Microsoft

Active Directory Certificate Services

2022 and 2025

Integration Guide

u.trust Anchor Se-Series

6.0.0, 6.1.1, and 6.2.0

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	2.0.0
Date	2025-08-12
Status	PUBLISHED
Document No.	IG-2025-0029

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle. All of Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

1.1 About This Guide

This guide describes how to enable HSM integration with Microsoft Active Directory Certificate Services (AD CS) including installation and set-up of Microsoft CA and integration with Online Certificate Service Protocol (OCSP). For more detailed information regarding Microsoft Active Directory Certificate Services and Online Certificate Service Protocol, please refer to the documentation provided by Microsoft.

1.2 Target Audience

This guide is intended for Microsoft AD CS and OCSP administrators and HSM administrators.

1.3 Abbreviations

Abbreviation	Meaning
AIA	Authority Information Access
AD CS	Active Directory Certificate Services
CA	Certificate Authority
CAT	CryptoServer Administration Tool
CER	Certified Emissions Reductions
CLI	Command Line Interface

Abbreviation	Meaning
CNG	Cryptography API Next Generation
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HSM	Hardware Security Module
KRA	Key Recovery Agent
MBK	Master Backup Key
MMC	Microsoft Management Console
OCSP	Online Certificate Service Protocol
PS	PowerShell
RSA	Rivest-Shamir-Adleman
URL	Uniform Resource Locator

Table 1: Abbreviations

1.4 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press the **OK** button.
`Monospaced`	File names, folder and directory names, commands, file outputs, programming code samples	You will find the file `example.conf` in the `/exmp/demo/ directory`.
Italic	References and important terms	See Chapter 3, "Sample Chapter", in the *u.trust Anchor - csadm Manual* or [CSADM].

Table 2: Document Conventions

Special icons are used to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

2 Product Overview

2.1 Microsoft Active Directory Certificate Services

A Microsoft Active Directory Certification Authority is responsible for attesting to the identity of users, computers, and organizations. The CA authenticates an entity and vouches for that identity by issuing a digitally signed certificate. The CA can also manage, revoke, and renew certificates. The CA can be public or private. A public CA provides certification services, typically for a fee, to the public over the Internet. A private CA provides this service to the members of a delimited population such as the employees of a business or members of some other private group.

If the security of the generated keys and certificates needs to be enhanced, the Microsoft Active Directory Certification Authority needs to be configured to use a Hardware Security Module (HSM). When the HSM module is enabled with Microsoft Active Directory Certification Authority, this strengthens the protection of keys and certificates.

2.2 Online Certificate Service Protocol

Online Certificate Status Protocol is an Internet Protocol and is used by certificate authorities to check the revocation status of specific digital certificates. The Online Responder Service is the component by Microsoft Windows service that is responsible for managing the configuration of OCSP responder by retrieving revocation information from revocation providers, signing responses, and auditing changes to the configuration of the OCSP responder.

The OCSP and CA uses Utimaco HSM for performing different operations like key generation, certificate signing, CRL signing and protecting their private keys.

2.3 Utimaco u.trust Anchor HSM

The u.trust Anchor is a next-generation hardware security module developed by Utimaco IS GmbH. It is a multi-tenant, physically protected, and tamper-resistant cryptographic appliance designed to perform high-assurance cryptographic operations and manage cryptographic keys securely. The u.trust General Purpose HSM is built on a modern, container-based design inspired by cloud technology. With support for up to 31 containers and multiple PKCS #11 partitions per cHSM, it ensures seamless application separation and key partitioning, making it an ideal choice for all types of cryptographic applications. It’s also upgradeable for specific use cases like blockchain and 5G, and offers flexibility for custom solutions, including proprietary algorithms and customer key derivations via the Software Development Kit.

3 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

These are the integrations that have been successfully tested with the Utimaco HSM and the Microsoft Active Directory Certificate Services (AD CS).

Operating Systems	Utimaco Security Server Version	Utimaco HSM
Windows Server 2022 Windows Server 2025	u.trust Anchor cHSM 6.0.0 u.trust Anchor cHSM 6.1.1 u.trust Anchor cHSM 6.2.0	u.trust Anchor Se-Series

Table 3: List of Tested Versions

3.2 Hardware and Software Requirements

Hardware	Hardware Requirements
Utimaco u.trust Anchor LAN HSM	u.trust Anchor Se-Series cHSM available with firmware SecurityServer 6.0.0, 6.1.1 or 6.2.0

Table 4: List of Hardware Requirements

Software	Software Requirements
Java	Version 8, Update 271 or higher
HSM Interfaces	CSP/CNG

Table 5: List of Software Requirements

> Set up an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/

3.3 Prerequisites

Before you begin, please ensure that you have:

- A u.trust Anchor cHSM set up and configured. Refer to the u.trust Anchor Se-Series documentation to set up the HSM.
- An MBK created and stored on each cHSM. Refer to the u.trust Anchor Se-Series documentation to set up the MBK.
- The u.trust Anchor cHSM Default Admin replaced with a new admin user for production environments.
- An operating system listed in Tested Versions.
- A cHSM SecurityServer version listed in Tested Versions.
- A cryptographic user on that SecurityServer.
- (If you are using Smartcard Authentication) An installed PIN PAD driver through the SecurityServer software file, a configured PIN PAD, and a started PIN Pad Daemon. Refer to the CryptoServer documentation for more information about PIN PAD driver installation and configuration.
- The Microsoft SDK installed and configured as listed in Tested Versions.

4 Installation and Configuration

This section describes the process of installing Utimaco HSM software with Microsoft AD CS.

4.1 Setting Up u.trust Anchor HSM

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

If you have purchased an HSM from Utimaco, you will need the associated product bundle containing the required Windows software packages. This bundle can be downloaded from the Utimaco Support Portal. Please ensure you request access to the product bundle beforehand through the support portal.

Install the latest version of the SecurityServer software following the instructions provided in Section 4.1 of *u.trust Anchor Administration Manual* [UTAADMIN]. For integration with Microsoft AD CS, only the CNG Application Interface is required.

4.2 Setting Up Microsoft AD CS

4.2.1 Install Microsoft AD CS with Windows Enterprise

To create an AD-integrated CA – that is, an Enterprise CA – an account with Enterprise Administrator level privileges is required for the role configuration.

1. Join a machine to the Domain and log in as a user with Administrative privileges.
2. Select **Start,** then select **Server Manager** to open **Server Manager.**
3. Select **Manage**, then select **Add Roles & Features**. The **Before you begin** window opens. Click **Next.**
4. On the **Select installation type** window, make sure the default **Role or Feature Based Installation** is selected. Click **Next.**
5. On **Server selection**, select a server from the server pool. Click **Next.**
6. On the **Select server roles** window, select the **Active Directory Certificate Services** role.

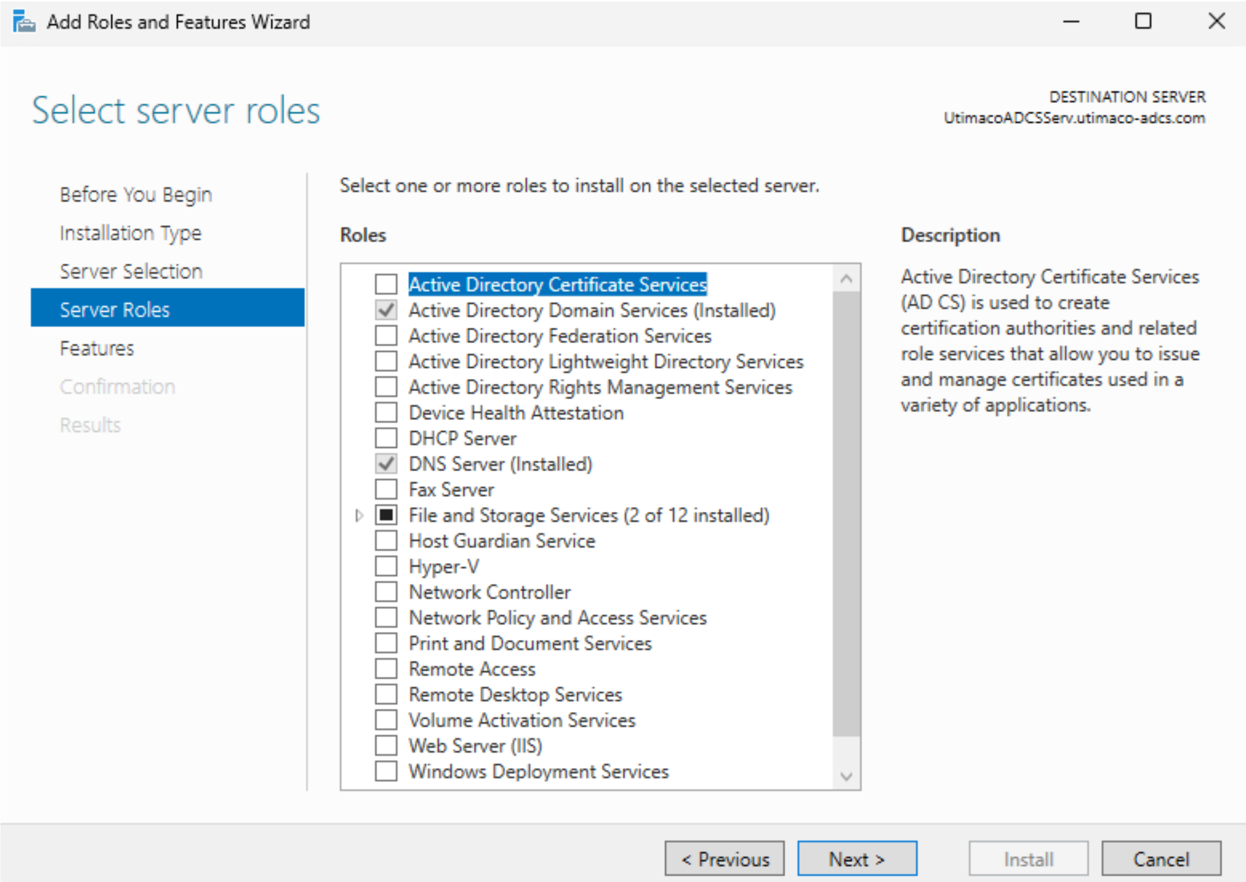

Figure 1 : "Select server roles" Window

7. When prompted to install **Remote Server Administration Tools**, select **Add Features**. Click **Next**.

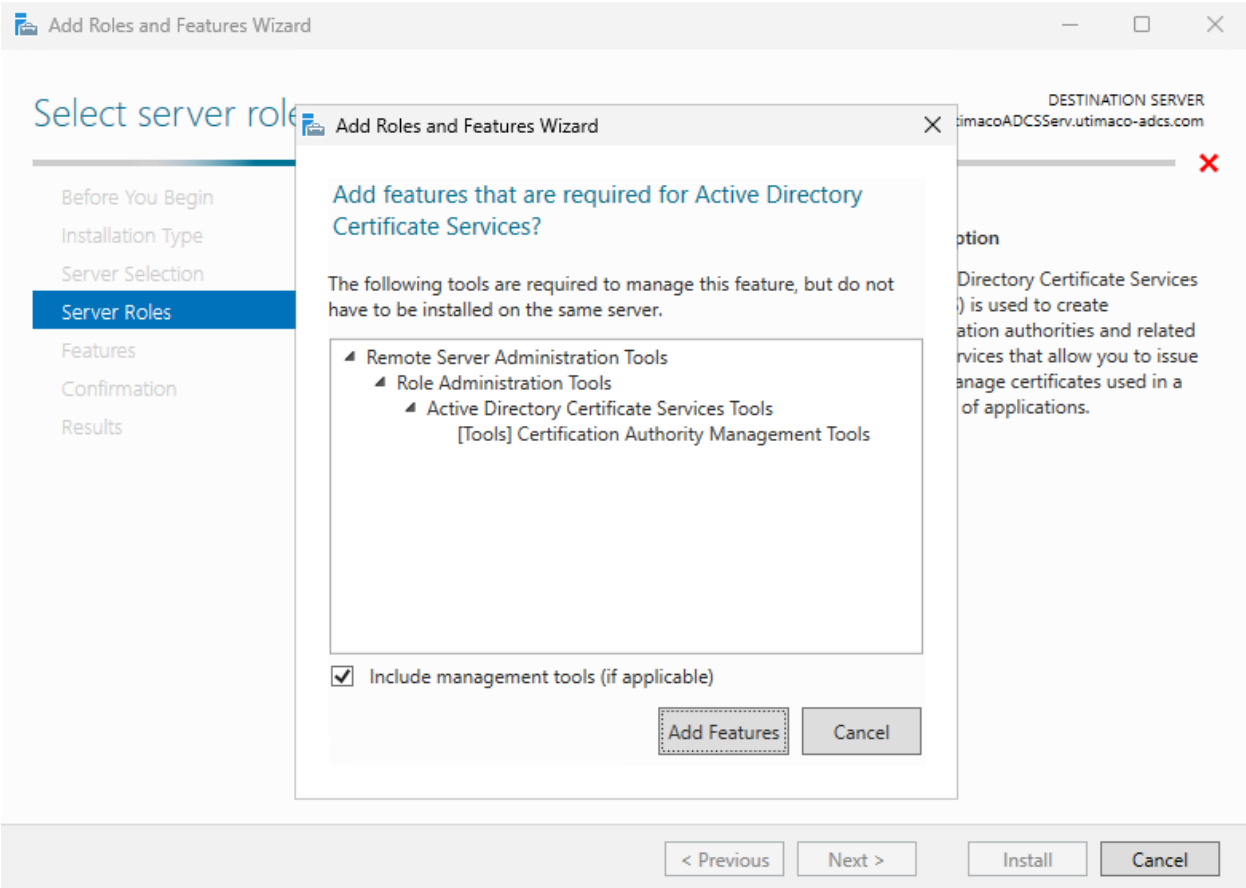

Figure 2 : "Add Roles and Features" Window

8. On the **Select features** window, click **Next.**

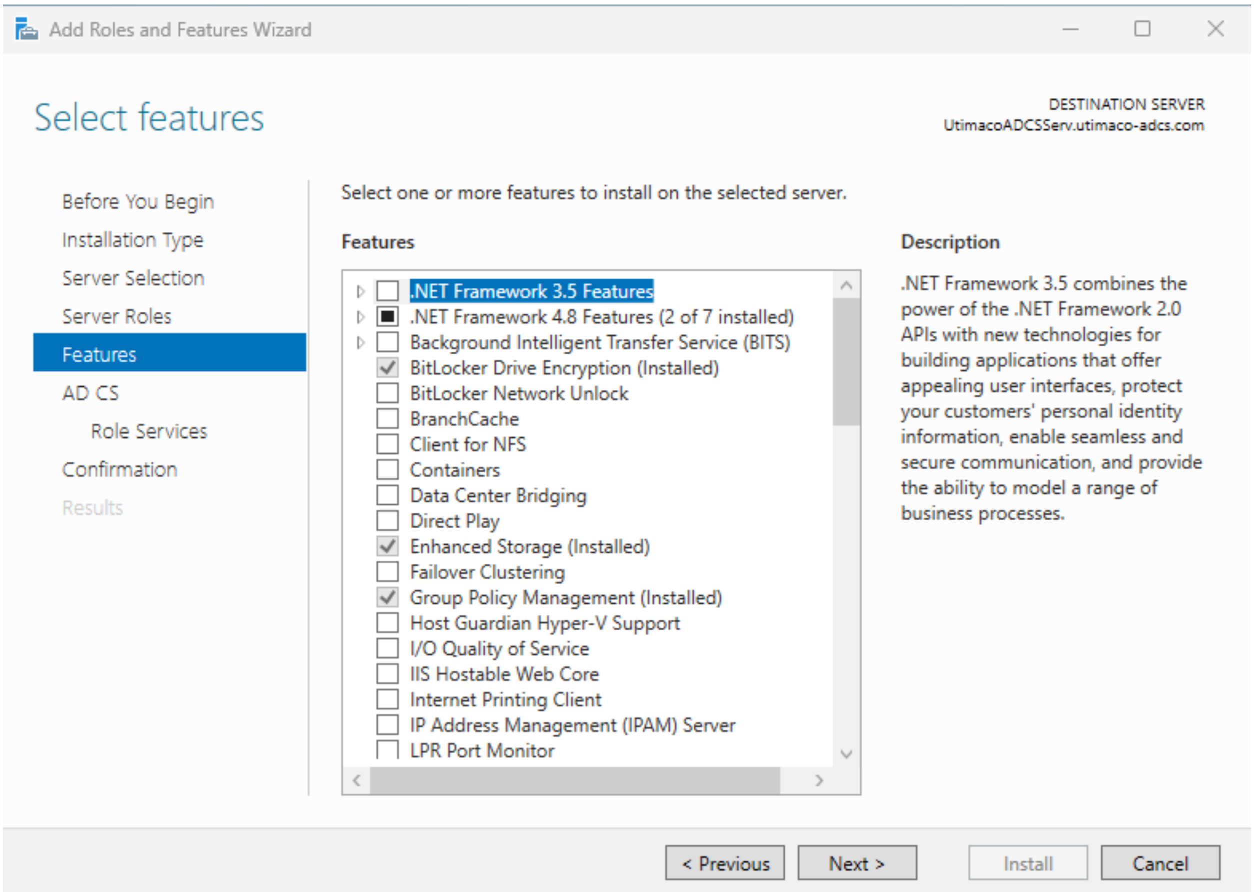

Figure 3 : "Select features" Window

9. On the **Active Directory Certificate Services** window, click **Next.**

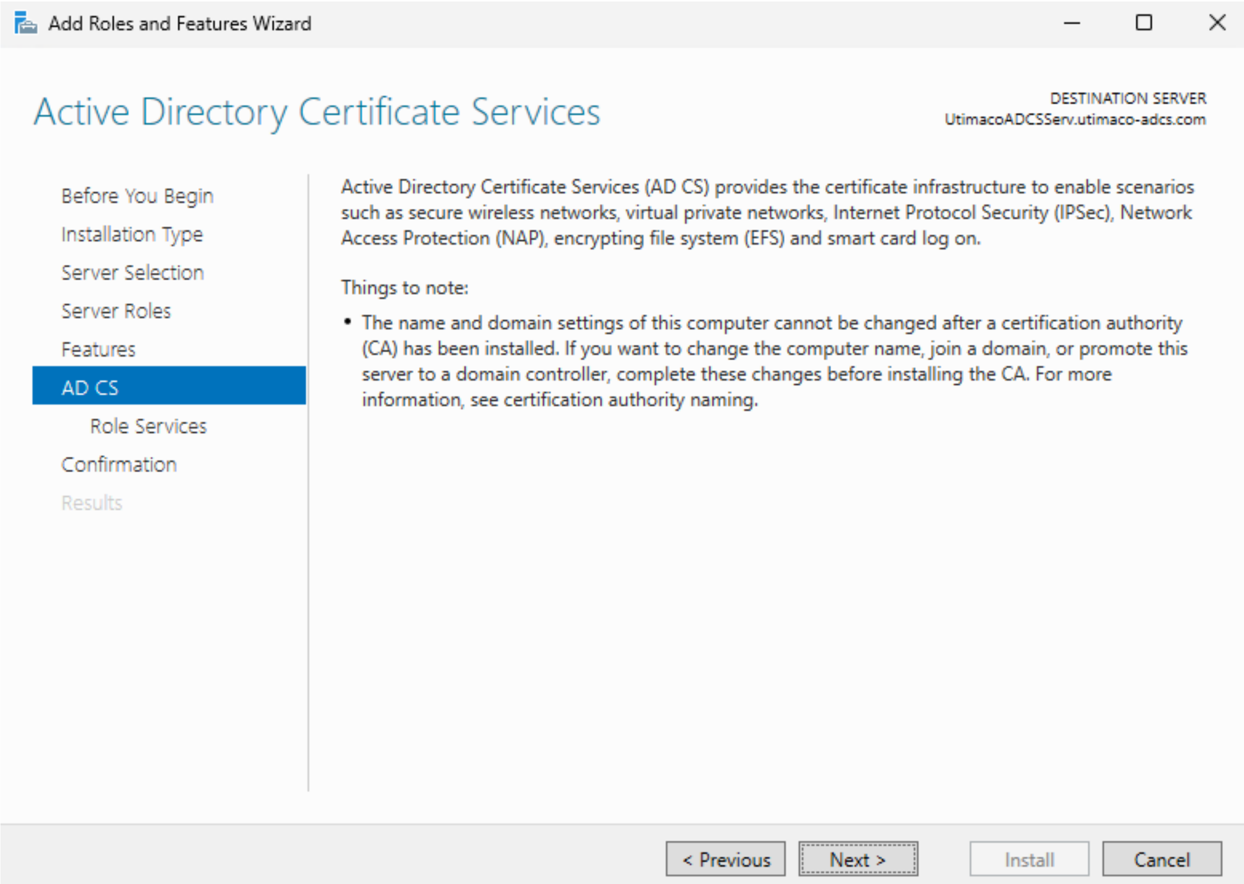

Figure 4 : "Active Directory Certificate Services" window

10. On the **Select role services** window, the **Certification Authority** role is selected by default. Click **Next.**

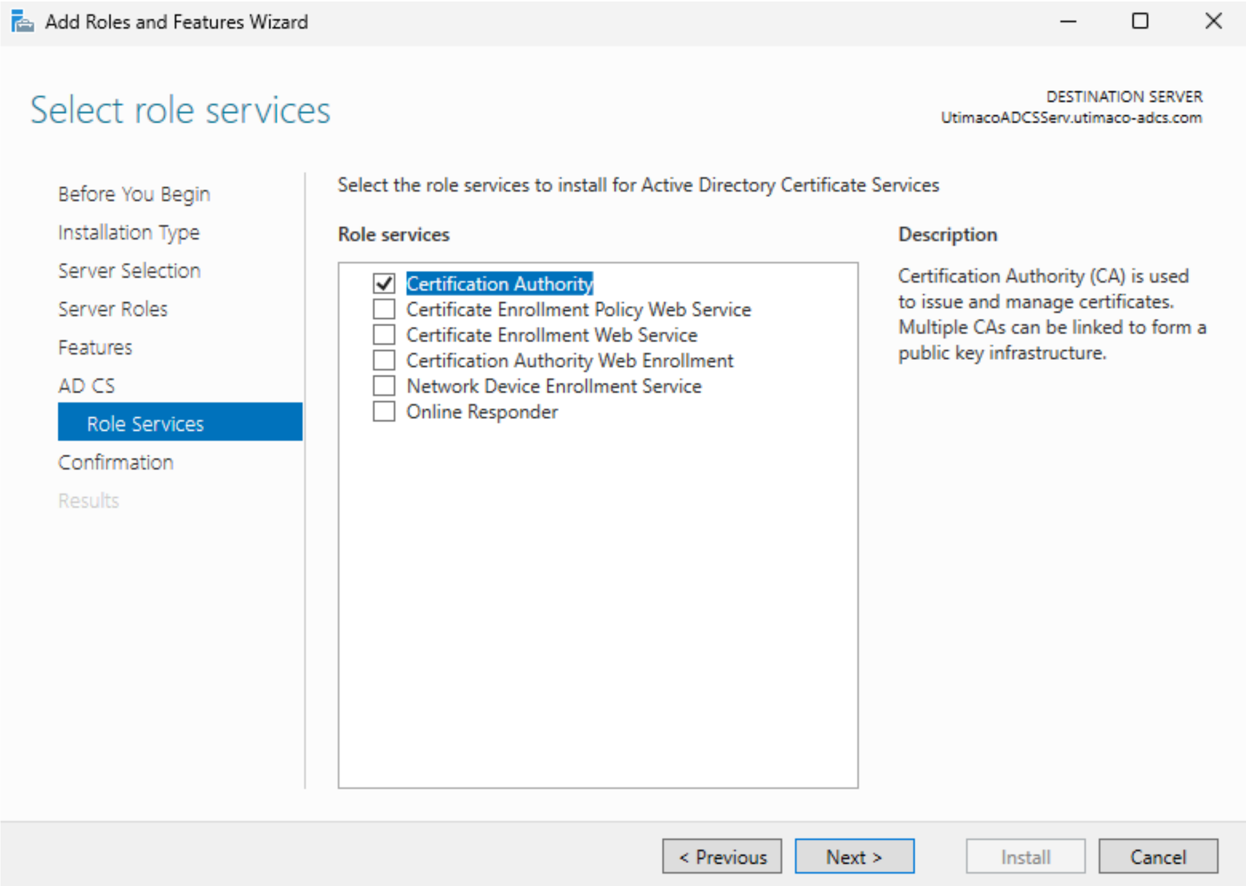

Figure 5 : "Select role services" Window

11. On the **Confirm installation selections** window, check and verify the information, then click **Install.**

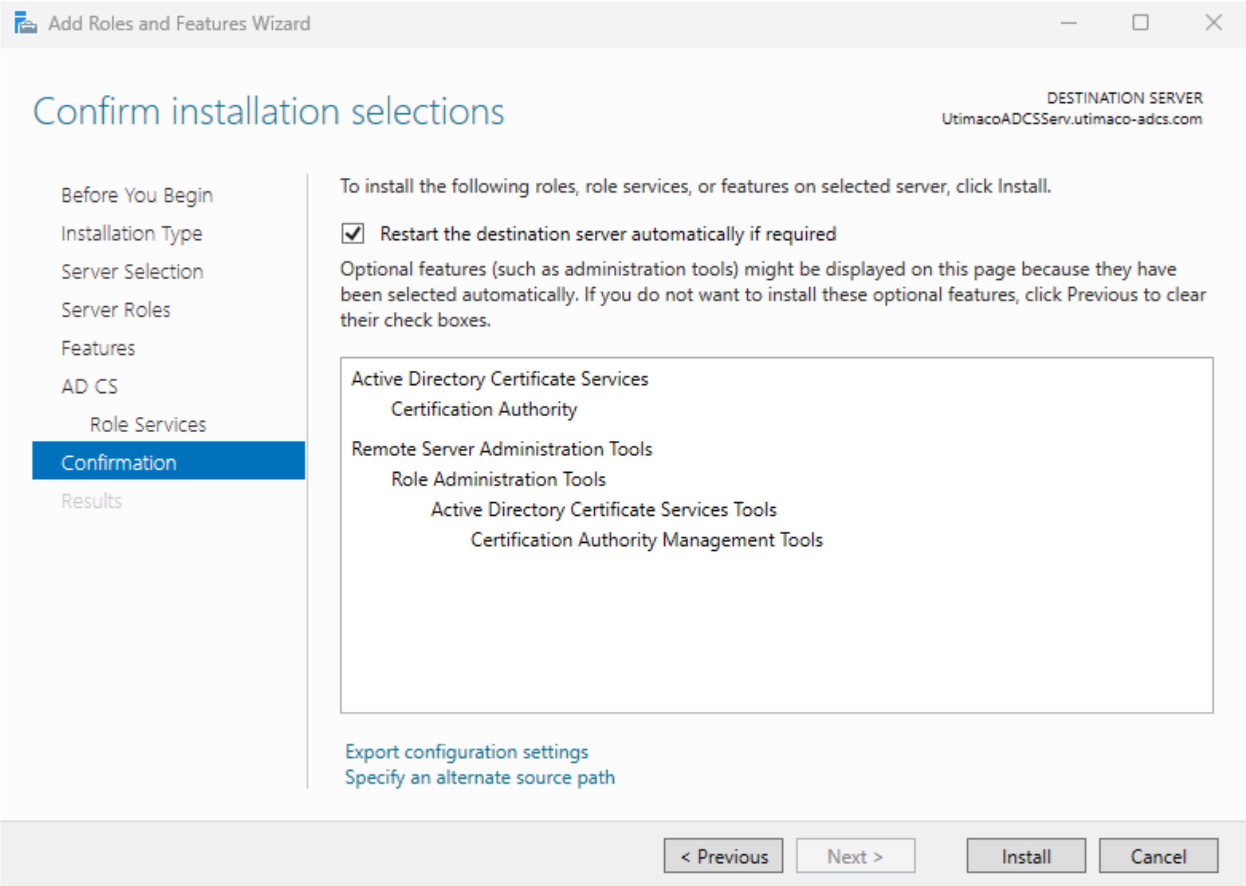

Figure 6 : "Confirm installation selections" Window

12. When the installation is finished, click the **Close** button.

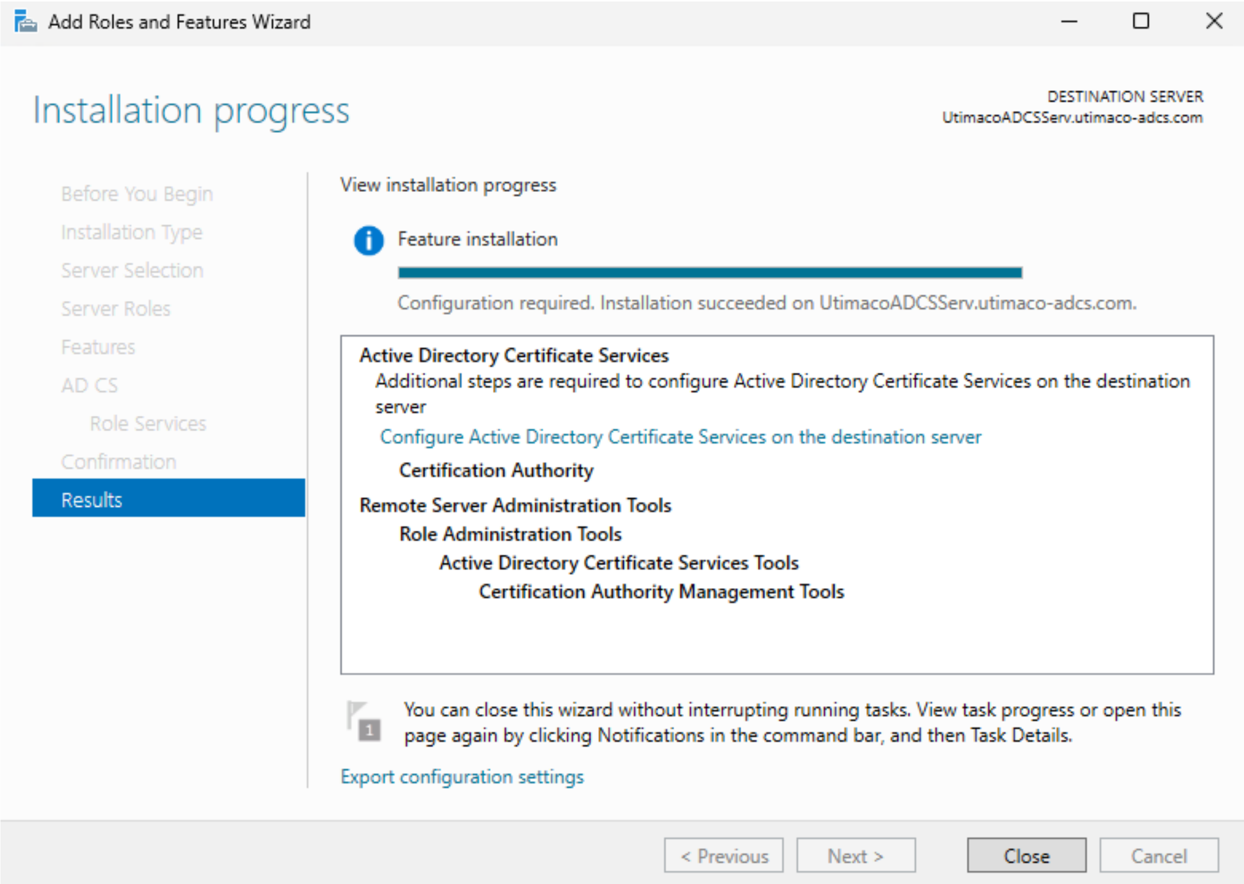

Figure 7 : "Installation progress" Window

Before going to the **Configure Active Directory Certificate Services on the destination server** menu, the CNG provider must be properly configured. Please refer to the CNG provider configuration section.

4.2.2 Install Microsoft AD CS with Windows Server Core

1. Join the domain by running the command.

›_ Console

```
> netdom join $(hostname) /domain:<full_DNS_domain_name>
/userd:<user_name> /passwordd:<password>
```

2. Restart the machine after joining the domain by running the command below.

›_ Console

```
> shutdown /r /t 0
```

3. Enable WOW64 if you are working with 32-bit applications.
4. Run PowerShell as an admin user.
5. Install CA binaries via PowerShell by running the command below.

›_ Console

```
PS> Add-WindowsFeature ADCS-Cert-Authority --IncludeManagementTools
```

5 Integration Steps

5.1 Configuration on u.trust Anchor

5.1.1 Configuring the CSP-CNG Provider

A CSP (Cryptographic Service Provider) is a general-purpose cryptography standard developed by Microsoft. It defines a cryptographic interface for applications (CryptoAPI) and an interface for manufacturers to integrate their cryptographic hardware.

A CNG (Cryptography API Next Generation) is Microsoft's second-generation cryptographic interface. It offers updated cryptographic algorithms and is intended to replace CSP in the long term.

When installing the SecurityServer setup, make sure to select the CPS/CNG - Cryptographic Service Provider (Microsoft) interface. A Cryptographic User should be created, and an MBK should be generated.

> Generating the MBK is necessary for the HSM to become operational. Without the MBK, one cannot run any cryptographic operations.

5.1.1.1 Creating HSM Users

Start the CryptoServer Administration Tool and log in as a user with the permission level of at least 02000000.

If the Key Manager and Crypto User roles are separated, a Key Manager user might need to be created.

More users with the permission level 00000010 might be needed (Group 1) to enforce "m of n" security policy for the key management, and smart card authentication might need to be used.

For this guide, only one Key Manager User will be created.

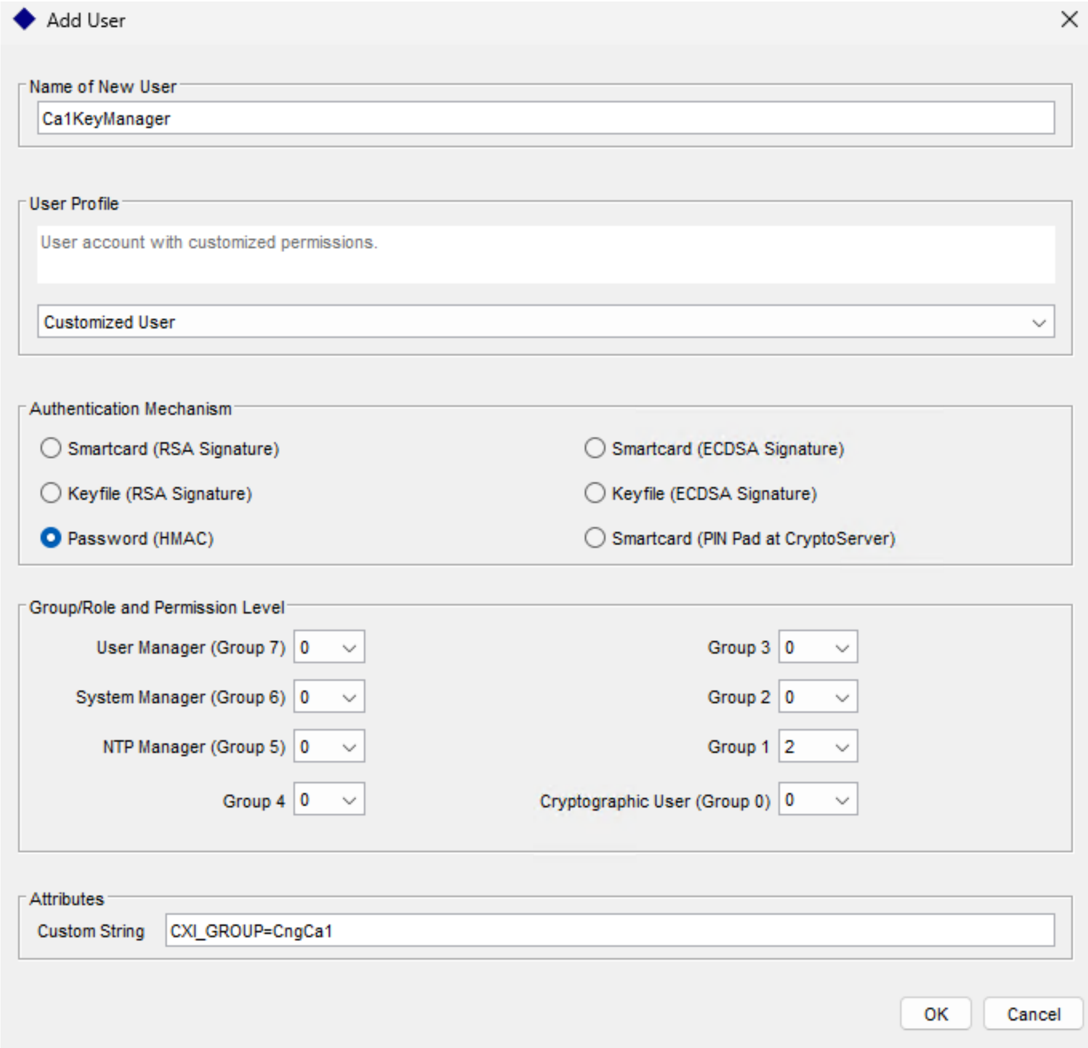

Figure 8 : Creating Key Manager User

When a Root CA with Subordinates is created, smart card authentication and the "m of n" rule with permission level of 00000001 need to be used. Because issuing certificates for subordinate CAs is not an automated task, smart card authentication allows a higher level of security to be achieved.

For subordinate CAs, where certificates are issued automatically, the credentials will have to be stored in the .cng configuration file, and Crypto Users with a permission level of 00000002 will have to be created. Use encrypted passwords. For this guide, a user with a permission level of 00000002, CXI Group "CngCa1," and HMAC password will be created.

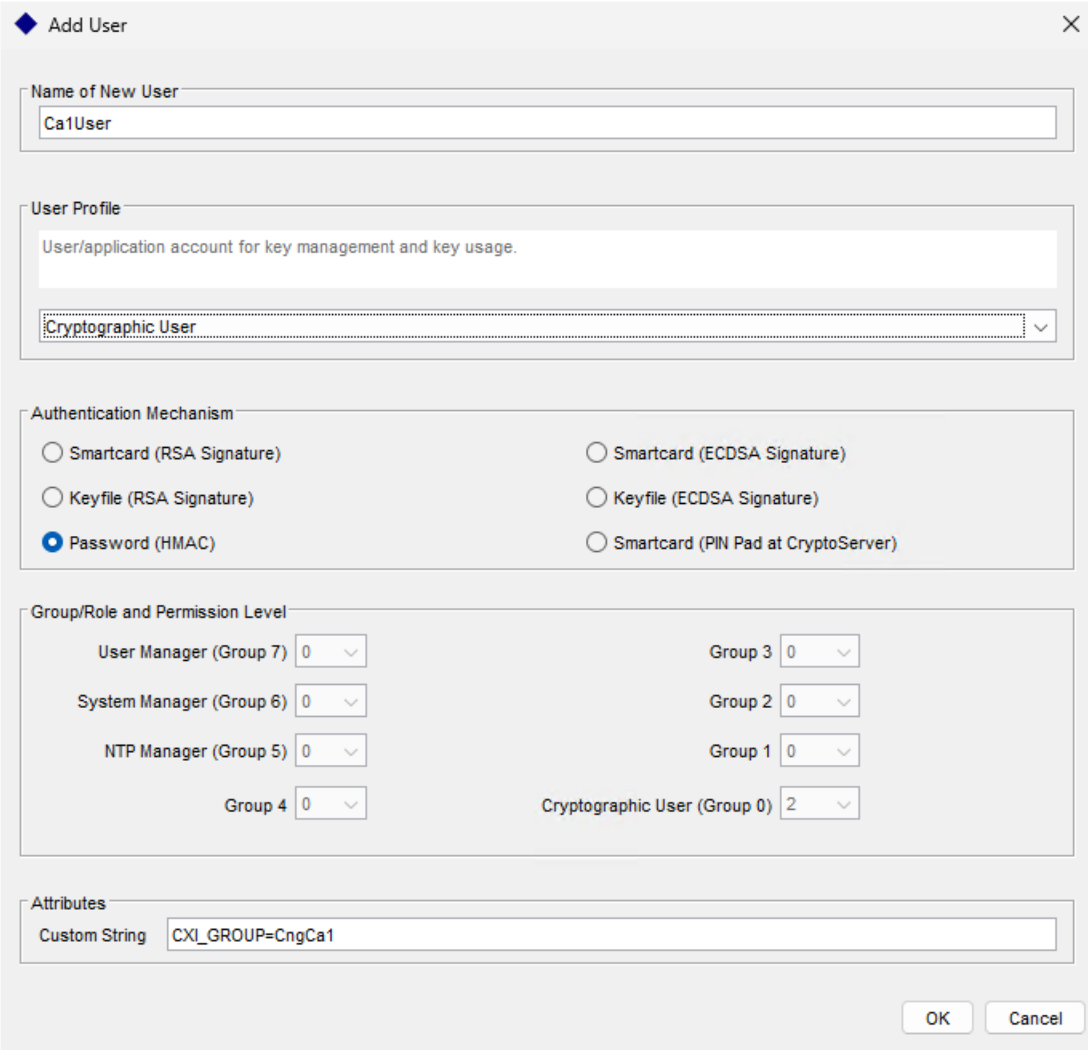

Figure 9 : Creating a Crypto User

Based on your requirement, the user can use a password (HMAC), smartcard, or keyfile protection type. If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the Smartcard and enter the pin. Then, press the OK button on the PIN Pad.

5.1.1.2 Setting up the CSP/CNG Provider

The `CS_CNG_CFG` environment variable contains the path and name of the configuration file. By default, it is located at `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`.

For advanced configuration, refer to the **CryptoServer_Manual_CSP_CNG.pdf** found on the product CD in the Documentation directory.

1. Open the `cs_cng.cfg` file with an appropriate text editor.

›_ Console

```
> notepad %CS_CNG_CFG%
```

2. For this installation, set the path to the log file and set the log level to "TRACE".

example.file

```
# Path to the logfile (name of logfile is attached by the API)
Logpath = C:\Logs\CNG\

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 4
```

To make your testing easier, it would be good to enable the CNG log file. That can be enabled by editing the Logging Loglevel. Set the LogPath and Logging Loglevel to 1. For testing, you may want to increase it to 4.

The added LogPath points to a writable directory, not to a file.

If you encounter problems, check the log file named cs_cng.log in the LogPath-defined directory. When you are done testing, you should change Logging to 1 or 2. This will limit the logging to only critical and important messages.

3. Set the Login. In this case, the name of the Cryptographic User is "Ca1User" and the HMAC password is "Utimaco19".

cs_cng.cfg

```
Login = Ca1User,HMACPwd=Utimaco19
```

If using smartcard or keyfile protection, make the appropriate change in the Login Section as shown below:

Login = username,RSASign=filename#password

Login = "SmartCardUser,RSASign=:cs2:auto:USB0@<HSM-IP>"

For additional information, refer to the **CryptoServer_csadm_Manual_Systemadministrators.pdf** document, which can be found on the product CD in the Documentation directory.

4. Set the IP address of the HSM.

cs_cng.cfg

```
[CryptoServer]

# Device specifier (here: CryptoServer is CSLAN with IP address 10.44.223.141)
Device = 10.44.223.141
```

5. The Configuration File used in this document.

cs_cng.cfg

```
# Path to the logfile (name of logfile is attached by the API)
Logpath = C:\Logs\CNG\

# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 4

# Maximum size of the logfile in bytes
Logsize = 8mb

# Keys are stored in an external or internal database
KeysExternal = false

# Path to the external keystore. Directory must be given, not file!
KeyStore = C:\ProgramData\Utimaco\CNG\keys

# Export policy for newly created keys: 0=allow all, 1=deny plain export
(standard), 2=deny all
ExportPolicy = 1

# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true

# Timeout of the open connection command in ms
ConnectionTimeout = 3000

# Timeout of command execution in ms
CommandTimeout = 60000

# CXI group for all keys. The user has to have access to this group.
Group = CngCa1

# Auto-login for CNG provider. This should be used for automated server
(re)start.
Login = Ca1User,HMACPwd=Utimaco19

# default device and fallback devices
Device = 10.44.223.141
```

For more information regarding the commands and command parameters, please check the Utimaco documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

Device = 288@<HSM IP address> Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

To test the correct configuration of the provider, the following command can be used.

›_ Console

```
> cngtool EnumProvider
Microsoft Key Protection Provider Microsoft Passport Key Storage Provider
Microsoft Platform Crypto Provider Microsoft Primitive Provider
Microsoft Smart Card Key Storage Provider Microsoft Software Key Storage
Provider Microsoft SSL Protocol Provider
Windows Client Key Protection Provider Utimaco CryptoServer Key Storage Provider
```

To get the provider information, use the following command.

›_ Console

```
>cngtool ProviderInfo
Provider : Utimaco CryptoServer Key Storage Provider
Device : 10.44.223.141
Group : CNG
Mode : Internal Key Storage
------------------------------------------------------------
Name : Utimaco CryptoServer Key Storage Provider
Name : Utimaco CryptoServer Key Storage Provider
Version : 0x02010000
Impl. -Type : 0x00000011
MaxNameLength : 0x00000104
Device : 10.44.223.141
Group : CNG
Mode : Internal Key Storage
```

5.2 Configuration on Microsoft AD CS

5.2.1 Configure the CA with Windows Enterprise

After installing Microsoft AD CS, a new CA needs to be configured.

The CNG Provider must first be configured to configure the CA. Please refer to the CNG provider configuration section.

1. On the **Notifications** menu of the Server Manager, click on **Post-deployment Configuration → Configure Active Directory Certificate Services on the destination Server**. The **AD CS Configuration menu** will appear.

2. On the **Credentials** window, make sure that Administrator's credentials are displayed in the Credentials box. If not, select **Change** and specify the appropriate credentials. Click **Next.**

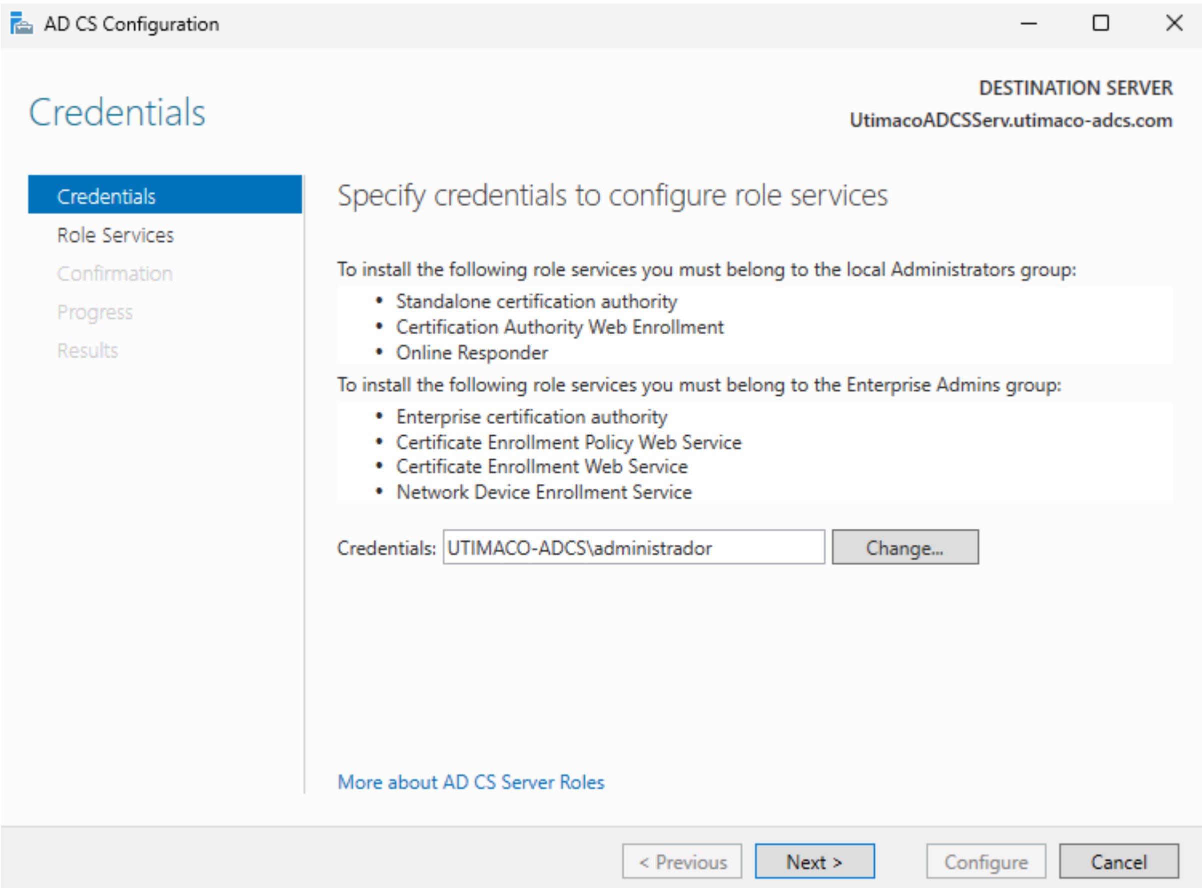

Figure 10 : "Credentials" Window

3. On the **Role Services** window, select **Certification Authority**. This is the only available selection when the certification authority role is installed on the server. Click **Next.**

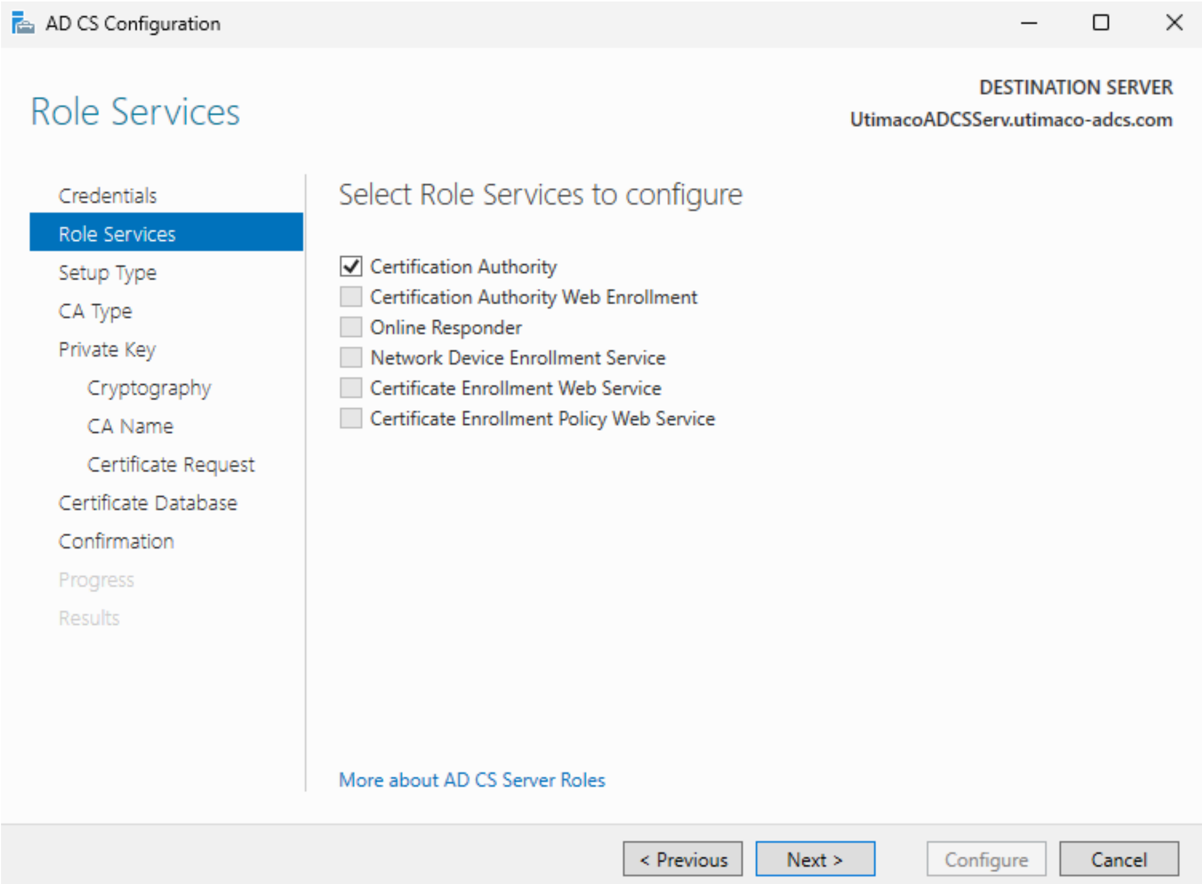

Figure 11 : "Role Services" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

4. On the **Setup Type** window, select the appropriate CA setup type for your requirements. Click **Next**.

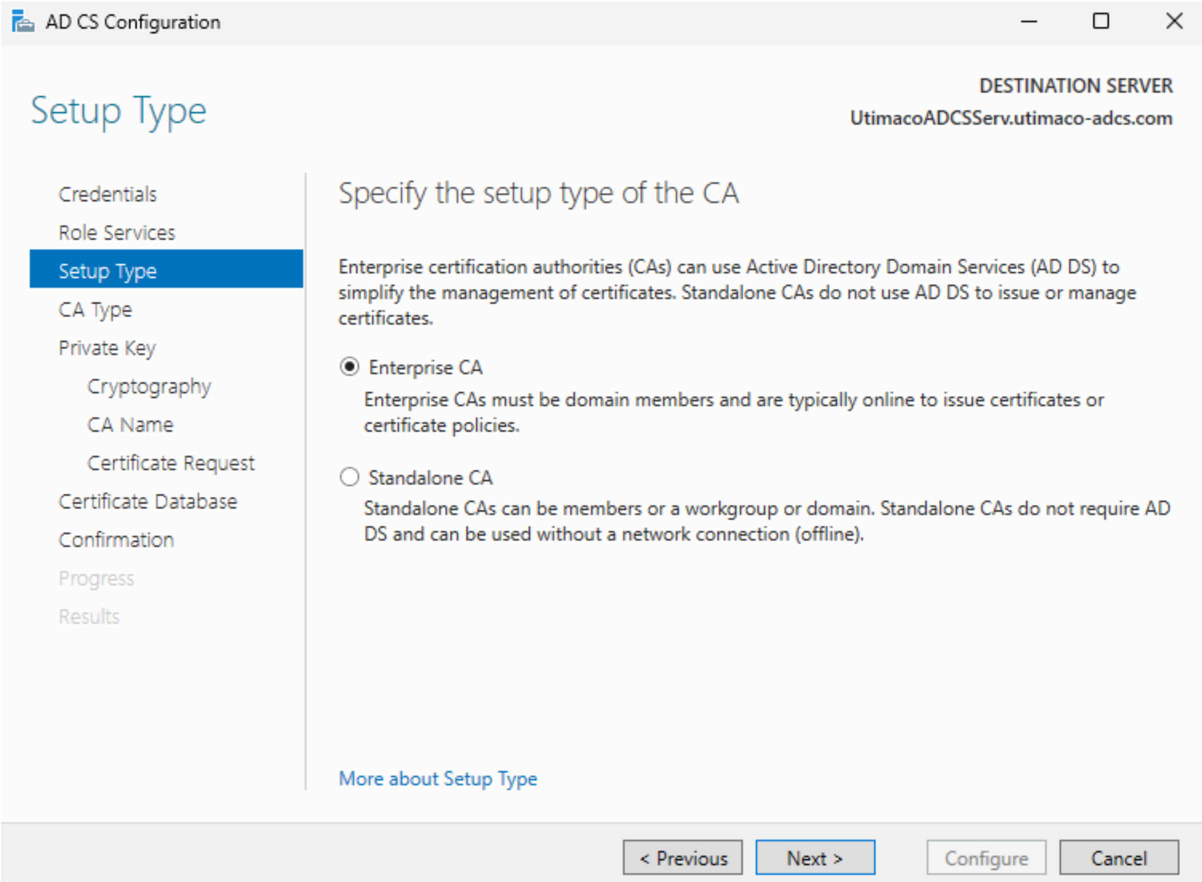

Figure 12 : "Setup Type" Window

5. On the **CA Type** window, **Root CA** is selected by default. Click **Next.**

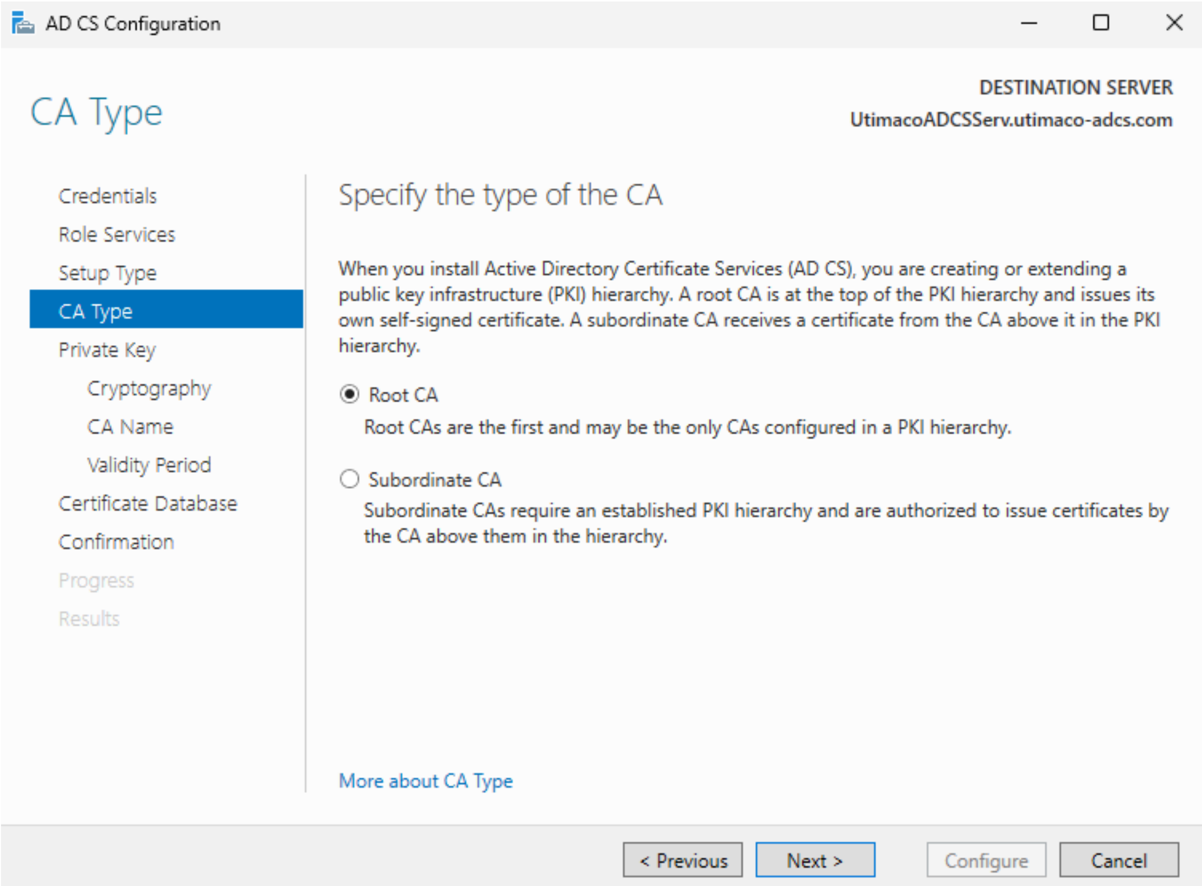

Figure 13 : "CA Type" Window

6. On the **Private Key** window, leave the default selection to **Create a new private key** selected. Click **Next.**

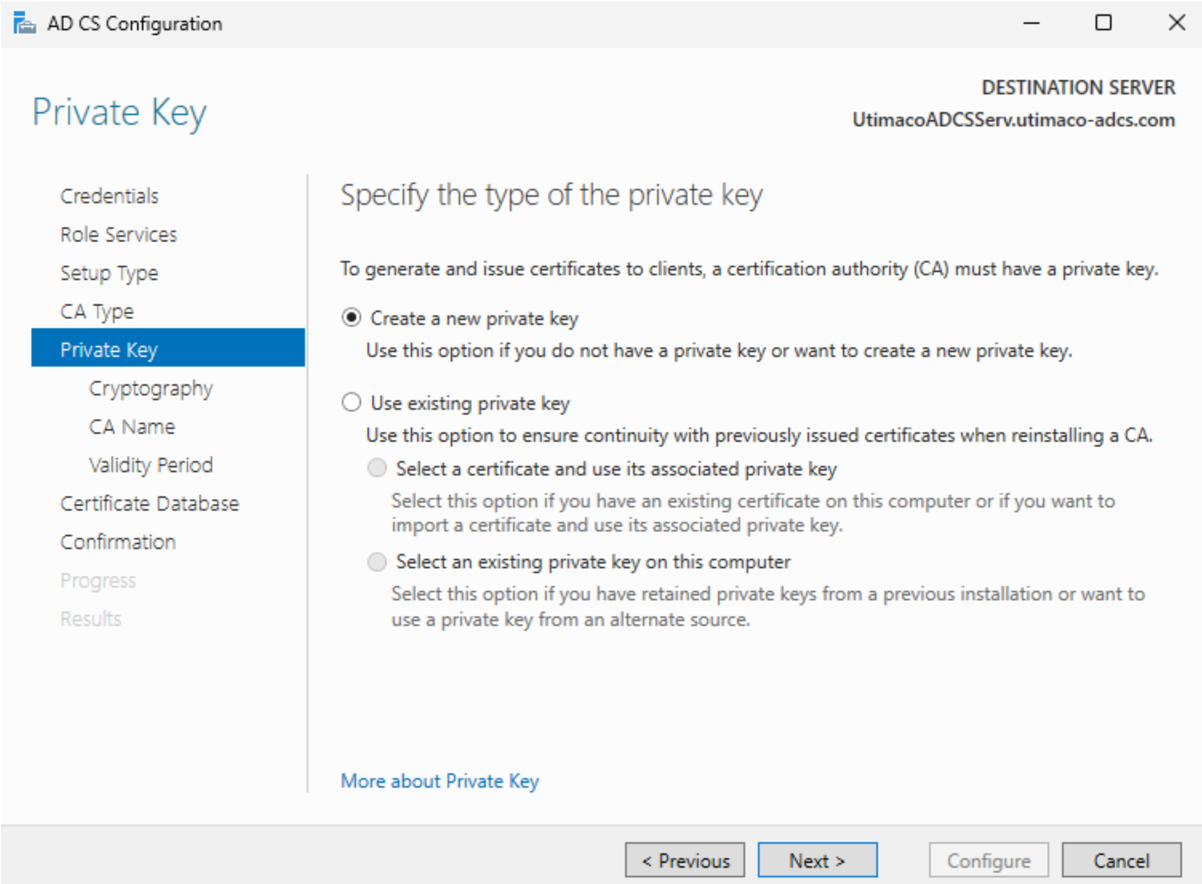

Figure 14 : "Private Key" Window

7. On the **Cryptography for CA** window, select the appropriate Utimaco CryptoServer cryptographic provider along with the key type, key length, and suitable hash algorithm:
    - RSA #Utimaco CryptoServer Key Storage Provider
    - ECDSA_P256 #Utimaco CryptoServer Key Storage Provider
    - ECDSA_P384 #Utimaco CryptoServer Key Storage Provider
    - ECDSA_P521 #Utimaco CryptoServer Key Storage Provider

If keyfile or smartcard protection is used, select the **Allow administrator interaction when the private key is accessed by the CA** option.

