Microsoft Active Directory Certificate Services

Integration Guide

gemalto
security to be free

Document Number: 007-008669-001, Rev. AA

Release Date: August 2018

Contents

Preface

This document guides security administrators through installing, configuring, and integrating Microsoft Active Directory Certificate Services (ADCS) with a SafeNet Luna HSM or an HSM on Demand service.

Scope

This document outlines the steps to integrate Microsoft Active Directory Certificate Services with SafeNet Luna HSM or HSM on Demand services.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document covers the necessary information to install, configure, and integrate Microsoft Active Directory Certificate Services (ADCS) on Windows with a SafeNet Luna Hardware Security Modules (HSM) or an HSM on Demand Service.

The Microsoft ADCS on Windows provides customizable services for creating and managing public key certificates used in software security systems employing public key infrastructure. Organizations use certificates to enhance security by binding the identity of a person, device, or service to a corresponding private key.

A server configured as a certification authority (CA) provides the management features needed to regulate certificate distribution and use. Active Directory Certificate Services is the Windows Server service that provides the core functionality for Windows Server CAs. ADCS provides customizable services for managing certificates for a particular CA and for the enterprise.

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

Using SafeNet HSMs to secure the Microsoft ADCS root 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.

> **NOTE:** HSM on Demand services do not have access to the secure audit trail.

- Load balancing and fail-over by clustering the HSMs.

*Validation for HSMoD services in progress

Third Party Application Details

- Microsoft Active Directory Certificate Services

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: SafeNet 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. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.
The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

This integration is supported with SafeNet Luna HSM on the following operating systems:

- Windows 2016 Server
- Windows Server 2012R2

NOTE: If you are using Windows Server 2008 R2 you require a previous version of the SafeNet Luna HSM Integration Guide. See MicrosoftADCS_SafeNetLunaHSM_Integration Guide_RevW for more information about integrating a SafeNet Luna HSM with Microsoft ADCS on Windows Server 2008R2.

NOTE: This integration is tested with Luna Clients in HA and FIPS Mode.

SafeNet Data Protection on Demand (DPoD): It is a cloud-based platform that provides on-demand HSM and Key Management services through a simple graphical user interface. With DPoD, 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 the services that you need.

This integration is supported/verified with SafeNet DPoD on the following operating systems:

- Windows 2016 Server
- Windows Server 2012R2

Prerequisites

Before starting the integration of Microsoft ADCS with SafeNet Luna HSM or HSM on Demand Service, ensure you have completed configuring the SafeNet Luna Network HSM or provisioning HSM on Demand service as per the requirement.

Configuring SafeNet Luna HSM

Before you get started ensure you have the following:

1. Ensure the HSM is setup, initialized, provisioned and ready for deployment. Refer to the HSM product documentation for help.
2. Create a partition on the HSM that will be later used by Microsoft ADCS.

3. If using a SafeNet Luna Network HSM, register a client for the system and assign the client to the partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition. Ensure that the partition is successfully registered and configured. The command to see the registered partition is:

```
<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: Follow the SafeNet Network Luna HSM documentation for detailed steps for creating NTLS connection, initializing the partitions and various user roles.

Using SafeNet HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet Luna HSM in FIPS mode, you have to make the following change in configuration file:

```
[Misc]
RSAKeyGenMechRemap=1
```

The above setting redirects the older calling mechanism to a new approved mechanism when SafeNet Luna HSM is in FIPS mode.

Provision your HSM on Demand Service

This service provides your client machine with access to an HSM Application Partition for storing cryptographic objects used by your applications. Application partitions can be assigned to a single client, or multiple clients can be assigned to, and share, a single application partition.

To use the HSM on Demand Service you need to provision you application partition, starting by initializing the following roles:

- **Security Officer (SO)** - responsible for setting the partition policies and for initialize the Crypto Officer.
- **Crypto Officer (CO)** - responsible for creating, modifying and deleting crypto objects within the partition. The CO can use the crypto objects and initialize an optional, limited-capability role called Crypto User that can use the crypto objects but cannot modify them.

- **Crypto User (CU)** - optional role that can use crypto objects while performing cryptographic operations.

NOTE: Refer to the "SafeNet Data Protection on Demand Application Owner Quick Start Guide" for procedural information on configuring the HSM on Demand service and create a service client.

The HSM on Demand Service client package is a zip file that contains system information needed to connect your client machine to an existing HSM on Demand service.

Constraints on HSM on Demand Services

Please consider the following if integrating an HSMoD service with Microsoft Active Directory Certificate Services.

HSM on Demand Service in FIPS mode

HSMoD services operate in a FIPS and non-FIPS mode. If your organization requires non-FIPS algorithms for your operations, ensure you enable the **Allow non-FIPS approved algorithms** check box when configuring your HSM on Demand service. The FIPS mode is enabled by default.

Refer to the "Mechanism List" in the SDK Reference Guide for more information about available FIPS and non-FIPS algorithms.

Verify HSM on Demand <slot> value

LunaCM commands work on the current slot. If there is only one slot, then it is always the current slot. If you are completing an integration using HSMoD services, you need to verify which slot on the HSMoD service you send the commands to. If there is more than one slot, then use the **slot set** command to direct a command to a specified slot. You can use slot list to determine which slot numbers are in use by which HSMoD service.

2
Integrate SafeNet HSM with Microsoft ADCS on Windows Server

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

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

Configuring the SafeNet Key Storage Provider (KSP)

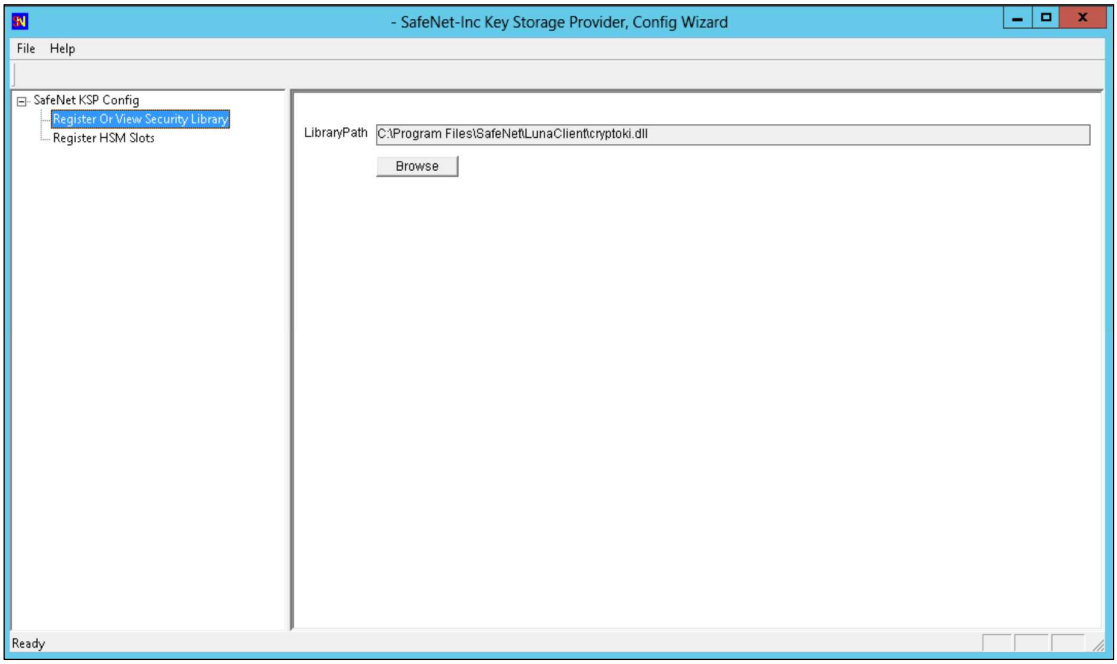
You must configure the SafeNet Key Storage Provider (KSP) to allow the user account and system to access the SafeNet Luna HSM or HSM on Demand Service.

- If using a SafeNet Luna HSM, the KSP package must be installed during the Luna Client software installation.
- If using an HSM on Demand (HSMoD) service, the KSP package is included in the HSMoD service client package inside of the /KSP folder.

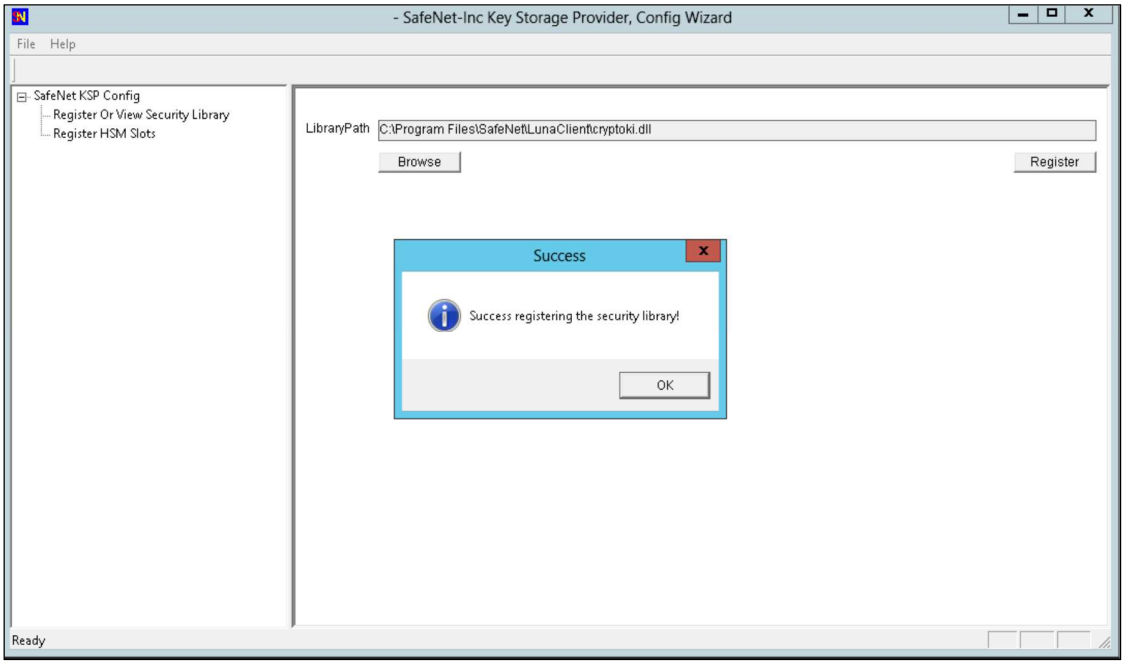
To configure the SafeNet Key Storage Provider

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 SafeNet Luna HSM Client installation directory or HSMoD service client package and click **Register**.

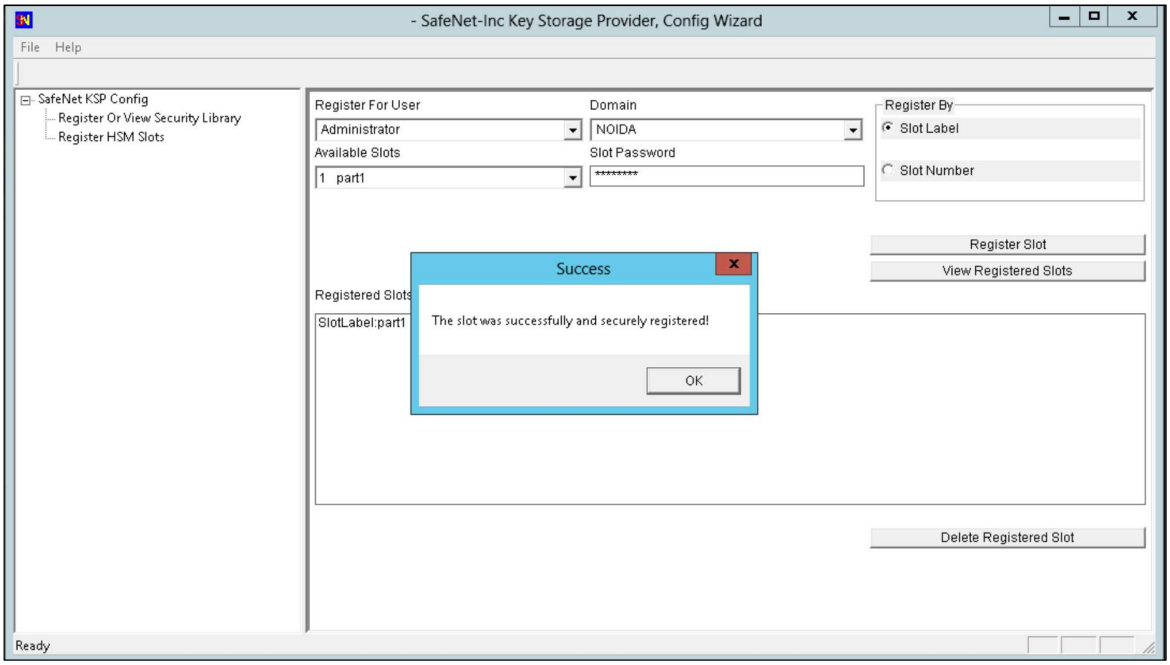


5. On successful registration, a message "**Success registering the security library**" displays.

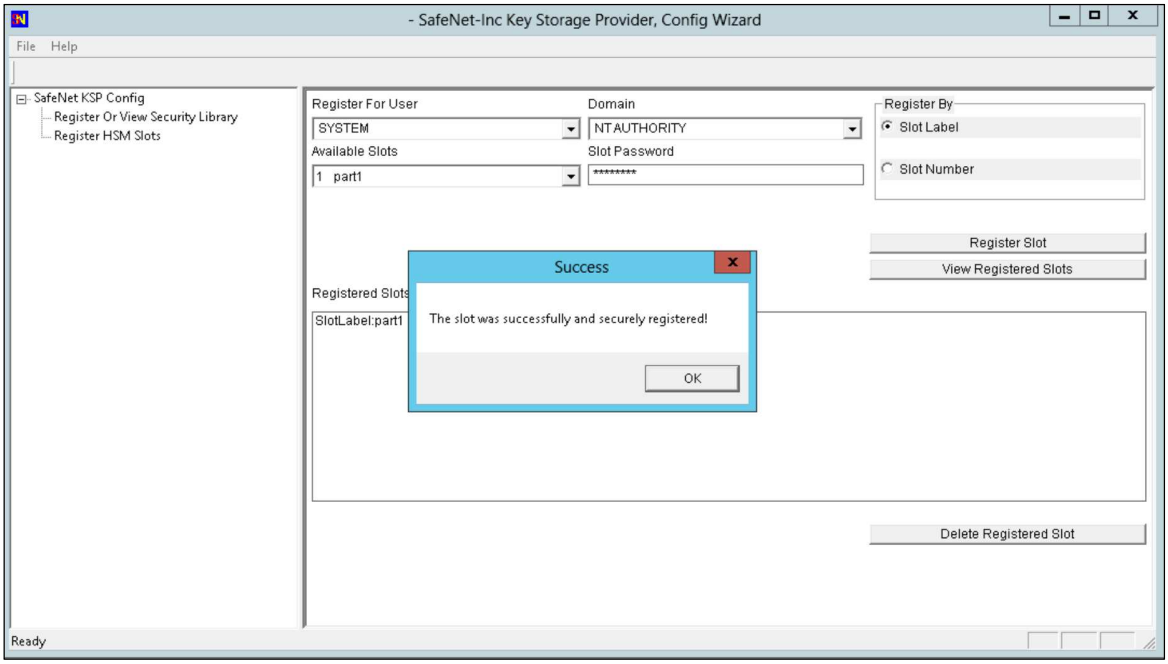


6. Double-click **Register HSM Slots** on the left side of the pane.
7. Enter the Slot (Partition) password.

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



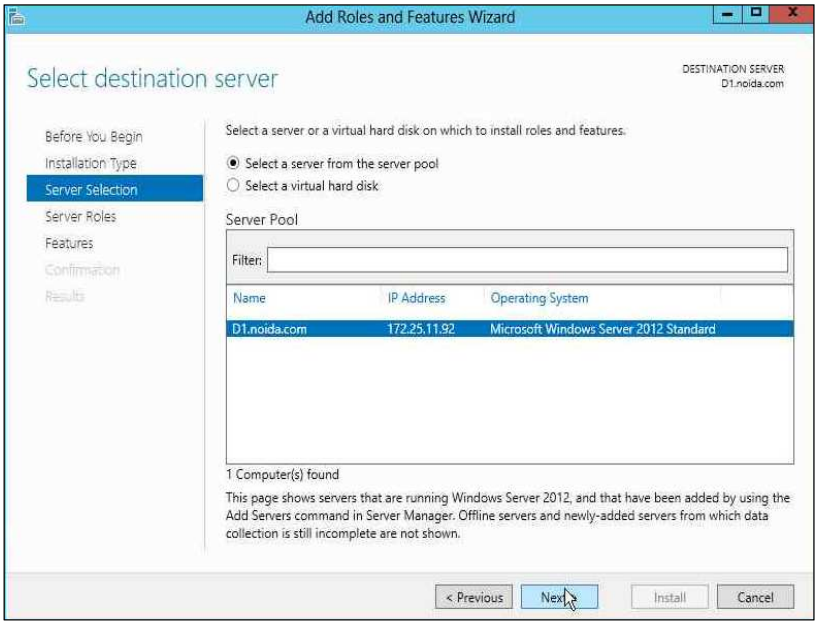
NOTE: Both slots have been registered, despite only one entry appearing for the service in the **Registered Slots** section of the KSP interface.

