THALES

Microsoft Active Directory Certificate Services: Integration Guide

THALES LUNA HSM AND LUNA CLOUD HSM

Document Information

Document Part Number	007-008669-001
Revision	AC
Release Date	20 April 2023

Trademarks, Copyrights, and Third-Party Software

CONTENTS

Overview

This document explains how to integrate Microsoft Active Directory Certificate Services (AD CS) with Luna HSM or Luna Cloud HSM. The Microsoft AD CS provides customizable services for creating and managing public key certificates used in software security systems employing public key infrastructure. Organizations use public key certificates to enhance their digital security by binding the identity of a person, device, or service to a corresponding private key.

The root of trust in a public key infrastructure is the certificate authority (CA). Fundamental to this trust is the CA's root encryption key, which is used to sign the public keys of certificate holders and more importantly its own public key. Microsoft AD CS integrates with Luna HSM or Luna Cloud HSM service to secure the root encryption key.

Using Luna HSMs to secure the Microsoft AD CS root encryption key provides the following benefits:

> Secure generation, storage and protection of the Identity signing private key on FIPS 140-2 level 3 validated hardware

> Full life cycle management of the keys

> HSM audit trail

> Load balancing and fail-over by clustering the HSMs

> Using cloud services with confidence

NOTE: Luna Cloud HSM does not have access to the secure audit trail

Certified Platforms

This integration is certified on the following platforms:

- Certified platforms on Luna HSM
- Certified platforms on Luna Cloud HSM

Certified platforms on Luna HSM

HSM Type	Platforms Tested
Luna HSM	Windows Server 2022 Windows 2019 Server Windows 2016 Server Windows Server 2012R2

Luna HSM: Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and

Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM Cloud HSM and AWS CloudHSM Classic.

Certified platforms on Luna Cloud HSM

HSM Type	Platforms Tested
Luna Cloud HSM	Windows Server 2022 Windows 2019 Server Windows 2016 Server Windows Server 2012R2

Luna Cloud HSM: Luna Cloud HSM services provide on-demand, cloud-based storage, management, and generation of cryptographic keys through a simple graphical user interface. With Luna Cloud HSM, security is simple, cost effective, and easy to manage because there is no hardware to buy, deploy, and maintain. As an Application Owner, you click and deploy services, generate usage reports, and maintain only those services that you need.

Prerequisites

Before you begin the integration process, ensure that you have completed the following tasks:

Configuring Luna HSM

Configuring Luna Cloud HSM

Configuring Luna HSM

To configure Luna HSM:

1. Ensure the HSM is setup, initialized, provisioned and ready for deployment.
2. Create a partition, establish a Network Trust Link (NTL) between the HSM and client, and enable the client to access the partition. Refer to Luna Network HSM documentation for the detailed process.
3. Initialize Crypto Officer and Crypto User roles for the partition.
4. Use the following command to validate that the partition is successfully registered and configured:

```
Path to lunacm utility>lunacm

lunacm.exe (64-bit) v7.3.0-139. Copyright (c) 2018 SafeNet. All rights
reserved.

Available HSMs:

      Slot Id ->              0

      Label ->                ms-adcs

      Serial Number ->        1238696044953

      Model ->                LunaSA 7.3.0
```

```
Firmware Version ->      7.3.0
Configuration ->         Luna User Partition With SO (PW) Key Export
With Cloning Mode
Slot Description ->      Net Token Slot
```

NOTE: For a detailed description of the steps involved in Luna HSM configuration, refer to Luna Network HSM documentation.

To configure Luna HSM HA (High-Availability)

Please refer to the Luna HSM documentation for HA steps and details regarding configuring and setting up two or more HSM appliances on Windows and UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stop functioning for some reason, all calls automatically routed to secondary till primary starts functioning again.

NOTE: This integration is tested in both HA and FIPS mode.

Configuring Luna Cloud HSM

Follow these steps to set up your Luna Cloud HSM:

1. Transfer the downloaded .zip file to your client workstation using pscp, scp, or other secure means.
2. Extract the .zip file into a directory on your client workstation.
3. Extract or untar the appropriate client package for your operating system using the following command:

   ```
   tar -xvf cvclient-min.tar
   ```

   NOTE: Do not extract to a new subdirectory. Place the files in the client install directory.

4. Run the `setenv` script to create a new configuration file containing information required by the Luna Cloud HSM service:

   ```
   source ./setenv
   ```

   NOTE: To add the configuration to an already installed UC client, use the -addcloudhsm option when running the setenv script.

5. Run the LunaCM utility and verify the Cloud HSM service is listed.

   NOTE: If your organization requires non-FIPS algorithms for your operations, ensure that the Allow non-FIPS approved algorithms check box is checked. For more information, refer to Supported Mechanisms.

Integrating Luna HSM with Microsoft AD CS on Windows Server

This section outlines the steps to install and integrate Microsoft Active Directory Certificate Services (AD CS) on Windows Server with a Luna HSM or Luna Cloud HSM service. Microsoft AD CS uses the SafeNet Luna KSP (Key Storage Provider) for integration.

We recommend familiarizing yourself with Microsoft Active Directory Certificate Services. Refer to the Microsoft AD CS Configuration documentation for more information.

Configure SafeNet Key Storage Provider (KSP)

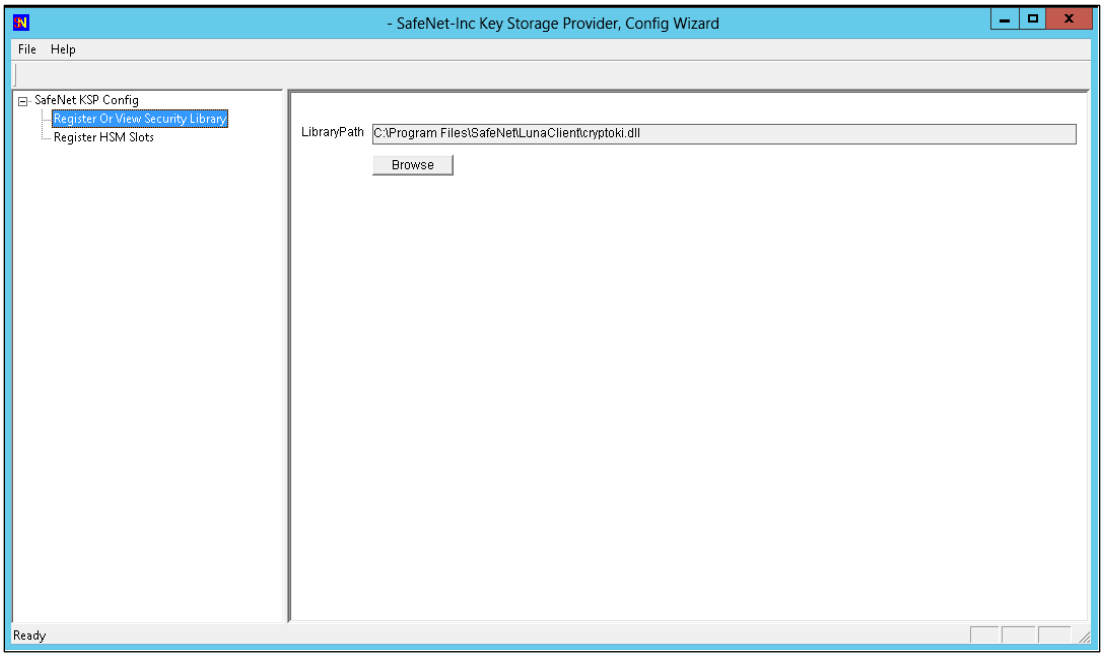
You must configure the SafeNet Key Storage Provider (KSP) to allow the user account and system to access the Luna HSM or Luna Cloud HSM service.

> If you are using a Luna HSM, the KSP package must be installed during the Luna Client software installation.

> If you are using Luan Cloud HSM service, the KSP package is included in the service client package inside of the /KSP folder.

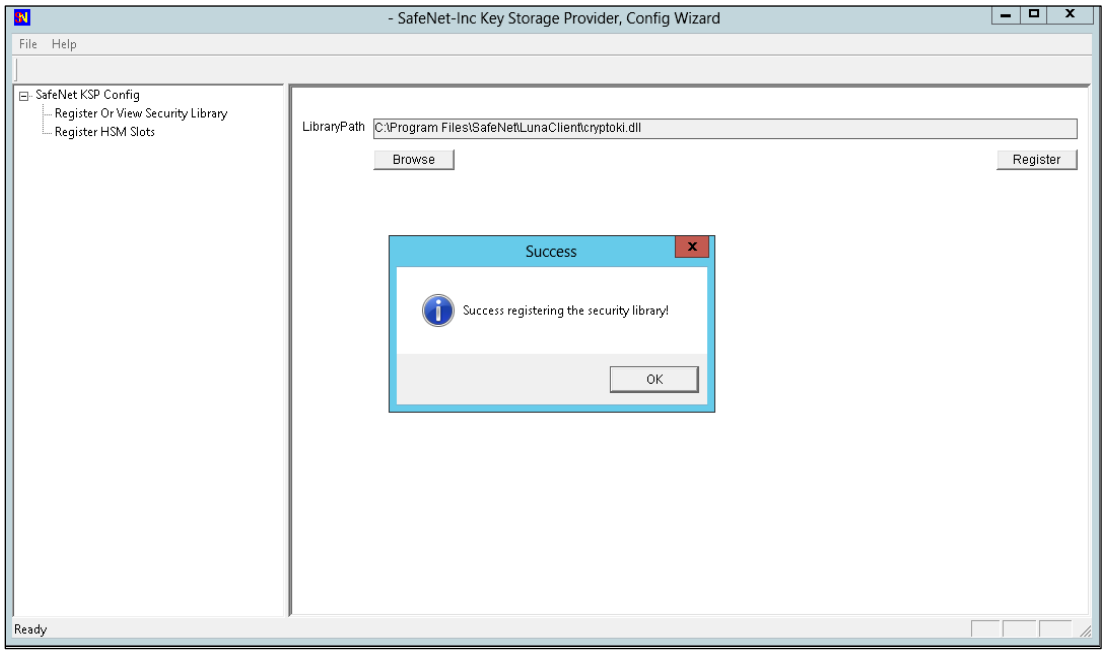
To configure the SafeNet Key Storage Provider:

1. Navigate to the <SafeNet HSM Client installation Directory>/KSP directory.
2. Run the KspConfig.exe (KSP configuration wizard).
3. Double-click Register Or View Security Library.
4. Browse the library cryptoki.dll from the Luna HSM Client installation directory or Luna Cloud HSM service client package and click **Register**.

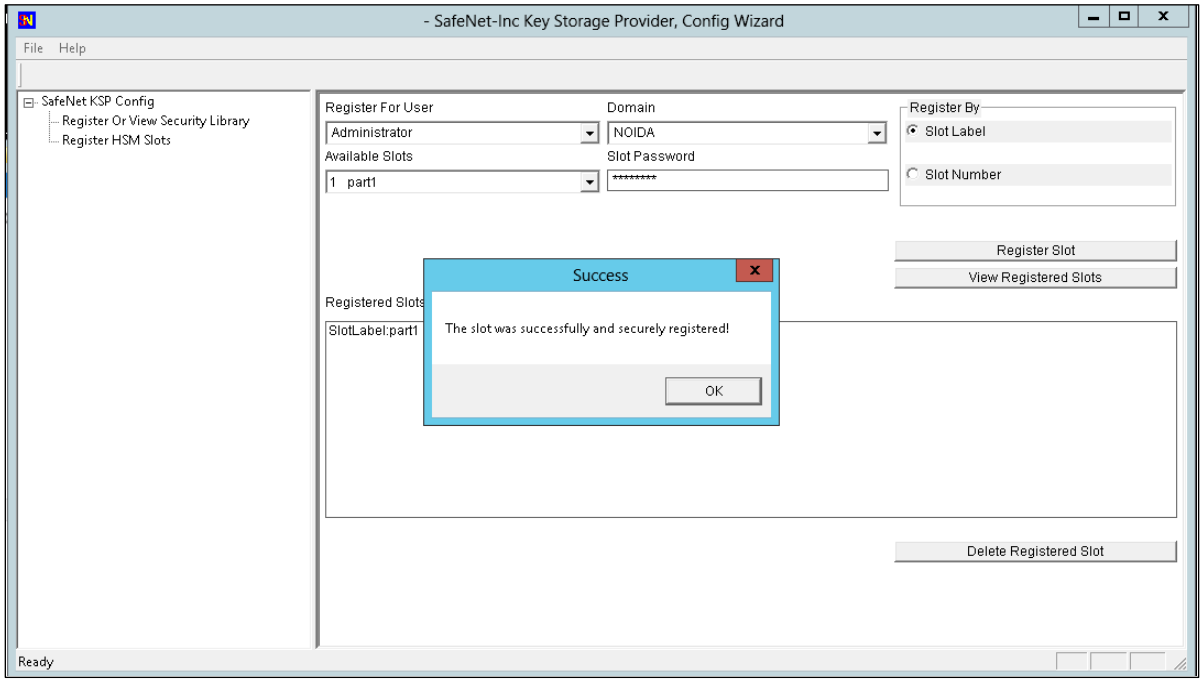


5. On successful registration, you will see the following message:

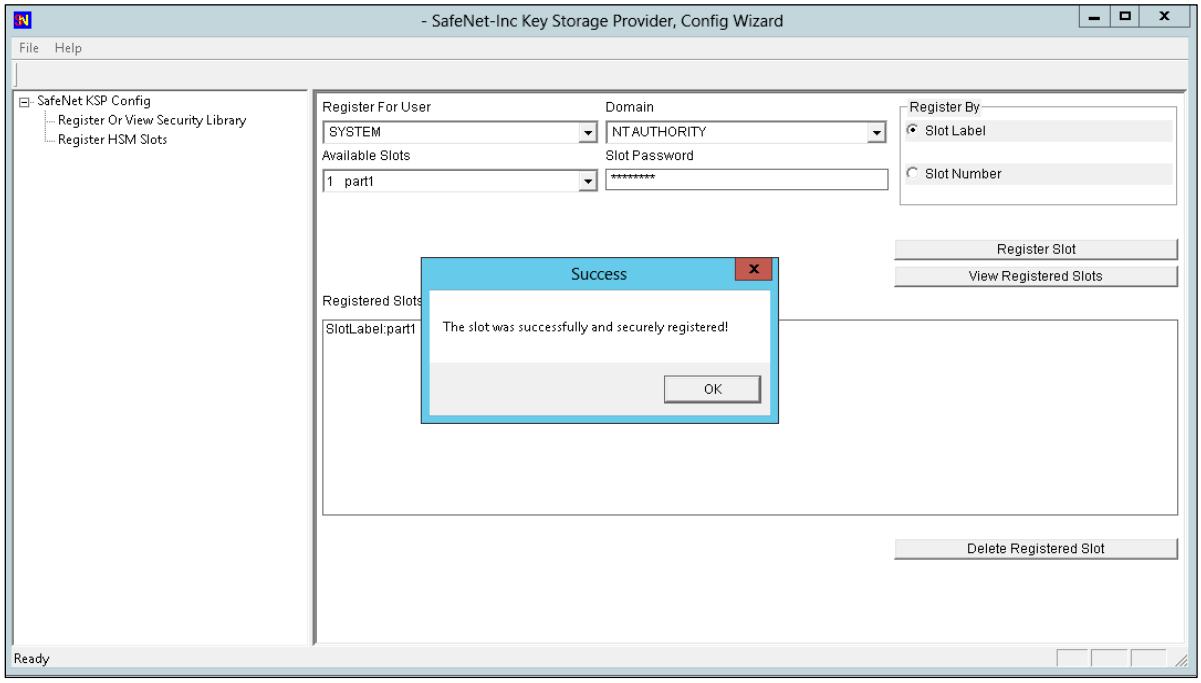
   Success registering the security library!



6. Double-click **Register HSM Slots** on the left side of the pane.
7. Enter the Slot (Partition) password.
8. Click **Register Slot** to register the slot for Domain\User. On successful registration, a message "**The slot was successfully and securely registered**" displays.



9. Register the same slot for **NT AUTHORITY\SYSTEM**.



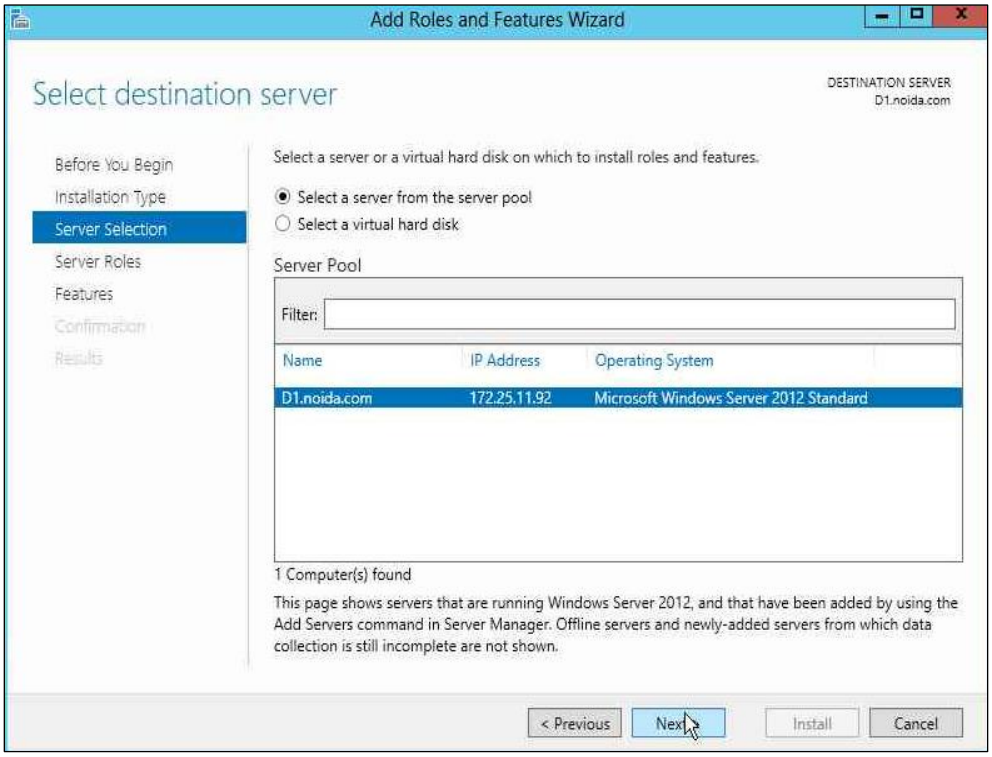
NOTE: Both slots have been registered, despite only one entry appearing for the service in the **Registered Slots** section of the KSP interface.

Install Microsoft AD CS on Windows Server using SafeNet KSP

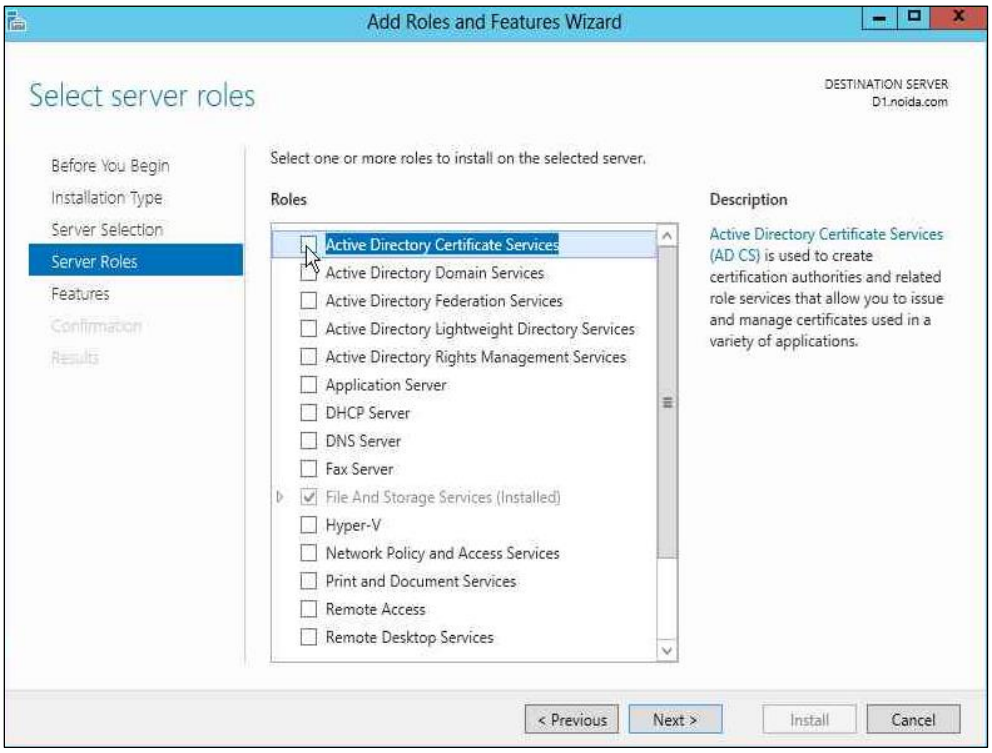
You must configure Microsoft AD CS to use the Luna HSM or Luna Cloud HSM service when you configure the Microsoft Certificate Authority (CA) user role. To install Microsoft AD CS:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Ensure you have configured the SafeNet KSP. Refer to the section Configure SafeNet Key Storage Provider (KSP) section for more information.
3. Open the **Server Manager** under **Configure this Local Sever** and click **Add Roles and Features**.
4. The **Add Roles** wizard displays.
5. Click **Next**.
6. Select the **Role-based or feature-based installation** radio button and click **Next**.

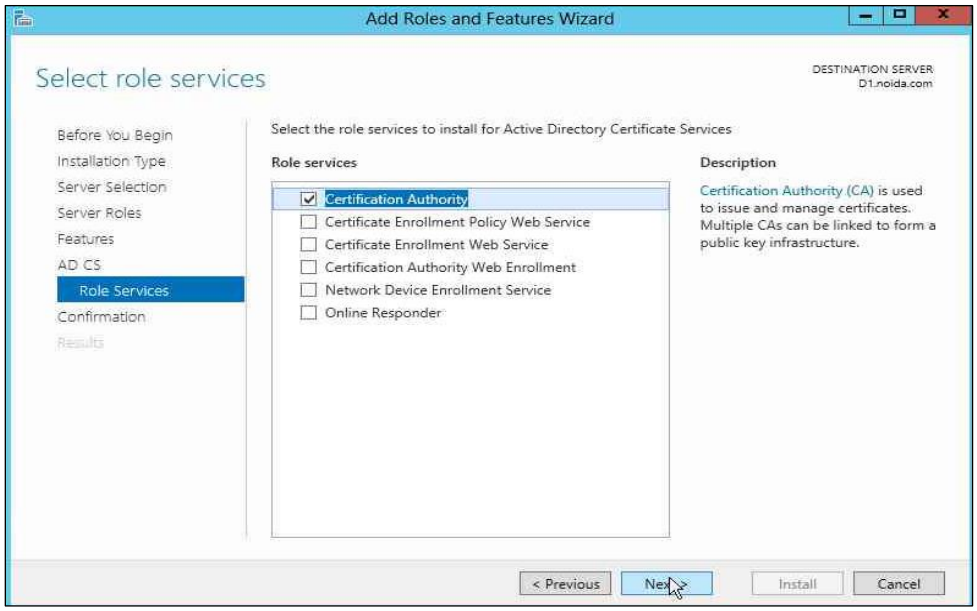
7. Select the **Select a server from the server pool** radio button and select your server from the **Server Pool** menu.



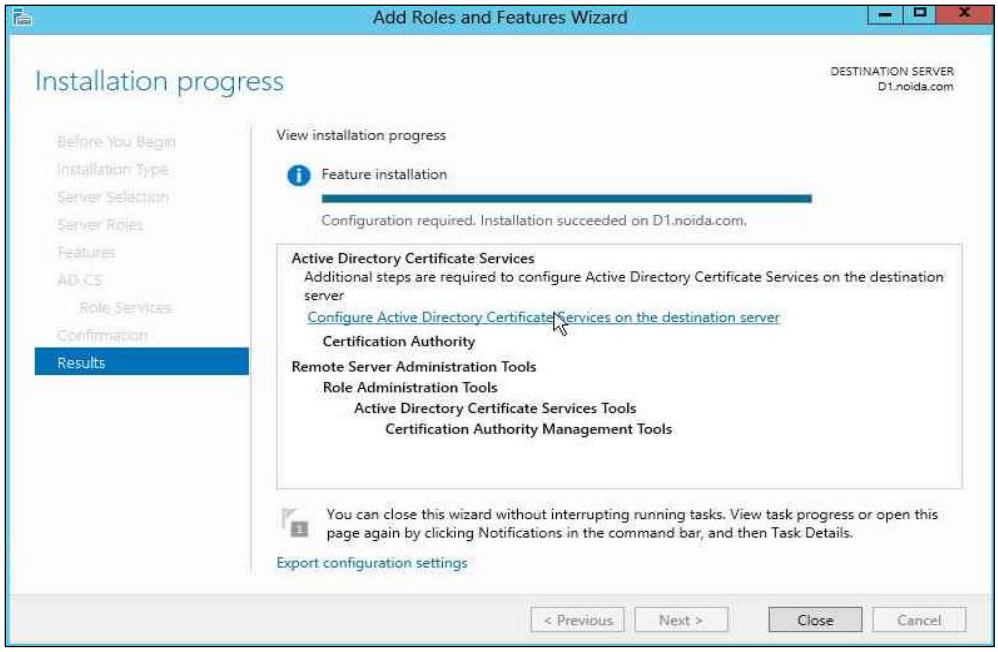
8. Click **Next**.Select the **Active Directory Certificate Services** check box.



9. A window displays stating **Add features that are required for Active Directory Certificate Services?** To add a feature, click the **Add Features** button.
10. Click **Next** to continue.
11. On the Active Directory Certificate Services page click **Next** to continue.
12. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

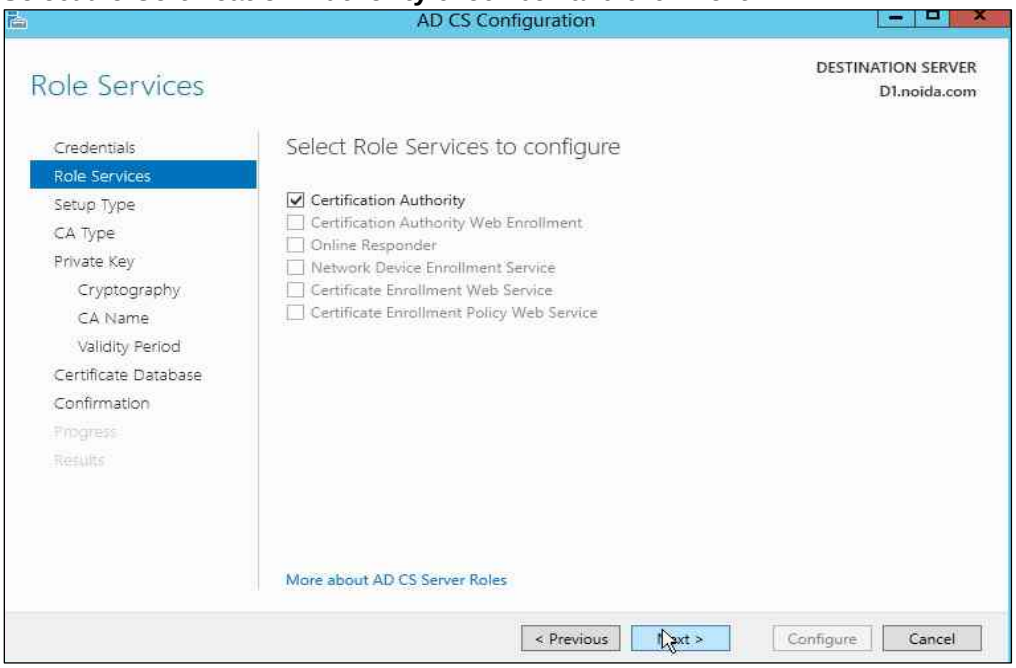


13. Click **Install**.
14. When installation is complete, click **Configure Active Directory Certificate Services on the destination server** and the AD CS Configuration wizard displays.



15. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.

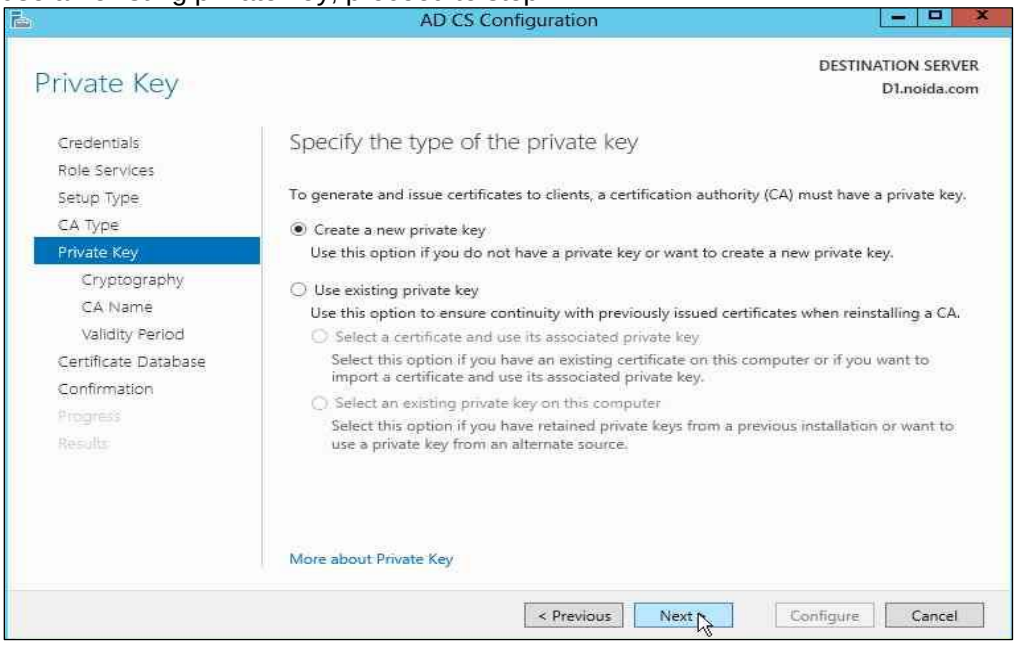
16. Select the **Certification Authority** check box and click **Next**.



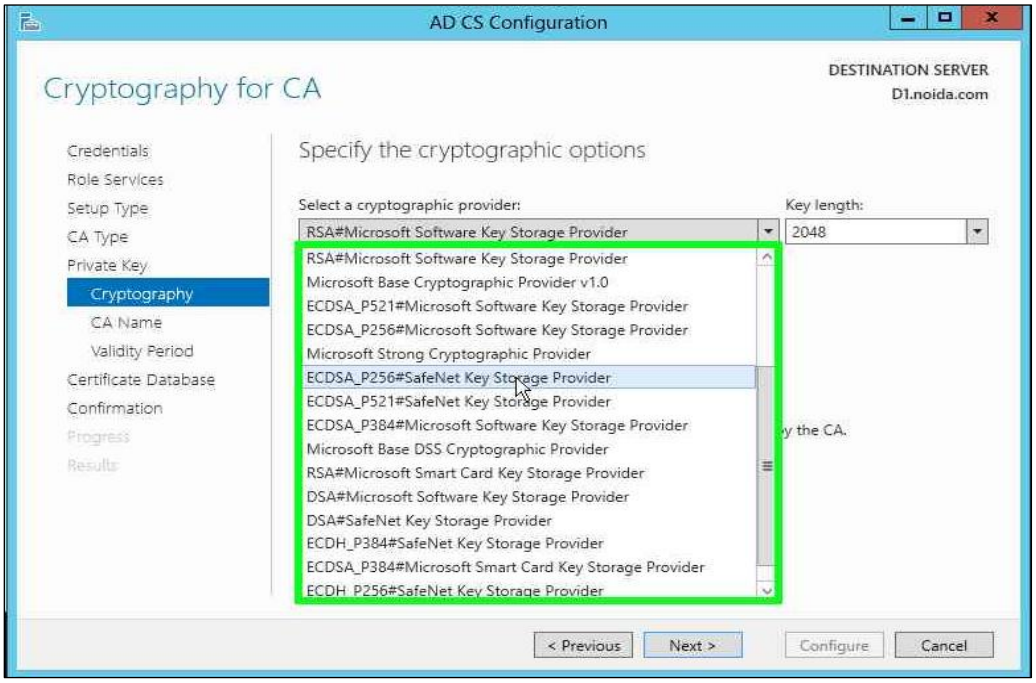
17. Select the **Enterprise CA** radio button and click **Next**.

18. Select the **Root CA radio button** and click **Next**.

19. Setup the Private Key for the CA to generate and issue certificates to clients. If you would like to create a new private key select the **Create a new private key** radio button. Click **Next**. If you would like to use an existing private key, proceed to step 24.



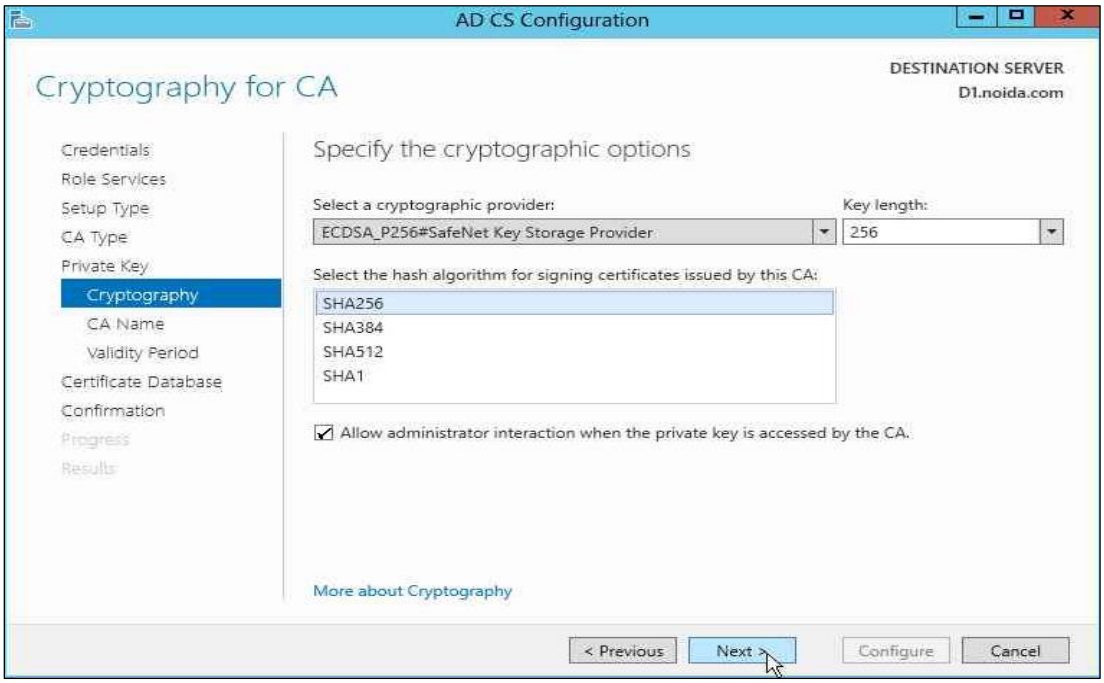
20. Open the **Select a cryptographic provider:** drop-down menu and select an algorithm using a **SafeNet Key Storage Provider**. Open the **Key length:** drop-down menu and select a key-length.



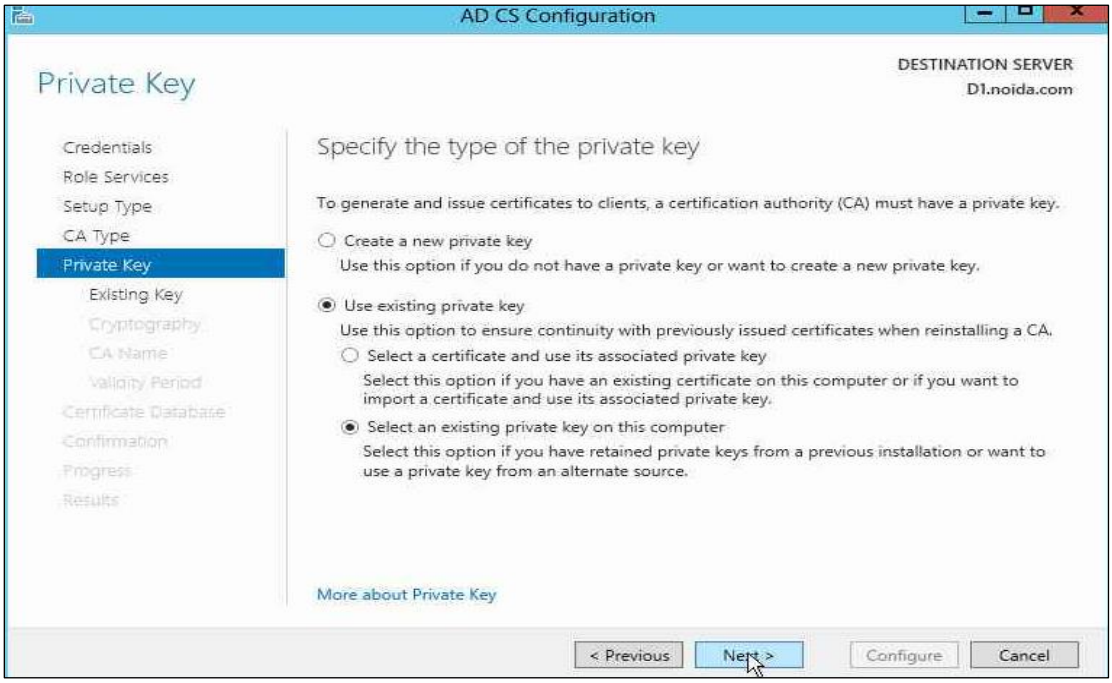
21. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.

22. Select the **Allow administrator interaction when the private key is accessed by the CA** check box.

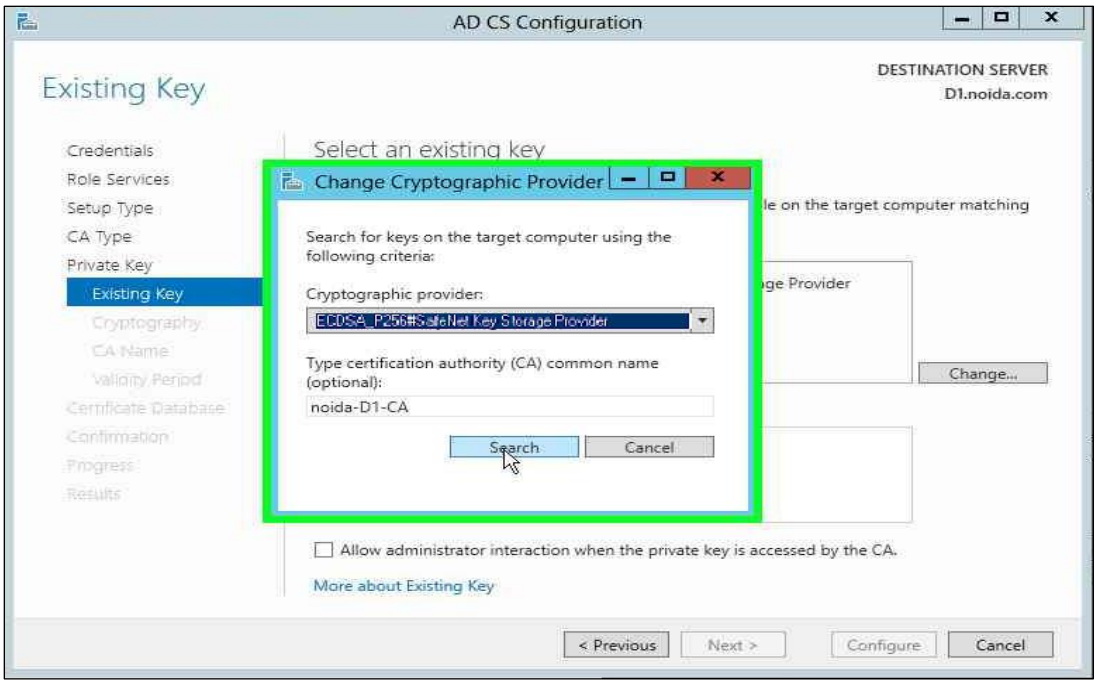
23. Click **Next**. Proceed to step 27.



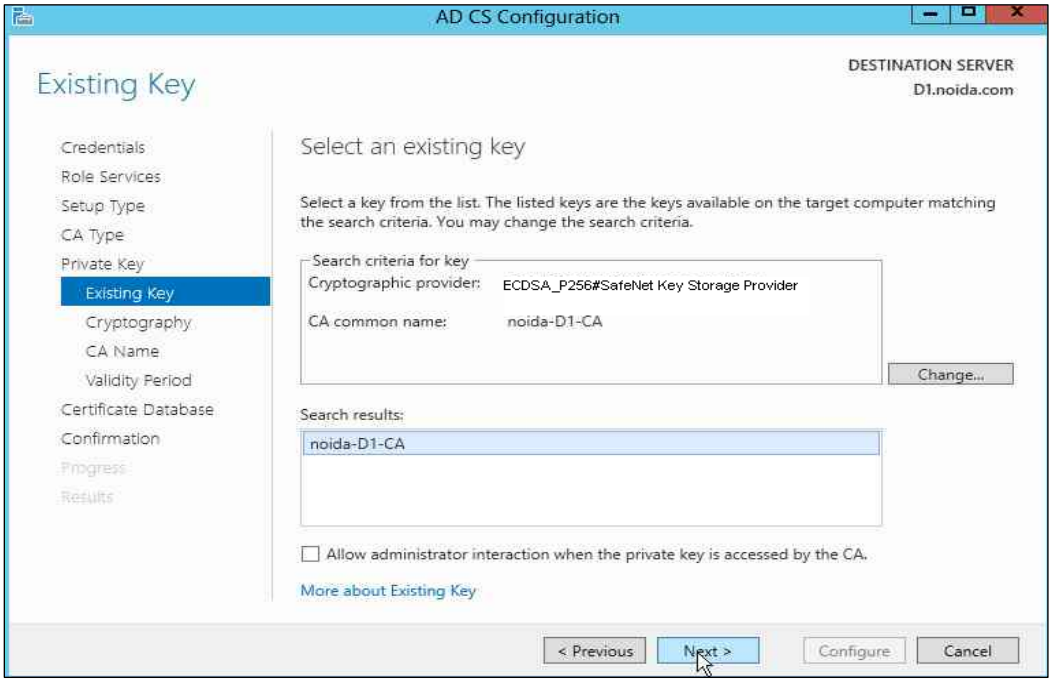
24. Select the **Use existing private key** check box. Setup the **Private Key** for CA to generate and issue certificates to clients. Select **Use existing private key** and **Select an existing private key on this computer.** Click **Next** to continue.



