Chapter 9 : Installing and Configuring Horizon TRUESSO

Overview

Traditionally when authenticating to Workspace ONE Access using a 3rd party authentication method, the user we 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

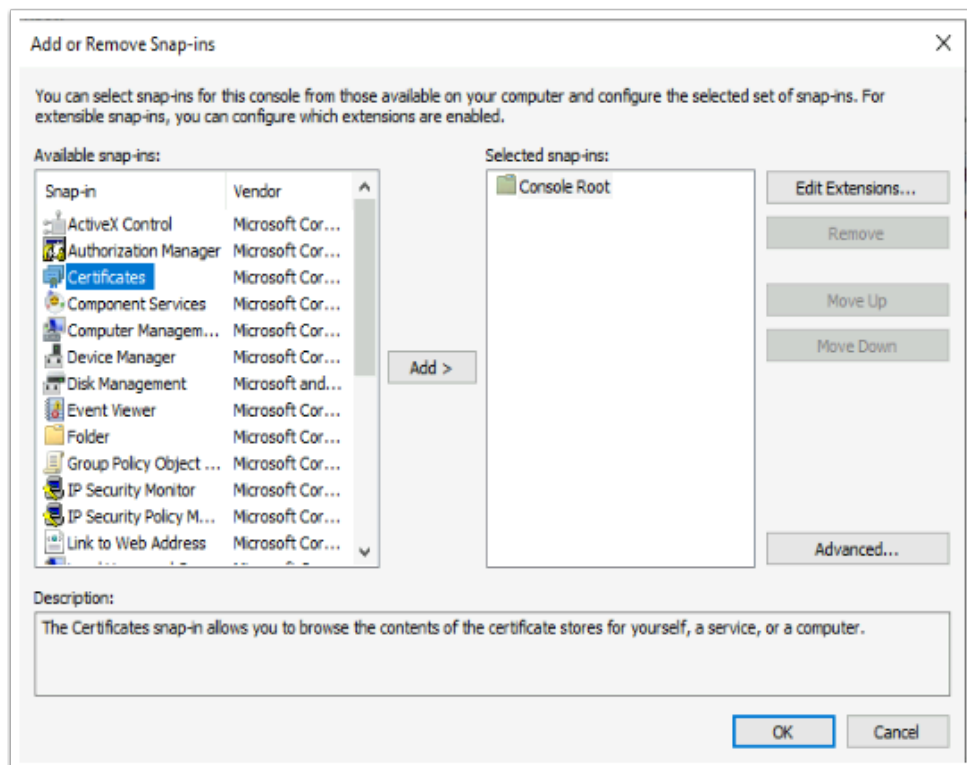# Part 1: Log into a Windows 10 Desktop and demonstrate the limitation
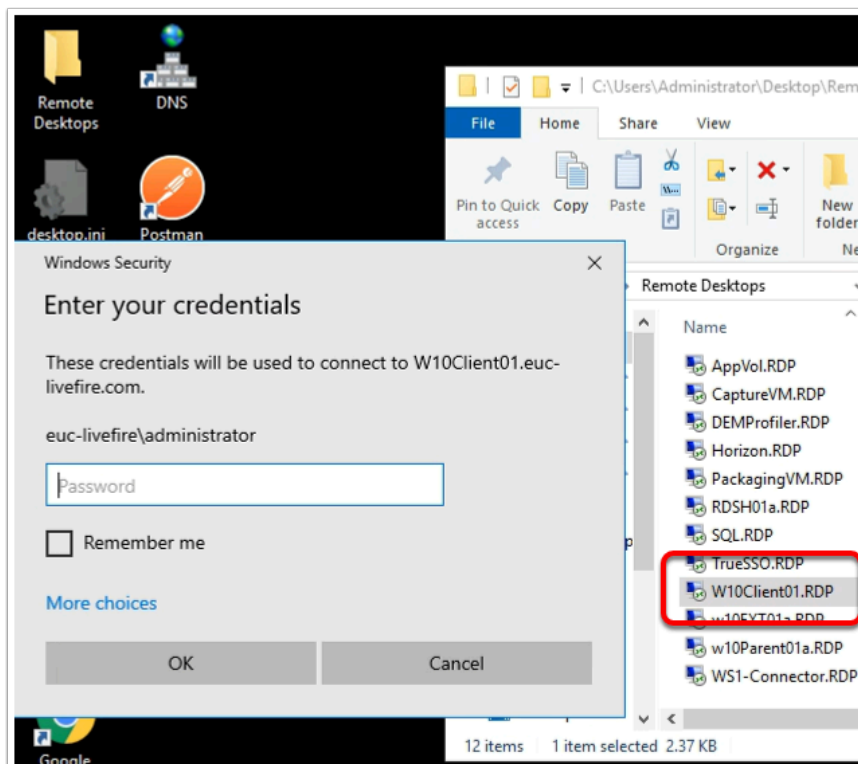
1. On the **ControlCenter** server Desktop,
    • Open the **Remote Desktops** folder,
    • Select the **W10Client01.RDP** shortcut
    • Log in as **EUC-Livefire\administrator**, enter the password **VMware1!,**
    • Select **OK**
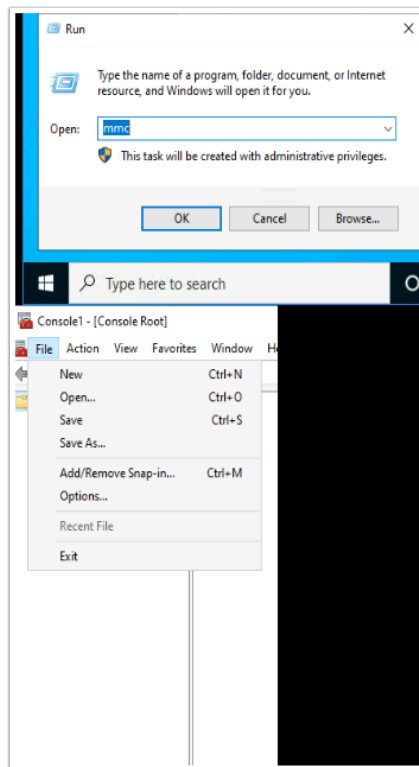
2. On **W10Client01** desktop
    - Select **Start** > **Run**,
    - Next to **Open**, type **mmc**,
    - Select **OK**
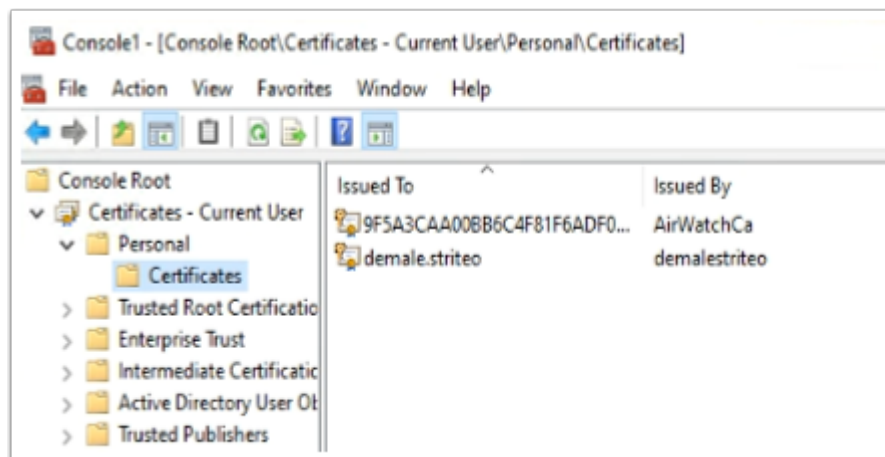   - In the **Console**, select **Add/Remove Snap-in**

3. In the **Add or Remove Snap-ins** window
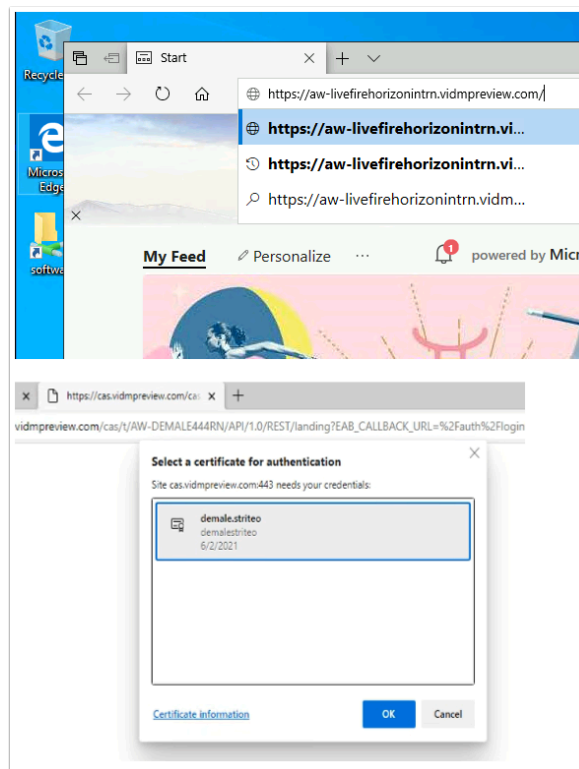   - Select **Certificates**,
   - Select **Add**
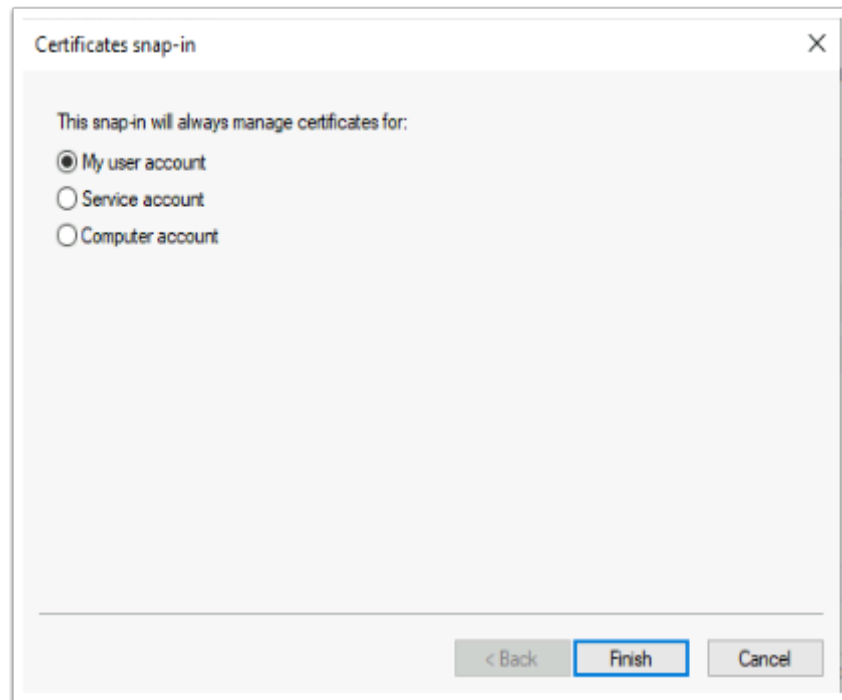
4. In the **Certificates snap-in**, accept the Defaults, select **Finish**
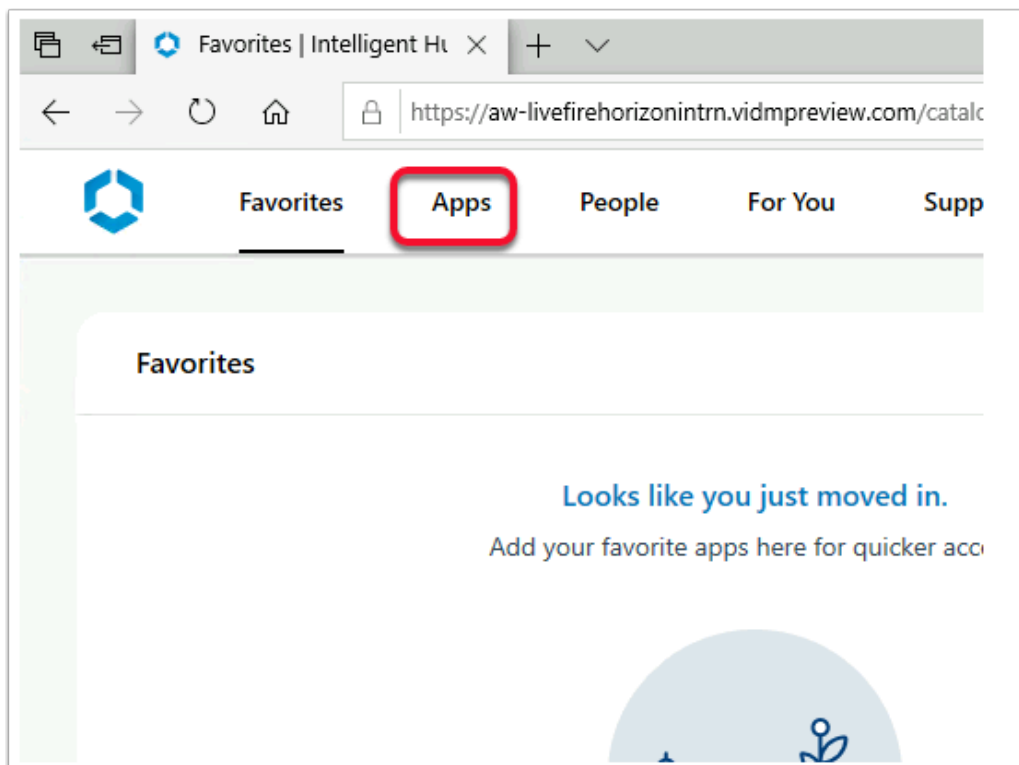   - Select **OK**

5. **Expand** **Certificates - Current User**
   - **Expand** **Personal**
   - Select **Certificates**
     - Note you have an enrolled certificate. If you dont 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
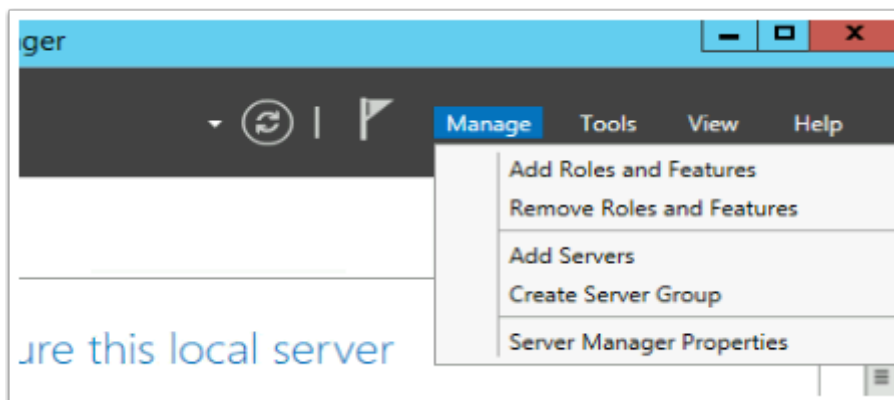   - Select **OK**

7. On the **Workspace ONE** console ,
   • Select the **Apps** tab
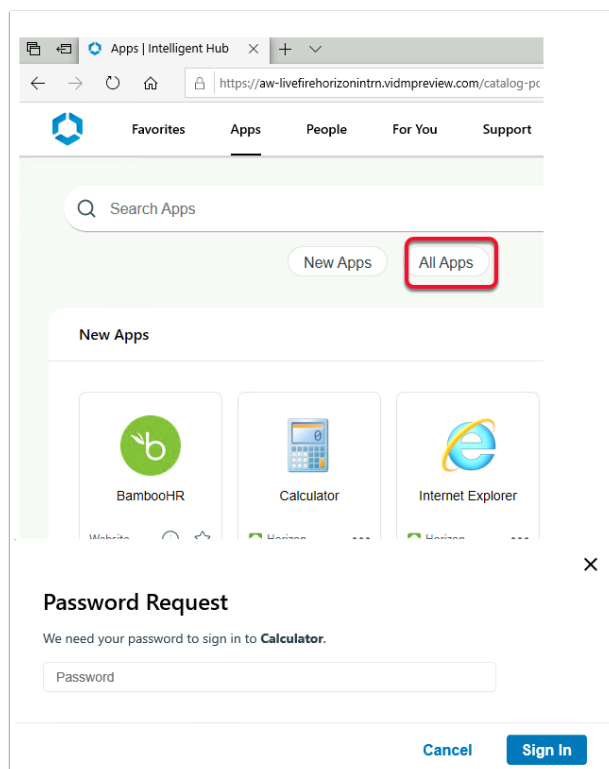
8. Select **Calculator**,
   • Notice we are getting a Password request.
      • The 1st reason is, we used a 3rd party Auth method to login to Workspace ONE Access. (In our session a Certificate based Auth method was used) Workspace ONE Access did not have the UPN it would have received from a password 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 2. 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-livefire\administrator** and enter the password **VMware1!**
   - On the **Server Manager** Interface select **Manage** > **Add Roles and Features**
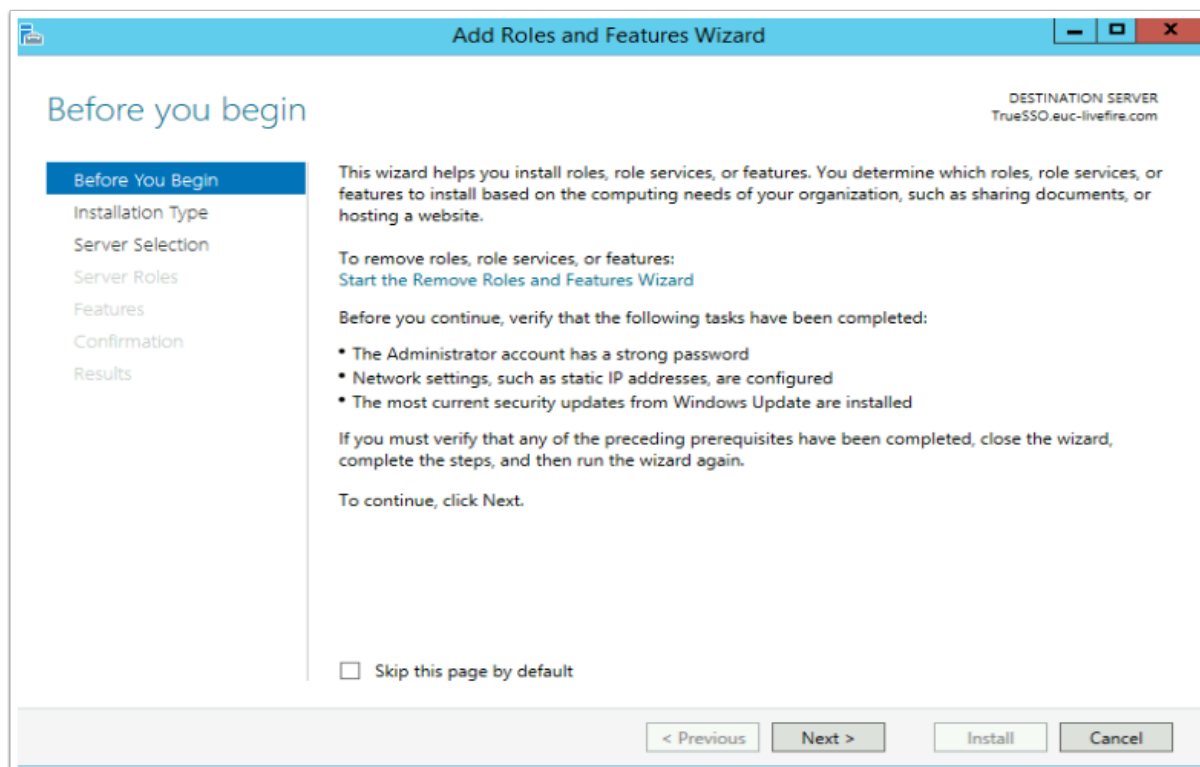
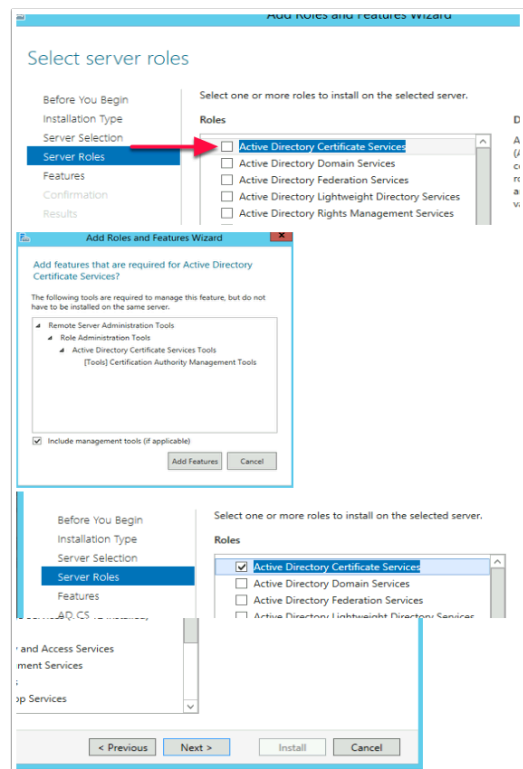2. On the **Before you begin** window
   - Select **Next**
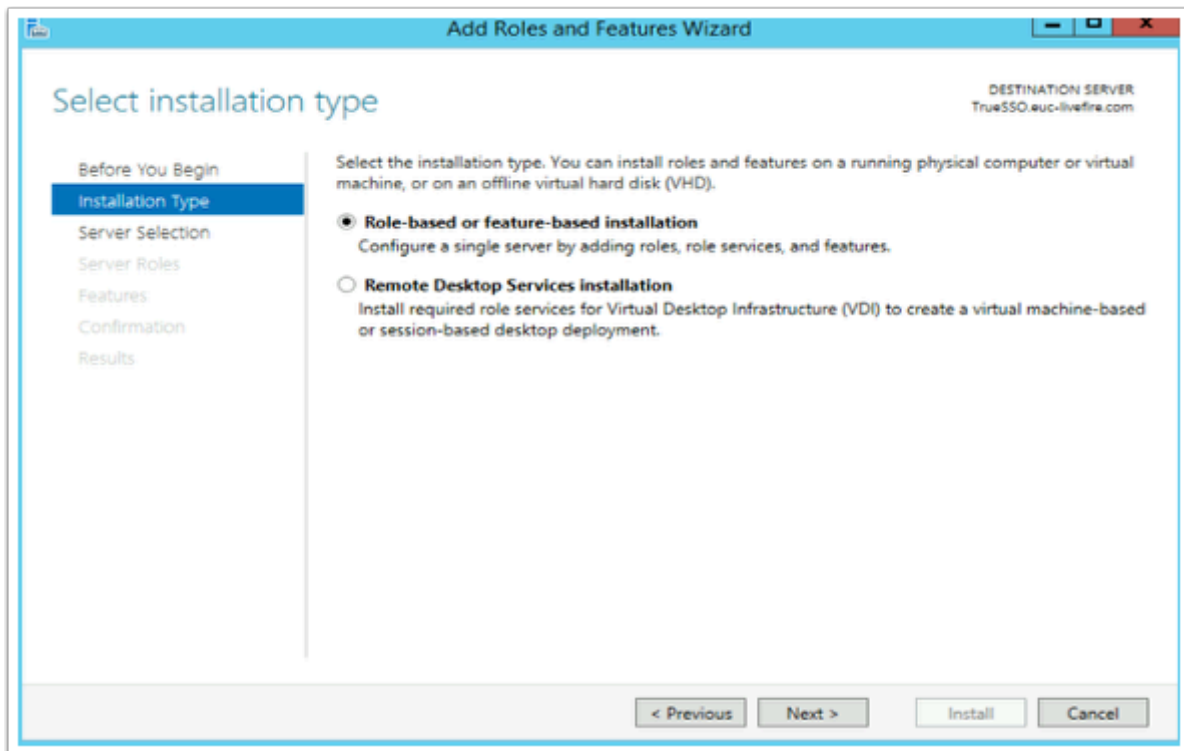
3. On the **Select installation type** window,
   - Ensure the **radio button** in front of **Role-based or feature-based installation** is selected
   - Select **Next**
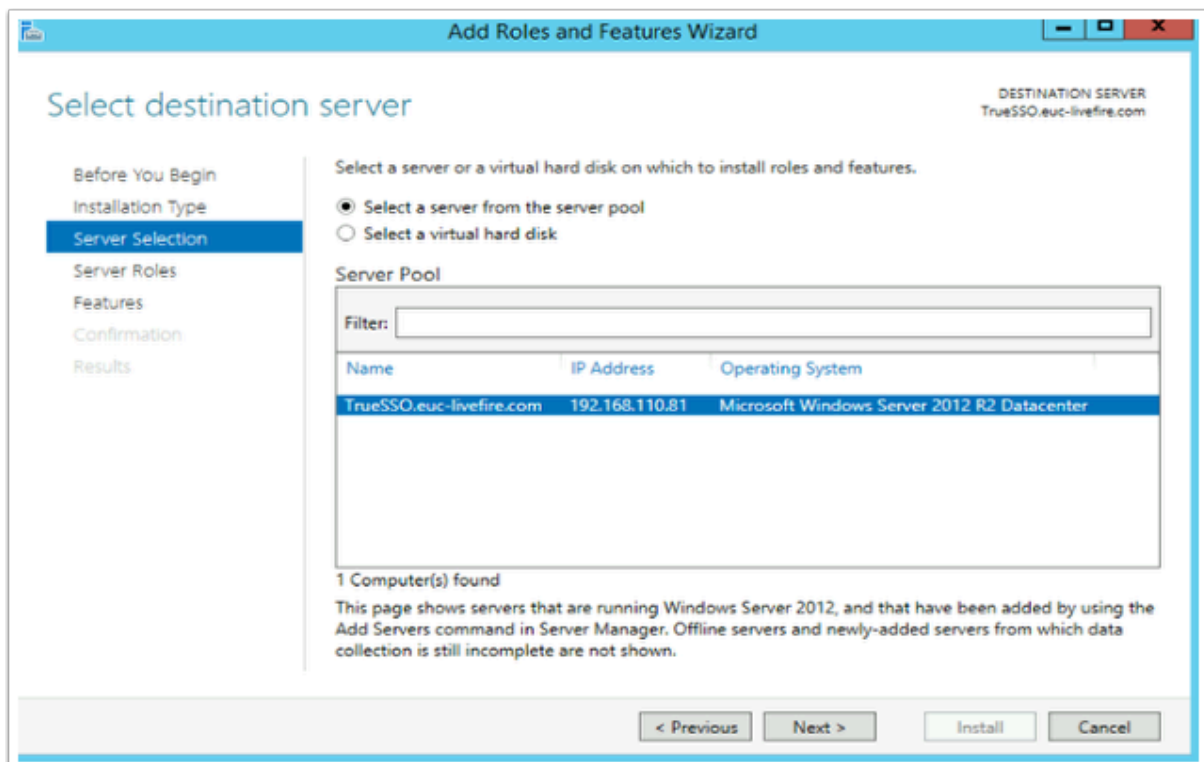
4. On **Select destination server** window (accept the defaults)

