


Installing and Configuring Horizon TRUESSO

Overview

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

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

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

Since December 2019

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

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

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

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

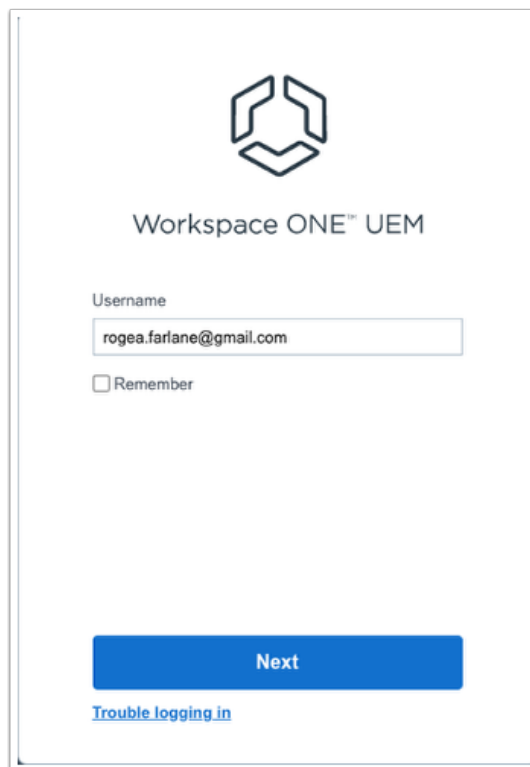
We will start off by doing the following:

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

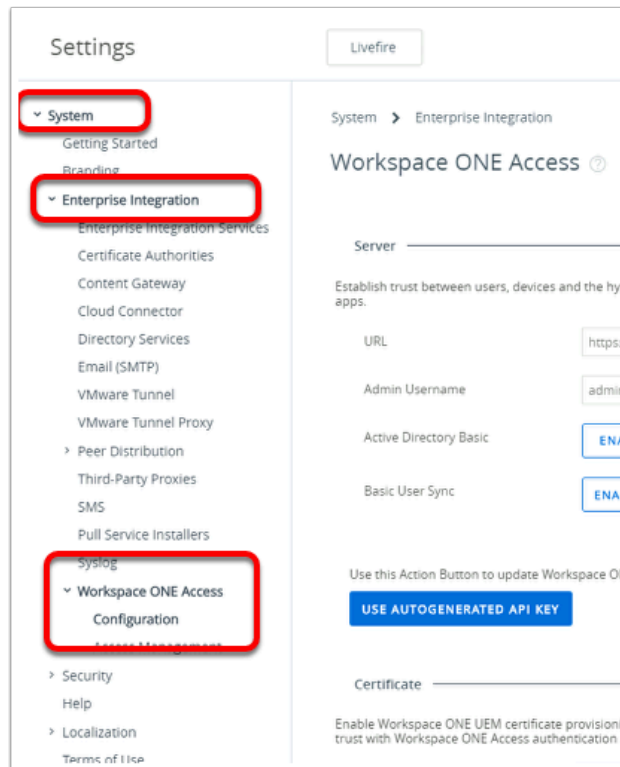
- Deploy and configure Horizon Enrollment services
- Integrate and configure Active Directory Certificate services with Horizon Enrollment services

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

Part 1: WorkspaceOne UEM - Certificate Profile

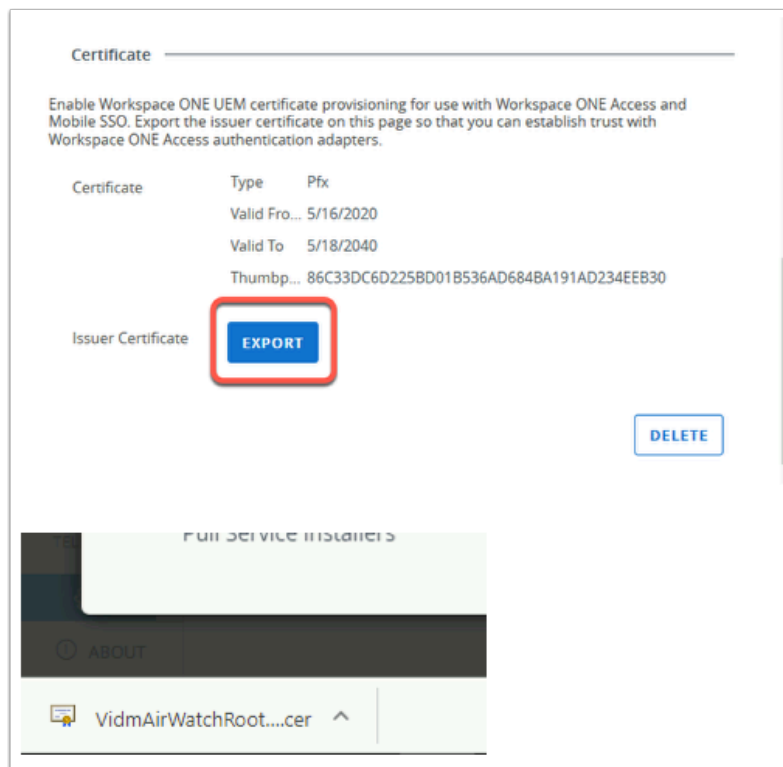
The image shows a login screen for Workspace ONE UEM. At the top center is the Workspace ONE logo, which consists of three interlocking hexagons. Below the logo, the text "Workspace ONE™ UEM" is displayed. Underneath, there is a "Username" label followed by a text input field containing the email address "rogea.farlane@gmail.com". Below the input field is a checkbox labeled "Remember". At the bottom of the form is a large blue button with the text "Next". Below the button is a link that says "Trouble logging in" in blue text.

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



2. In the Workspace ONE UEM Admin Console

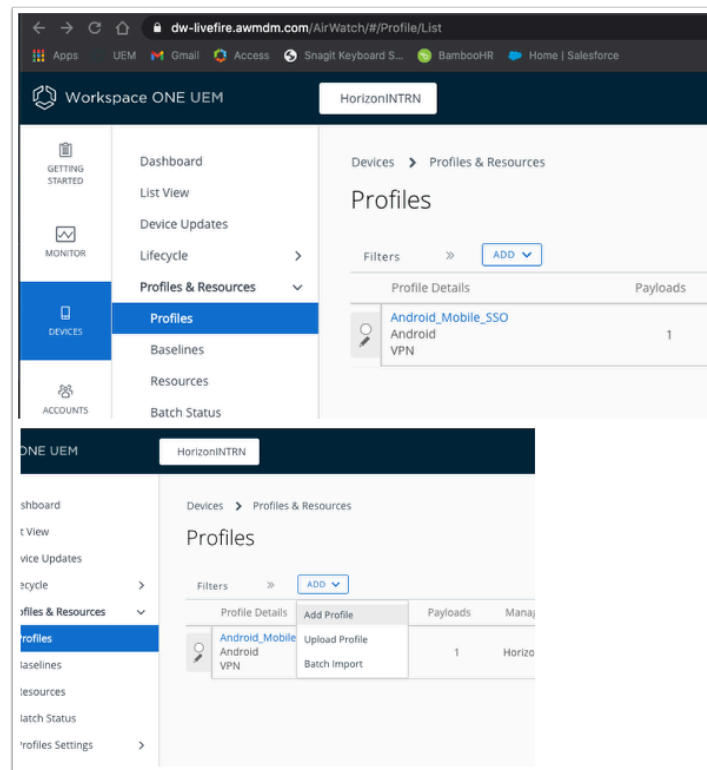
- Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Workspace ONE Access > Configuration**



3. Click **EXPORT** in the **Certificates** section on the **Workspace ONE Access** page

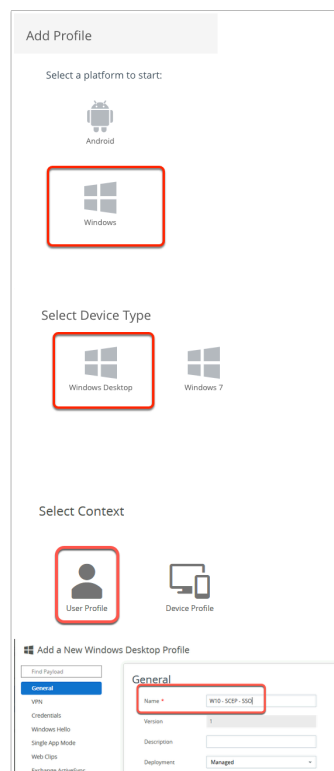
- Note this will download a .cer file (**VidmAirWatchRootCertificate.cer**)

- Select **X** to close the **Settings** window



4. From the UEM Console

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



5. In the Add Profile window

- Select **Windows > Windows Desktop > User Profile**
- Next to **Name*** enter: **W10 - SCEP - SSO** .

Allways
 demale.striteo
 ✱ All Devices (demale.striteo) ✕
 Start typing to add a group 🔍
 NO YES
 VIEW DEVICE ASSIGNMENT

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

General
 VPN
 Credentials
 Windows Hello
 Single App Mode
 Web Clips
 Exchange ActiveSync
 SCEP
 Exchange Web Services
 SCEP
 CONFIGURE

7. Now navigate to the **SCEP** tab on the left menu
 - Select **CONFIGURE**

Add a New Windows Desktop Profile

General

VPN

Credentials

Windows Hello

Single App Mode

Web Clips

Exchange ActiveSync

SCEP ①

SCEP

Credential Source:

Certificate Authority *:

Certificate Template *:

Key Location:

+

−

SAVE AND PUBLISH CANCEL

8. Set the following:

- Credential Source: **AirWatch Certificate Authority**
- Certificate Template: **Single Sign-On**
- Key Location: **Software**
- Click **SAVE AND PUBLISH** at the bottom right of the window

View Device Assignment

Assignment Status:

Assignment Status	Friendly Name	User	Platform/OS/Model	Phone Number	Organization Group
Added	User35ANL Desktop Windows Desktop 1...	User35ANL	Windows Desktop / Windows 10 (10.0.18363) ...		HorizonRTRN

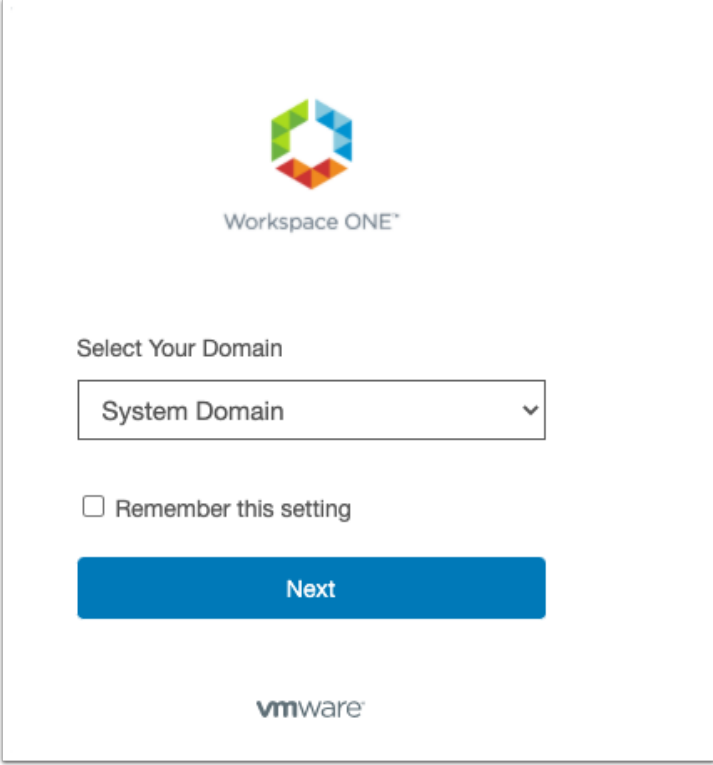
Items: 1-1 of 1

Page Size: 20

PUBLISH CANCEL

9. Confirm your device is shown in the **View Device Assignment** page
 - Select **PUBLISH**

Part 2 : Configure Workspace ONE Access



Workspace ONE™

Select Your Domain

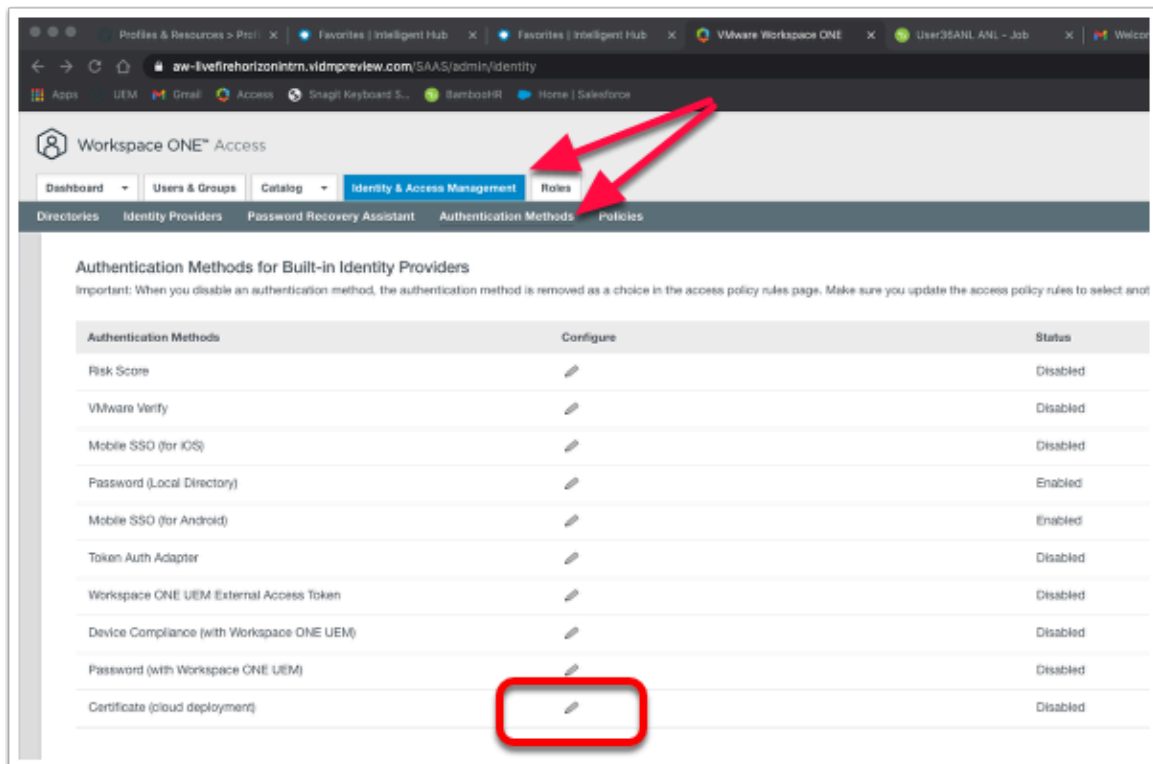
System Domain ▼

☐ Remember this setting

Next

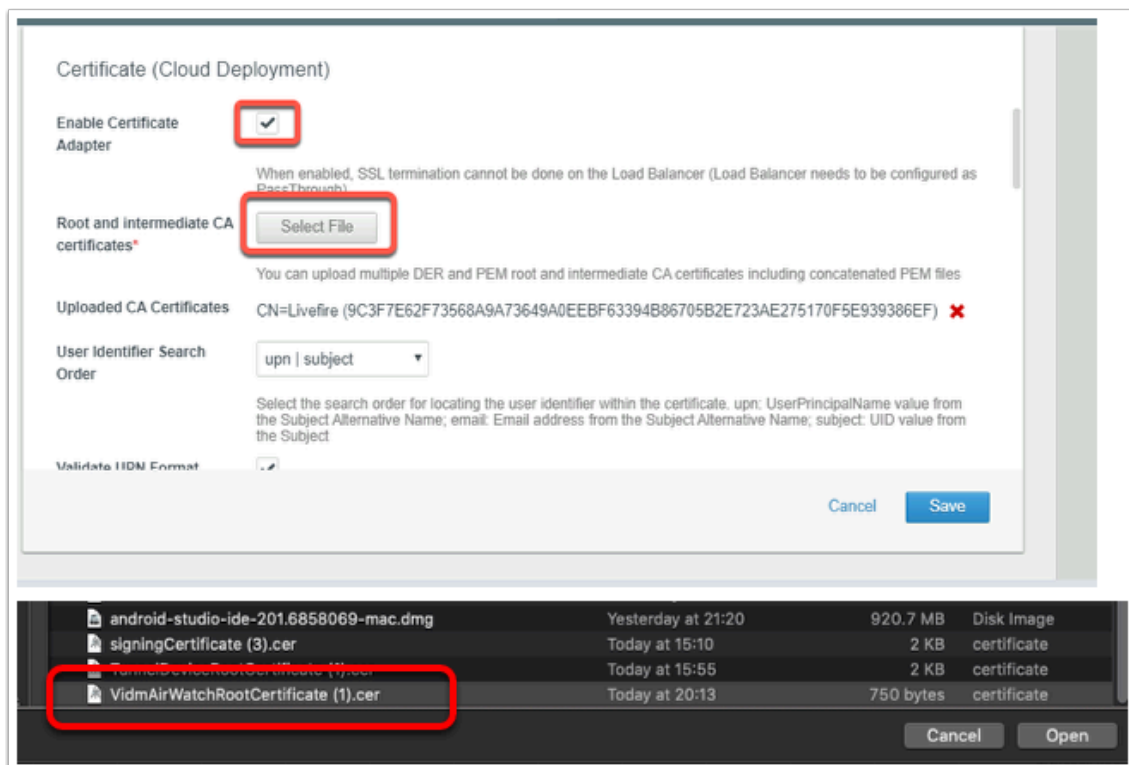
vmware™

1. Switch to your custom SaaS **Workspace ONE Access** tenant
 - If necessary, authenticate as **System Domain**, select **Next**
 - Sign in with your Admin credentials for your SaaS Tenant



2. In the Access admin console

- Navigate to **Identity & Access Management > Authentication Methods**.
- Select the **pencil icon** next to **Certificate (Cloud Deployment)**




3. In the **Certificate (Cloud Deployment)** page click the **tickbox** to **Enable Certificate Adapter**

- Click **Select File** for the **Root and Intermediate CA Certificates**
- Select the **certificate** (VIDMAirWatchRootCertificate.Cer) we have downloaded from the UEM console earlier and
- Select **Open**


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

Cancel OK

Certificate (Cloud Deployment)

certificates* 

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

Uploaded CA Certificates CN=Livefire (9C3F7E62F73568A9A73649A0EEBF63394B86705B2E723AE275170F5E939386EF) 

User Identifier Search Order upn | subject


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

Validate UPN Format ☒

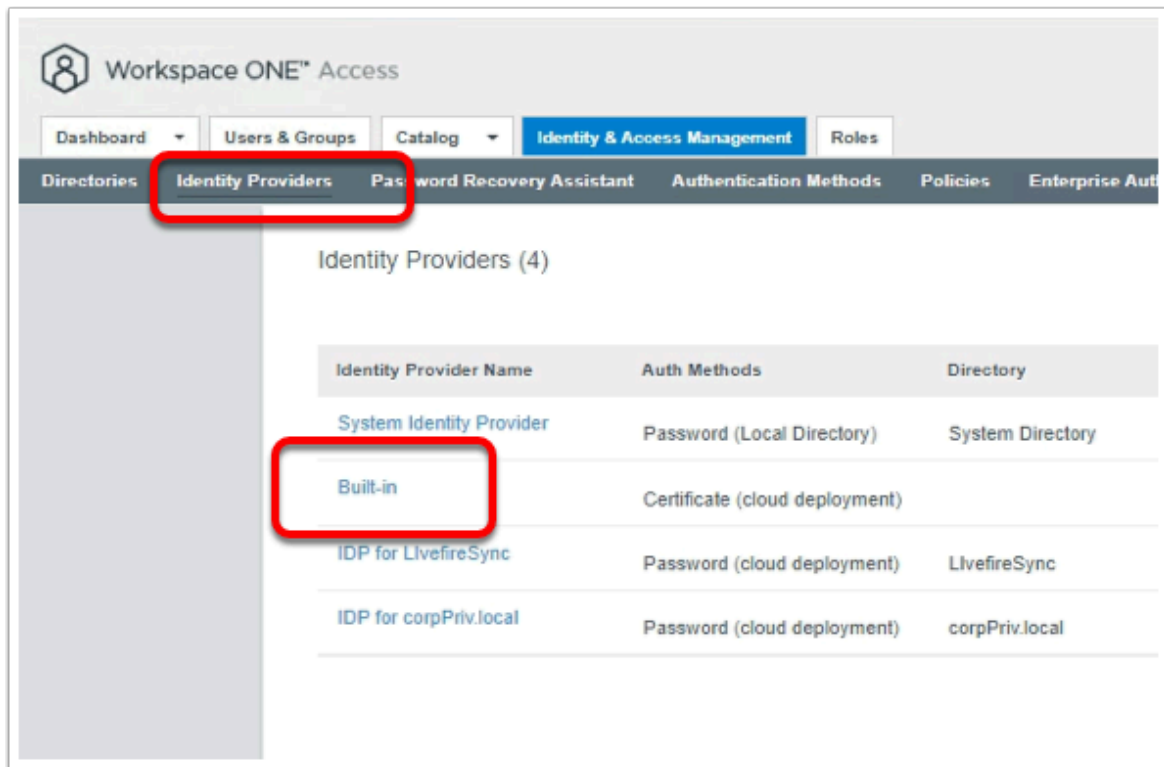
Validate the format of the UserPrincipalName field

Request Timeout

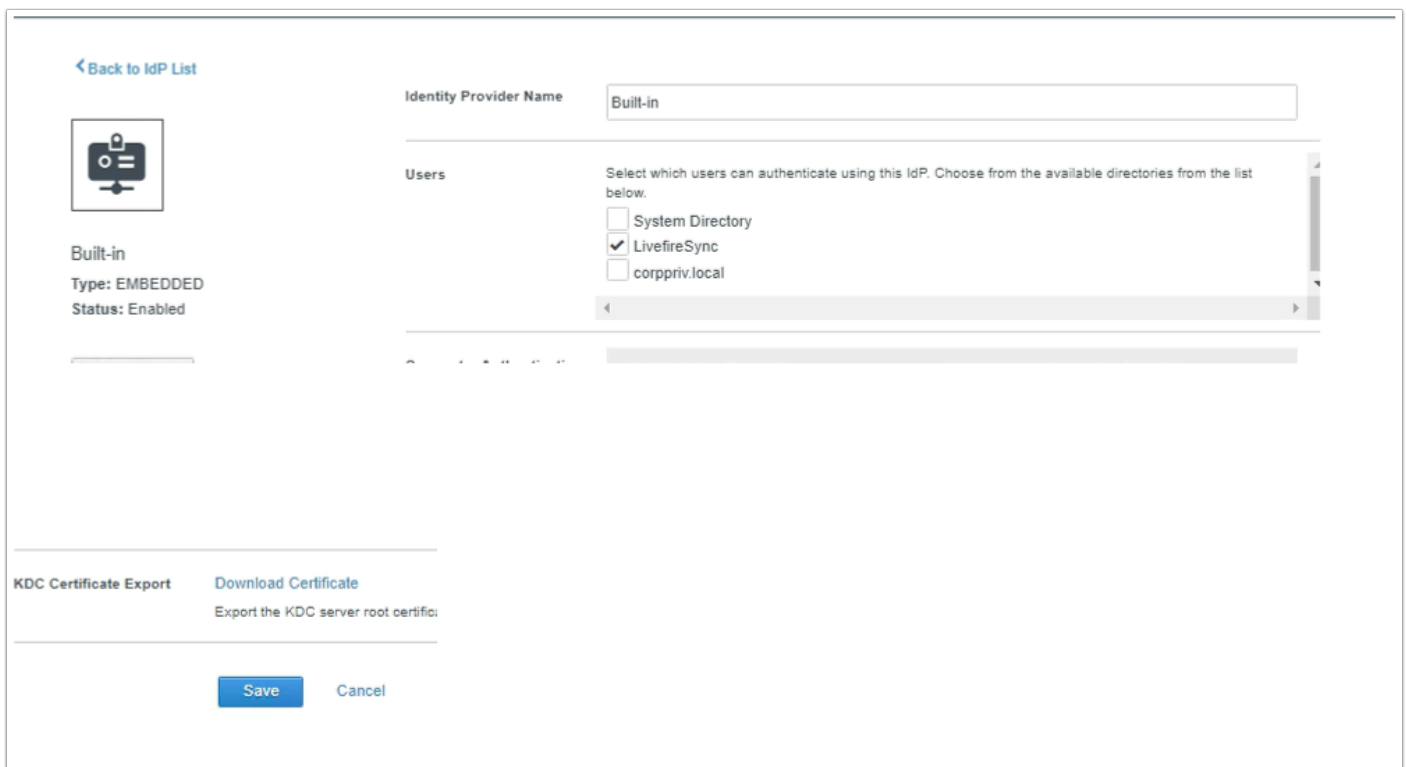
Timeout in seconds to wait for a response. A value of zero will wait indefinitely.

Cancel 

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

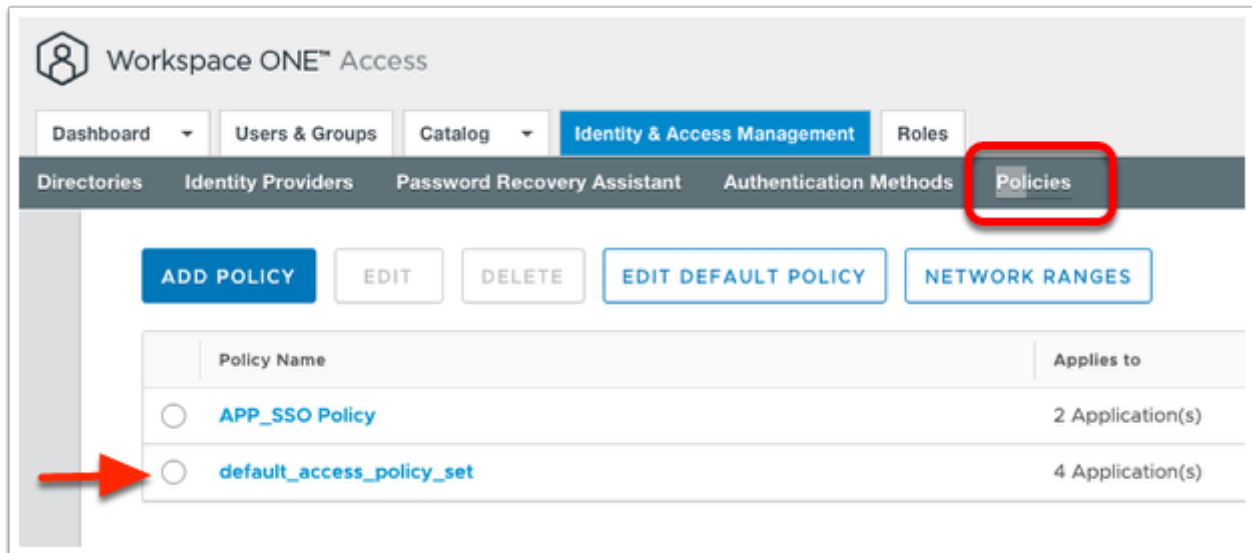


5. In the Workspace ONE Access Console
 - Under **Identity & Access Management**
 - Select **Identity Providers**
 - Select **Built-in**

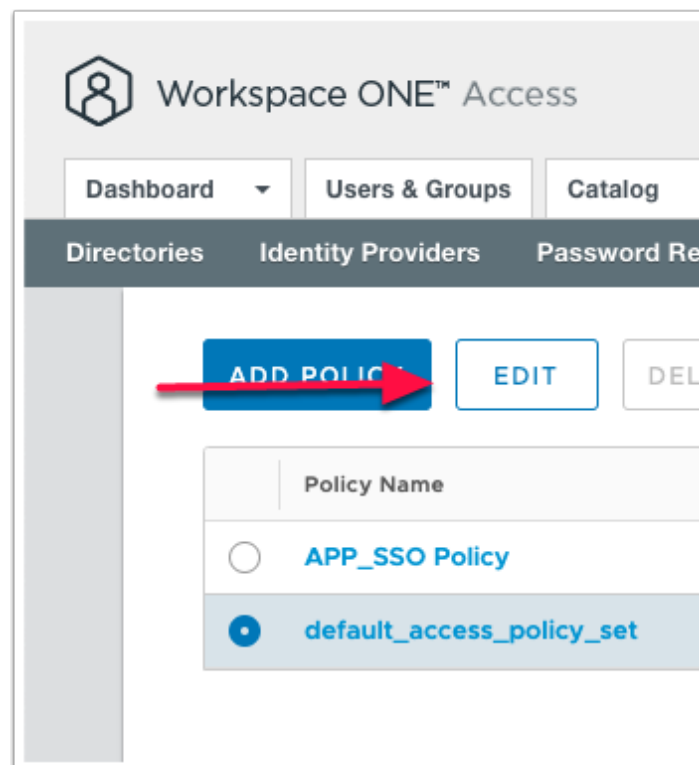


6. In the **Built-In** Identity Providers window

- In the Users area
 - Notice checkbox for **LivefireSync** is select but not **corpriv.local**
 - Select the **checkbox** next to **corpriv.local**
- In the Authentication Methods area
 - Select the **checkbox** next **Certificate (cloud deployment)**
- Select **Save** at the bottom of the page.



7. In the Workspace ONE Access Admin console
 - Navigate to **Identity & Access Management > Policies**
 - Select the **radio button** next to **default_access_policy_set**



8. In the Policies area

- Select **EDIT**

Edit Policy

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

Network Range	Device Type
:: ALL RANGES	Web Browser
:: ALL RANGES	Workspace ONE App ...

+ ADD POLICY RULE

9. In the **Edit Policy** window,

- Select, the second header, from the left column **Configuration**
- Select **All Ranges** next to **Web Browser**,

< CONFIGURATION

Edit Policy Rule

If a user's network range is • ALL RANGES

and the user accessing content from • Web Browser

and user belongs to group(s) Select Groups...

