ENCRYPTION CONSULTING
www.encryptionconsulting.com

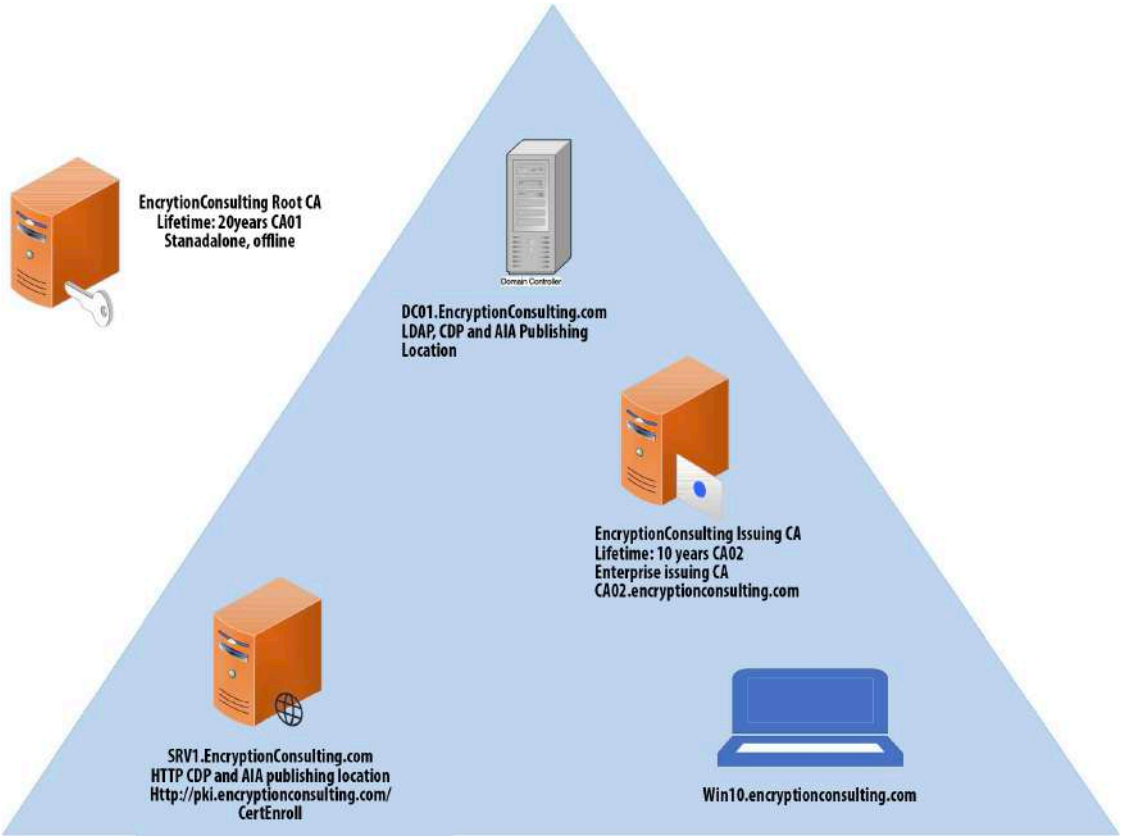
ADCS Two Tier PKI Hierarchy Deployment

Detailed guide for Basic Configuration

Introduction and overview of the Test Lab:

There are five computers/machines involved in this two-tier PKI hierarchy lab.

1. There is one domain controller (DC01) that is also running Active Directory-integrated Domain Name Service (DNS). This computer will also provide the Lightweight Directory Access Protocol (LDAP) location for the CDP and the AIA point for the PKI configuration.
2. One Standalone Offline Root CA (CA01).
3. One Enterprise Issuing CA (CA02).
4. One Web Server (SRV1) (HTTP CDP/AIA) and
5. One Windows 10 (Win10) Client computer.



AD DS forest – encryptionconsulting.com

Virtual Machine	Roles	OS Type	IP Address	Subnet mask	Preferred DNS server
DC01.encryptioncon-sulting.com	DC & DNS – LDAP CDP/AIA	Windows Server 2019	192.168.1.10	255.255.255.0	192.168.1.10
CA01	Standalone Offline Root CA	Windows Server 2019	NA	NA	NA
CA02.encryptioncon-sulting.com	Enterprise Issuing CA	Windows Server 2019	192.168.1.12	255.255.255.0	192.168.1.10
SRV1.encryptioncon-sulting.com	Web Server - HTTP CDP/AIA	Windows Server 2019	192.168.1.13	255.255.255.0	192.168.1.10
WIN10.encryption-consulting.com	Windows Client Computer	Windows 10	192.168.1.14	255.255.255.0	192.168.1.10

Major Steps:

There are eight major steps in this step-by-step guide as listed below (each includes several sub tasks).

1. Install the Active Directory Forest
2. Prepare the web server for CDP and AIA publication
3. Install the standalone offline root CA
4. Perform post installation configuration steps on the standalone offline root CA
5. Install Subordinate Issuing CA
6. Perform the post installation configuration on the subordinate issuing CA
7. Install and configure the online responder
8. Verify the PKI hierarchy health

1: Active Directory Forest

Task 1: Configure Server Name and Network Settings

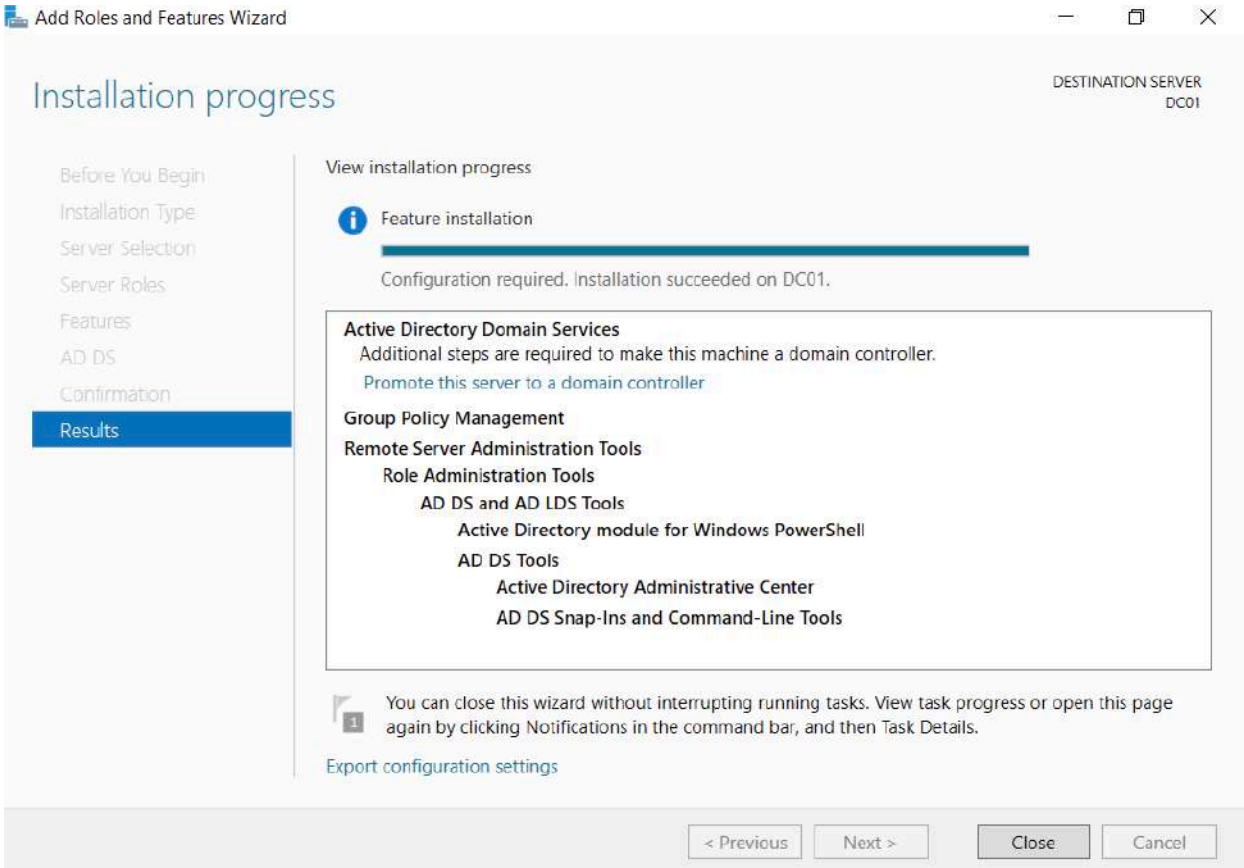
Name server DC01 and create network for this lab:

1. Log in as DC01 and the local administrator.
2. Select **Start,** type **ncpa.cpl** and press **ENTER**.
3. When on Network Connections, right-click the **Local Area Connection** and then click **Properties**.
   - 3.1. If there are more than one Local Area Connection icons in the Network Connections, you want to modify the one that is connected to network segment shared by all the computers that you have installed for this lab.
   - 3.2. Click the **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties.**
   - 3.3. Select the **Use the Following IP address**. Configure the **IP address, Subnet mask,** and **Default gateway** appropriately for your test network.
     - **IP Address**: 192.168.1.10
     - **Subnet mask**: 255.255.255.0
     - **Default gateway**: <optional>
4. Select the Use the following DNS server address. Configure the **Preferred DNS server** for the IP address of your domain controller. Click **OK.** Click **Close**.
   - **Preferred DNS Server:** 192.168.1.10
5. Click Start, type **sysdm.cpl** and press **ENTER**. Click Change.
6. In **Computer name**, type **DC01** and then click **OK**.
7. When prompted that you need to restart the computer, click **OK**. Click **Close.** Click **Restart Now**.

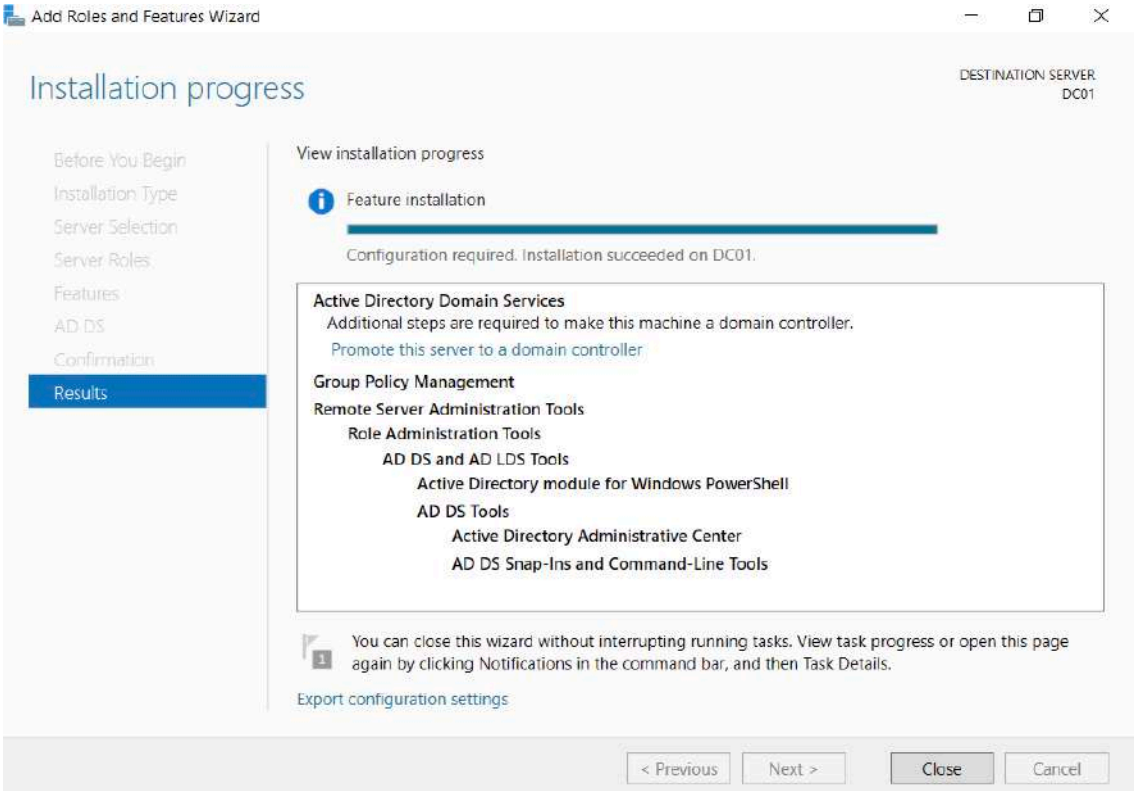
Task 2: Install a new forest by using Server Manager

To install the EncryptionConsulting.com forest:

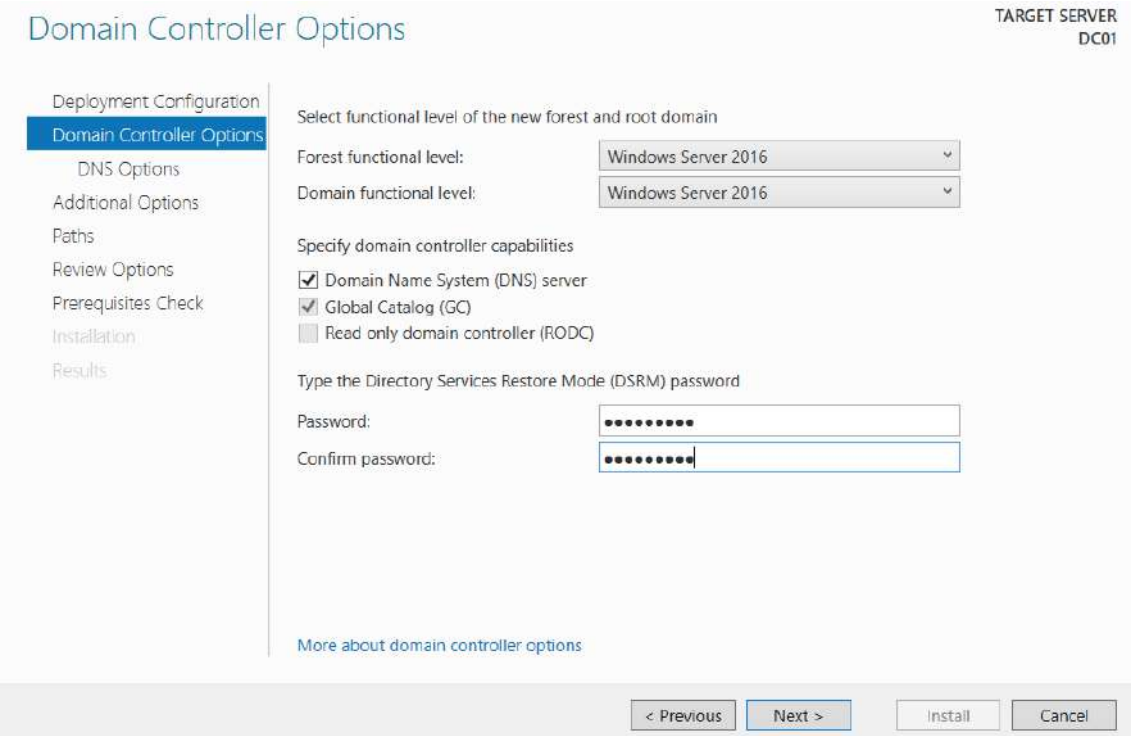
1. Log onto **DC01** as **DC01\Administrator.**
2. Open **Server Manager.** Select **Start,** click **Administrative Tools**, and then click **Server Manager.**
3. In the console tree, right-click **Manage** and then click **Add Roles & Features**
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Installation type**, click **Role Based or Feature Based** installation
6. On **Server Selection**, select **server from server pool** and click on **DC01.** Then click **Next**
7. On the **Select Server Roles** page, select **Active Directory Domain Services**. Click **Next.**
    - If prompted by the **Add Roles Wizard**, click **Add Required Features** and then click **Next.**
8. On the **Features** page, click next.
9. On the **Active Directory Domain Services** page, click **Next.**
10. On the **Confirm Installation Selections** page, click **Install.**
11. When completed, Click the hyperlink to Promote this server to a domain controller



12. On the **Welcome to the Active Directory Domain Services Installation Wizard** page, click **Next**.
13. On the **Deployment Configuration** page, select **Add a new forest**, Specify **Forest Root Domain** page, in **FQDN of the forest root domain**, type **EncryptionConsulting.com**, and then click **Next**.



