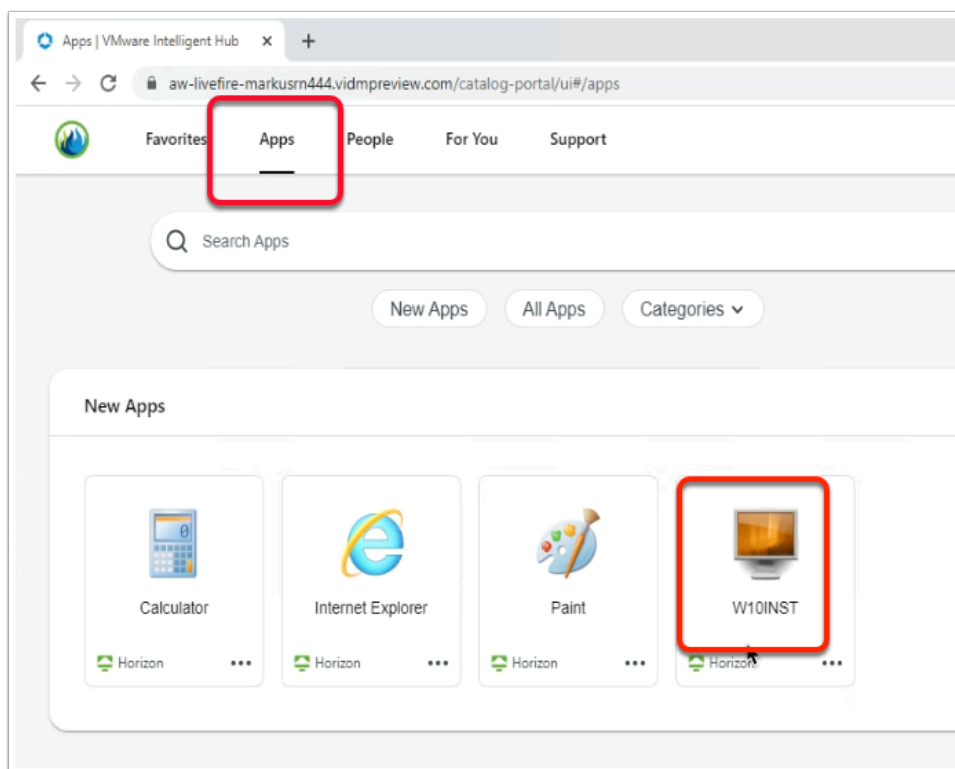
1. On your **ControlCenter** server,
 - Switch your **Remote Desktops** session to **W10EXT01a.RDP**.



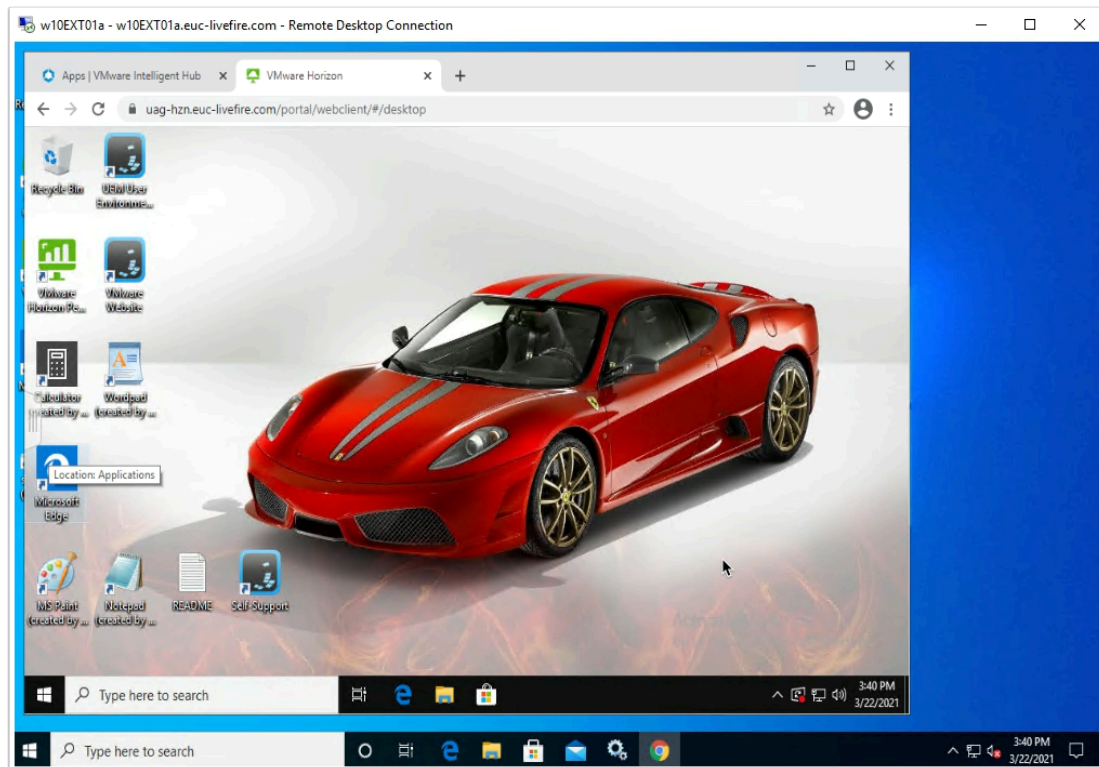
2. On your **W10EXT01a** desktop,
 - **Open** your browser and type **custom Workspace ONE Access URL**



3. On the **Select a certificate** window,
- Select **OK**



4. In the **Apps** tab
- Select **W10INST**



5. In the **All Apps** area,
- Observer your Horizon Desktop session
 - Possibly launch a RDSH session from your Workspace ONE Access console
 - This concludes this lab as

Acknowledgements

A huge thank you Spas Kaloferov from Livefire and Rahul Jha from GSS in assisting me Troubleshoot this lab when authoring the first version

About the Author

About the Author Reinhart Nel

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

For any questions please email Reinhart RACE-Livefire-EUC@vmware.com