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

Then perform this action Authenticate using...

then the user may authenticate using • Certificate (cloud deployment)

If the preceding method fails or is not applicable, then Password (cloud deployment)

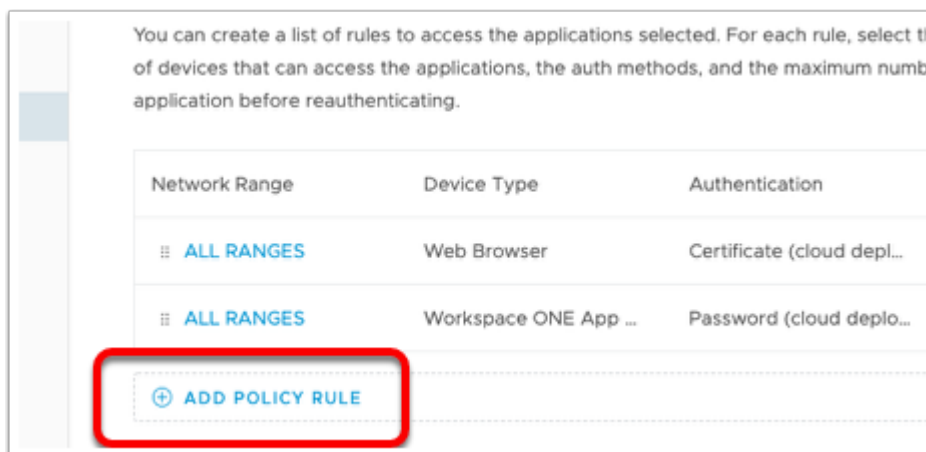
If the preceding method fails or is not applicable, then Password (Local Directory)

+ ADD FALLBACK METHOD

CANCEL SAVE

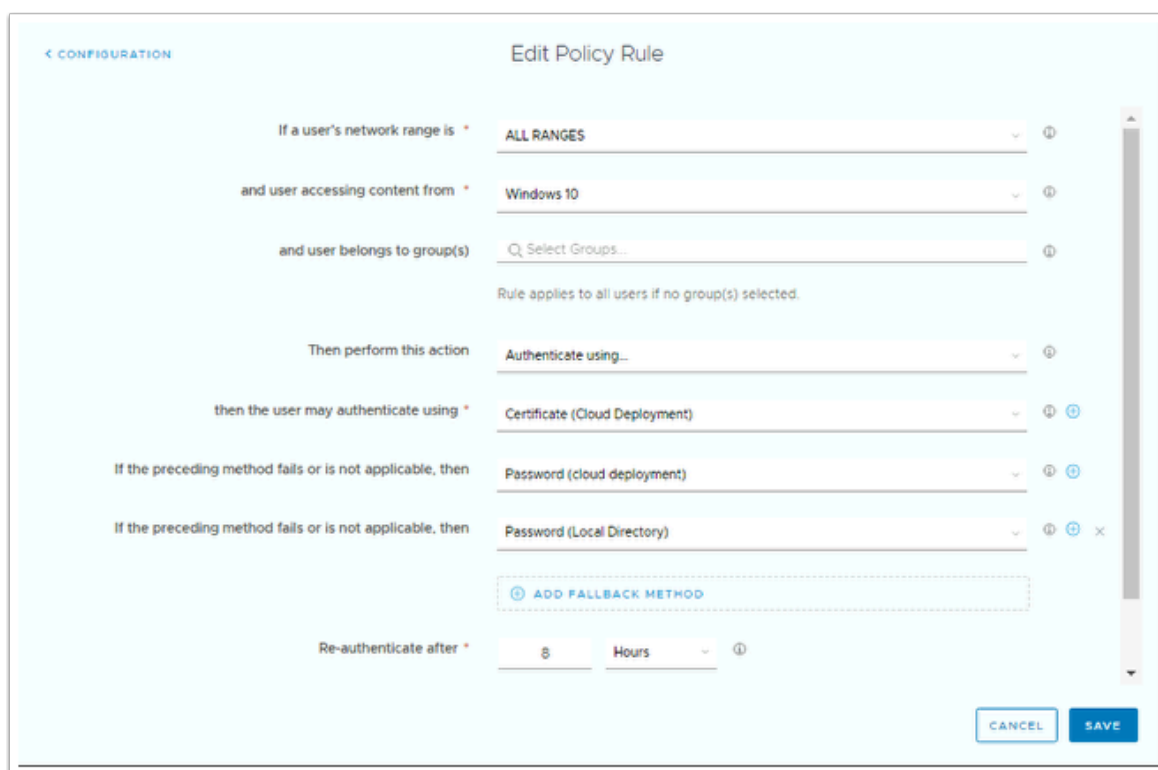
10. In the **Edit Policy Rule** window

- Next to **then the user may authenticate using *** to select **Certificate (Cloud Deployment)**
- Next to **if preceding method fails or is not applicable, then *** select **Password (Cloud Deployment)**,
- Select **ADD FALLBACK METHOD**
- Next to **if preceding method fails or is not applicable, then *** select **Password (Local Directory)**
- Select **SAVE** at the bottom of the window



11. In the **Edit Policy Rule** window

- Select **ADD POLICY RULE**



12. Select **Windows 10** from the **user accessing content** from drop down.

- Select **Certificate (Cloud Deployment)** for the first authentication method

- Select **Password (cloud deployment)** for **if the preceding method fails ...**
- Select **Password (Local Directory)** for **if the preceding method fails ...**
- Click **SAVE** at the bottom right hand side of the page

Network Range	Device Type
ALL RANGES	Workspace ONE App ...
ALL RANGES	Web Browser
ALL RANGES	Windows 10

+ ADD POLICY RULE

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

Edit Policy

1 Definition
2 Configuration
3 Summary

Definition

Name
default_access_policy_set

Description
Default access policy set

Applications
4 Application(s)

Configuration

Policy Rule 1
If a user's network range is **ALL RANGES**
and the user is accessing content from **Windows 10**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **Certificate (cloud deployment)**

Fallback method 1: **Password (cloud deployment)**
Fallback method 2: **Password (Local Directory)**
Re-authenticate after **8 hour(s)**

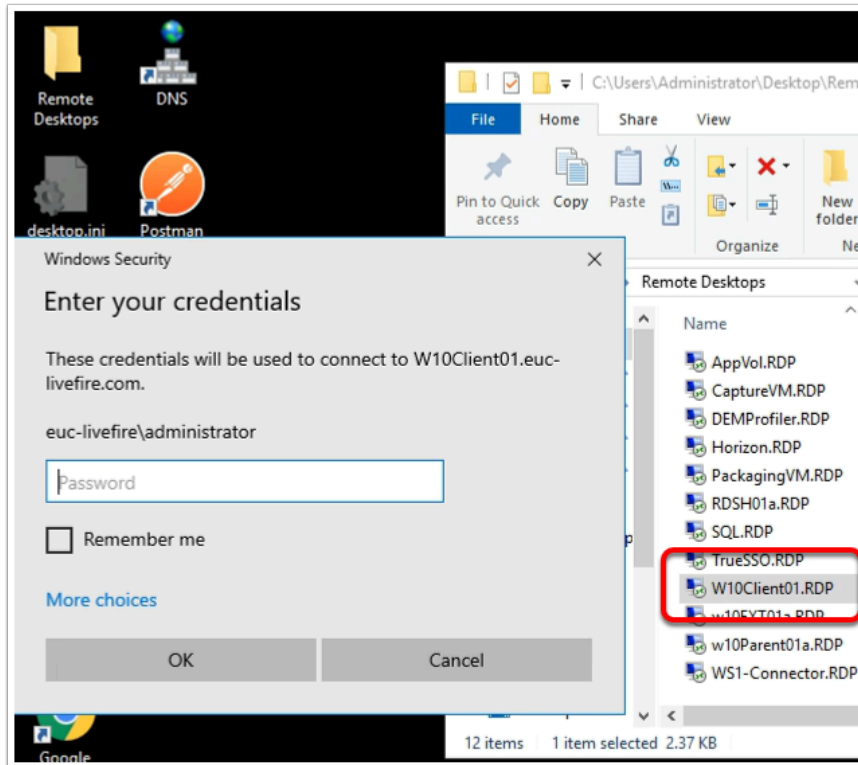
[Advanced Properties](#)

Policy Rule 2
If a user's network range is **ALL RANGES**
and the user is accessing content from **Web Browser**

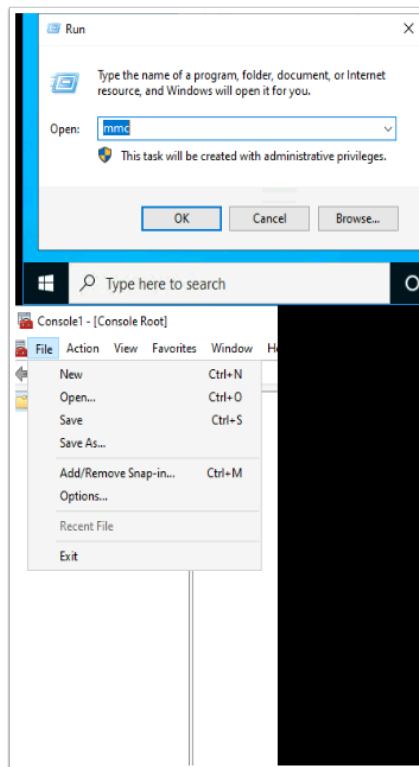
CANCEL BACK SAVE

14. Select **SAVE** on the Summary tab of the **Edit Policy** Page.
 - You have now enabled Certificate (Cloud Deployment) as an authentication method on the default access policy.
 - Our next step is to ensure this implementation is working.

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

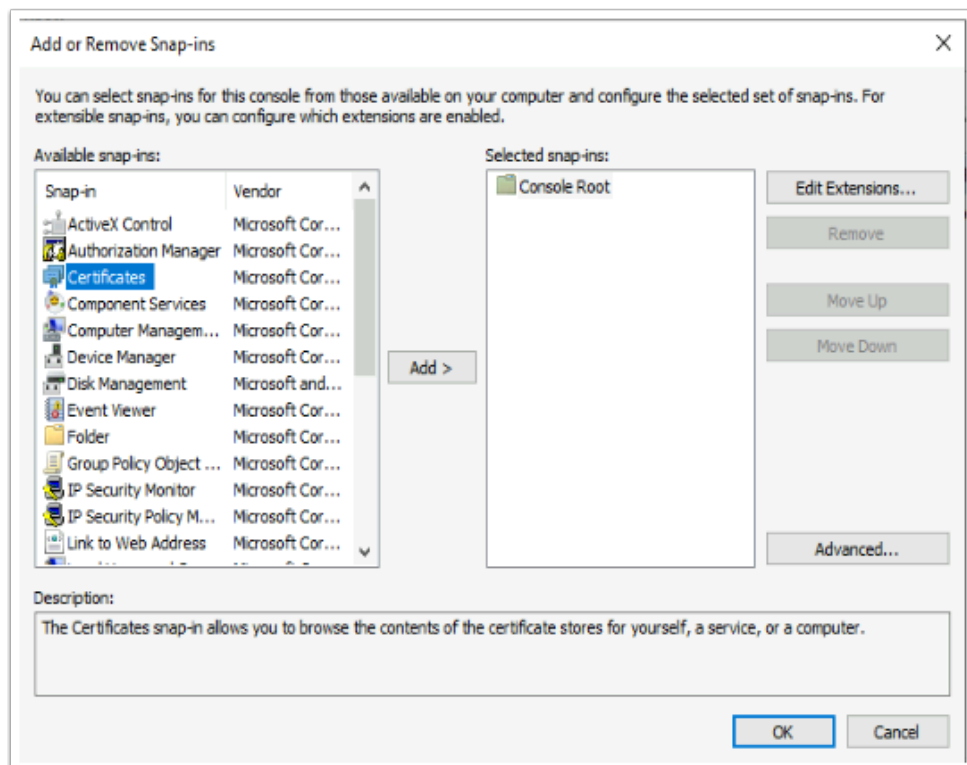


1. On the **ControlCenter** server Desktop,
 - Open the **Remote Desktops** folder,
 - Select the **W10Client01.RDP** shortcut
 - Log in as **EUC-Livefire\administrator**, enter the password **VMware1!**,
 - Select **OK**



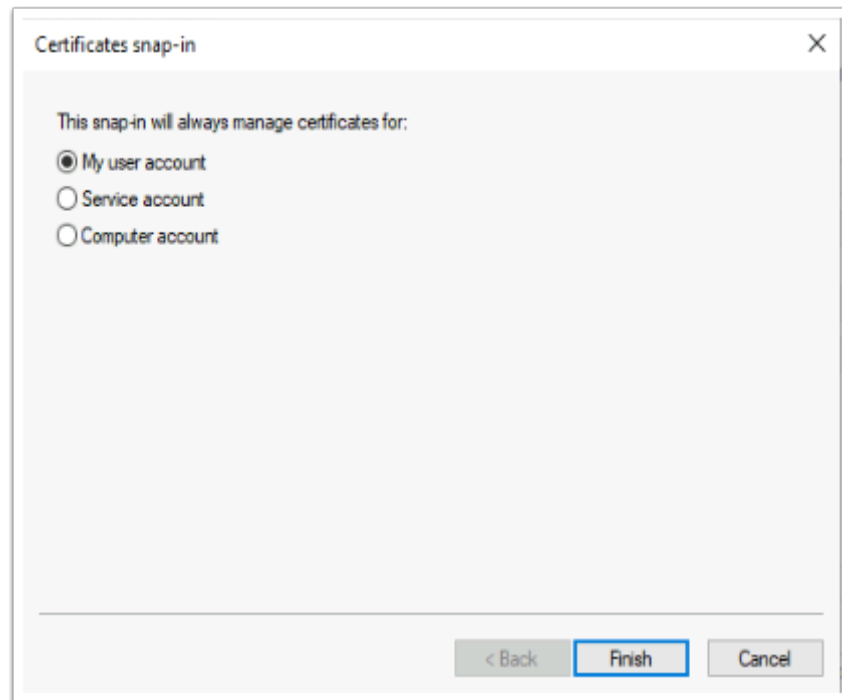
2. On **W10Client01** desktop

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



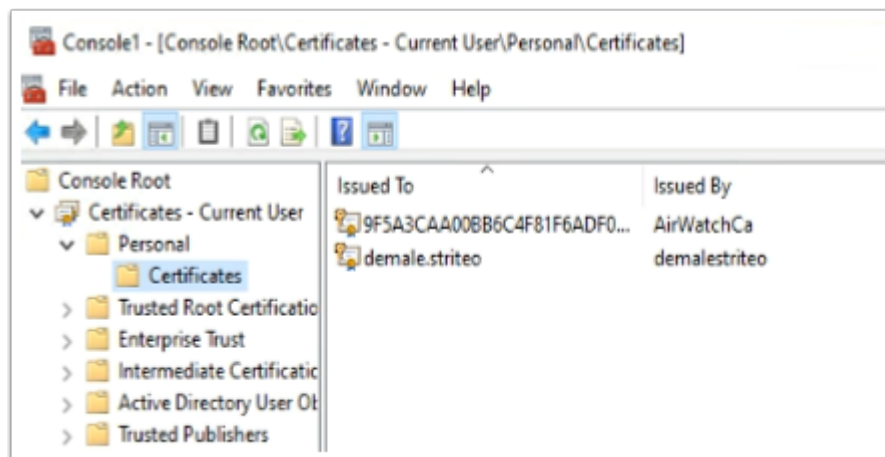
3. In the **Add or Remove Snap-ins** window

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



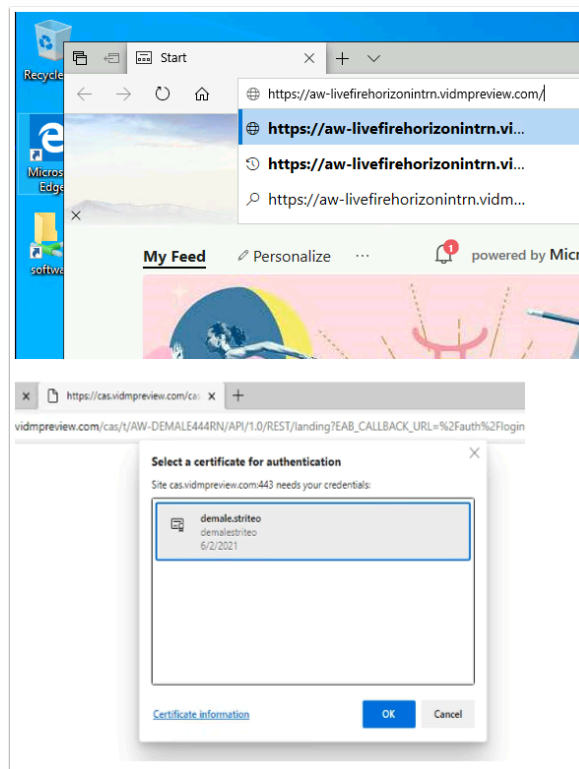
4. In the **Certificates snap-in**, accept the Defaults, select **Finish**

- Select **OK**

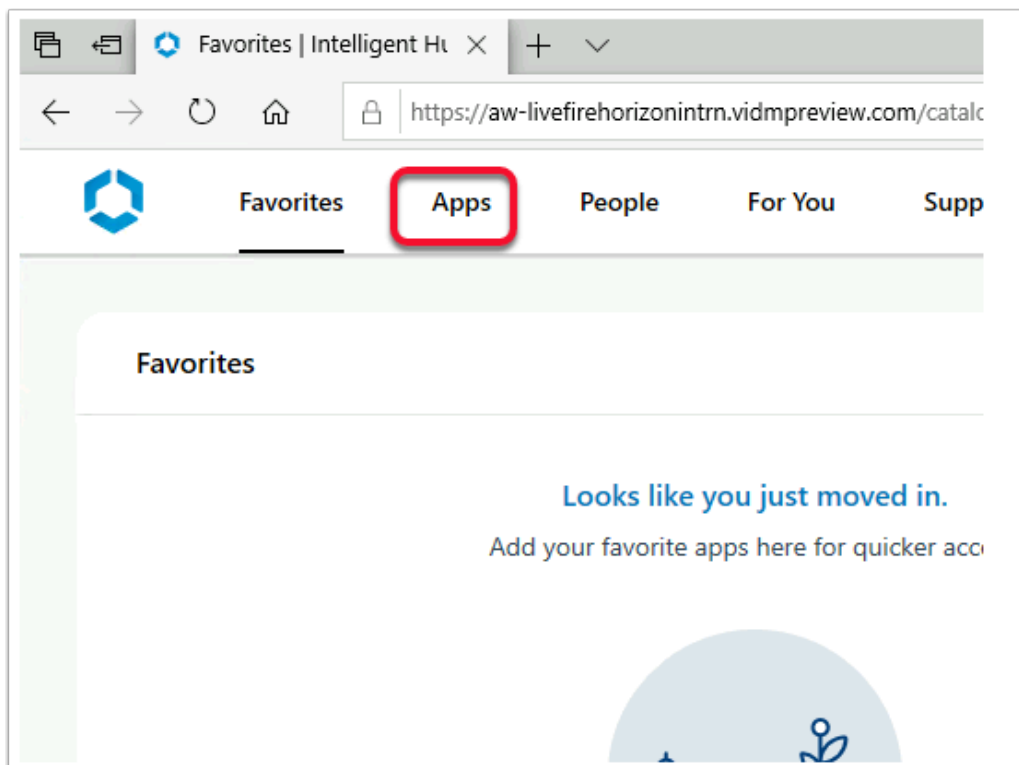


5. **Expand Certificates - Current User**

- **Expand Personal**
- Select **Certificates**
 - Note you have an enrolled certificate. If you don't have a certificate, reach out for support.

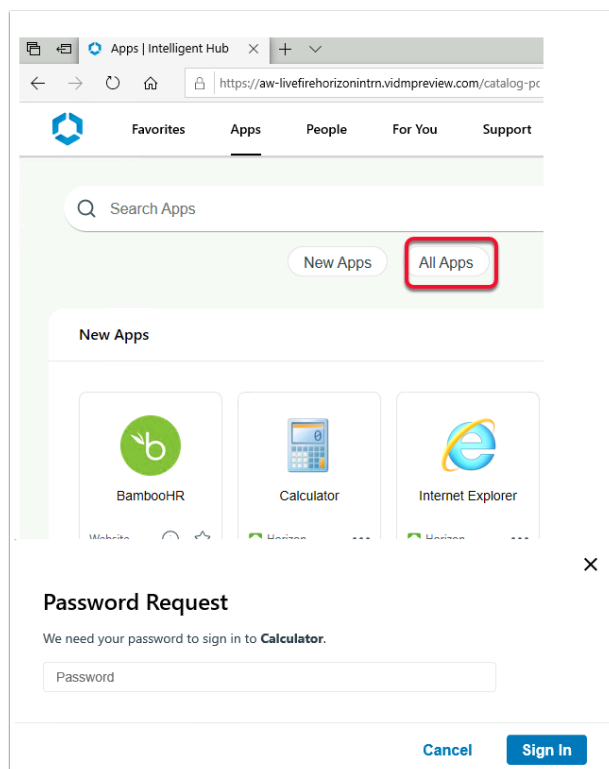


6. On your **W10Client01** Desktop
 - Open a **browser** on your windows 10 desktop
 - In the address bar enter the **URL of your SaaS Access Tenant**
 - On the **Select a certificate** window note the account of the certificate
 - Select **OK**



7. On the **Workspace ONE** console ,

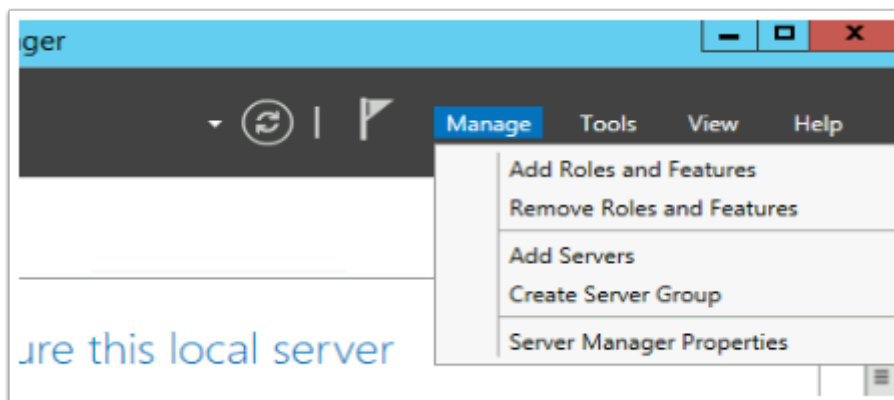
- Select the **Apps** tab



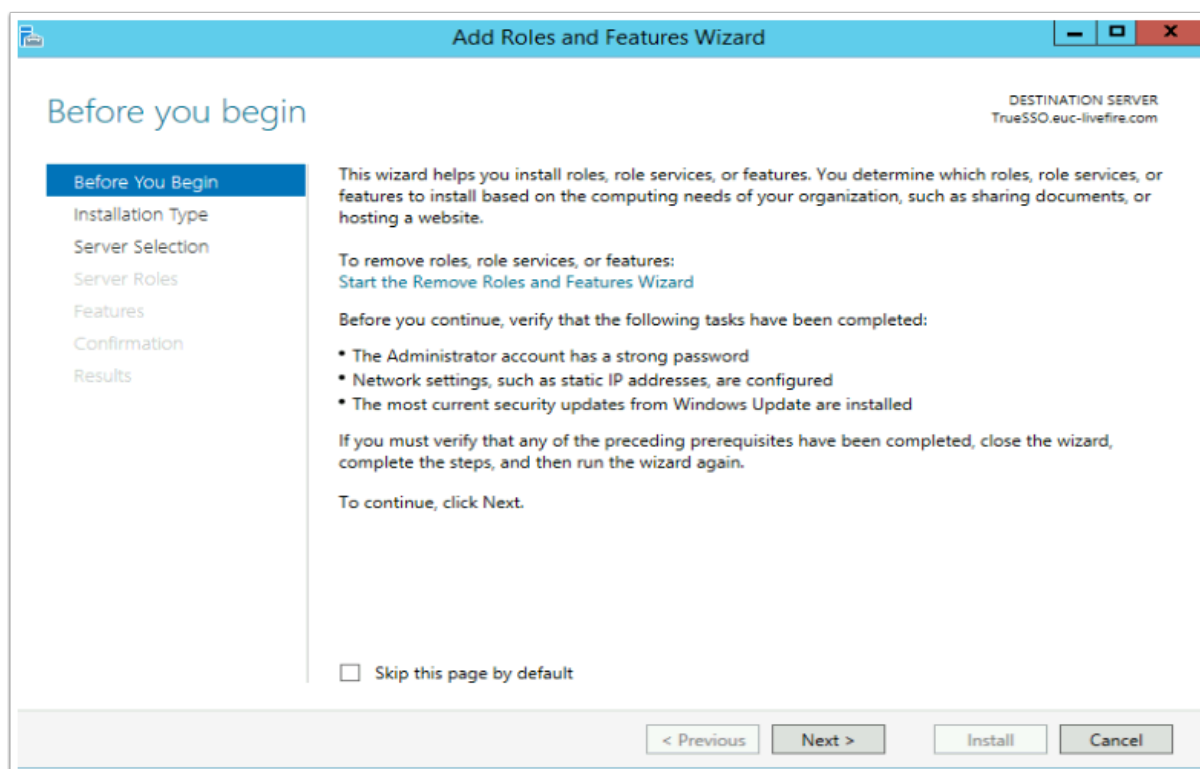
8. Select **Calculator**,

- Notice we are getting a Password request.
 - The 1st reason is, we used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password Auth method, to pass on to the Horizon Agent.
 - Up to version 1903, Workspace ONE Access would CACHE the credential when a password method of Authentication was used to login to the Console. Prior to version 20.01 or up to version 1903, when a user logged into Workspace ONE Access with a password method of authentication, the user would enjoy a Single-Sign on experience. It was therefore only necessary to Deploy TRUESSO if the users were authenticating with an Auth method that was NOT password based.
 - From version 20.01 SaaS onwards, the automatic CACHING of password credentials is no longer a feature in Workspace ONE Access. This is an enhancement of Workspace ONE Access security.
 - In June this year a feature was re-introduced to allow Automatic Caching of Passwords on the SaaS Instance of Access
 - We however still need Enrollment services when authenticating with 3rd party auth methods
- In the next Part, we will proceed with the deployment of TRUESSO to solve this challenge.
- Select **Cancel** to close the **Password Request** window.
- **Logout** and **close** all windows on **W10Client01**

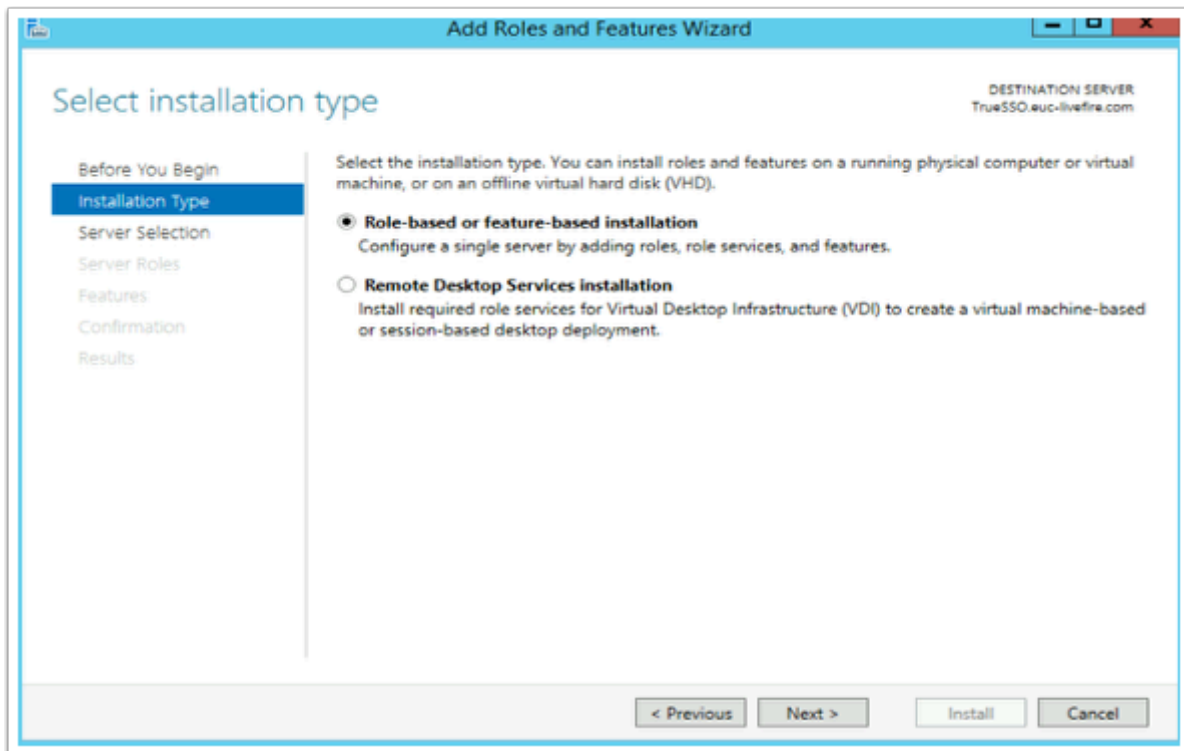
Part 4. Installing a sub-ordinate CA and the Enrollment services



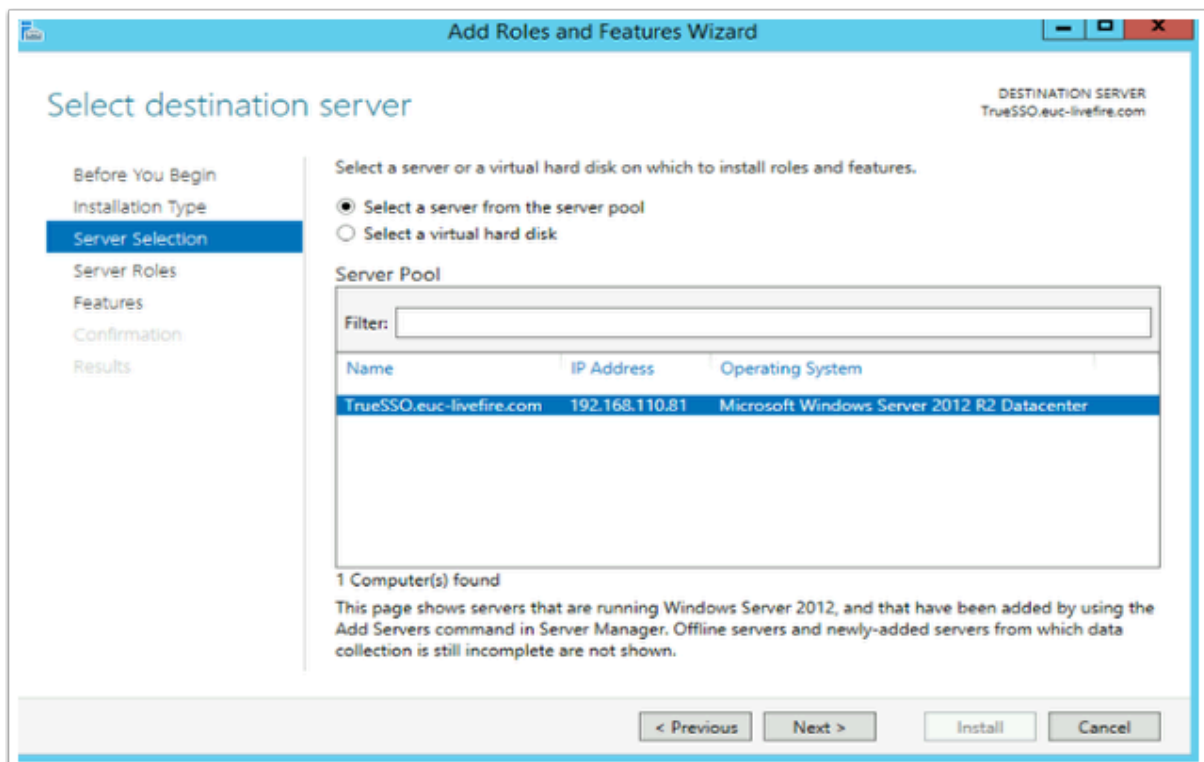
1. On your **ControlCenter** server
 - Open the **Remote Desktop** Folder
 - Launch **TrueSSO.RDP** shortcut
 - Login as **Euc-livfire\administrator** and enter the password **VMware1!**
 - On the **Server Manager** Interface select **Manage** > **Add Roles and Features**



2. On the **Before you begin** window
 - Select **Next**

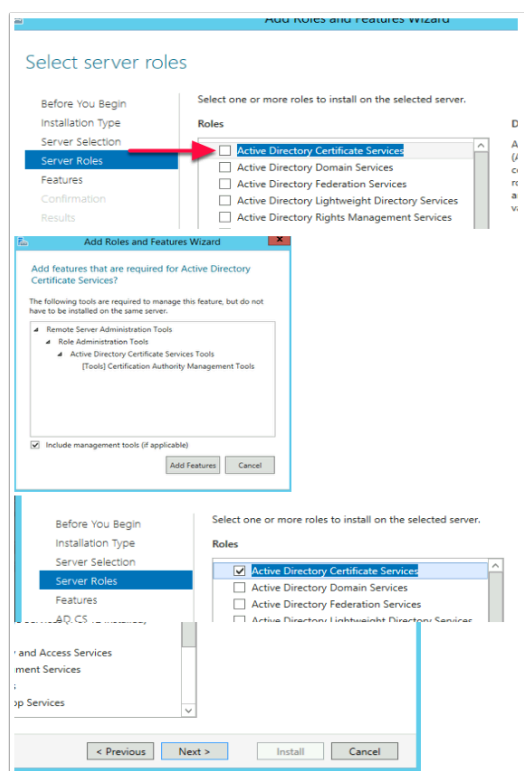


3. On the **Select installation type** window,
 - Ensure the **radio button** in front of **Role-based or feature-based installation** is selected
 - Select **Next**