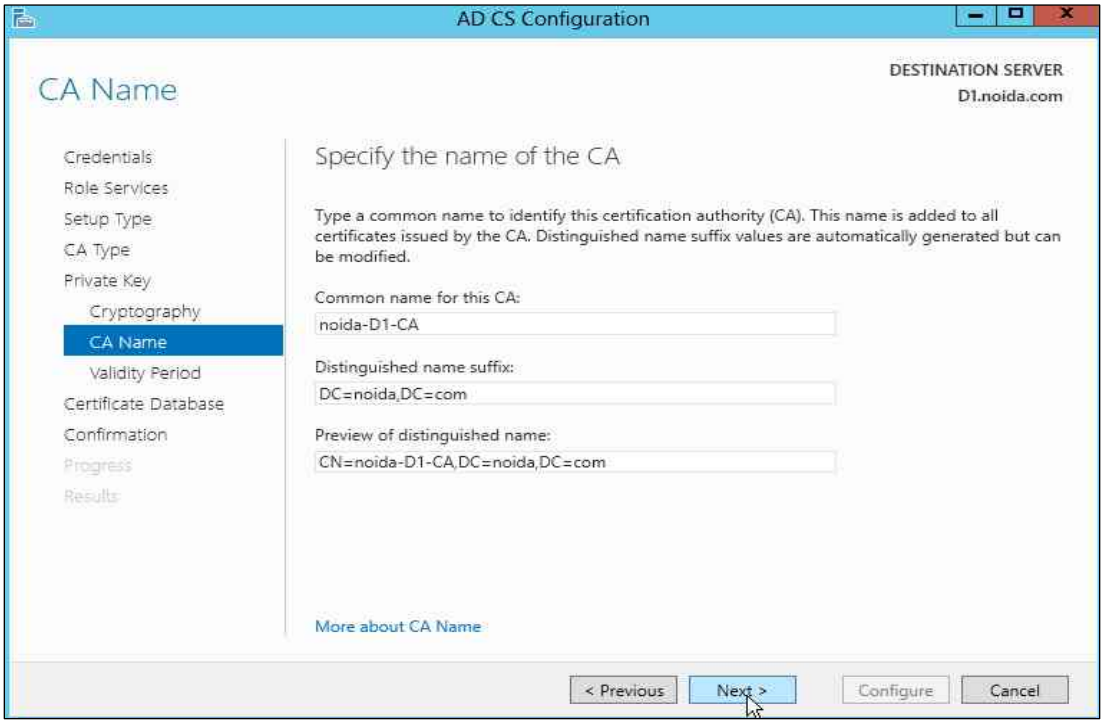
25. Click **Change**. Select the SafeNet Key Storage Provider algorithm that you have used to generate the private keys and clear the CA Common name, click **Search**.



26. Select the **Existing Key** and click **Next.**



27. Configure a common name to identify this Certificate Authority. Click **Next**.



28. Proceed to set the **Certificate Validity Period**. Click **Next**. Configure the **Certificate database location**. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click **Next**.
29. Click **Configure** to configure the selected roles, role services, or features.
30. Click **Close** to exit the **AD CS Configuration** wizard after viewing the installation results.

    A private key for the CA will be generated and stored on the HSM.
31. Open a command prompt and run the following command to verify that service is running:

    ```
    sc query certsvc
    ```
32. Open a command prompt and run the following command to verify the CA key:

    ```
    certutil –verifykeys
    ```

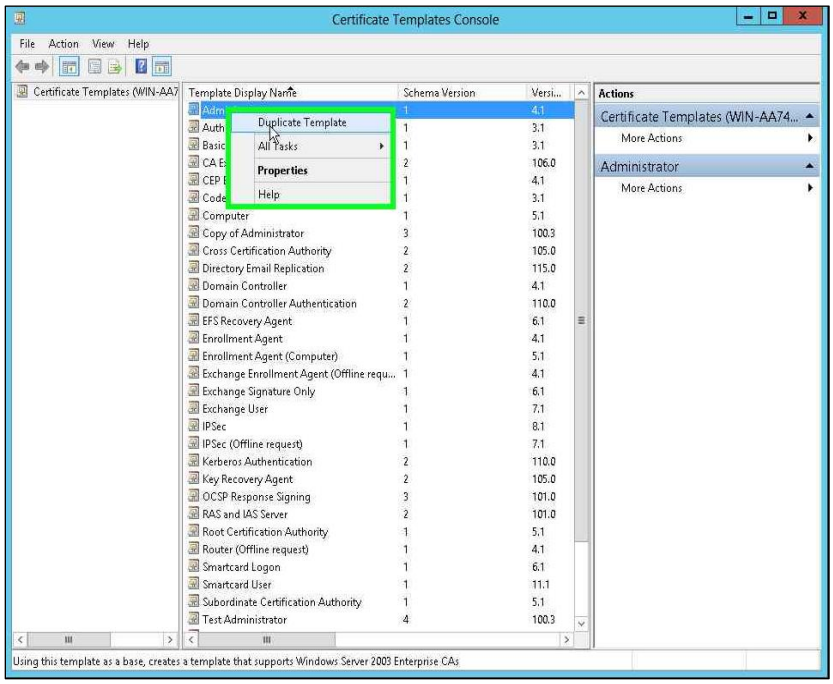
    The result of the command shows the CA keys have successfully been verified.

Enroll Certification Authority Certificate

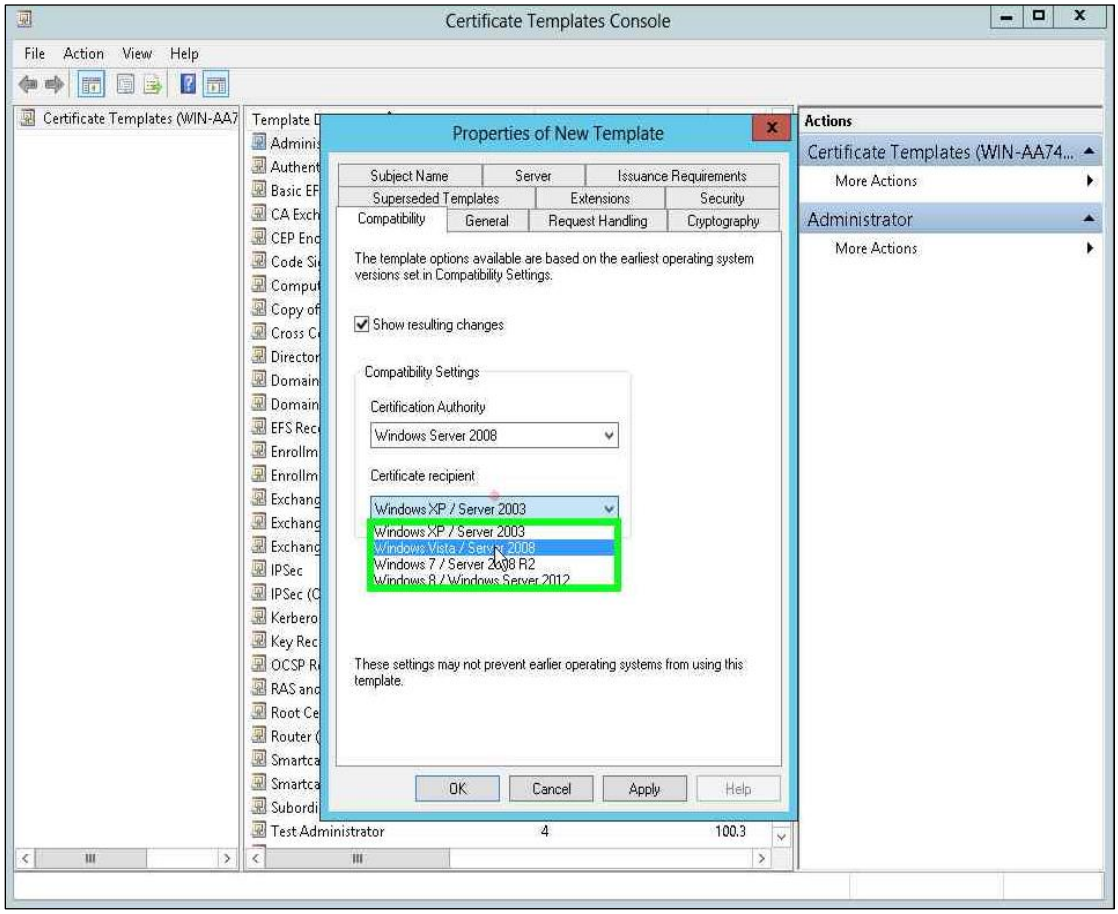
1. Create a CA template that uses SafeNet Key Storage Provider.

   Open a command prompt and run **certtmpl.msc**.

   Right click the **Administrator** template.Click Duplicate Template.

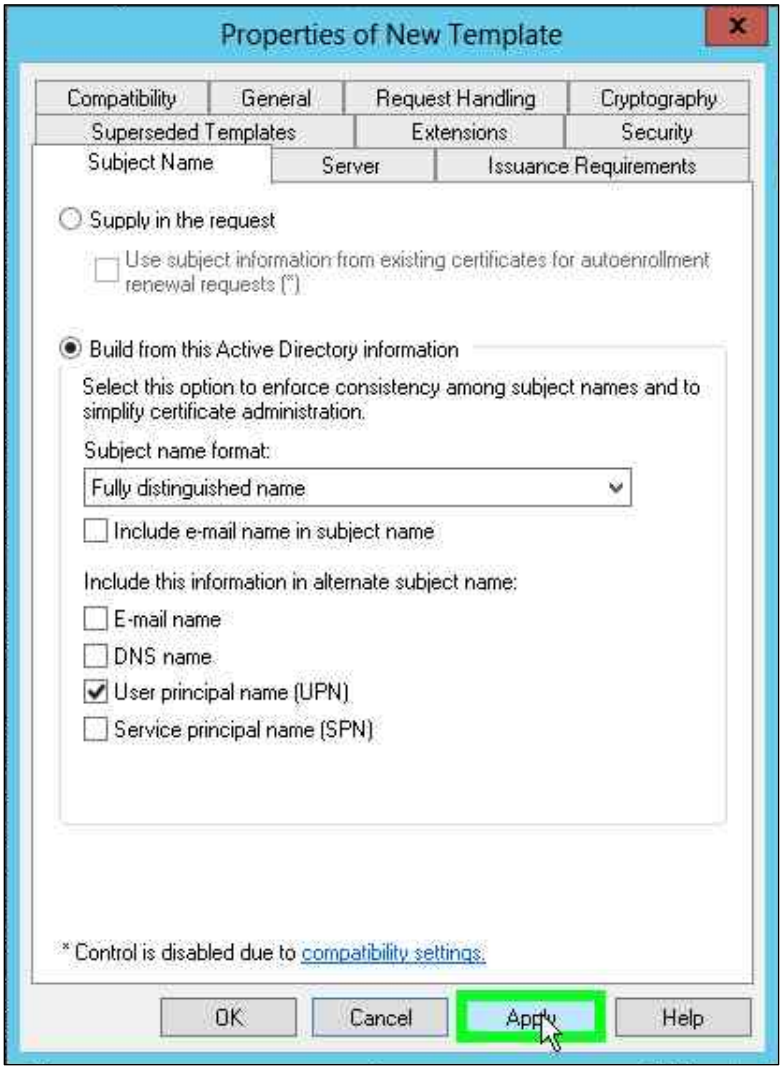


2. Select **Windows Server 2008** for both Certification Authority and Certificate recipient under **Compatibility Settings**, Click **OK**.



3. Verify the changes on the Resulting Changes window. Click **OK**.
   a. Select the General tab. Enter template name.
   b. Go to the Cryptography tab. Select Key Storage Provider for Provider Category.
   c. Select the Requests must use one of the following providers radio button.
   d. In the Providers field select the SafeNet Key Storage Provider only.
   e. For Algorithm Name select an algorithm.
   f. Select Request Hash.
   g. Go to the Subject Name tab.
   h. Uncheck the Include e-mail name in subject name check box

i. Uncheck the E-mail name check box.



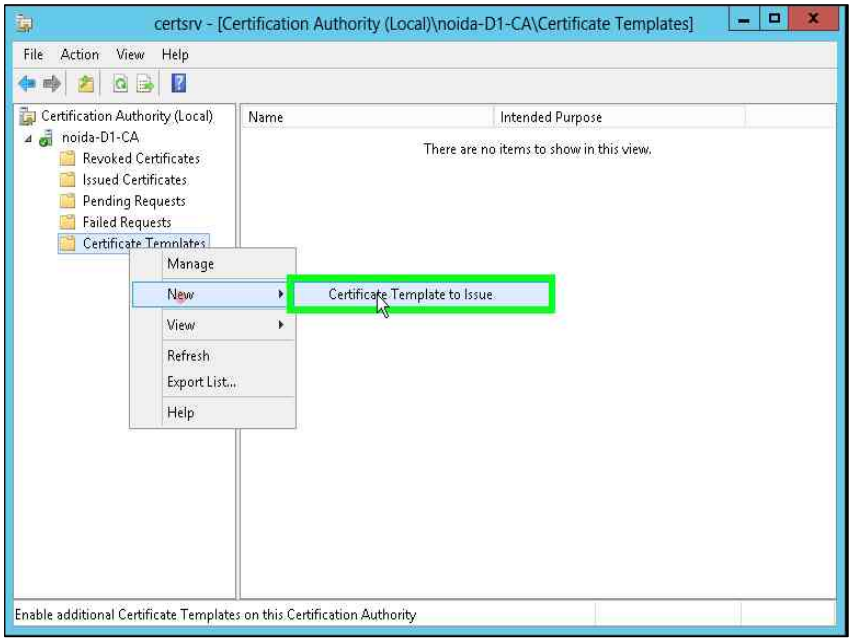
j. Click **Apply** to save the template. Click **OK**.

k. Open the command prompt and run **certsrv.msc**.

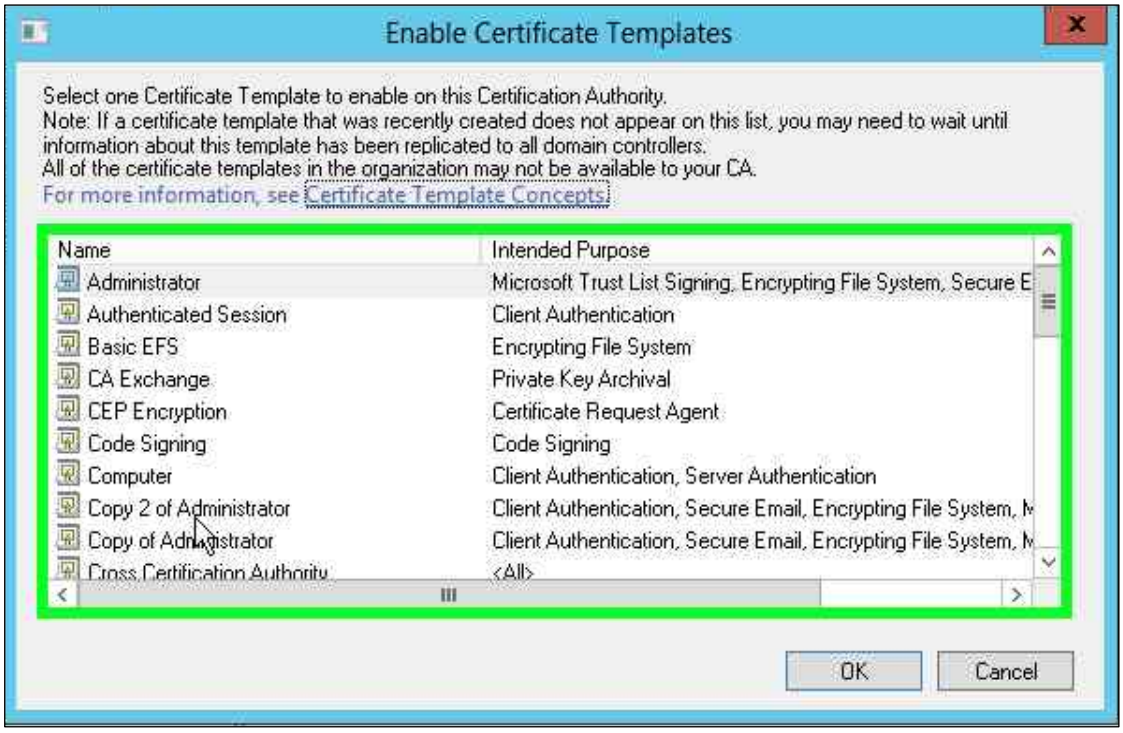
l. Double-click the CA name.

m. Right-click the **Certificate Templates** node.

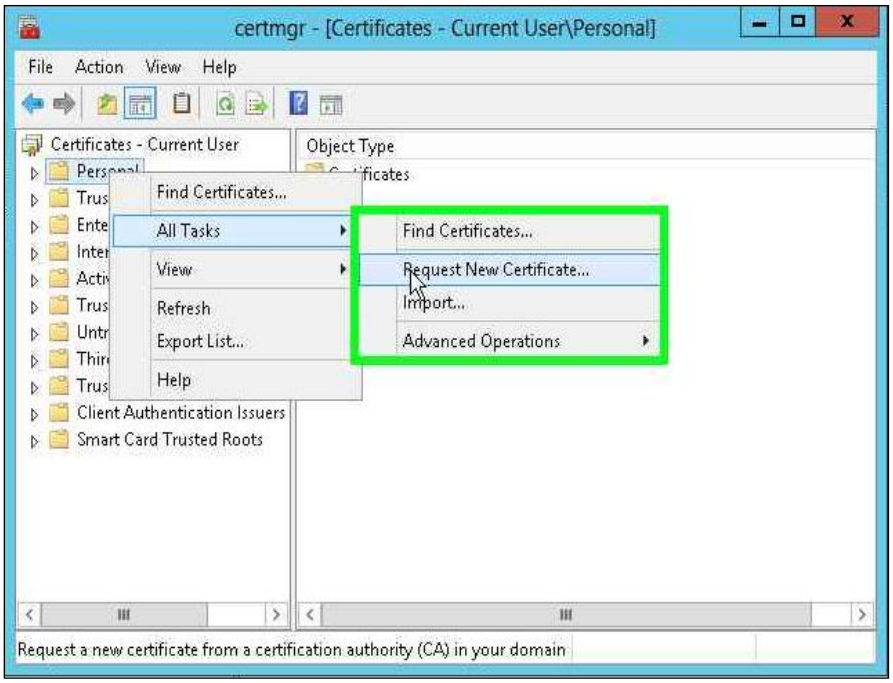
n. Select **New -> Certificate Template to Issue**



o. Select the template you recently created and click **OK.**



4. Request a certificate based on the template.
   a. Request a certificate based on the template.
   b. Open the command prompt and run the **certmgr.msc** command.
   c. Right-click the **Personal** node.
   d. Select **All Tasks -> Request New Certificate…**



   e. Click **Next**.
   f. Click **Next**.
   g. Enable the check box for the template you created above.
   h. Click **Enroll**.
   i. Verify the certificate is enrolled successfully. The UI enrollment wizard shows if the certificate enrollment was successful.

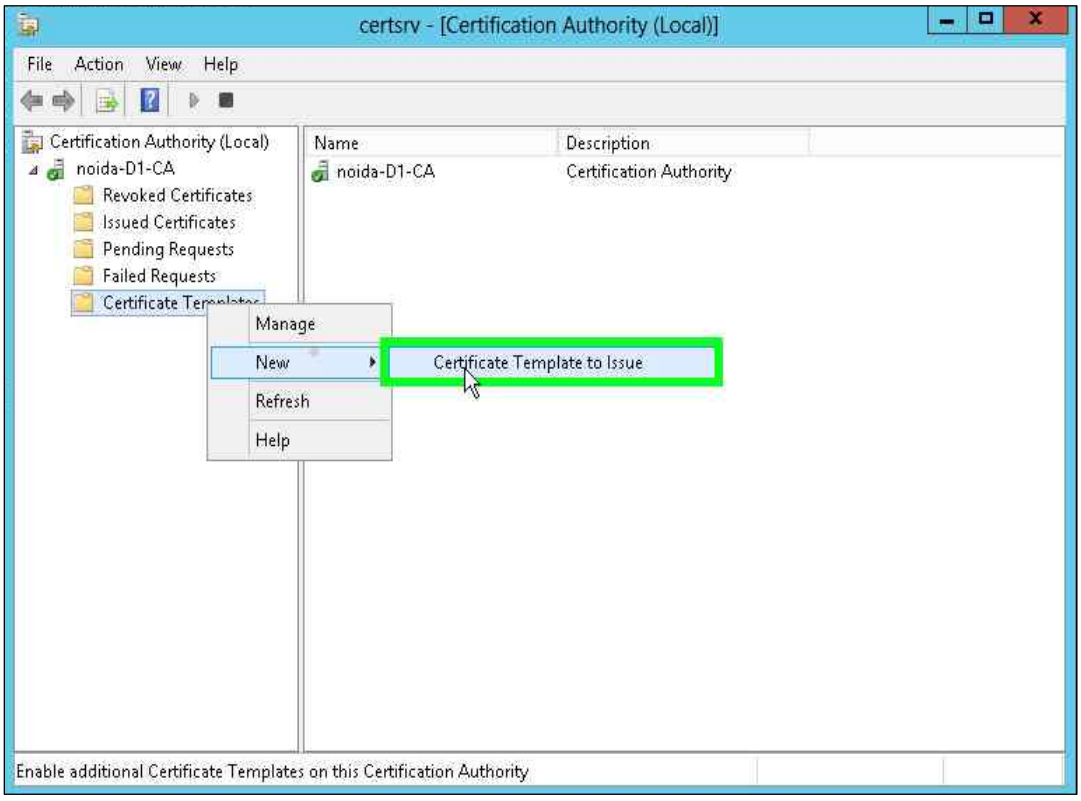
Archive CA Key

You can verify that the configurations that are possible with the Luna HSM or Luna Cloud HSM service can be used and do not interfere with the CA key archival functionality. To complete archiving the CA-Key you must complete the following tasks:

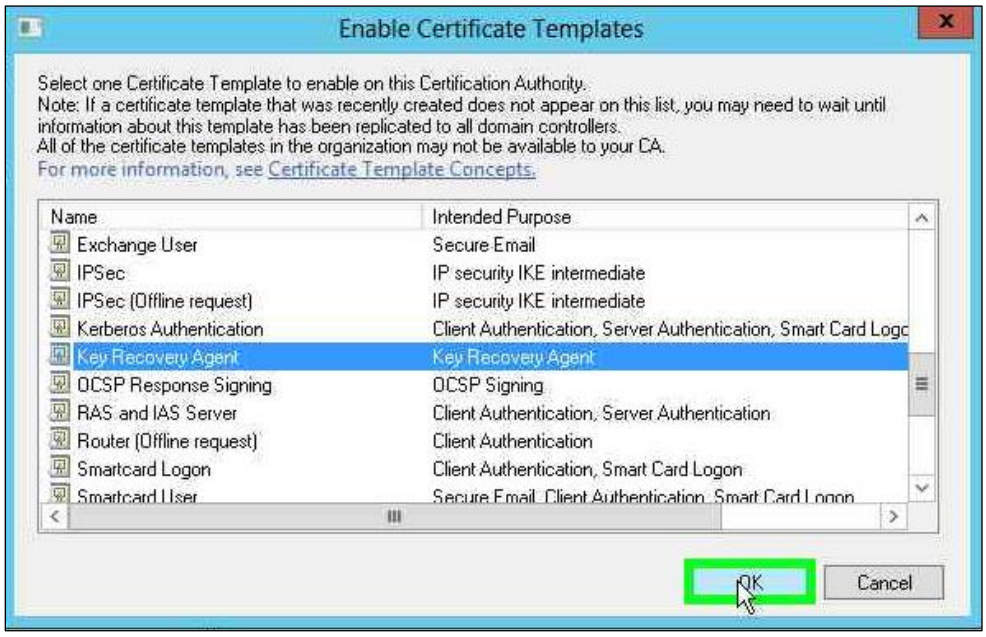
> **NOTE**: If you wish to secure the key on Luna HSM that is used to encrypt the Archived Keys then you need to select the SafeNet Key Storage Provider for generating the keys for Key Recovery Agent certificate.

Archive the CA key

1. Install the Enterprise Certificate Server using the SafeNet Key Storage Provider and ECC key.
2. Verify the CA is installed correctly.
3. Add a Key Recovery Agent (KRA) template to CA for issuing.
4. Open the command prompt and run the **certsrv.msc** command.
5. Right-click the **Certificate Templates** node. Select **New -> Certificate Template to Issue**.

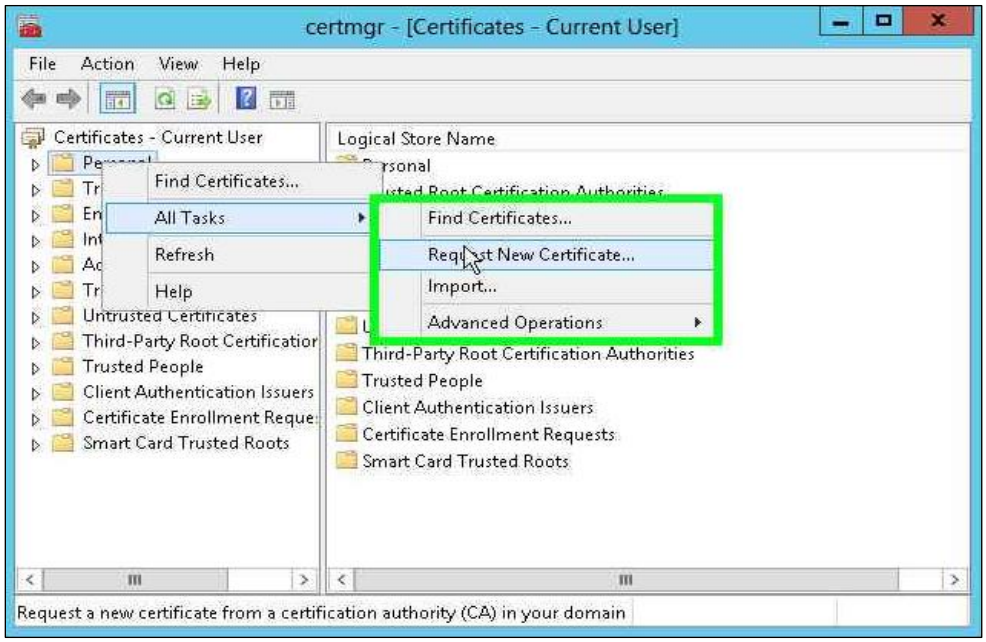


6. Select the **Key Recovery Agent** template and click **OK**.



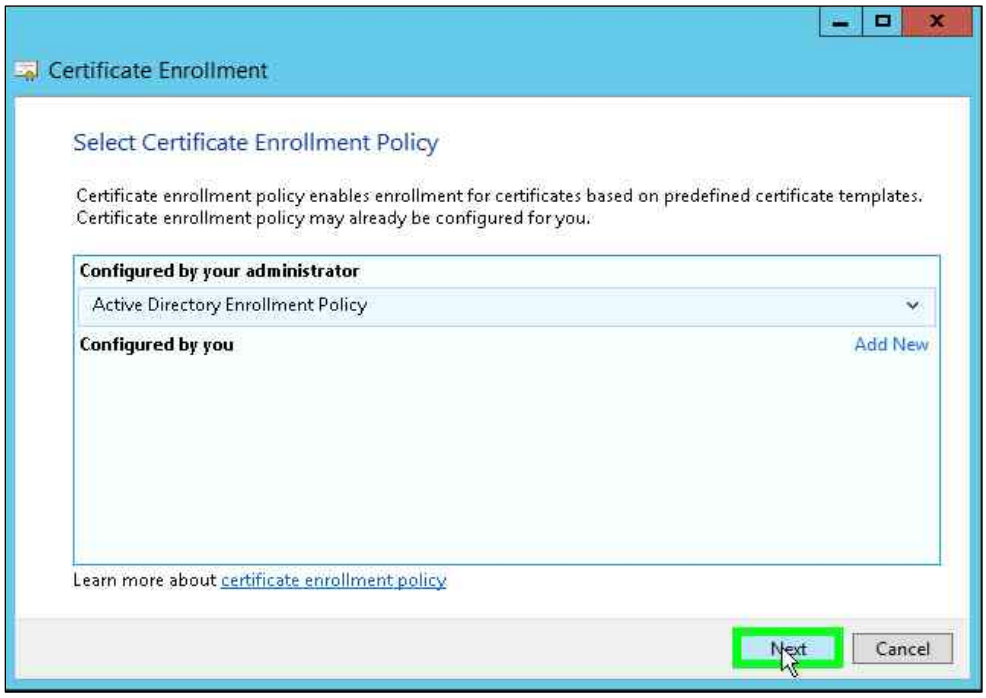
Issue the KRA Certificate.

1. Request the KRA certificate. Open the command prompt and run the **certmgr.msc** command.
2. Right-click **Personal** node. Select **All Tasks -> Request new certificate….**

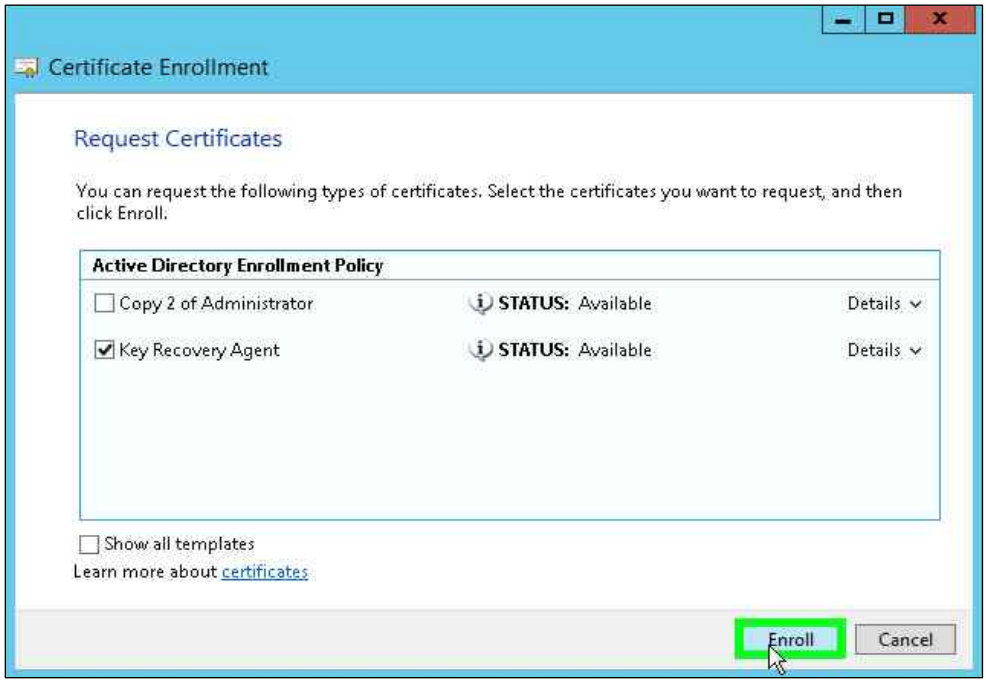


3. Click **Next**.

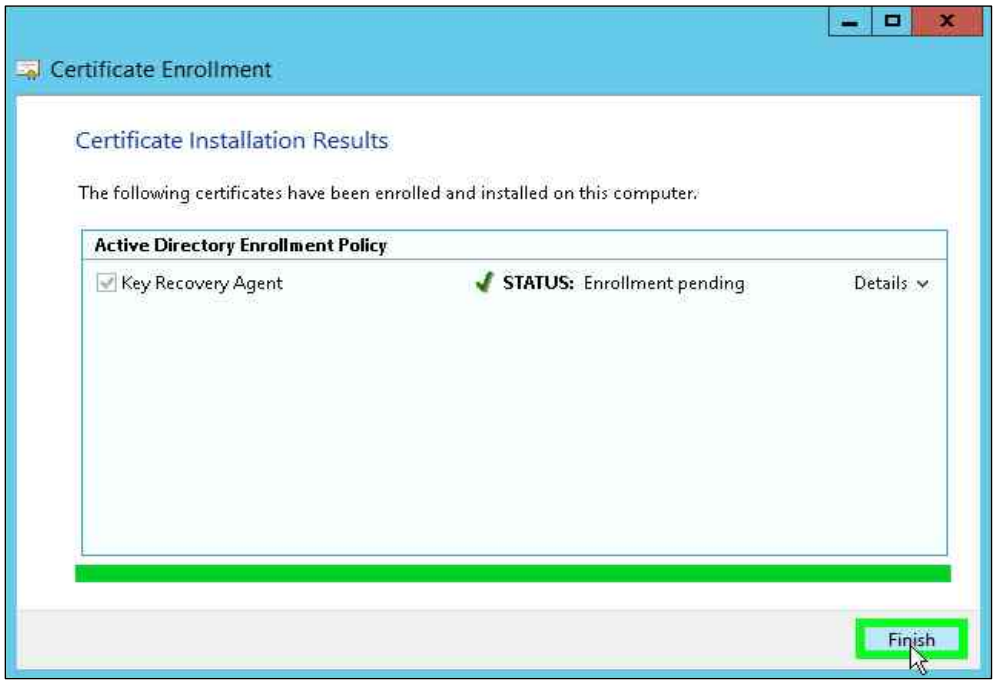
4. Select **Active Directory Enrollment Policy** and click **Next**.



5. Select the **Key Recovery Agent** check box template and click **Enroll**.

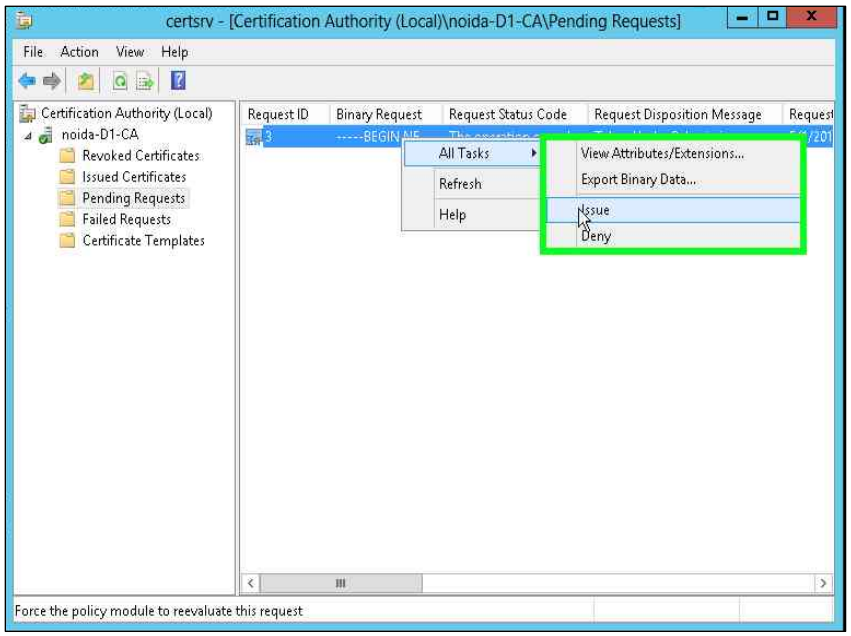


6. Verify the enrollment is pending and click **Finish**.



Issue the KRA certificate from the CA snap-in.

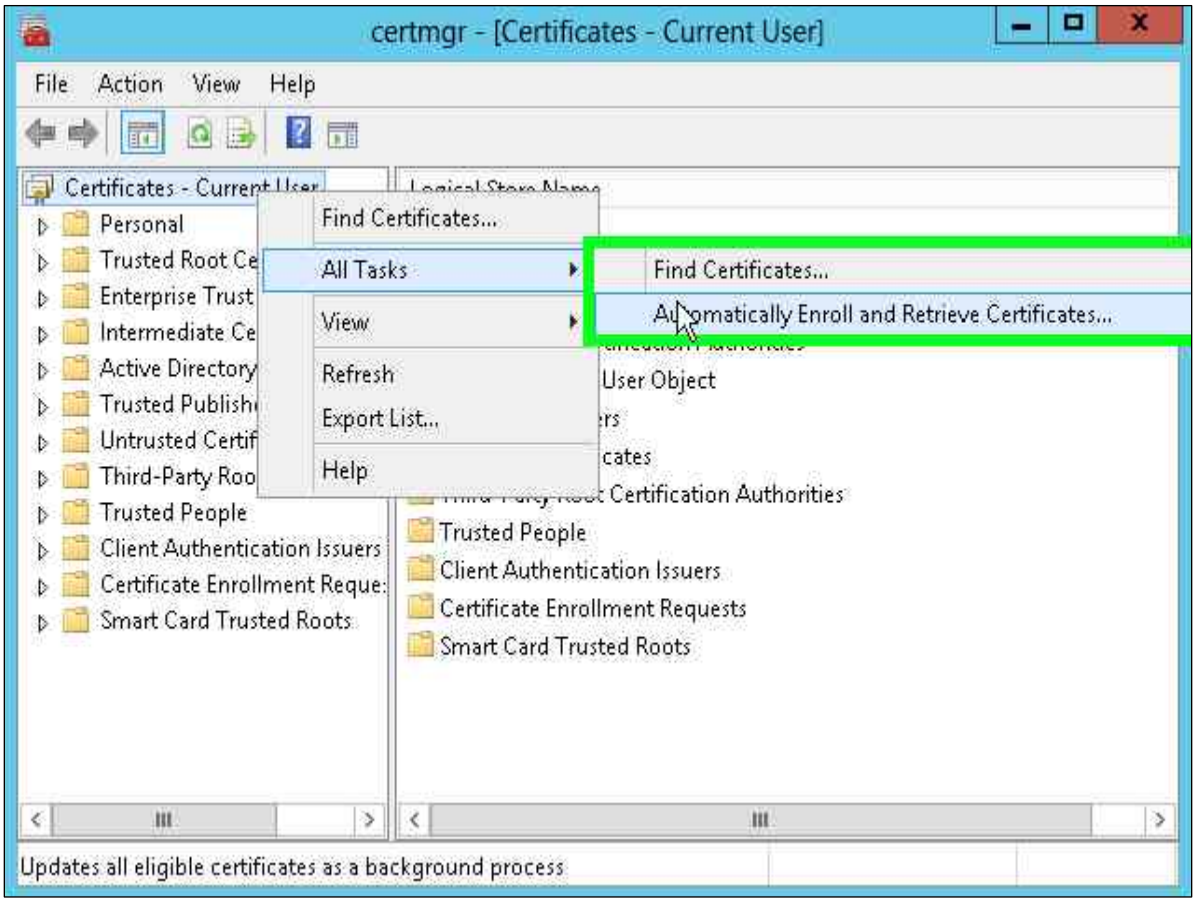
1. Open the command prompt and run the **certsrv.msc** command.
2. Select the **Pending Requests** node. Right-click on the latest request for the KRA template. Select **All Tasks** and click **Issue**.



3. Click on **Issued Certificates**. Verify that the new certificate is issued.

Retrieve the issued certificate from CA

1. Open the command prompt and run **certmgr.msc** command.
2. Right click **Certificates – Current User**
3. Select **All Tasks** and click **Automatically enroll and retrieve certificates…**

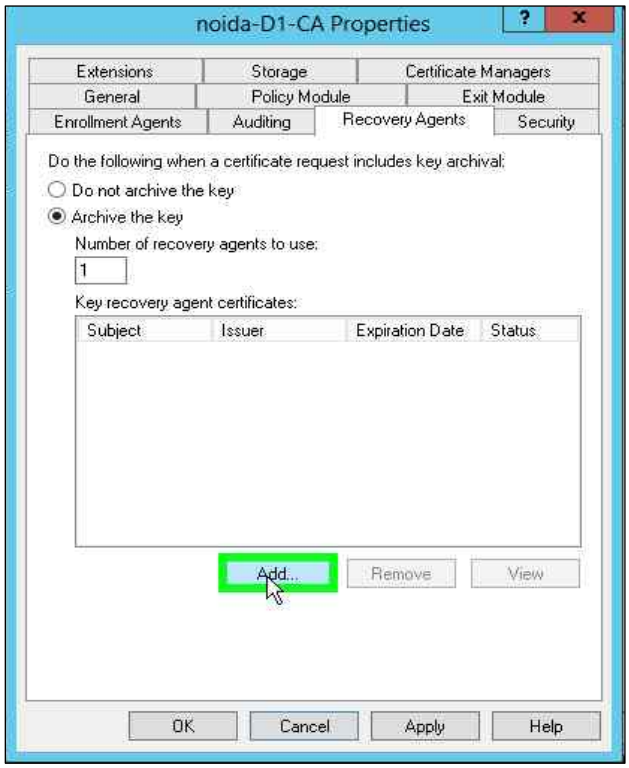


4. Click **Next**.
5. Select the KRA certificate you just issued and enroll it.

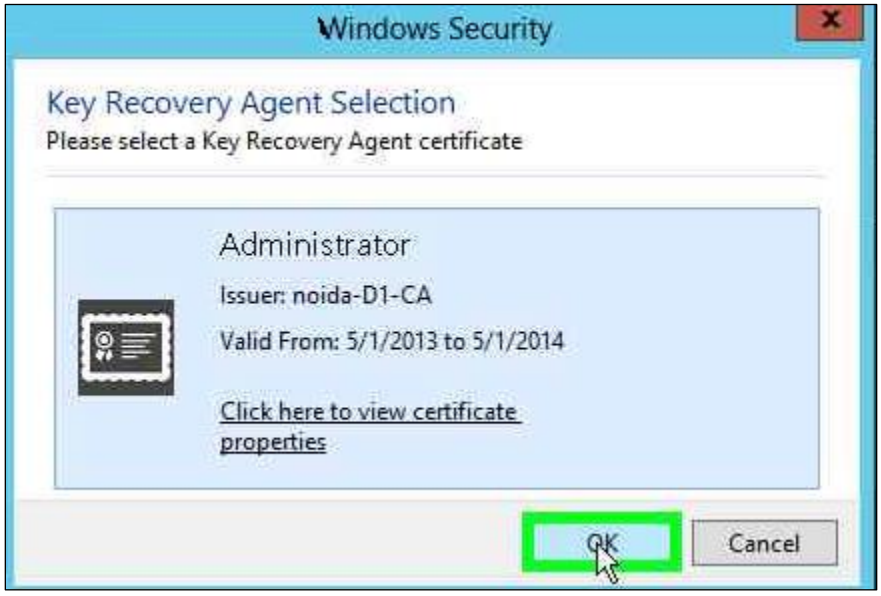
Configure the CA to support Key Archival.

1. Open the command prompt and run the **certsrv.msc** command.
2. Right-click CA Name and select **Properties**.
3. Select the **Recovery Agent** tab.
4. Select the **Archive the key** radio button.

5. Click the **Add** button.



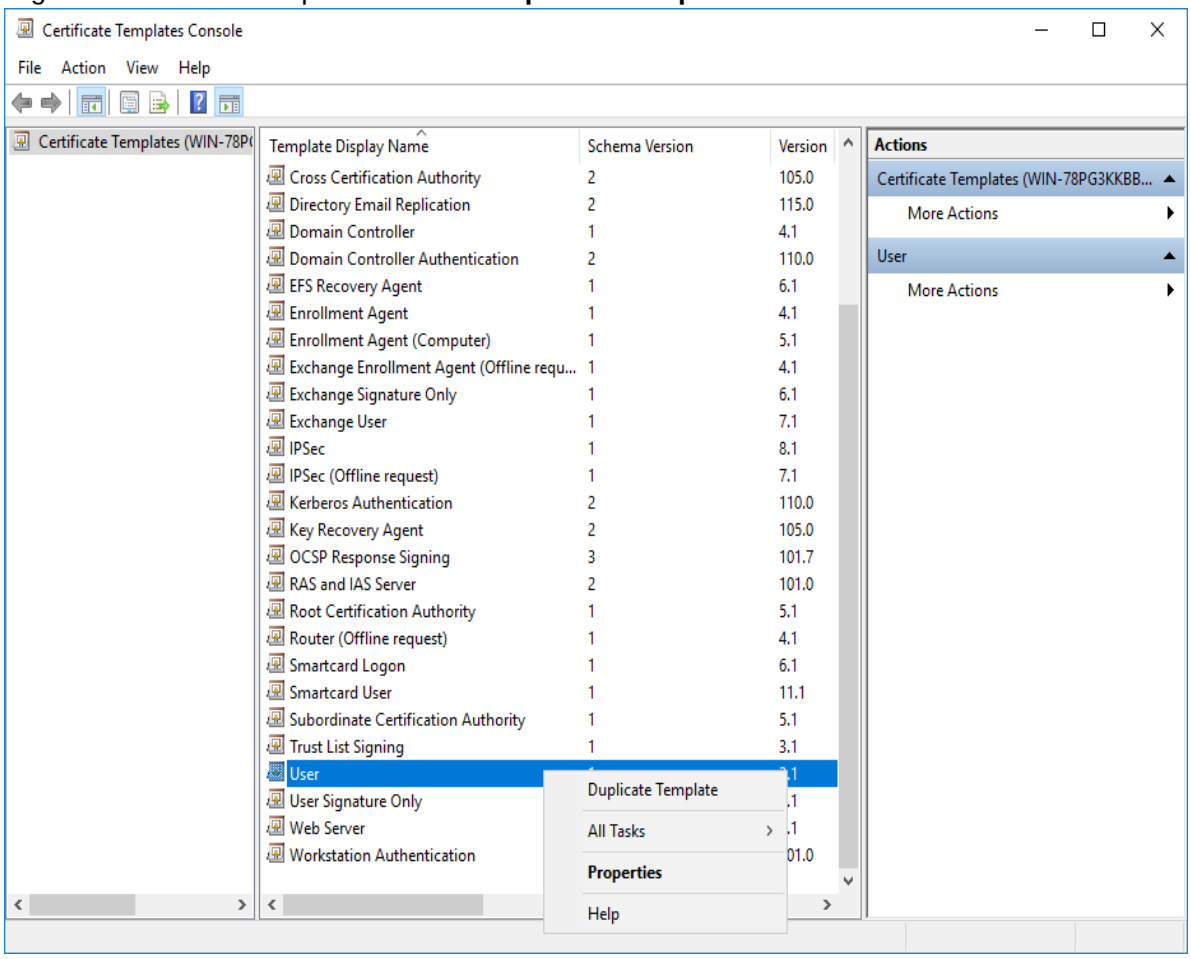
6. Select the KRA certificate you just issued, Click **OK**.