Installing Microsoft ADCS on Windows Server using SafeNet KSP

You must configure Microsoft ADCS to use the SafeNet Luna HSM or HSMoD service when you configure the Microsoft Certificate Authority (CA) user role.

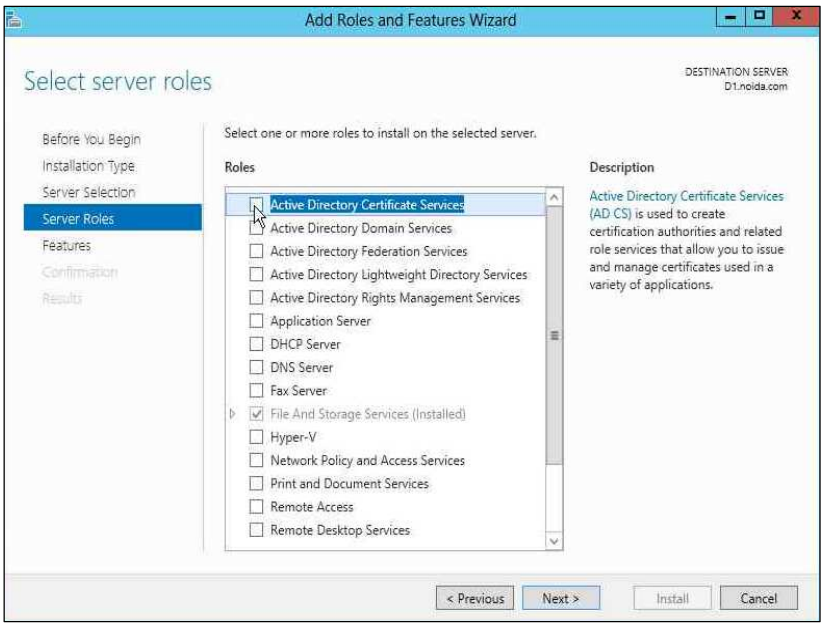
To install Microsoft ADCS

1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Ensure you have configured the SafeNet KSP. Refer to the section Configuring the 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.

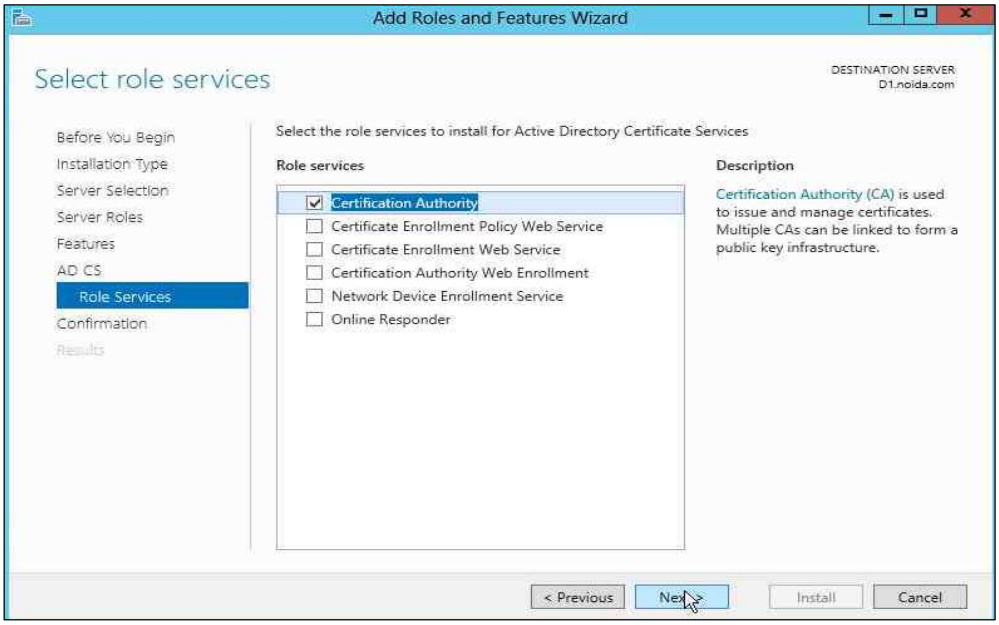


8. Click **Next**.

9. Select the **Active Directory Certificate Services** check box.

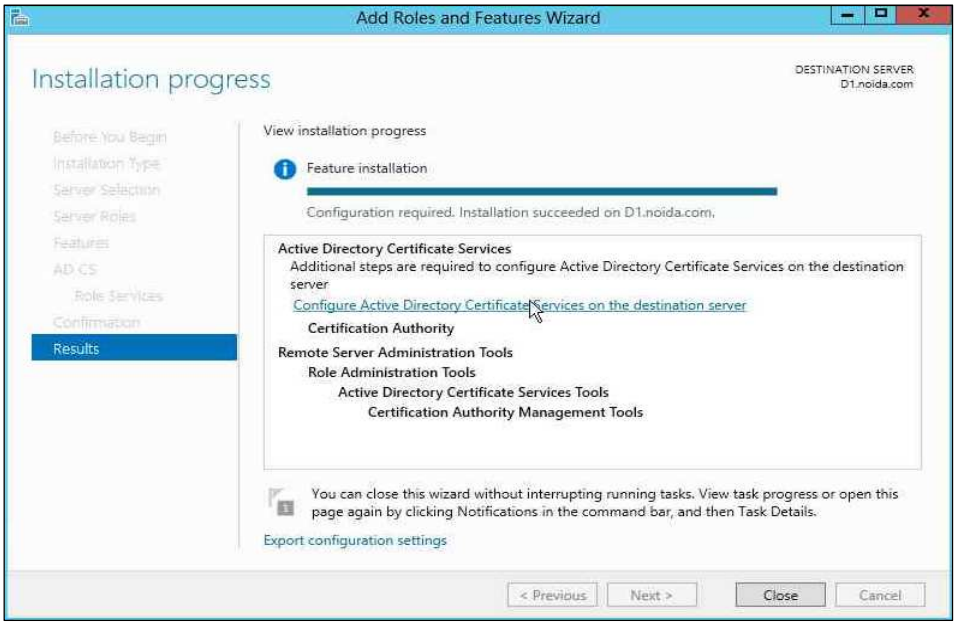


10. A window displays stating **Add features that are required for Active Directory Certificate Services?** To add a feature, click the **Add Features** button.
11. Click **Next** to continue.
12. On the Active Directory Certificate Services page click **Next** to continue.
13. Select the **Certification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



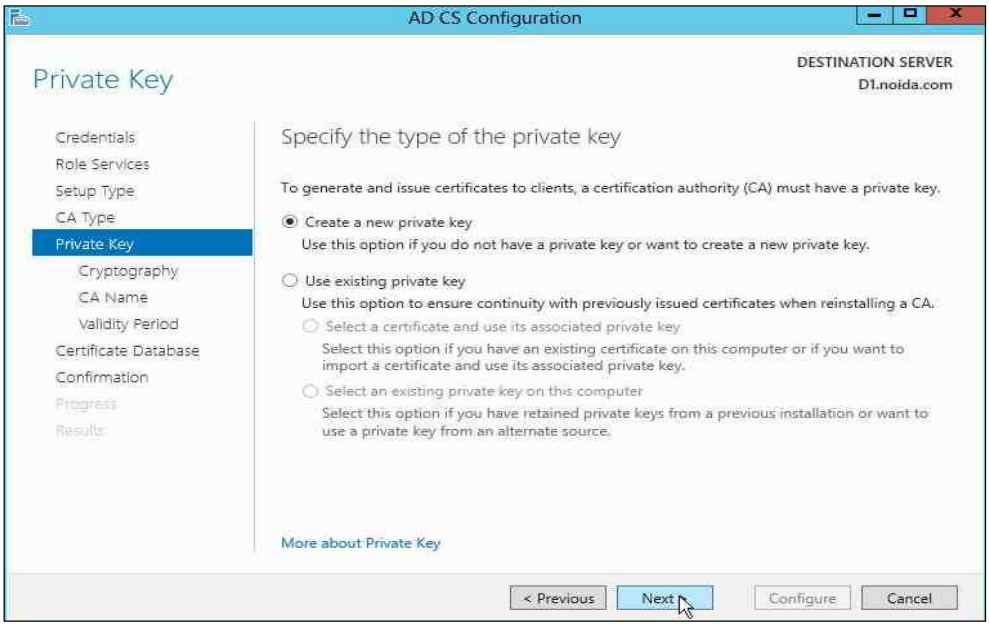
14. Click **Install**.

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



16. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.
17. Select the **Certification Authority** check box and click **Next**.

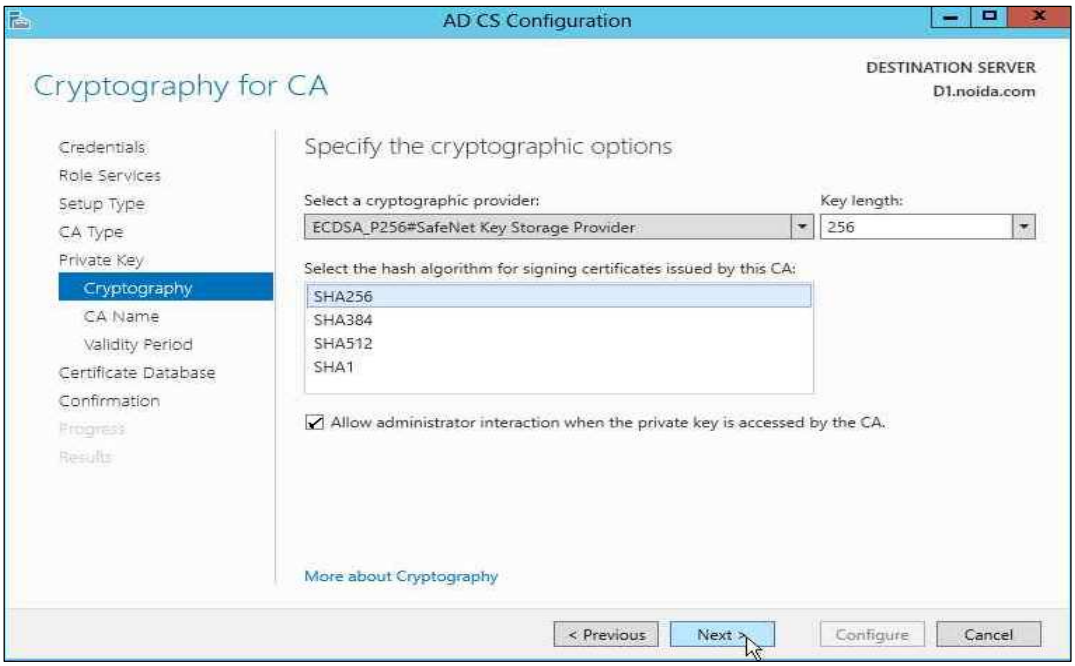
18. Select the **Enterprise CA** radio button and click **Next**.
19. Select the **Root CA radio button** and click **Next**.
20. Setup the Private Key for the CA to generate and issue certificates to clients. If you would like to create a new private key select the **Create a new private key** radio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



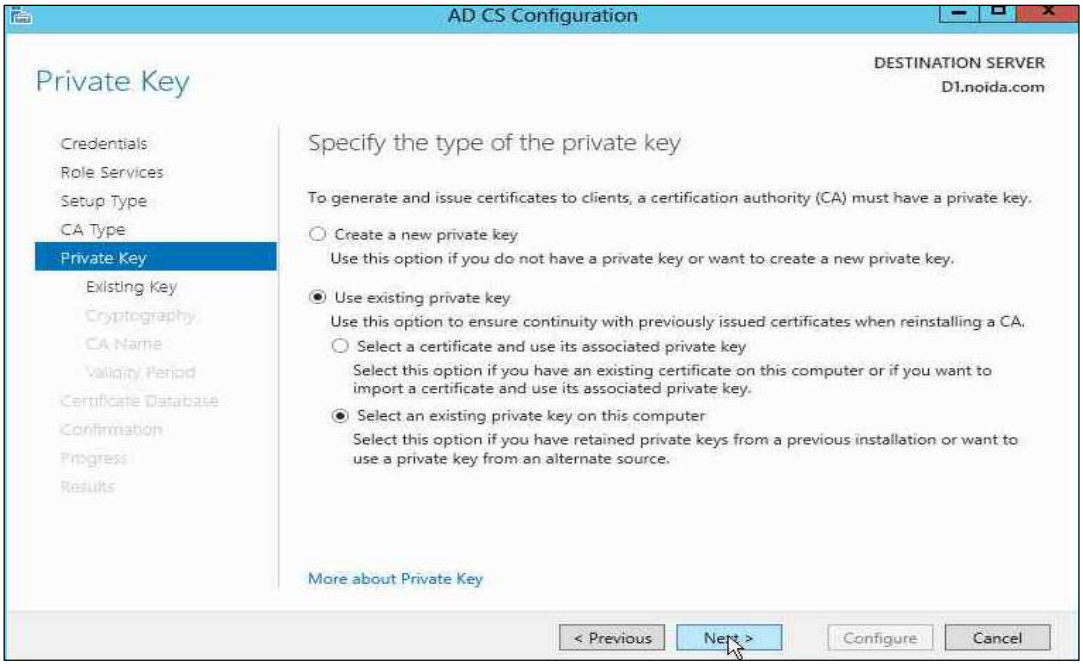
21. Open the **Select a cryptographic provider:** drop-down menu and select an algorithm using a **SafeNet Key Storage Provider**. Open the **Key length:** drop-down menu and select a key-length.

22. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.
23. Select the **Allow administrator interaction when the private key is accessed by the CA** check box.

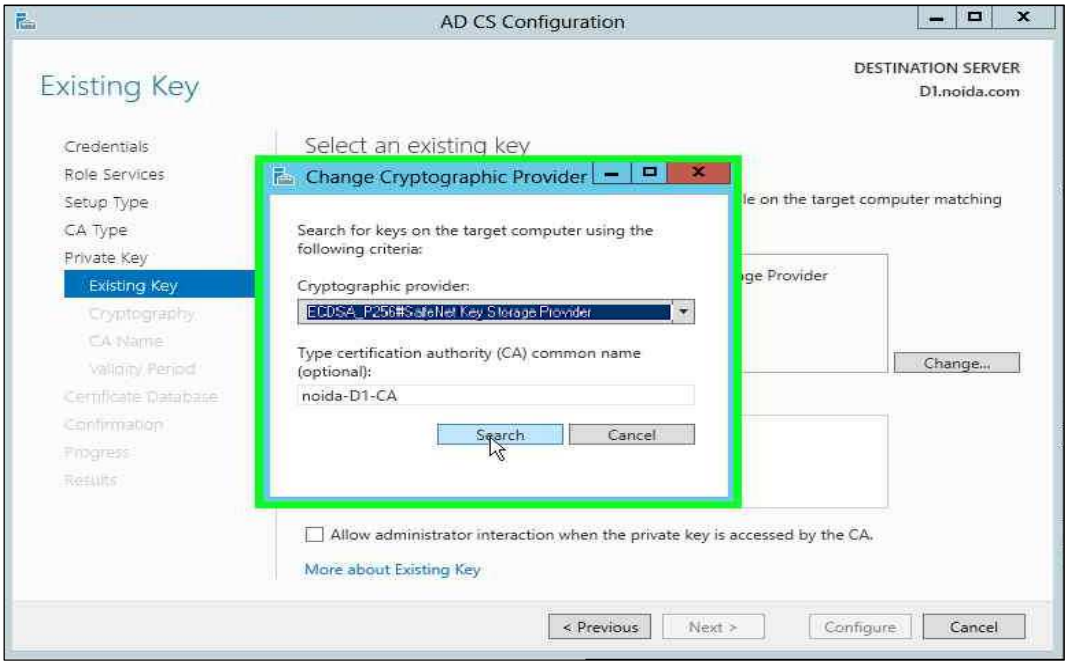
Click **Next**. Proceed to step 27.



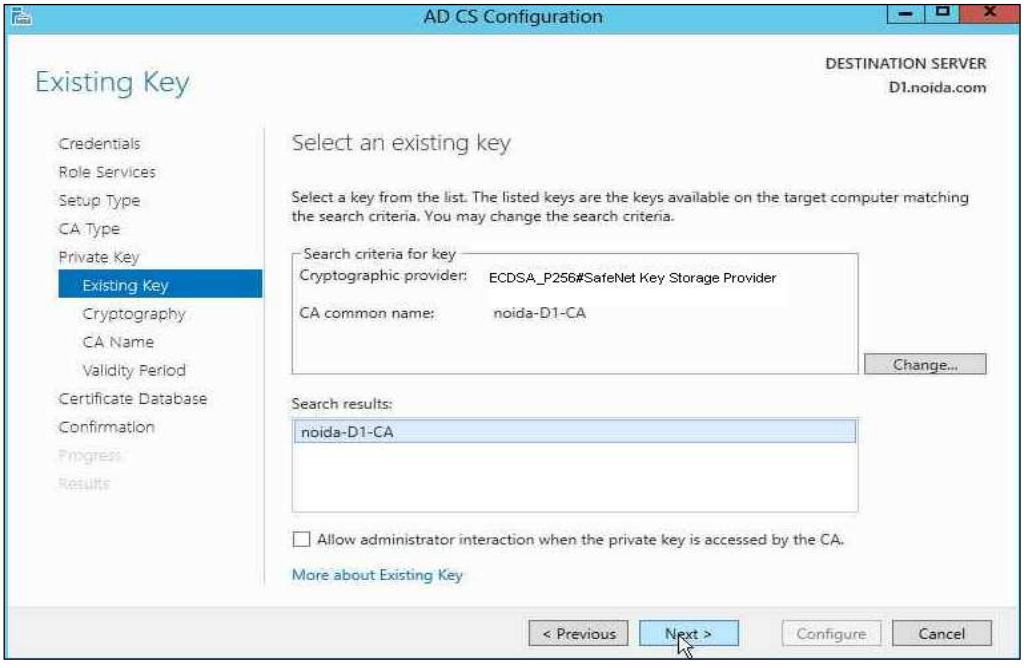
24. Select the **Use existing private key** check box. Setup the **Private Key** for CA to generate and issue certificates to clients. Select **Use existing private key** and **Select an existing private key on this computer.** Click **Next** to continue.



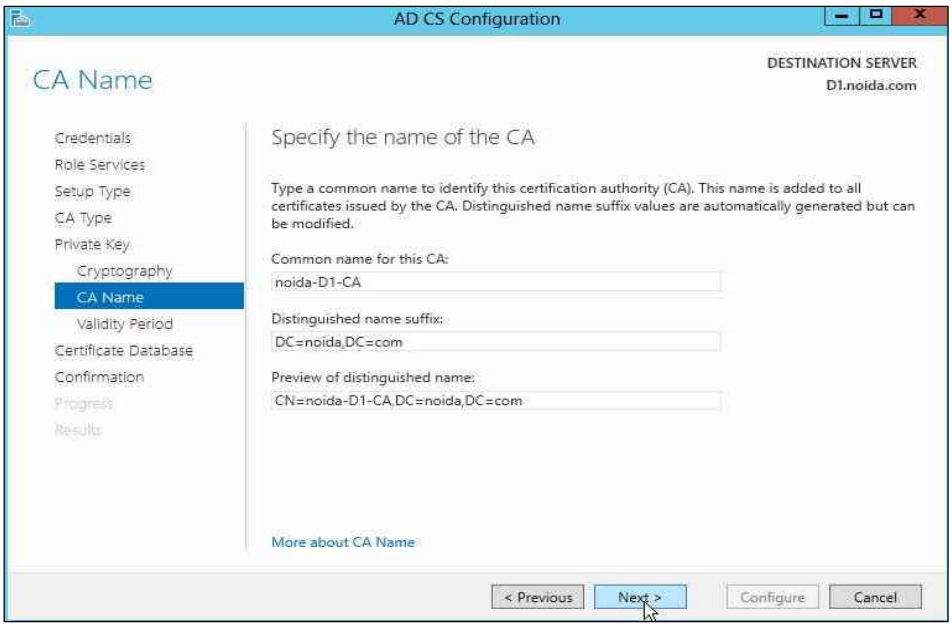
25. Click **Change**. Select the SafeNet Key Storage Provider algorithm that you have used to generate the private keys and clear the CA Common name, click **Search**.



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:

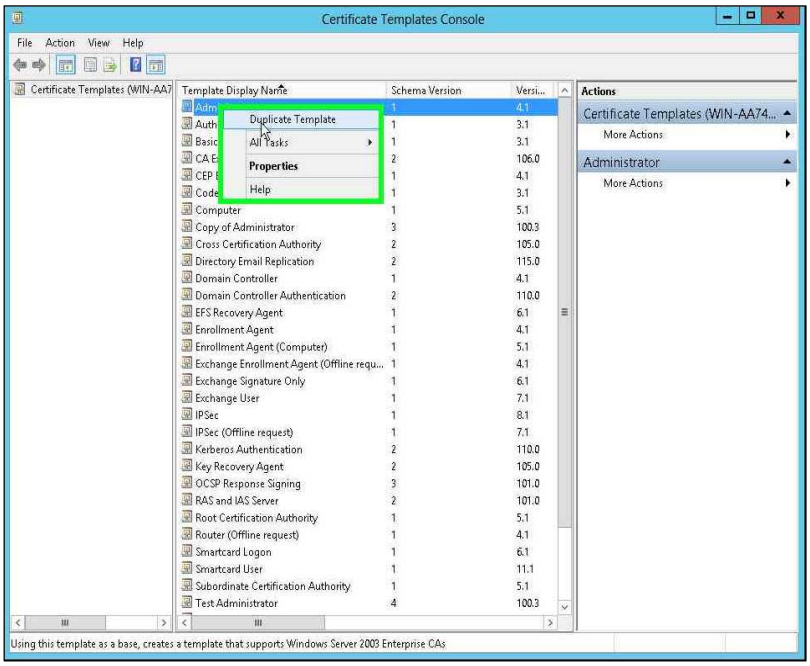
    ```
    sc query certsvc
    ```
32. Open a command prompt and run the following command to verify the CA key:

    ```
    certutil -verifykeys
    ```

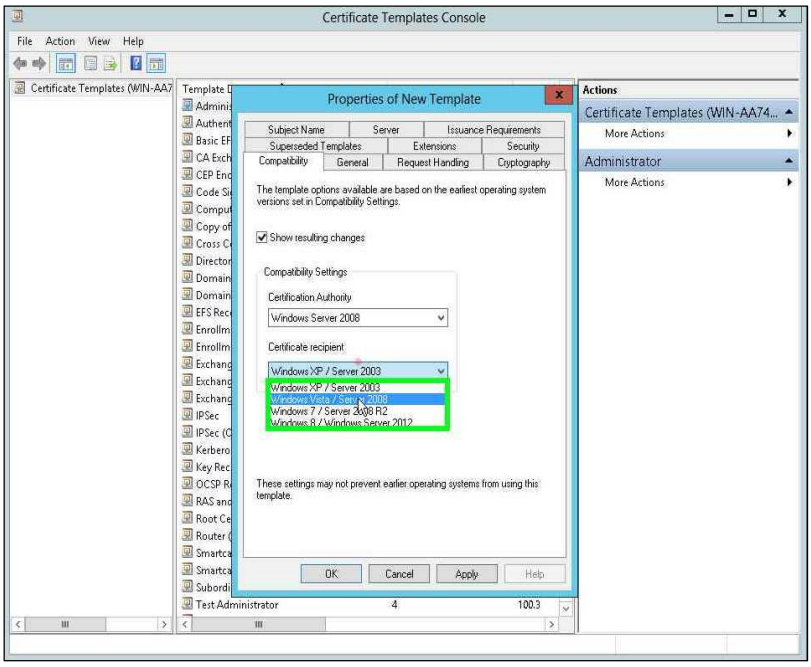
    The result of the command shows the CA keys have successfully been verified.

Enrolling the Certification Authority Certificate

1. Create a CA template that uses SafeNet Key Storage Provider.
   a. Open a command prompt and run **certtmpl.msc**
   b. Right click the **Administrator** template
   c. 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.

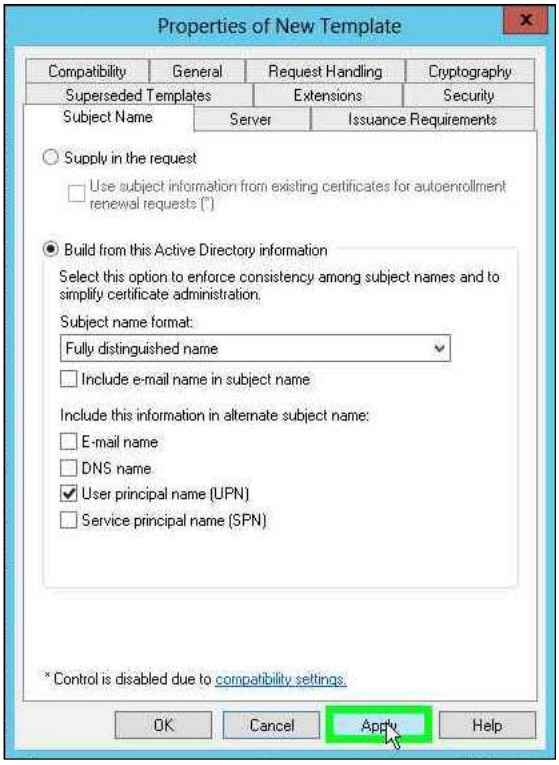
e) For **Algorithm Name** select an algorithm.

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.



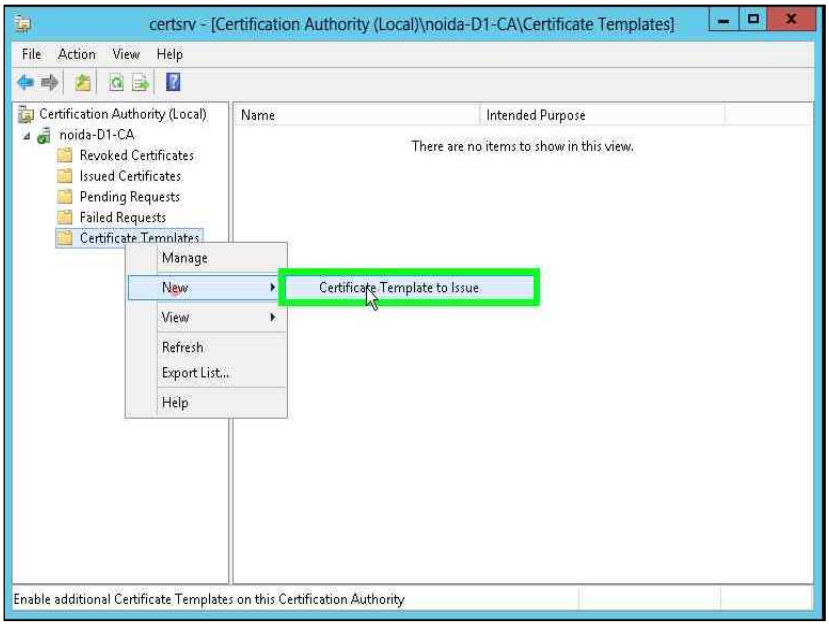
j) Click **Apply** to save the template. Click **OK**.

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

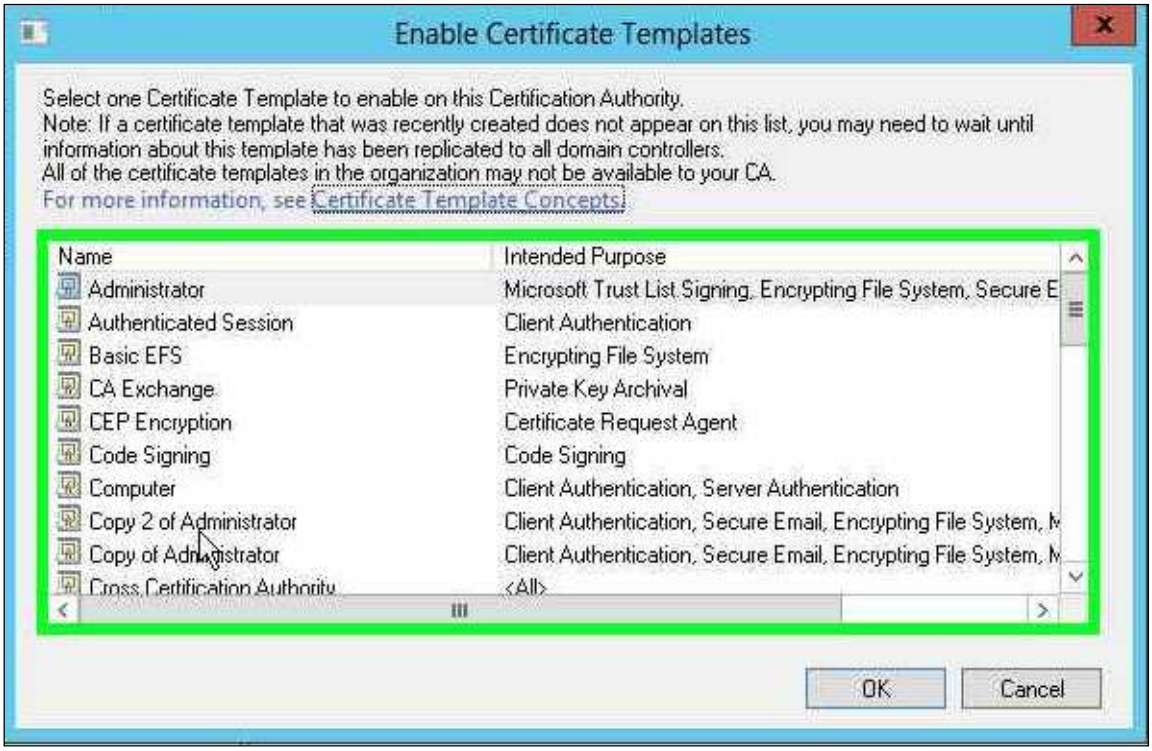
l) Double-click the CA name.

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

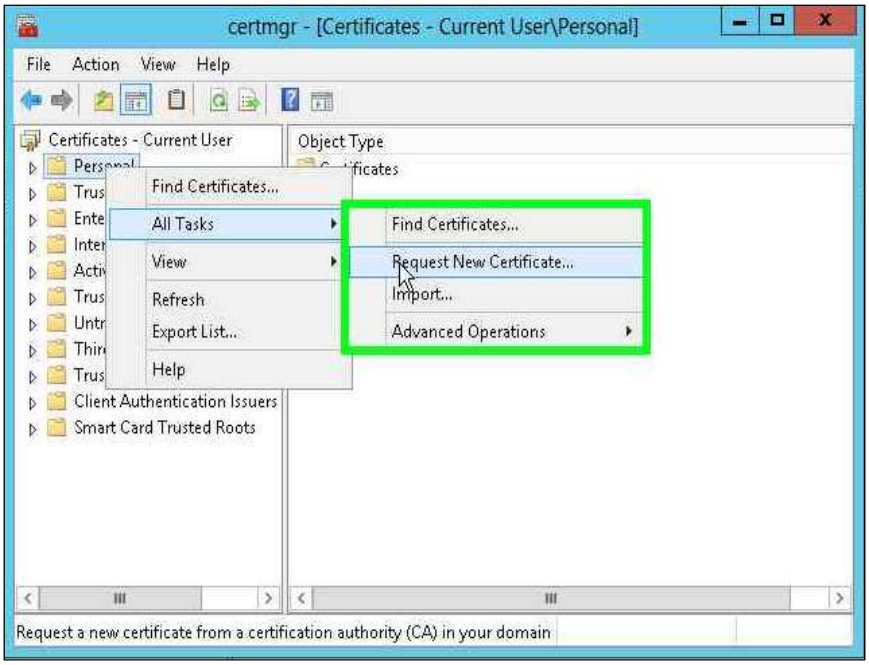
n) Select **New -> Certificate Template to Issue**



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.

Archiving the CA Key