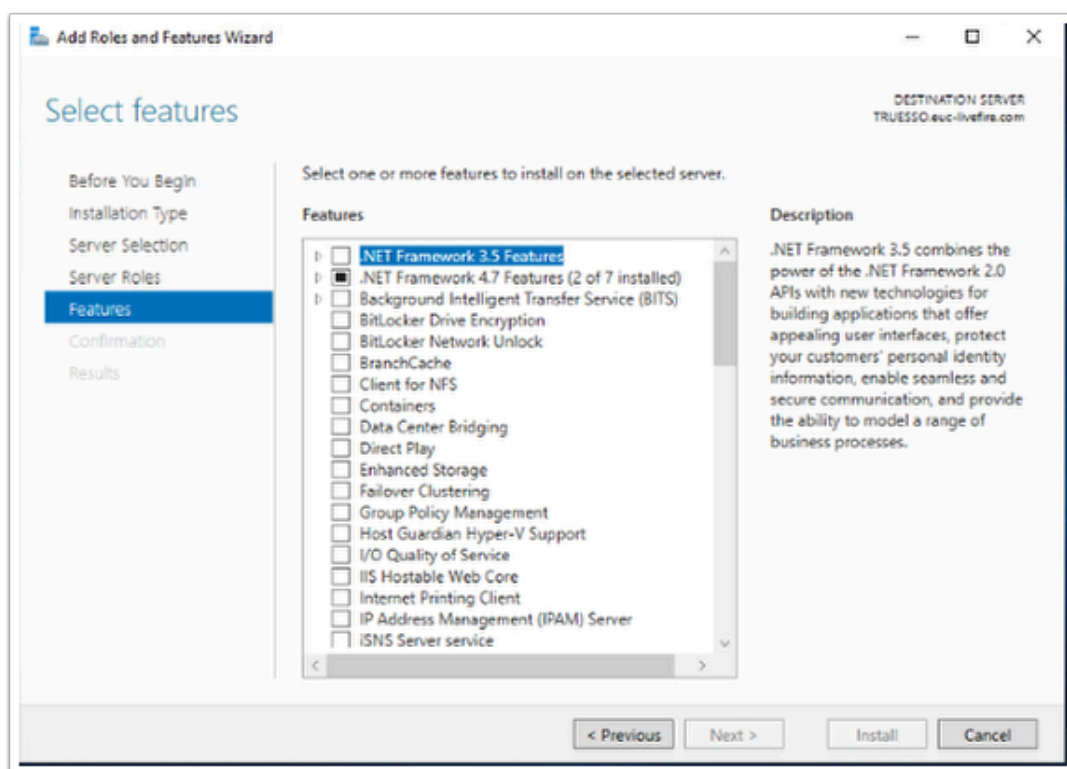
4. On **Select destination server** window (accept the defaults)

- Select **Next**



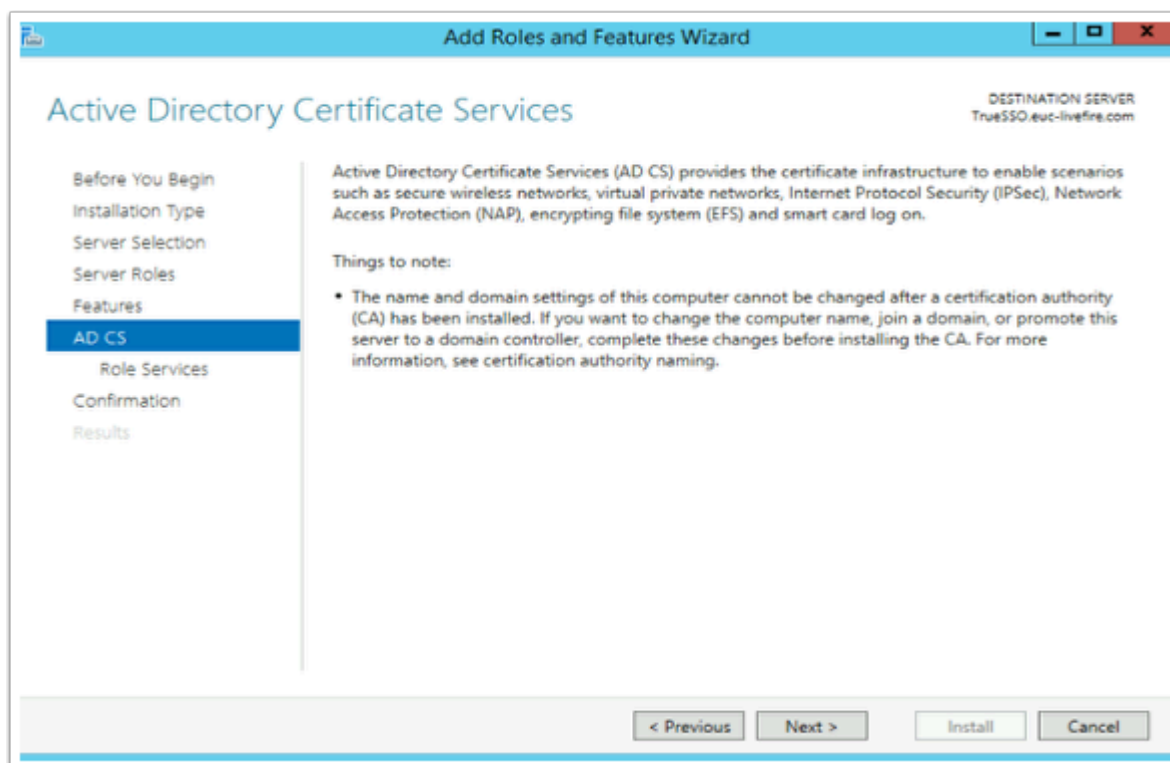
5. On the **Select server roles** window,

- 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**



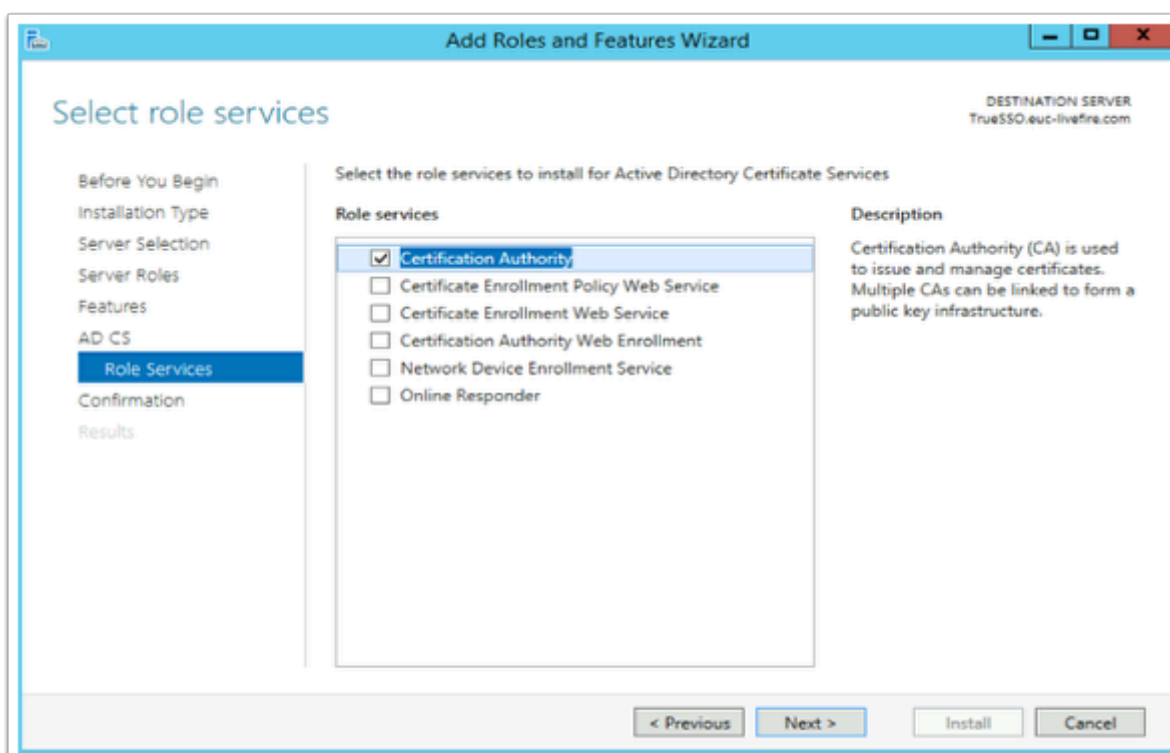
6. On the **Select features** window

- Select **Next**



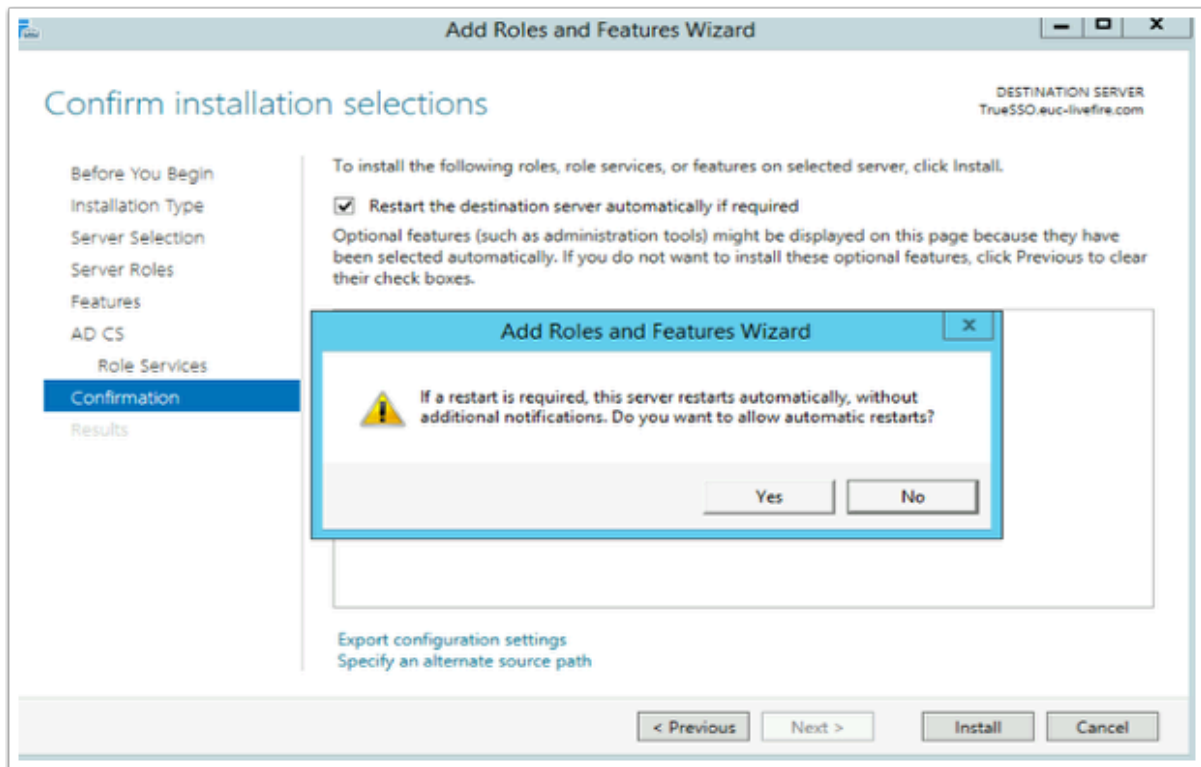
7. On the **Active Directory Certificate Services** window

- Select **Next**



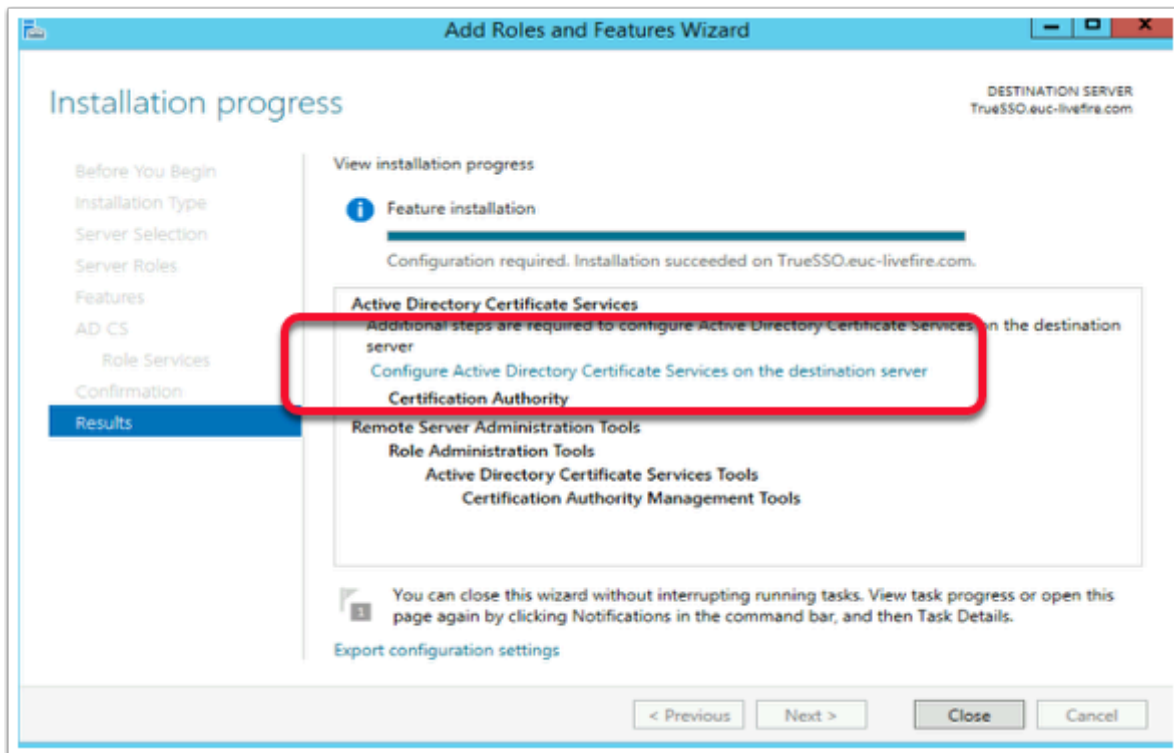
8. On the **Select role services** window

- Select **Next**

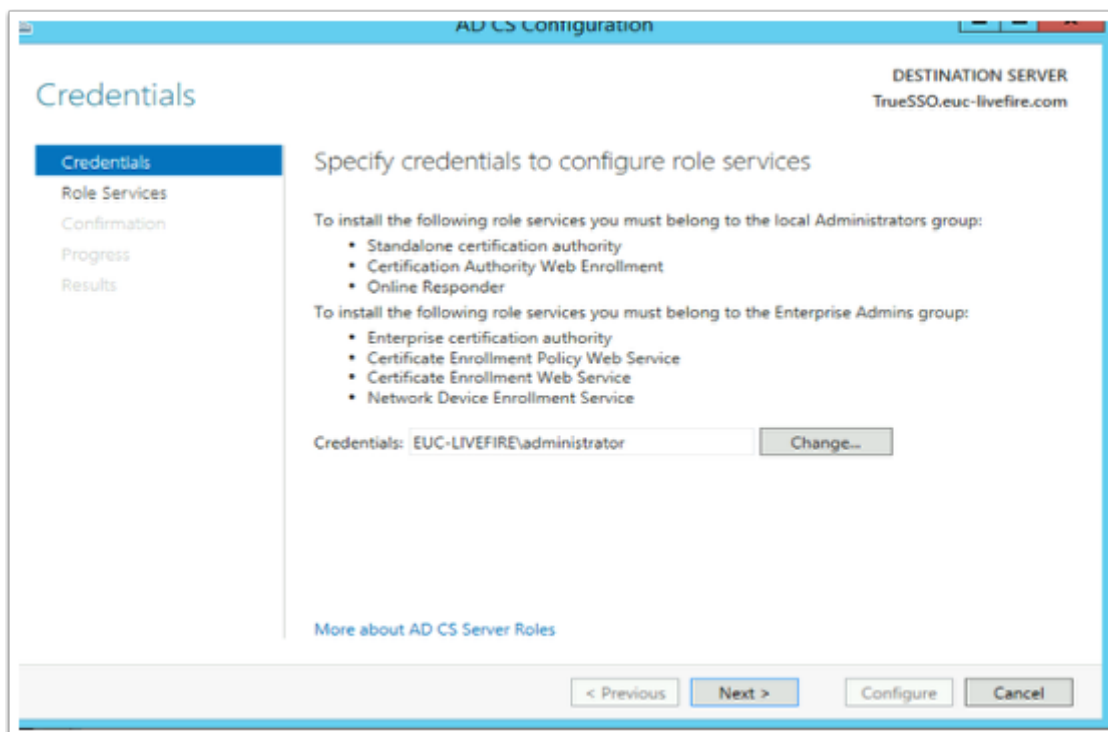


9. On the **Confirm Installation selections** window,
- Select the **checkbox** next to **Restart the destination server automatically if required**,
 - On the **Add Roles and Features Wizard** window select **Yes**
 - Select **Install**

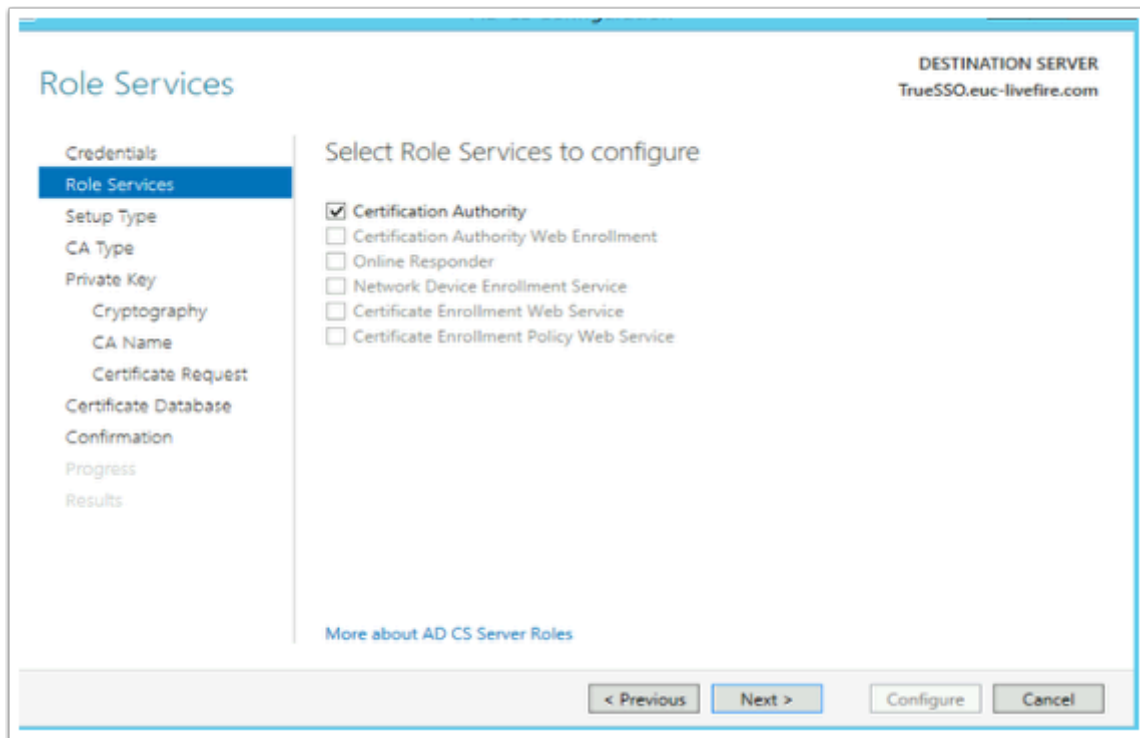
You will have to wait a short while before moving on to step 10



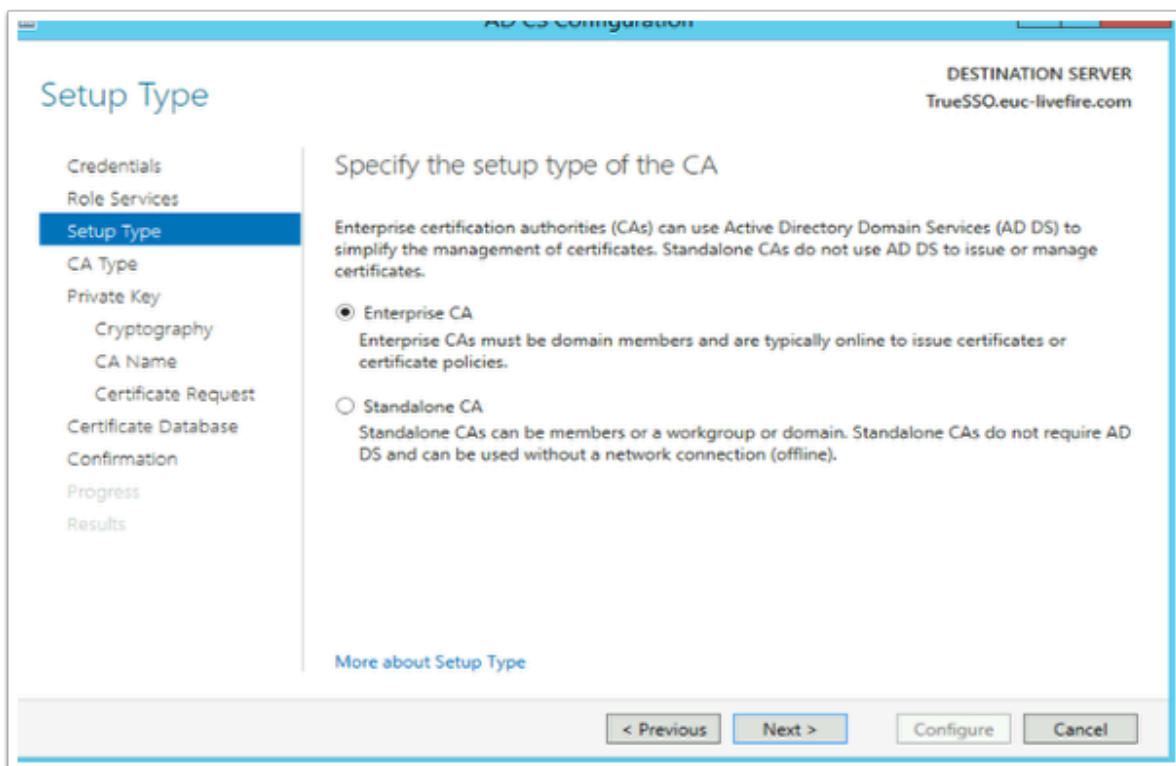
10. On the **Installation progress** page,
 - Select the **Configure Active Directory Certificate Services on the destination server** hyper-link



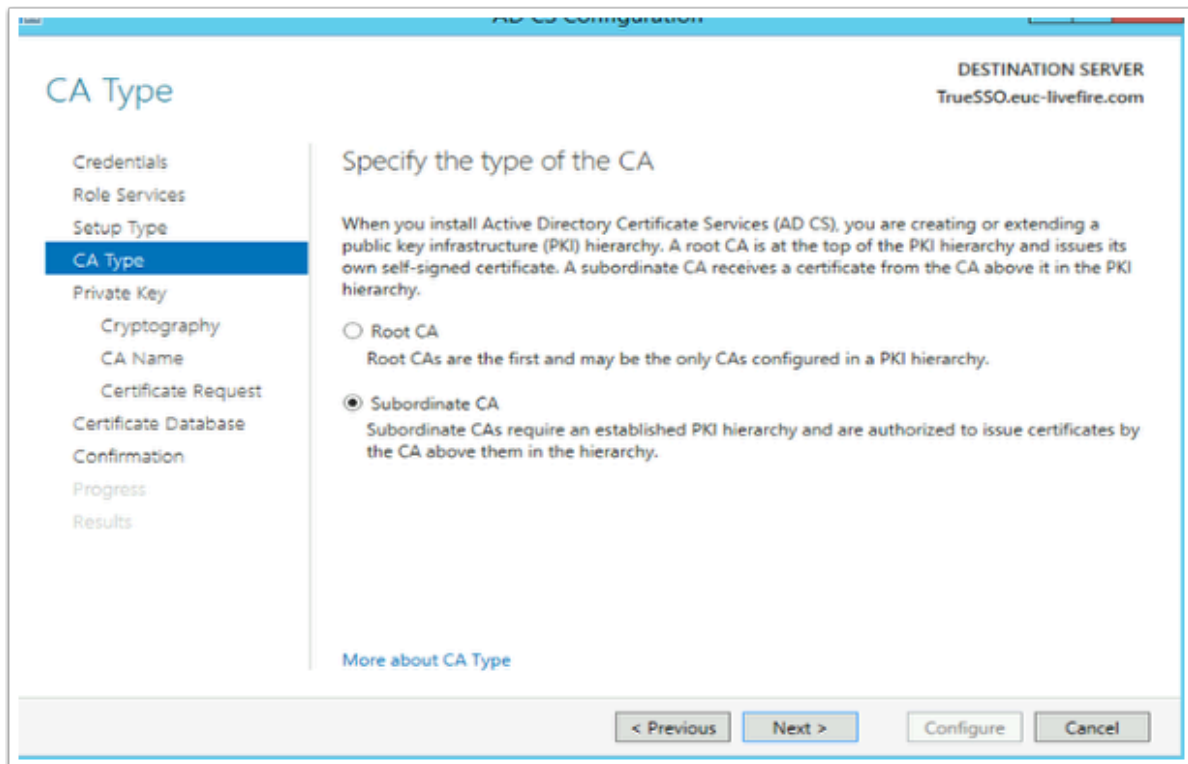
11. On the **Credentials** window
 - Select **Next**



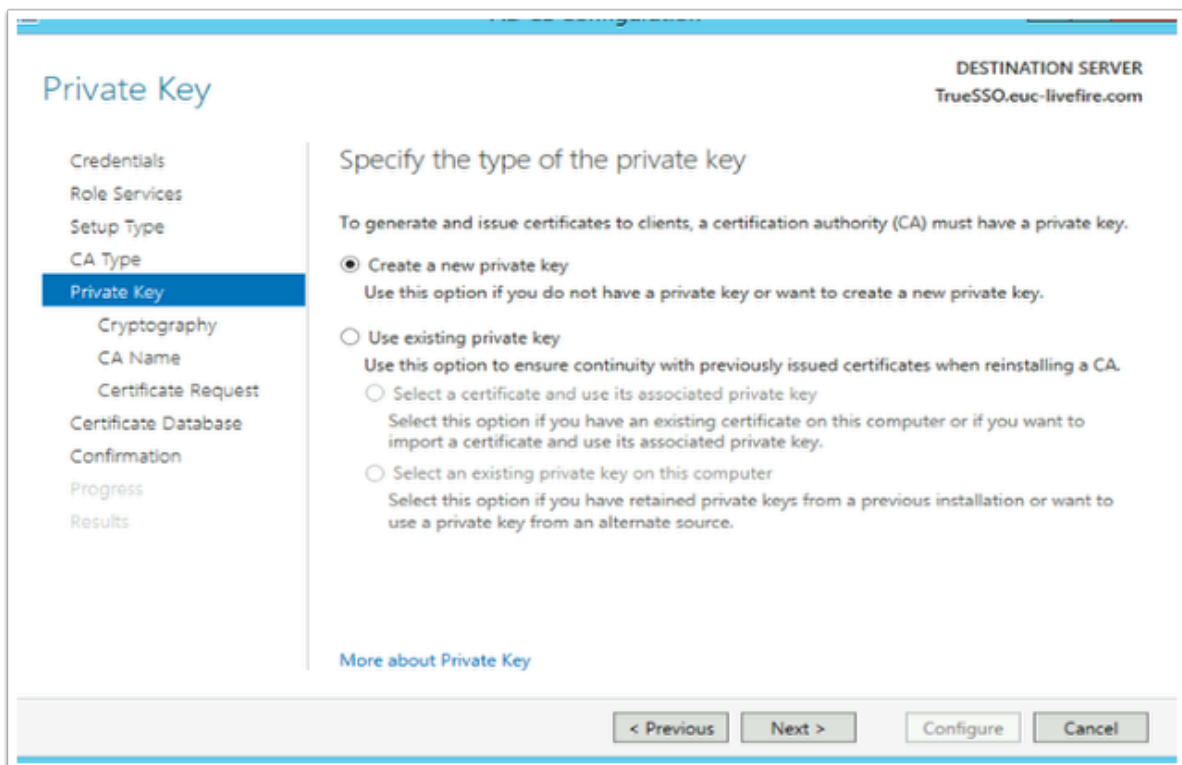
12. On the **Role Services** page,
 - Select the **Certificate Authority** checkbox
 - Select **Next**