- 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**
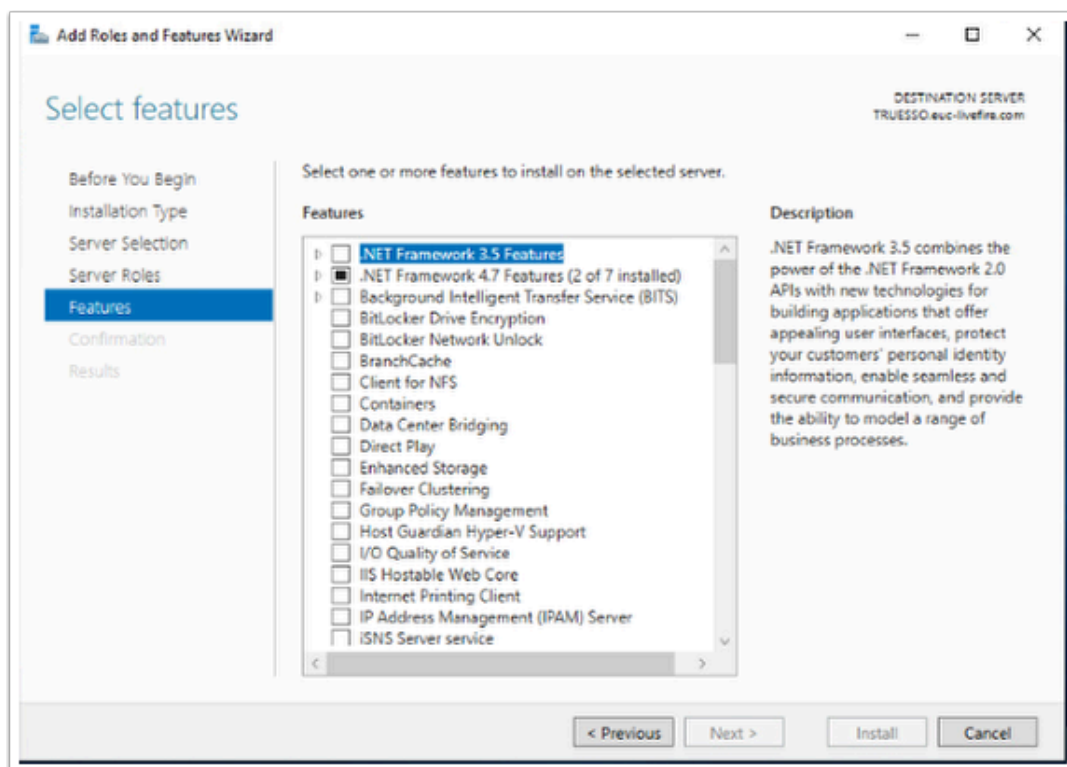
6. On the **Select features** window
   - Select **Next**
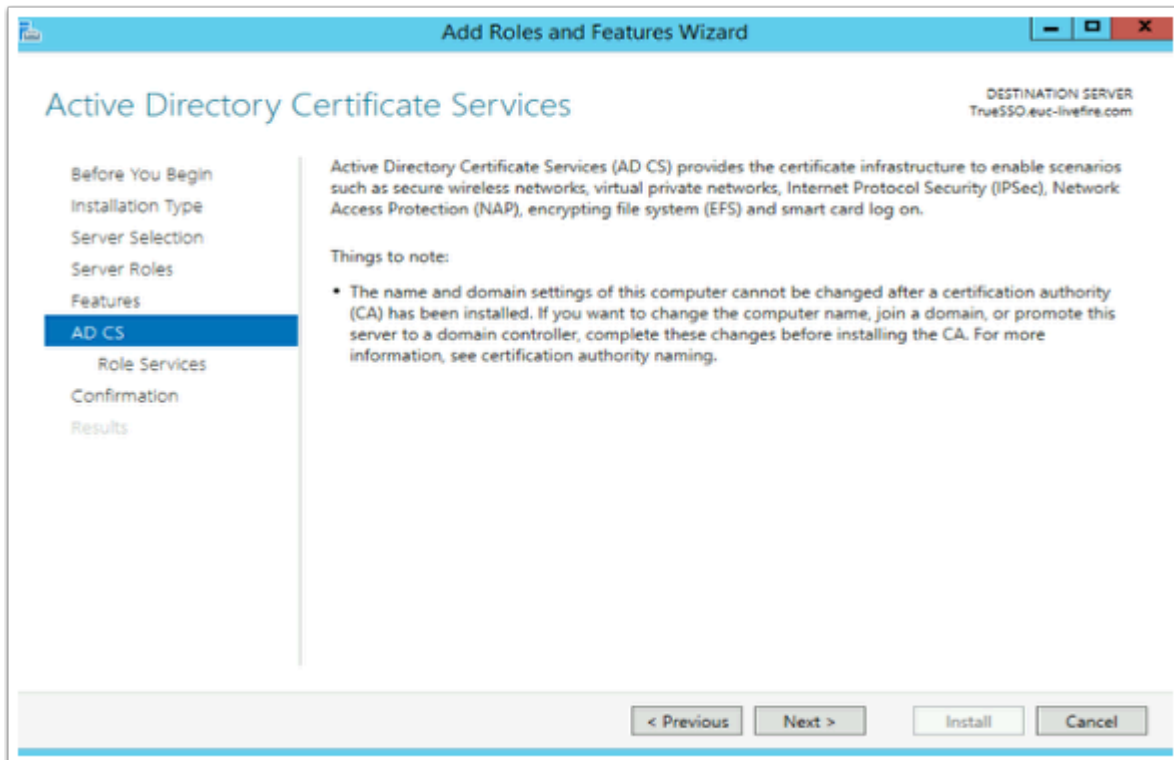
7. On the **Active Directory Certificate Services** window
   - Select **Next**
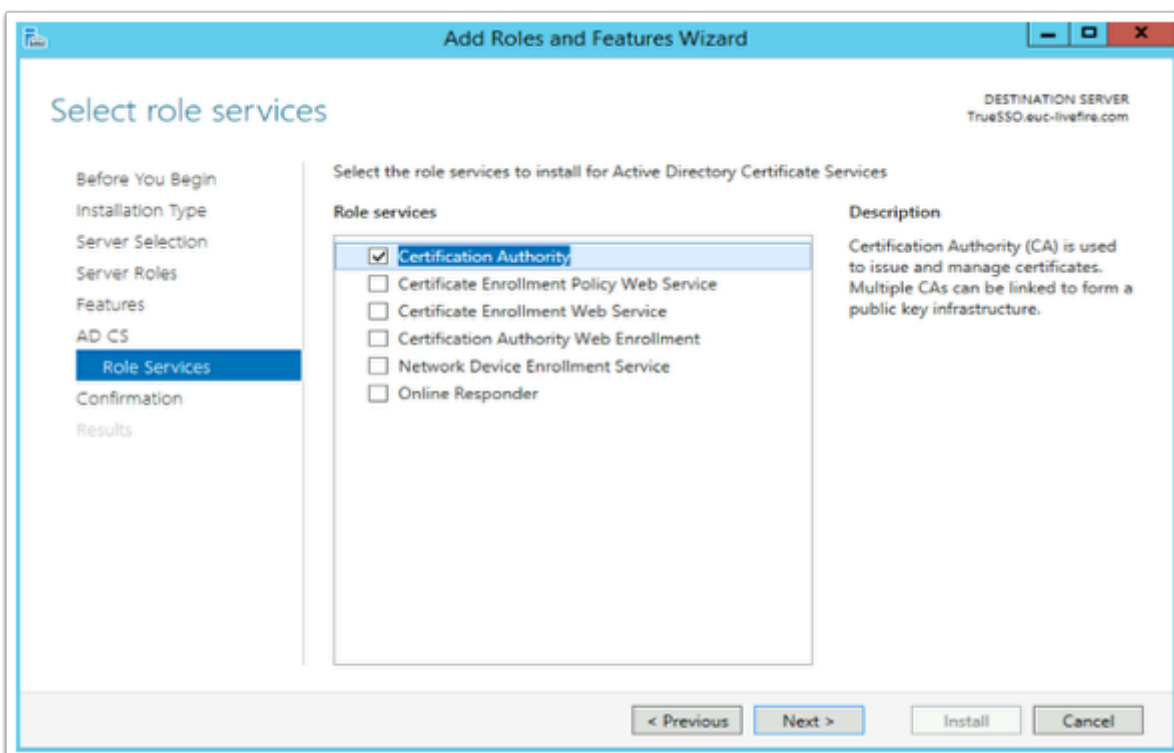
8. On the **Select role services** window

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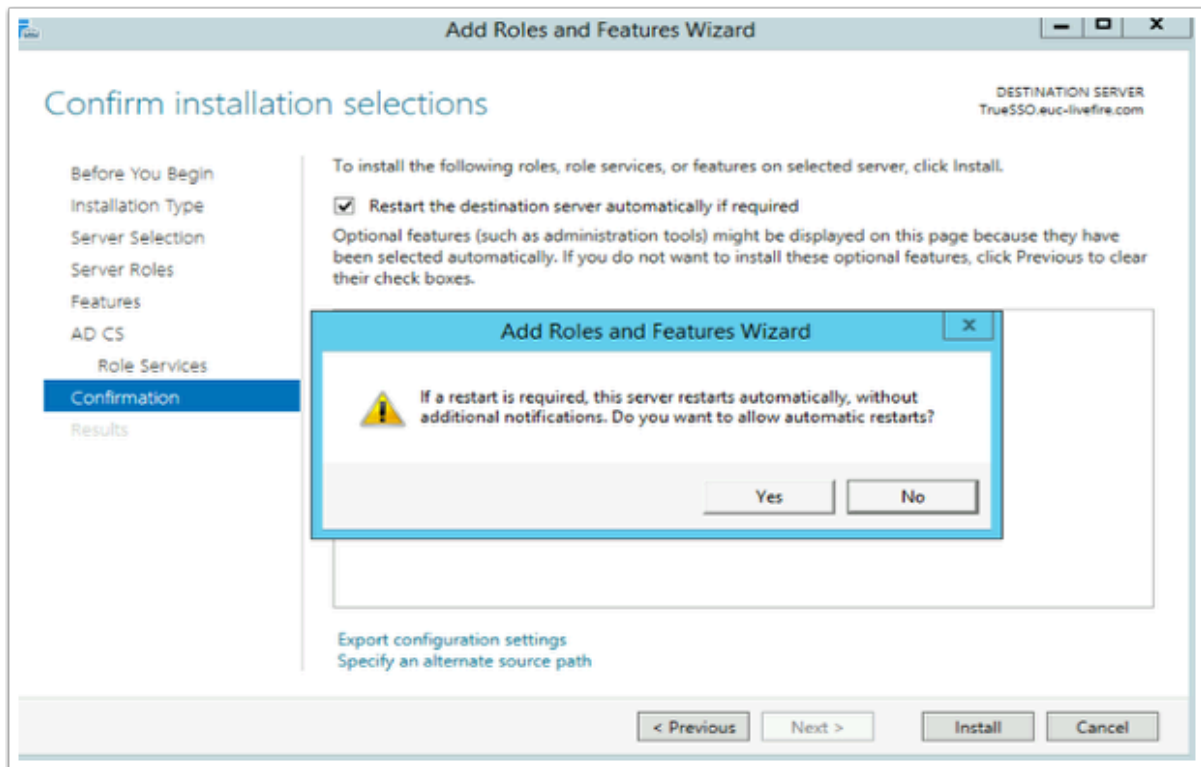
9. On the **Confirm Installation selections** window,
   - Select the **checkbox** next to **Restart the destination server automatically if required,**
   - On the **Add Roles and Features Wizard** window select **Yes**
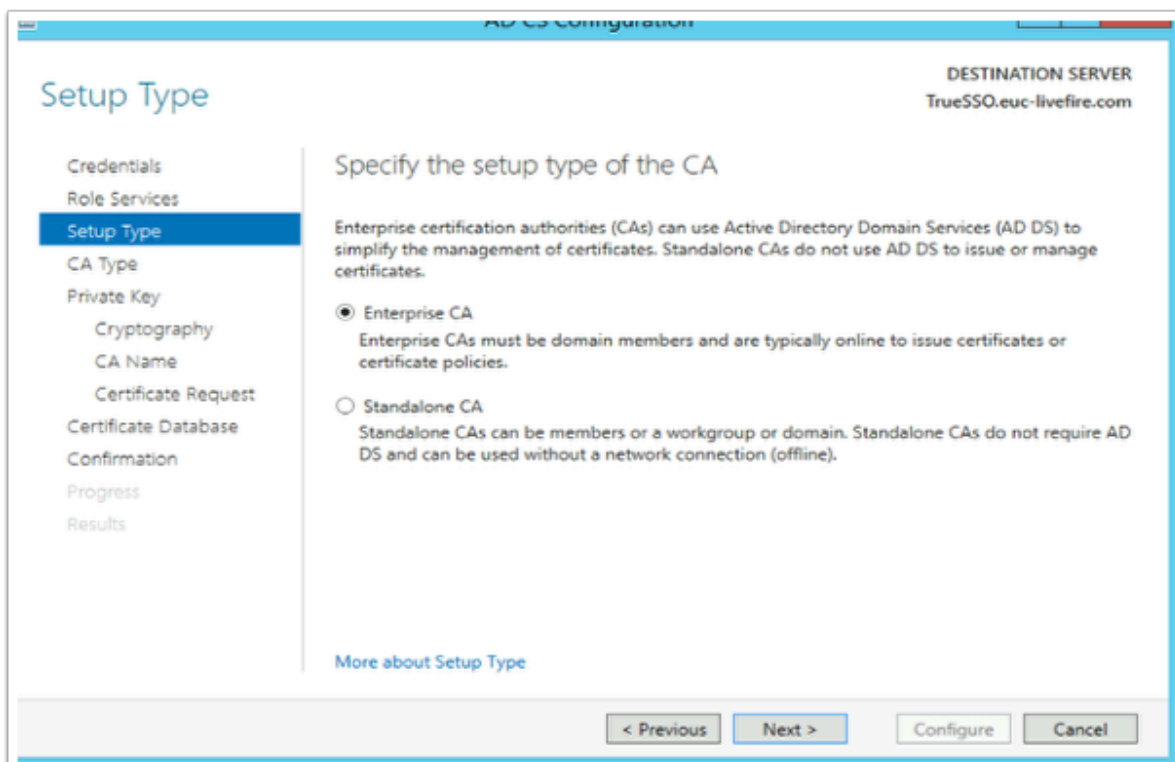   - Select **Install**

You will have to wait a short while before moving on to step 10
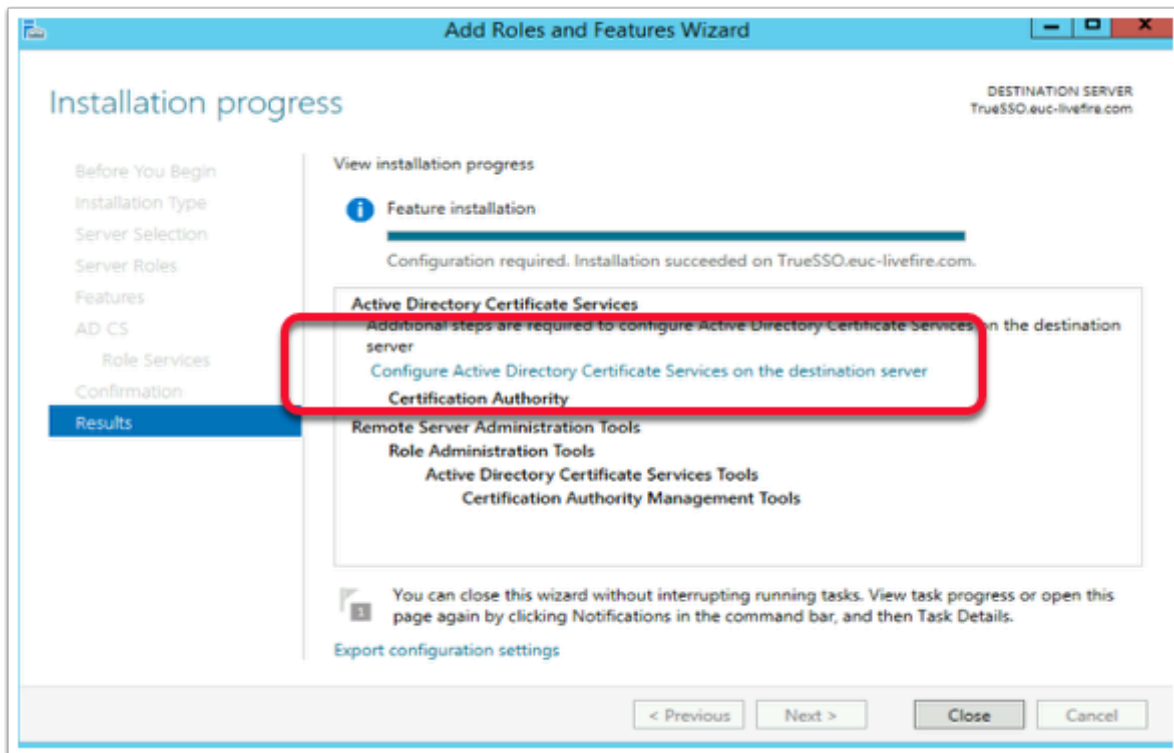
10. On the **Installation progress** page,
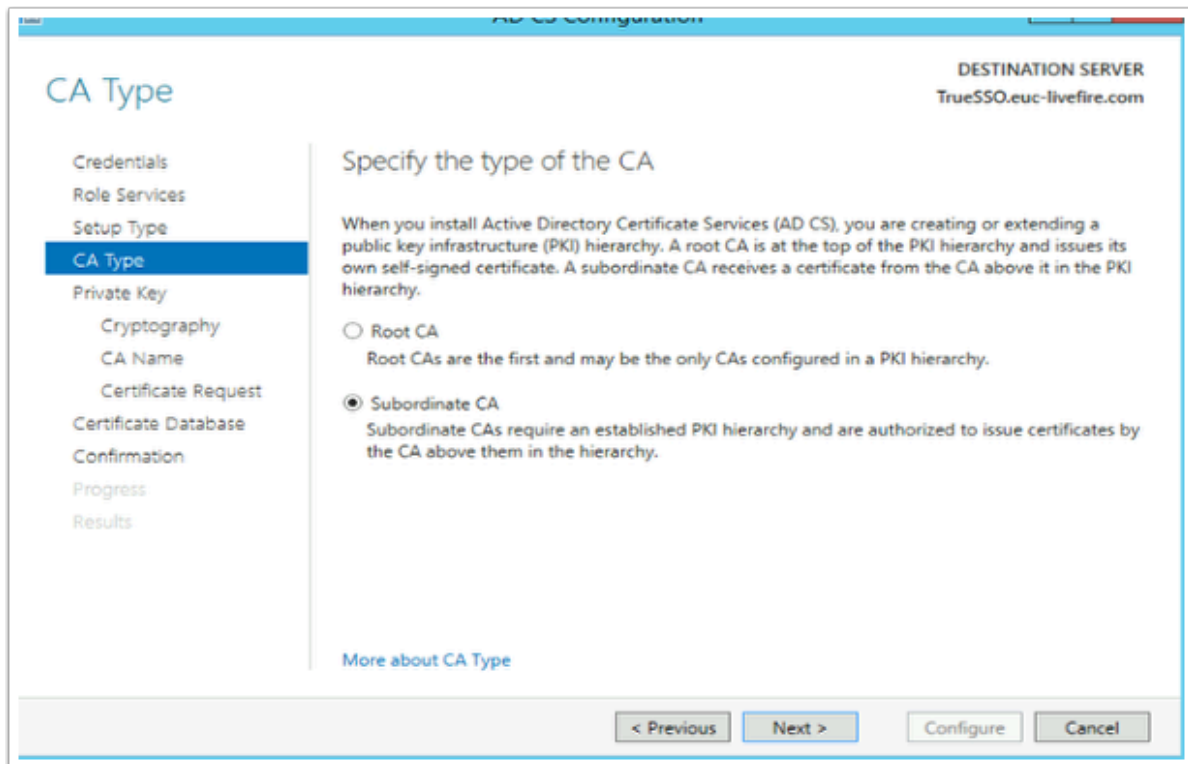   - Select the **Configure Active Directory Certificate Services on the destination server** hyper-link
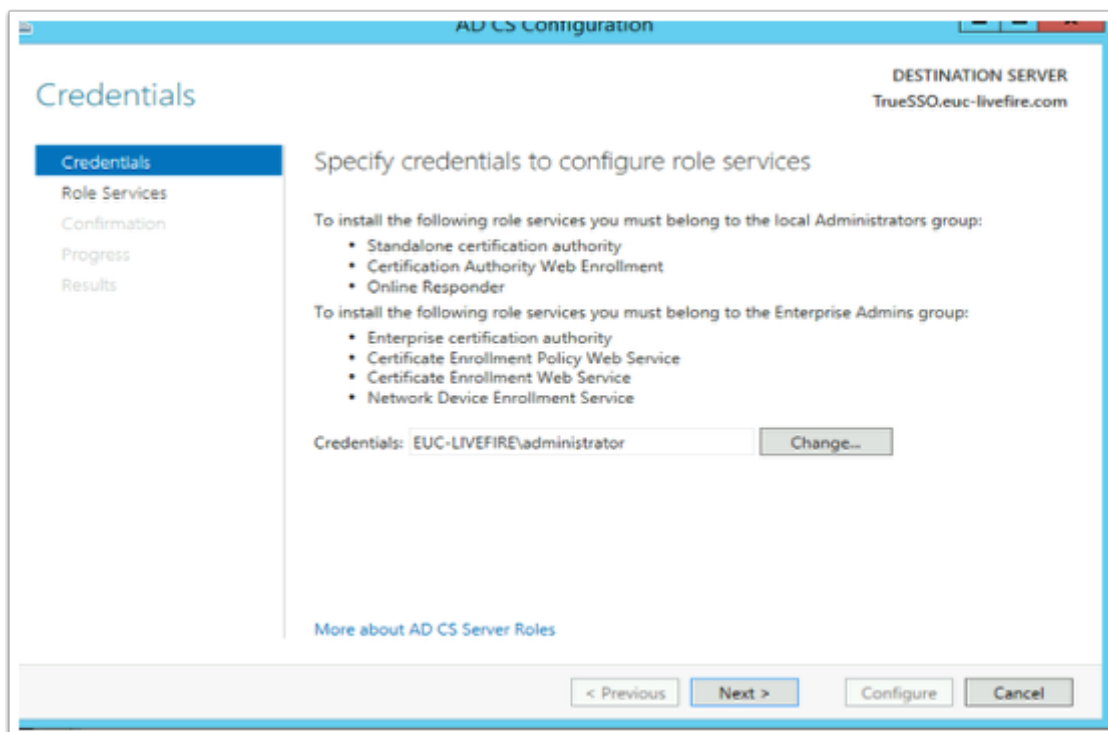
11. On the **Credentials** window
    - Select **Next**
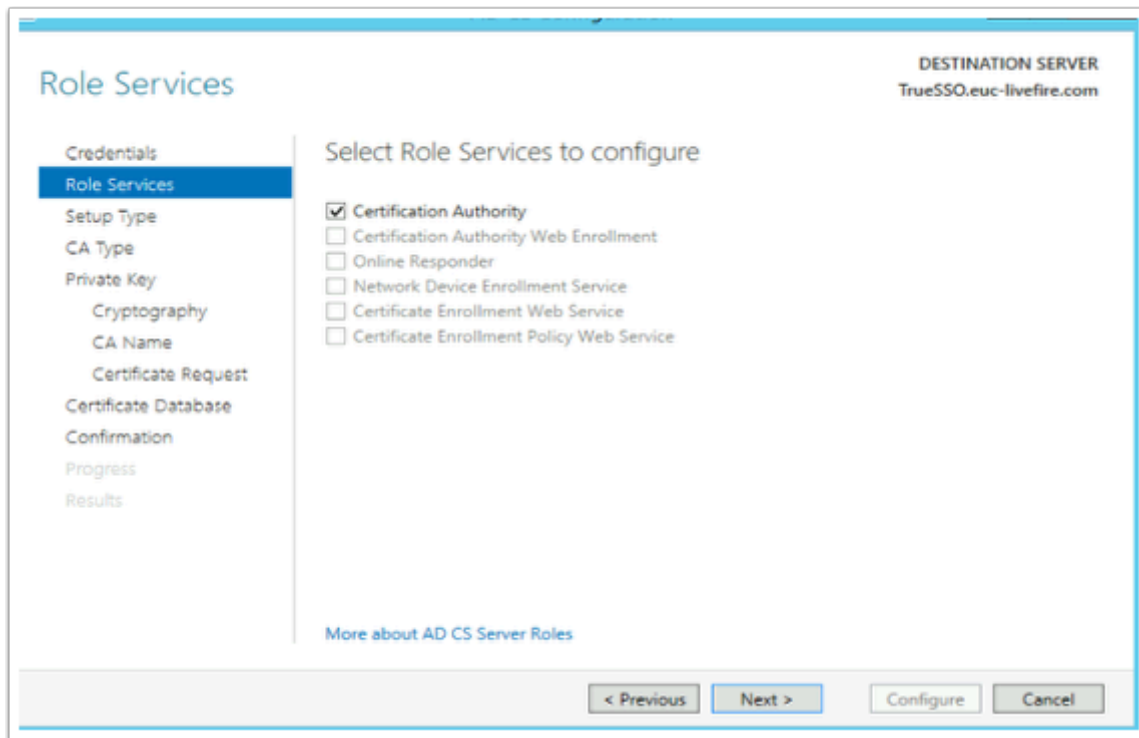
12. On the **Role Services** page,
    - Select the **Certificate Authority checkbox**
    - Select **Next**

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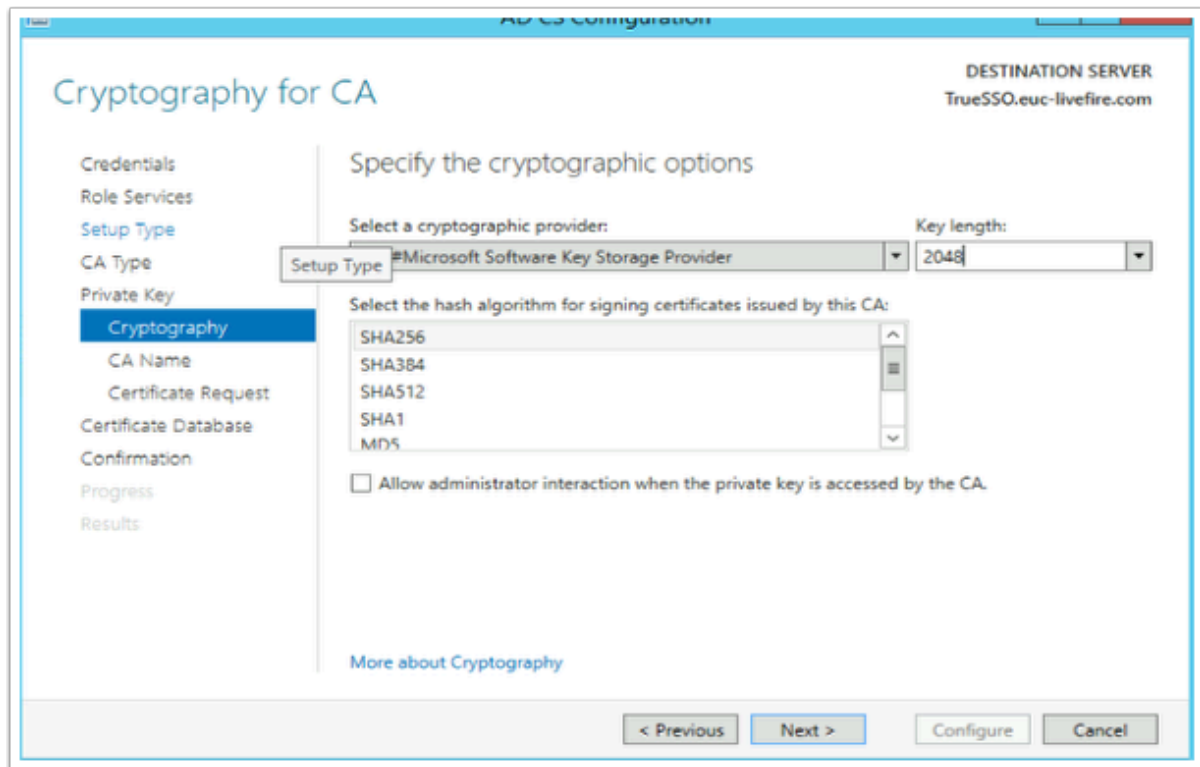   - Select the **radio button** next to **Enterprise CA**
    - Select **Next**