You can verify that the configurations that are possible with the SafeNet Luna HSM or HSM on Demand 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:

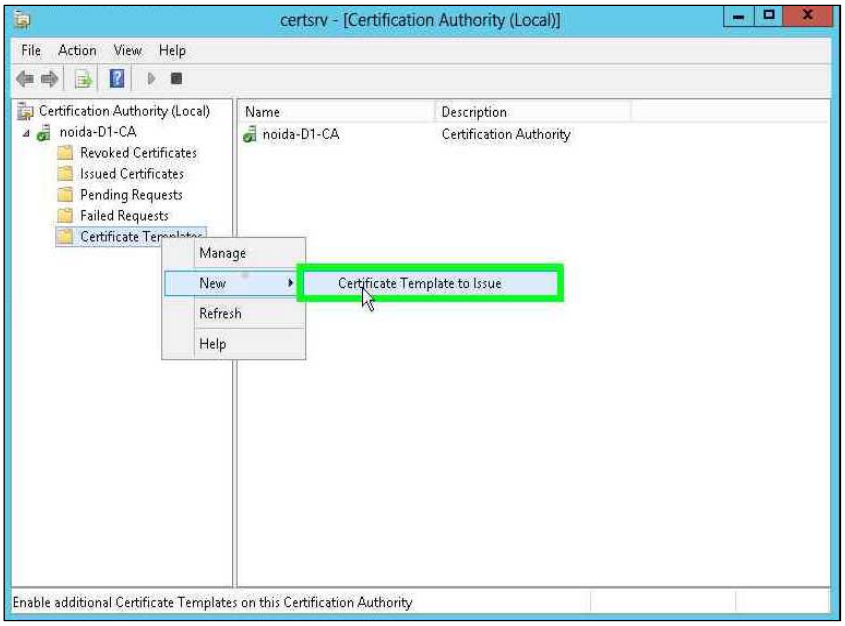
- archive the CA key
- issue the KRA certificate from the CA snap-in
- issue the KRA certificate from the CA snap-in
- retrieve the issued certificate from CA
- configure CA to support Key Archival

- create a template with Key Archival enabled
- add a new template to CA for issuing
- issue a user template with key archival enabled

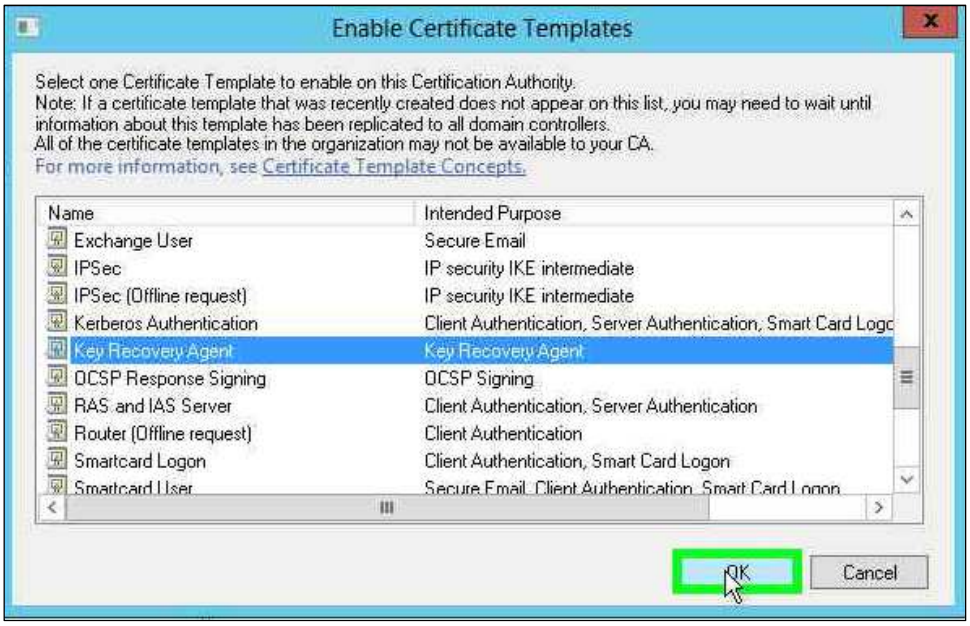
NOTE: If you wish to secure the key on SafeNet HSM that is used to encrypt the Archived Keys then you need to select the SafeNet Key Storage Provider for generating the keys for Key Recovery Agent certificate.

To 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**.

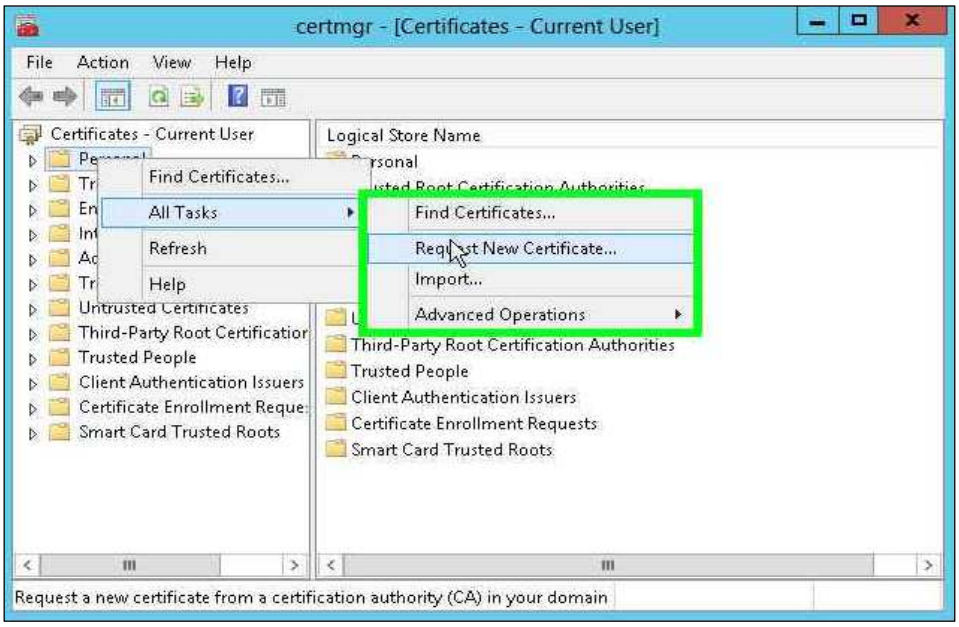


6. Select the **Key Recovery Agent** template and click **OK**.



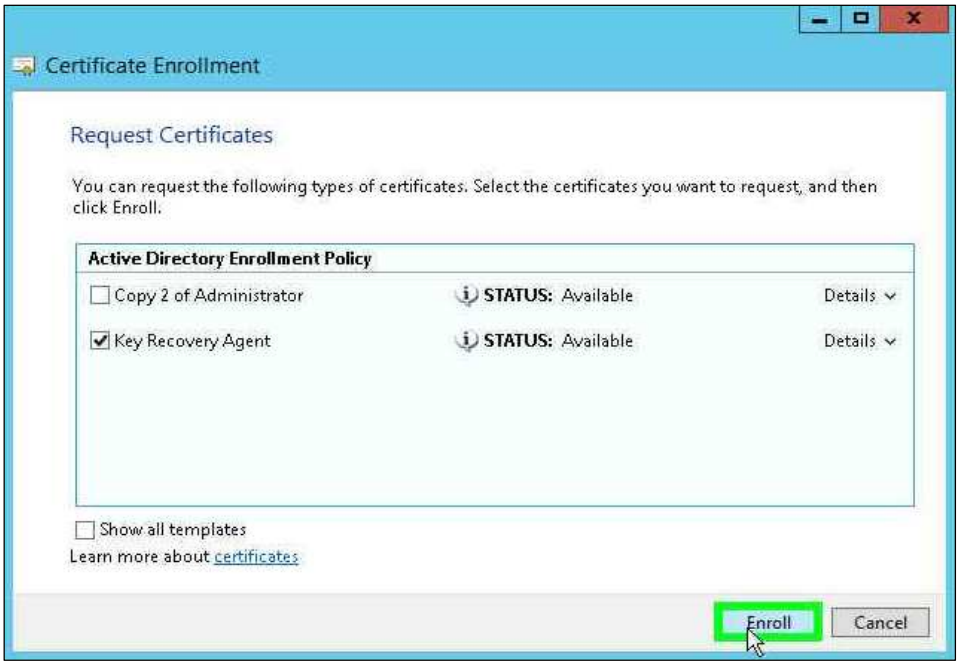
To Issue the KRA Certificate.

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….**

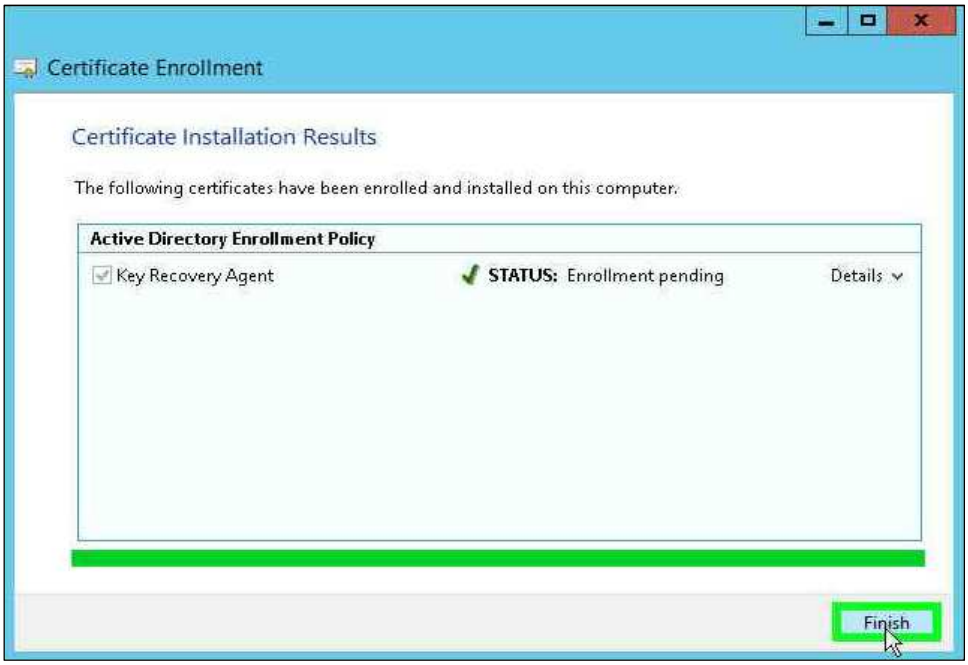


3. Click **Next**.
4. Select **Active Directory Enrollment Policy** and click **Next**.

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

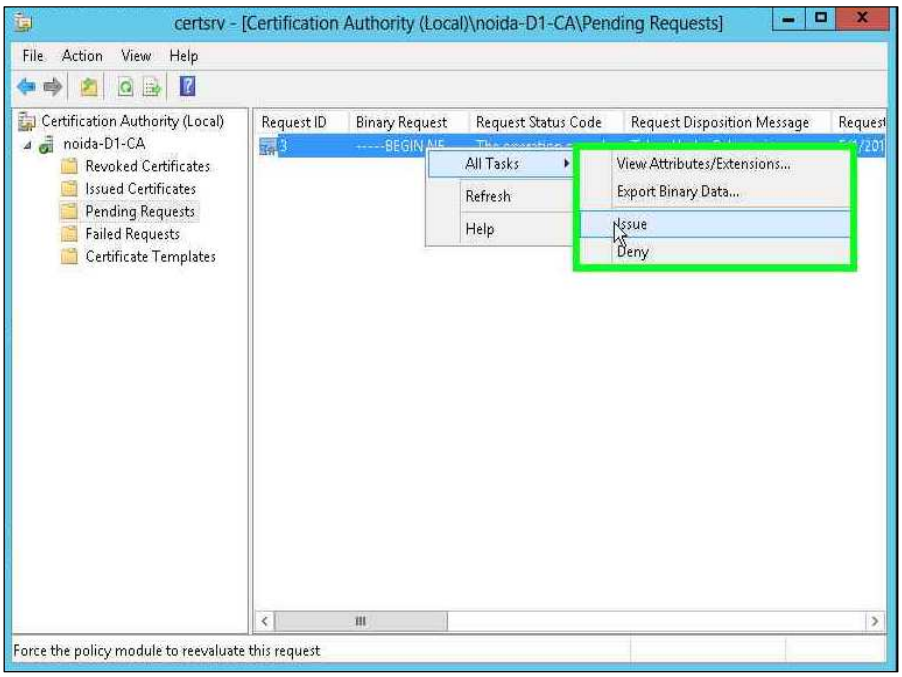


6. Verify the enrollment is pending and click **Finish**.



To issue the KRA certificate from the CA snap-in.

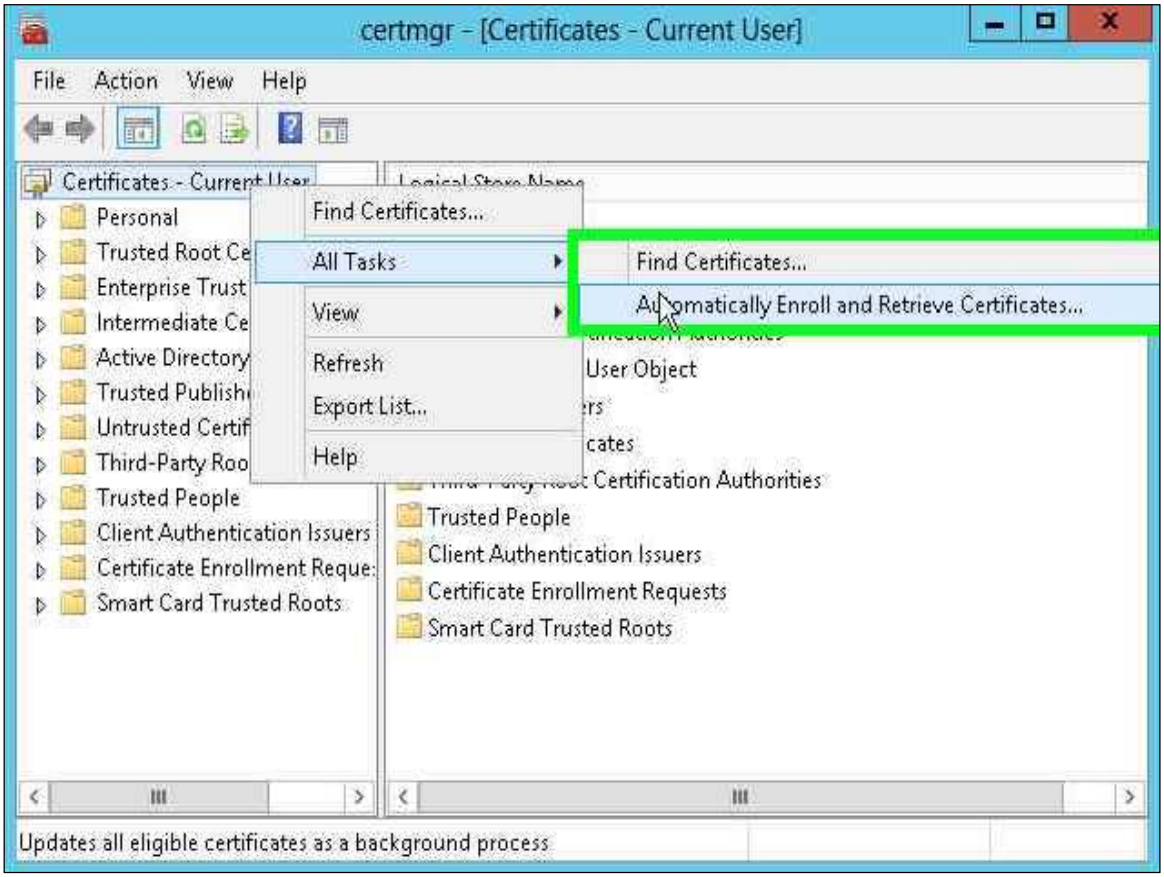
1. Open the command prompt and run the **certsrv.msc** command.
2. Select the **Pending Requests** node. Right-click on the latest request for the KRA template. Select **All Tasks** and click **Issue**.



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

To 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…**

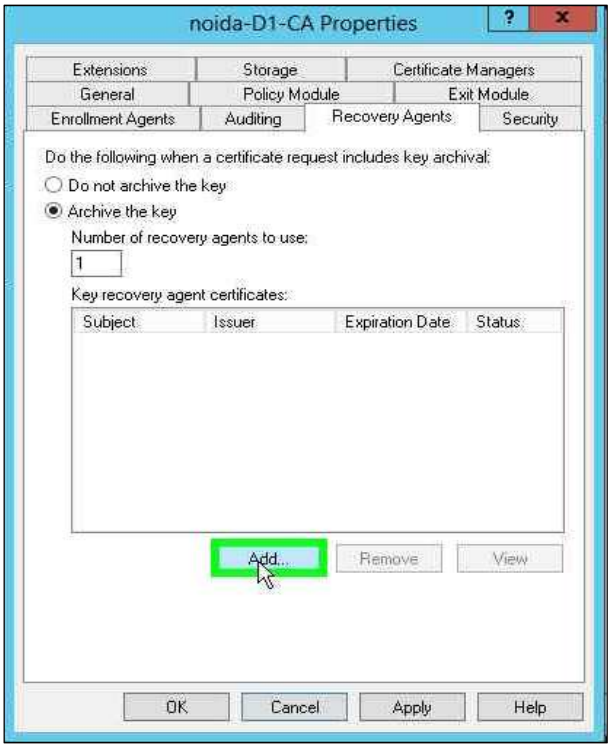


4. Click **Next**.
5. Select the KRA certificate you just issued and enroll it.

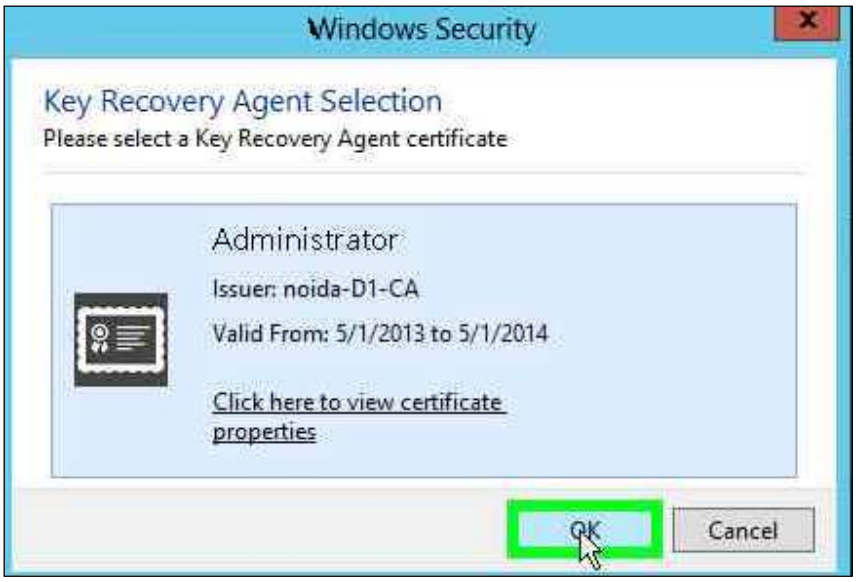
To configure the CA to support Key Archival.

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.



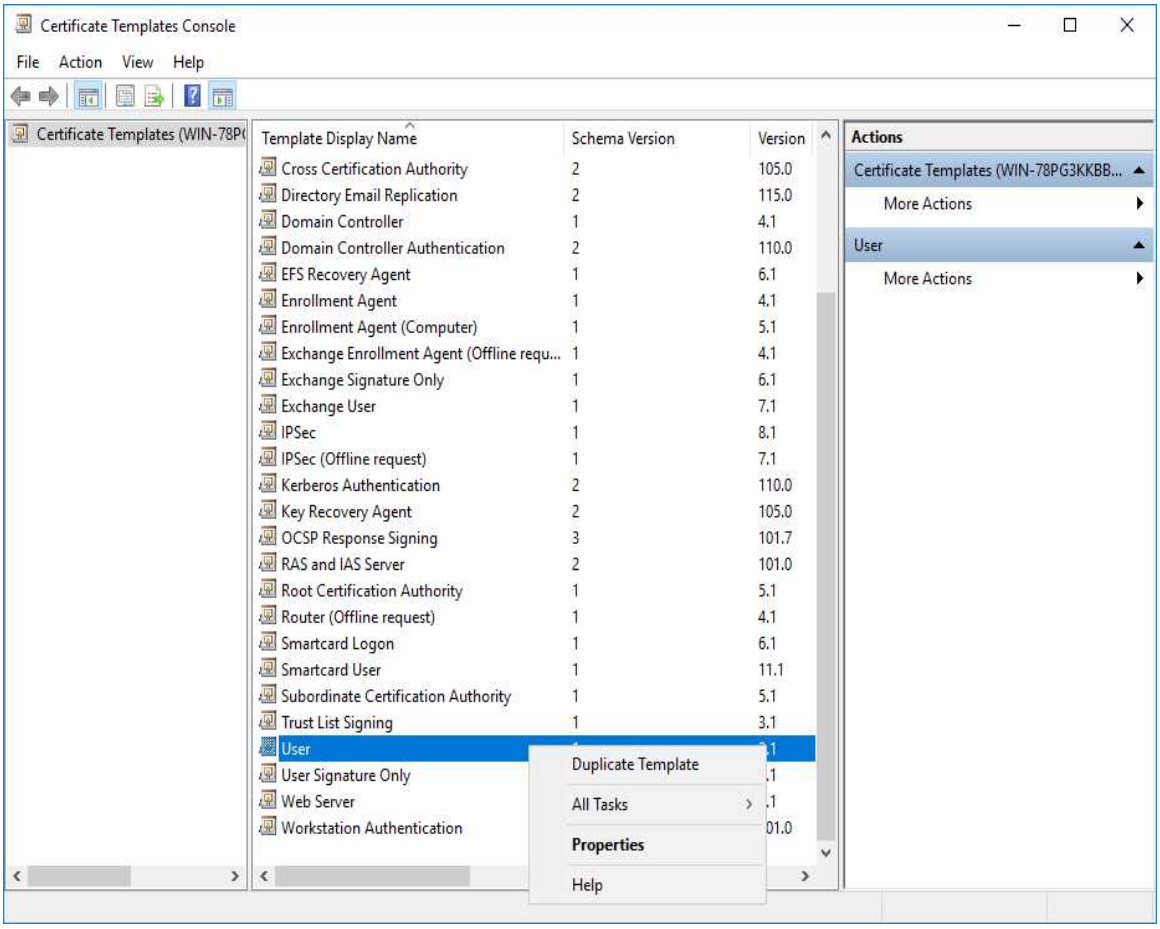
6. Select the KRA certificate you just issued, Click **OK**.



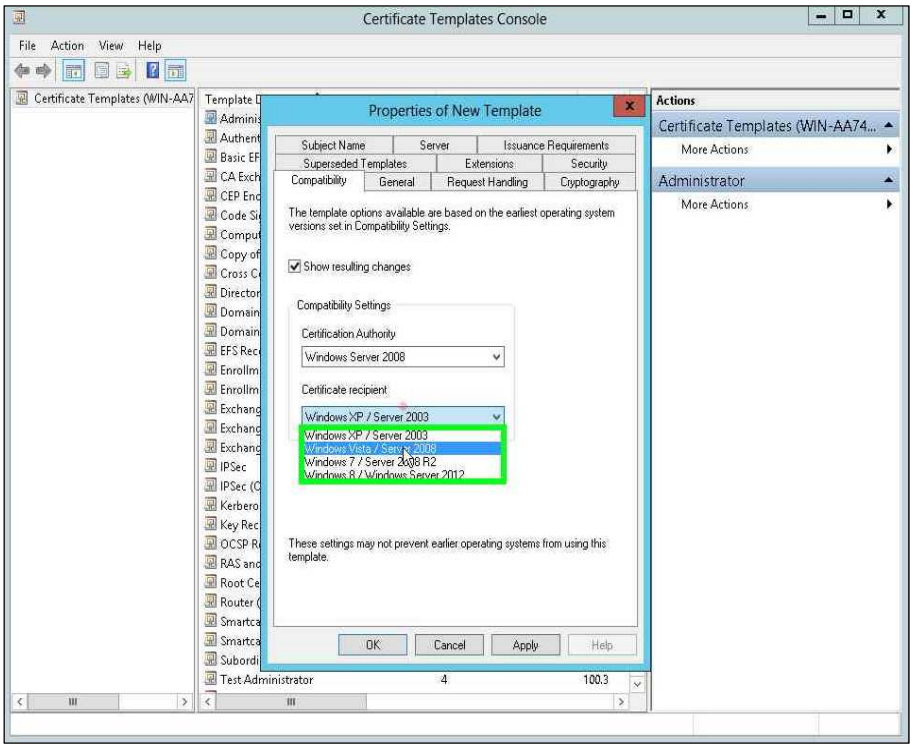
7. Click **OK**
8. Verify the CA service must be restarted, click **Yes**.

To 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**.

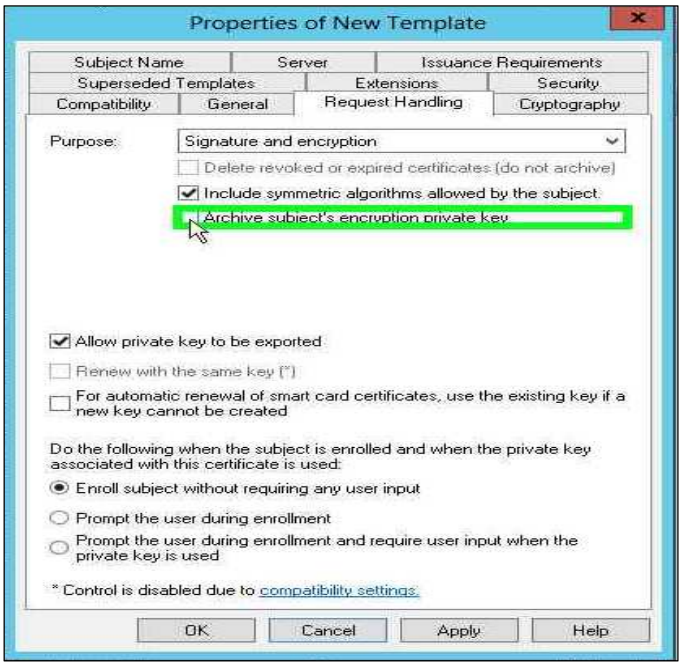


3. Select **Windows Server 2008** for both Certification Authority and Certificate recipient under **Compatibility Settings**, Click **OK**.

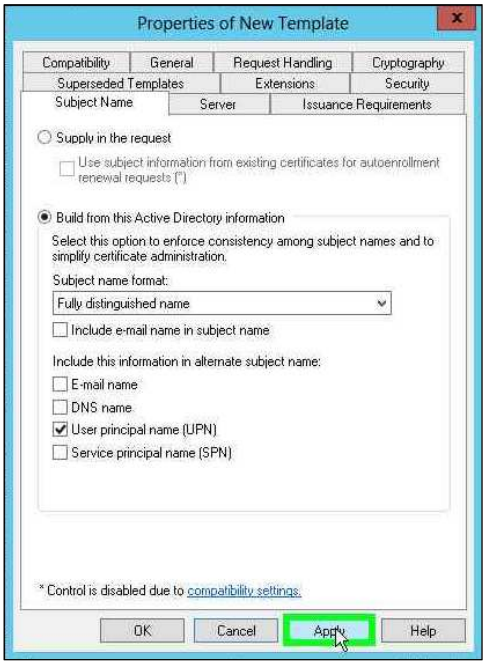


4. On the **Resulting Changes** menu click OK.

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.



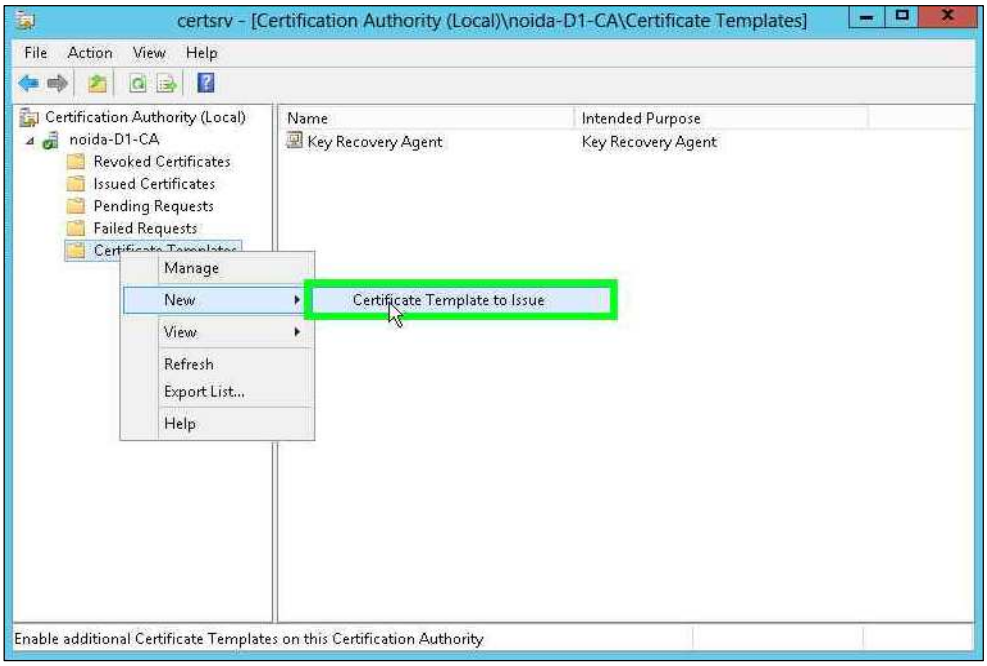
7. Select the **Subject Name** tab.
8. Uncheck the **Include e-mail name in subject name** check box.
9. Uncheck the **E-mail name** check box.



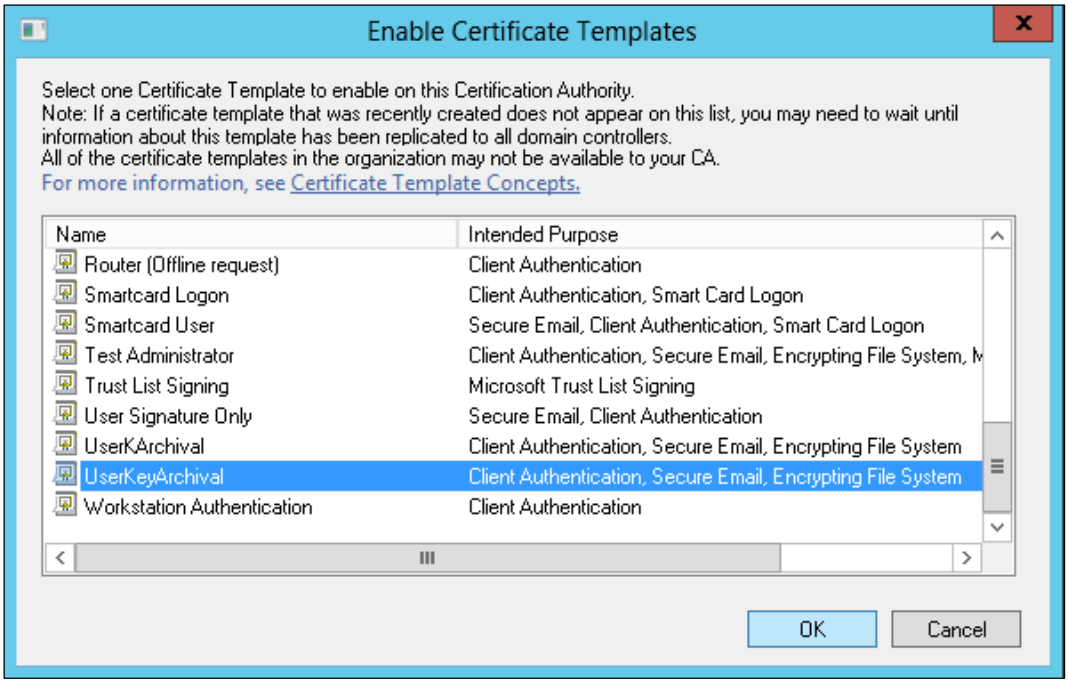
10. Click **Apply** and then **OK**.

To 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**.

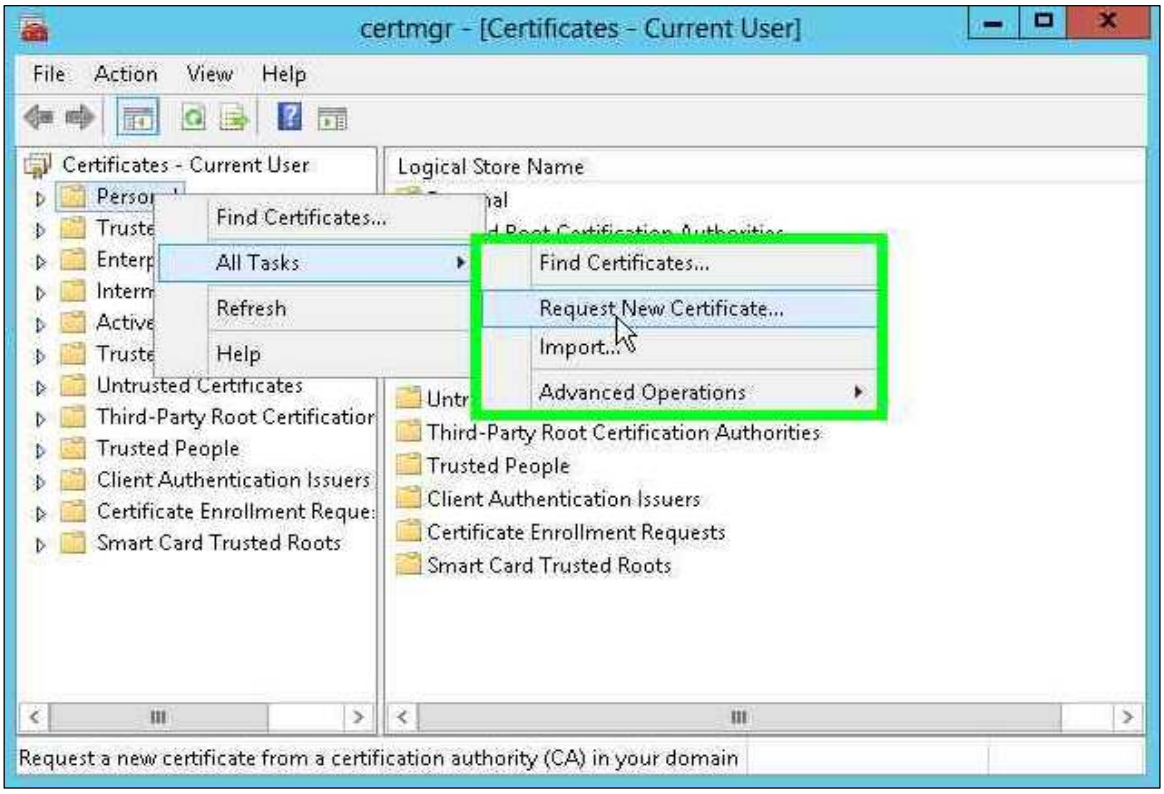


4. Select new template for key archival, click **OK**.

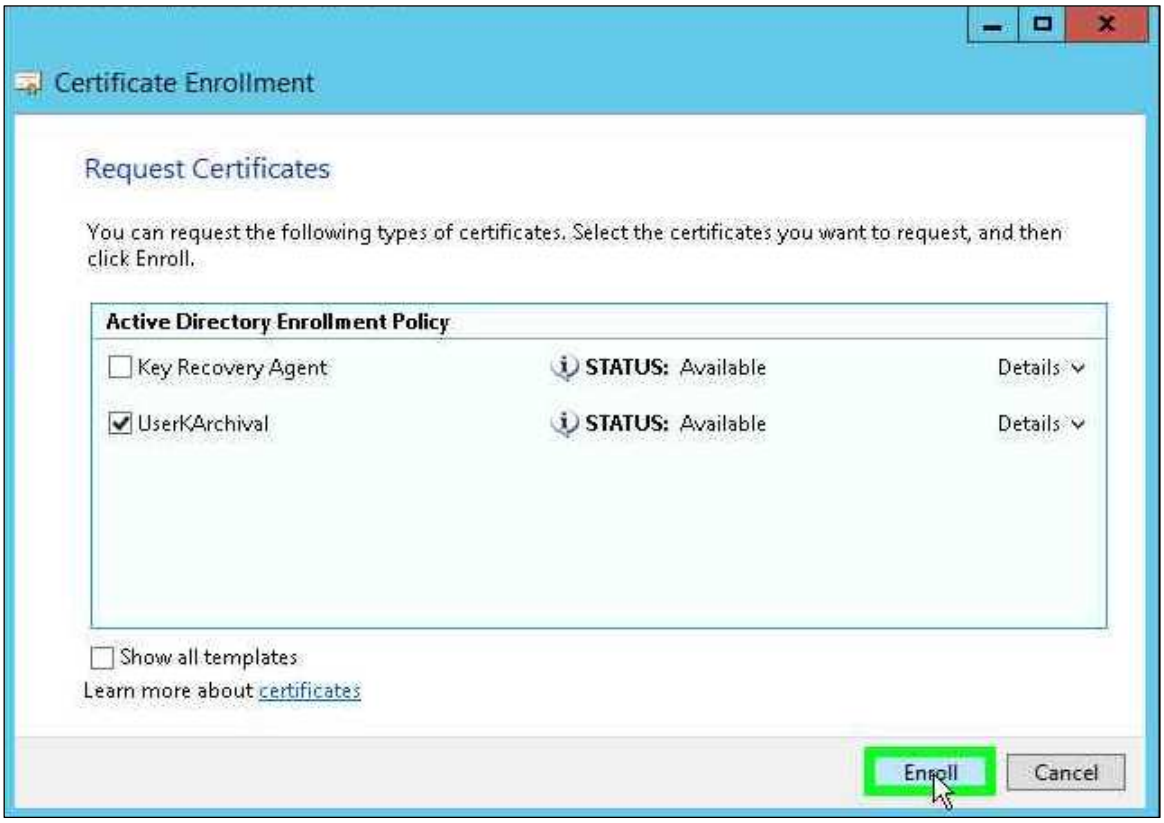


To issue a user template with key archival enabled

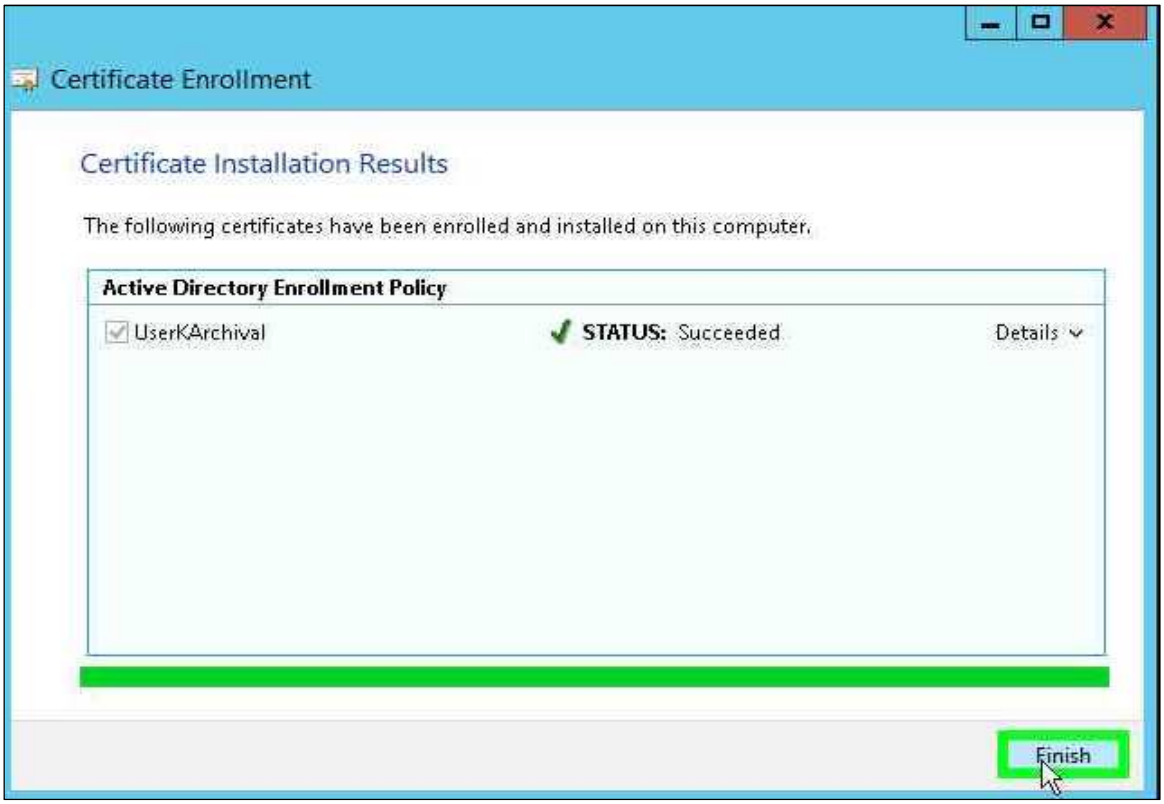
1. Open the command prompt and run the **certmgr.msc** command.
2. Right-click **Personal** node.
3. Select **All Tasks -> Request New Certificate**.



4. Click **Next**
5. Click **Next**.
6. Select the new template for key archival check box and click **Enroll**.


Certificate Enrollment
Request Certificates
You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.
Active Directory Enrollment Policy
Key Recovery Agent
STATUS: Available
Details
UserKArchival
STATUS: Available
Details
Show all templates
Learn more about certificates
Enroll
Cancel

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



9. Click **Finish**.

Performing a 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.

Install and configure 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.)