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

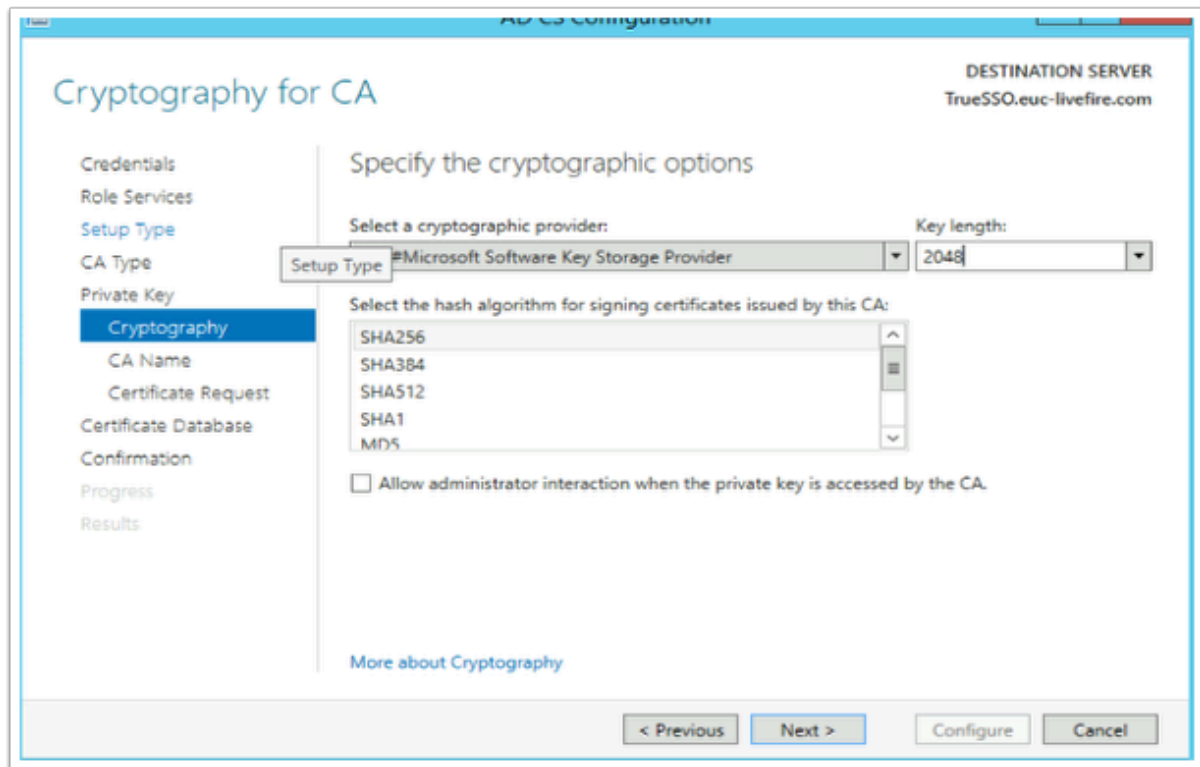


14. On the **CA type** window
- Ensure the **Subordinate CA** radio button is selected,
 - Select **Next**

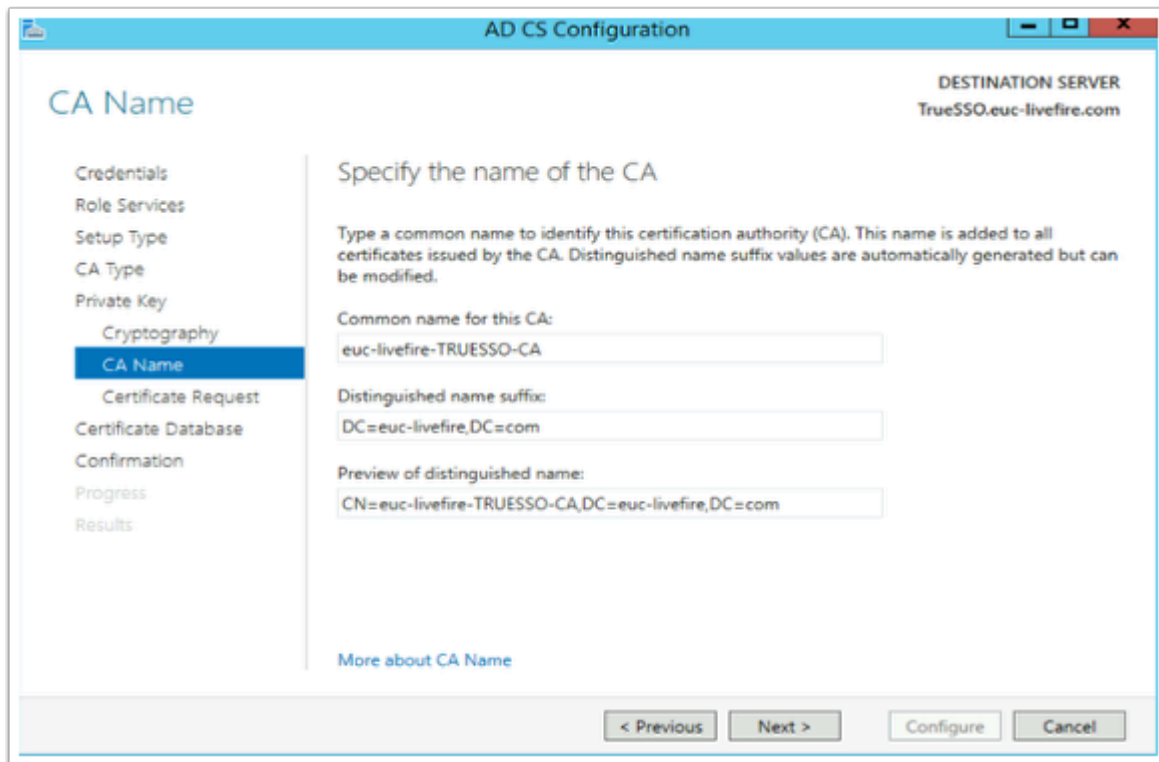


15. On the **Private Key** window,
- Ensure the radio button next to **Create a new private key** is selected

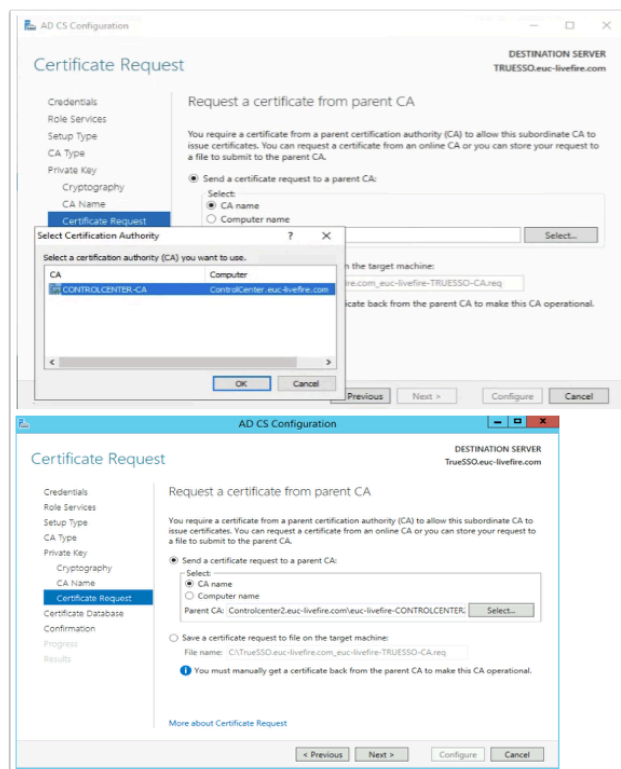
- Select **Next**



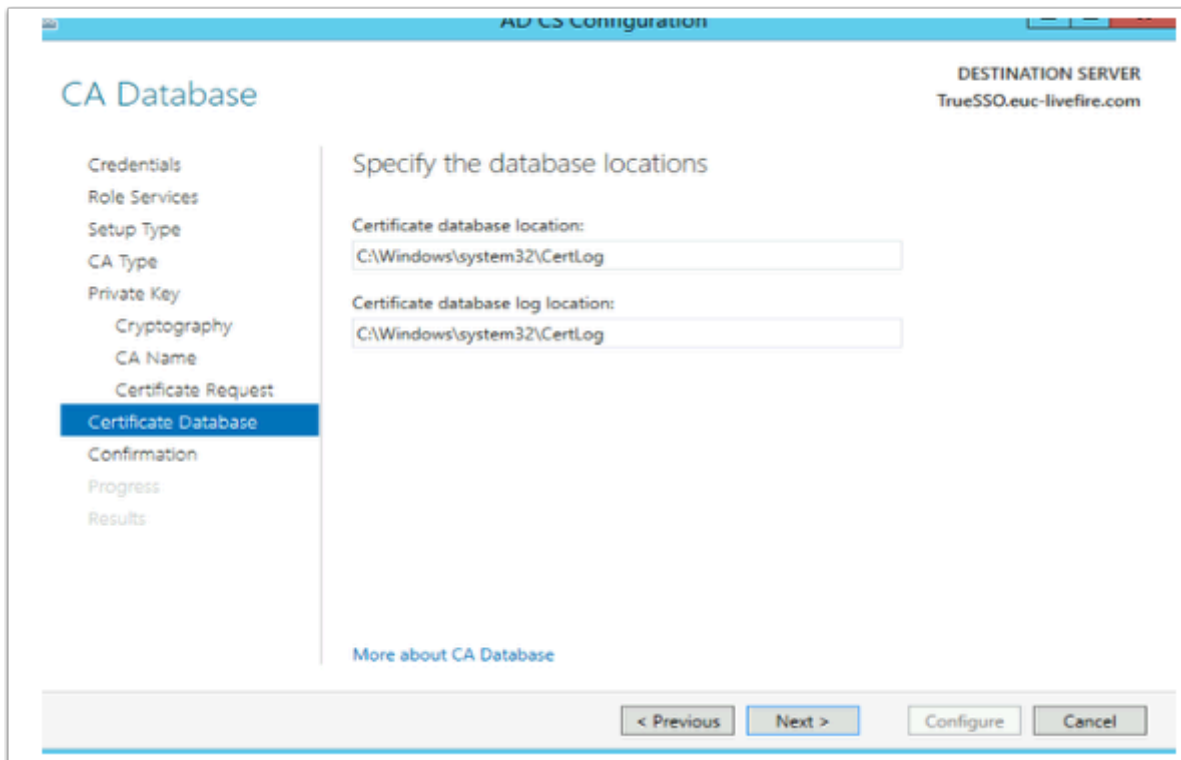
- On the Cryptography for CA window select the following
 - Under **Cryptographic Provider:** **RSA#Microsoft Software Key Storage Provider**
 - Next to **Key Length:** **2048**
 - **Hash Algorithm:** **SHA256**
- Select **Next**



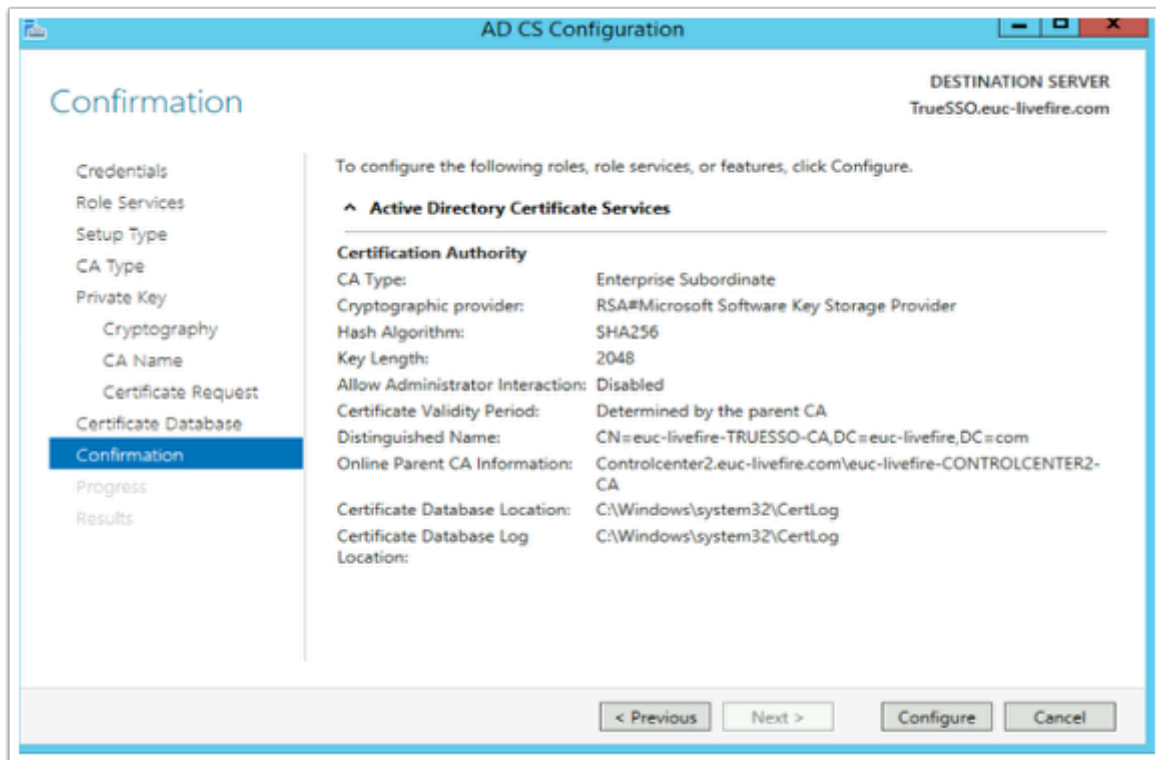
17. On the **Specify the Name of the CA** window
 - Observe the CA naming convention
 - Select **Next**



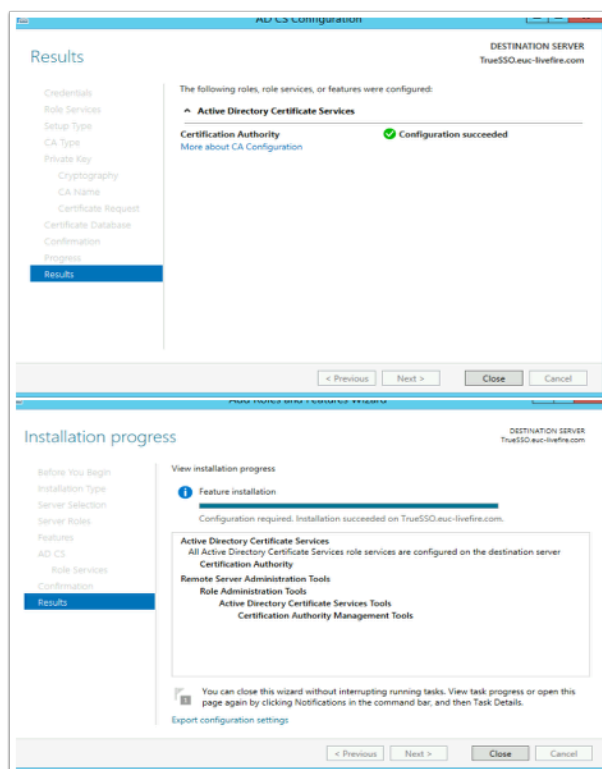
18. On the **Request a certificate from parent CA** ,
- Select the **radio button** next to **Send a certificate request to a parent CA:**
 - To the right of the **Parent CA** box, click the **Select** button
 - Select **OK** accept the Default
 - Select **Next**



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



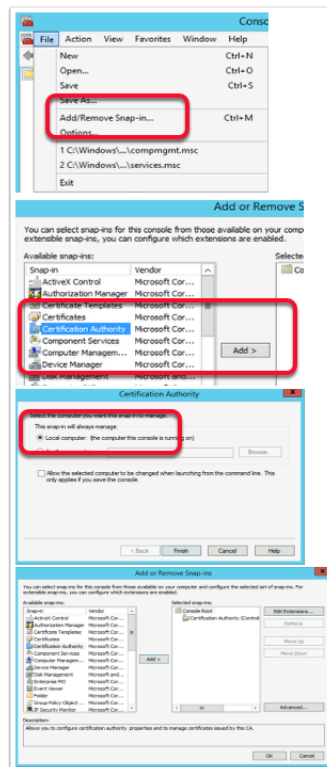
20. On the **Confirmation** window
 - Select **Configure**



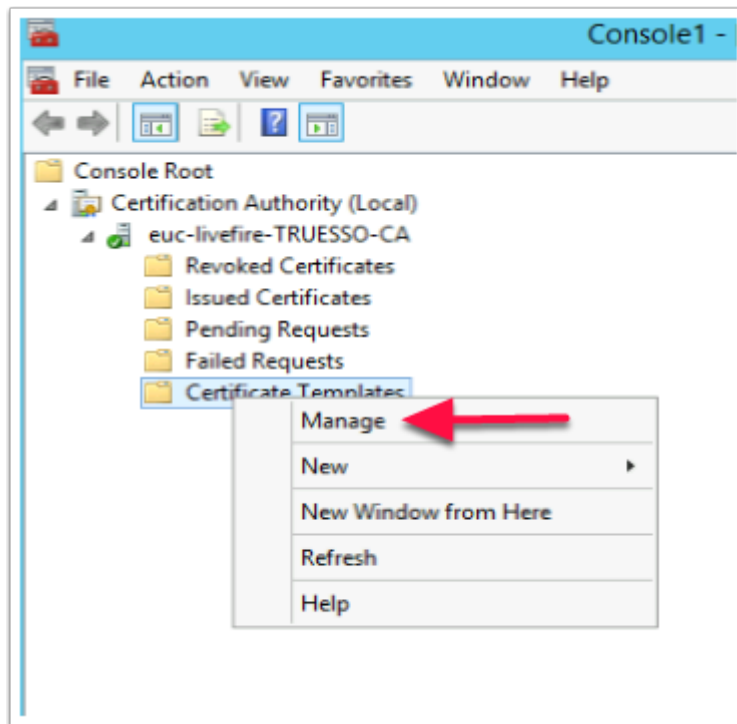
21. On the **Results** window
 - Select **Close**
 - On the **Installation progress** window,

- Select **Close**

Part 5: Deploying and Configuring Horizon TRUE SSO

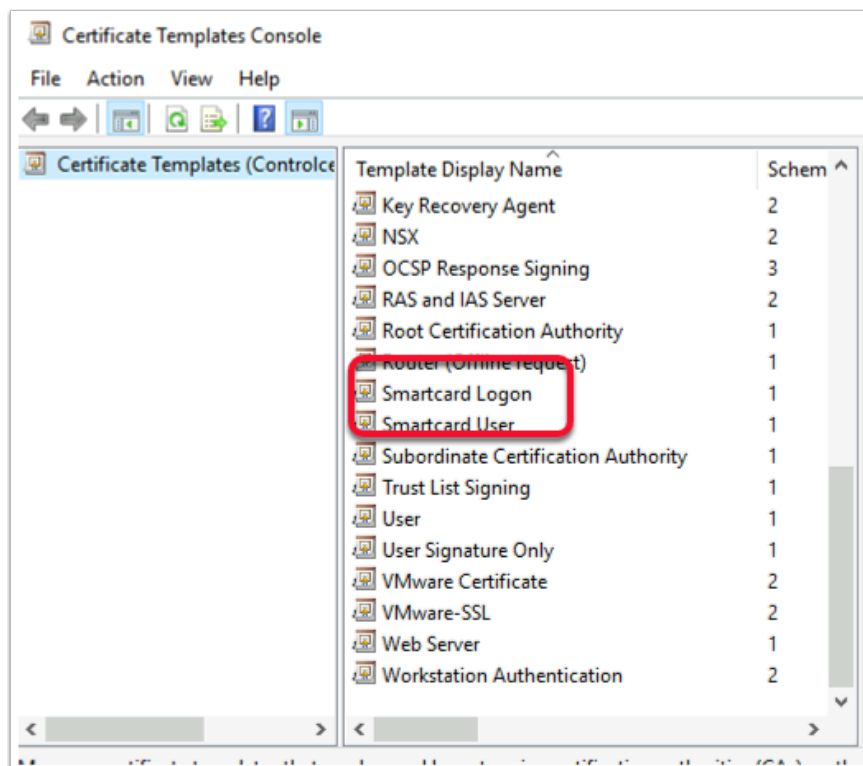


1. In this section we will create a certificate template for Horizon TRUE SSO
 - On your **TRUESSO** server select **Start** > **Run** > type **mmc**
 - Select **File** > **Add/Remove Snap-in...**
 - Select the **Certificate Authority** services snap-in, select **Add**
 - In the Certificate Authority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



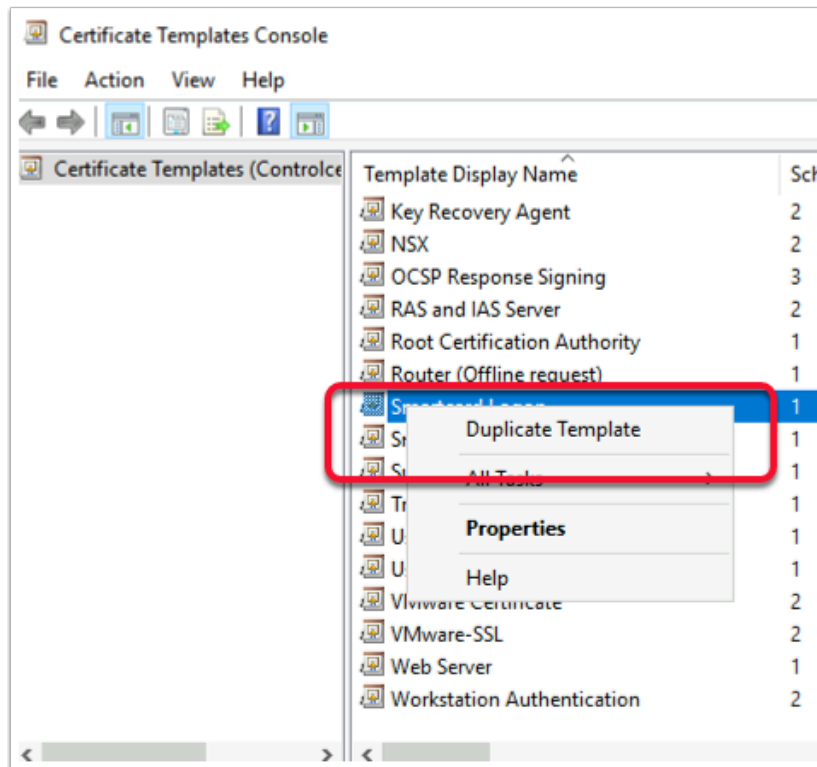
2. Expand the **euc-livewire-TRUESSO-CA** inventory

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

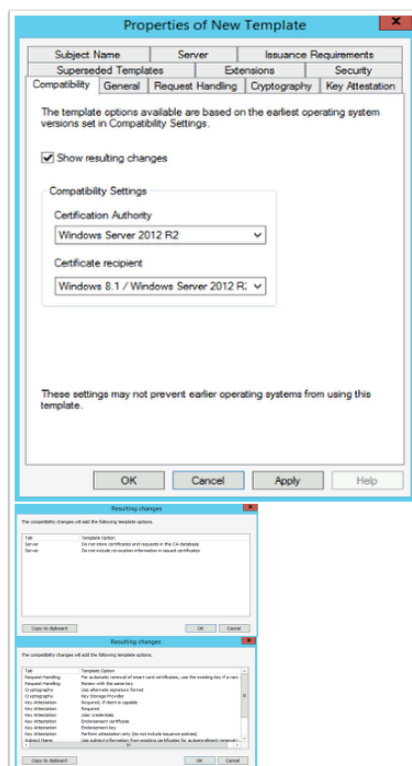


3. In the **Certificate Template** Console

- Find and select the **Smartcard Logon** template

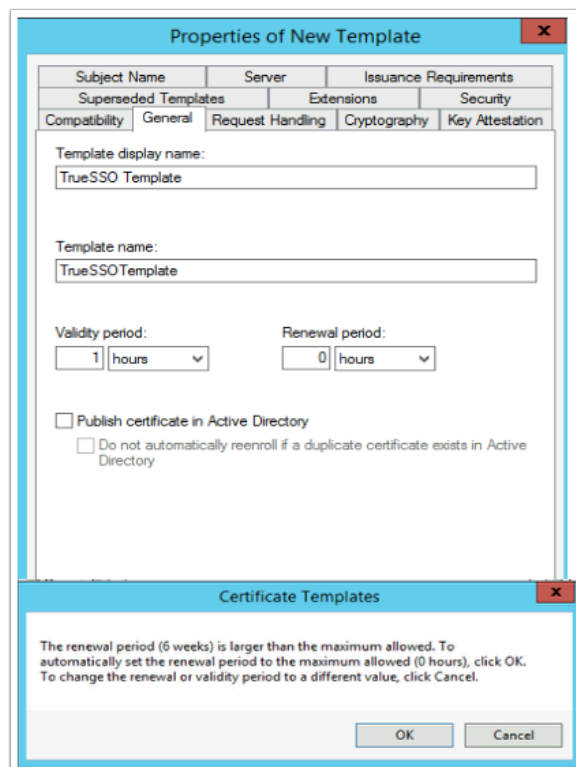


4. Right-click the **Smartcard Logon** template
 - Select **Duplicate Template**

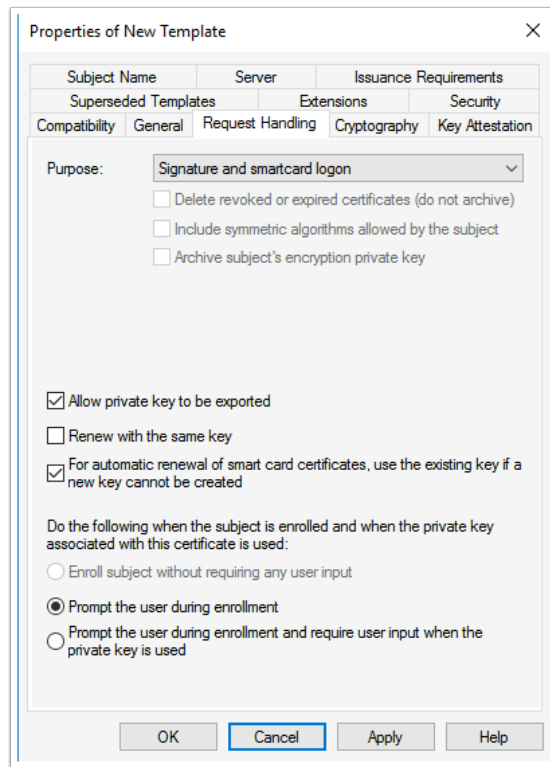


5. In the **Properties of New Template** window in the **Compatibility** tab under **Certificate Authority**
 - Change from **Windows 2003** to **Windows 2012 R2**

- 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**.

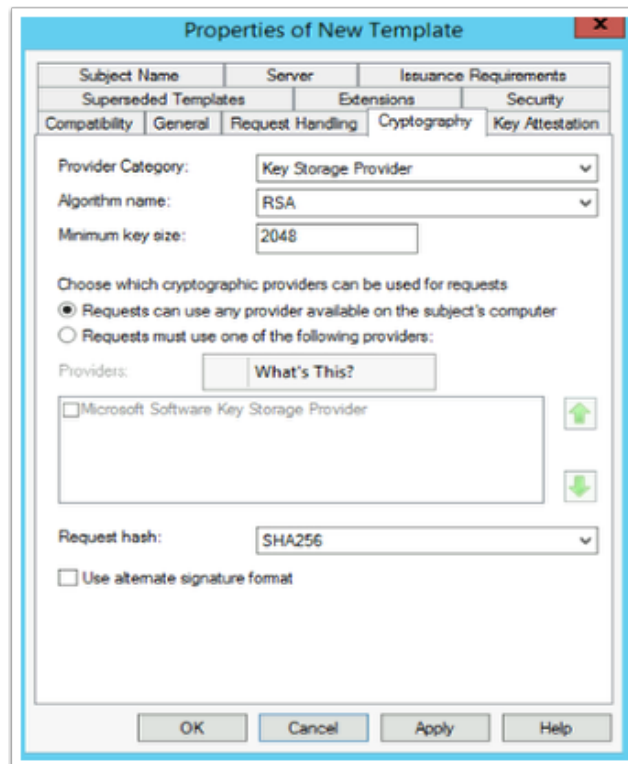


6. Select the **General** tab,
 - Under **Template display name:** type **TrueSSO Template**, you will notice Template name gets filled in automatically.
 - **(Don't edit the TemplateName)**
 - Under **Validity period** change the period from **1 years** to **1 hours**
 - When prompted by **the Certificate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

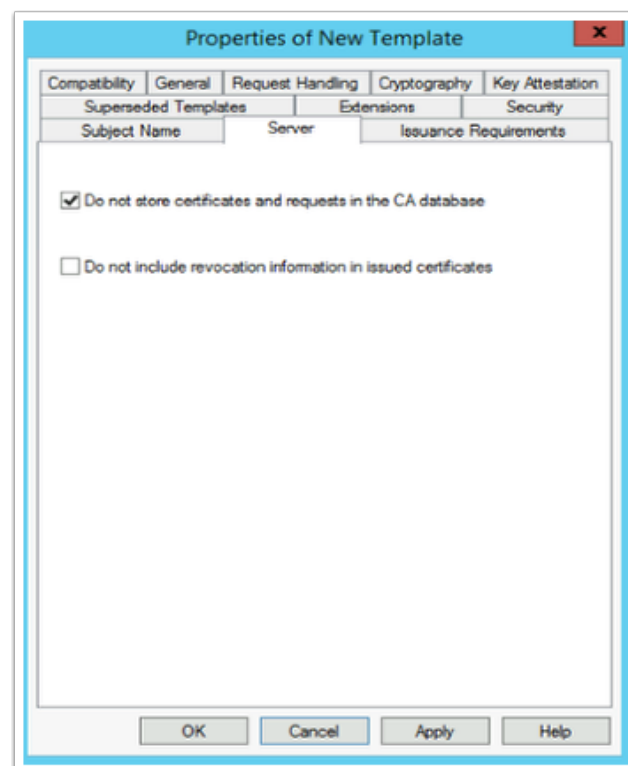


7. Select the **Request Handling** tab change the following next to :-

- **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**

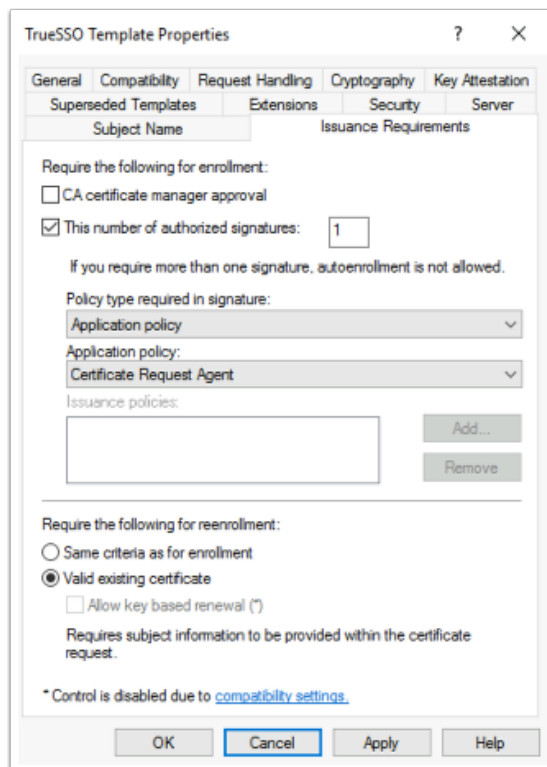


8. Select the **Cryptography** tab change the following next to
- **Provider Category:** **Key Storage Provider**
 - **Minimum key size:** **2048**
 - **Request hash:** **SHA256**

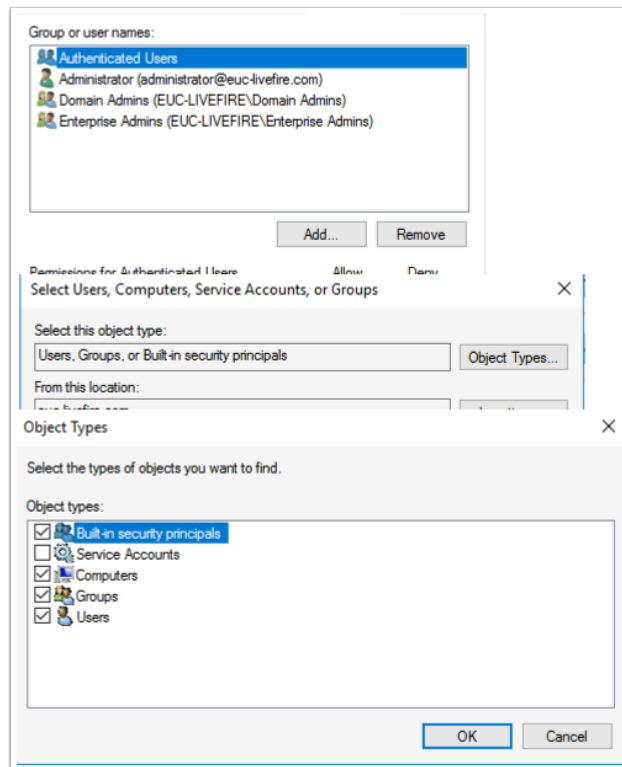


9. Select the **Server** tab,

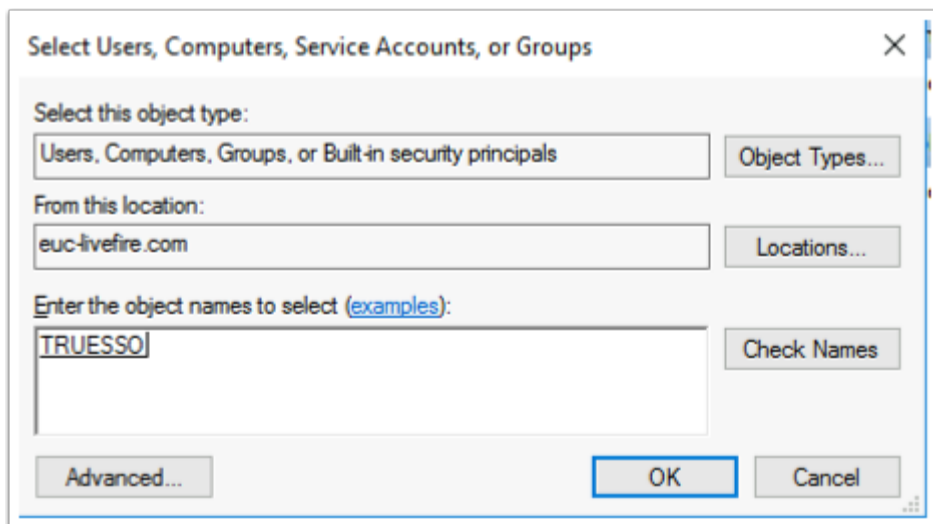
- Select the **checkbox** in front of **Do not store certificates and requests in the CA database**
 - You will notice that **Do not include revocation information in issued certificates** is selected automatically.
- Uncheck the **check box** next to **Do not include revocation information in issued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



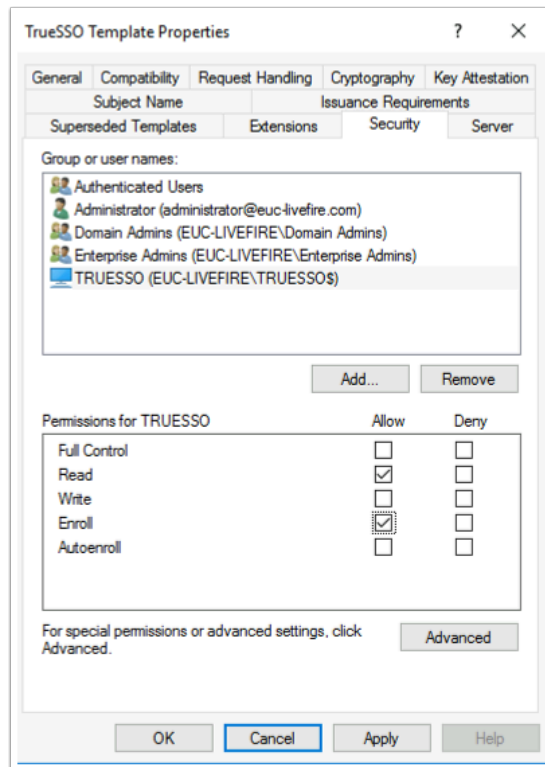
10. Select the **Issuance Requirements** tab, configure the following:
 - Select the **checkbox** : **This number of authorized signatures** and change the value to **1** in the **box**
 - Under **Policy type required in signature**
 - Ensure the **Application policy** is selected (default config)
 -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