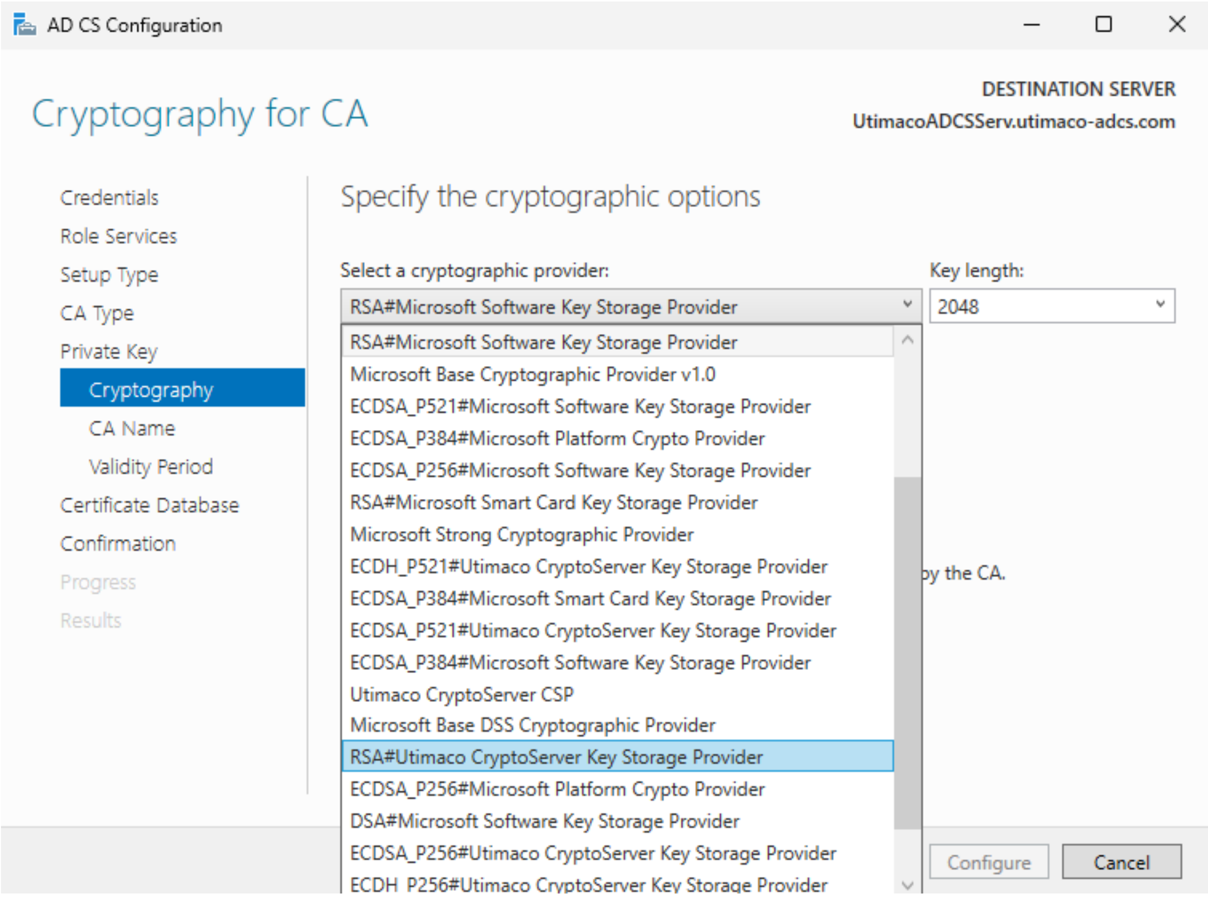

Figure 15 : "Cryptography for CA" Window

> If the `Utimaco CryptoServer Key Storage Provider` options are missing, it means there is an error with the Utimaco CNG Provider. Please refer to the CNG provider configuration section if the provider has not been configured, or execute `certutil -csplist` on a Windows terminal to see the error. If more information on the error is needed, please review the logging file placed by default in `C:\ProgramData\Utimaco\CNG\log\cs2cng.log`.

8. Click **Next.**
9. On the **CA Name** window, give the appropriate CA name. Click **Next.**

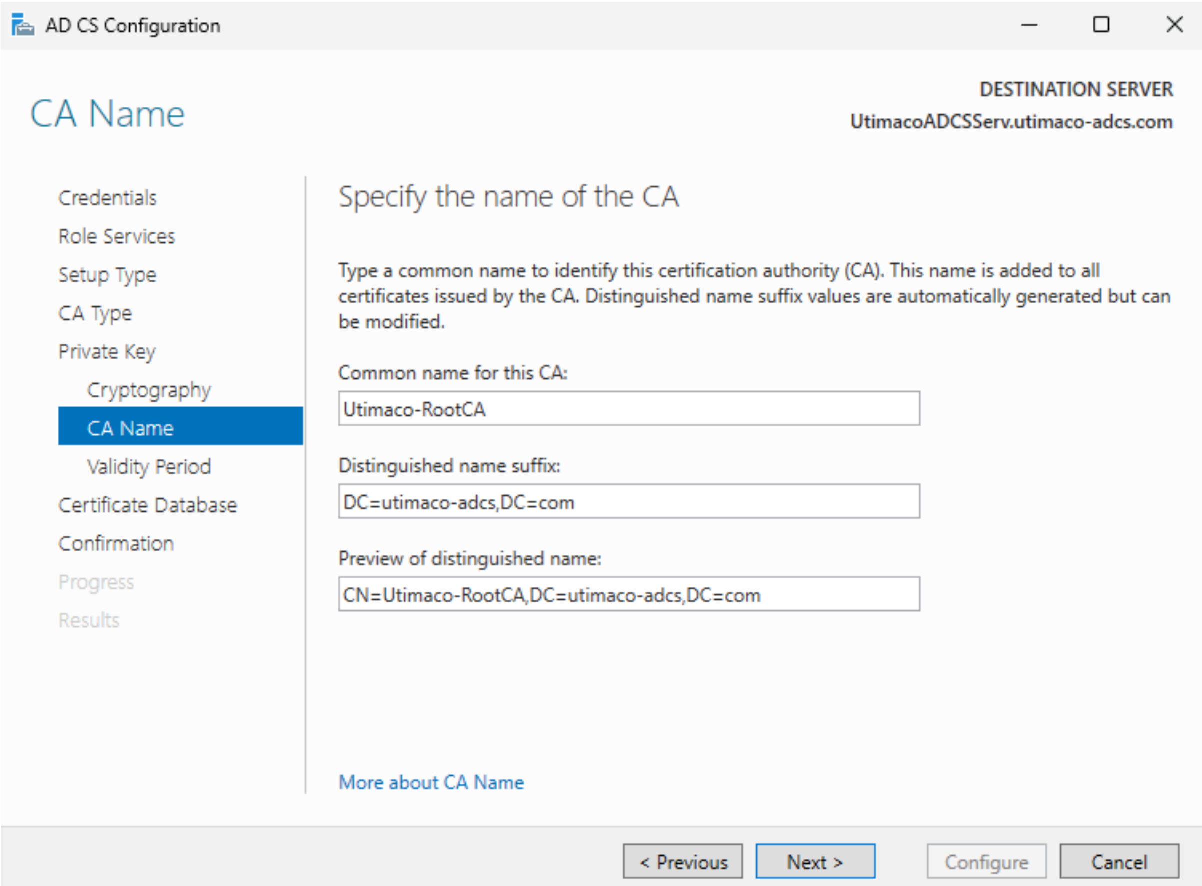

Figure 16 : "CA Name" Window

10. On the **Validity Period** window, enter the number of years for the certificate to be valid. Click **Next.**

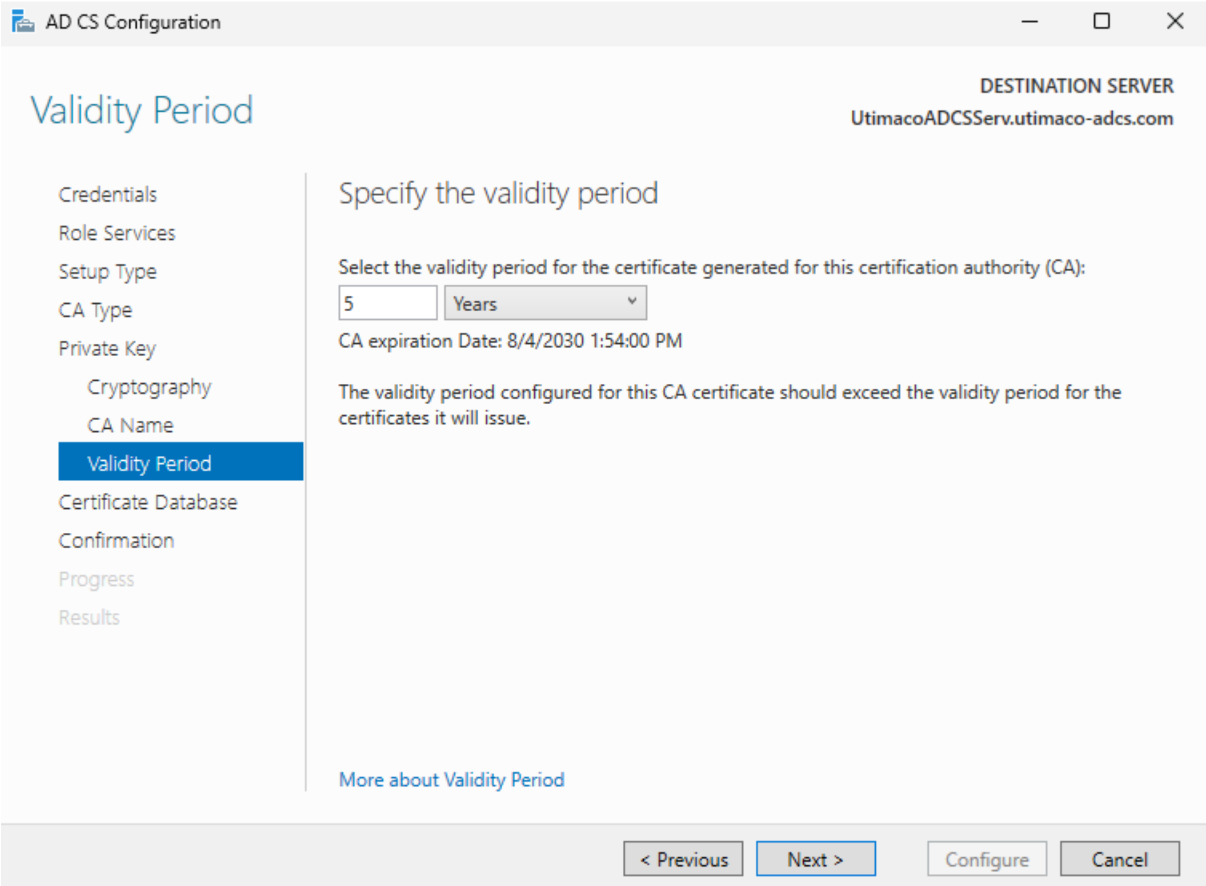

Figure 17 : "Validity Period" Window

11. On the **CA Database** window, leave the default locations for the database and database log files. Click **Next.**

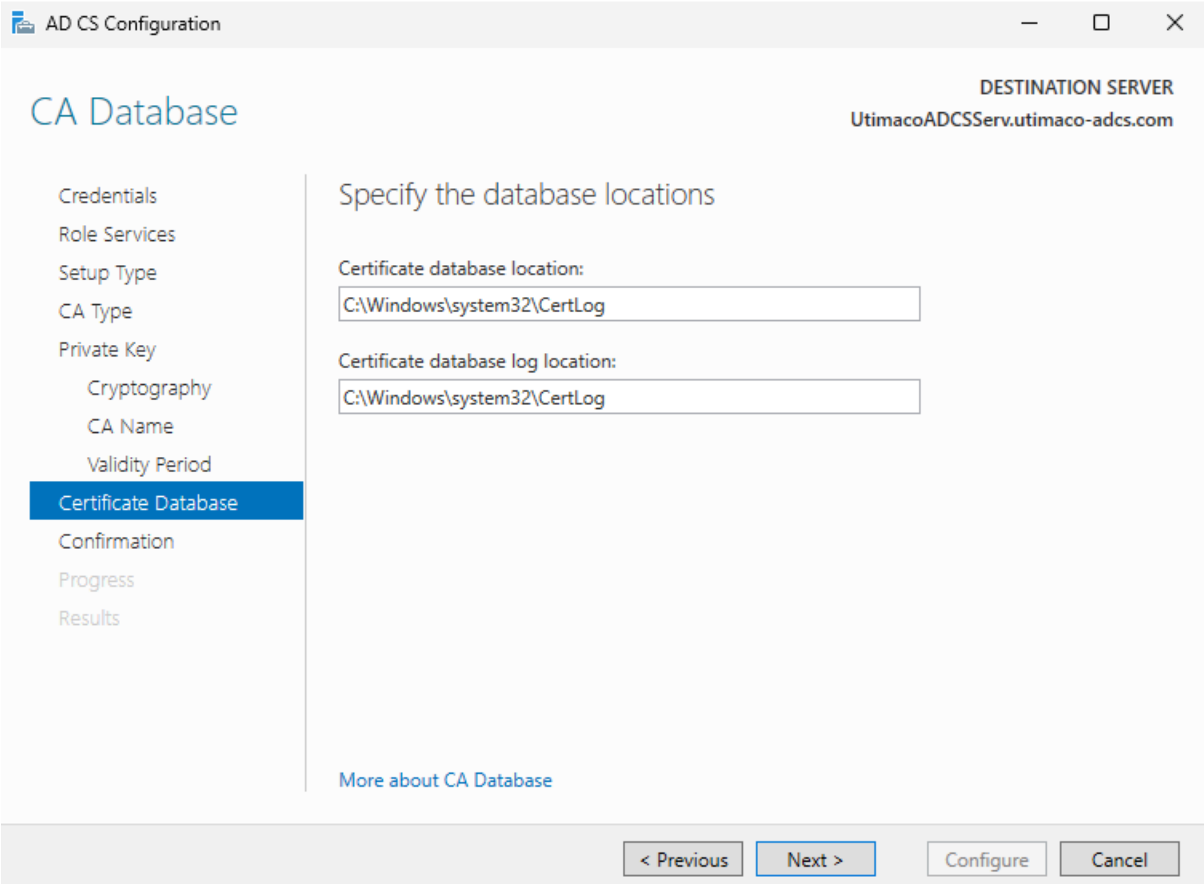

Figure 18 : "CA Database" Window

12. On the **Confirmation** window, click **Configure.**

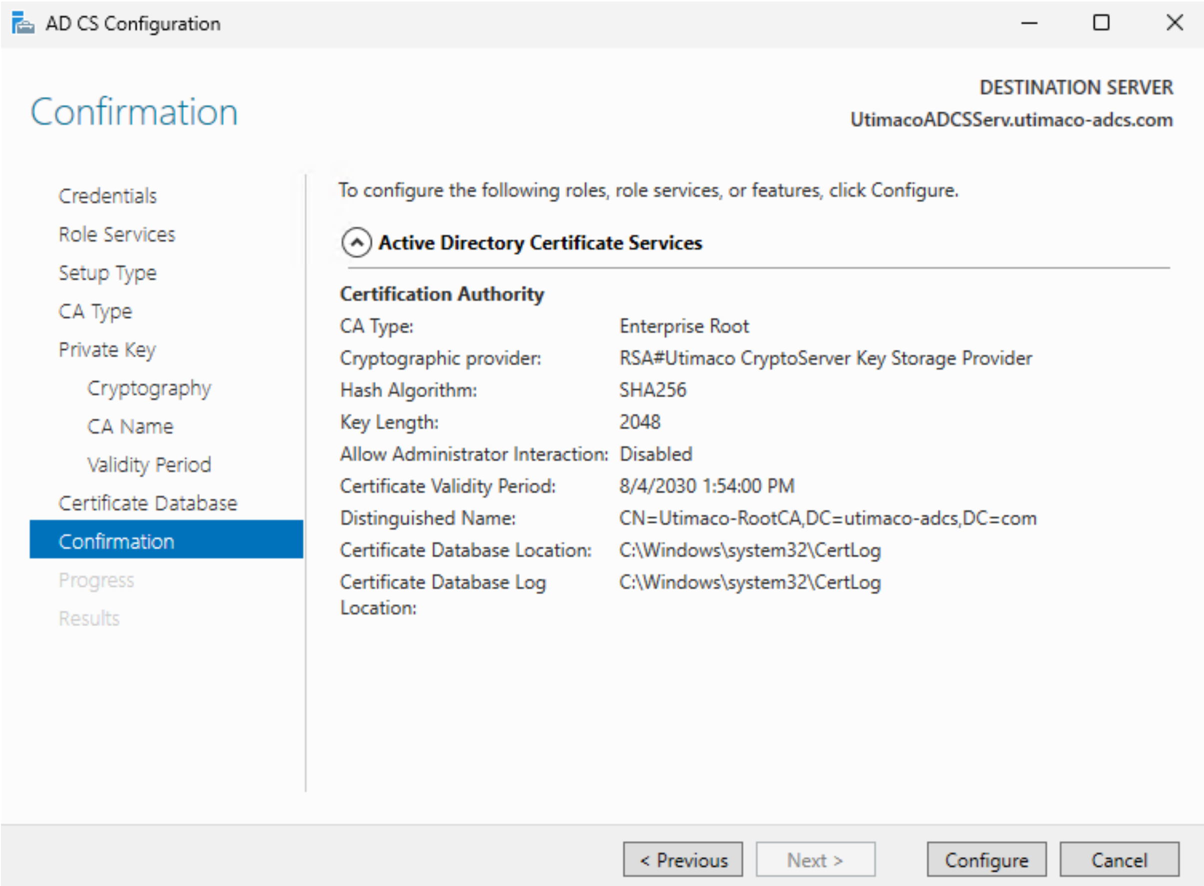

Figure 19 : "Confirmation" Window

13. 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.

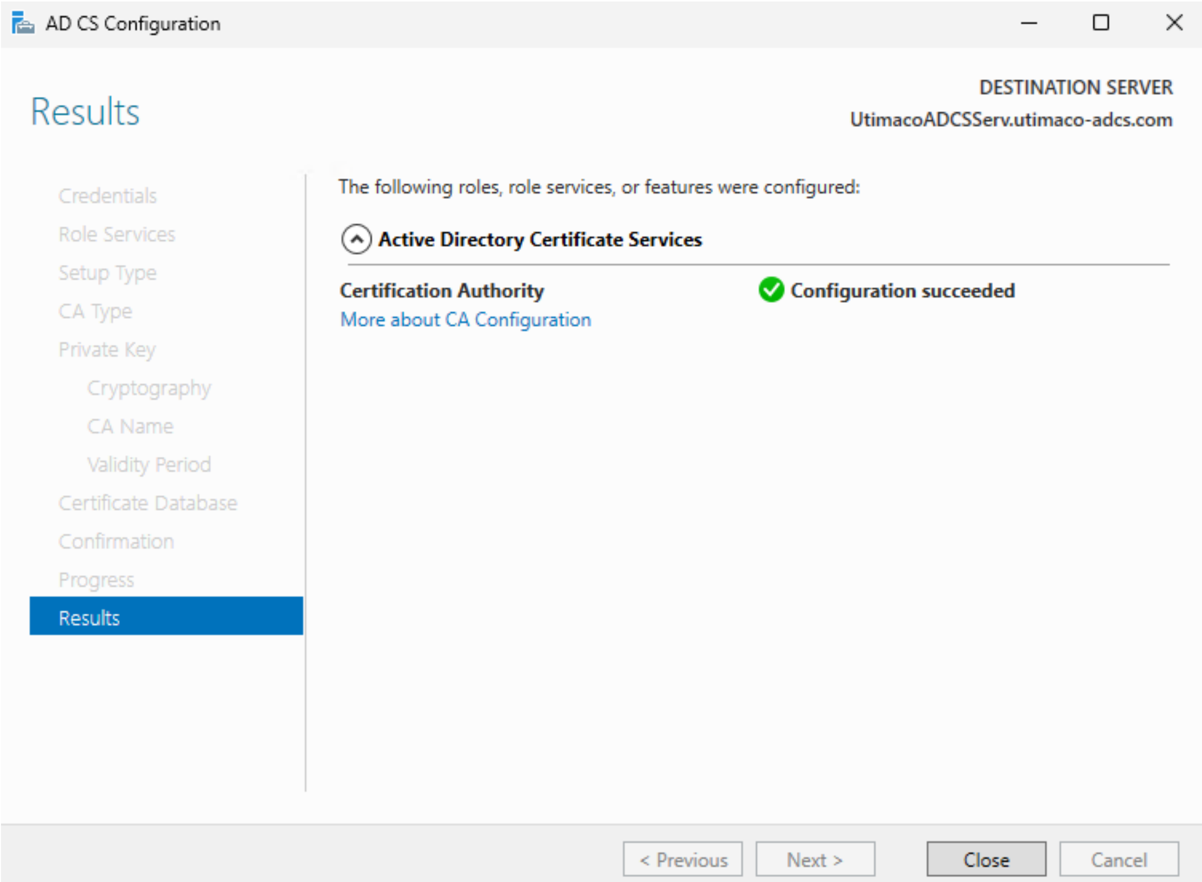

Figure 20 : "Results" Window

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

14. Open a command prompt and run the following command to verify that the service is running:

›_ Console

```
> sc query certsvc
```

15. Open a command prompt and run the following command to verify the CA key.

›_ Console

```
> certutil -verifykeys
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

The command shows that the CA keys have successfully been verified.

5.2.2 Configure the CA with Windows Server Core

After installing AD CS, the Certification Authority must be configured.

1. Configure CA via PowerShell, by running the command below.

›_ Console

```
PS> Install-AdcsCertificationAuthority -AllowAdministratorInteraction -caType
EnterpriseRootCA -CryptoProviderName ECDSA_P256#HSM_KSP_NAME -KeyLength 256 -
HashAlgorithmName SHA256
```

The `cngtool` utility by Utimaco can be used to get the `CryptoProviderName` . The command to list the Algorithms available in the provider is `cngtool ListAlgos` .

Example

›_ Console

```
PS> Install-AdcsCertificationAuthority -AllowAdministratorInteraction -caType
EnterpriseRootCA -CryptoProviderName "ECDSA_P384#Utimaco CryptoServer Key
Storage Provider" -KeyLength 384 -HashAlgorithm SHA384 -CACommonName Root-CA
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

2. When the confirmation message appears, type A and press Enter.
3. To verify that the CA service has started, open a command prompt and run the command below.

›_ Console

```
PS> sc query certsvc
```

5.2.3 Testing the AD CS

To test that the installation is successful, try to issue a certificate.

1. Open the command prompt and run `certmgr.msc` command.

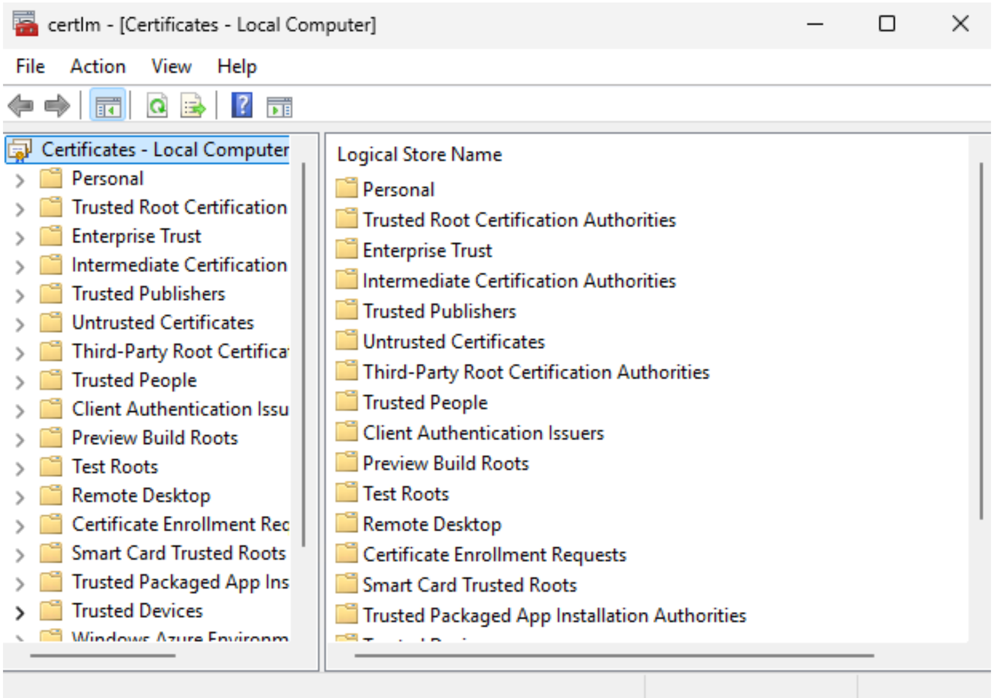

Figure 21 : "Certificate Manager Console" Window

2. Go to the **Certificates,** then select **Current User.** Then select **Personal** and click on the **Certificates** directory.

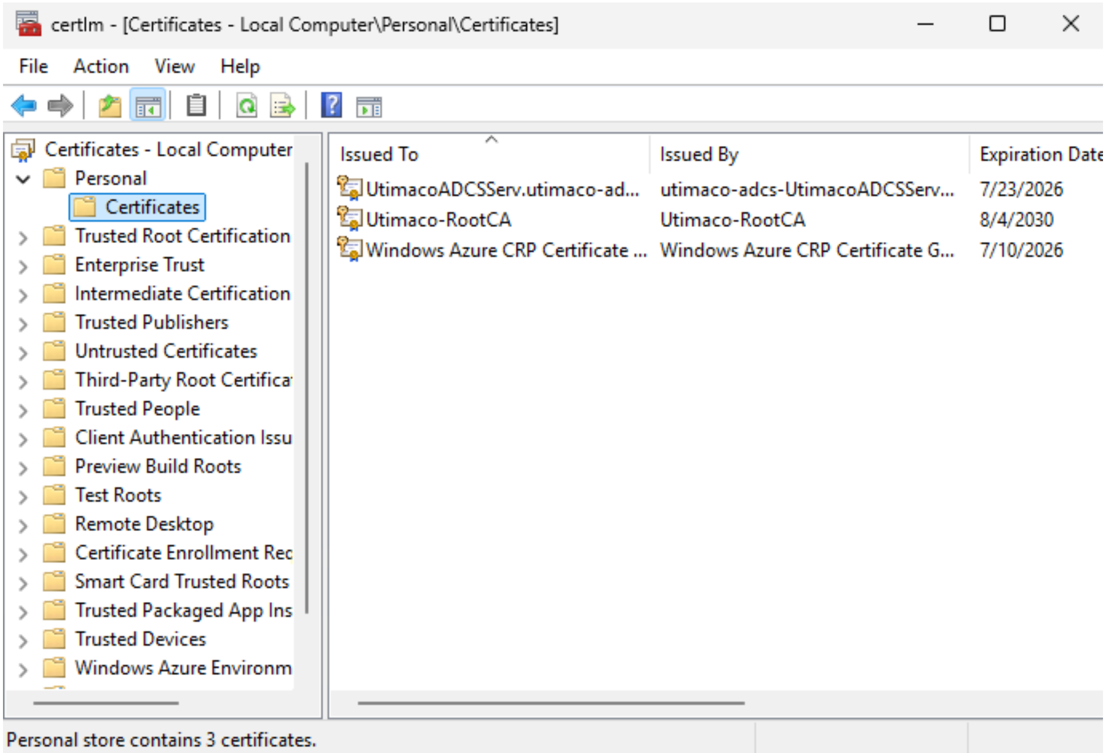

Figure 22 : "Certificate Directory" Window

3. Right-click on the directory **Certificates,** followed by **All tasks**, then **Request New Certificate.**

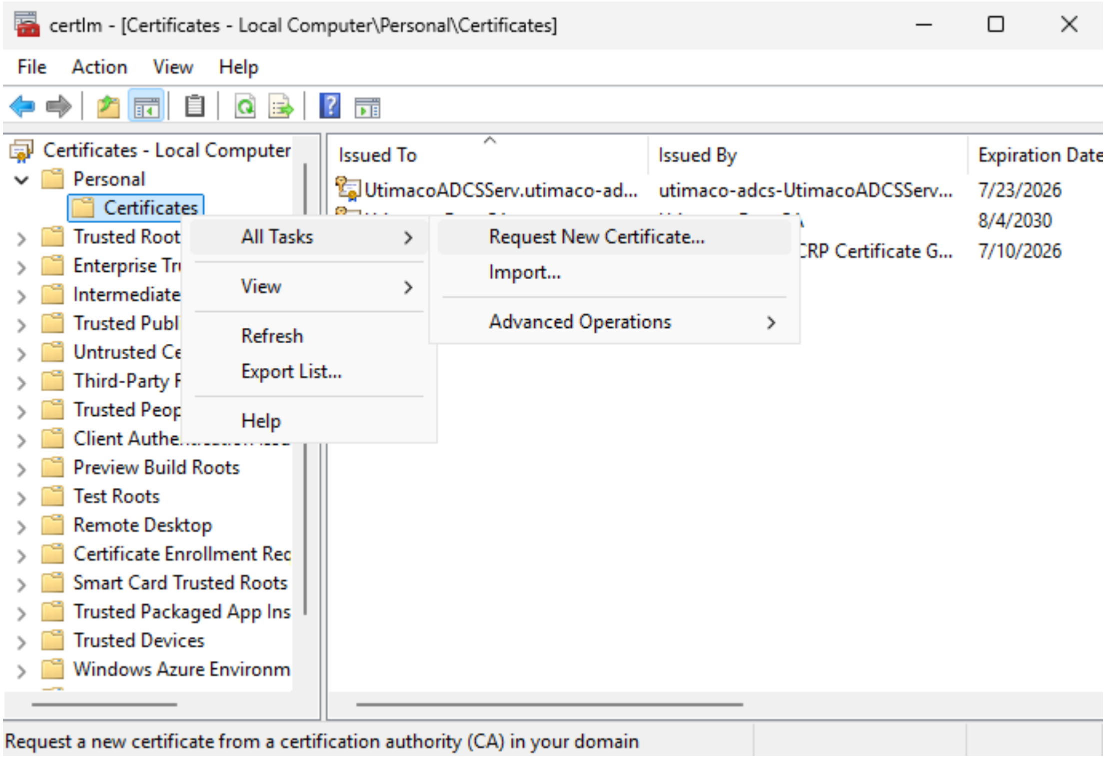

Figure 23 : "Certificate Directory" Window

4. In the **Before You Begin** window, click **Next.**

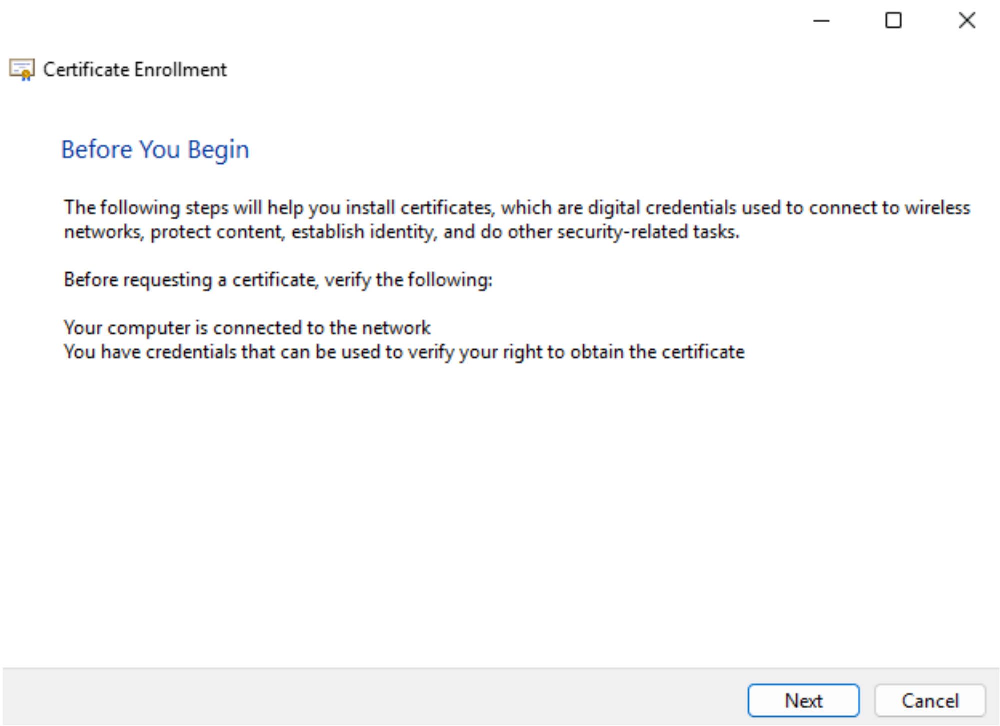

Figure 24 : "Before You Begin" Window

5. In the **Select Certificate Enrollment Policy** window, click **Next.**

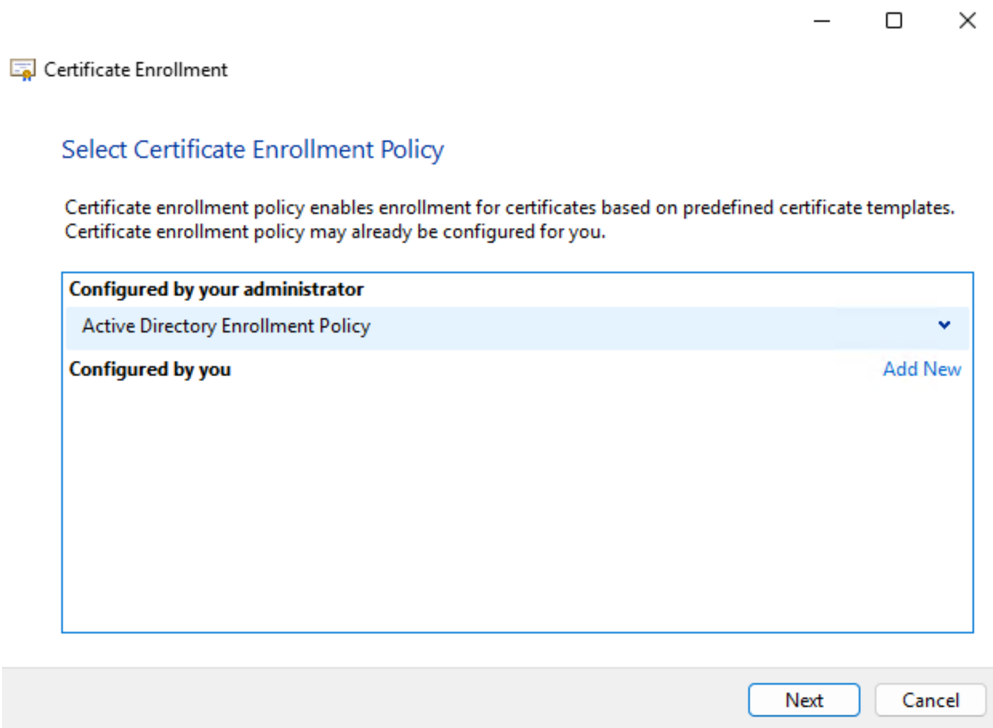

Figure 25 : "Certificate Enrollment" Window

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6. Enable the checkbox for **User template** and click **Enroll.**

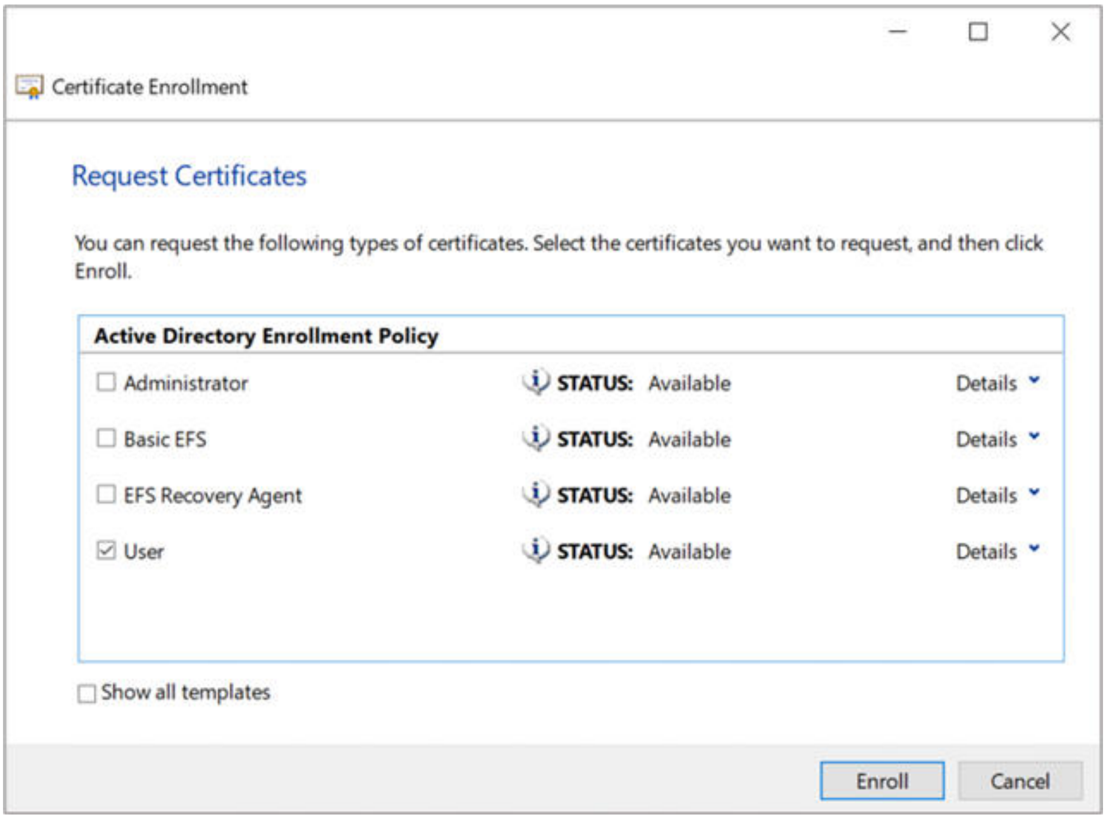

Figure 26 : "Request Certificates" Window

Verify that the certificate is enrolled successfully. The **Enrollment** wizard shows if the certificate enrollment was successful.

5.2.4 Configuring the Auto-Enrollment Group Policy for a Domain

To complete the integration, you must configure the auto-enrollment as a group policy.

1. On the domain controller, select **Start,** then click on **Administrative Tools,** then click on **Group Policy Management.**
2. Select **Forest**, then select your **Domain** and expand it.

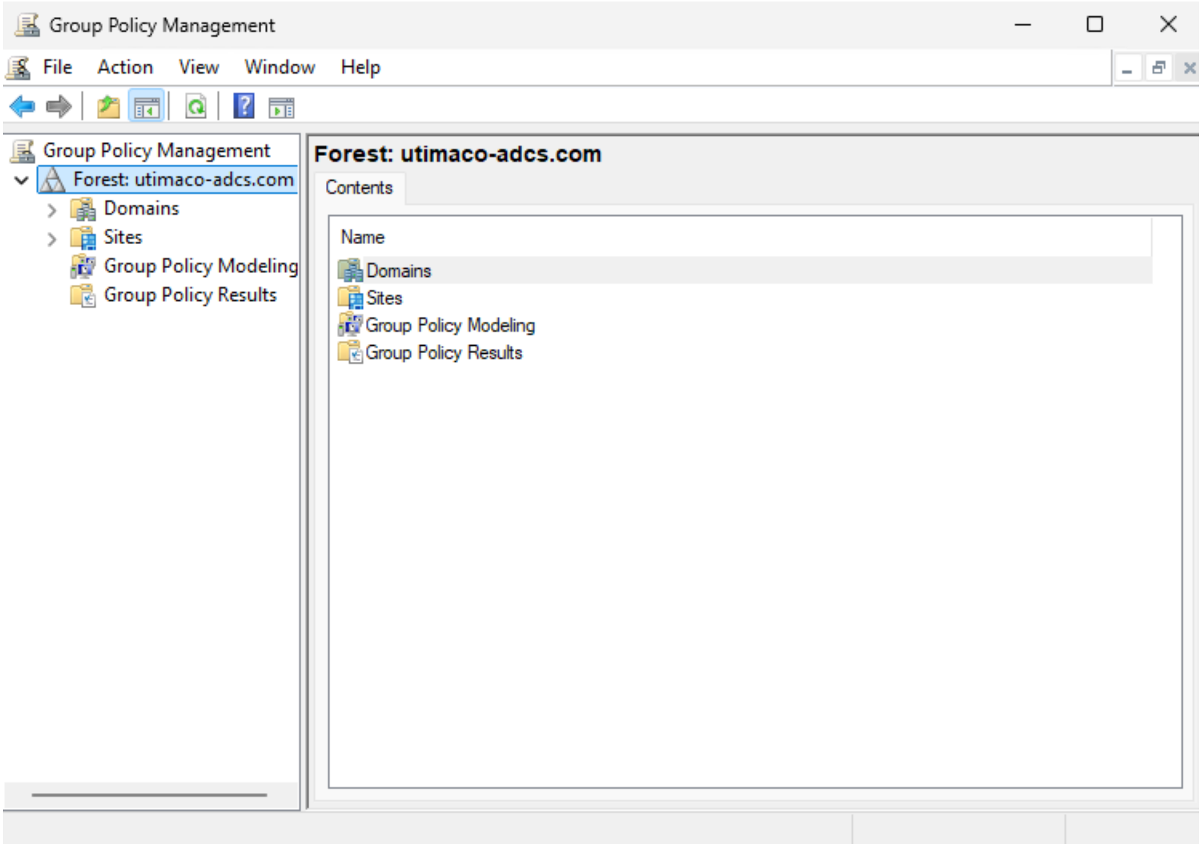

Figure 27 : "Group Policy Management" Window

3. Double-click **Group Policy Objects** in the Forest.

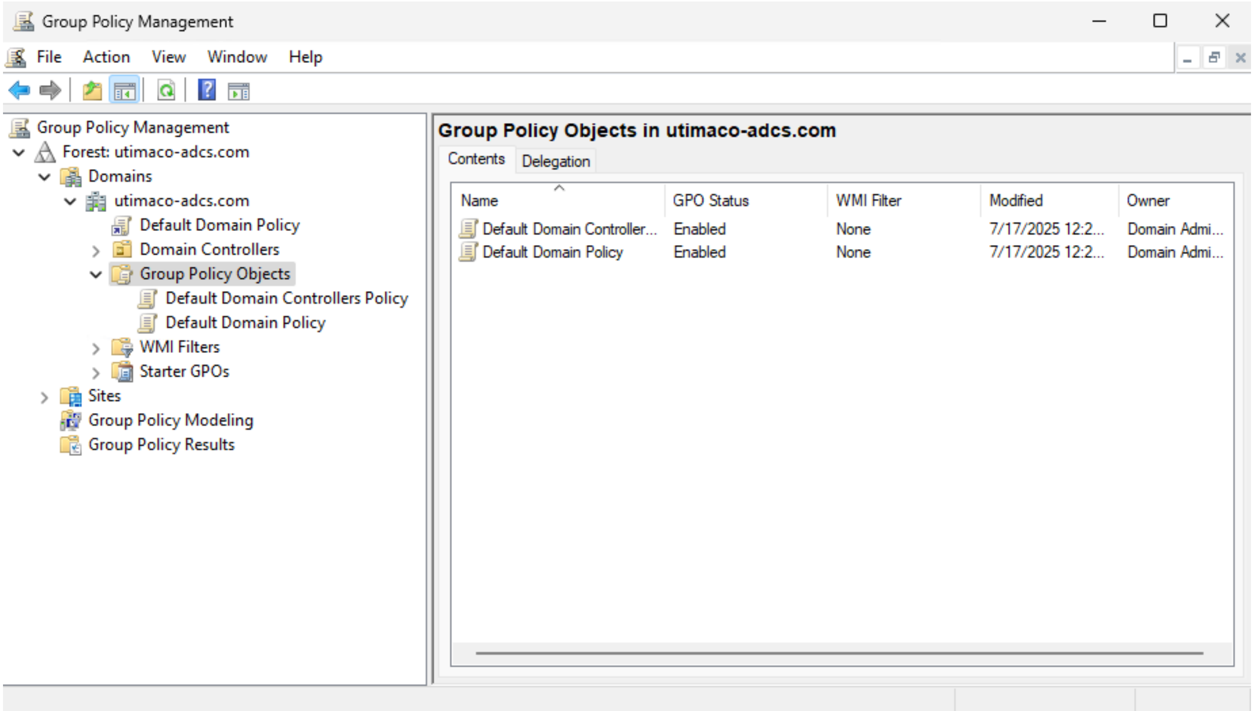

Figure 28 : "Group Policy Management" Window

4. Right-click the **Default Domain Policy**, then select **Edit.**

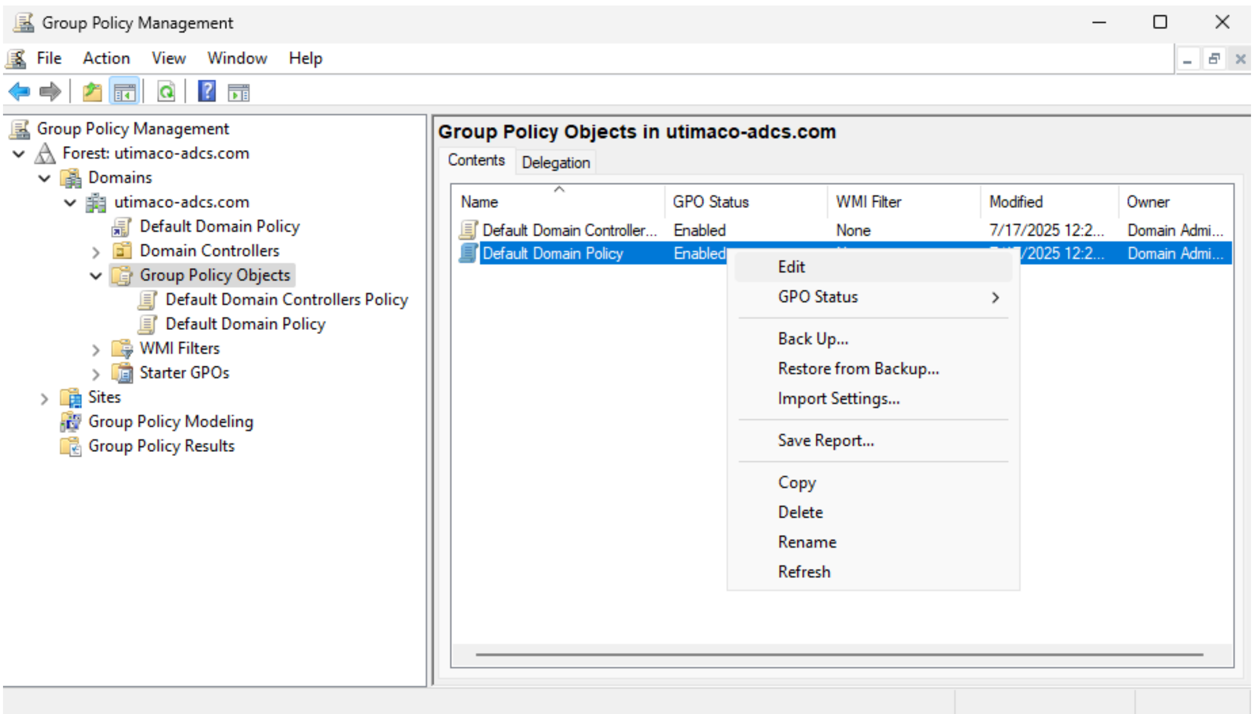

Figure 29 : "Group Policy Management" Window

5. In the **Group Policy Management Editor**, select **Computer Configuration,** then click on **Policies.** Next, click on **Windows Settings**, followed by **Security Settings, and** then click on **Public Key Policies.**

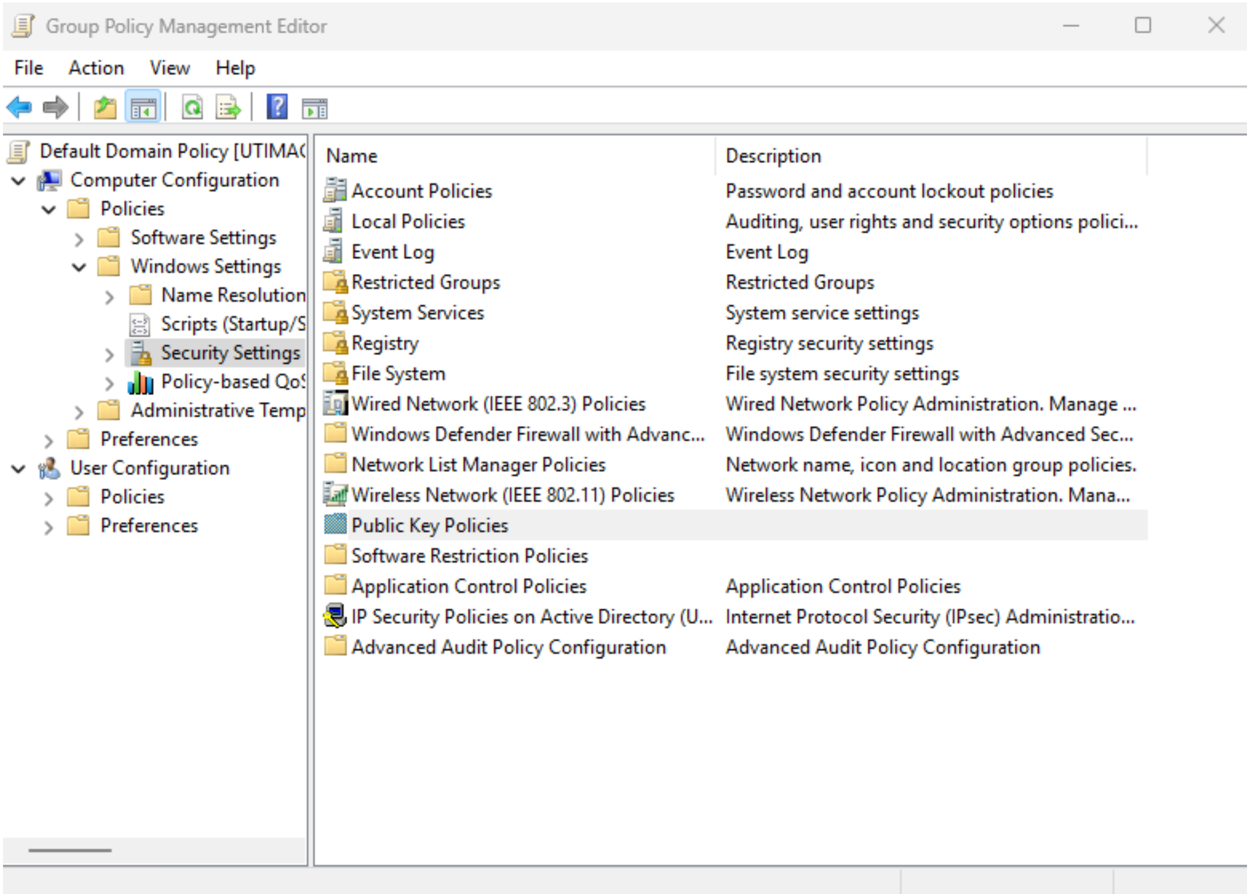

Figure 30 : "Group Policy Management Editor" Window

6. Double-click **Certificate Services Client,** then click on **Auto-Enrollment.**

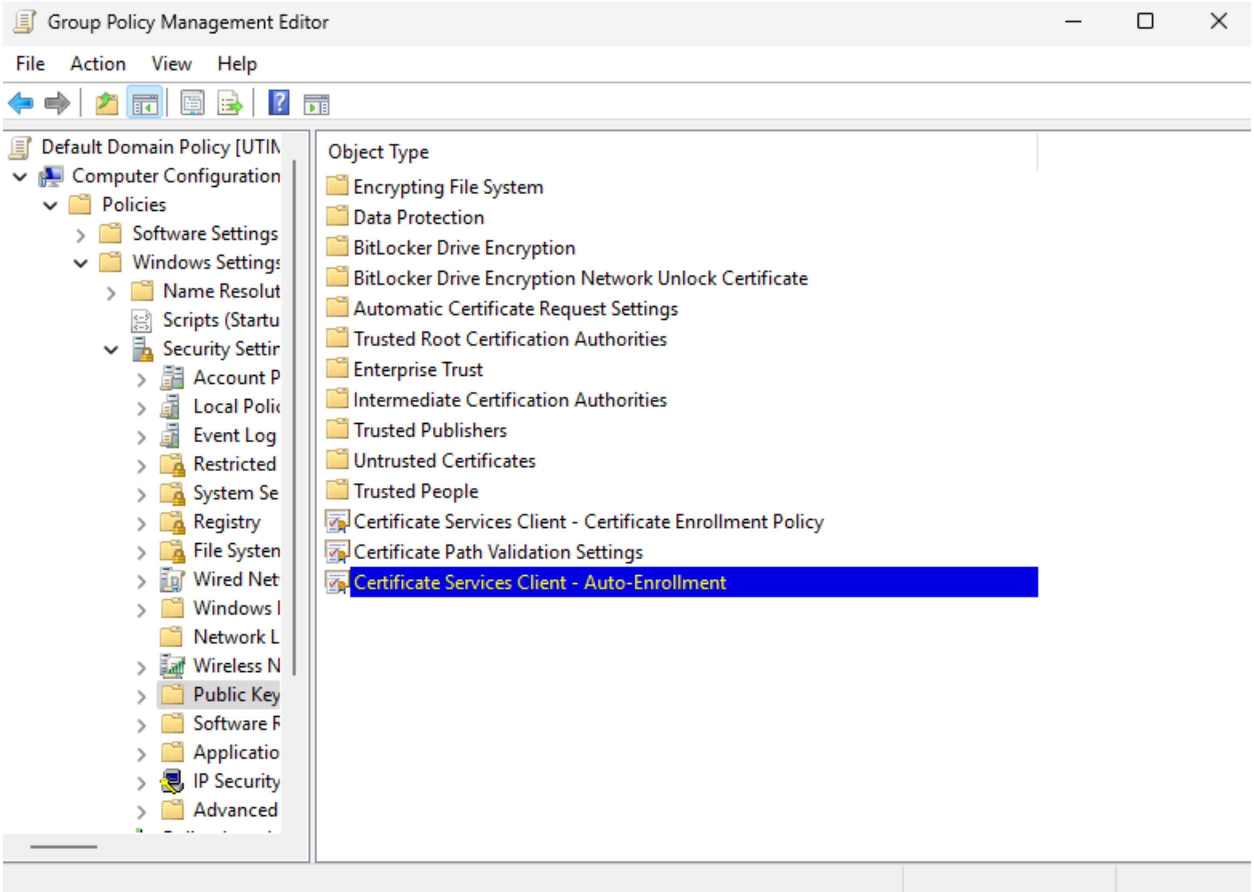

Figure 31 : "Group Policy Management Editor" Window

7. In **Configuration Model**, select **Enabled** to enable auto-enrollment. Select the following options:

    - Renew expired certificates, update pending certificates, and remove and revoke certificates.
    - Update certificates that use the certificate template.

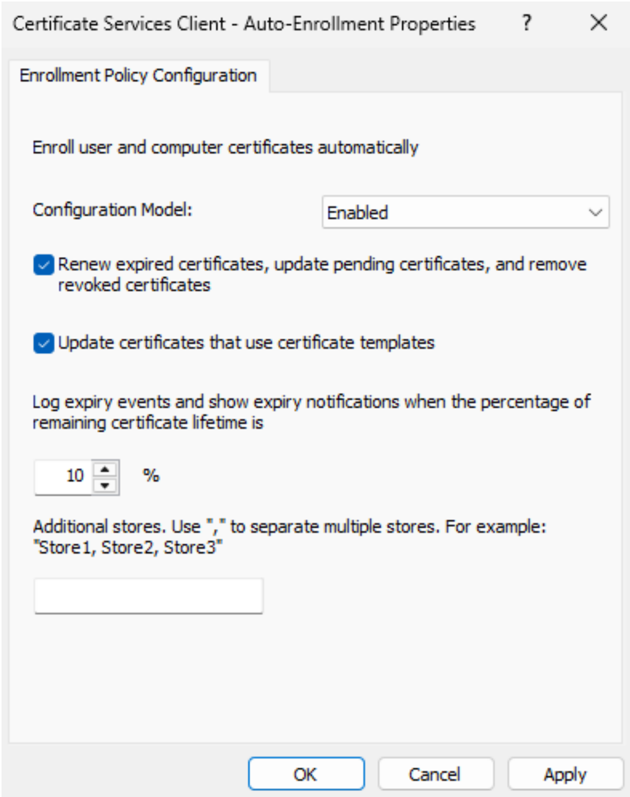

Figure 32 : "Enrollment Policy Configuration" Window

8. Select **Apply** and **OK** to accept your changes and close the Editor.

6 Verification and Testing

6.1 Functional Testing

6.1.1 Configuring the Certificate Enrollment to Use CA Templates on the AD CS Server

This section describes how to create certificate templates when the private key is managed using an HSM. All subscribers who enroll for a certificate based on such a template must have a client connection to the HSM.

> If a CA installed on Windows Server Core is managed remotely, the snap-ins in this section must run on a separate machine with GUI capabilities.