Setting 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 ADCS is successfully installed, 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 SafeNet 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. 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.

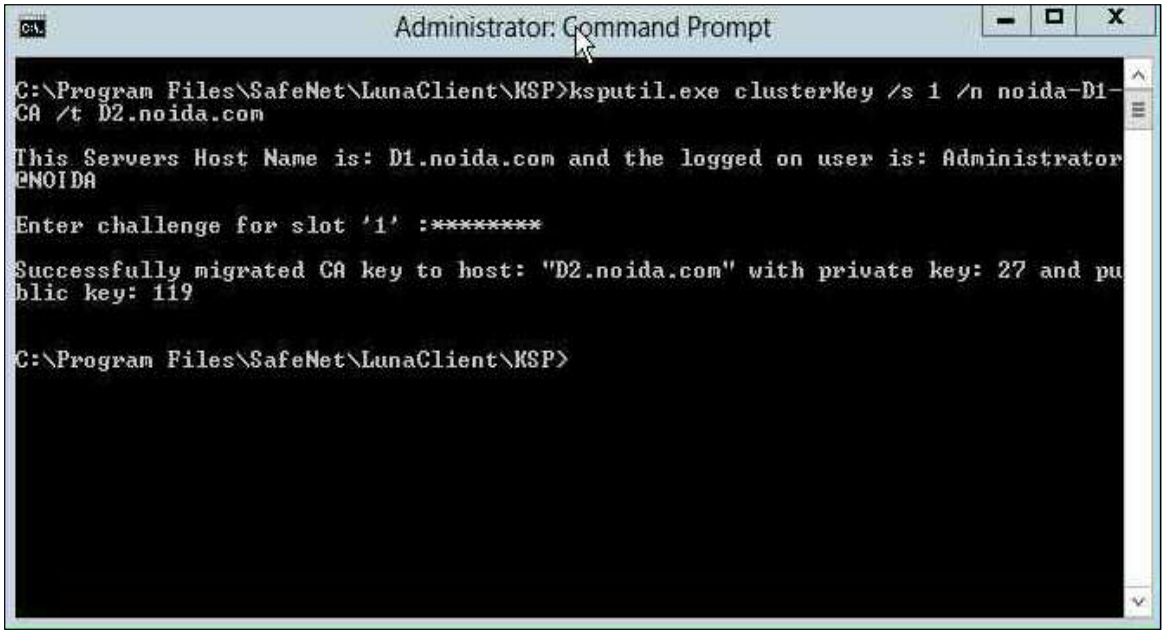
    ```
    ksputil clusterKey /s <slotNum> /n <CA_Name> /t <TargetHost_Name>
    ```

    Where,

    slotNum – slot number

    CA_name – name of the CA

    TargetHost_Name – FQDN of the second node



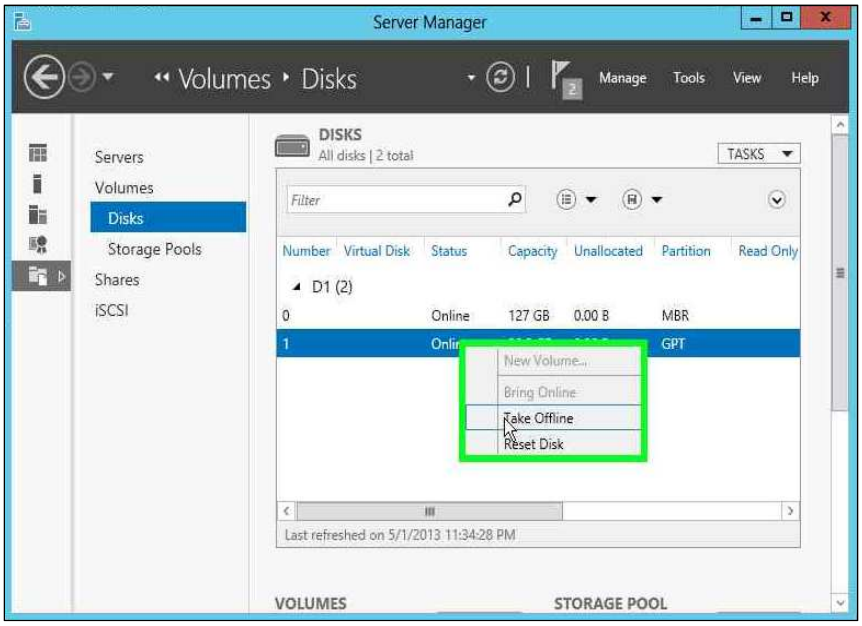
12. Click the **Action** menu, **All Tasks** and then **Stop Service**.

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

13. 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

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

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

Setting up the CA server role on the second cluster node

This section explains how to set up the second cluster node. To install the CA on the second node, complete the following:

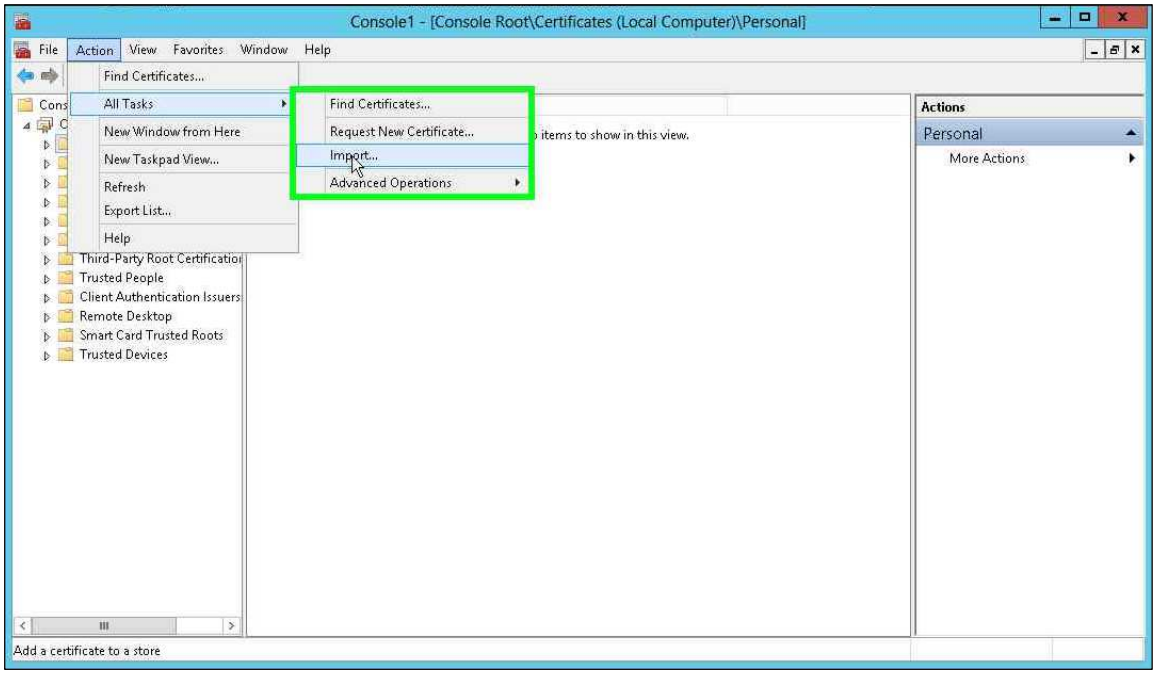
- To configure the secondary cluster node
- To import an existing CA certificate
- To add the AD CS role
- To configure the AD CS Role

To configure the secondary cluster node

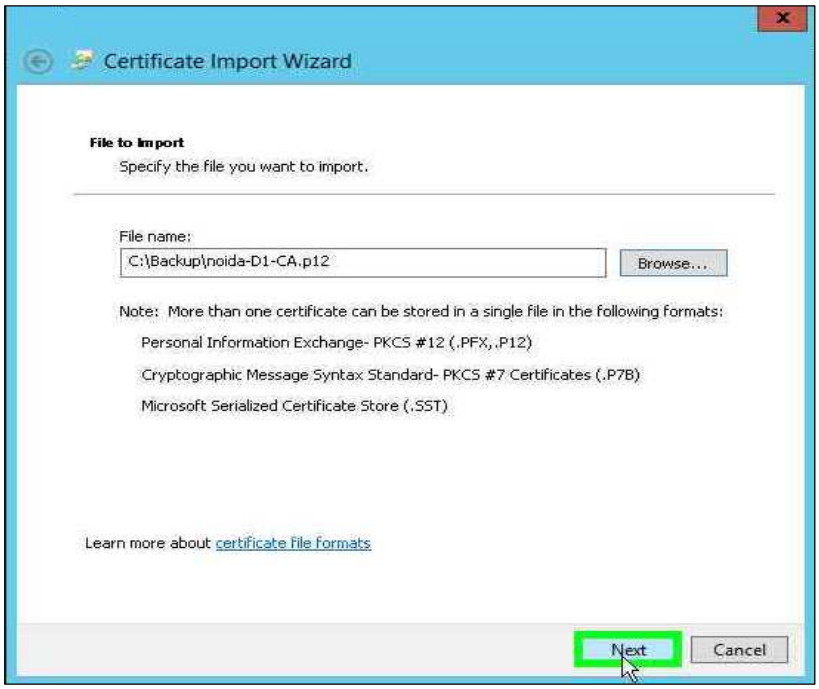
1. Log on to the cluster node with permissions to install the second cluster node. To install an enterprise CA, logon with enterprise permissions to the Active Directory domain. To install a standalone CA you may logon with local admin permissions if you don't want to register the CA in the Active Directory 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**.

To 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)*.



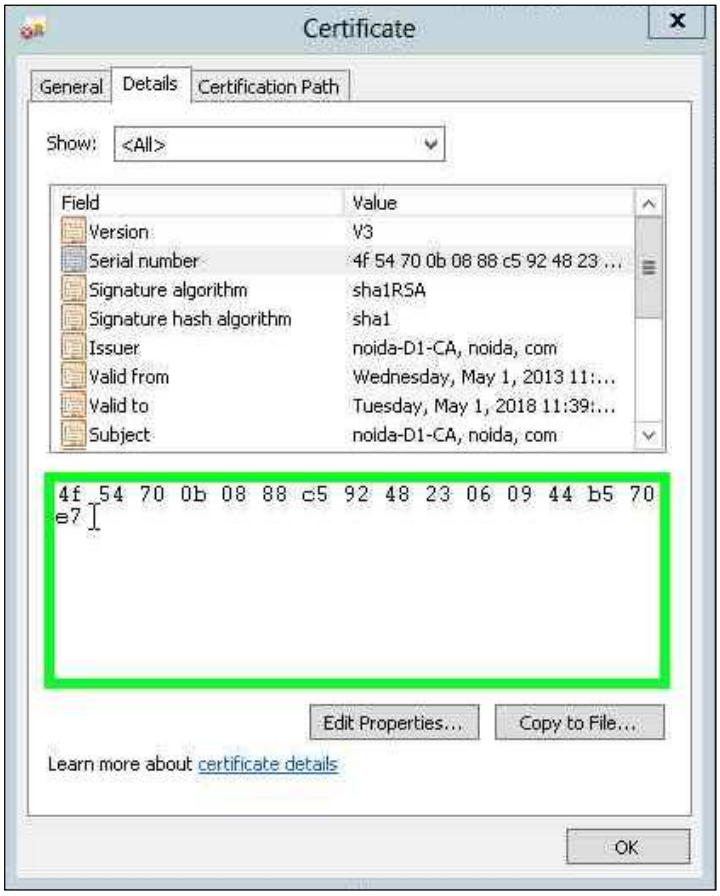
5. Type the password previously used to protect the private key. The password is required even if there is no private key in the PFX file. Click **Next.**

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

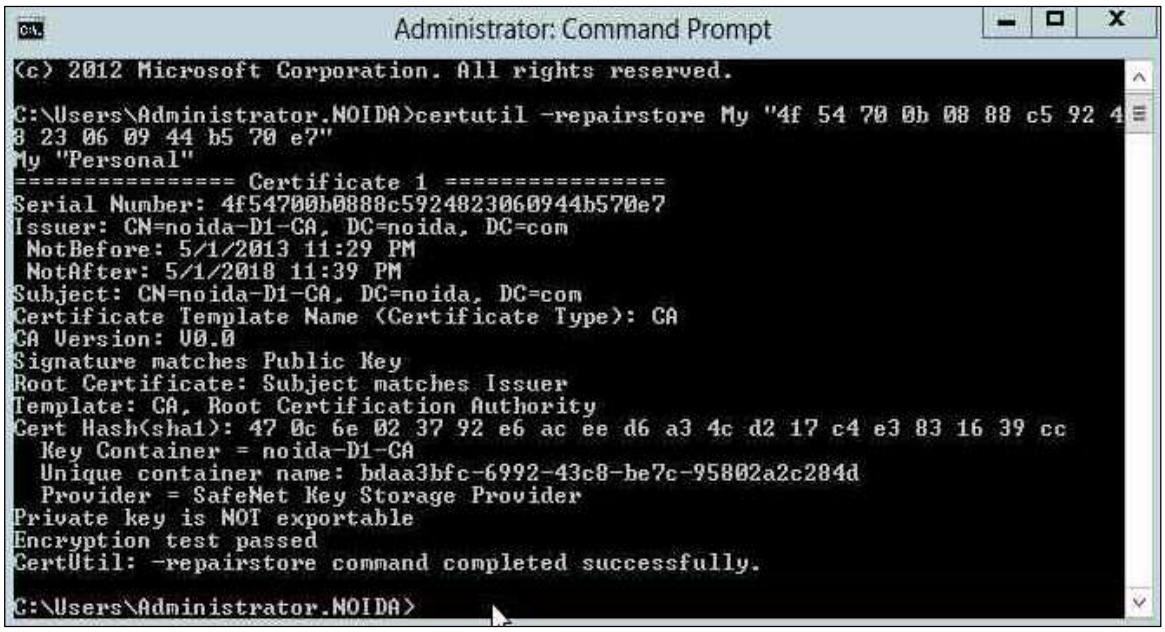
6. Select the Place all certificates in the following store radio button and select the **Personal** certificate store. Click **Next**.

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

12. Select the field **Serial Number** and copy the serial number into the clipboard. Click **OK**.

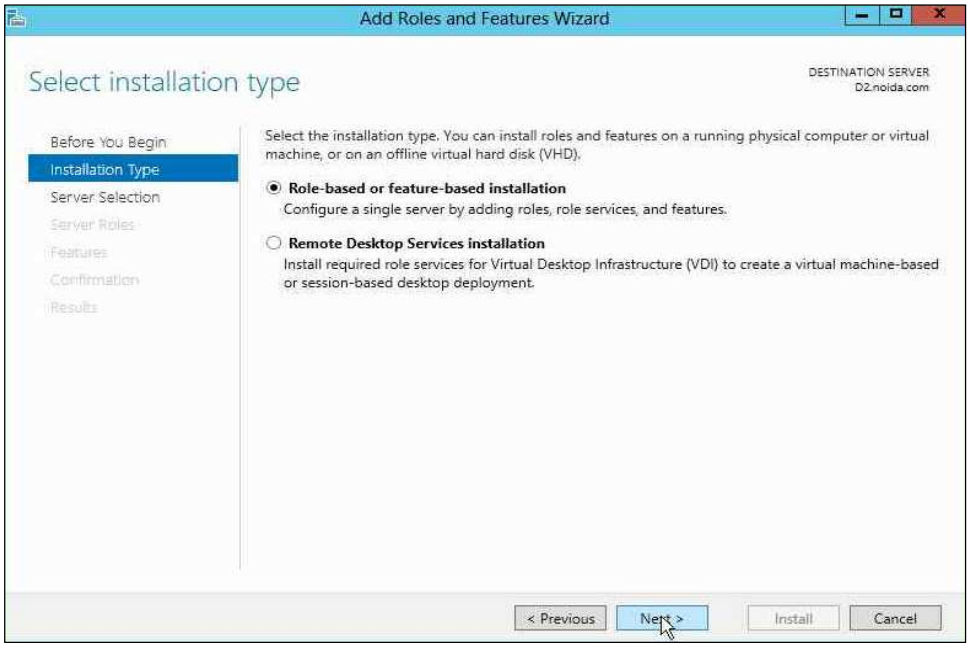


13. Open the command prompt and type `certutil -repairstore My "{Serial number}"` and press **Enter**.

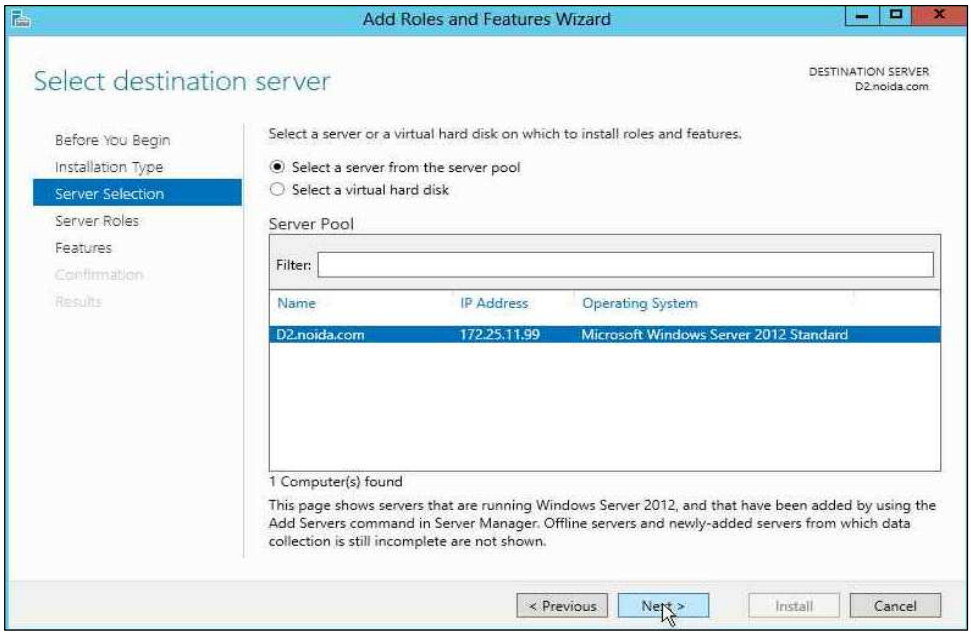


To add the AD CS role

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**.

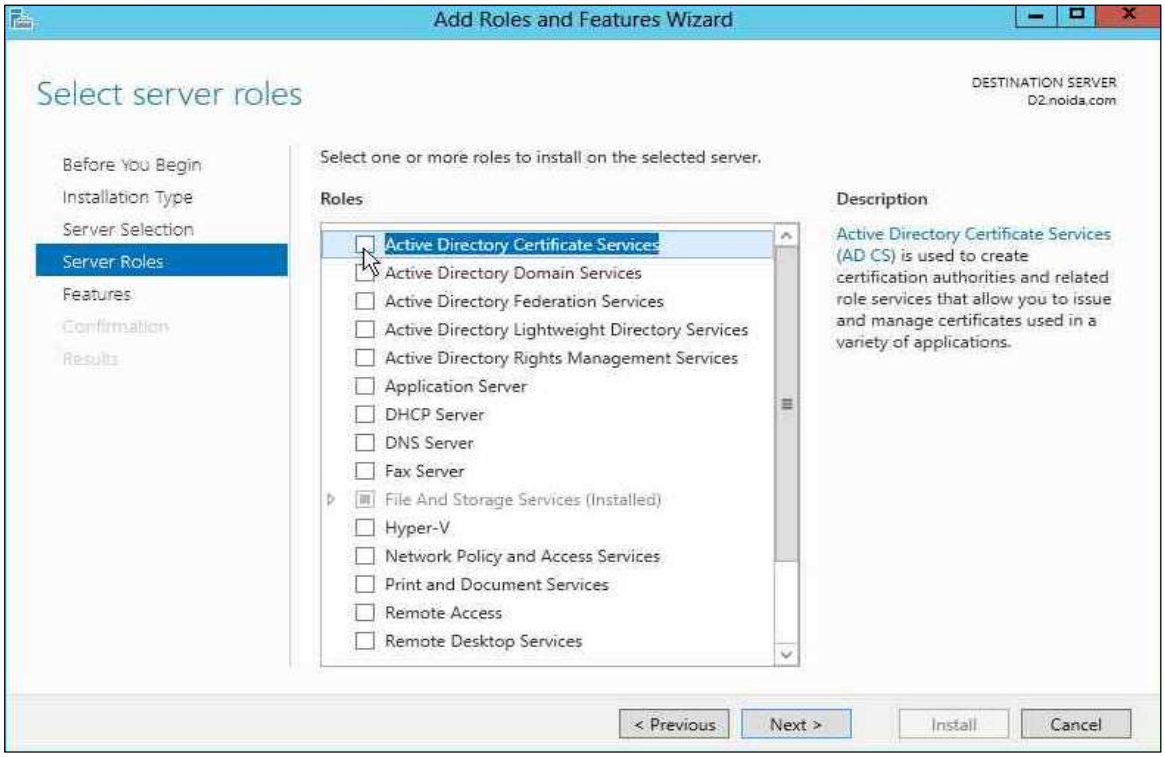


5. Select the **Select a server from the server pool** radio button and from **Server Pool** select your server.



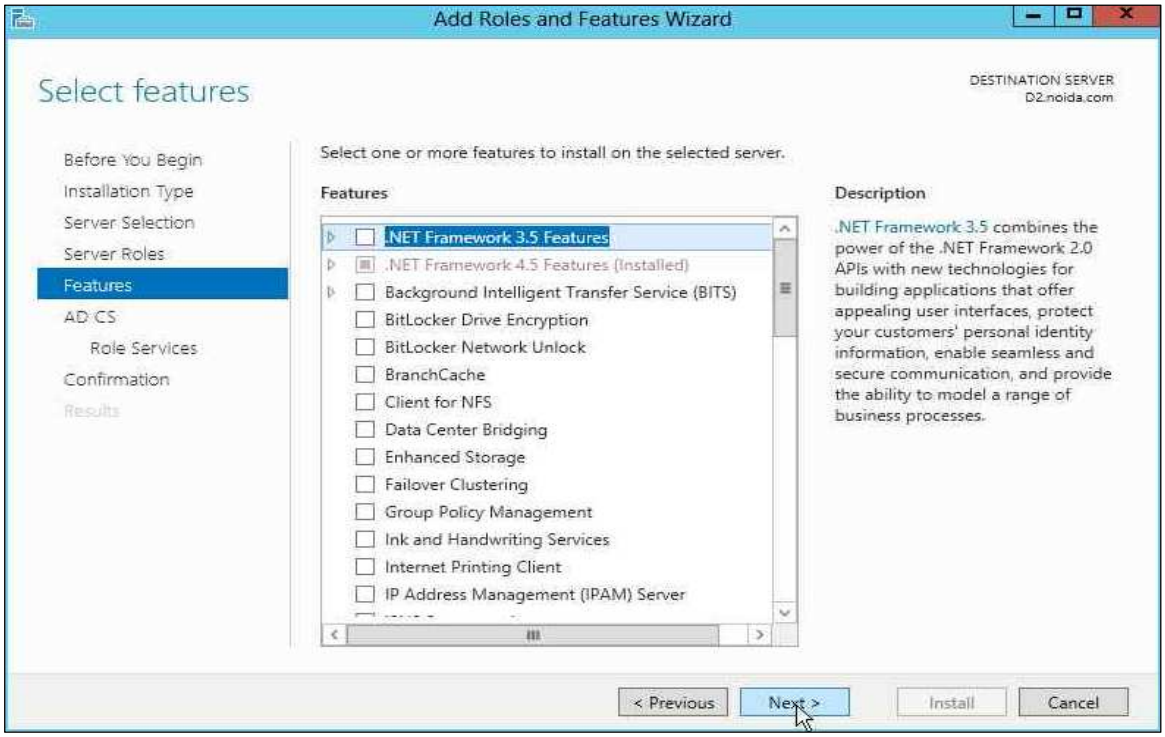
6. Click **Next**.

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



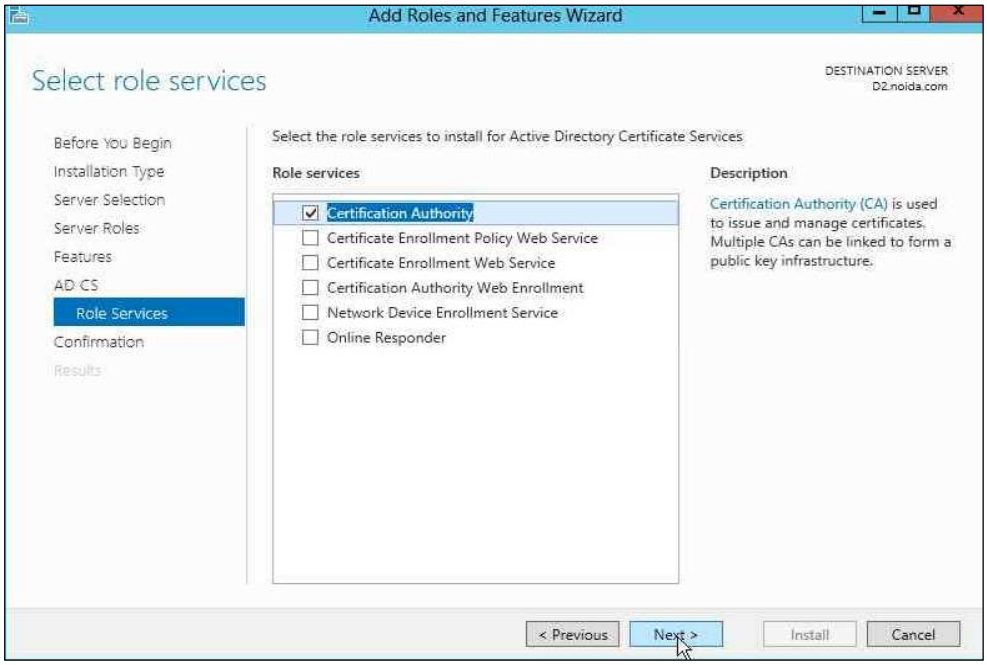
8. The **Add features that are required for Active Directory Certificate Services?** window displays. To add a feature, click the **Add Features** button.
9. Click **Next** to continue.

10. Click **Next** to continue.

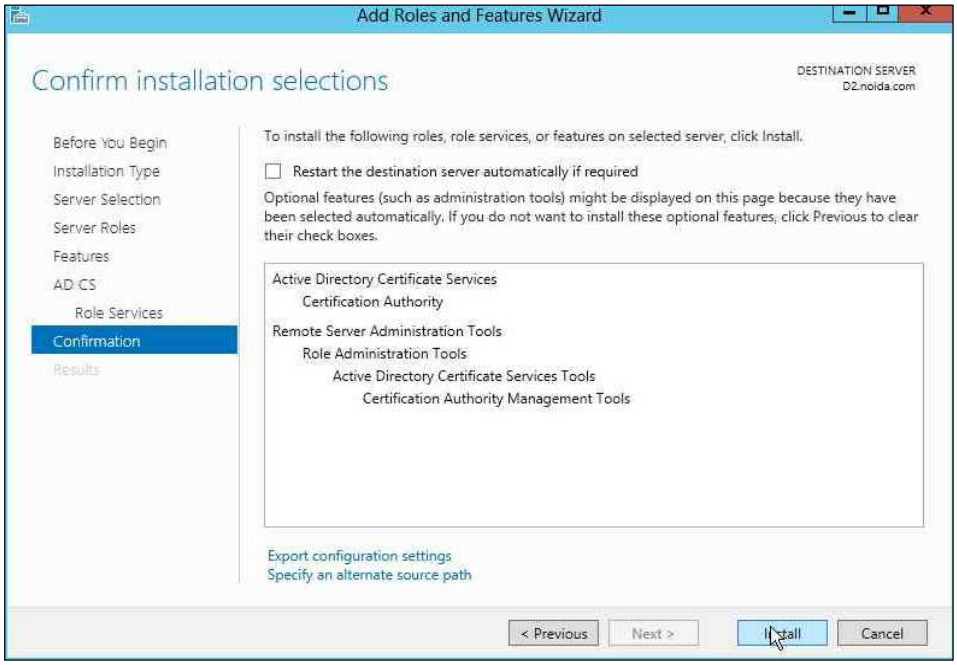


11. Click **Next** to continue.

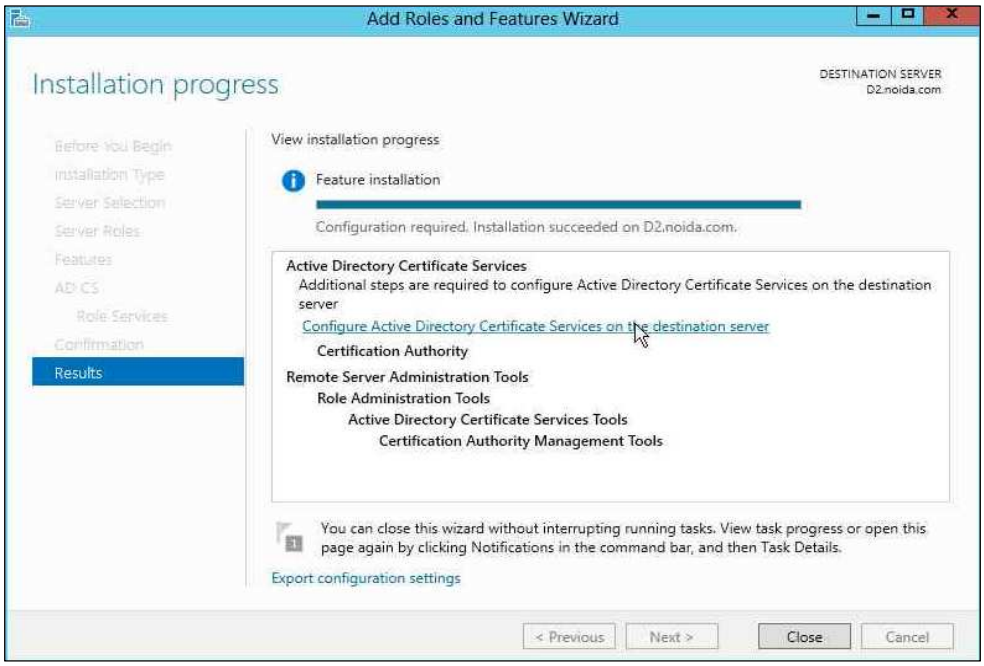
12. Select the **Certification Authority** check box from the **Role services** list and click **Next**.



13. Click **Install.**

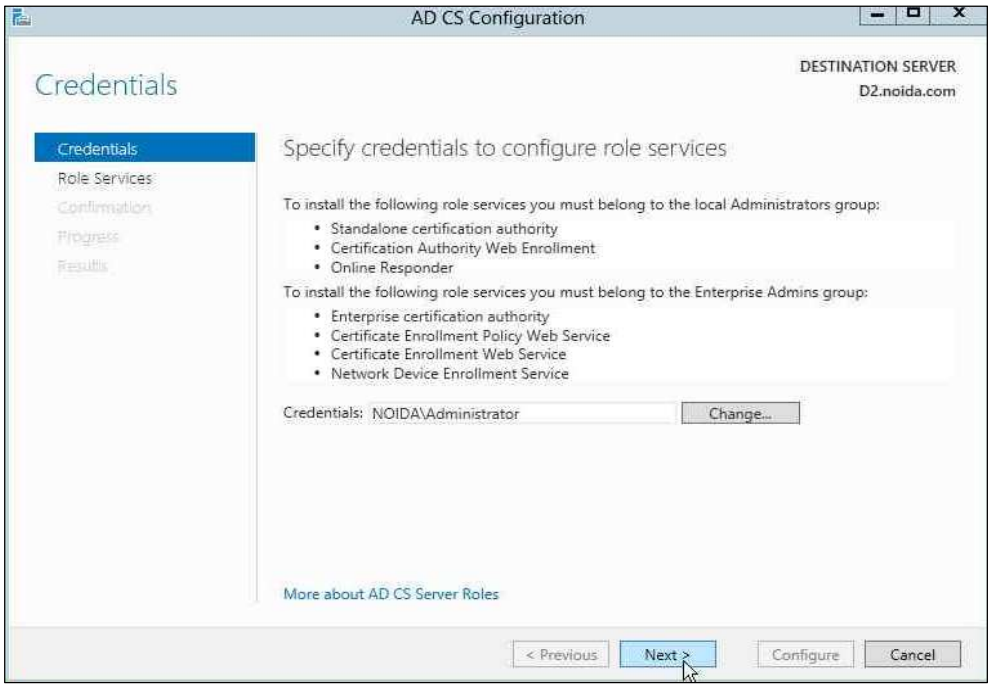


14. Once installation is complete, click the link **Configure Active Directory Certificate Services on the destination server** the AD CS Configuration wizard displays.



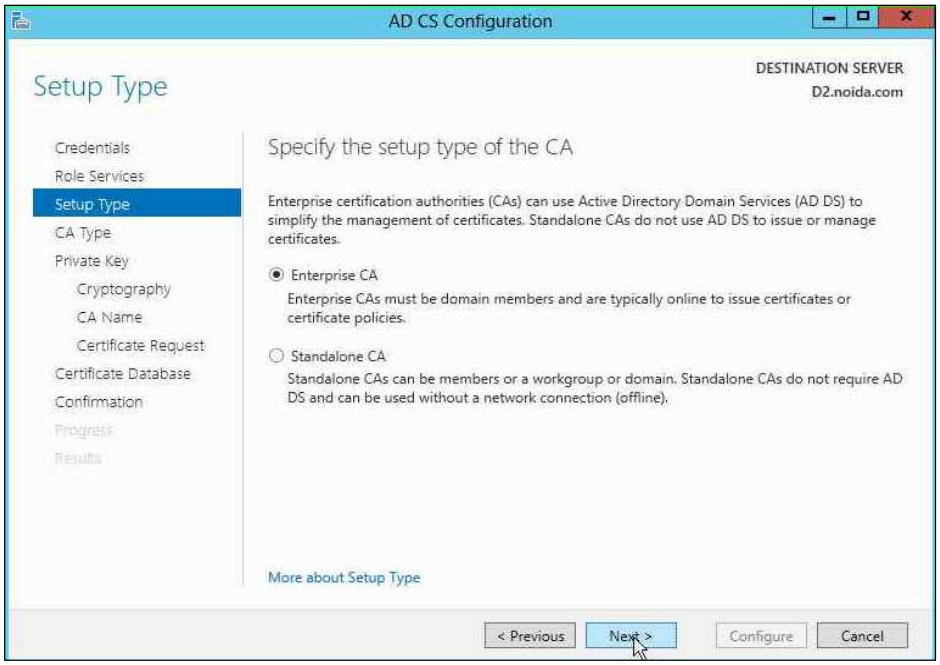
To configure the AD CS Role

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

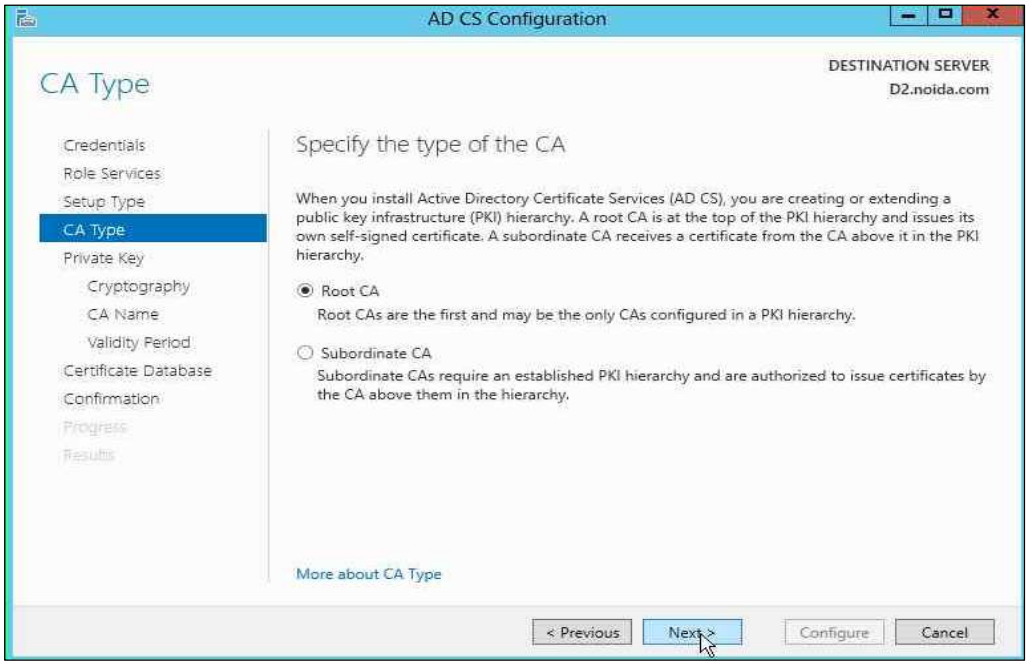


2. Select the **Certification Authority** check box and click **Next**.

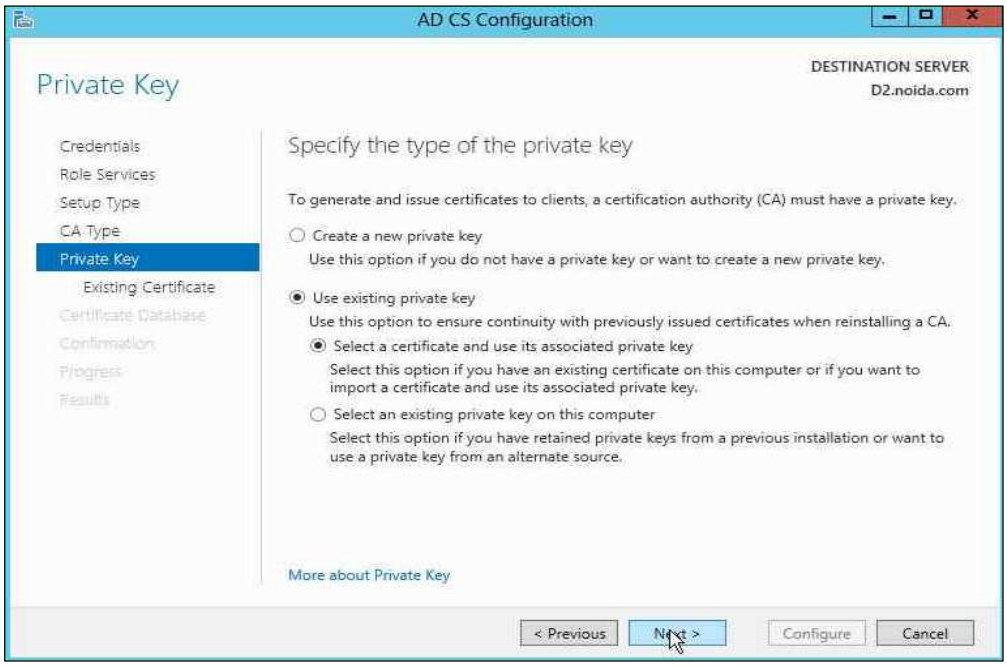
3. Select **Enterprise CA** as **Setup Type** and click **Next**.



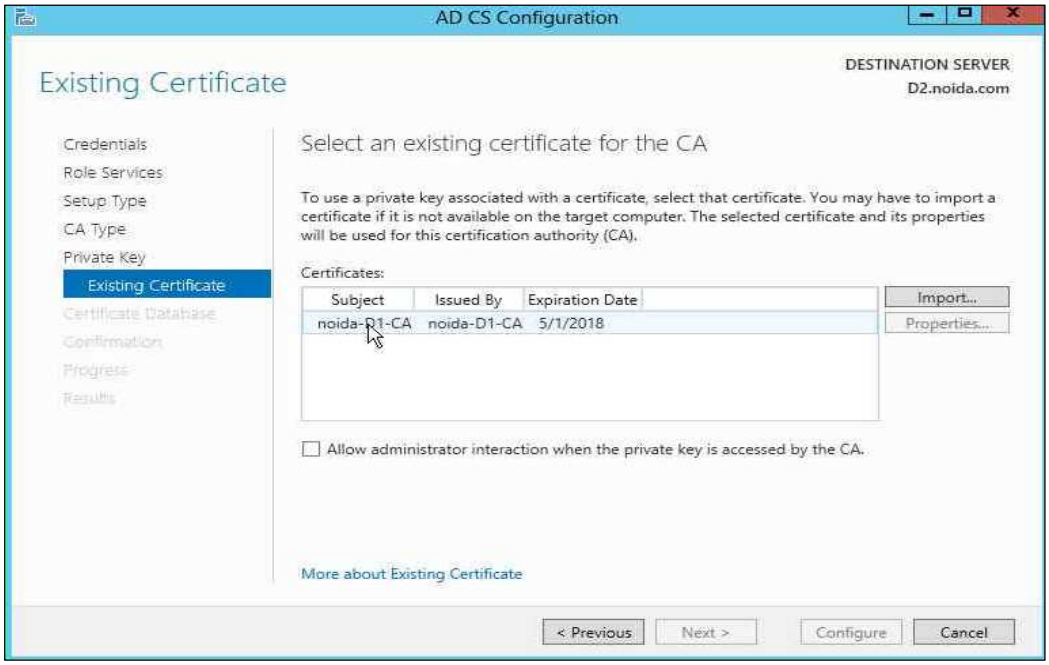