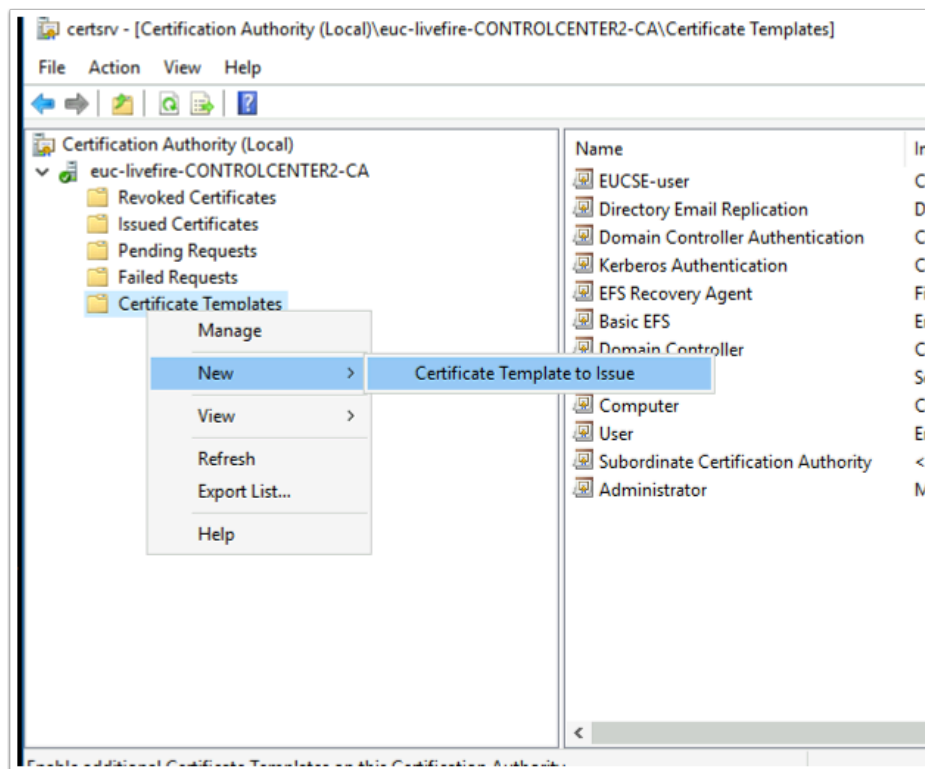


12. In the **Enter the object names to select**
 - Type **Truessso**
 - To the right select **Check Names**
 - Select **OK**



13. For the **Permissions for TRUESSO**

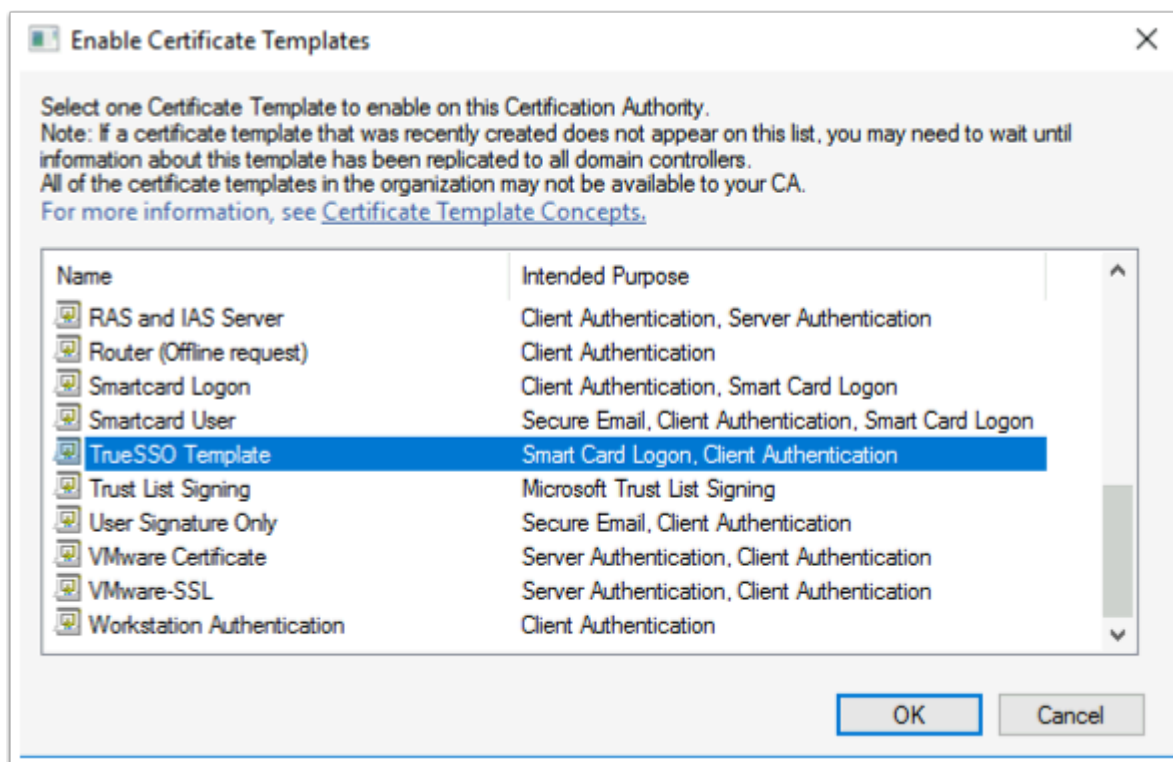
- Ensure that the permission **Read** and **Enroll** checkboxes are selected.
- Select **OK** to close the **TrueSSO Template Properties**,



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

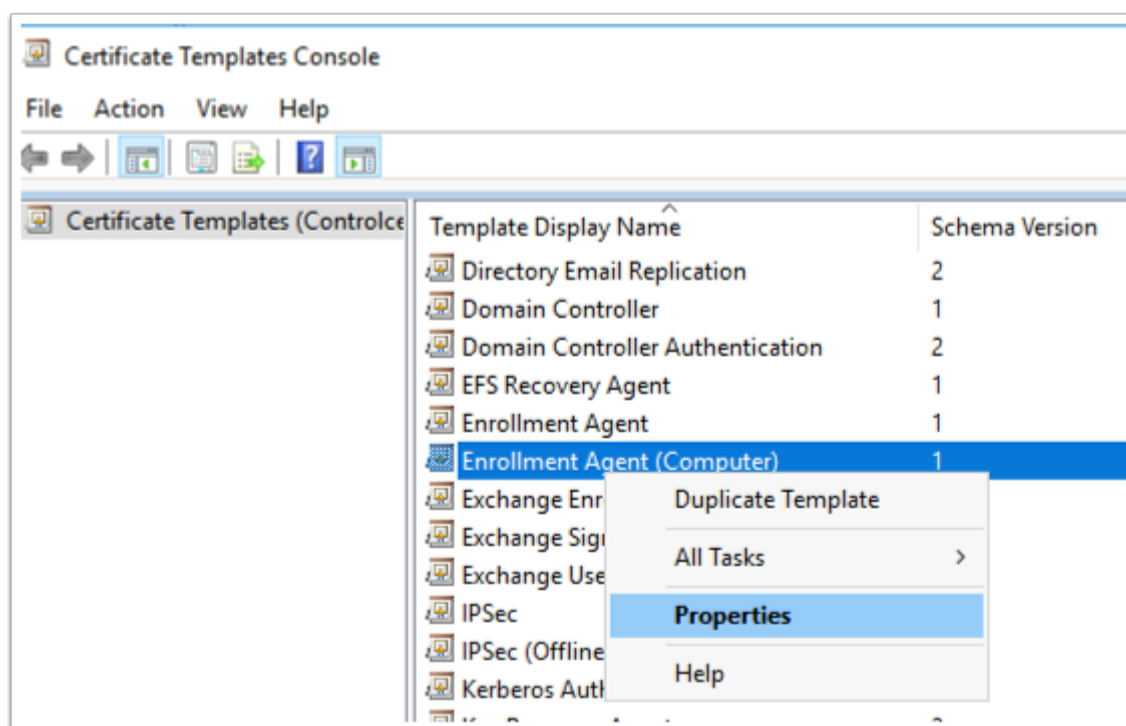
- Select and right-click the **Certificate Templates** container,

- Select **New** > **Certificate Template** to Issue

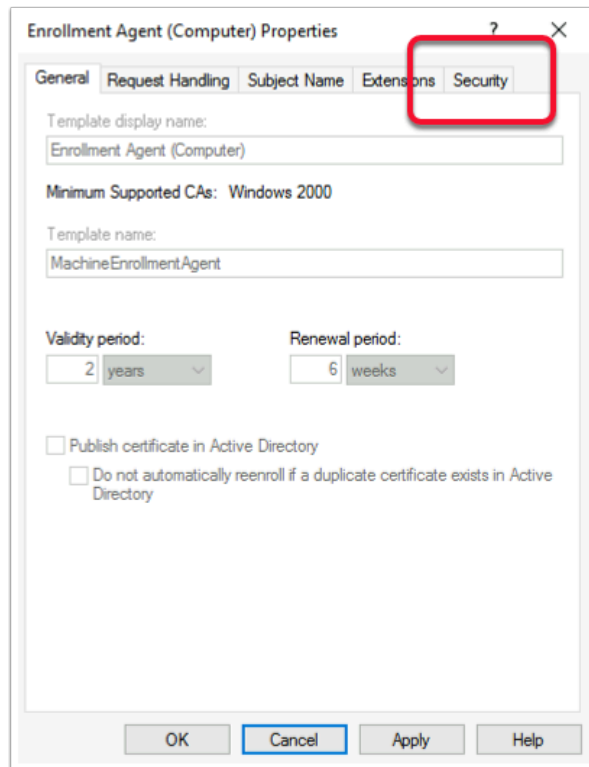


15. In the **Enable Certificate Templates** window,

- Select your **TrueSSO Template**
- Select **OK**

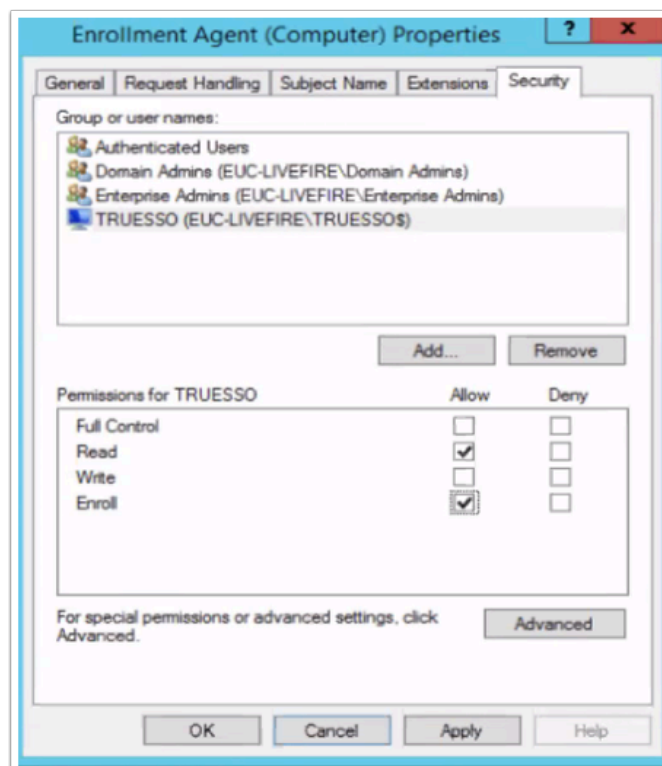


16. Switch back to the **Certificate Templates** Console select and right-click the **Enrollment Agent (computer)** template and select **Properties**



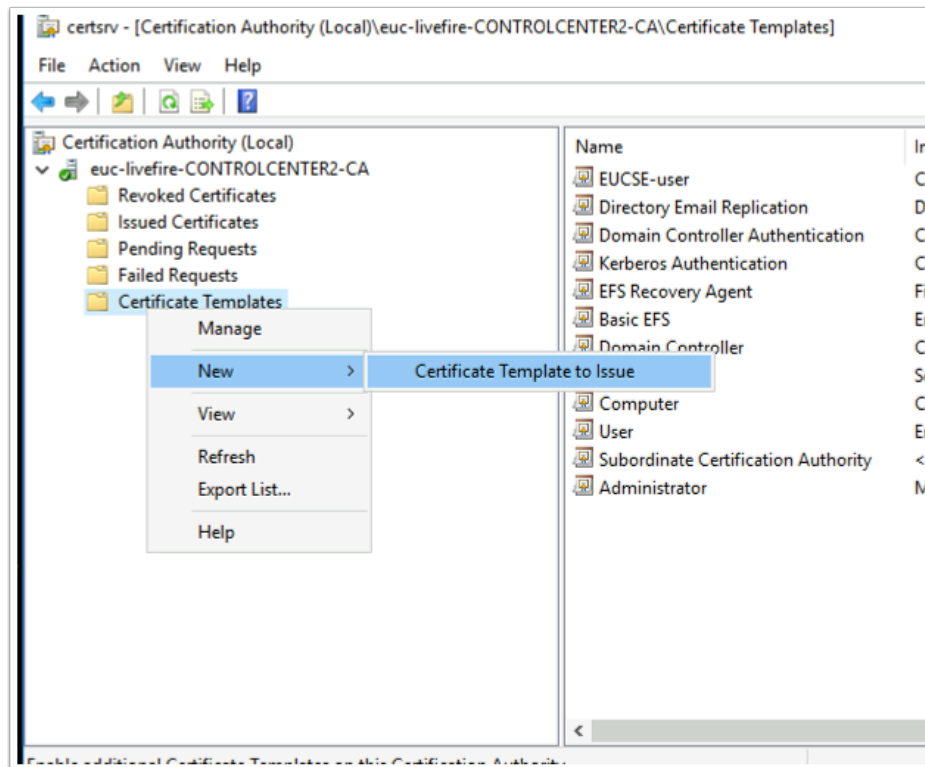
17. In the **Enrollment Agent Properties** window

- Select the **Security** tab

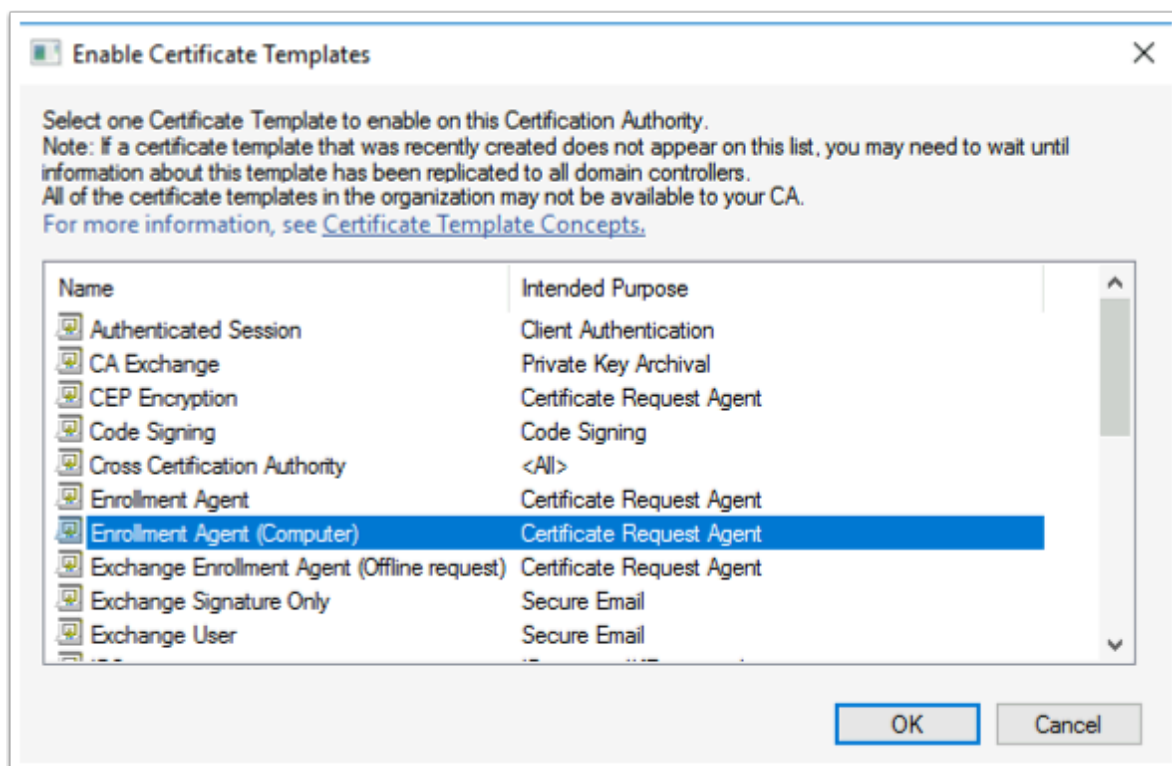


18. Select **Add** and add the **TRUESSO** Computer account with Read and **Enroll** permissions .

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

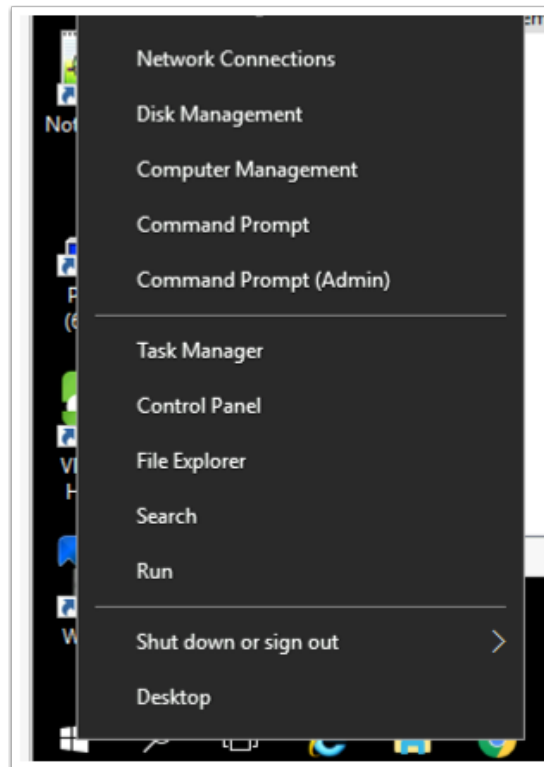


19. Switch back to the **Certificate Authority Console** select
- Right-click the **Certificate Templates** container,
 - Select **New** > **Certificate Template** to Issue



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 **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-CONTROLCENTER2-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`

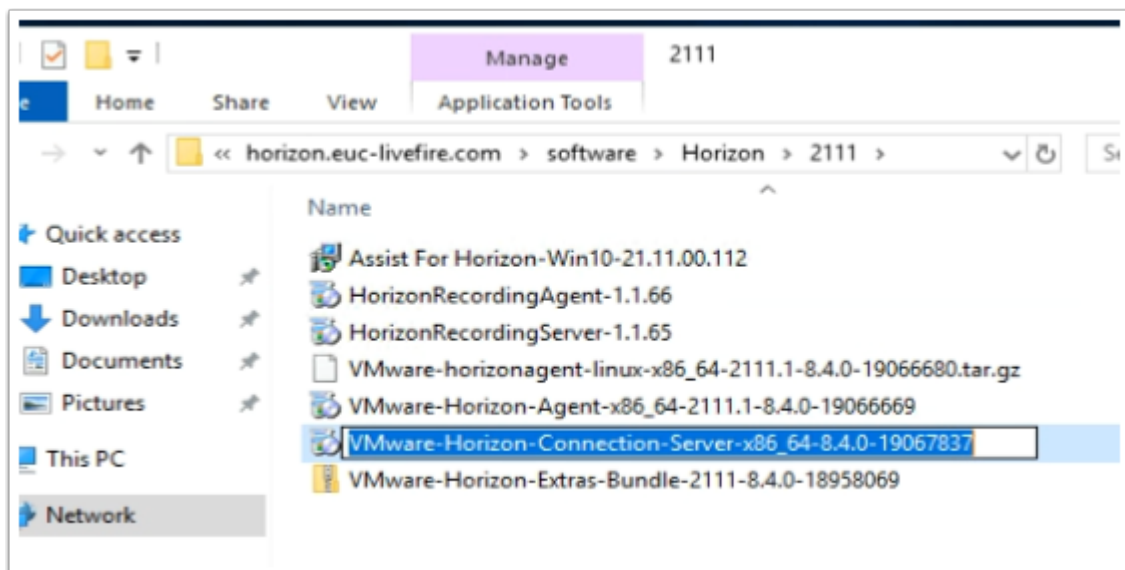
```
C:\Windows\system32>net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.

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>
```

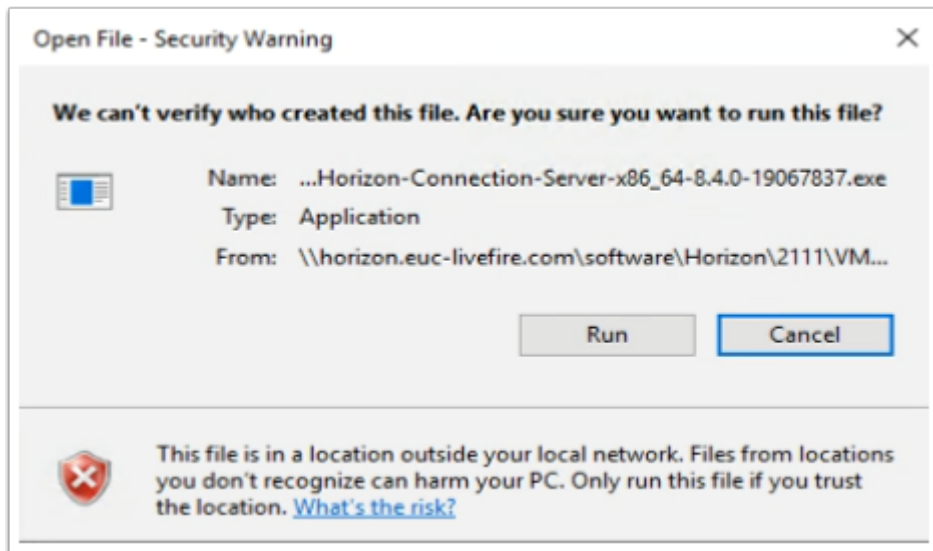
24. Restart the CA service. From the command prompt run:

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

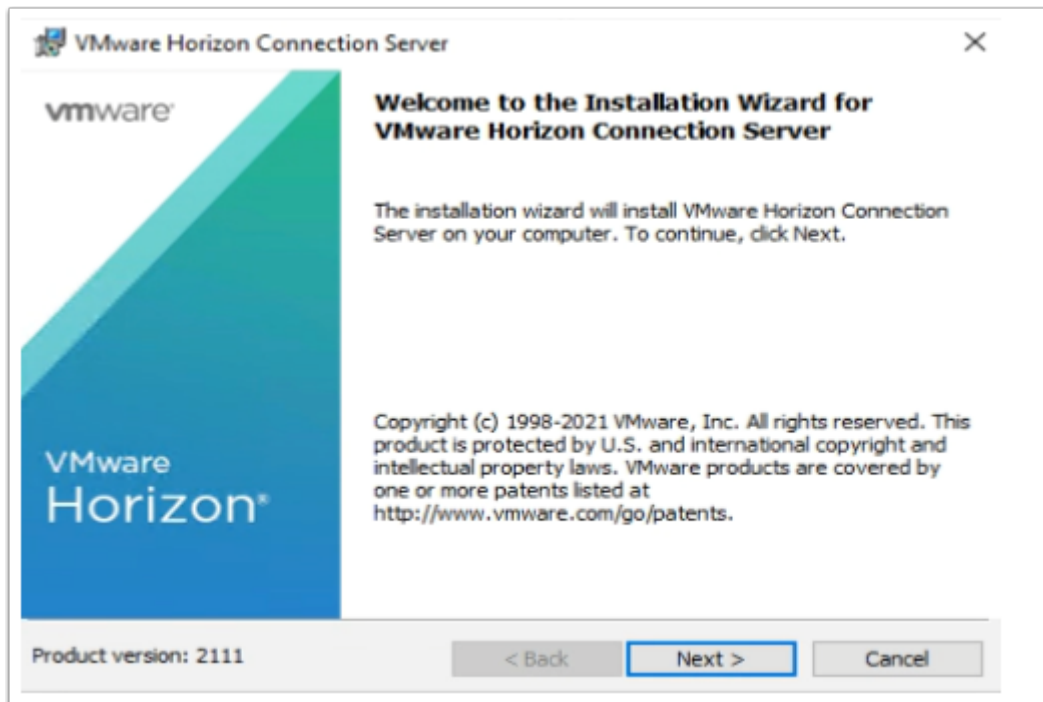


25. On the **TrueSSO** server desktop

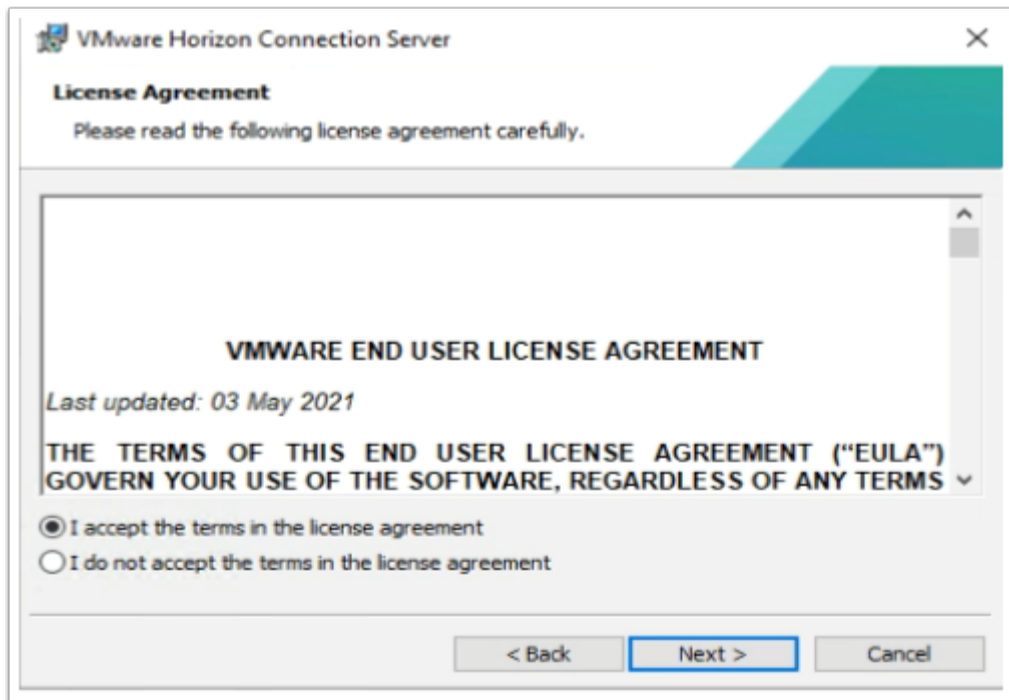
- Launch the **software** shortcut
- In the Software folder, open the **Horizon\2111** folder.
- Select and launch the **VMware-Horizon-Connection-Server-x86_64-8.4.0-19067837.exe**



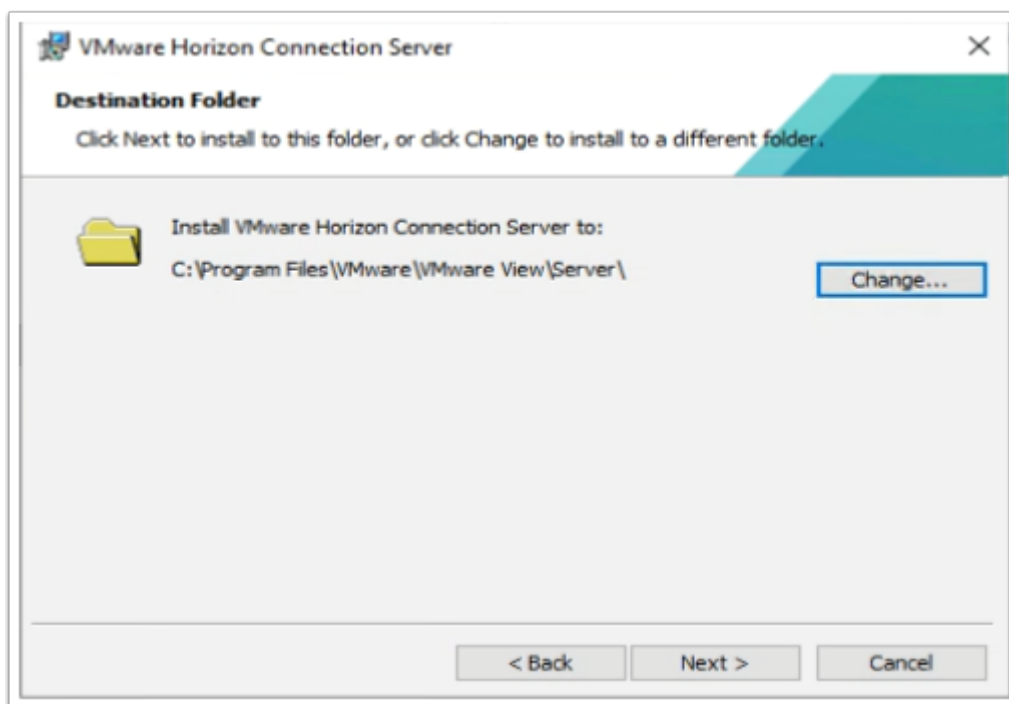
26. On the **Open File - Security Warning** window
- Select **Run**



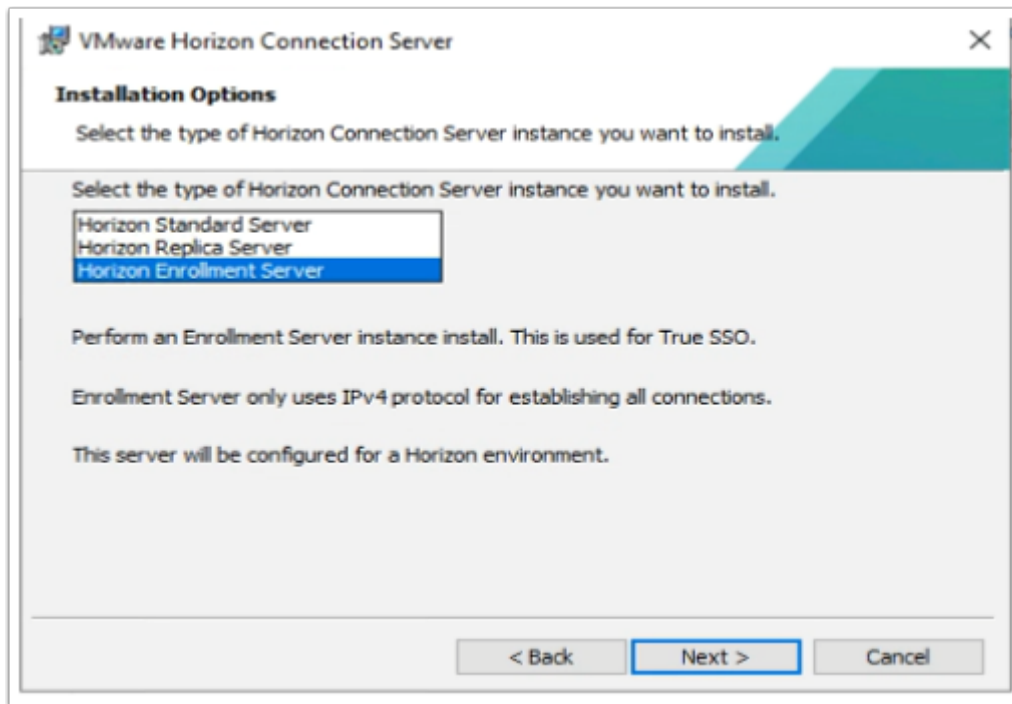
27. On the **Welcome** window
- Select **Next**



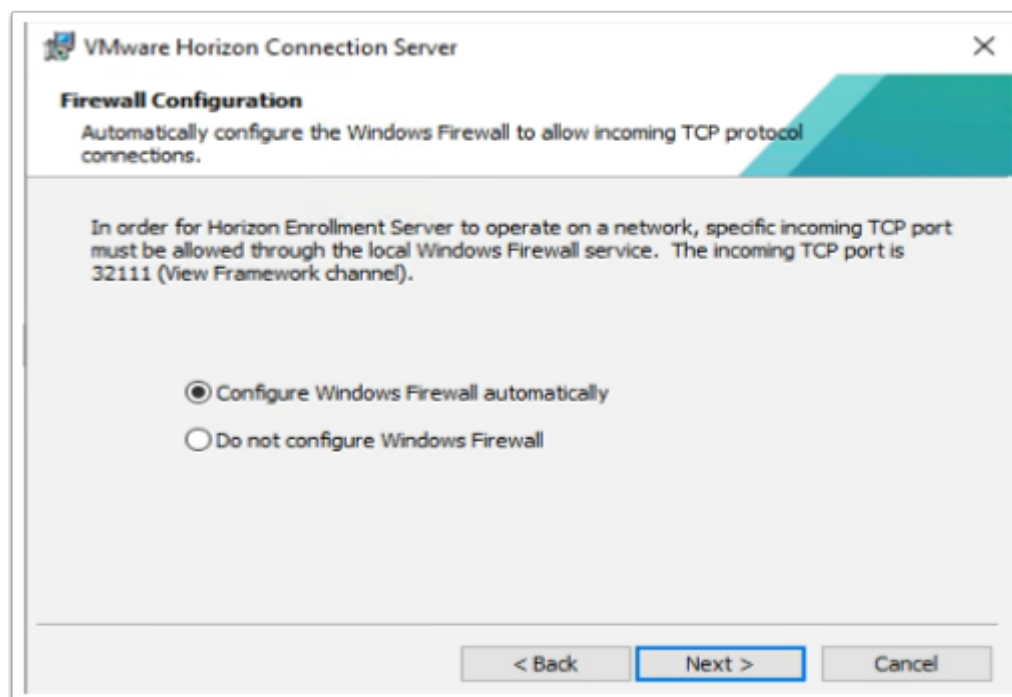
28. On the **License agreement** window
- Select the **radio button** next **I accept the terms in the license agreement**,
 - Select **Next**