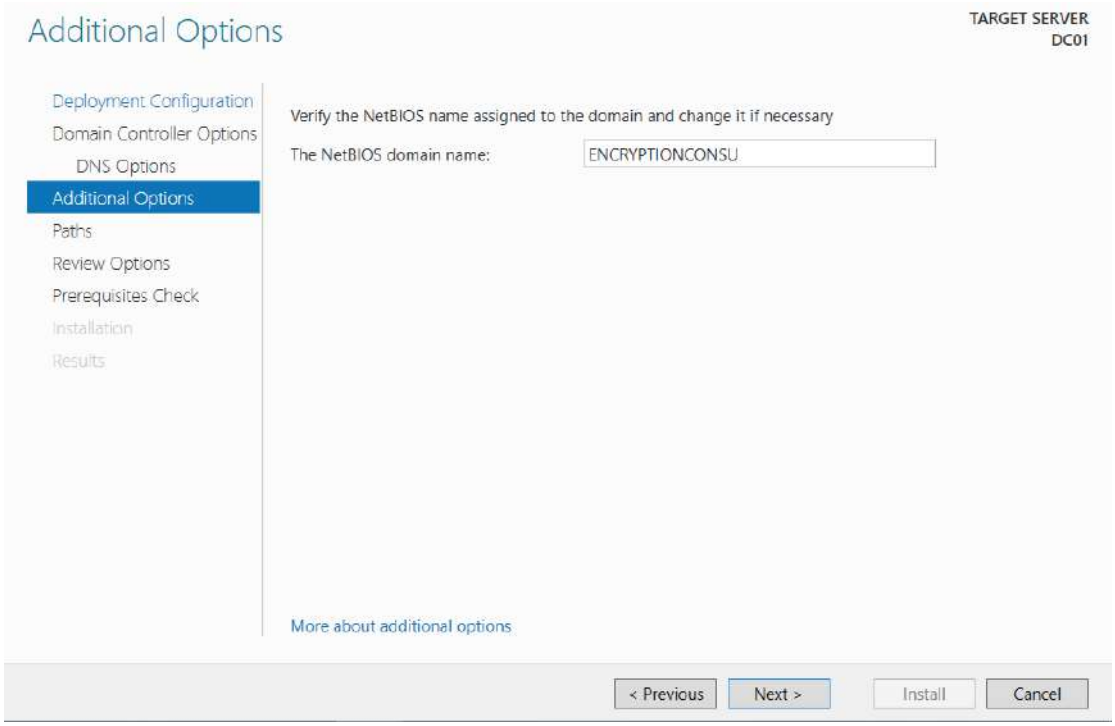
14. On the **Set Forest Functional Level** page, in the **Forest functional level** drop down menu, select **Windows Server 2016** and then click **Next**



On the **Directory Services Restore Mode Administrator Password** page, type and confirm the restore mode password, and then click **Next.** This password must be used to start Restore Mode for tasks that must be performed offline.

DNS server is selected by default so that your forest DNS infrastructure can be created during AD DS installation. In our scenario we are going to use Active Directory–integrated DNS so we have selected to install DNS

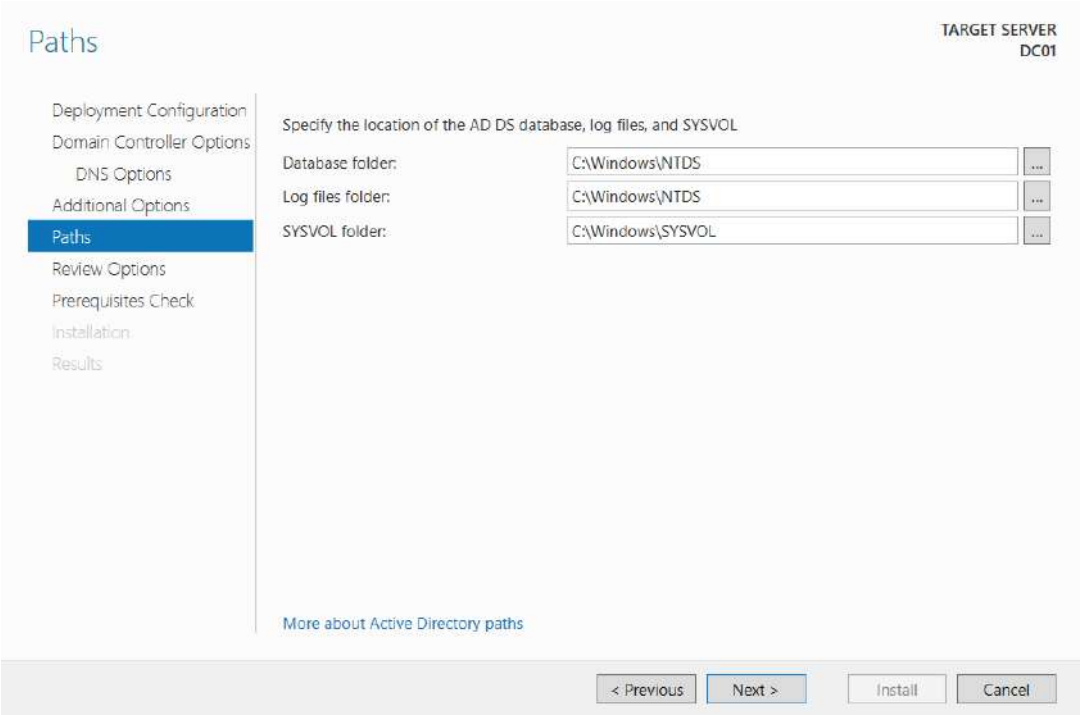
15. On the Additional **Options** page, click **Next.**



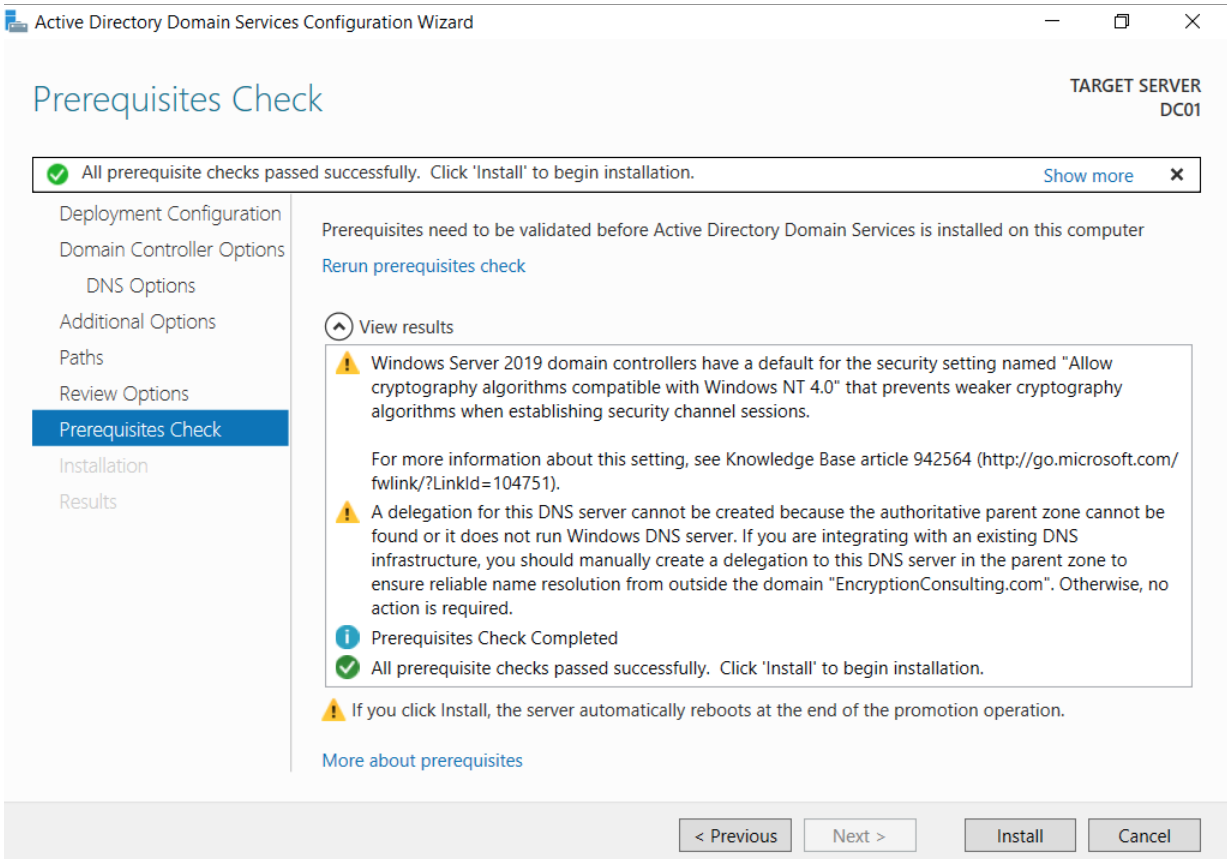
If no static IP address assigned for network adapter, a warning message appears advising you to set static addresses.

The wizard displays a message indicating that it cannot create a delegation for the DNS server. Click **Yes** to continue.

16. On the **Location for Database, Log Files, and SYSVOL** page, click **Next.**



17. On the **Prerequisites Check** page, review your selections and click **install** Active Directory Domain Services.

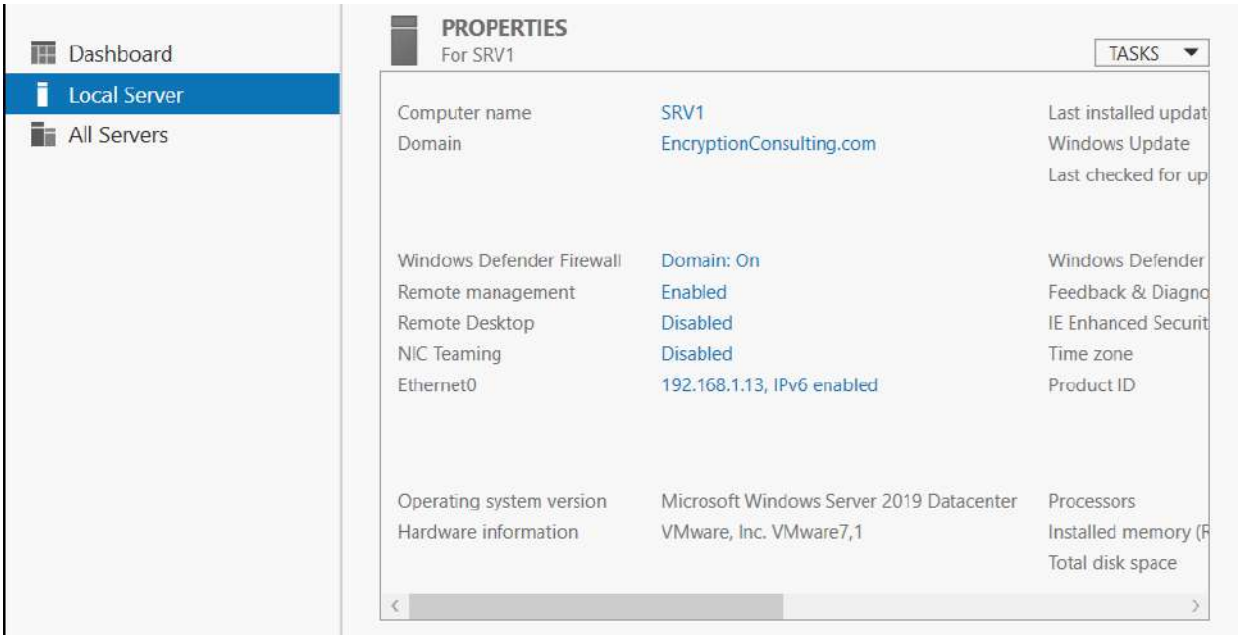


18. Wait for some time until installation completes and system restarts.

NOTE: If you are using Active Directory-integrated DNS, the IP address for the **Preferred DNS server** for the first domain controller in the forest is automatically set to the loopback address of 127.0.0.1. This helps assure that the IP address of the first domain controller will be resolved in DNS even if the static IP address of the server is changed. **If you prefer to configure actual IP address of the DNS sever rather than loop-backaddress, then replace it with 192.168.1.10 after the restart.**

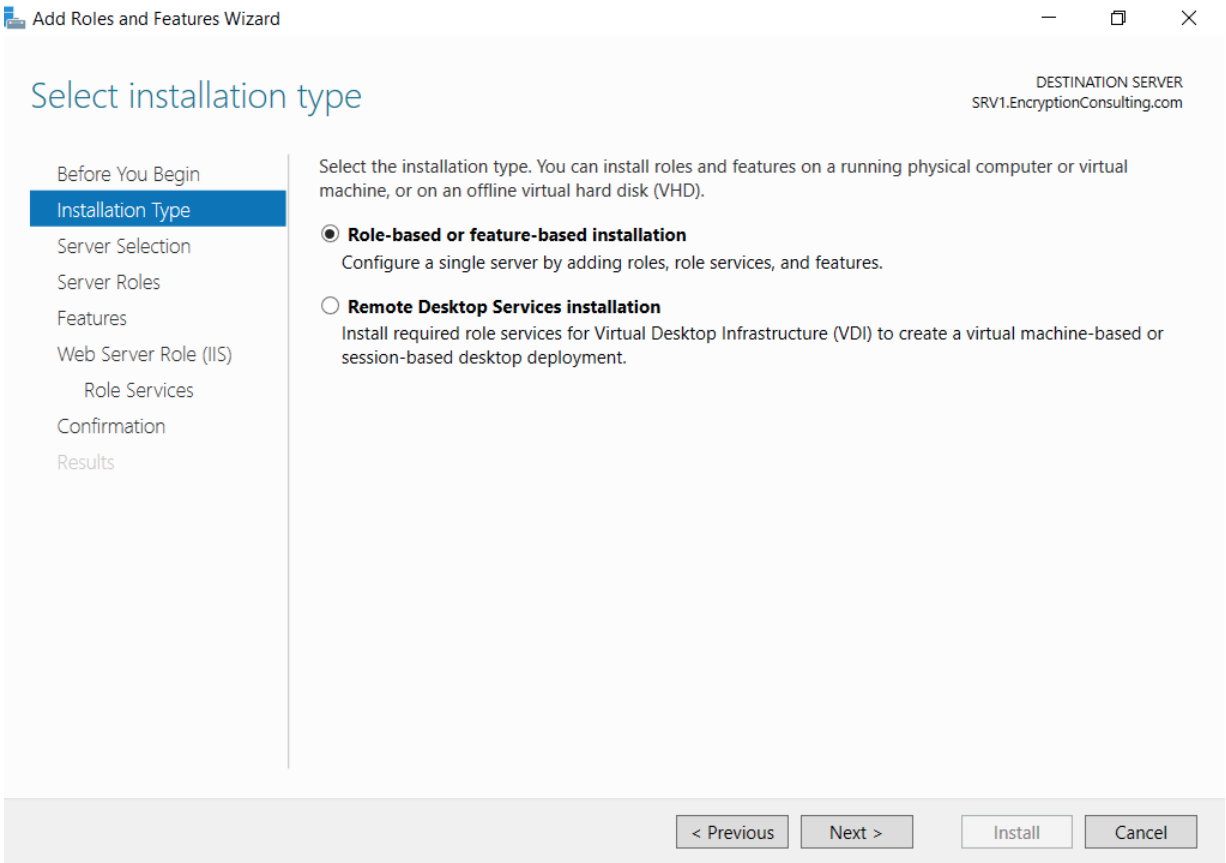
Task 3: HTTP Web Server: CDP and AIA Publication

1. Log on to SRV1 as the local administrator
2. Click **Start**, type **ncpa.cpl** and press ENTER.
3. In Network Connections, right-click the **Local Area Connection** and then click **Properties.**
    - If there are more than one Local Area Connection icons in the Network Connections, you want to modify the one that is connected to network segment shared by all the computers that you have installed for this lab.
4. Click the **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties.**
5. Select the **Use the Following IP address.** Configure the **IP address, Subnet mask,** and **Default gateway** appropriately for your test network.
    - **IP Address:** 192.168.1.13
    - **Subnet mask:** 255.255.255.0
    - **Default gateway:** <optional>
6. Select the Use the following DNS server address. Configure the **Preferred DNS server** for the IP address of your domain controller. Click **OK.** Click **Close.**
    - **Preferred DNS Server:** 192.168.1.10
7. Click **Start**, type **sysdm.cpl** and press ENTER. Click **Change.**
8. In **Computer name**, type **SRV1** and then click **OK.**
9. When prompted that you need to restart the computer, click **OK**. Click **Close**. Click **Restart Now.**
10. After SRV1 restarts, log on as a local administrator.
11. Click **Start**, type **sysdm.cpl** and press ENTER. Click **Change.**
12. In **Member of,** select **Domain**, and then type **EncryptionConsulting.com** Click **OK.**
13. In **Windows Security**, enter the **User name** and **password** for the domain administrator account. Click **OK.**
14. You should be welcomed to the **Encryption Consutling domain.** Click **OK.**
15. When prompted that a restart is required, click **OK**. Click **Close**. Click **Restart Now.**