4. Select **Root CA** as type of CA and click **Next**.



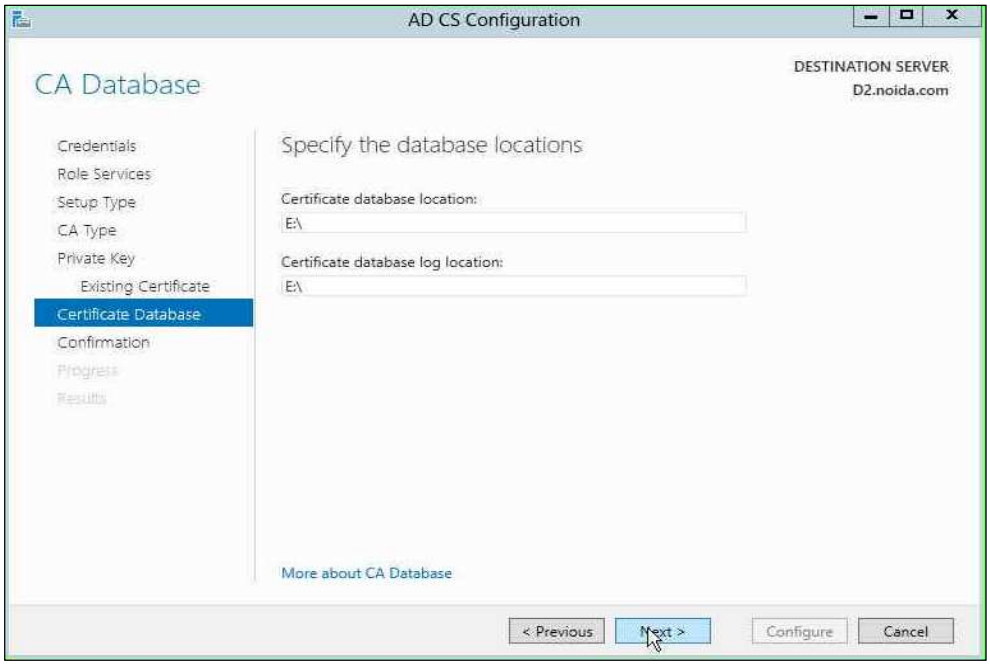
5. Select the **Use existing private key** radio button and choose the option **Select a certificate and use its associated private key** and click **Next**.



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

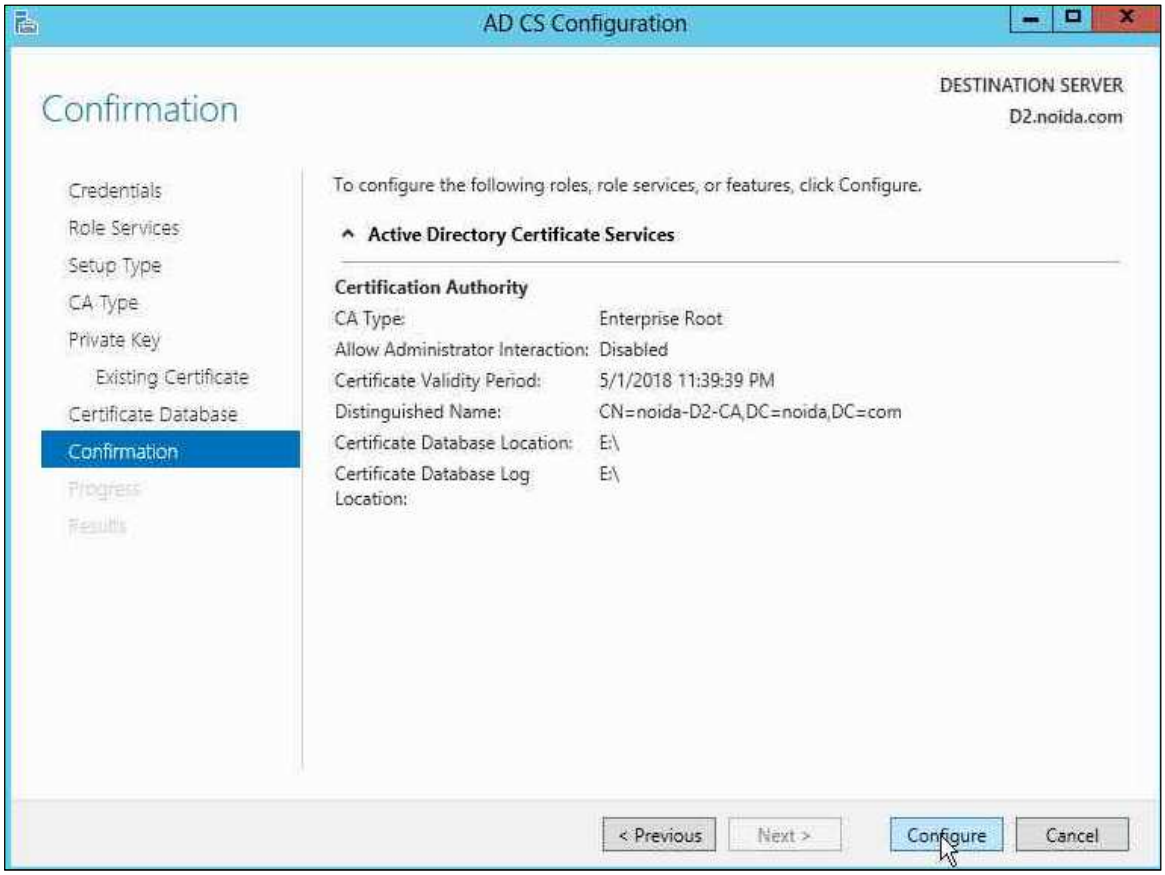


7. Change the default paths for the database log location. Click **Next** to continue.



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

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

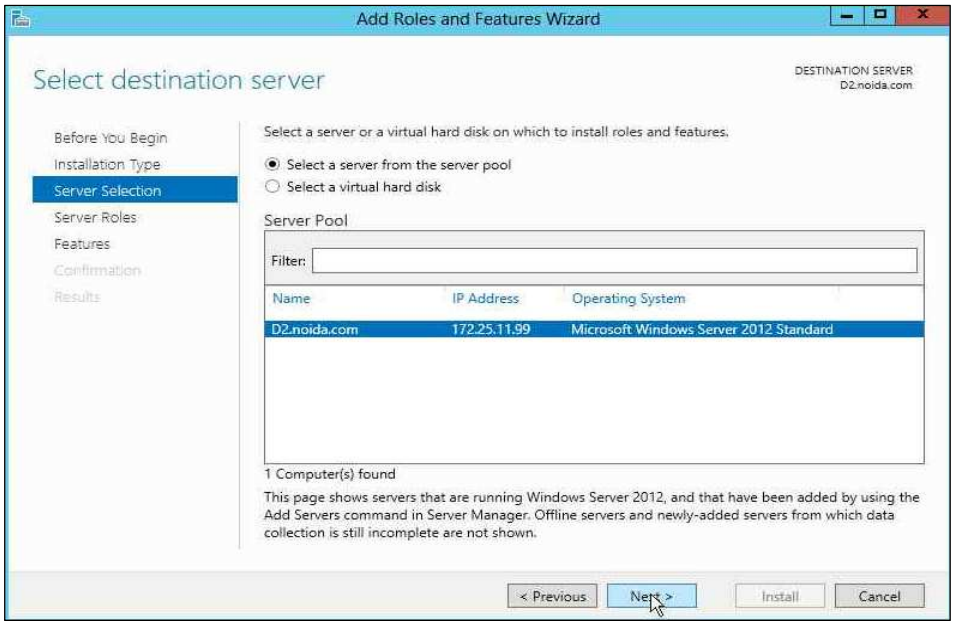


10. Click **Close** to finish the **Role** installation.
11. Log off of the cluster node two.

Setting up the Failover Cluster feature on both the cluster nodes

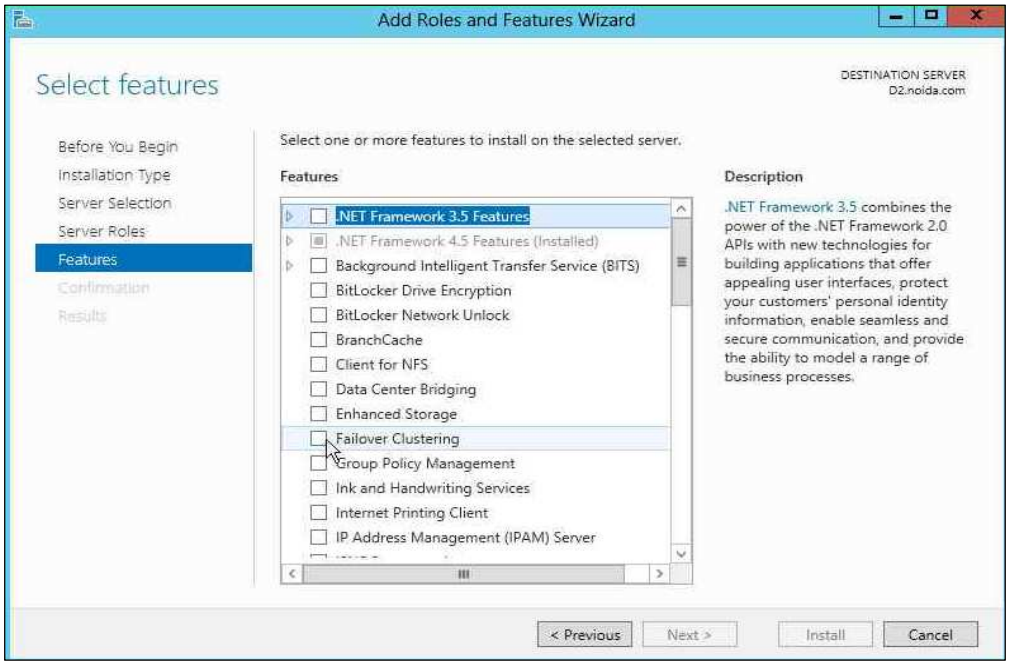
Repeat the following steps on both the cluster nodes:

1. Log on to the cluster nodes 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 pool** radio button option and from **Server Pool** select your server.

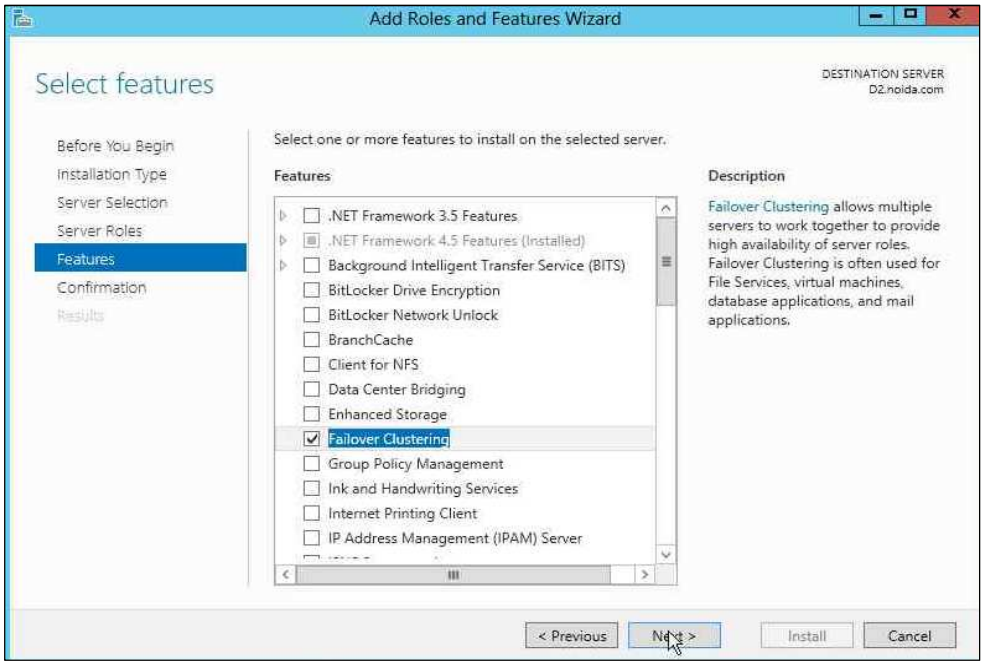


7. Click **Next** twice.

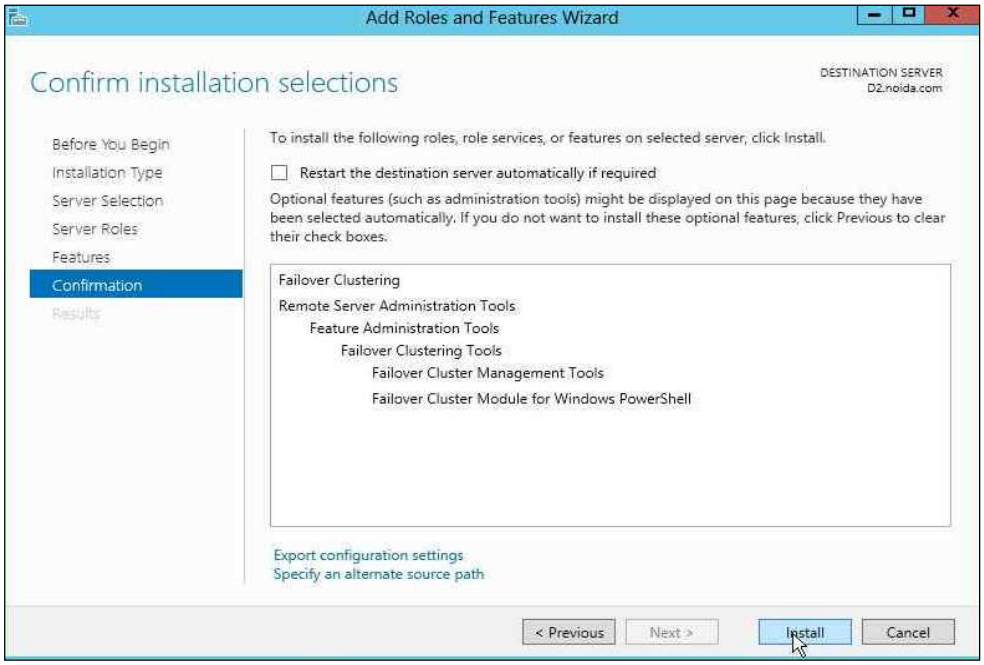
8. From the list of available features, select the **Failover Clustering** check box and click **Next**.



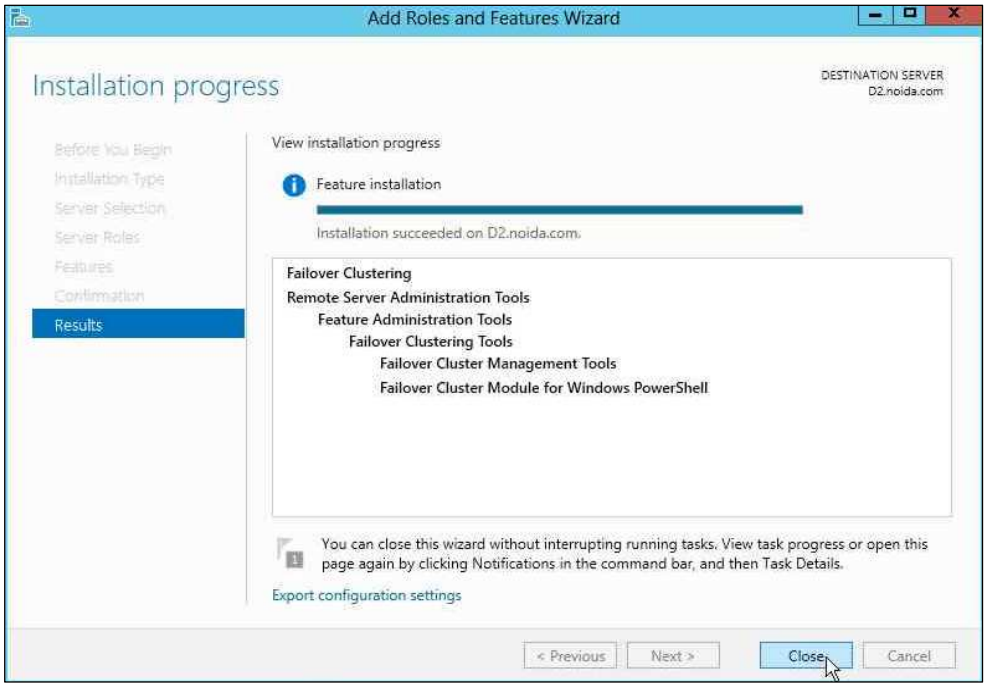
9. A pop up displays stating **Add features that are required for Failover Clustering?** To add a feature, click the **Add Features** button.
10. Click **Next**.



11. Click **Install**.

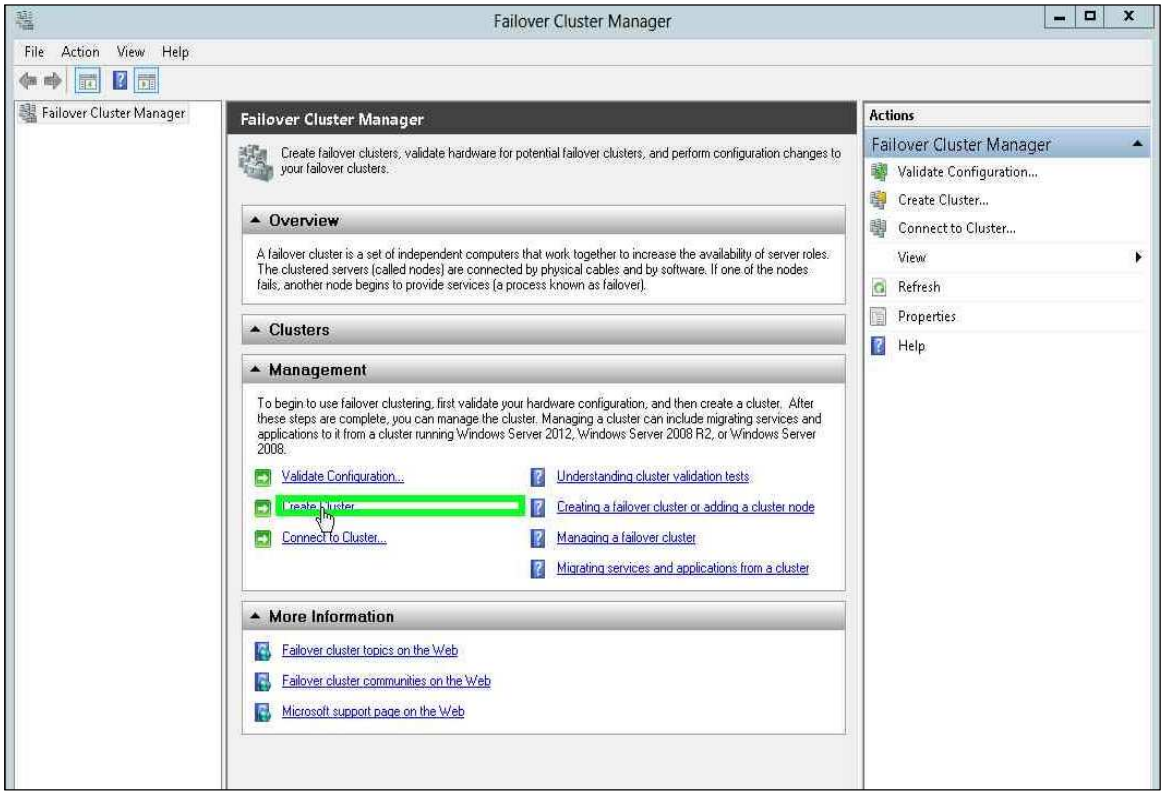


12. Click **Close**.



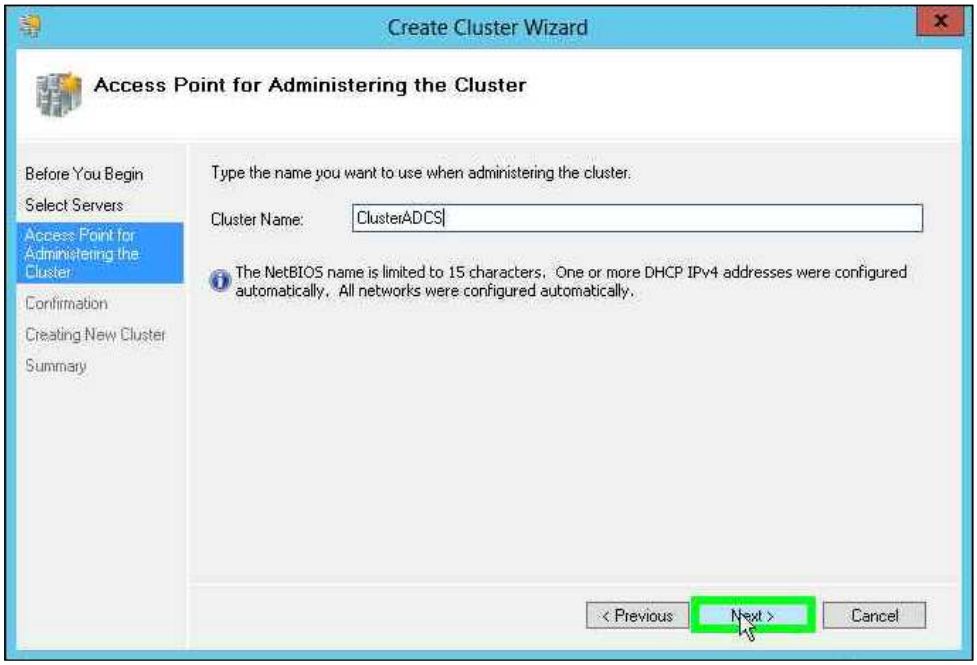
Creating a Failover Cluster

1. Log on to the cluster node where the storage is attached.
2. Open **Server Manager**, Click **Tools** and select **Failover Cluster Manager**.
3. From the **Action** menu, click **Create a Cluster**.

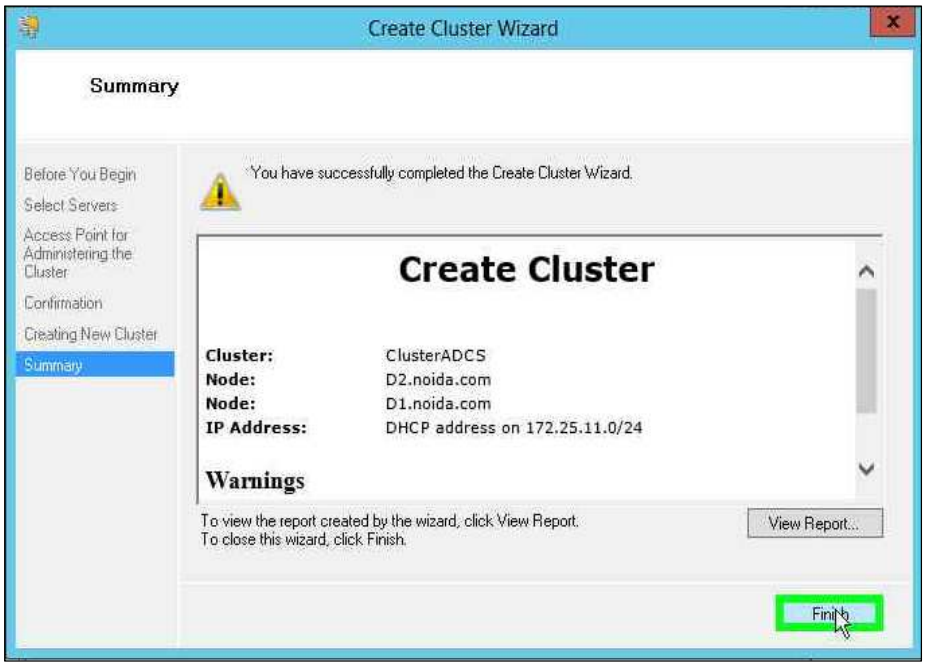


4. On the **Before You Begin** page click **Next**.
5. Enter the cluster node name (computer name) of the first cluster node in the **Enter Server Name** field and click **Add**.
6. Enter the cluster node name of the second cluster node in the **Enter Server Name** field and click **Add**.
7. Click **Next**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

8. Enter the **Cluster Name** and click **Next** until you reach the Summary page. .



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

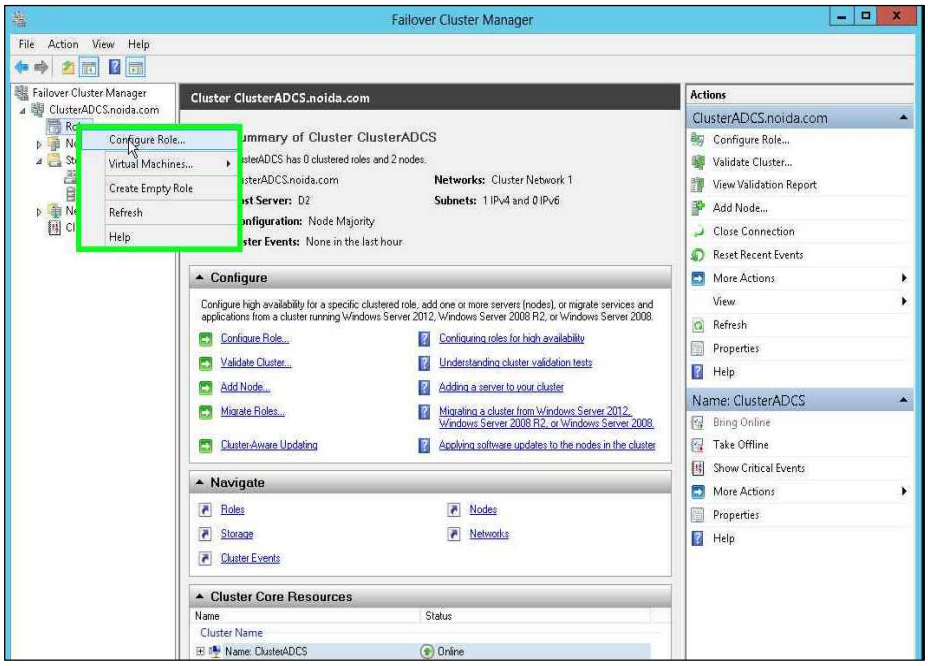


Configuring the ADCS Failover Cluster

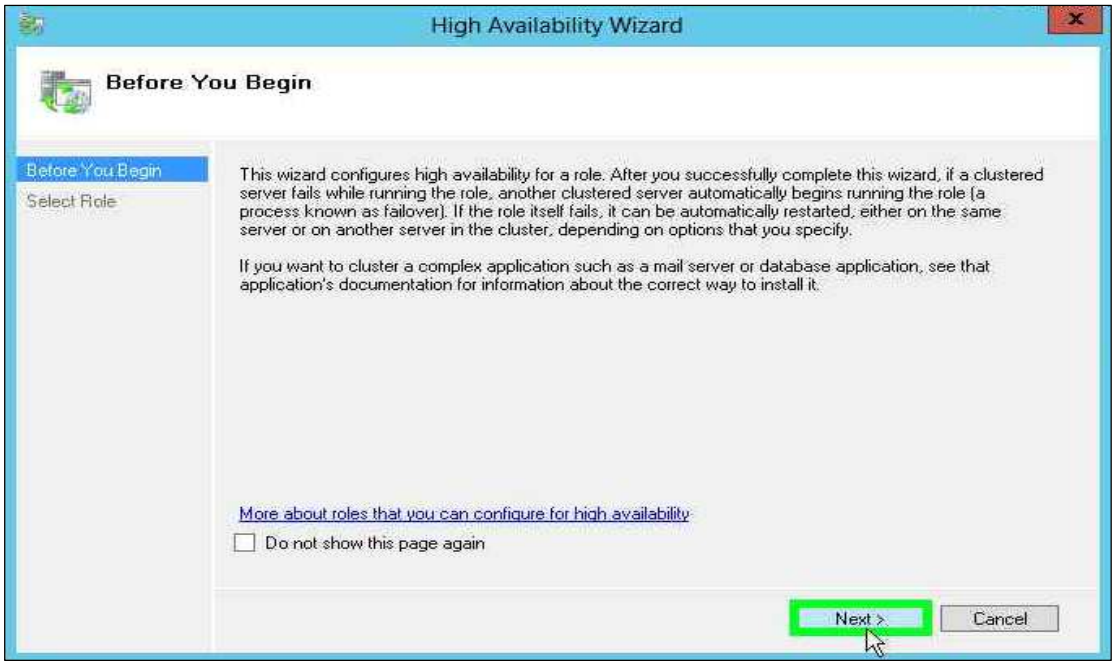
You can configure an ADCS Failover configuration to support your certificate eservices.

To configure the ADCS failover cluster

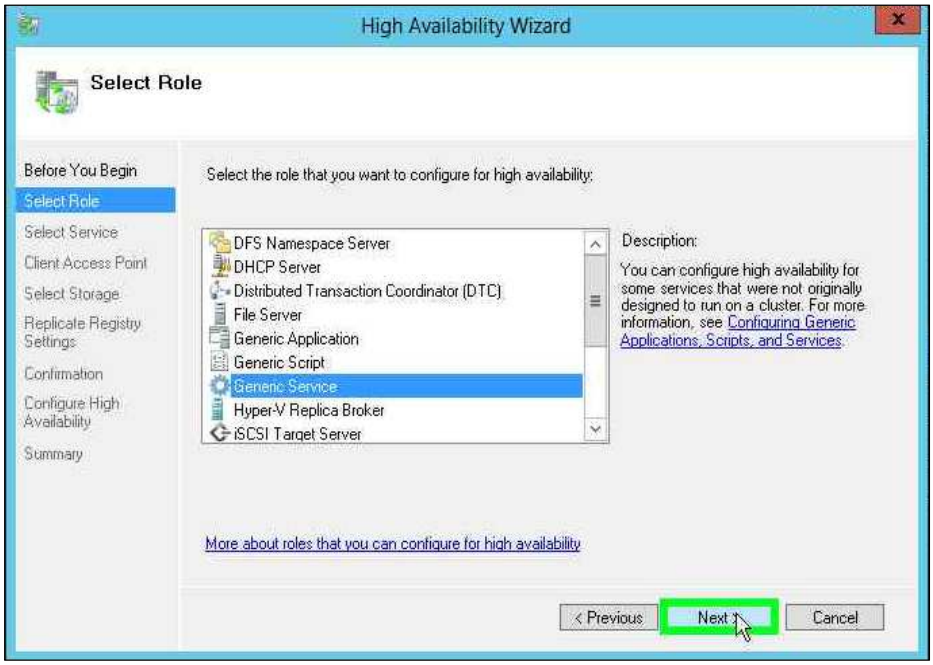
1. In the **Failover Cluster Management** snap-in, right-click **Role** and select **Configure Role**.



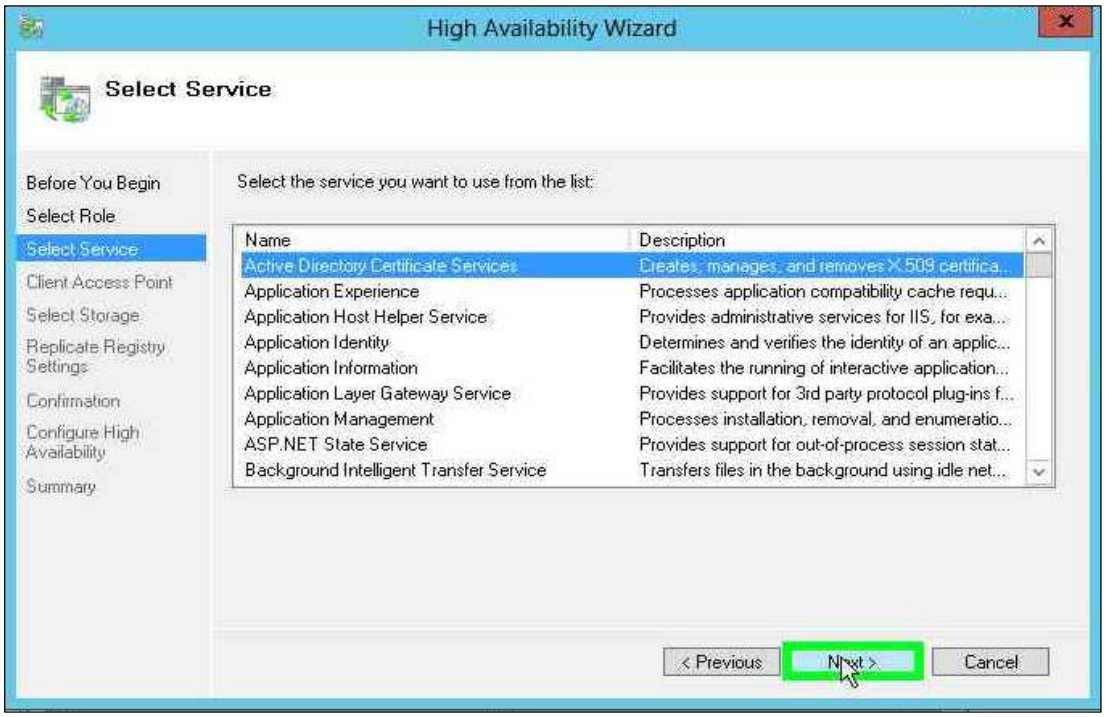
2. On the **Before you Begin** page click Next.



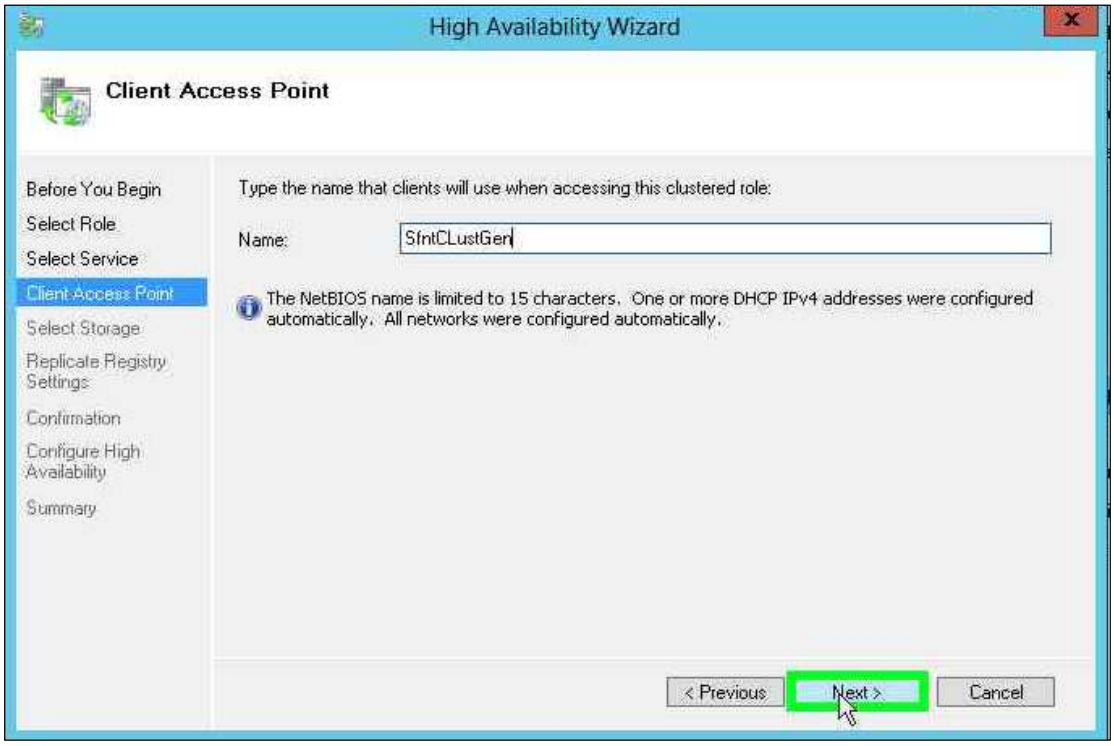
3. From the role list, select **Generic Service** and click **Next**.



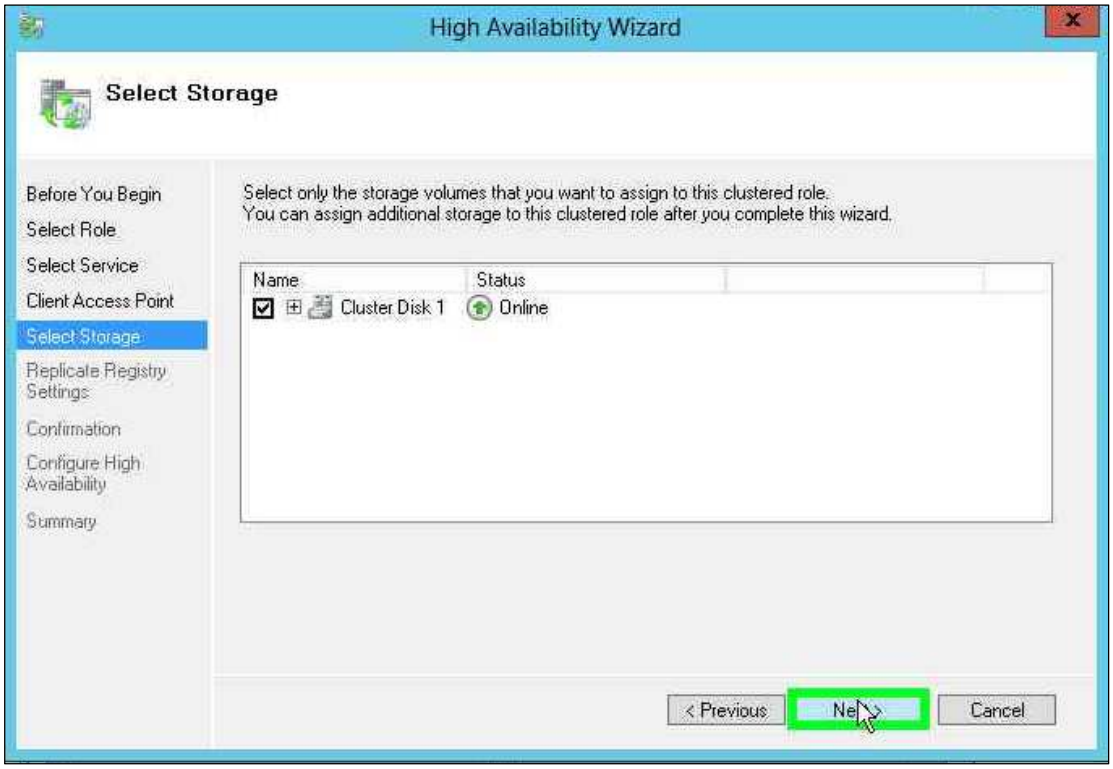
4. From the service list, select **Active Directory Certificate Services** and click **Next**.



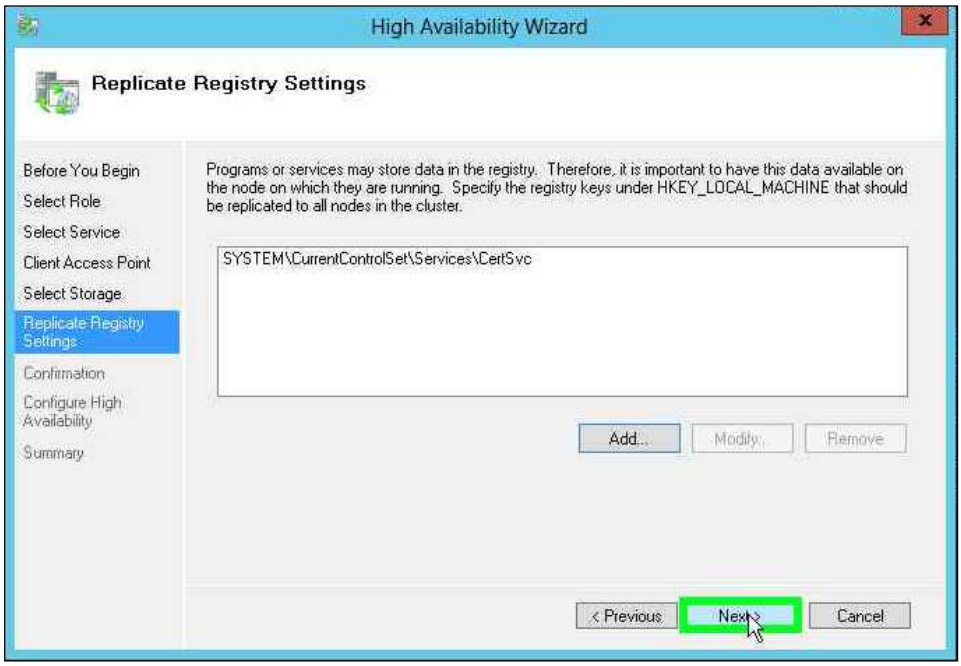
5. On the Client Access Point page enter the service name in the **Name** field and click **Next**.



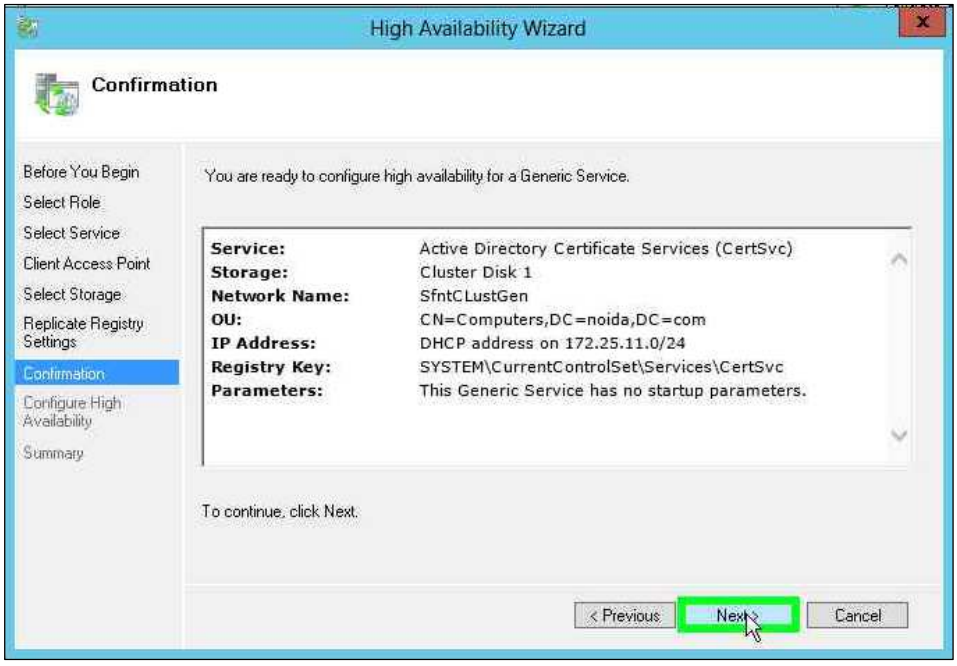
6. Select the disk storage that is still mounted to the node and click **Next**.



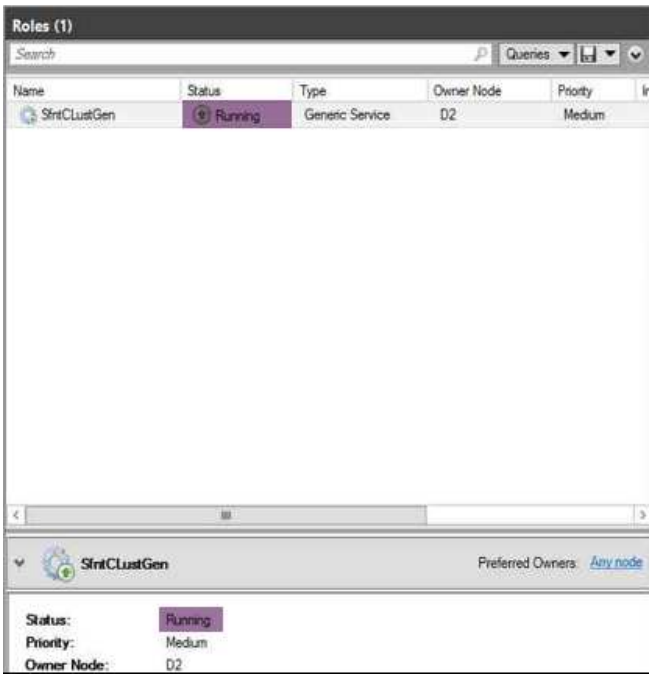
7. Configure a shared registry hive, click the **Add** button and enter **SYSTEM\CurrentControlSet\Services\CertSvc** and click **OK**.



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.



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. Execute the ksputil.exe utility to migrate the keys to the cluster.

    ```
    ksputil c /s <SlotNum> /t <CAClusterService_Name> /n <CA_Name>
    ```

    Where,

    <SlotNum> – slot number

    <CAClusterService_Name> – name of the CA Cluster service configured

    <CA_Name> – name of the CA