To integrate the CA certificate enrollment functionality with a CA private key generated by the Utimaco HSM:

1. Create a CA template that uses the Utimaco HSM.
2. Open the command prompt and run the `certtmpl.msc` command.

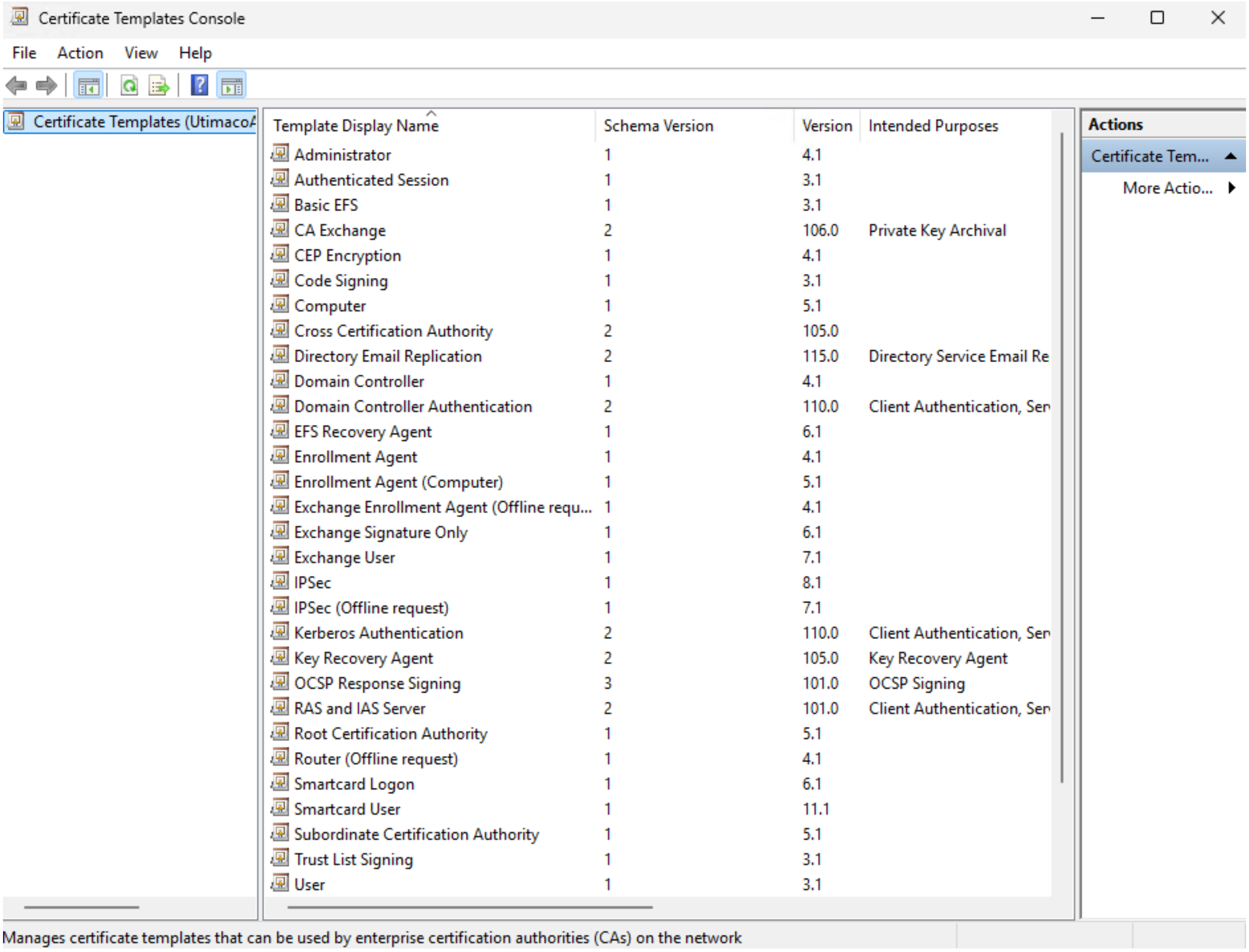

Figure 33 : "Certificate Template Console" Window

3. Right-click the **Administrator** template, then select **Duplicate Template**. The **Properties** window opens, showing the **Compatibility** tab.

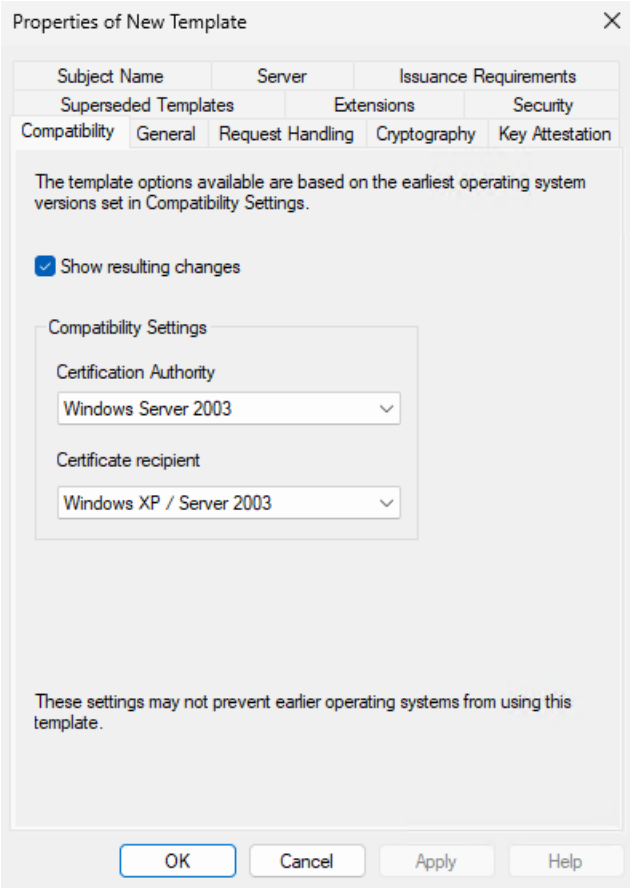

Figure 34 : "Compatibility Tab" Window

4. Select the appropriate windows version under **Certificate Authority** and **Certificate Recipient** drop-down box.

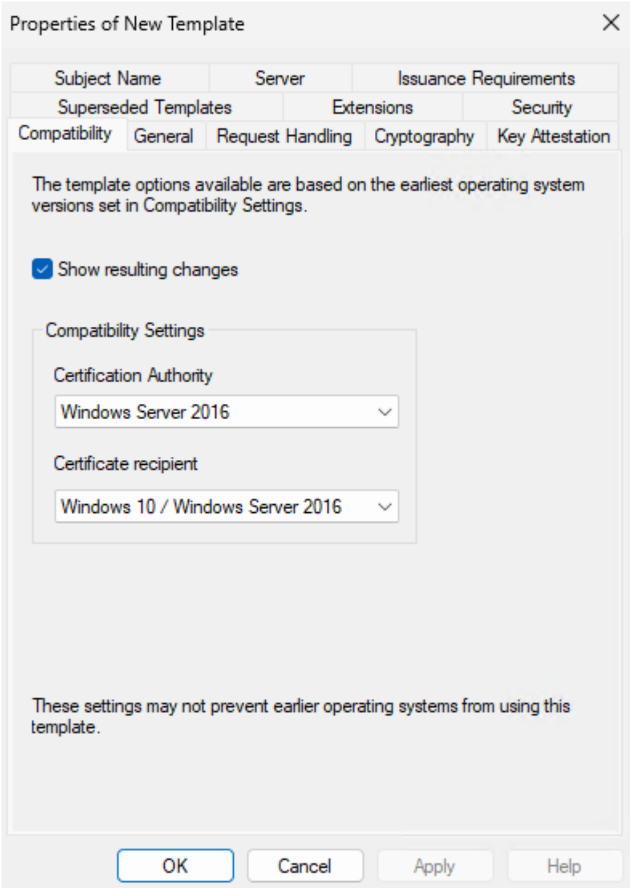

Figure 35 : "Compatibility Tab" Window

5. Select the **General** tab. In the Template display name, type a name for the template.

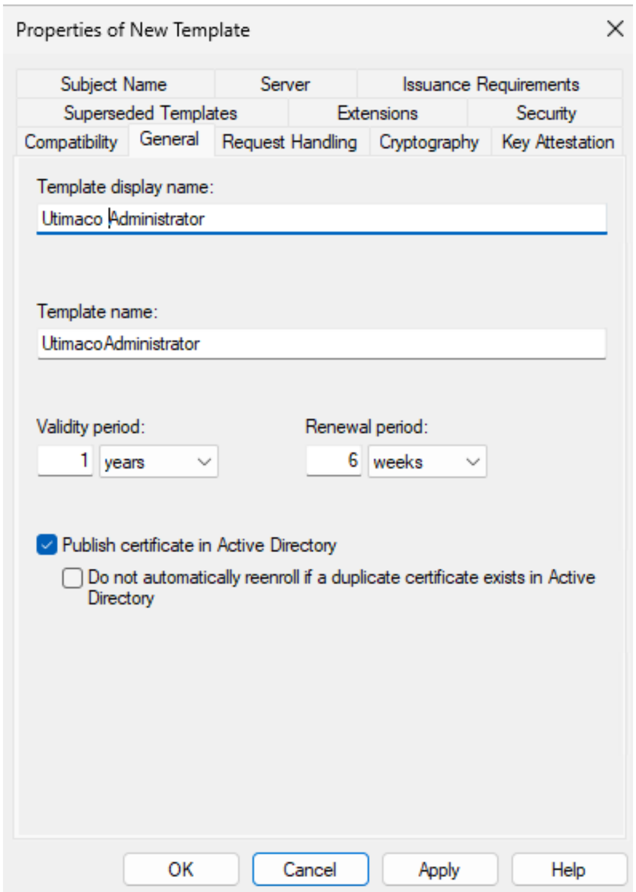

Figure 36 : "General Tab" Window

6. Select the **Request Handling** tab, and in **Purpose** select **Signature** and deselect **Allow private key to be exported.**

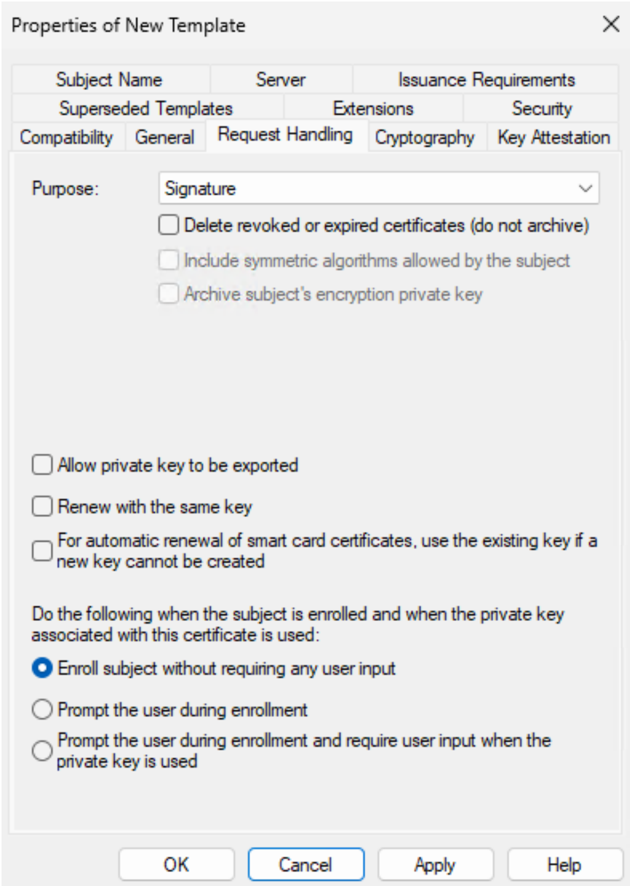

Figure 37 : "Request Handling Tab" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

7. Select the **Cryptography** tab and in the **Provider** category, select **Key storage provider.**
8. In **Algorithm Name**, select the algorithm from the list.
9. Click on the radio button for **Requests must use one of the following providers,** and in **Providers**, select **Utimaco CryptoServer Key Storage Provider** only.

If the CA is on Windows Server Core and you are managing it remotely using certtmpl.msc on a different PC, you need to install the Utimaco CryptoServer Key Storage Provider on the PC that is running certtmpl.msc. Otherwise, the Utimaco CryptoServer provider will not appear.

10. In **Request Hash**, select a hash type.

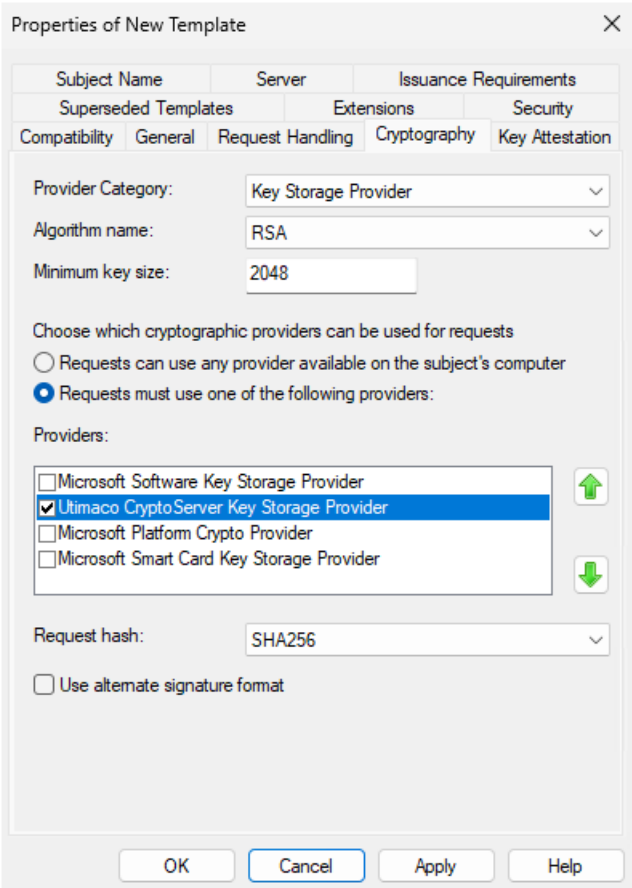

Figure 38 : "Cryptography Tab" Window

11. Select **Subject Name** tab and deselect **Include e-mail name in subject name** and deselect **E-mail name.**

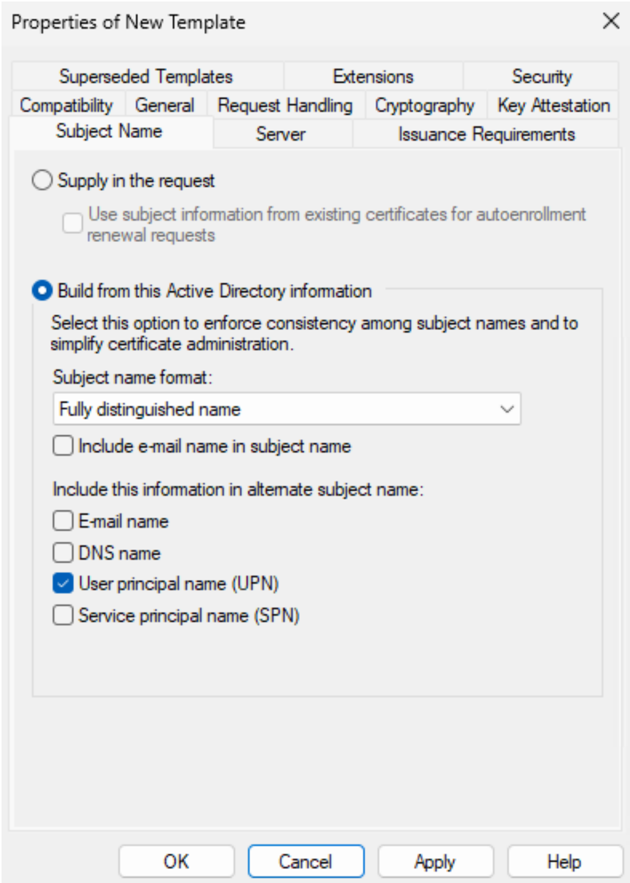

Figure 39 : "Subject Name Tab" Window

12. Select **Apply** and **OK** to save the template settings and close the **Certificate Template** console.

13. Open the command prompt and run the `certsrv.msc` command.

> Windows Server Core: If a CA is configured on Windows Server Core and is managed via the Microsoft Management Console (MMC) from a different machine, you might get an error that states: Cannot manage Active Directory Certificate Services. To fix this, select **OK**, then in the certsrv.msc~ console that appears, select **Action** and click on **Retarget Certification Authority**. In the window that appears, select **Another Computer**, then select **Browse** to find the CA you want to manage.

> Windows Server Core: Sometimes an error appears indicating that the RPC server is unavailable. To fix this, sign in to the Windows Server Core machine and minimize the command prompt. A window prompts you to load a key. Complete the steps in the window and attempt to select the CA again from certsrv.msc.

14. In the left-hand pane, select the **Certificate Authority** name.

15. Right-click the **Certificate Template** node, then select **New,** then select **Certificate Template to Issue.**

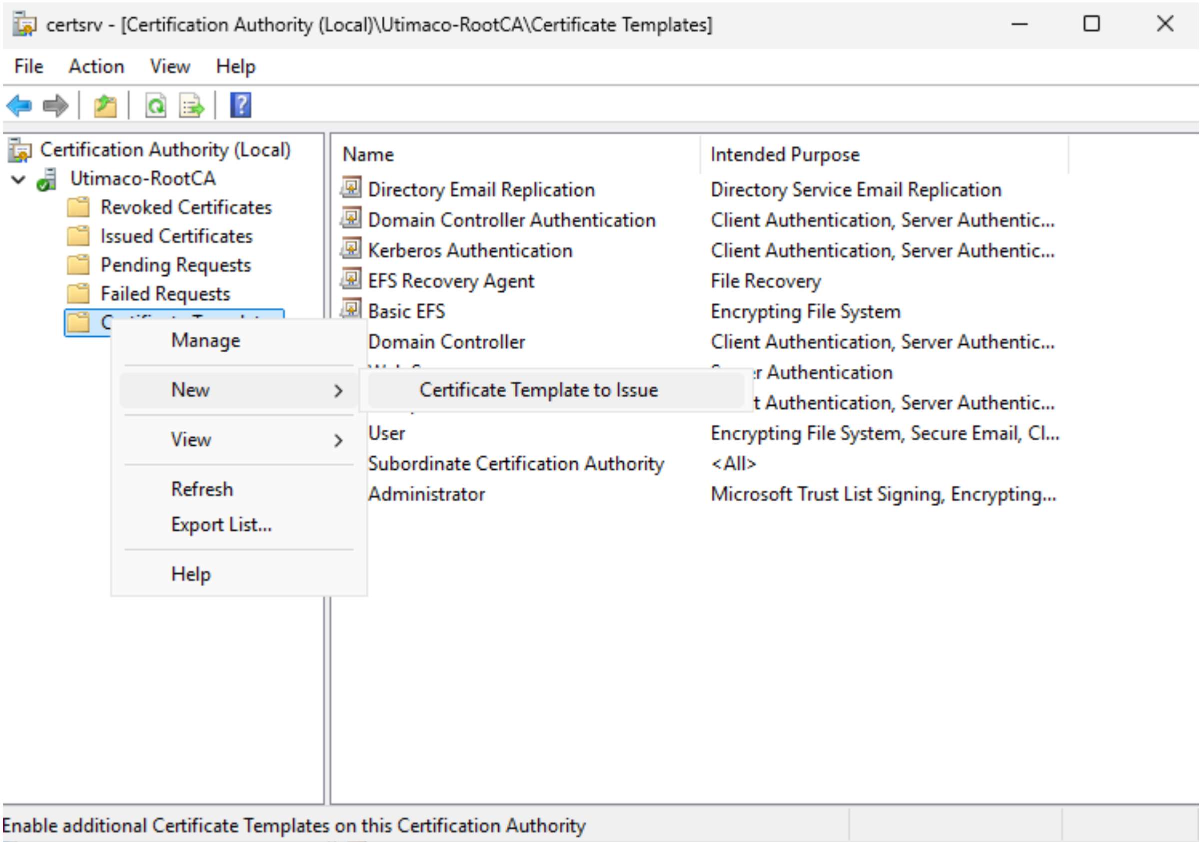

Figure 40 : "Certificate Templates Tab" Window

16. Select the template you just created, then click **OK.**

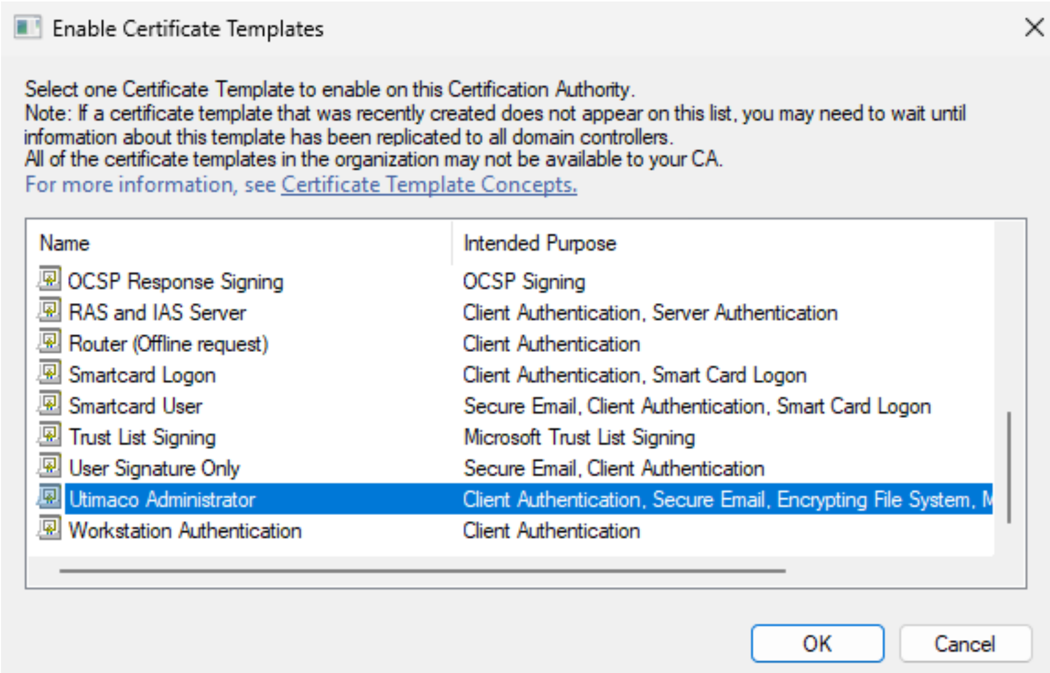

Figure 41 : "Enable Certificate Templates" Window

17. Request a certificate based on the template:

    a. Open the command prompt and run the `certmgr.msc` command.

    b. In the left-hand pane, right-click the **Personal** node, then select **All Tasks,** then **Request New Certificate.**

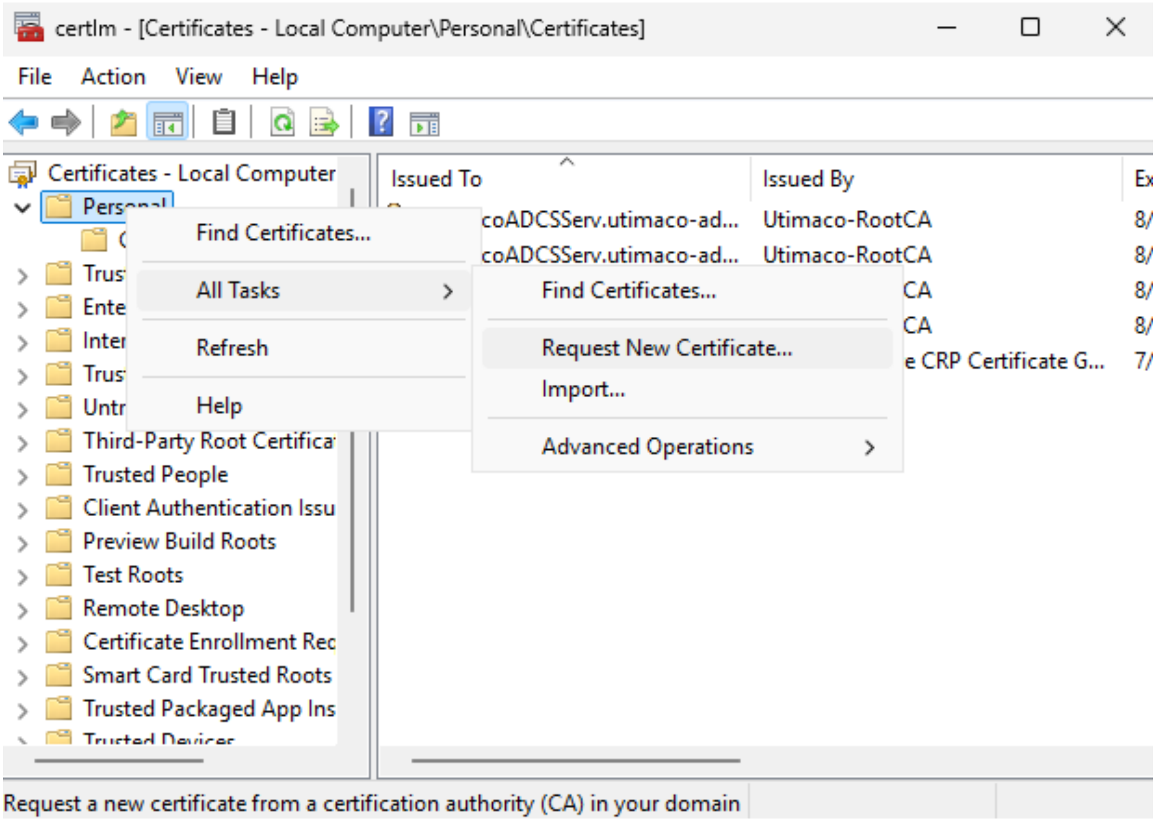

Figure 42 : "Certificate Manager" Window

18. Select **Next** in the first two windows.

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

19. Select the template that you created, then click **Enroll.**

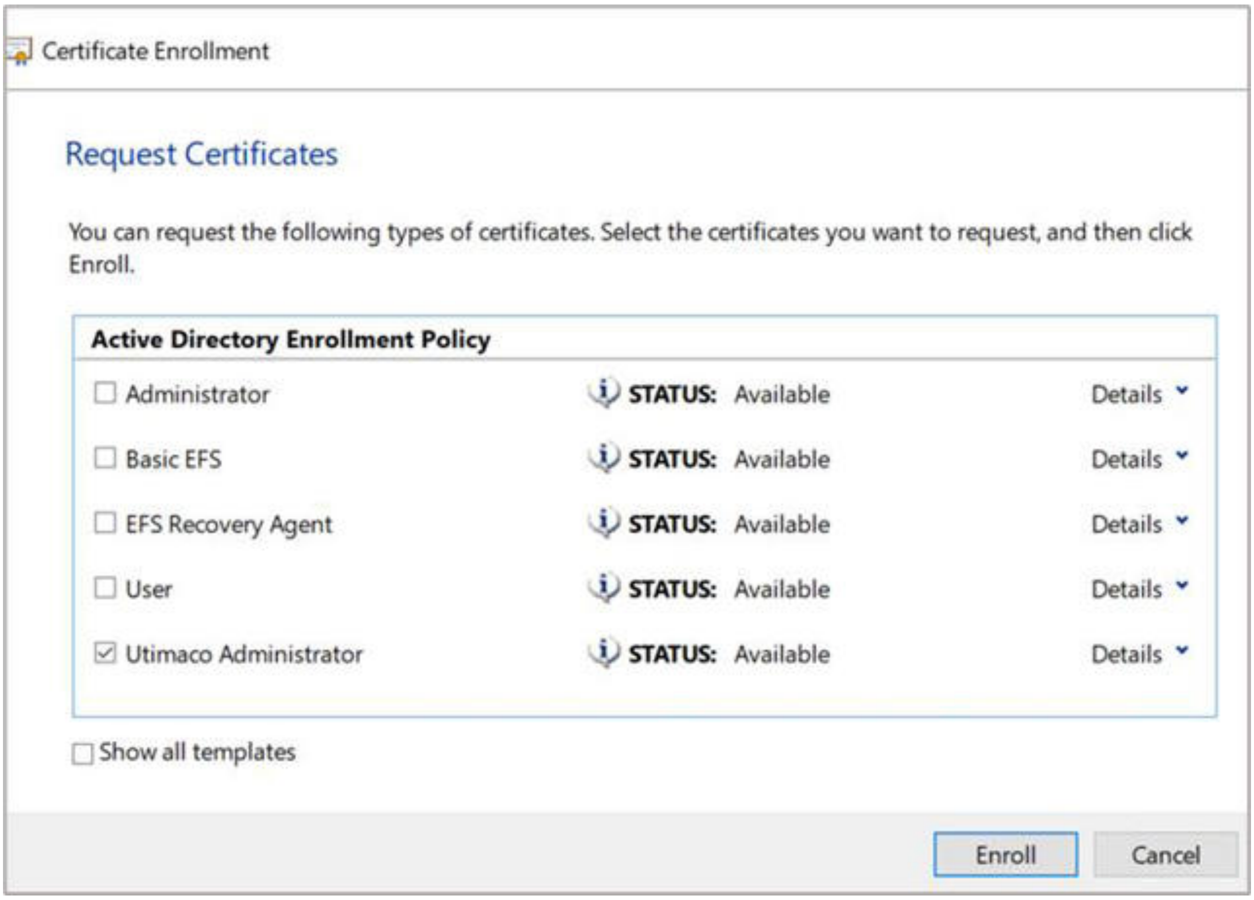

Figure 43 : "Certificate Enrollment" Window

20. The **Certificate Installation Results** window should show STATUS: Succeeded. Select **Finish.**
21. Verify that the certificate is enrolled successfully. If the certificate fails to enroll because the CA is not started or the RPC ports are blocked, the following error is displayed:

```
Error: the RPC server is unavailable. 0x800706ba (win32: 1722
RPC_S_SERVER_UNAVAILABLE
```

The enrollment wizard shows if the certificate enrollment was successful or failed.

Use **Details** to check the main information.

6.1.2 Private Key Archiving and Recovery

6.1.2.1 Archive the CA Key

Archive the CA key to validate that the configurations are possible with the Utimaco HSM and do not interfere with the CA key archival functionality.

To complete archiving the Certificate Authority-Key you must follow the tasks below:

6.1.2.1.1 Archiving the CA Key

1. Log in as a user with Administrative Privileges.
2. The steps to install the Microsoft Active Directory Certificate Services are the same as the Installing Microsoft Active Directory Certificate Services with Windows Enterprise section. After Microsoft ADCS is successfully installed, continue with the steps below.
3. Verify the Certificate Authority is installed successfully.

6.1.2.1.2 Add a Key Recovery Agent (KRA) Template to CA

1. Open the command prompt and run the `certtmpl.msc` command. Right-click on the **Key Recovery Agent** template, then select **Duplicate Template.**

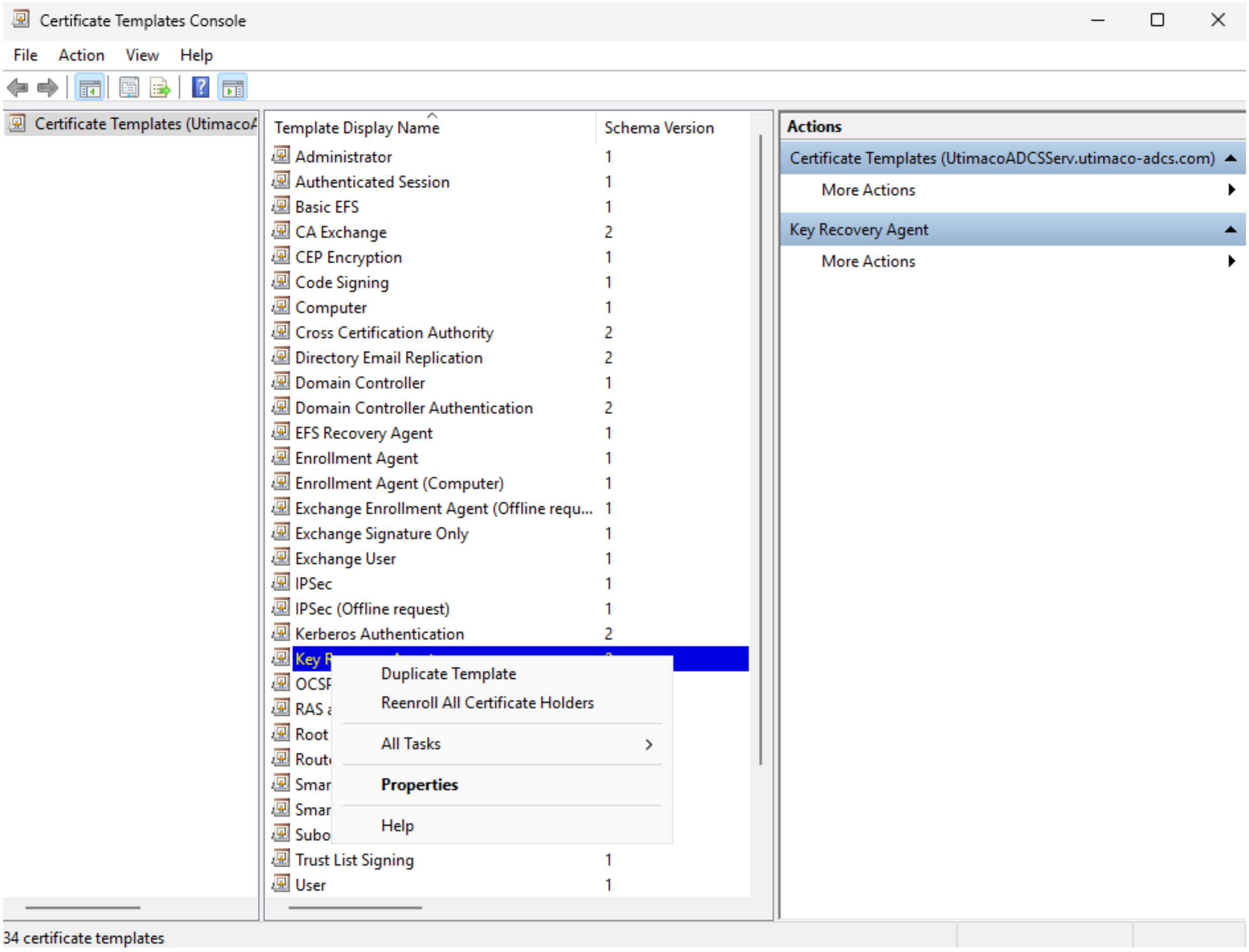

Figure 44 : "Certificate Template" Window

2. The **Properties** window opens, showing the **Compatibility** tab. Select appropriate Windows version under **Certificate Authority** and the **Certificate Recipient** drop-down box.

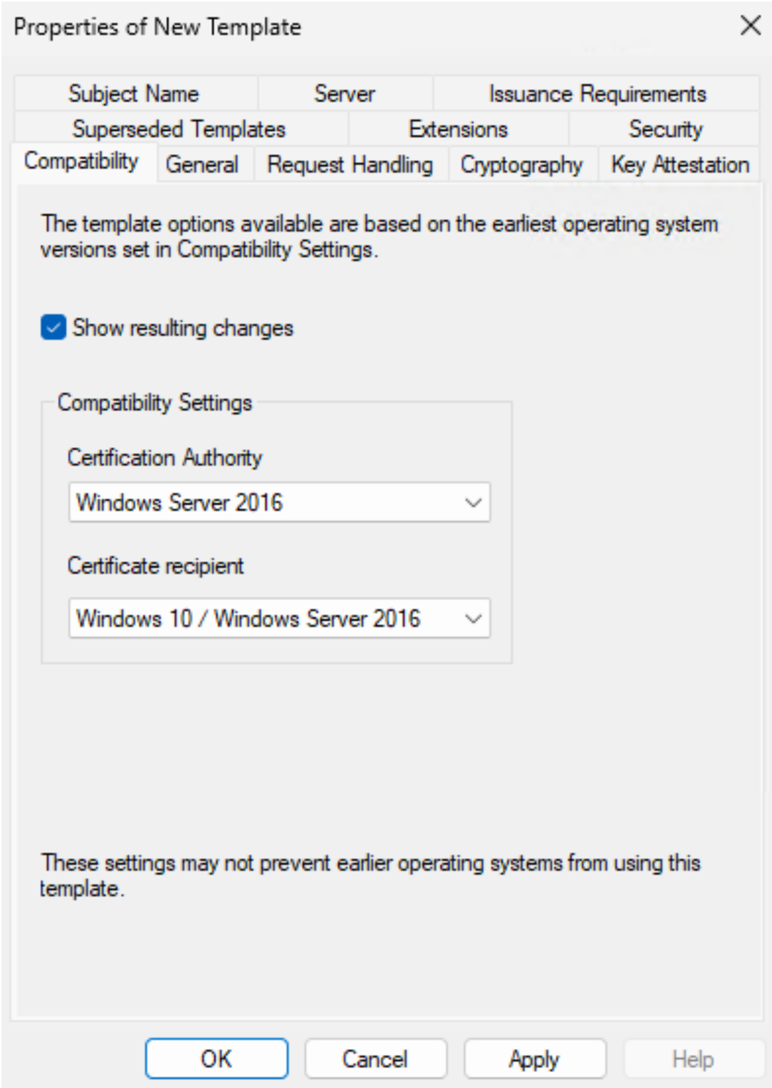

Figure 45 : "Compatibility Tab" Window

3. Select the **General** tab. In **Template display name**, type a name for the template.
4. Select the **Request Handling** tab, and in **Purpose** select **Encryption,** and **Allow private key to be exported** is selected.

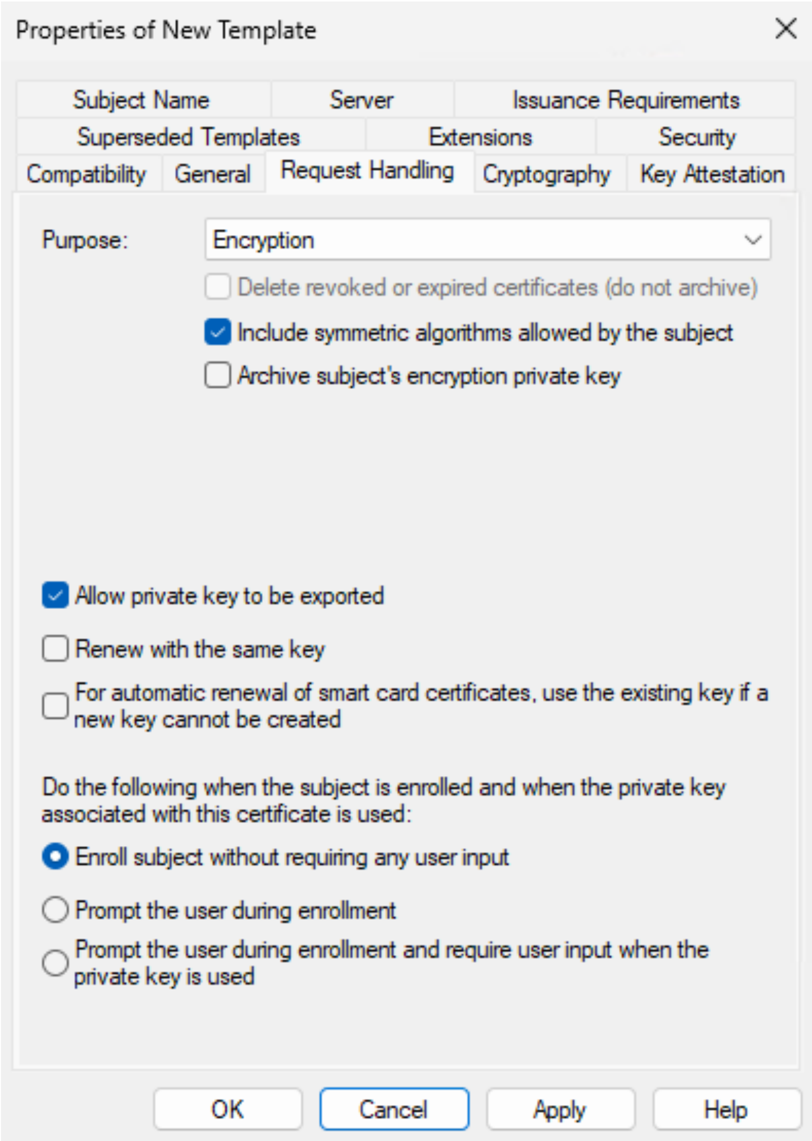

Figure 46 : "Request Handling" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

5. Select the **Issuance Requirement** tab and deselect **CA Certificate manager approval.**
6. Select the **Cryptography** tab, and in the **Provider** category, select **Key storage provider.**
7. In **Algorithm Name**, select the algorithm from the list.

8. Select **Requests must use one of the following providers**, and in **Providers** select **Utimaco CryptoServer Key Storage Provider** only.

> If the CA is on Windows Server Core and you are managing it remotely using certtmpl.msc on a different PC, you need to install the Utimaco CryptoServer Key Storage Provider on the PC that is running certtmpl.msc. Otherwise, the Utimaco CryptoServer provider will not appear.

9. In **Request Hash**, select a hash type.
10. From the **Security** tab, verify if **Domain Admins** and **Enterprise Admins** have **Enroll** Permissions.
11. Select **Apply** and click **OK** to save the template settings and close the **Certificate Template** console.
12. Open the command prompt and run the `certsrv.msc` command.
13. Right-click the **Certificate Templates** node. Select **New,** then select **Certificate Template to Issue.**
14. Select the template created in the above steps and click **OK.**

6.1.2.1.3 Issue the Key Recovery Agent Certificate

1. Open the command prompt and run the `certmgr.msc` command.

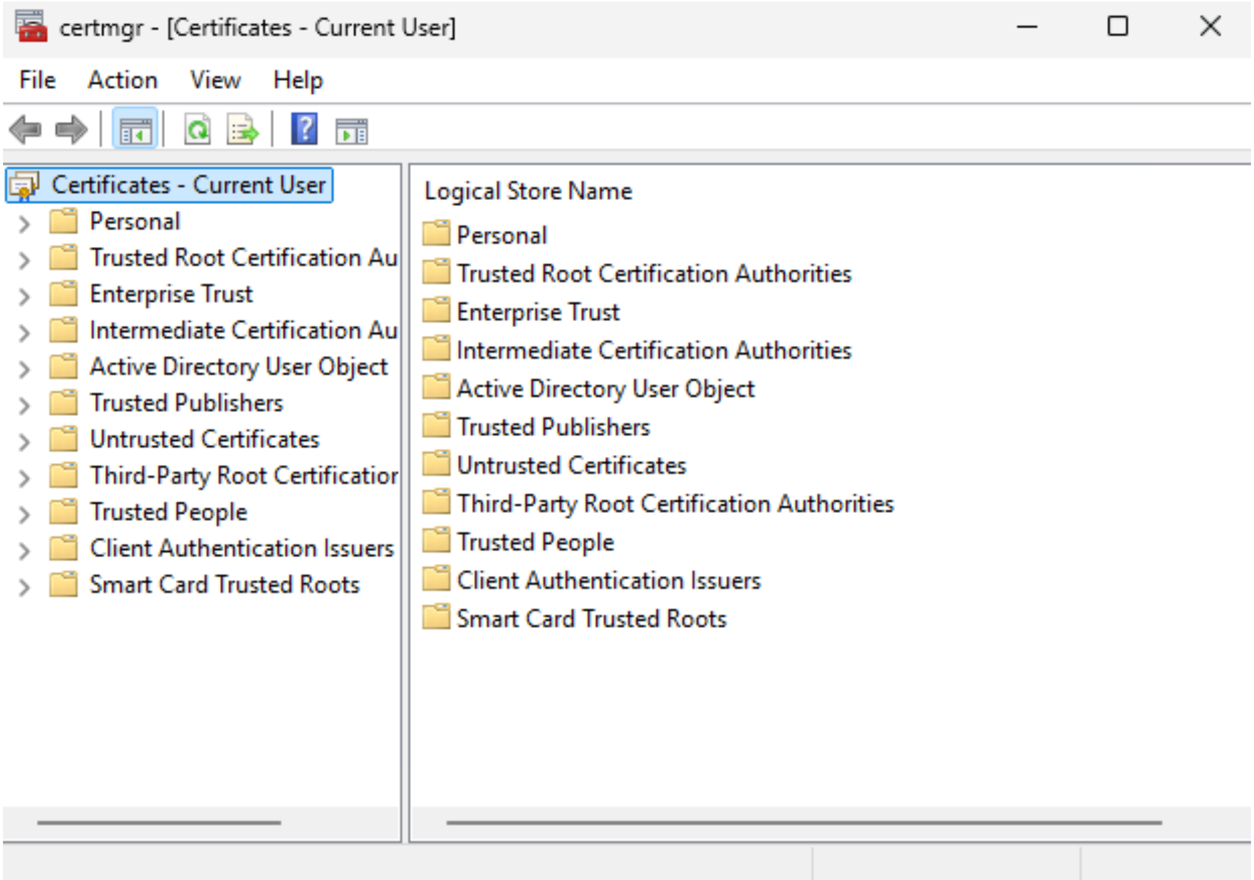

Figure 47 : "Certificate Manager" Window

2. Right-click **Personal** node. Select **All Tasks,** then select **Request new certificate…**

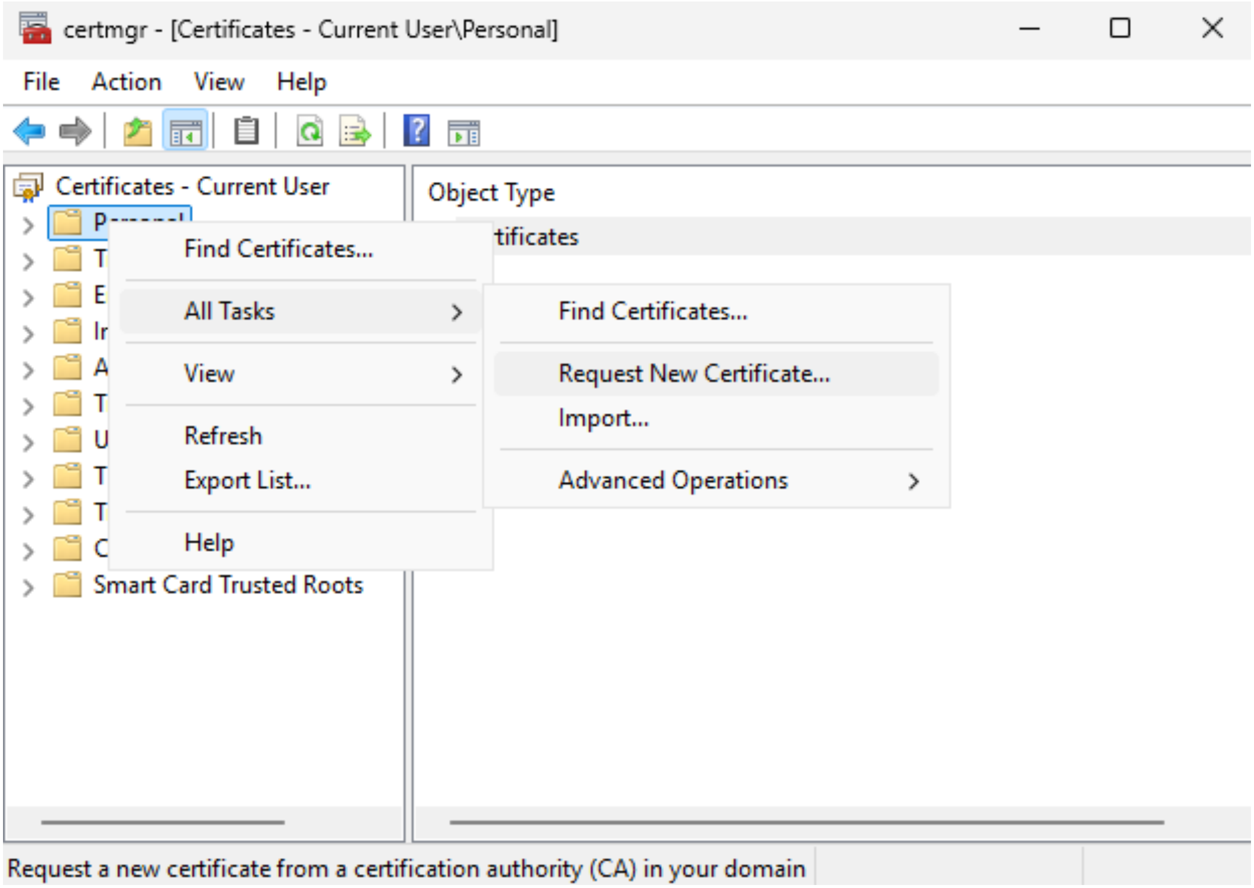

Figure 48 : "Certificate Manager" Window

3. Click **Next.**

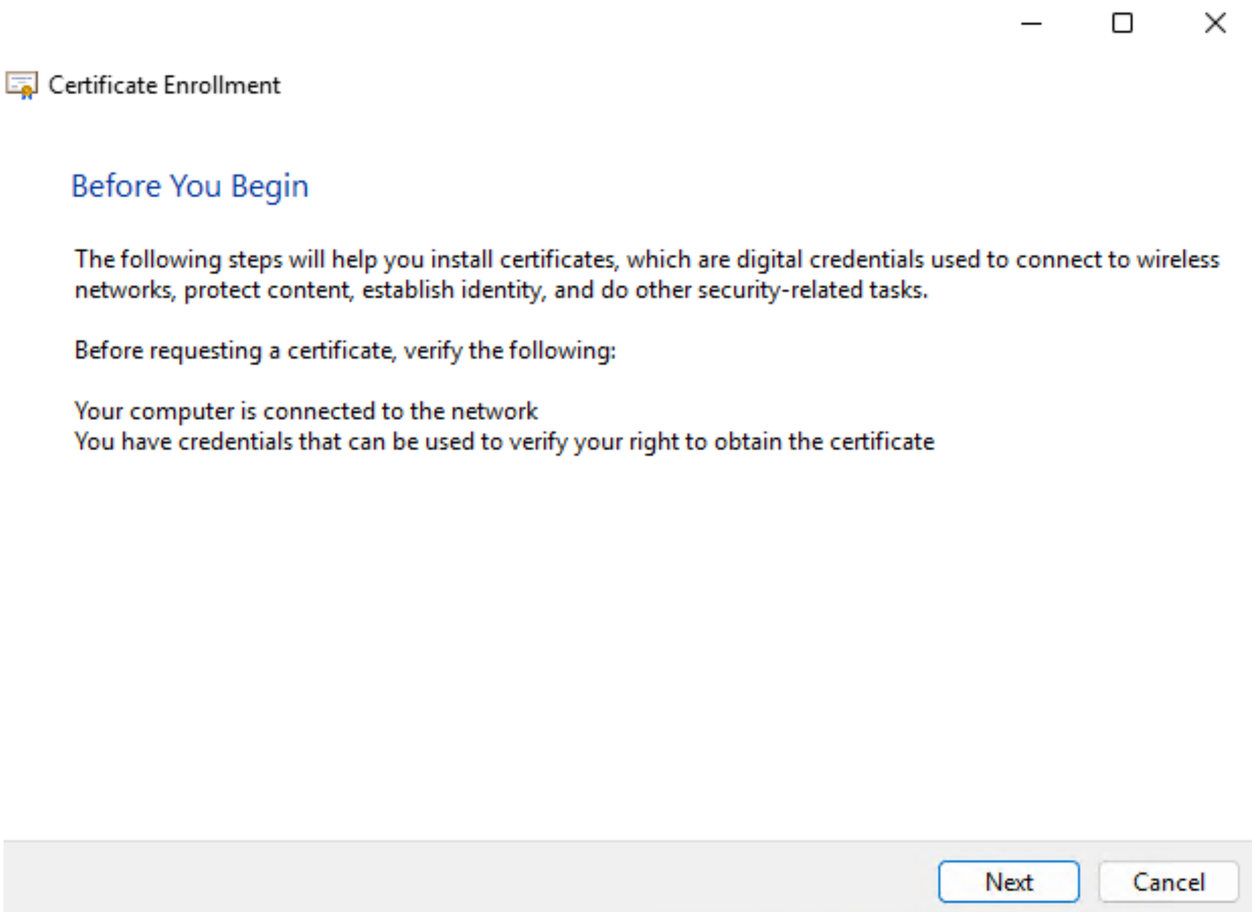

Figure 49 : "Before You Begin" Window

4. Select **Certificate Enrollment Policy** and click **Next.**

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

5. Select the above-created **Key Recovery Agent** checkbox and click **Enroll.**

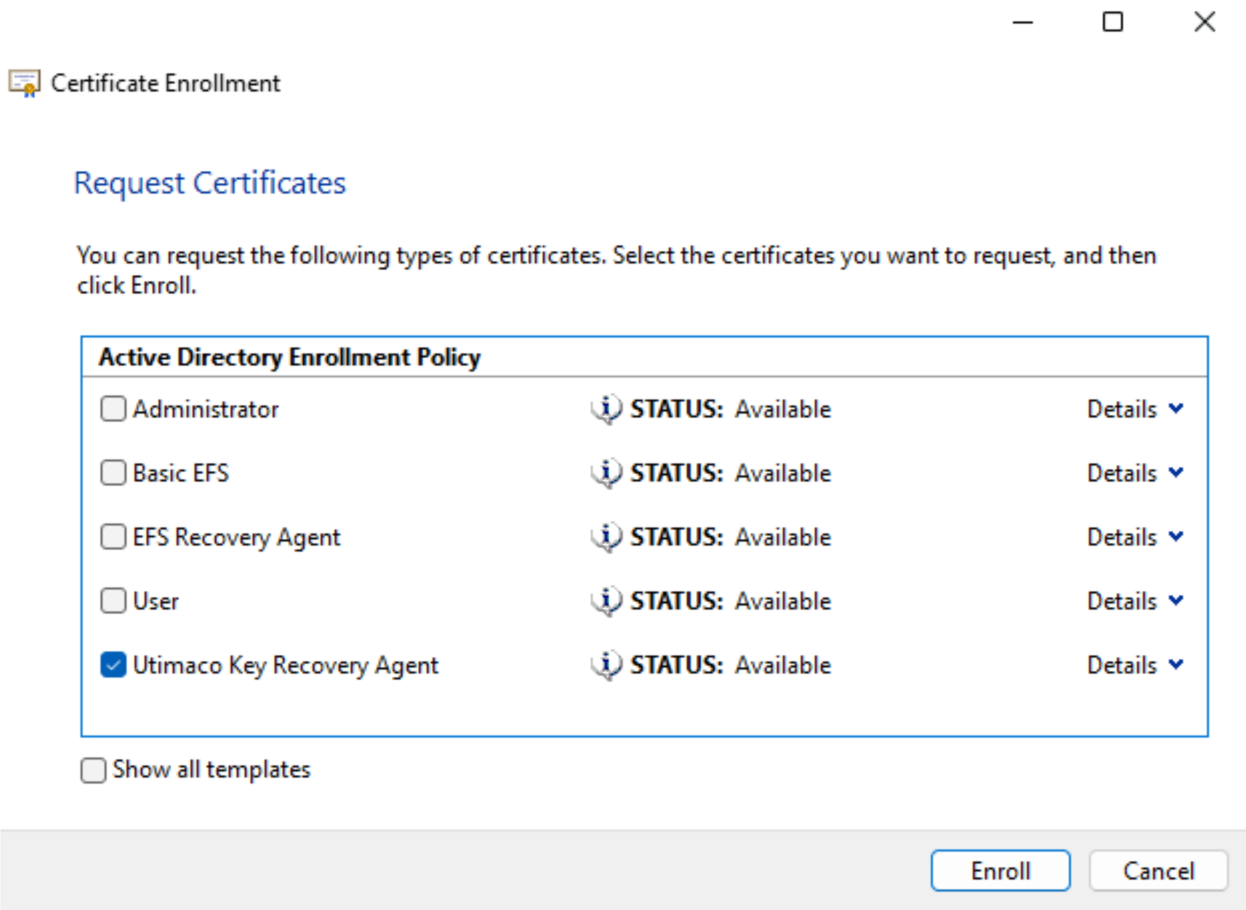

Figure 50 : "Certificate Enrollment" Window

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

6.1.2.1.4 Issue the KRA Certificate

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.**

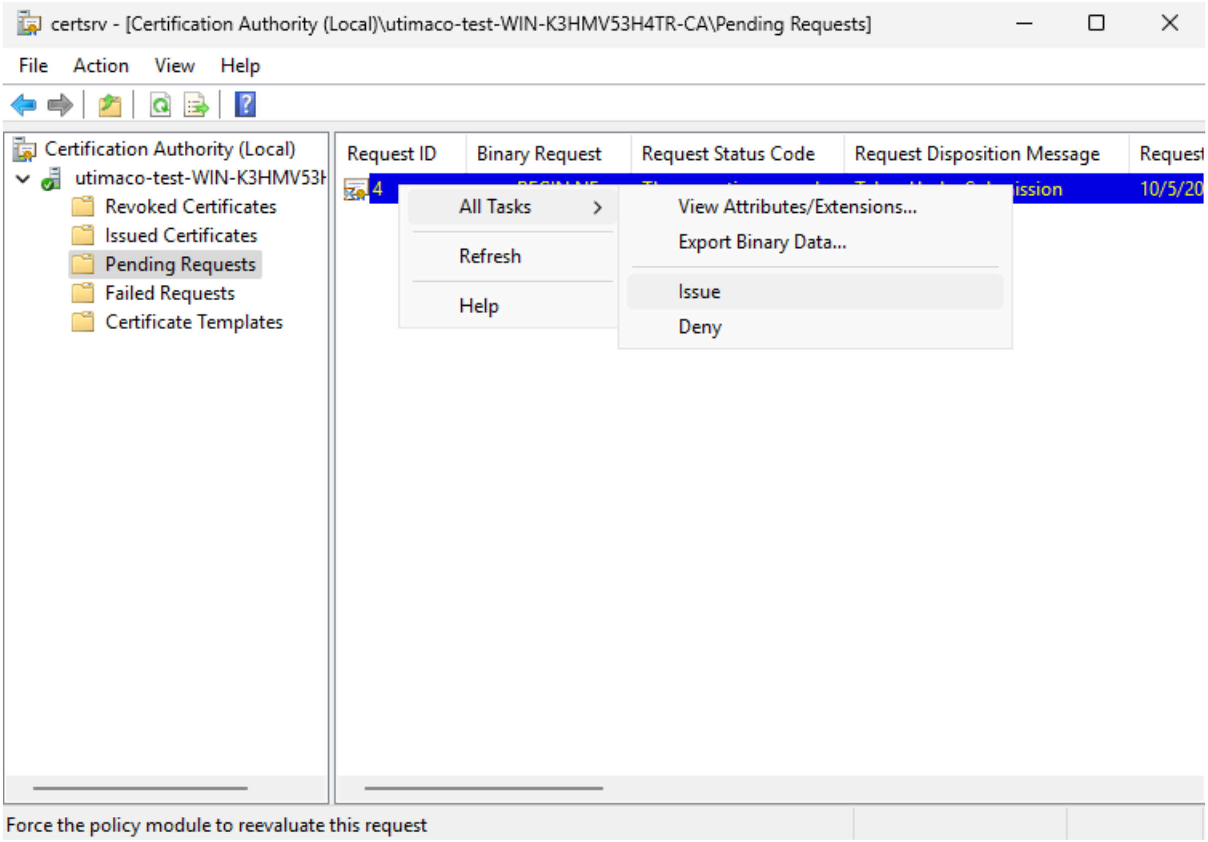

Figure 51 : "Certificate Authority" Window

3. Select the **Issued Certificates.**

4. Verify that the new certificate is issued.

6.1.2.1.5 Retrieve the Issued Certificate from CA

1. Open the command prompt and run `certmgr.msc` command.

2. Right-click on the **Certificates,** then select **Current User.**

3. Select **All Tasks** and select **Automatically Enroll and Retrieve Certificates...** and click **Next.**

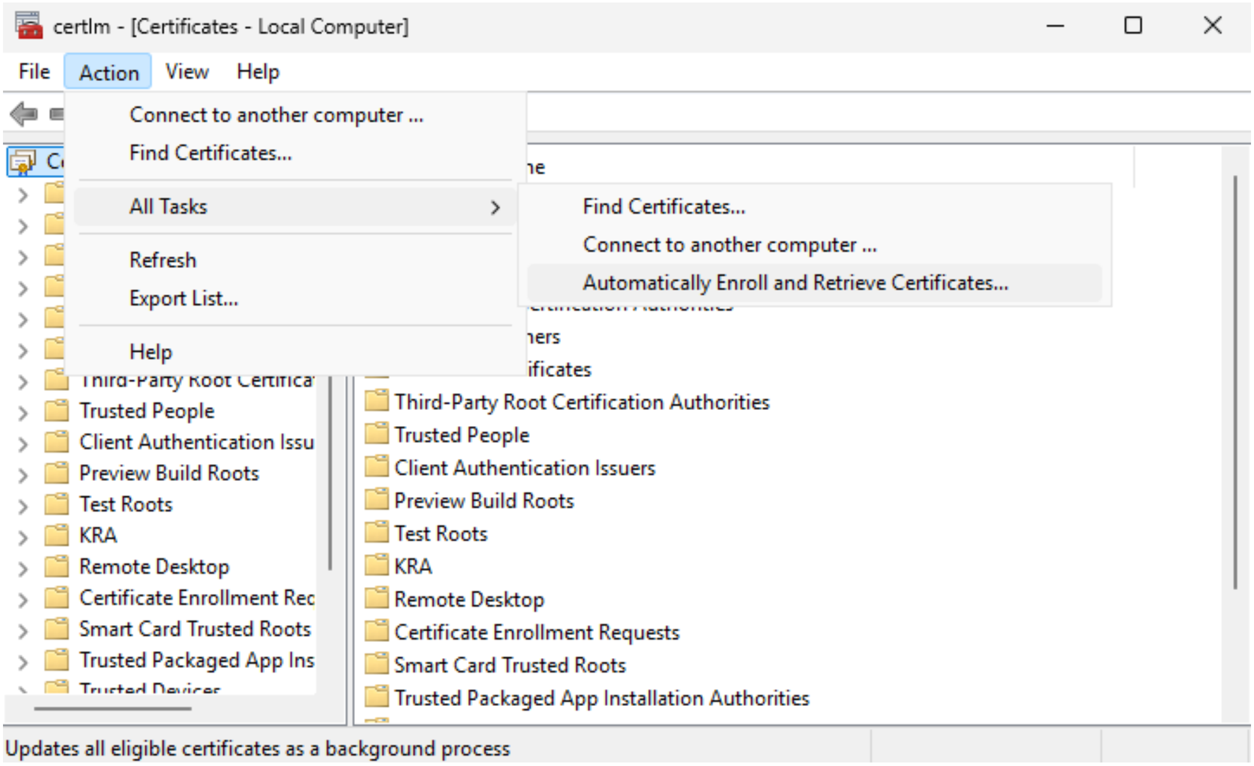

Figure 52 : "Certificate Manager" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

4. Select the KRA certificate you just issued and enroll it.

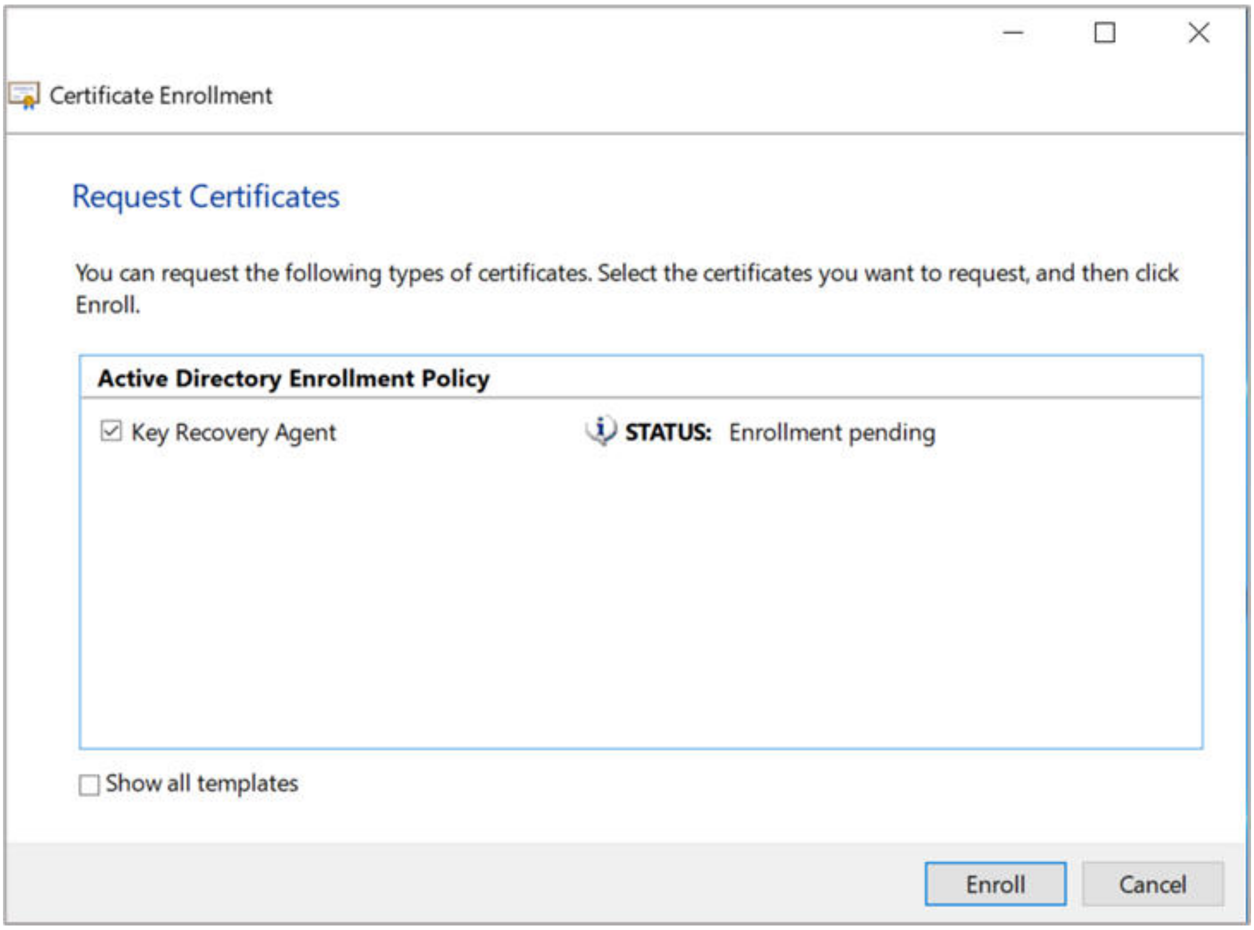

Figure 53 : "Request Certificates" Window

5. Click **Finish.**

6.1.2.1.6 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.