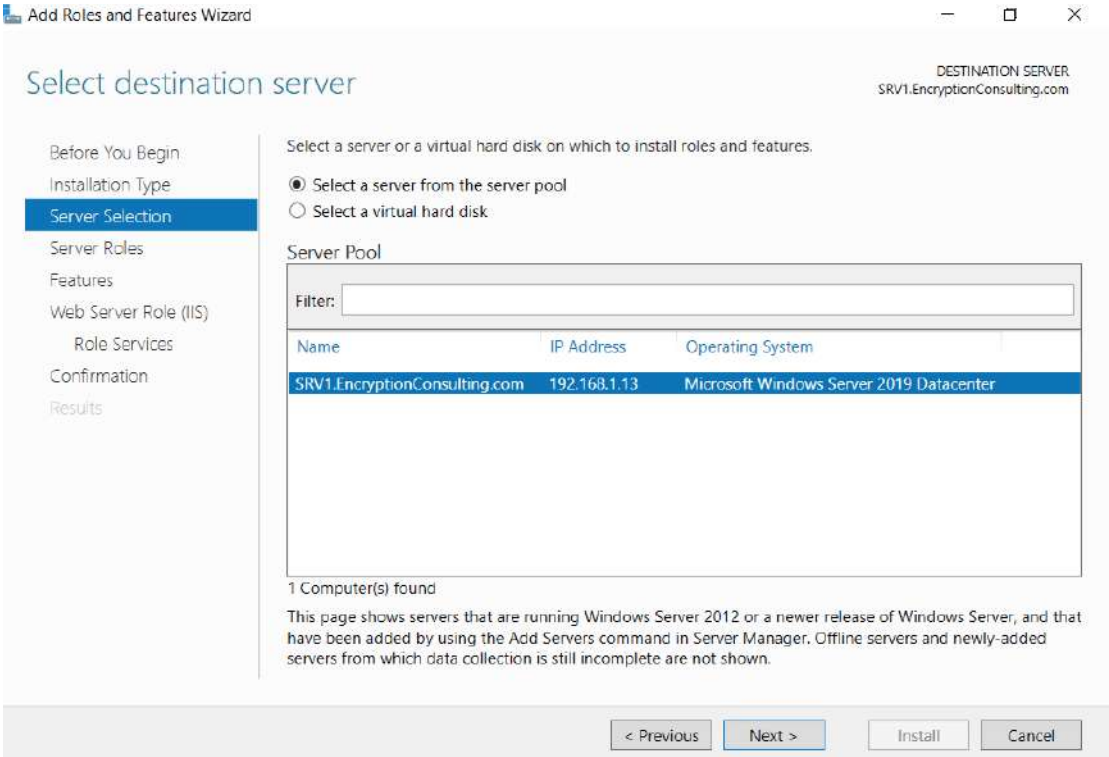


Task 4: Install Web Server (IIS) Role

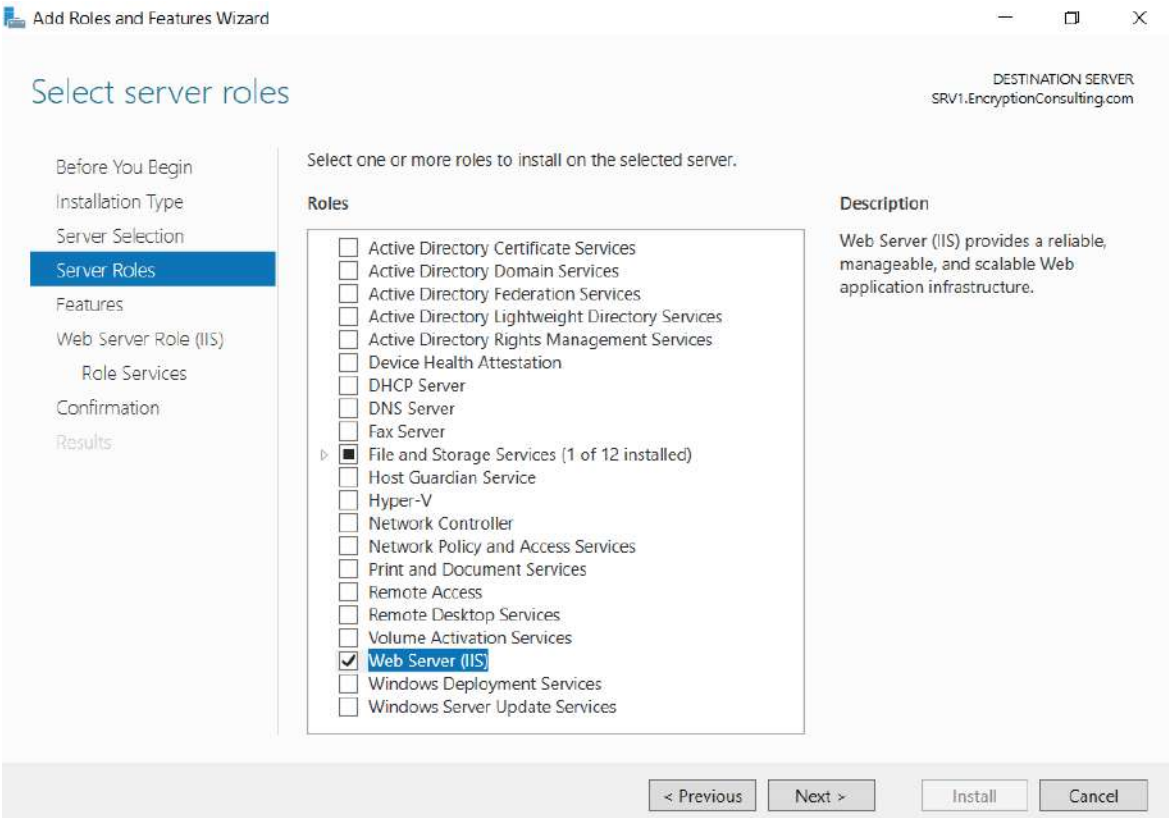
1. Log on to **SRV1.EncryptionConsulting.com** as **Encryptionconsu\Administrator.** (Ensure that you switch user to log on as Encryptionconsu\Administrator)
2. Open Server Manager.
3. Right-click on **Roles** and then select **Add Roles.**
4. On the **Before You Begin** page select **Next.**
5. On the Select Installation type page, Select Role-based or feature-based installation



6. On **Select Destination Server**, select **server from server pool** and click on **SRV1.EncryptionConsulting.com**, then click **Next**

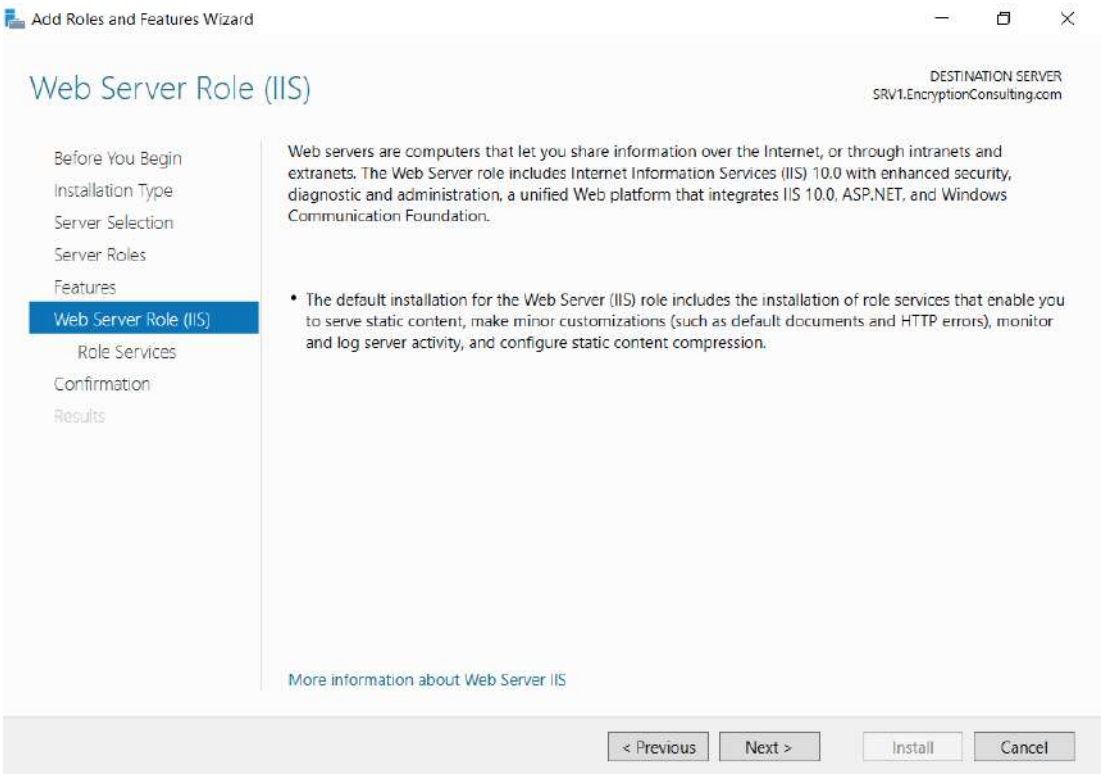


7. On the **Select Server Roles** page select **Web Server (IIS)** and then click **Next**

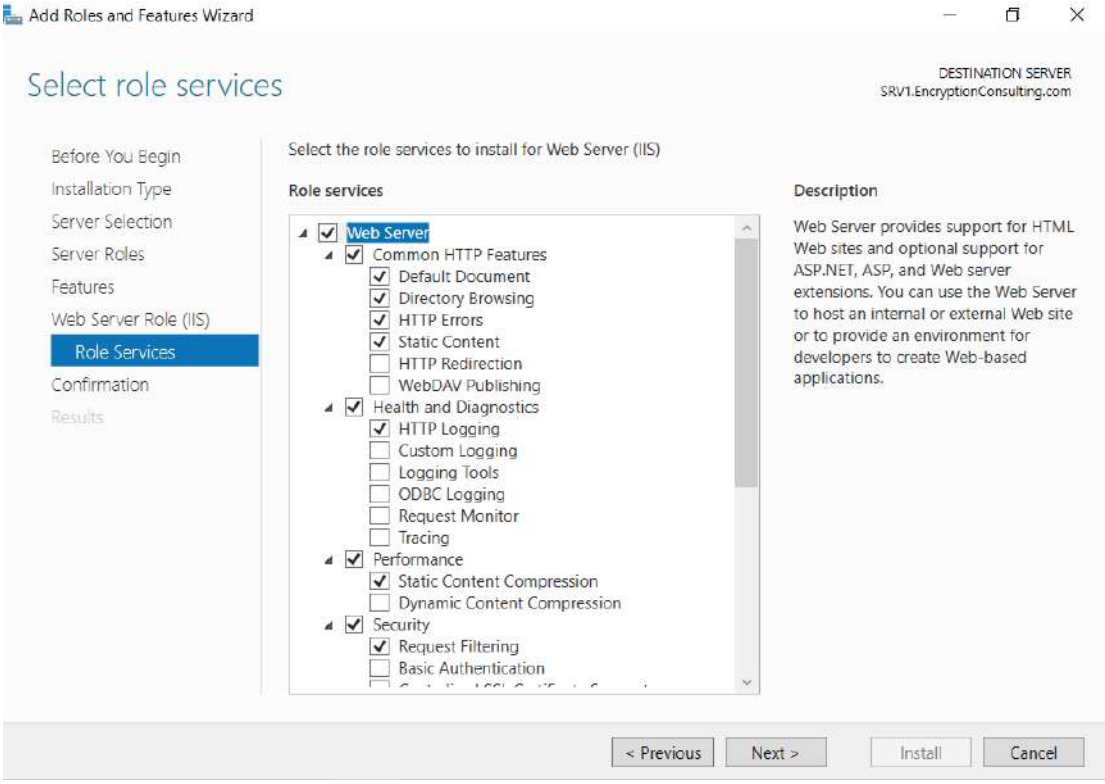


8. On the **Select features** page, click **next**

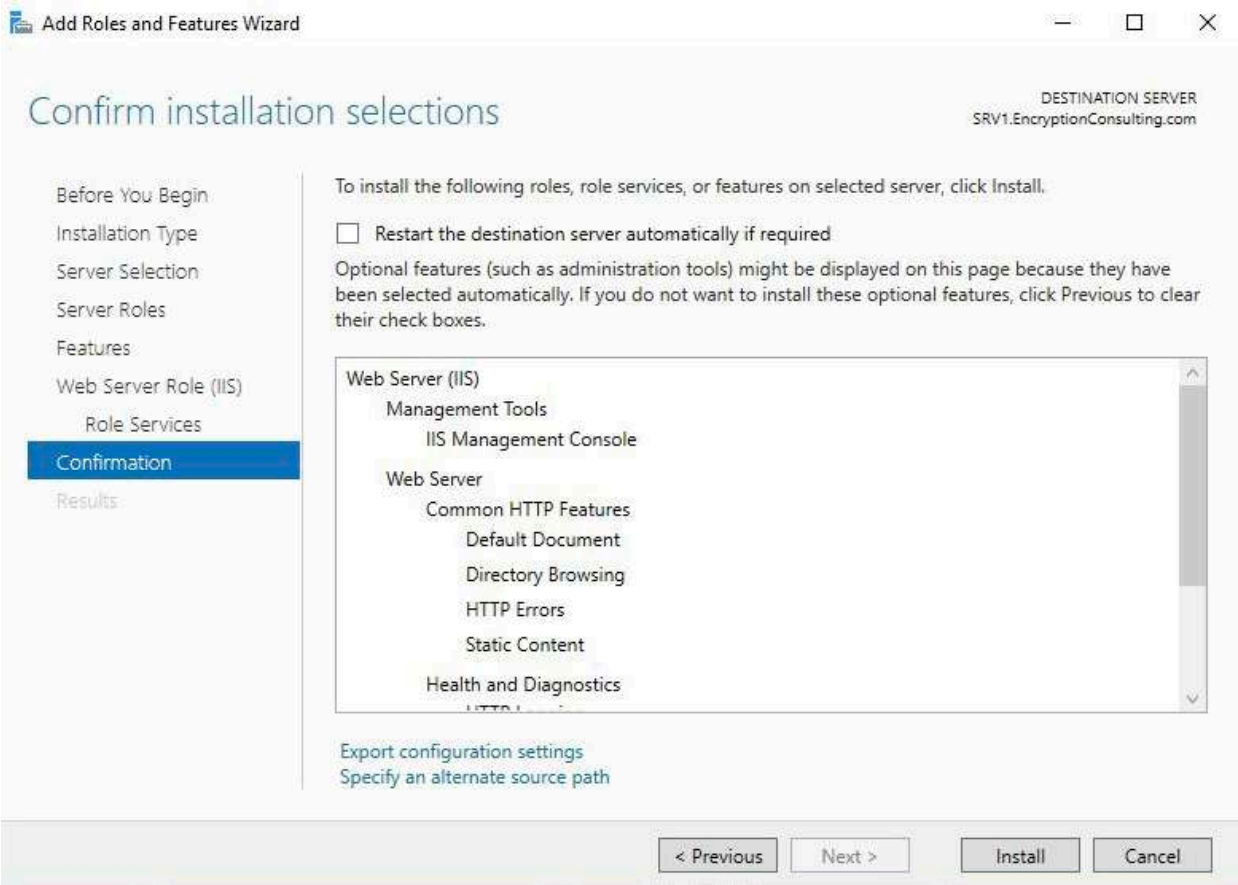
9. On **Web Server (IIS)** page, click **Next**