Creating 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}`.

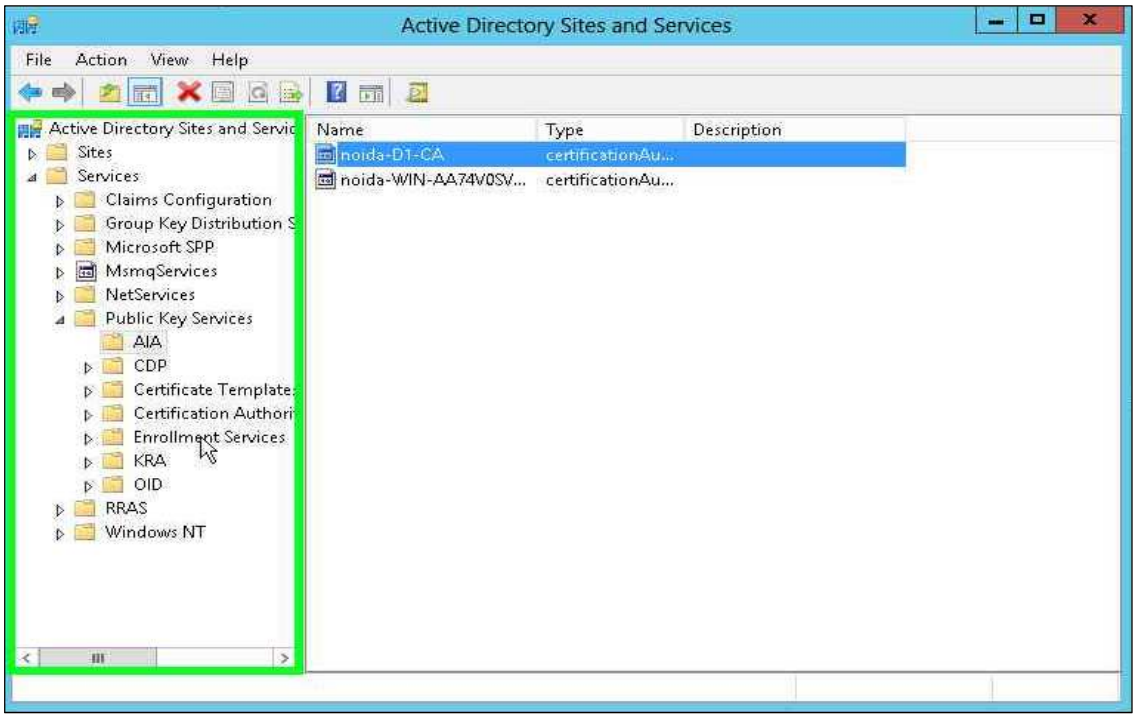
Modifying the CA configuration in Active Directory

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.

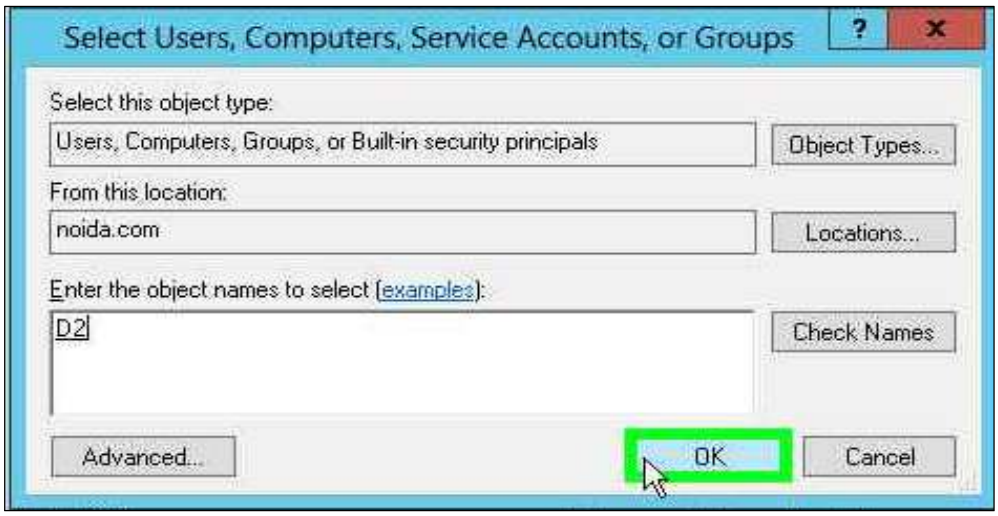
To modify the CA configuration in the Active Directory

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**.

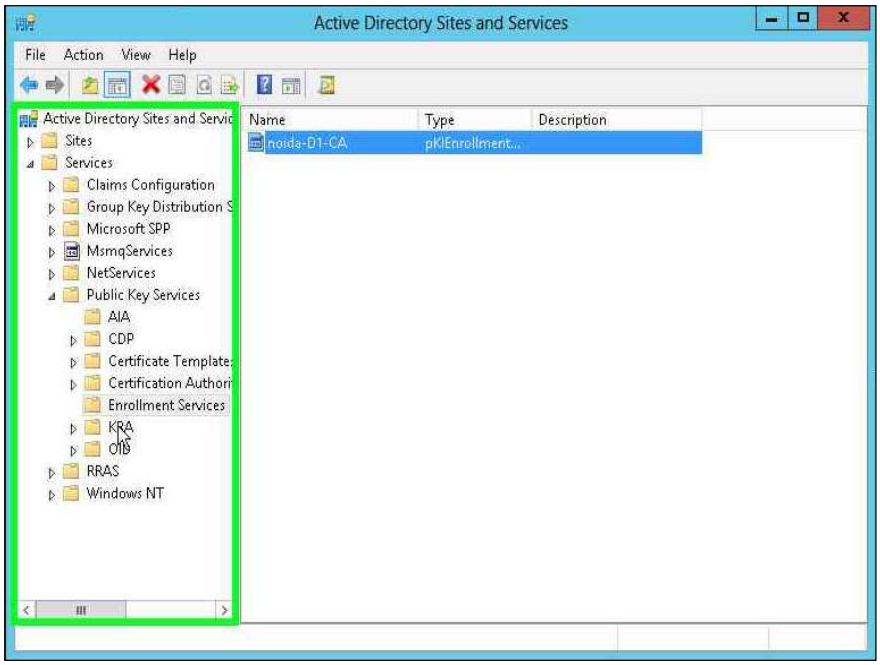


5. In the middle pane, select the CA name as it shows in the **Certification Authority** MMC snap-in.
6. From the **Action** menu select **Properties**. Click the **Security** tab and select **Add…**.

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**.

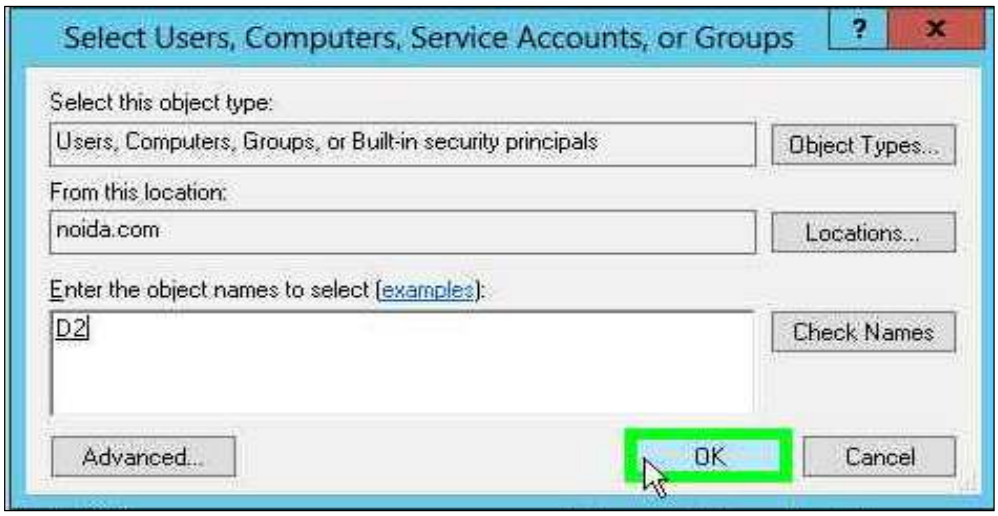


9. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.
10. Click **OK**.
11. In the left pane, select **Enrollment Services**.

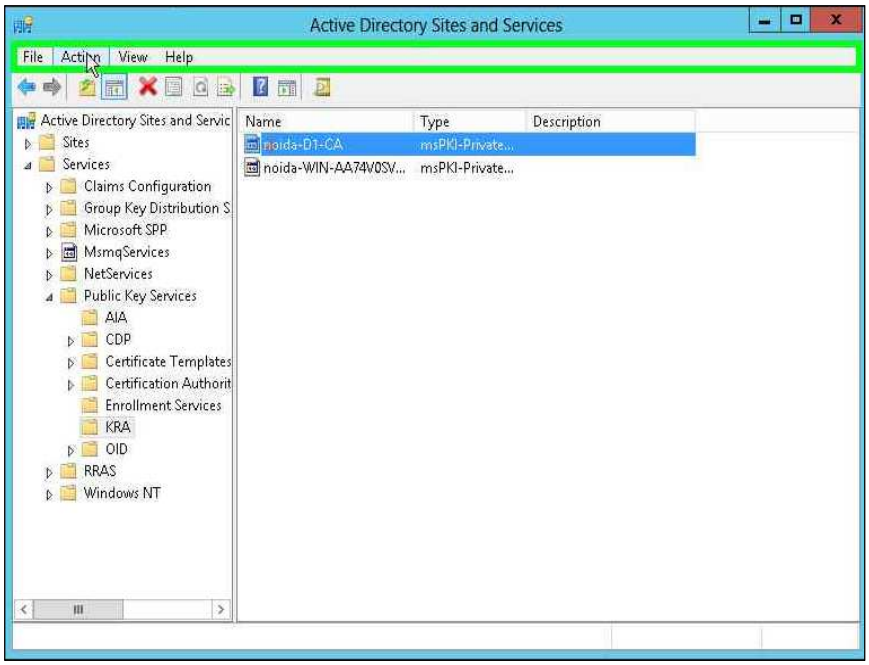


12. In the middle pane, select the CA name.
13. From the **Action** menu, select **Properties** click the **Security** tab and select **Add…**.

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**.

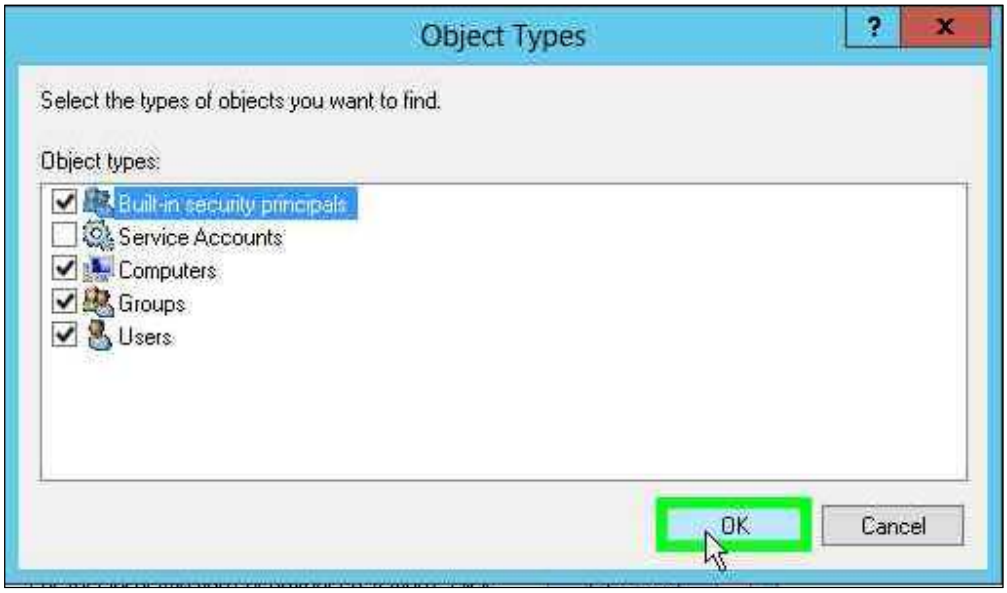


16. Ensure that the computer accounts of both the cluster nodes have **Full Control** permissions.
17. Click **OK**.
18. In the left pane, select **KRA**.

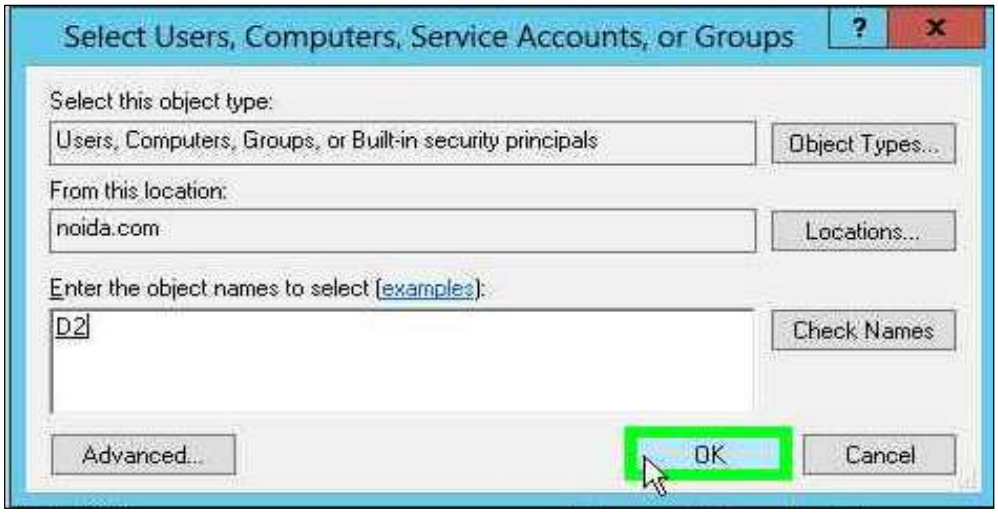


19. In the middle pane, select the CA name.
20. From the **Action** menu select **Properties** click the **Security** tab and select **Add…**.

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.

3

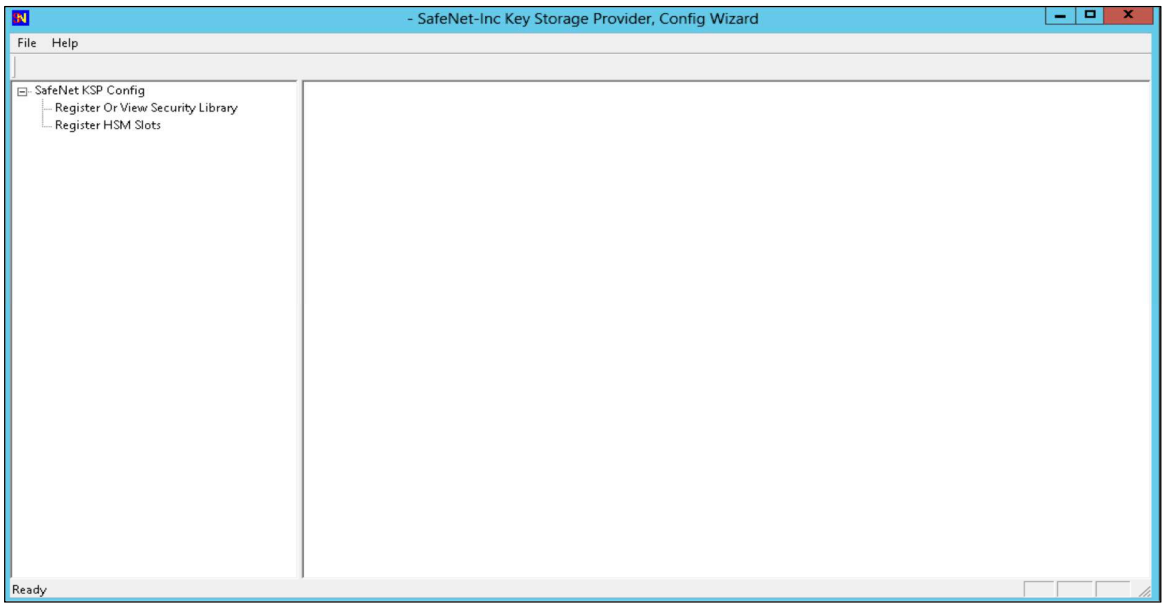
Migrate CA keys from Microsoft Software Key Storage Provider to SafeNet Key Storage Provider

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

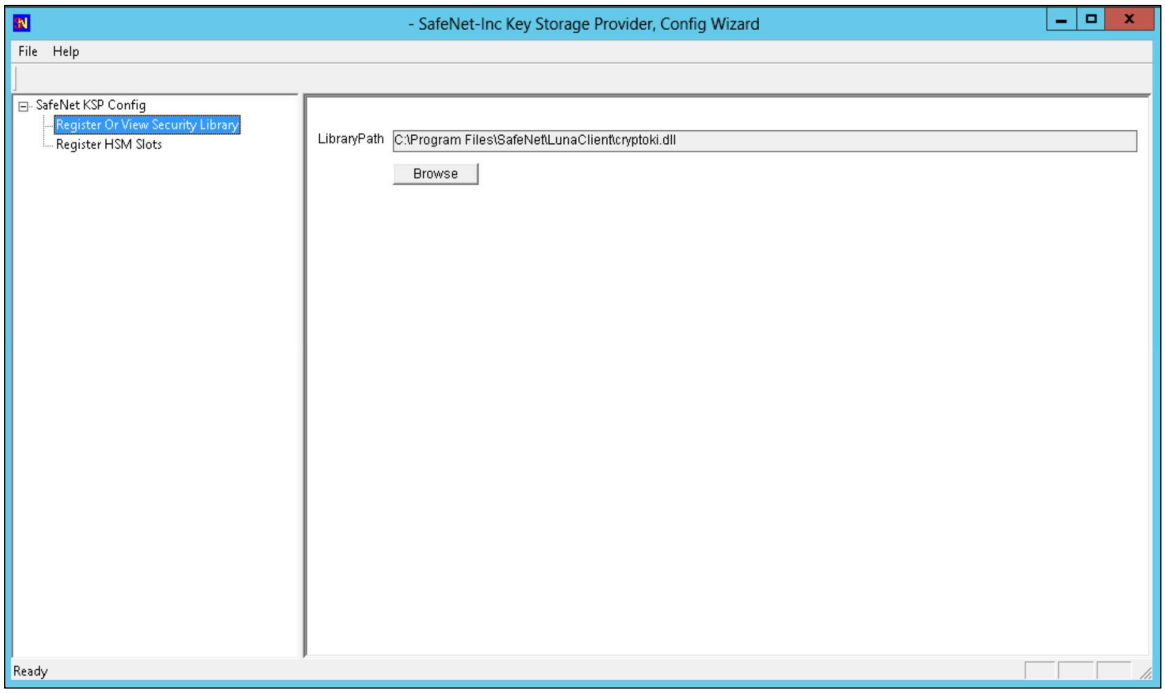
Configuring the SafeNet KSP

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

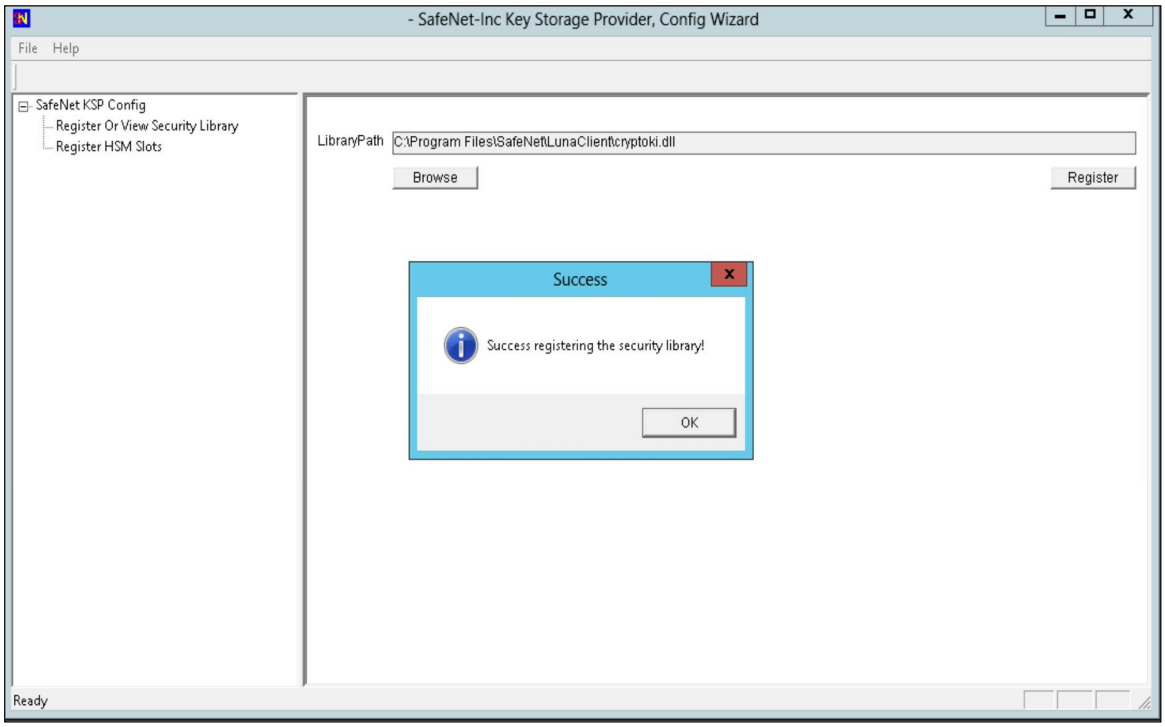
1. Navigate to the KSP installation directory.
2. Run the `KspConfig.exe` (KSP configuration wizard).
3. Double-click **Register Or View Security Library** on the left side of the pane.



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

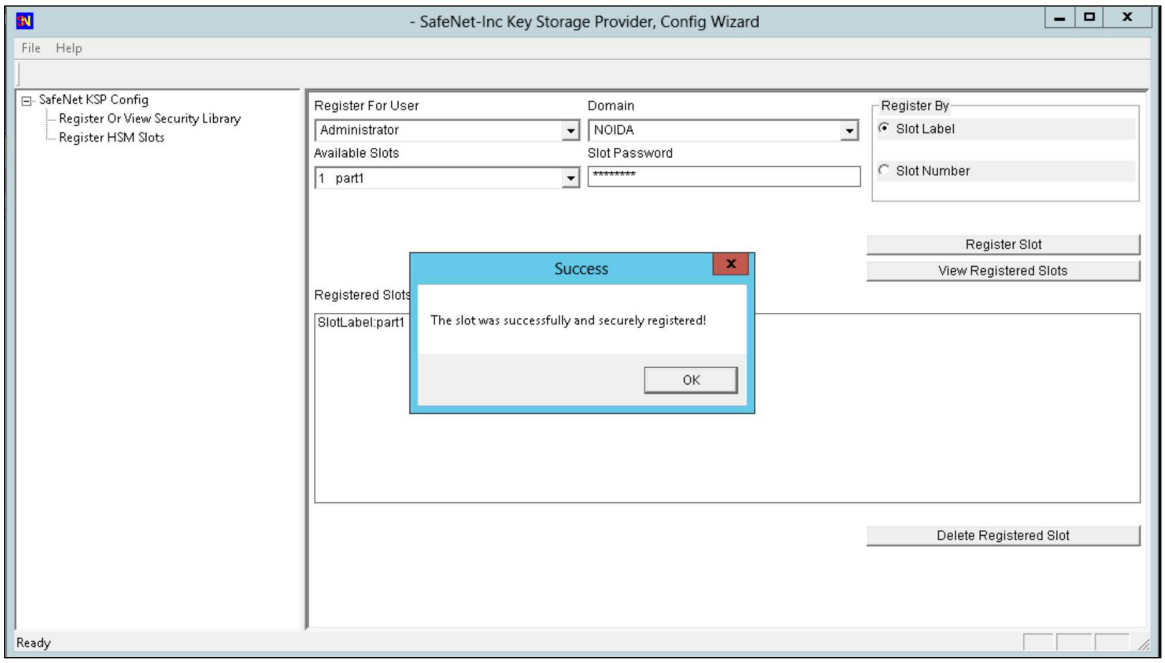


5. On successful registration, a message "**Success registering the security library**" displays.

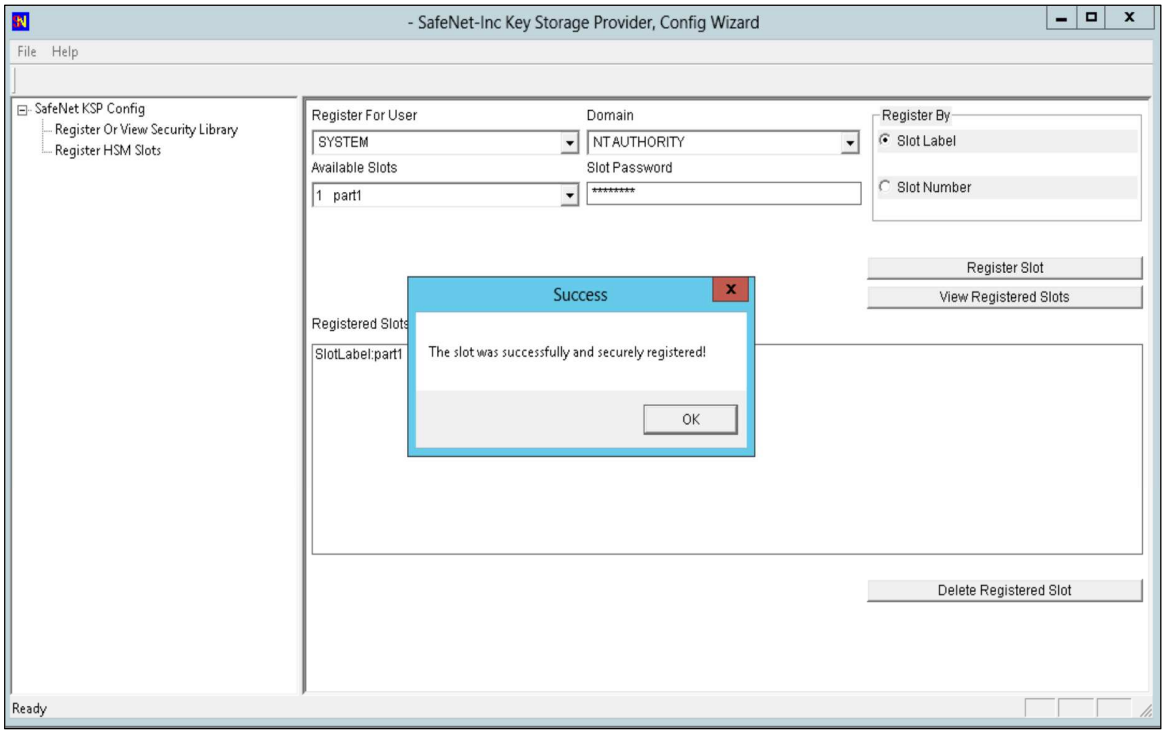


6. Double-click **Register HSM Slots** on the left side of the pane.
7. Enter the Slot (Partition) password.

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**.



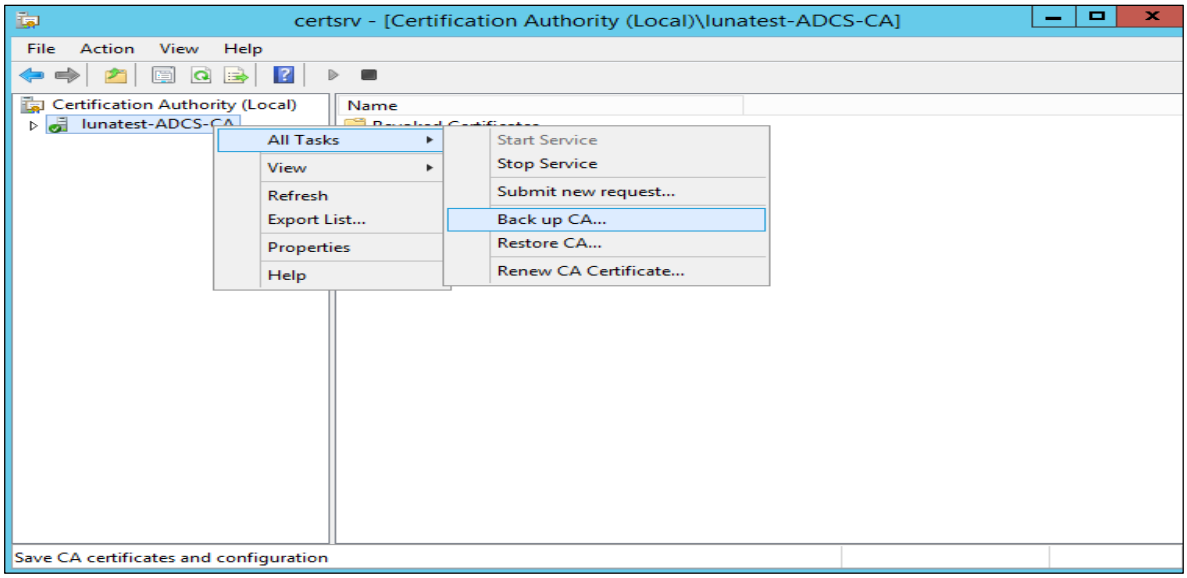
NOTE: Both slots have been registered, despite only one entry appearing for the service in the **Registered Slots** section of the KSP interface.

Backing 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.

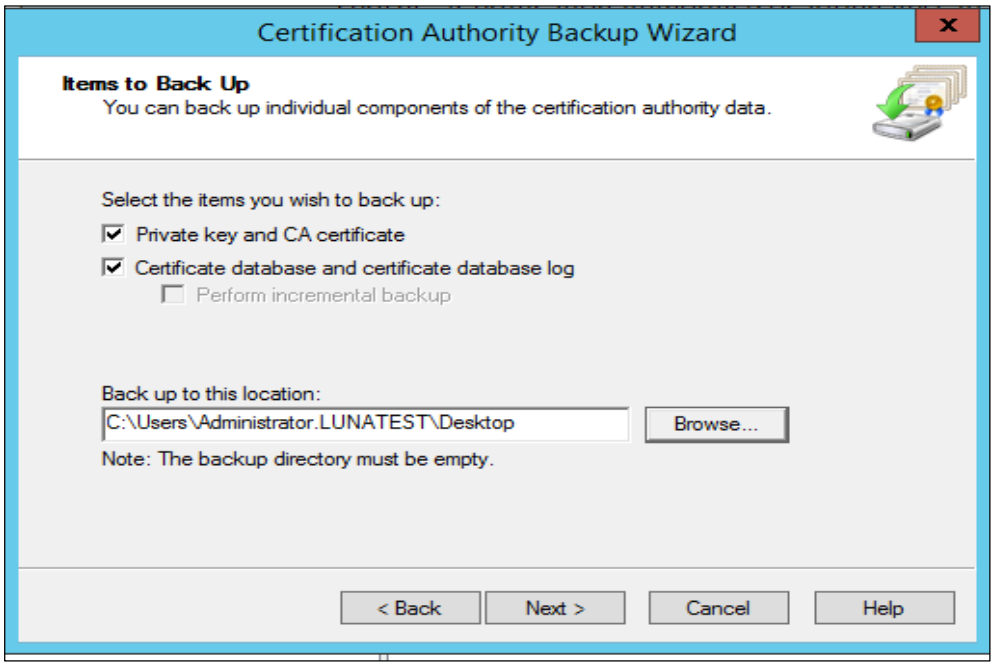
To back up the CA

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



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

5. 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**.



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

Migrating a MS CA onto a SafeNet Luna HSM or HSM on Demand service using ms2Luna

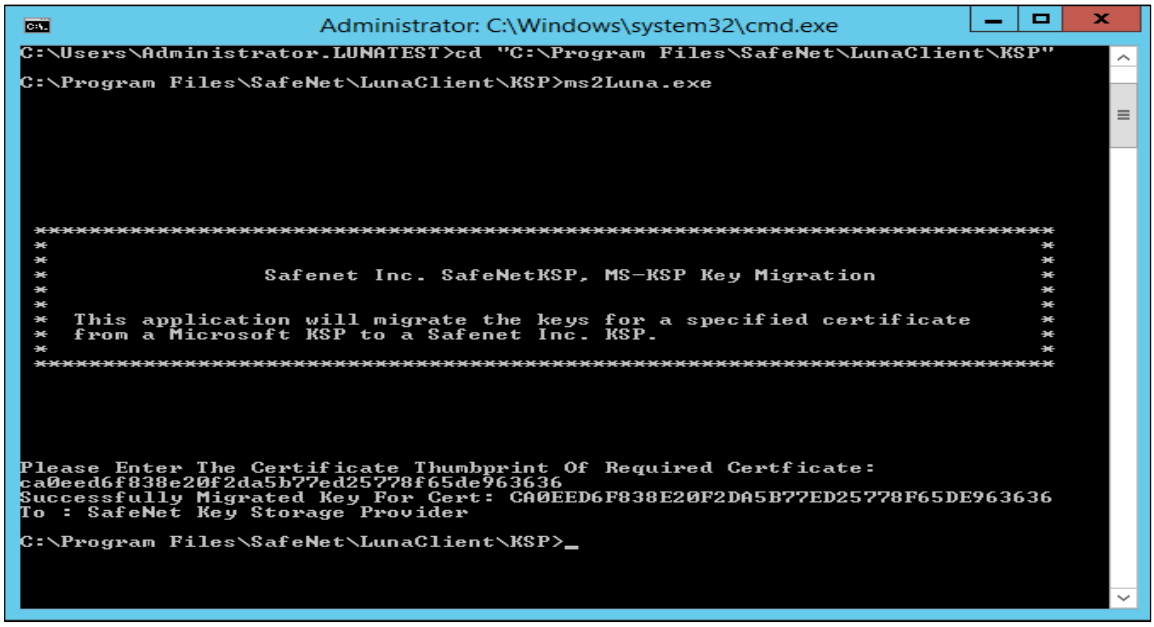
The Keys stored in the Software is not secure and can be compromised anytime.So to enforce operational and logical security of the CA it is required to be migrated onto HSM.Also migration ensures that the same key created in previous section is used for verification of CA.

To migrate a MS CA onto a SafeNet HSM using ms2Luna

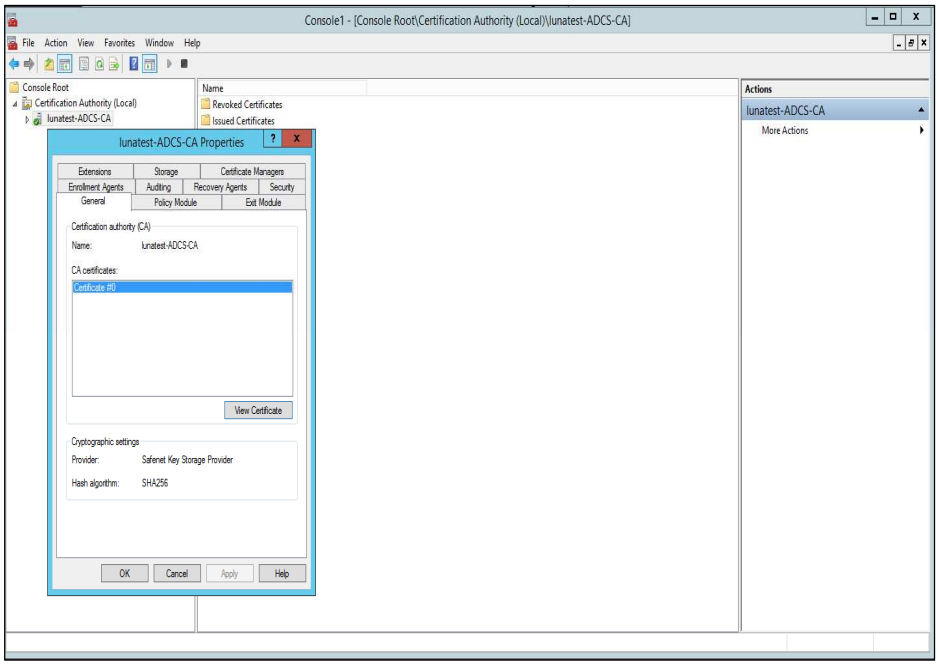
1. Copy the CA certificate thumbprint.
2. Open a command prompt and run `ms2Luna.exe` from `"<SafeNet HSM Client installation Directory>/KSP directory"` in case of KSP registration.

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

3. Enter the Thumbprint of CA certificate and press **Enter**.



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

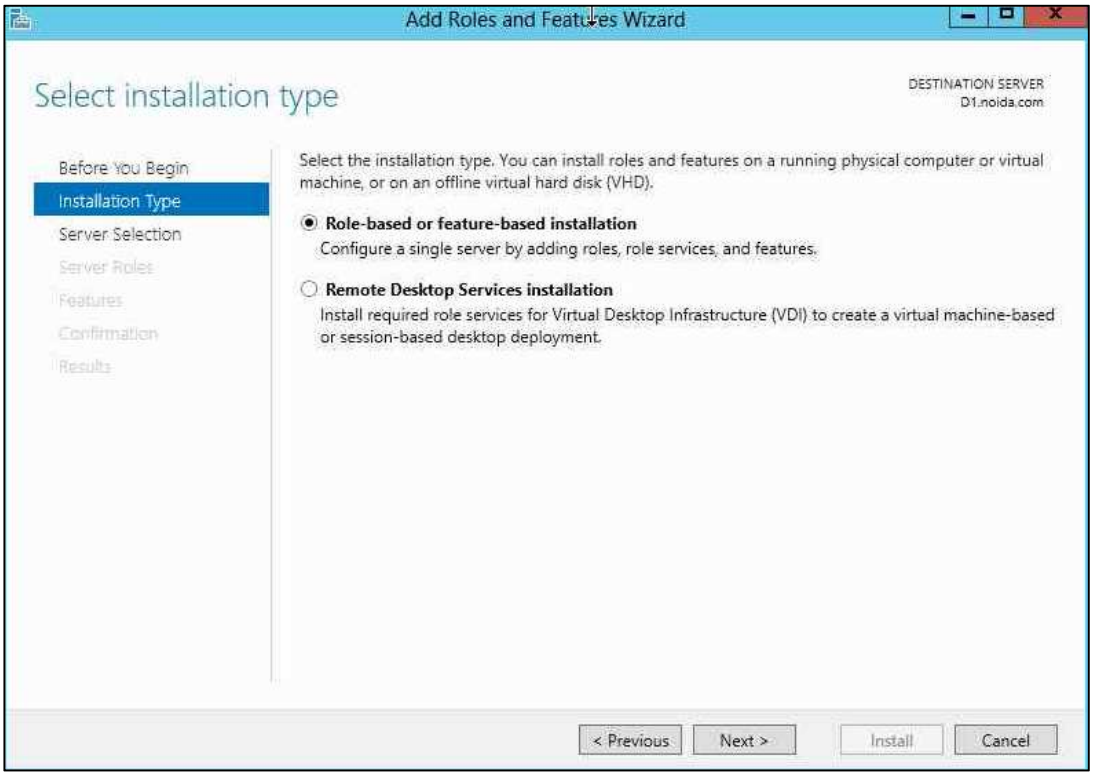


5. Uninstall the existing CA that the key was removed from.