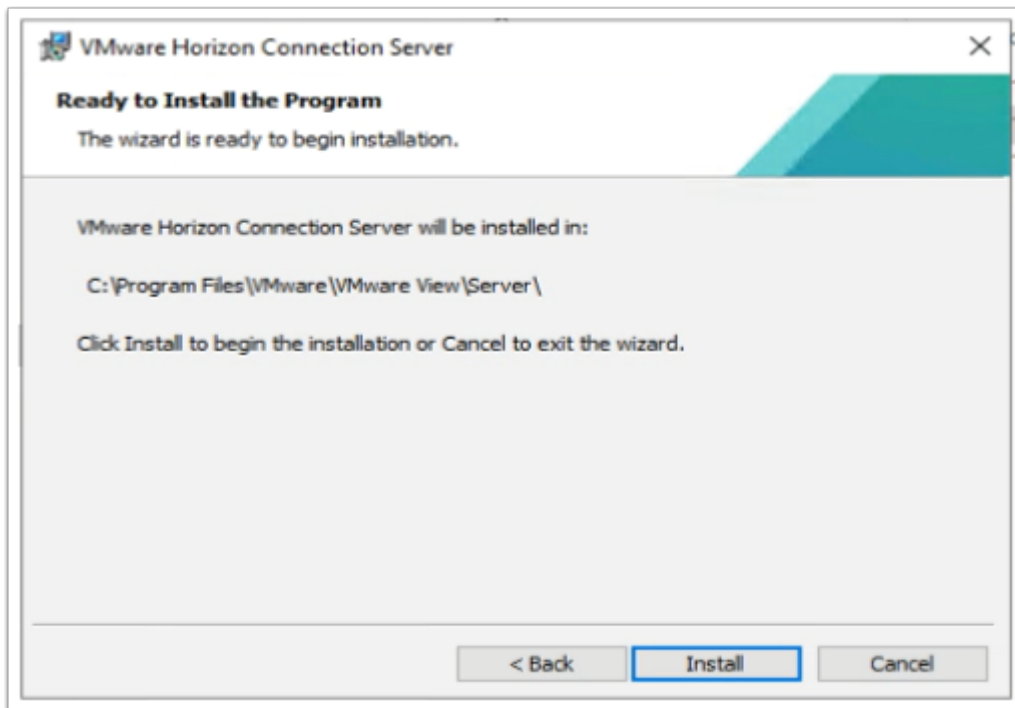
29. On **Destination Folder** window
- Select **Next**



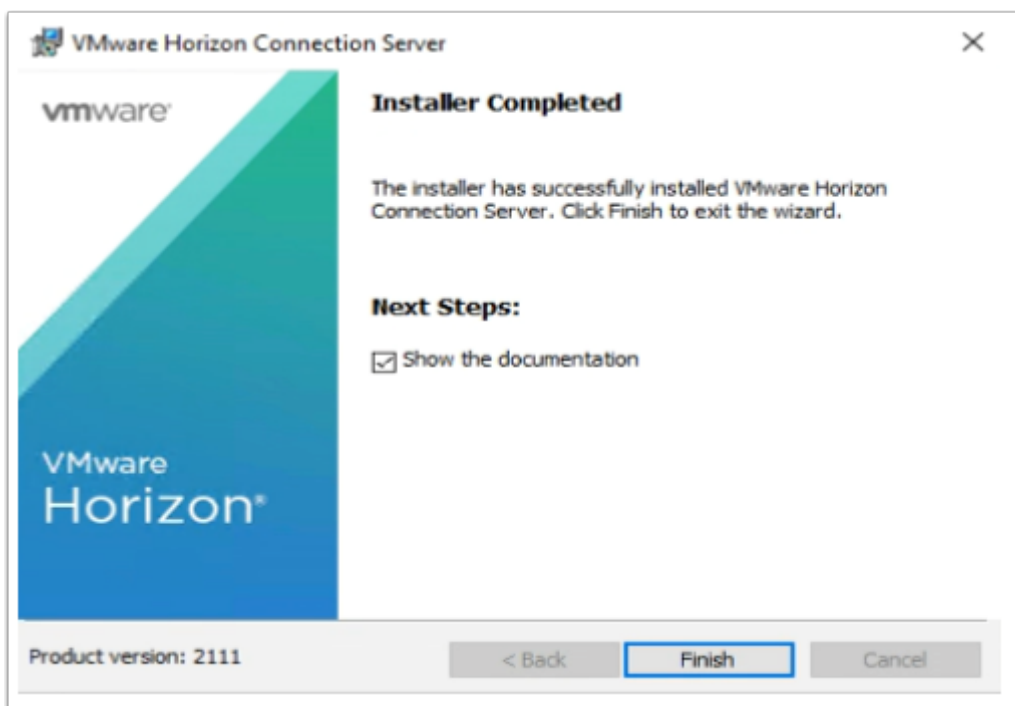
30. On the **Installation Options** window select **Horizon Enrollment Server**
- Select **Next**



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

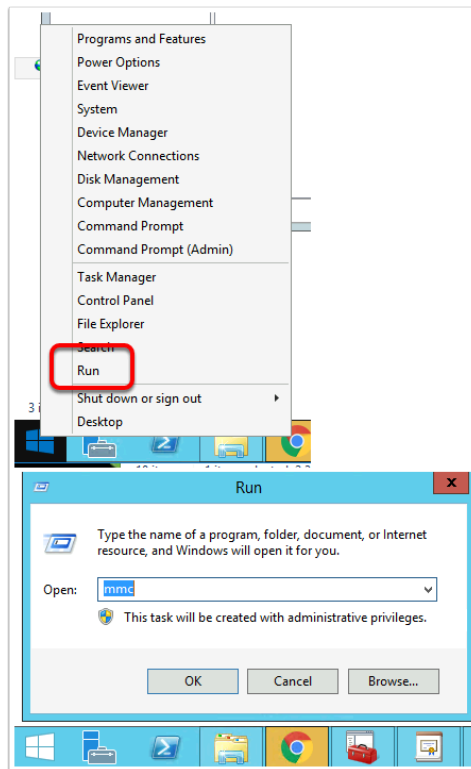


32. Select **Install**

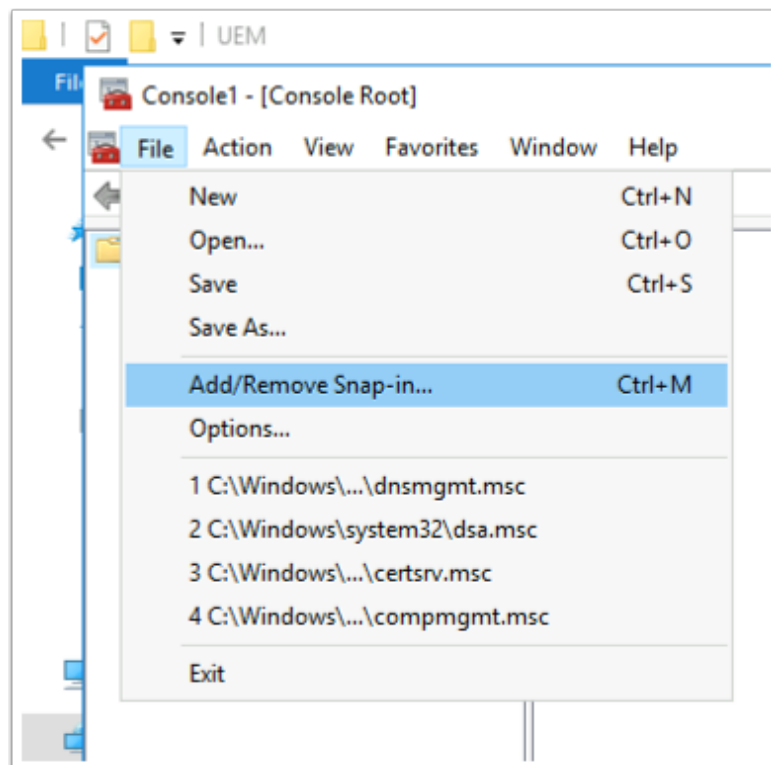


33. On the **Installer Completed** Window

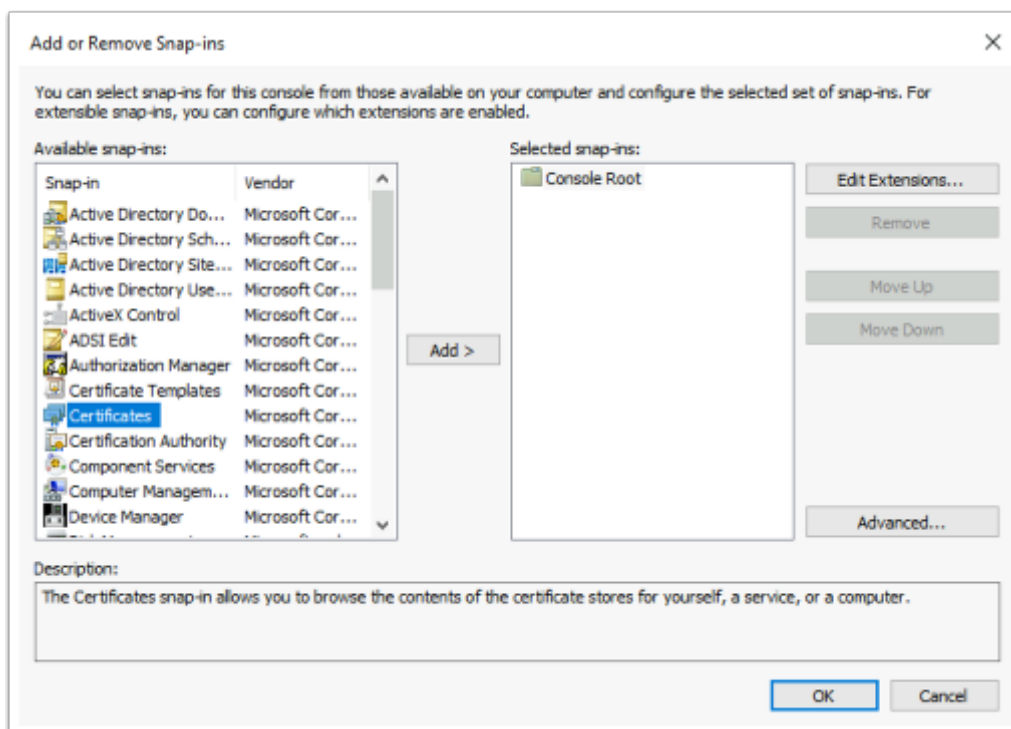
- Select **Finish**



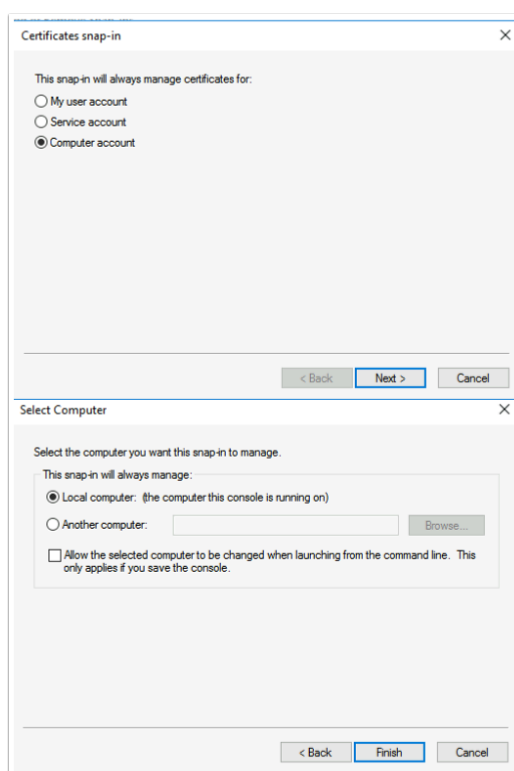
34. On the **TrueSSO** server
- Select and right-click the **Start Button**,
 - Select **Run**,
 - Type **MMC**,
 - Select **OK**



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

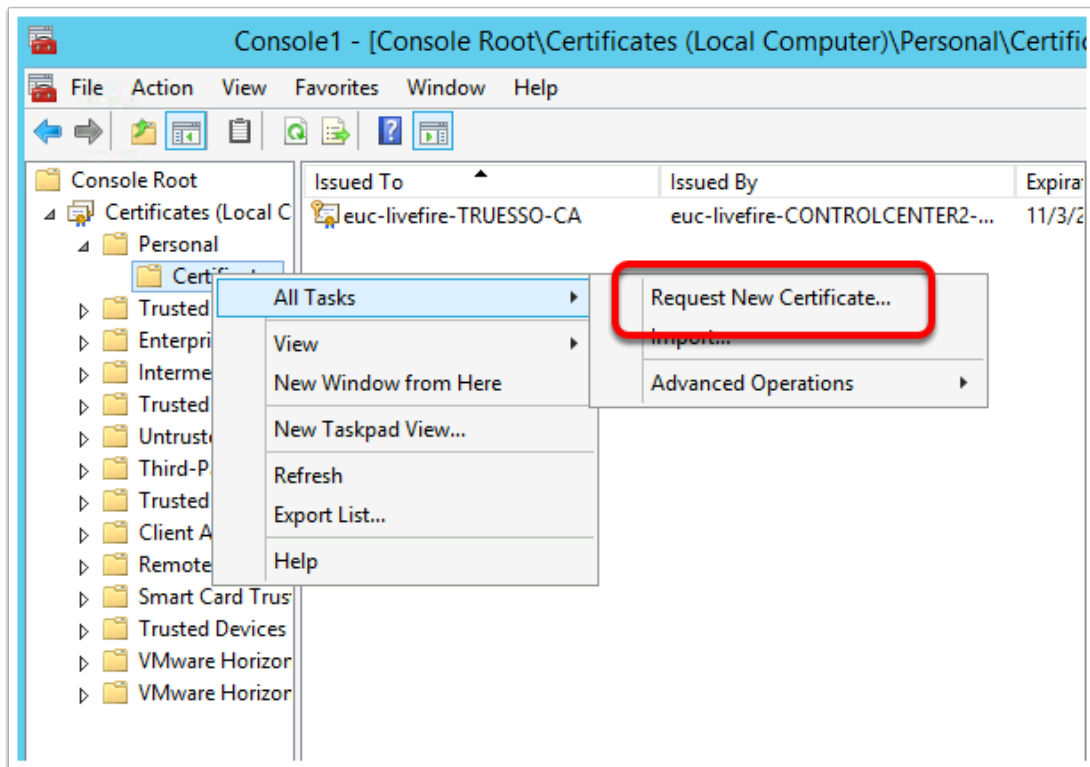


36. In the **Add or Remove Snap-ins** window,
- Select **Certificates**
 - Select **Add**

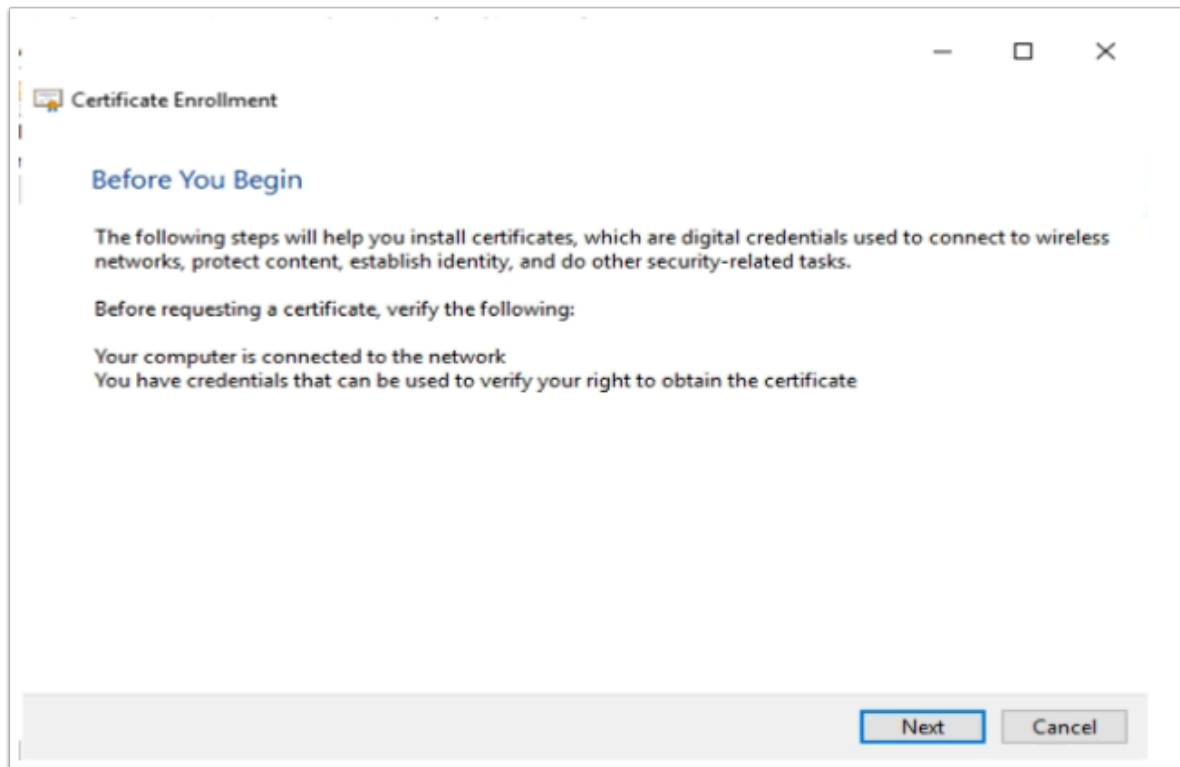


37. Select **Computer account** radio button

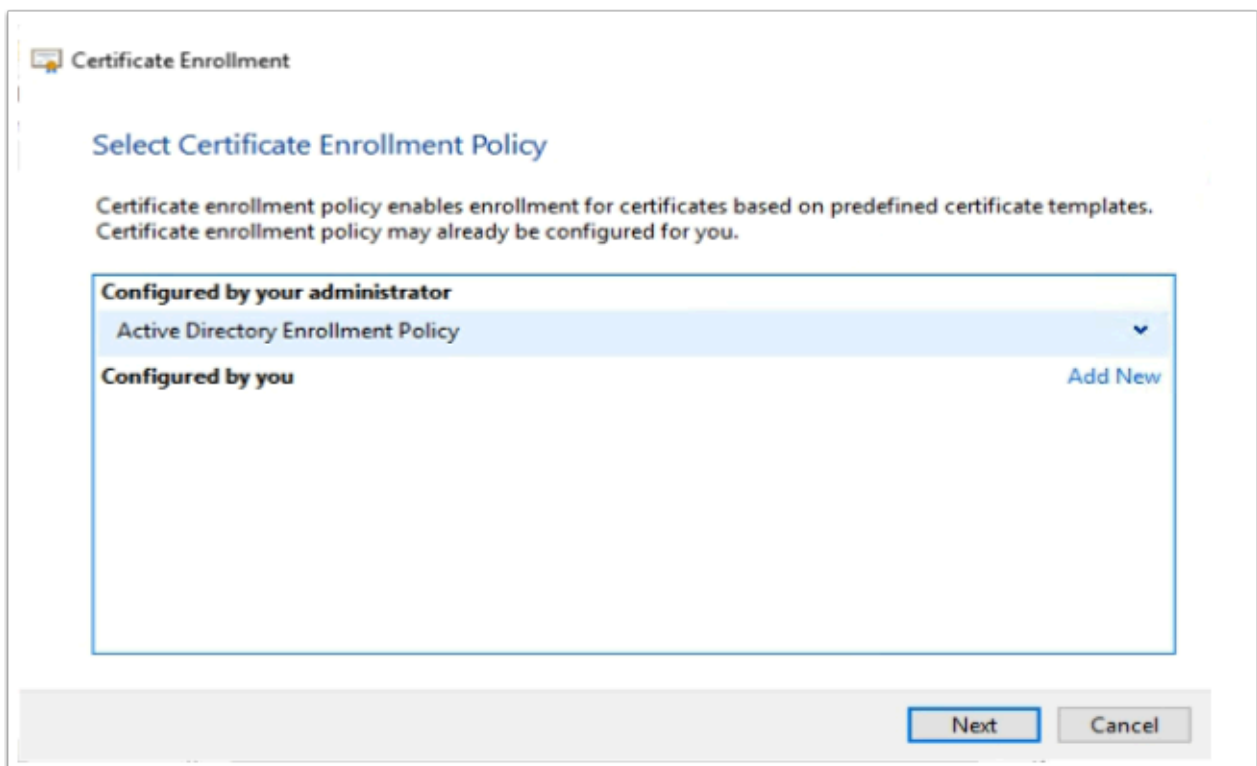
- Select **Next**
- Select **Finish**
- Select **OK**



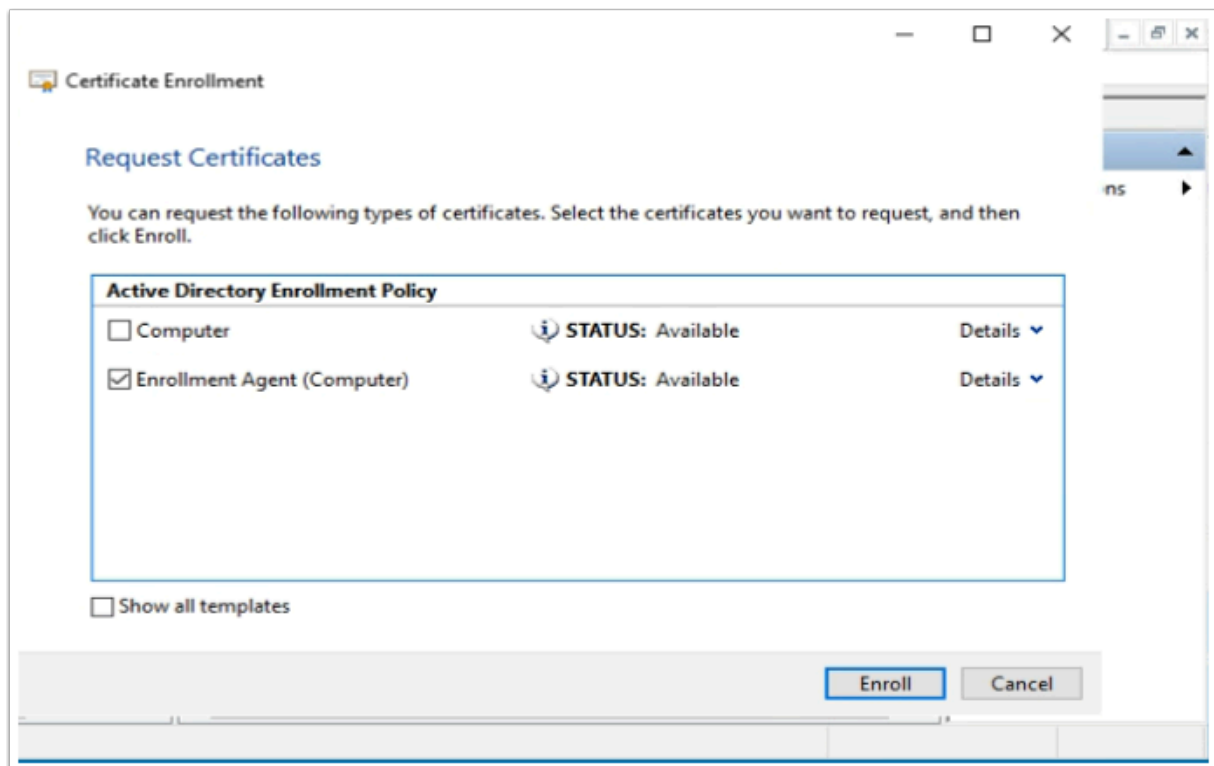
38. Expand the **Certificates** console inventory
- Select and right-click the **Personal** container.
 - Select **All Tasks** > **Request New Certificate**



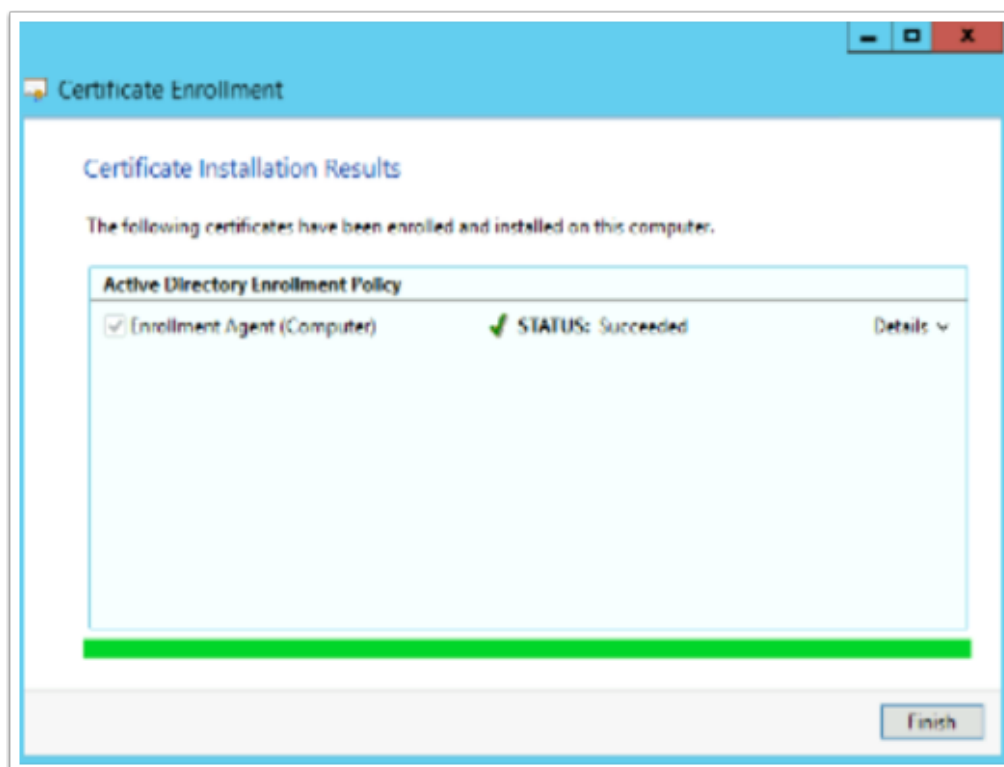
39. On the **Certificate Enrollment > Before you Begin** window
- Select **Next**



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

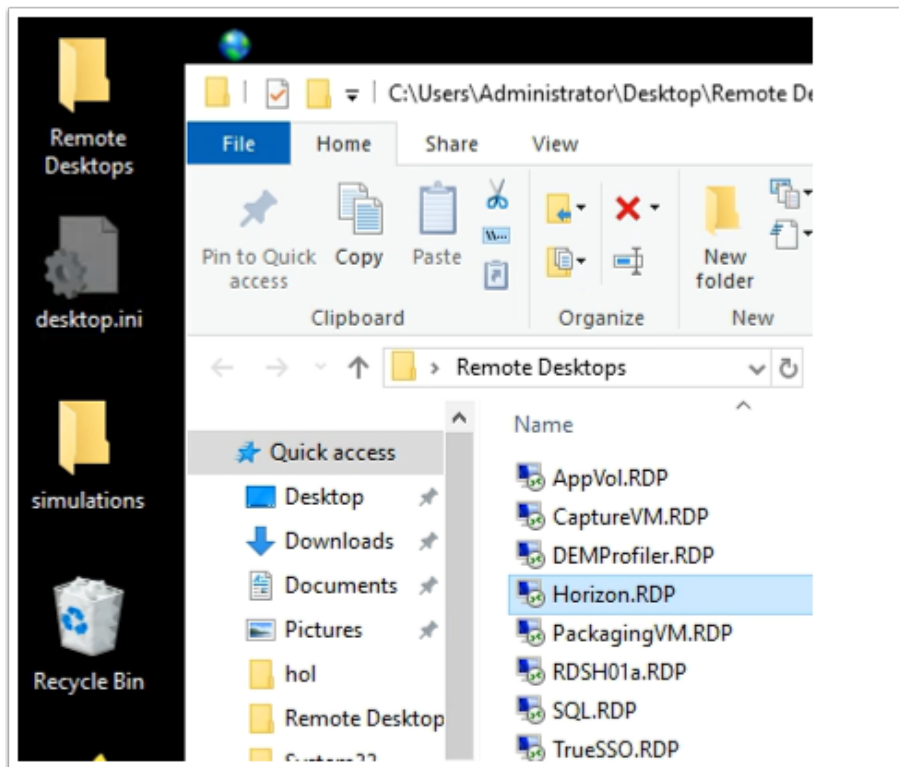


41. On the **Request Certificates** windows
- Select the **checkbox** in front of **Enrollment Agent (Computer)**
 - Select **Enroll**

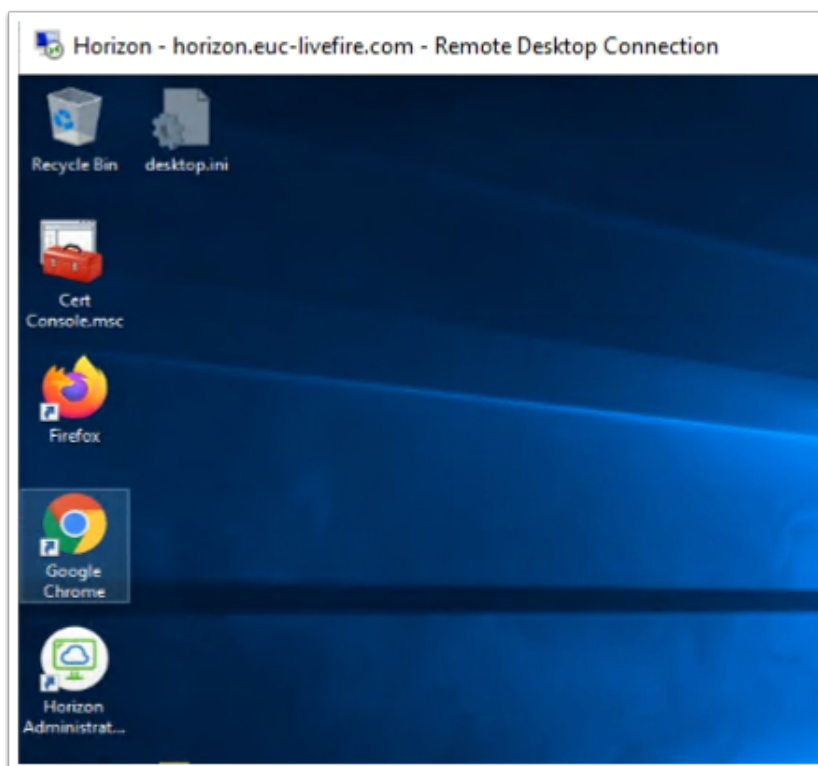


42. On the **Certificate Installation Results** window,
- Ensure the enrollment was successful

- Select **Finish**.