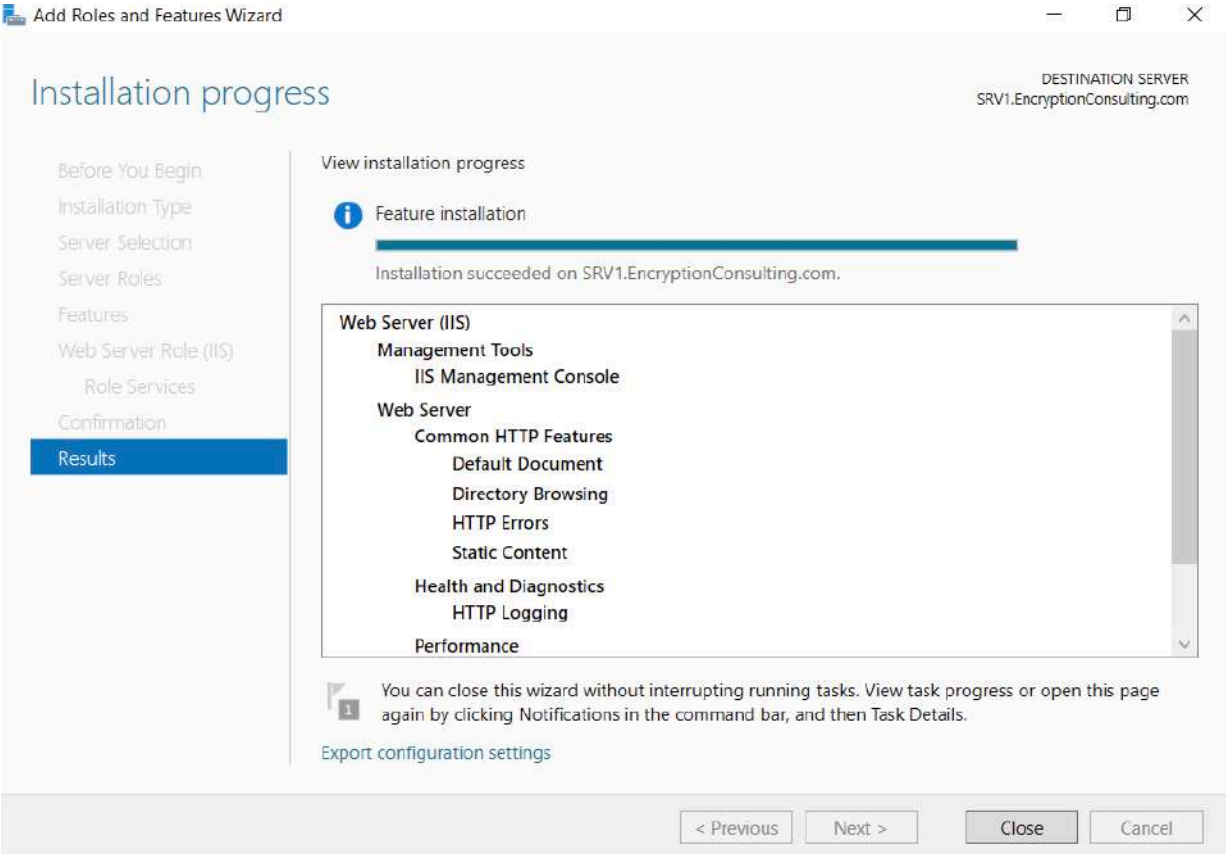
10. Leave the defaults on **Select Role Services** page and then click **Next.**



11. On **Confirm Installation Selections** page, click **Install.**

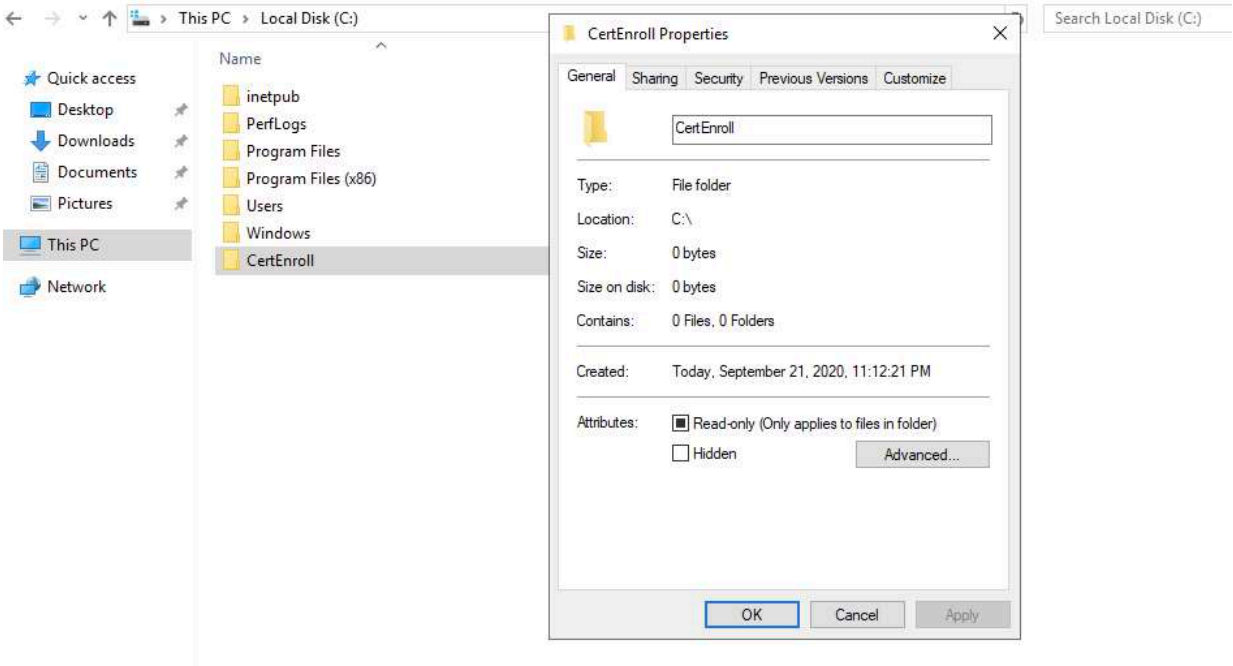


12. On the **Installation Results** page, click **Close**



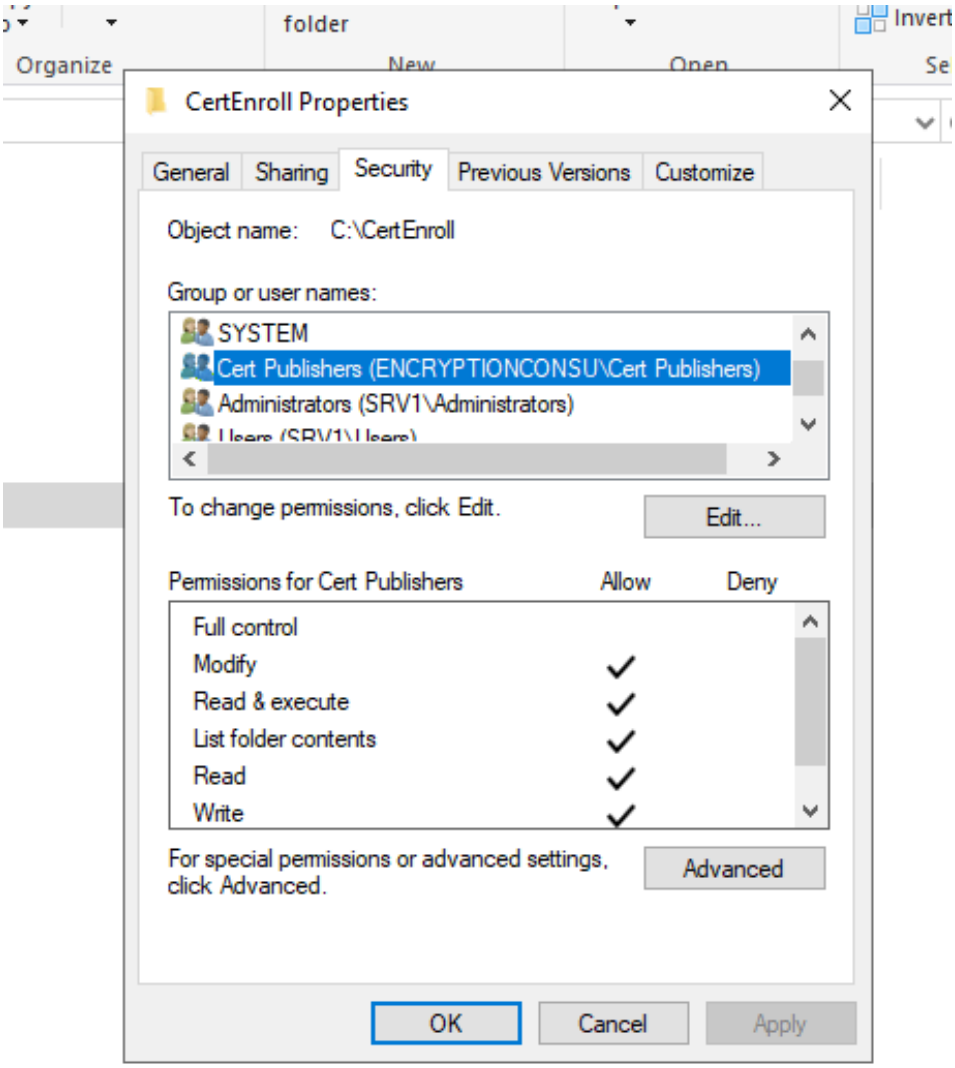
Task 5: Create CertEnroll Folder and grant Share & NTFS Permissions to Cert Publishers group

1. Log onto **SRV1.EncryptionConsulting.com** as **Encryptionconsu\Administrator.**
2. Click **Start** and select Computer to open **Windows Explorer** and then go to **C:** drive.
3. Create folder called **CertEnroll** at the root of **C:** drive.
4. Right-click on **CertEnroll** folder and select **Properties.**



5. On **CertEnroll Properties** page select **Sharing** tab to configure share permissions.
6. Click on **Advanced Sharing** option and then select **Share this folder.**
7. Click on **Permissions** and then click **Add.**
8. On **Select Users or Groups** page, in the **Enter the object names to select,** type **Encryptionconsu\Cert Publishers** and then click **OK.**
9. On **Permissions for CertEnroll** dialog box, select **Cert Publishers** group and then in the **Allow** column select **Change** permission. Click **OK** twice to go back to **CertEnroll Properties** page.

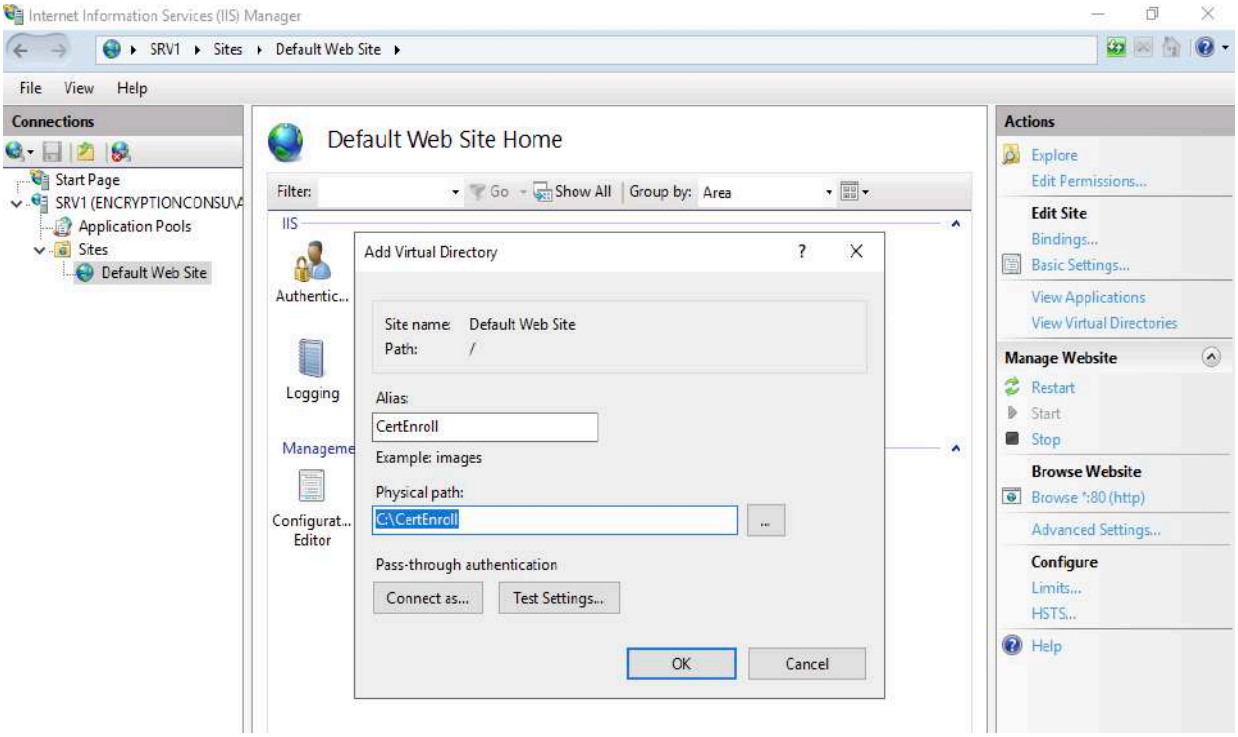
10. Select **Security** tab and click **Edit** to configure NTFS permissions.
11. On **Permissions for CertEnroll** page click **Add.**
12. On **Select Users or Groups** page, under the **Enter the object names to select**, enter **EncryptionConsulting\Cert Publishers** and then click **OK.**
13. On **Permissions for CertEnroll** page highlight **Cert Publishers** group and then under the **Allow** column select **Modify** permission. Click **OK.**



14. On **CertEnroll Properties** page, click **OK.**

Task 6: Create CertEnroll Virtual Directory in IIS

1. Ensure you are logged on to **SRV1.EncryptionConsulting.com** as **Encryptionconsu\Administrator.**
2. Click **Start, Administrative Tools** and then select **Internet Information Services (IIS) Manager.**
3. On the **Connections,** expand **SRV1** and then expand **Sites.**
4. Right-click on **Default Web Site** and select **Add Virtual Directory.**
5. On **Add Virtual Directory** page, in **Alias,** type **CertEnroll.** In **Physical path**, type **C:\Certenroll,** and then click **OK.**

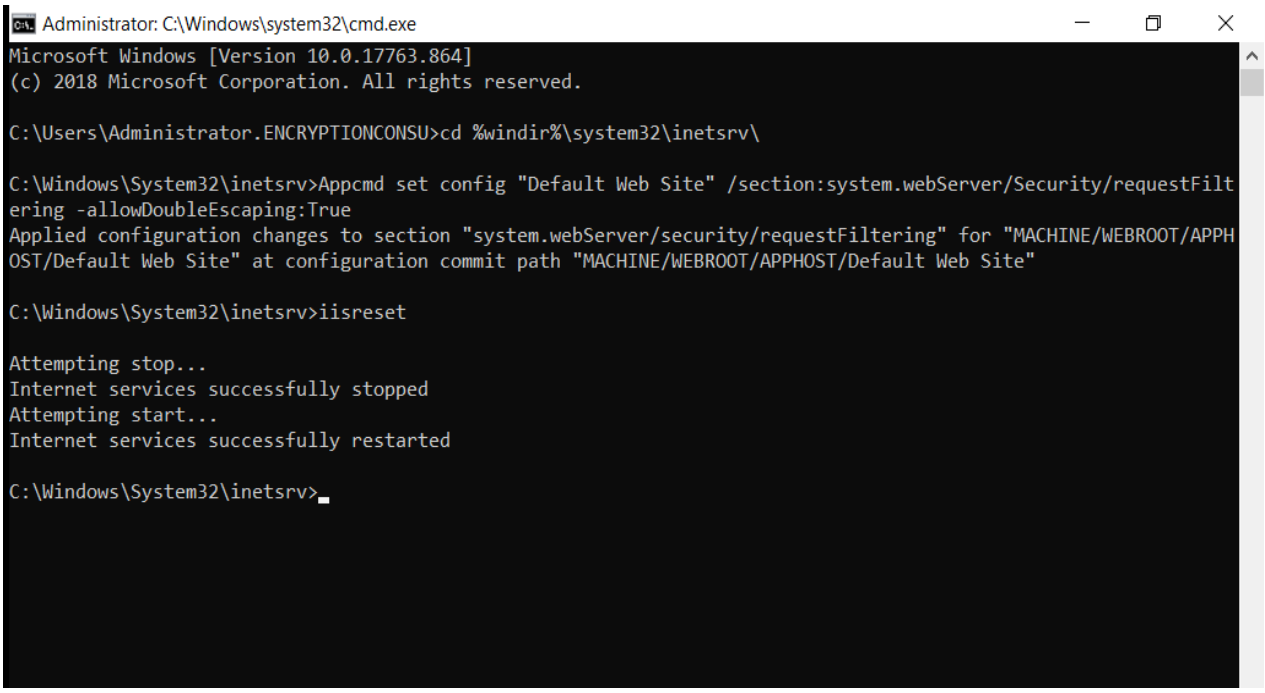


6. In the **Connections** pane, under the **Default Web Site,** ensure the **CertEnroll** virtual directory is selected.
7. In the **CertEnroll Home** pane, double-click on **Directory Browsing.**
8. In **Actions** pane click **Enable.**

Task 7: Enable Double Escaping on IIS Server

Allowing double escaping makes it possible for the web server to host Delta CRLs.