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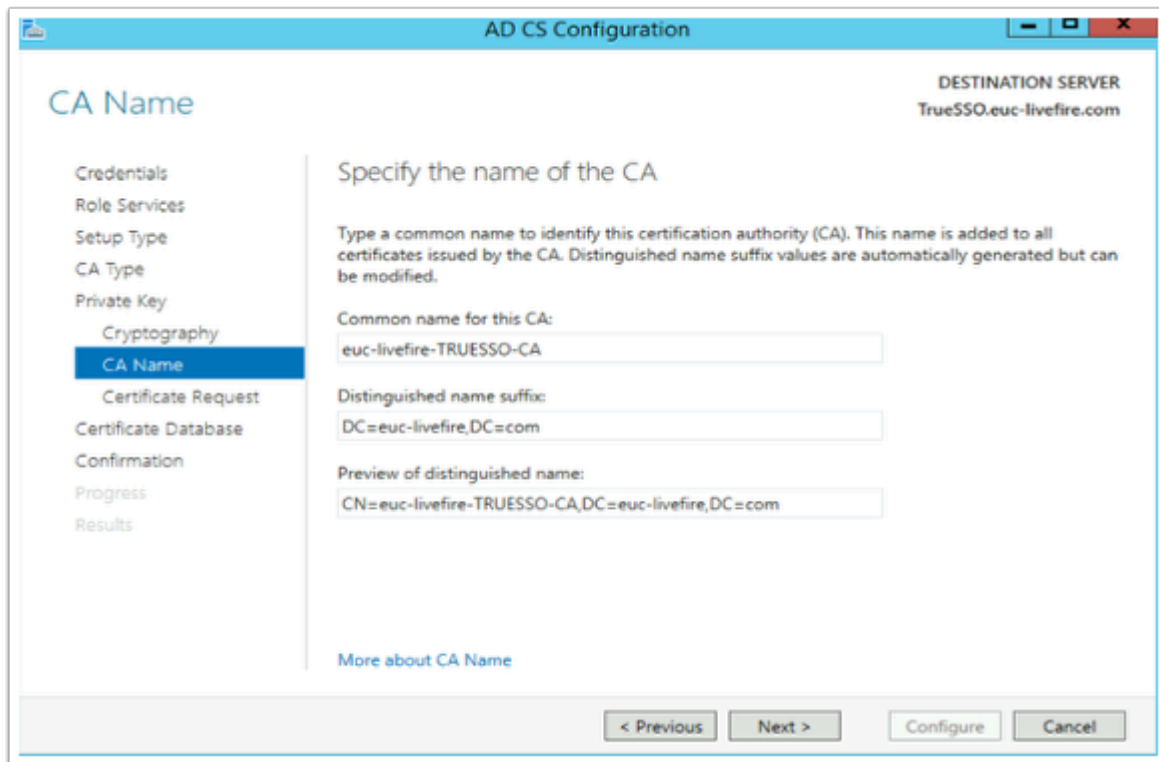   - Select **Next**
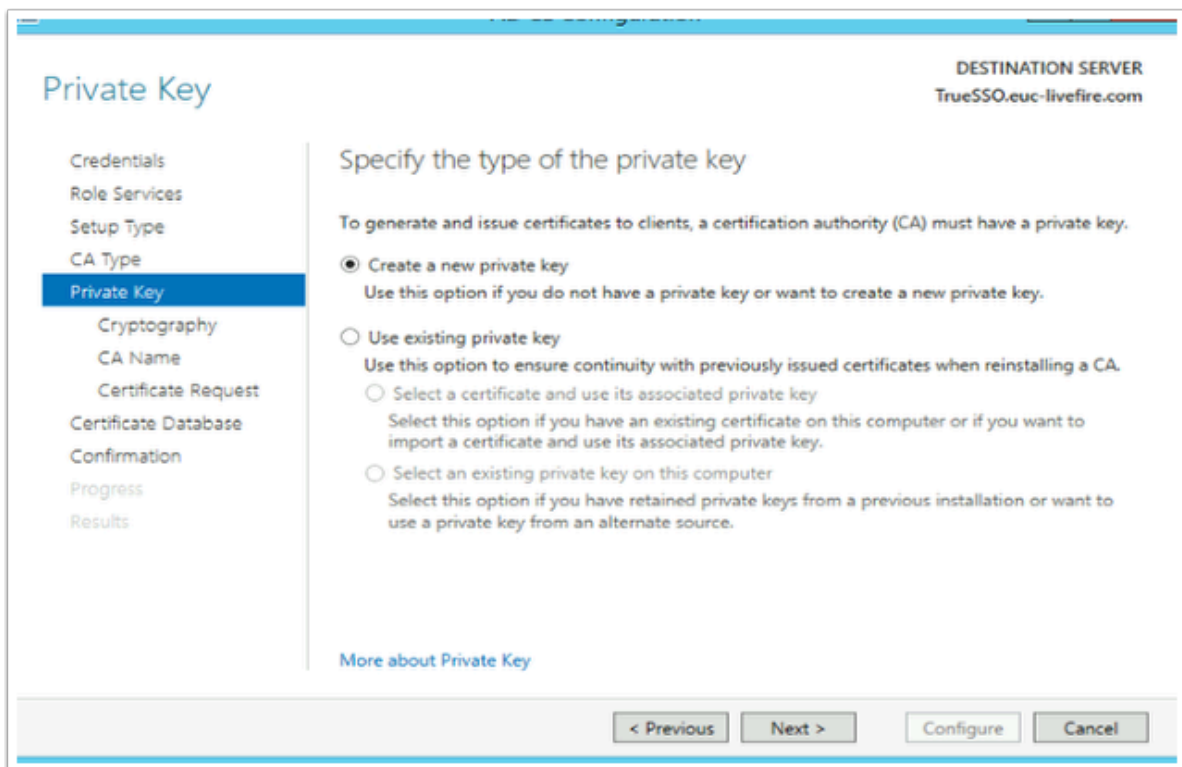
15. On the **Private Key** window,
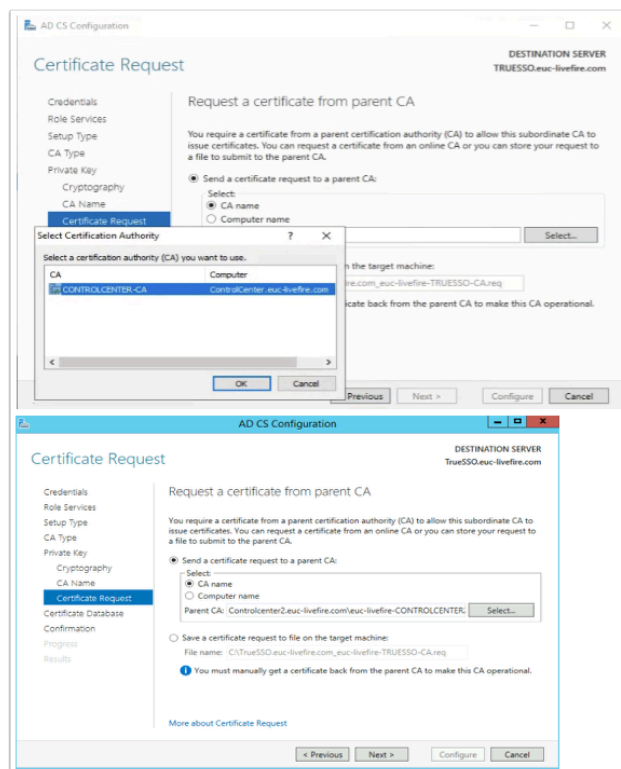   - Ensure the **radio button** next to **Create a new private key** is selected
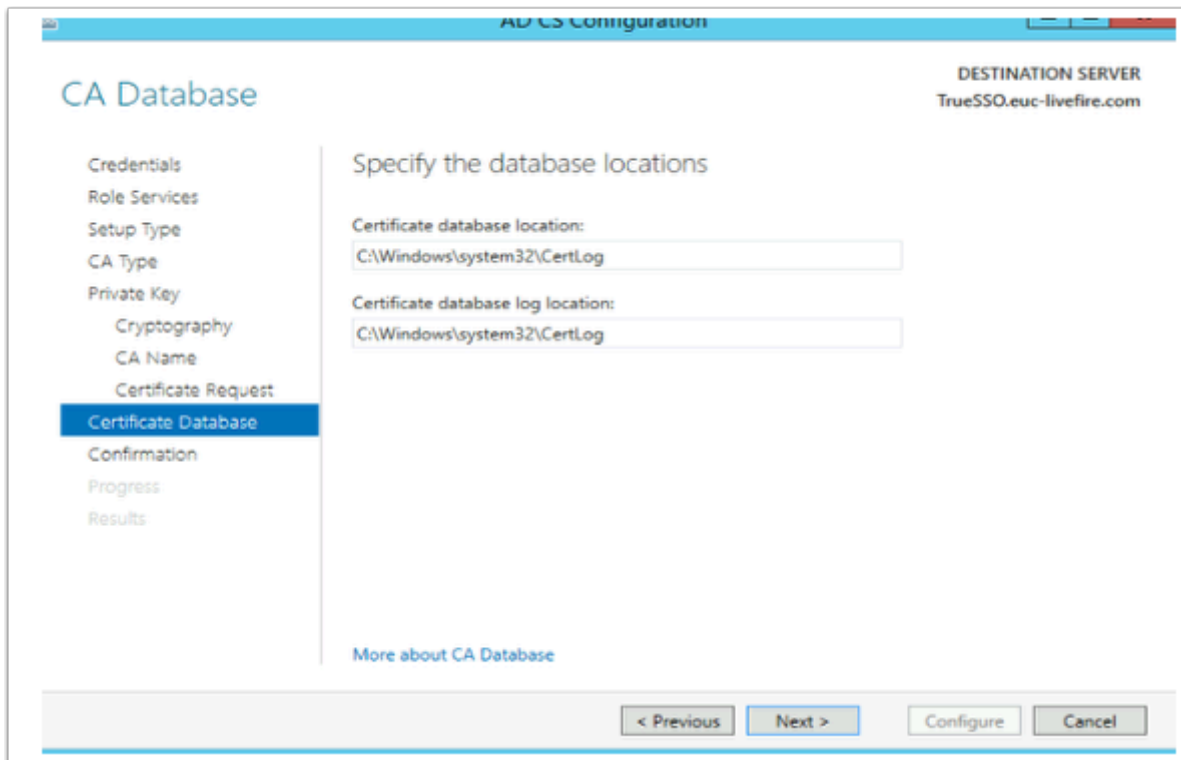

- Select **Next**

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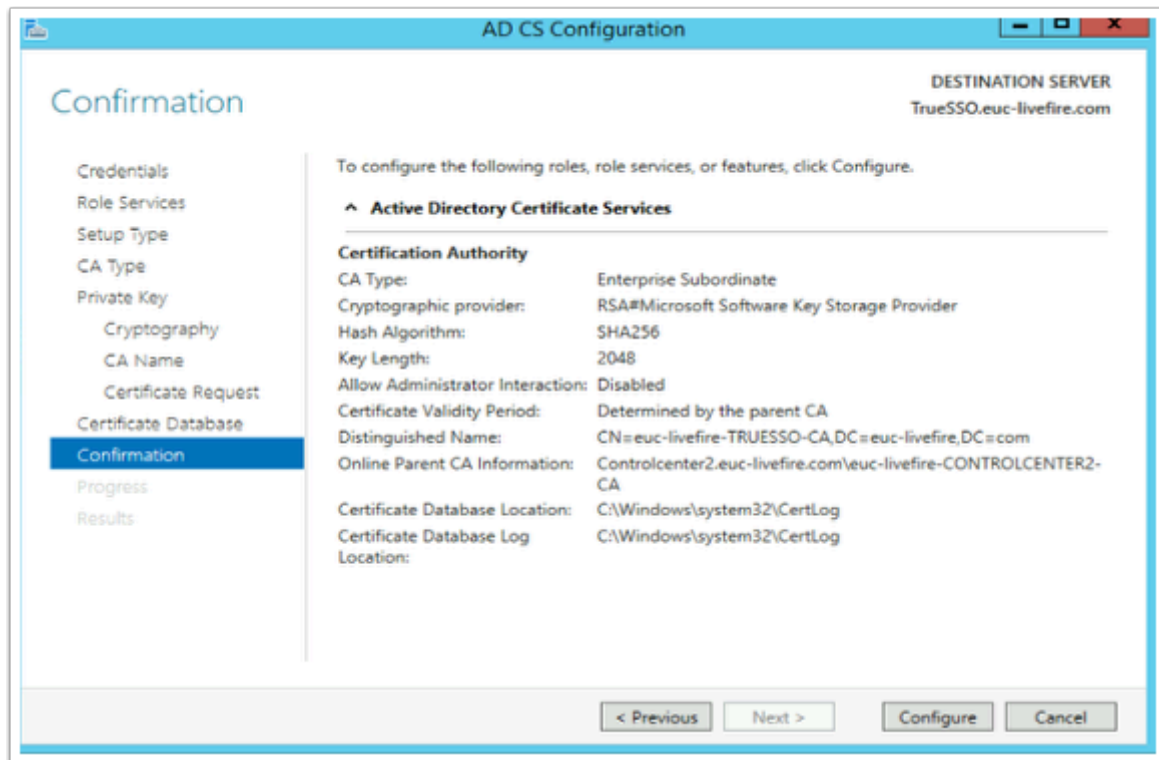
  - Select **Next**

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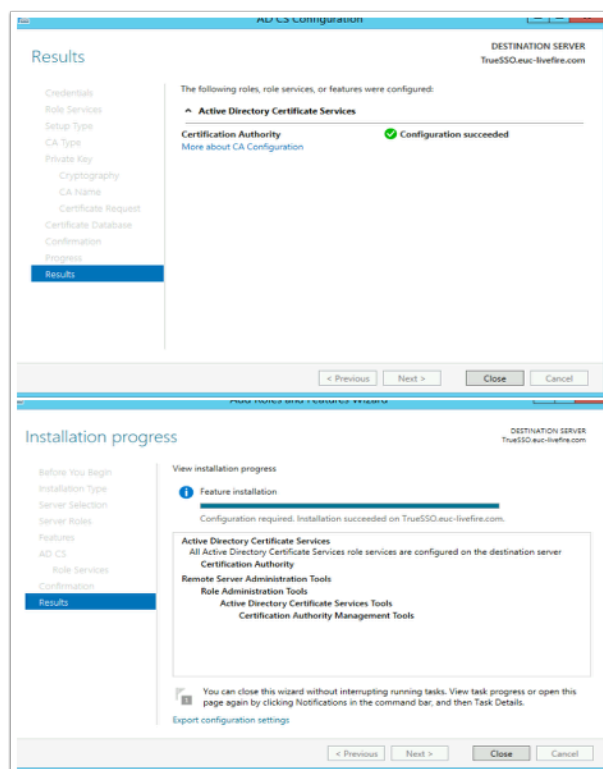   - Observe the CA naming convention
    - Select **Next**

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

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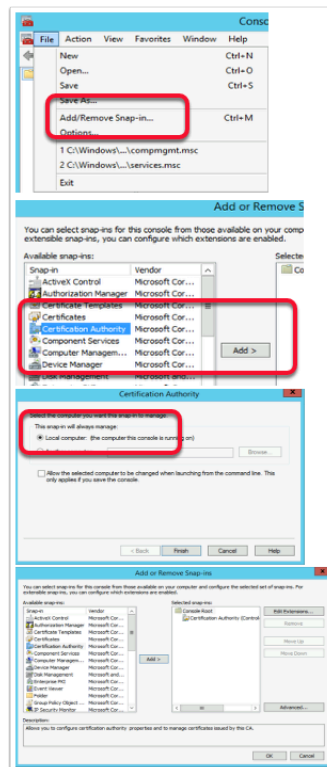   - Select **Next**

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

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

- Select **Close**

# Part 3: 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**

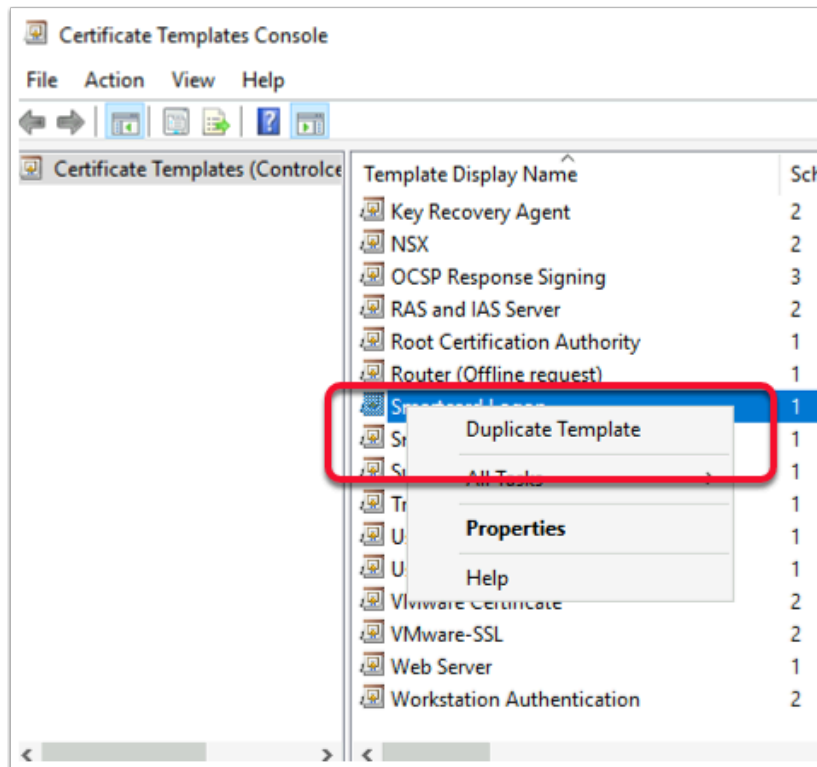   - Select **OK** to close the **Snap-ins** window
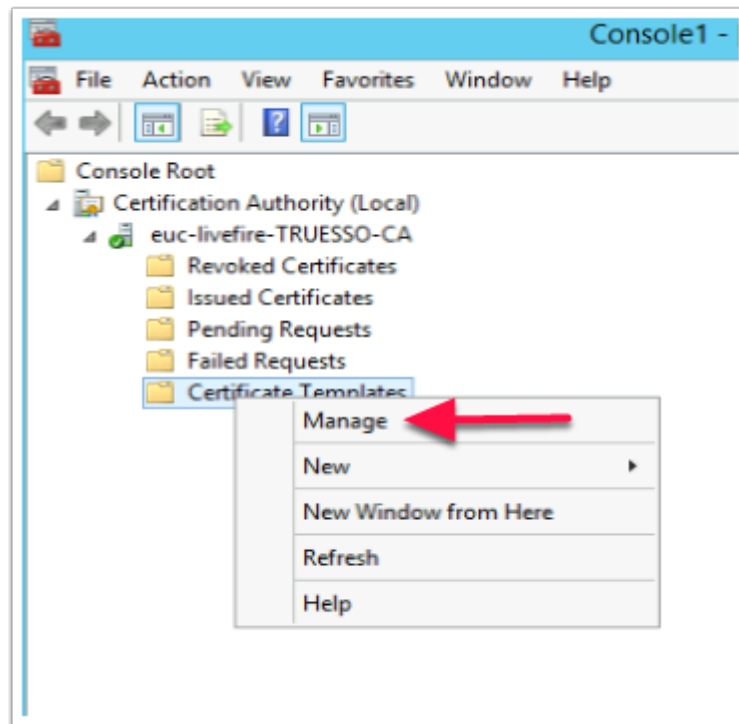
2. Expand the **euc-livefire-TRUESSO-CA i**nventory
   - Select **Certificate Templates,**
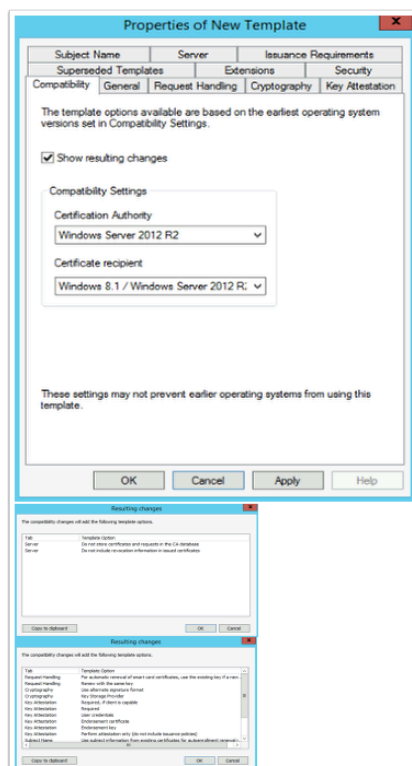   - right-click and select **Manage**
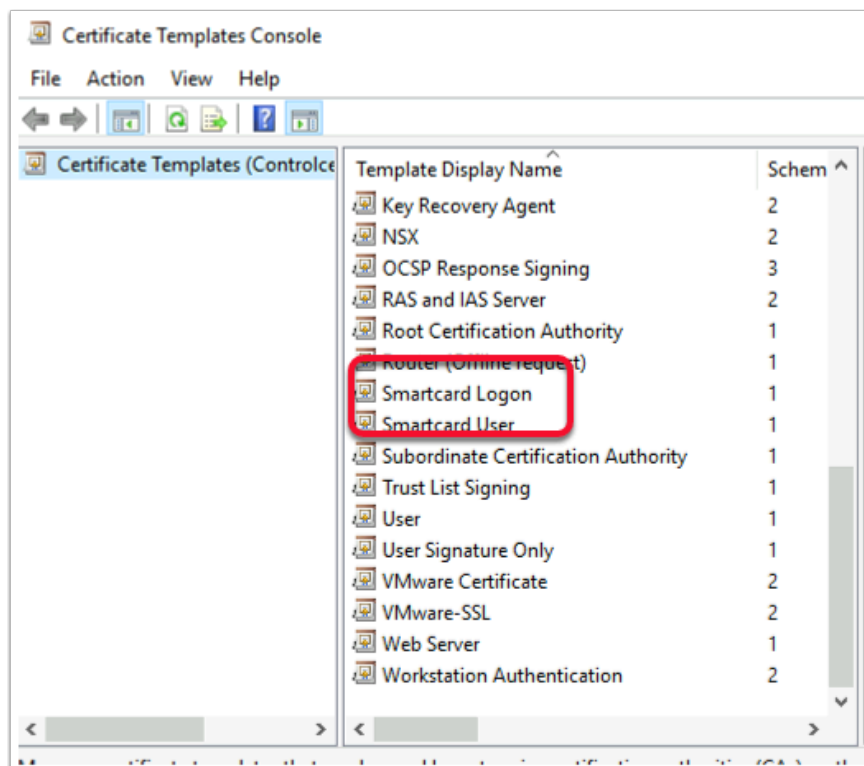
3. In the **Certificate Template** Console
   - Find and select the **Smartcard Logon** template

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
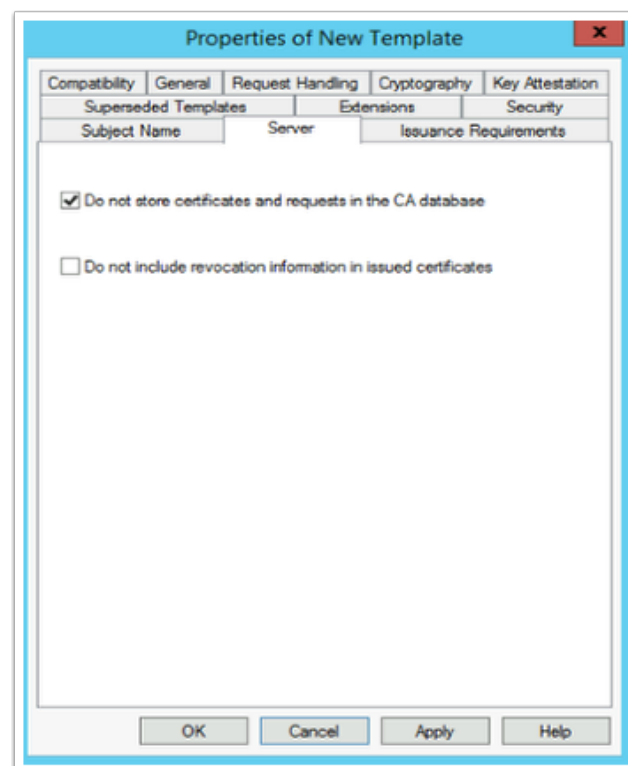   - Select **OK.**
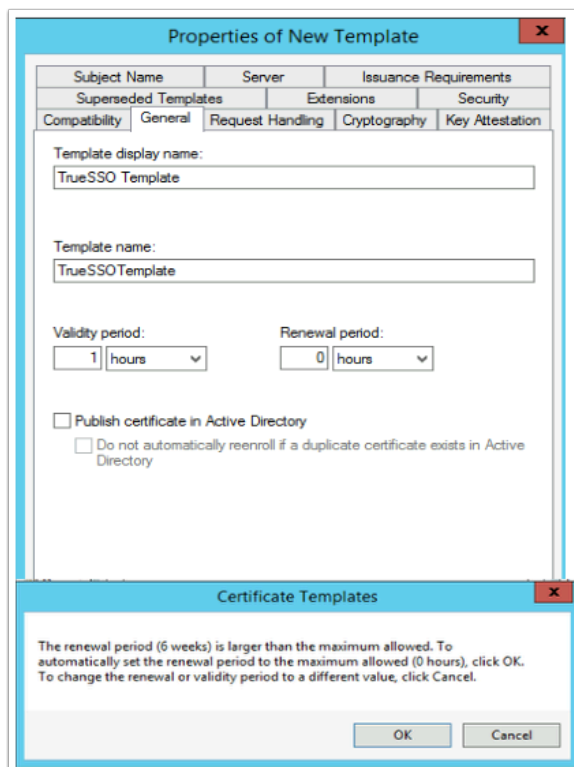
6. Select the **General** tab,
    - Under **Template display name:** type **TrueSSO Template**, you will notice Template name gets filled in automatically.
        - **(Don't edit the TemplateName)**

    - 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**
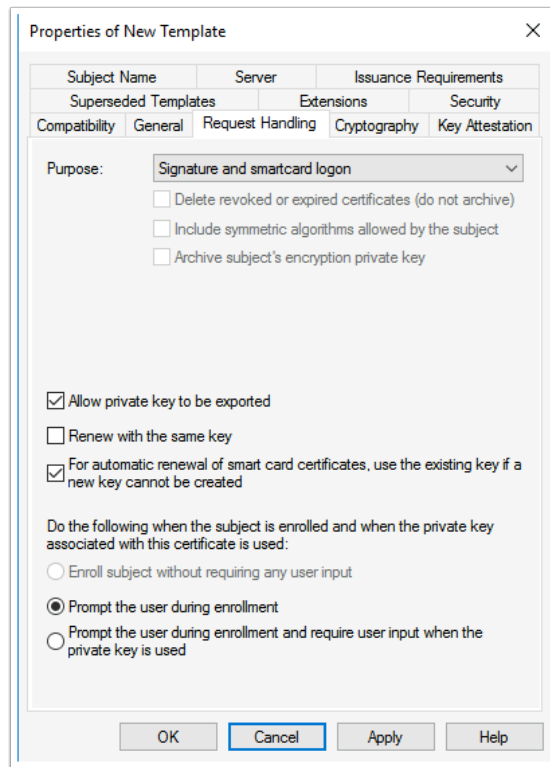
7. Select the **Request Handling** tab change the following next to :-
   - **Purpose:** change: **Signature and encryption** to **Signature and smartcard logon**.
     - When prompted, select **Yes**