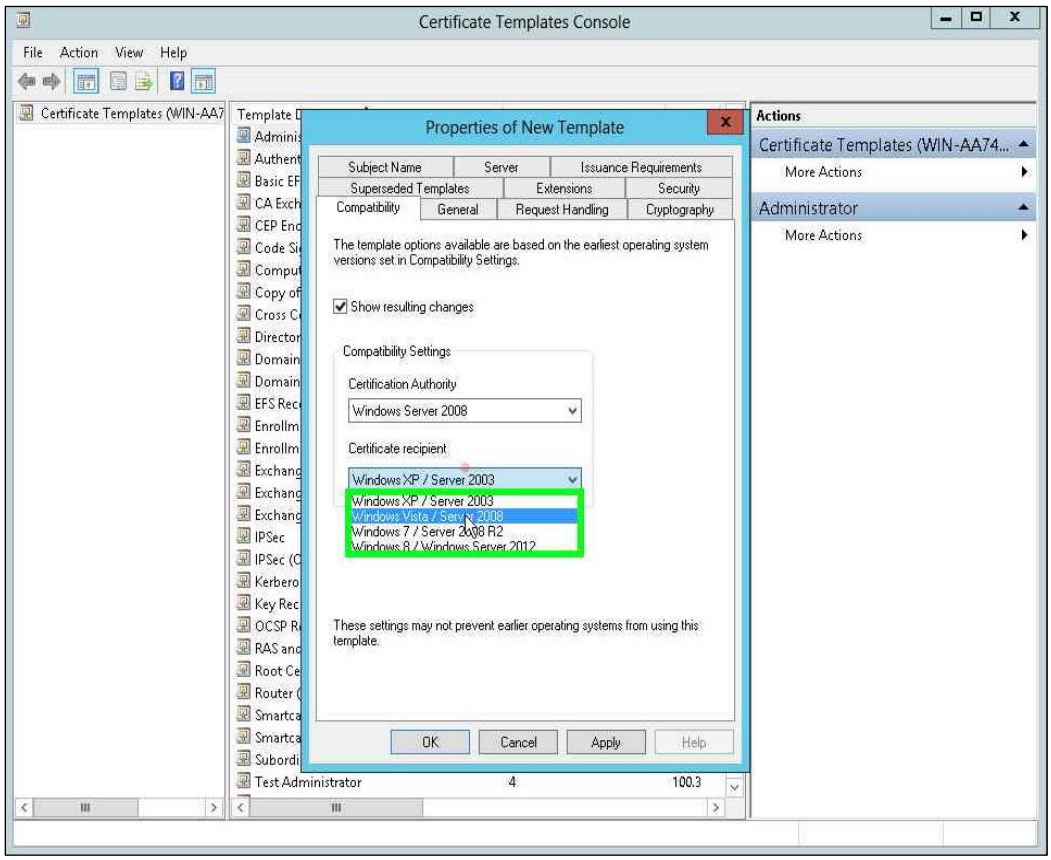
7. Click **OK**
8. Verify the CA service must be restarted, click **Yes**.

Create a template with Key Archival enabled

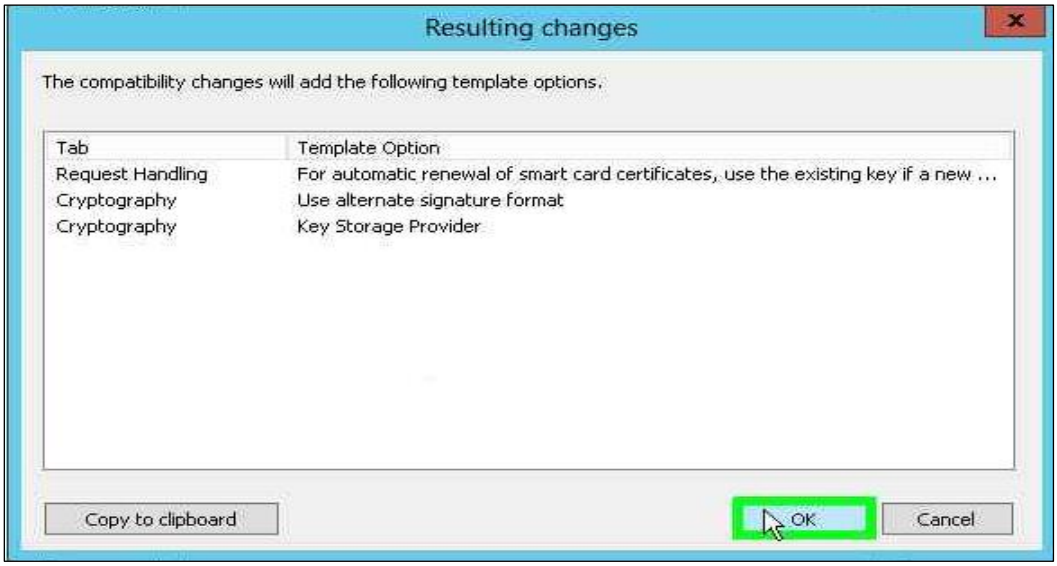
1. Open the command prompt and run the **certtmpl.msc** command.
2. Right-click the User template and click **Duplicate Template**.



3. Select **Windows Server 2008** for both Certification Authority and Certificate recipient under **Compatibility Settings**, Click **OK**.

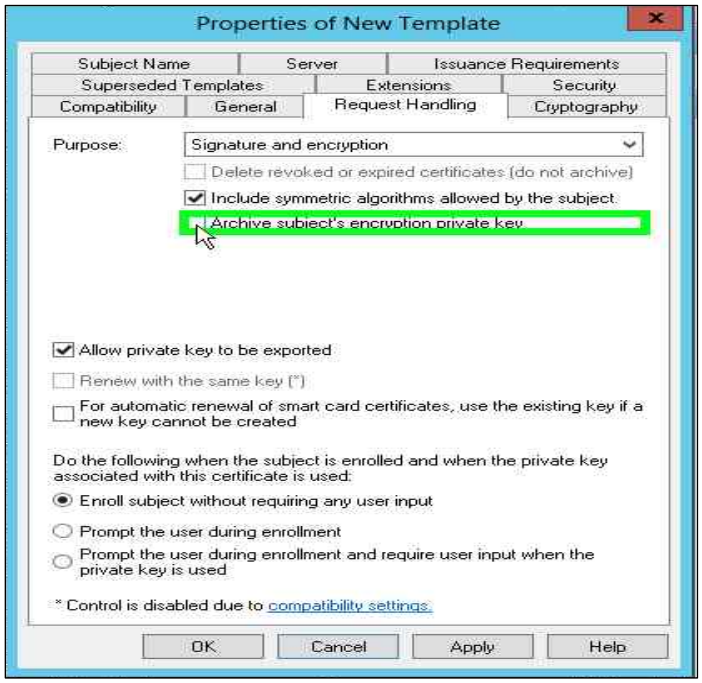


4. On the **Resulting Changes** menu click OK.

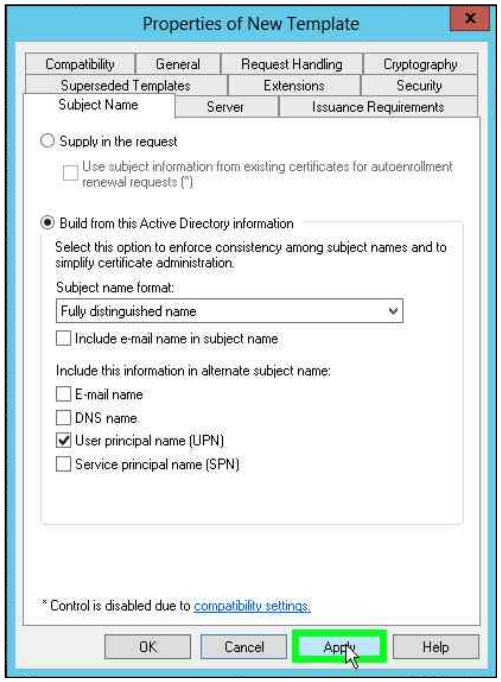


5. Go to the **General** tab and enter a name for the template (UserKeyArchival).

6. Go to the **Request Handling** tab and enable the **Archive subject's encryption private key** check box.



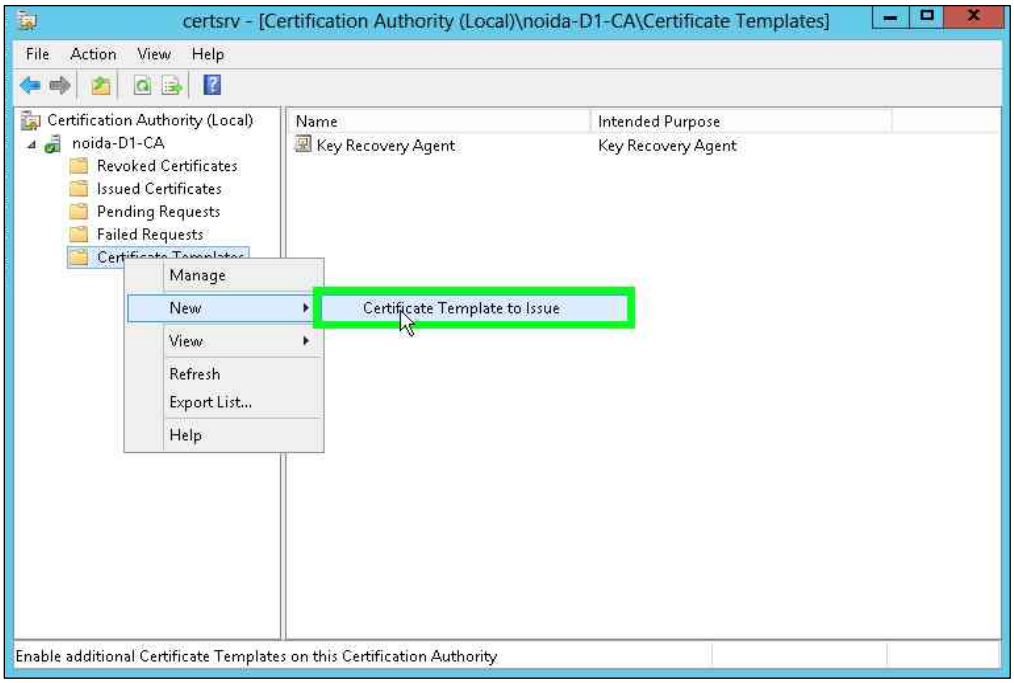
7. Select the **Subject Name** tab.
8. Uncheck the **Include e-mail name in subject name** check box.
9. Uncheck the **E-mail name** check box.



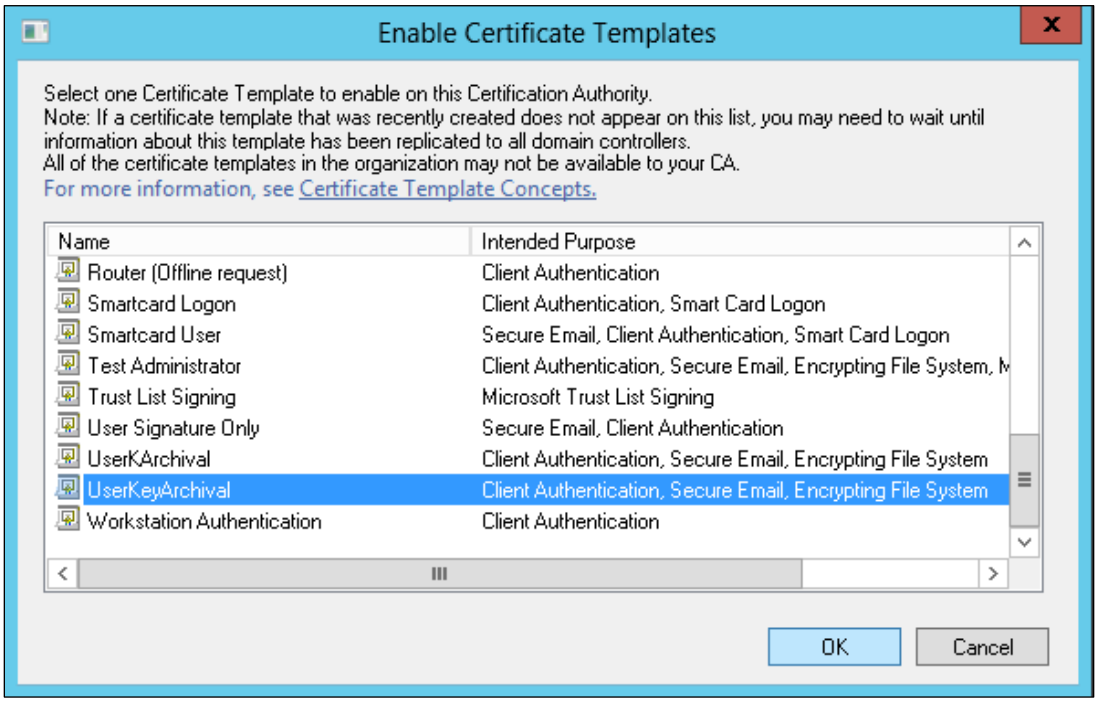
10. Click **Apply** and then **OK**.

Add a new template to CA for issuing

1. Open the command prompt and run the **certsrv.msc** command.
2. Right-click the **Certificate Templates** node.
3. Select **New -> Certificate Template to Issue**.

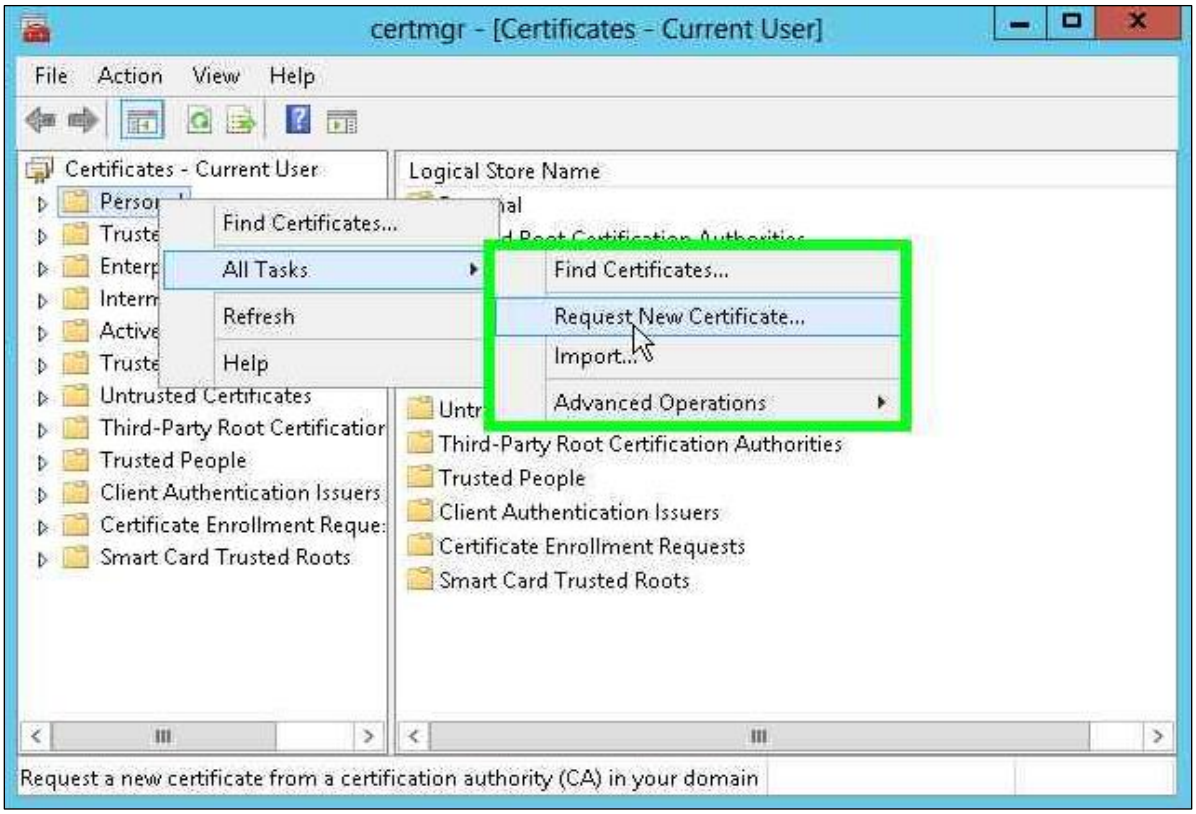


4. Select new template for key archival, click **OK**.



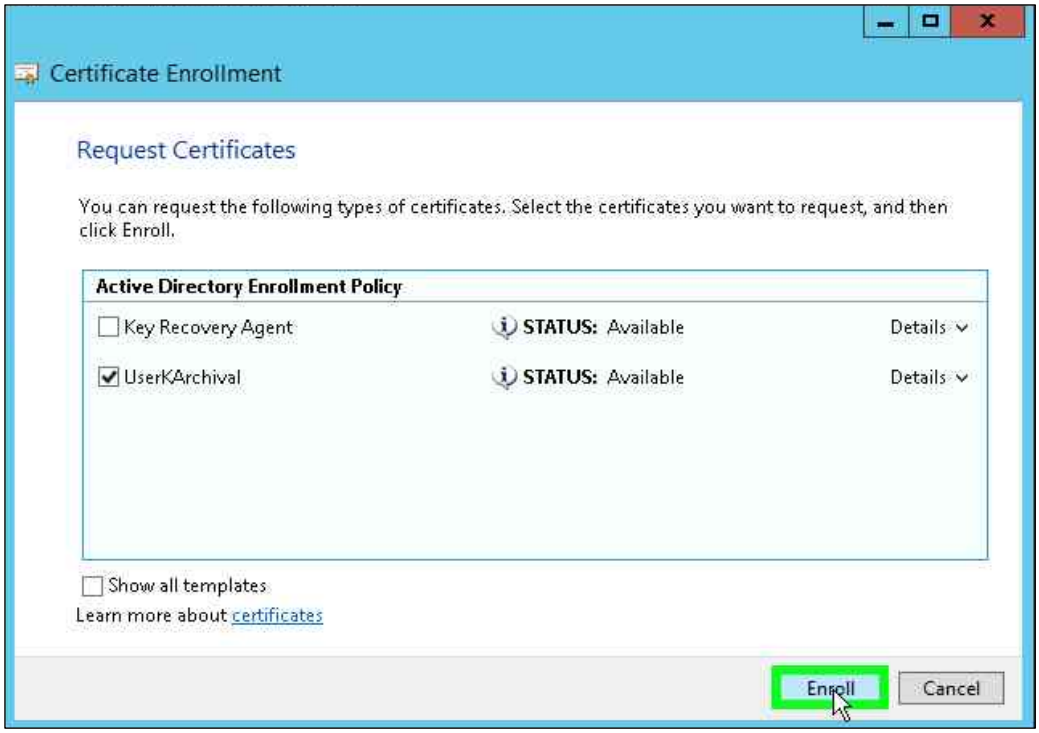
Issue a user template with key archival enabled

1. Open the command prompt and run the **certmgr.msc** command.
2. Right-click **Personal** node.
3. Select **All Tasks -> Request New Certificate**.

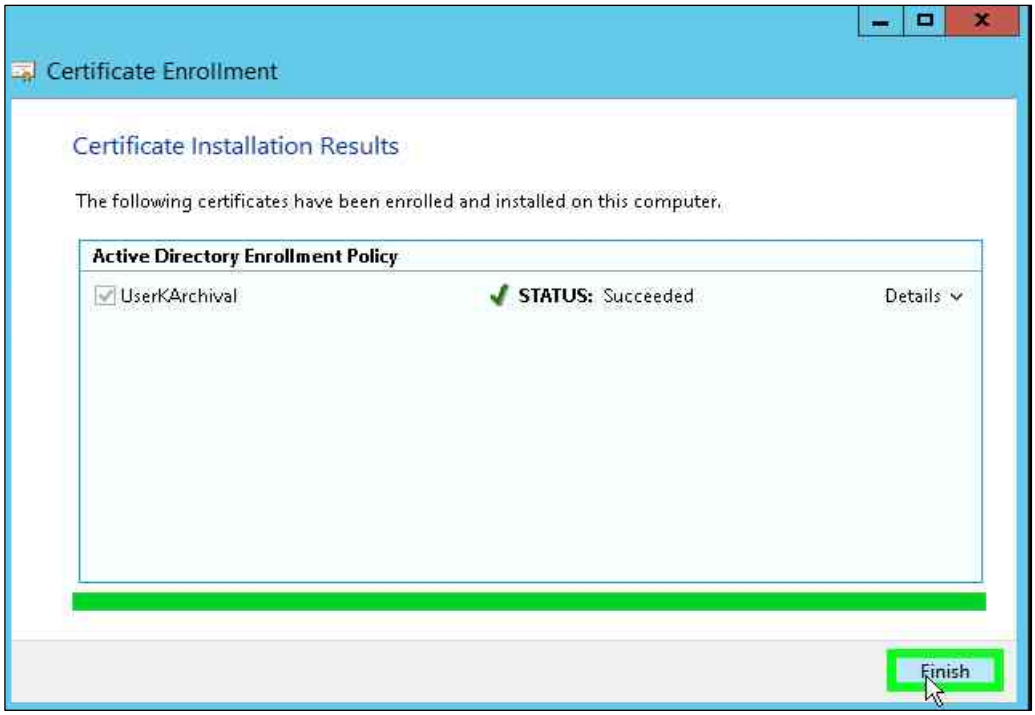


4. Click **Next**
5. Click **Next**.

6. Select the new template for key archival check box and click **Enroll**.



7. The Enrollment Wizard UI displays. Verify the enrollment is successful.



8. Click **Finish**.

Perform Key Recovery

You can recover archived keys. To perform a key recovery:

1. Log on to the system as Domain Administrator and ensure that the private key is still recoverable by viewing the Archived Key column in the Certification Authority console.
   a. Log on as Domain Administrator.
   b. From **Administrative Tools**, open **Certification Authority**.
   c. In the console tree, double-click **CA**, and then click **Issued Certificates**.
   d. From the **View** menu, click **Add/Remove Columns**.
   e. In **Add/Remove Columns**, in **Available** Column, select **Archived Key**, and then click **Add**. Archived Key should now appear in Displayed Columns.
   f. Click **OK** and then, in the details pane, scroll to the right and confirm that the last issued certificate to **UserKeyArchival** has a **Yes** value in the **Archived Key** column.

      NOTE: A certificate template must have been modified so that the Archive bit and Mark Private Key as Exportable attributes were enabled. The private key is only recoverable if there is data in the Archived Key column.

   g. Double-click the **Archive User** certificate.
   h. Click the **Details** tab.

      Write down the serial number of the certificate. (Do not include spacing between digit pairs.) This is required for recovery.

      The serial number is a hexadecimal string which is 20 characters long. The serial number of the private key is the same as the serial number of the certificate. For the purpose of this walkthrough, the serial number will be referred to as **serialnumber**.

   i. Click **OK**.
   j. Close Certification Authority.
2. Recover the private key into a BLOB output file by using **certutil.exe**.
   a. On the taskbar, click the **Start** button, click **Run**, type **cmd**, then click **OK** to open command prompt window.
   b. Type **cd ** and then press **ENTER**.
   c. Ensure that you are in the **c:** directory.
   d. At the command prompt, type:

      ```
      Certutil -getkey  serialnumber outputblob
      ```

   e. At the command prompt, type

      ```
      dir outputblob
      ```

      NOTE: If the file outputblob does not exist, you probably typed the serial number incorrectly for the certificate.

   The outputblob file is a PKCS#7 file containing the KRA certificates and the user certificate and chain. The inner content is an encrypted PKCS#7 containing the private key (encrypted by the KRA certificates).

3. Recover the original private/public key pair using Certutil.exe
   a. On the taskbar, click the **Start** button, click **Run**, type **cmd**, and click **OK** to open a command prompt window.
   b. At the command prompt, type:

      ```
      Certutil -recoverkey outputblob user.pfx
      ```

   c. When prompted, enter the following information:

      Enter new password: password

      Confirm new password: password

   d. Type exit, and then press **ENTER**.
   e. Close all windows and log off as the current user.
4. Import the recovered private key/certificate.
   a. At the command prompt, type **certmgr.msc**
   b. Right click **Certificates (Current User)**, and then click **Find Certificates**.
   c. In **Find Certificates**, under **Contains**, type CA Name and then click **Find Now**.
   d. In **Find Certificates**, on the **Edit** menu, click **Select All**.
   e. In **Find Certificates**, on the **File menu**, click **Delete**.
   f. In **Certificates**, click **Yes**.
   g. Close **Find Certificates**.
5. Import the certificate at `c:\user.pfx` and let the certificates be placed by the system.
   a. In the console tree, right-click **Personal** and then click **All Tasks** and then click **Import**.
   b. In the **Certificate Import Wizard**, click **Next**.
   c. On **Files to Import**, in the **File name** box, type `c:\user.pfx`, and then click **Next**.
   d. In **Password**, type password and then click **Next**.
   e. On **Certificate Store**, click **Automatically select the certificate store based on the type of certificate** and then click **Next**.
   f. On **Completing the Certificate Import Wizard**, click **Finish**.
6. Verify the serial number of the imported certificate.
   a. In the console tree, double-click **Personal** and then click **Certificates**.
   b. Double-click certificate.
   c. In **Certificate**, go to the **Details** tab. Verify that the serial number matches the original.

   This completes the key recovery process when your key recovery keys are in Luna HSMs.

Microsoft Certificate Services Integration using Luna HSM for signing keys has been completed now as we have secured the CA signing keys and CA recovery keys on Luna HSMs.

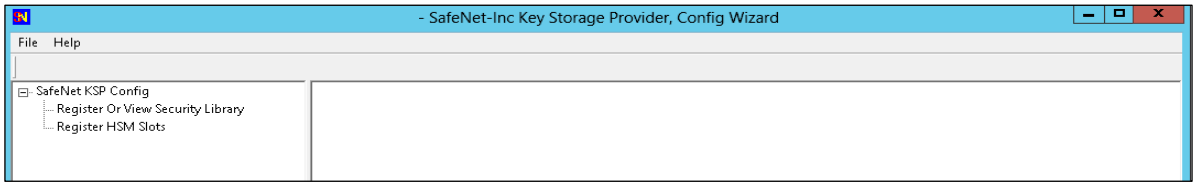
Migrating CA keys from Microsoft Software Key Storage Provider to SafeNet Key Storage Provider

This chapter outlines the steps to migrate a CA signing key from Microsoft software storage to the Luna HSM or Luna Cloud HSM service on Windows Server using the Ms2luna utility for both CSP and KSP.

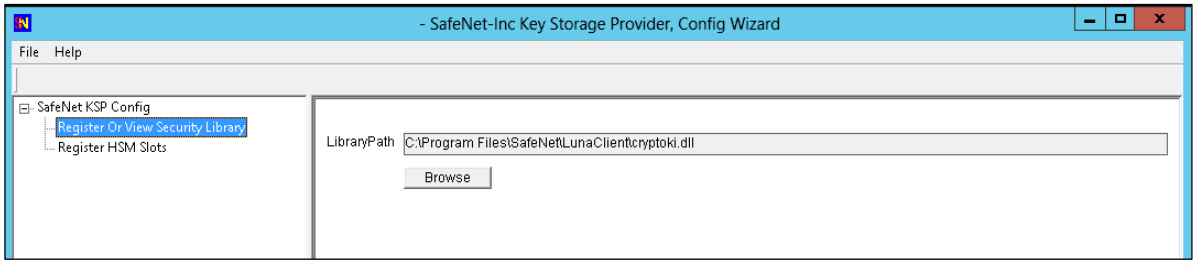
Configure SafeNet KSP

You must configure the SafeNet Key Storage Provider (KSP) to allow the user account and system to access the Luna HSM or Luna Cloud HSM Service. If using a Luna HSM, the KSP package must be installed during the Luna Client software installation. If using Luna Cloud HSM service, the KSP package is included in the service client package inside of the **/KSP** folder.

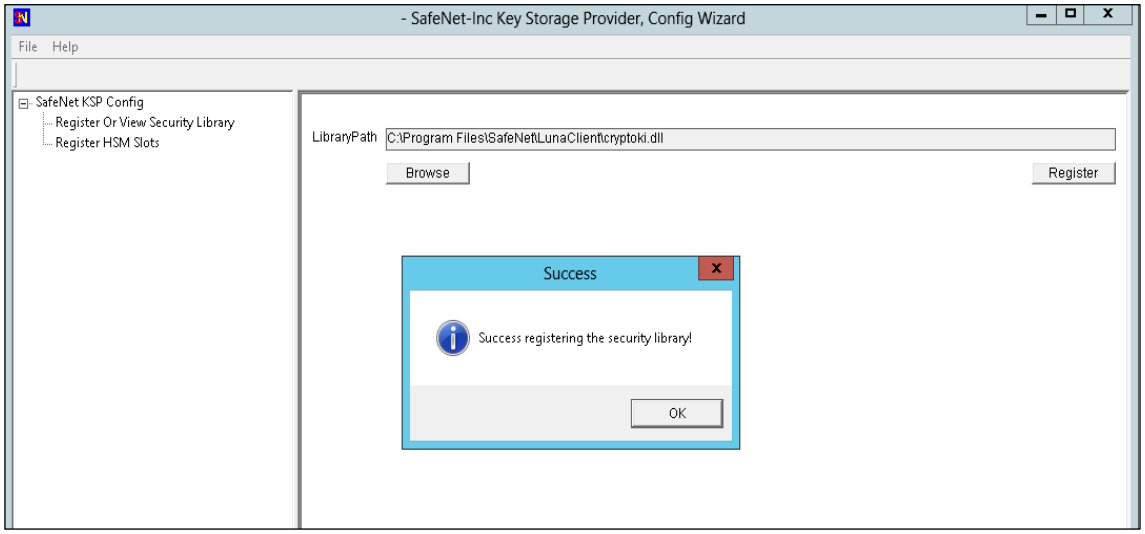
1. Navigate to the KSP installation directory.
2. Run the KspConfig.exe (KSP configuration wizard).
3. Double-click Register Or View Security Library on the left side of the pane.



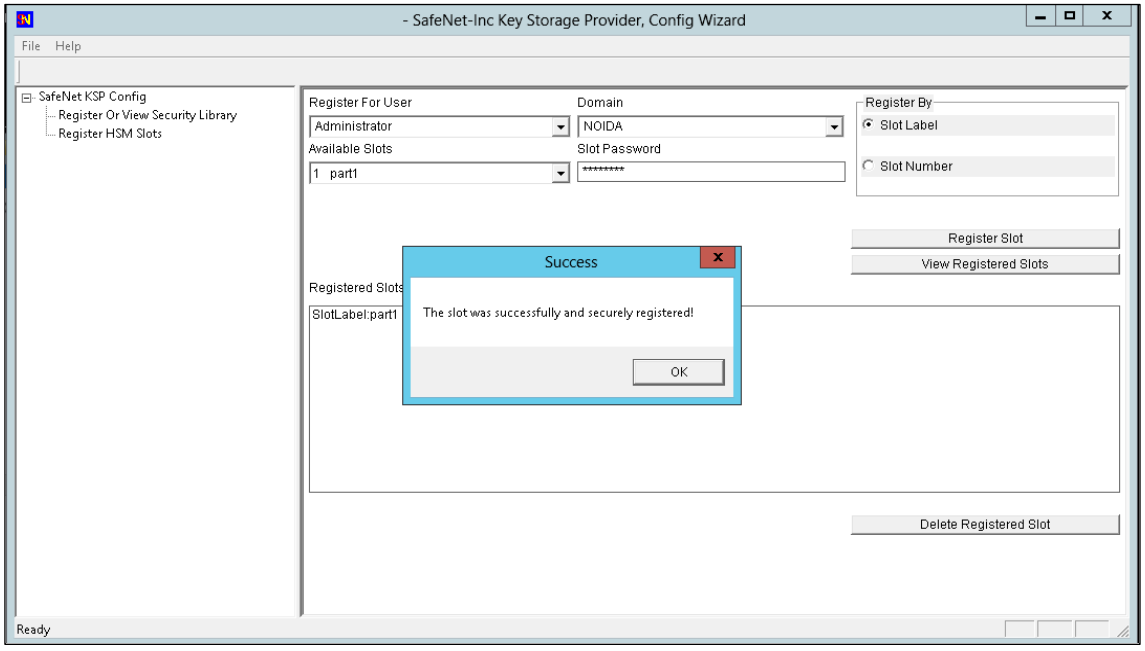
4. Browse the library cryptoki.dll from Luna Network HSM Client installation directory and click **Register**.



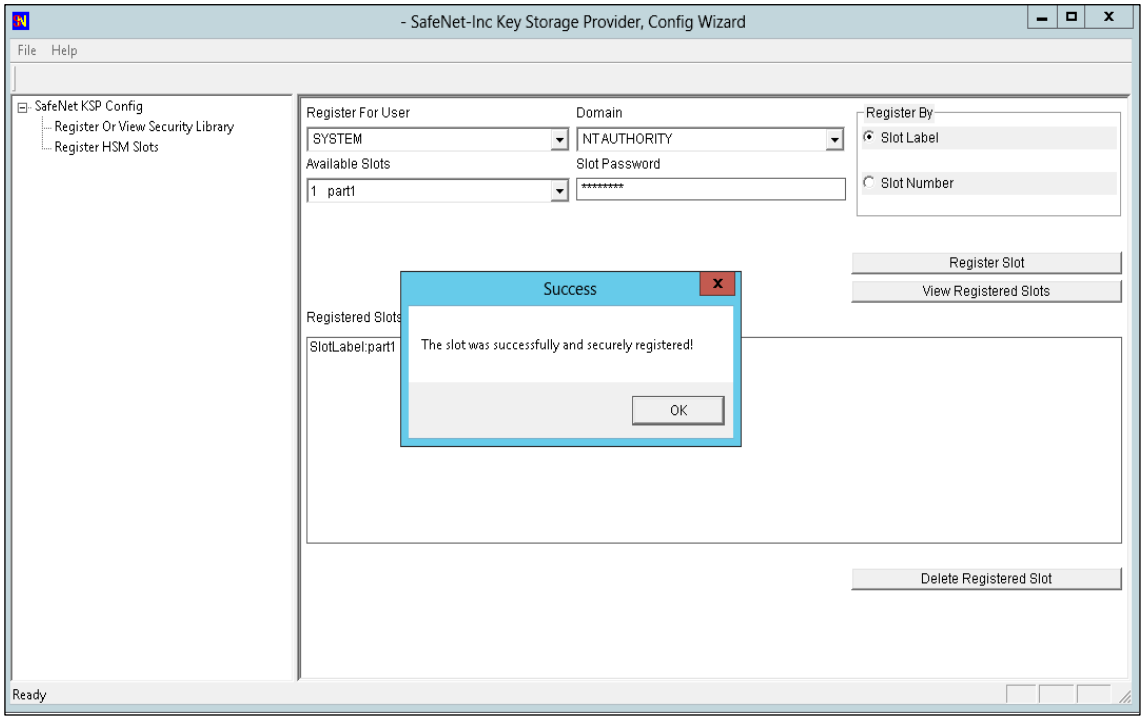
5. On successful registration, a message "**Success registering the security library**" displays.



6. Double-click **Register HSM Slots** on the left side of the pane.
7. Enter the Slot (Partition) password.
8. Click **Register Slot** to register the slot for Domain\User. On successful registration, a message "**The slot was successfully and securely registered**" displays.



9. You need to register the same slot for **NT AUTHORITY\SYSTEM**.

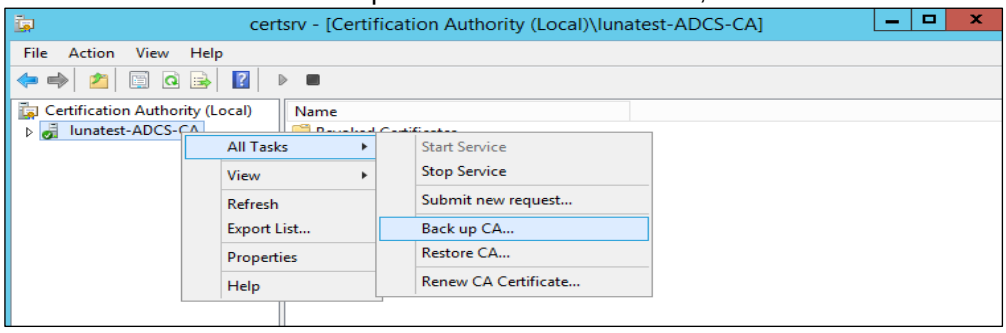


NOTE: Both slots have been registered, despite only one entry appearing for the service in the **Registered Slots** section of the KSP interface.

Back up the CA

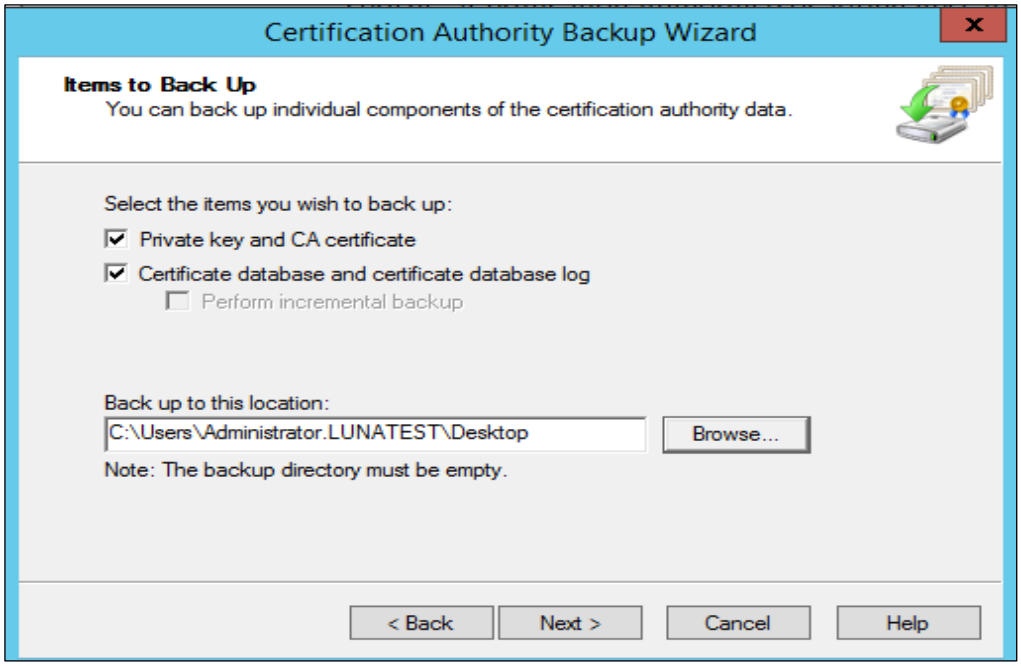
You can enable and configure the location where the CA backup files will be stored using the Active Directory certificate services management console. To back up the CA:

1. Click the **Start** button, click **Run**, type **certsrv.msc**, and then click **OK**.
2. Select the CA node in the left pane.On the **Action** menu, click **All Tasks** and then **Backup CA.**



3. Click **Next** on the Welcome page of the CA backup wizard.

4. Select the **Private key and CA certificate** check box and provide a directory name where the system will temporarily store the CA certificate and optionally the key. Click **Next**.



5. Provide a password to protect the CA key and click **Next**.
6. Click **Finish**.

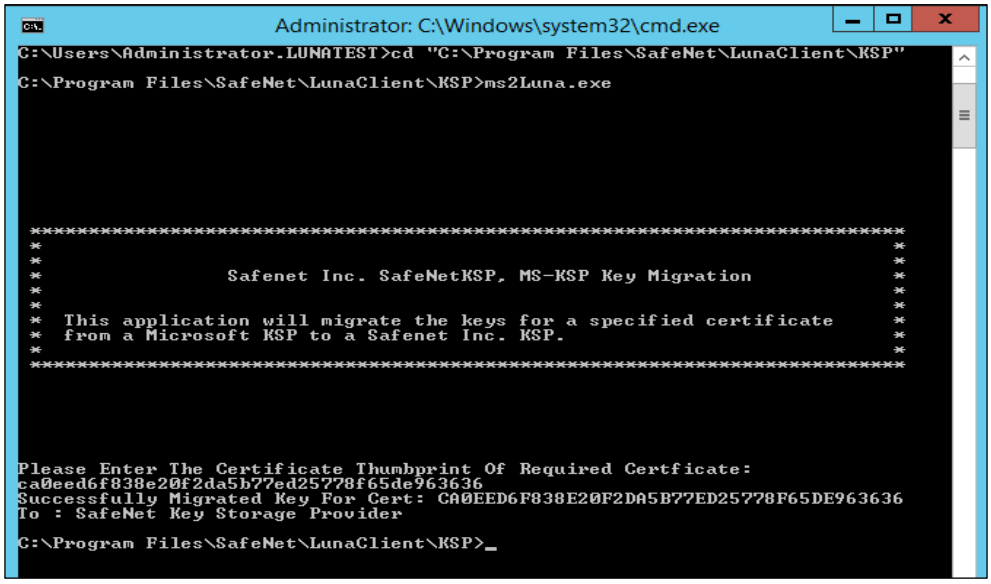
Migrate a MS CA onto a Luna HSM or Luna Cloud HSM service using ms2Luna

The Keys stored in the Software is not secure and can be compromised anytime. So to enforce operational and logical security of the CA it is required to be migrated onto HSM. Also migration ensures that the same key created in previous section is used for verification of CA. To migrate a MS CA onto a Luna HSM using ms2Luna:

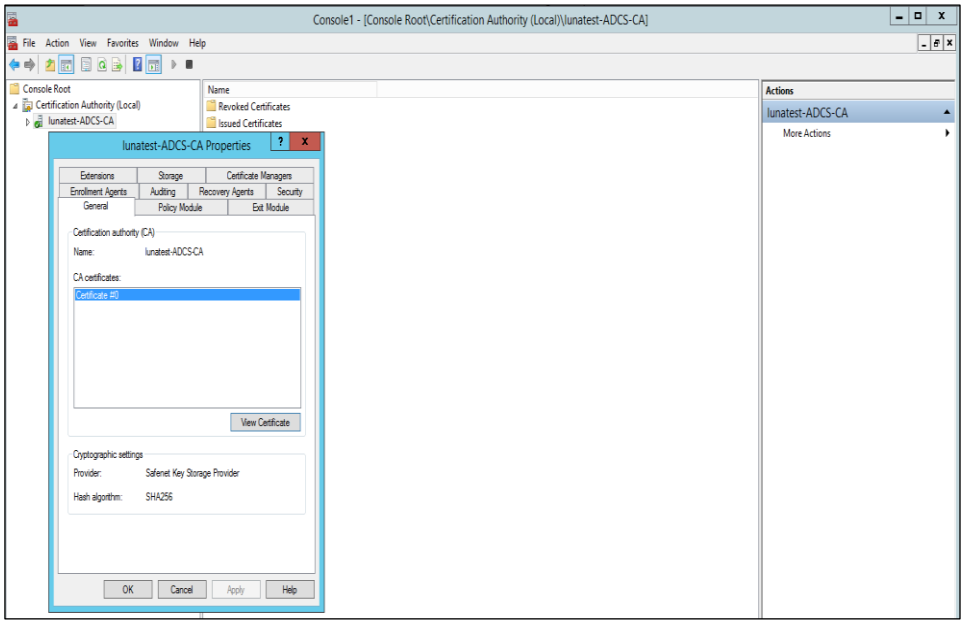
1. Copy the CA certificate thumbprint.
2. Open a command prompt and run `ms2Luna.exe from "<SafeNet HSM Client installation Directory>/KSP directory"` in case of KSP registration.