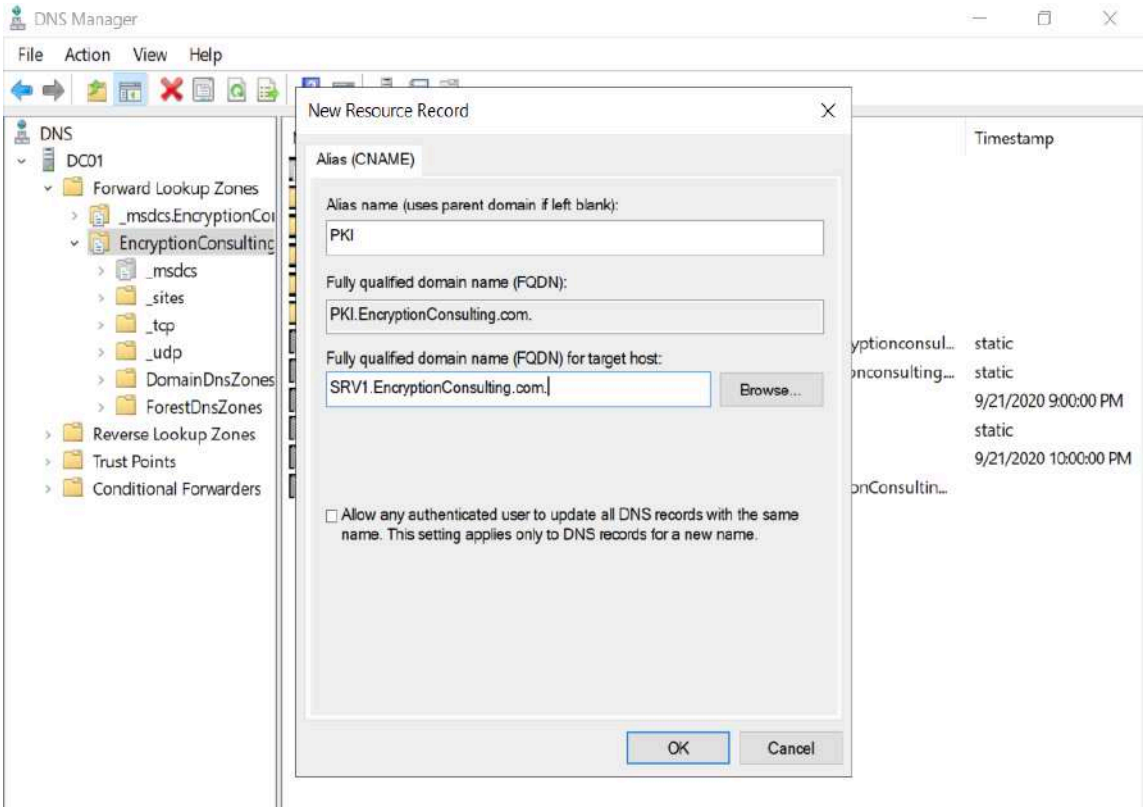
1. Ensure you are logged on to **SRV1.EncryptionConsulting.com** as **Encryptionconsu\Administrator.**
2. Open a Command Prompt. To do so, click **Start,** click **Run,** and then type **cmd.** Click **OK.**
3. Then type **cd %windir%\system32\inetsrv**\ and press ENTER.
4. Type following command and press **Enter. Appcmd set config "Default Web Site" /section:system.webServer/Security/requestFiltering -allowDoubleEscaping:True**
5. Restart IIS service. To do so, type **iisreset** and press ENTER.

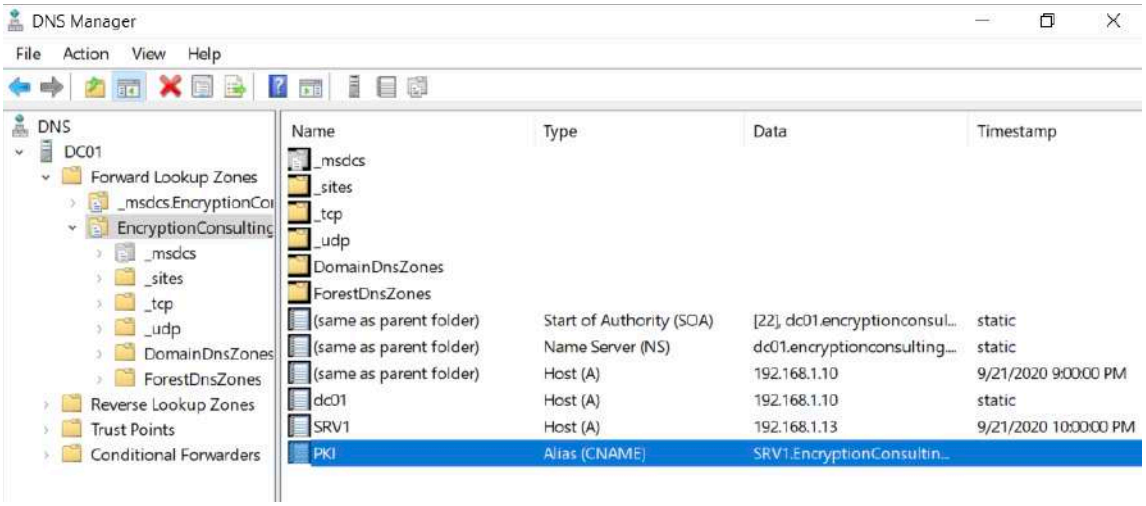


Task 8: Create CNAME (pki.EncryptionConsulting.com) in DNS

1. Ensure that you are logged on to **DC01.EncryptionConsulting.com** as **Encryptionconsu\Administrator.**
2. Open the DNS Console. You can do so by clicking **Start,** click **Run,** and then type **dnsmgmt.msc.** Click **OK.**
3. Expand **Forward Lookup Zones**, select and then right-click **EncryptionConsulting.com zone.** Click **New Alias (CNAME).**
4. In **Alias name (uses parent domain if left blank)**, type **PKI.** In the **Fully qualified domain name (FQDN) for target host** field, type **SRV1.EncryptionConsulting.com.** and then click **OK.**

Note - Include the terminating "." in the FQDN in the previous step. In a production environment this alias can resolve to a lad balancer which distributes requests to any number of web servers that contain the CA certificates and CRLs.





Activity 2: Install the Standalone Offline Root CA

The standalone offline root CA should not be installed in the domain. As a matter of fact, it should not even be connected to a network at all.

Task 1: Create a CAPolicy.inf for the standalone offline root CA

To create a CAPolicy.inf for the standalone offline root CA:

1. Log onto CA01 as **CA01\Administrator.**
2. Click **Start,** click **Run** and then type **notepad C:\Windows\CAPolicy.inf** and press ENTER.
3. When prompted to create new file, click **Yes.**
4. Type in following as contents of the file.

```
[Version]
Signature="$Windows NT$"
[Certsrv_Server]
RenewalKeyLength=2048 ; recommended 4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
AlternateSignatureAlgorithm=0
```

   - Click File and Save to save the CAPolicy.inf file under C:\Windows directory.

     Warning CAPolicy.inf with the .inf extension. Type .inf at the end of the file name and select the options as described, the file will be saved as a text file and will not be used during CA installation.

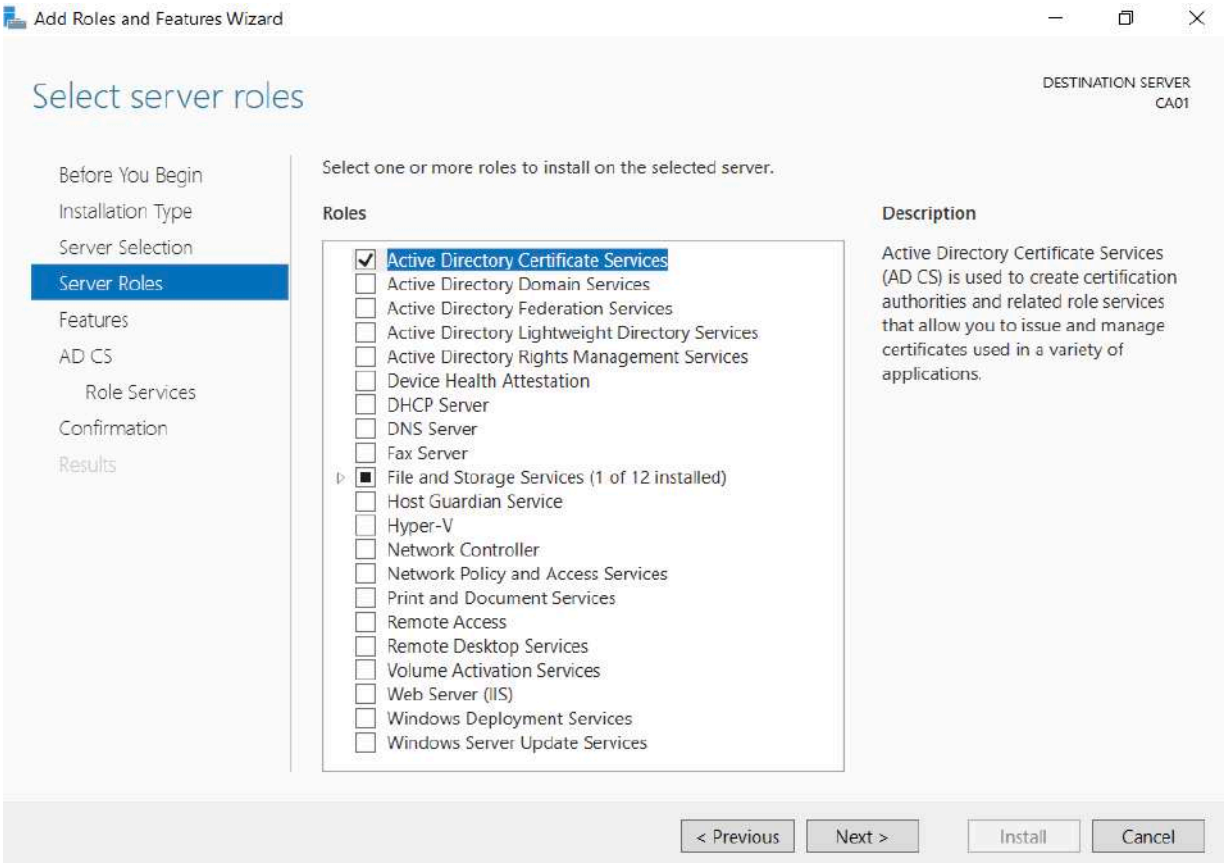
5. Close Notepad.

NOTE: Make sure you change the computer name as "CA01". Windows > Run > sysdm.cpl > Change the computer name and restart the machine.

Task 2: Installing the Standalone Offline Root CA

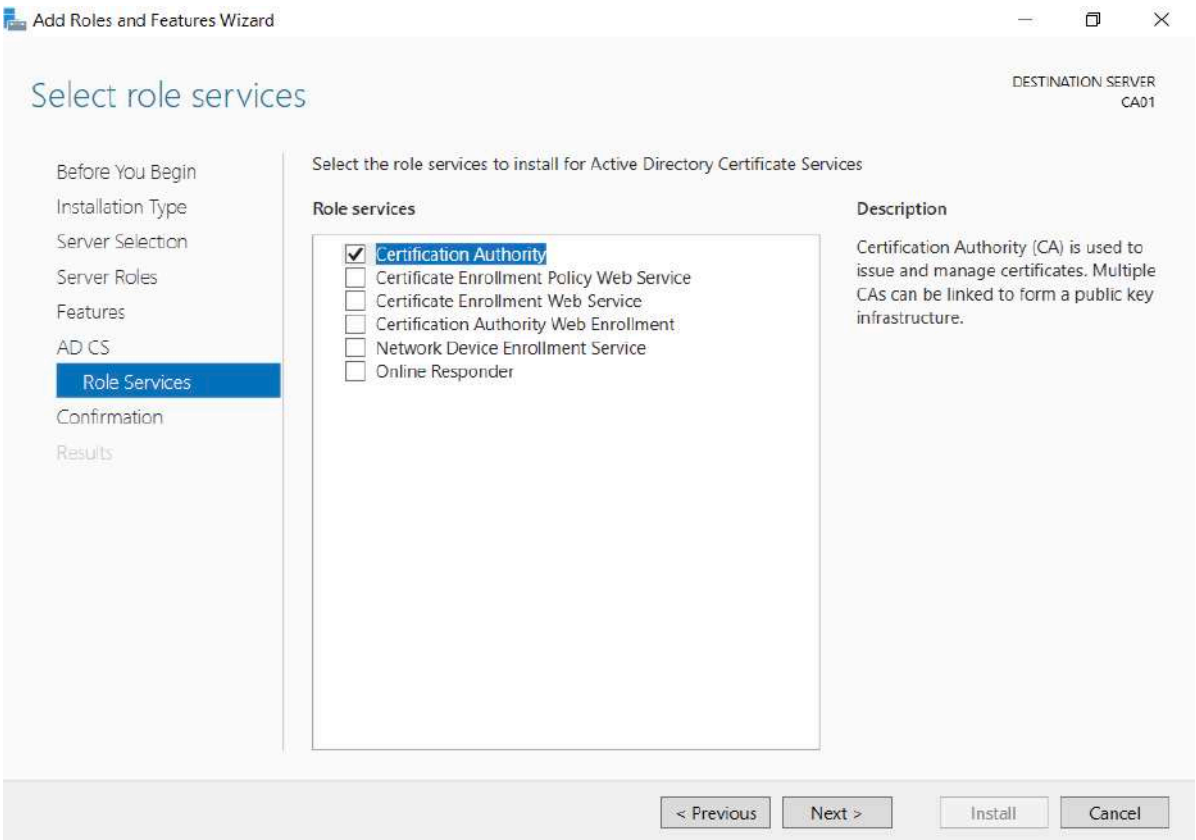
To install the standalone offline root CA:

1. Log onto CA01 as CA01\Administrator.
2. Click **Start**, click **Administrative Tools,** and then click **Server Manager.**
3. Right-click on **Roles** and then click **Add Roles.**
4. On the **Before You Begin** page click **Next.**
5. On the **Installation Type** page, choose **Role based or Featured based installation** and then click **Next.**
6. On the **server selection** page, click **next.**
7. On the **Select Server Roles** page select **Active Directory Certificate Services,** and then click **Next.**

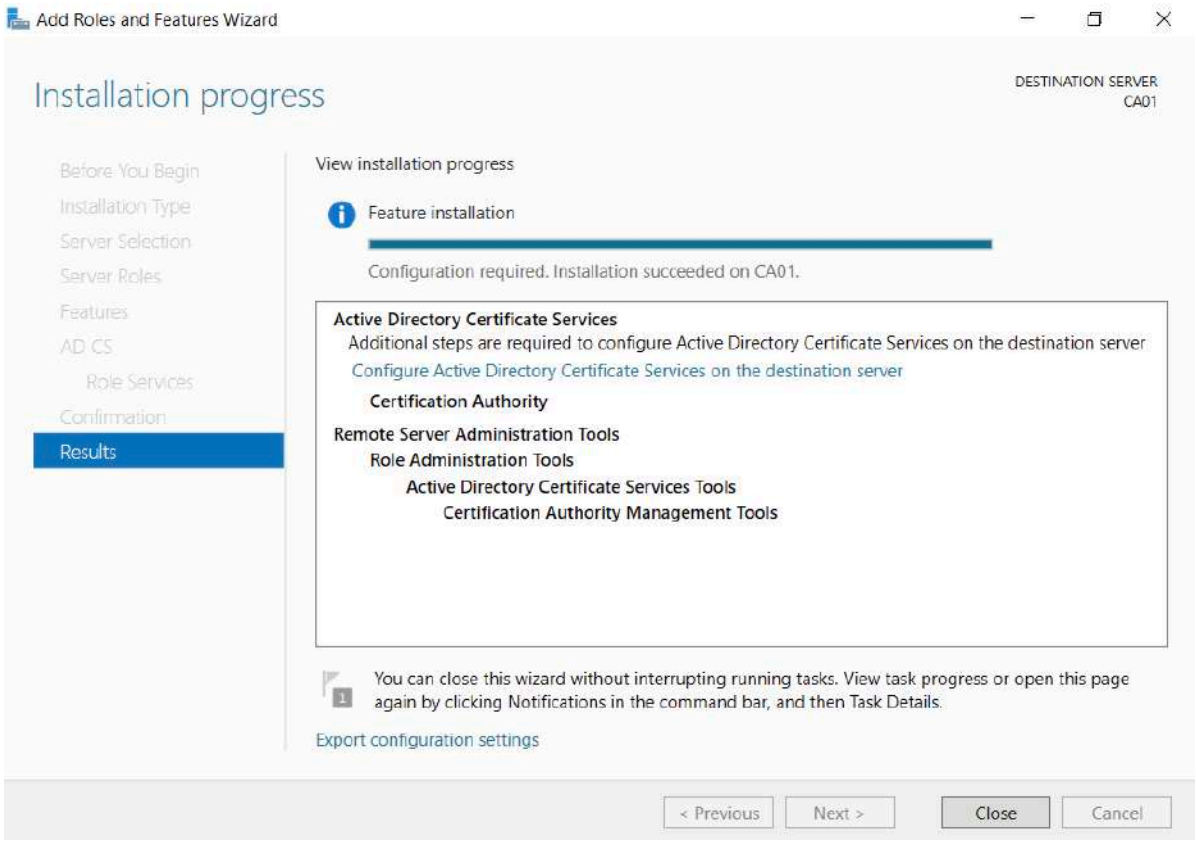


8. On the select features page, click next.
9. On the Introduction to Active Directory Certificate Services page, click Next.