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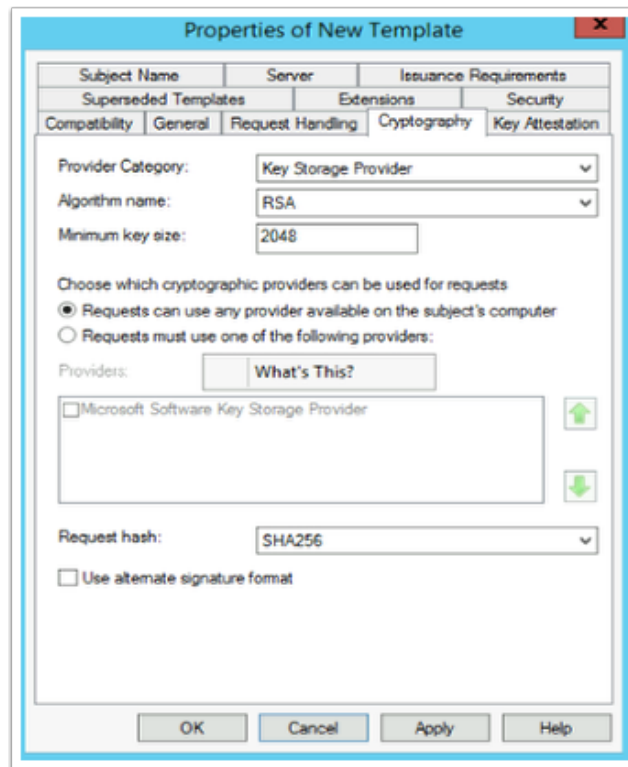
8. Select the **Cryptography** tab change the following next to
   - **Provider Category: Key Storage Provider**
   - **Minimum key size: 2048**
   - **Request hash: SHA256**


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**
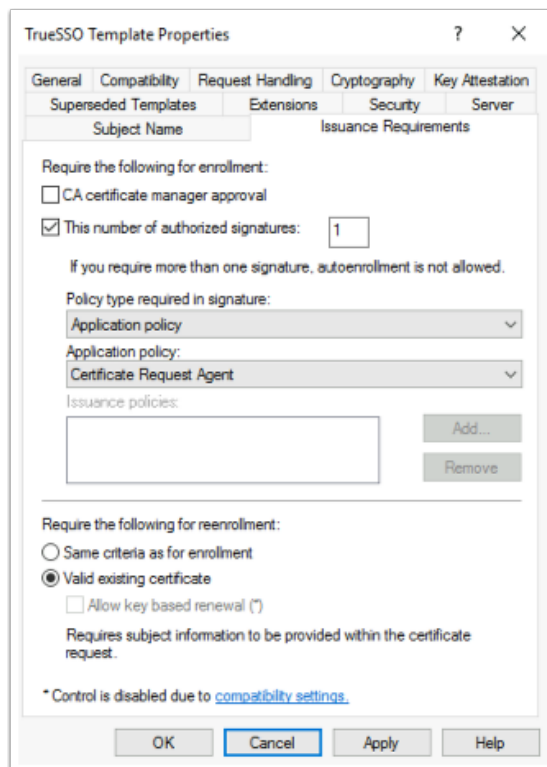

10. Select the **Issuance Requirements** tab, configure the following:
- Select the **checkbox** : **This number of authorized signatures** and change the value to **1** in the **box**
- Under **Policy type required in signature**
  - Ensure the **Application policy** is selected (default config)

- Under **Application Policy**
  - Select **Certificate Request Agent** from the dropdown

- Under the **Require the following for reenrollment**
  - Select the **Valid existing certificate** radio button
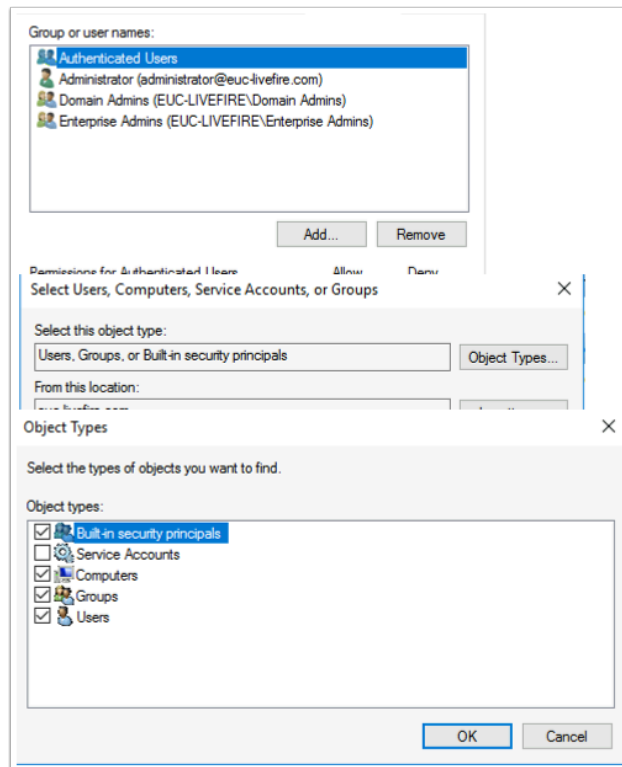
11. On the **Security** tab in the **Group or user names:** area
    - Select **Add**
        - To the right of the **Select this object type:** box
            - Select the **Object types** button
            - Select the **checkbox** next to **Computers,**
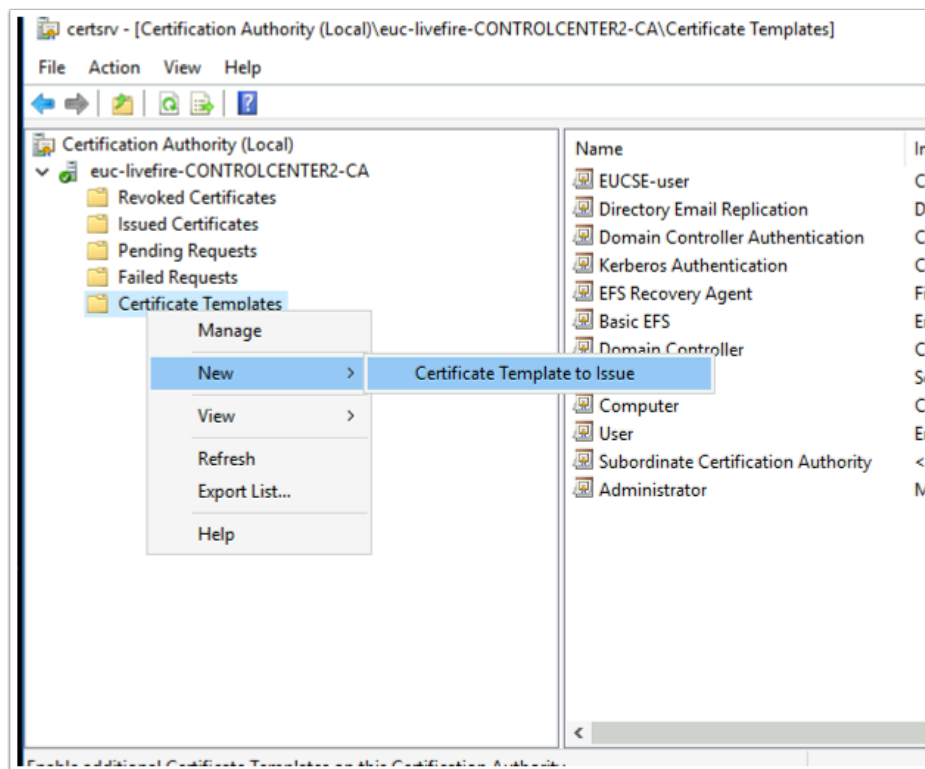   - Select **OK**
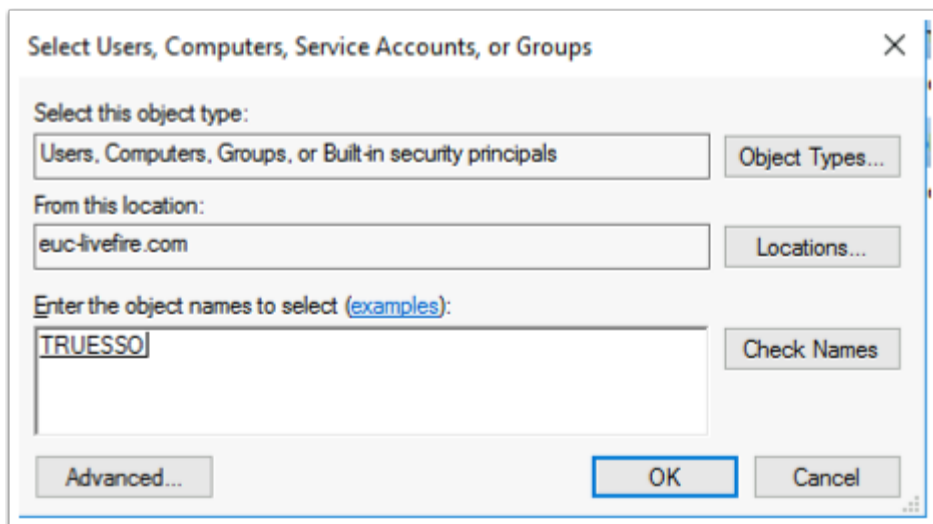
12. In the **Enter the object names to select**
    - Type **Truesso**
    - To the right select **Check Names**
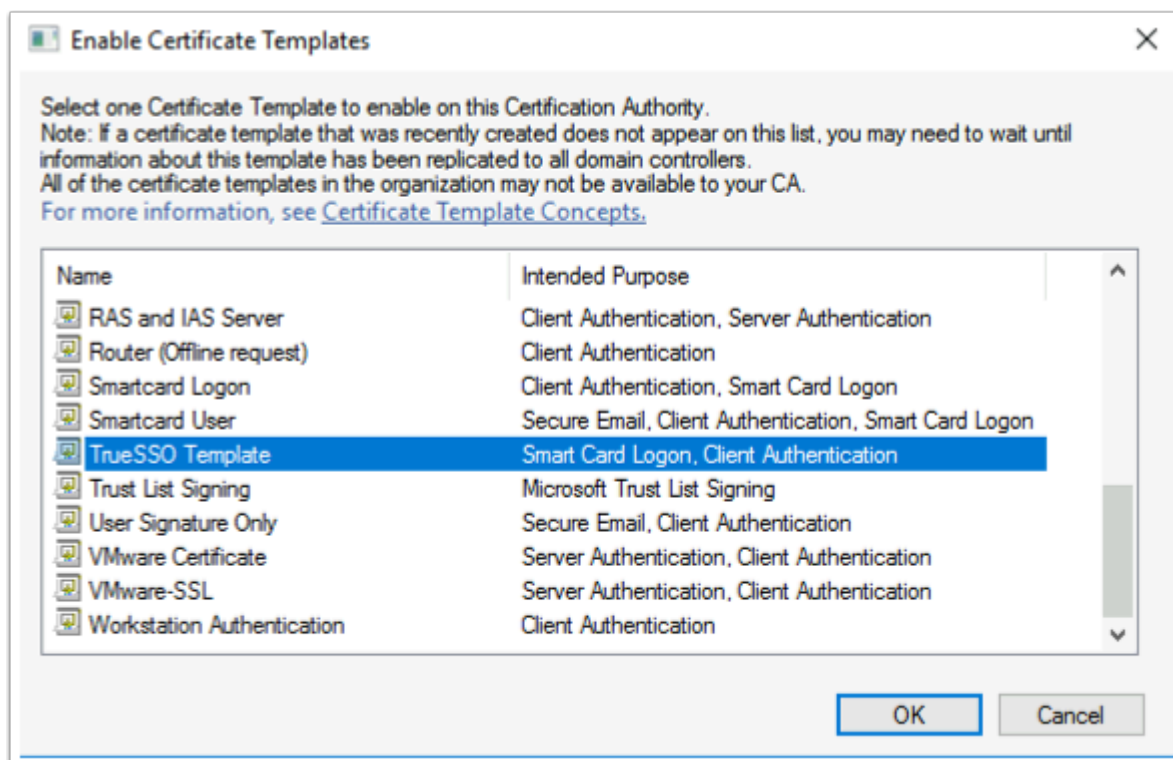   - Select **OK**
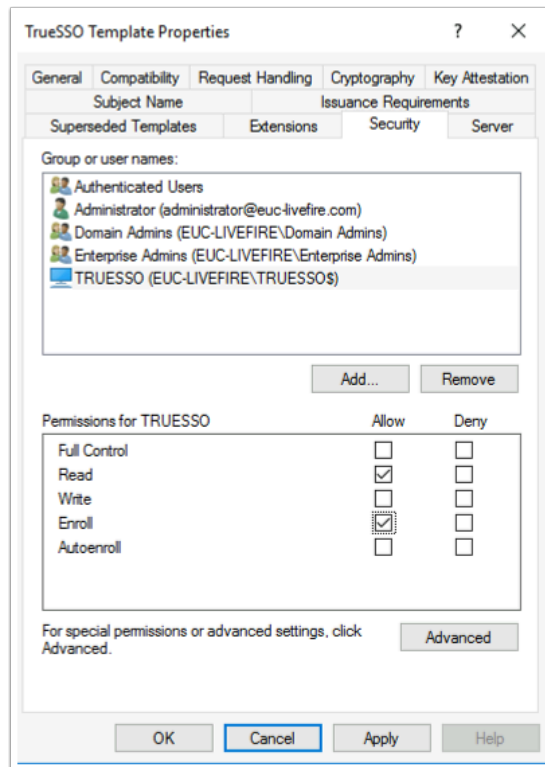
13. For the **Permissions for TRUESSO**
    - Ensure that the permission **Read** and **Enroll checkboxes** are selected.
    - Select **OK** to close the **TrueSSO Template Properties,**

14. Switch to the **Certificate Authority Console**
    - Select and right-click the **Certificate Templates** container,

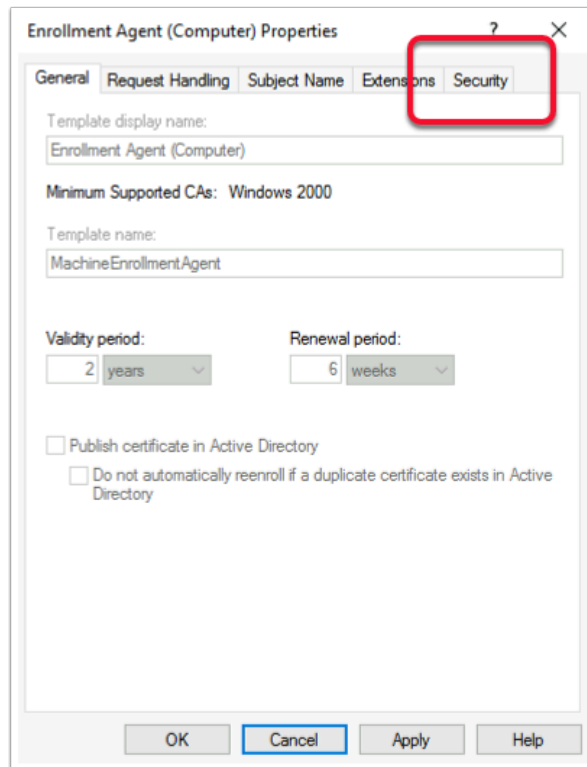- Select **New** > **Certificate Template** to Issue

15. In the **Enable Certificate Templates** window,
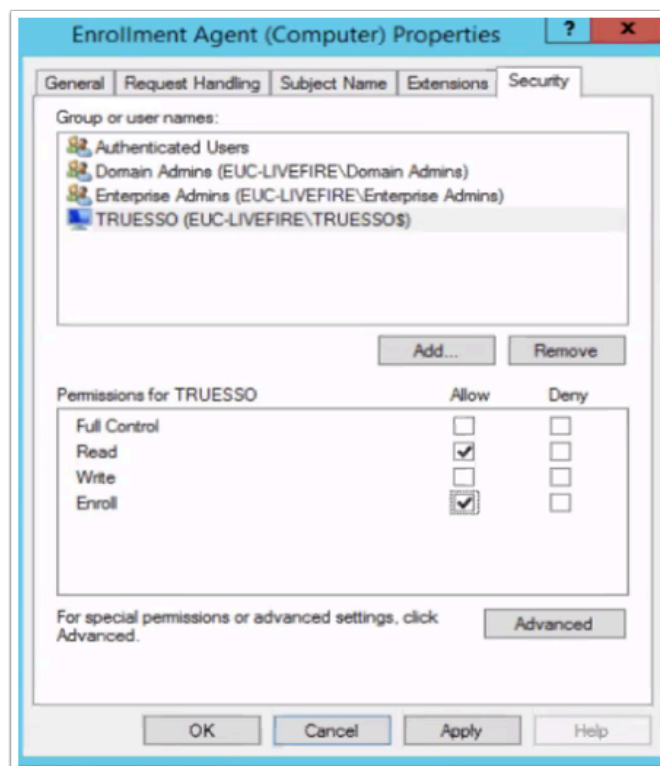   - Select your **TrueSSO Template**
    - Select **OK**
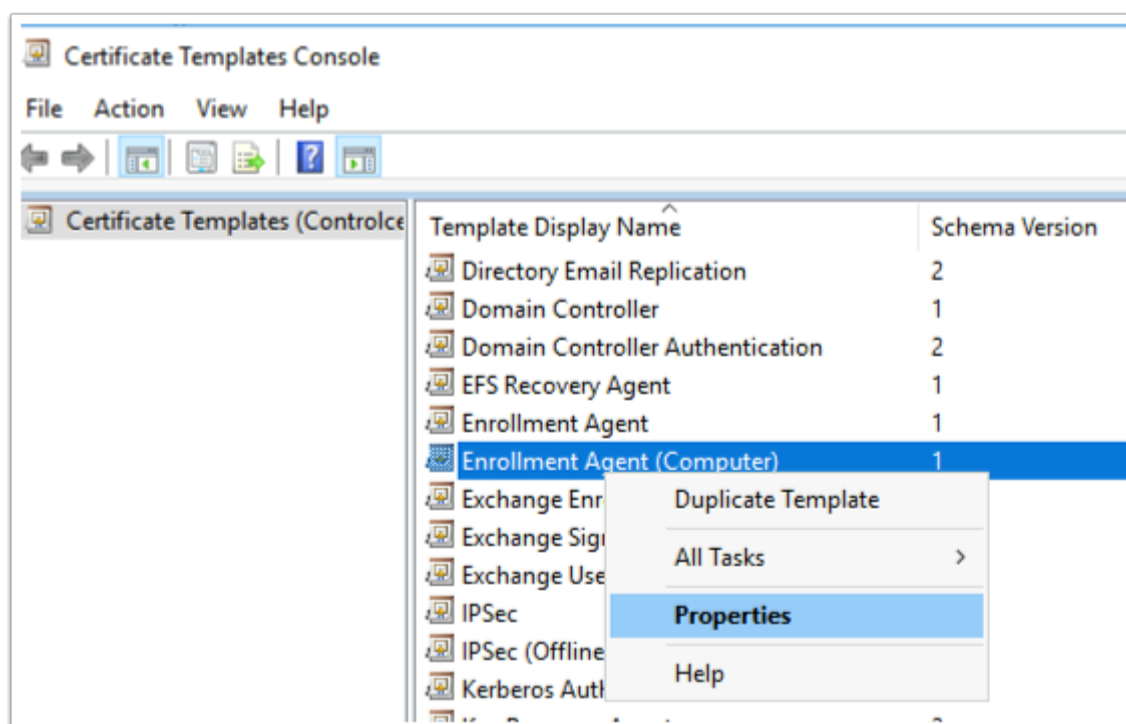
16. Switch back to the **Certificate Templates** Console select and right-click the **Enrollment Agent (computer)** template and select **Properties**
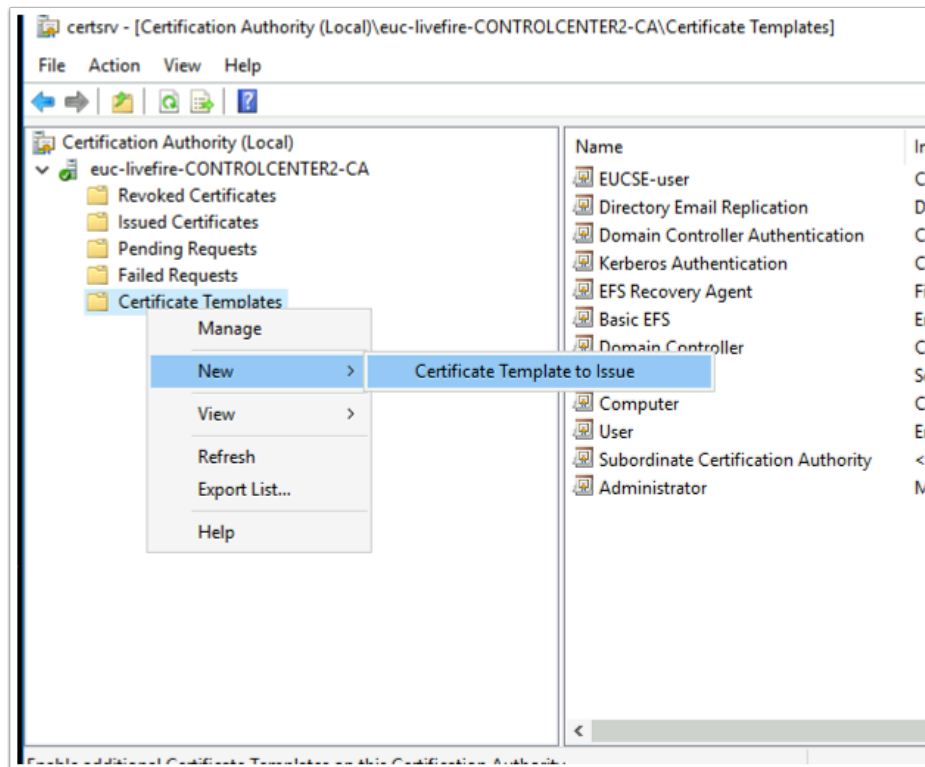
17. In the **Enrollment Agent Properties** window
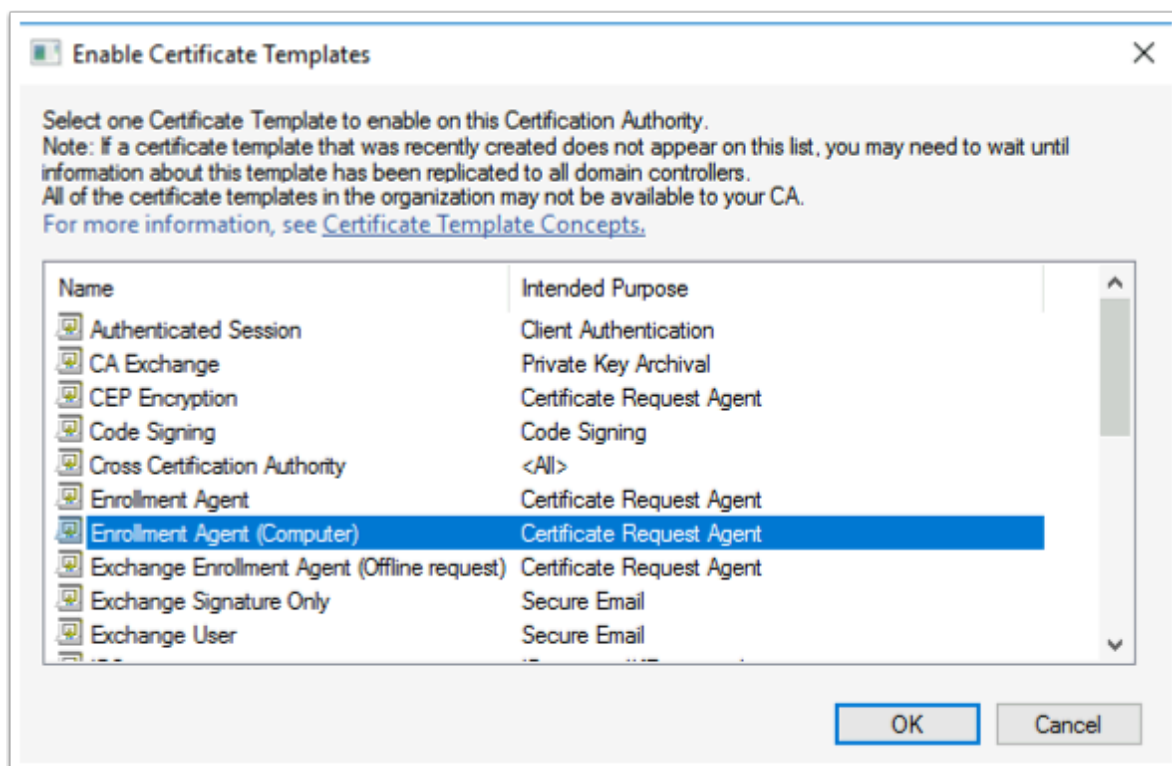   - Select the **Security** tab

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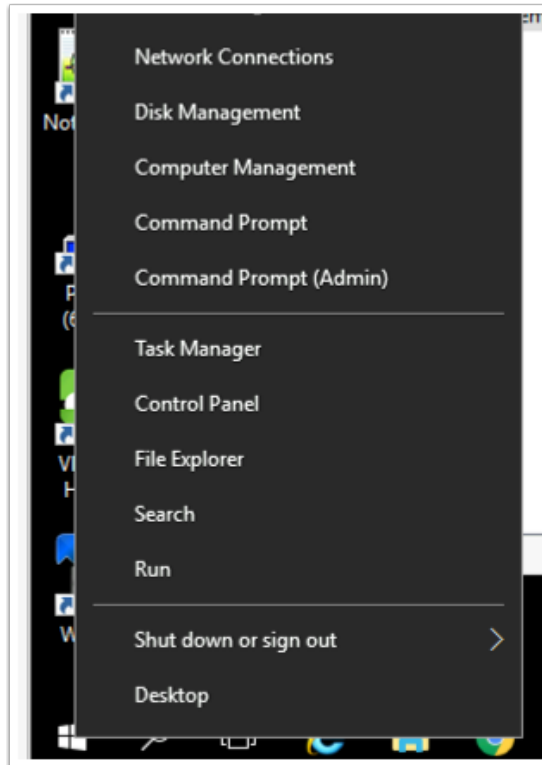   - Select **OK** to close the **Enrollment agent** properties