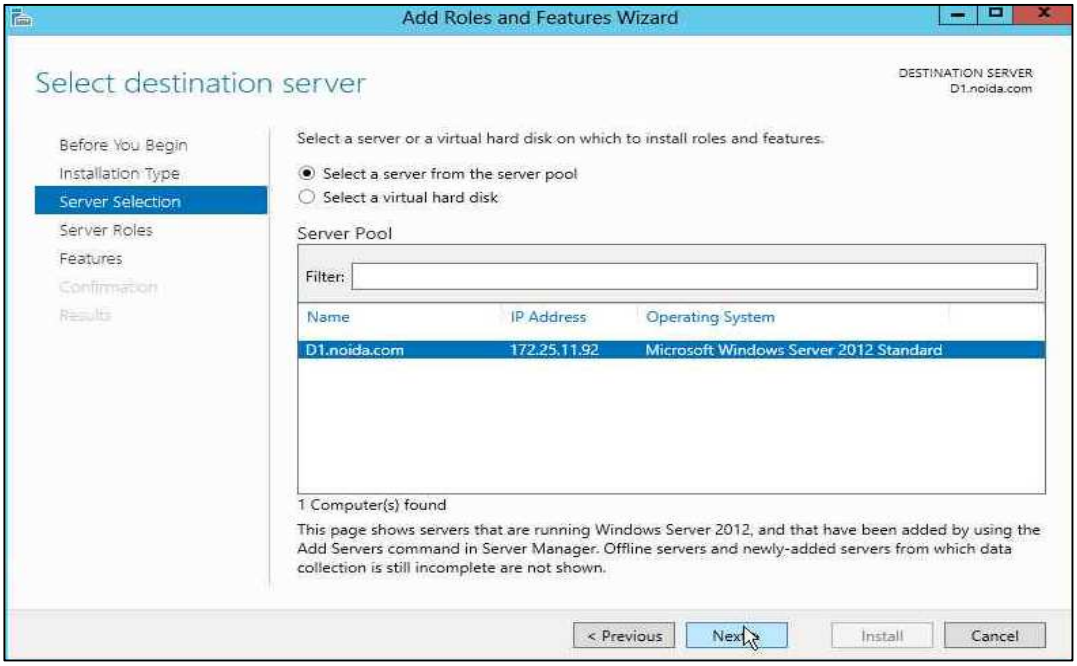
Installing Microsoft Active Directory Certificate Services on Windows Server using SafeNet Key Storage Provider with migrated key

To install the Microsoft Active Directory Certificate Services software

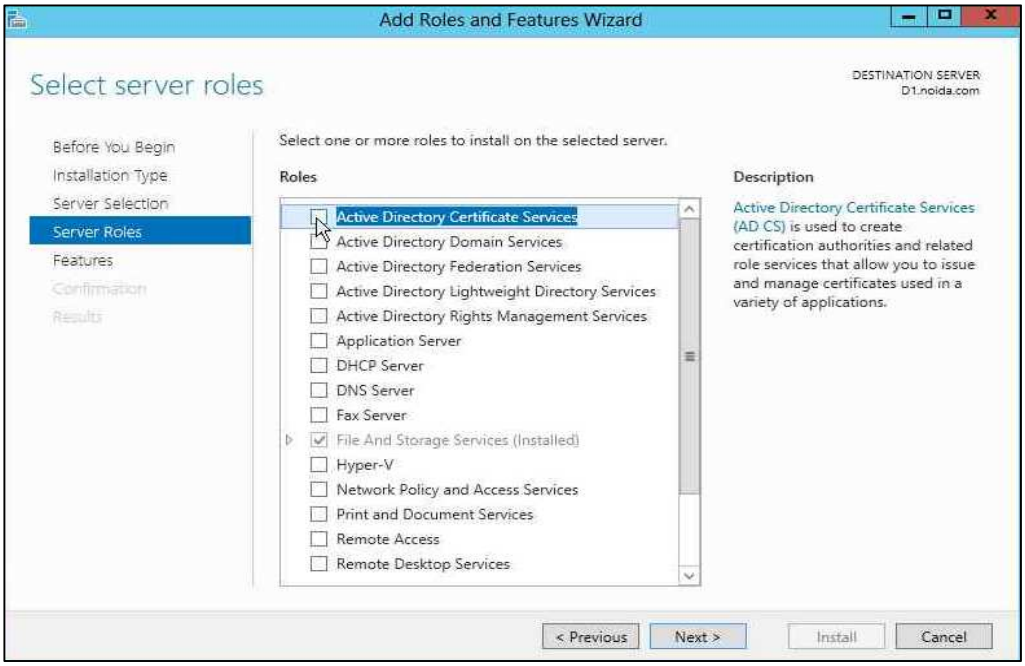
1. Log in as an Enterprise Admin/Domain Admin with Administrative privileges.
2. Open **Server Manager** under Configure this **Local Server** and click **Add Roles and Features**.
3. The **Add Roles and Features Wizard** displays.
4. On the **Before you Begin** page click **Next.**
5. Select the **Role-based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



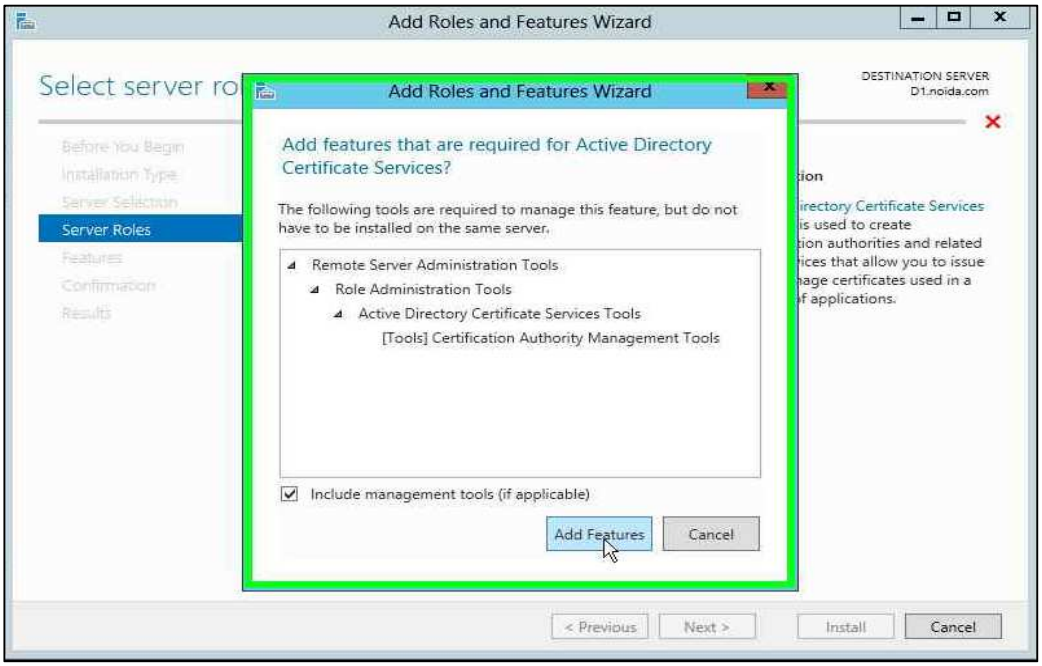
6. Select the **Select a server from the server pool** radio button and from **Server Pool** select your server.



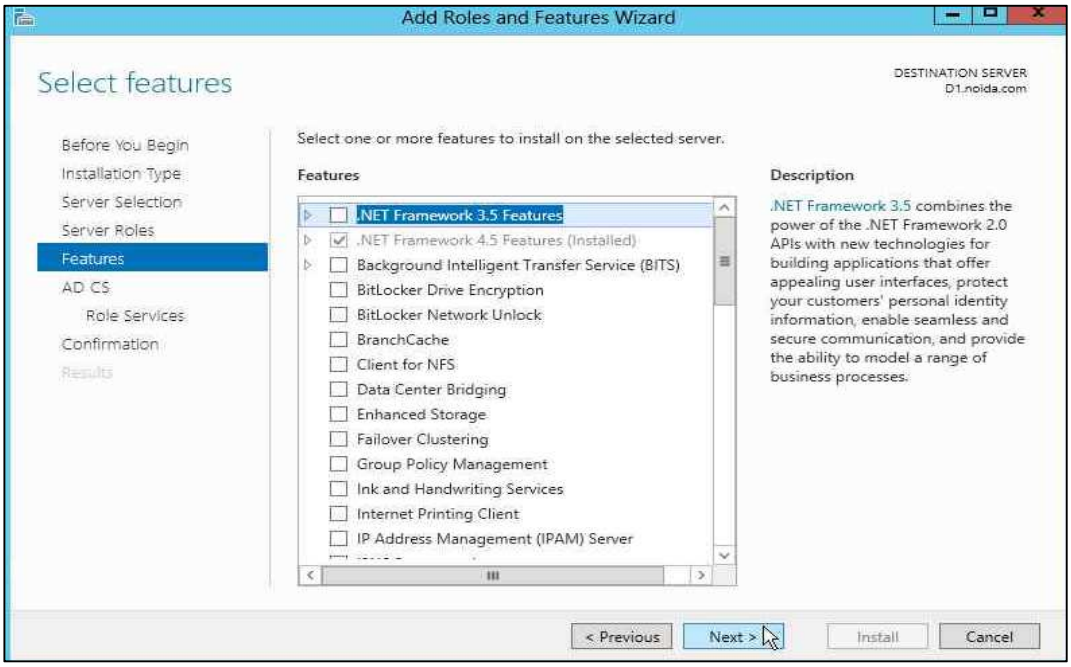
7. Click **Next**.
8. Select the **Active Directory Certificate Services** check box from the **Server Roles**.



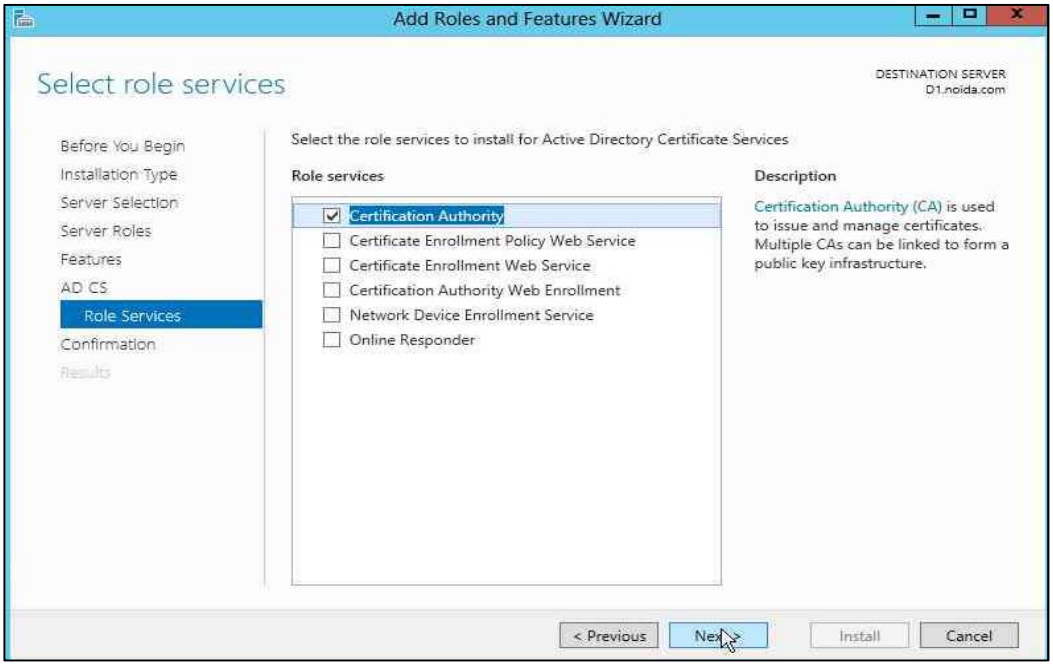
9. A window stating "**Add features that are required for Active Directory Certificate Services?**" displays. To add a feature, click **Add Features**.



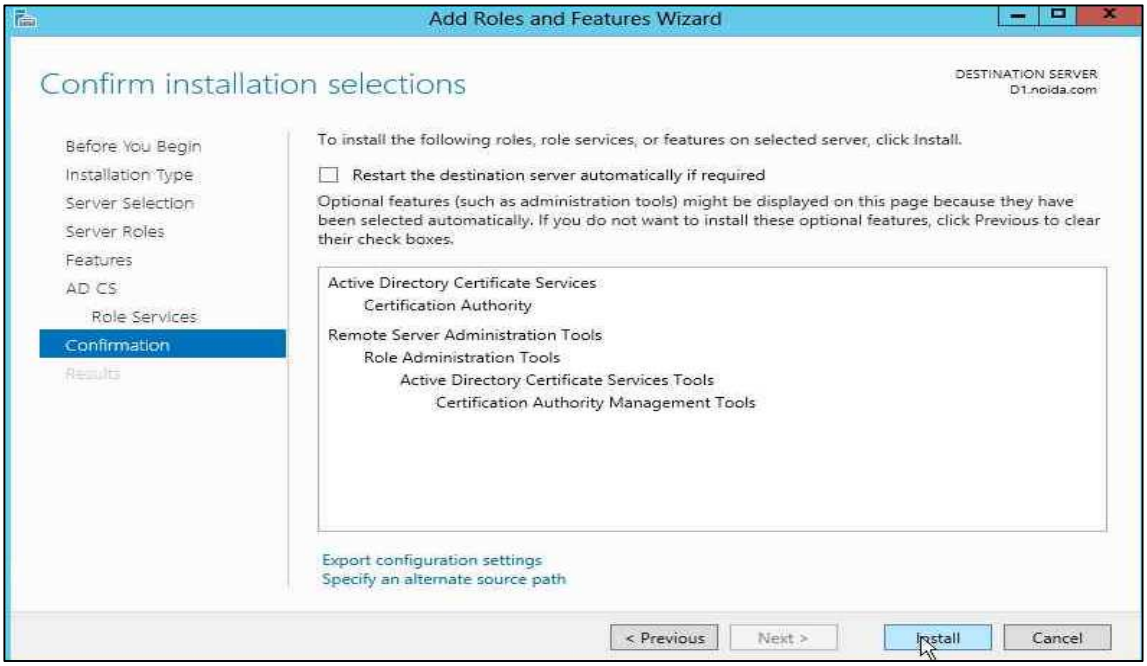
10. Click **Next** twice to continue until the Role Services options are displayed.



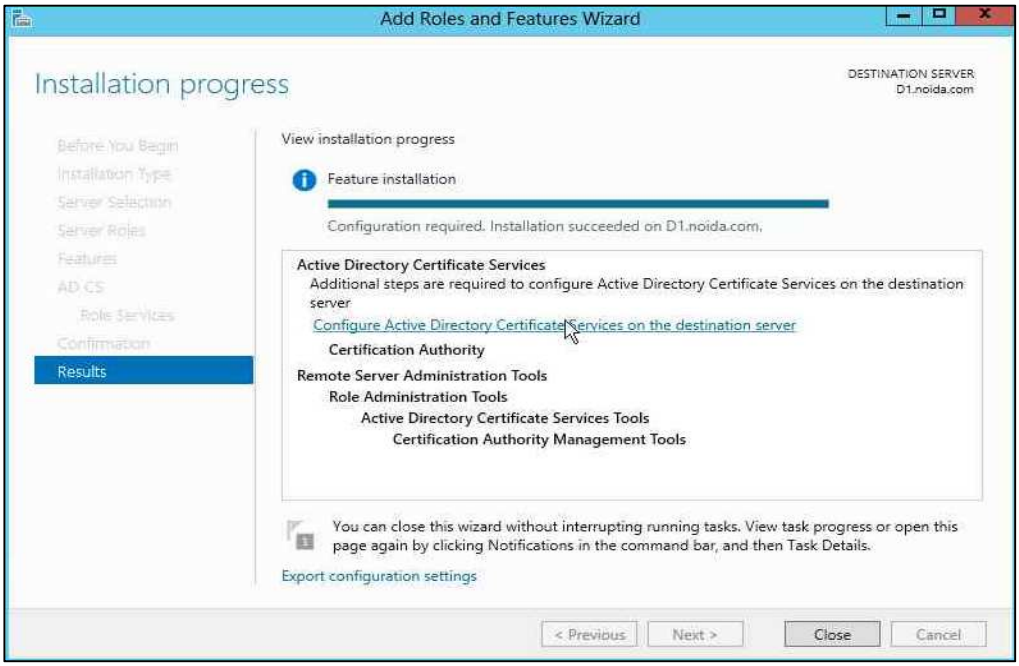
11. Select the **Certification Authority** check box from the **Role services** list and click **Next**.



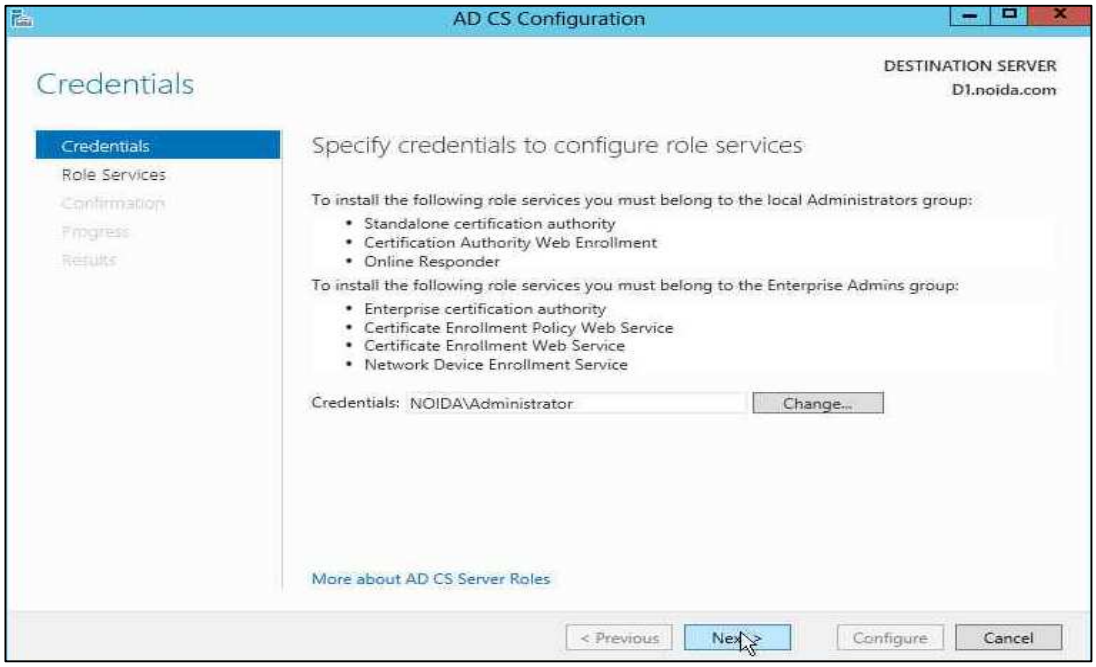
12. Verify that the role you are about to install is appropriate and click **Install**.



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

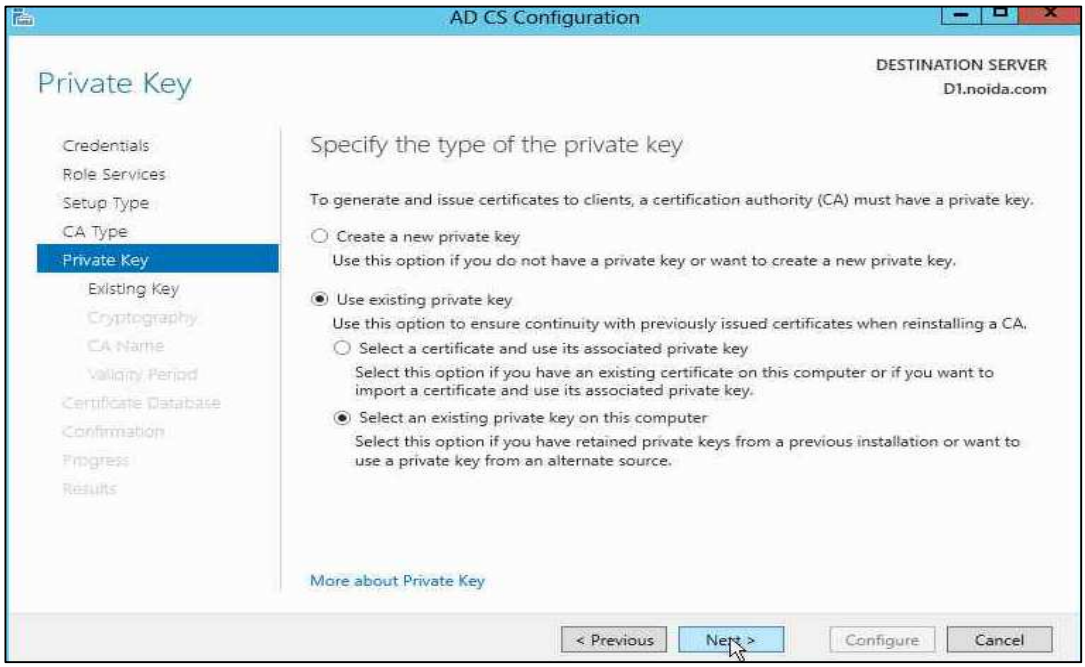


14. On the **Credentials** page of AD CS Configuration wizard, click **Next** to continue.

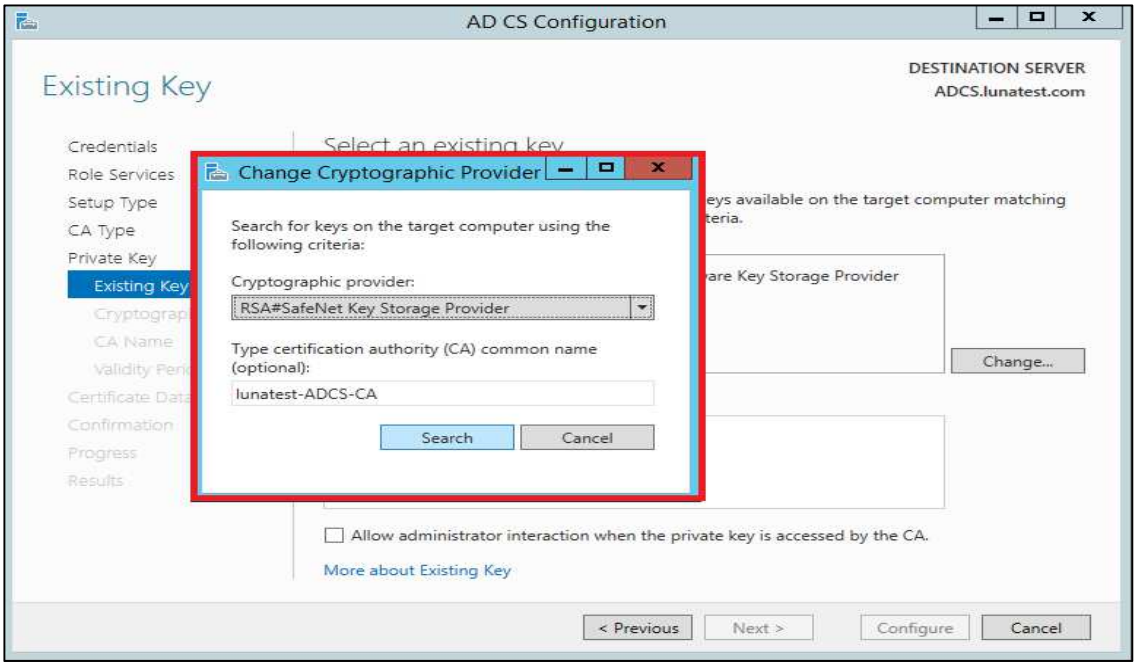


15. Select the **Certification Authority** check box and click Next.

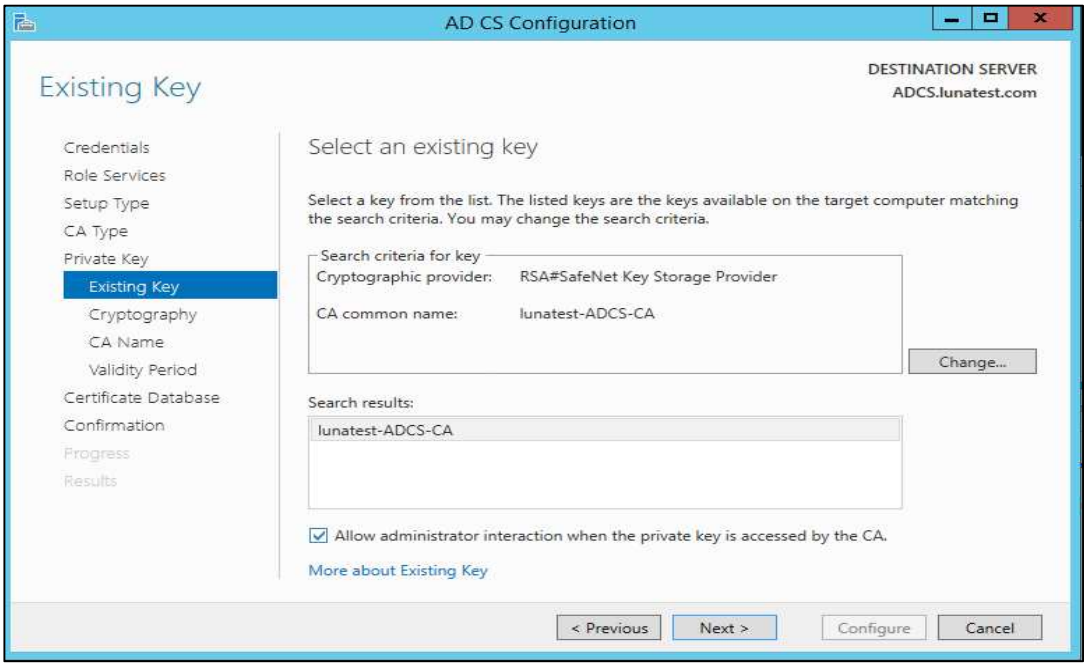
16. Select the **Enterprise CA** radio button and click **Next**.
17. Select the **Root CA** radio button and click **Next**.
18. Proceed to setup the **Private Key** for CA to generate and issue certificates to clients. Select **Use existing private key** and **Select an existing private key on this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



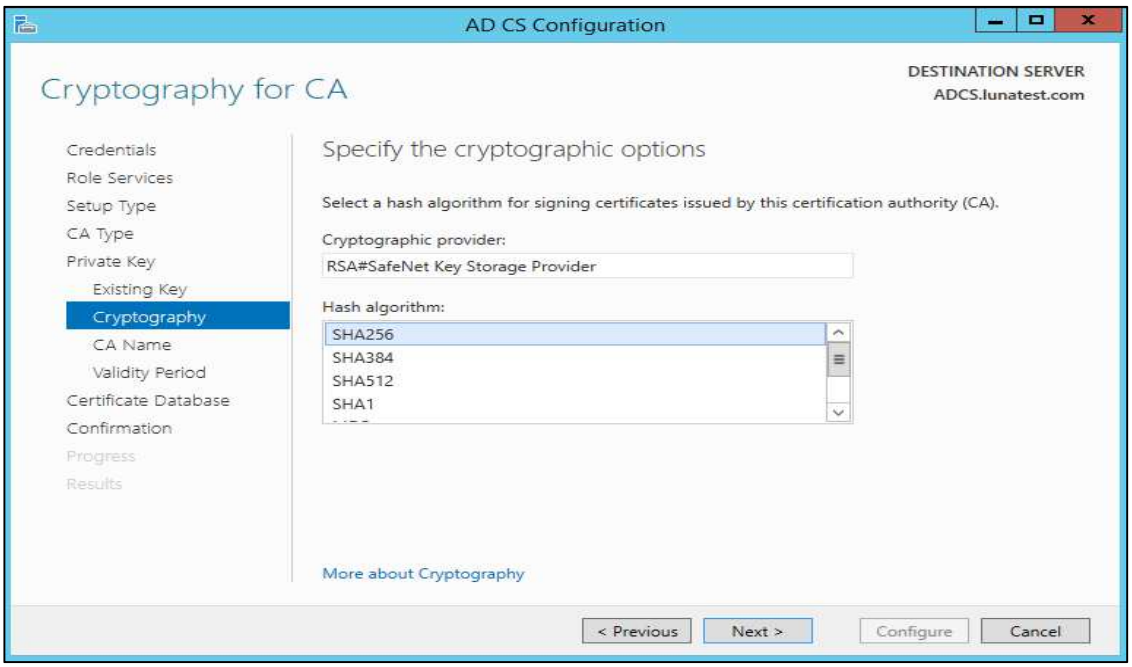
19. Click **Change…**. Select the **SafeNet Key Storage Provider** algorithm that you used to generate the private keys. Clear the CA Common name. Click **Search**.



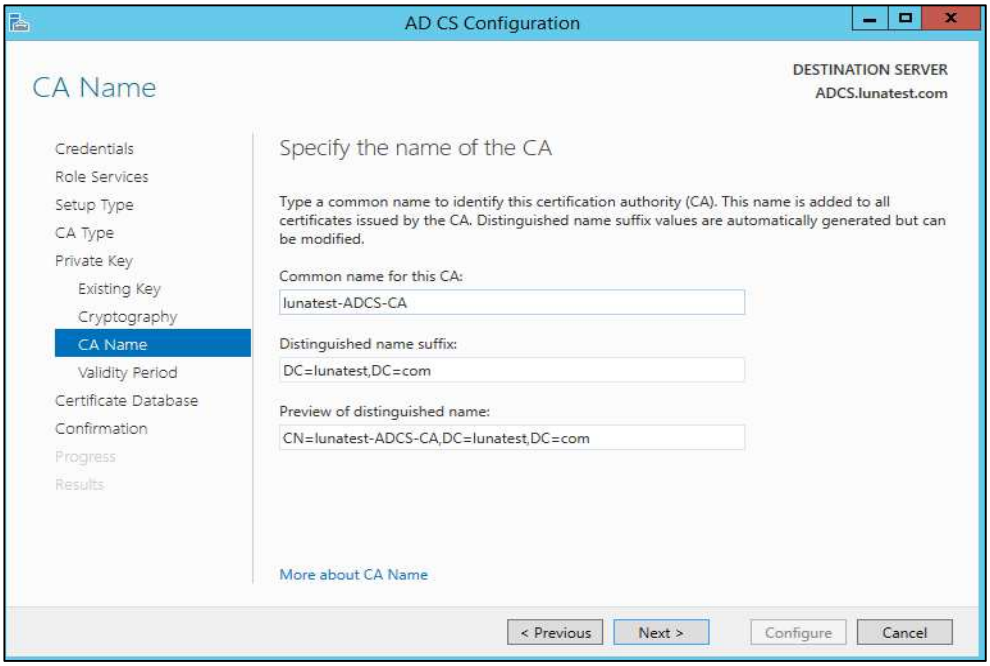
20. Select the existing key and click **Next.** Select the **Allow administrator interaction when the private key is accessed by the CA** check box.



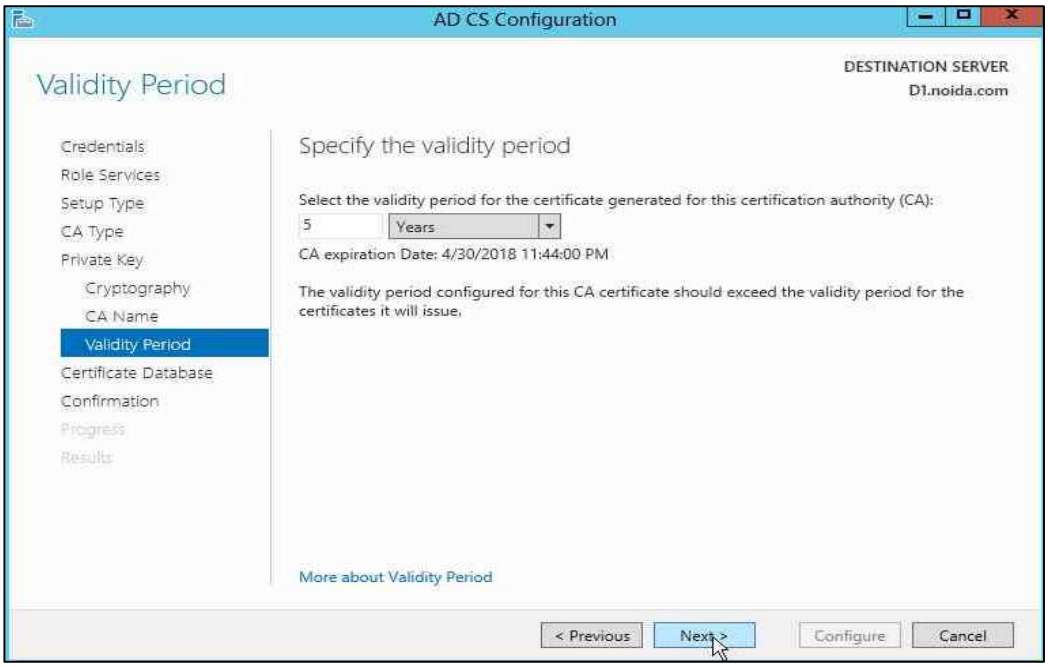
21. Select the **Hash Algorithm** for signing certificates issued by this Certificate Authority and key length settings for your installation.



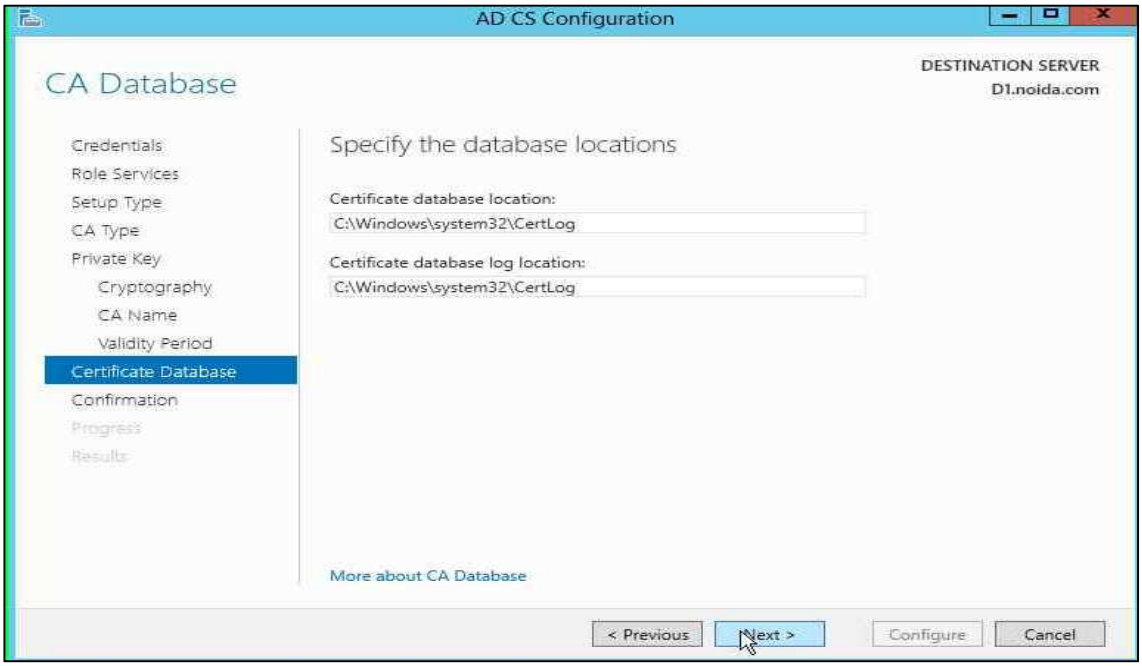
22. Click **Next** to continue.
23. Configure a common name to identify this Certificate Authority. Click **Next** to continue.



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.

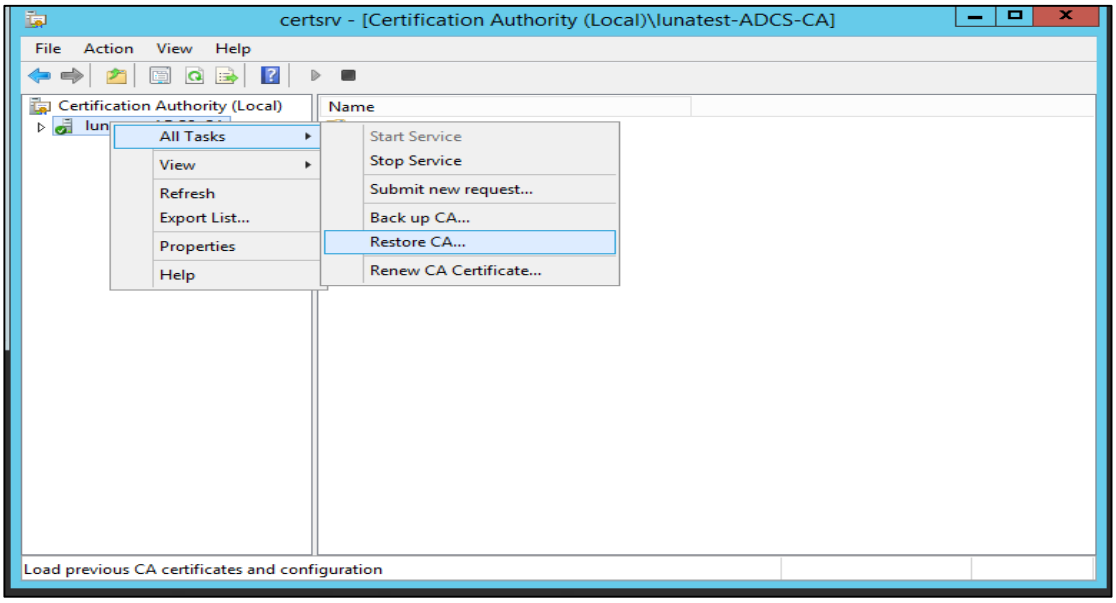
    After successful installation, the CA certificate must be imported.

Restoring an MS CA

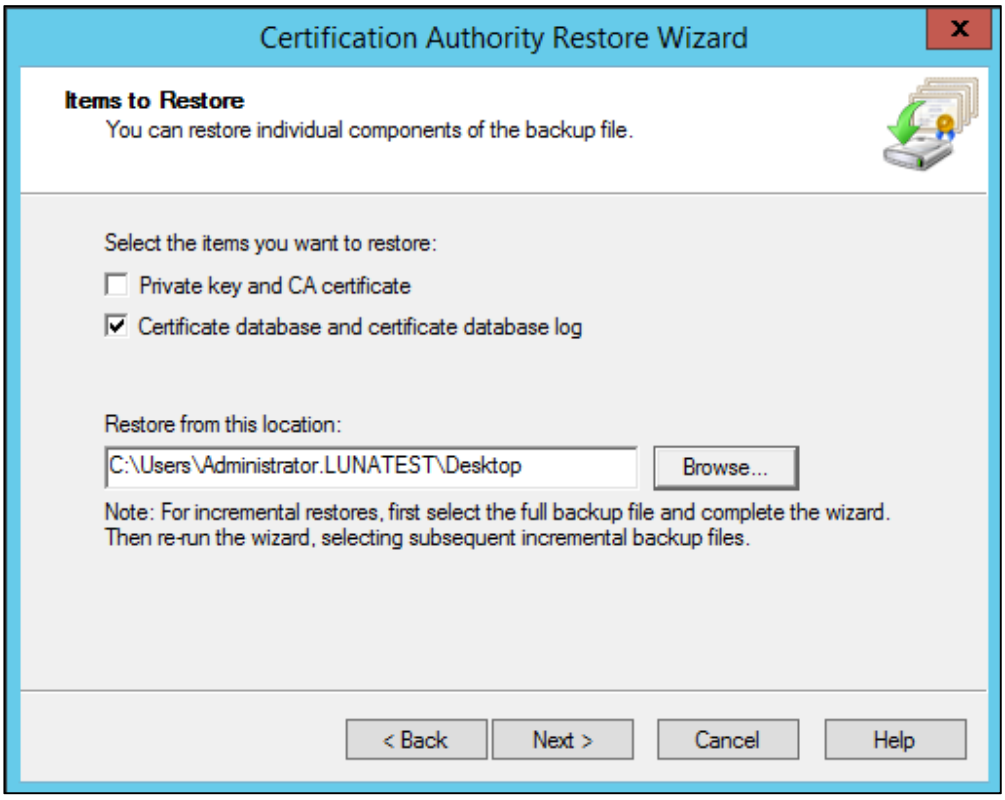
You can restore a backed-up MS CA user account.

To restore an MS CA

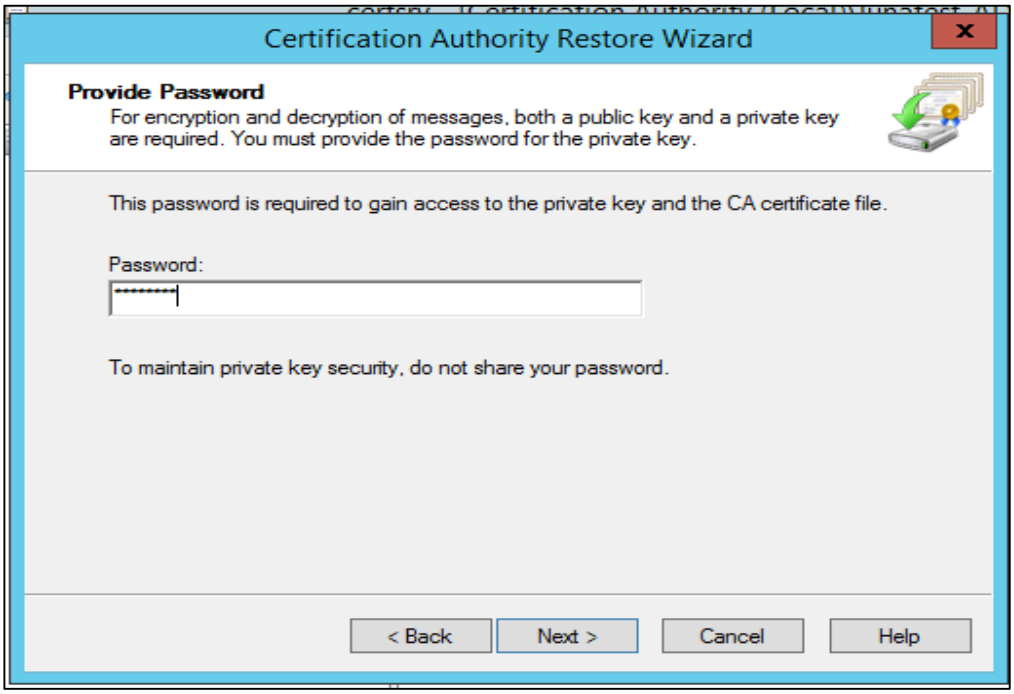
1. Click the **Start** button, click **Run**, type **certsrv.msc**, and then click **OK**.
2. Select the CA node in the left pane.
3. On the **Action** menu, click **All Tasks** and then **Restore CA.**



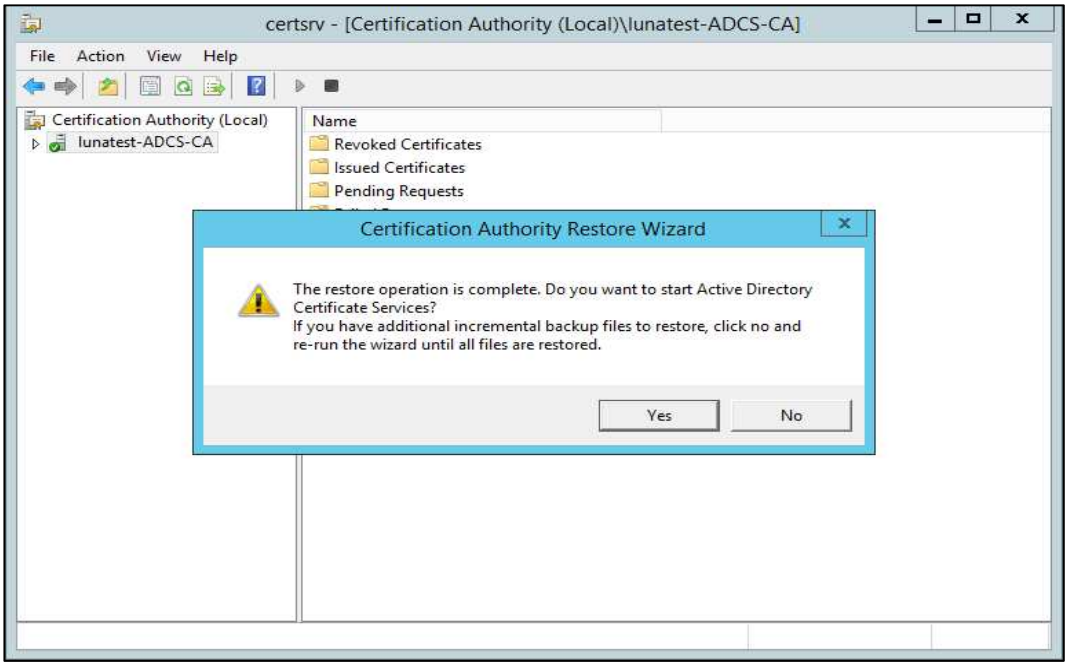
4. Click **Next** on the Welcome page of the CA Restore wizard.
5. Select the **Certificate database and certificate database log** check box and provide a directory name where you want to temporarily store the CA certificate and optionally the key. Click **Next**.



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.