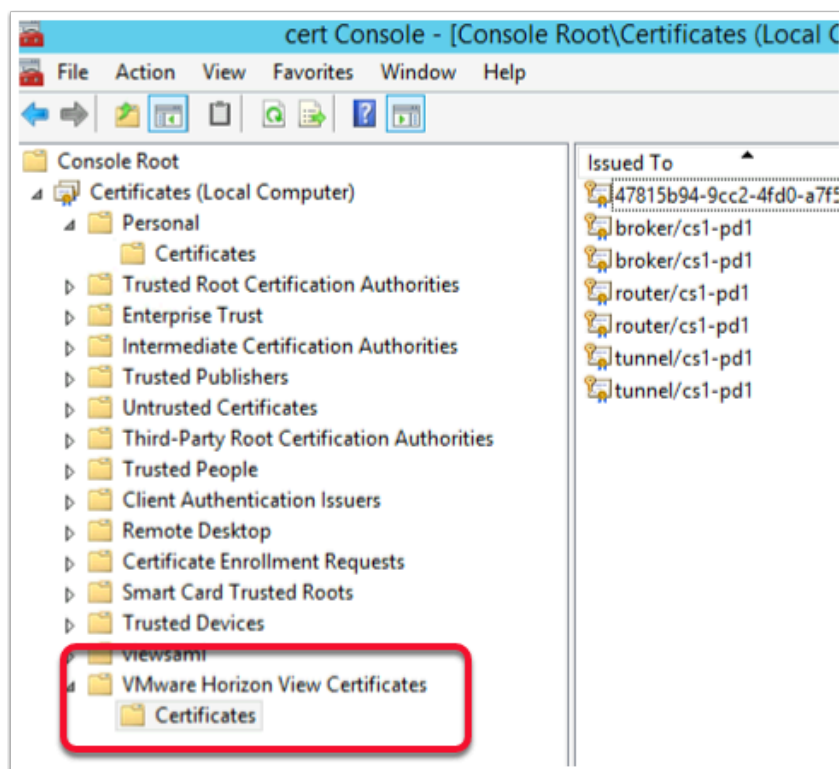


43. Switch to your **ControlCenter** server,
- Open up your **Remote Desktop** folder and **RDP** to **Horizon**
 - With username **euc-livefire\administrator** and password **VMware1!**



44. On the **Horizon Server** desktop

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



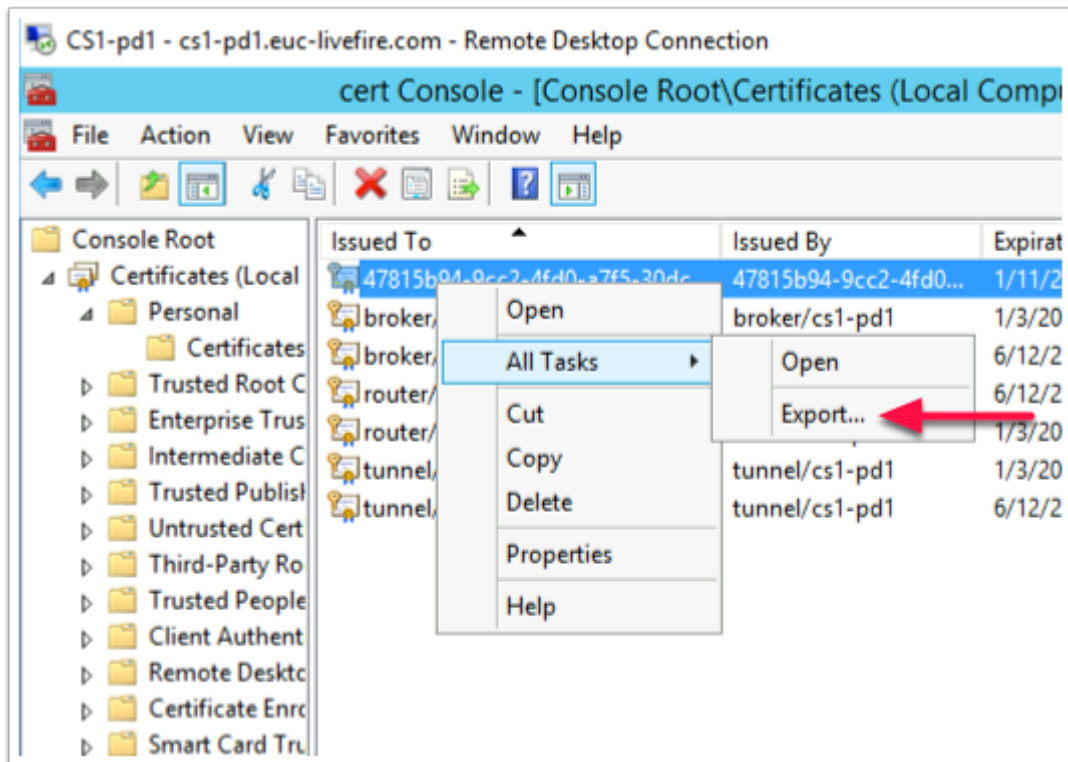
45. In the **Certificates** Console

- **Expand** the inventory
- Browse down to **VMware Horizon View Certificates > Certificates**

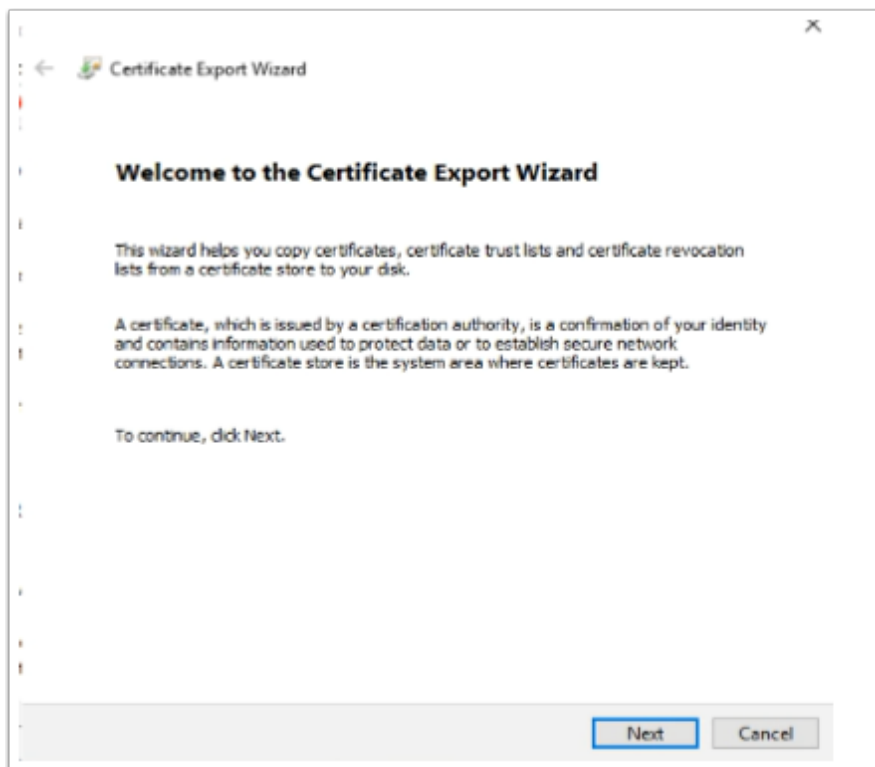
Issued To	Issued By	Expiration Date	Intended Purpose	Friendly Name
47815b94-9cc2-4fd0-a7f5-30dc...	47815b94-9cc2-4fd0...	1/11/2030	<All>	vdm.ec
broker/cs1-pd1	broker/cs1-pd1	1/3/2021	<All>	ConnectionBroker
broker/cs1-pd1	broker/cs1-pd1	6/12/2020	<All>	ConnectionBroker
router/cs1-pd1	router/cs1-pd1	6/12/2020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

46. In the **VMware Horizon View Certificates > Certificates** folder

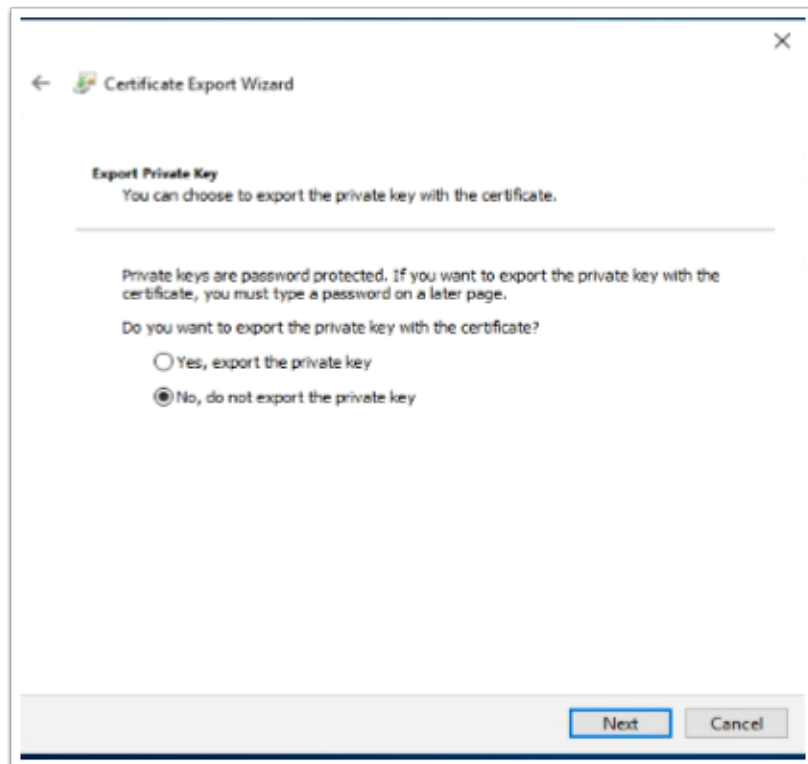
- Expand the console or **scroll** across the console and notice the **guid** based certificate has a friendly name of **vdm.ec**



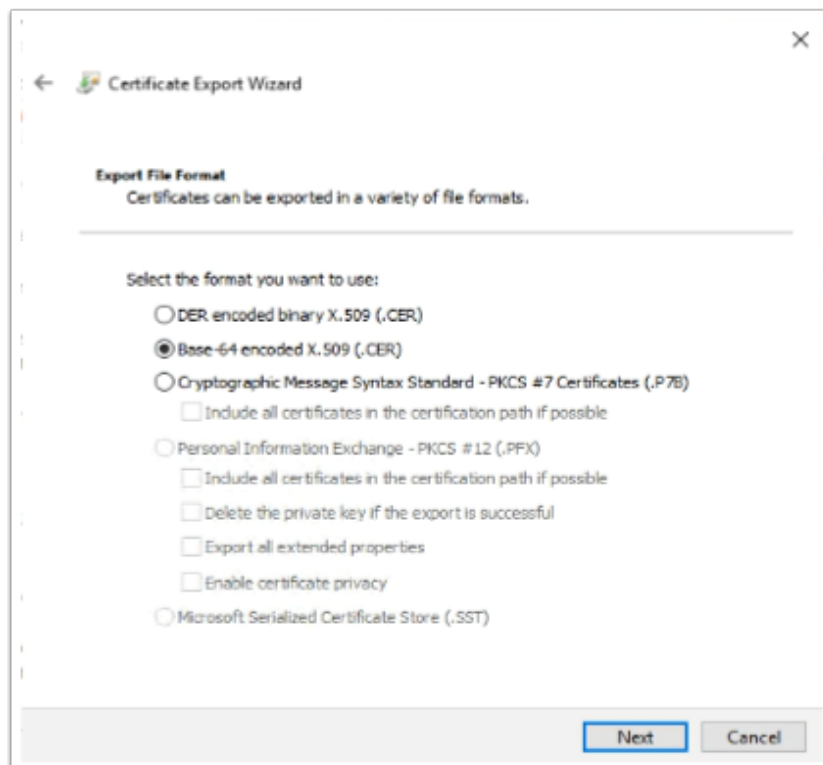
47. Select your **GUID certificate** with the friendly name of **vdm.ec**.
- Right-Click select **All Tasks**
 - Select **Export**



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

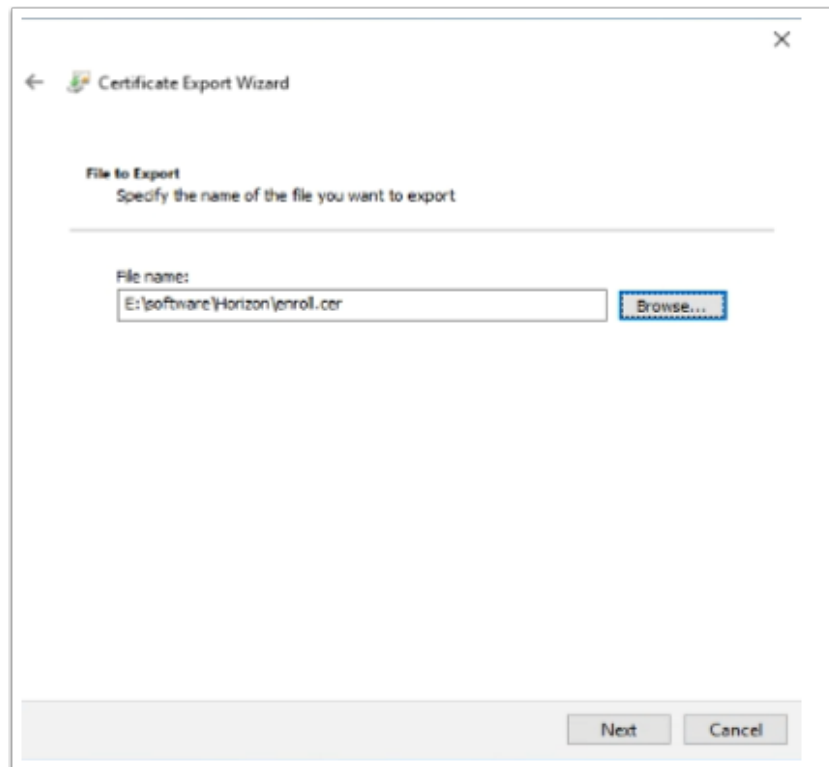


49. On the **Export Private Key** page
- Select the **radio button** next to **No, do not export the private key**
 - Select **Next**



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

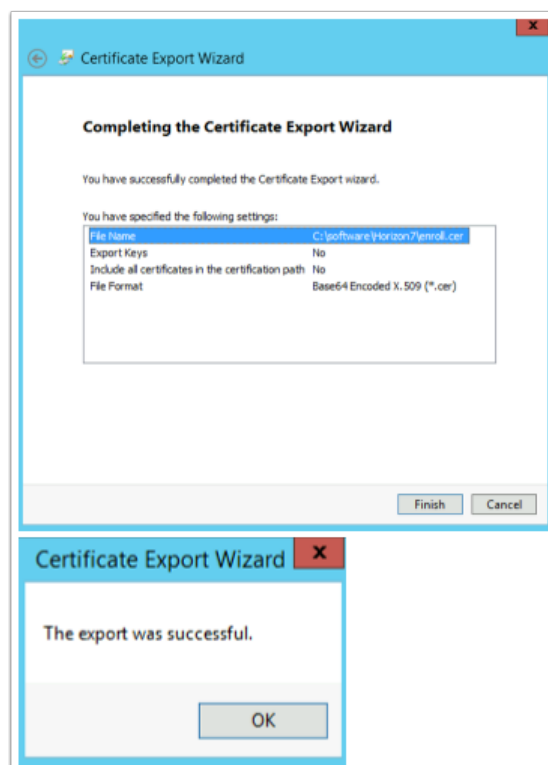
- Select **Next**



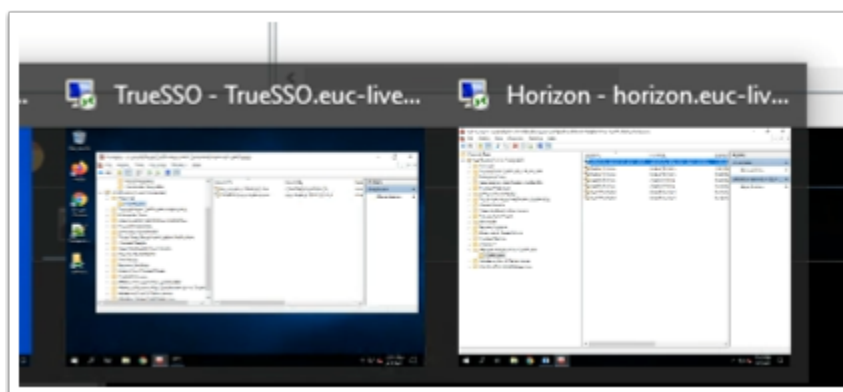
51. In the **File to Export** window

- Under **File name** type the following **E:\software\Horizon\enroll.cer**
- Select **Next**

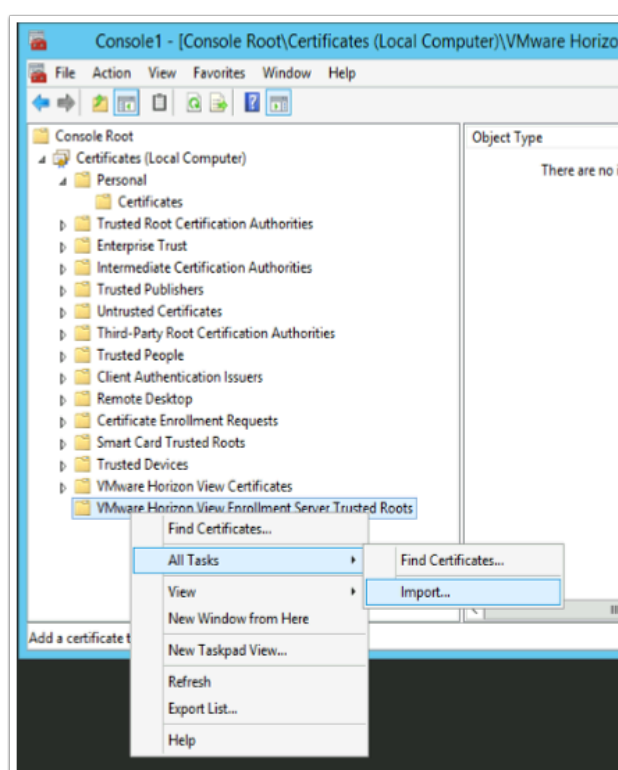
(**Software** is a shared folder which we will use to copy from on the TrueSSO server)



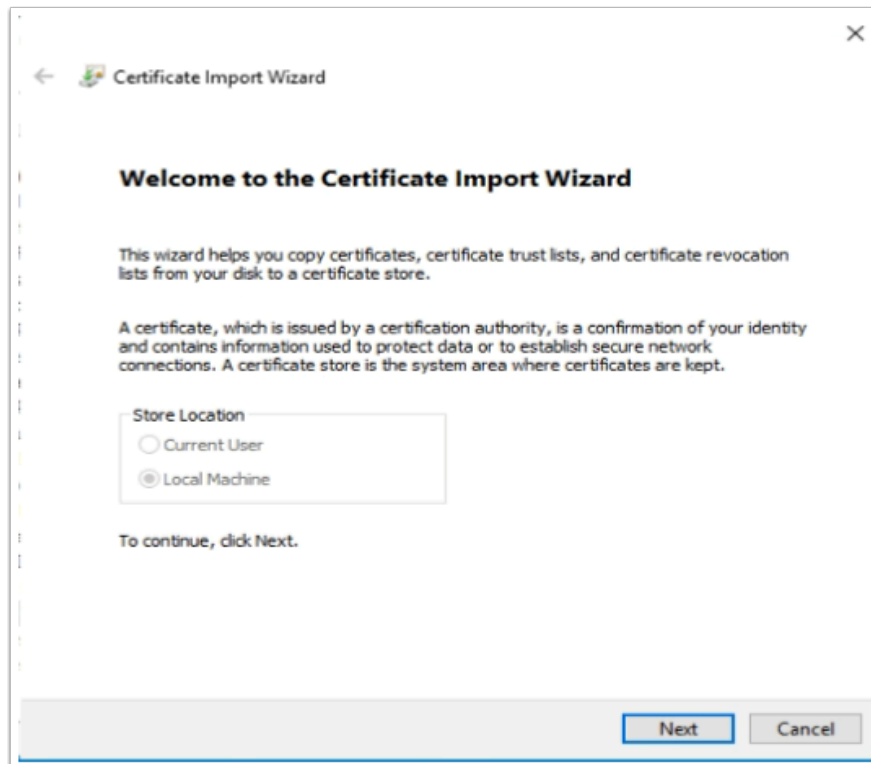
52. On the **Completing the Certificate Export Wizard** window
- Select **Finish**. When prompted that **The export was successful**,
 - Select **OK**



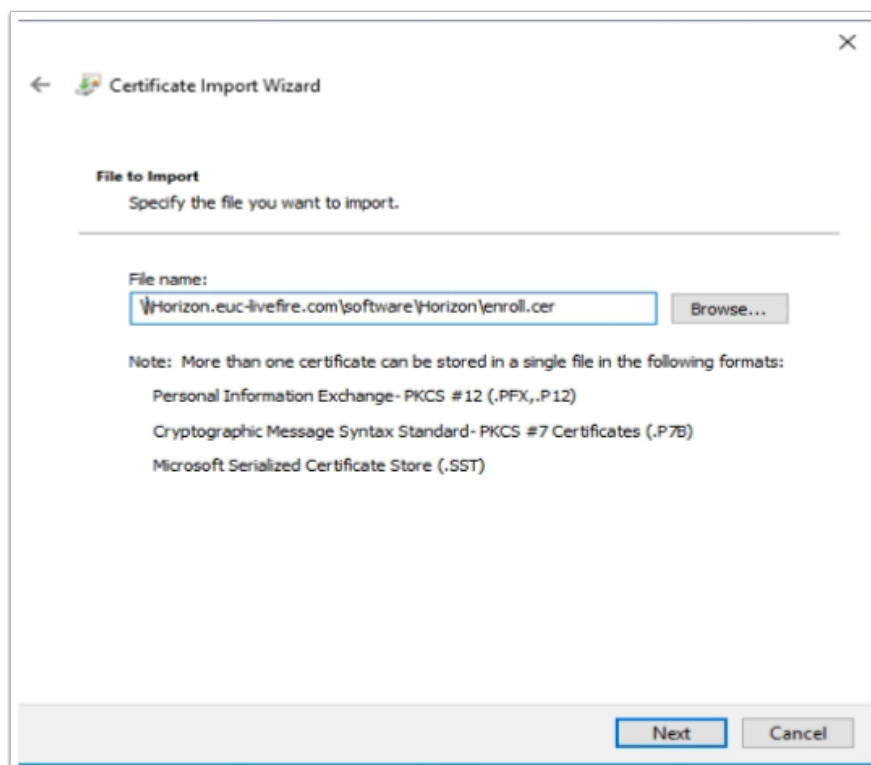
53. On your **ControlCenter** server desktop
- Switch from your **Horizon** RDP session to your **TrueSSO** RDP session



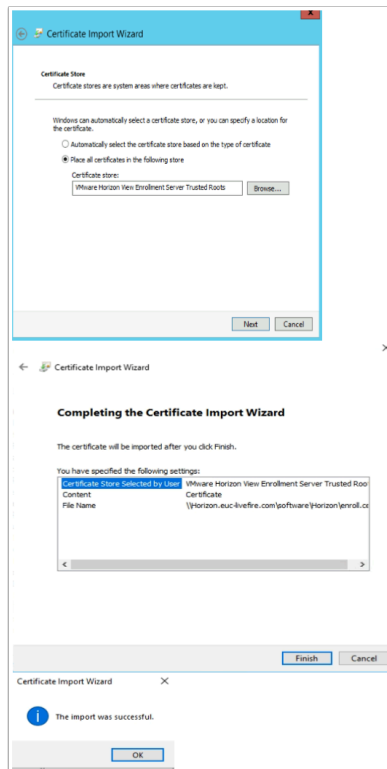
54. On our **TrueSSO** server
- Select your **Certificate services** Snap-in,
 - Select and right-click the last container in the inventory **VMware Horizon View Enrollment Server Trusted Roots**,
 - Select **All Tasks > Import**



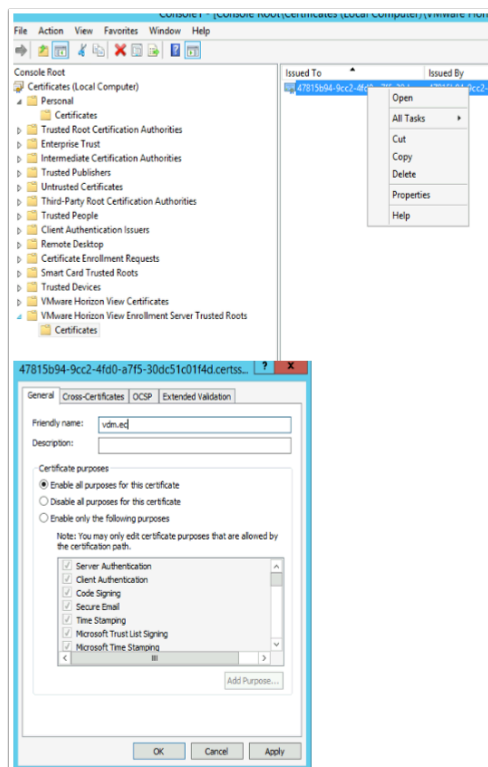
55. On the **Welcome** window select **Next**



56. In the **File to import** window
- Under **File name**, type the following **\\Horizon.euc-livefire.com\\software\\Horizon\\enroll.cer**
 - Select **Next**

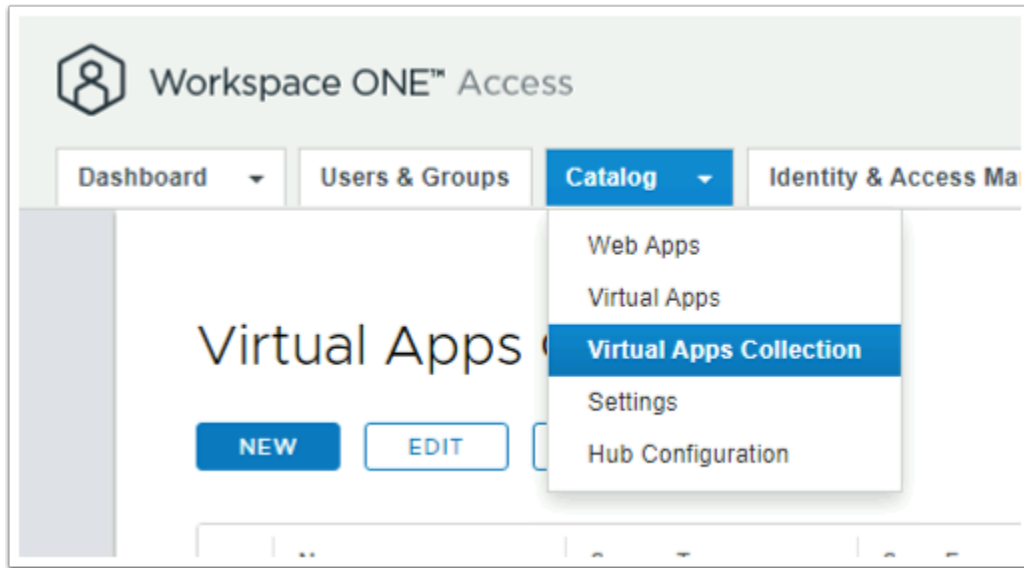


57. In the **Certificate Store** window accept the defaults and
- Select **Next**.
 - On the **Summary** page select **Finish**.
 - When Prompted that **The Import was succesful** select **OK**

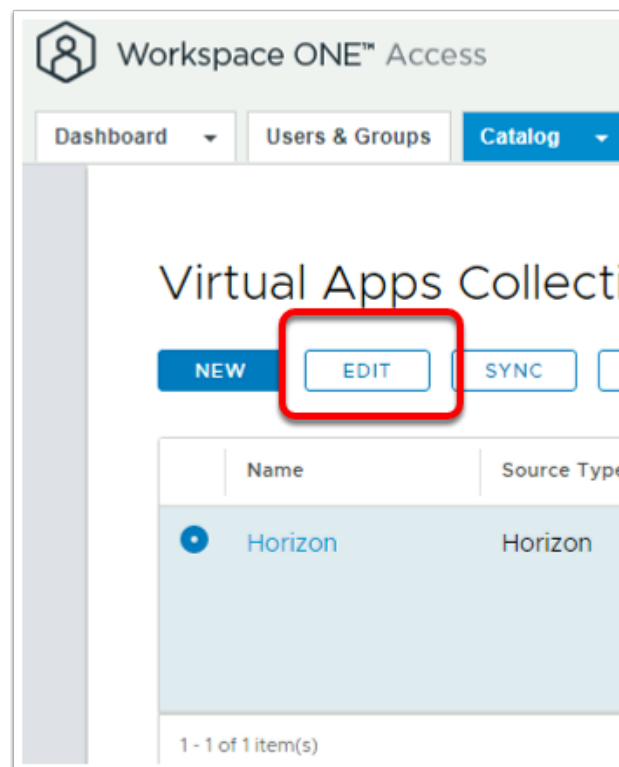


58. In the **Certificates** Folder

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



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



60. Select the **radio button** next **HORIZON**
- Select **EDIT**

Edit Horizon Collection

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

Add or modify pods. If a pod has multiple Horizon information for any of the Horizon Connection !