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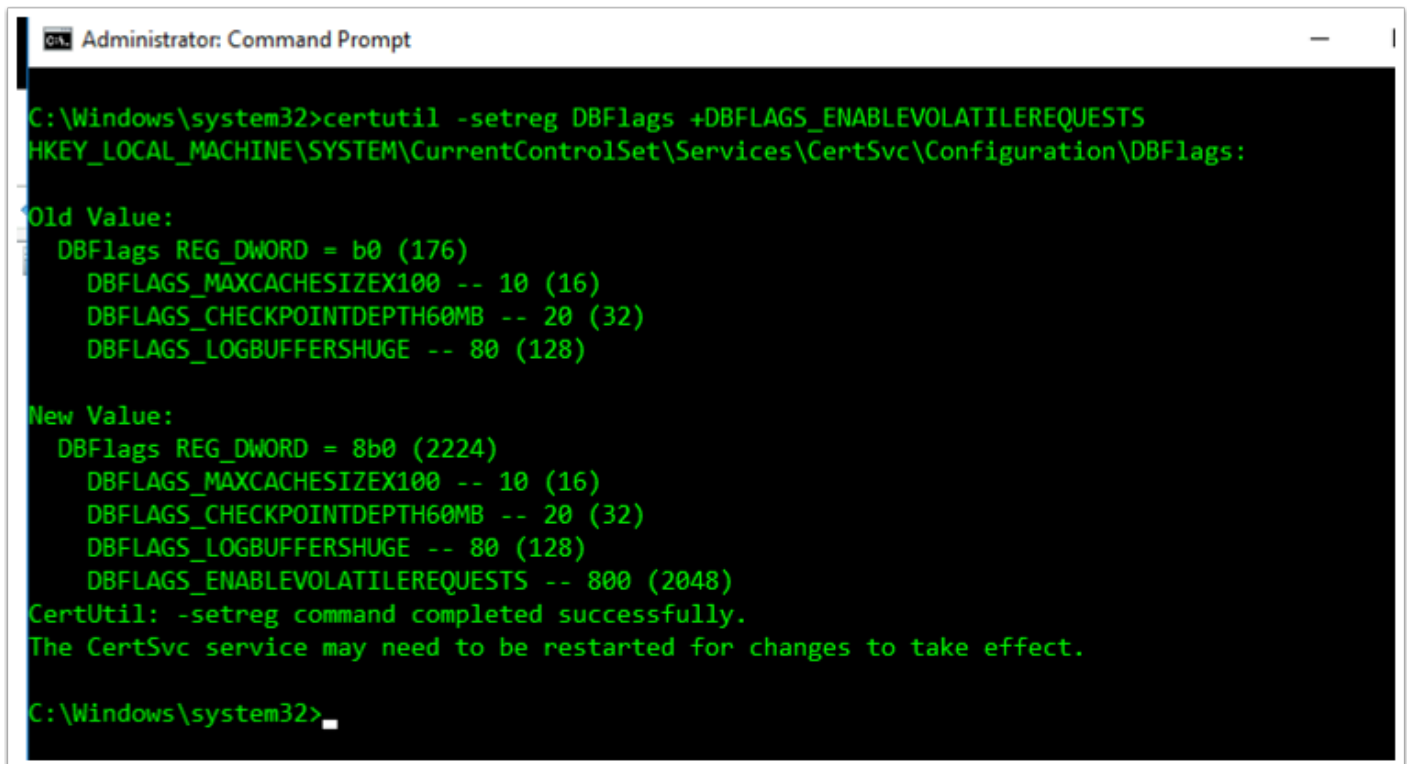   - Select **New** > **Certificate Template** to Issue

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)**

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

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

New Value:
  DBFlags REG_DWORD = 8b0 (2224)
    DBFLAGS_MAXCACHESIZEX100 -- 10 (16)
    DBFLAGS_CHECKPOINTDEPTH60MB -- 20 (32)
    DBFLAGS_LOGBUFFERSHUGE -- 80 (128)
    DBFLAGS_ENABLEVOLATILEREQUESTS -- 800 (2048)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>
```
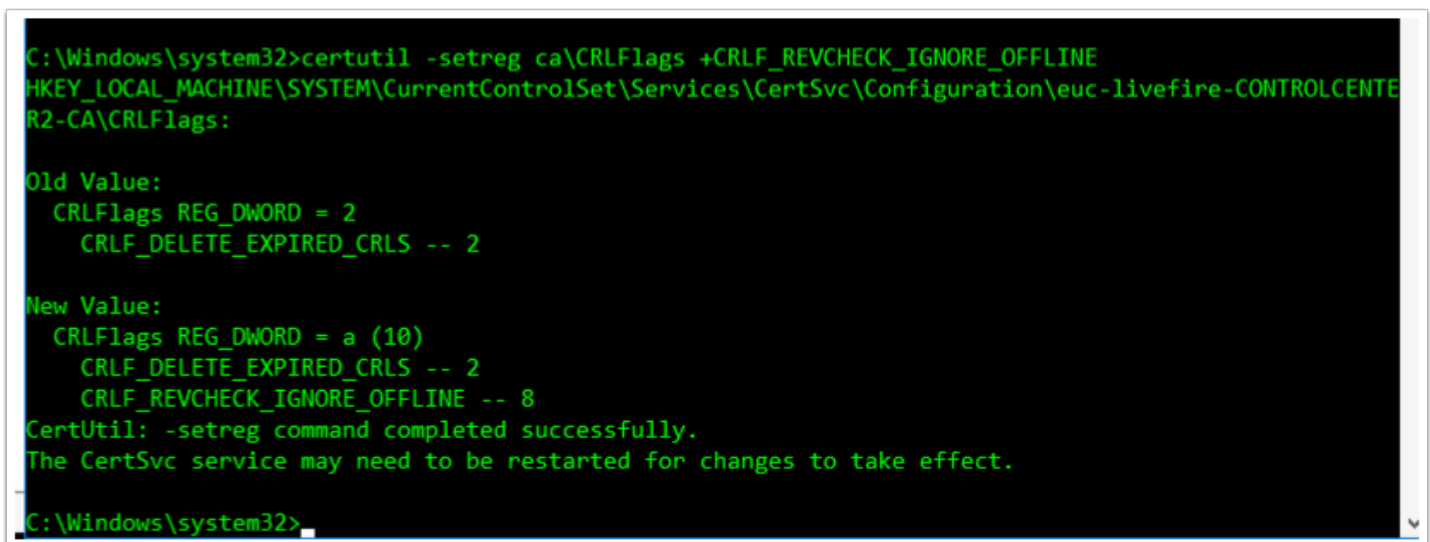
22. In the Administrator: Command Prompt enter the following commands

- `certutil –setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS`