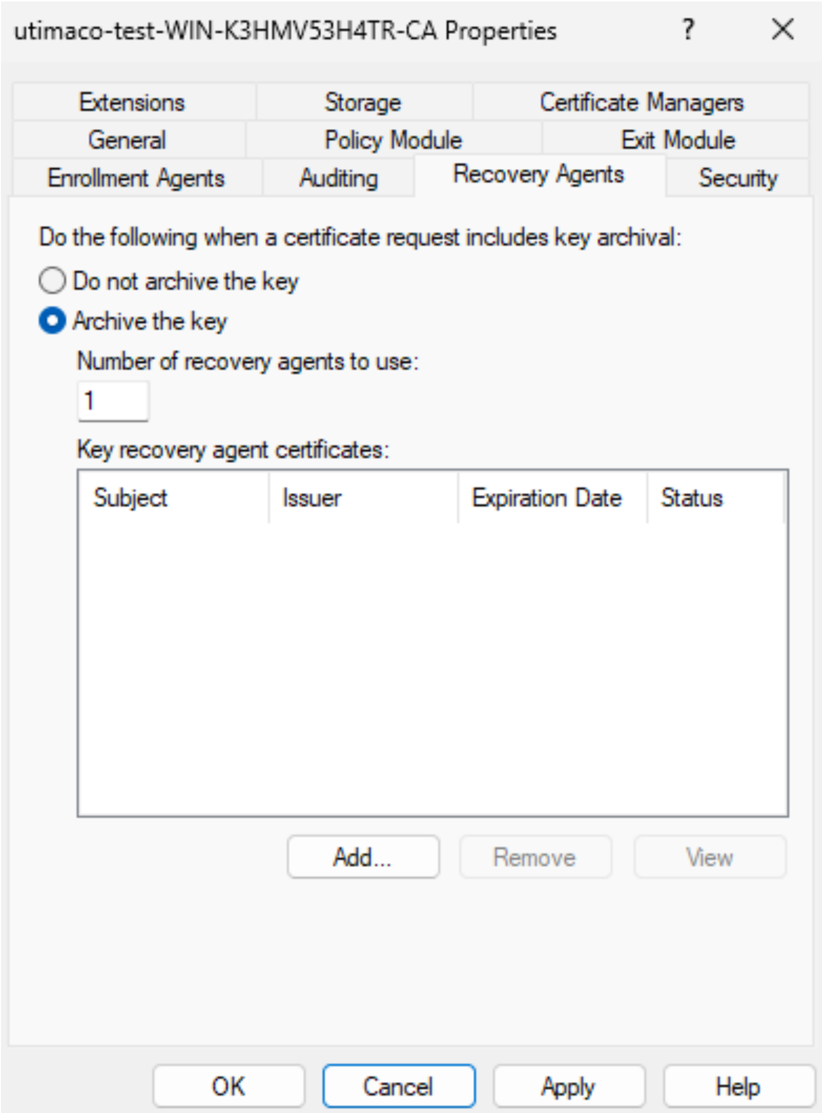

Figure 54 : "Recovery Agents Tab" Window

4. Select the radio button for **Archive the key.**

5. Click **Add.**

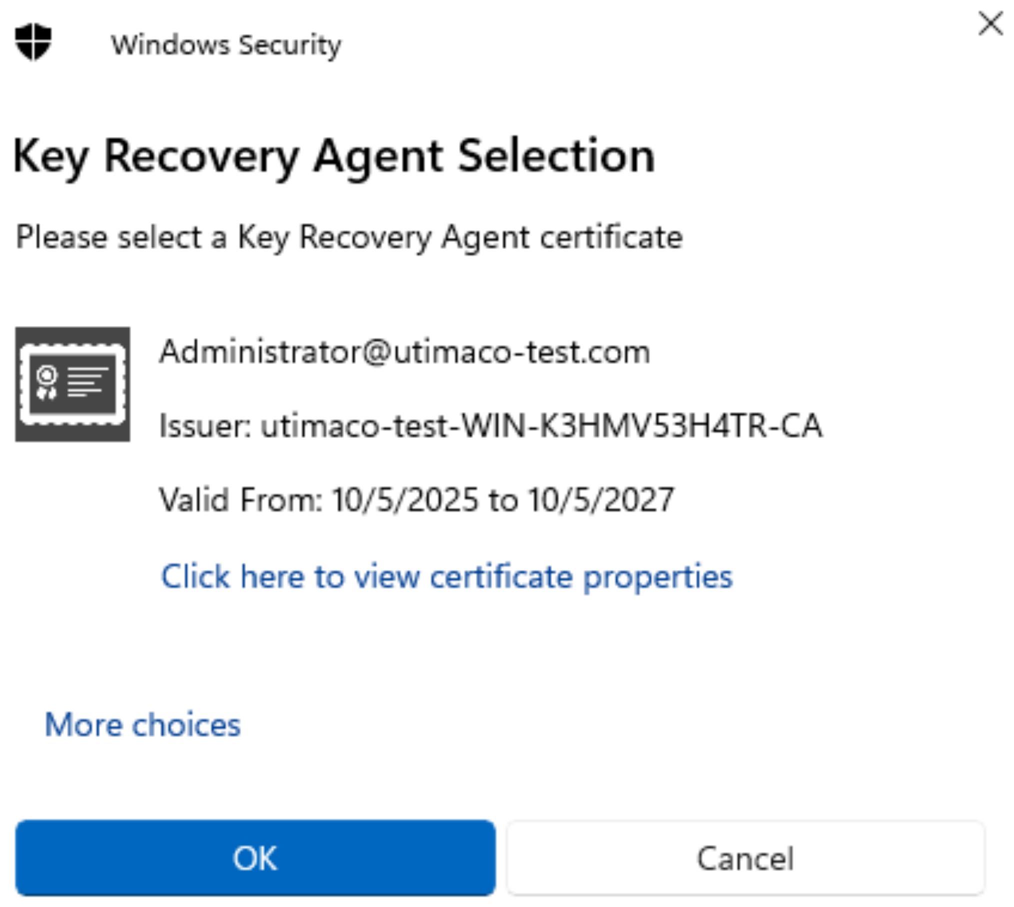

Figure 55 : "Key Recovery Agent Selection" Window

6. Select the KRA certificate you just issued and click **OK.**
7. Click **OK.**
8. Click **Yes** to restart the AD CS.

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.2.1.7 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 select **Duplicate Template.**

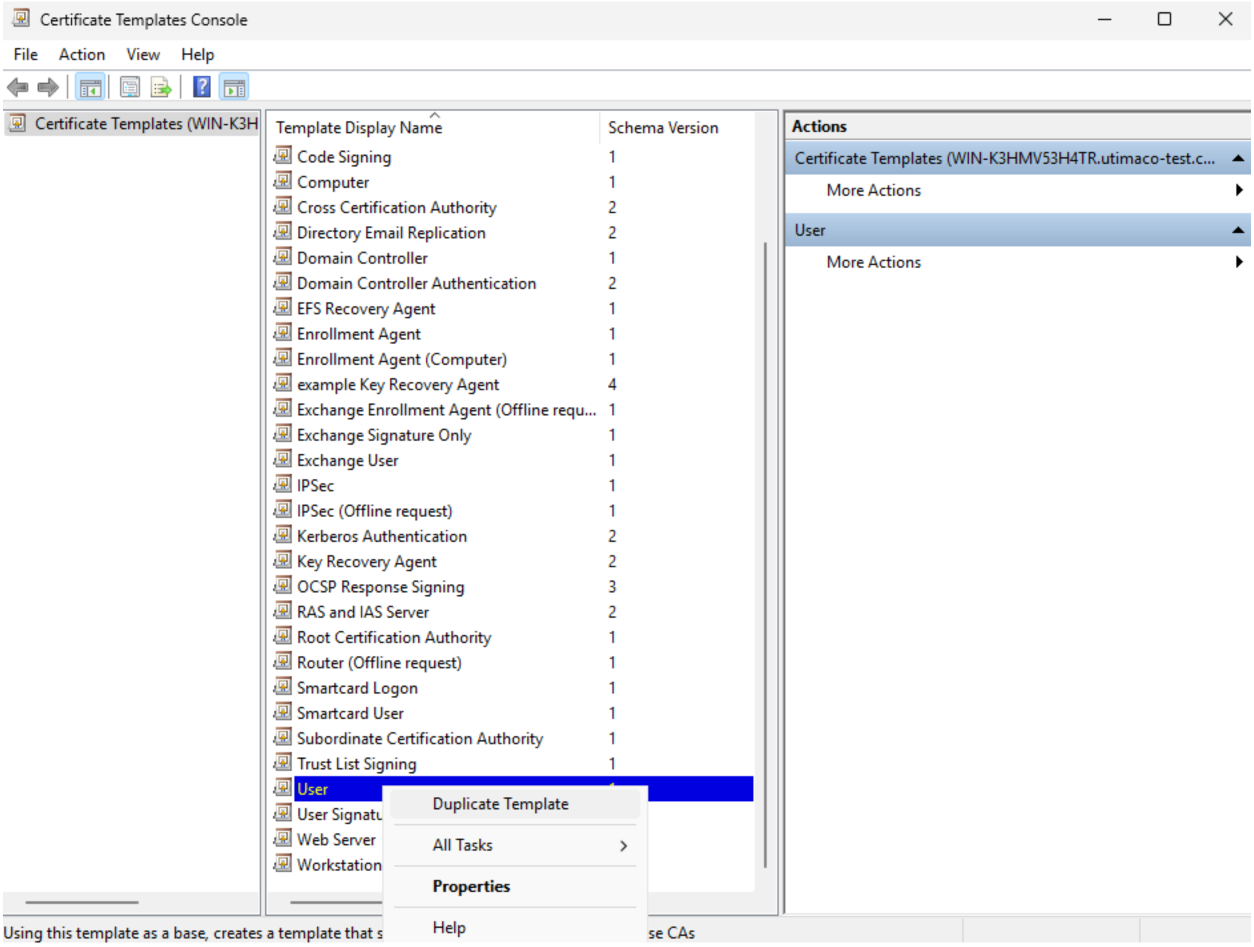

Figure 56 : "Certificate Template" Window

3. Select the appropriate windows version under **Certificate Authority** and **Certificate Recipient** drop-down box under **Compatibility Settings**.
4. Click **OK**.

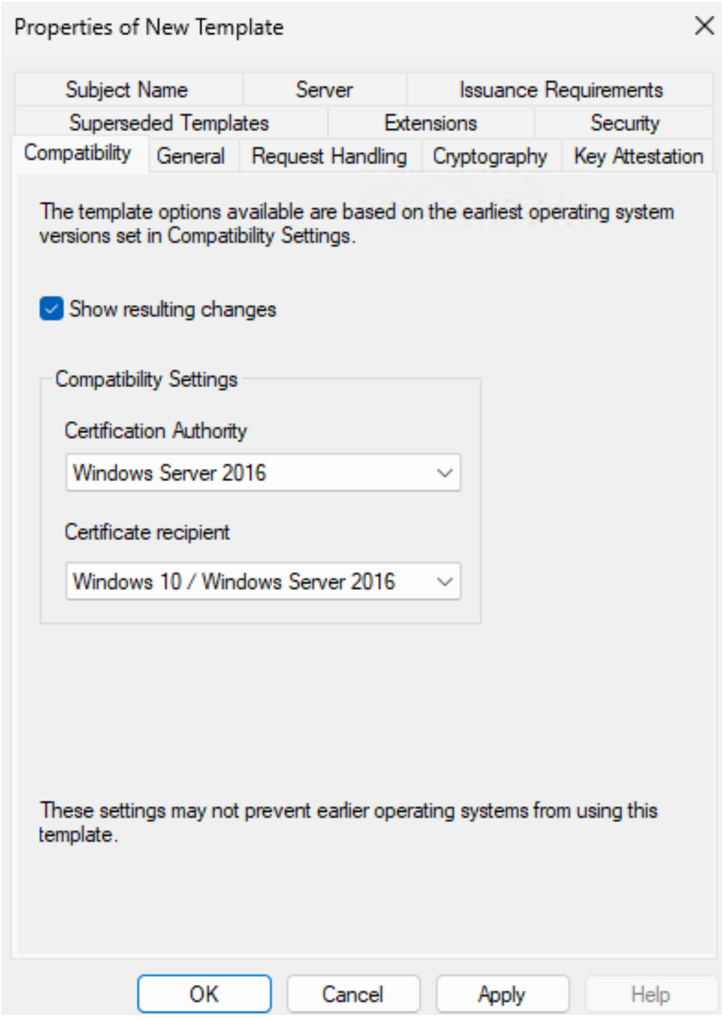

Figure 57 : "Compatibility" Window

5. On the **Resulting Changes** menu, click **OK.**
6. Go to the **General** tab and enter a name for the template (e.g. UserKeyArchival).
7. Go to the **Request Handling** tab and select the checkbox for **Archive Subject's encryption private key.**

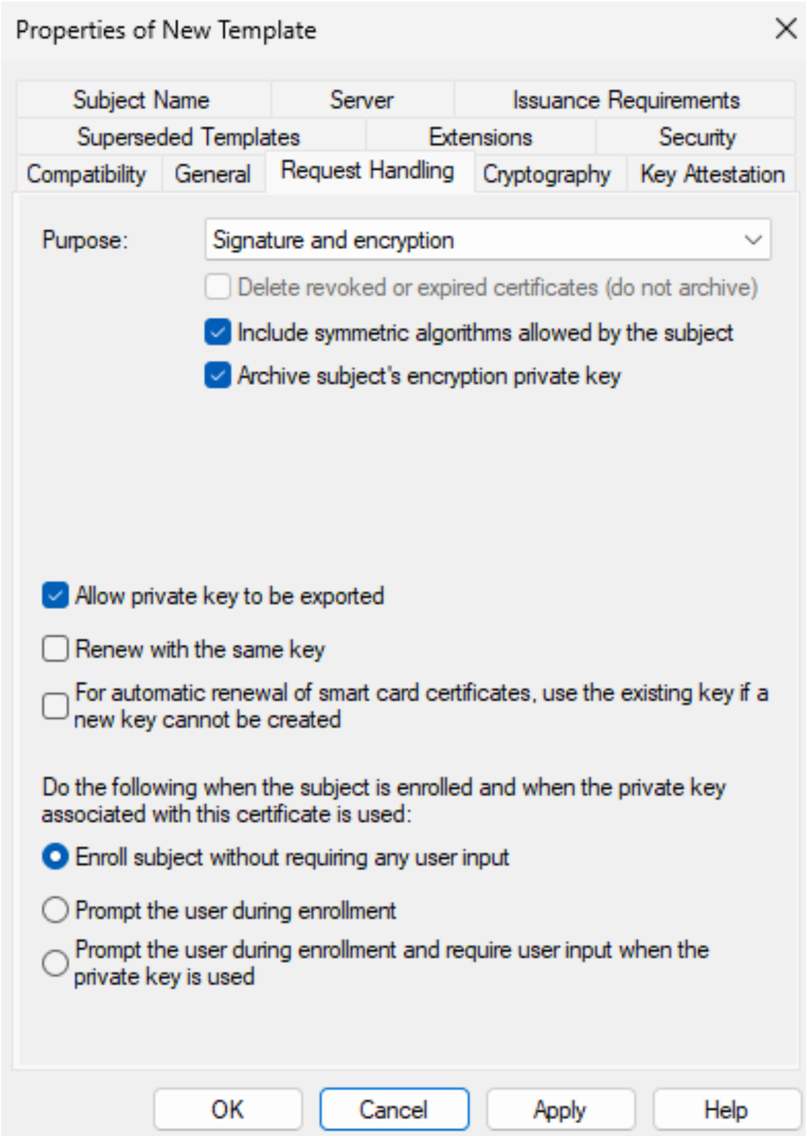

Figure 58 : "Request Handling" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

8. Select the **Subject Name** tab. Uncheck the checkbox for **Include e-mail name in subject name** and uncheck the checkbox for **E-mail name.**

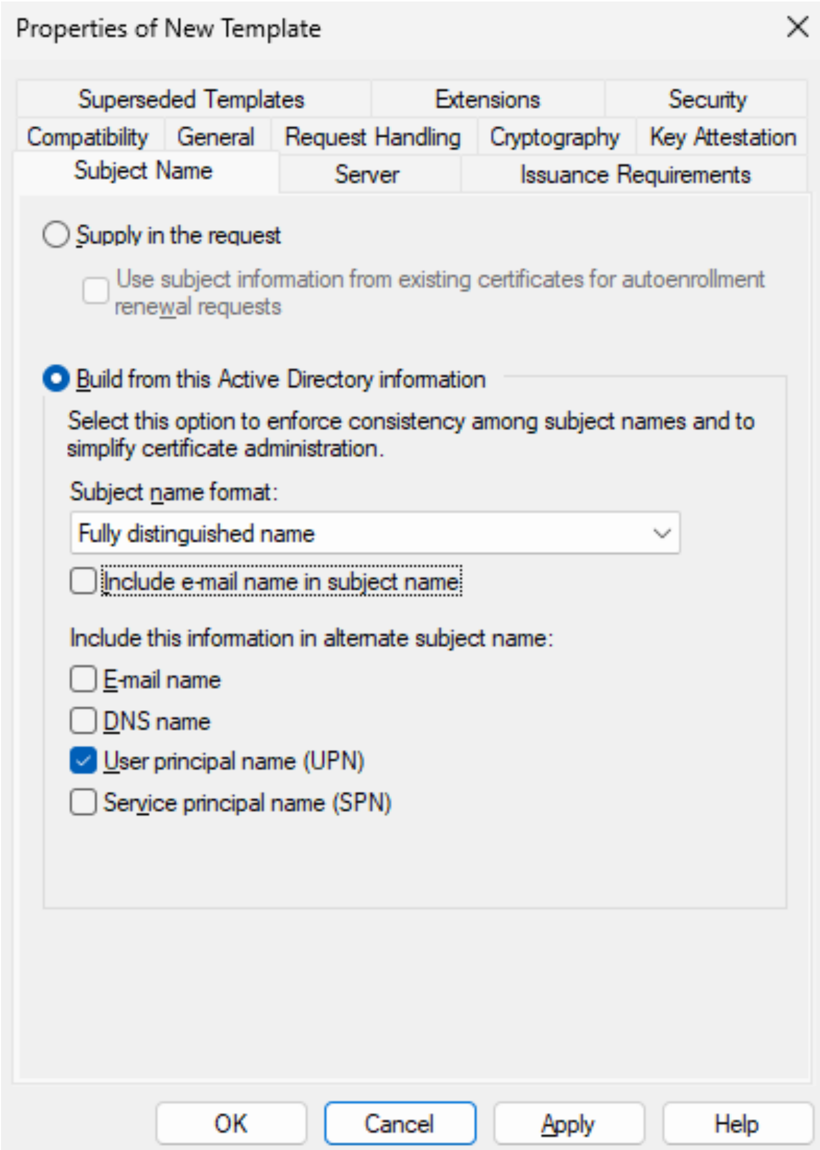

Figure 59 : "Subject Name Tab" Window

9. Click **Apply** and then click **OK.**

6.1.2.1.8 Add a New Template to CA for Issuing

1. Open the command prompt and run the `certsrv.msc` command.
2. Right-click on the **Certificate Templates** node. Select **New** and then select **Certificate Template to Issue.**

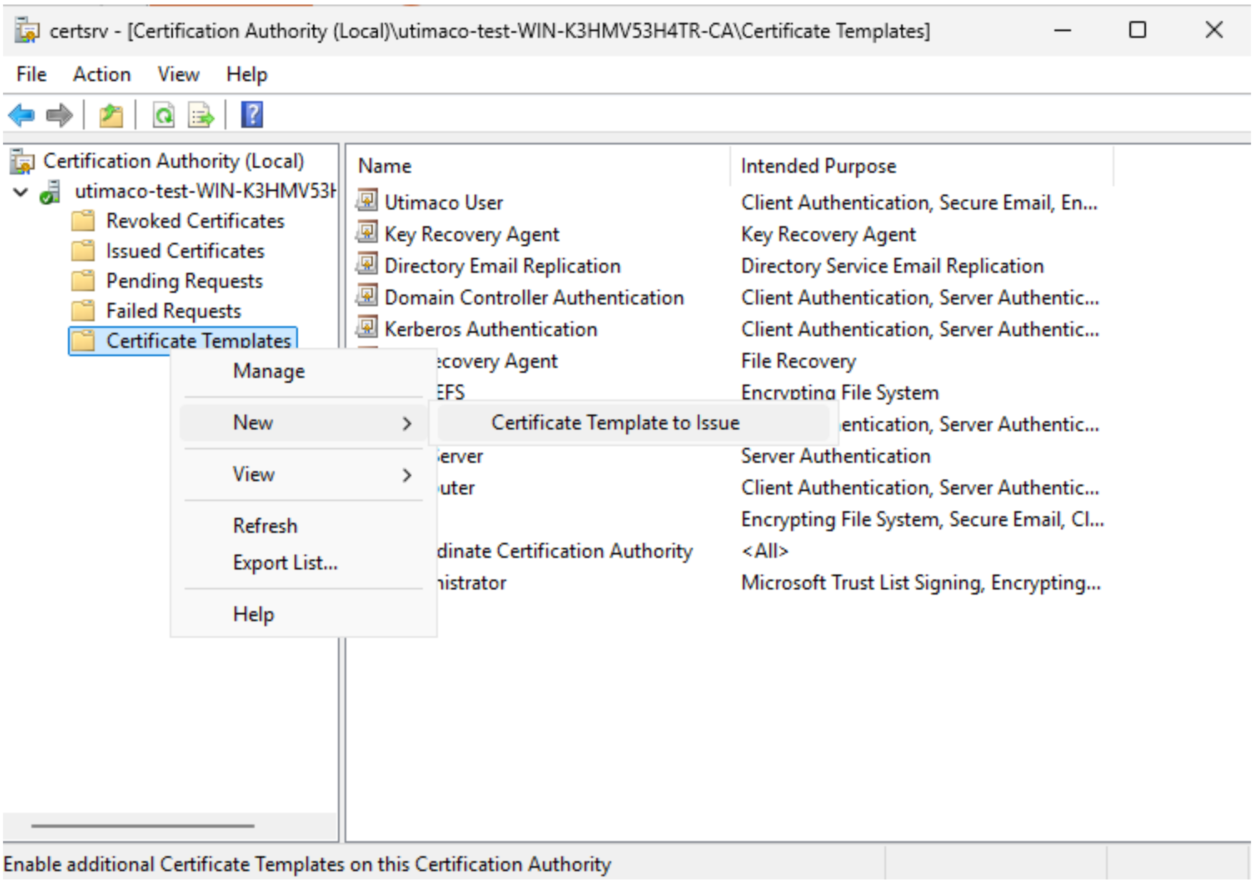

Figure 60 : "Certificate Authority" Window

3. Select **new template for key archival** and click **OK**.

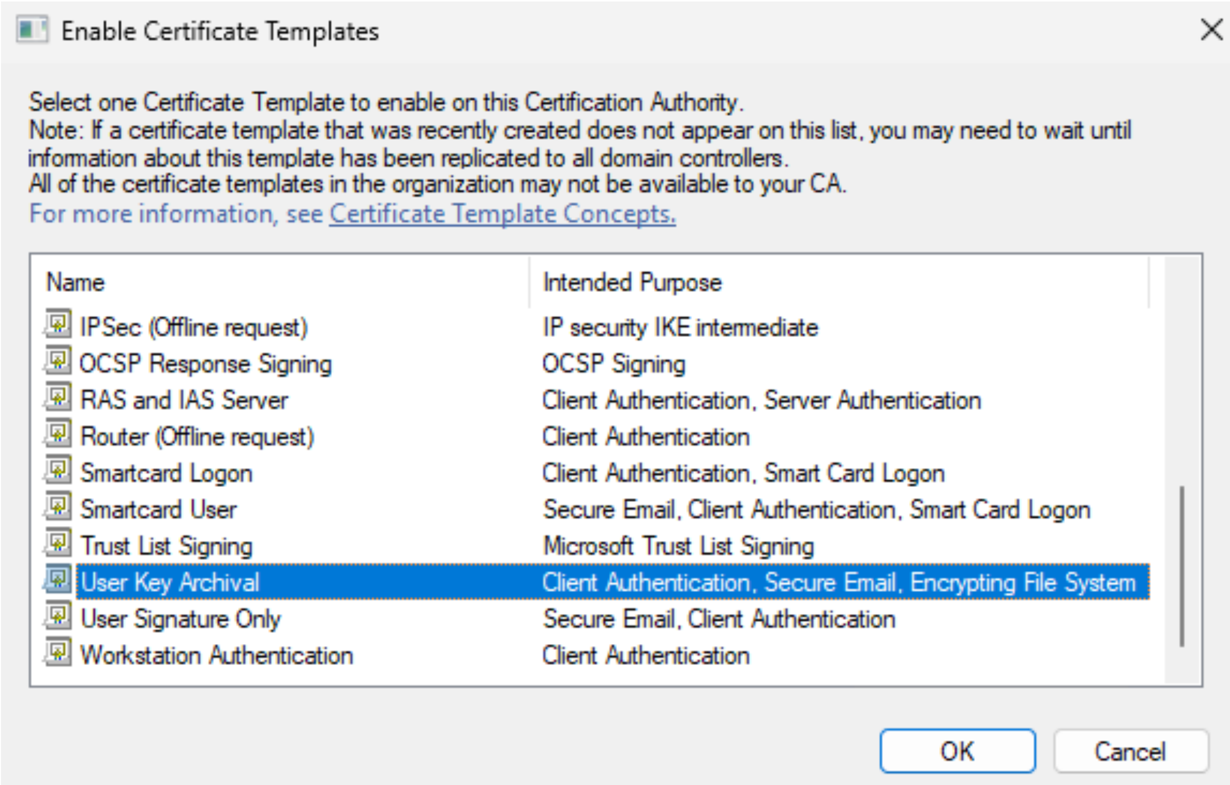

Figure 61 : "Enable Certificate Templates" Window

4. Now the template will be available in the **Certificate Templates** list.

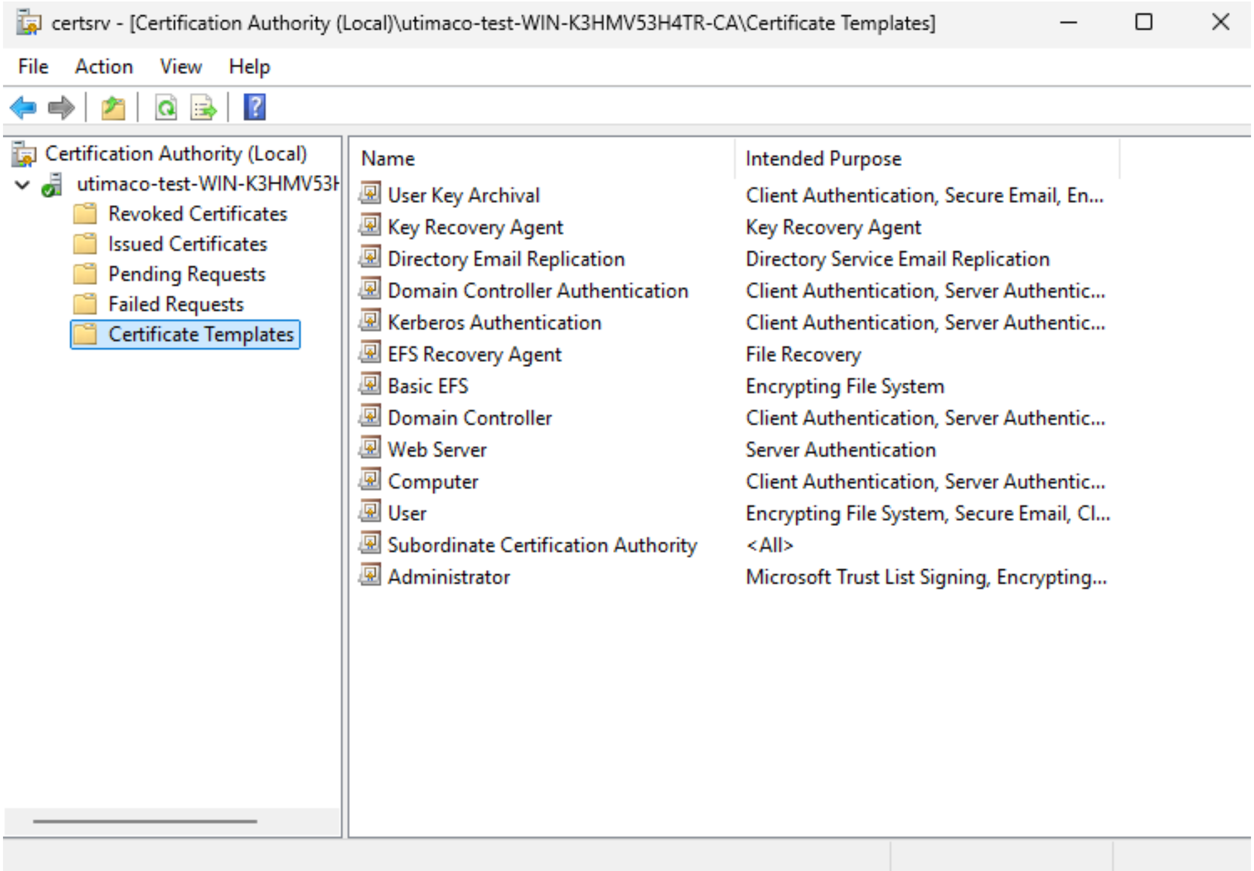

Figure 62 : "Certificate Templates" Window

6.1.2.1.9 Issue a User Template with Key Archival Enabled

1. Open the command prompt and run the `certmgr.msc` command.
2. Right-click **Personal** node. Select **All Tasks** and select **Request New Certificate**. Click **Next** for the next two windows.

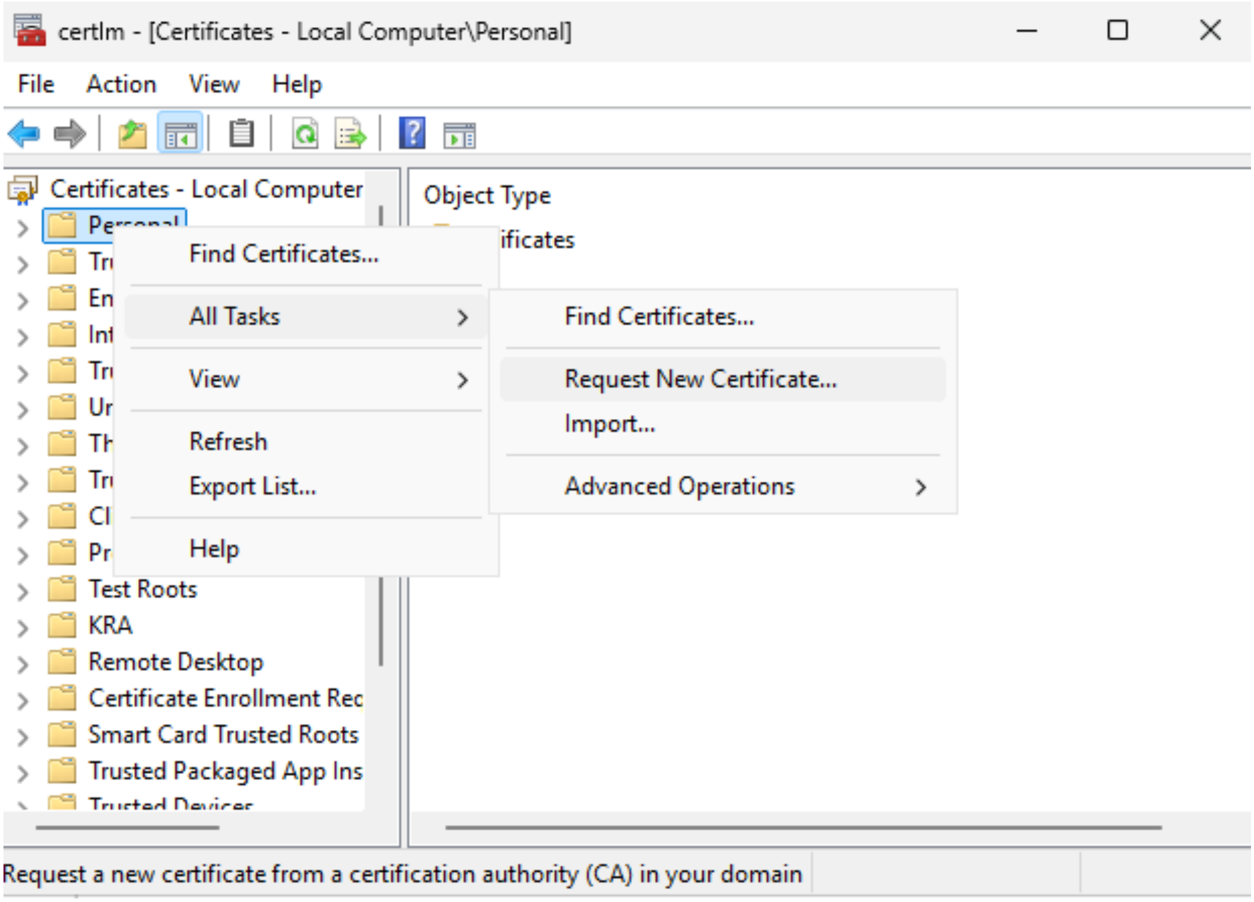

Figure 63 : "Certificate Manager" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

3. Select the checkbox for **New template for key archival** and click **Enroll.**

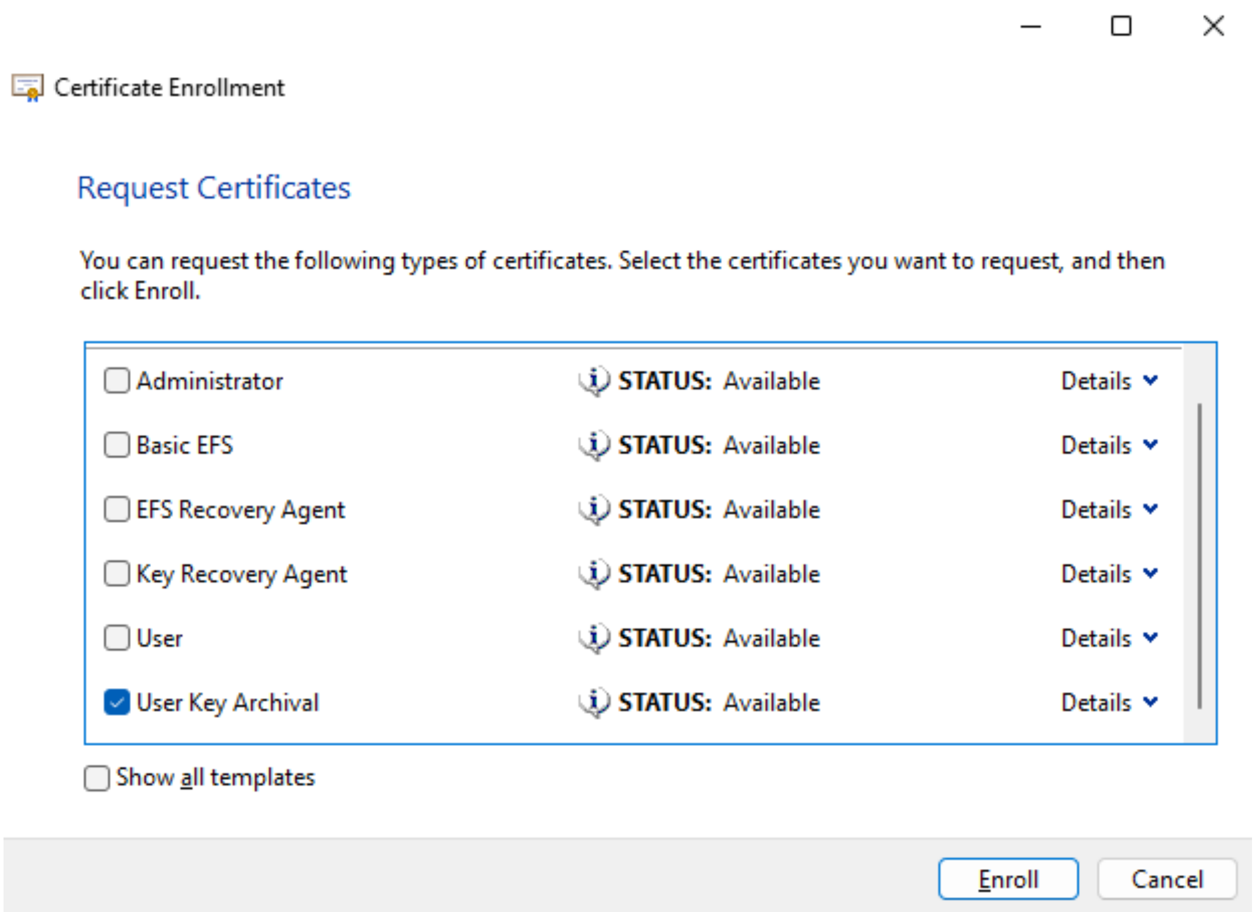

Figure 64 : "Certificate Templates" Window

4. The **Enrollment** Wizard displays. Verify the enrollment is successful and click **Finish.**

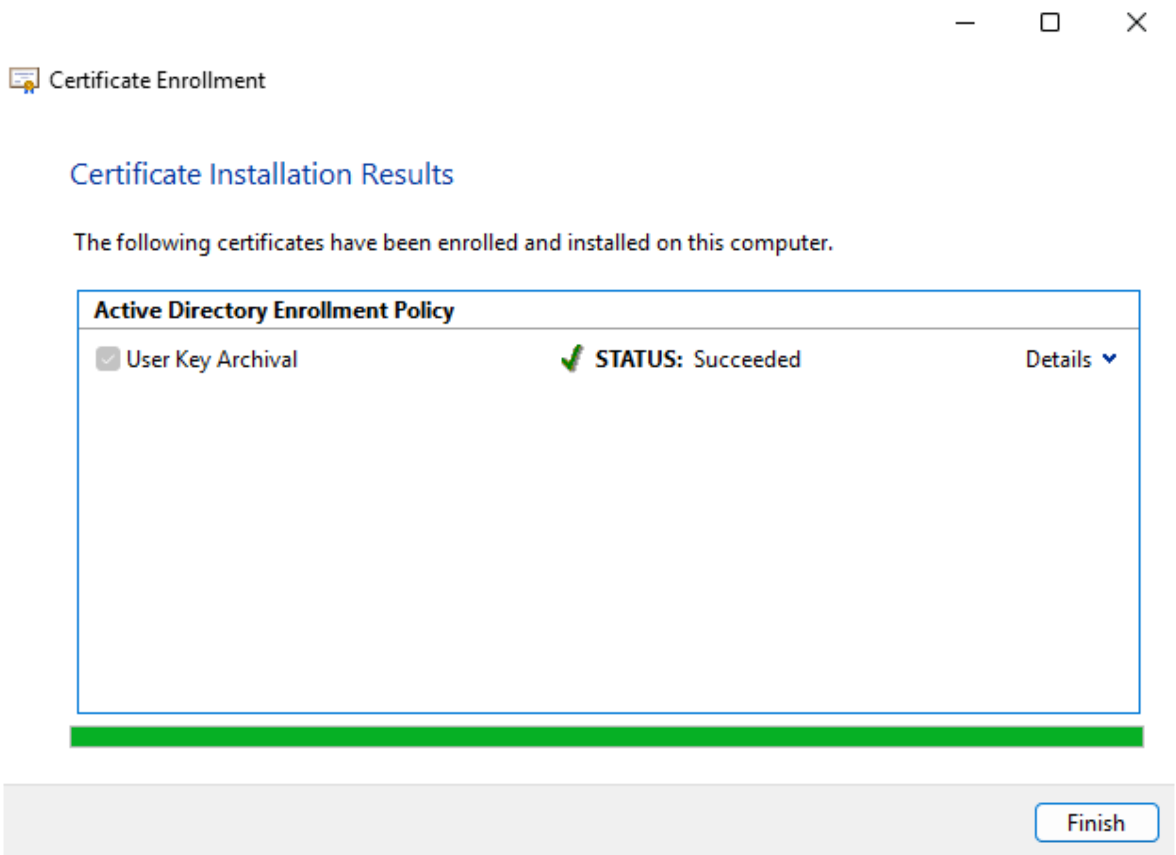

Figure 65 : "Certificate Enrollment" Window

6.1.2.2 Perform Key Recovery

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

1. Open the command prompt and run the `certsrv.ms` c command.
2. In the console tree, double-click **Certificate Authority**, and then click **Issued Certificates.**
3. Select **View** and select **Add/Remove Columns.**
4. In **Add/Remove Columns** within the **Available Column,** select **Archived Key**, and then click **Add**. Archived Key should now appear in **Displayed Columns.**

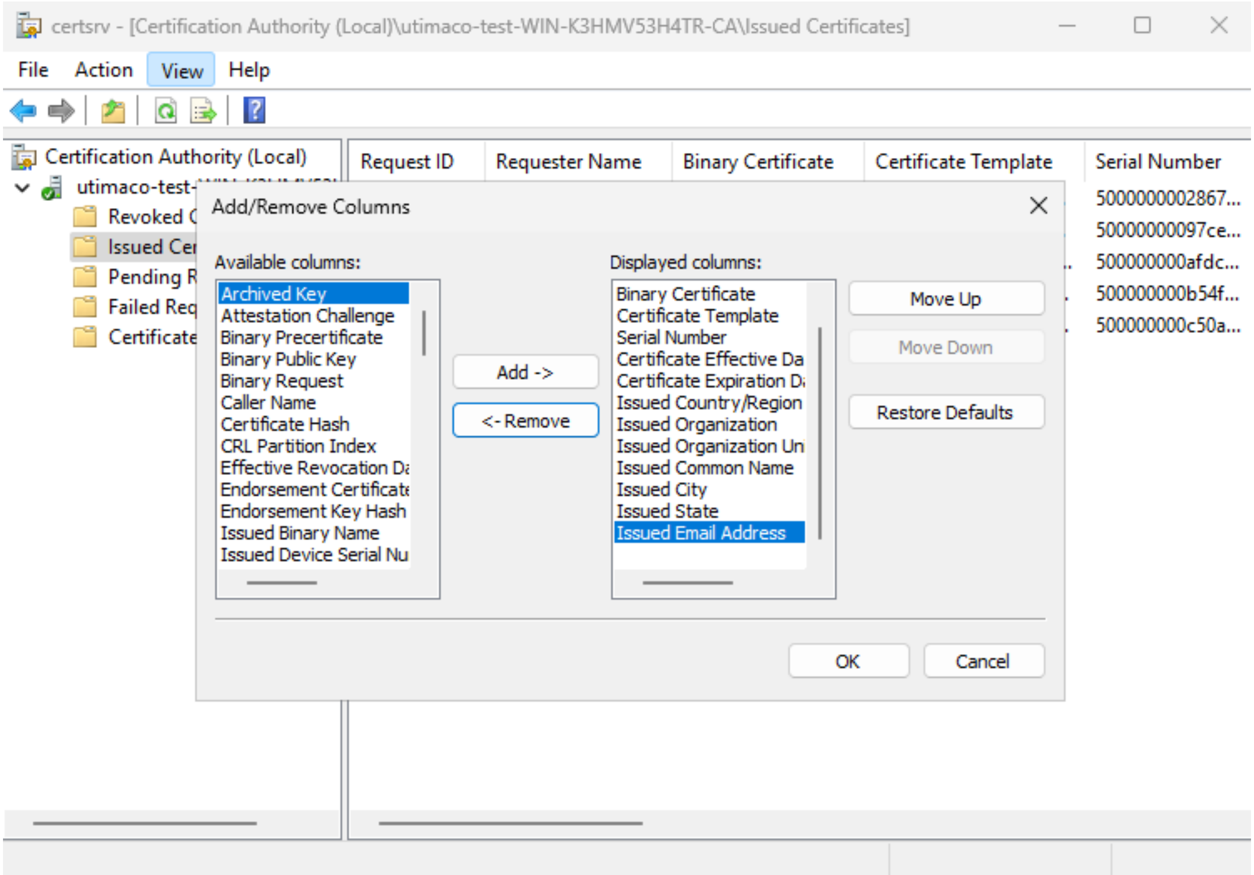

Figure 66 : "Archived Key" Window

5. 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.

> 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.

6. Double-click the **Archive User** certificate.
7. Select the **Details** tab and write down the serial number of the certificate.
8. Click **OK.**
9. Close the **Certification Authority.**

10. Recover the private key into output file, open the command prompt and run the command below.

›_ Console

```
> certutil -getkey <serialnumber> output
```

11. Recover the certificate, open the command prompt, and run the command below.

›_ Console

```
> certutil -recoverkey output user.pfx
```

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

12. When prompted, enter the following information:

    Enter new password: password

    Confirm new password: password

13. Type exit, and then press **ENTER.**
14. Close all windows and log off as the current user.
15. Import the recovered private key/certificate.
    a. Open the command prompt and run the `certmgr.msc` command.
    b. Right-click **Certificates** (Current User), and then select **Find Certificates.**
    c. In **Find Certificates**, under **Contain,** type the 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.**

16. 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 select **All Tasks,** and then click **Import.**
   b. In the **Certificate Import** Wizard, click **Next.**
   c. In the **Files to Import**, in the **File name** box, type `c:\user.pfx` and then click **Next.**
   d. In **Password**, type the password and then click **Next.**
   e. In **Certificate Store**, select **Automatically select the certificate store based on the type of certificate,** and then click **Next.**
   f. In the **Completing the Certificate Import** Wizard, click **Finish.**

17. Verify the serial number of the imported certificate.
   a. In the console tree, double-click **Personal** and then click **Certificates.**
   b. Double-click the certificate.
   c. In **Certificate**, go to the **Details** tab. Verify that the serial number matches the original.

6.1.3 Migrating the Microsoft Software Key of AD CS to Utimaco HSM

6.1.3.1 Installing AD CS with Locally Stored Primary Key

1. Join a machine to the Domain and log in as a user with Administrative privileges.
2. Select **Start** and select **Server Manager** to open **Server Manager**. Select **Manage**, then select **Add Roles & Features.**

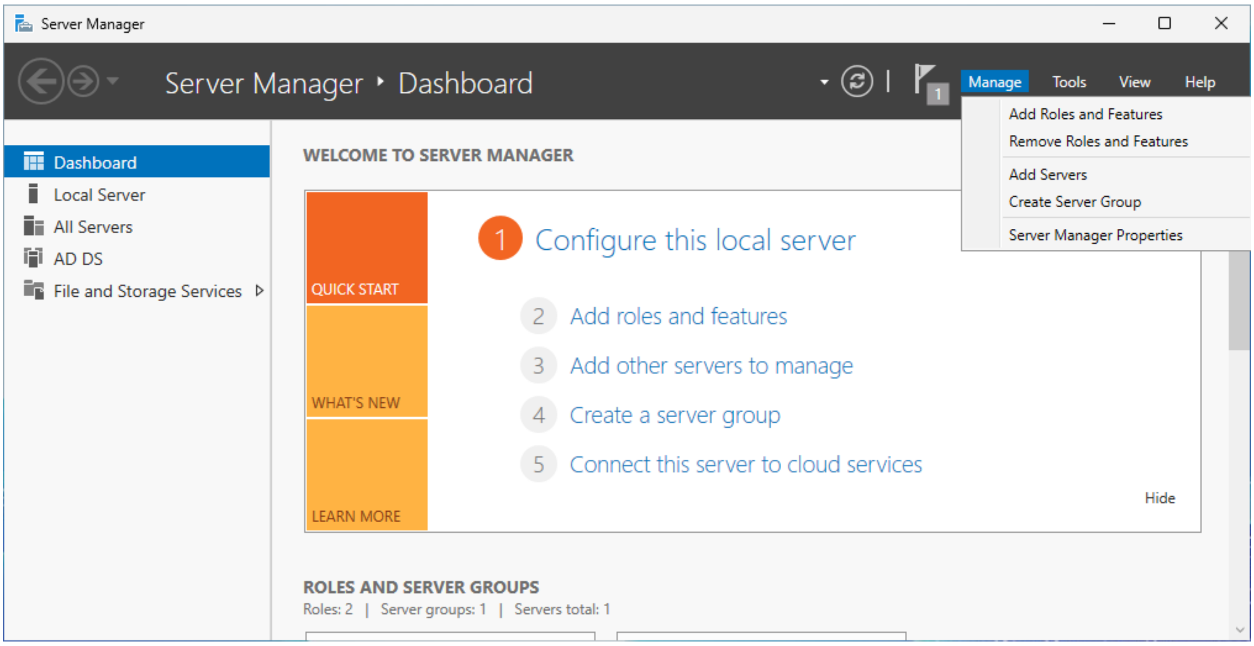

Figure 67 : "Server Manager" Window

3. The **Before you begin** window opens. Select **Next.**

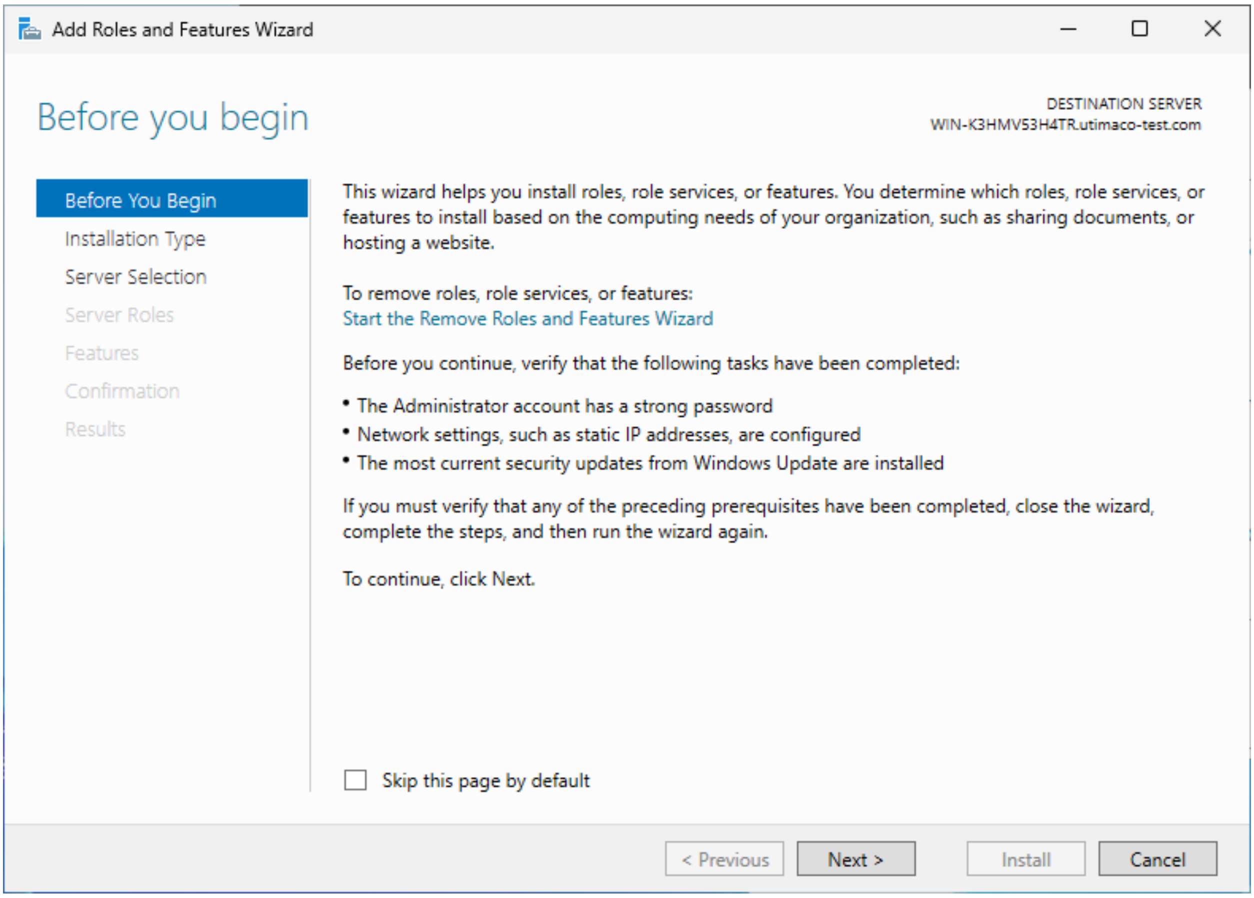

Figure 68 : "Before You Begin" Window

4. On the **Select installation type** window, make sure the default **Role or Feature Based Installation** is selected. Click **Next.**