> **NOTE**: You need to register a slot using KSP before migrating MSCA to Luna HSM.

3. Enter the Thumbprint of CA certificate when prompted, and press **Enter**.



4. Verify that CA provider changes to **SafeNet Key Storage Provider**.



5. Restart the CA services and after restarting CA services will use the keys from Luna HSM for signing new certificate request and verify the already signed certificates.

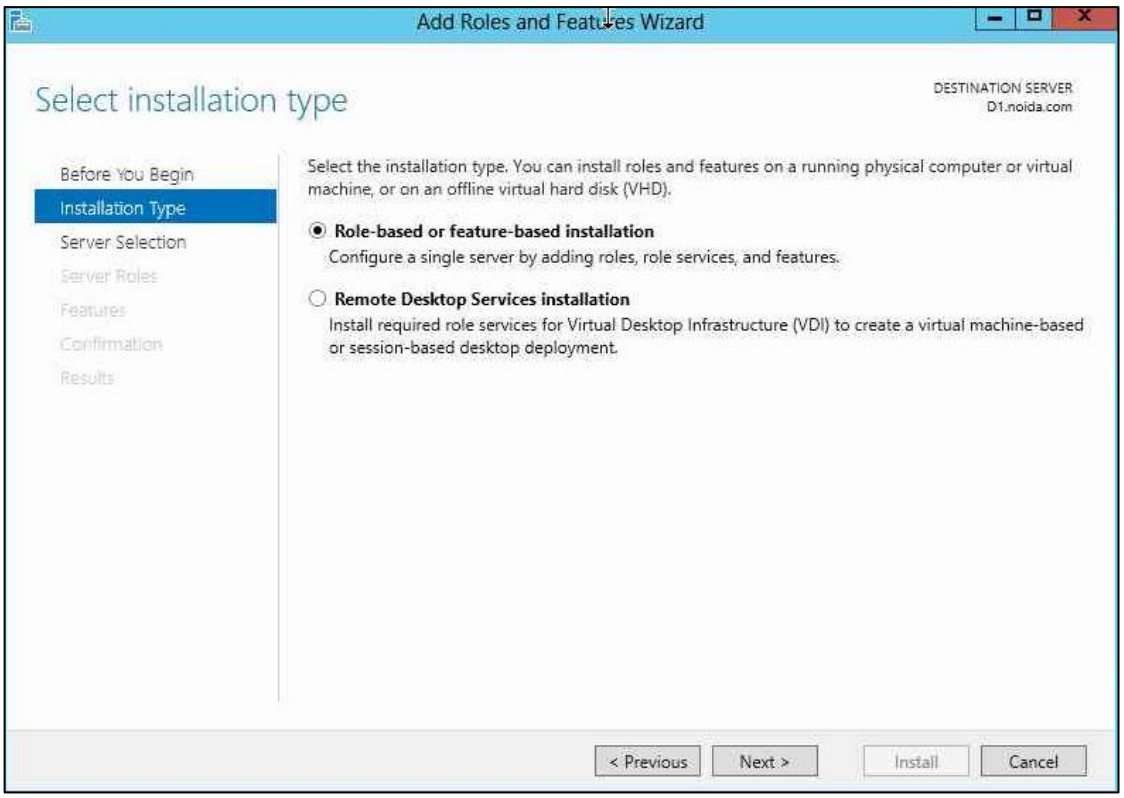
6. Now you can restore the CA certificate database that you have backed up before migration. To restore the CA database follow the steps to Restore MS CA.

   In case if CA Services are not restarting even after CA keys are migrated to Luna HSM using ms2luna then uninstall the CA services and follow the instructions to Install Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storage Provider with migrated key.

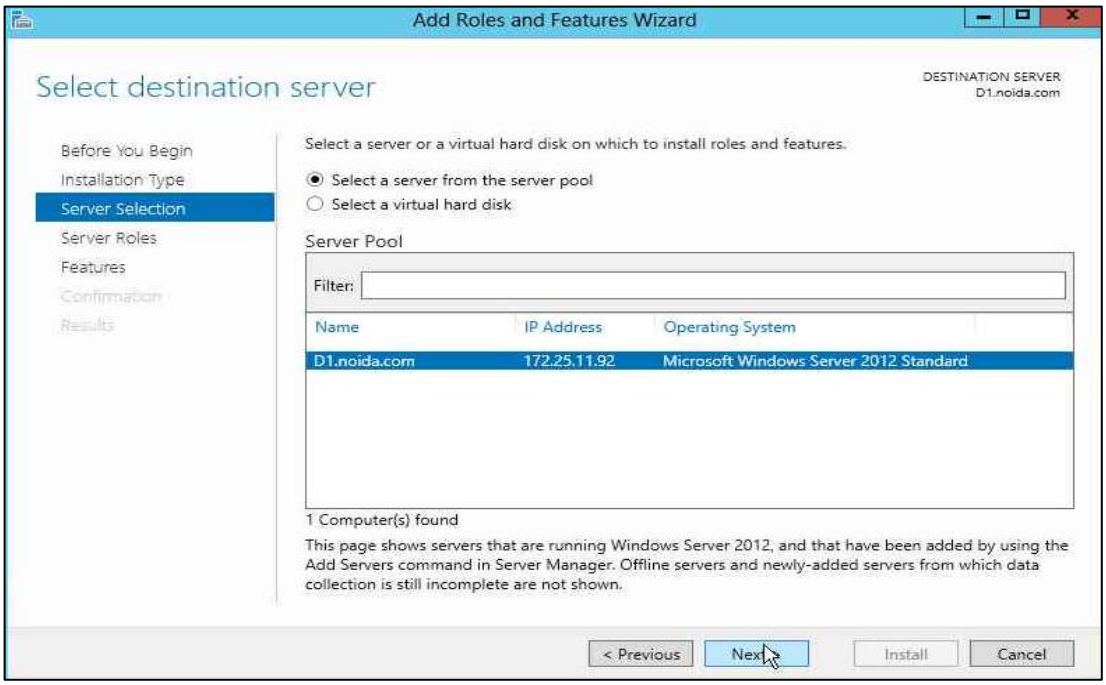
Install Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storage Provider with migrated key

To install the Microsoft Active Directory Certificate Services software:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Open **Server Manager** under Configure this **Local Server** and click **Add Roles and Features**.
3. The **Add Roles and Features Wizard** displays.
4. On the **Before you Begin** page click **Next.**
5. Select the **Role-based or feature-based installation** radio button and click **Next**.

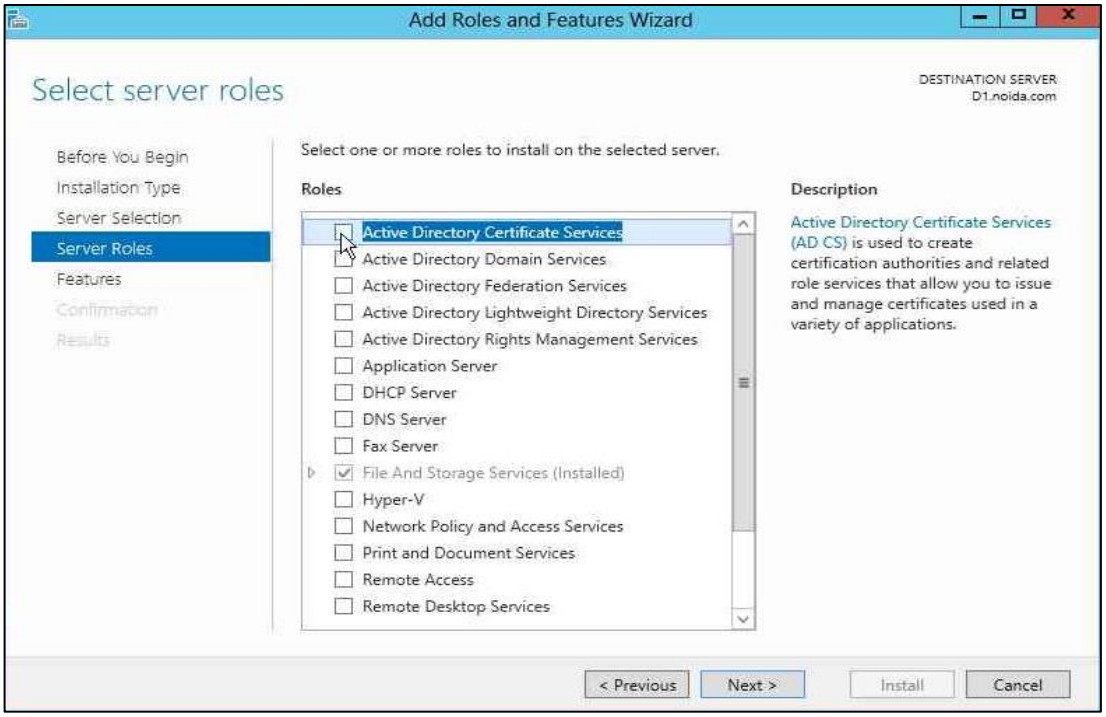


6. Select the **Select a server from the server pool** radio button and from **Server Pool** select your server.

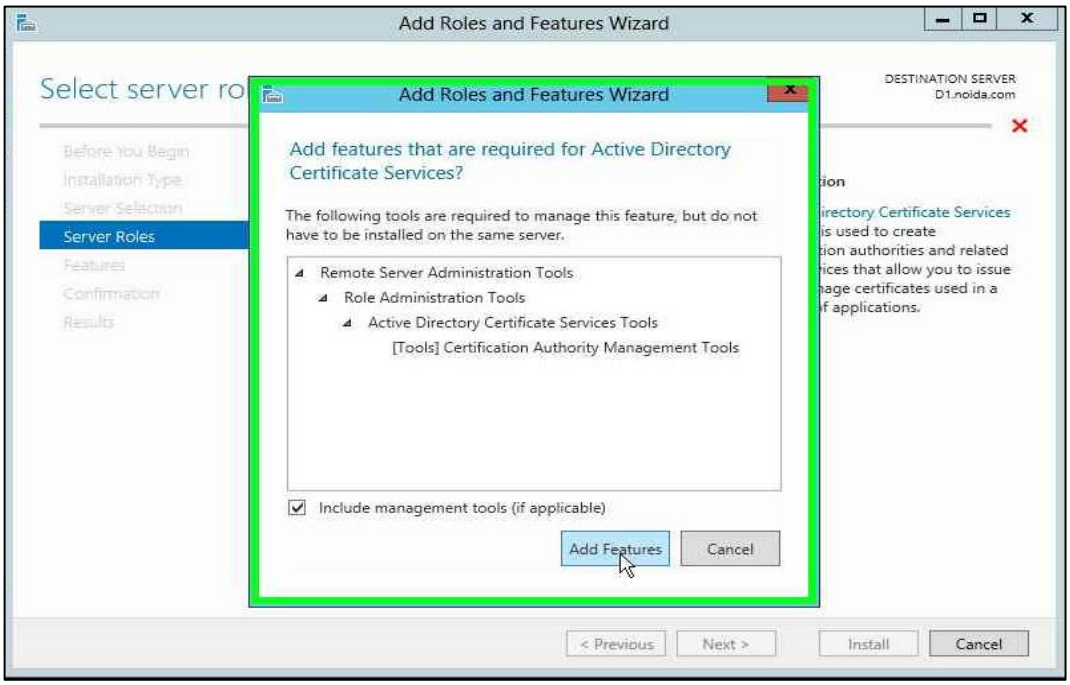


7. Click **Next**.

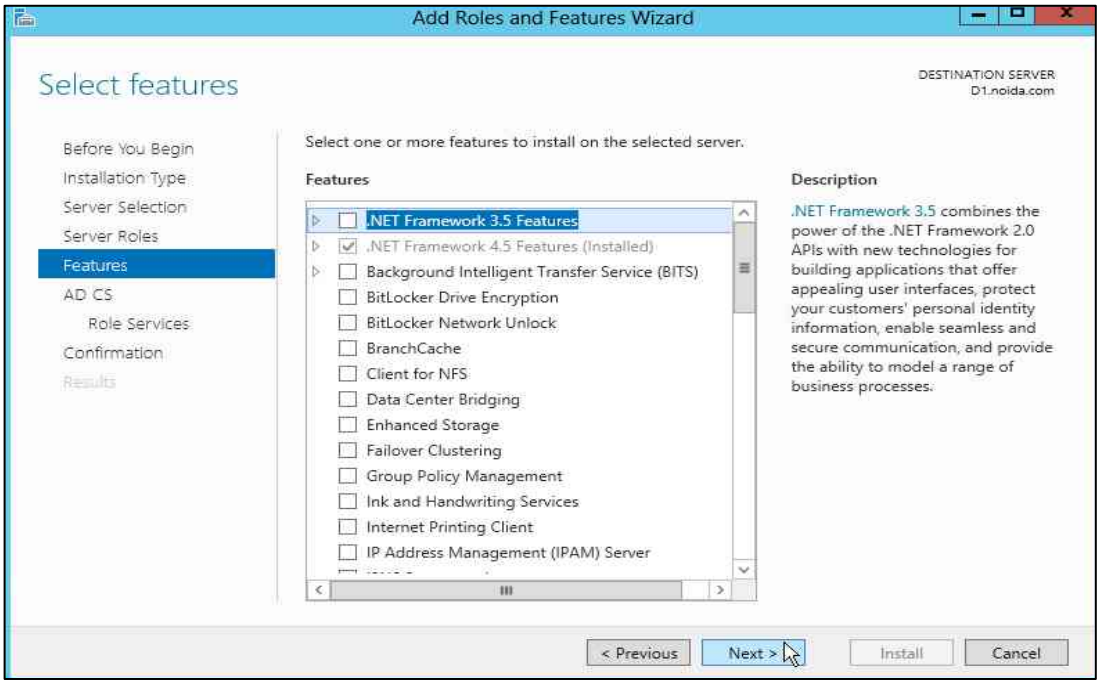
8. Select the **Active Directory Certificate Services** check box from the **Server Roles**.



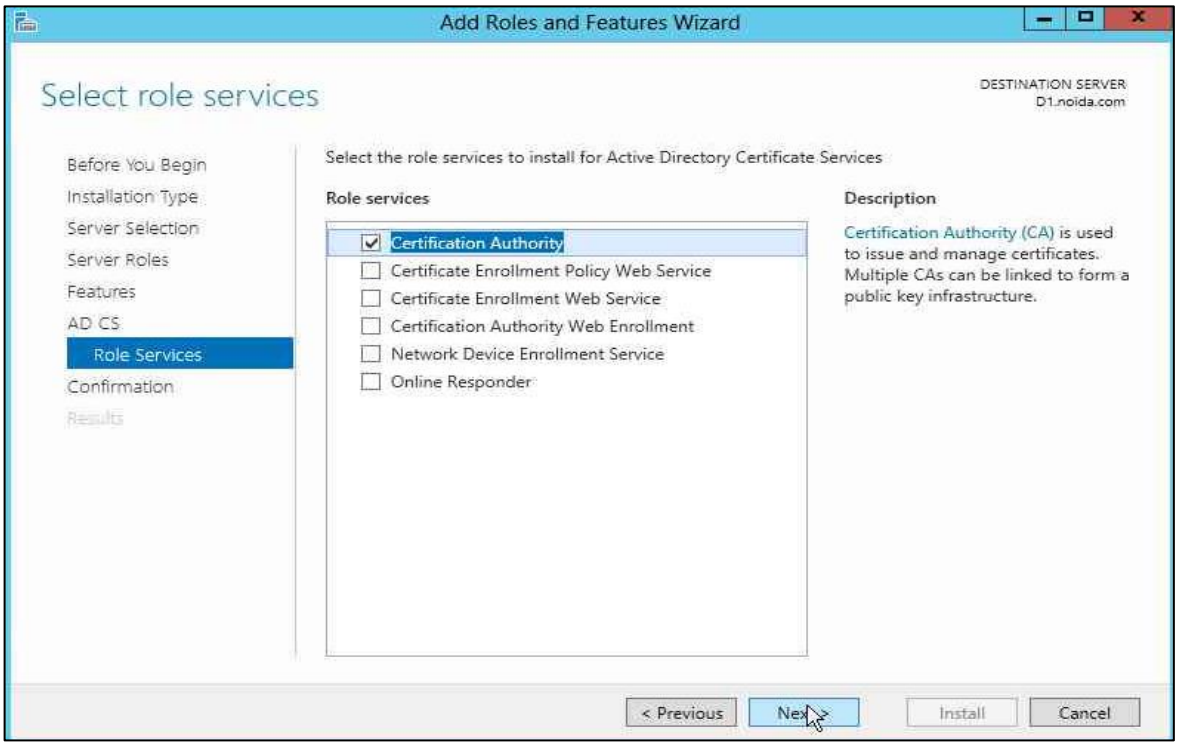
9. A window stating "**Add features that are required for Active Directory Certificate Services?**" displays. To add a feature, click **Add Features**.



10. Click **Next** twice to continue until the Role Services options are displayed.

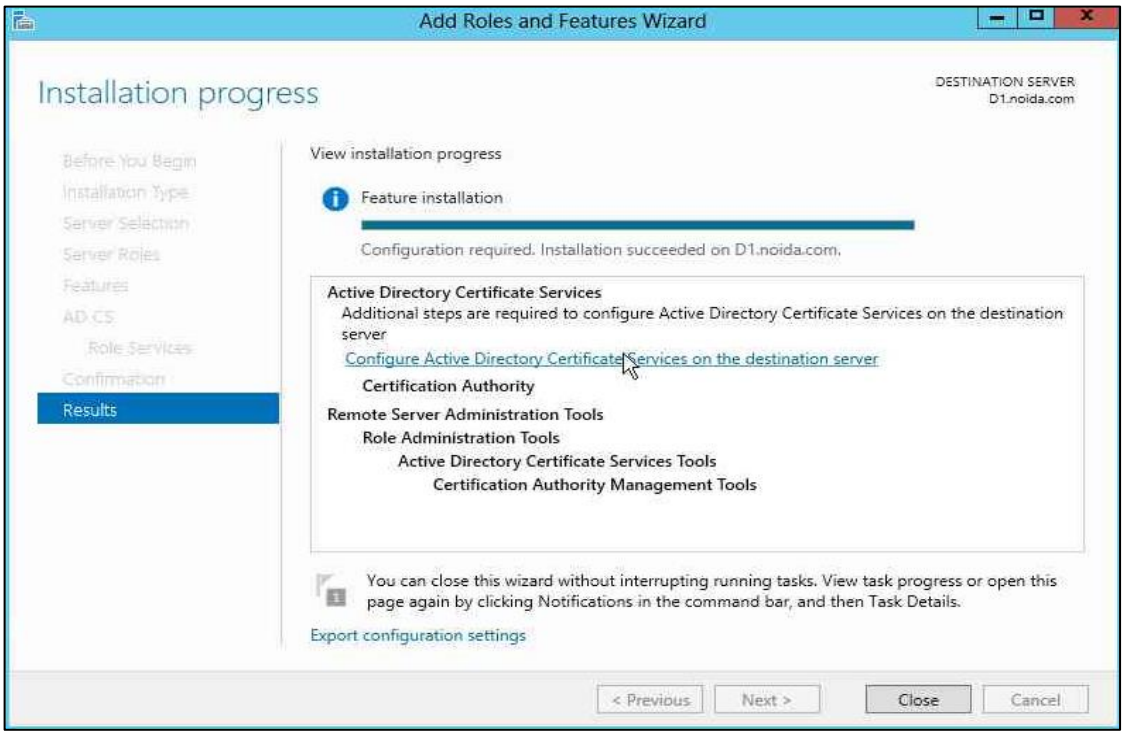


11. Select the **Certification Authority** check box from the **Role services** list and click **Next**.

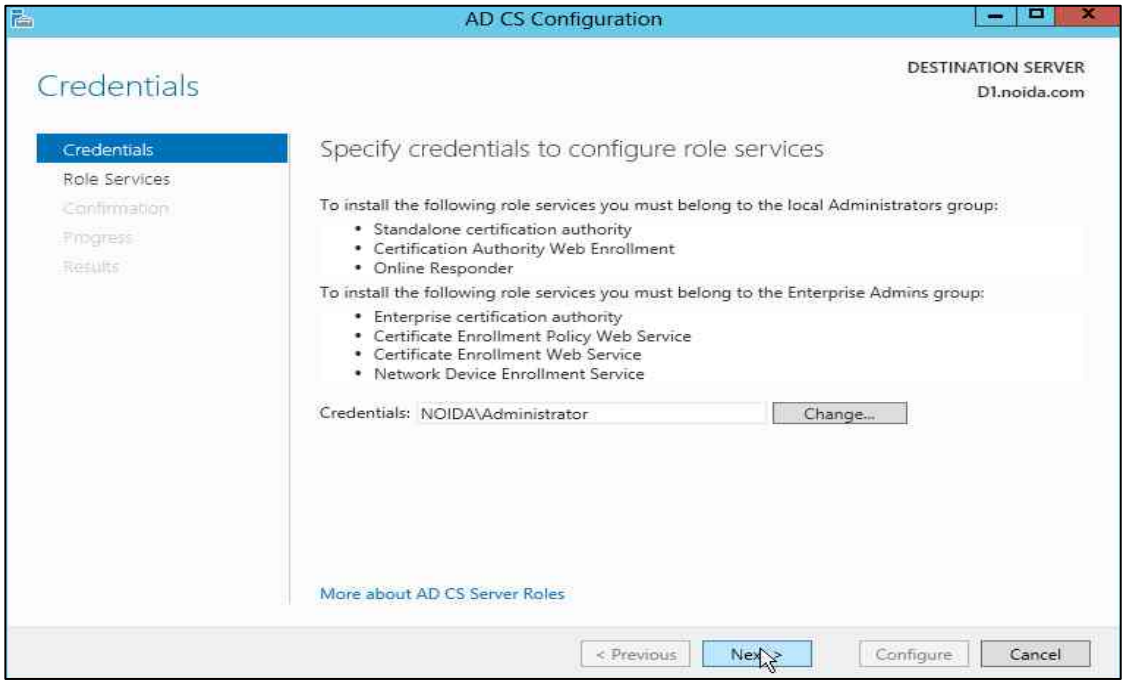


12. Verify that the role you are about to install is appropriate and click **Install**.

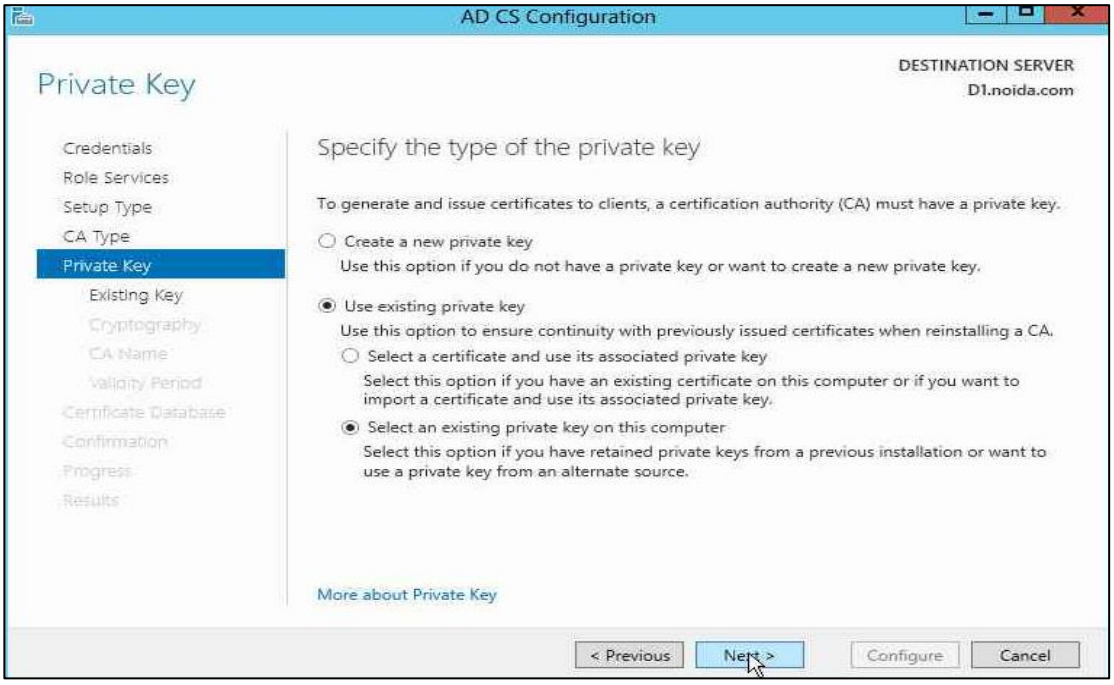
13. Once installation is complete, click the link **Configure Active Directory Certificate Services on the destination server** it opens AD CS Configuration wizard.



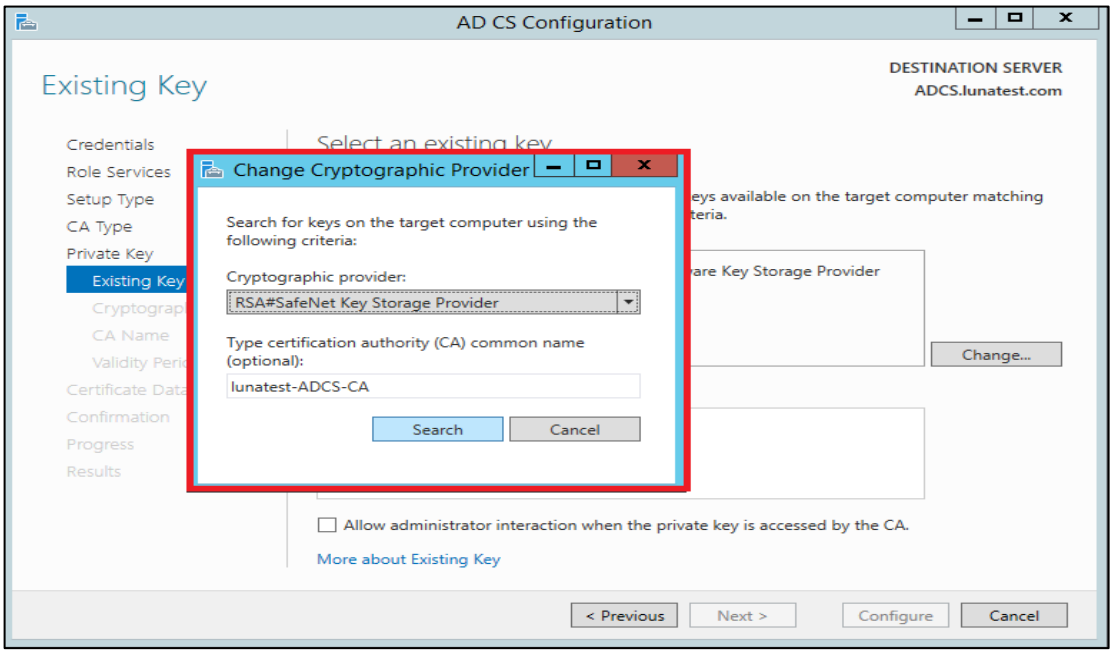
14. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.



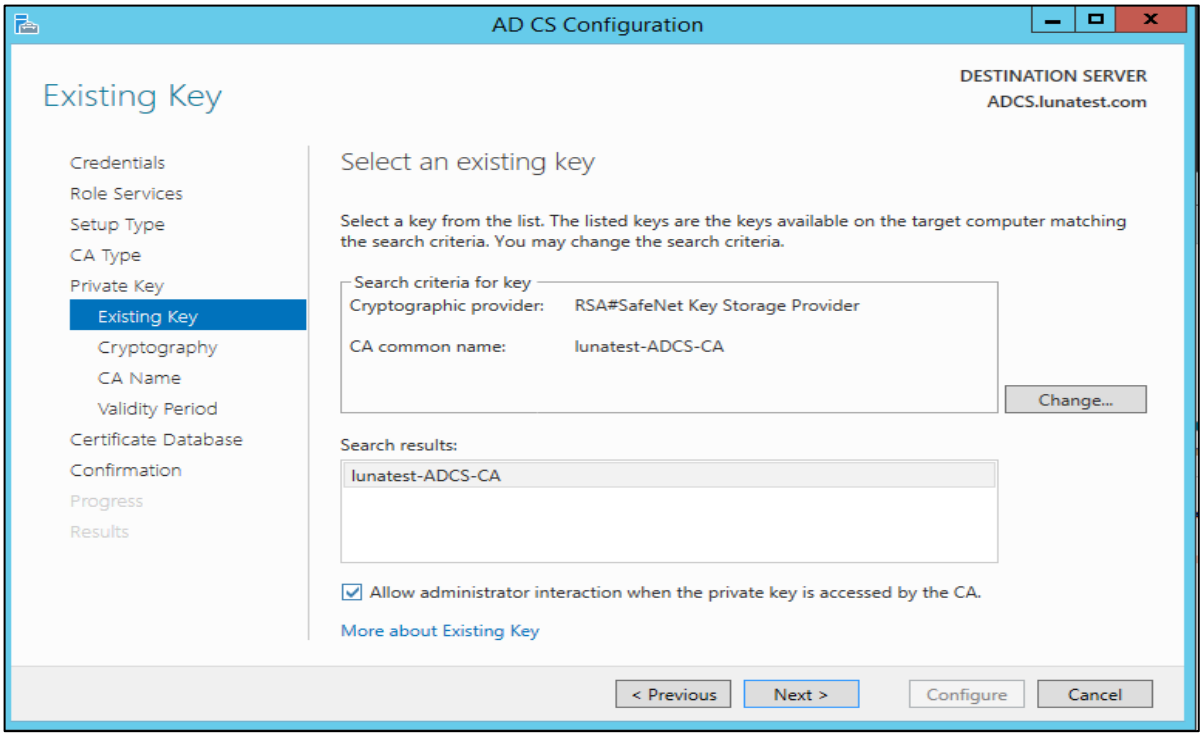
15. Select the **Certification Authority** check box and click Next.
16. Select the **Enterprise CA** radio button and click **Next**.
17. Select the **Root CA** radio button and click **Next**.
18. Proceed to setup the **Private Key** for CA to generate and issue certificates to clients. Select **Use existing private key** and **Select an existing private key on this computer.** Click **Next** to continue.



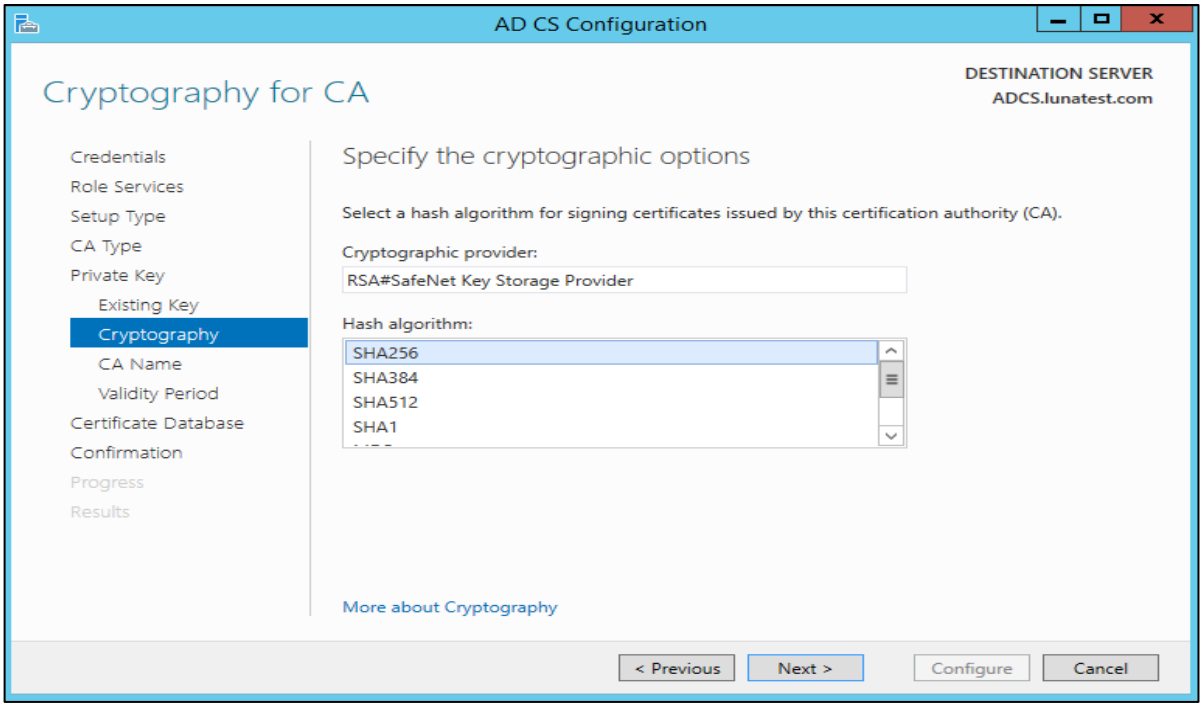
19. Click **Change…**. Select the **SafeNet Key Storage Provider** algorithm that you used to generate the private keys. Clear the CA Common name. Click **Search**.



20. Select the existing key and click **Next.** Select the **Allow administrator interaction when the private key is accessed by the CA** check box.

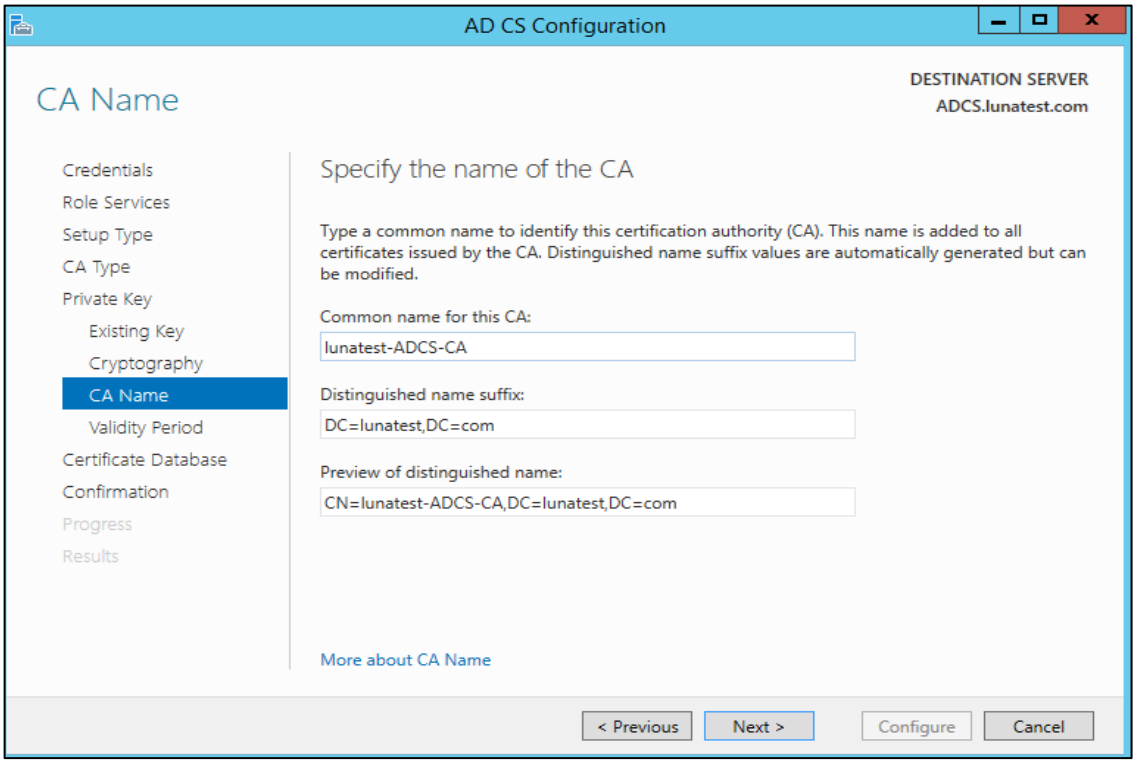


21. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.

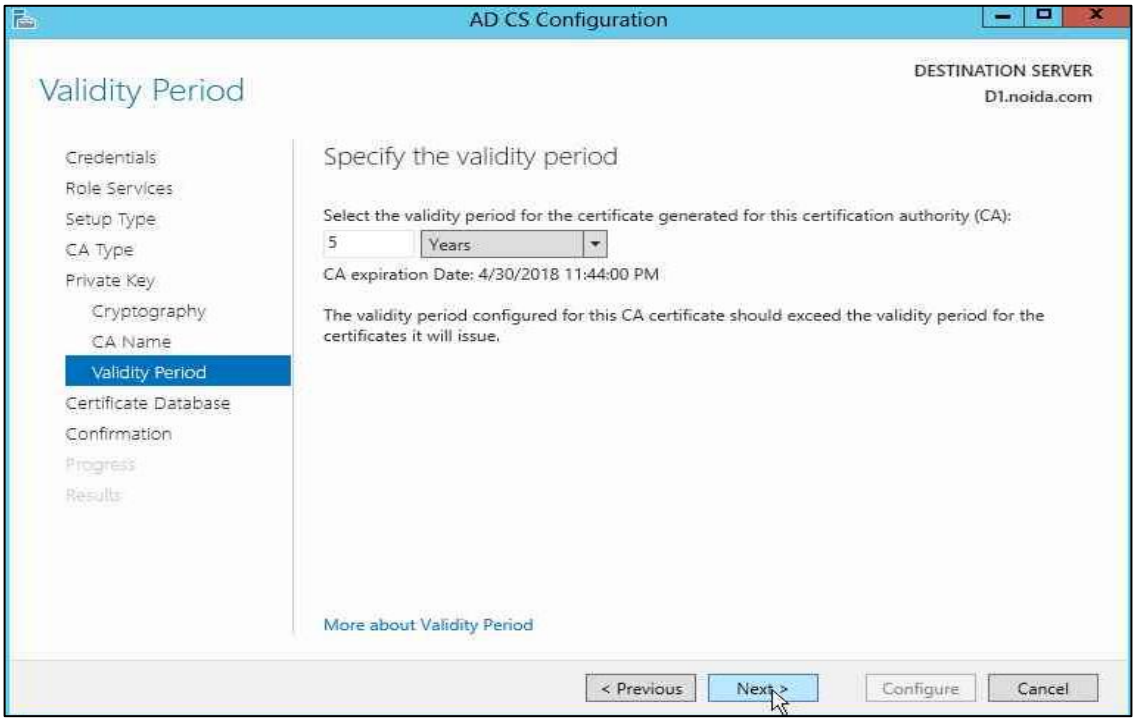


22. Click **Next** to continue.

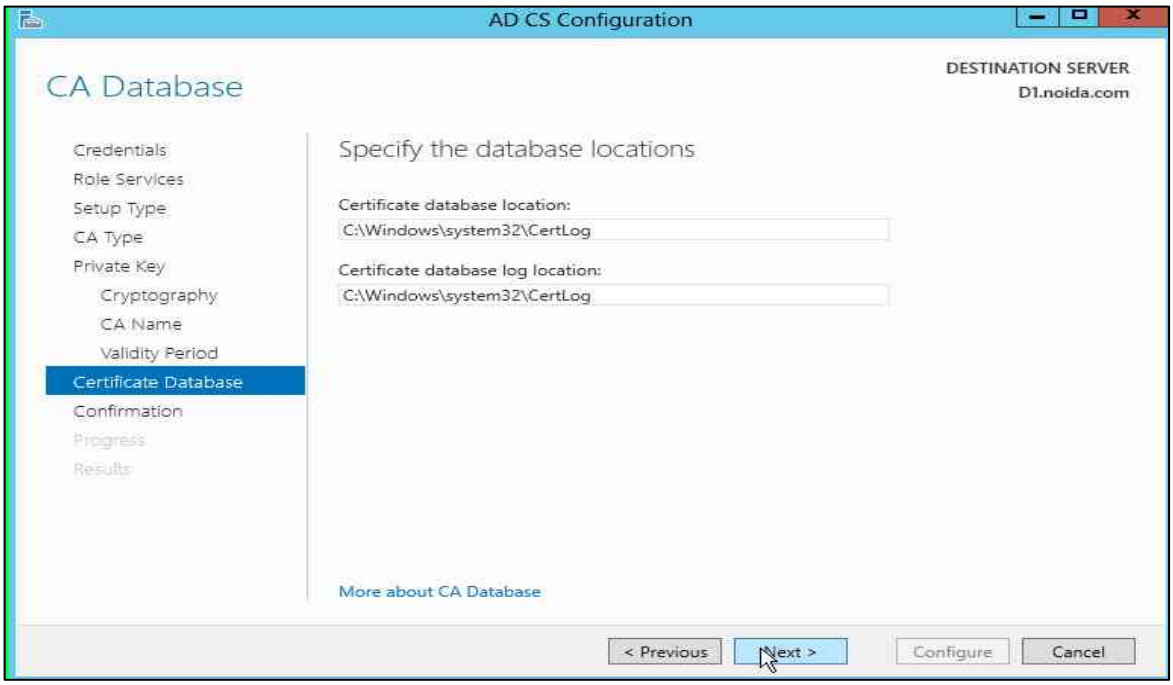
23. Configure a common name to identify this Certificate Authority. Click **Next** to continue.



24. Proceed to set the **Certificate Validity Period**. Click **Next** to continue.



25. Configure the **Certificate Database**. It records all the certificate requests, issued certificates, and revoked or expired certificates. Click **Next** to continue.



26. Click **Configure** to configure the selected roles, role services, or features.

27. Click **Close** to exit the **AD CS Configuration** wizard after viewing the installation results.

After successful installation, the CA certificate database needs to be restore which you have backed up before beginning the key migration.

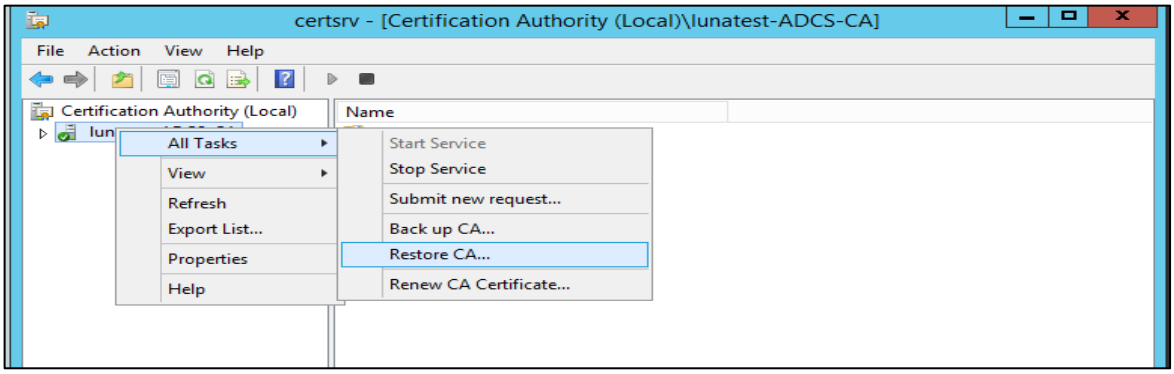
Restore MS CA

You can restore a backed-up MS CA database account. To restore an MS CA:

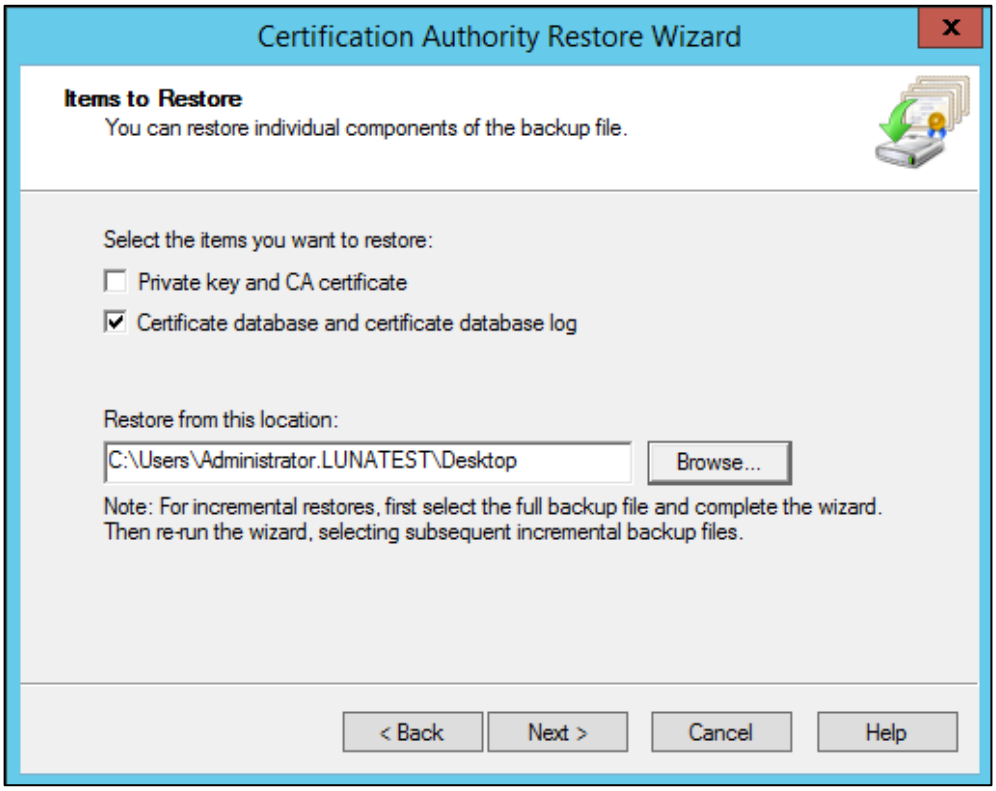
1. Click the **Start** button, click **Run**, type **certsrv.msc**, and then click **OK**.