```
C:\Windows\system32>certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\euc-livefire-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>
```
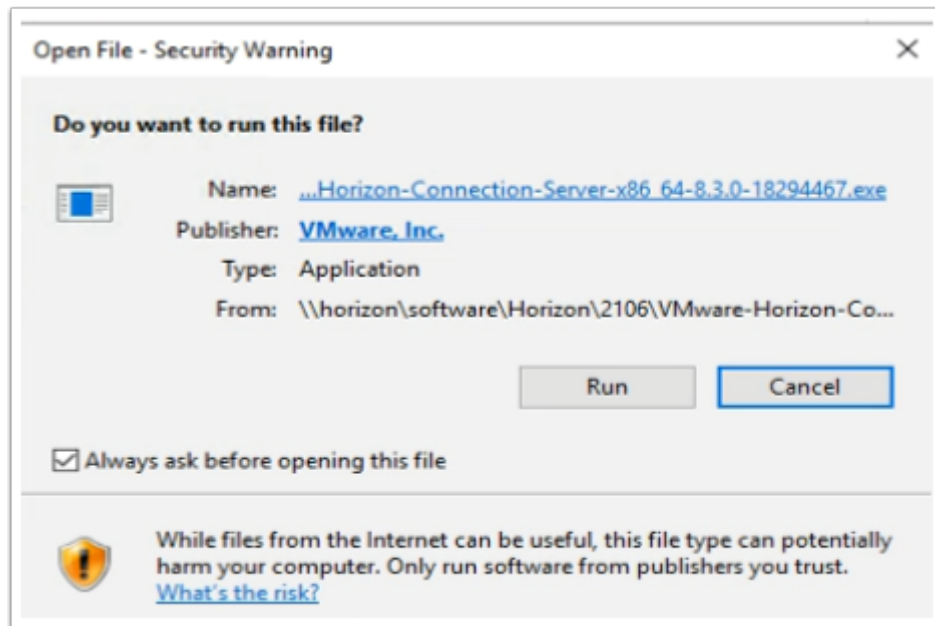
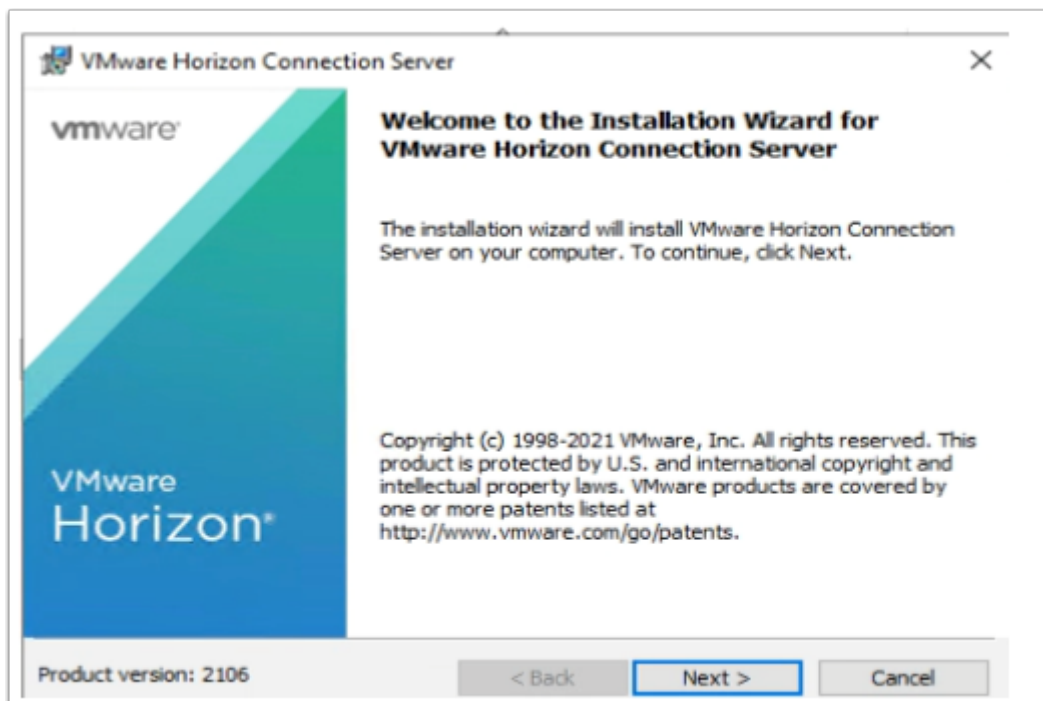24. Restart the CA service. From the command prompt run:
    • `net stop certsvc`
    • `net start certsvc`
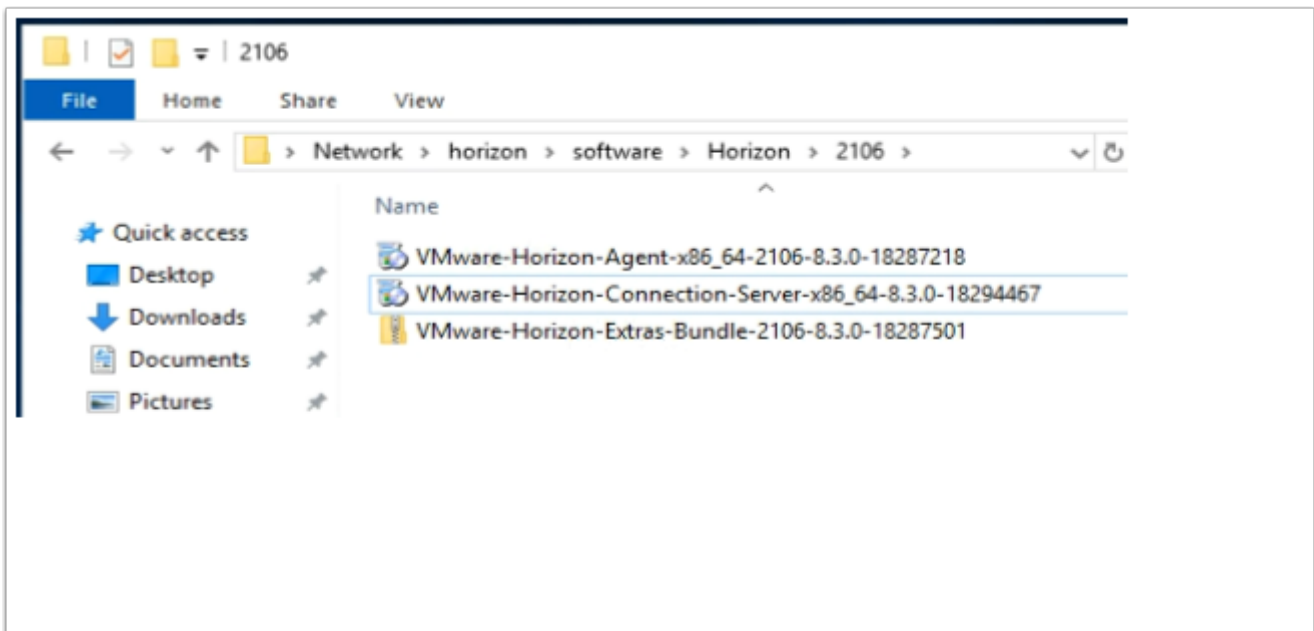
25. On the **TrueSSO** server desktop
    • Launch the **software** shortcut
    • In the Software folder, open the **Horizon\2106** folder.
    • Select and launch the **VMware-Horizon-Connection-Server-x86_64-8.3.0-18294467.exe**

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

27. On the **Welcome** window
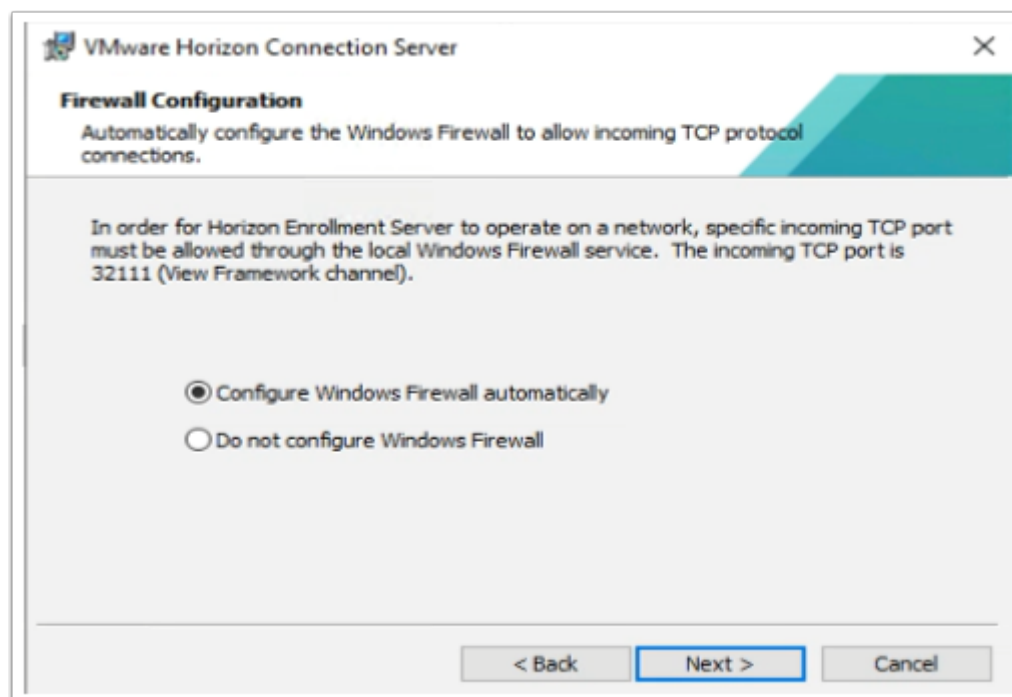   • Select **Next**
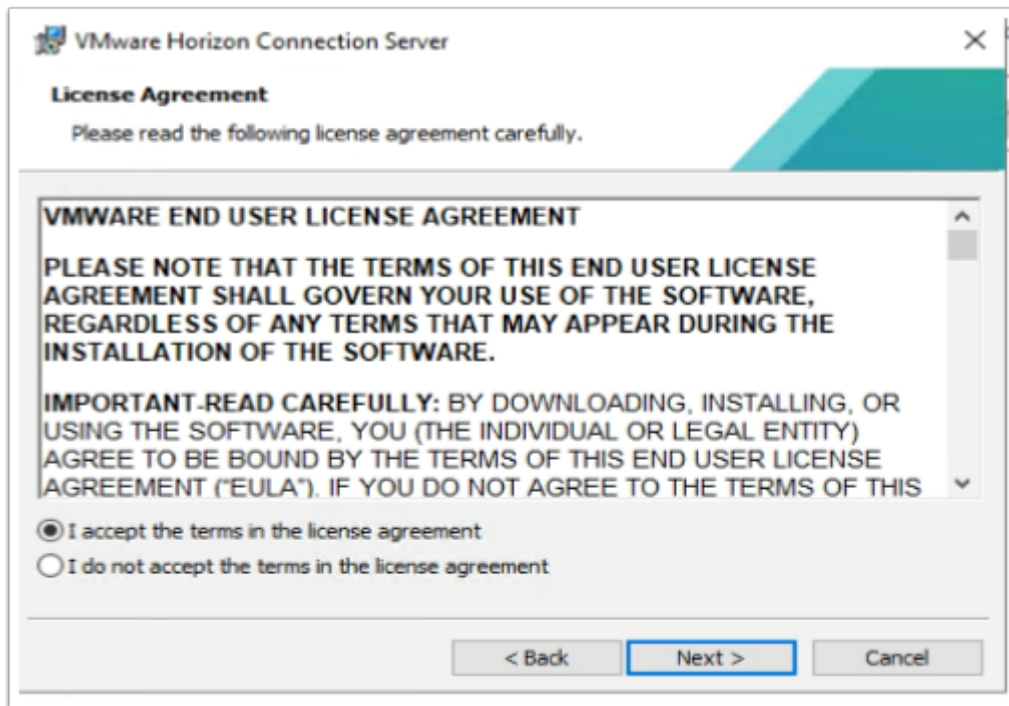
28. On the **License agreement** window
   - Select the **radio button** next **I accept the terms in the license agreement,**
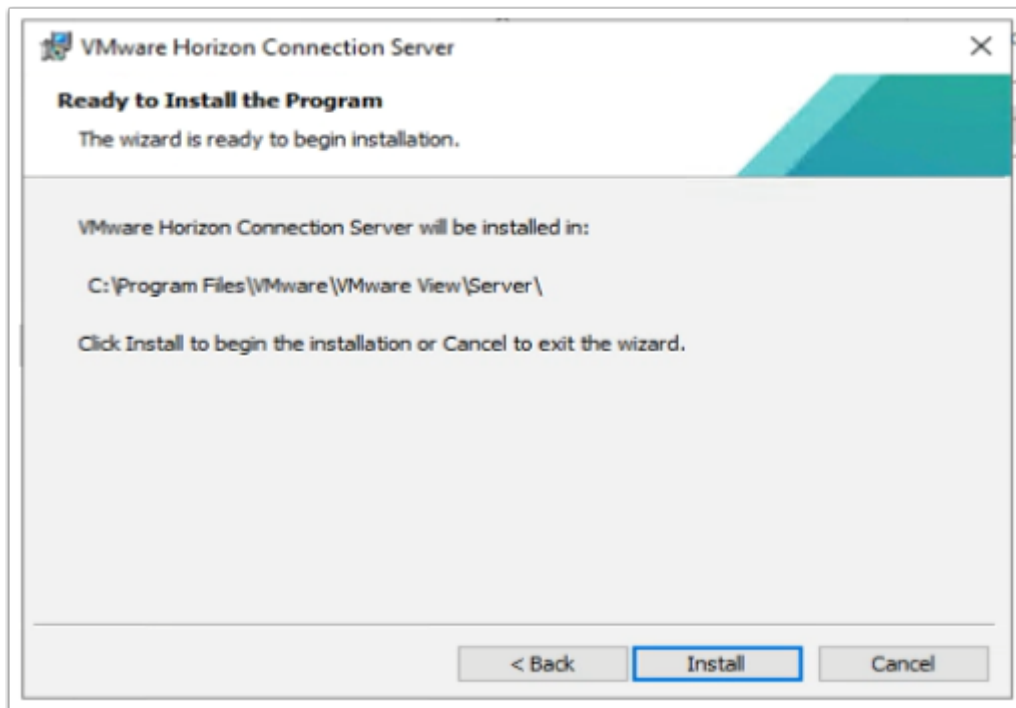   - Select **Next**
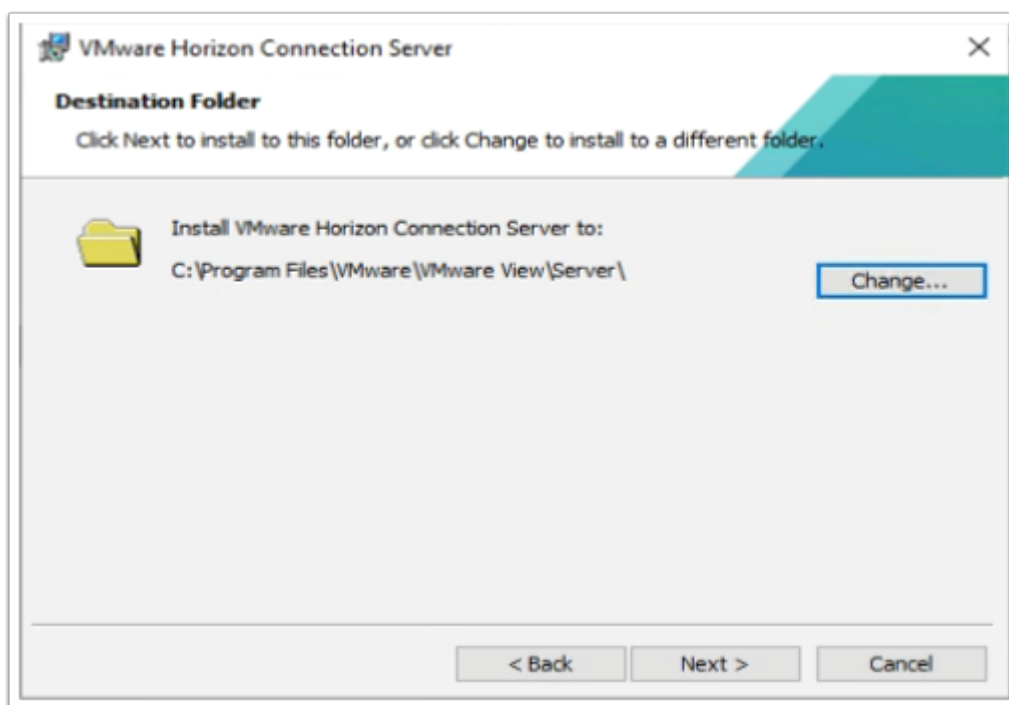
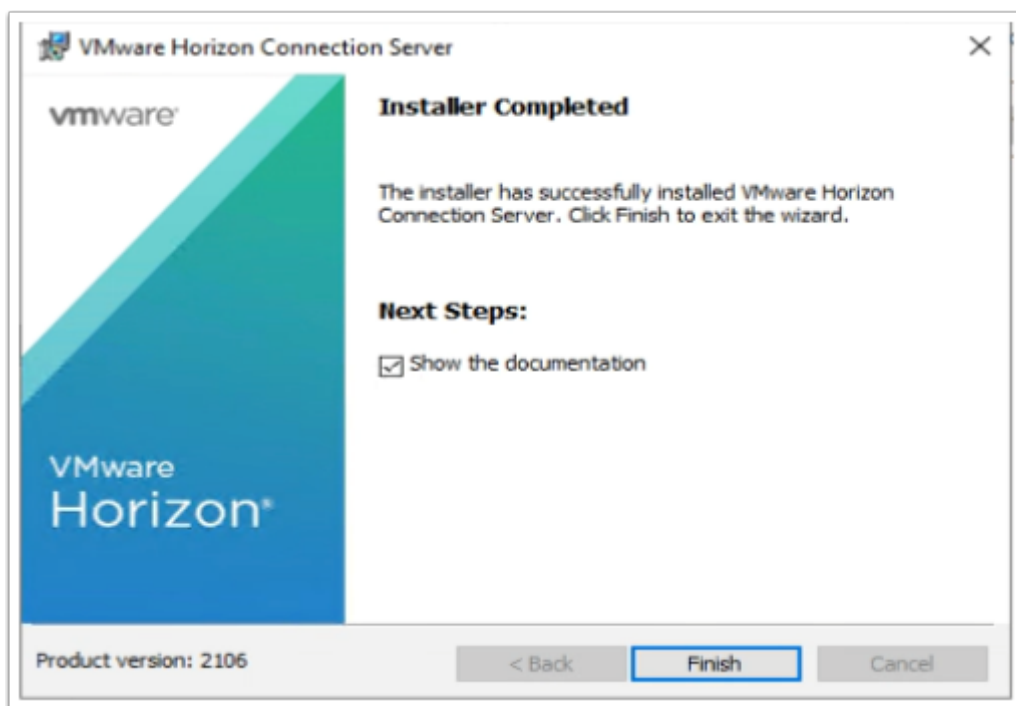29. On **Destination Folder** window
   - Select **Next**
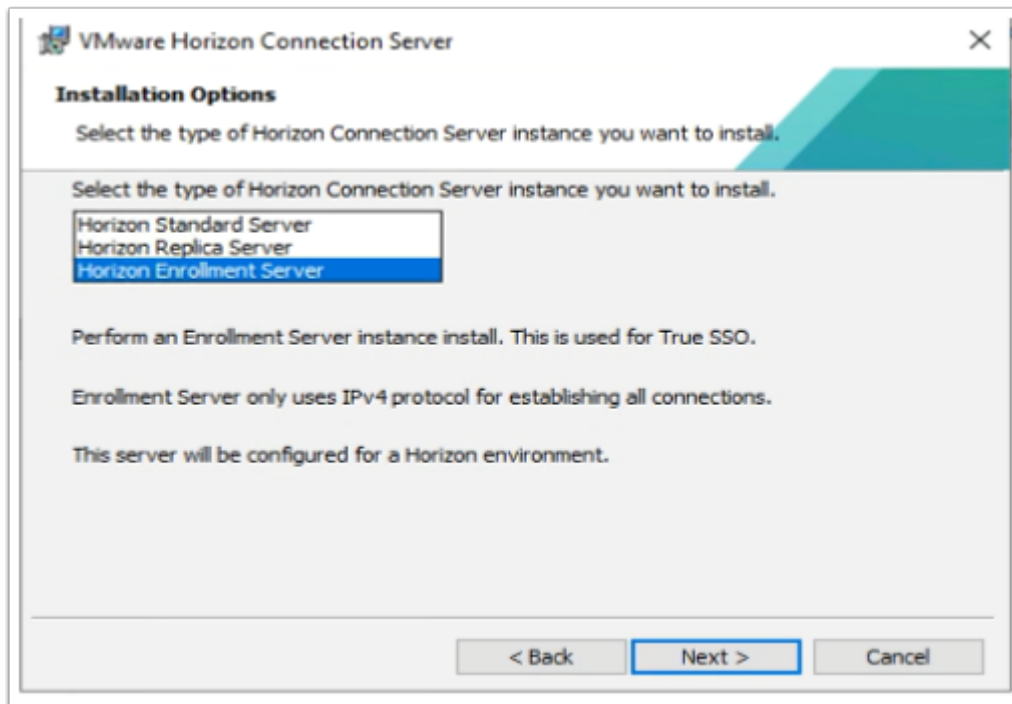
30. On the **Installation Options** window select **Horizon Enrollment Server**
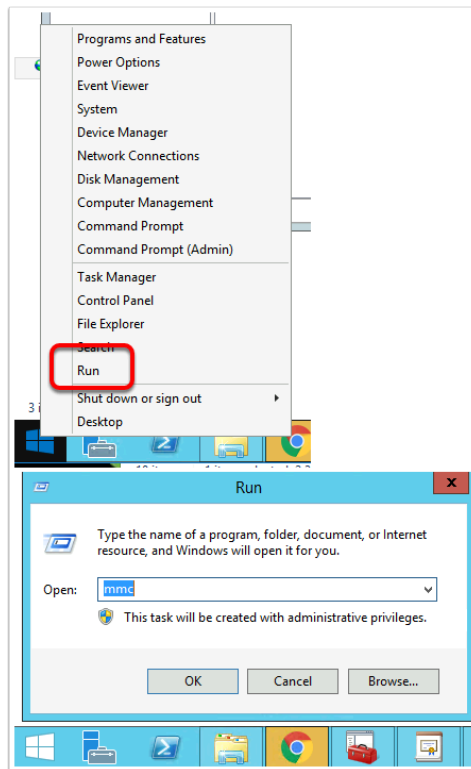   • Select **Next**

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

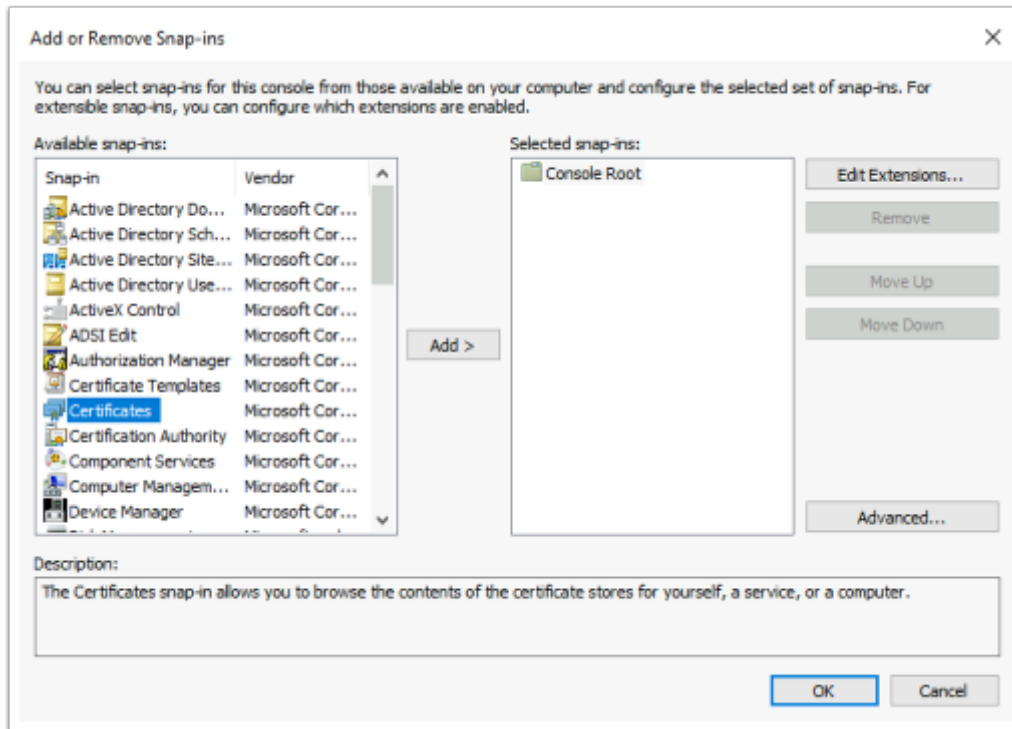32. Select **Install**

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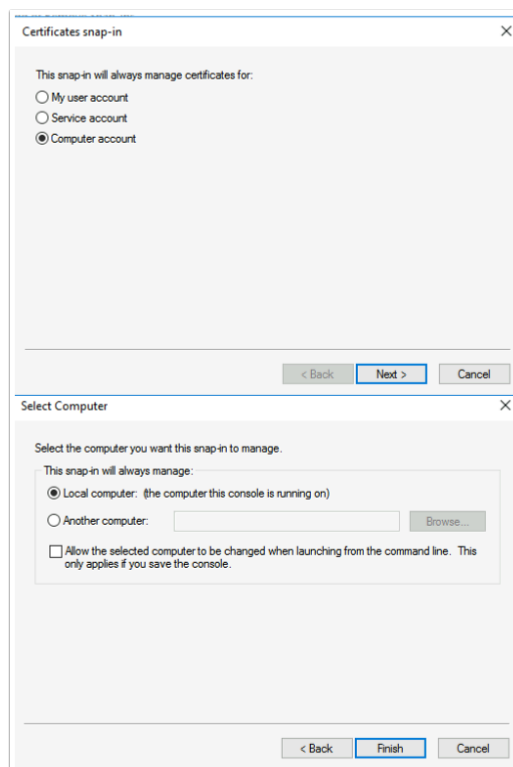   - Select **Finish**

34. On the **TrueSSO** server
    - Select and right-click the **Start Button**,
    - Select **Run**,
    - Type **MMC**,
    - Select **OK**
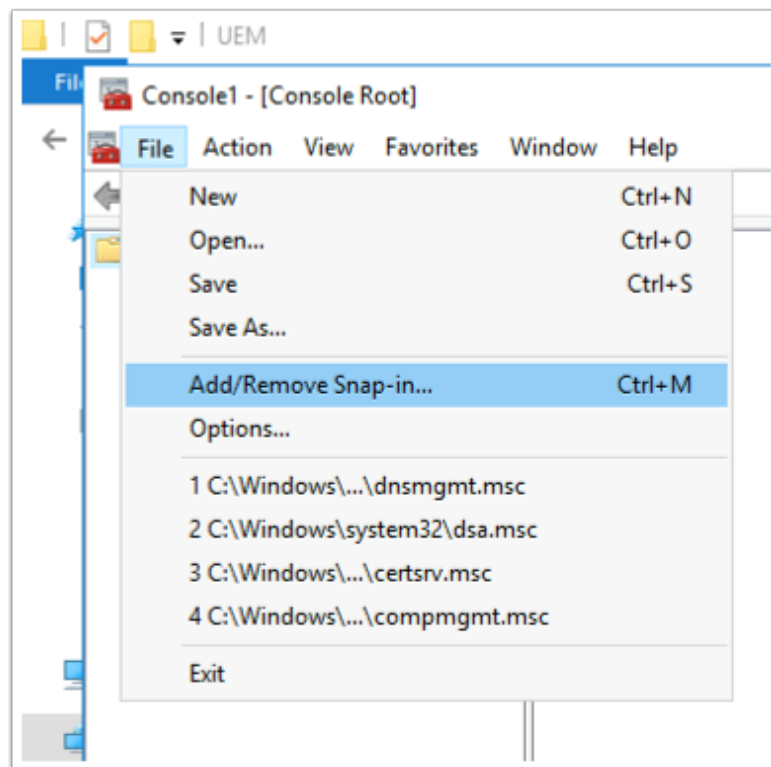
35. In the **Console** window
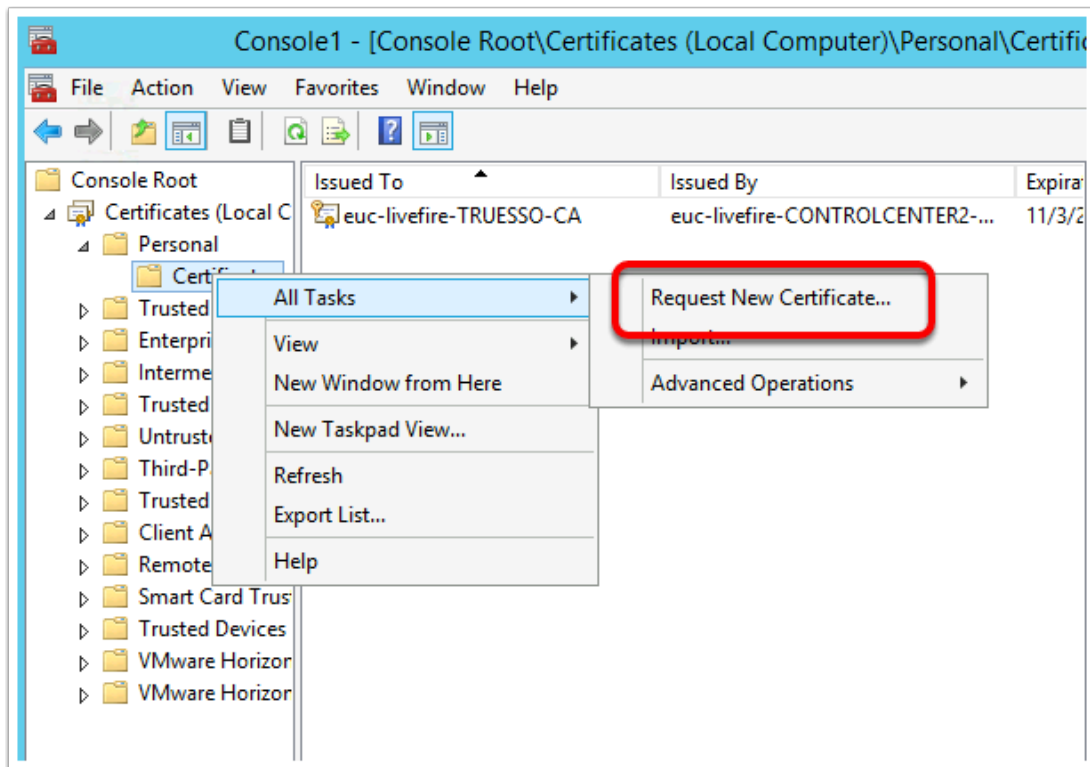   - Select **File** > **Add/Remove Snap-in..**

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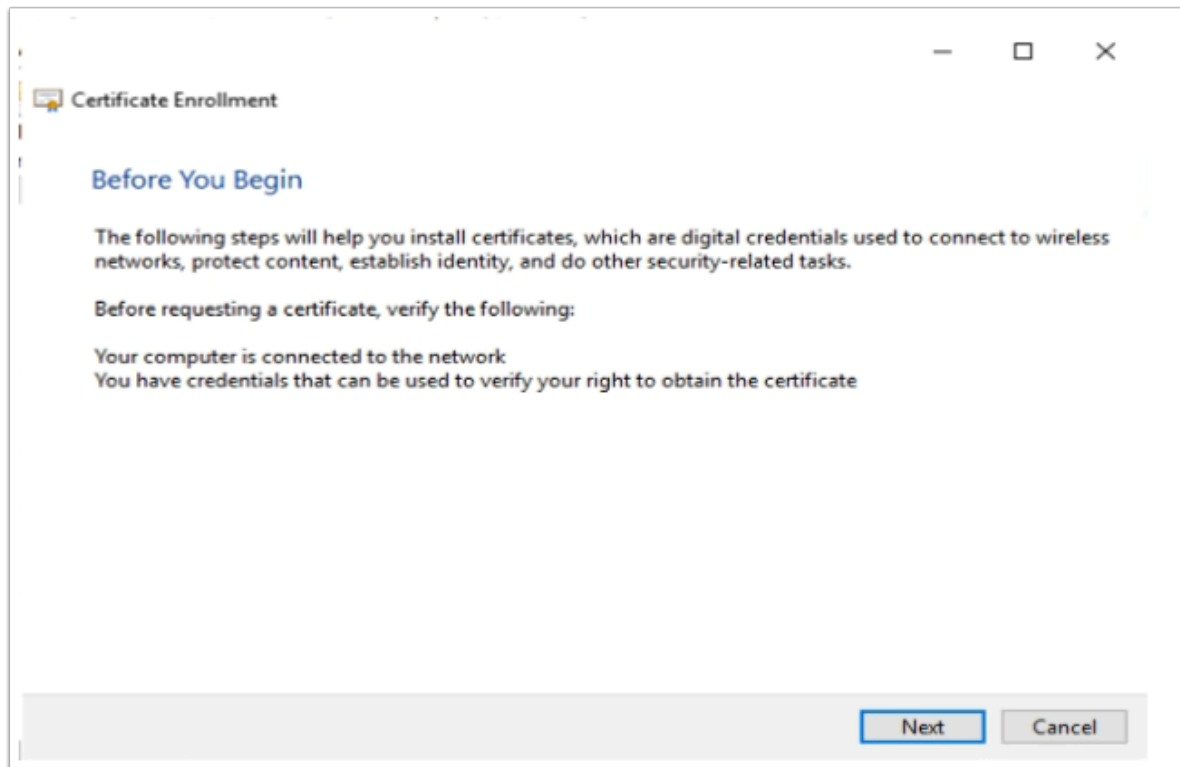   - Select **Add**
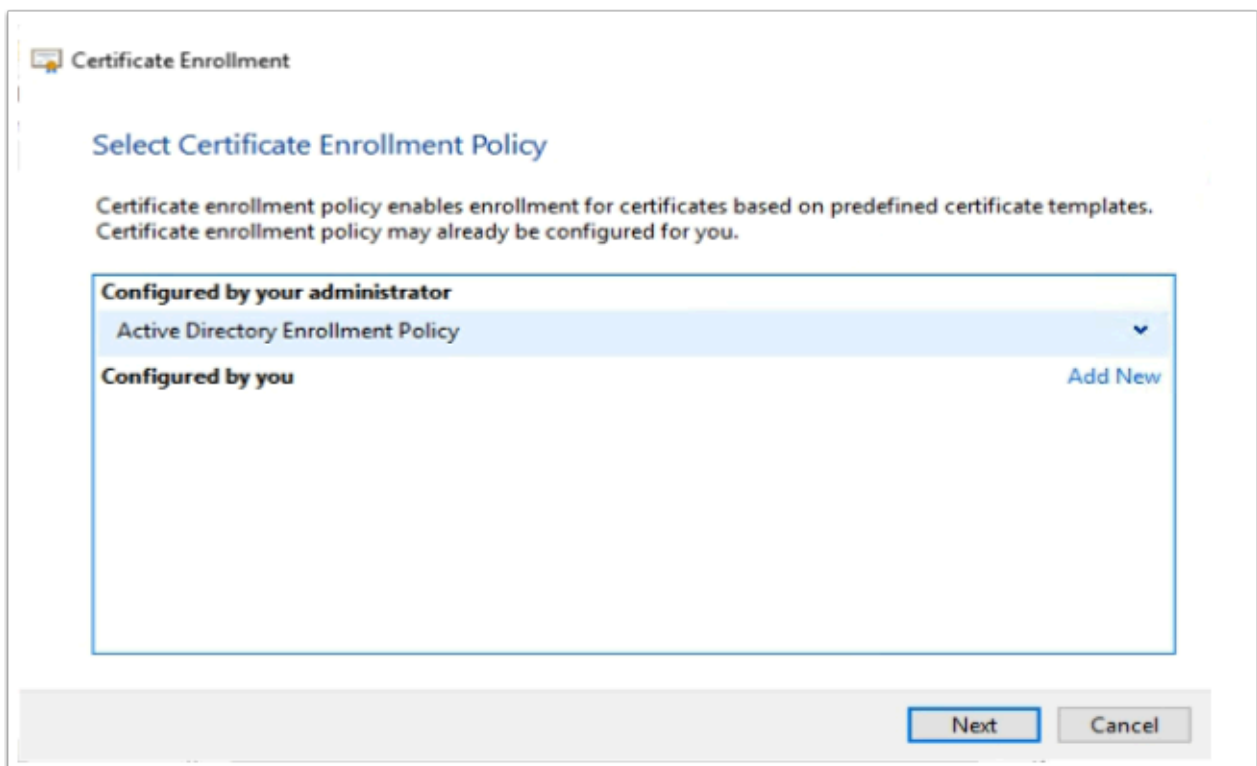

37. Select **Computer account** radio button

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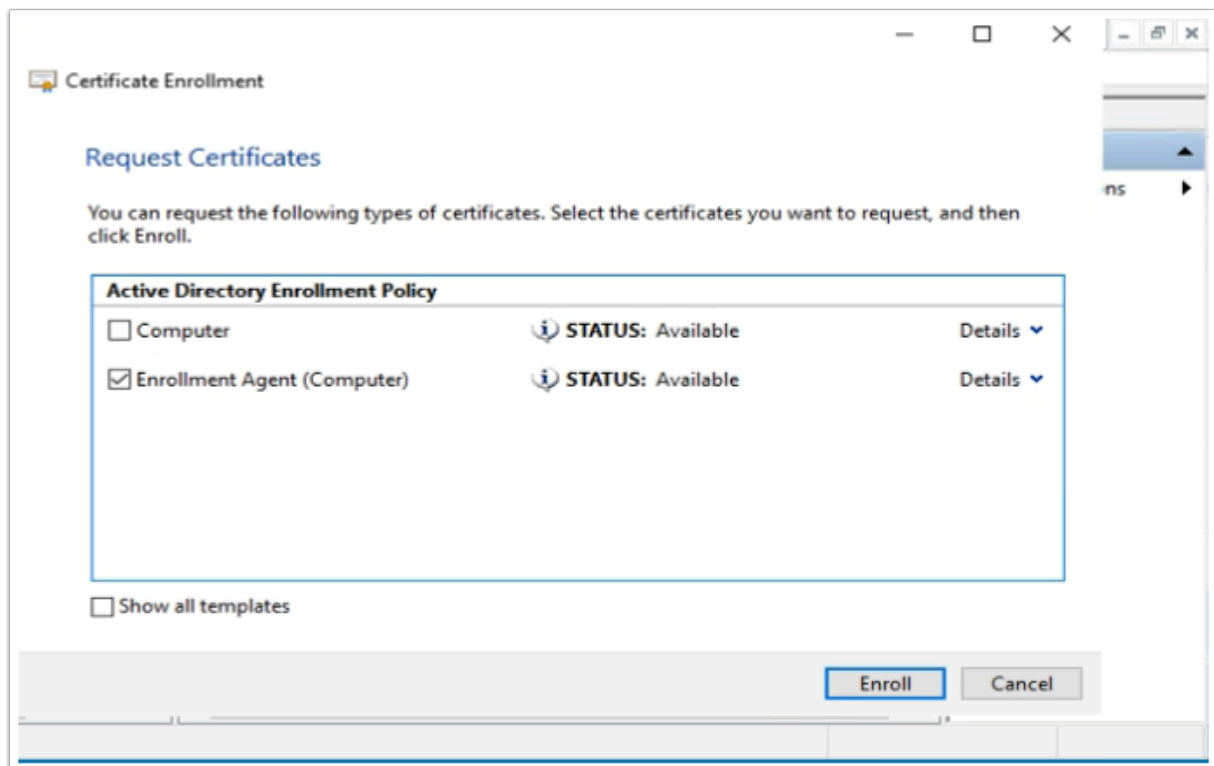- Select **OK**

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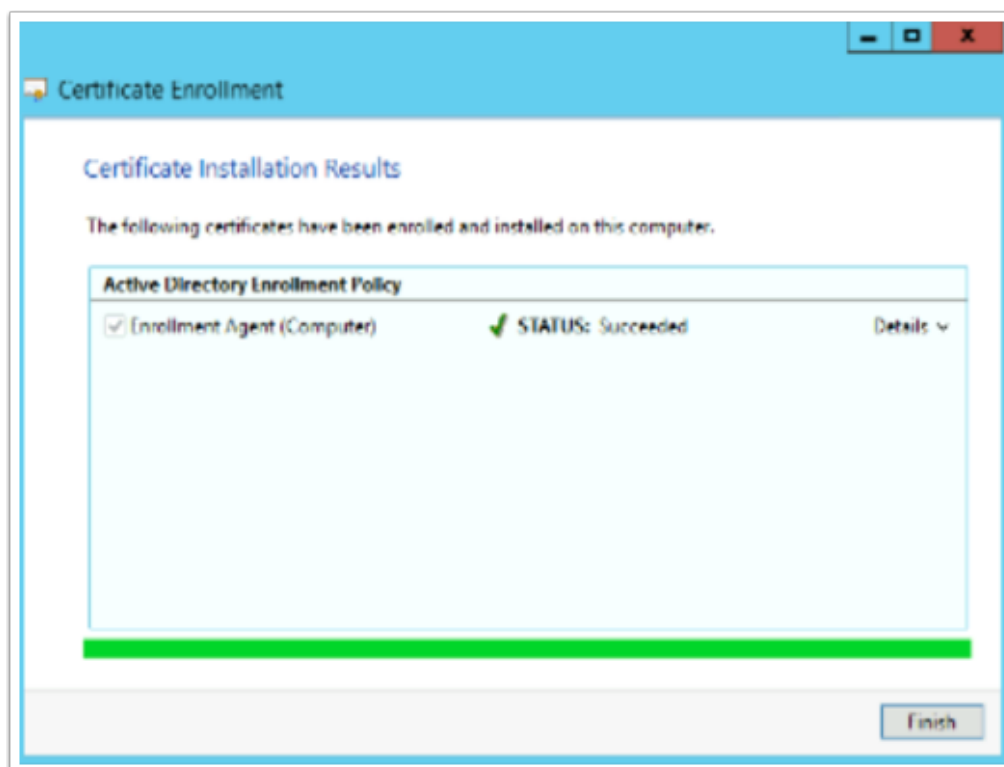   - Select **All Tasks** > **Request New Certificate**

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

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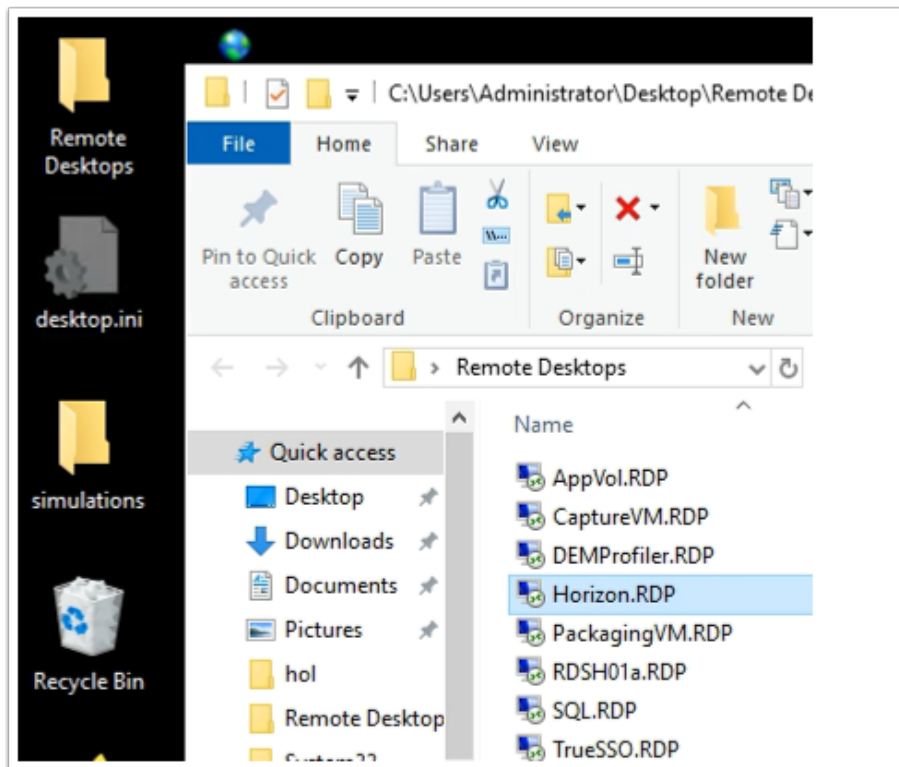   • Select **Next**

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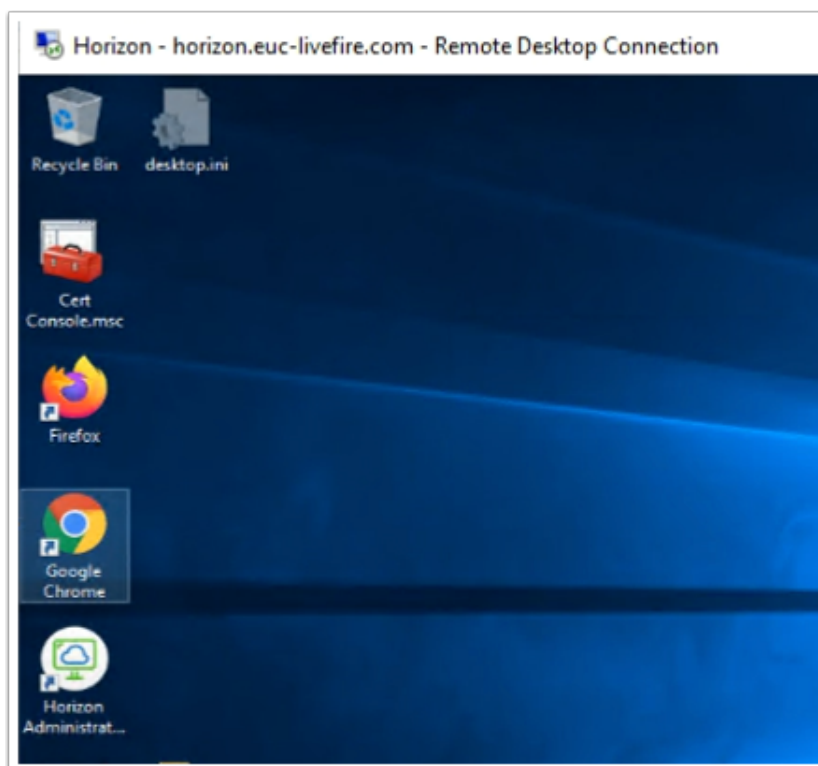   - Select **Enroll**

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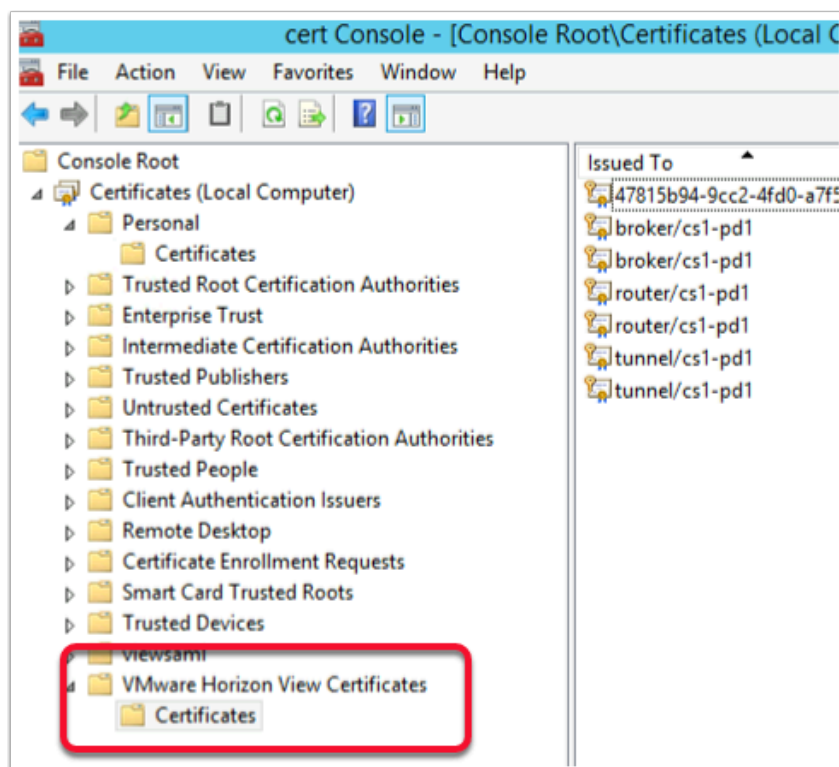
- Select **Finish**.

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

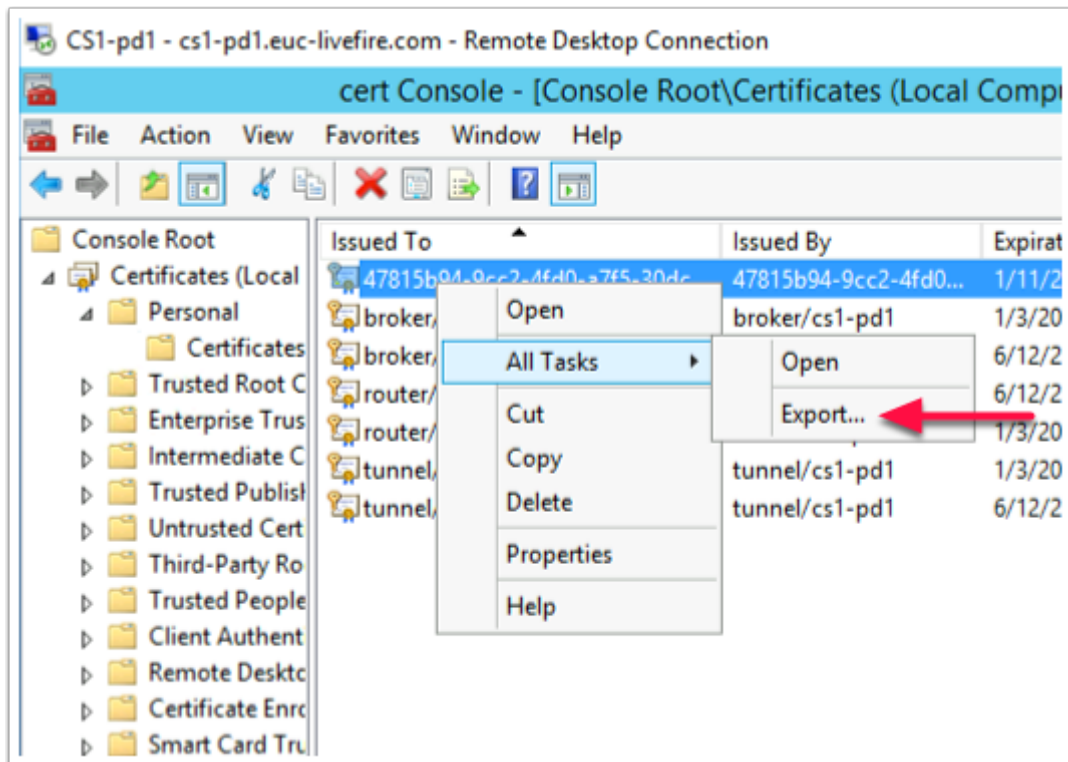- Select and open your **Cert Console.mmc**

45. In the **Certificates** Console
    - **Expand** the inventory
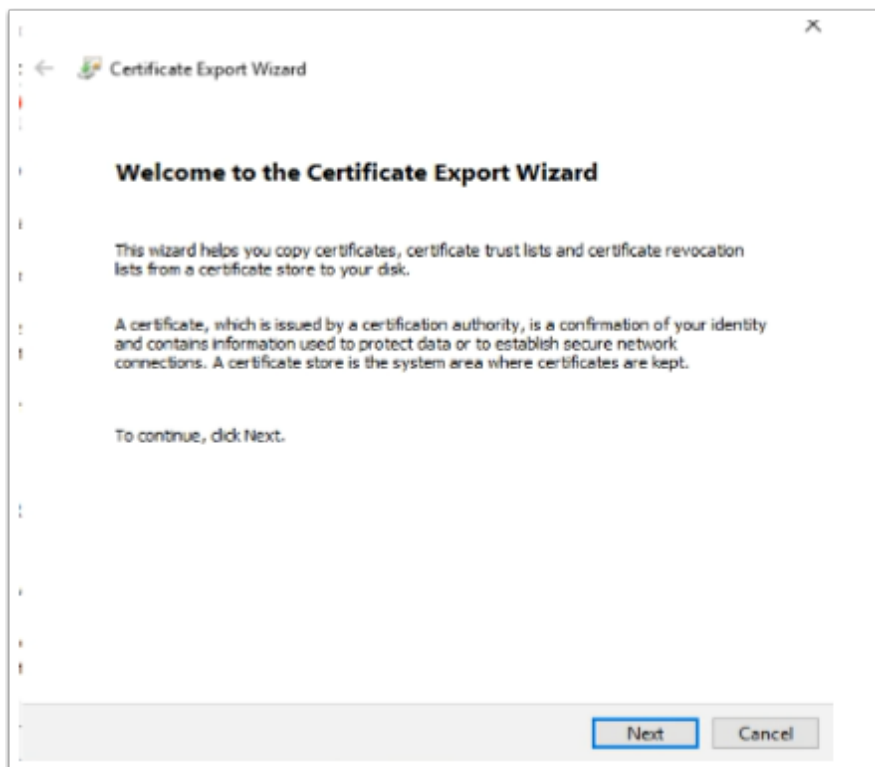   - Browse down to **VMware Horizon View Certificates** > **Certificates**

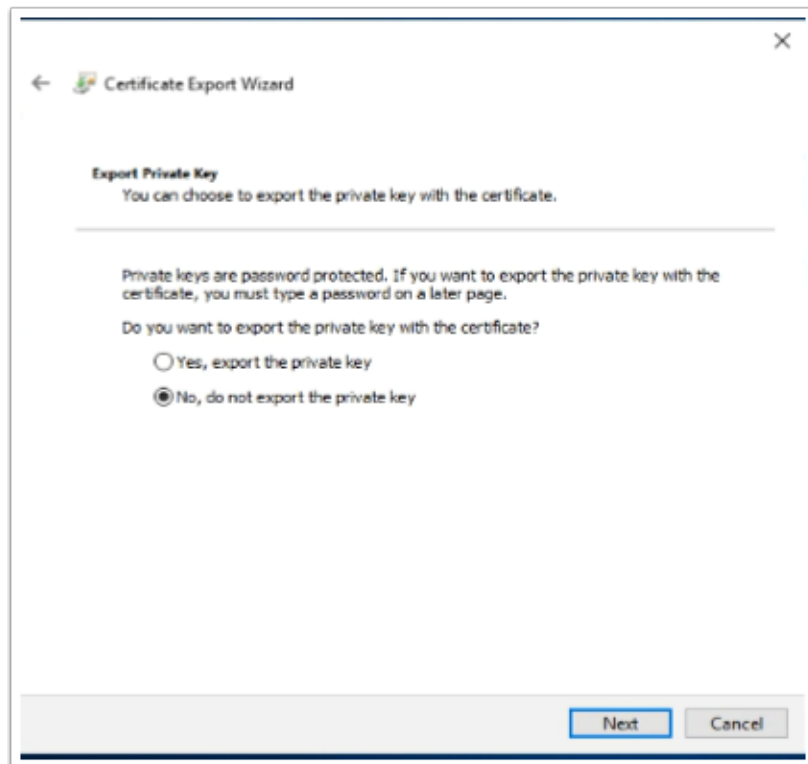46. In the **VMware Horizon View Certificates** > **Certificates** folder
    - Expand the console or **scroll** across the console and notice the **guid** based certificate has a friendly name of **vdm.ec**
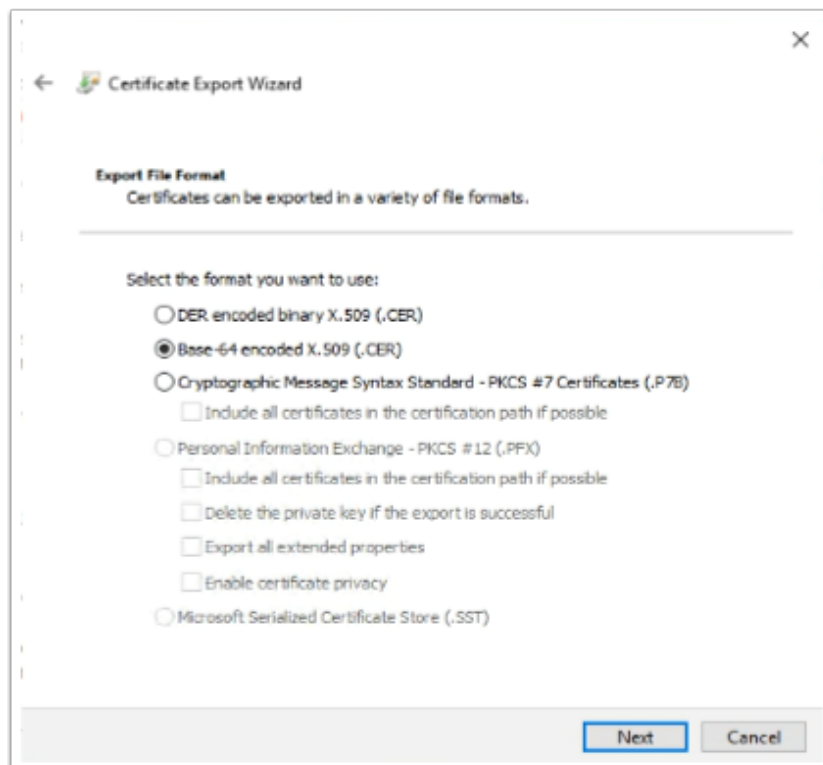
47. Select your **GUID certificate** with the friendly name of **vdm.ec.**
    - Right-Click select **All Tasks**
    - Select **Export**

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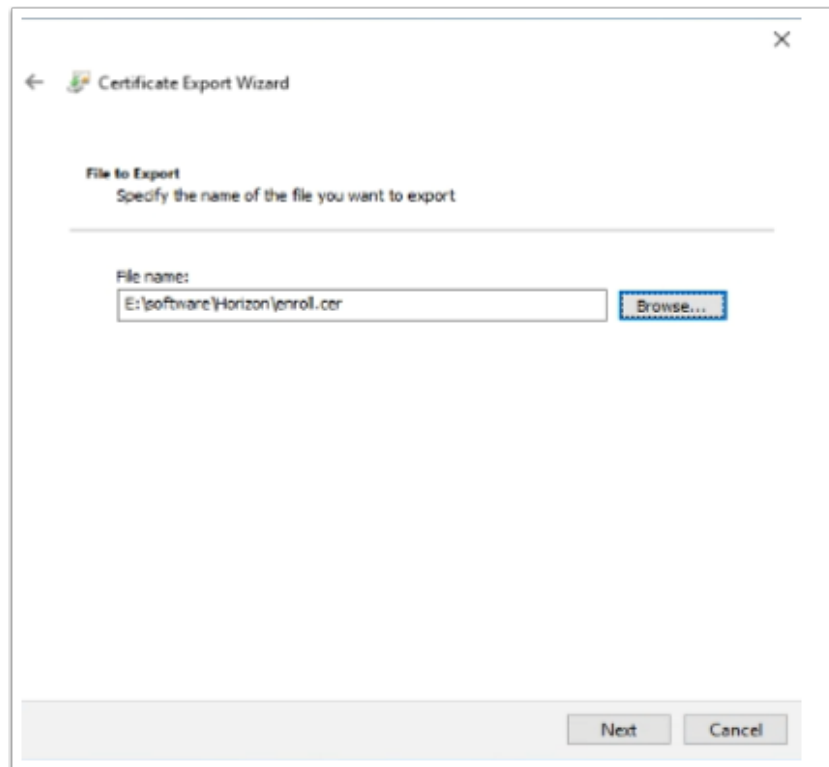   - Select **Next**