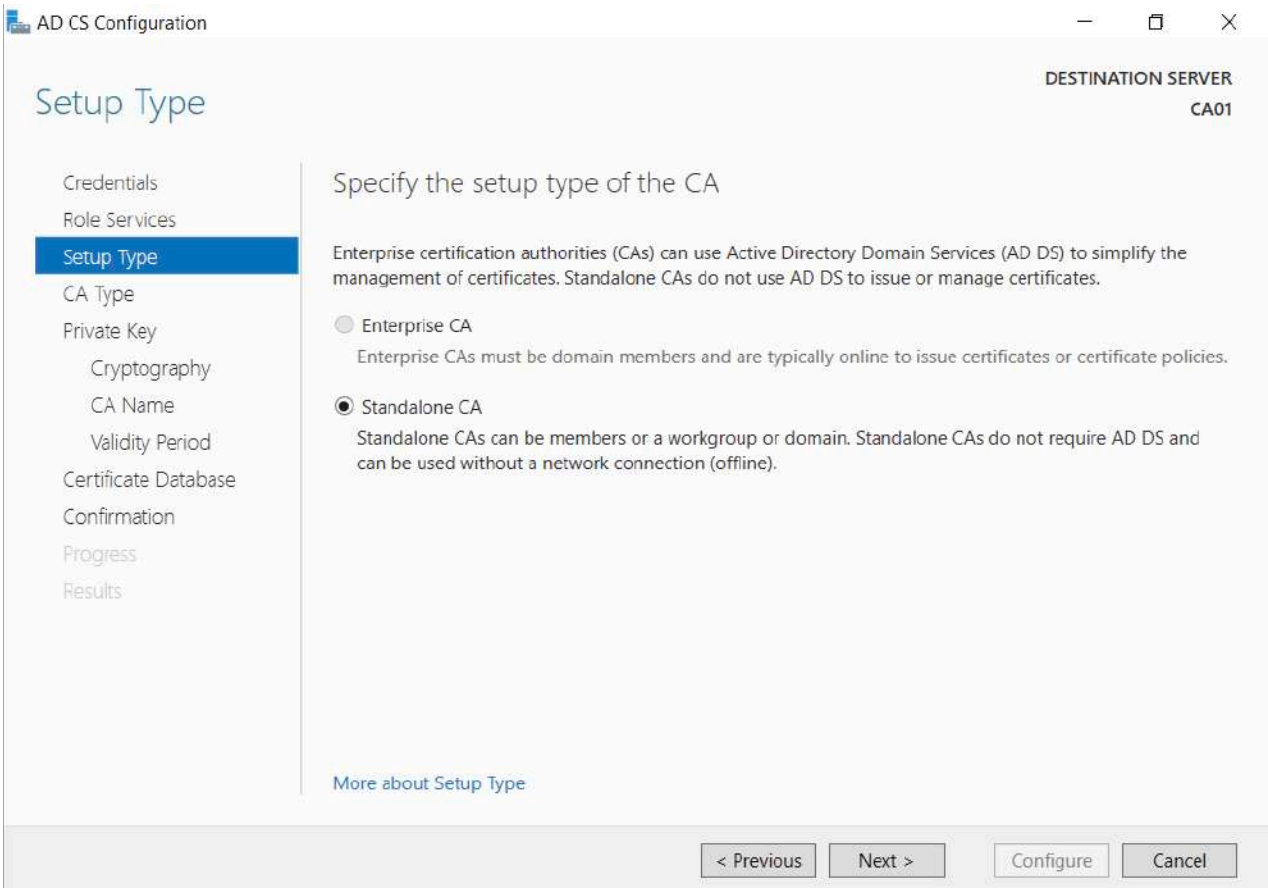
10. On the Select Role Services page, ensure that Certification Authority is selected, and then Next.



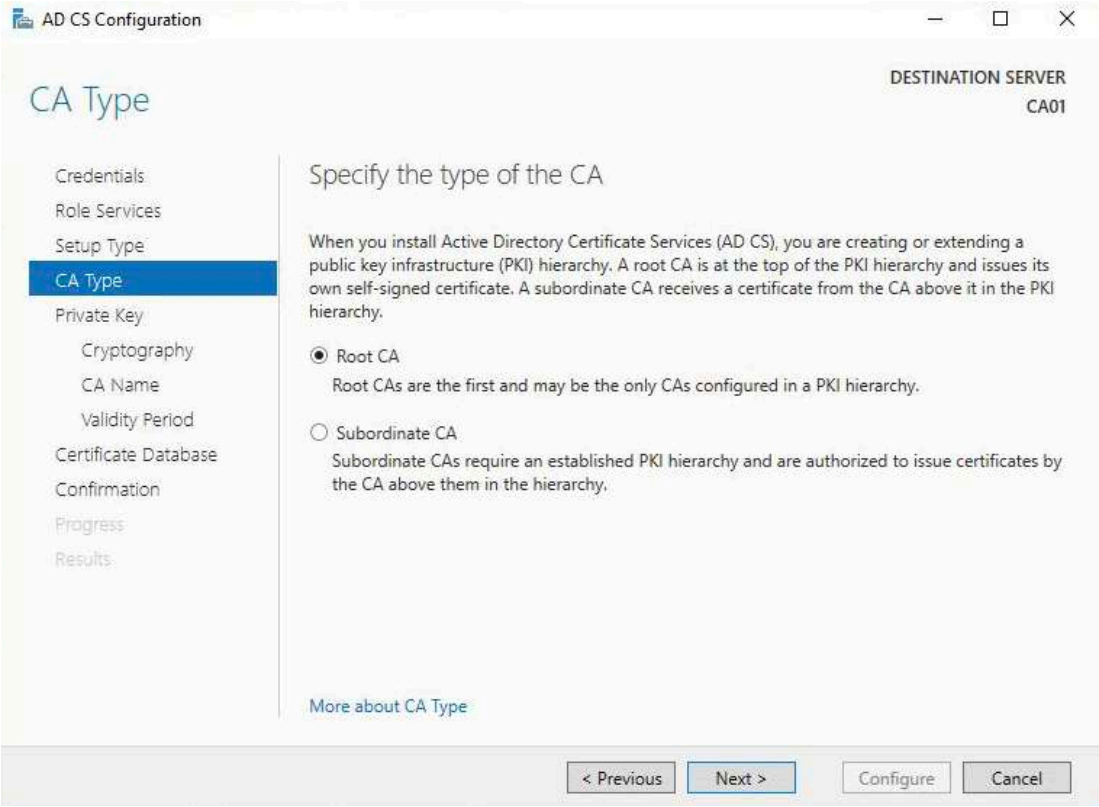
11. On the confirmation page, click install



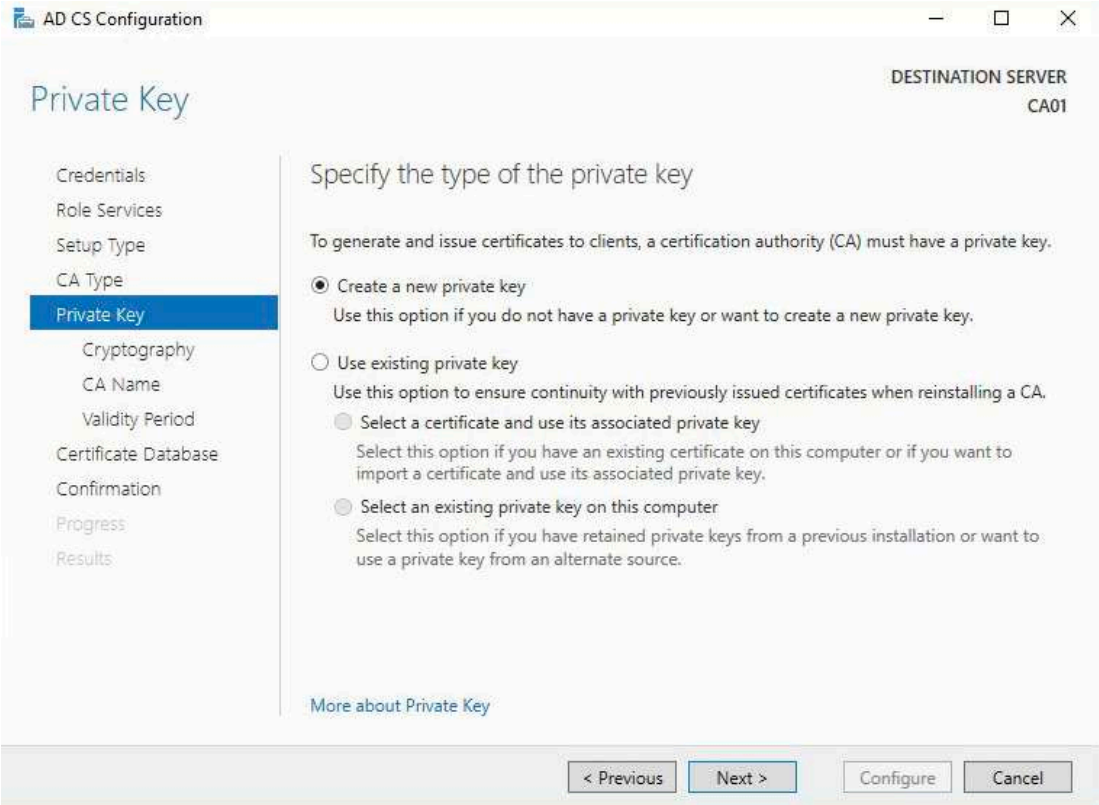
12. Click on configure "Active Directory Certificate Services on the destination server".
13. On the **Specify Credential to configure roles and services** page, credential should be **CA01\Administrator,** then click **Next.**
14. On the **Select Role services to configure** page, choose **Certificate Authority** and then click **Next.**
15. On the **Specify Setup Type** page, ensure that **Standalone** is selected, and then click **Next.**
    - Note: Enterprise option is greyed out as CA01 server is not joined to Active Directory domain.



16. On the **Specify CA Type** page, ensure that **Root CA** is selected, and then click **Next.**



17. On the **Set Up Private Key** page, ensure that **Create a new private key** is selected, and then click **Next.**

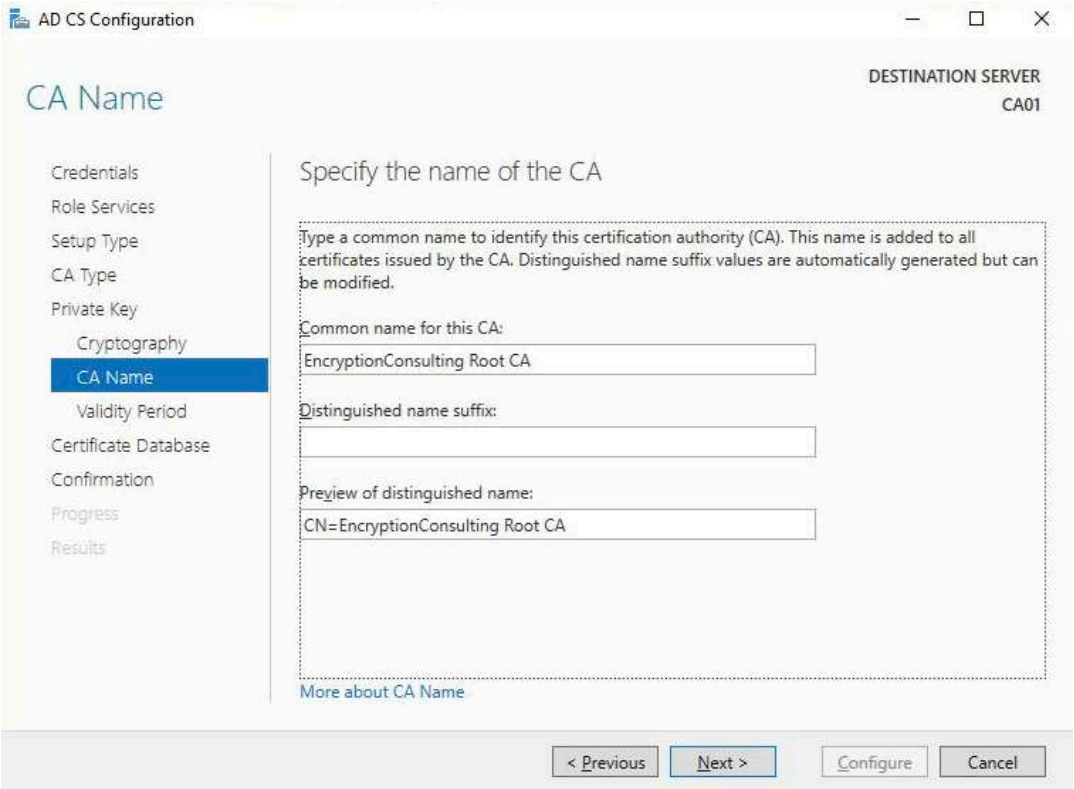


18. Leave the defaults on the **Configure Cryptography for CA** page, and then click **Next.**

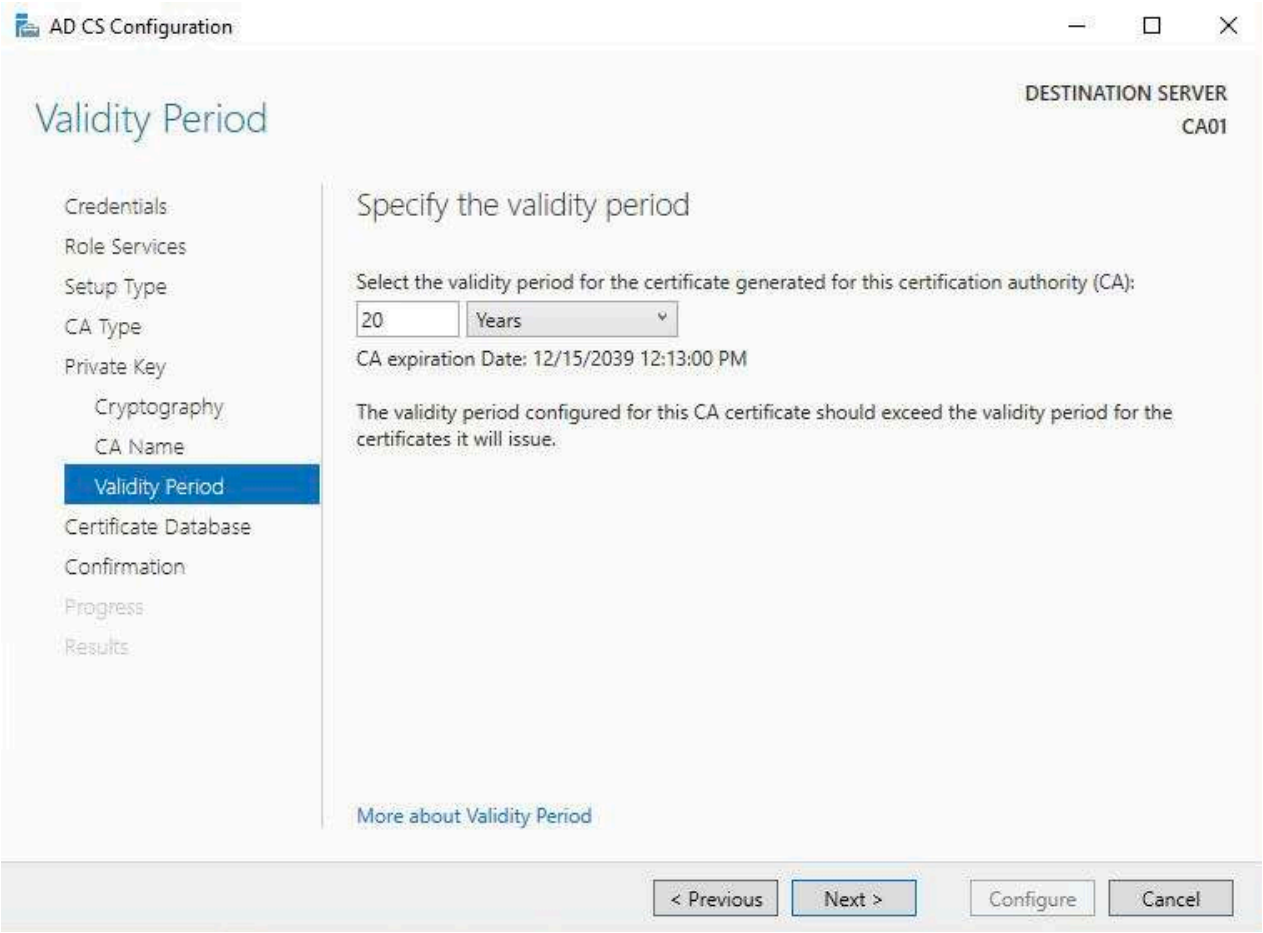
- **Important:** In a production environment, you would set the CSP, Hash Algorithm, and Key length to meet application compatibility requirements.