Horizon Connection Server	Username
Horizon.euc-liveware.com	administrator@euc-liveware.com

[+ ADD A POD](#)

Have you enabled Cloud Pod Architecture for

☐ No

61. In the **Edit Horizon Collection** window,
- Select **2 Pod and Federation**,
 - Under **Horizon Connection Server**
 - Select **Horizon.euc-liveware.com**

Edit Pod

Horizon Connection Server *

Username *

Password *

Smart Card Authentication ☐ Disabled

True SSO ☒ Enabled

Sync Local Assignments ☒ Enabled

[CANCEL](#) [SAVE](#)

[CANCEL](#) [BACK](#) [NEXT](#)

Pod and Federation

Pod

Horizon Connection Server	Username	Smart Card Authentication	True SSO	Sync Local Assignments
Horizon.euc-liveware.com	administrator@euc-liveware.com	Disabled	Enabled	Enabled

Cloud Pod Architecture (CPA)
Disabled

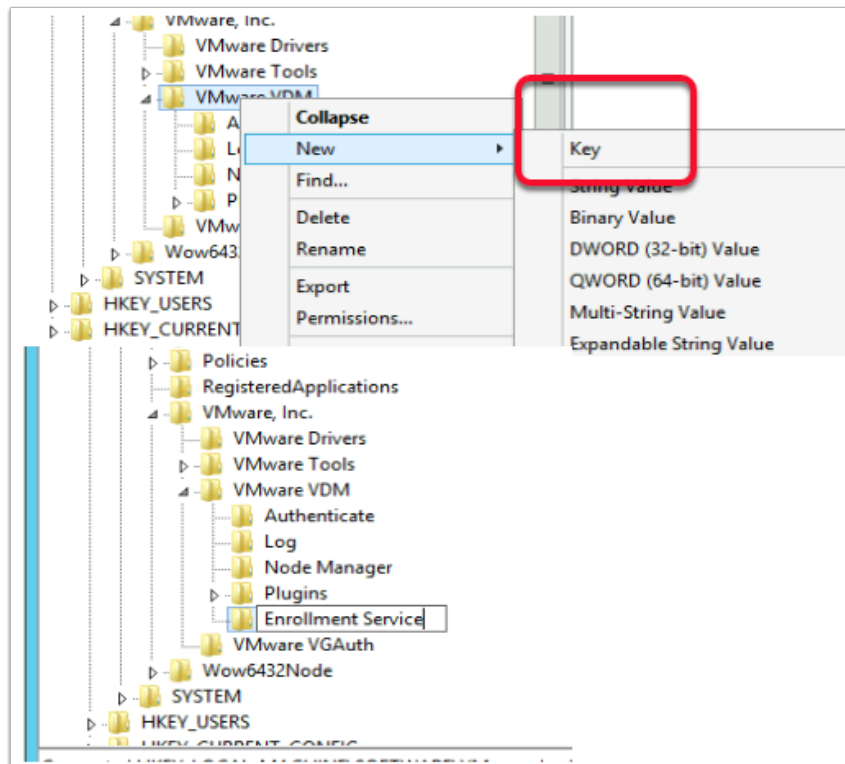
Configuration

Sync

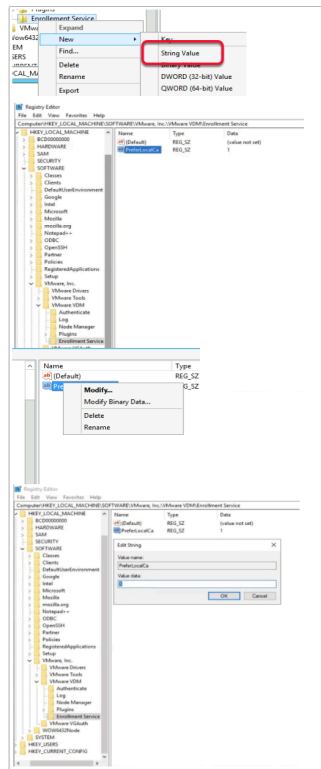
[CANCEL](#) [BACK](#) [SAVE](#)

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

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

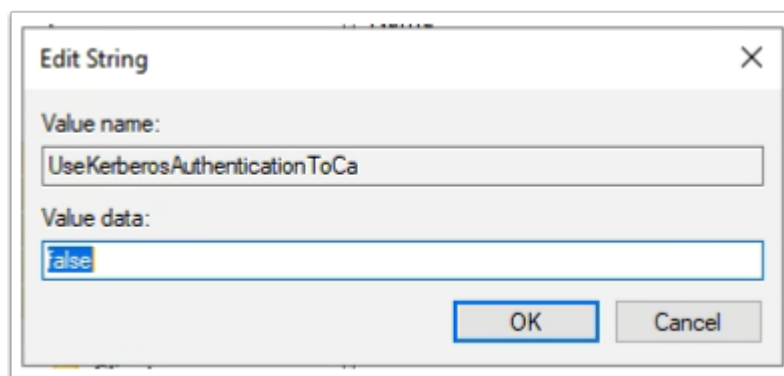


63. On the **ControlCenter** server, switch back to your **TrueSSO.RDP** session
 1. Select the **Start button** > **RUN** and type **regedit.exe**
 2. In the regedit inventory, browse to the following location, browse to
 - **HKLM\SOFTWARE\VMware, Inc.\VMware VDM**
 - What we should see is an **Enrollment 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



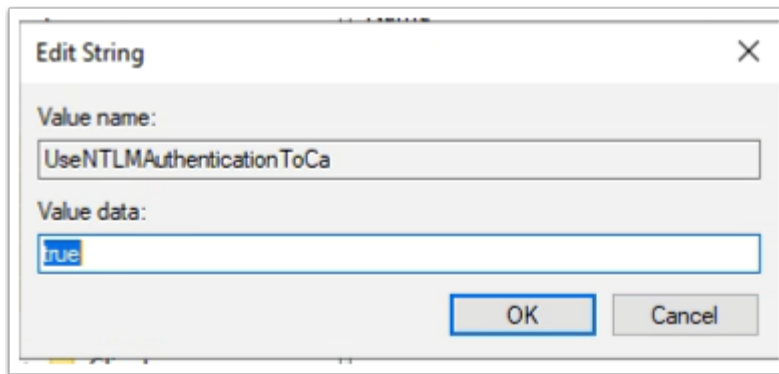
64. Configure the enrollment service to give preference to the local certificate authority when they are co-located:

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



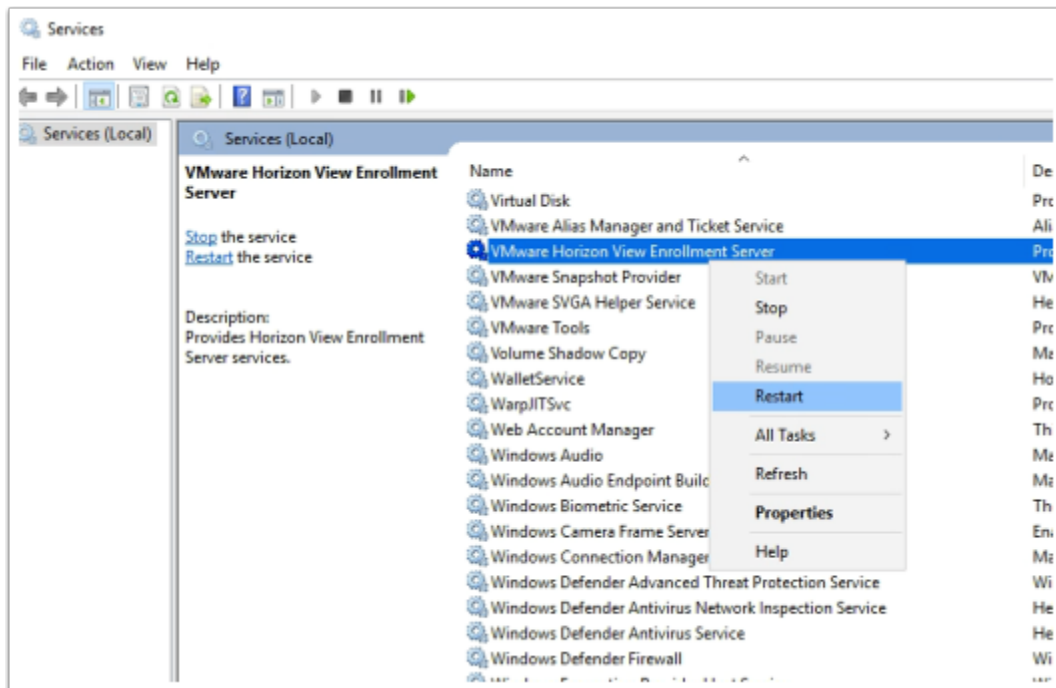
65. Add a new **String Value** (this is to rectify a bug in 2111)

- 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.



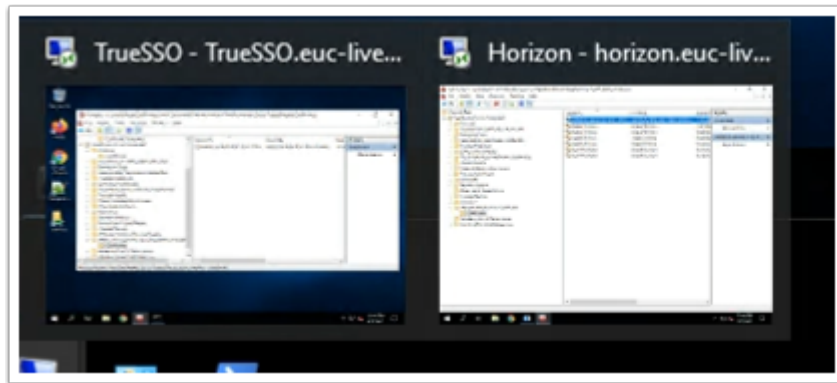
66. Add a new **String Value (this is to rectify a bug in 2111)**

- 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.

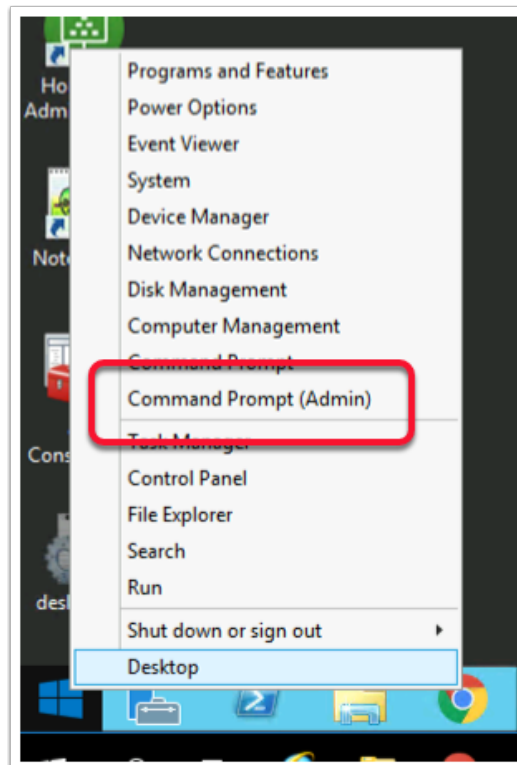


67. On your TrueSSO server

- 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



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



69. 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>
```

70. 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 administrator --authDomain euc-livfire --authPassword VMware1! --truessso --environment --add --enrollmentServer TrueSSO.euc-livfire.com
Enrollment server(s) added to the environment

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

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

The enrollment server is added to the global list.

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

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

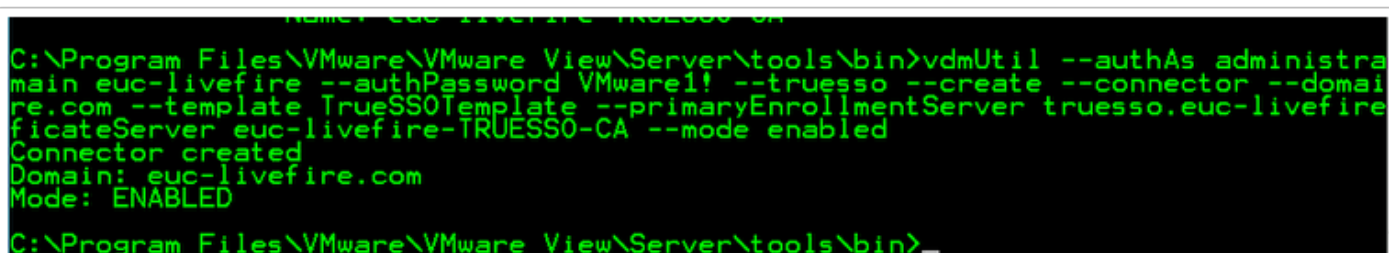
C:\Program Files\VMware\VMware View\Server\tools\bin>
```

72. **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.

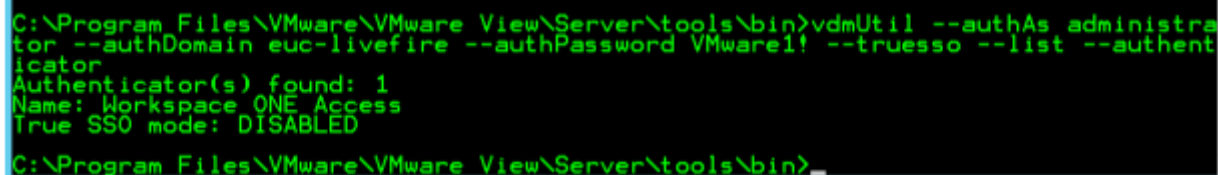
```
vdmUtil --authAs administrator --authDomain euc-liveware --authPassword VMware1! --truessso --environment --list --enrollmentServer TrueSSO.euc-liveware.com --domain euc-liveware.com
```



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

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

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



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

74. 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-liveware --authPassword VMware1! --truessso --list --authenticator
```

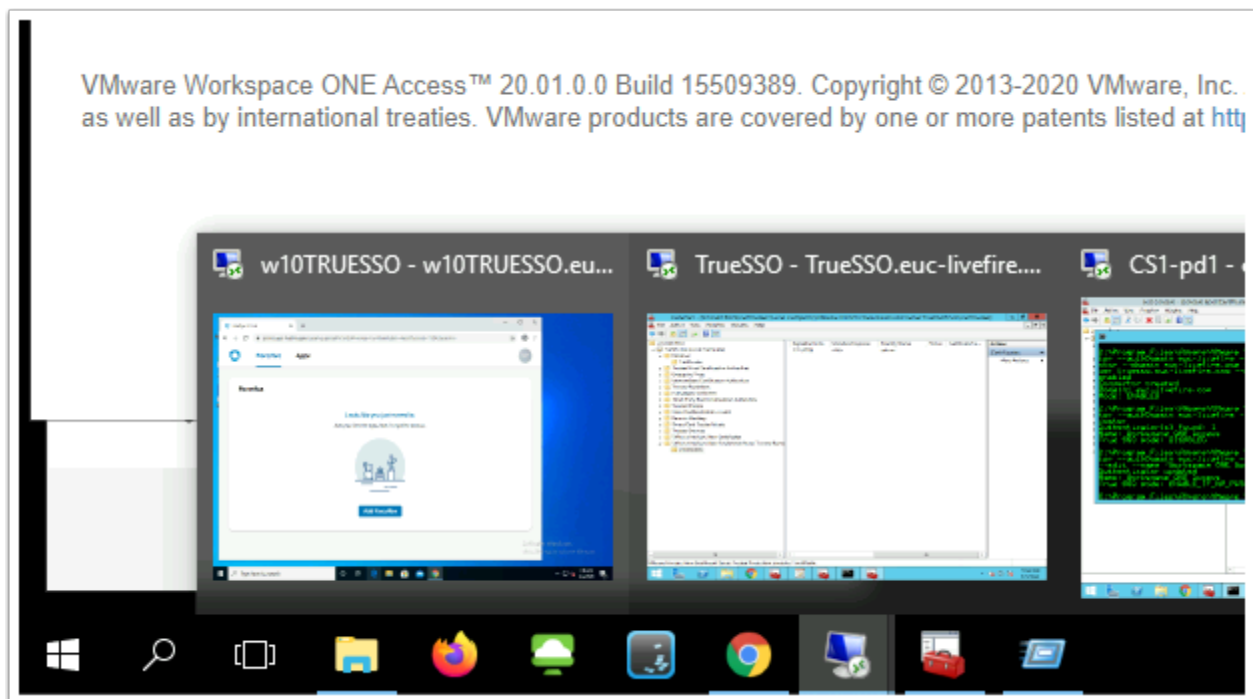
```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administrator --authDomain euc-livfire --authPassword VMware1! --truesso --authenticator --edit --name "Workspace ONE Access" --truessoMode ENABLED
Authenticator updated
Name: Workspace ONE Access
True SSO mode: ENABLE_IF_NO_PASSWORD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

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

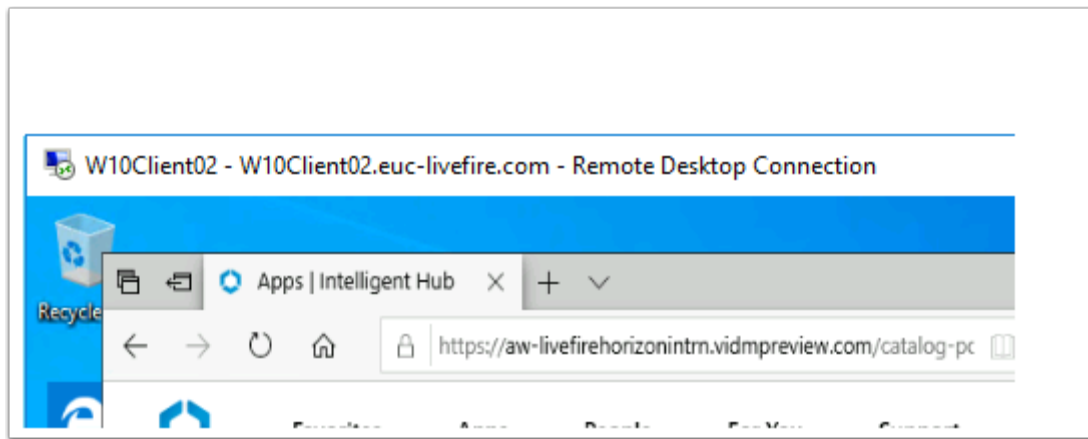
```
vdmUtil --authAs administrator --authDomain euc-livfire --authPassword VMware1! --truesso --authenticator --edit --name "Workspace ONE Access" --truessoMode ENABLED
```

For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to 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

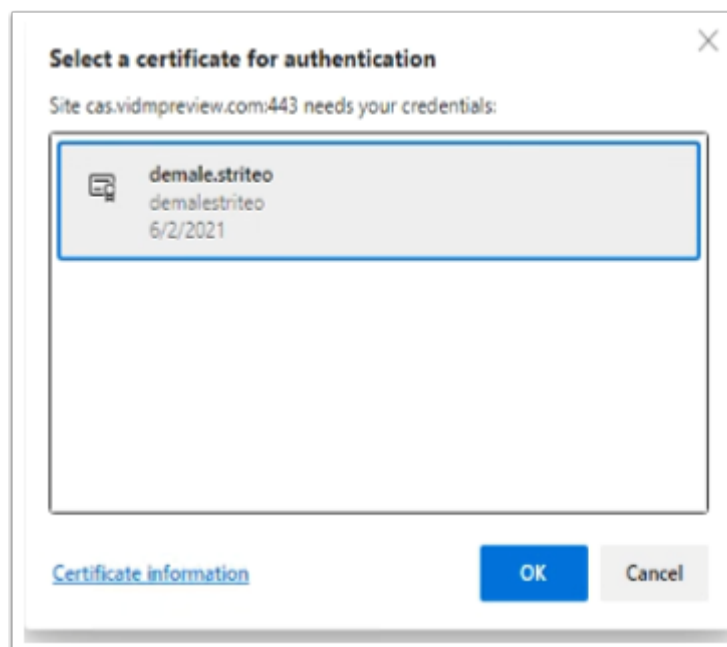
Part 6: Testing to see if TrueSSO works



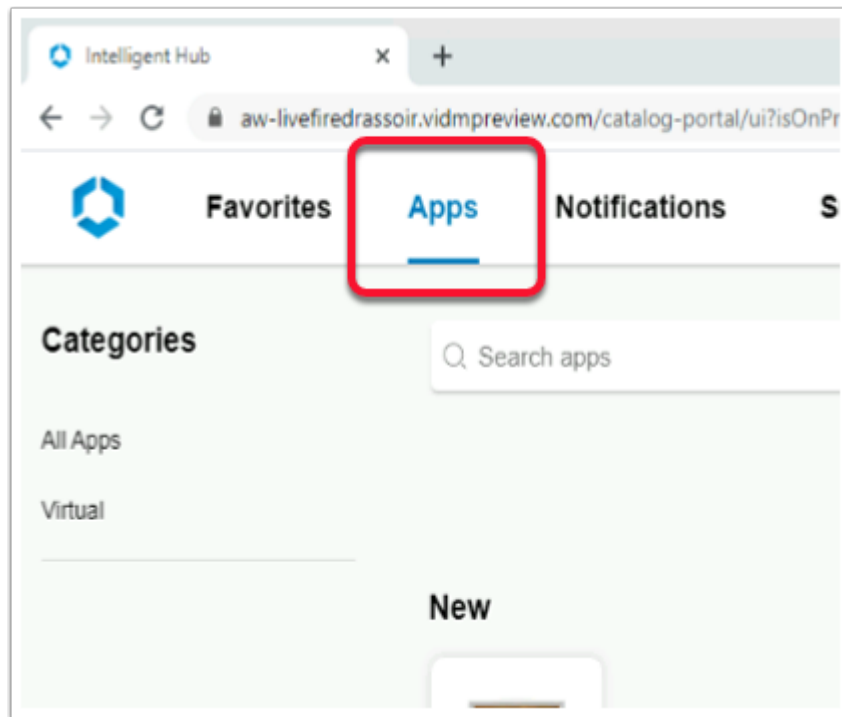
1. On your **ControlCenter** server, switch your **Remote Desktops** session for **W10Client01.RDP**.



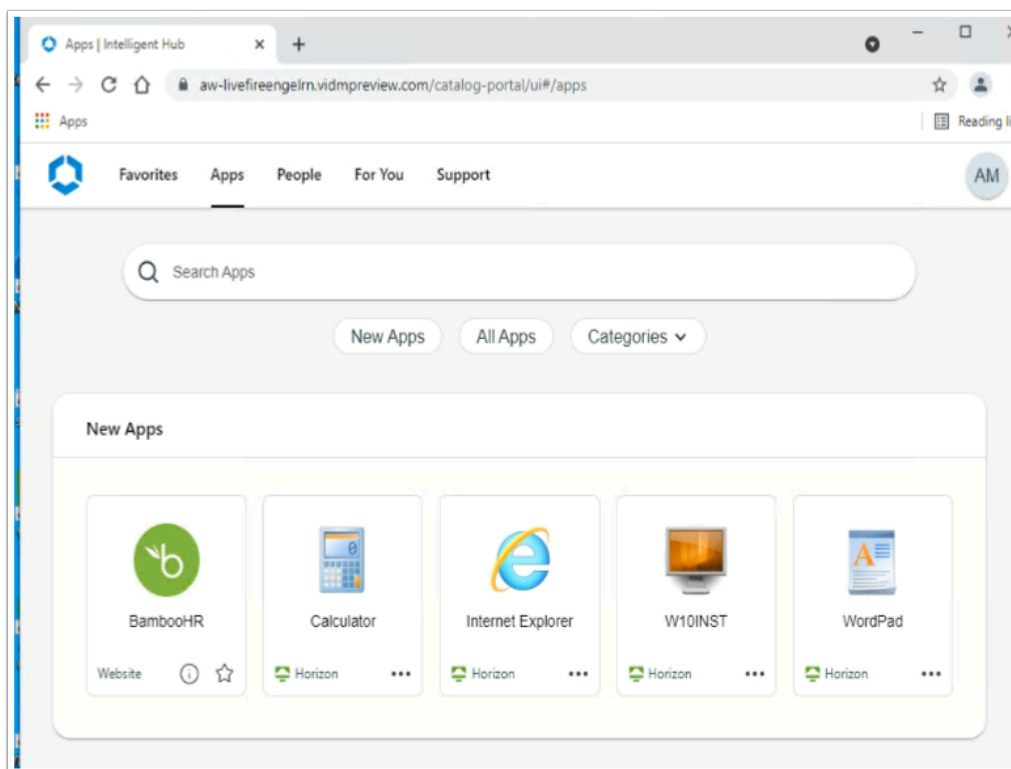
2. On your **W10Client01** desktop, ensure that any existing browser session is **CLOSED**
 - **Open** your browser and type enter your custom **Access Tenant URL**



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

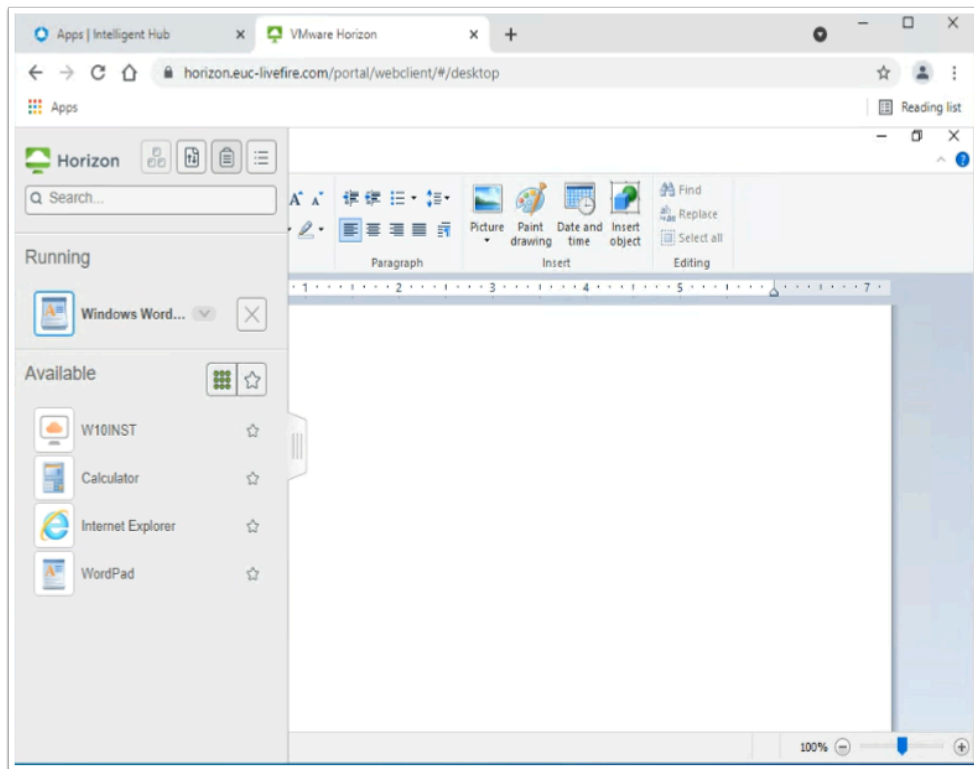


4. Select **Apps** tab in the Console

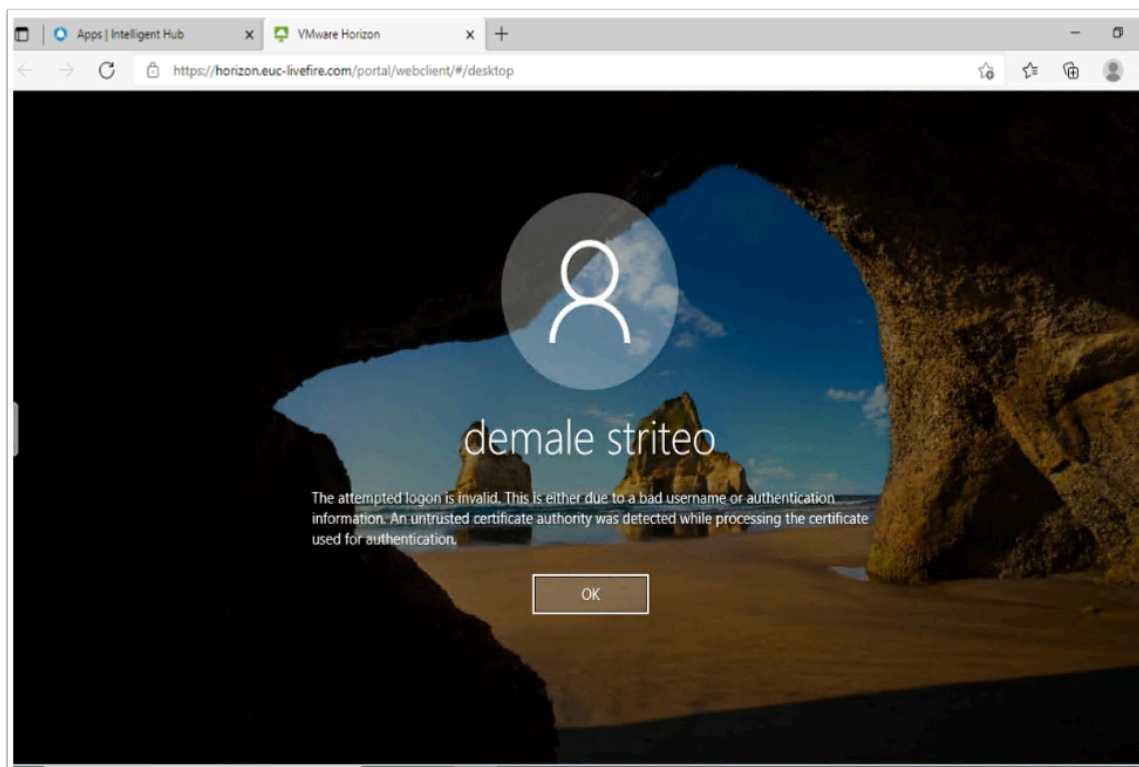


5. In the Web based Intelligent Hub

- In the **Apps** area, under **New Apps** select **Wordpad**

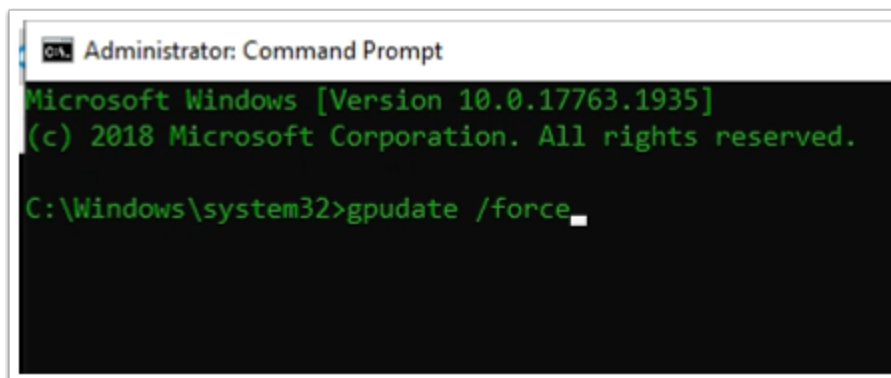


6. On the W10Client01
 - Note your WordPad session launch
 - Launch the **W10INST** desktop pool
 - If this is not the result, move on to **Step 8**



7. This might be the result. If so, move on to **Step 8**

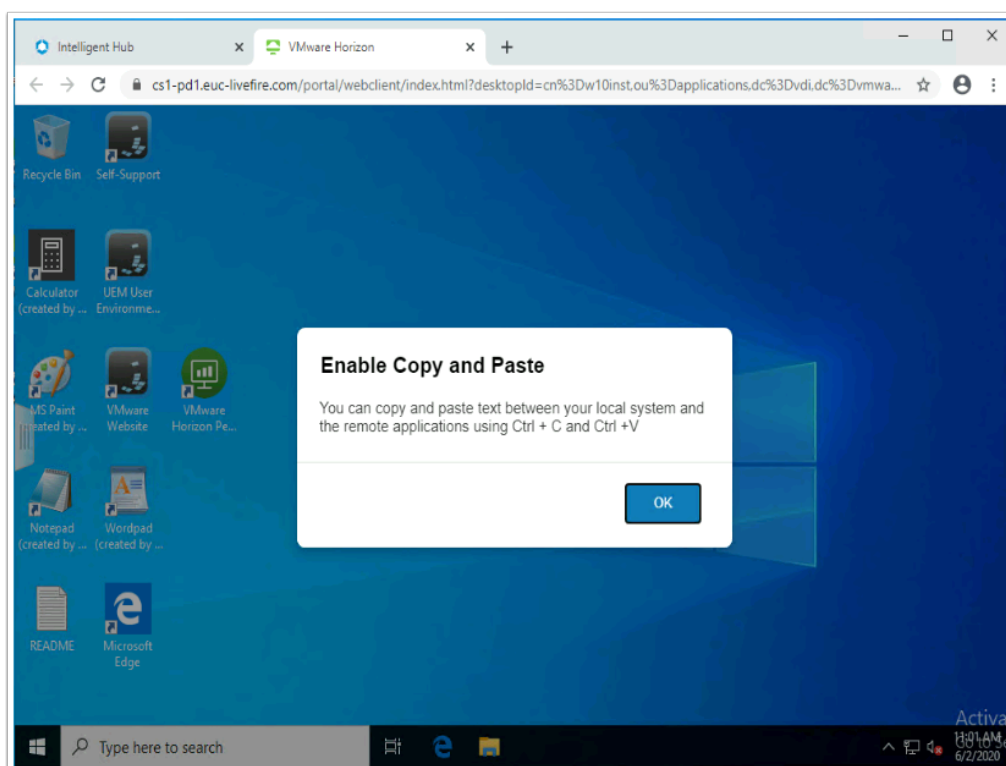
- As we mentioned early, for VMware Horizon Enrolment services to work, it critical we have a Healthy Certificate Services environment.
- Also an environment where our new sub-ordinate CA is trusted on all servers.
- The Servers we are concerned with are the Horizon and Control Center servers



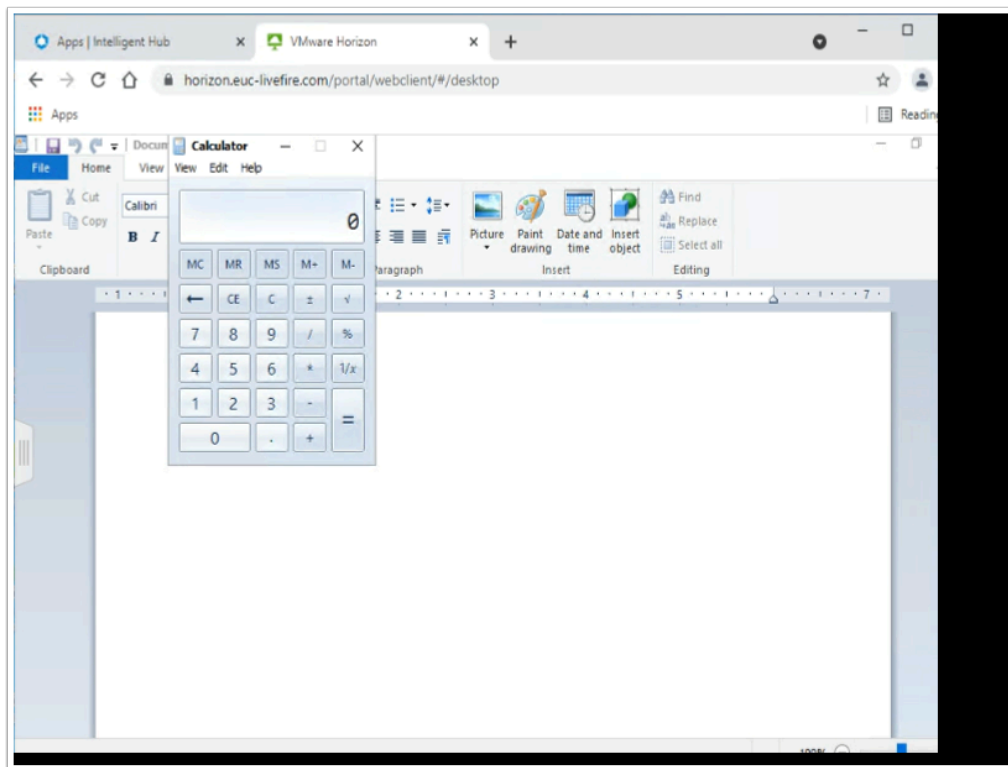
8. On the ControlCenter server

- Open the **Command Prompt** on all **stakeholder platforms** and type the command **GPUPDATE /Force**
- Repeat this same task on the Horizon server

You are now ready to again test your login through **Workspace ONE Access**. If necessary go back to Paragraph1 and repeat the login process



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



10. Launch another session from the **Workspace ONE** portal and launch an **Application** entitlement.
- This could be the result, I have just launched Calculator and WordPad

Acknowledgments

A Huge thank you to

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

References

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

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

About the Author: Reinhart Nel

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

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