---

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**
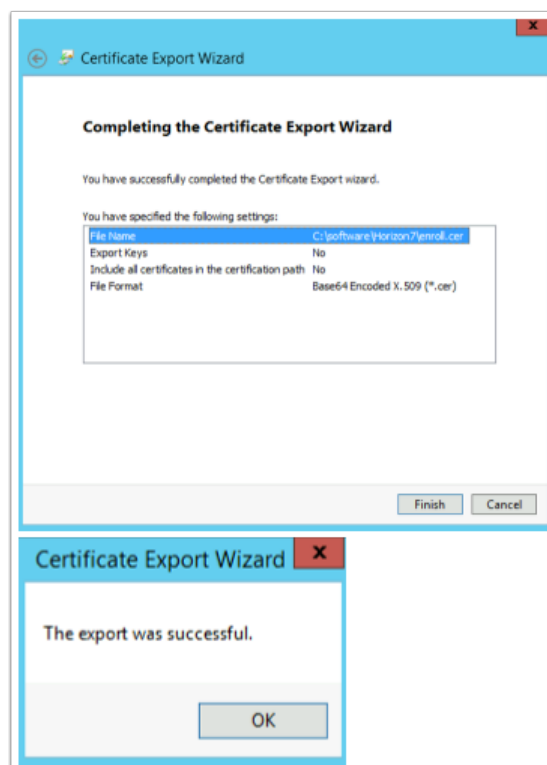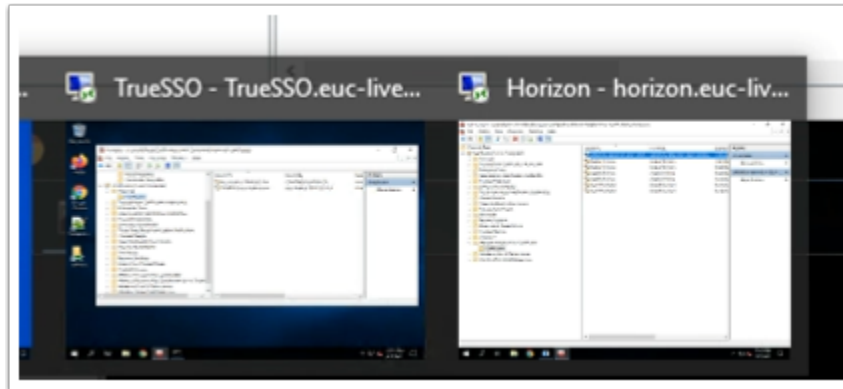

- Select **Next**

51. In the **File to Export** window
    - Under **File name** type the following **E:\software\Horizon\enroll.cer**
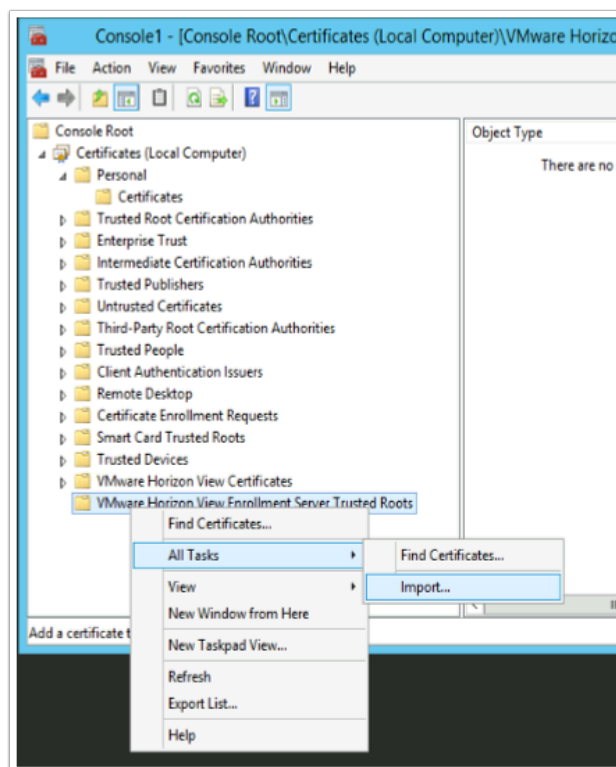   - Select **Next**

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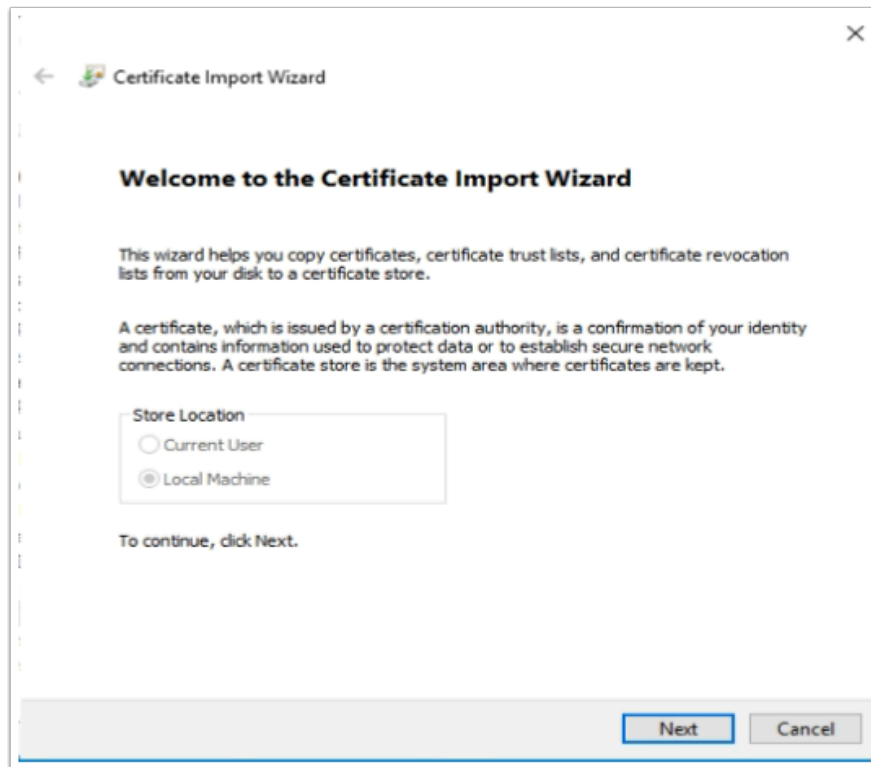
55. On the **Welcome** window select **Next**

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

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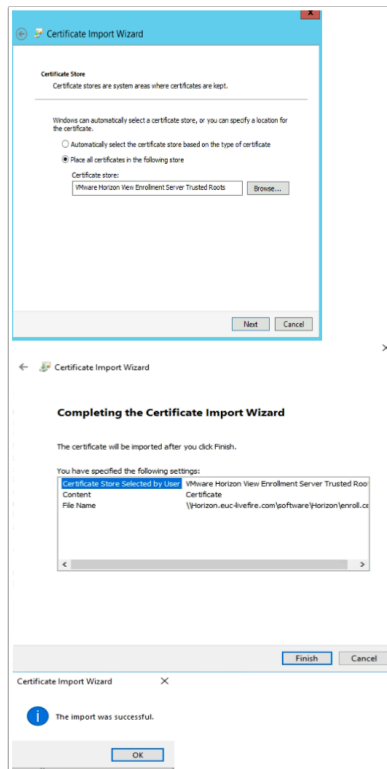
57. In the **Certificate Store** window accept the defaults and
    - Select **Next.**
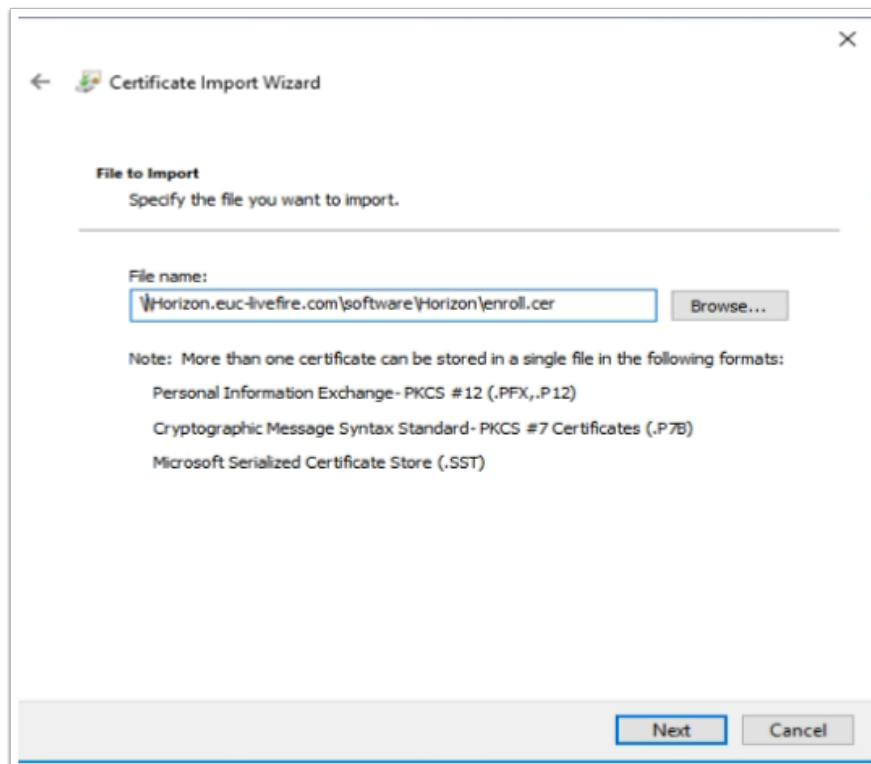   - On the **Summary** page select **Finish**.
    - When Prompted that **The Import was succesful** select **OK**
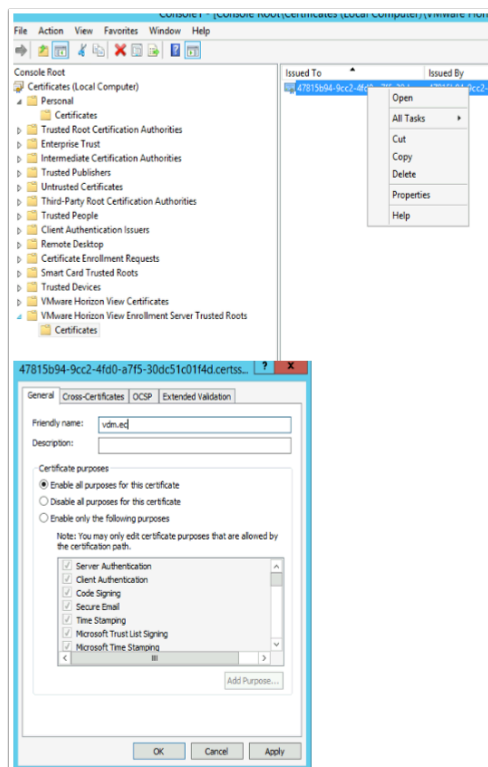
58. In the **Certificates** Folder

- Right-click the **imported certificate**
- Select **Properties.**
- In the **Friendly name:** section type **vdm.ec**
- Select **OK**
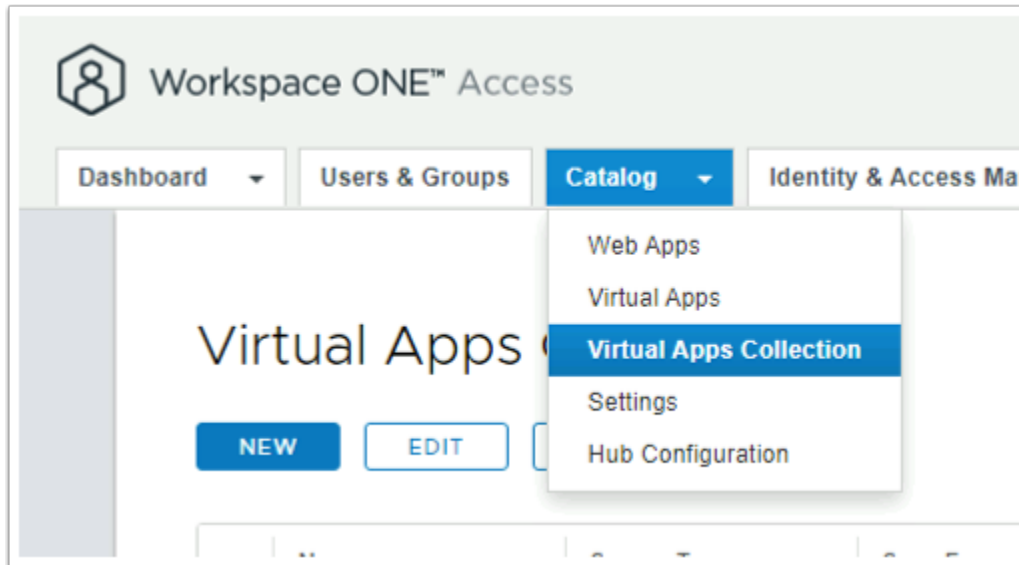
59. Switch to your **browser, Workspace ONE Access Saas** session,
    - Select the **Catalog** tab > **Virtual Apps Collection**

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

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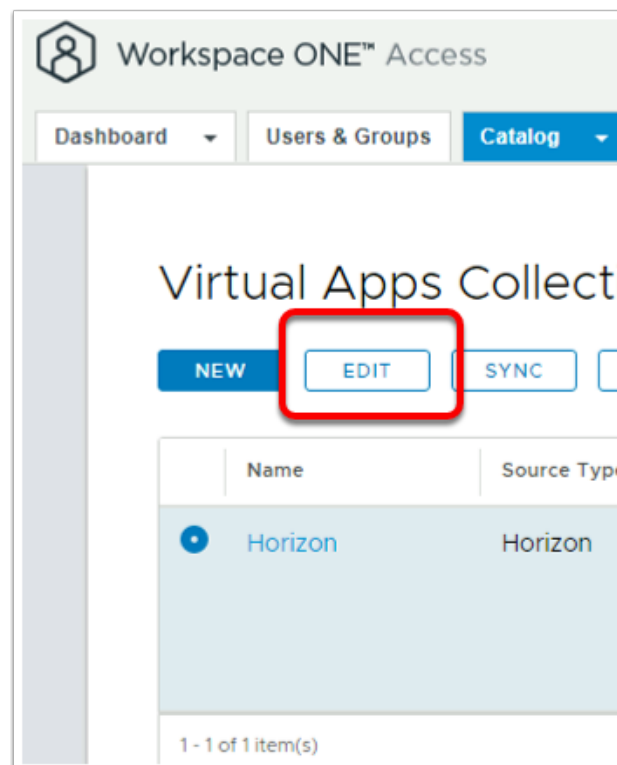- Select **2 Pod and Federation**,
  - Under **Horizon Connection Server**
    - Select **Horizon.euc-livefire.com**

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

- Select **SAVE ,**
- Select **NEXT**,
- Select **NEXT**,
- Select **SAVE**
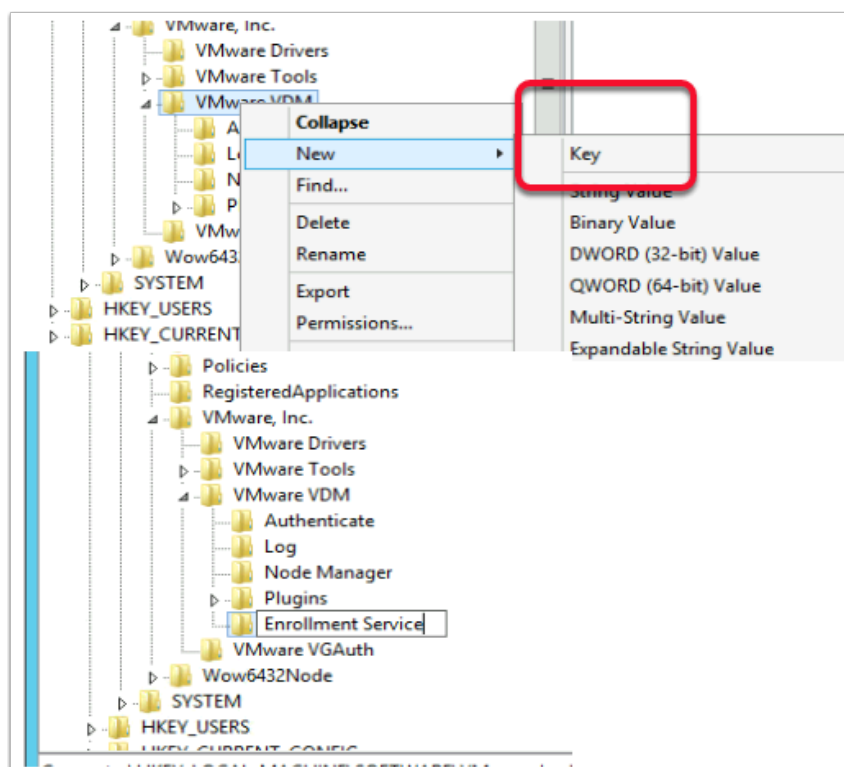
63. On the **ControlCenter** server, switch back to your **TrueSSO.RDP** session
    1. Select the **Start button** > **RUN** and type **regedit.exe**
    2. In the regedit inventory, browse to the following location, browse to
        - **HKLM\SOFTWARE\VMware, Inc.\VMware VDM**
        - What we should 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
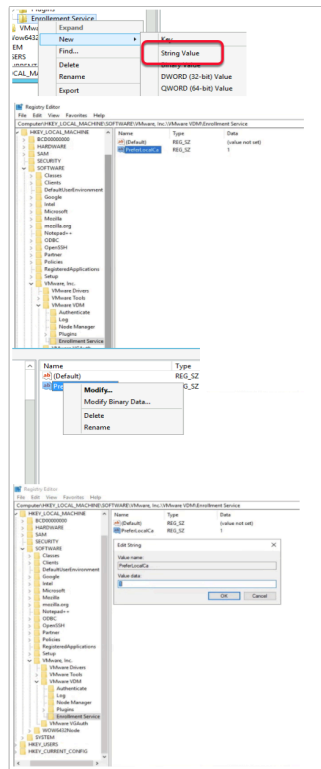
64. Configure the enrollment service to give preference to the local certificate authority when they are co-located:
    - Add a new **String Value**
        - Right-click the **Enrollment Service** key > **New** > **String Value** and type the name **PreferLocalCa**
        - Right-click the **PreferLocalCa** String value and select **Modify** and in the **Value data:** field enter **1**
        - Select **OK** to close the window.
        - Click to **close RegEdit**
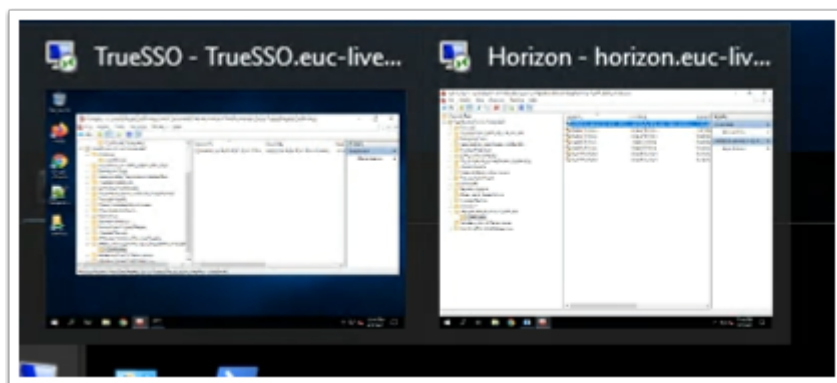
65. On your **ControlCenter** server
    - Switch to your **HORIZON.**RDP session
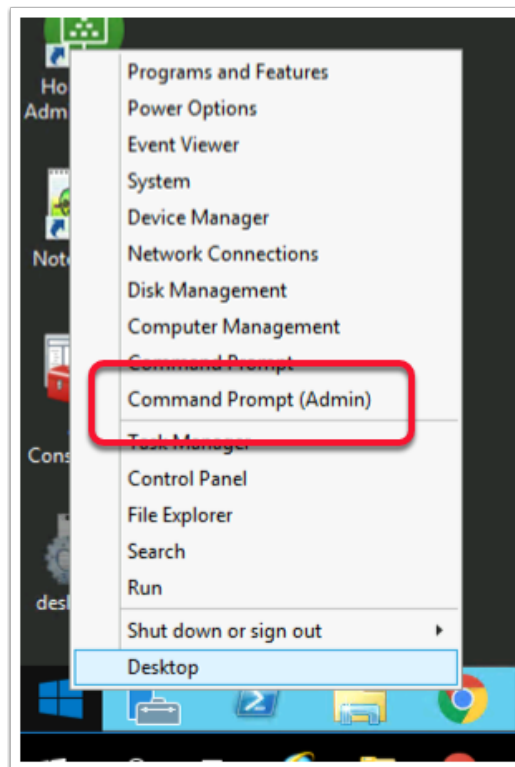
66. Select and right-click the **Start** button
    - Select **Command Prompt (Admin)**

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

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

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

The enrollment server is added to the global list.

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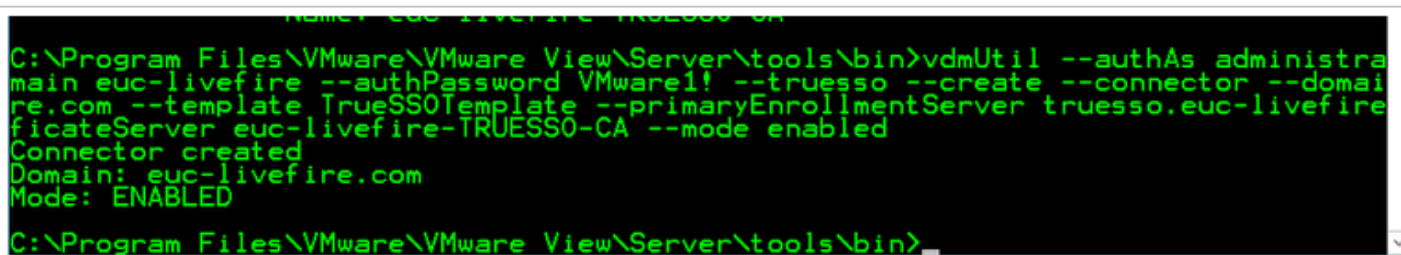
```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administra
tor --authDomain euc-livefire --authPassword VMware1! --truesso --environment --
list --enrollmentServer TrueSSO.euc-livefire.com --domain euc-livefire.com
True SSO environment info
Enrollment server: truesso.euc-livefire.com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