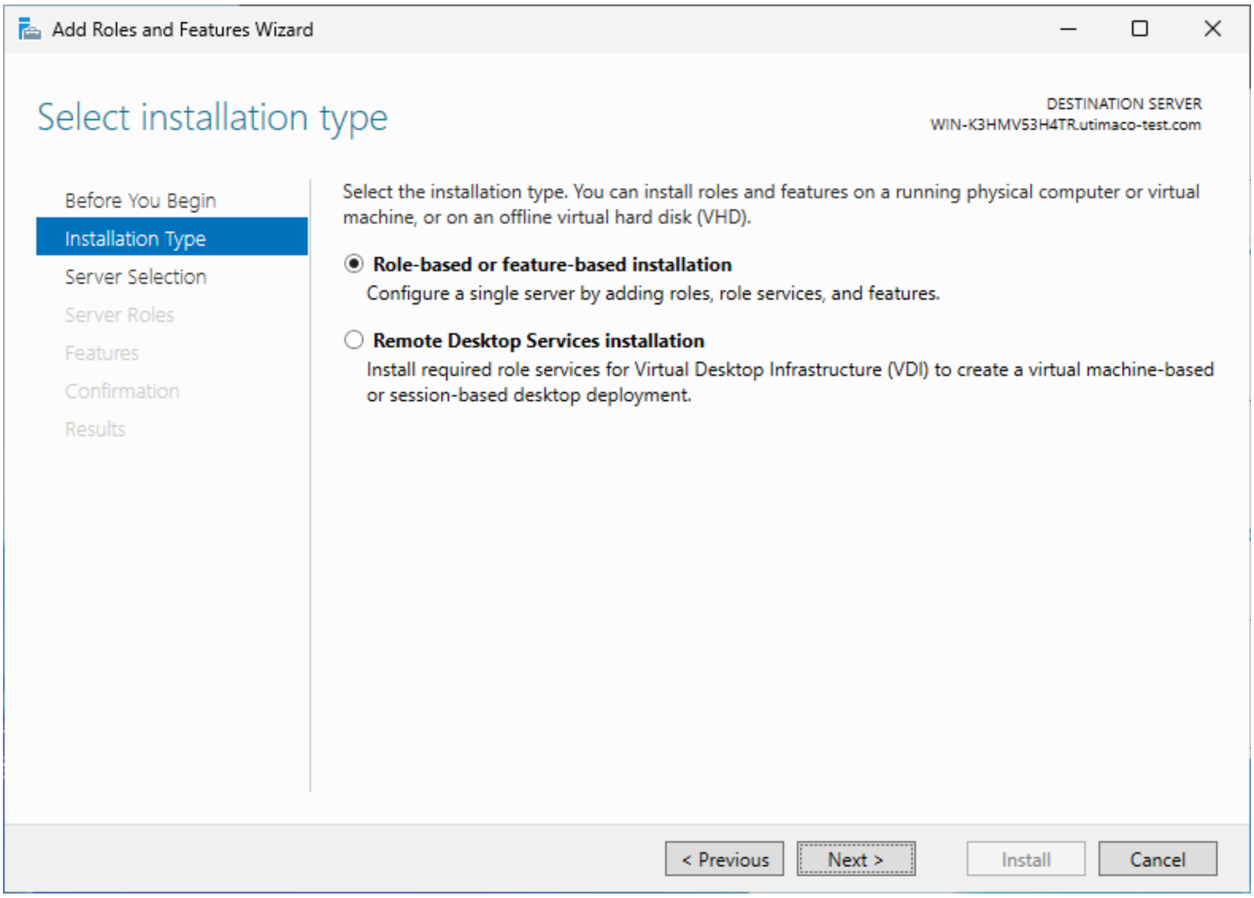

Figure 69 : "Select Installation Type" Window

5. On **Server selection**, select a server from the server pool. Click **Next.**

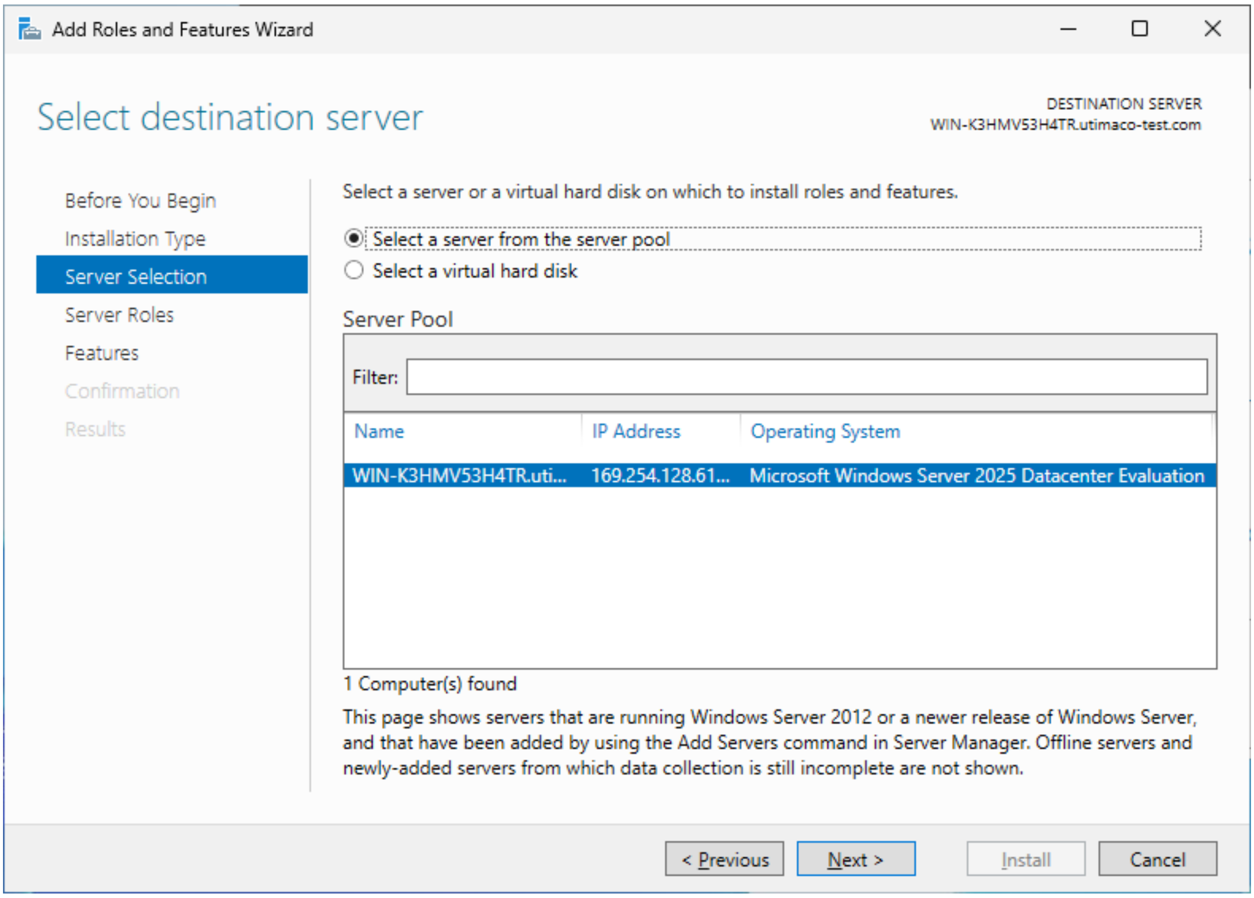

Figure 70 : "Select Destination Server" Window

6. On the **Select server roles** window, select the **Active Directory Certificate Services** role.

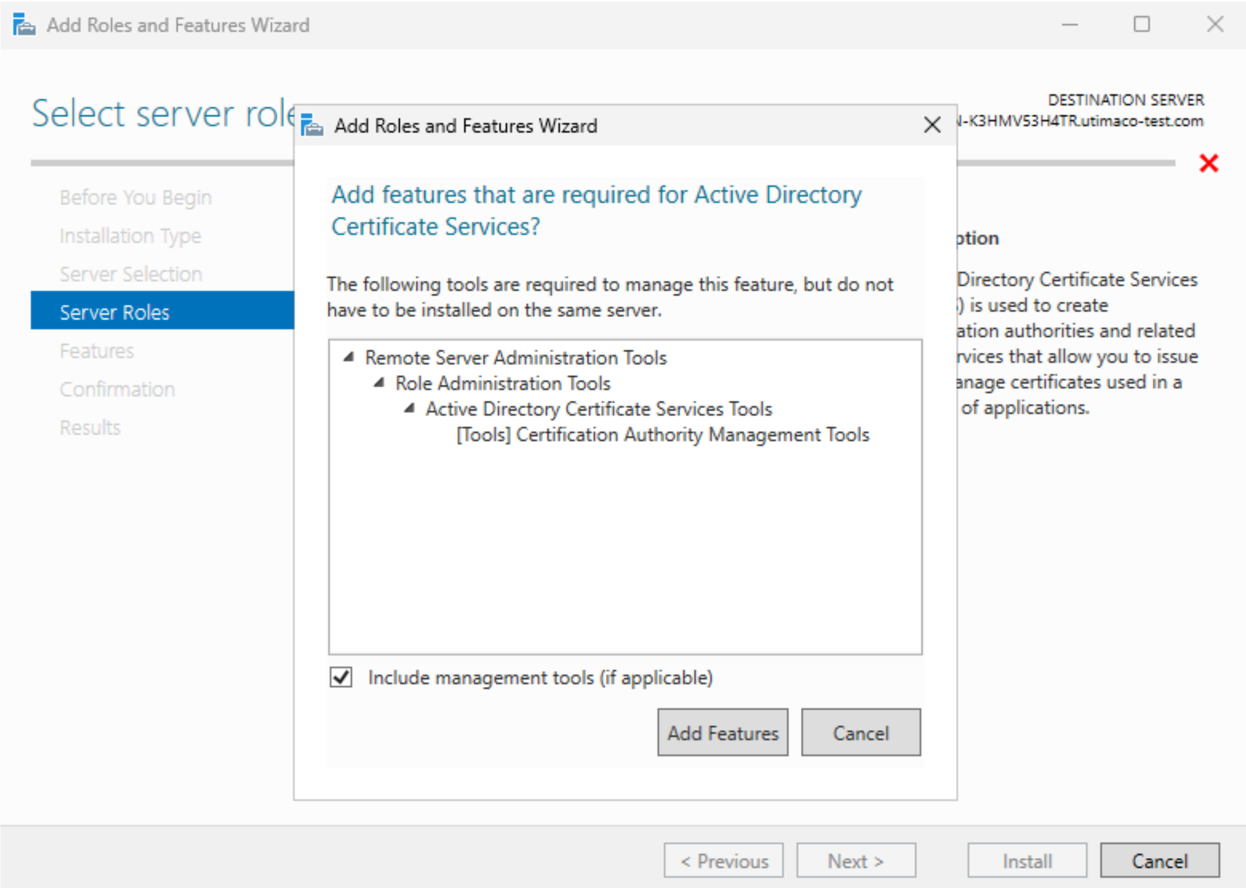

Figure 71 : "Select Server Roles" Window

7. When prompted to install **Remote Server Administration Tools**, select **Add Features**. Click **Next.**
8. On the **Select features** window, click **Next.**
9. On the **Active Directory Certificate Services** window, click **Next.**

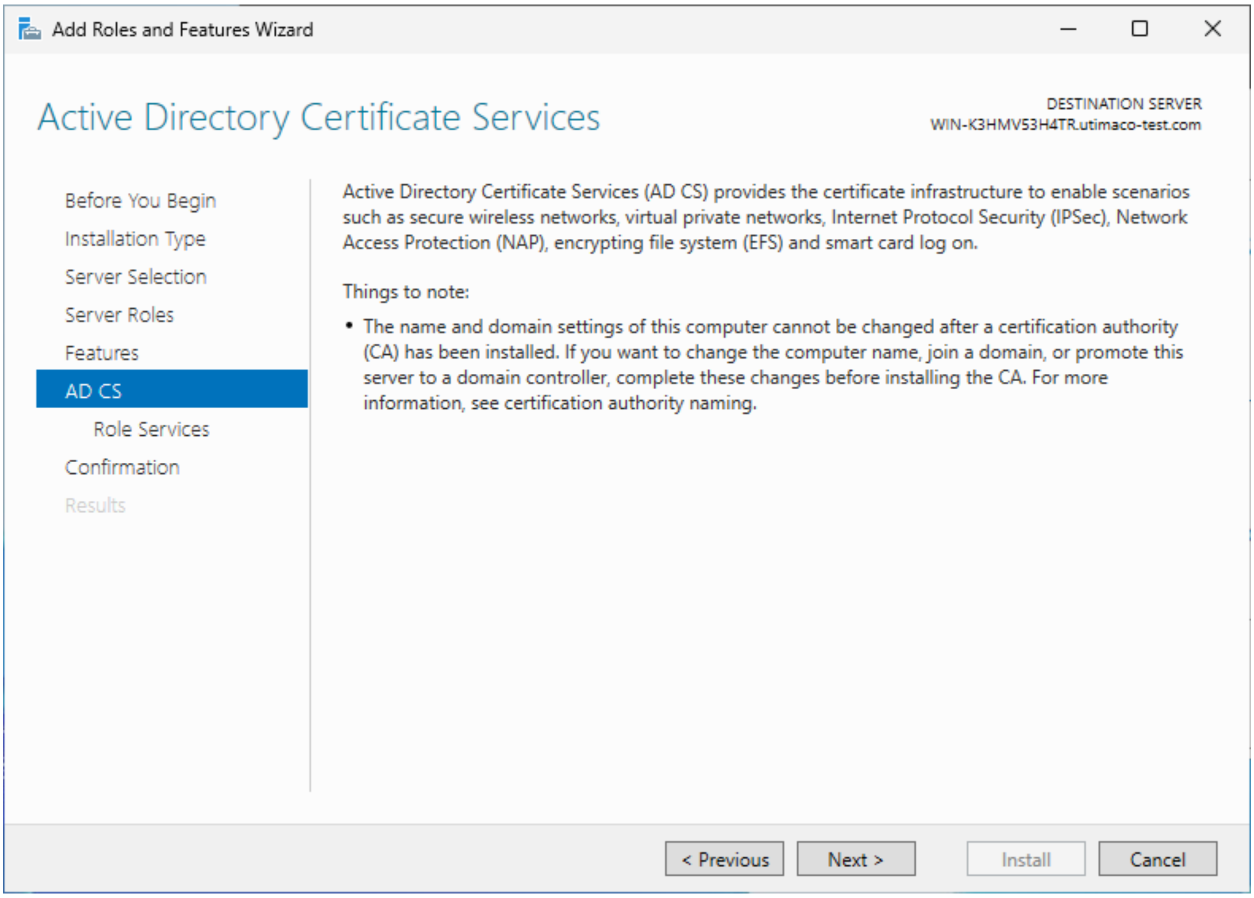

Figure 72 : "Active Directory Certificate Services" Window

10. On the **Select role services** window, the **Certification Authority** role is selected by default. Click **Next.**

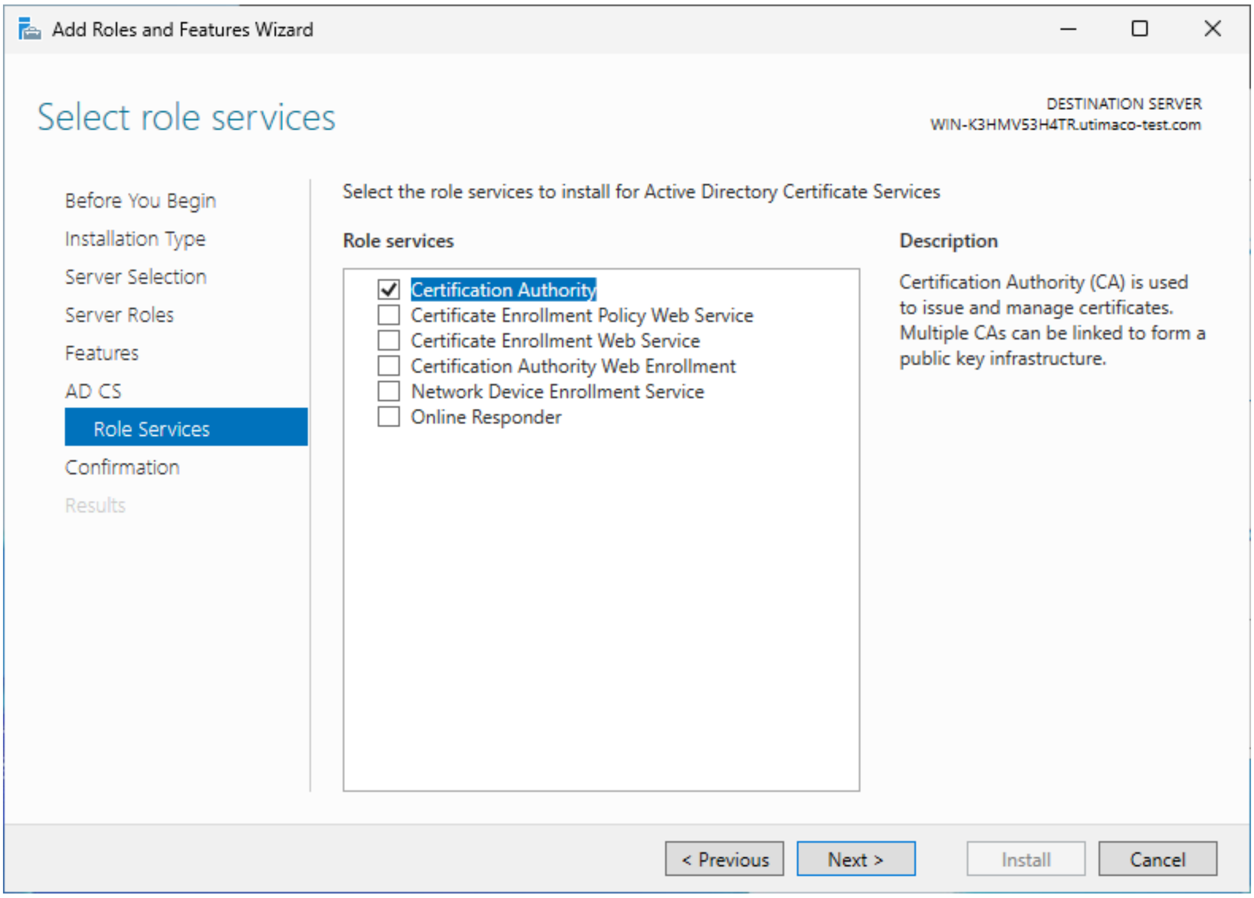

Figure 73 : "Select Role Services" Window

11. On the **Confirm installation selections** window, verify the information, then click **Install.**

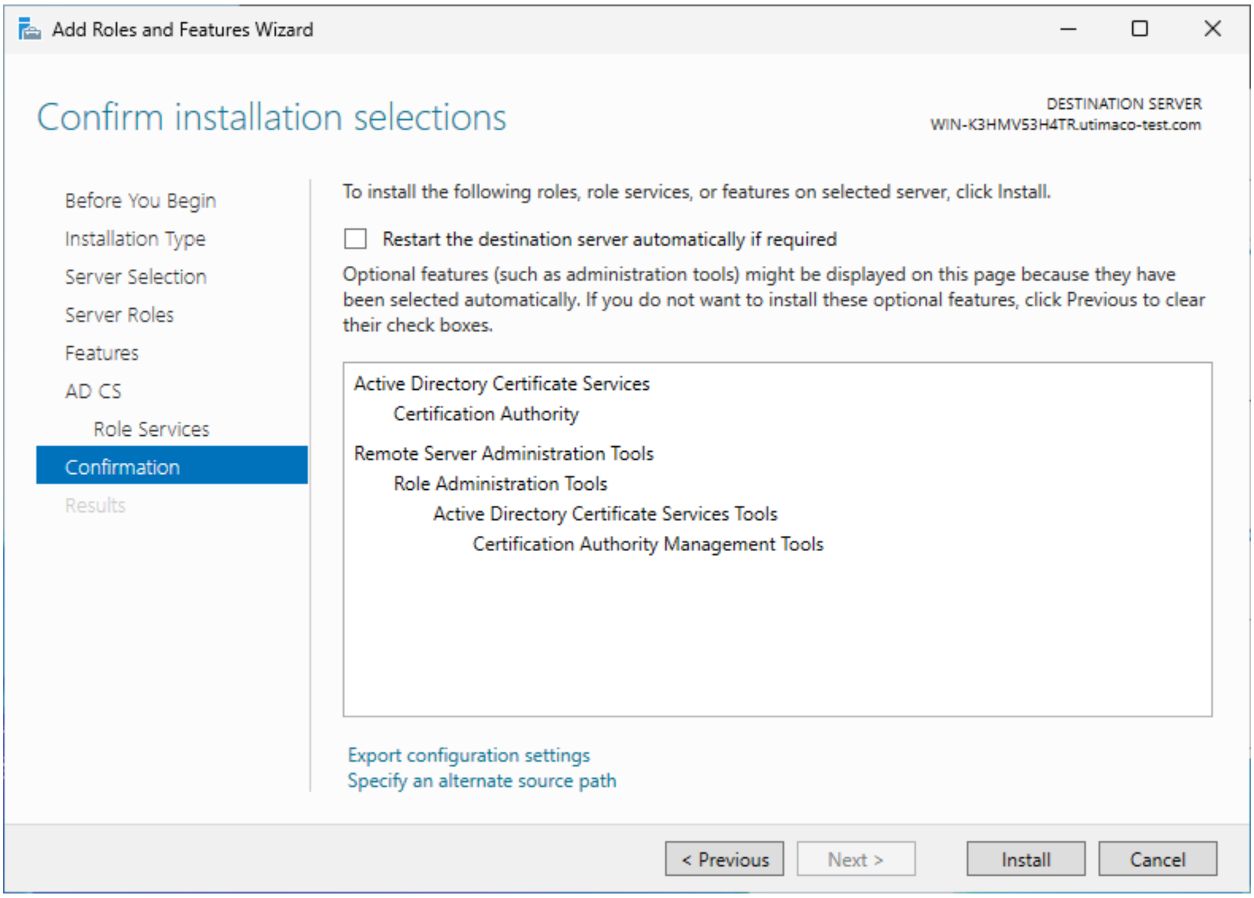

Figure 74 : "Confirm Installation Selections" Window

12. When the installation is complete, select the **Configure Active Directory Certificate Services on the destination server** link.

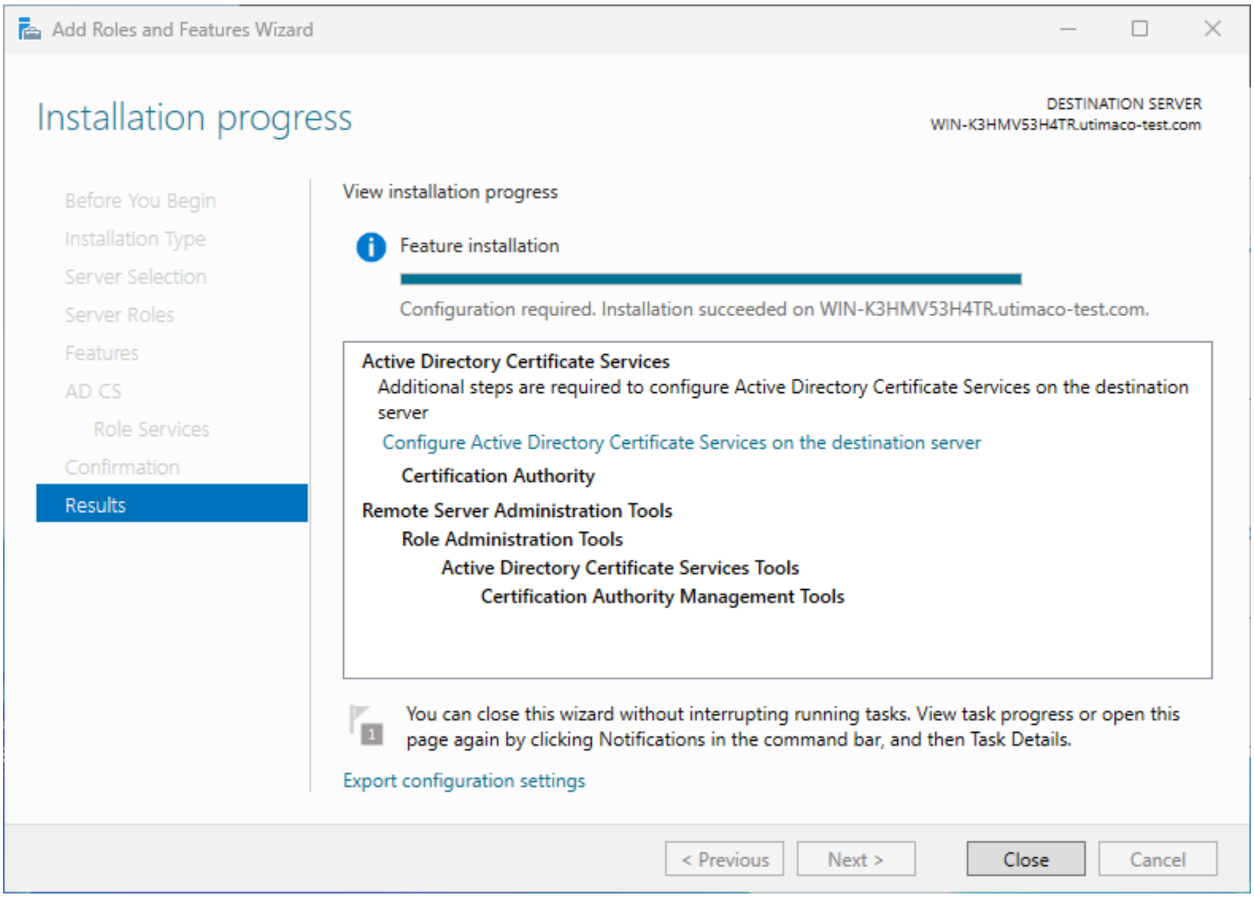

Figure 75 : "Installation Progress" Window

13. On the **Credentials** window, make sure that the Administrator's credentials are displayed in the **Credentials** box. If not, select **Change** and specify the appropriate credentials. Click **Next**.

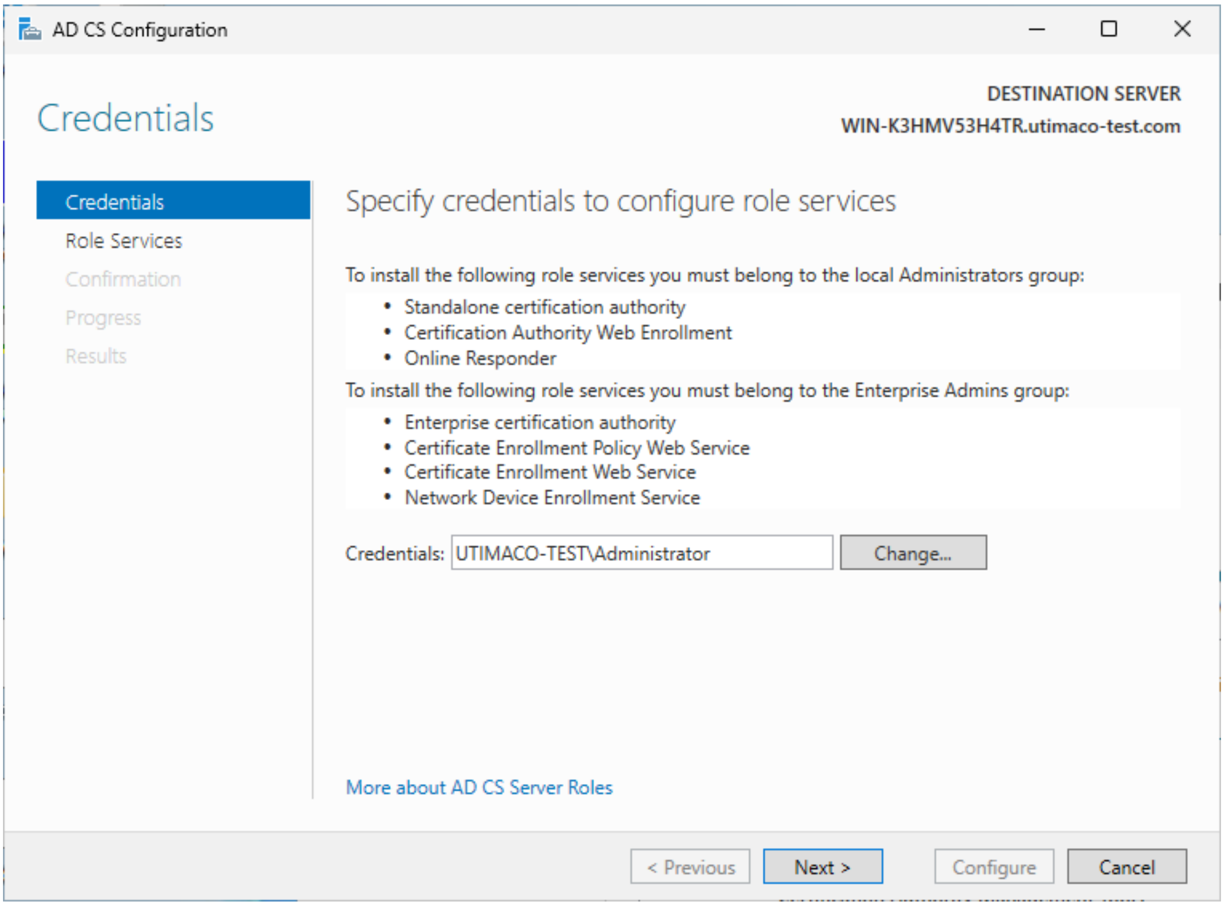

Figure 76 : "Credentials" Window

14. On the **Role Services** window, select **Certification Authority**. This is the only available selection when the certification authority role is installed on the server. Click **Next.**

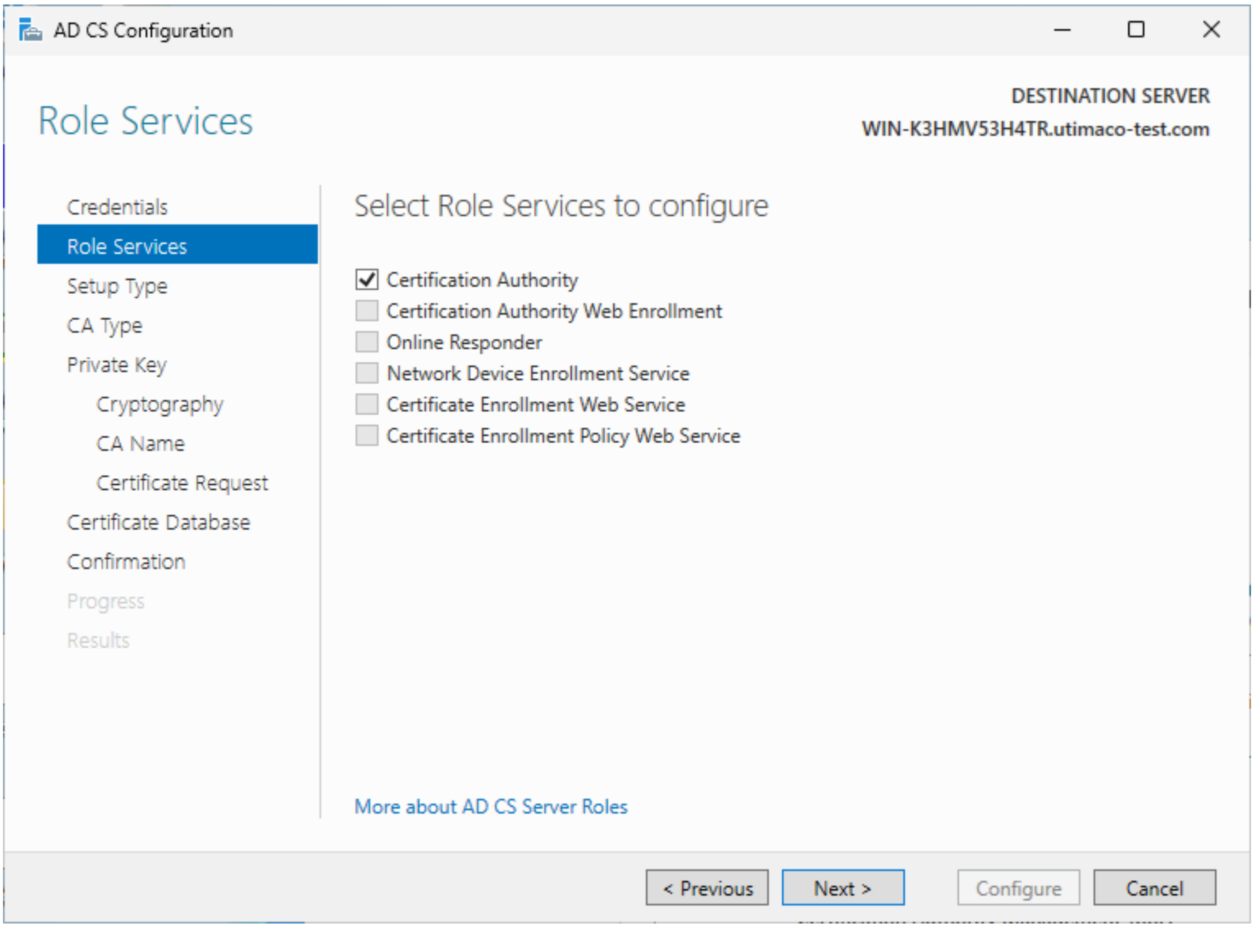

Figure 77 : "Select Roles to configure" Window

15. On the **Setup Type** window, select the appropriate CA setup type for your requirements. Click **Next.**

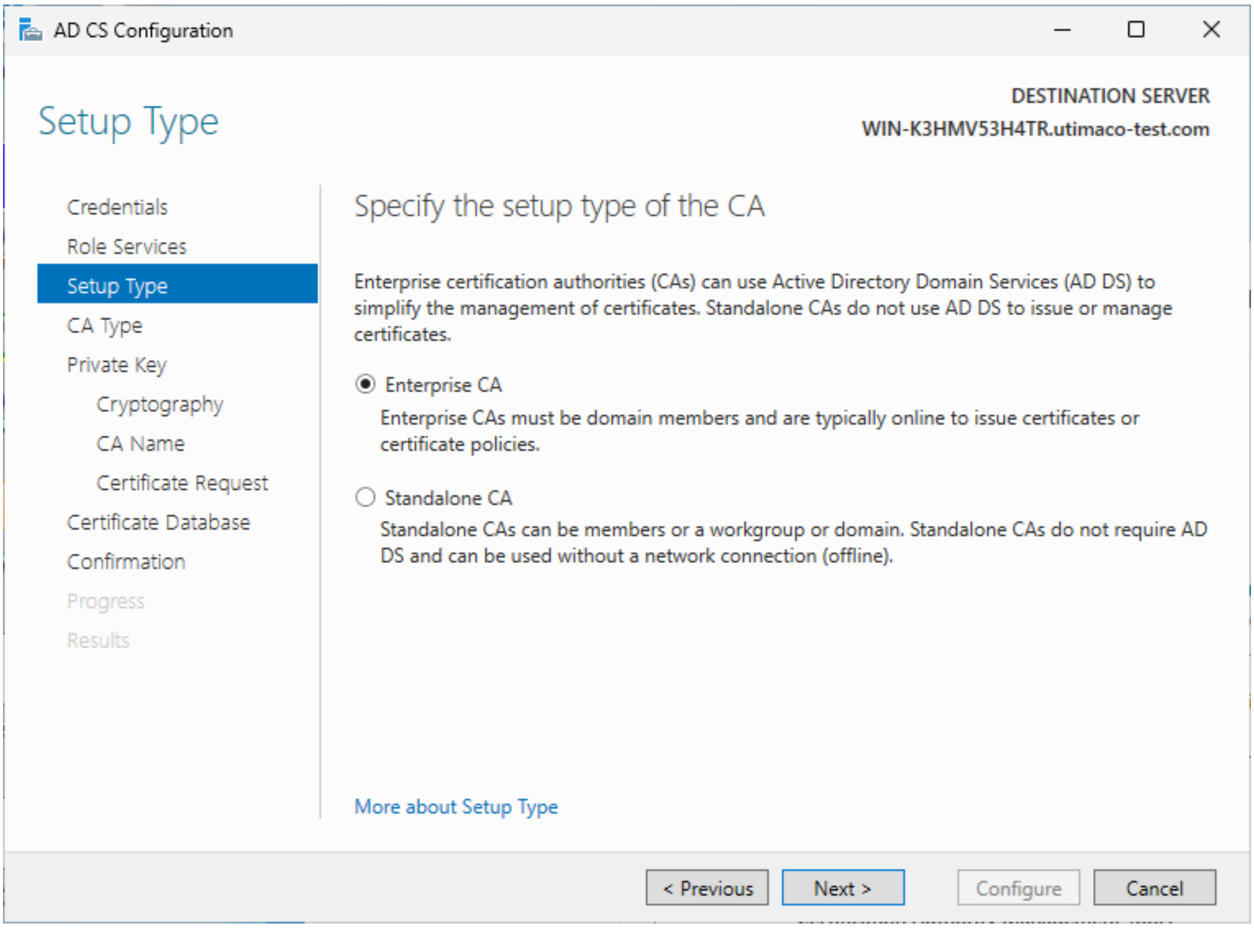

Figure 78 : "Setup Type" Window

16. On the **CA Type** window, **Root CA** is selected by default. Click **Next.**

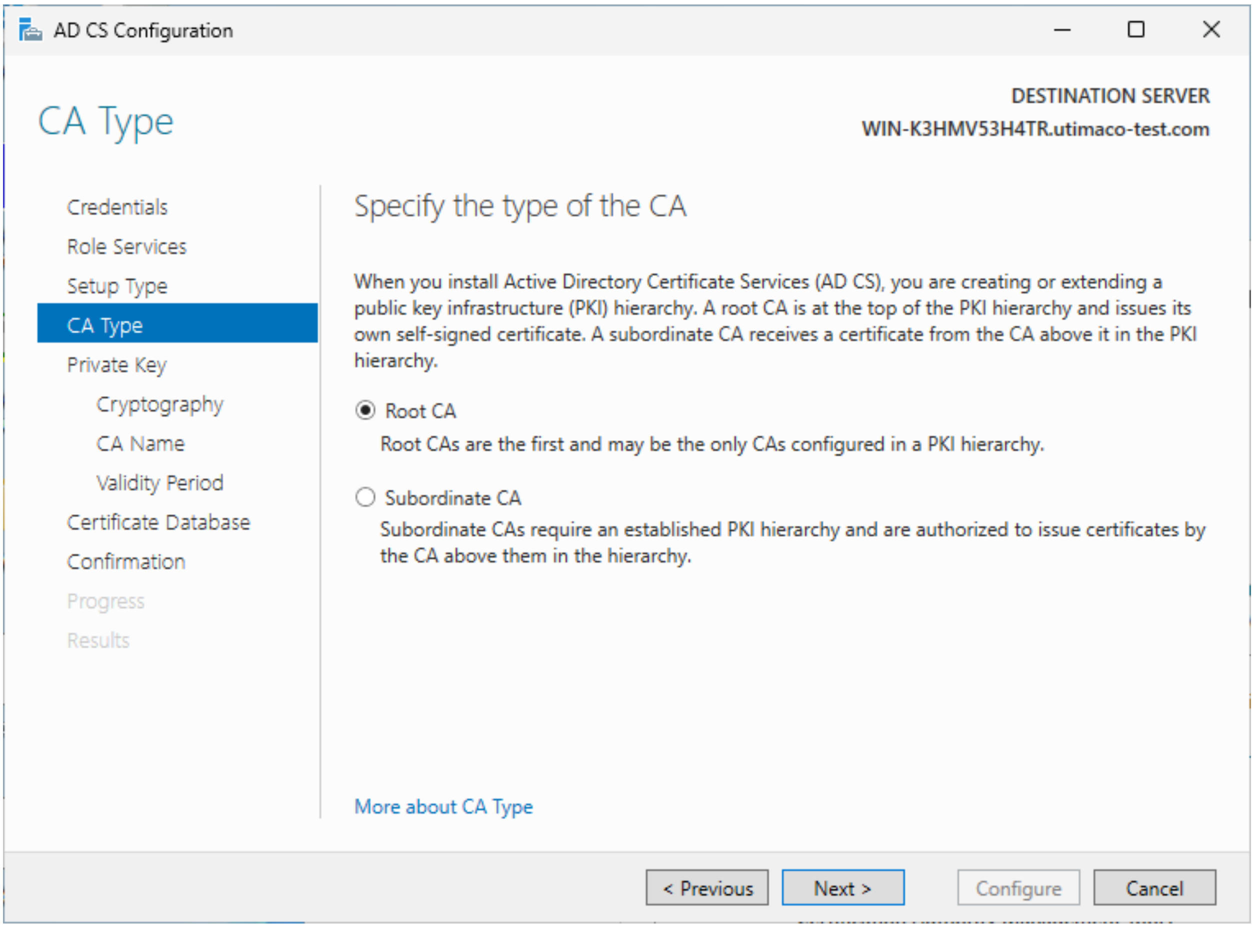

Figure 79 : "CA Type" Window

17. On the **Private Key** window, leave the default selection to **Create a new private key** selected. Click **Next.**

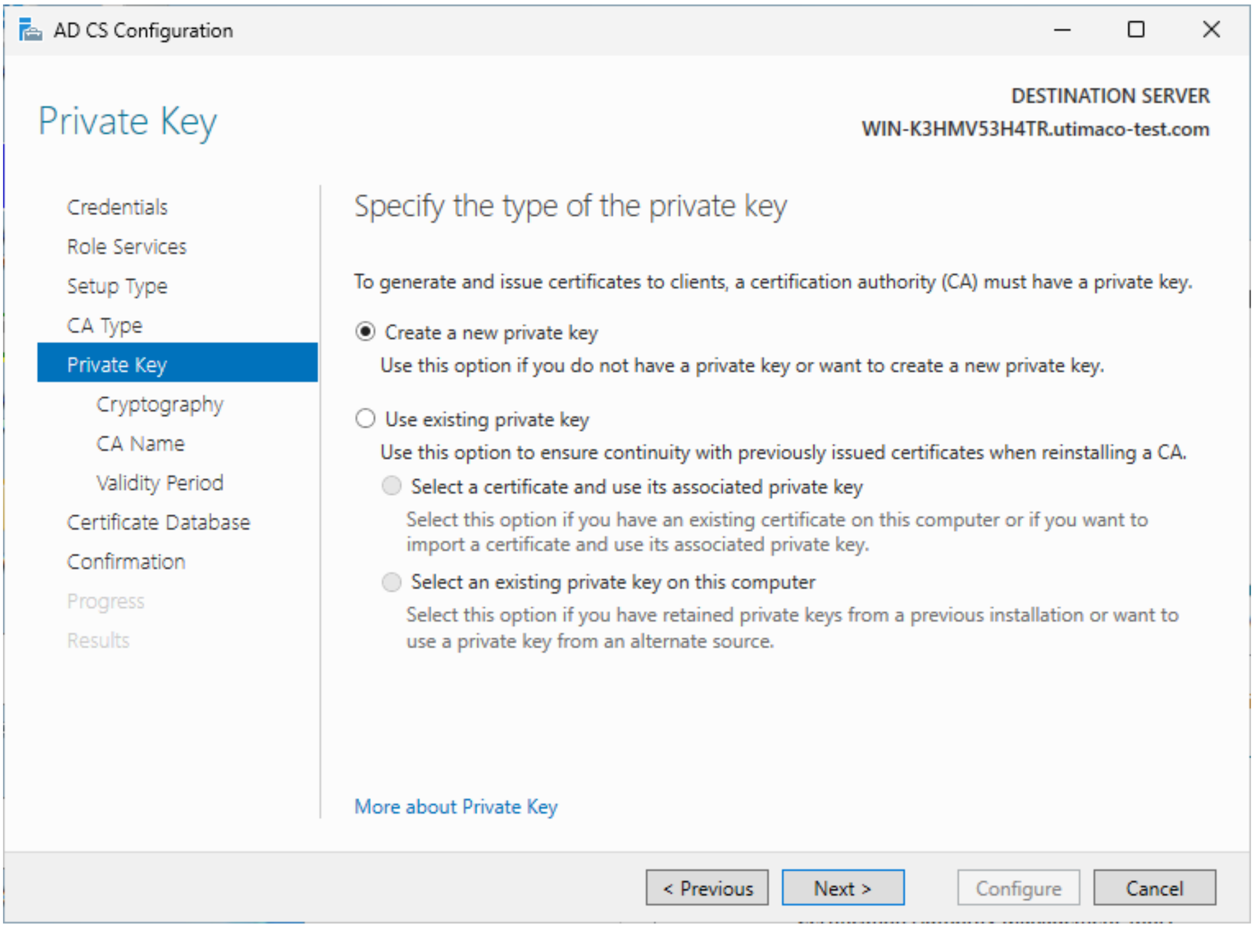

Figure 80 : "Private Key" Window

18. On the **Cryptography for CA** window, select the appropriate **Microsoft cryptographic provider** along with the key type, key length, and suitable hash algorithm. Click **Next.**

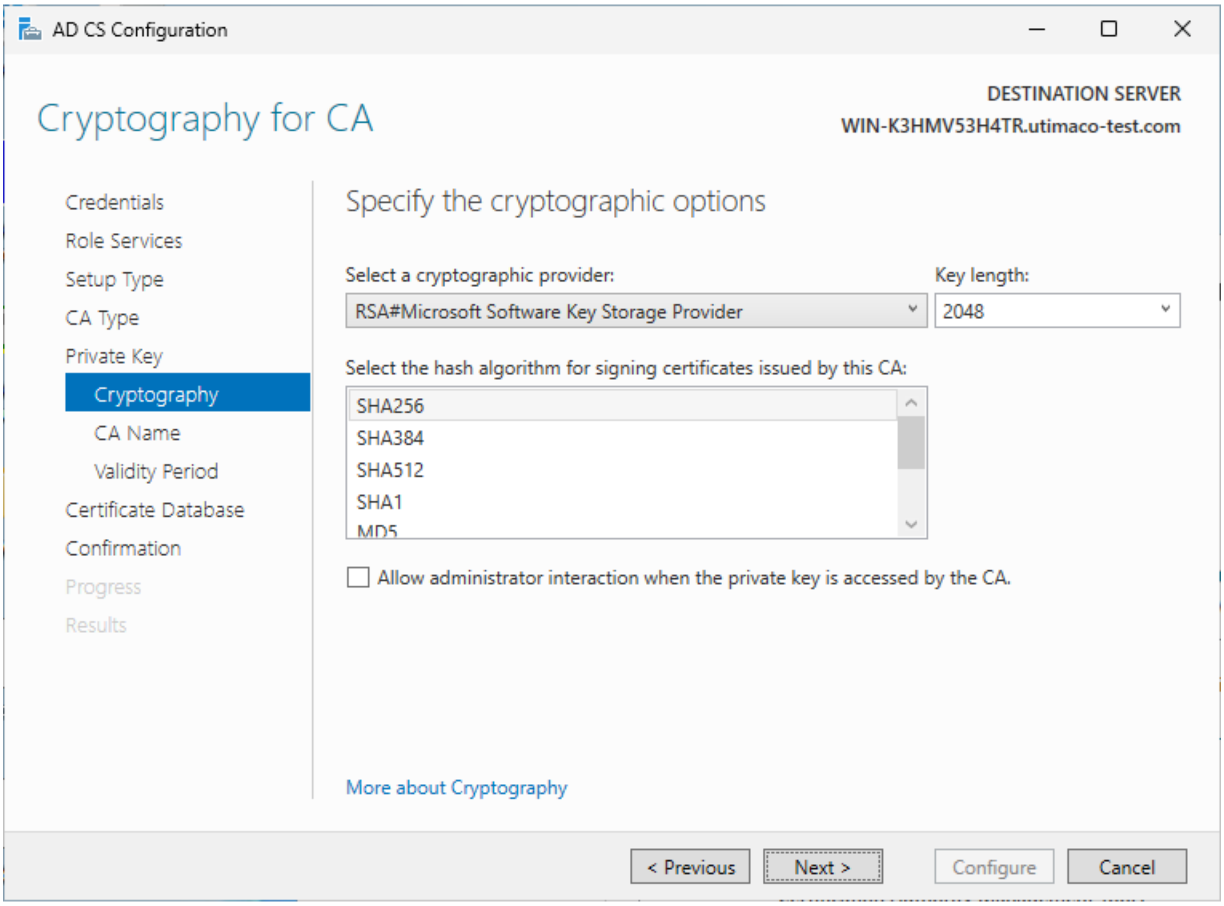

Figure 81 : "Cryptography for CA" Window

19. On the **CA Name** window, give the appropriate CA name. Click **Next.**

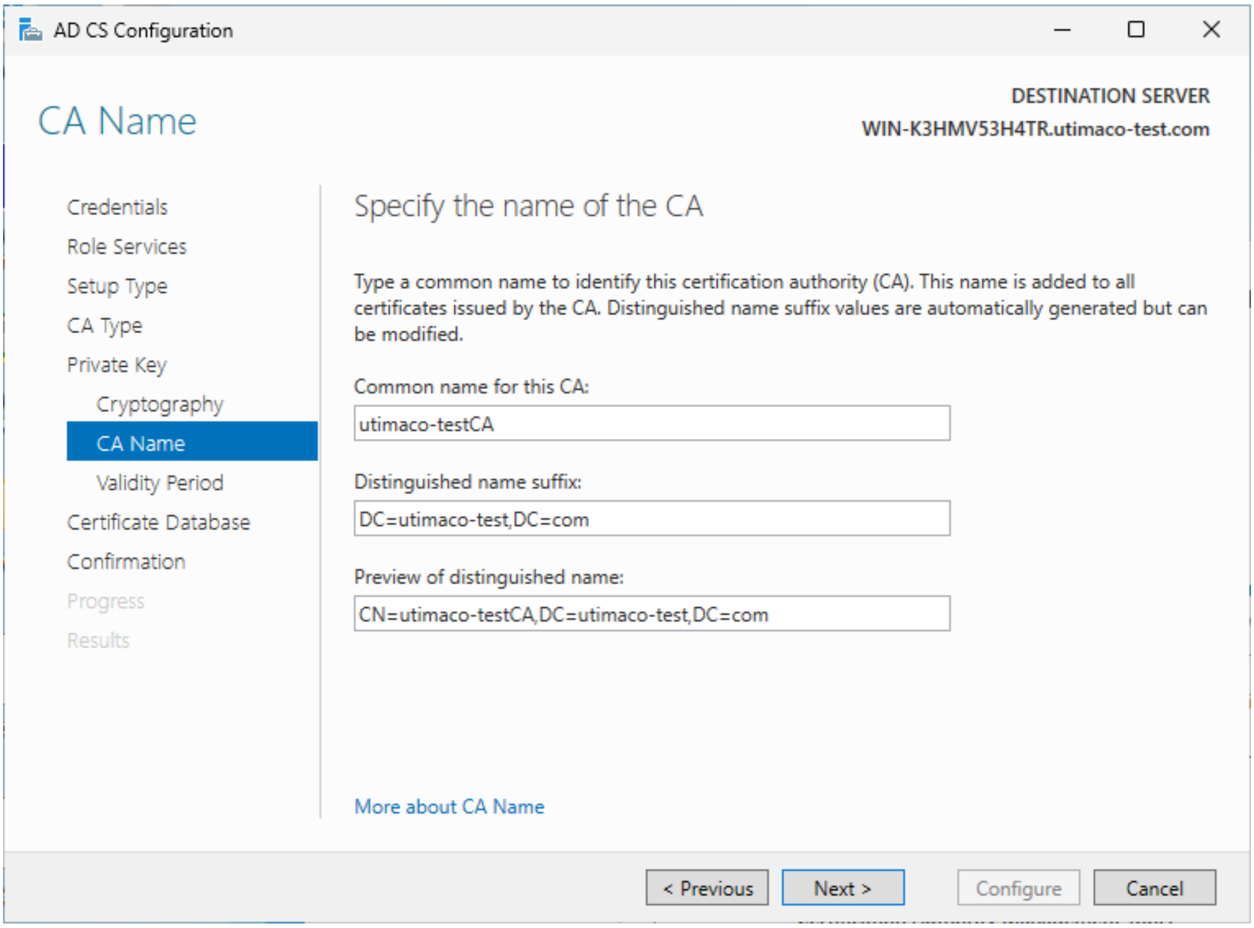

Figure 82 : "CA Name" Window

20. On the **Validity Period** window, enter the number of years for the certificate to be valid. Click **Next.**

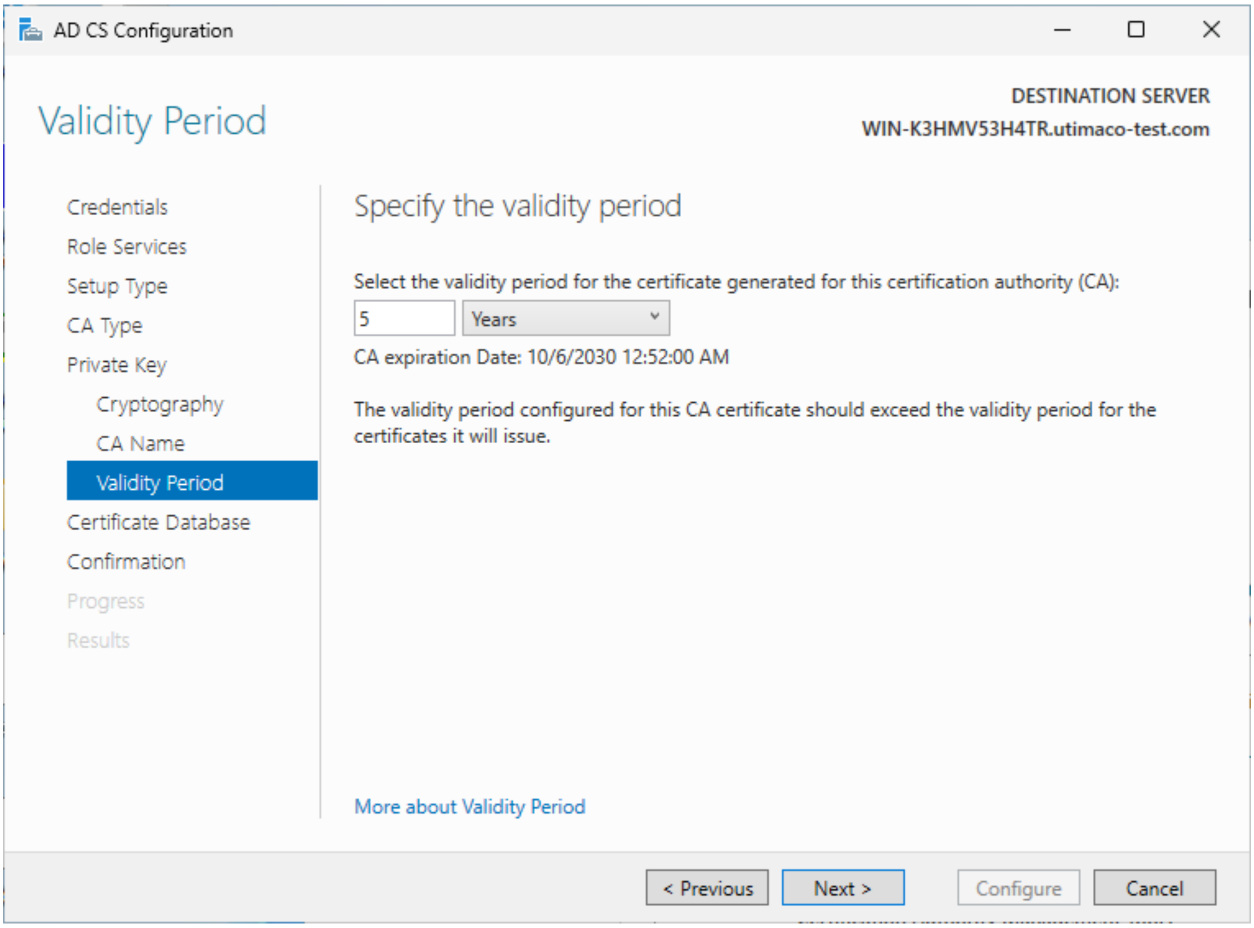

Figure 83 : "Validity Period" Window

21. On the **CA Database** window, leave the default locations for the database and database log files. Click **Next.**

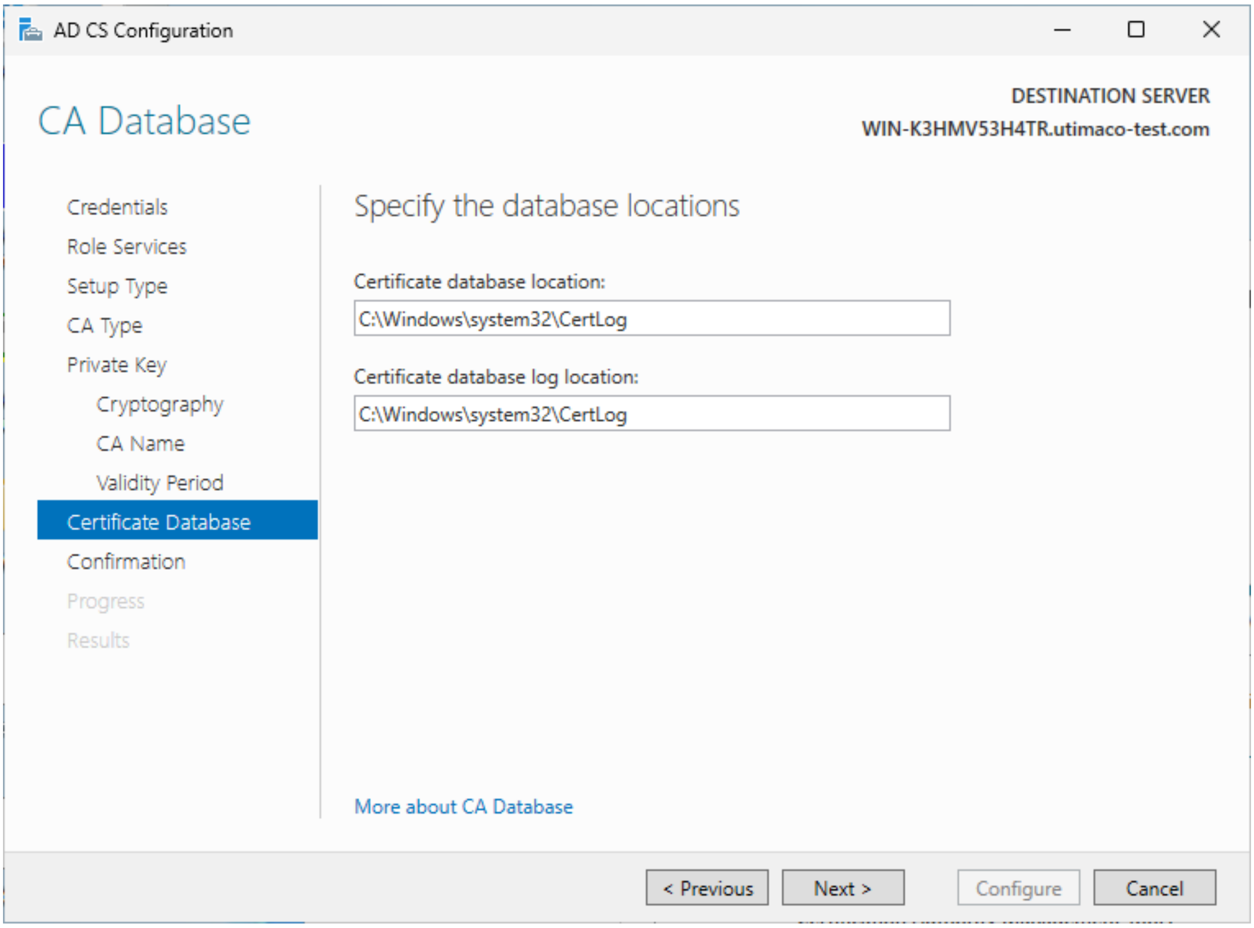

Figure 84 : "CA Database" Window

22. On the Confirmation window, click **Configure.**

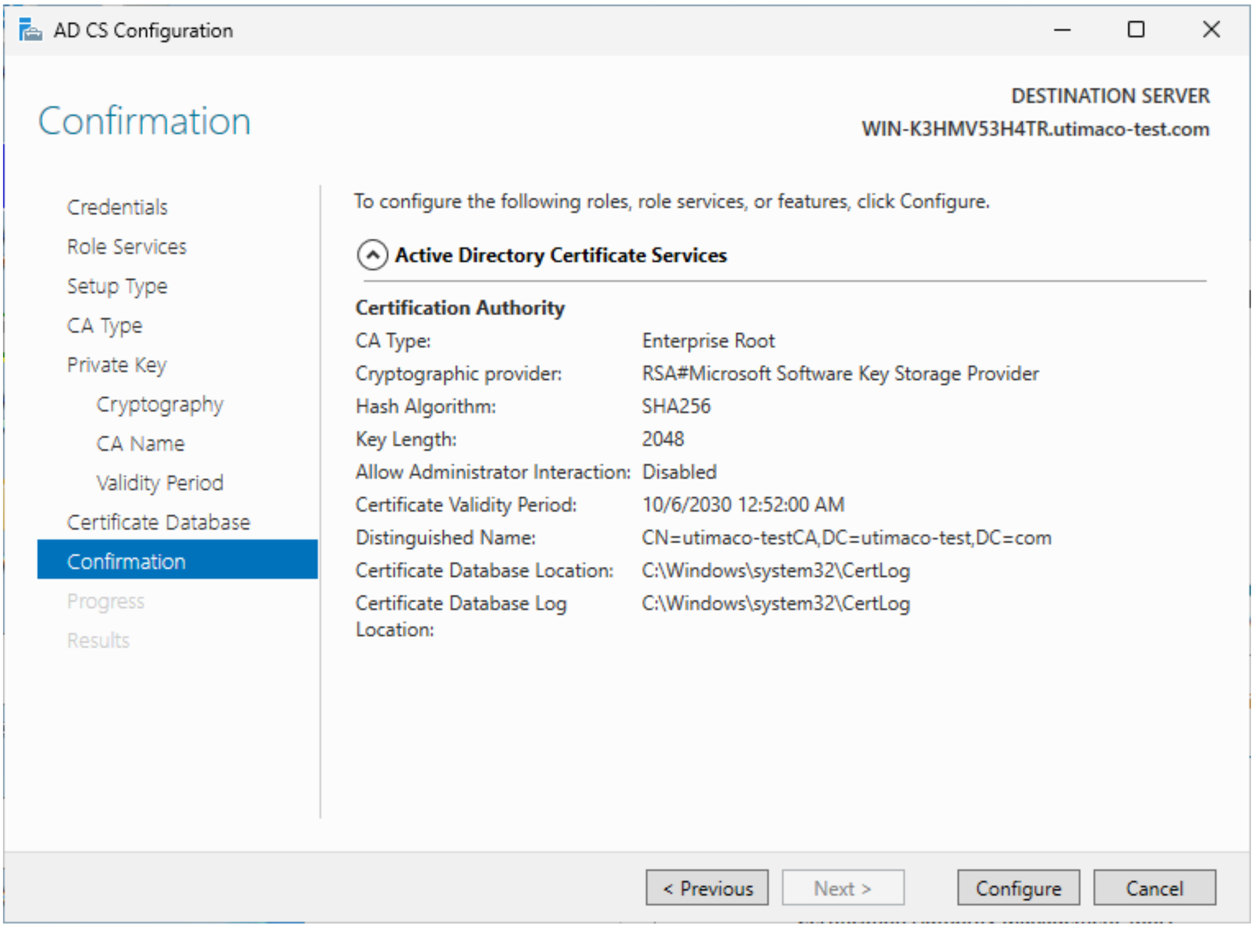

Figure 85 : "Confirmation" Window

23. 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.