2. Select the CA node in the left pane.

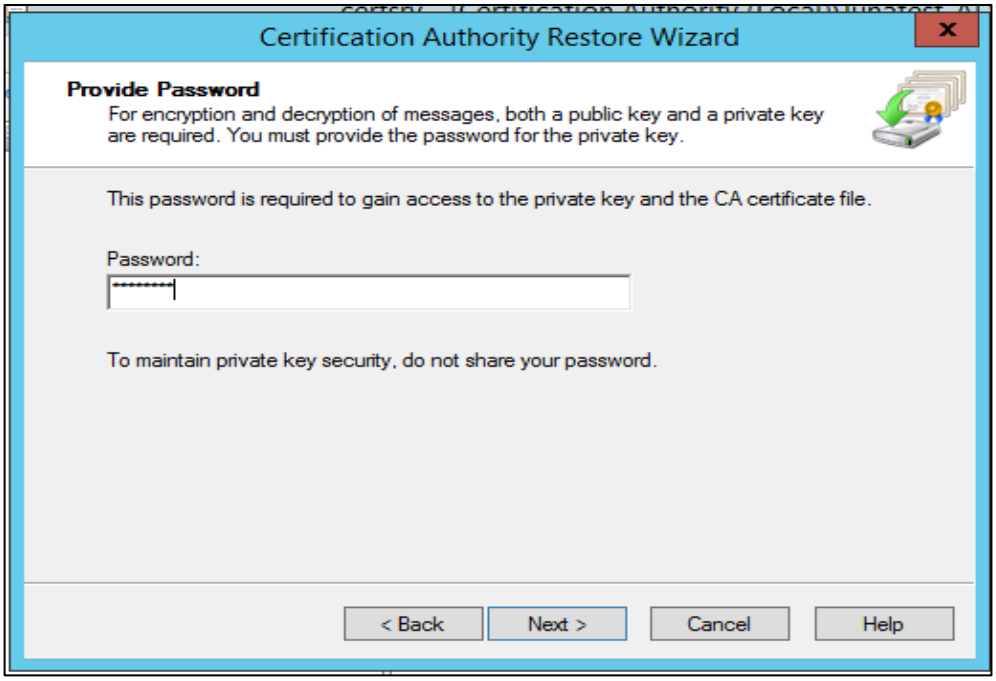
3. On the **Action** menu, click **All Tasks** and then **Restore CA**.



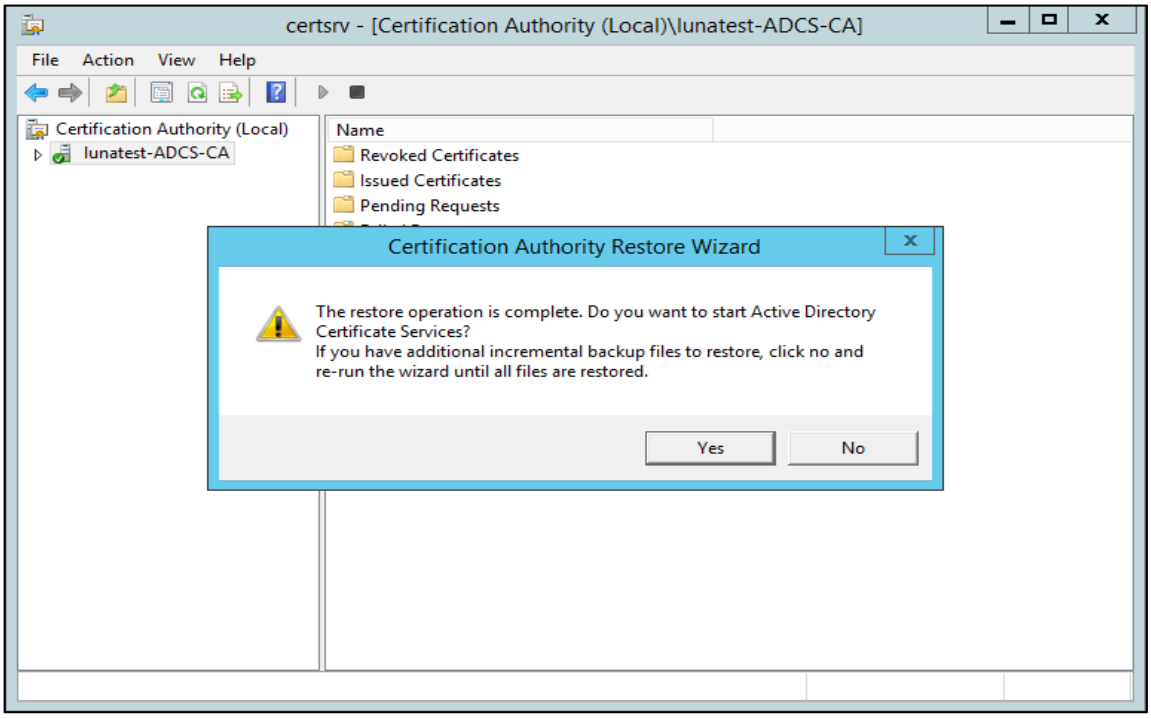
4. Click **Next** on the Welcome page of the CA Restore wizard.
5. Select the **Certificate database and certificate database log** check box and provide a directory name where you want to temporarily store the CA certificate and optionally the key. Click **Next**.



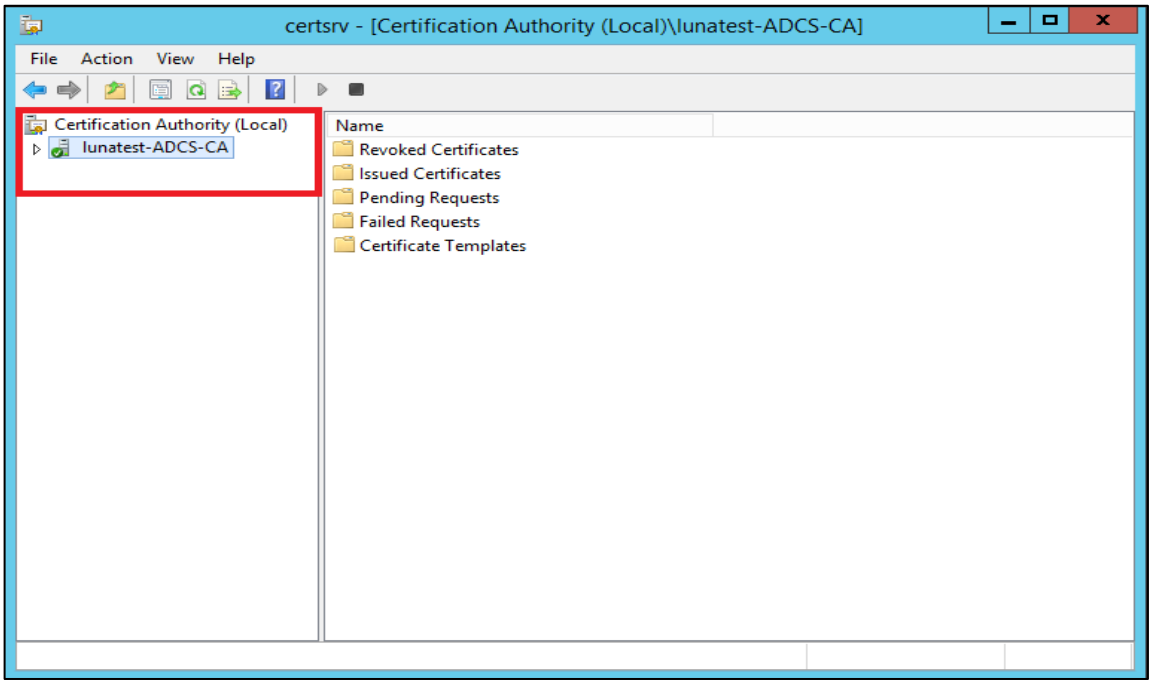
6. Enter password to protect the CA key and click **Next**.



7. Click **Finish**.
8. The "**Do you want to start Active directory certificate services**" window displays. Click **Yes**.



9. Verify that **Active Directory Services** has been successfully restarted.



This completes the CA keys migration from Microsoft Key Storage Provider to SafeNet Key Storage Provider which uses Luna HSM for accessing the CA keys when CA Services needs the keys.

Installing and Configuring the CA cluster using SafeNet Key Storage Provider

The following sections describe the installation and configuration of a CA on a failover cluster running on Windows Server. Register SafeNet Luna KSP using `KSPConfig.exe`. (Refer to the Configure the SafeNet HSM Key Storage Provider section.)

Set up the CA server role on the first cluster node

This section explains how to install certificate services on the first cluster node. To setup the CA server role on the first cluster node:

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. The steps to install the Microsoft Active Directory Certificate Services are same as the Install Active Directory Certificate Services section. After Microsoft AD CS is successfully installed on first node, continue with the below steps.
3. Click the **Start** button, point to **Run**, type **certsrv.msc**, and then click **OK**.
4. Select the CA node in the left pane.
5. On the **Action** menu, click **All Tasks** and then **Backup CA.**
6. Click **Next** on the Welcome page of the CA backup wizard.
7. Select **Private key and CA certificate** and provide a directory name where you will temporarily store the CA certificate and optionally the key. Click **Next**.

8. Provide a password to protect the CA key and click **Next**.
9. Click **Finish**.

> **NOTE**: You will receive a warning message that the private key cannot be exported. This is expected behavior because the private key will never leave the Luna HSM.

10. Click **OK** to continue.

> **NOTE:** You need to run the *ksputil.exe* utility to migrate keys to the cluster. Please contact Customer Support, in case you do not have the `ksputil.exe` utility.

11. Create a cluster key for second node using existing key as the keys generated by KSP is bound with the system on which they are generated. Creating the cluster key will duplicate the CA key and bind the same key with second node.

12. Run the ksputil.exe utility to make the keys visible to the secondary node in the cluster. You will be prompted to enter the partition password.

    ```
    ksputil clusterKey /s <slotNum> /n <CA_Name> /t <TargetHost_Name>
    ```

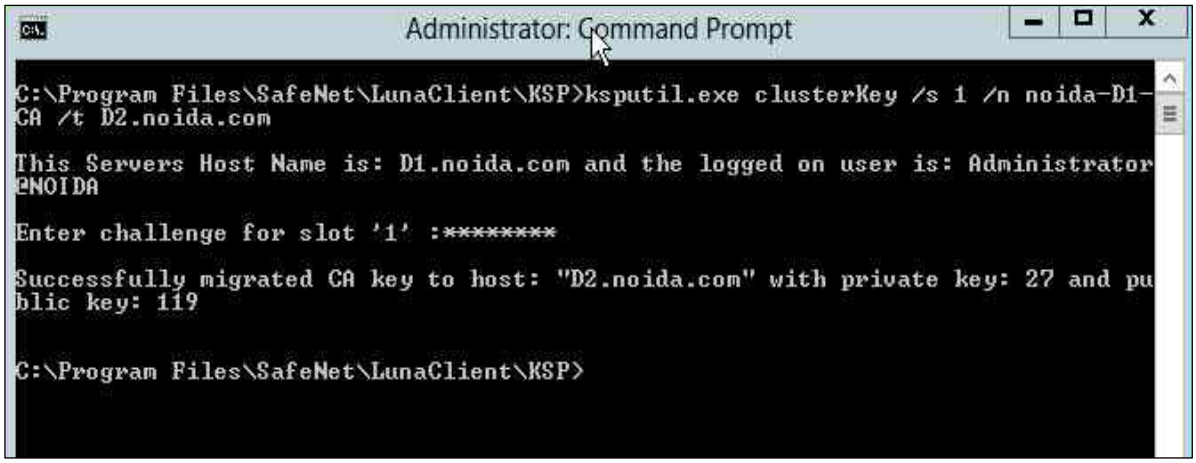
    Where,

    slotNum – slot number

    CA_name – name of the CA

    TargetHost_Name – FQDN of the second node

    > **Note:** This steps is need to be executed for each node if you have more nodes in your cluster and bind all your nodes with the same CA key to access the key from each node when these nodes will be part of your AD CS Cluster.



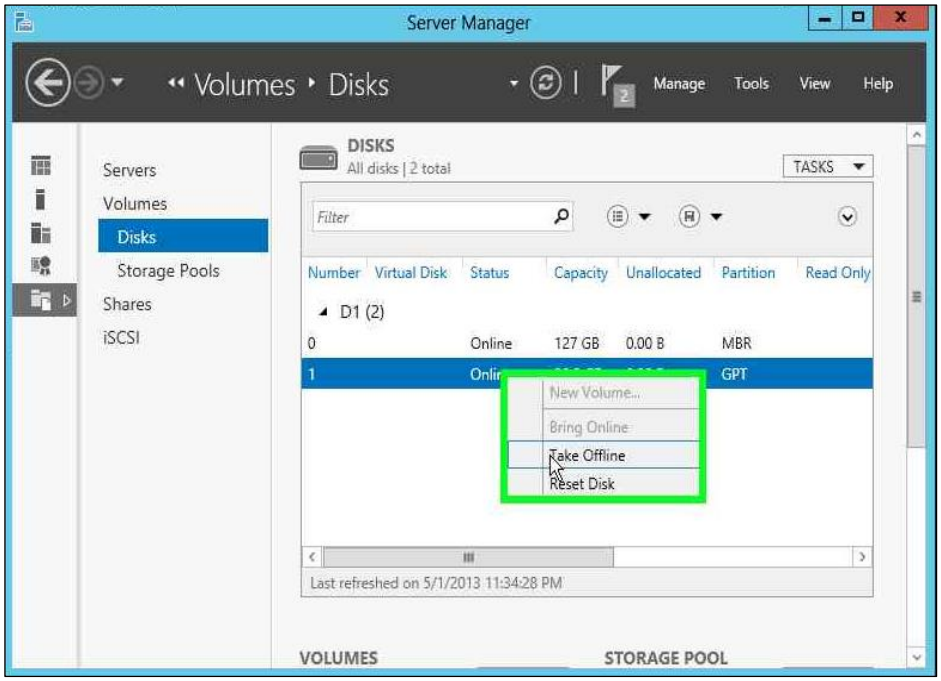
13. Click the **Action** menu, **All Tasks** and then **Stop Service**.

    > **NOTE**: After the successful migration of keys to the second node, the CA service must be shut down to unlock the disk resources.

14. Close the CA management snap-in.

To detach the shared storage form the cluster node

1. Go to the **Server Manager** MMC snap-in. Click the **File and Storage Services**. Click **Disks**, select shared disk resource, right click on it and select **Take Offline**.



To release the HSM from the cluster node

1. Since Luna HSM is a network attached HSM, therefore disable the network connection to release it from cluster node one.
2. Logoff from the first node.

   The installation of the Certification Authority on the first node is completed now.

Set up the CA server role on the second cluster node

This section explains how to set up the second cluster node. If you have more than two cluster nodes you need to follow the steps for each cluster node.

To install the CA on the second node, complete the following tasks:

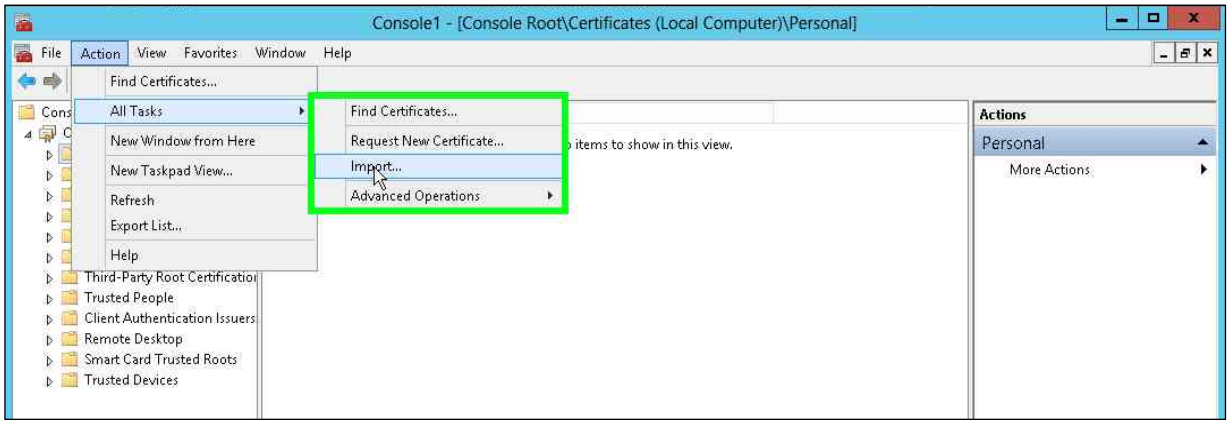
Configure the secondary cluster node:

1. Log on to the cluster node with a user having permissions to install the second cluster node. To install an enterprise CA, logon with enterprise admin permissions to the Active Directory domain. To install a standalone CA you may logon with local admin permissions if you don't want to register the CA in the Active Directory configuration container.
2. Click the **Start** button open **Run**, type **servermanager.msc**, and click **OK**.
3. The **Server Manager** MMC snap-in opens. Click the **File and Storage Services**. Click **Disks**.
4. Ensure that the shared disk that is used for the CA is online.

5. Copy the previously exported CA certificate to the second cluster node.
6. Click the **Start** button, point to **Run**, type **mmc**, and then click **OK**.
7. From the **File** menu, click **Add/remove Snap-in…**
8. Select **Certificates** from the list of available snap-ins and click **Add**.
9. Select the **Computer Account** radio button and click **Next**.
10. Select the **Local Computer** radio button and click **Finish**.
11. Click **OK**.

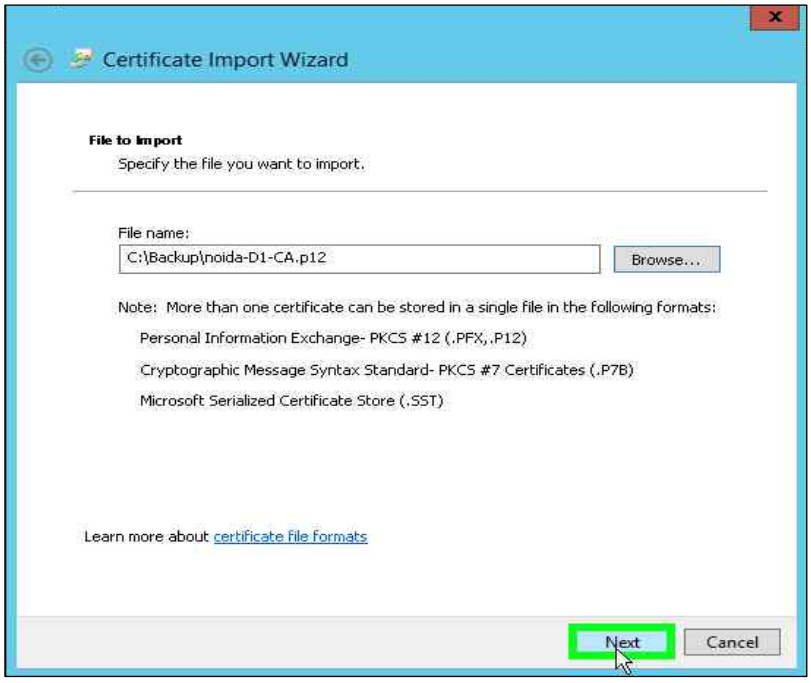
Import an existing CA certificate

1. In the Certificate Manager MMC snap-in, expand the **Certificates (Local Computer)** node and select the **Personal** store.
2. From the **Action** menu click **All Tasks** and then **Import …**



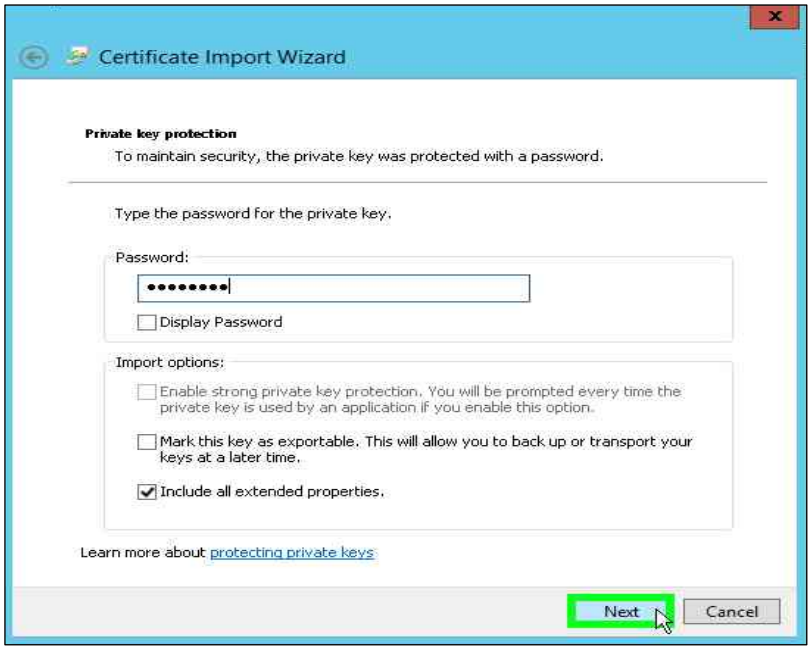
3. In the **Certificate Import Wizard**, click **Next.**

4. Enter the filename of the CA certificate that was previously created on the first node and click **Next**. If you use the Browse button to find the certificate, change the file type to *Personal Information Exchange *pfx,*.p12)*.

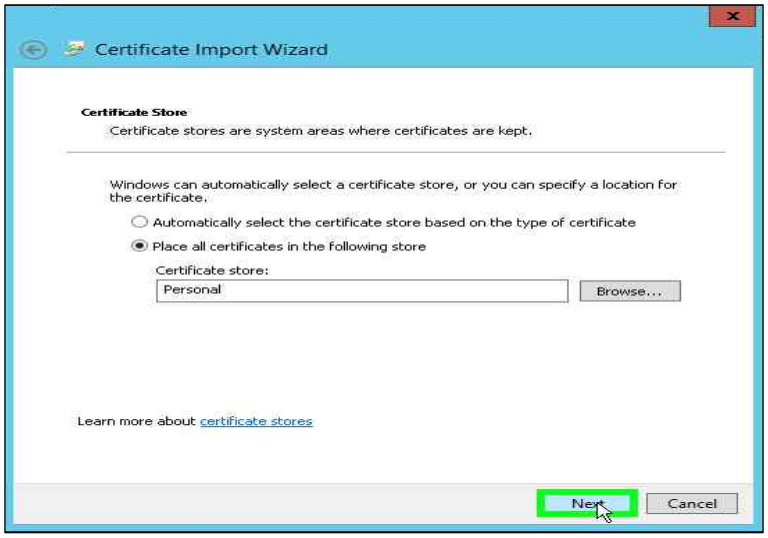


5. Type the password previously used to protect the private key. The password is required even if there is no private key in the PFX file. Click **Next.**

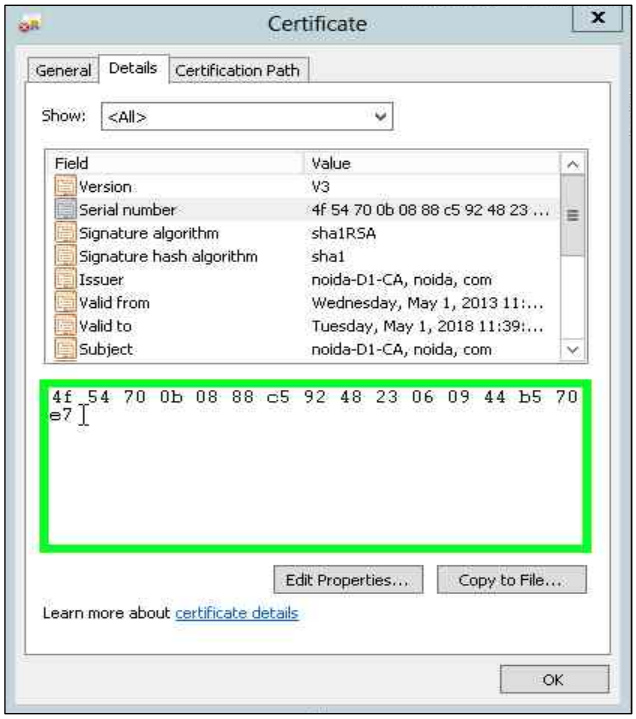
> **NOTE**: Do not select the Mark this key as exportable check box.



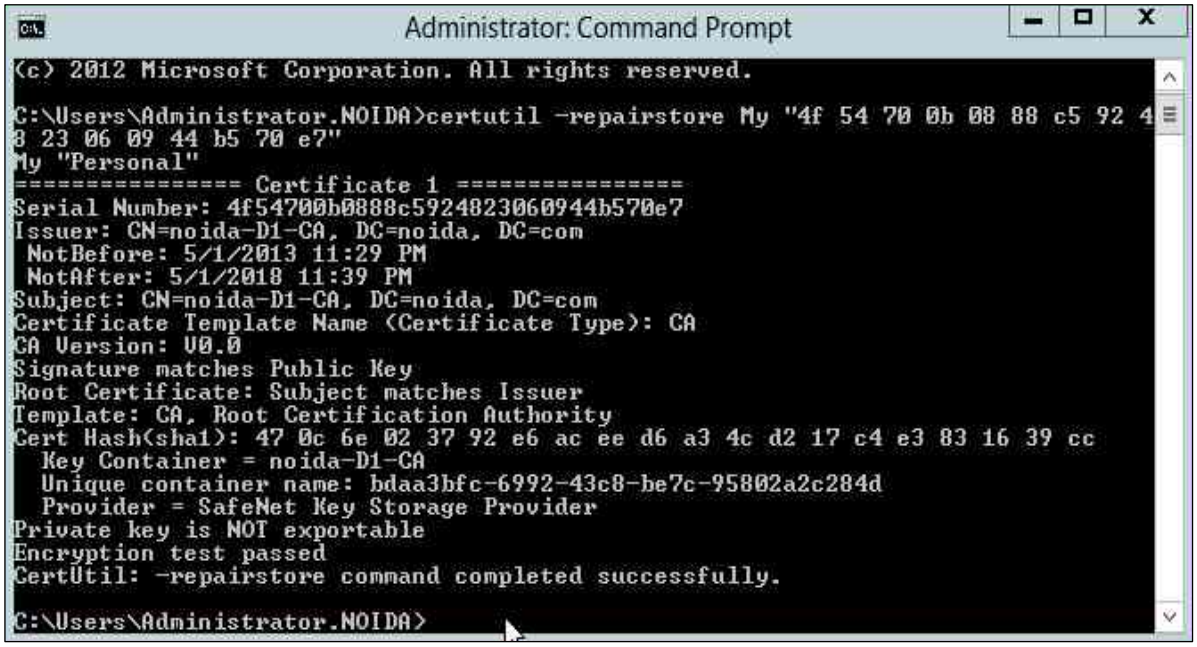
6. Select the Place all certificates in the following store radio button and select the **Personal** certificate store.



7. Click **Next**.
8. Click **Finish** to import the certificate.
9. Click **OK** to confirm the successful import.
10. Repair the association between the certificate and the private key that is stored in the HSM.
11. In the Certificate manager, expand the **Personal** store and select the **Certificates** container.
12. Select the imported certificate and select **Open** from the **Action** menu. Go to the **Details** tab.
13. Select the field **Serial Number** and copy the serial number into the clipboard. Click **OK**.



14. Open the command prompt and type `certutil -repairstore My "{Serial number}"` and press **Enter**.



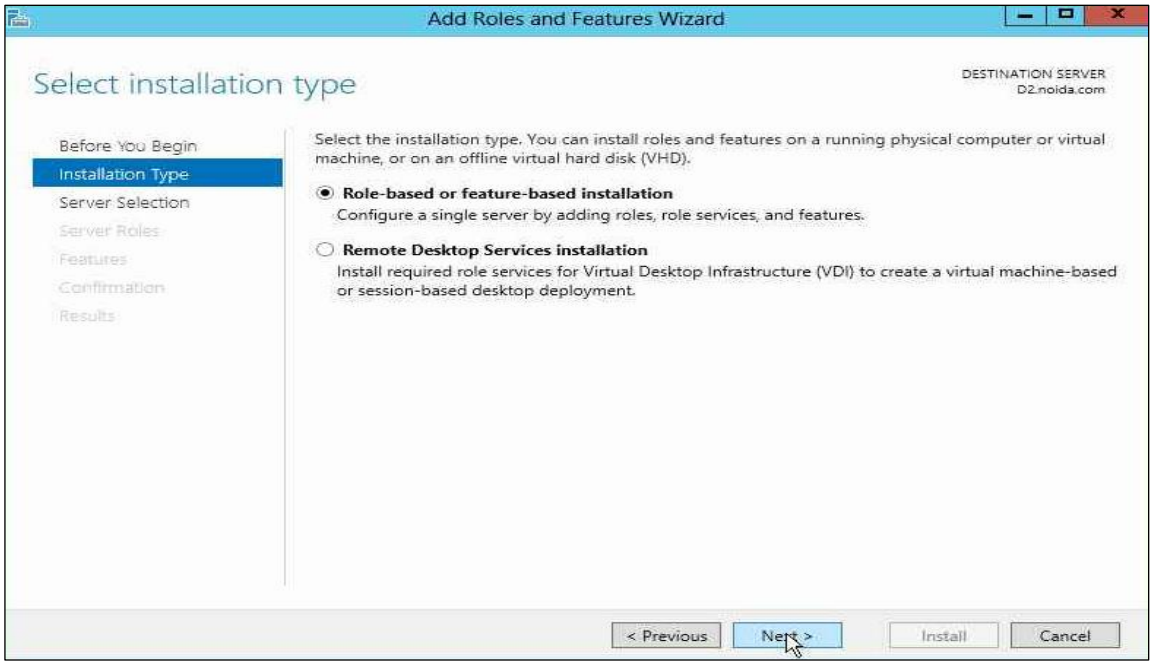
Add the AD CS role

1. Open **Server Manager** under **Configure this Local Sever** and click **Add Roles and Features**.

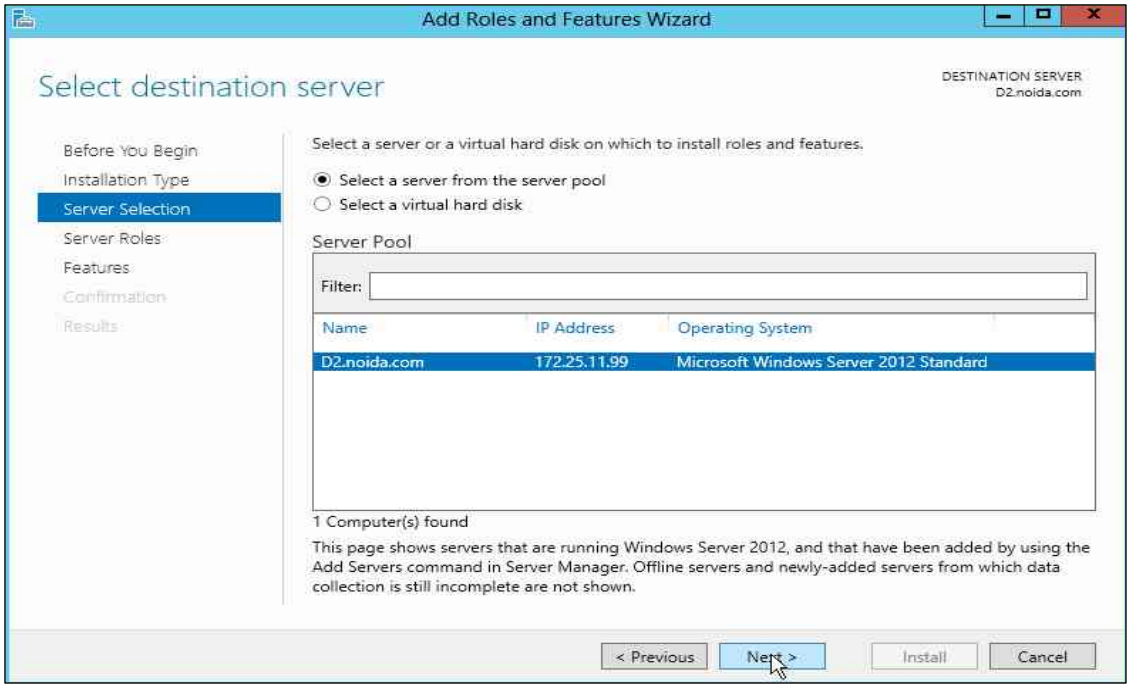
2. The **Add Roles and Features Wizard** displays.

3. Click **Next**.

4. Select the **Role-based or feature-based installation** radio button and click **Next**.

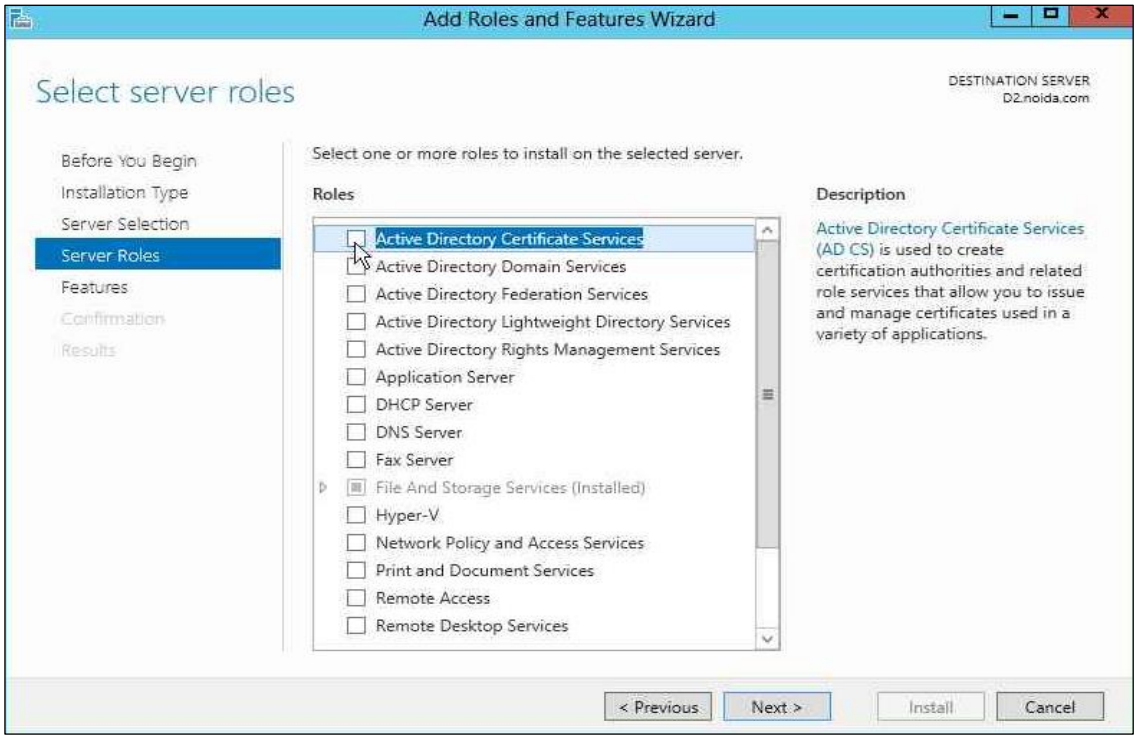


5. Select the **Select a server from the server pool** radio button and from **Server Pool** select your server.



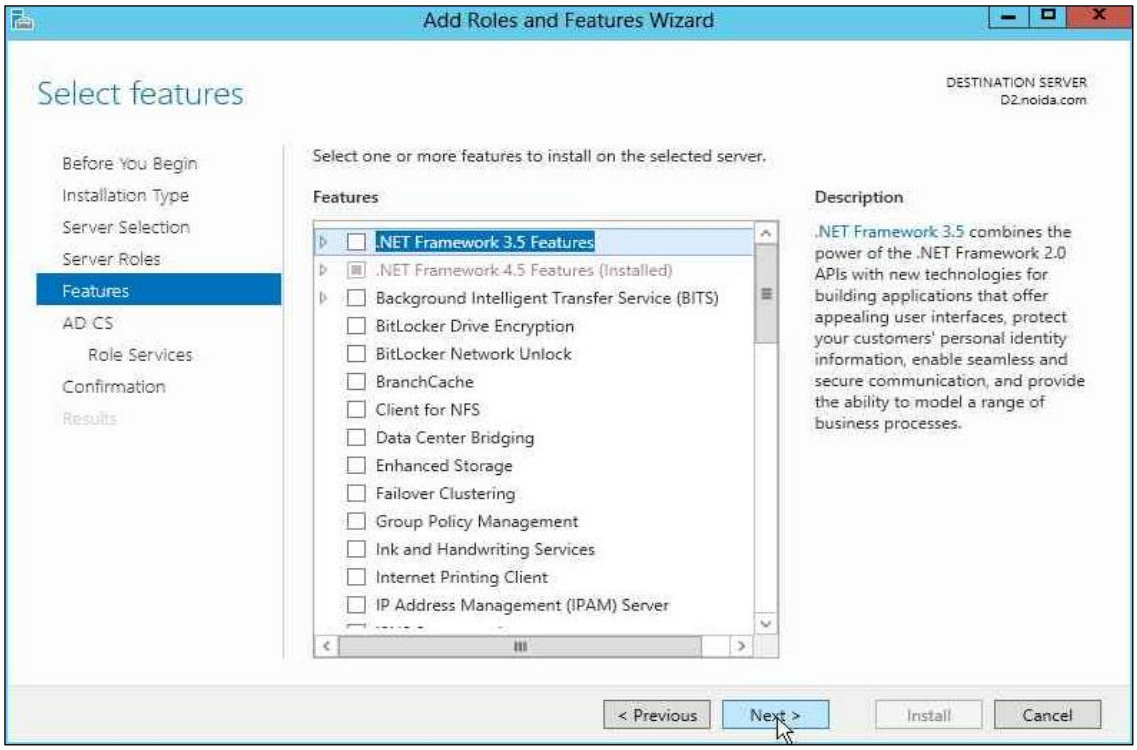
6. Click **Next**.

7. Select the **Active Directory Certificate Services** check box from the **Server Roles.**



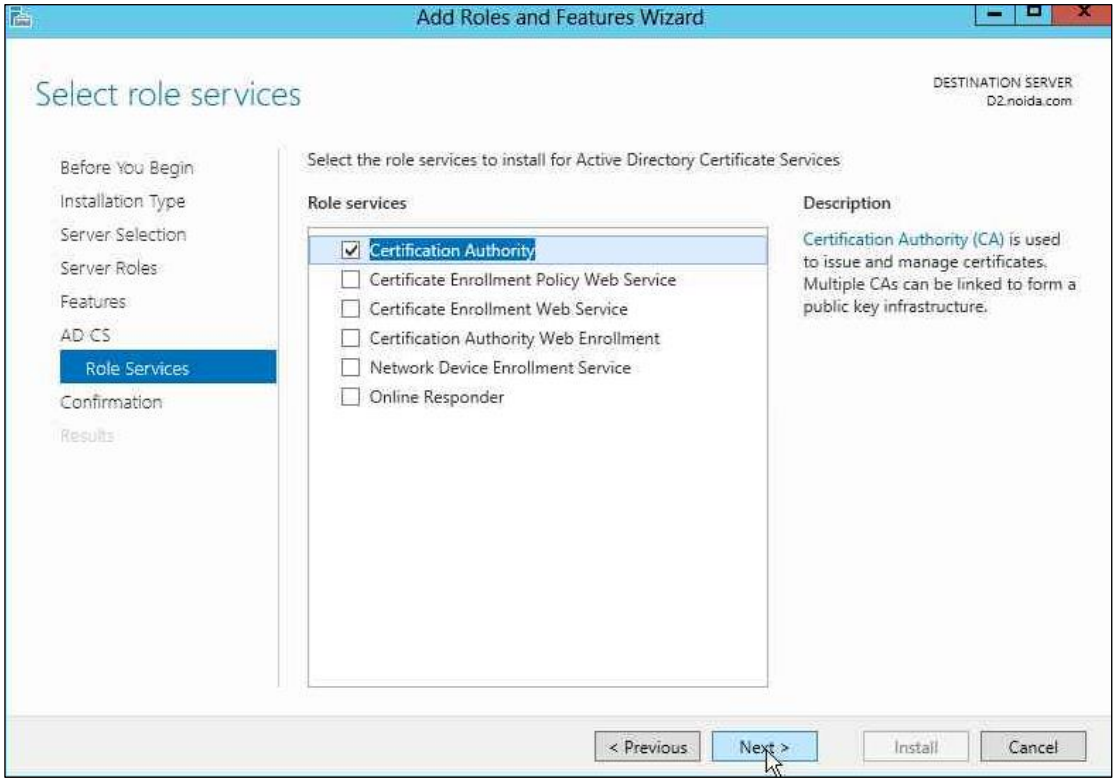
8. The **Add features that are required for Active Directory Certificate Services** window will appear. To add a feature, click the **Add Features** button.