19. On **Configure CA Name** page, under Common name for this CA, clear the existing entry and type **EncryptionConsulting Root CA.** Click **Next.**

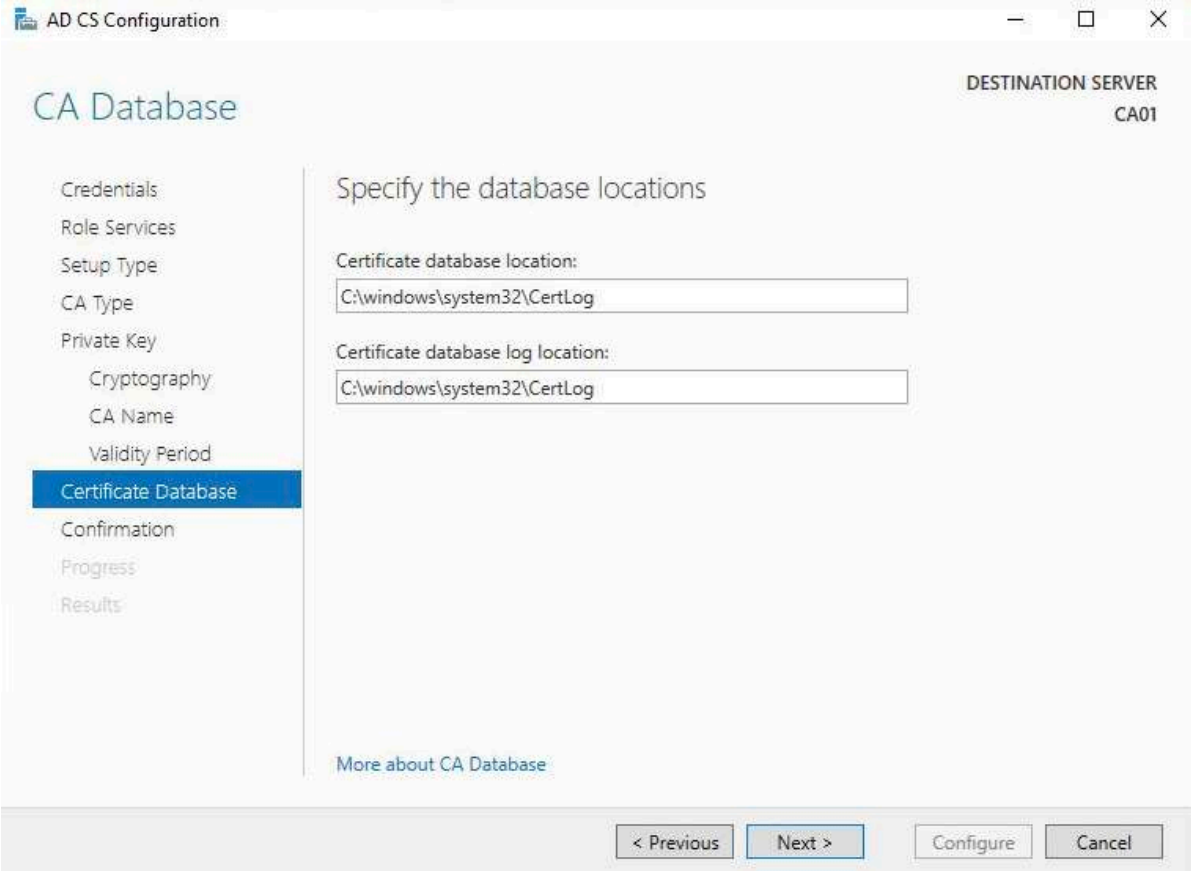
Note: A **Distinguished Name Suffix** is optional for a root CA. This will be configured in a later step.



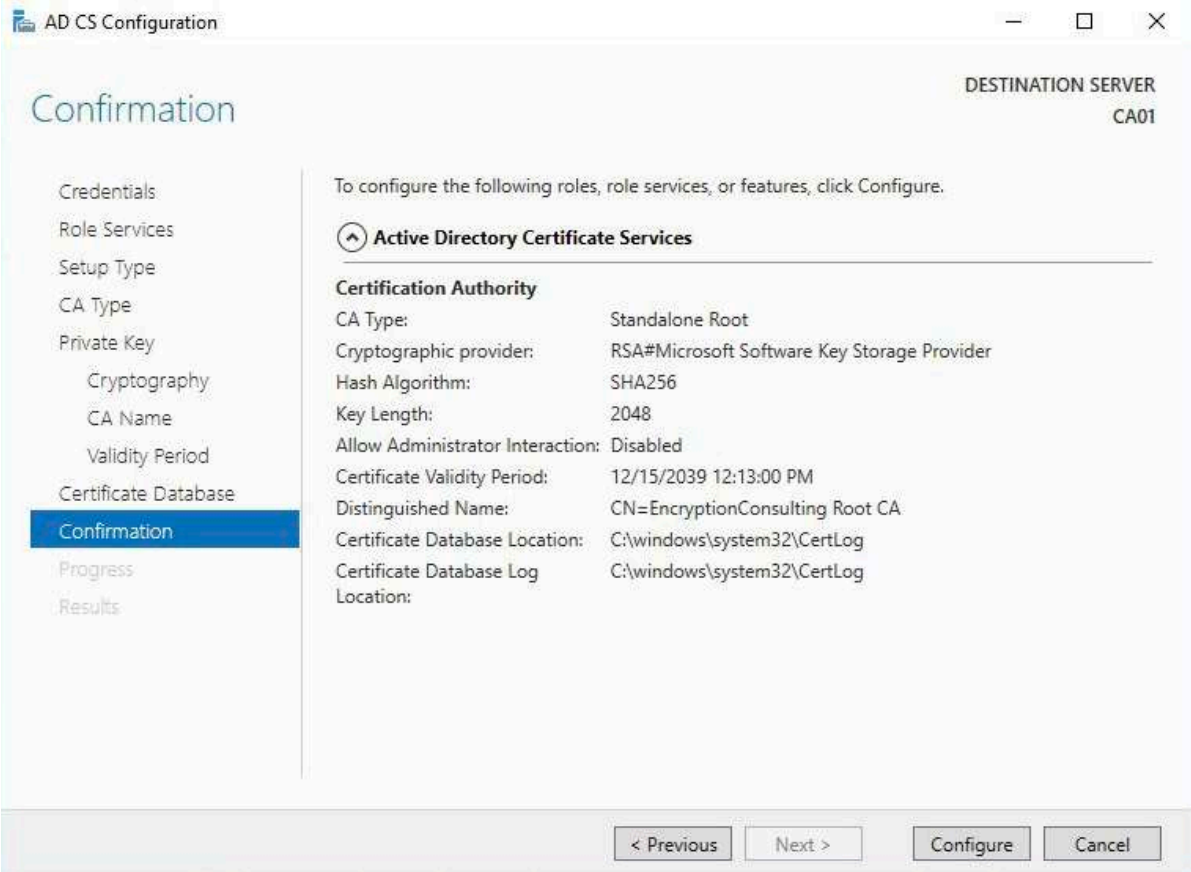
20. On **Set Validity Period** page, under **Select validity period for the certificate generated for this CA,** clear the existing entry and then type **20.** Leave the selection box set to **Years.** Click **Next.**



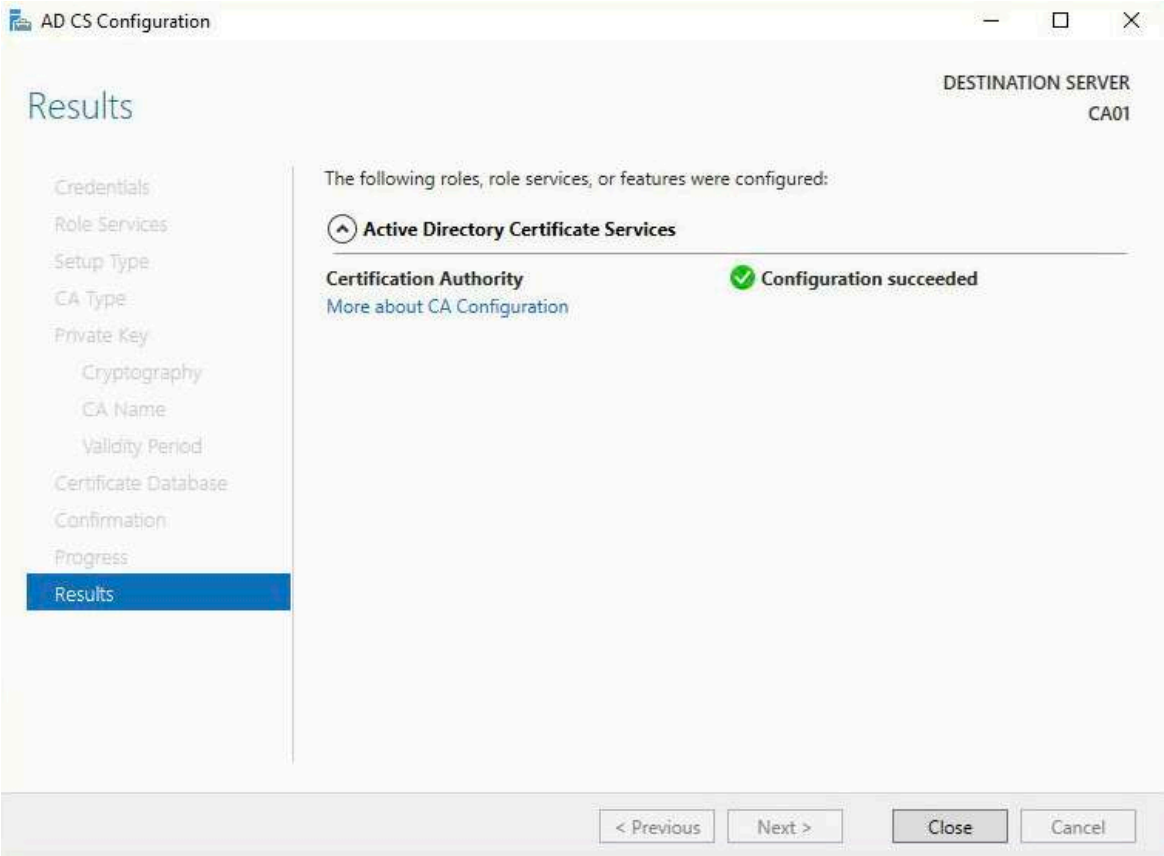
21. Keep the default settings on the **Configure Certificate Database** page, and then click **Next.**



22. On the **Confirm Installation Selections** page, review the settings, and then click **Configure.**



23. Review the information on the **Installation Results** page to verify that the installation is successful and then click **Close.**



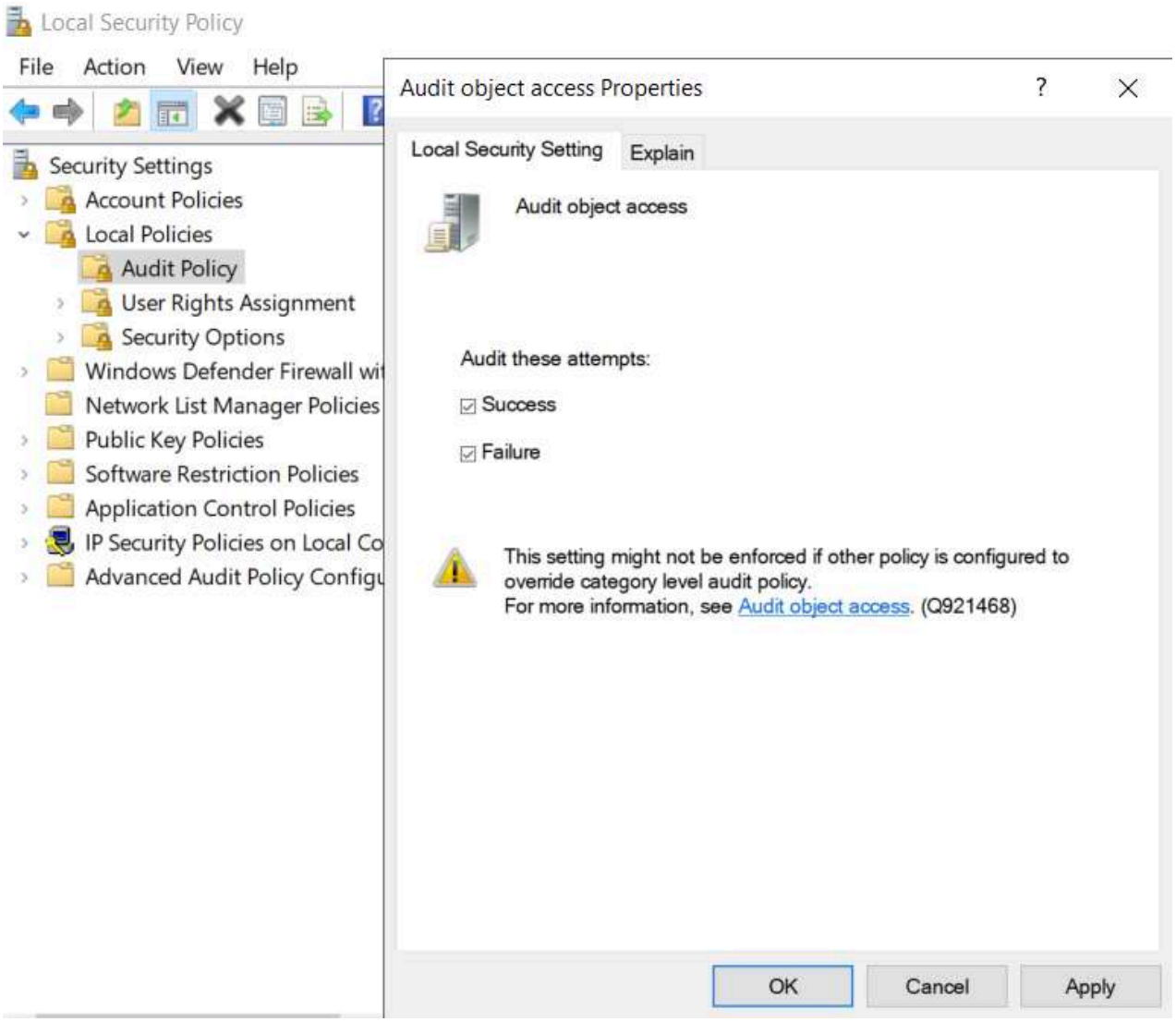
Activity 3: Perform Post Installation Configuration for Root CA

1. Ensure that you are logged on to **CA01** as **CA01\Administrator.**
2. Open a command prompt. To do so, you can click **Start,** click **Run,** type **cmd** and then click **OK.**
3. To define Active Directory Configuration Partition Distinguished Name, run the following command from an administrative command prompt:
   - **Certutil -setreg CA\DSConfigDN "CN=Configuration,DC=EncryptionConsulting,DC=com"**
4. To define **CRL Period Units** and **CRL Period,** run the following commands from an administrative command prompt:
   - **Certutil -setreg CA\CRLPeriodUnits 52**
   - **Certutil -setreg CA\CRLPeriod "Weeks"**
   - **Certutil -setreg CA\CRLDeltaPeriodUnits 0**
5. To define **CRL Overlap Period Units** and **CRL Overlap Period,** run the following commands from an administrative command prompt:
   - **Certutil -setreg CA\CRLOverlapPeriodUnits 12**
   - **Certutil -setreg CA\CRLOverlapPeriod "Hours"**
6. To define **Validity Period Units** for all issued certificates by this CA, type following command and then press Enter. In this lab, the Enterprise Issuing CA should receive a 10 year lifetime for its CA certificate. To configure this, run the following commands from an administrative command prompt:
   - **Certutil -setreg CA\ValidityPeriodUnits 10**
   - **Certutil -setreg CA\ValidityPeriod "Years"**

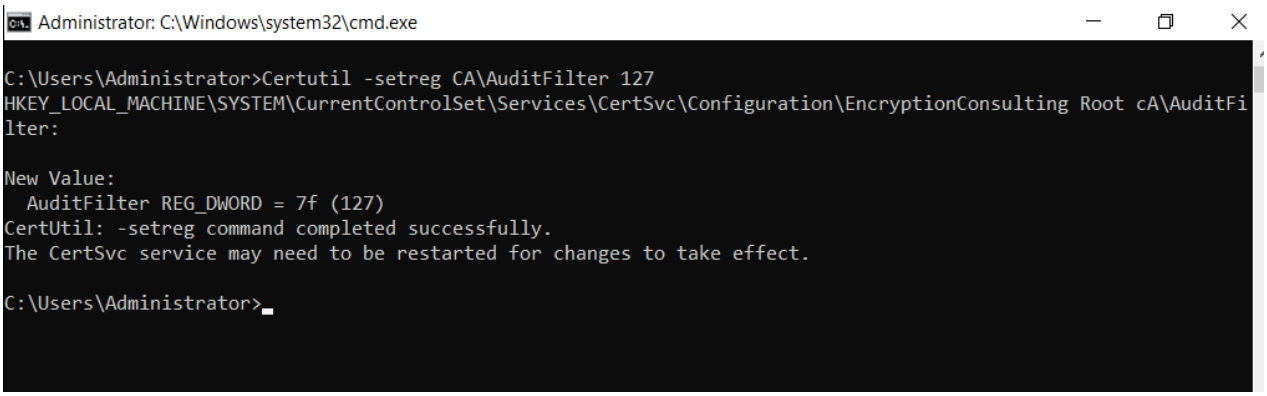
Task 1: Enable Auditing on the Root CA

CA auditing depends on system **Audit Object Access** to be enabled. The following instructions describe how to use Local Security Policy to enable object access auditing.