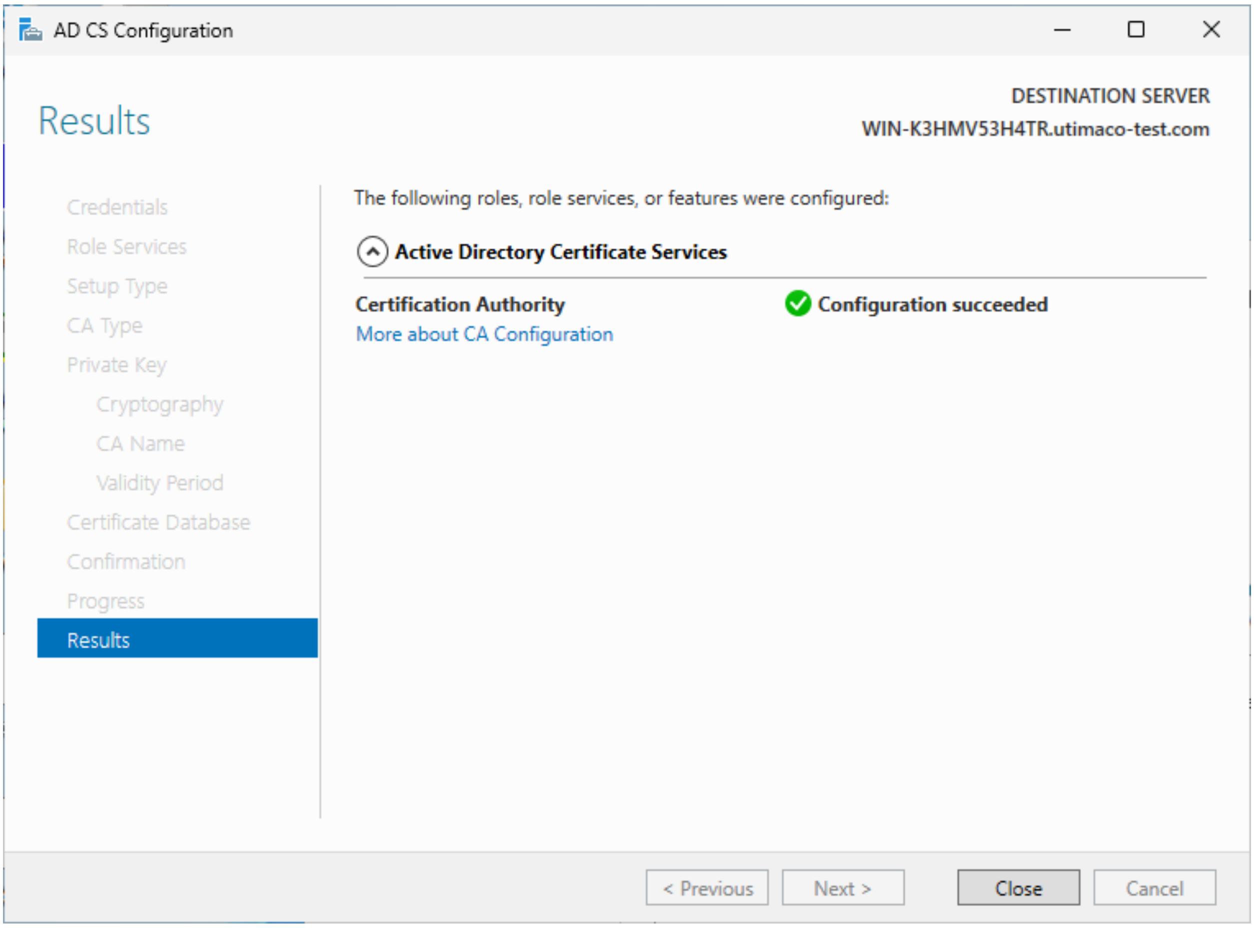

Figure 86 : "Results" Window

24. Open a command prompt and run the following command to verify that the service is running:

›_ Console

```
sc query certsvc
```

25. Open a command prompt and run the following command to verify the CA key:

›_ Console

```
certutil -verifykeys
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.3.2 Create a Backup of CA Database

The following command can be used to generate a backup of the CA database that can be restored after an incident.

›_ Console

```
# Create a database and private key backup
> certutil.exe -backup <drive>:\CaBackup

# Create a certificate backup
> certutil -ca.cert "<drive>:\CaBackup\<CA_Name>.cer"

# Create a registry export
>reg export HKLM\SYSTEM\CurrentControlSet\services\CertSvc
<drive>:\CaBackup\CAregistry.reg

# Stop the AD CS service
> net stop certsvc
```

6.1.3.3 Importing Private Key to HSM

The private key, created with the backup command (check the Section Create a Backup of CA Database), needs to be imported to the HSM.

1. Open a command prompt as an Administrator and use the below command to import the .p12 file to the HSM.

›_ Console

```
cngtool Name=<key_name> [Spec=<key_specifier>] [Type=<type>] [Password=<pass>]
ImportKey=<filename>
```

Example

›_ Console

```
cngtool Name=PrivateKey Spec=0 Type=PKCS8 Password=123456 ImportKey=C:
\CaBackup\Root-CA.p12
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

2. Check with the cngtool whether the private key was imported successfully.

›_ Console

```
cngtool ListKeys
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.3.4 Synchronizing HSMs

If the environment has a High Availability setup, the HSMs must be synchronized.

1. Open the Crypto Administration Tool.
2. Make sure the HSM is connected and in an operational mode.

3. Select on **Login/Logoff** to open the **Login/Logoff User** window.

4. Log in the appropriate users to achieve the permission level of at least 22000000.

5. Select **Backup/Restore** to open the **CryptoServer Database Backup/Restore** Wizard window.

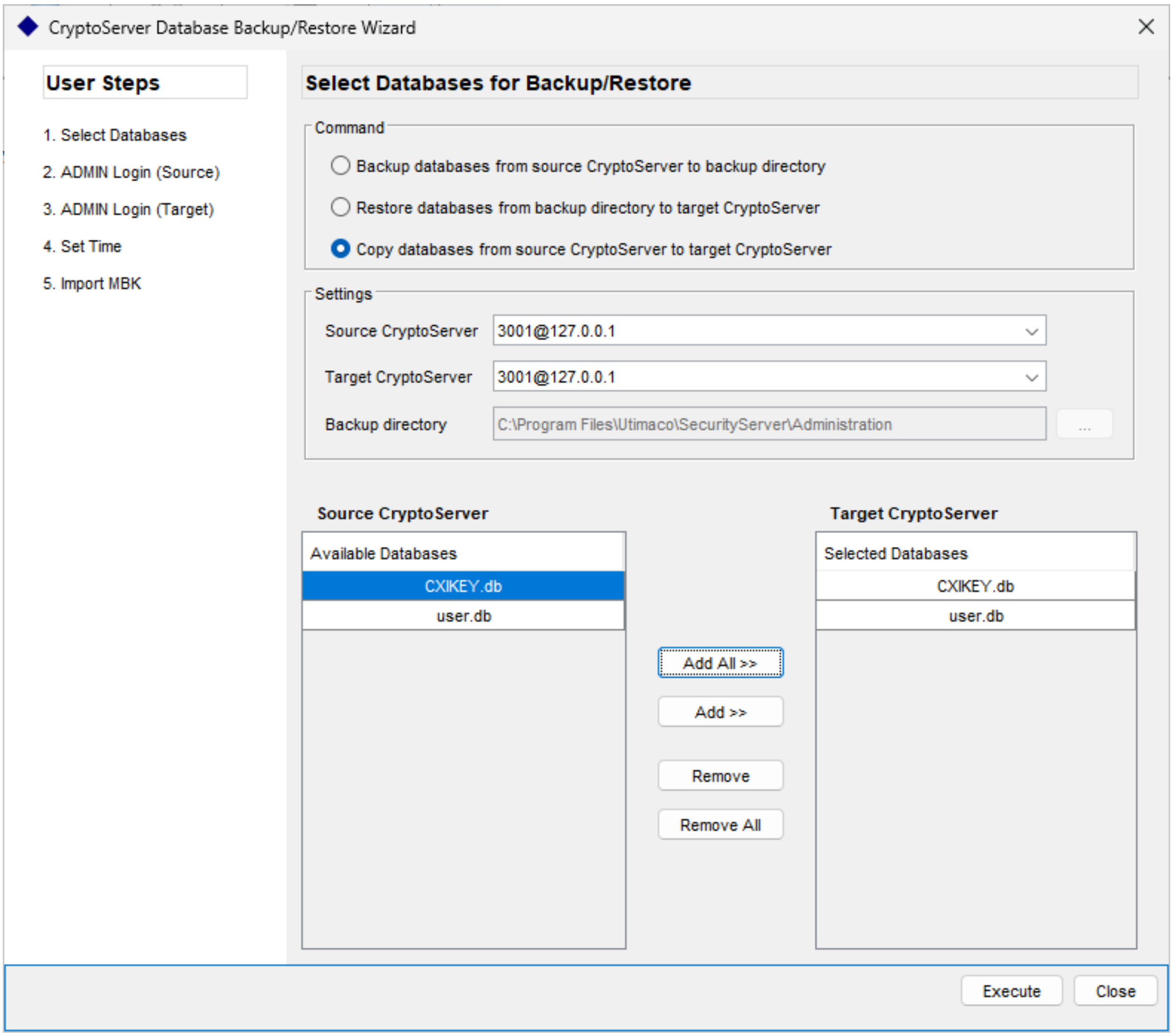

Figure 87 : "CryptoServer Database Backup/Restore Wizard" Window

6. In the Command section, select **Copy databases from Source CryptoServer to Target CryptoServer.**

7. In the Settings section, select the appropriate Source CryptoServer. If available, select the appropriate **Target CryptoServer**. In the **Backup directory** section, type the appropriate

backup directory path (set to `C:\Program Files\Utimaco\CryptoServer\Administration` as default) or click ... to browse to the appropriate directory.

8. Select the databases to copy.
9. Click **Execute.**
10. A confirmation window appears.

6.1.3.5 Reintroduce the Certificate

The certificate must be deleted and imported to connect it with the key that is stored in the HSM. PowerShell was used for this task.

1. Get the certificate thumbprint.

›_ PowerShell

```
PS> Get-ChildItem -Path cert:\LocalMachine\My
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint Subject
---------- -------
BE82E0FEC4B7F9DA33FF5CC2A0CC4D987F04A11B CN=DemoRootCa, DC=Uti2, DC=si
Then we extract the container name
PS> certutil -store my BE82E0FEC4B7F9DA33FF5CC2A0CC4D987F04A11B | findstr
"Subject: sha1 Unique Provider"
Subject: CN=DemoRootCa, DC=Uti2, DC=si
Cert Hash(sha1): be82e0fec4b7f9da33ff5cc2a0cc4d987f04a11b
Unique container name: 2fc25277ec718baa2886124e04bc16e7_36ed1a95-76e3-
4398-a4c7-c31d5fce304f
Provider = Microsoft Software Key Storage Provider
```

2. Make sure that the file is located on the local disk (one of the two possibilities, depending on the installation).

›_ PowerShell

```
PS> Get-Item C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\<container> PS>
Get-Item C:\ProgramData\Microsoft\Crypto\Keys\<container>
```

3. Delete the certificate.

›_ PowerShell

```
PS>Remove-Item -Path cert:\LocalMachine\My\<thumbprint> -DeleteKey
```

4. Check if the certificate was deleted (one of the two possibilities, depending on the installation).

›_ PowerShell

```
PS> Get-Item C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\<container> PS>
Get-Item C:\ProgramData\Microsoft\Crypto\Keys\<container>
```

5. Import the certificate.

›_ PowerShell

```
PS> certutil -addstore -f "My" "<CaName>.cer" Signature matches Public Key
Certificate "DemoRootCa" added to store.
CertUtil: -addstore command completed successfully.
```

6. To create a link between the certificate and the private key, first find the certificate serial number.

›_ PowerShell

```
PS> certutil "<CaName>.cer" | findstr Serial Serial Number:
3a9f8a8c61129593400f6738896afcc0
```

7. And use the certutil command to repair the link.

›_ PowerShell

```
PS> certutil -f -repairstore -csp "Utimaco CryptoServer Key Storage Provider" my
<serial>
CertUtil: -repairstore command completed successfully
```

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.3.6 Configuring AD CS to Use Utimaco CryptoServer Key Storage Provider

1. Create a .reg file and run it as an administrator or edit registry manually to configure the AD CS to use the private key stored in the HSM.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CertSvc\Configuration\<CaName>\CSP] "Provider"="Utimaco CryptoServer Key Storage Provider"
```

2. Start the service and check the status of the AD CS.

›_ Console

```
>net start certsvc
```

3. Verify that the CA service has successfully started by running the command.

›_ Console

```
>sc query certsvc
```

4. Verify the CA key by running the command:

›_ Console

```
>certutil -verifykeys
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.4 Installing and Configuring the AD CS Failover Cluster

The following sections describe the installation and configuration of a CA on a failover cluster running on Windows Server. Register the Utimaco CryptoServer Key Storage Provider.

6.1.4.1 Installing AD CS Server Role on First Cluster Node

1. Join a machine to the Domain and log in as a user with Administrative privileges.
2. The steps to install the Microsoft Active Directory Certificate Services are the same as those in the Installing Microsoft Active Directory Certificate Services with Windows Enterprise section. After Microsoft AD CS is successfully installed, continue with the steps below.
3. Open the command prompt and run `certsrv.msc,` and then click **OK.**

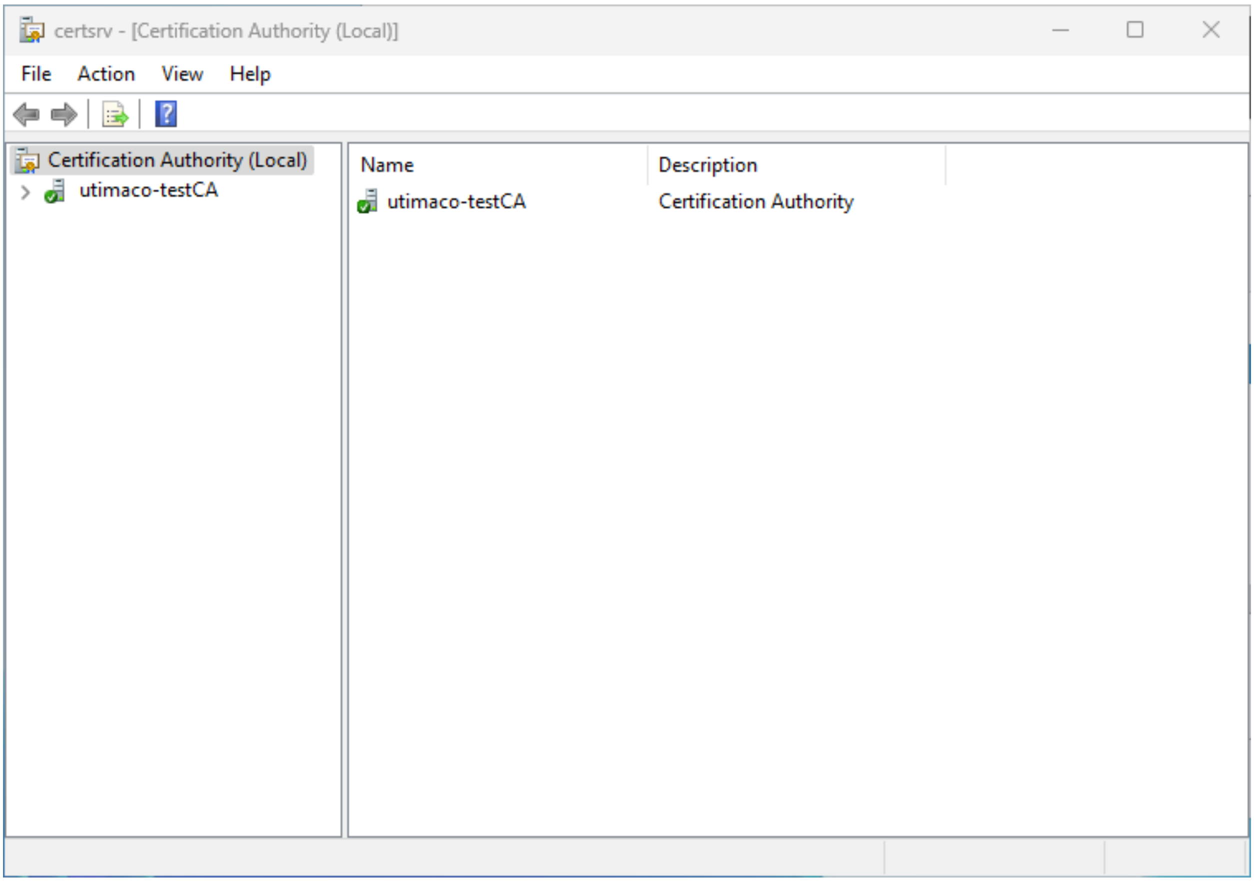

Figure 88 : "Certificate Authority" Window

4. Select the **Certificate Authority** node in the left pane.
5. In the **Action** menu, select **All Tasks** and then select **Backup CA.**

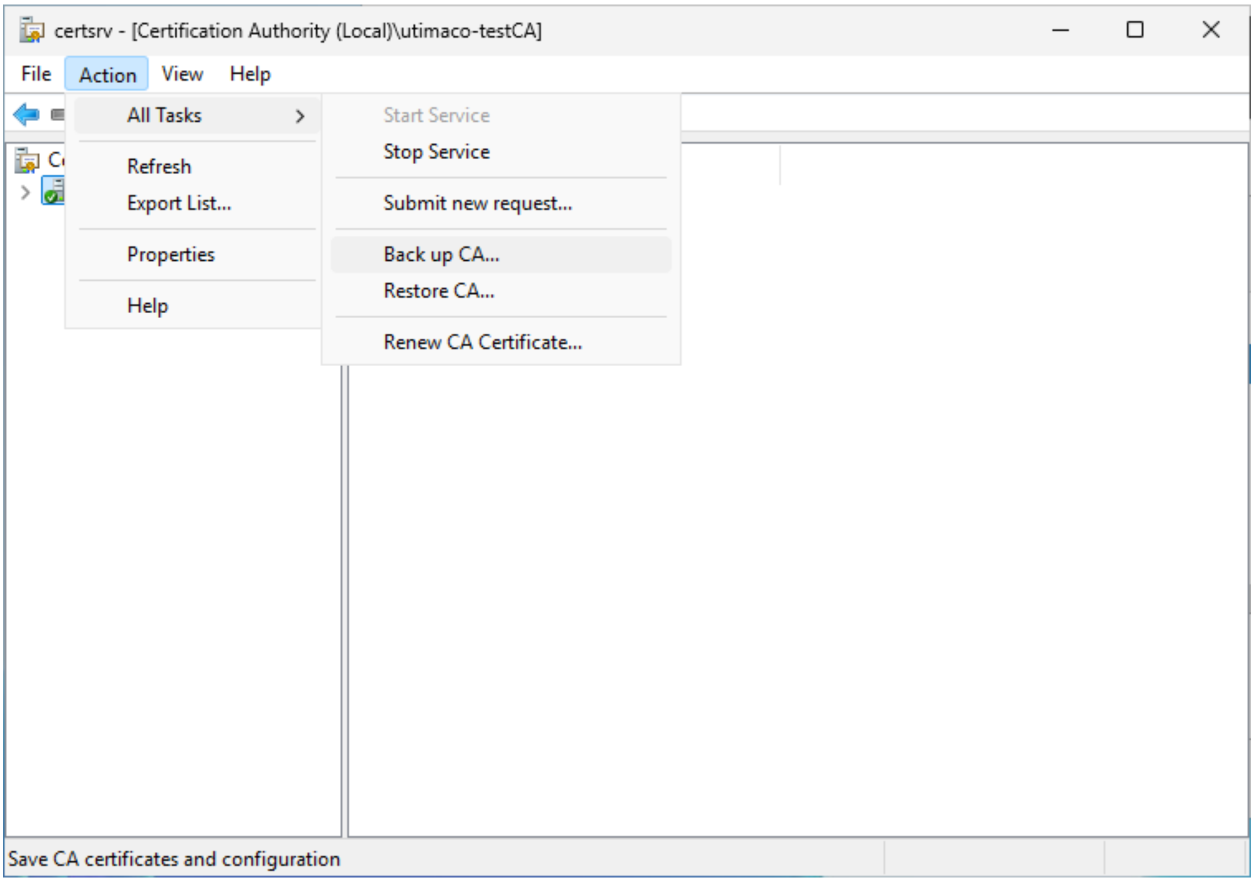

Figure 89 : "Certificate Authority" Window

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6. On the **Welcome page** of the **CA backup** wizard, click **Next.**
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.**

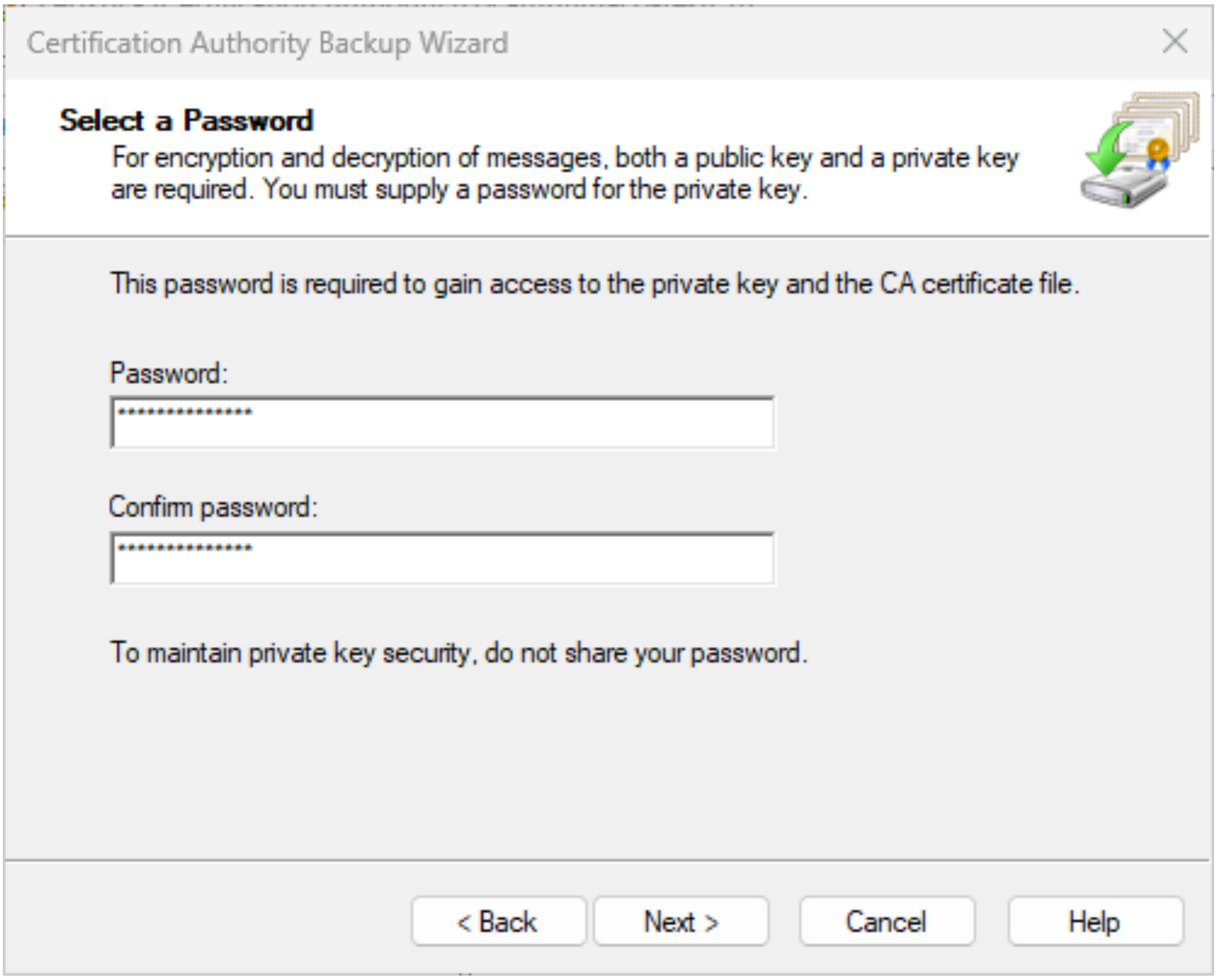

Figure 90 : "Certification Authority Backup" Window

9. Click **Finish.**

Figure 91 : "Certification Authority Backup" Window

> 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 Utimaco HSM.

10. Click **OK** to continue.
11. Export the CA Certificate.

›_ Console

```
>certutil --ca.cert rootca_certificate.cer
CertUtil: -ca.cert command completed successfully.
```

12. Generate the MBK and backup of the databases from the first node using the CryptoServer Administrator Tool (CAT).

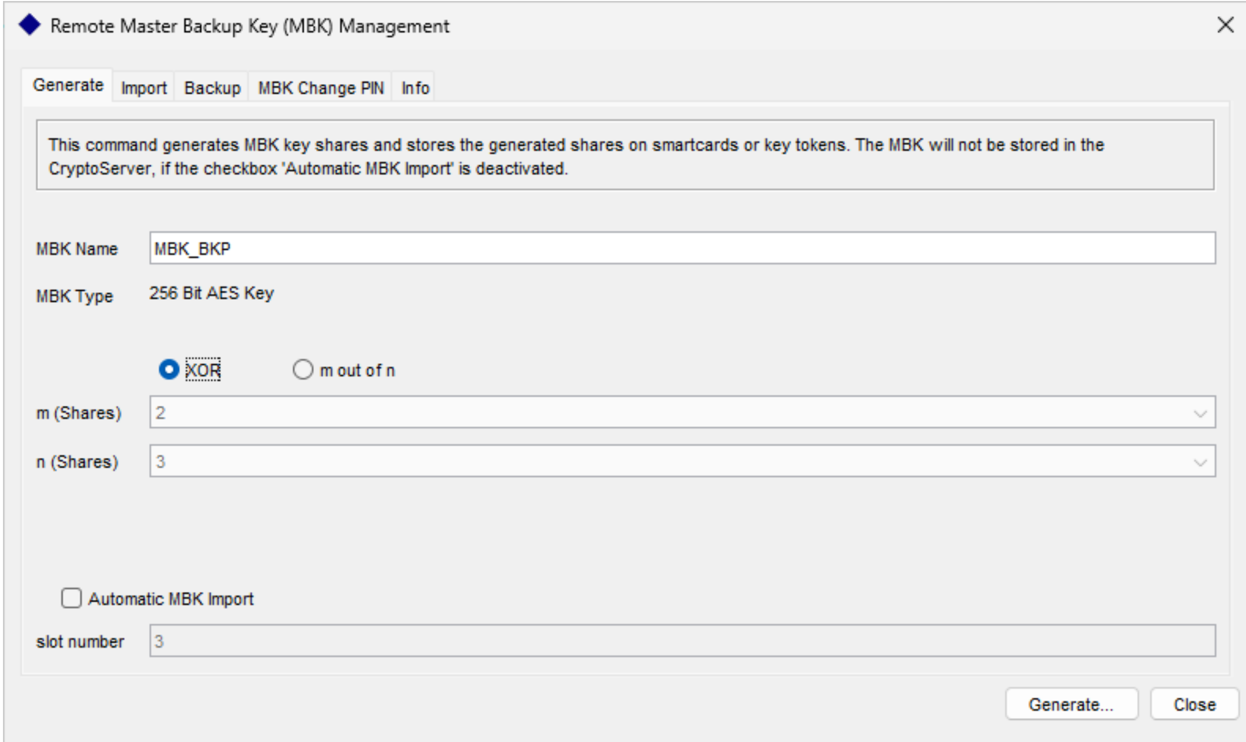

Figure 92 : "Remote Master Backup Key Management" Window

13. Stop the certsvc service. The following command can be executed to accomplish this.

›_ Console

```
net stop certsvc
```

6.1.4.2 Detach the Shared Storage from the First Cluster Node

1. Select **Start,** then select **Server Manage**r to open **Server Manager.**
2. Select the **File and Storage Services**. Select **Disks**, select shared disk resource, **right-click** on it, and select **Take Offline.**

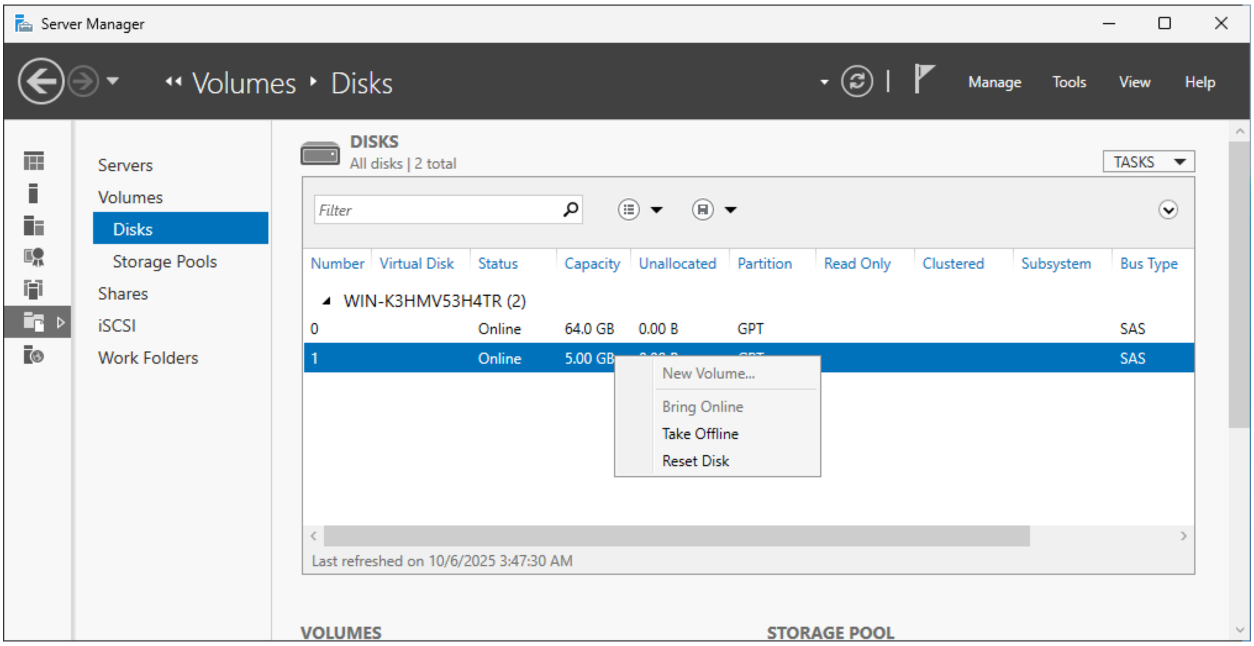

Figure 93 : "Server Manager" Window

6.1.4.3 Import MBK and Restore the Databases on Second Cluster Node

1. Copy the MBK shares and database files from the first cluster node onto the second cluster node.
2. Using **CAT** utility, log in to the CryptoServer with administrative privileges.
3. Select **Manage MBK** and select the **Import** tab, and import the MBK shares which copied from first cluster node.

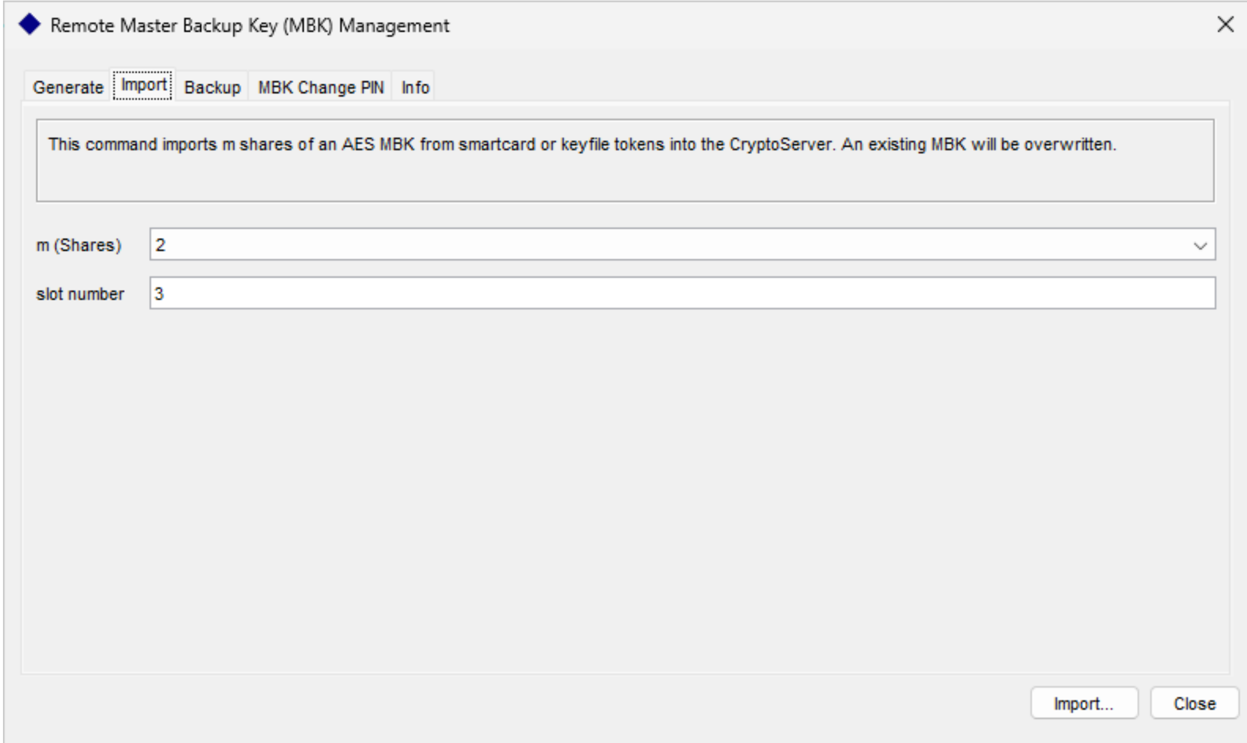

Figure 94 : "Remote Master Backup Key Management" Window

4. Select the **Backup/Restore** button on the CAT tool and select the radio button for **Restore databases from backup directory to target Cryptoserver.**
5. Add `CXIKEY.db` and `user.db` to the target Crytoserver and click **Execute.**

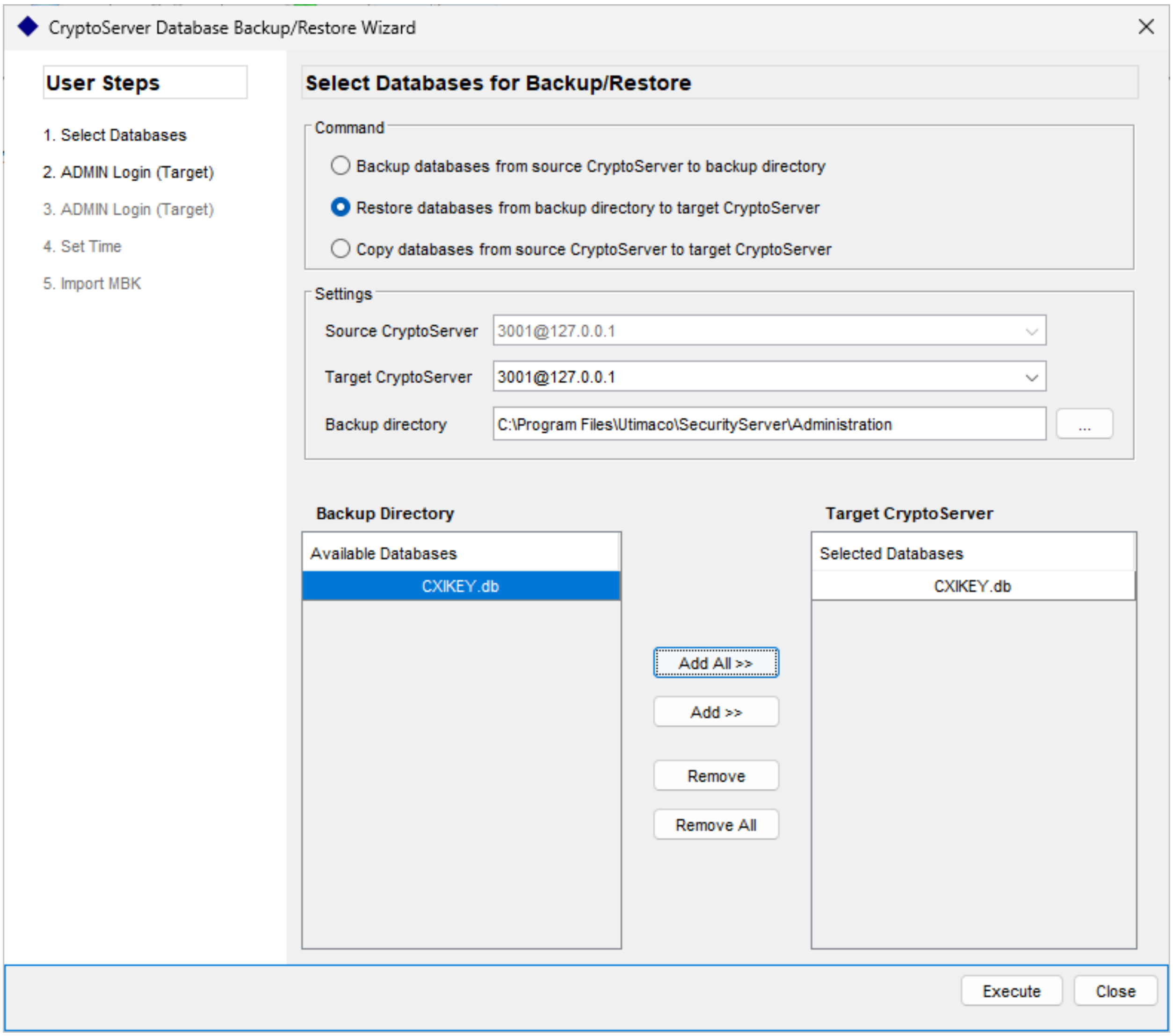

Figure 95 : "CryptoServer Database Backup/Restore" Window

6. Restart the CryptoServer service and ensure that users and keys were restored successfully.
7. Use the cngtool to check whether the private key was imported successfully.

›_ Console

```
cngtool ListKeys
```

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.4.4 Installing AD CS Server Role on Second Cluster Node

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

1. Log in as a user with Administrative privileges.
2. Select **Start,** then select **Server Manager** to open **Server Manager.**
3. Select the **File and Storage Services**. Click **Disks.**

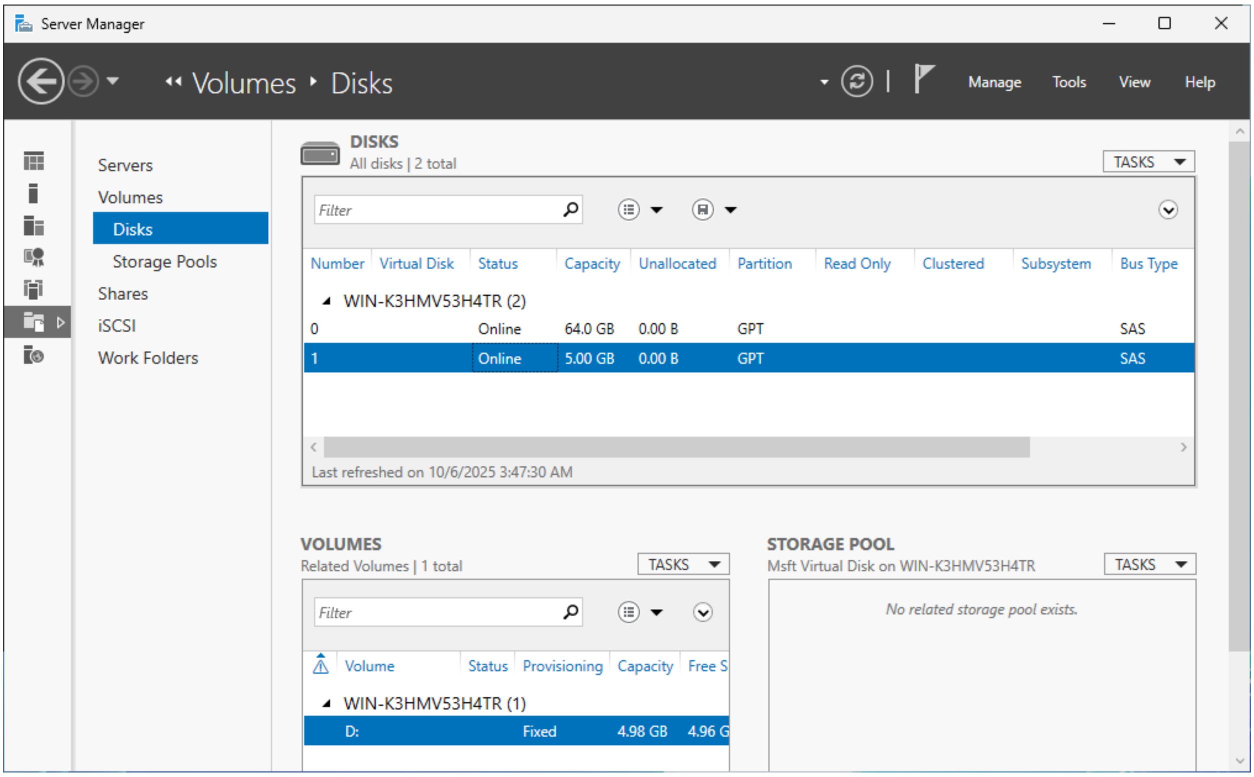

Figure 96 : "Server Manager" Window

4. Bring the shared disk online on the second cluster node.
5. Copy the exported CA certificate to the second cluster node.
6. Import the CA certificate that was previously created on the first cluster node.

›_ PowerShell

```
PS> certutil -addstore -f "My" "<CaName>.cer"
Signature matches Public Key
Certificate "DemoRootCa" added to store.
CertUtil: -addstore command completed successfully.
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

7. To create a link between the certificate and the private key, first find the certificate serial number.

›_ PowerShell

```
PS> certutil -addstore -f "My" "<CaName>.cer"
Signature matches Public Key
Certificate "DemoRootCa" added to store.
CertUtil: -addstore command completed successfully.
```

8. And use the certutil command to repair the link.

›_ PowerShell

```
PS> certutil –f –repairstore –csp "Utimaco CryptoServer Key Storage
Provider" my <serial>
CertUtil: -repairstore command completed successfully
```

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

9. Open **Server Manager** under **Configure this Local Server** and click **Add Roles and Features.**
10. The **Add Roles and Features Wizard** displays.
11. Click **Next**. Select radio for the **Role-based or feature-based installation** and click **Next.**
12. Select the radio button for a server from the server pool, select the second cluster node from the server pool, and click **Next.**
13. Select the **Active Directory Certificate Services** check box from the Server Roles.
14. **Add features that are required for Active Directory Certificate Services** window displays. To add a feature, click the **Add Features** button.
15. Click **Next.**
16. Click **Next.**
17. Select the check box for **Certification Authority** from the **Role services** list and click **Next.**
18. Click **Install.**
19. Once installation is complete, select the link **Configure Active Directory Certificate Services** on the destination server. The **AD CS Configuration** wizard displays.
20. In the **Credentials** page of the **AD CS Configuration** wizard, click **Next.**
21. Select the check box for **Certification Authority** and click **Next.**
22. Select **Enterprise CA** as **Setup Type** and click **Next.**
23. Select **Root CA** as the type of CA and click **Next.**
24. Select the radio button for **Use existing private key** and choose the option **Select a certificate and use its associated private key,** and click **Next.**
25. Select the CA certificate that was generated on the first cluster node and click **Next.**
26. Change the default paths for the database and log location to the shared disk and click **Next.**
27. A dialog box displays stating that an existing database was found. Click **Yes** to overwrite.

28. In the **Confirmation page,** click **Configure.**

29. Verify that the CA service has successfully started by running the following command.

›_ PowerShell

```
sc query certsvc
```

6.1.4.5 Installing Failover Cluster Feature on Both the Cluster Nodes

Please execute the following steps on both the cluster nodes:

1. Log in to the cluster node as a user with Administrative privileges.

2. Select **Start** and then **Server Manager** to open **Server Manager.**

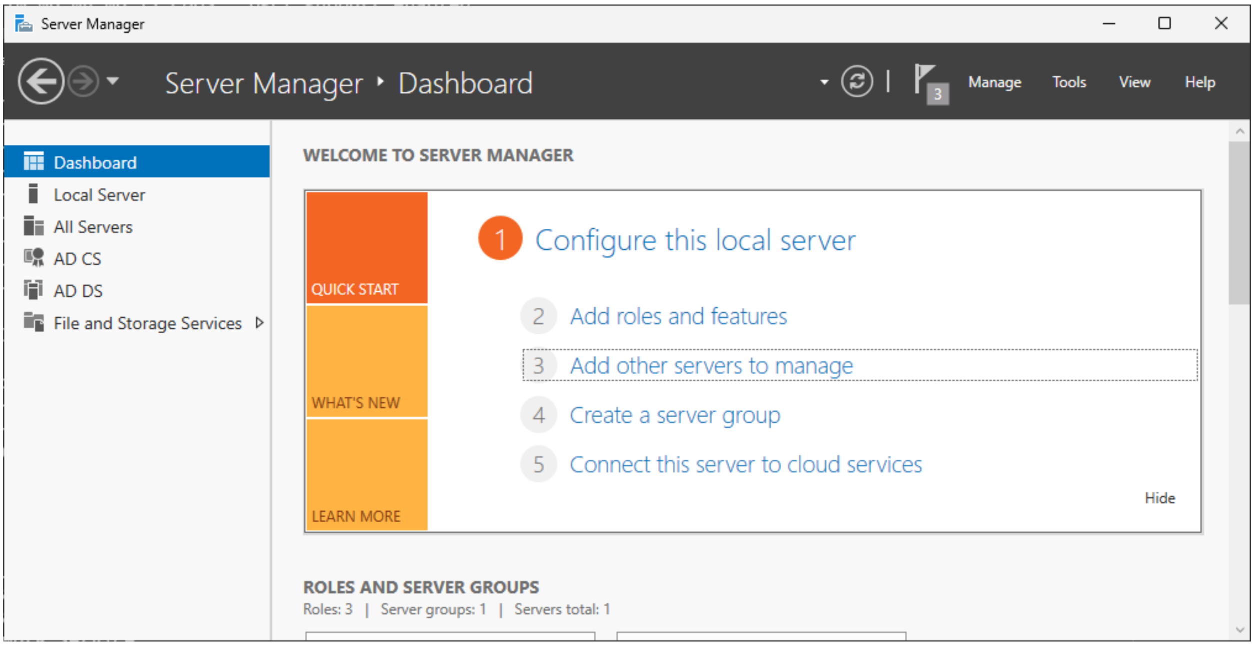

Figure 97 : "Server Manager" Window

3. Under **Configure this Local Server**,click **Add Roles and Features**. The **Add Roles and Features** Wizard displays. Click **Next.**

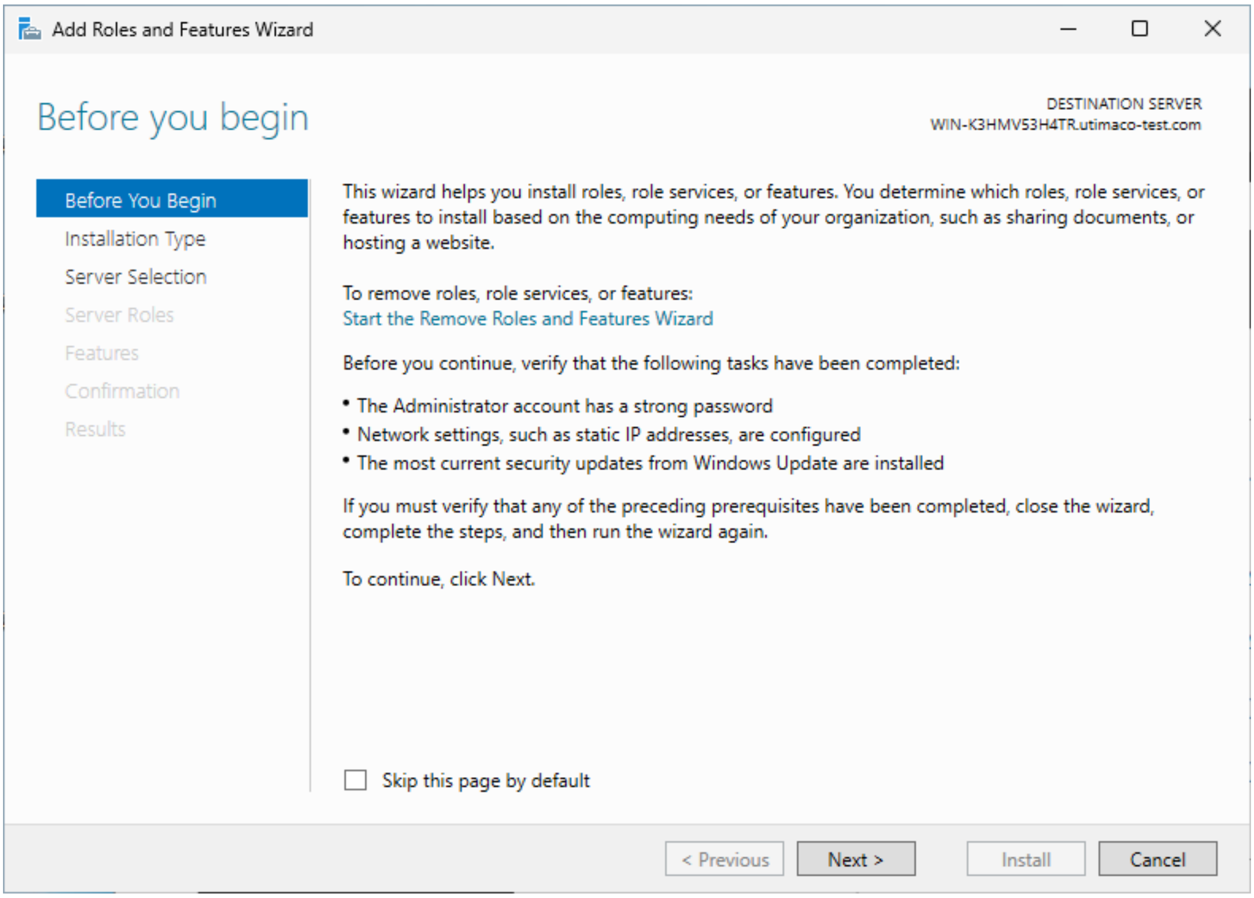

Figure 98 : "Before you begin" Window

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

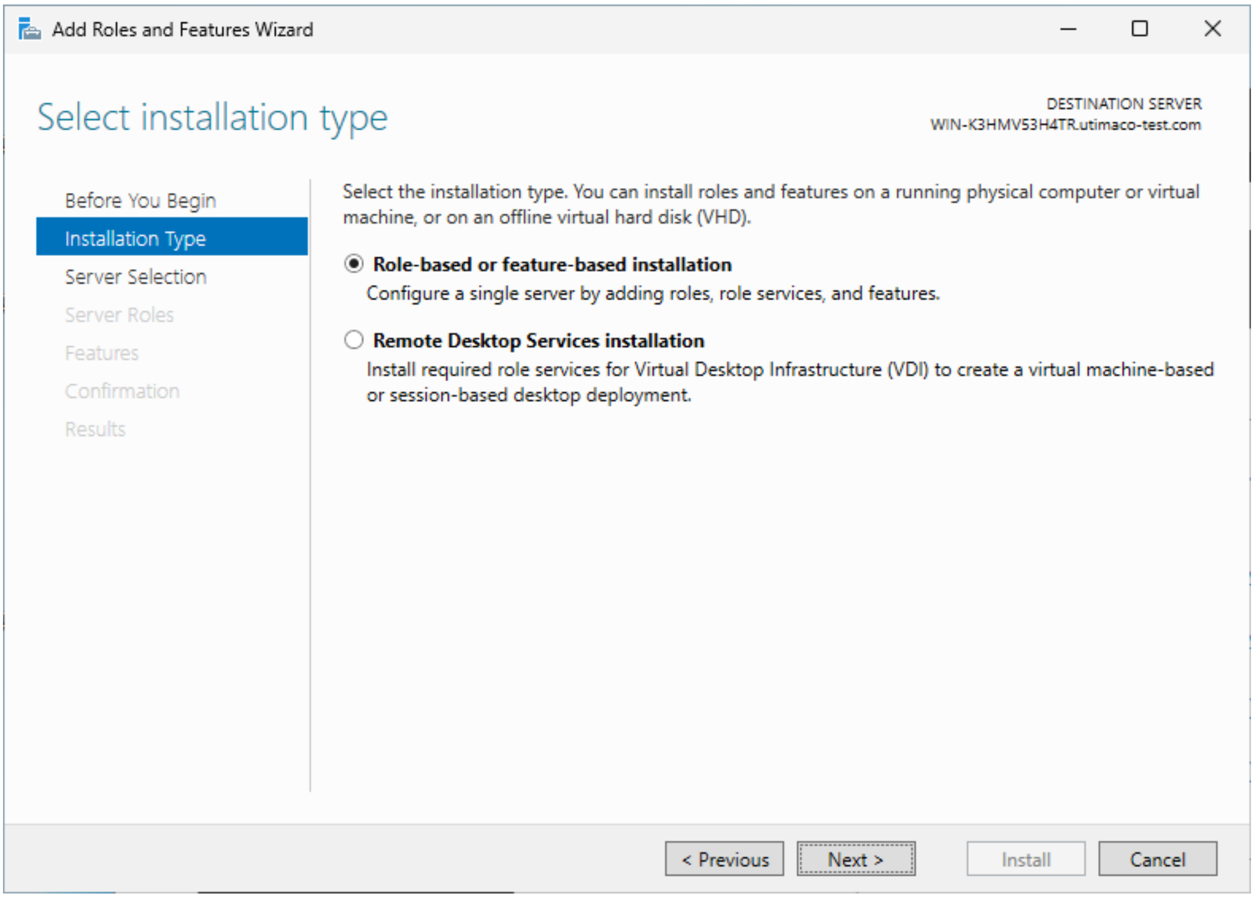

Figure 99 : "Select installation type" Window

5. Select the radio button for **Select a server from the server pool** option, and select the cluster node from the **Server Pool**. Click **Next.**

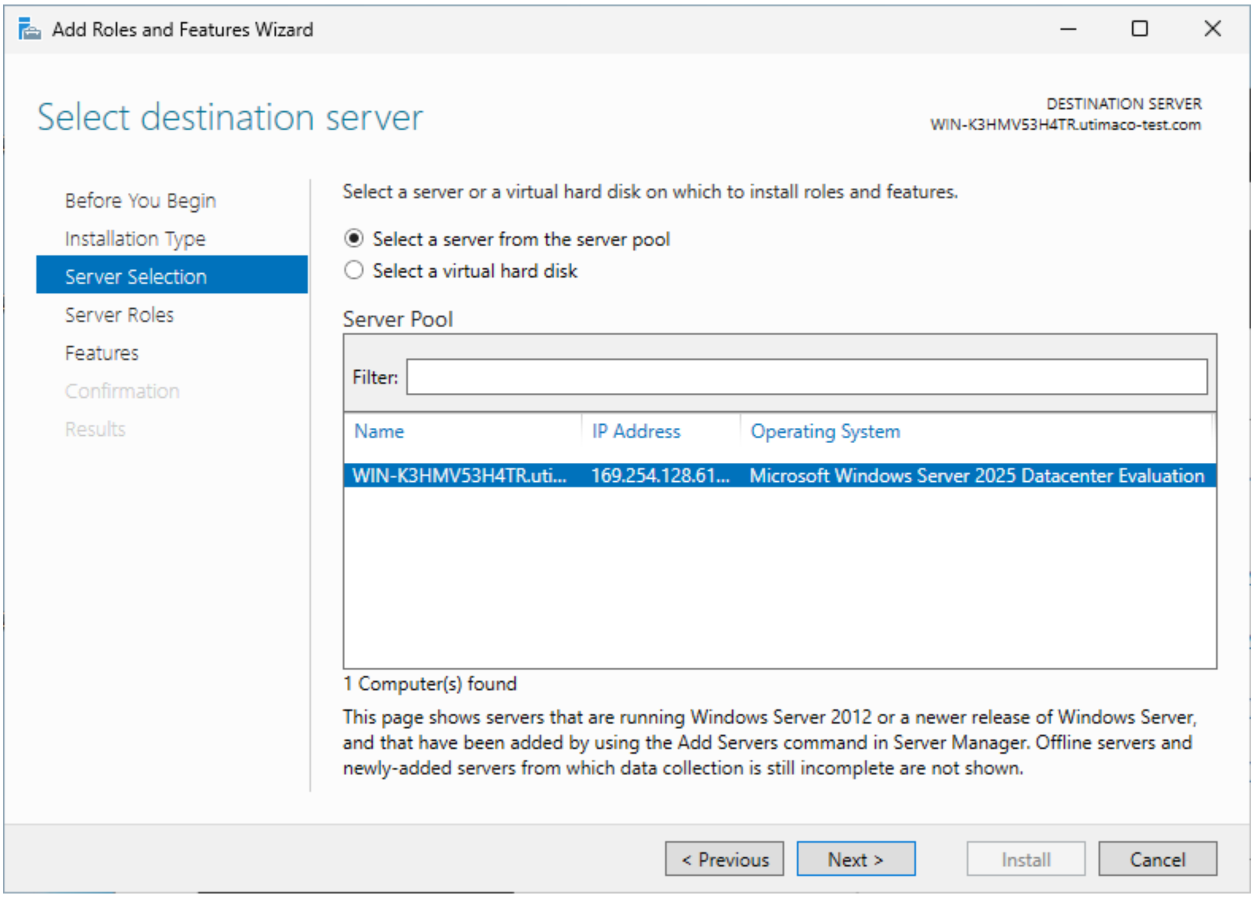

Figure 100 : "Select destination server" Window

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

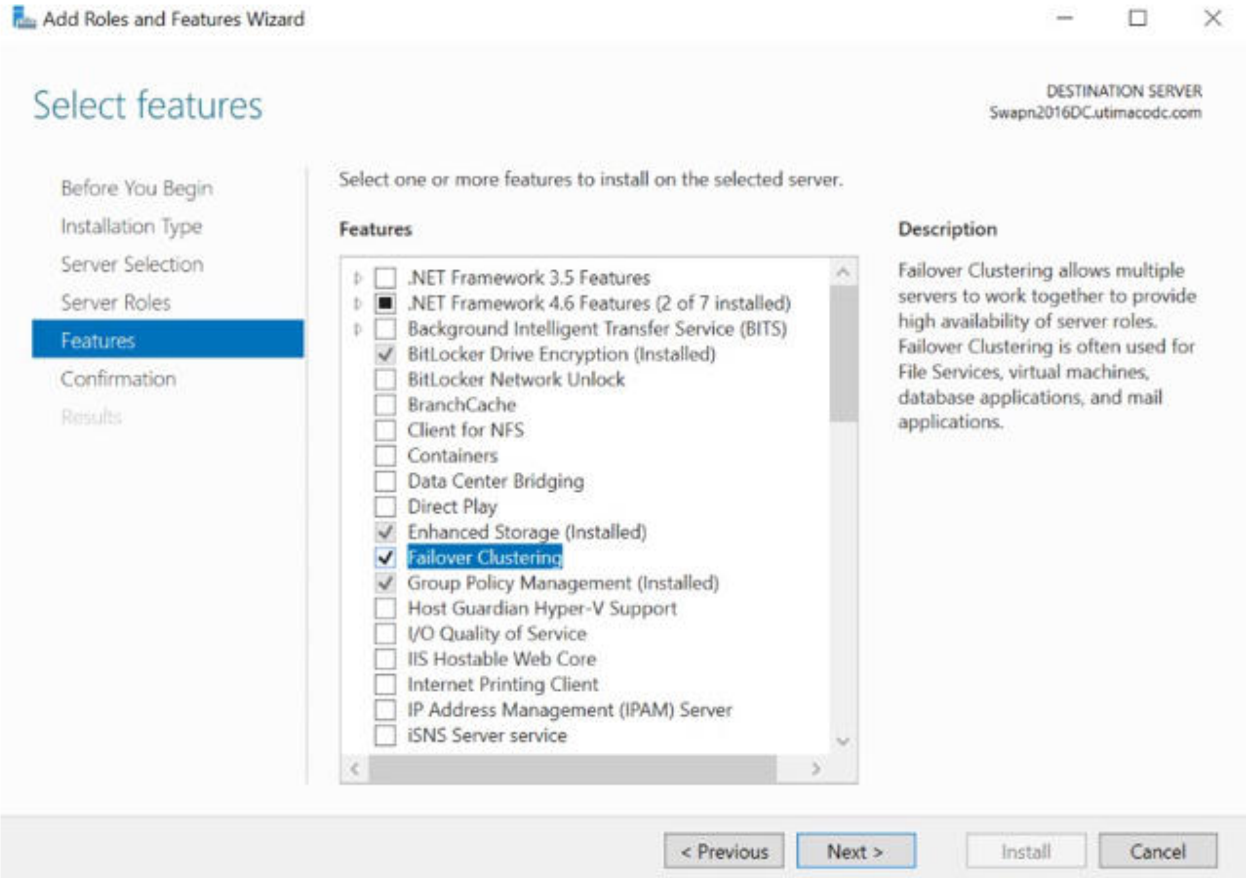

Figure 101 : "Select features" Window

8. A pop-up display stating **Add features that are required for Failover Clustering?** To add a feature, click the **Add Features** button.
9. Click **Next.**
10. Click **Install.**
11. Once Feature installation is complete, click **Close.**

6.1.4.6 Create a Failover Cluster

1. Log in to cluster node as a user with Administrative privileges where disk is attached.
2. Open **Server Manager**, Select **Tools,** and select **Failover Cluster Manager.**

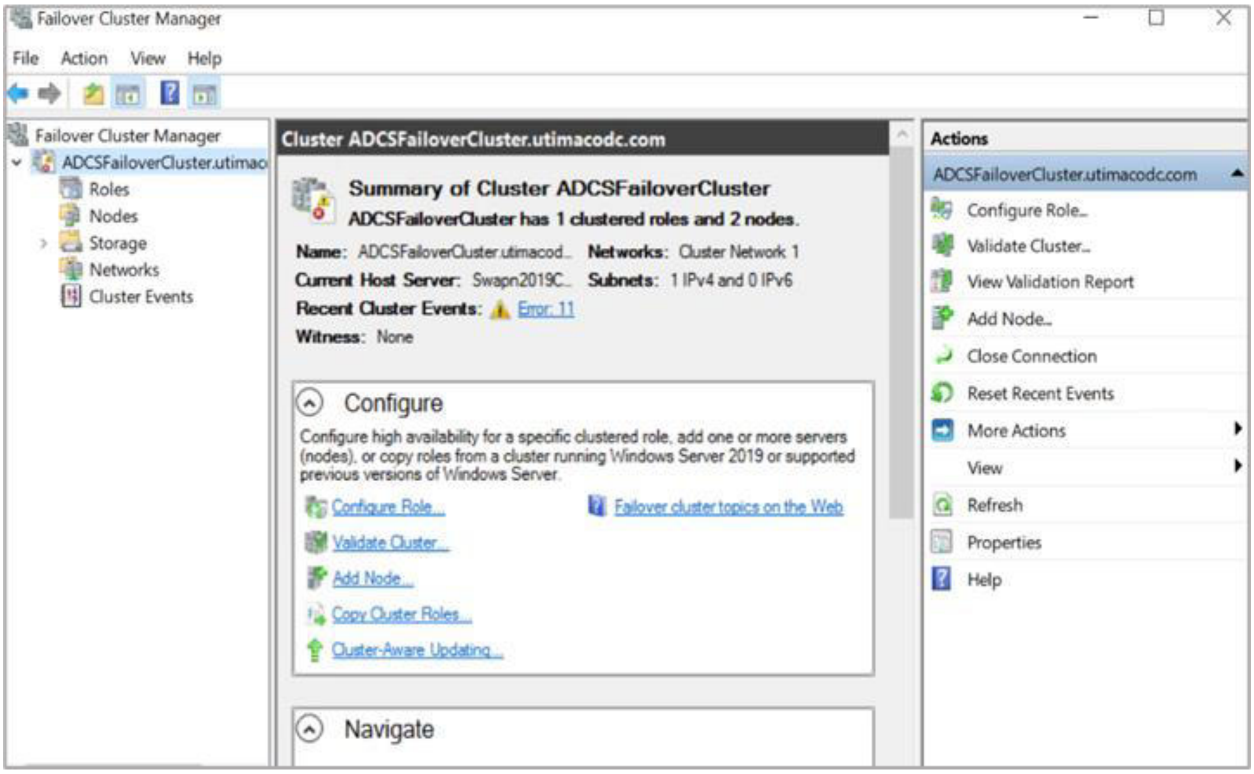

Figure 102 : "Failover Cluster Manager"indow

3. From the **Actions** menu, click **Create a Cluster.**

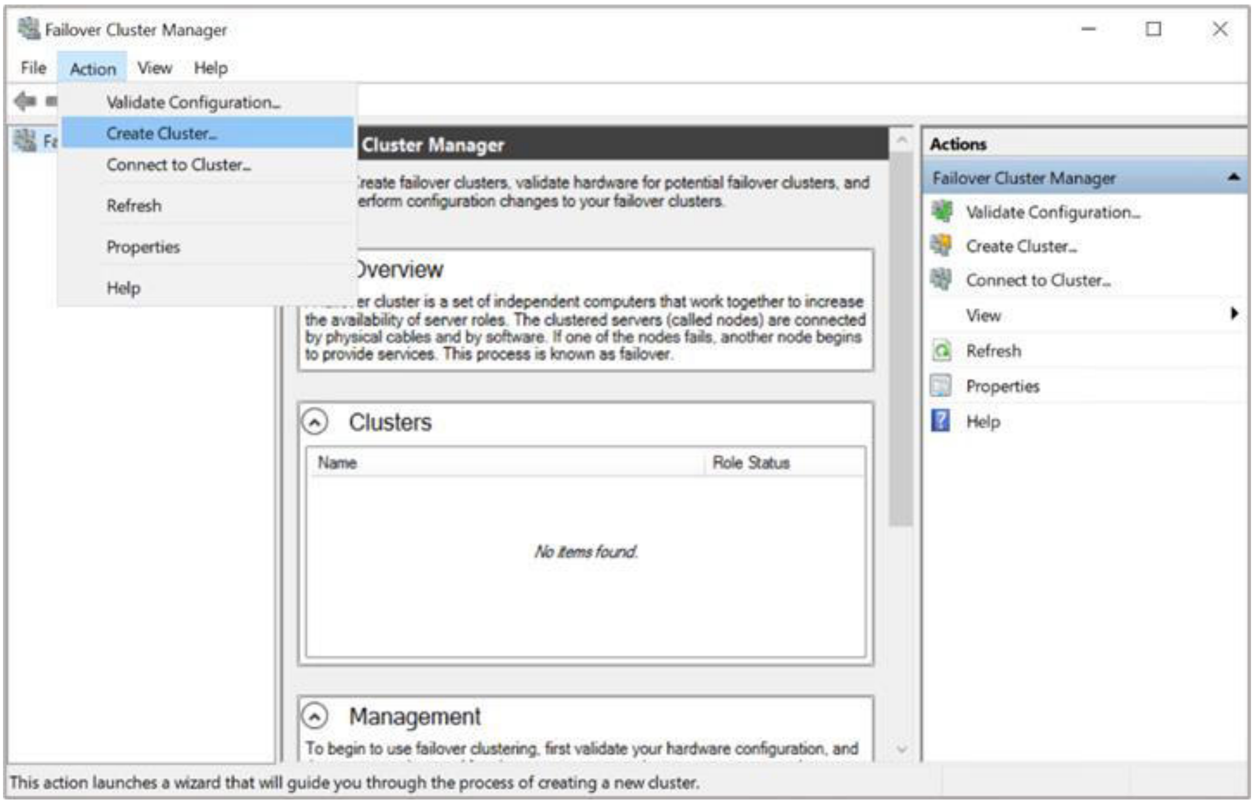

Figure 103 : "Failover Cluster Manager" Window

4. On the **Before You Begin** page, click **Next.**

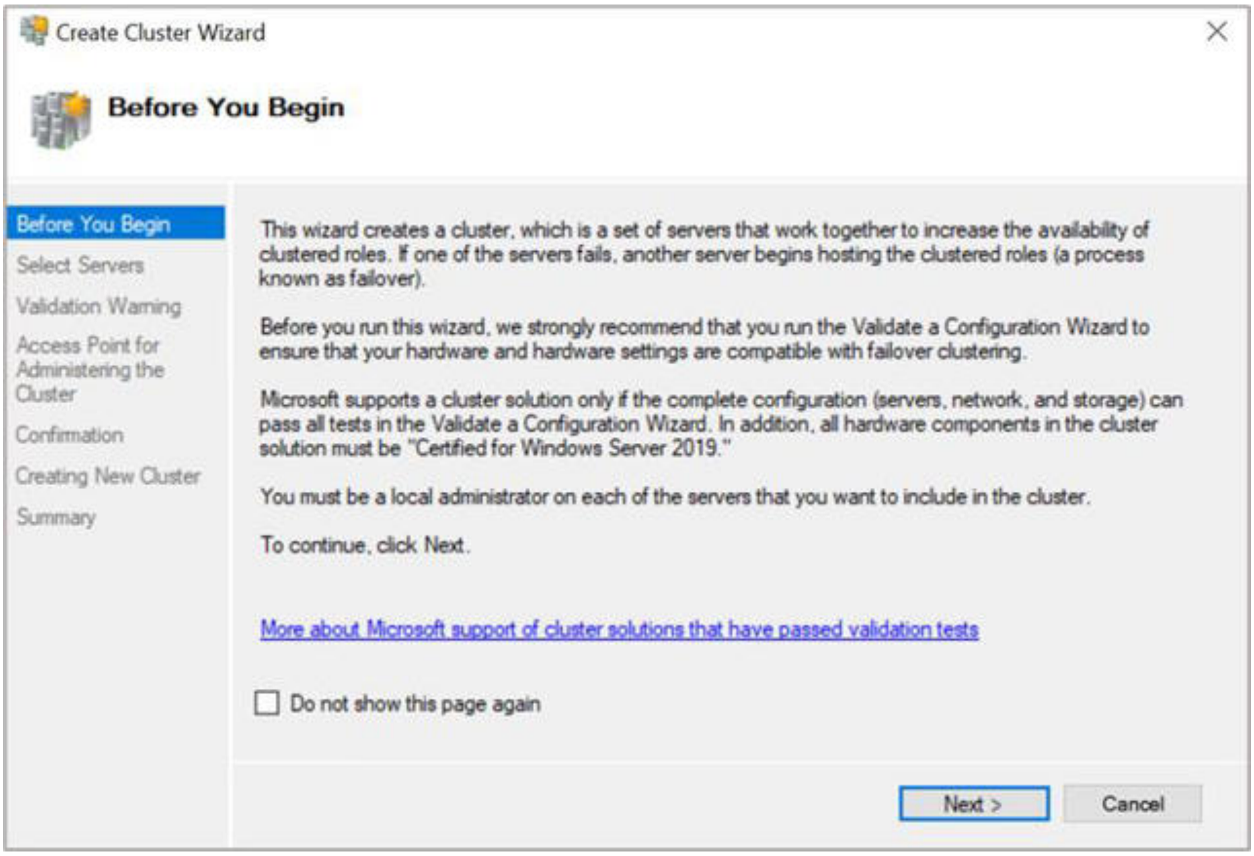

Figure 104 : "Before You Begin" Window

5. Enter the first cluster node name in the **Enter Server Name** field and click **Add.**
6. Enter the second cluster node name in the **Enter Server Name** field and click **Add.**
7. Click **Next.**
8. Enter the **Cluster Name** and click **Next** until you reach the **Summary** page.
9. To perform the validation tests, choose **Yes** and click **Next** two times.
10. Keep the default option to **Run all tests** and click **Next** two times.
11. Verify the test report and click **Finish.**
12. Provide the cluster name and click **Next** until you reach the **Summary** page.