9. Click **Next** to continue.
10. Click **Next** to continue.

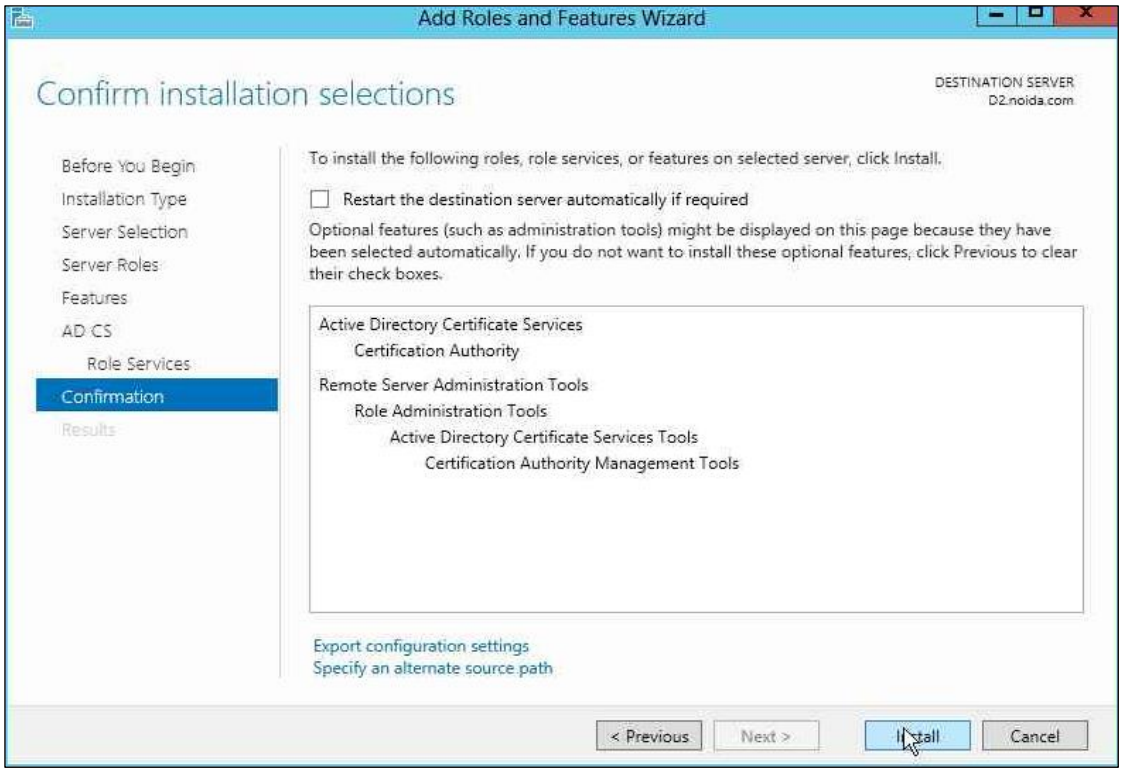


11. Click **Next** to continue.

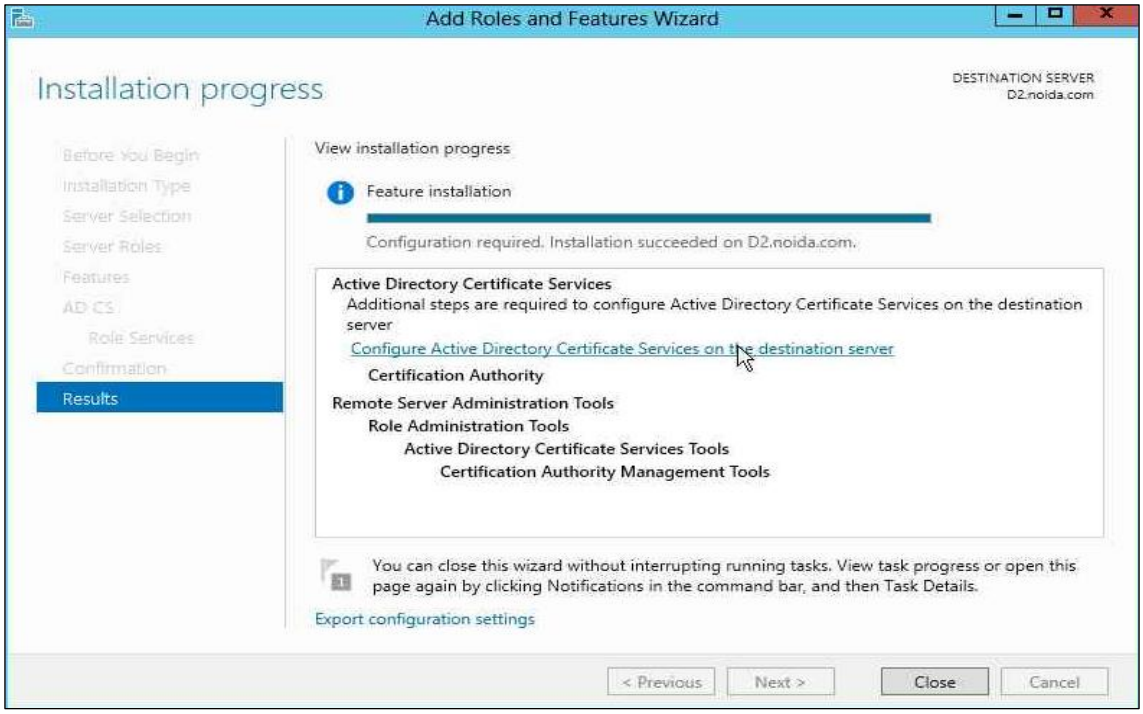
12. Select the **Certification Authority** check box from the **Role services** list and click **Next**.



13. Click **Install.**

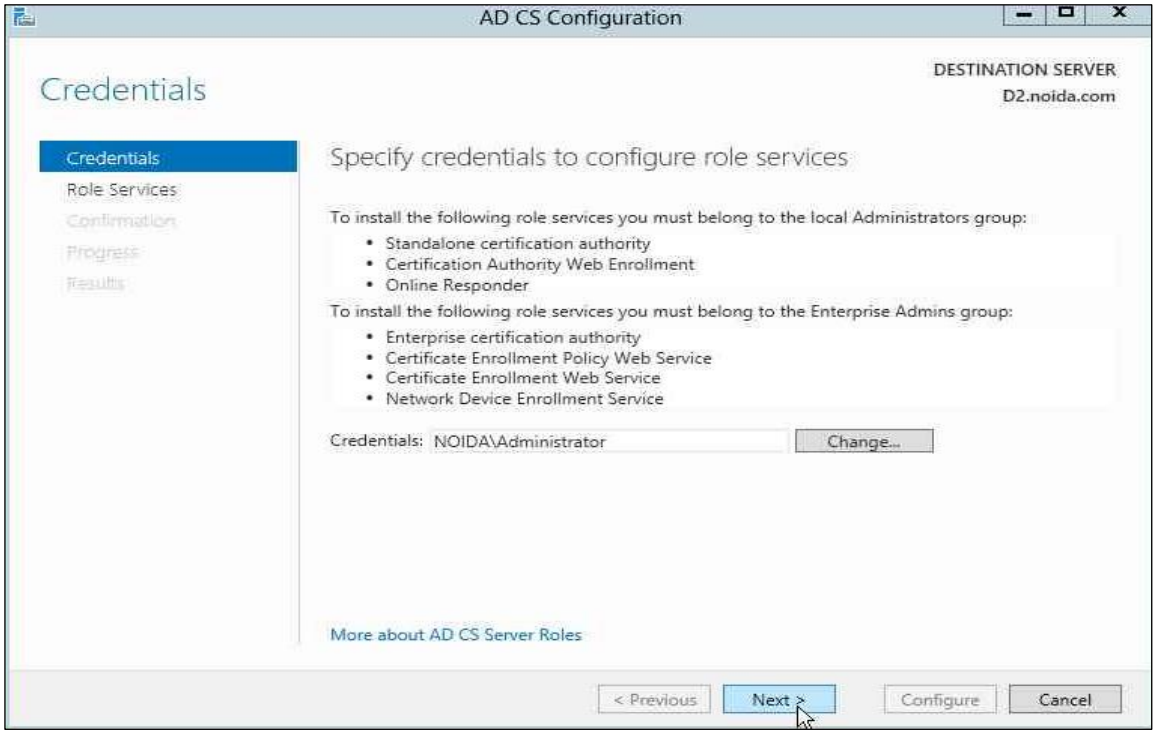


14. Once installation is complete, click the link **Configure Active Directory Certificate Services on the destination server** the AD CS Configuration wizard displays.



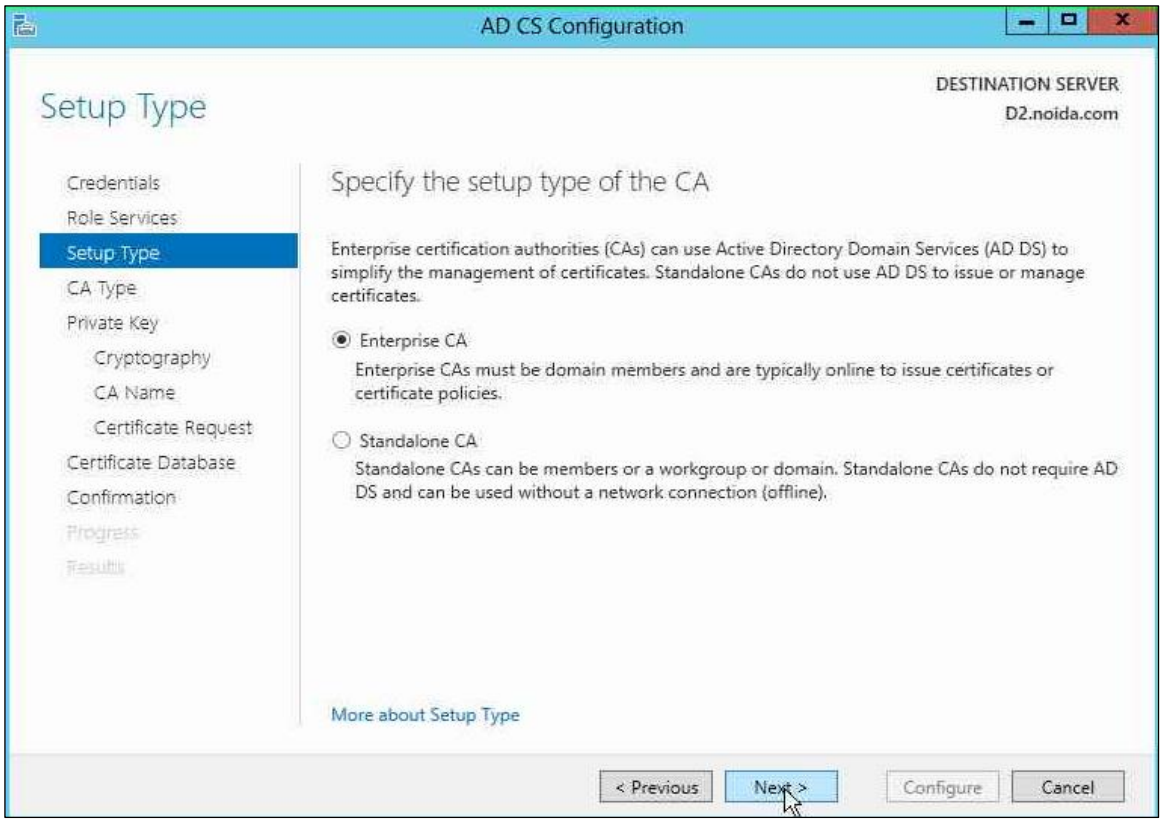
To configure the AD CS Role

1. On the **Credentials** page of the AD CS Configuration wizard click **Next** to continue.

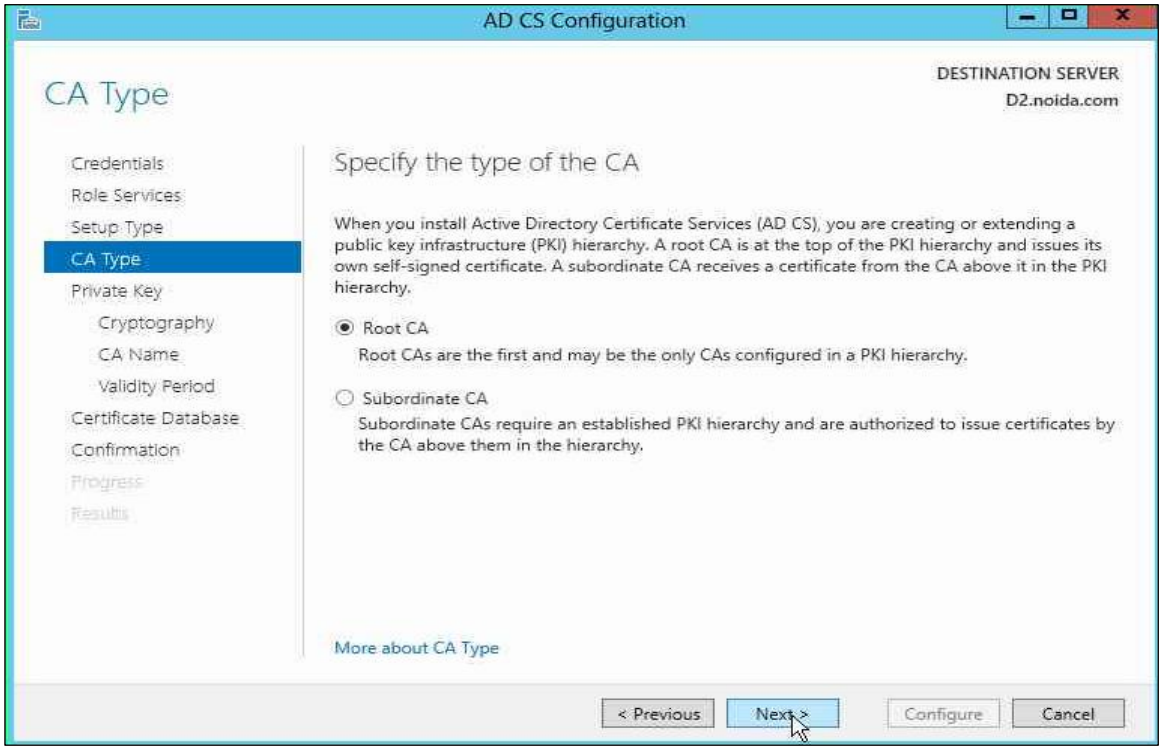


2. Select the **Certification Authority** check box and click **Next**.

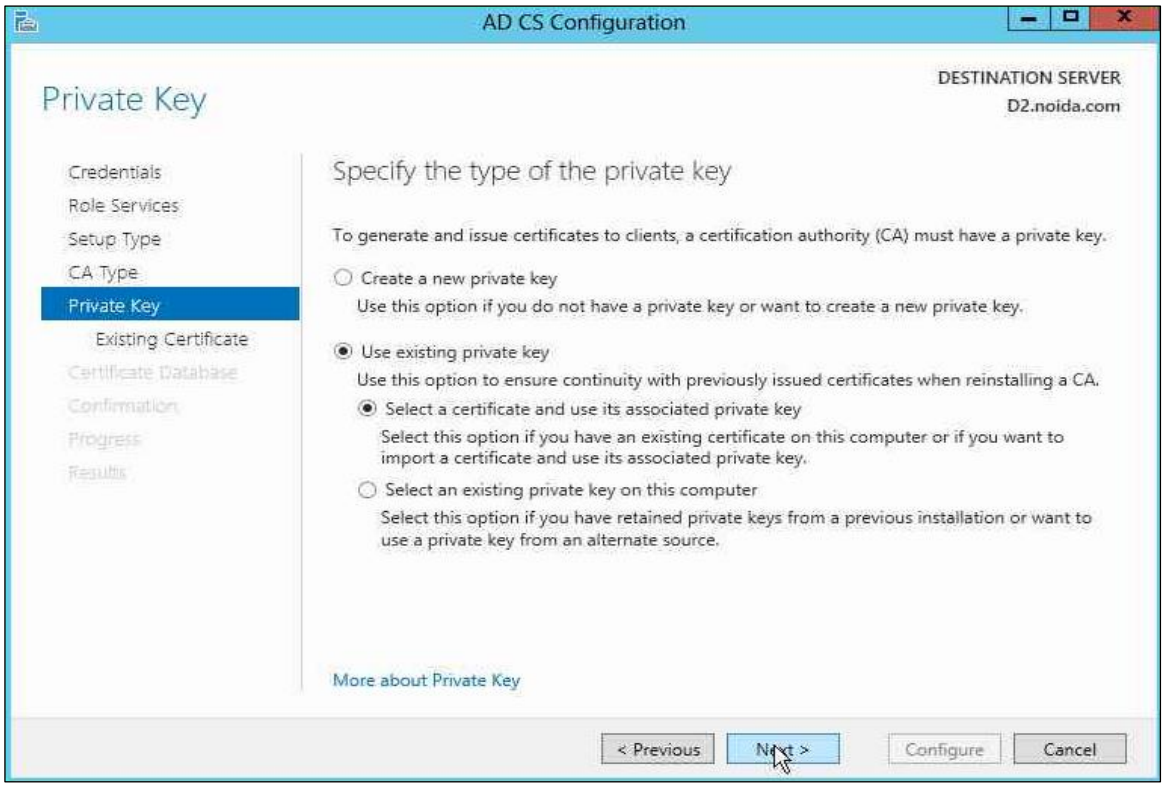
3. Select **Enterprise CA** as **Setup Type** and click **Next**.



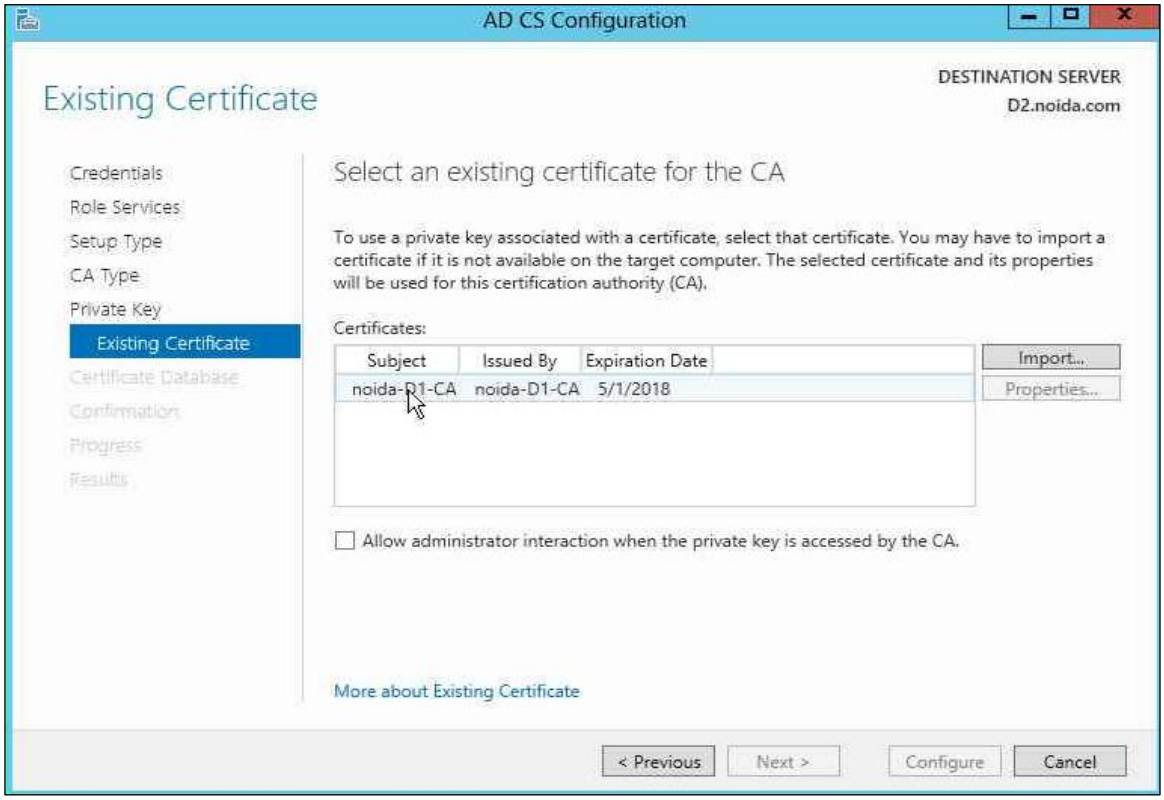
4. Select **Root CA** as type of CA and click **Next**.



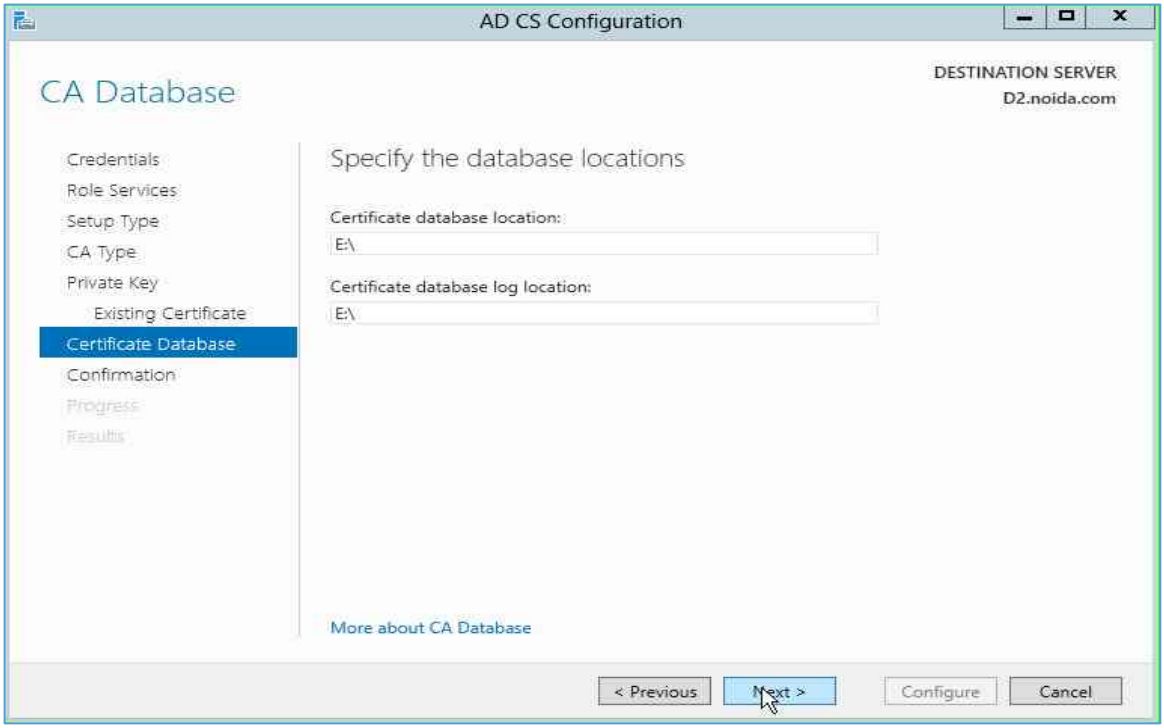
5. Select the **Use existing private key** radio button and choose the option **Select a certificate and use its associated private key** and click **Next**.



6. Select the CA certificate that was generated on the first node and click **Next**.

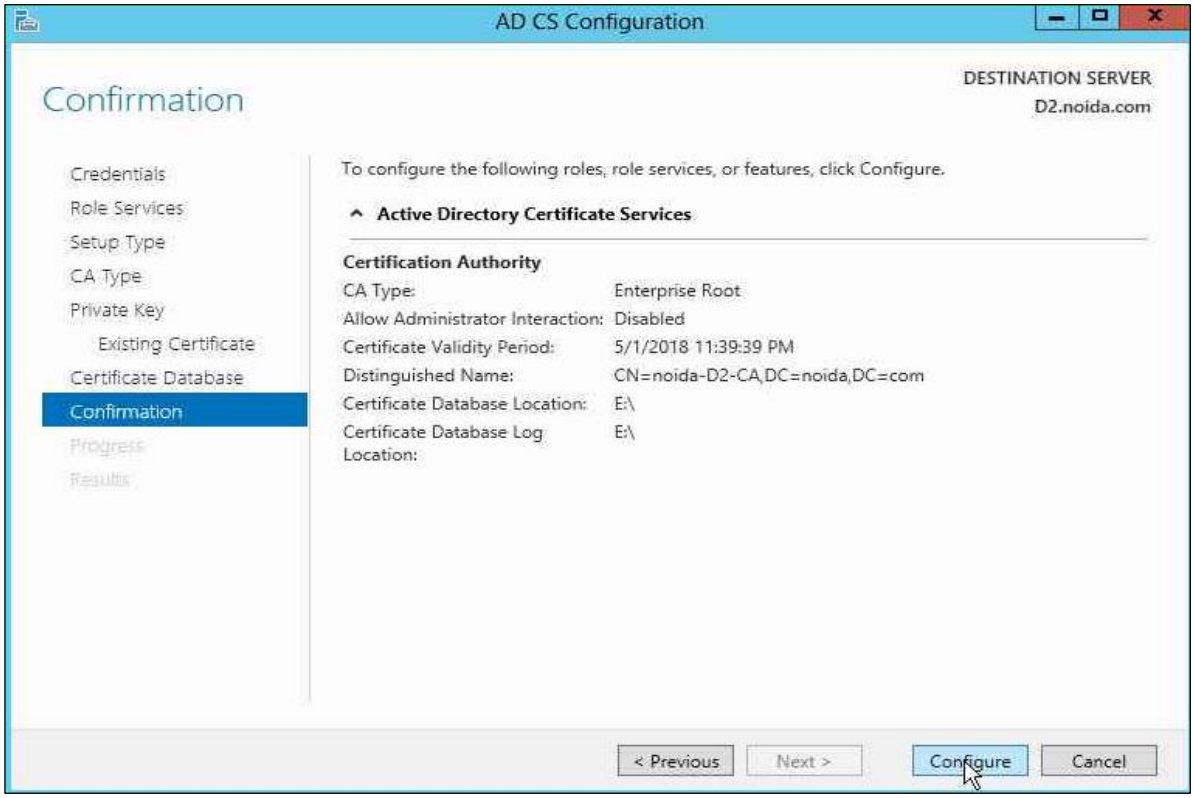


7. Change the default paths for the database log location. Click **Next** to continue.



8. A dialog box displays stating that an existing database was found displays, click **Yes** to overwrite.

9. On the Confirmation page click **Configure**.



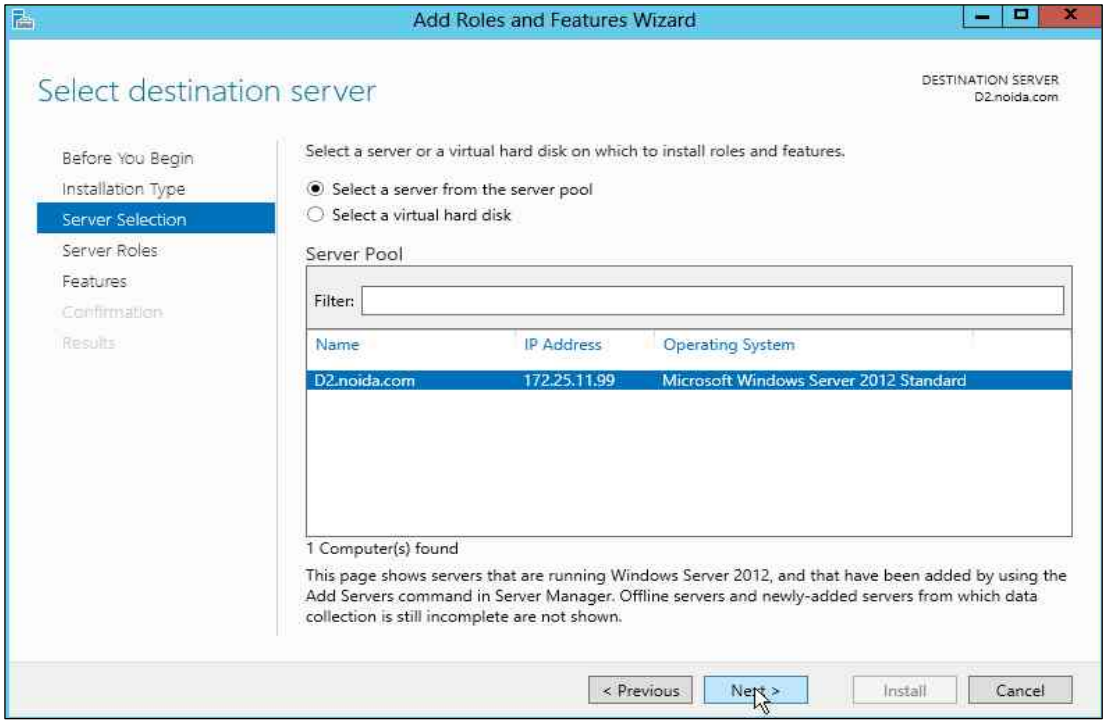
10. Click **Close** to finish the **Role** installation.
11. Log off from the second cluster node.

Set up the Failover Cluster feature on the cluster nodes

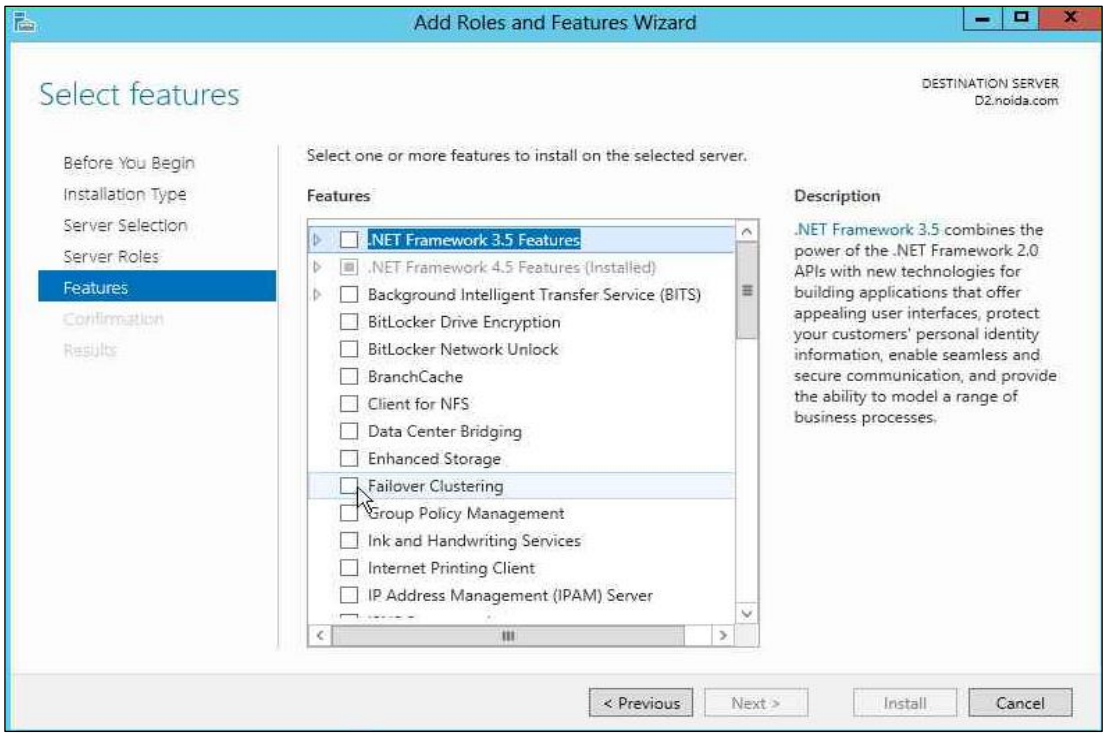
Repeat the following steps on each node of the cluster nodes:

1. Log on to the cluster node with local administrator permissions.
2. Open **Server Manager** under **Configure this Local Sever** and click **Add Roles and Features**.
3. The **Add Roles and Features Wizard** displays.
4. Click **Next**.
5. Select the **Role-based or feature-based installation** radio button and click **Next**.

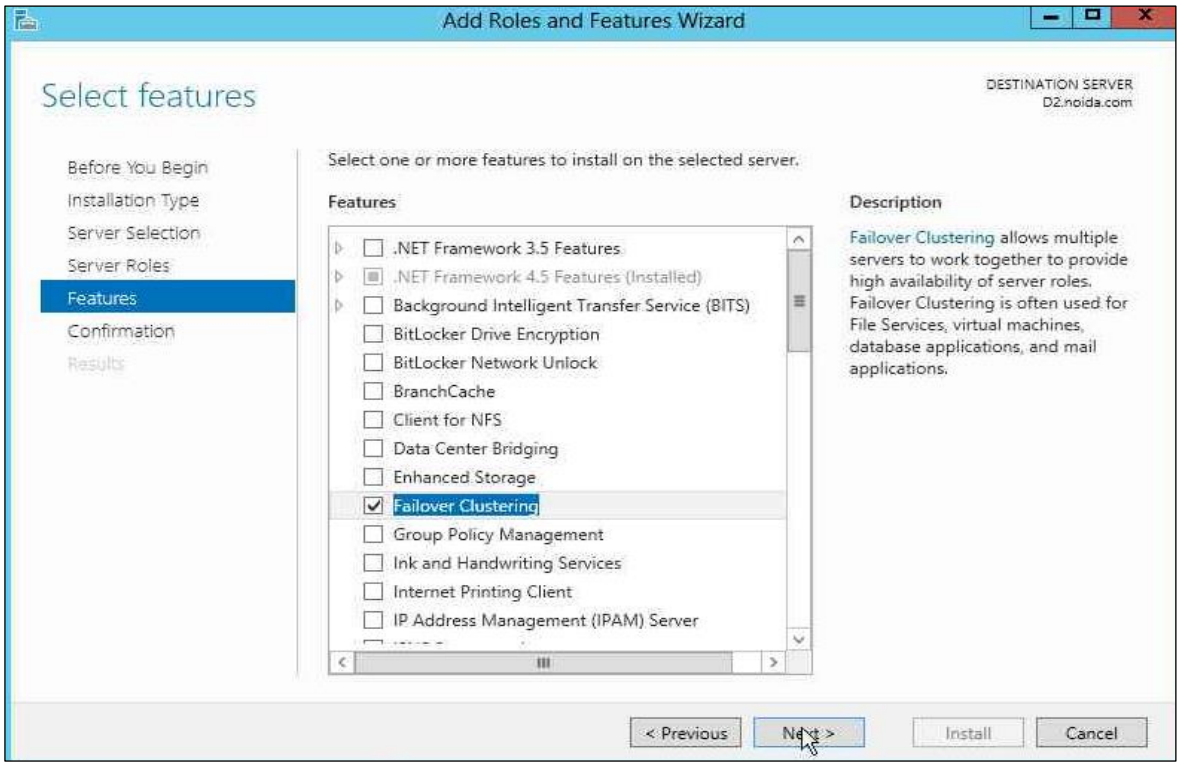
6. Select the **Select a server from the server poo**l radio button option and from **Server Pool** select your server.



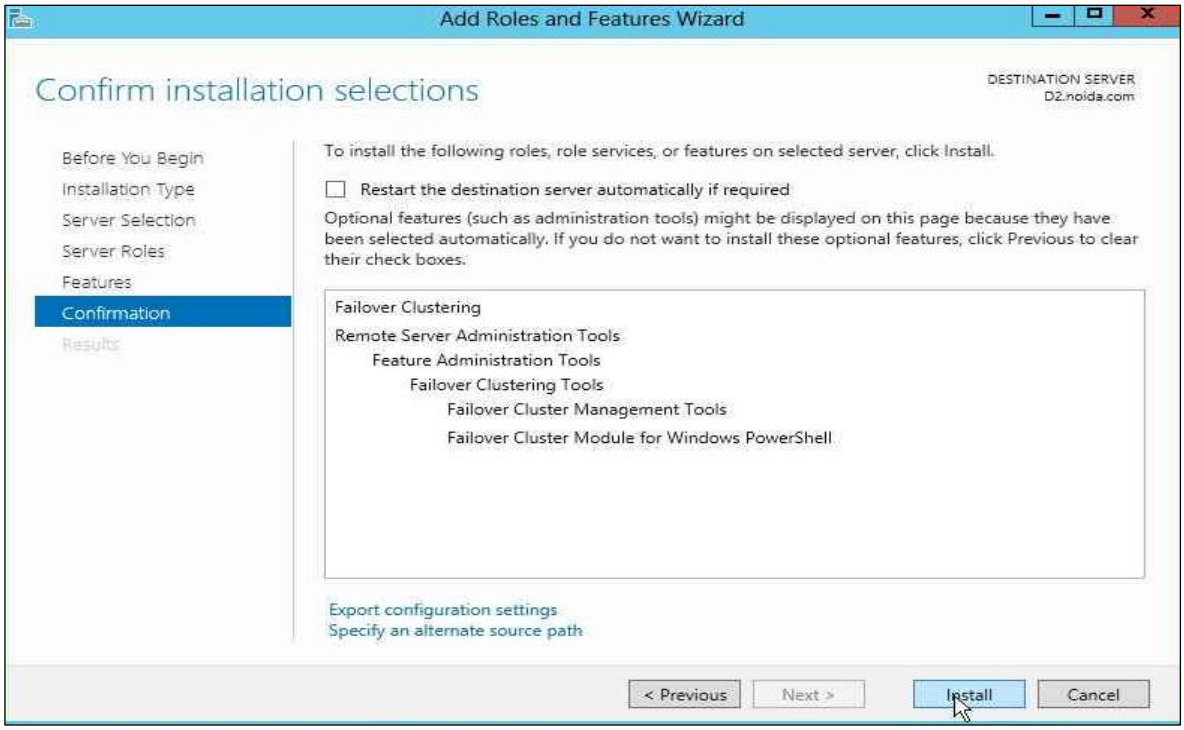
7. Click **Next** twice. From the list of available features, select the **Failover Clustering** check box and click **Next**.



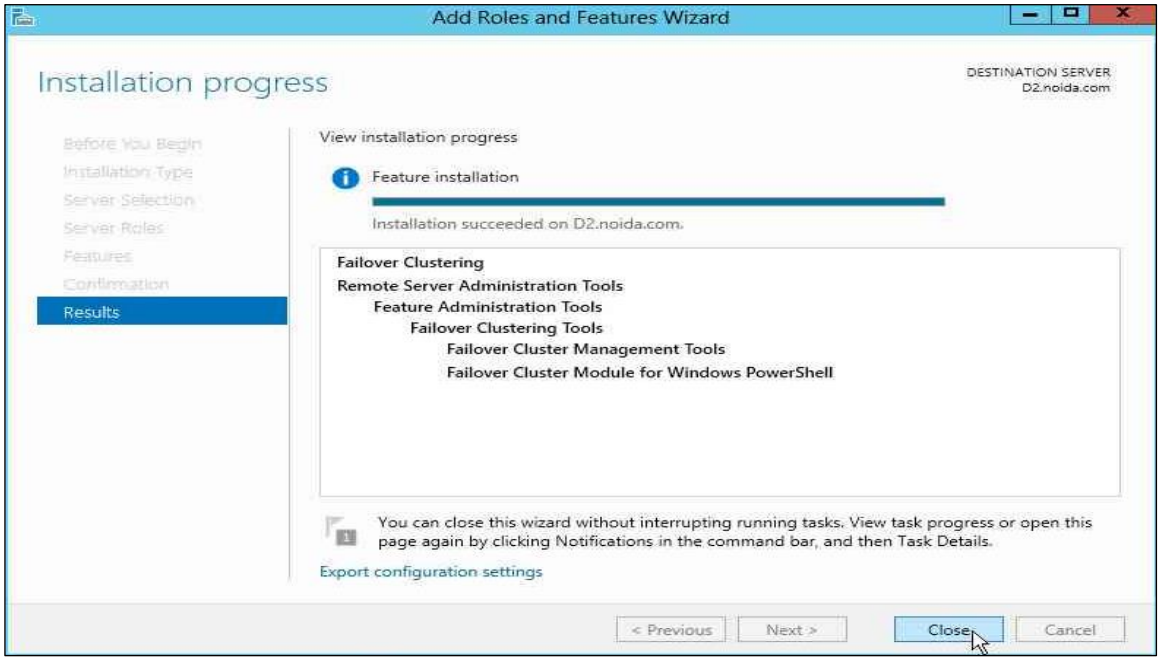
8. A pop up displays stating **Add features that are required for Failover Clustering**, click the **Add Features** button.
9. Click **Next**.



10. Click **Install**.



11. Click **Close**.

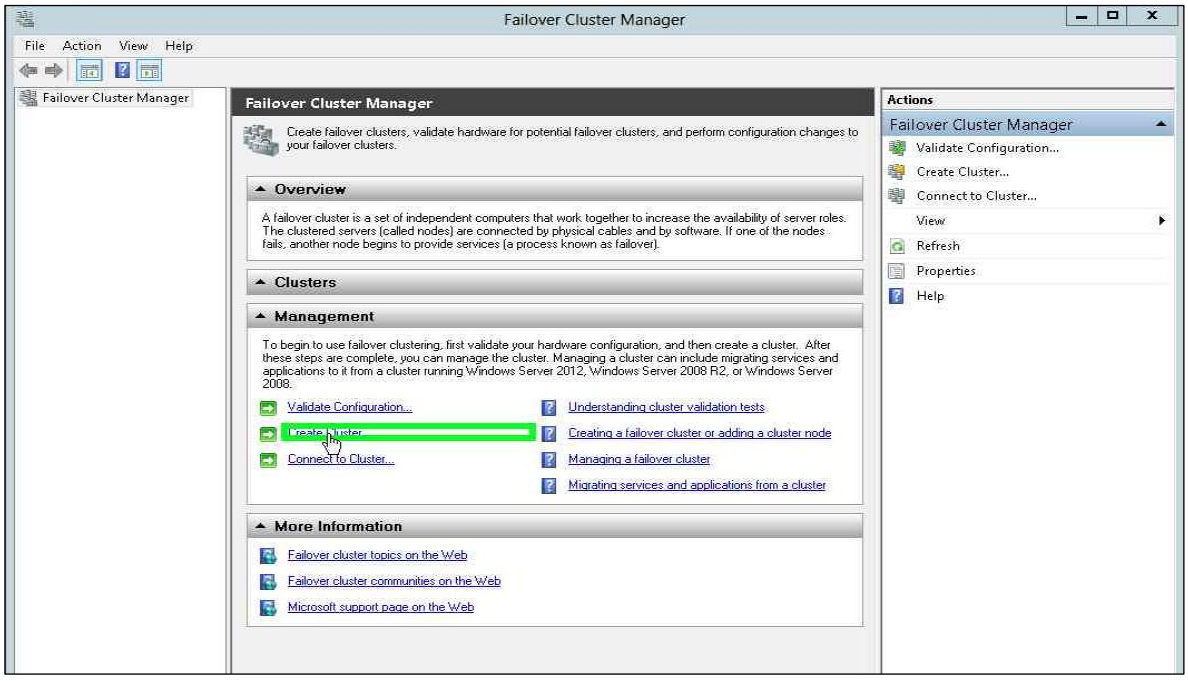


Create a Failover Cluster

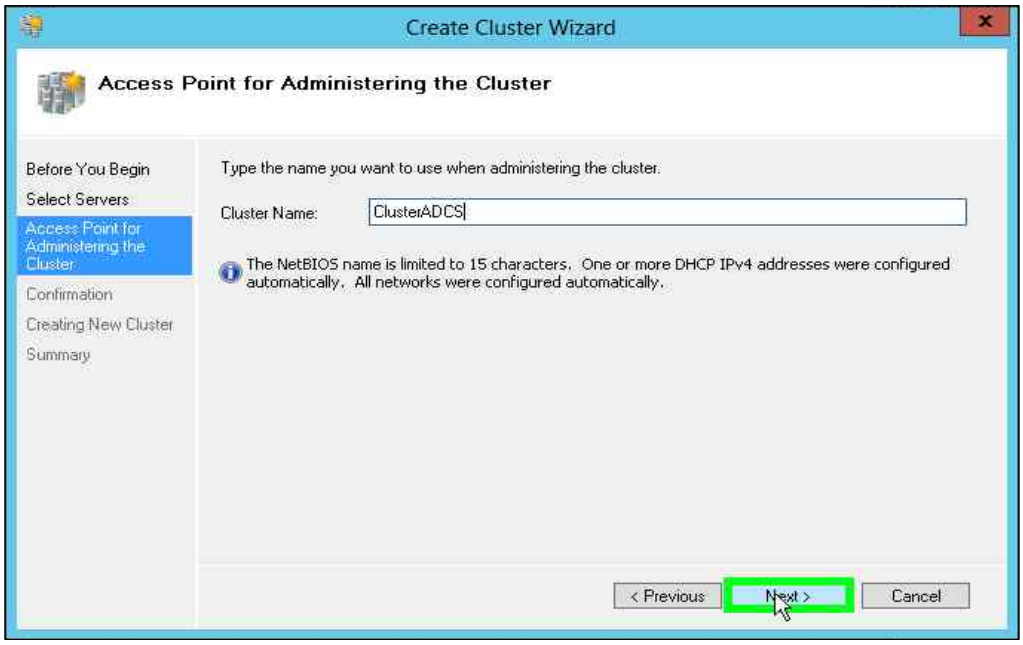
To create a Failover Cluster:

1. Log on to the cluster node where the shared storage is attached and available.

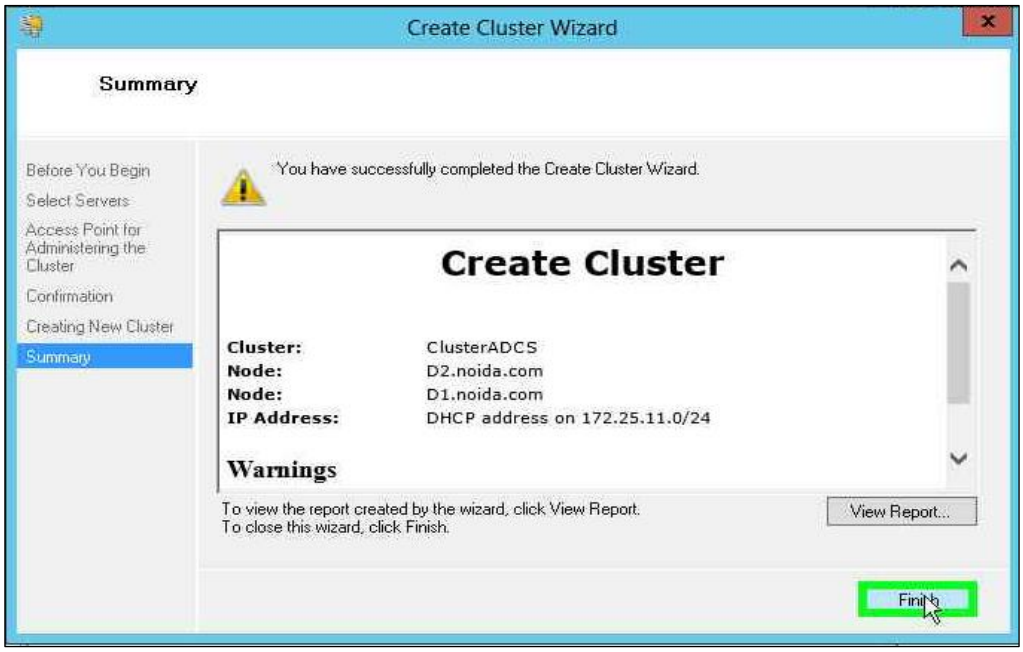
2. Open **Server Manager**, Click **Tools** and select **Failover Cluster Manager**. From the **Action** menu, click **Create a Cluster**.