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

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

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

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

```
                    Name: euc-livefire-TRUESSO-CA
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmUtil --authAs administra
main euc-livefire --authPassword VMware1! --truesso --create --connector --domai
re.com --template TrueSSOTemplate --primaryEnrollmentServer truesso.euc-livefire
ficateServer euc-livefire-TRUESSO-CA --mode enabled
Connector created
Domain: euc-livefire.com
Mode: ENABLED
C:\Program Files\VMware\VMware View\Server\tools\bin>_
```

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

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

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

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

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

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


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

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

For --truessoMode, use ENABLED if you want True SSO to be used only if no password was supplied when the user logged in to VMware Identity Manager. In this case if a password was used and cached, the system will use the password. Set --truessoMode to ALWAYS if you want True SSO to be used even if a password was supplied when the user logged in to VMware Identity Manager
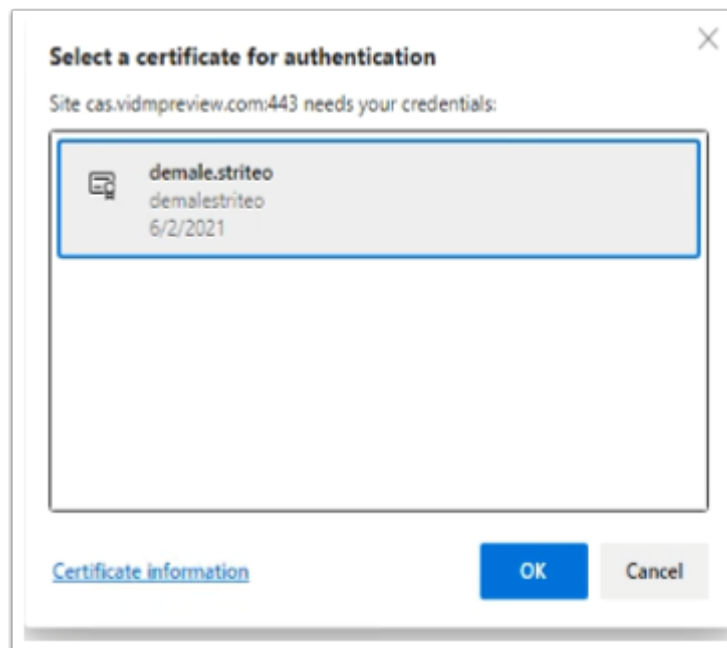
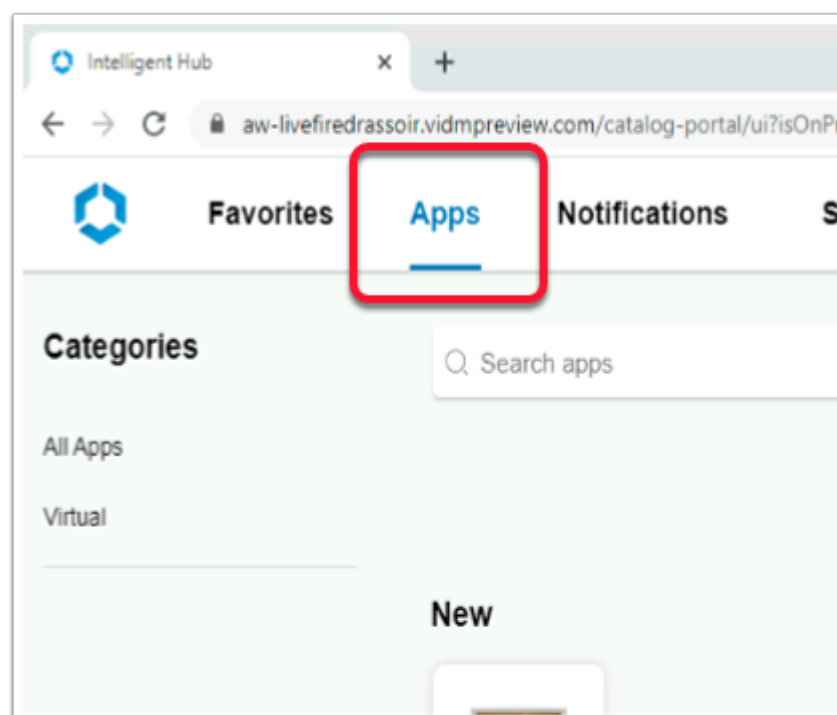# Part 4: Testing to see if TrueSSO works
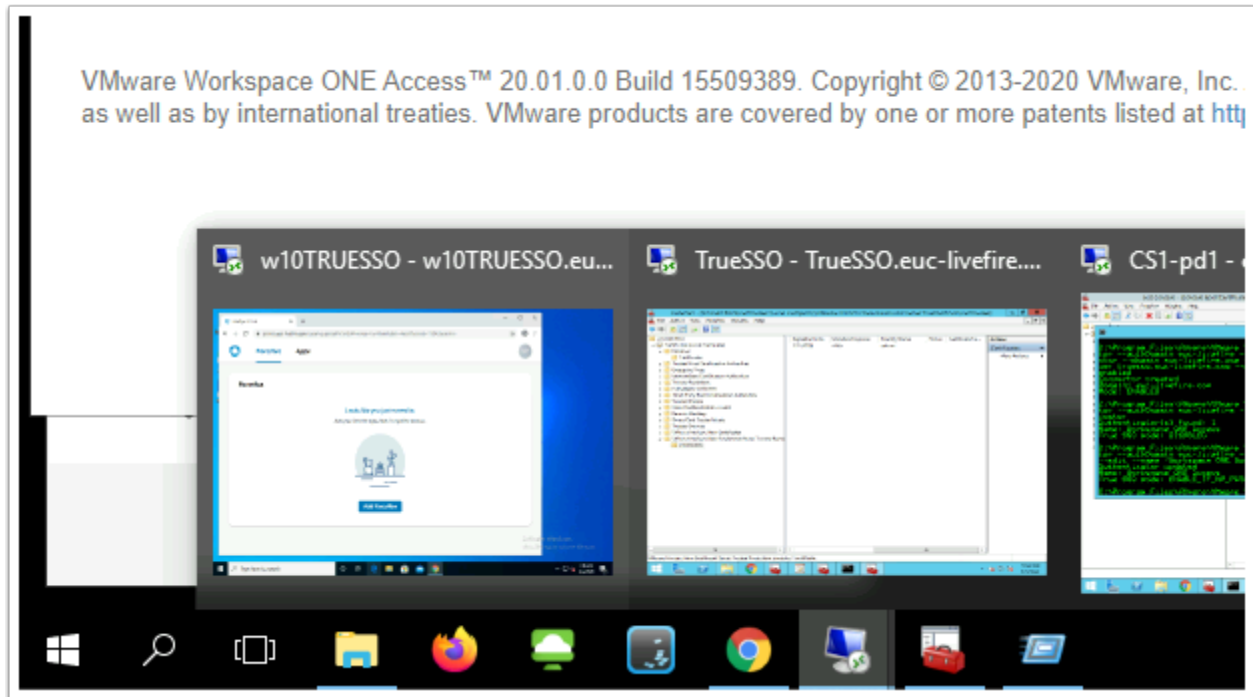
1. On your **ControlCenter** server, switch your **Remote Desktops** session for **W10Client01.RDP**.
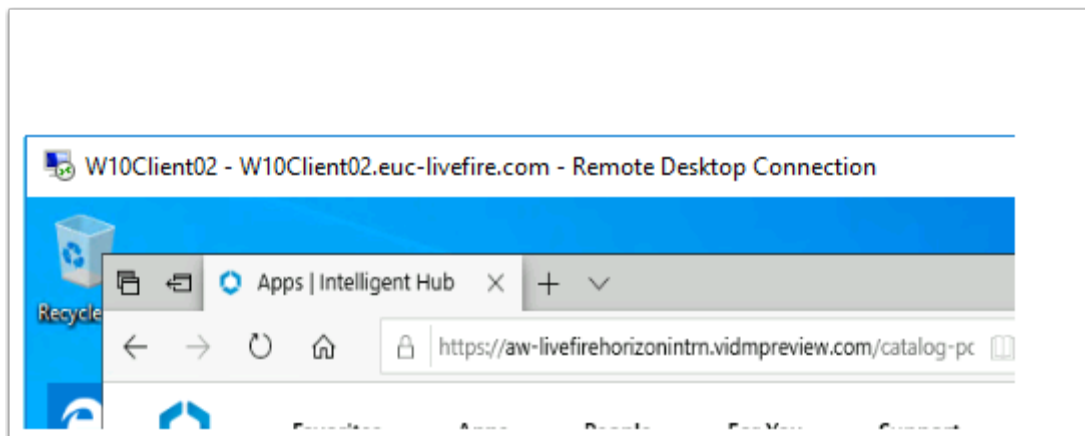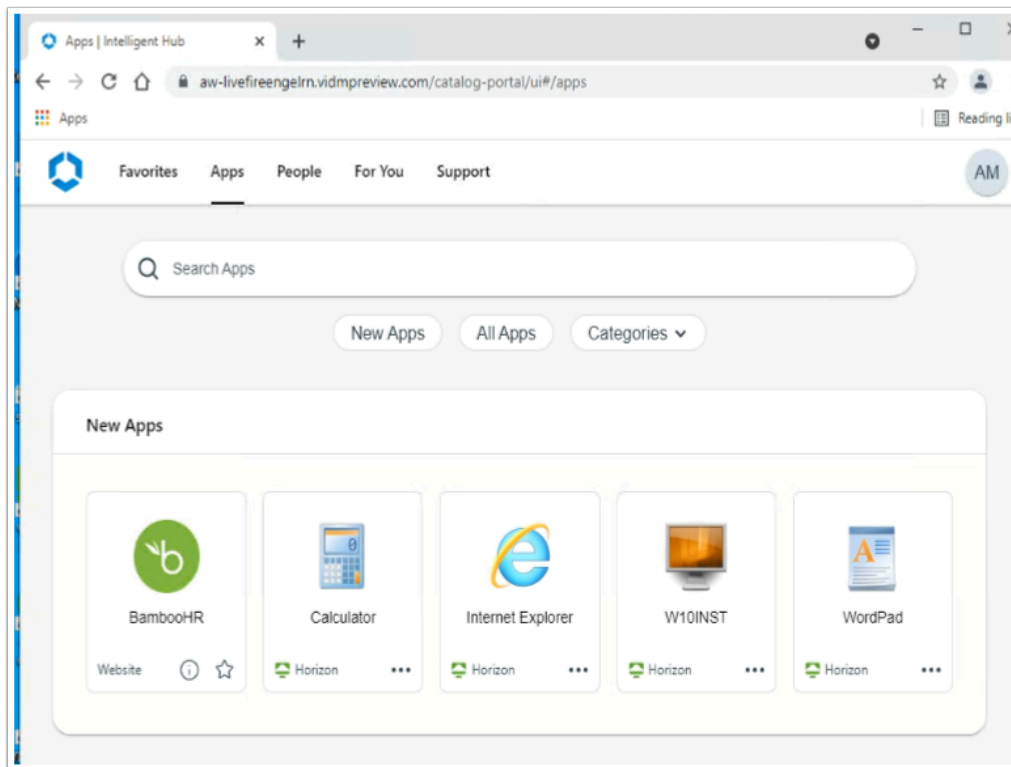

2. On your **W10Client01** desktop, ensure that any existing browser session is **CLOSED**
   • **Open** your browser and type enter your custom **Access Tenant URL**

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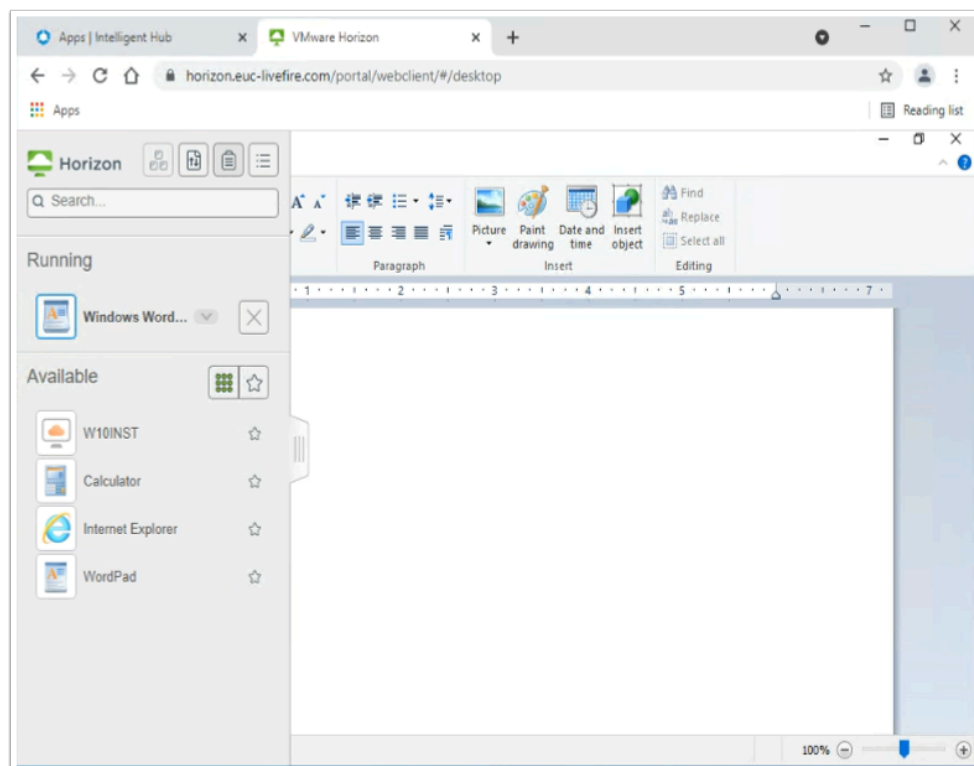

4. Select **Apps** tab in the Console

5. In the Web based Intelligent Hub
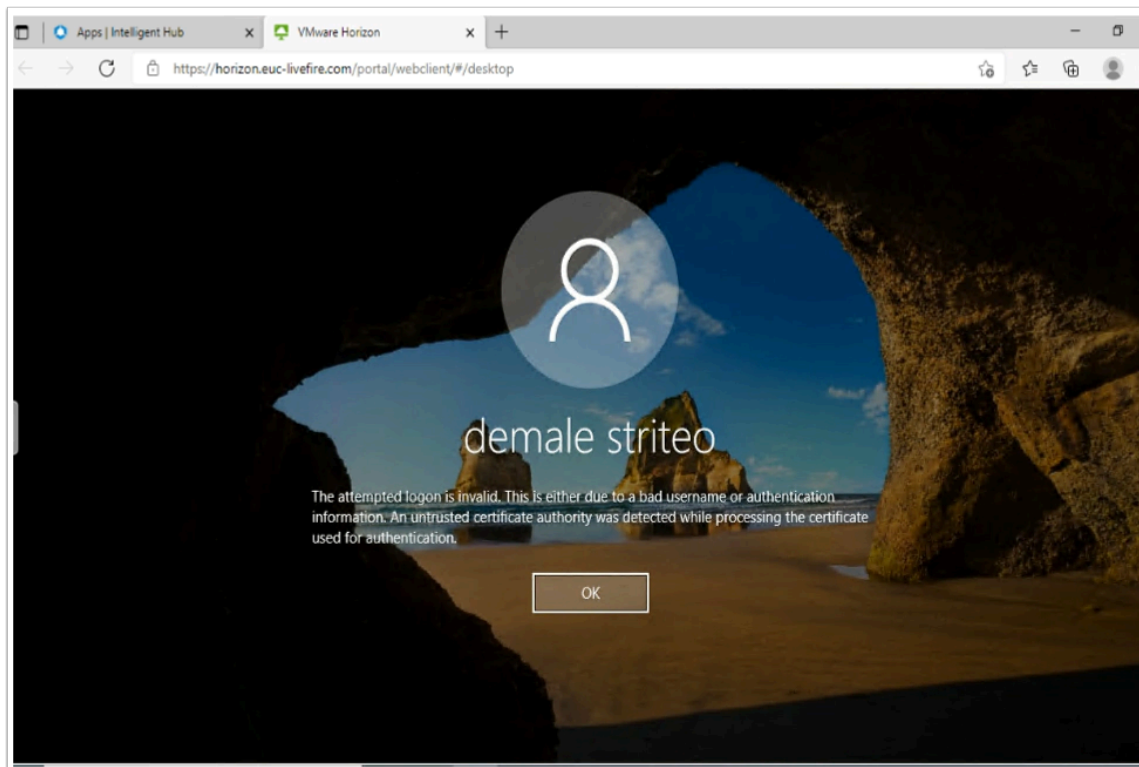   - In the **Apps** area, under **New Apps** select **Wordpad**


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
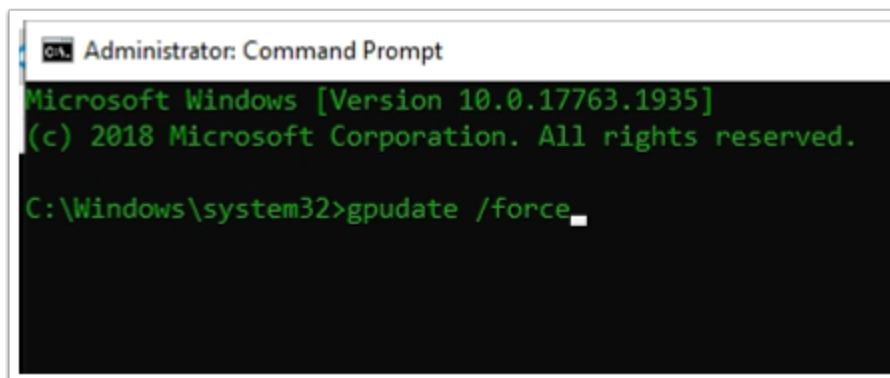

8. On the ControlCenter server
    - Open the **Command Prompt** on all **stakeholder platforms** and type the command **GPUPDATE /Force**
    - Repeat this same task on the Horizon server

You are now ready to again test your login through **Workspace ONE Access**. If necessary go back to Paragraph1 and repeat the login process
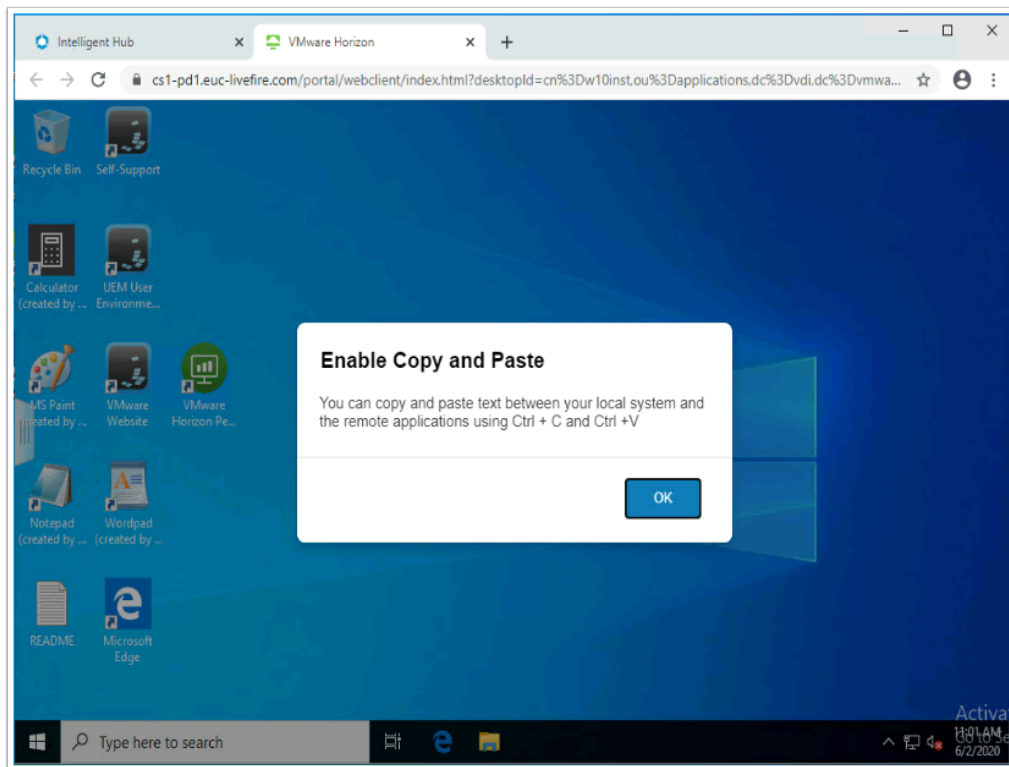
9. Launch another session from the **Workspace ONE** portal and launch your **Desktop** entitlement.
   - This should be the result
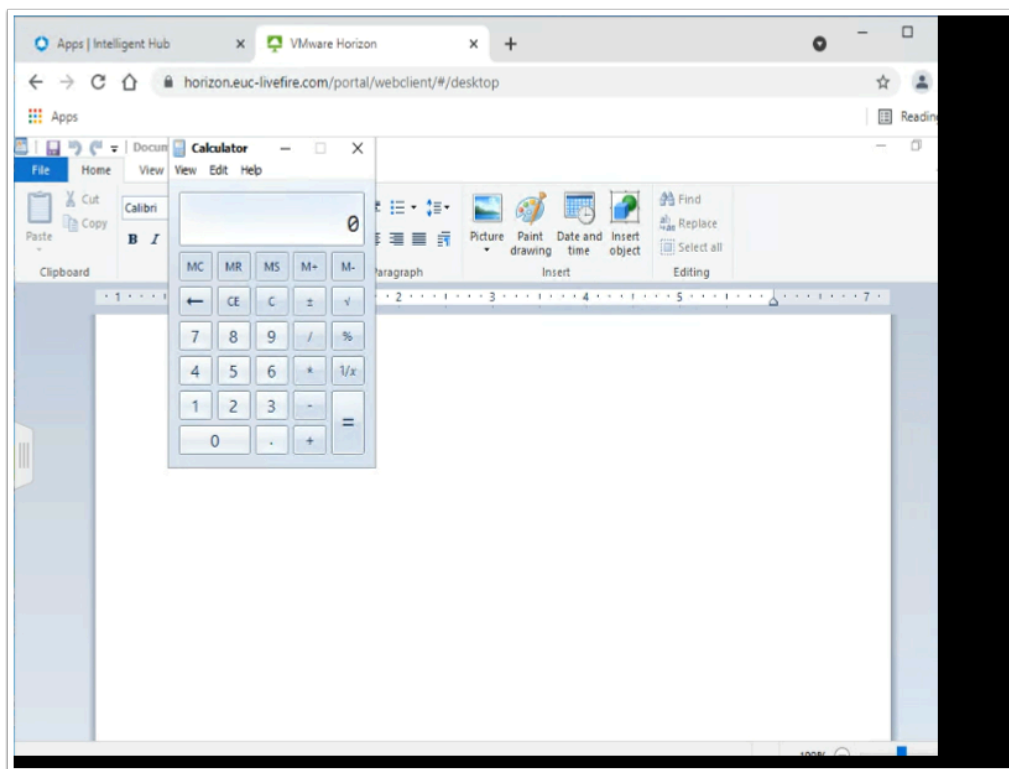
10. Launch another session from the **Workspace ONE** portal and launch an **Application** entitlement.

- 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>