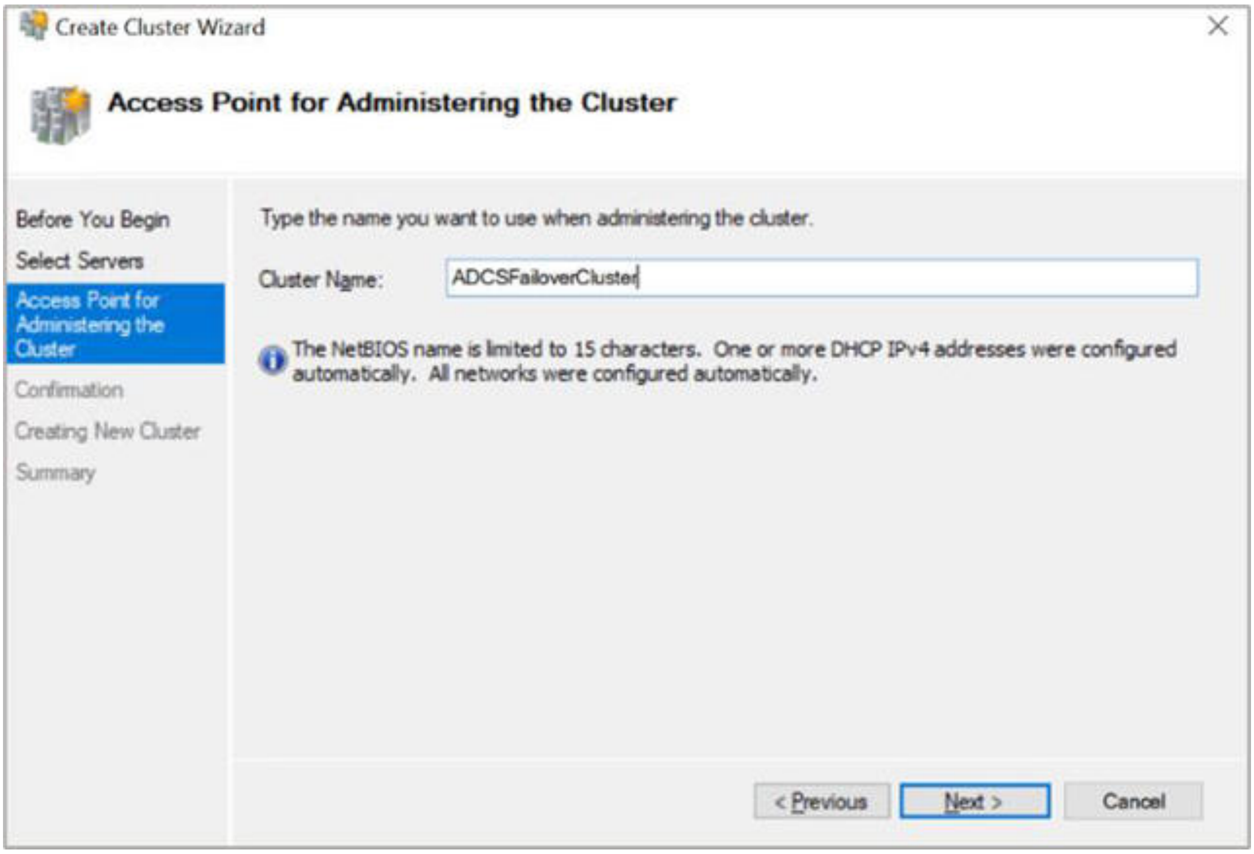

Figure 105 : "Access Point for Administering the Cluster" Window

13. Verify the cluster got configured successfully. Check the status of both nodes, disk, and network. It should be in green.

6.1.4.7 Configure Role for ADCS Failover

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.**

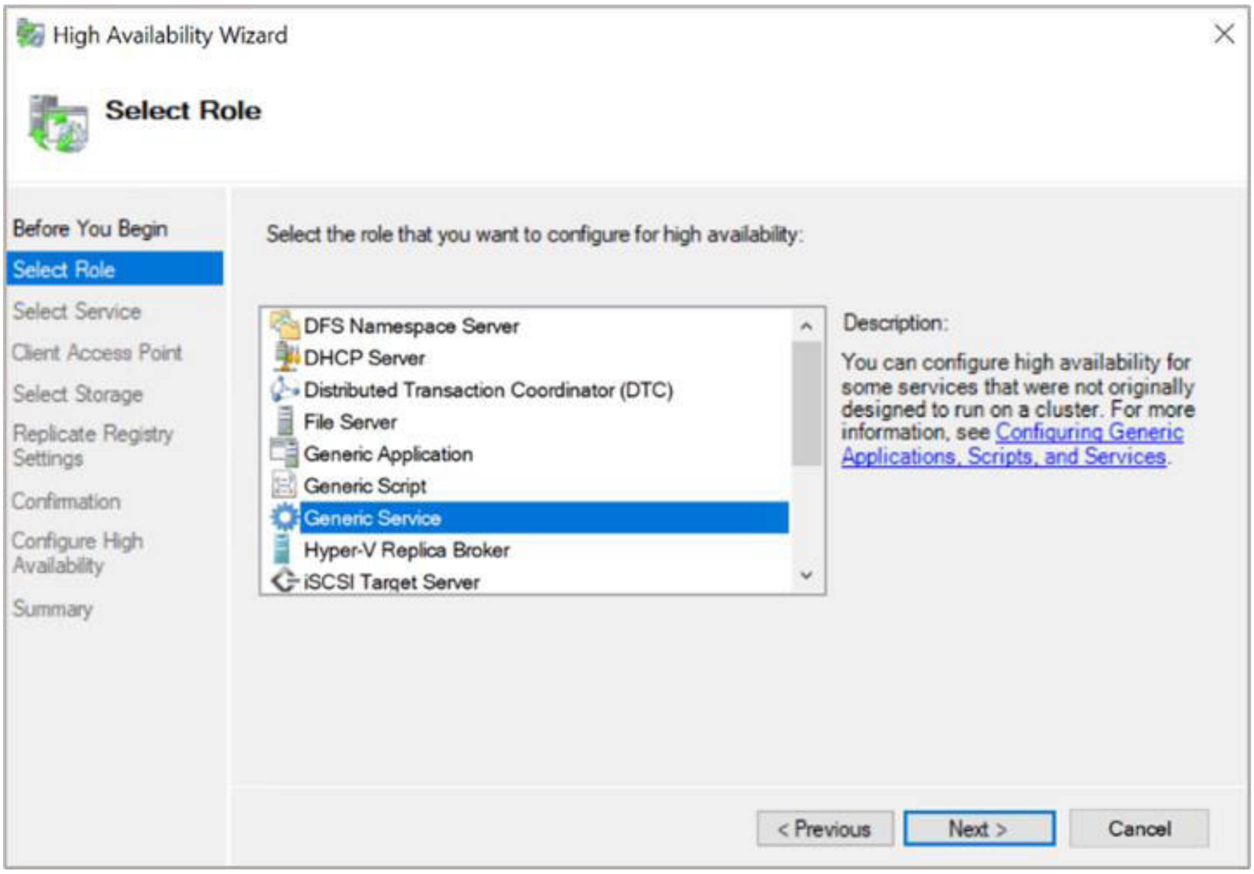

Figure 106 : "Select Role" Window

4. From the service list, select **Active Directory Certificate Services** and click **Next.**
5. On the **Client Access Point** page, enter the role name in the **Name** field and click **Next.**

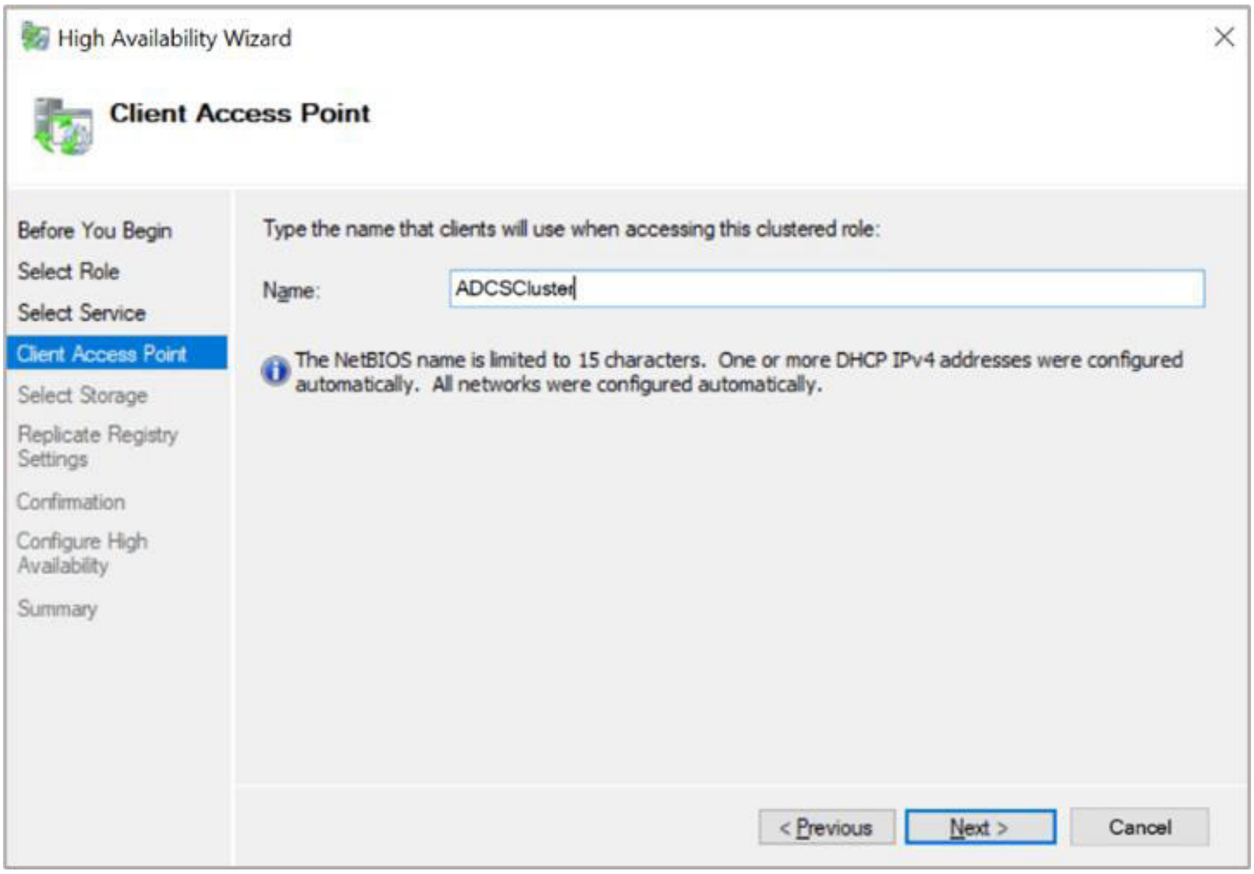

Figure 107 : "Client Access Point" Window

6. Select the disk storage that is still mounted to the node and click **Next**.
7. Configure a shared registry hive, select the **Add button**, enter `SYSTEM\CurrentControlSet\Services\CertSvc` and click **OK**.

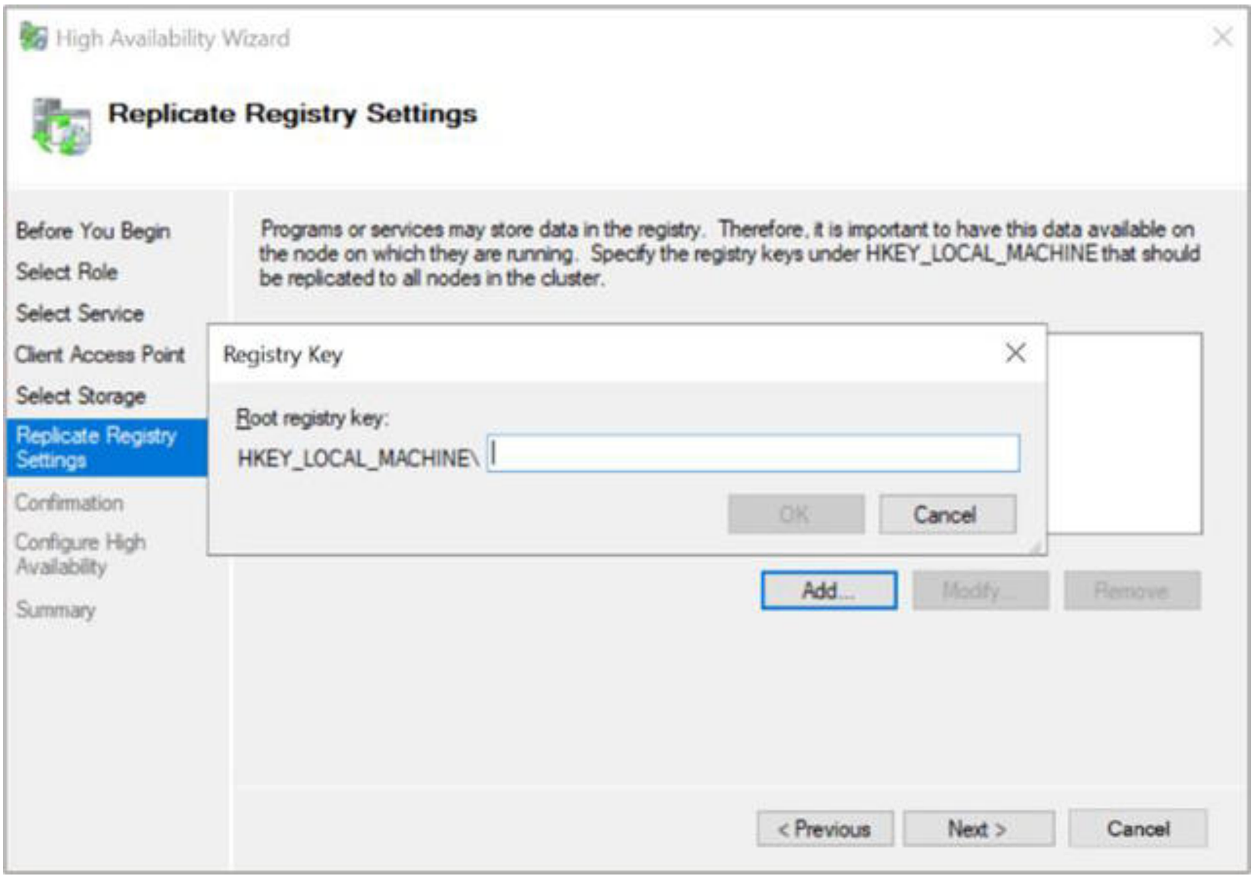

Figure 108 : "Replicate Registry Settings" Window

8. Click **Next** on the **Confirmation** page.
9. Click **Finish** to complete the failover role configuration.
10. Open the **Failover Cluster Manager** and verify that the newly created **Roles Status** is in the **Running** state and **Green.**
11. The **AD CS Failover** was configured successfully. At this stage, you can move the certification authority between all nodes.

6.1.4.8 Creating the CRL Objects in Active Directory

The CRL container must be created in the Active Directory manually, and the CRL must be published manually.

1. Log on to the active cluster node with enterprise permissions.

2. On the command prompt, type the following commands.

›_ Console

```
> cd %WINDIR%\System32\CertSrv\CertEnroll
> certutil -f -dspublish {CRLfile}

For example:
> certutil -f -dspublish "CA Cluster.crl"
```

6.1.4.9 Updating the CA Configuration in Active Directory

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

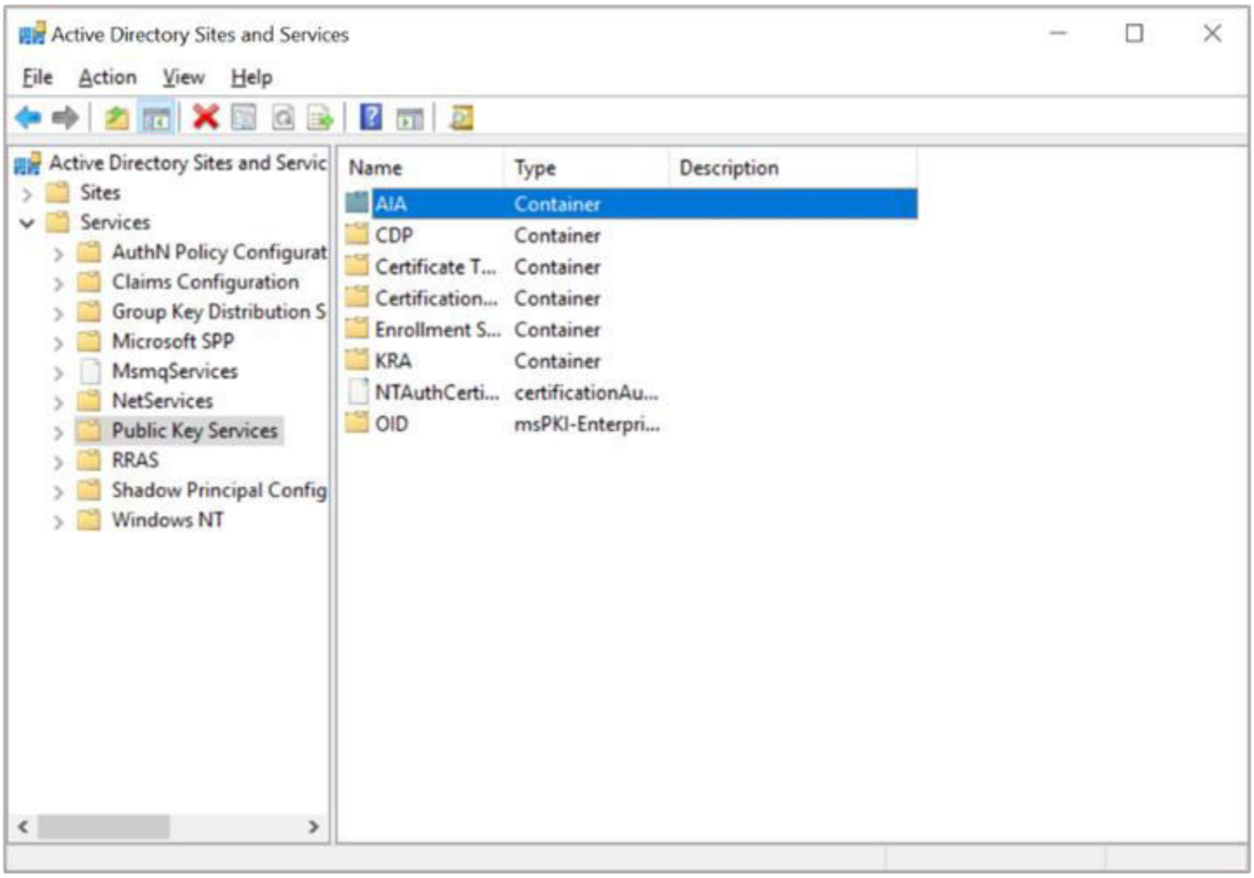

Figure 109 : "Active Directory Sites and Services" Window

6. In the middle pane, select the CA name as it shows in the Certification Authority MMC Snap-in.
7. In the **Action** menu, select **Properties.**
8. Click **Security.**
9. Click **Add.**
10. Select **Object Types,** then select **Computers**, and then click **OK.**
11. Type the computer name(s) of the other cluster node(s) as the object name and click **OK.**
12. Make sure that the computer accounts of all cluster nodes have **Full Control** permissions.
13. Click **OK.**
14. All cluster nodes also have to be permitted on the Enrollment Services container.
15. In the left pane, select **Enrollment Services**.

16. In the middle pane, select the **Certificate Authority** name.
17. In the **Action** menu, select **Properties**. Select the **Security** tab and click **Add...**
18. Select **Object Types**, select **Computers,** and click **OK.**
19. Type the computer name(s) of the all-cluster node(s) as the object name.
20. Make sure that the computer accounts of all cluster nodes have **Full Control** permissions.
21. Click **OK.**
22. In the left pane, select **KRA.**
23. In the middle pane, select the **Certificate Authority** name.
24. In the **Action** menu, select **Properties,** then select the **Security** ta,b and click **Add.**
25. Select **Object Types**, select **Computers,** and then click **OK.**
26. Type the computer name of all cluster nodes as object names and click **OK.**
27. Make sure that the computer accounts of all cluster nodes have **Full Control** permissions.
28. Click **OK.**

6.1.5 Online Certificate Status Protocol Service

Before integrating the Utimaco CryptoServer with Microsoft Windows Server Online Certificate Status Protocol Service (OCSP), first complete the **Utimaco CSP/CNG Installation**.

> It is strongly recommended to use the external key storage for OCSP if using HSMs in cluster mode. Therefore, the servers that serve OCSP should be separated from the certificate authorities.

You can install OCSP if you are already running an enterprise certificate authority. The following steps are necessary to install OCSP in general:

- Prepare certificate template for OCSP signing
- CA Configuration
- Install and configure the online responder
- Make a revocation configuration

- Test the online responder

6.1.5.1 Prepare Certificate Template for OCSP Signing

First, it is necessary to prepare a template to enroll OCSP servers for a certificate which uses the Utimaco CryptoServer.

1. Open the command prompt and run the `certtmpl.msc` command.
2. Right-click the **OCSP Response Signing** template and click **Duplicate Template.**
3. Selectthe appropriate Windows version under **Certificate Authority** and **Certificate Recipient** drop-down box under **Compatibility Settings.**
4. Click **OK.**

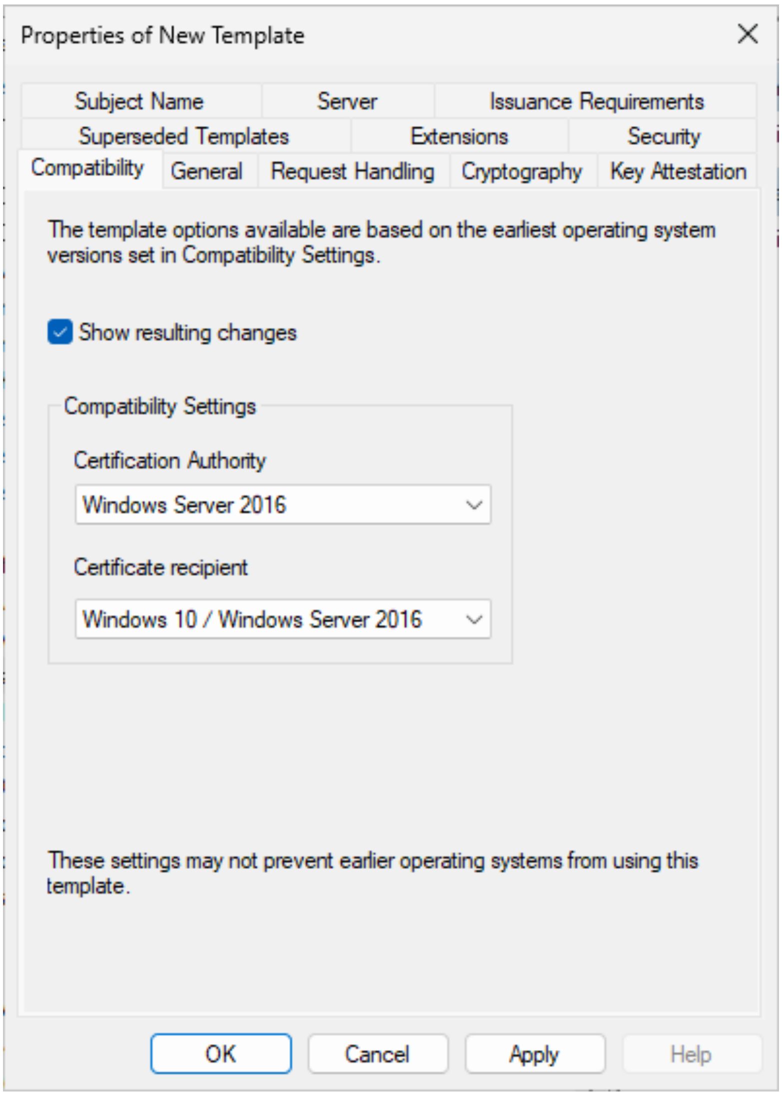

Figure 110 : "Compatibility Tab" Window

5. In the **Resulting Changes** menu, click **OK.**

6. Go to the **General** tab and enter a name for the template.

7. Select the **Subject Name** tab.

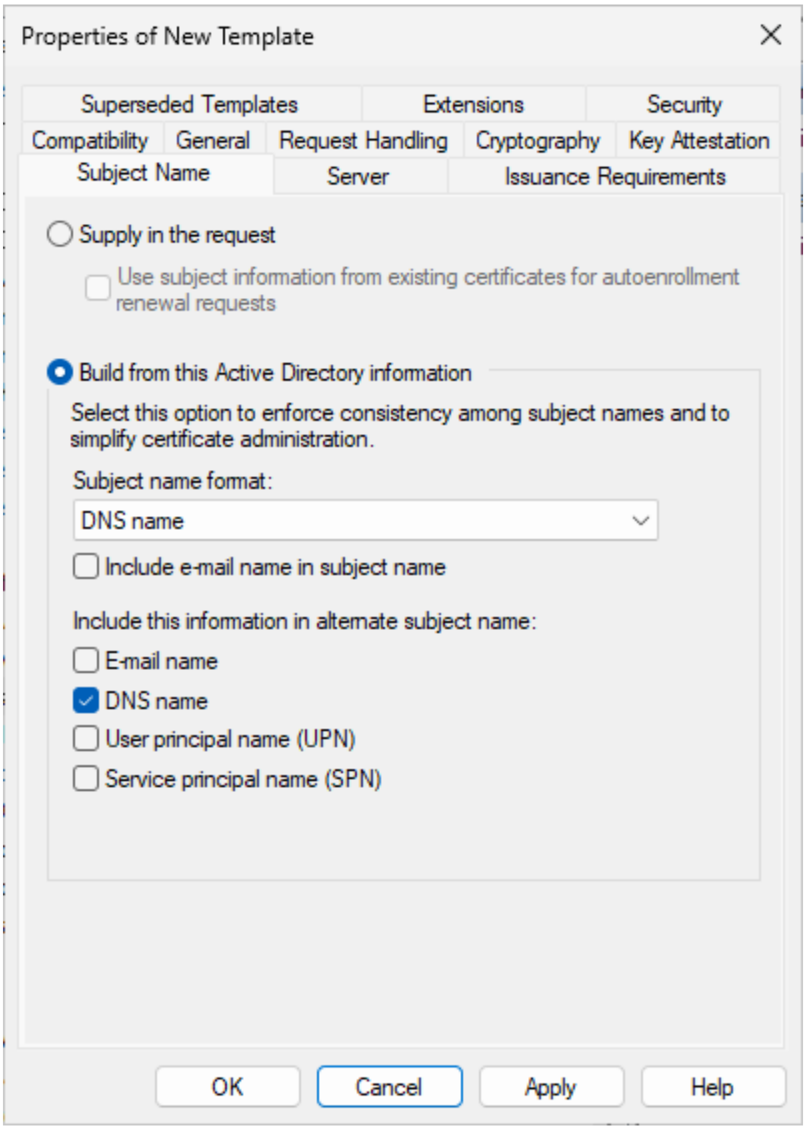

Figure 111 : "Subject Name Tab" Window

8. Uncheck the **Include e-mail name in subject name** checkbox.
9. Uncheck the **E-mail name** checkbox.
10. In the **Request Handling** tab, select the **Purpose as Signature** from the drop-down list. Select **Authorize additional service accounts to access the private key** checkbox.

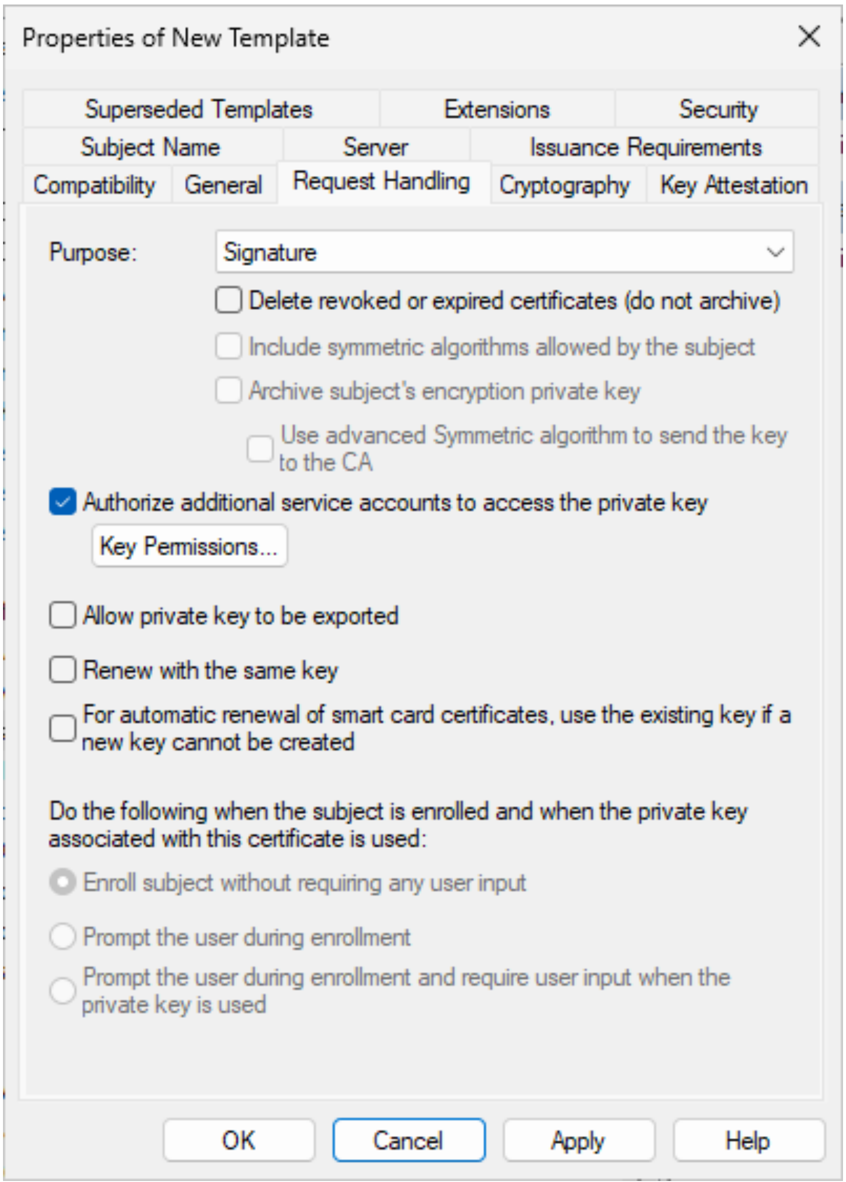

Figure 112 : "Request Handling" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

11. Go to the **Cryptography** tab, select **Key Storage provider** in the **Provider category,** then select **Algorithm name,** then **Key Size**. Check the radio button for **Request must use one**

of the following providers, then selectthe radio button for **Utimaco CryptoServer Key storage provider**, and select the appropriate **Hash Value**.

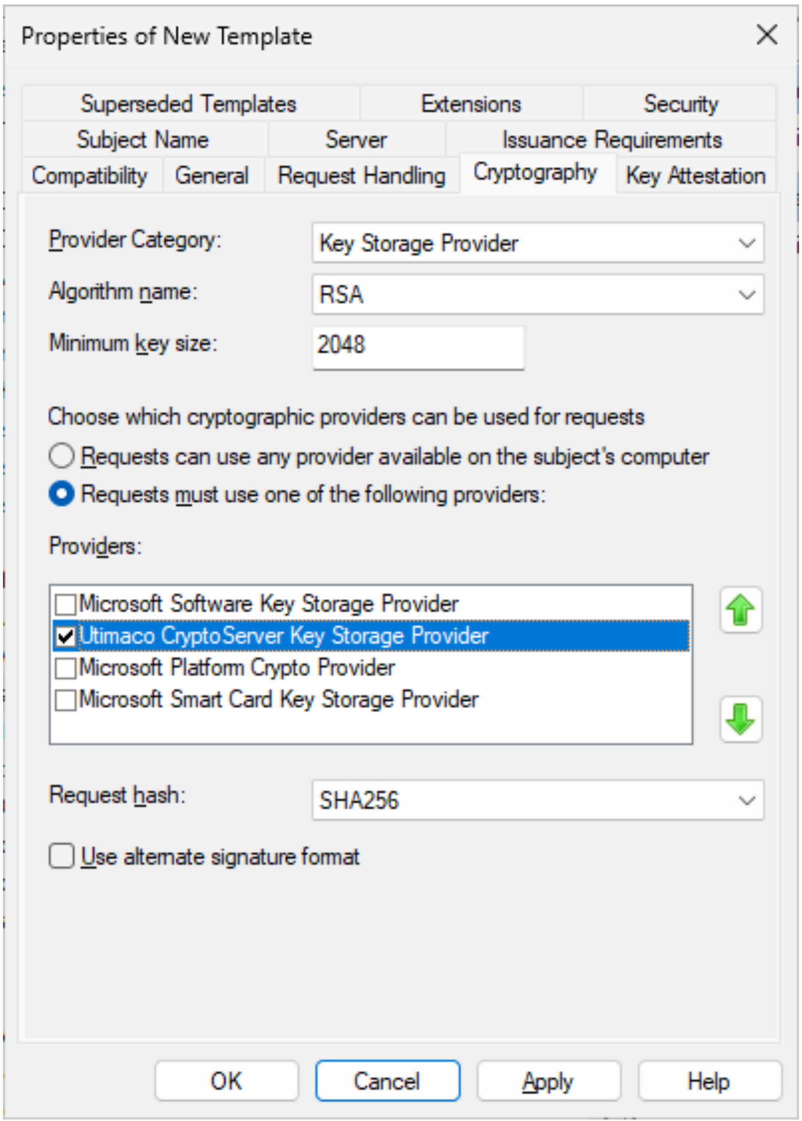

Figure 113 : "Cryptography Tab" Window

12. Go to the **Security** Tab. Add the **Computer Account** and give **Read, Write and Enroll** permissions. Ensure Domain Admins and Enterprise Admins have **Enroll Permissions.**
13. Click **Apply** and then click **OK.**
14. Open the command prompt and run the `certsrv.msc` command.

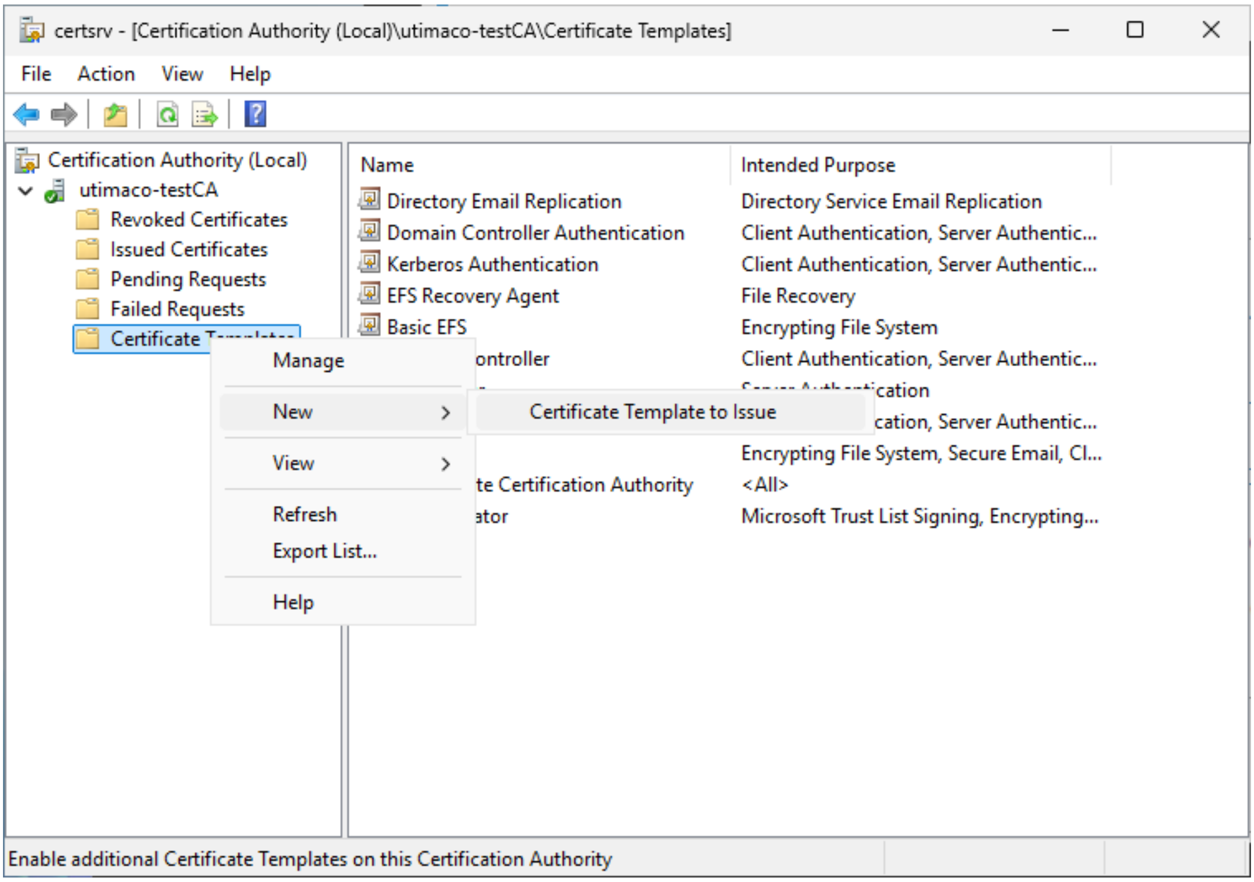

Figure 114 : "Certificate Authority" Window

15. Right-click the **Certificate Templates** node.
16. Select **New,** then select **Certificate Template to Issue.**
17. Select a new template for OCSP Response Signing, and click **OK.**

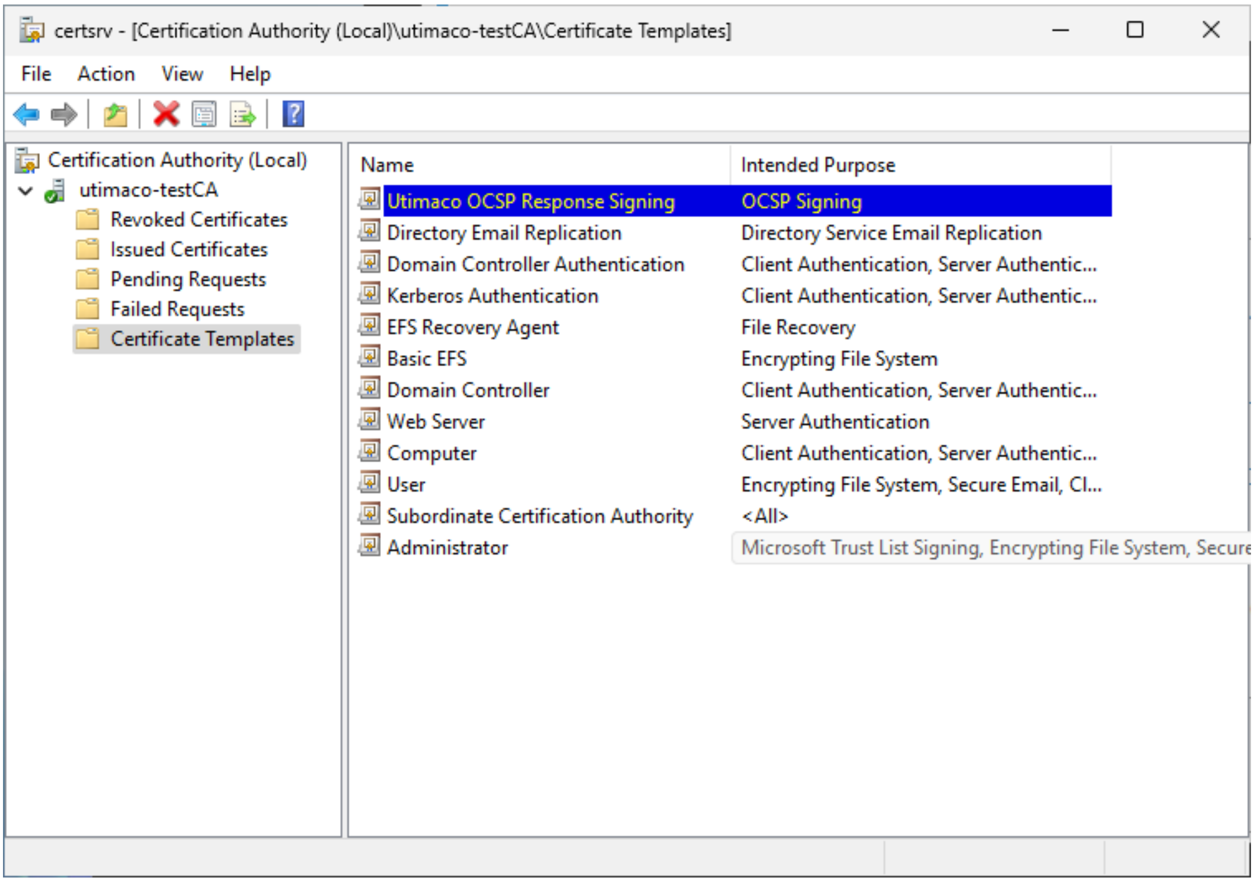

Figure 115 : "Certificate Authority" Window

6.1.5.2 CA Configuration

Some more steps are necessary to use OCSP with a CA. Perform the next steps on the CA server.

1. Open the command prompt and run the `certsrv.msc` command.
2. Right-click Certificate Authority Name and select **Properties.**

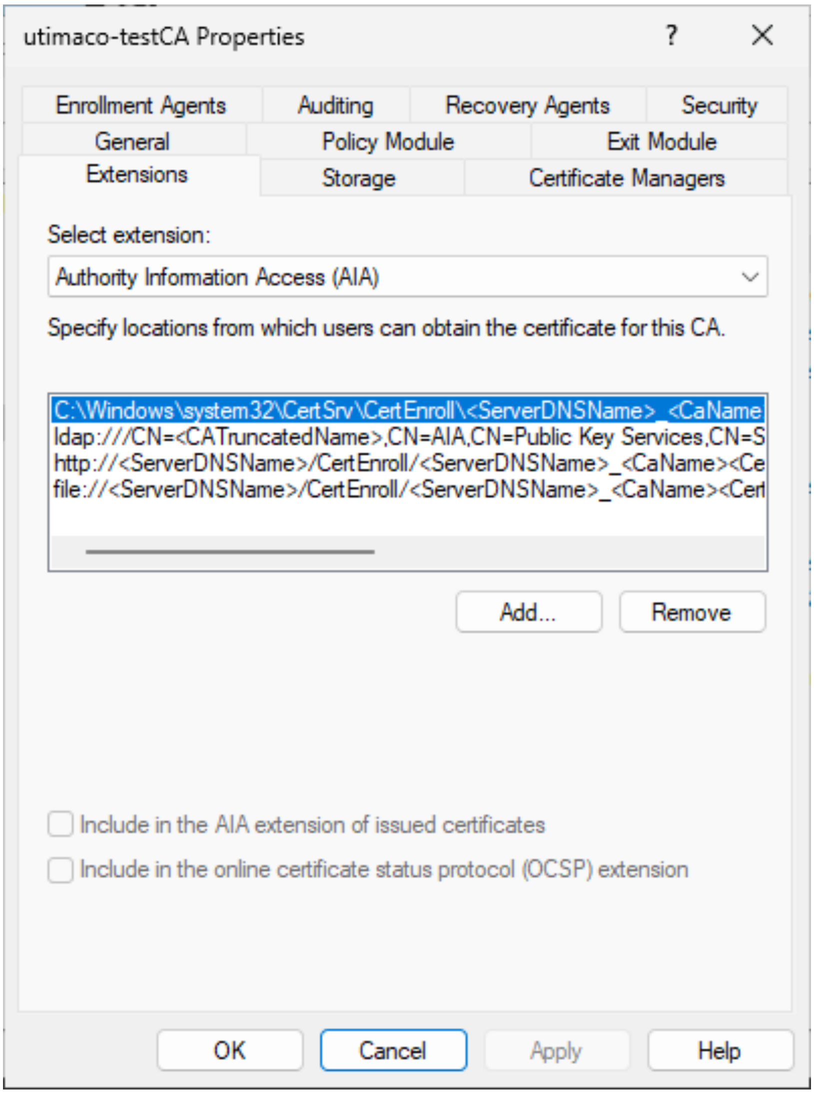

Figure 116 : "Extensions Tab" Window

3. Change to the **Extensions** tab and select **Authority Information Access (AIA)**. Add the URL of the OCSP service. Typically, this is the FQDN of the OCSP server with the path OCSP, e.g., http://FQDN-OF-SERVER/ocsp. Click **OK**. After adding, select the URL previously entered, select **Include in the online certificate status protocol (OCSP) extension**. Click **Apply** and then click **OK.**
4. You will receive a pop-up window to restart the AD CS, for the changes to take effect. Click **Yes** and click **OK.**

6.1.5.3 Request a Certificate from OCSP Response Signing Template

1. Select the Start menu, open Run, type `mmc`, and click **OK.**
2. In the mmc console that appears, select **File,** then select **Add/Remove Snap-in...**
3. In the **Add or Remove Snap-Ins** pop-up dialog that appears, find the **Certificates** snap-in (under the **Available snap-ins** section).