3. On the **Before You Begin** page, click **Next**.
4. Enter the cluster node name (computer name) of the first cluster node in the **Enter Server Name** field and click **Add**.
5. Enter the cluster node name of the second cluster node in the **Enter Server Name** field and click **Add**.
6. Click **Next** to continue.
7. Enter the **Cluster Name** and click **Next** until you reach the Summary page. .



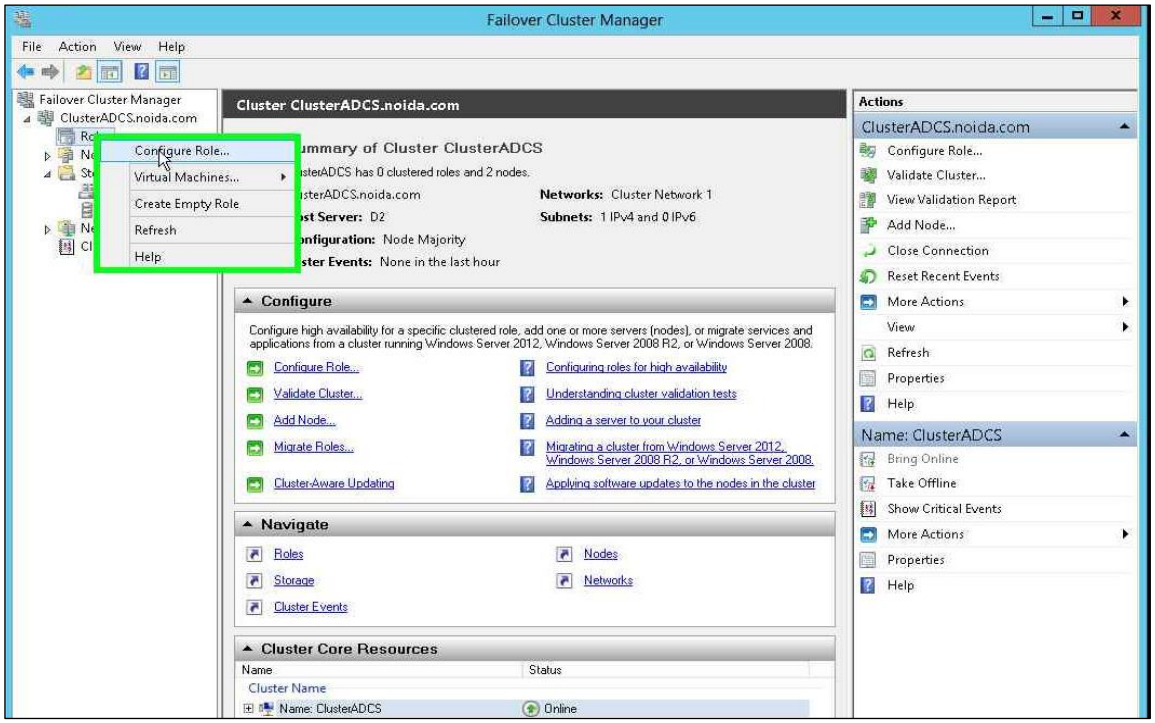
8. Verify the cluster configuration is appropriate and click **Finish**.



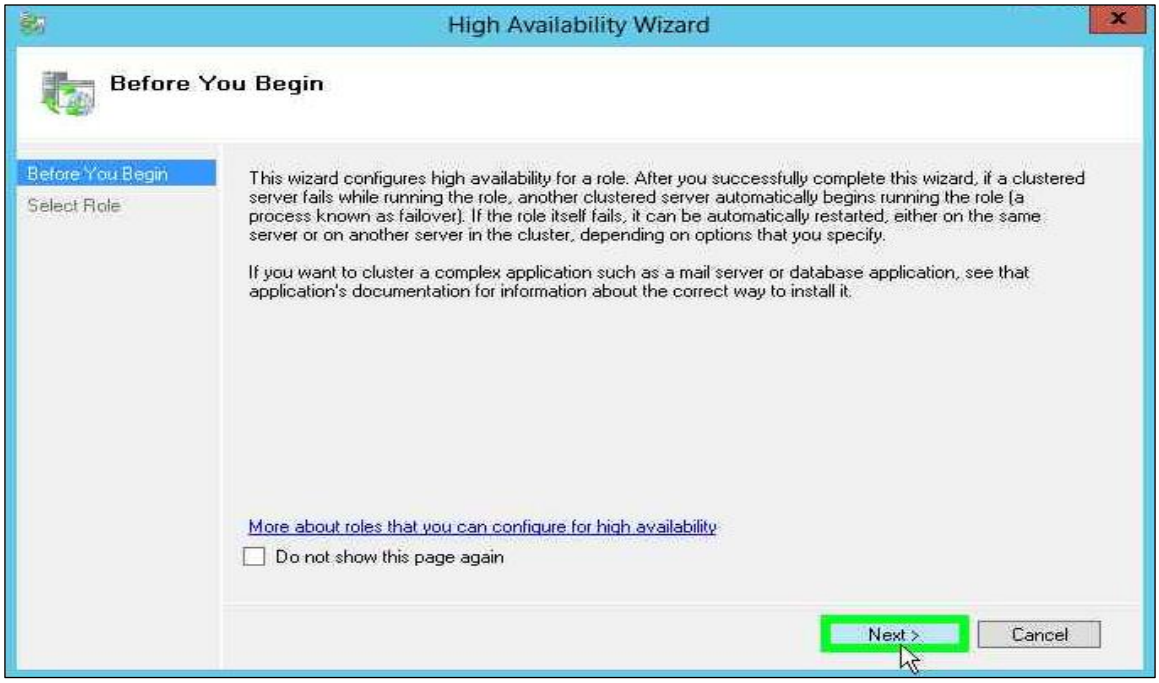
Configure AD CS Failover Cluster

You need to configure an AD CS Failover configuration for certificate services. To configure the AD CS failover cluster:

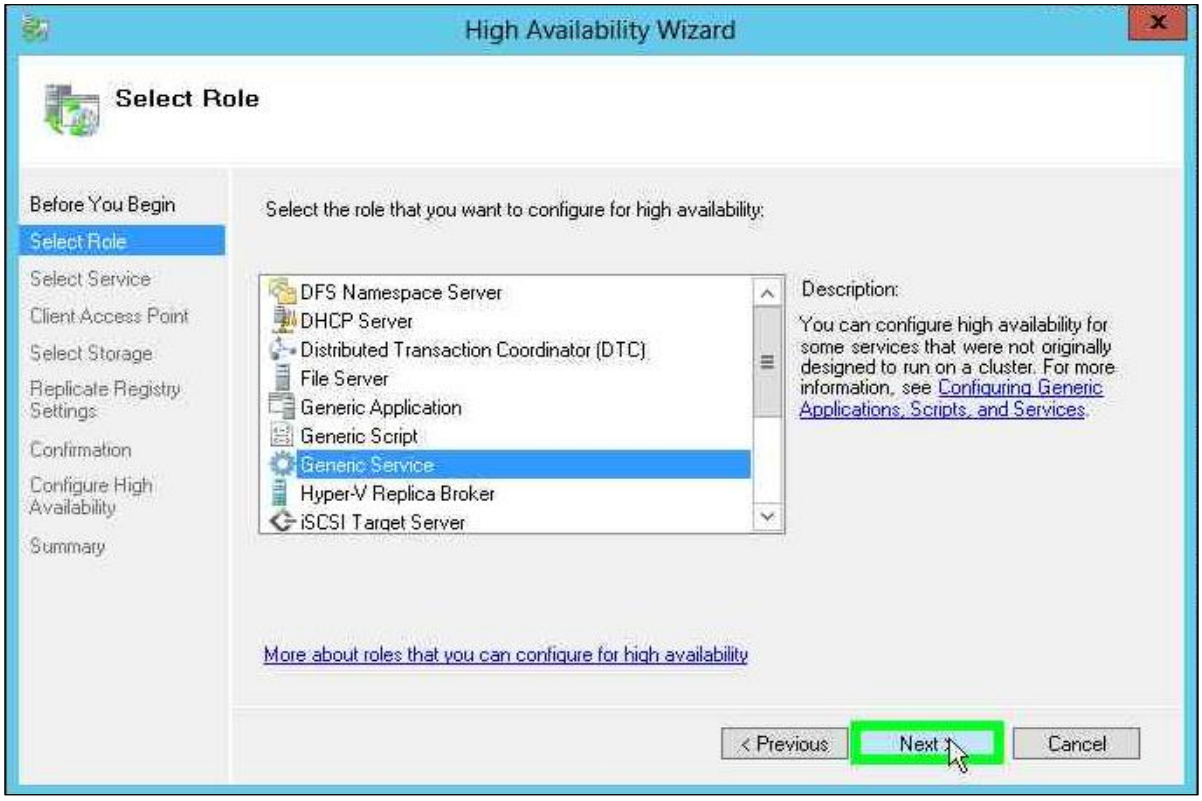
1. In the **Failover Cluster Management** snap-in, right-click **Role** and select **Configure Role**.



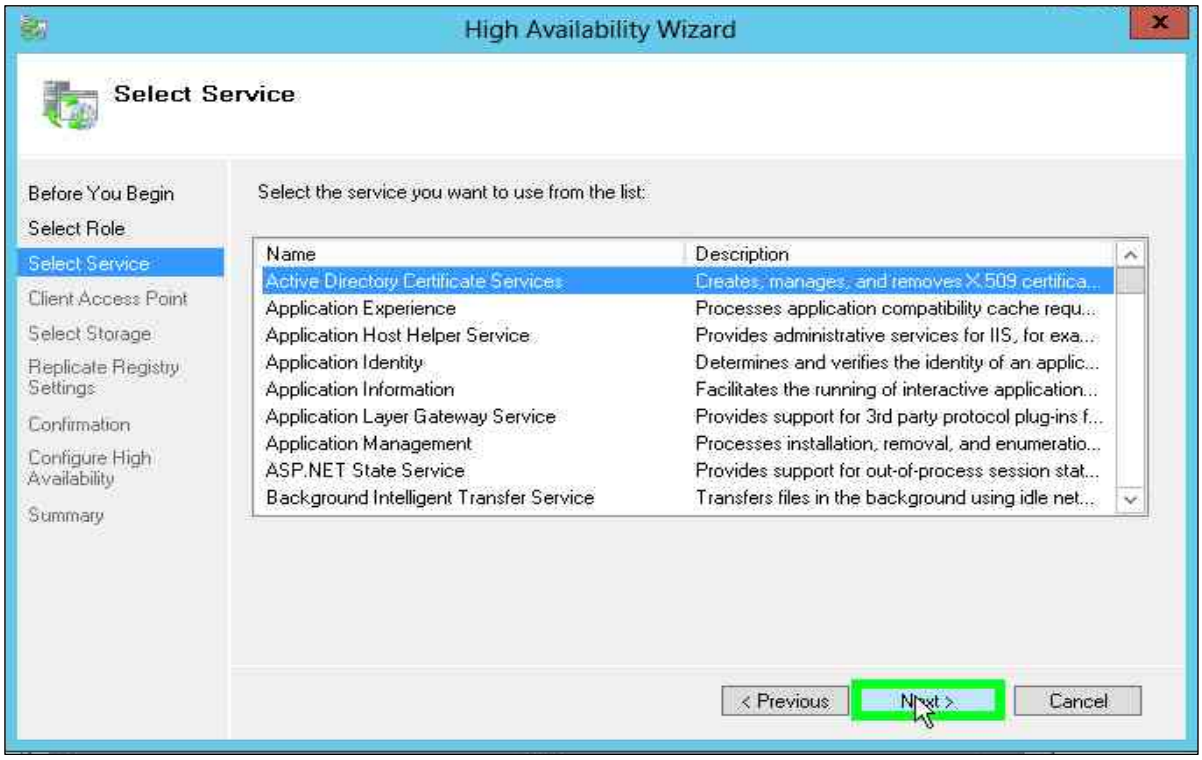
2. On the **Before you Begin** page, click Next.



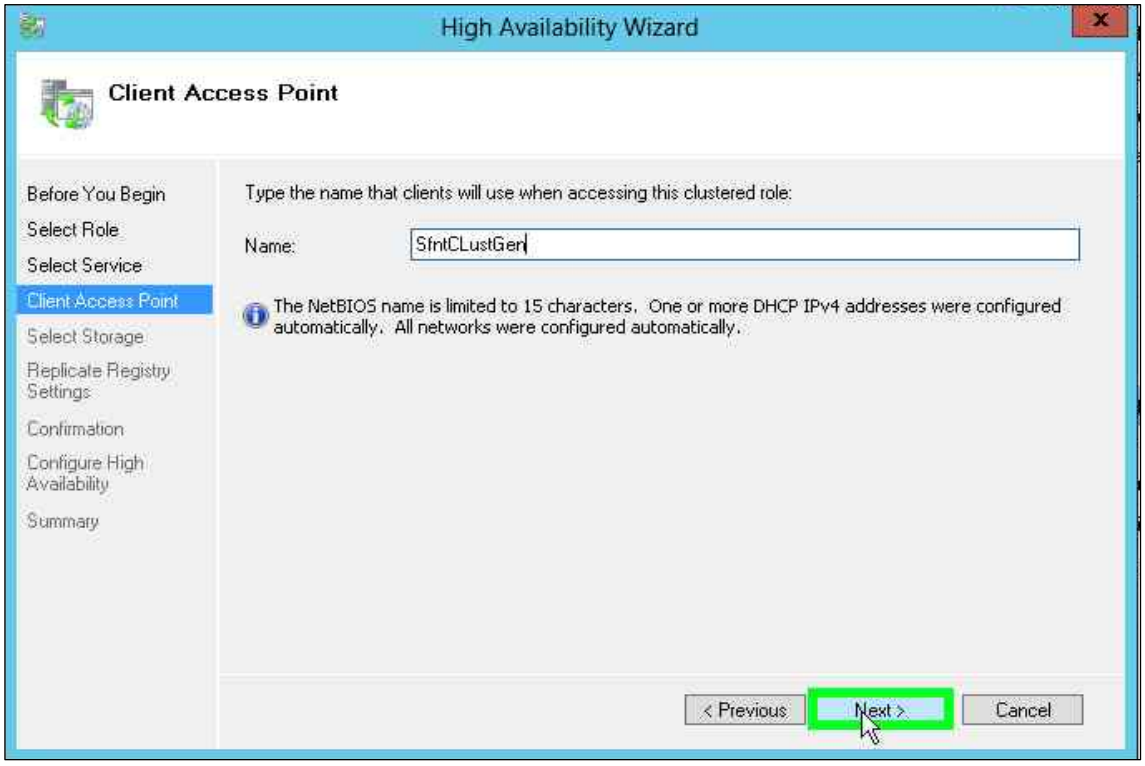
3. From the role list, select **Generic Service** and click **Next**.



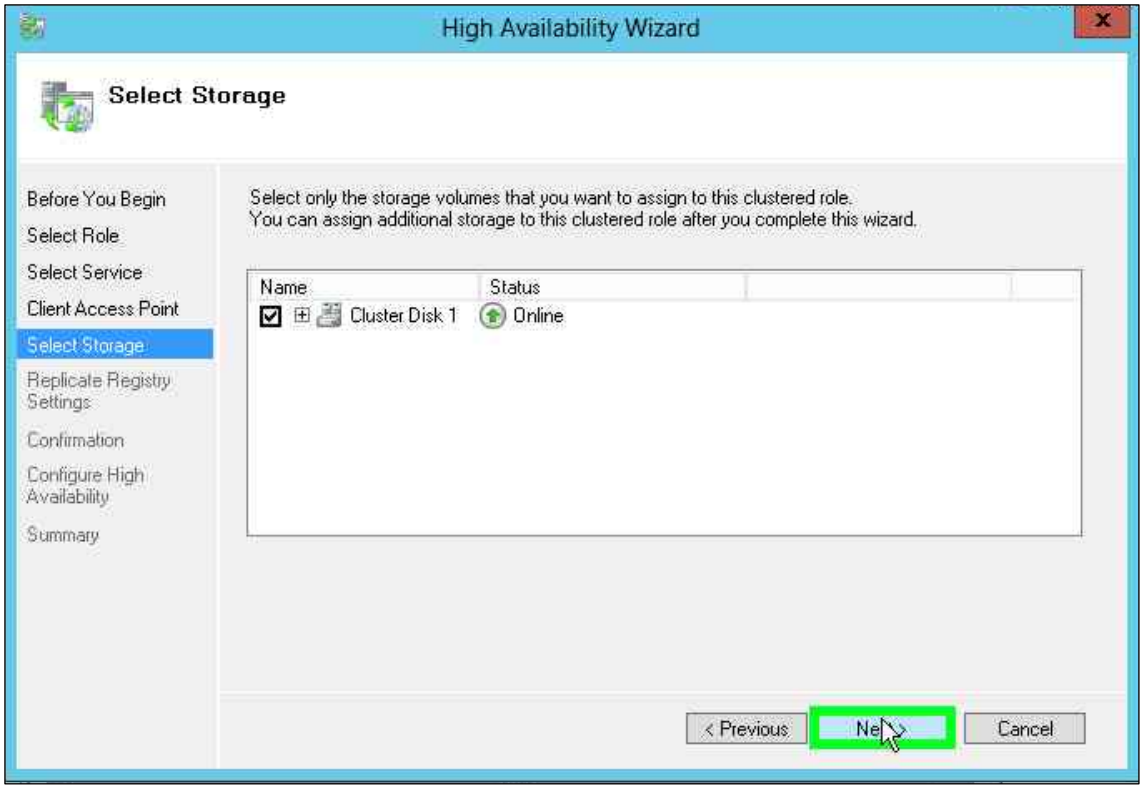
4. From the service list, select **Active Directory Certificate Services** and click **Next**.



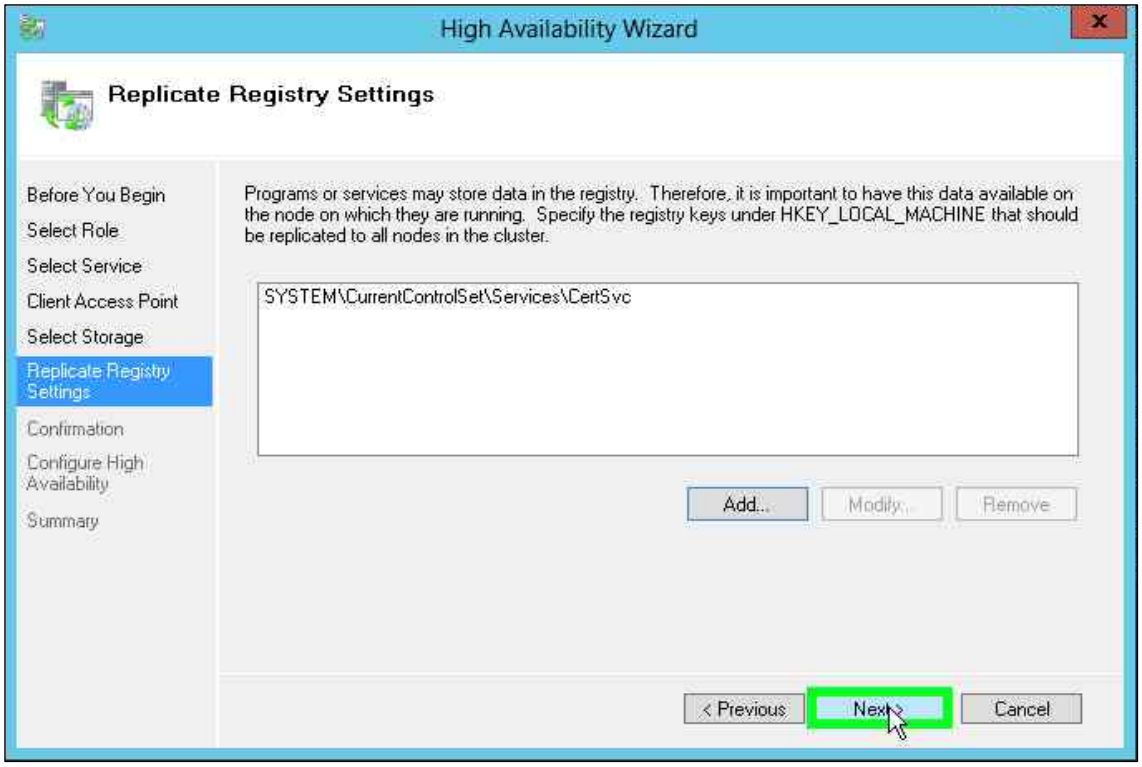
5. On the Client Access Point page enter the service name in the **Name** field and click **Next**.



6. Select the disk storage that is still mounted to the node and click **Next**.

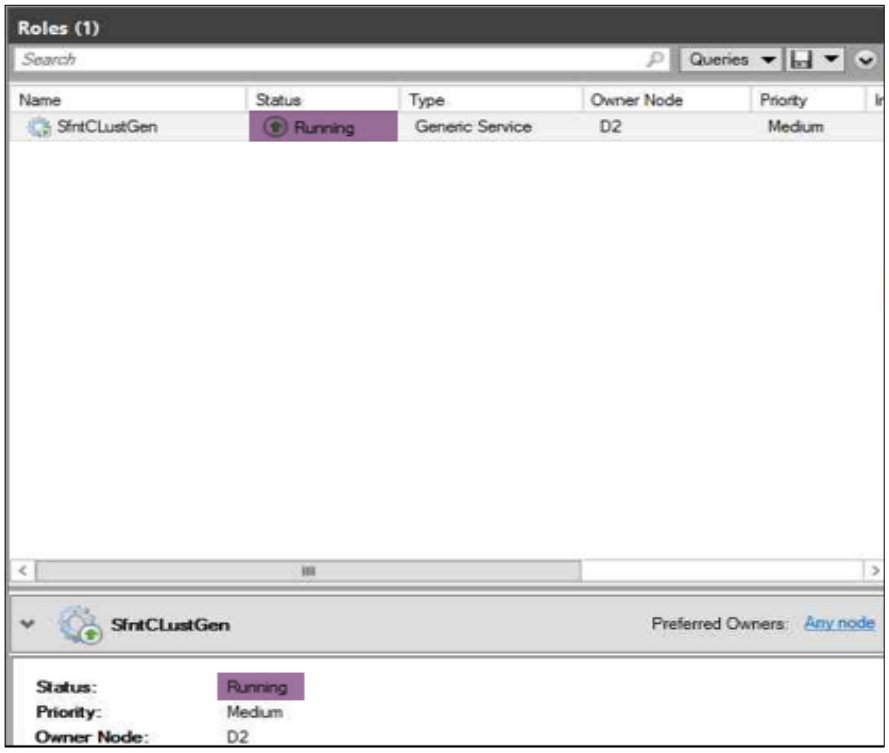


7. Configure a shared registry hive, click the **Add** button, enter "**SYSTEM\CurrentControlSet\Services\CertSvc"** and click **OK**.



8. Click **Next** on the Confirmation page.

9. Click **Finish** to complete the failover configuration for certificate services.
10. Open the Failover Cluster Manager and verify that the newly created service's **Status** is in the **Running** state.



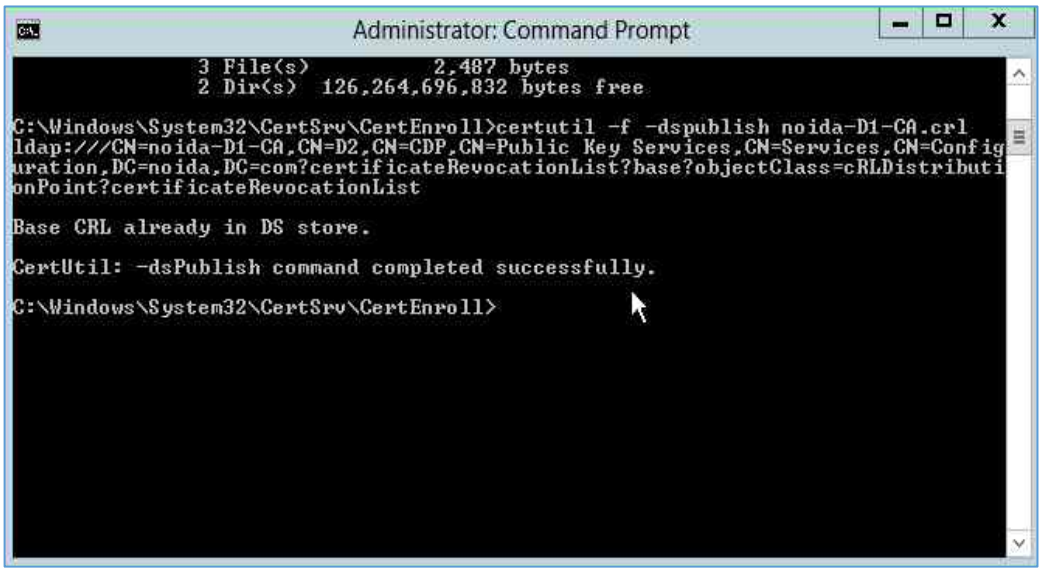
Create CRL objects in the Active Directory

The default AD permissions for the CA cluster do not permit publishing the CRL into the Active Directory. Alternatively, the user can create a CRL container to publish the CRL into the Active Directory.

You must use the certutil command with the –f option to create the CRL container. To create CRL objects in the Active Directory:

1. Log on to the active cluster node with enterprise permissions.
2. Click the **Start** button, point to **Run**, type **cmd**, and then click **OK**.
3. At the command line, type `cd %WINDIR%\System32\CertSrv\CertEnroll` and press **Enter**.

4. To publish the CRL into Active Directory, type `certutil -f -dspublish {CRLfile}`.

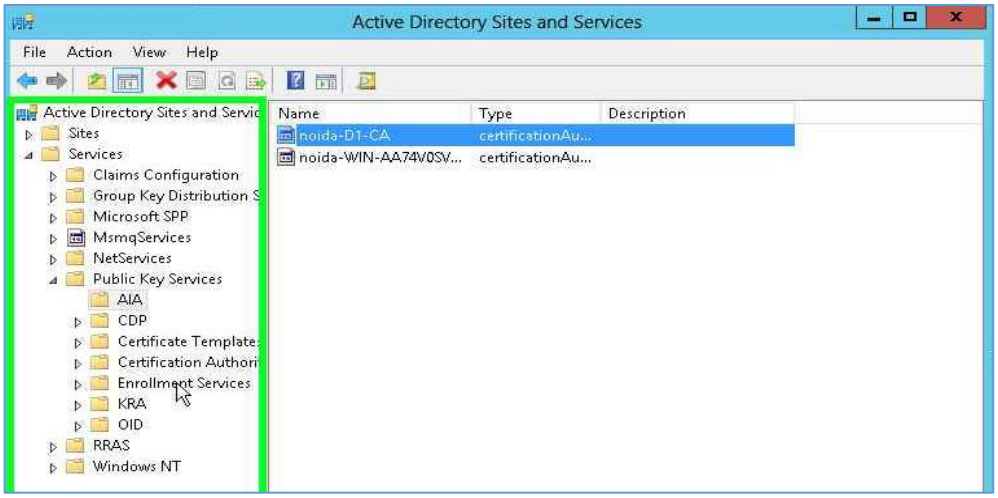


Modify CA configuration in Active Directory

The AIA object in Active Directory stores the CA's certificate. You can enable both the cluster nodes to update the CA certificate when required.

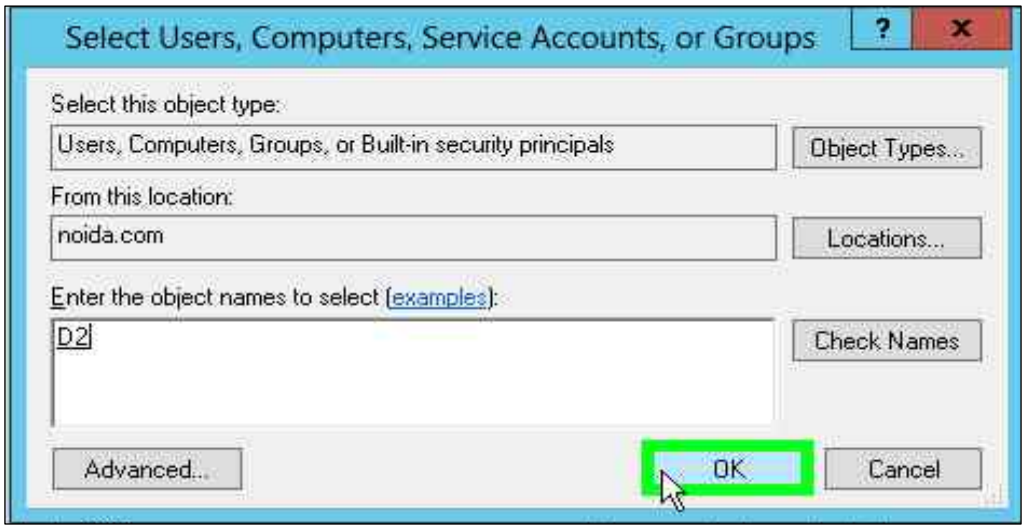
You can perform the following tasks from any computer in your Active Directory configuration where the Active Directory Sites and Services snap-in and ADSIEDIT is installed. To modify the CA configuration in the Active Directory:

1. Log on to the computer with enterprise permissions.
2. Click the **Start** button, point to **Run**, type **dssite.msc** and then click **OK**.
3. Select the top node in the left pane. In the **View** menu, select the **Show services** node.
4. In the left pane, expand the **Services** and **Public Key Services** and select **AIA**.

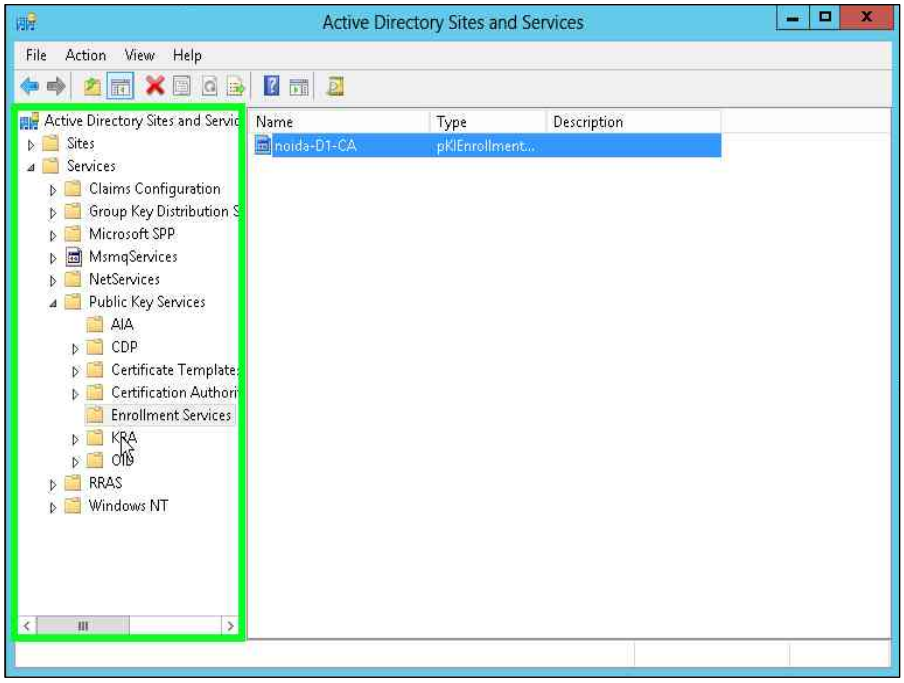


5. In the middle pane, select the CA name as it shows in the **Certification Authority** MMC snap-in.
6. From the **Action** menu select **Properties**. Click the **Security** tab and select **Add…**.

7. Click **Object Types** and select the **Computers** check box and click **OK**.
8. In the **Enter the object names to select** field enter the computer name of the second cluster node. Click **OK**.



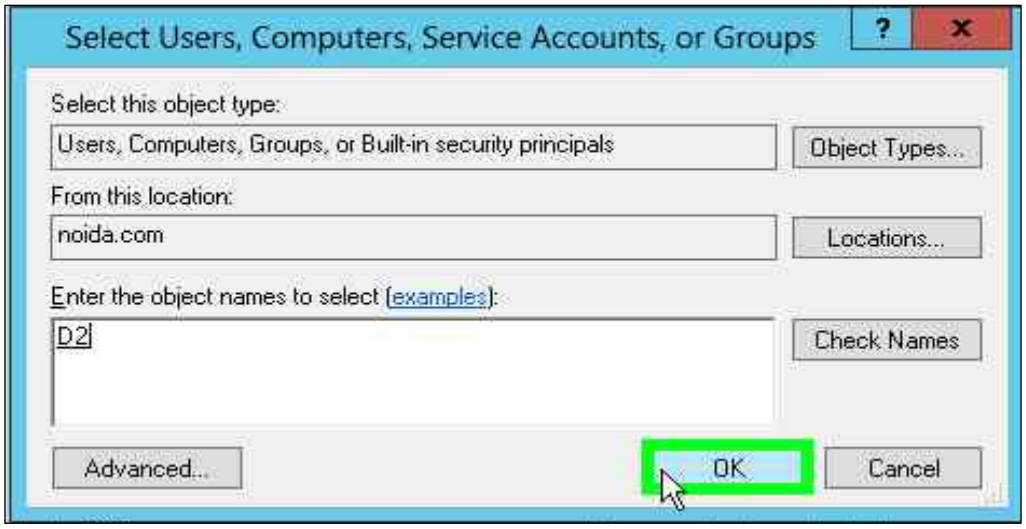
9. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.
10. Click **OK**.
11. In the left pane, select **Enrollment Services**.



12. In the middle pane, select the CA name.
13. From the **Action** menu, select **Properties** click the **Security** tab and select **Add…**.

14. Click **Object Types** and select the **Computers** check box and click **OK**.

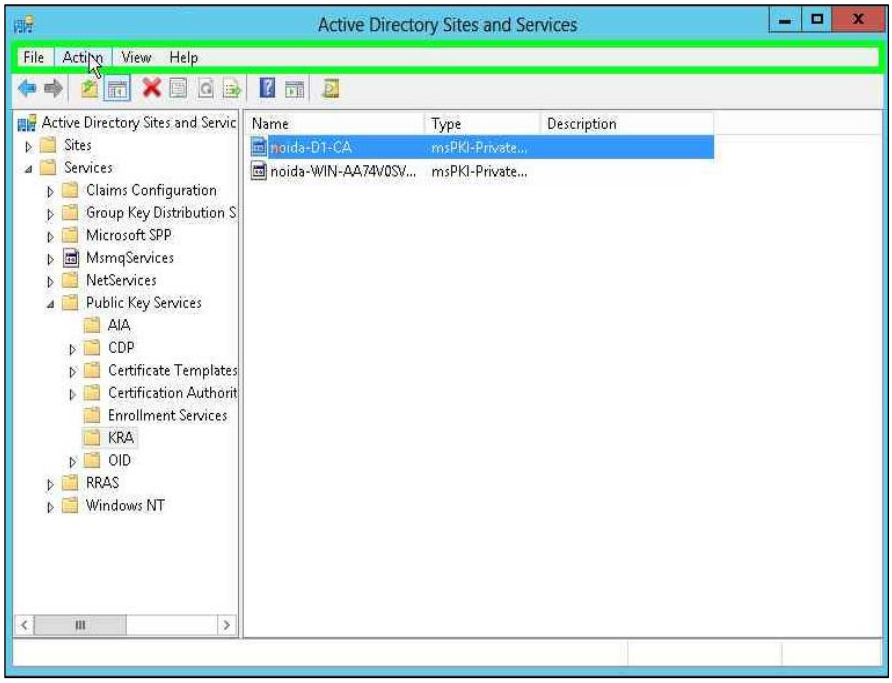
15. In the **Enter the object names to select** field enter the computer name of the second cluster node. Click **OK**.



16. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.

17. Click **OK**.

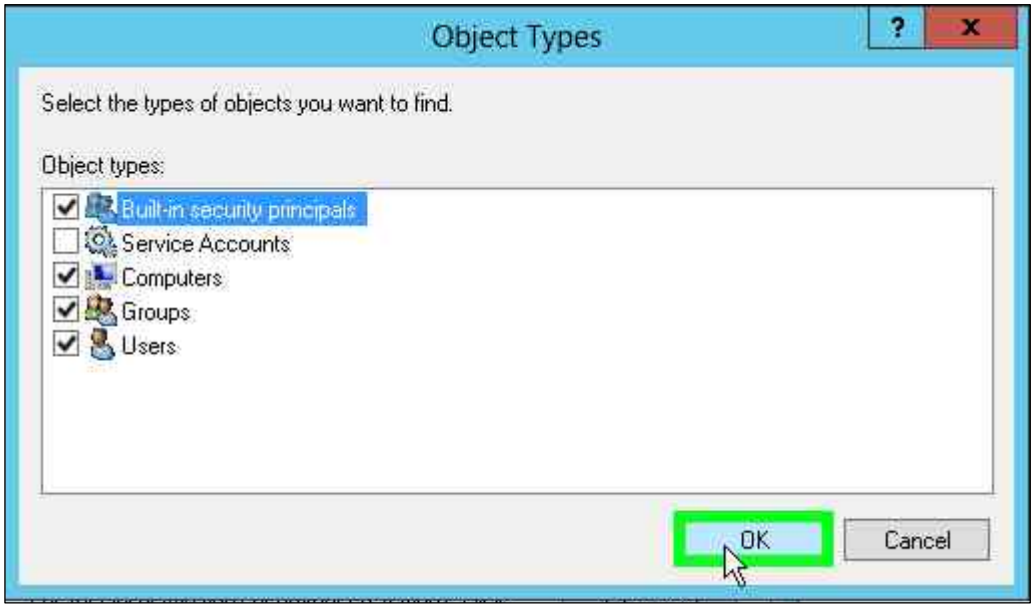
18. In the left pane, select **KRA**.



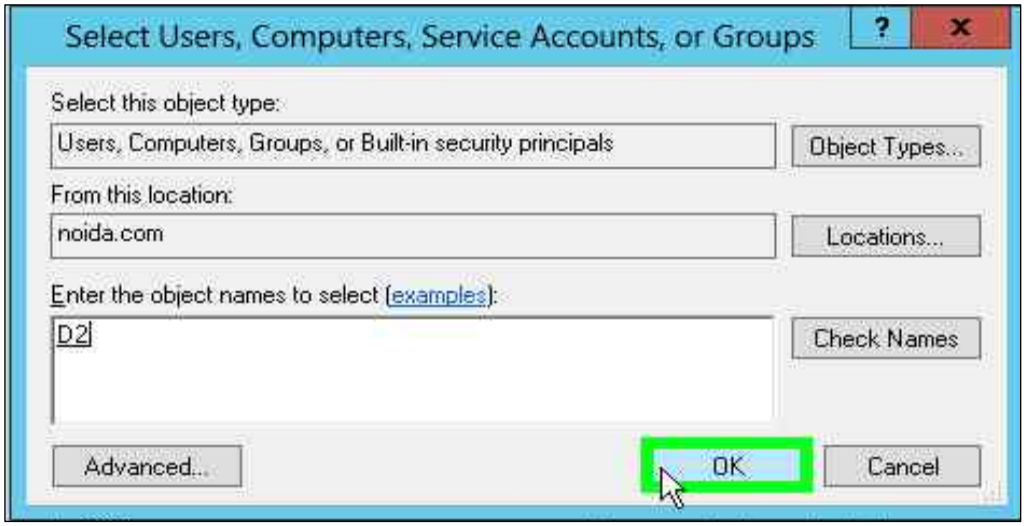
19. In the middle pane, select the CA name.

20. From the **Action** menu select **Properties** click the **Security** tab and select **Add…**.

21. Click **Object Types** and select the **Computers** check box and click **OK**.



22. Type the computer name of the second cluster node as object name and click **OK**.



23. Verify that the computer accounts of both the cluster nodes have **Full Control** permissions.

24. Click **OK**.

25. Close the Sites and Services MMC snap-in.

This completes the creation of ADSC cluster with 2 cluster nodes using the keys secured on the Luna HSMs.

Migrating AD CS Cluster keys from Microsoft Software KSP to SafeNet KSP

This section explains the procedure for migrating the CA Keys used by the AD CS from the Microsoft Software Key Storage Provider to the SafeNet Key Storage Provider. After the migration is completed, the AD CS cluster will use the CA signing keys stored in the Luna HSM.

Before initiating the migration process, ensure that:

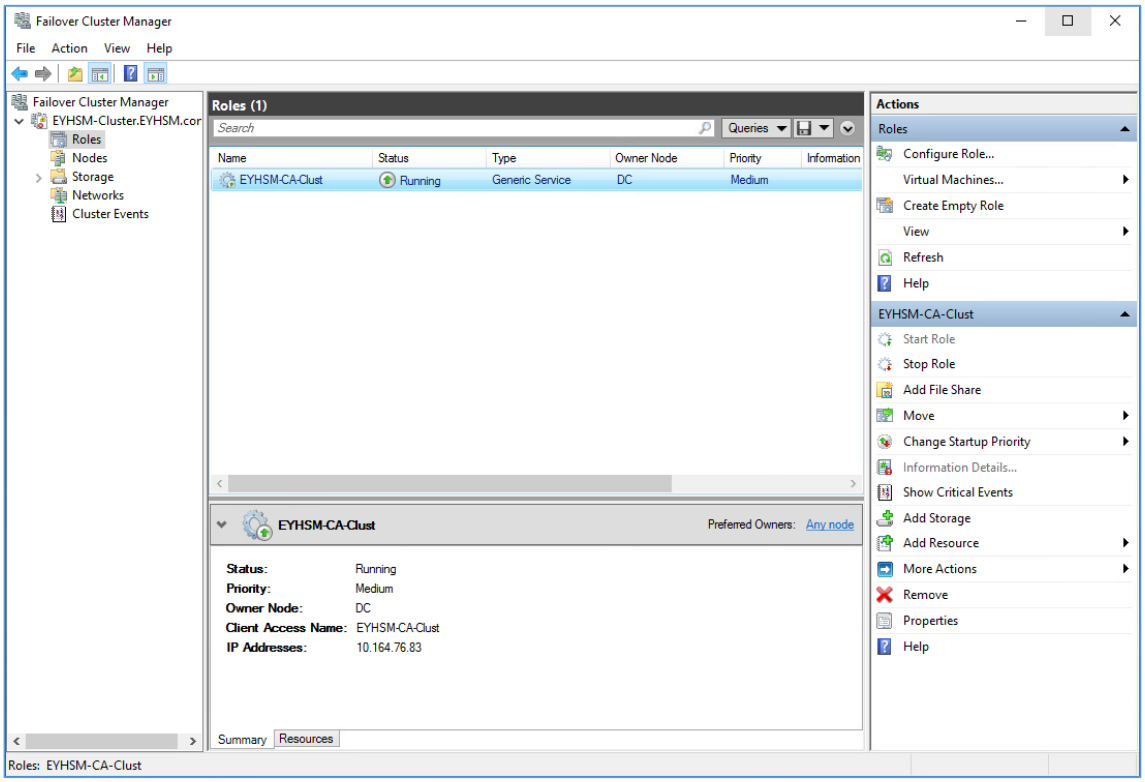
> The AD CS Cluster is currently operational using the Microsoft Software Key Storage Provider.

> The Luna Client is installed and a partition is registered on each node of the cluster.

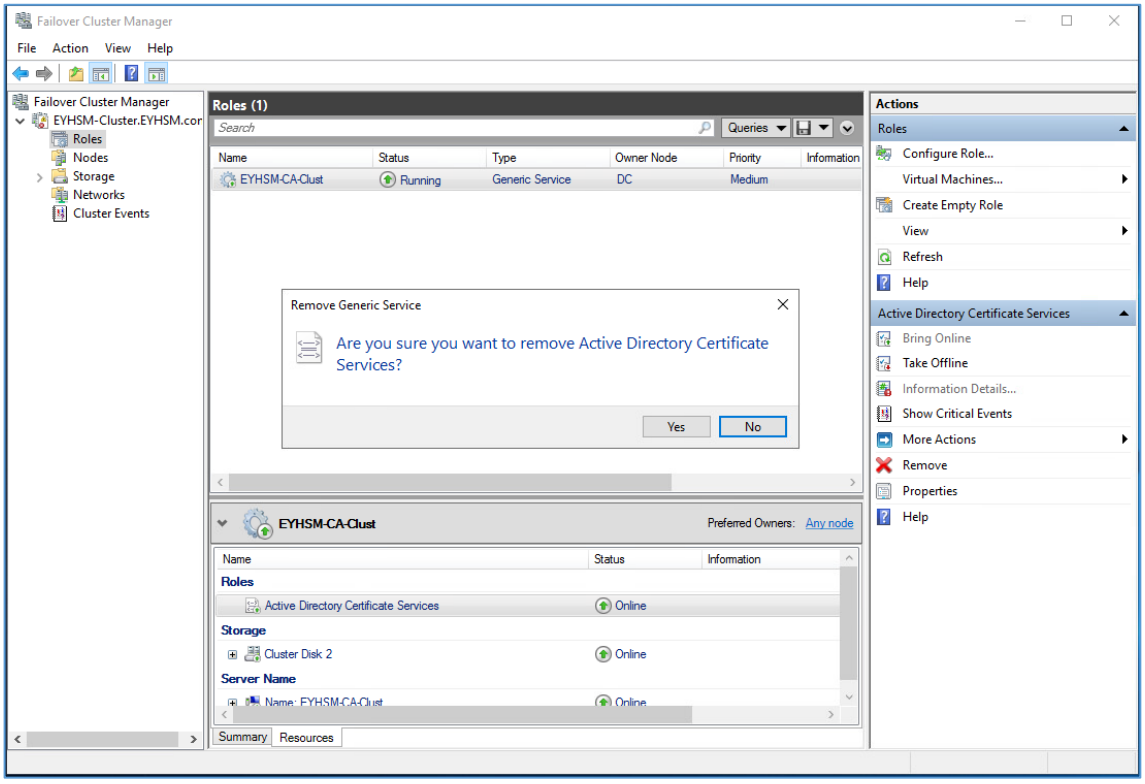
> The SafeNet KSP is registered and configured on every node of the cluster.

For migrating the AD CS Cluster from Microsoft KSP to SafeNet KSP, the CA key must be associated with the SafeNet KSP on each node of the cluster. The steps for performing the migration process are outlined below.

1. Log on to the first node of the cluster and ensure that the AD CS Cluster service is running and owned by the first cluster node where the CA keys were initially generated.



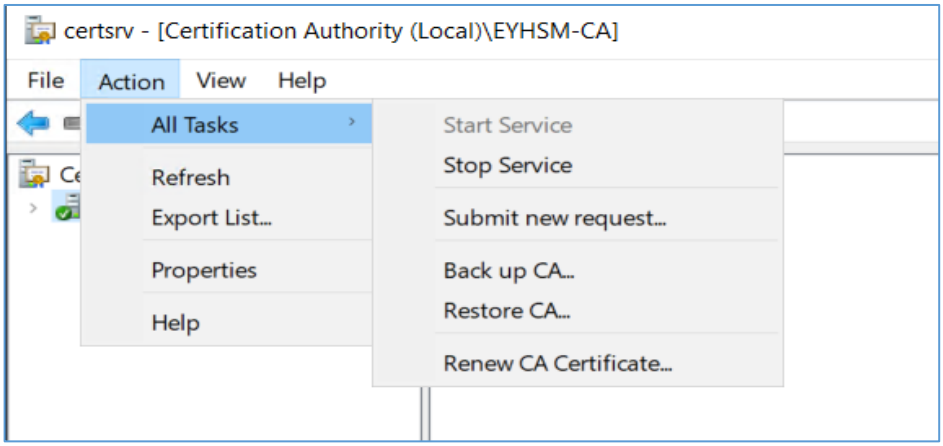
2. Navigate to the **Resources** tab, select **Active Directory Certificate Services**, and then click on **Remove** in the **Actions** pane to remove the AD CS service from the cluster. When prompted, click **Yes** to remove the service.



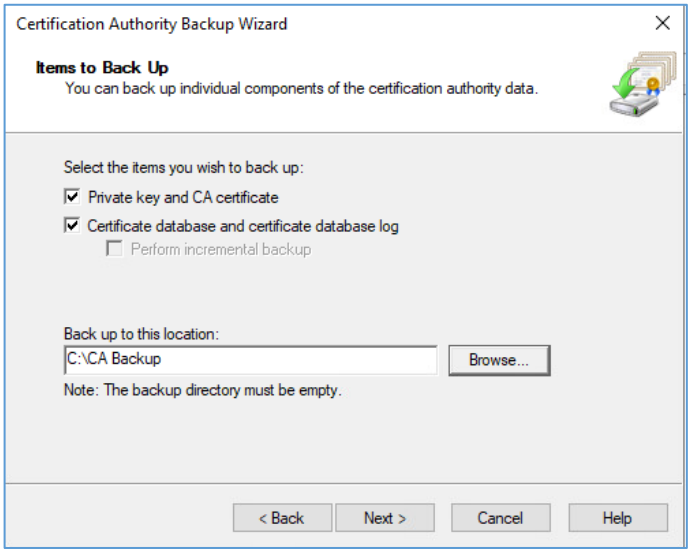
3. Launch the Certificate Authority snap-in from the **Administrative Tools** menu.

4. Before proceeding with the backup of the existing CA database and keys, ensure that CA certificate services are running. If the services are not running, start them before proceeding with the backup process.

5. Select the CA in the **Certificate Authority**, and then click on **Action** in the menu bar. From there, select **All Tasks** and then choose **Back up CA…** to initiate the backup process.



6. Open the **Certificate Authority Backup Wizard** and follow the steps provided by the wizard to create a backup of the CA certificate database. When prompted to select a directory for the backup, make sure to choose an empty directory.



7. Follow the steps provided by the wizard to complete the backup process and then click on the **Finish** button to close the wizard.

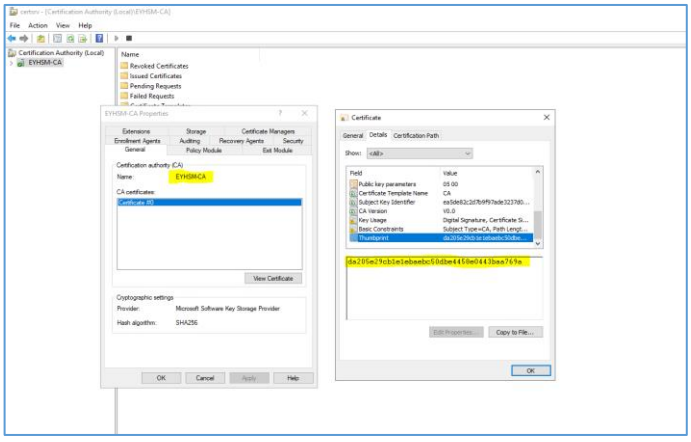
8. In the certificate authority snap-in, select the CA-Name, then click on the **Action** menu and then click **Properties**. This will open the **CA Properties** window where you can view the current provider and CA Name. Next, click on **View Certificate** and when the certificate is displayed, click on **Details.** In the **Field** section click **Thumbprint**.

   Take note of the certificate Thumbprint and CA-Name, as you will need them later when migrating the key.

   For example:

   CA-Name: **EYHSM-CA**

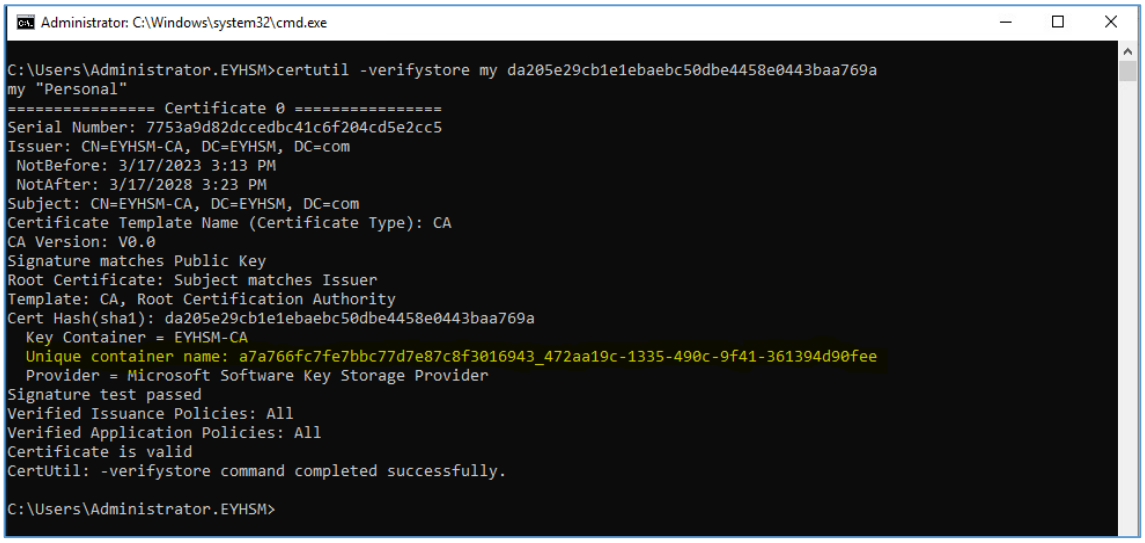
   Thumbprint: **da205e29cb1e1ebaebc50dbe4458e0443baa769a**



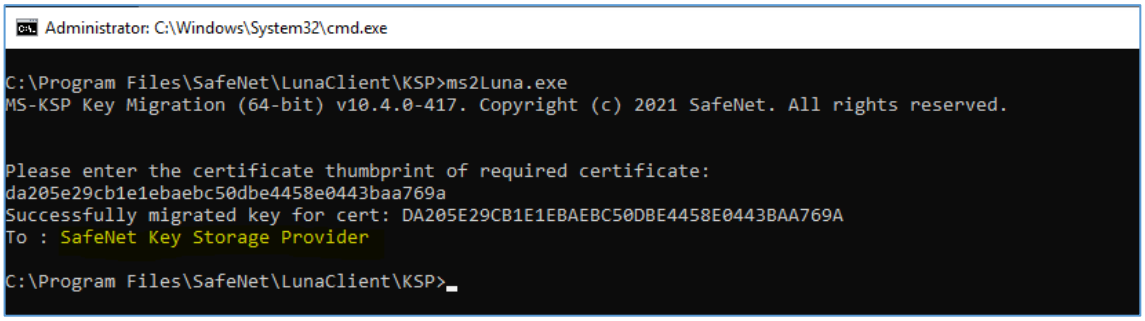
9. Close the **Certificate and Properties** window by clicking the **OK** button twice.

10. Open the command prompt and run the below command to find the unique key container. Take note of the container name as you will need it later when migrating the keys to Luna HSM. For example:

```
certutil -verifystore my <CA_Certificate_Thumbprint>
```



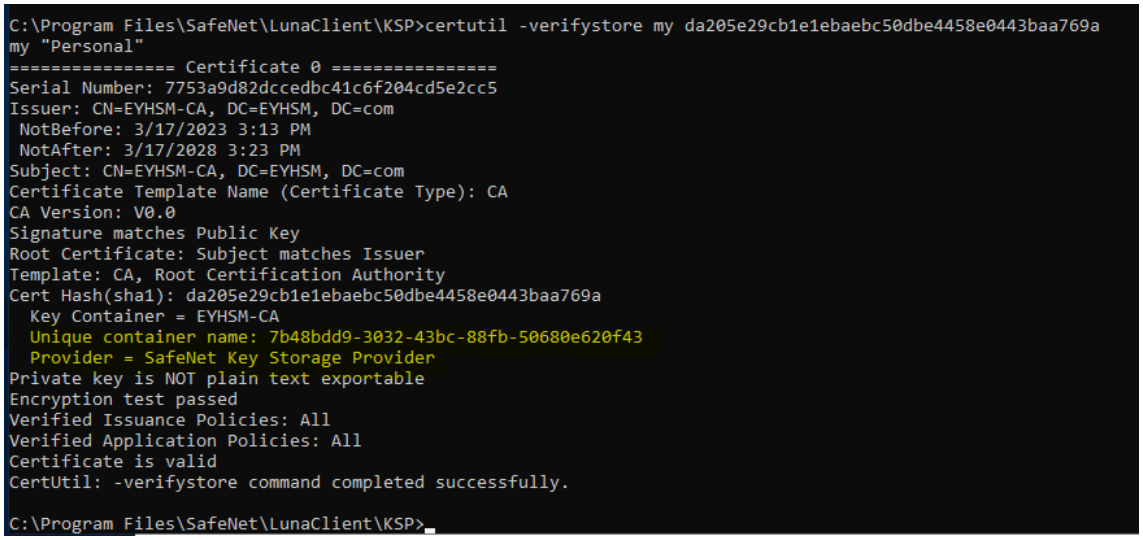
11. Go to the KSP folder of Luna Client and open the command prompt. Run the `ms2luna` command and provide the CA certificate thumbprint when prompted to migrate the CA key.



12. Ensure that CA service provider is now set to SafeNet Key Storage Provider. You can confirm this in two ways. First, check the CA Service Properties window in the Certificate Authority snap-in. Alternatively, you can use the following command to verify the store:

    ```
    certutil -verifystore My <CA_Certificate_Thumbprint>
    ```

    Make sure to replace <CA_Certificate_Thumbprint> with the thumbprint of the certificate for which you migrated the key using the "ms2luna" command. Check that the Unique container name and Provider have been changed accordingly.

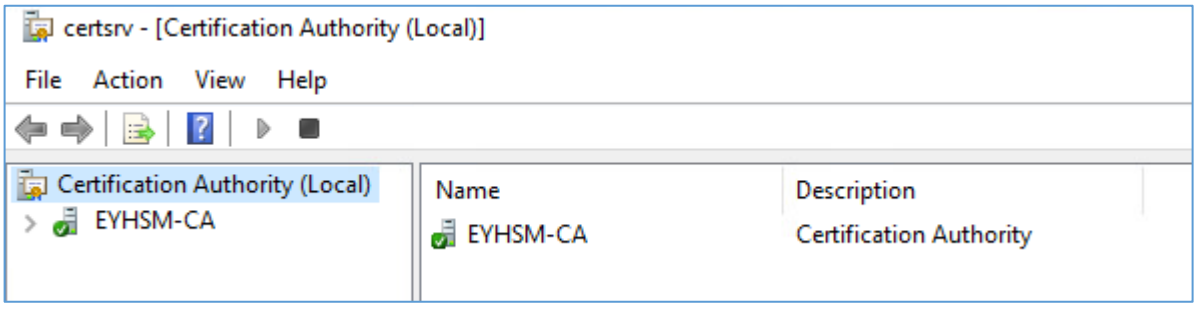


13. Ensure that the output shows **Encryption test passed.** If the command output does not show the association of CA certificate with the key migrated to Luna HSM, run the Repair store command.

    ```
    certutil -repairstore -csp "SafeNet Key Storage Provider" My
    <CA_Certificate_Thumbprint>
    ```

    Replace <CA_Certificate_Thumbprint> with the thumbprint of the CA certificate.

14. Ensure that AD CS services are running correctly after the key migration by stopping and then restarting the services.



15. Use the ksputil utility to create a key for all the other nodes in the AD CS Cluster. Provide the partition password when prompted.

    ```
    ksputil clusterKey /s <SlotNum> /n <CA_Name> /t <TargetCluster_Host>
    ```

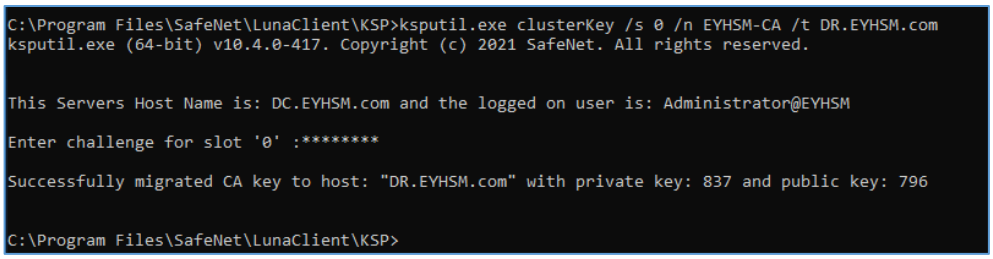
    Where,

    <SlotNum> : Luna HSM partition slot id

    <CA_Name>: Name of the CA

    <TargetCluster_Host>: Fully qualified domain name of cluster node

    > **Note:** You must create a key for every node in the cluster. The above command will duplicate the same key and associate it with the cluster node so that each node has access to the same key.



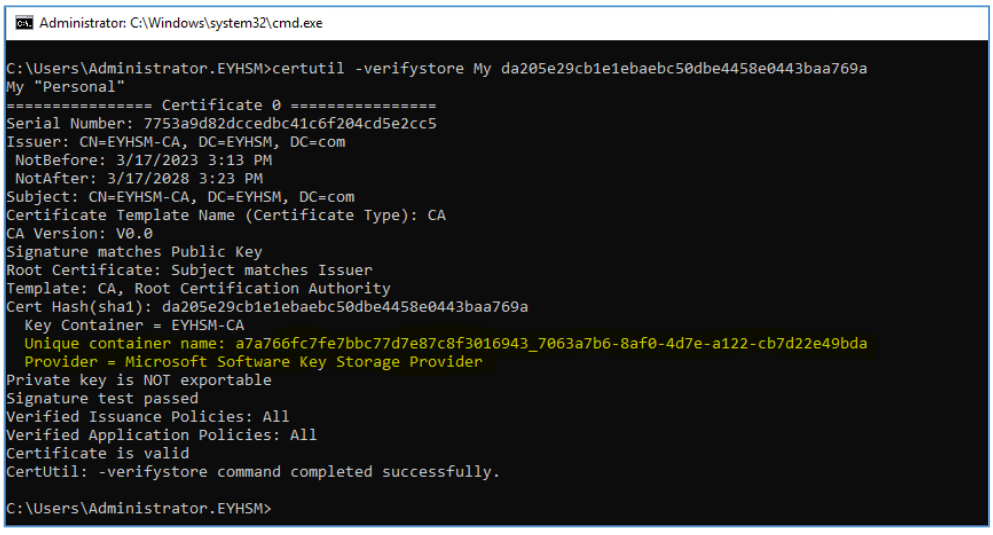
16. Log in to the other cluster nodes and associate the CA certificate with the key migrated and created in the HSM for that particular node.

    > **Note:** Ensure to create key for every node in the cluster.

17. Open the command prompt and run the following command to check that the CA certificate is initially associated with Software Key Storage Provider:

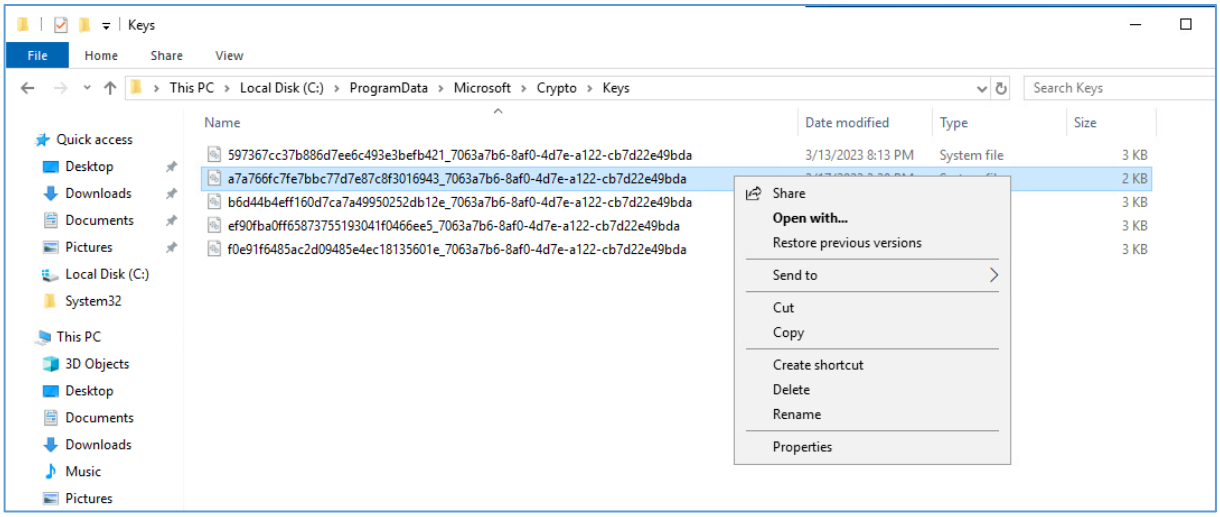
    ```
    certutil -verifystore My <CA_Certificate_Thumbprint>
    ```

    The thumbprint must be the same on all the nodes of the cluster because the cluster is using the same key and certificate for each node. From the output of the command note the **Unique key container** which contains the key.



18. Go to the `C:\ProgramData\Microsoft\Crypto\Keys` directory and locate the **Unique key container** associated with the CA certificate. Right-click on container and select **Delete** to delete the key container.

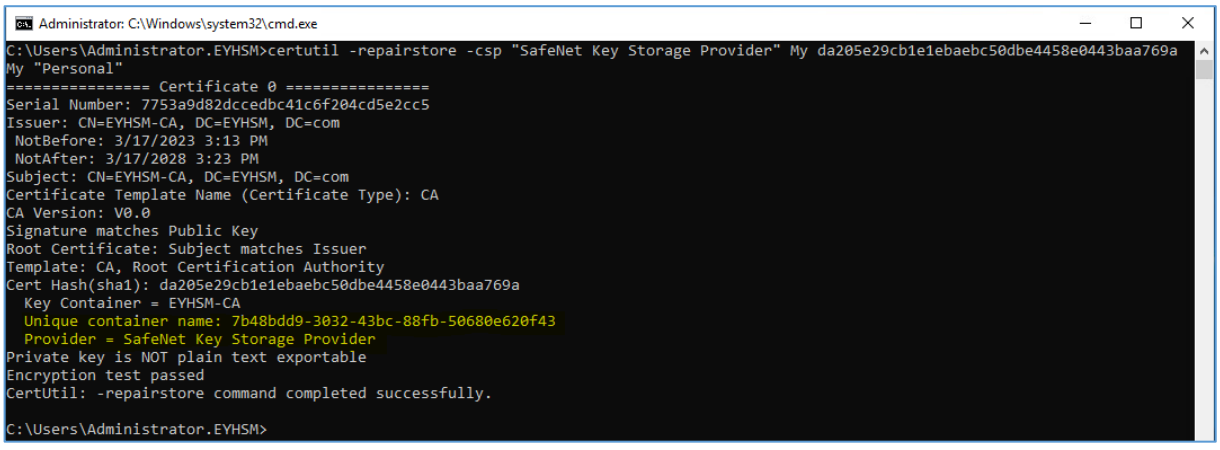
> **Note:** Ensure that you are deleting the correct key container that matches the Unique Key Container from the previous step.



19. Run the repair store command below in the command prompt, to associate the CA certificate with the key migrated to Luna HSM.

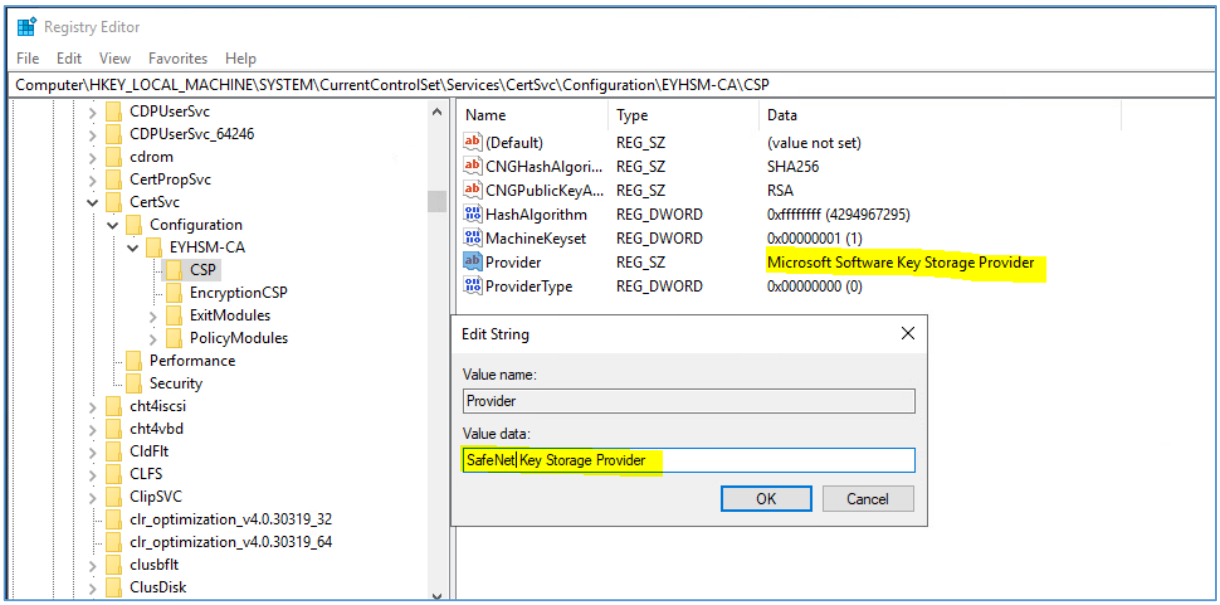
```
certutil -repairstore -csp "SafeNet Key Storage Provider" My
<CA_Certificate_Thumbprint>
```

20. When the command is successfully completed, it will show that the Provider now points to SafeNet Key Storage Provider and Unique container name has been changed.

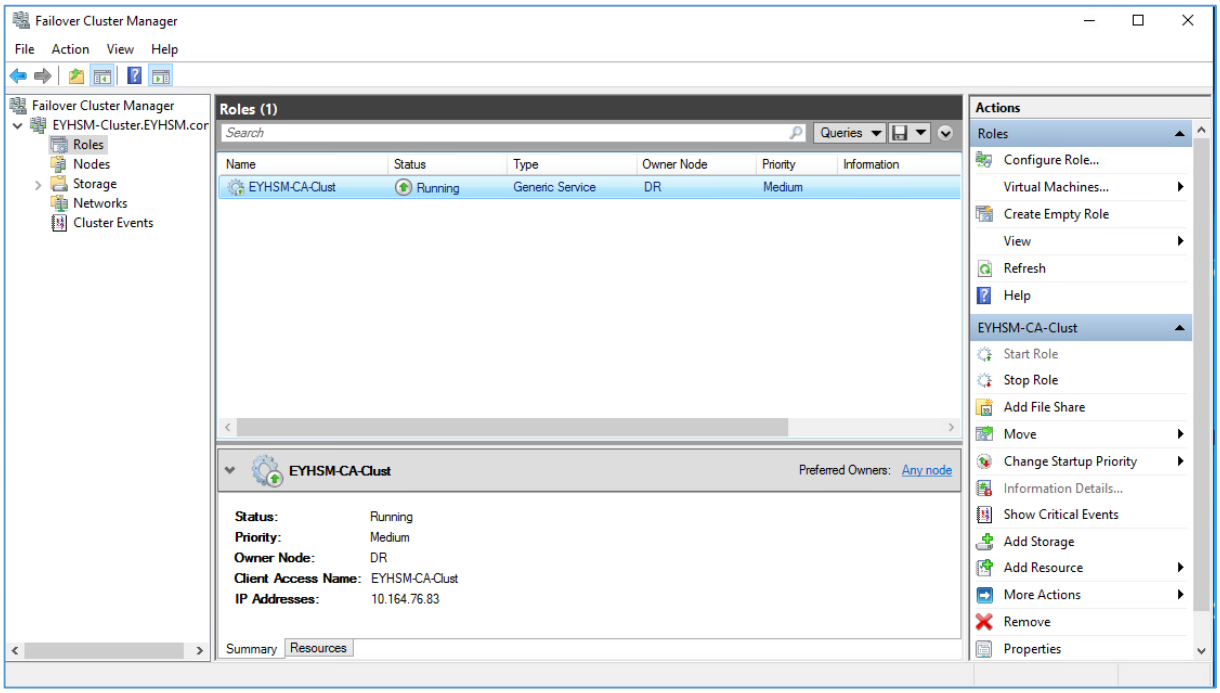


21. Open the registry editor and navigate to the following path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CA-Name>\CSP`. Then, change the value of **Provider** form `Microsoft Software Key Storage Provider` to `SafeNet Key Storage Provider`.

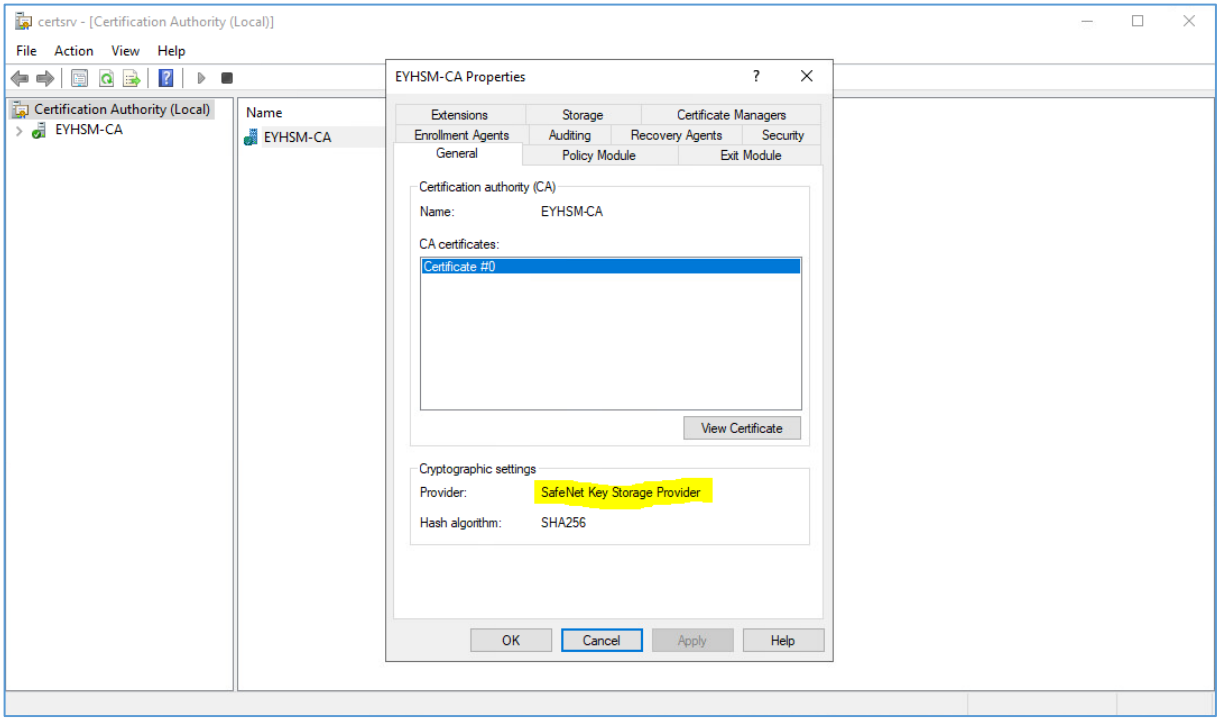
Where the `<CA-Name>` is the actual name of your CA.



22. Launch the **Failover Cluster Manager**, navigate to the Roles section and then select the cluster service. In the **Actions** pane, choose the **Move** option and then select the **Best Possible Node** to assign the shared disk to the node that's currently in use.



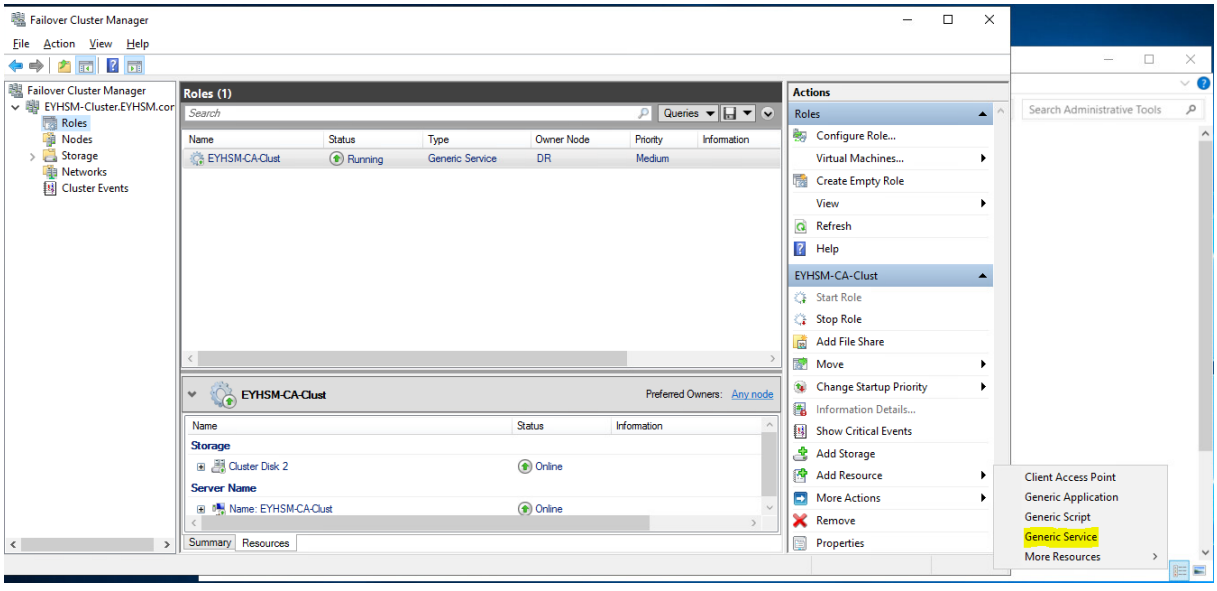
23. Open the certificate authority snap-in and start the CA service. When it starts successfully, ensure that provider is **SafeNet Key Storage Provider**.



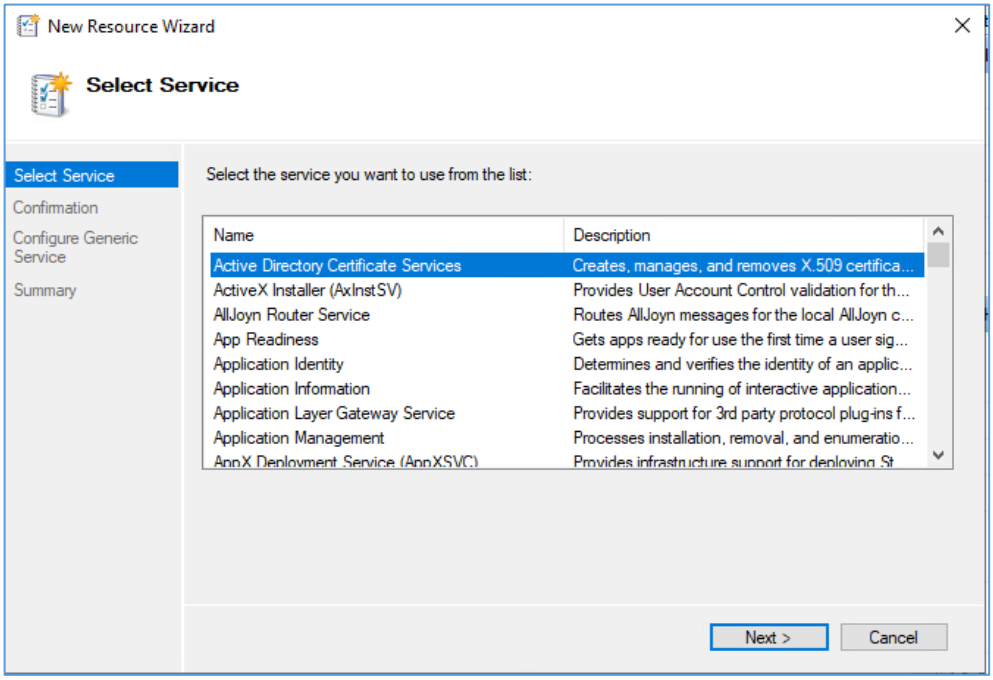
24. Perform steps 16-23 on each node of the cluster. Proceed to next step only after you have associated the CA certificate to the key on Luna HSM using SafeNet Key Storage Provider and confirmed that CA Services are active when the shared disk is connected to that node.

25. Log on to any node where the shared storage is available and CA services are operational.

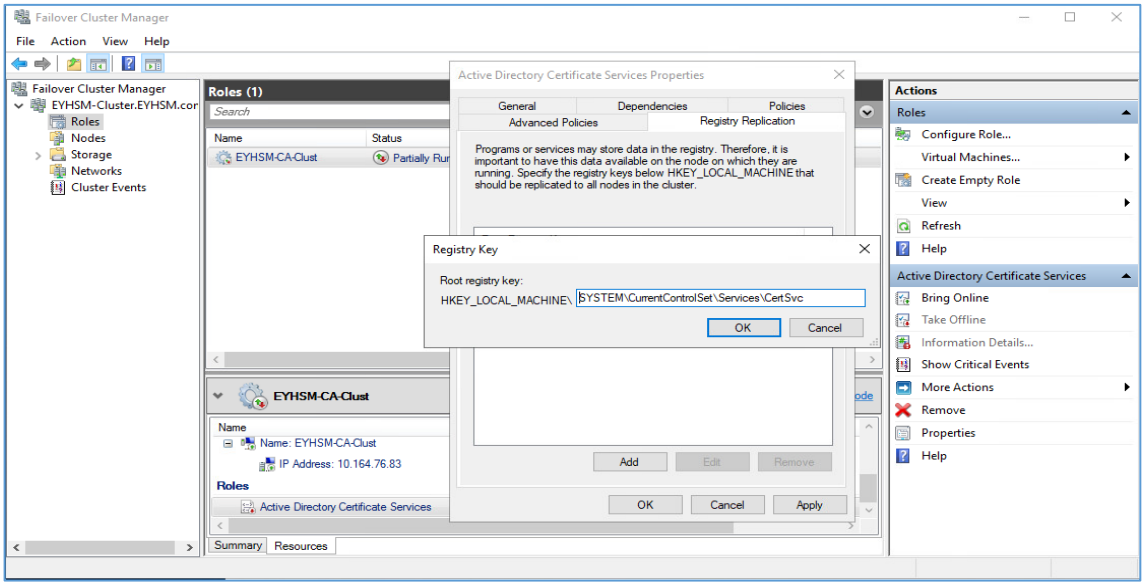
26. In the **Failover Cluster Manager**, navigate to the **Roles** section and select the service. Then, click on **Resources**, followed by **Add Resource**>**Generic Service**.



27. In New Resource Wizard, select **Active Directory Certificate Services** and follow the instructions to complete the Wizard.



28. Navigate to the **Resources** section and choose **Active Directory Certificate Services**. Click on **Properties** to open the property window, select **Registry Replication**, and then click **Add**. Enter the registry value for CA services as "`SYSTEM\CurrentControlSet\Services\CertSvc`" and then click **OK** to save the changes.



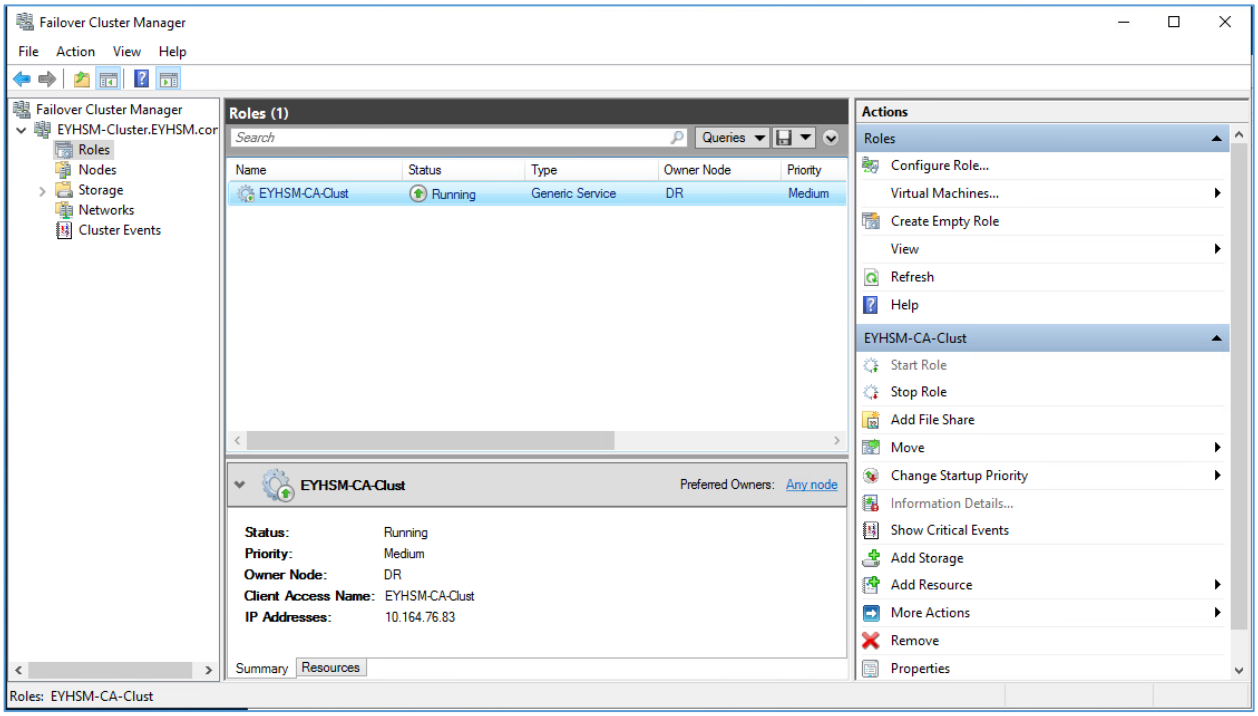
29. Click **OK** to close the **Properties** window and save the settings.

30. In the **Failover Cluster Manager**, go to **Roles** and select the service. Click **Stop Role** in the **Actions** pane to stop the cluster service.

31. Click **Start Role** in the Actions pane to restart the cluster service. Verify that the service is starting and is running properly.

32. Log in to each node of the cluster one by one and verify that the cluster services are running on each node.

33. Open the **Failover Cluster Manager** and select the cluster service under **Roles**. In the **Actions** pane, click **Move** and then click **Best Possible Node**. If the cluster service starts and runs on the currently logged-in node, then everything is working properly and you have successfully migrated the CA keys from the Microsoft Provider to the Luna HSM Provider.



With the execution of the preceding steps, the migration of the failover cluster from the software provider to the Luna HSM provider has been successfully accomplished.

Contacting Customer Support

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.