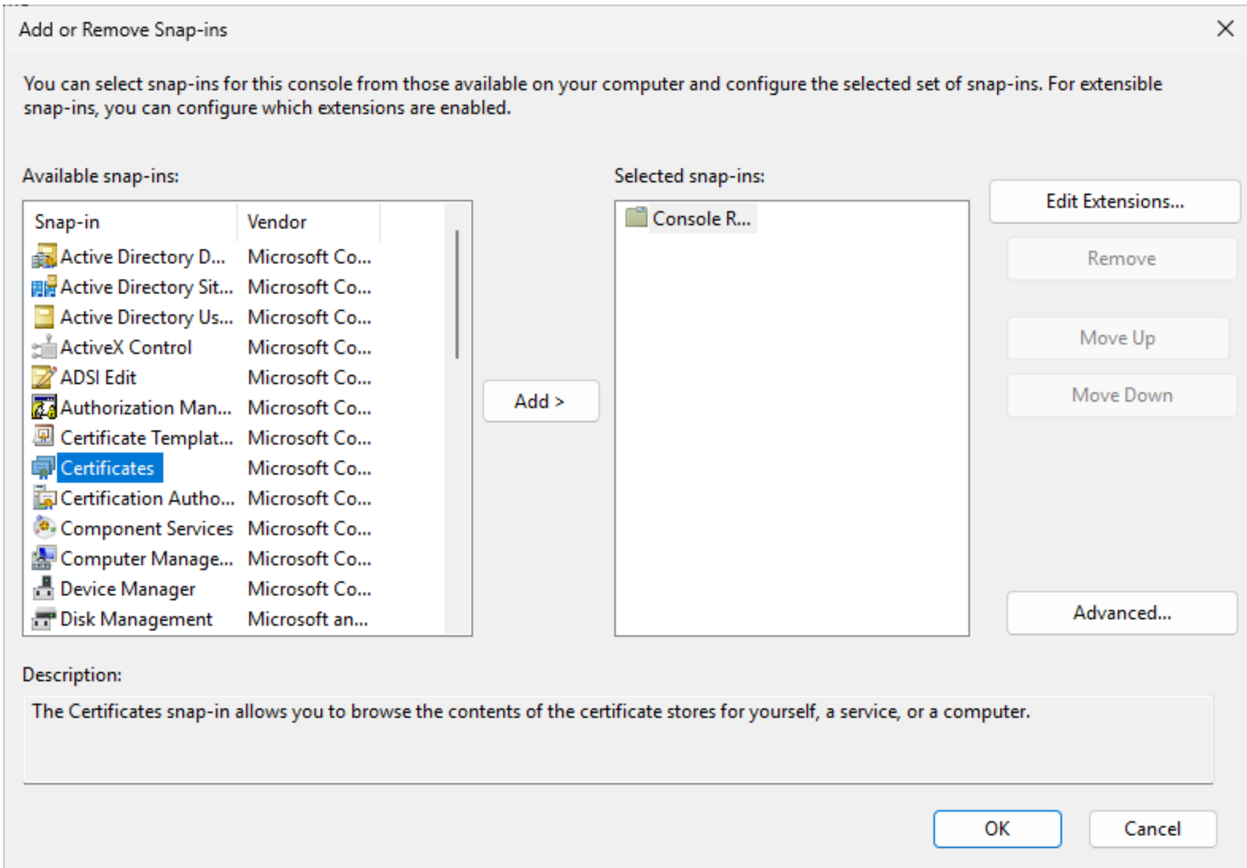

Figure 117 : "Add/Remove Snap-in" Window

4. Select the snap-in and click **Add.**
5. In the dialog that appears, select the radio button for **Computer Account** and then click **Next.**

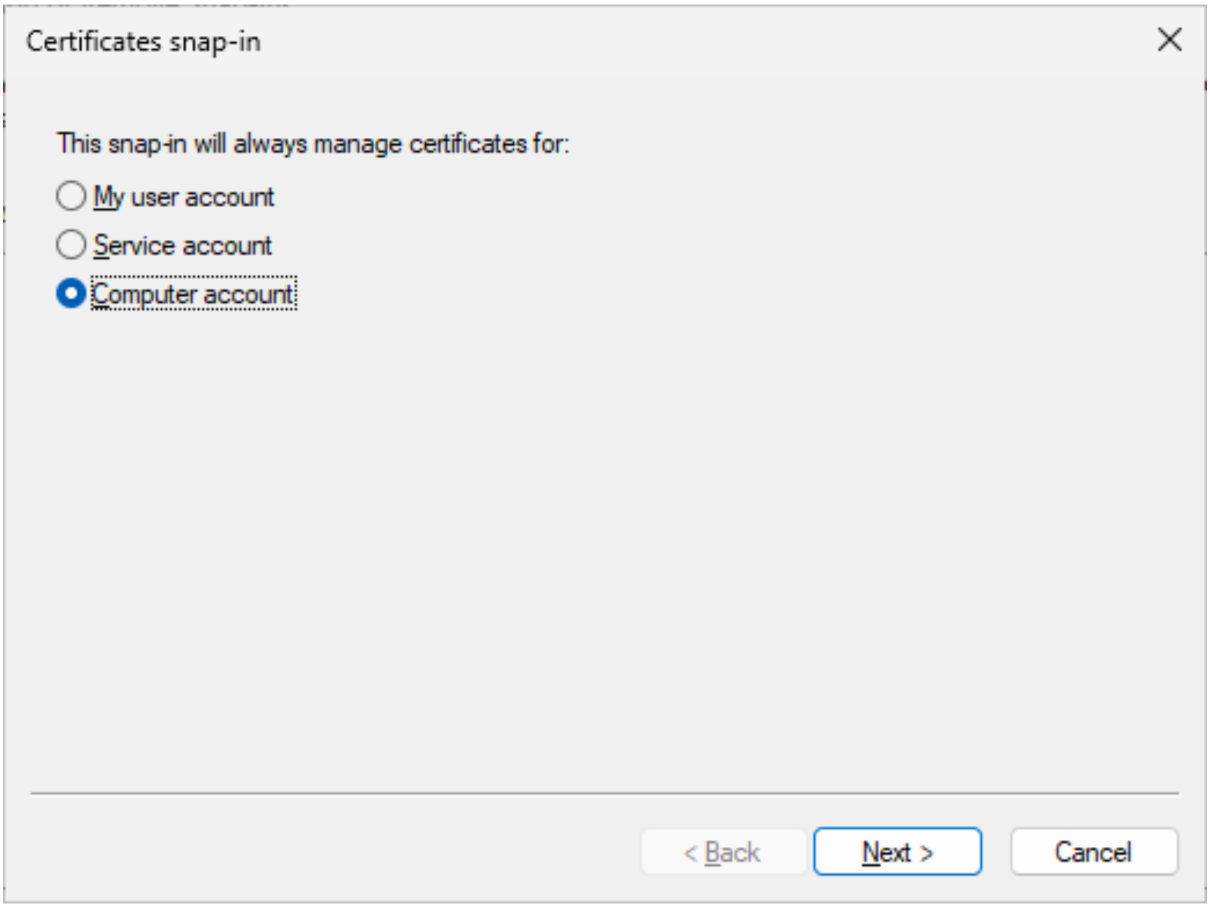

Figure 118 : "Certificate Snap-in" Window

6. In the **Select Computer** dialog, ensure that **Local Computer** is selected and click **Finish.**

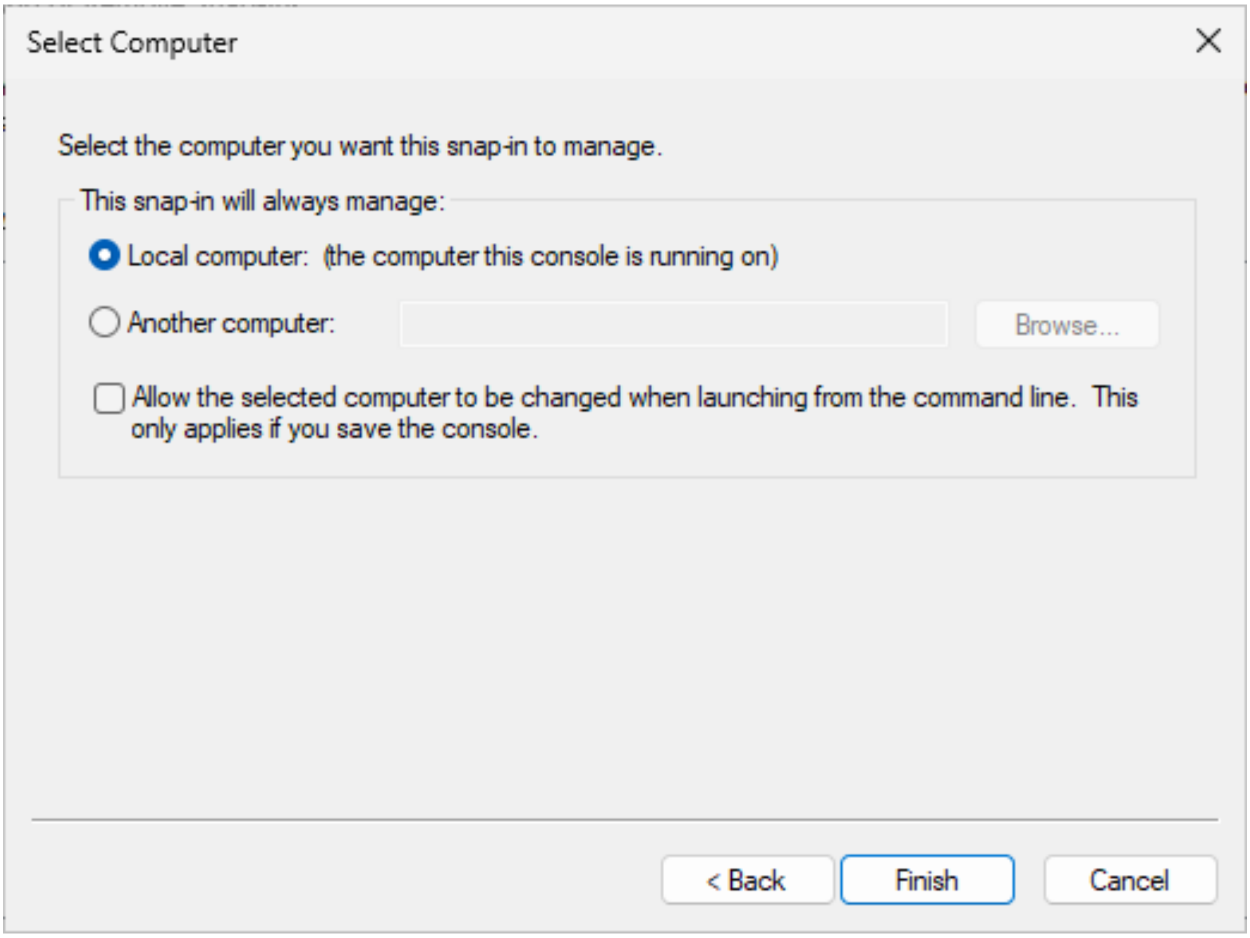

Figure 119 : "Select Computer" Window

7. Click **OK.**
8. Under the **Console Root**, select the **Certificates** heading.
9. Select the **Personal** folder and expand it.
10. Right-click on **Certificates** and select **All Tasks,** and select **Request New Certificate.**

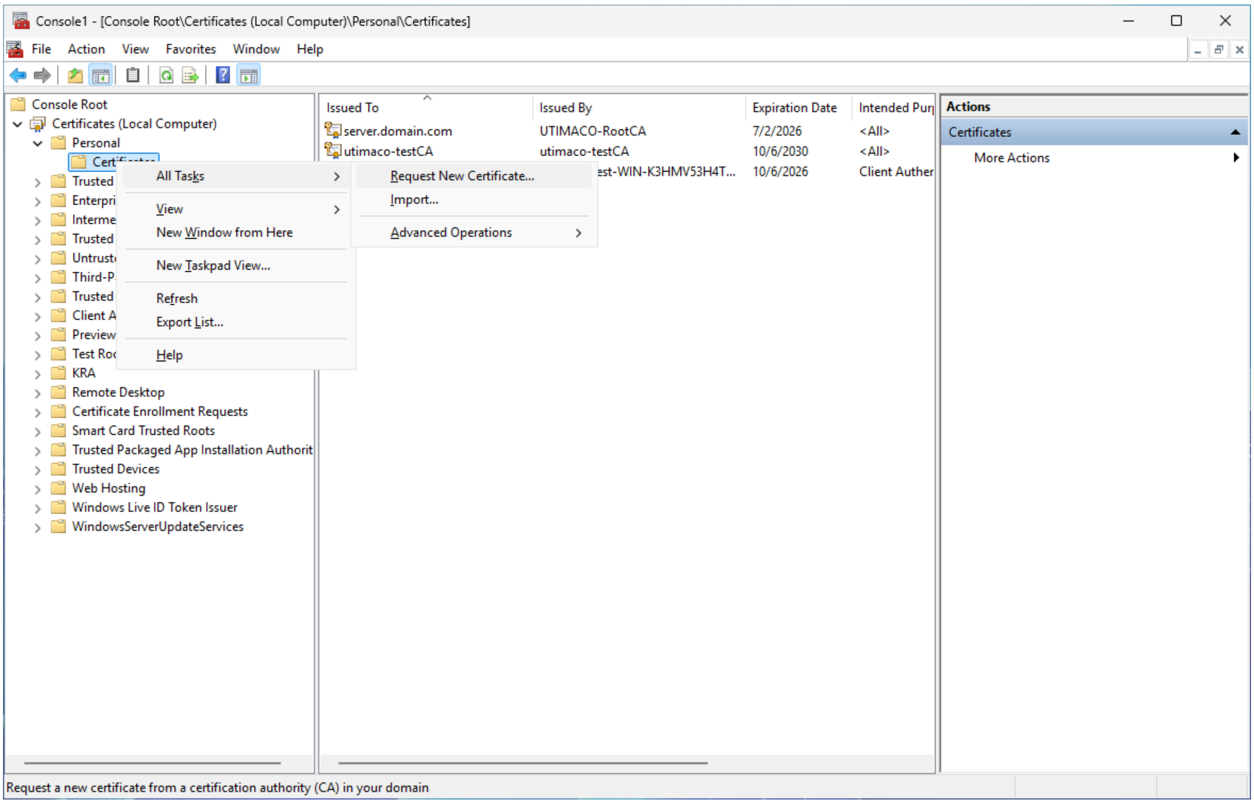

Figure 120 : "Console" Window

11. On the **Before You Begin** page, click **Next.**
12. On the **Select Certificate Enrollment Policy** page, click **Next.**

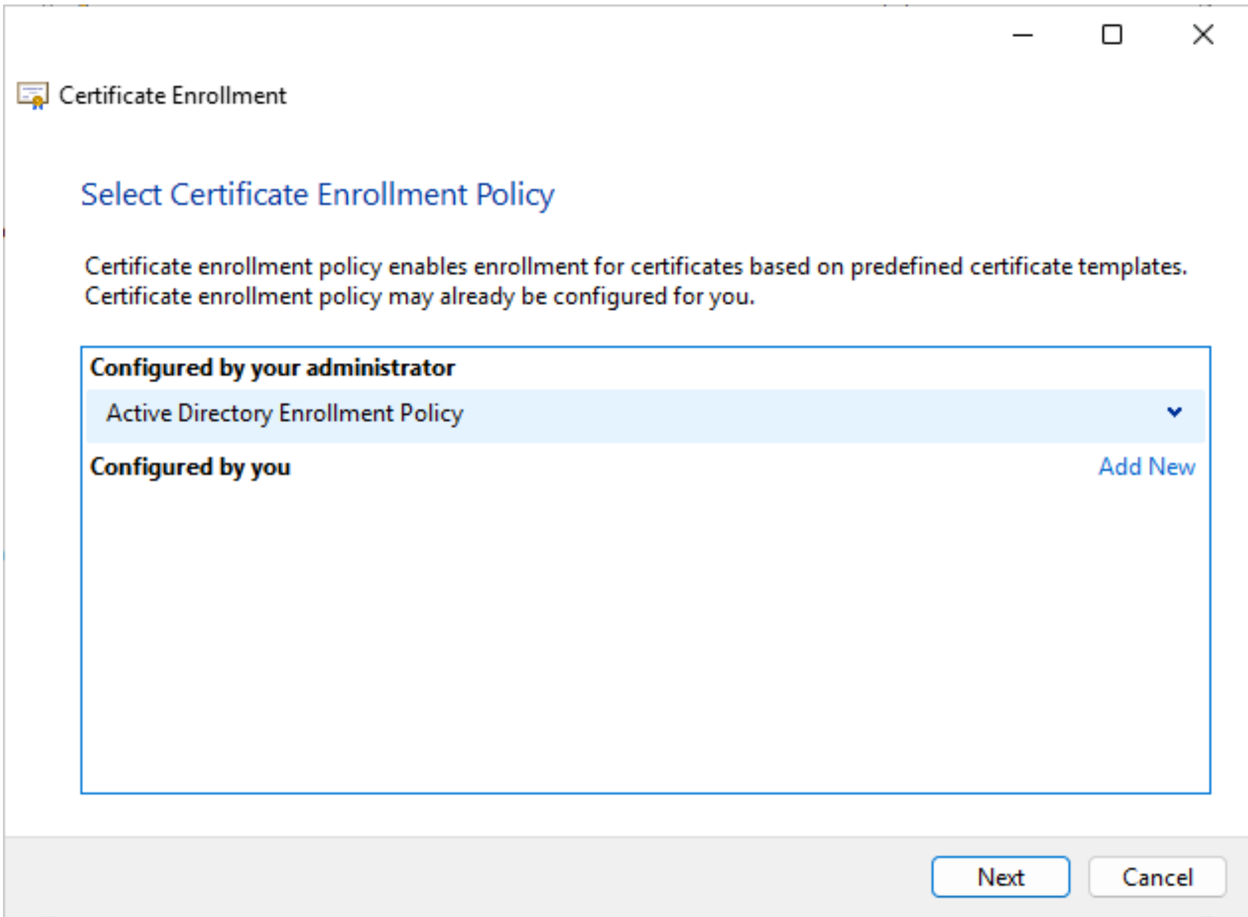

Figure 121 : "Certificate Enrollment Policy" Window

> If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

13. On the **Request Certificates** page, select the **OCSP Response Signing** template and click **Enroll**.

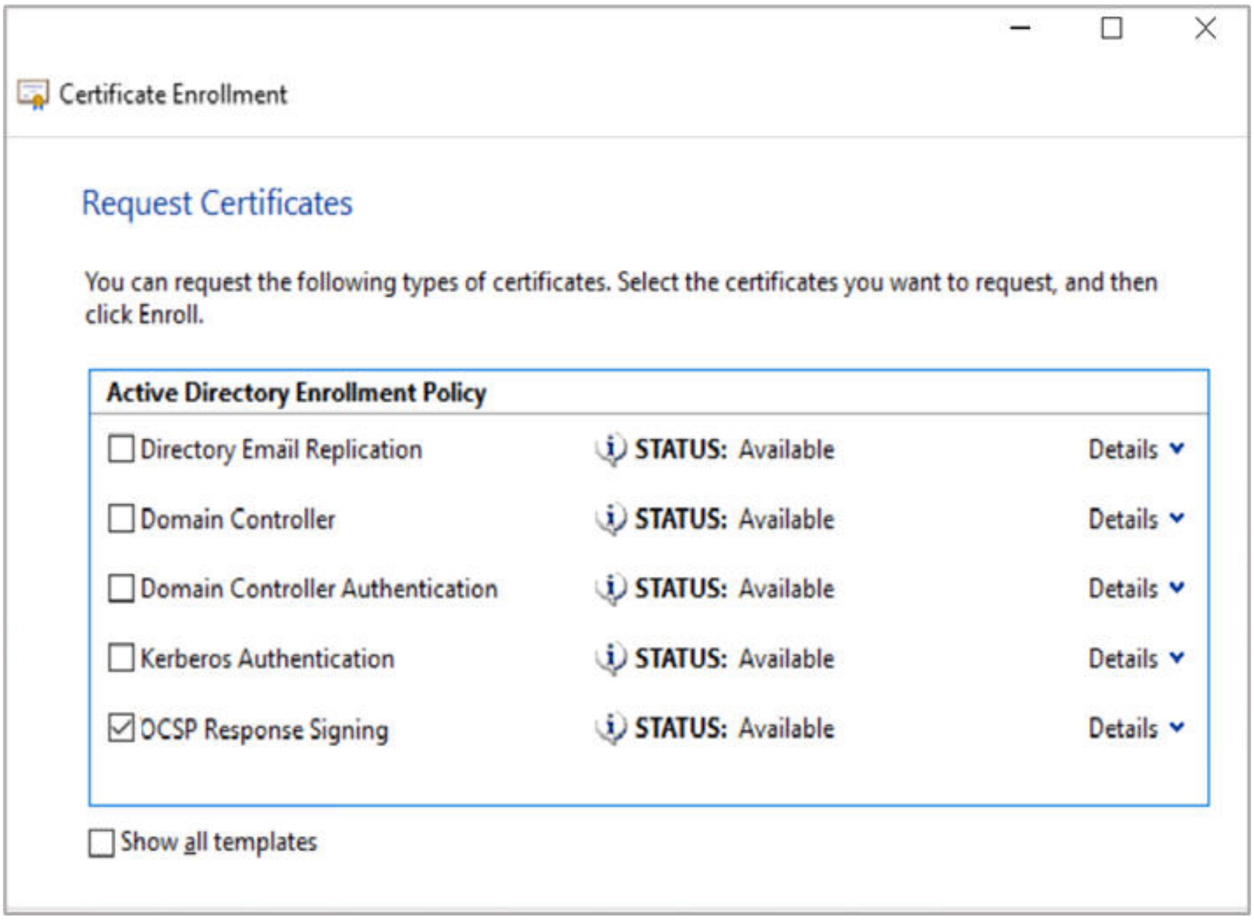

Figure 122 : "Certificate Enrollment Policy" Window

14. On the **Certificate Installation Results** page, click **Finish**.

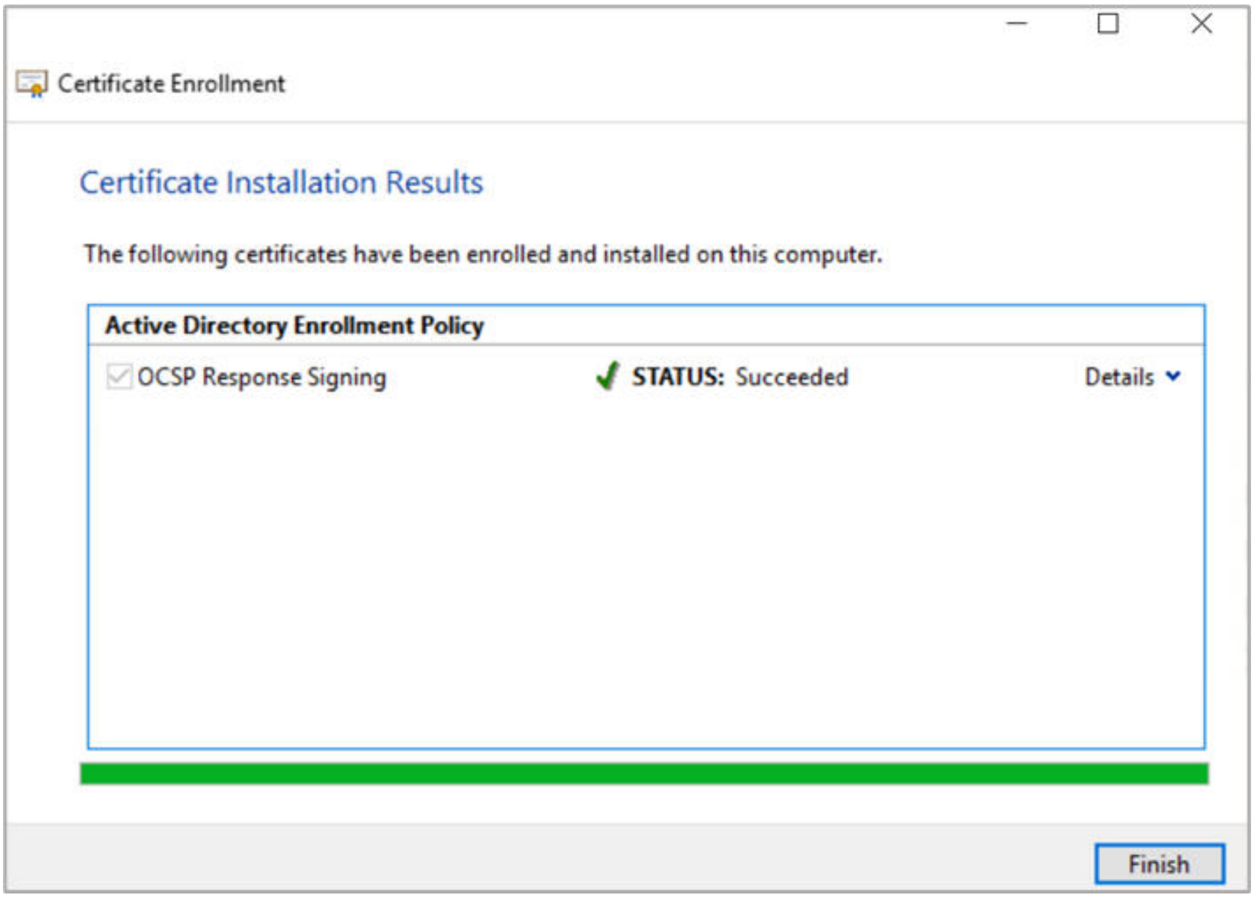

Figure 123 : "Certificate Installation Results" Window

6.1.5.4 Install and Configure Online Responder

Now change to your OCSP server and install the OCSP service.

1. Select **Start,** then select **Server Manager** to open **Server Manager.**
2. Select **Manage,** then select **Add Roles & Features**. The **Before you begin** window opens. Click **Next.**

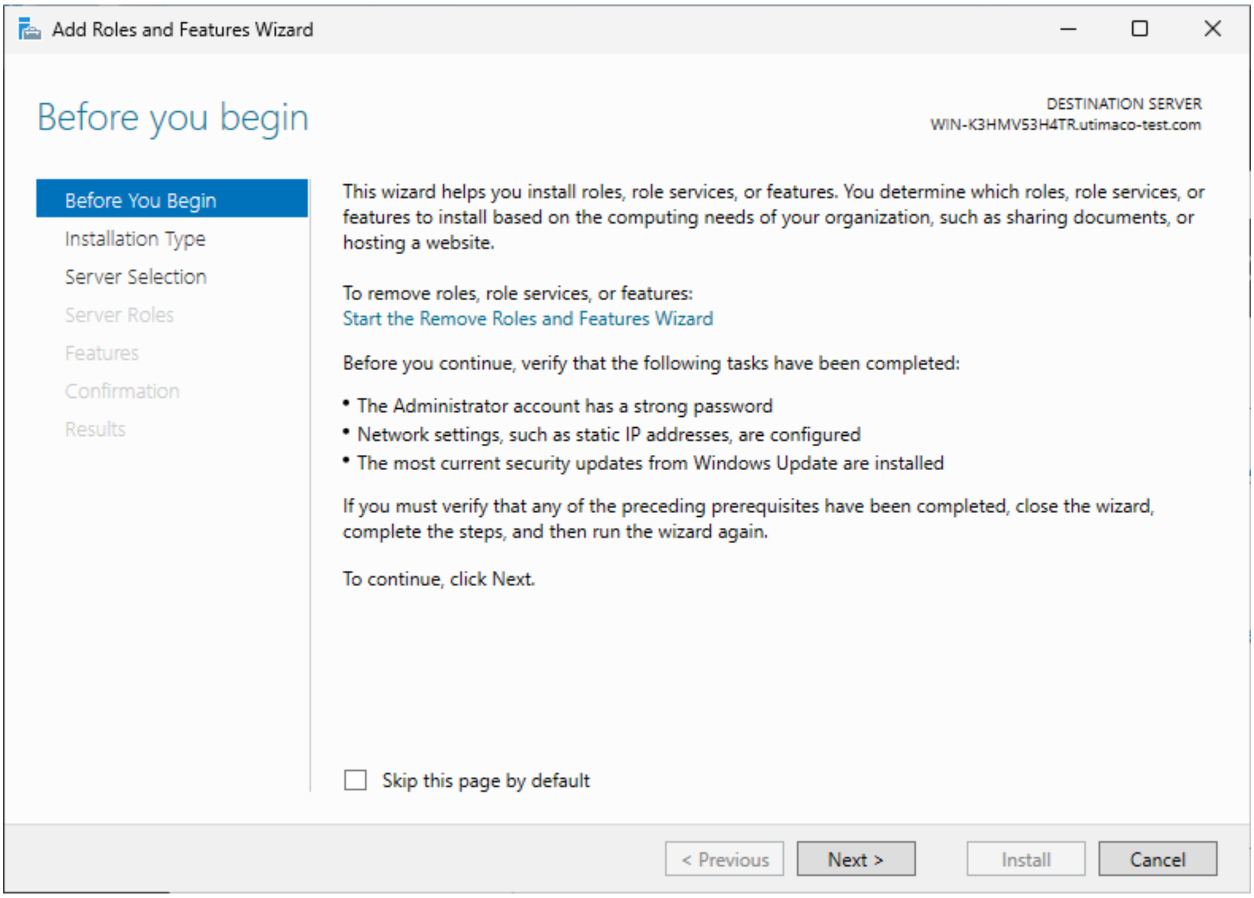

Figure 124 : "Before You Begin" Window

3. On the **Select installation type** window, make sure the **default Role or Feature Based Installation** is selected. Click **Next.**
4. On **Server selection**, select a server from the server pool. Click **Next.**
5. On the **Select server roles** window, select the **Active Directory Certificate Services** role.
6. When prompted to install **Remote Server Administration Tools**, select **Add Features**. Click **Next.**
7. On the Select features window, click **Next.**
8. On the **Active Directory Certificate Services** window, click **Next.**
9. On the **Select role services** window, select the **Online Responder**. Click **Next.**

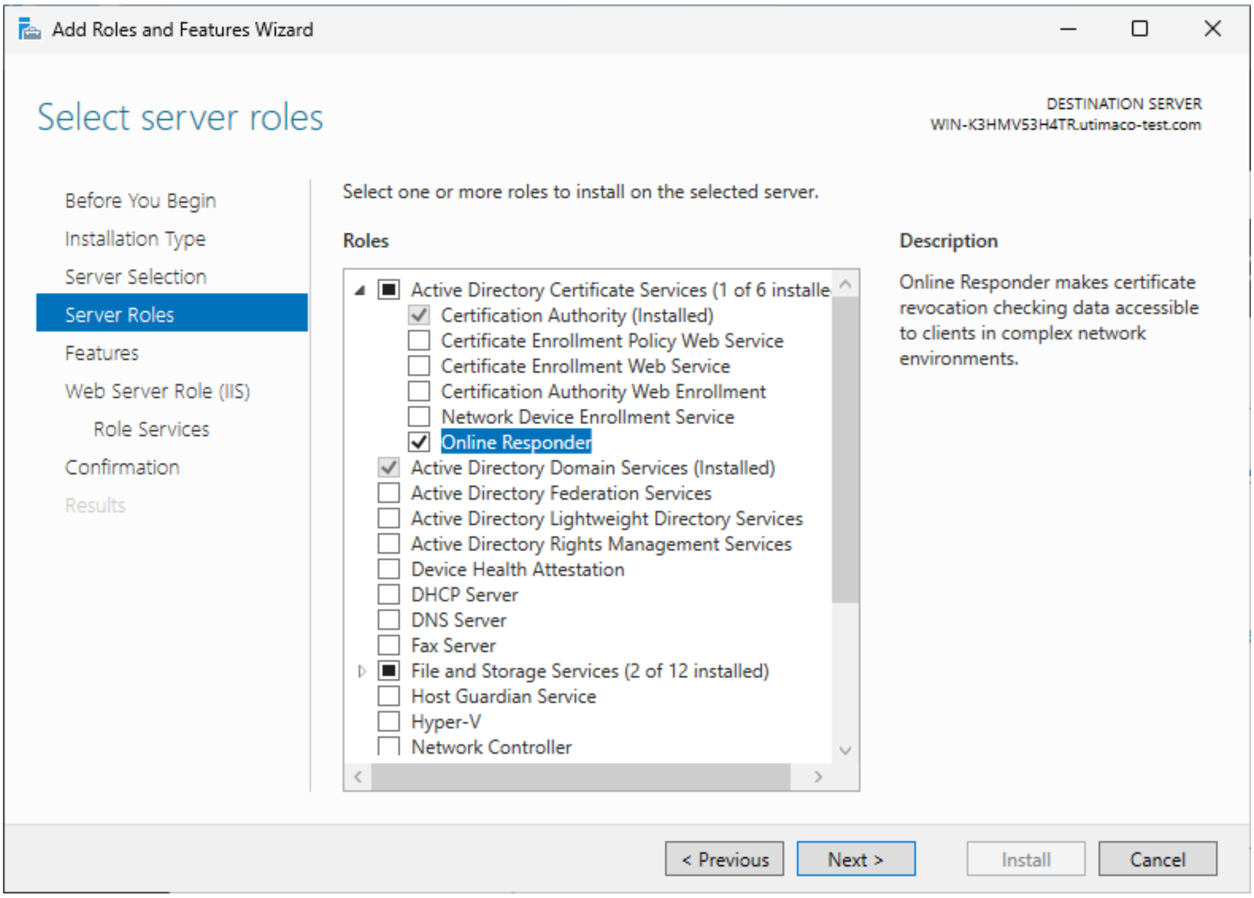

Figure 125 : "Select Server Roles" Window

10. When prompted to install **Remote Server Administration Tools**, select **Add Features**. Click **Next.**
11. On the **Confirm installation selections** window, verify the information, then click **Install.**

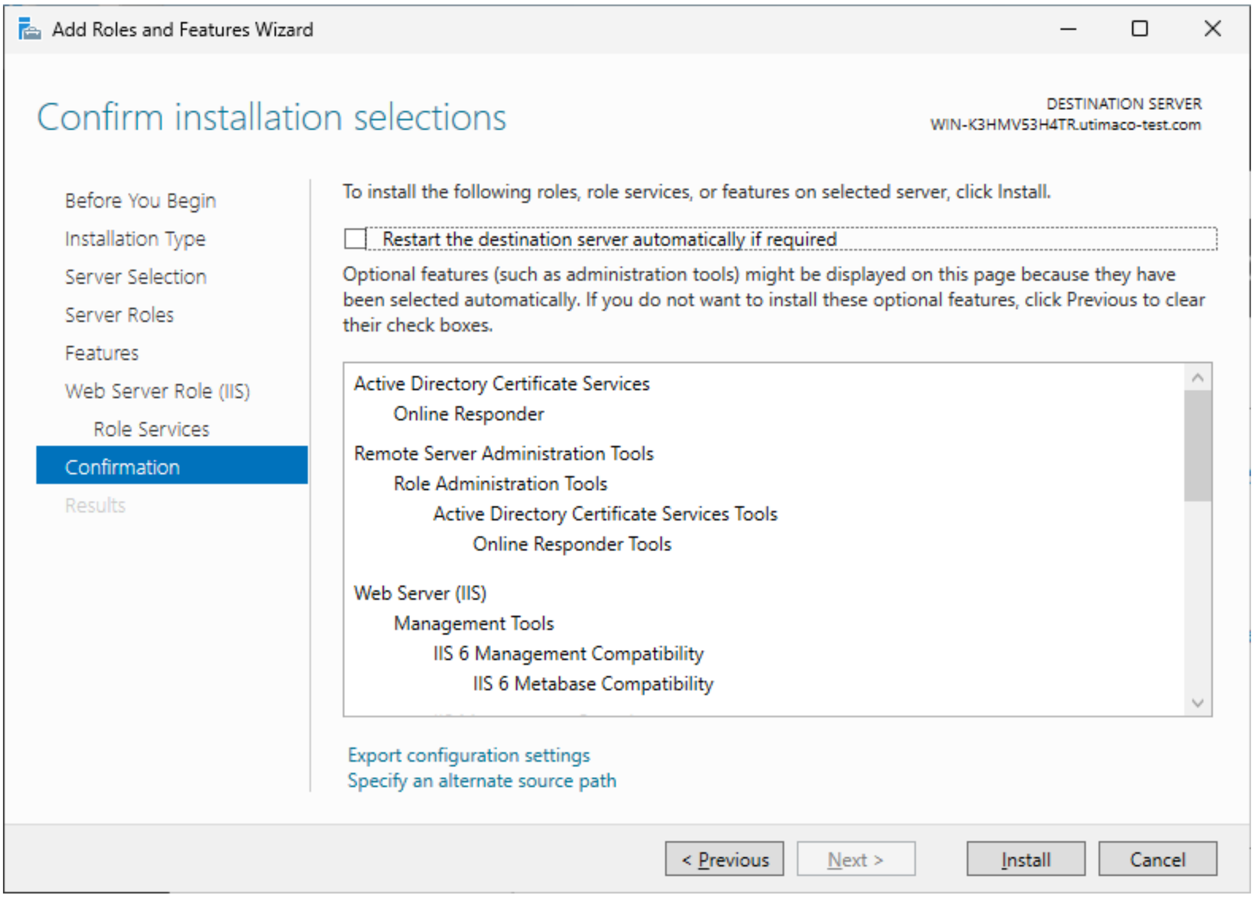

Figure 126 : "Confirm Installation Selections" Window

12. Click **Configure Active Directory Certificate Server** on the destination server. The **ADCS Configuration** Wizard displays.

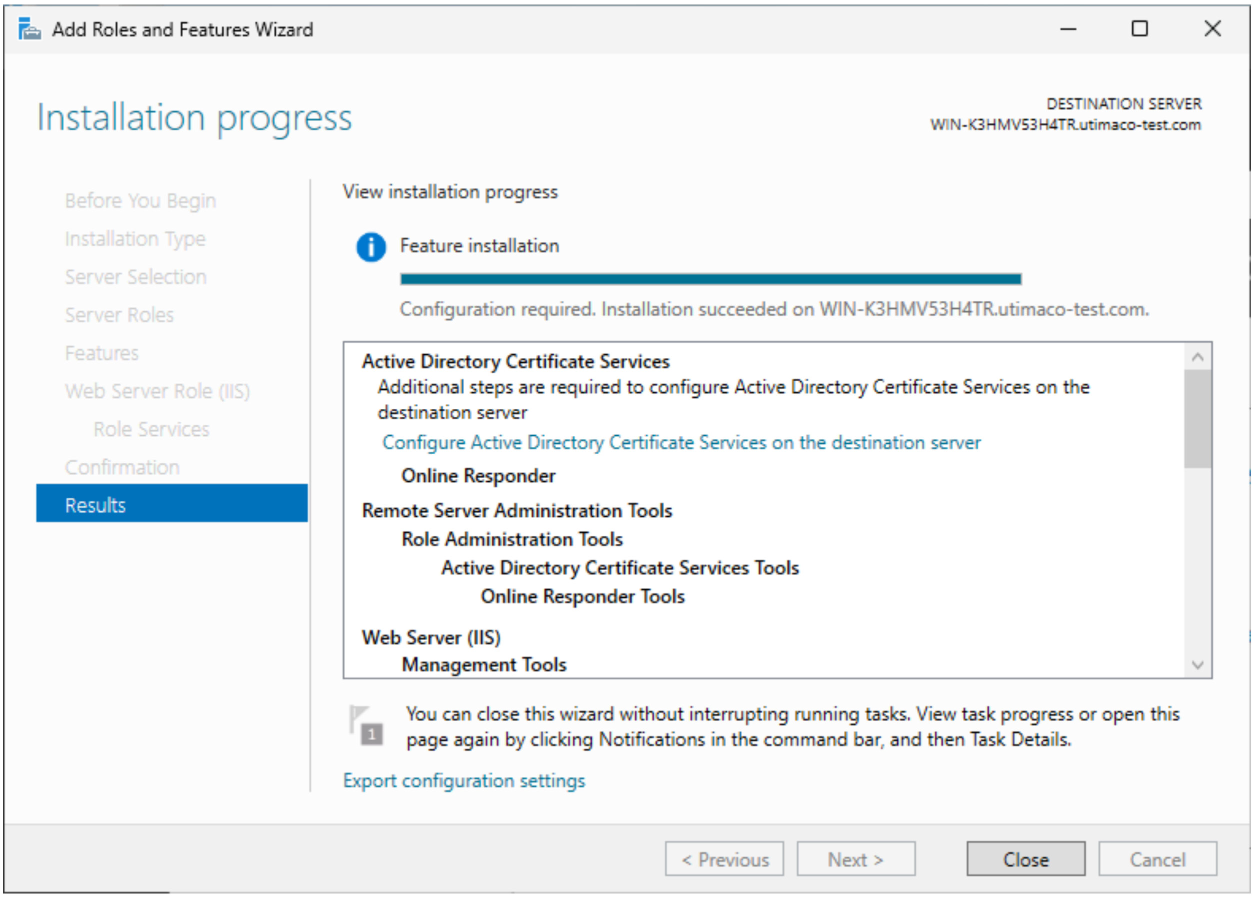

Figure 127 : "Installation Progress" Window

13. On the **Credentials** page, click **Next.**

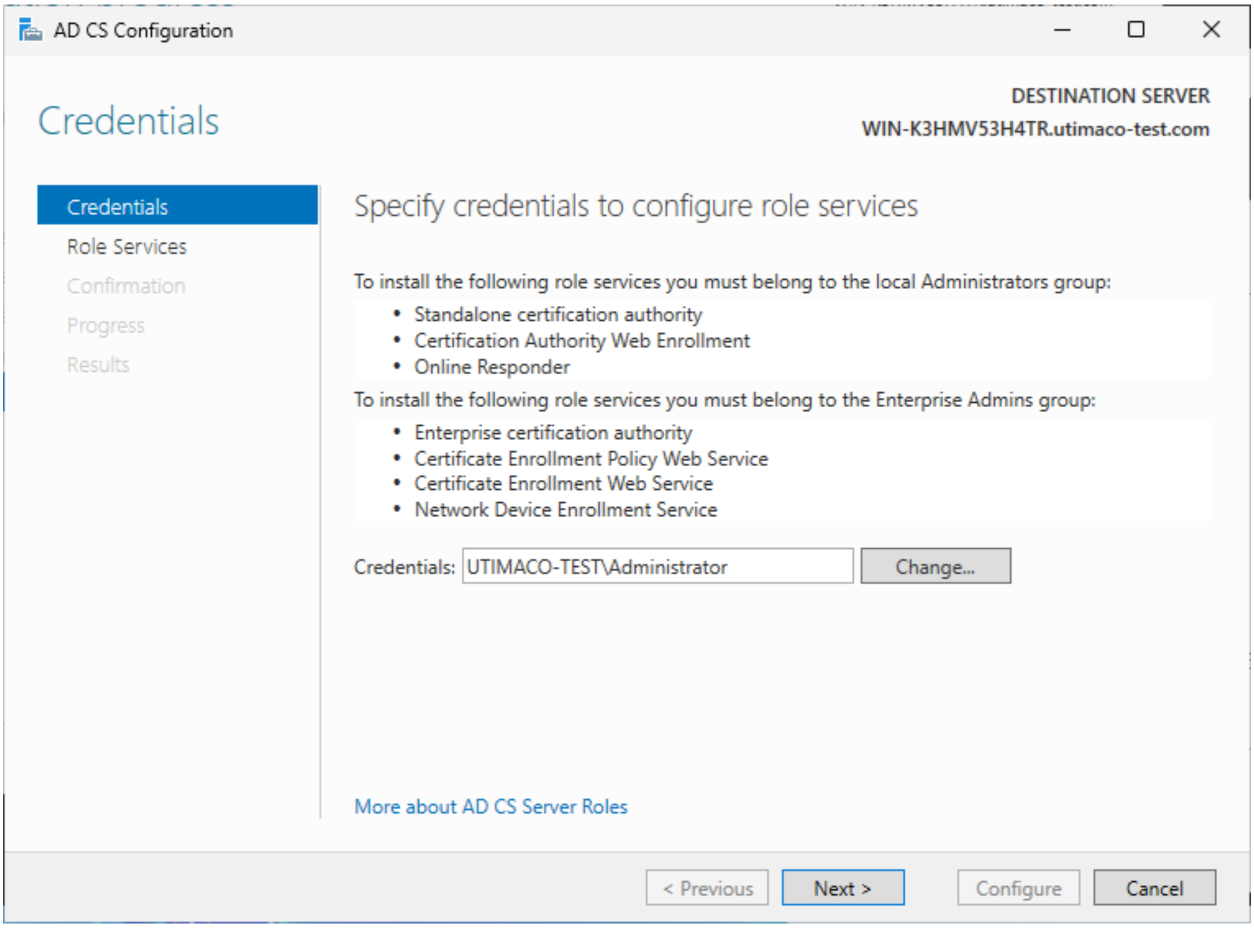

Figure 128 : "Credentials" Window

14. On the **Role services** page, select the **Online Responder** checkbox. Click **Next.**

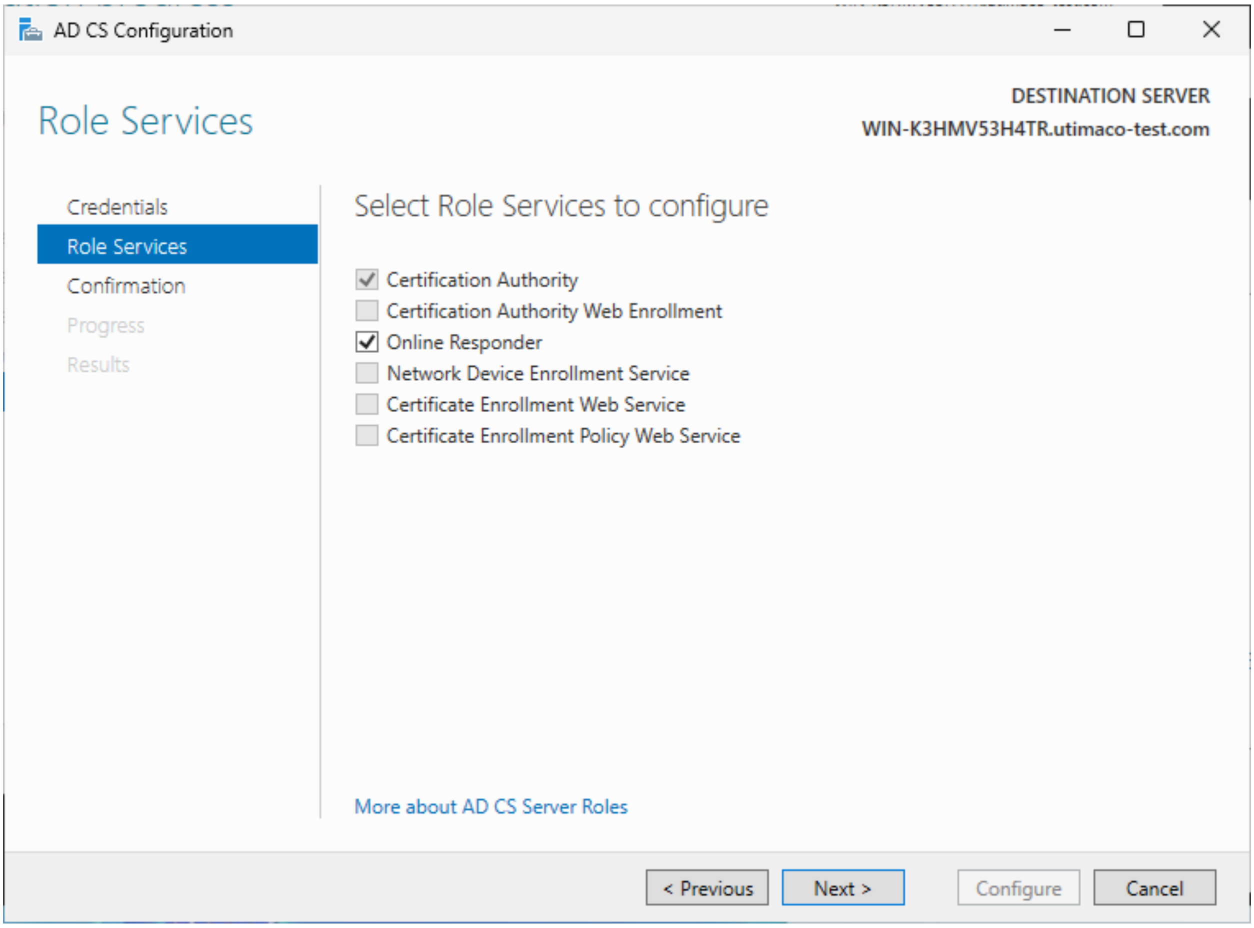

Figure 129 : "Role Services" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

15. On the **Confirmation** page, click **Configure** and wait for the confirmation message. A message displays after successful configuration.

16. On the **Results** page, click **Close** to exit the **ADCS Configuration** Wizard.

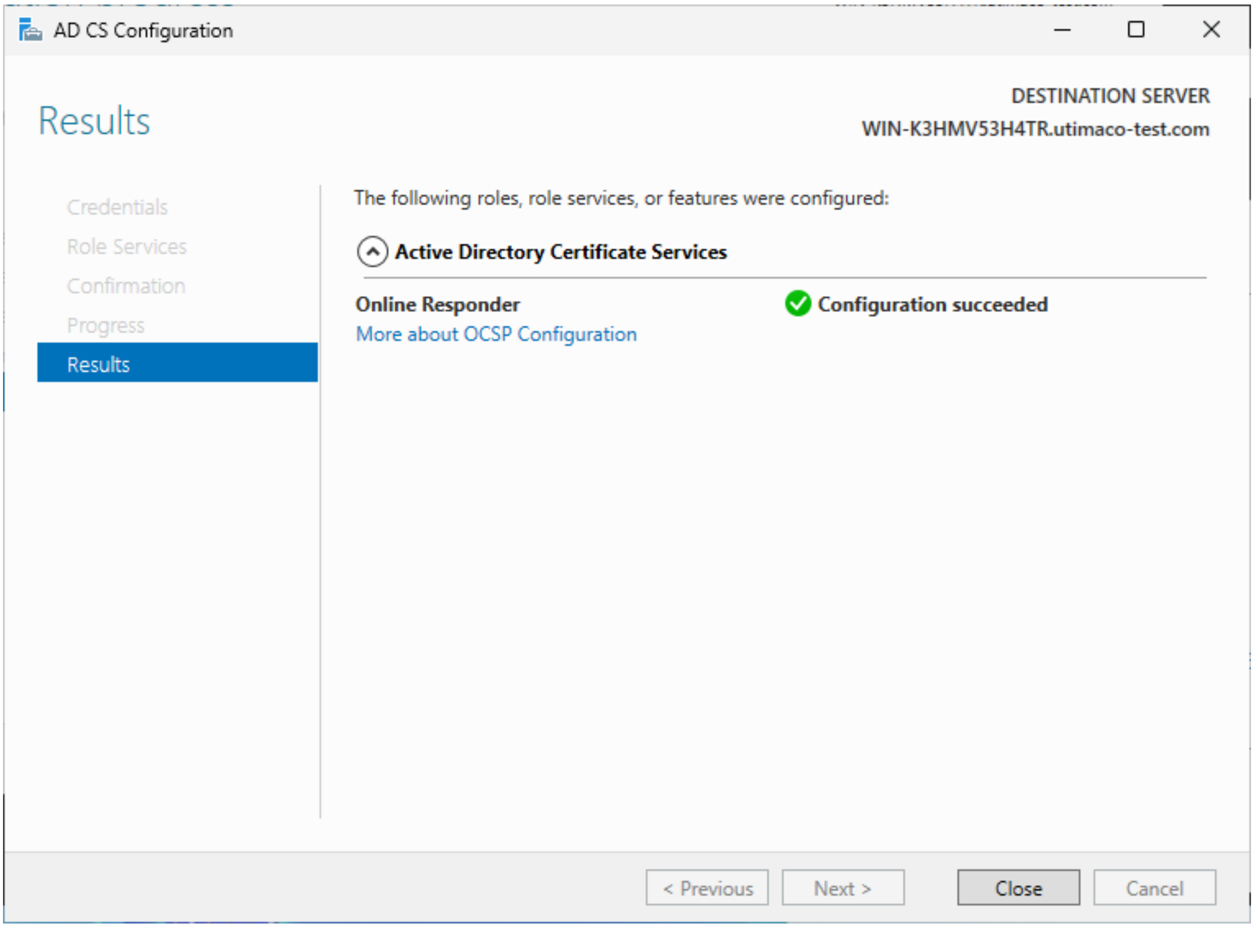

Figure 130 : "Results" Window

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.5.5 Make a Revocation Configuration

To use OCSP you must create a new revocation configuration.

1. Open the **Administrative tool** and select **Online Responder Management.**
2. Launch the **Online Responder Management** console.
3. Select **Revocation Configuration** and then click on **Action,** and then **Add Revocation Configuration.**

4. On the **Add revocation** wizard, click **Next,** then enter a Name for your configuration.

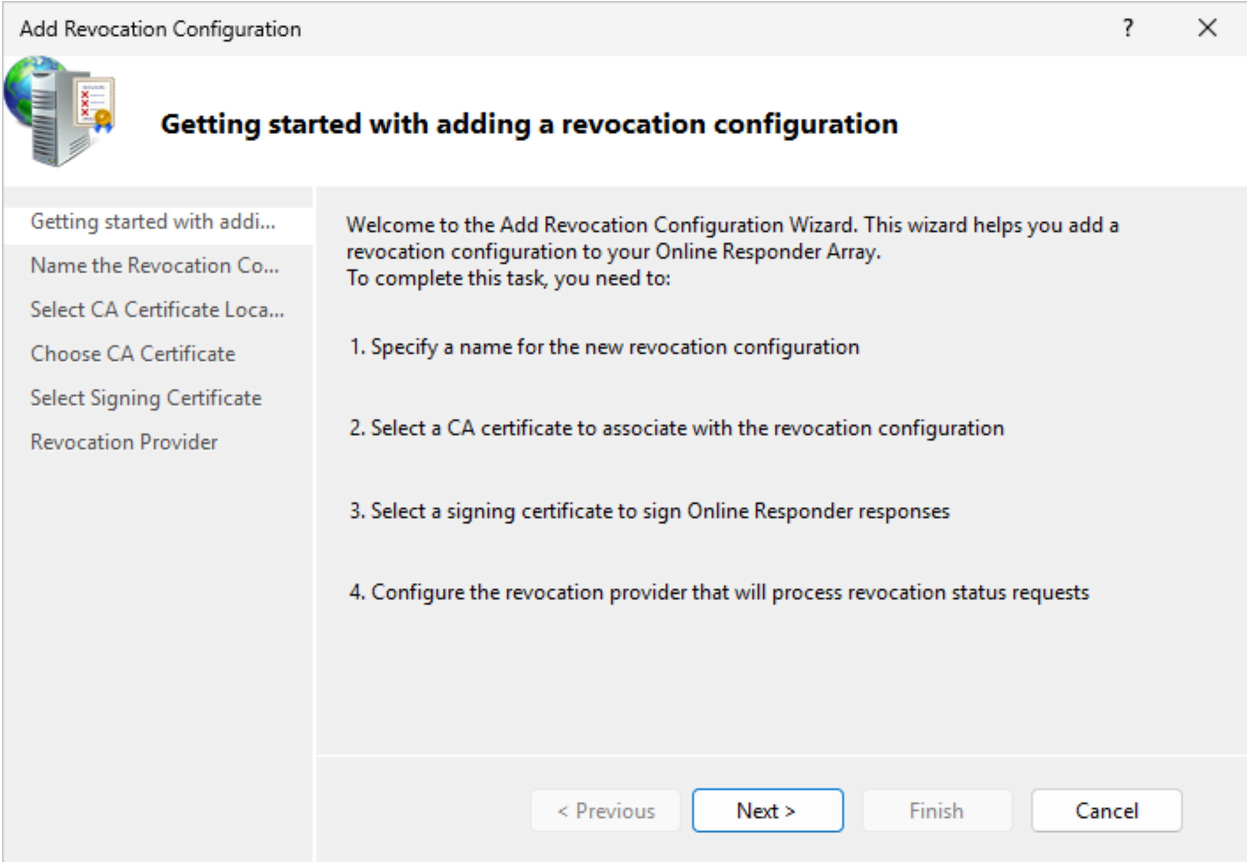

Figure 131 : "Add Revocation Configuration" Window

5. Specify the location of your CA certificate relative to your environment.

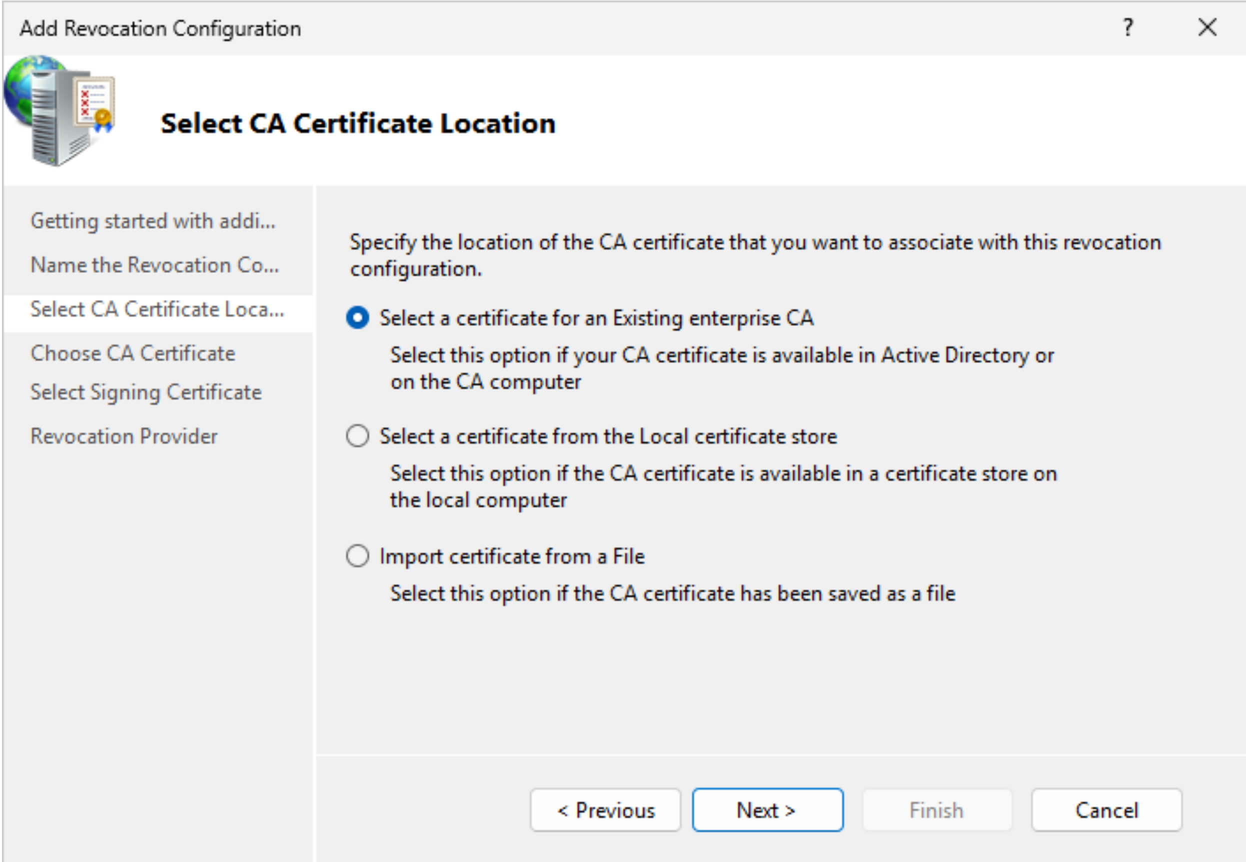

Figure 132 : "Select CA Certificate Location" Window

6. Select the OCSP certificate template created earlier and click **Browse.**
7. Click **Next** on the **Select signing certificate** wizard, click **Next.**

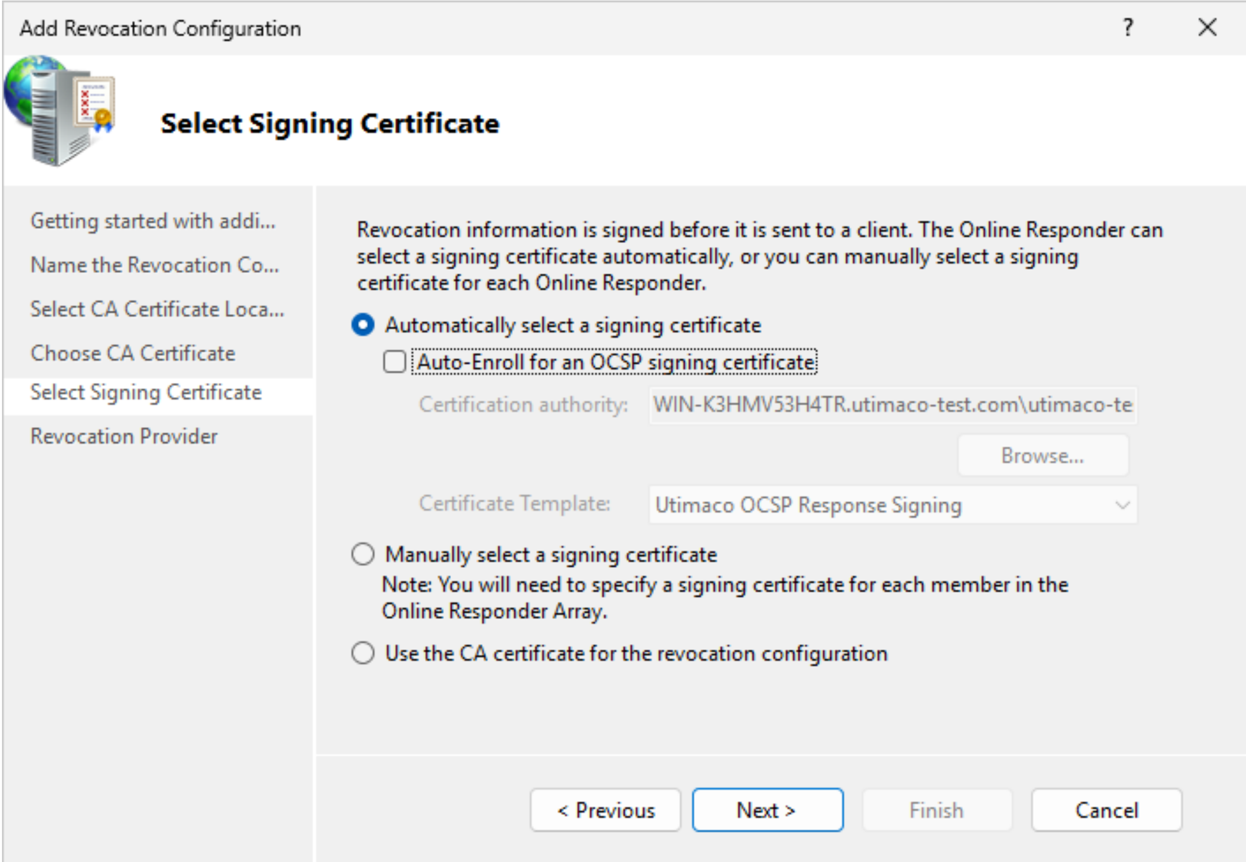

Figure 133 : "Select Signing Certificate" Window

8. To finish, configure the revocation provider. It is the location where the CRLs or Delta CRLs are stored. The configuration automatically retrieves this information in the CDP extension of the certificate.
9. Once you have set up the Revocation Configuration, the **Revocation Configuration Status** Box displays the Online Responder status. The status should display **Bad Signing** on the **Array Controller**.
10. To fix this, click on **Revocation Configuration** in the left-hand pane. Right-click on the certificate and select **Edit Properties**.
11. Click on the **Signing** tab. Deselect the **Do not prompt for credentials for cryptographic operations** checkbox. Click **OK**.
12. Go back to the **Online Responder Management** tool. Open **Actions** and click **Refresh**. Its status would be working now.
13. You can check if the key to this certificate is really created and stored by the Utimaco CNG provider. To do this, open a PowerShell and enter `cngtool ListKeys`. If there is a key,

then you can be assured that your Online Responder Service uses the Utimaco CryptoServer HSM correctly.

›_ Console

```
> cngtool ListKeys

------------------------------------------------------------

Provider          : Utimaco CryptoServer Key Storage Provider
Device            : <PORT>@<IP>
Group             : CNG
Mode              : Internal Key Storage

------------------------------------------------------------

Index  AlgId        Size   Group            Name
Spec
--------------------------------------------------------------------------------
-
1      RSA          2048   CNG              utimaco-adcs-UtimacoADCSServ-CA   0
```

If you are using smartcard authentication, the prompt will appear on the PIN Pad device to insert the smartcard and enter the PIN. Then, press the **OK** button on the PIN Pad.

6.1.5.6 Test the Online Responder

To test the online responder, you can create a new computer certificate. After you have exported this certificate to a CER file run certutil –URL `c:\temp\MyCertificate.cer`. This command opens the window.

Select OCSP and click **Retrieve**. The status of this certificate should change to Verified. Now you can revoke this certificate on your CA and publish the CRL again. If you now click again on **Retrieve,** the status should change to **Revoked**.

7 Troubleshooting

7.1 Common Issues and How to Resolve Them

Error	Diagnosis
When executing `certutil -csplist`: `Utimaco CryptoServer Key Storage Provider: Provider DLL failed to initialize correctly.`	1. Create a new variable `CS_CNG_CFG` in System variables. 2. Assign Path to Configuration File `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`
When executing `certutil -csplist`: `Utimaco CryptoServer Key Storage Provider: Object was not found.`	1. Check if the Configuration File is pointing towards the IP Address of the HSM and the corresponding port for the cHSM.

When executing `cngtool.exe ProviderInfo`
`E: NCryptOpenStorageProvider [Utimaco CryptoServer Key Storage Provider] returned: Error 0x80090011`
`Object was not found.`
	1. Check if the Configuration File is pointing towards the IP Address of the HSM and the corresponding port for the cHSM.

When configuring the Certification Authority, the `Utimaco CryptoServer Key Storage Provider` does not appear	There is an error with the Utimaco CNG Provider. Please refer to the CNG provider configuration section if the provider has not been configured.

Error	Diagnosis
When configuring the Certification Authority, there is a permission error in the last step.	1. Check the User and Password on the CNG Provider configuration file (by default in `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`) 2. Check that the CXI group configured in the CNG Provider configuration file matches the CXI_GROUP variable on the user (this can be checked using the CAT application.

Table 6: List of Errors and their Diagnoses

7.2 Log Locations and Interpretation

The following logs can be reviewed to check for errors:

- Utimaco CNG provider log: The default path is `C:\ProgramData\Utimaco\CNG\log`. The path is configured in the CNG Provider configuration file, by default in `C:\ProgramData\Utimaco\CNG\cs_cng.cfg`. More information about the configuration file can be obtained in CNG Provider configuration section.
    - This log contains errors related to the CNG provider. These include errors with the connection to the HSM, with the Keystore, or during the execution of cryptographic operations.

Error	Diagnosis
`cng_prov_session_open | E: cs_open_connection [PORT@IP] returned: Error B902B03D CryptoServer API Windows tcp: can't get connection connection attempt refused cng_prov_open | E: unable to open any device`	Error connecting to the cHSM. Please check that the cHSM port and IP are configured correctly in the configuration file and that the cHSM is running.

Error	Diagnosis
`cng_key_create | E: cng_prov_exec returned: Error B0680001 CryptoServer module CXI permission denied FinalizeKey | E: cng_key_create returned: Error B0680001 CryptoServer module CXI permission denied`	The User and password are incorrect, or the CXI Group is incorrectly configured in the CNG Configuration file.

Table 7: List of Common Errors on the CNG Provider Log

8 Appendices

8.1 References

Reference	Title/Company	Document No.
[CSADM]	u.trust Anchor – csadm Manual / Utimaco IS GmbH	2021-0037
[UTAADMIN]	u.trust Anchor - Administration Manual / Utimaco IS GmbH	2020-0035

Table 8: List of References

8.2 Command Summary

Task	Command
List installed cryptographic providers	`certutil -csplist` `cngtool EnumProvider`
Check if the CNG Provider is correctly configured	`cngtool ProviderInfo`
Verify that the CA service is running	`sc query certsvc`
Verify the CA key	`certutil -verifykeys`
Create DB Schema for External Key Storage in MSSQL	`cxitool dbConnString="DSN=<ODBC>;Uid=<Username>;Pwd=<Password>" CreateDBSchema=mssql`

Task	Command
Create Key using an SDB external keystore	`cxitool Dev=<port@IP> LogonPass=<user>,<password> keystoretype=SDB keystoreparam="<SDB_PATH>" group="" | Name=<KEY_NAME> Usage=ENCRYPT,DECRYPT,SIGN,VERIFY spec=0 generatekey=AES,256`

Table 9: List of Commands