1. Click **Start,** click **Administrative Tools,** and then select **Local Security Policy.**
2. Expand **Local Policies** and then select **Audit Policy.**
3. Double click **Audit Object Access** and then select **Success** and **Failure** then click **OK.**



4. Close Local Security Policy editor.
5. Enable auditing for the CA by selecting which group of events to audit in the Certificate Authority MMC snap-in or by configuring AuditFilter registry key setting. To configure Auditing for all CA related events, run the following command from an administrative command prompt: **Certutil -setreg CA\AuditFilter 127**



Task 2: Configure the AIA and CDP

There are multiple different methods for configuring the Authority Information Access (AIA) and certificate revocation list distribution point (CDP) locations. You can use the user interface (in the Properties of the CA object), certutil, or directly edit the registry. The AIA is used to point to the public key for the certification authority (CA). The CDP is where the certificate revocation list is maintained, which allows client computers to determine if a certificate has been revoked. In this lab there will be three locations for the AIA and four locations for the CDP.

Task 3: Configure the AIA

Using a certutil command is a quick and common method for configuring the AIA. When you run the following certutil command, you will be configuring a static file system location, a lightweight directory access path (LDAP) location, and http location for the AIA. The certutil command to set the AIA modifies the registry, so ensure that you run the command from an command prompt run as Administrator. Run the following command:

certutil -setreg CA\CACertPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\ %1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA, CN=Public Key Services,CN=Services,%6%11\n2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt"

After you have run that command, run the following command to confirm your settings:

certutil -getreg CA\CACertPublicationURLs

If you look in the registry, under the followingpath:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Root CA, you can confirm the CACertPublicationURLs by opening that REG_MULTI_SZ value. You should see the following:

1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt

2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt

You can also see this in the the CA (certsrv) console. To open the console, click **Start,** click **Administrative Tools,** and then click **Certification Authority.** In the navigation pane, expand the **Certificate Authority(Local).** Right-click **EncryptionConsulting Root CA** and then click **Properties**. On the **Extensions** tab, under **Select extension,** click **Authority Information Access (AIA)** and you will see the graphical representation of the AIA settings.

Task 4: Configure the CDP

The certutil command to set the CDP modifies the registry, so ensure that you run the command from an command

certutil -setreg CA\CRLPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n10:ldap:///CN=%7%8,CN=%2, CN=CDP,CN=Public Key Services,CN=Services,%6%10\n2:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl"

After you run that command, run the following certutil command to verify your settings:

certutil -getreg CA\CRLPublicationURLs

In the registry

location: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Root CA** you can open the REG_MULTI_SZ valueand see the configuration of these values:

1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl

10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

2:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl

You can also see this in the the CA (certsrv) console. To open the console, click **Start,** click **Administrative Tools,** and then click **Certification Authority.** In the navigation pane, ensure that **Certificate Authority (Local)** is expanded. Right-click **EncryptionConsultng Root CA** and then click **Properties.** On the **Extensions** tab, under **Select extension,** click **CRL Distribution Point (CDP)** and you will see the graphical representation of the CDP settings.

At an administrative command prompt, run the following commands to restart Active Directory Certificate Services and to publish the CRL.

net stop certsvc

Net start certsvc

certutil -crl

Activity 4: Install Enterprise Issuing CA

Task 1: Join CA02 to the domain

1. Log on to CA02 as the local administrator.
2. Click **Start,** type **ncpa.cpl** and press ENTER.
3. In Network Connections, right-click the **Local Area Connection** and then click **Properties.**
4. Click the **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties.**
5. Select the **Use the Following IP address.** Configure the **IP address, Subnet mask,** and **Default gateway** appropriately for your test network.
    - **IP Address:** 192.168.1.12
    - **Subnet mask**: 255.255.255.0
    - **Default gateway**: <optional>
6. Select the Use the following DNS server address. Configure the **Preferred DNS server** for the IP address of your domain controller. Click **OK**. Click **Close.**
    - **Preferred DNS Server**: 192.168.1.10
7. Click **Start,** type **sysdm.cpl** and press ENTER. Click **Change.**
8. In **Computer name,** type **CA02** and then click **OK.**
9. When prompted that you need to restart the computer, click **OK.** Click **Close.** Click **Restart Now.**
10. After CA02 restarts, log on as a local administrator.
11. Click **Start,** type **sysdm.cpl** and press ENTER. Click **Change.**
12. In **Member of,** select **Domain,** and then type **EncryptionConsulting.com.** Click **OK.**
13. In **Windows Security,** enter the **User name** and **password** for the domain administrator account. Click **OK.**
14. You should be welcomed to the EncryptionConsulting domain. Click **OK.**
15. When prompted that a restart is required, click **OK.** Click **Close.** Click **Restart Now.**

Task 2: Create CAPolicy.inf for Enterprise Root CA

1. Log onto CA02.EncryptionConsulting.com as EncryptionConsulting\Administrator. (Ensure that you switch user to log on as EncryptionConsulting\Administrator)
2. Click Start, select Run and then type notepad C:\Windows\CAPolicy.inf and press ENTER.
3. When prompted to create new file, click Yes.
4. Type in following as content of the file.

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
```

OID= 1.2.3.4.1455.67.89.5

URL=http://pki.EncryptionConsulting.com/cps.txt

[Certsrv_Server]

RenewalKeyLength=2048

RenewalValidityPeriod=Years

RenewalKeyLength=2048

RenewalValidityPeriod=Years

AlternateSignatureAlgorithm=0

5. Click **File** and **Save** to save the **CAPolicy.inf** file under **C:\Windows** directory.

   Important: Ensure that the **CAPolicy.inf** is saved as an **.inf** file. The file will not be used if it is saved with any other file extension.

6. Close Notepad.

Task 3: Publish the Root CA Certificate and CRL

1. Ensure you are logged on to CA02. **EncryptionConsulting.com** as **EncryptionConsulting\Administrator.**
2. Copy Root CA Certificate (CA01_EncryptionConsulting Root CA.crt) and Root CA CRL(EncryptionConsulting Root CA.crl) files from C:\Windows\System32\CertSrv\CertEnroll directory on CA01 server to removable media (A:).
3. On CA02, to publish EncryptionConsulting Root CA Certificate and CRL in Active Directory, run the following commands at an administrative command prompt. Ensure that you substitute the correct drive letter of your removable media (for A:) in the commands that follow:

   certutil -f -dspublish "A:\CA01_EncryptionConsulting Root CA.crt" RootCA

   certutil -f -dspublish "A:\EncryptionConsulting Root CA.crl" CA01

4. To publish EncryptionConsulting Root CA Certificate and CRL to http://pki. EncryptionConsulting.com/CertEnroll, copy EncryptionConsulting Root CA Certificate and CRL to \\srv1.

   EncryptionConsulting.com\C$\CertEnroll directory. Run the following commands from an administrative command prompt. Ensure that you substitute the correct drive letter of your removable media (for A:)

   copy "C:\CA01_EncryptionConsulting Root CA.crt" \\SRV1.EncryptionConsulting.com\C$\CertEnroll

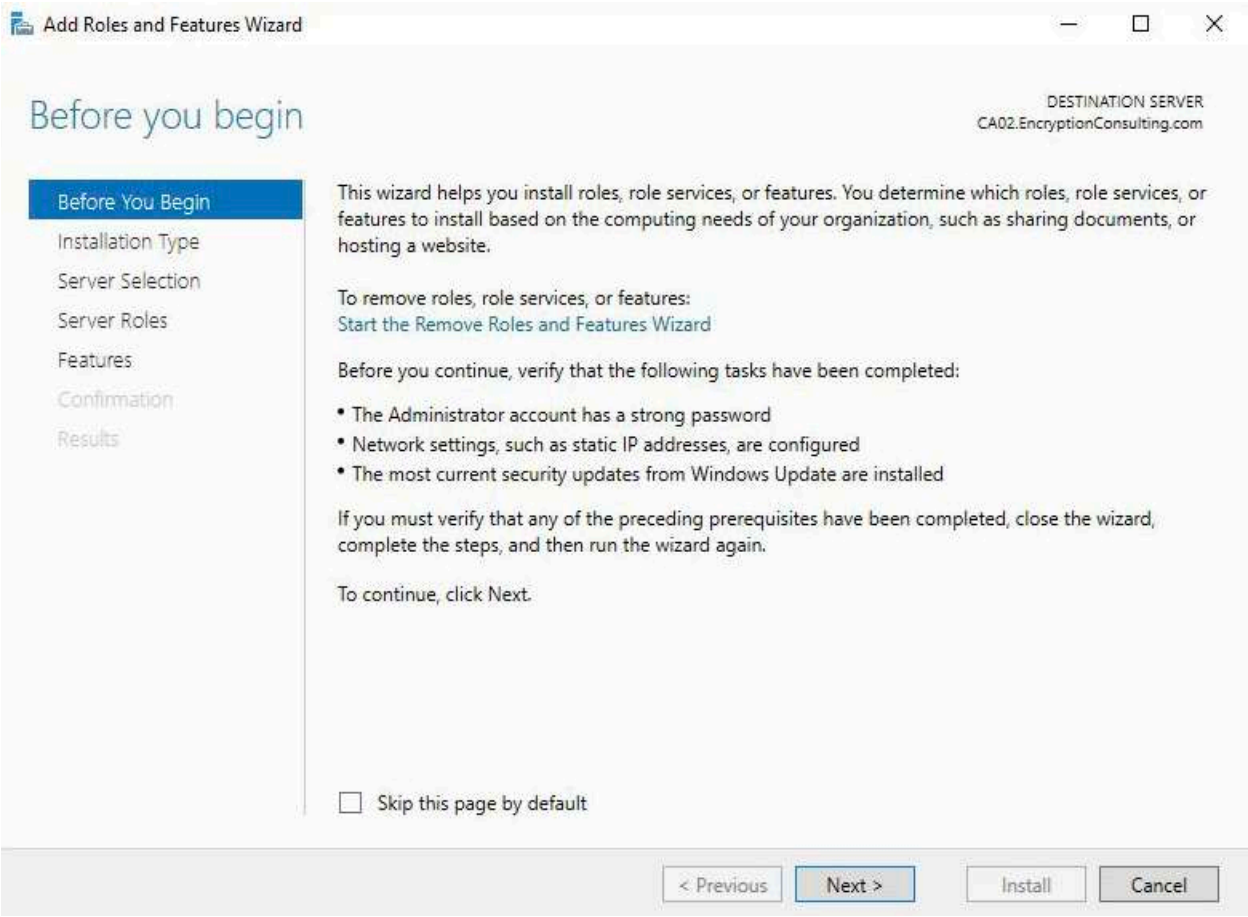
   copy "C:\EncryptionConsulting Root CA.crl" \\SRV1.EncryptionConsulting.com\C$\CertEnroll

5. To add EncryptionConsulting Root CA Certificate and CRL in CA02. EncryptionConsulting.com local store, run the following command from an administrative command prompt. Ensure that you substitute the correct drive letter of your removable media (for A:) in the commands that follow:
   - **certutil -addstore -f root "CA01_ EncryptionConsulting Root CA.crt"**
   - **certutil -addstore -f root " EncryptionConsulting CA.crl"**

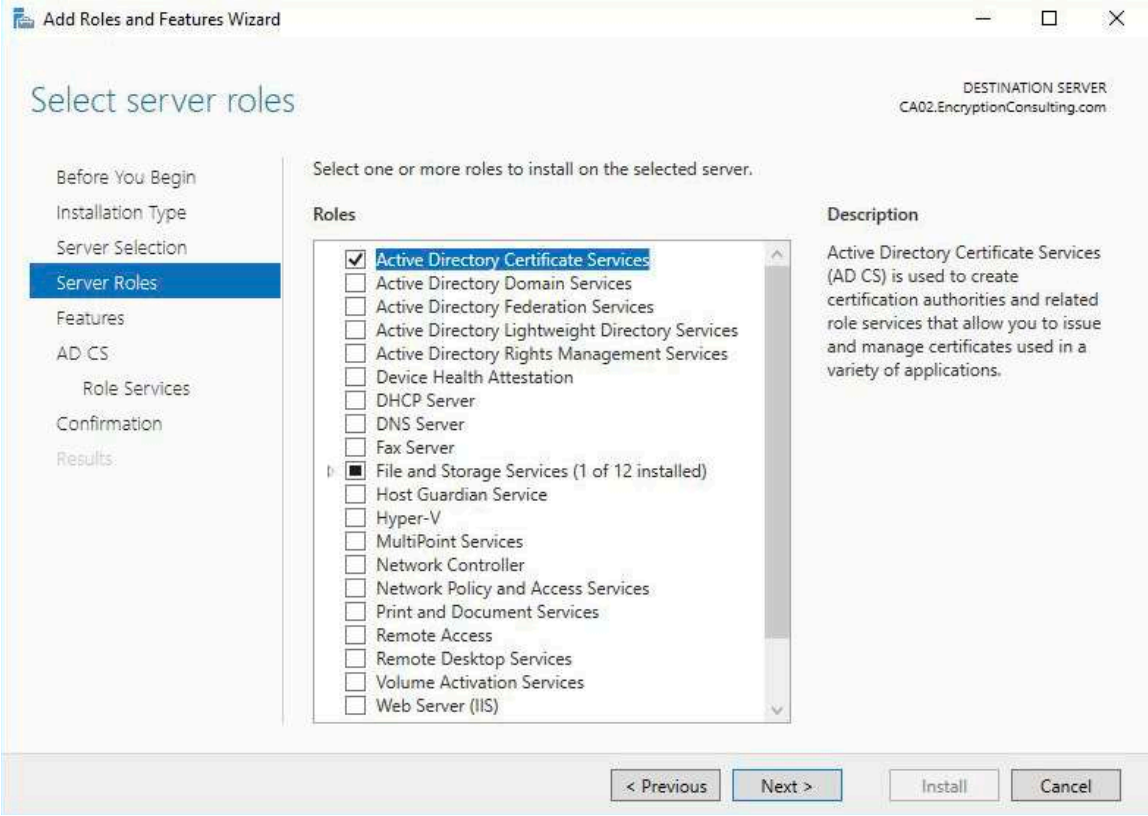
Activity 5: Install Subordinate Issuing CA

Subordinate issuing CA on CA02. EncryptionConsulting com:

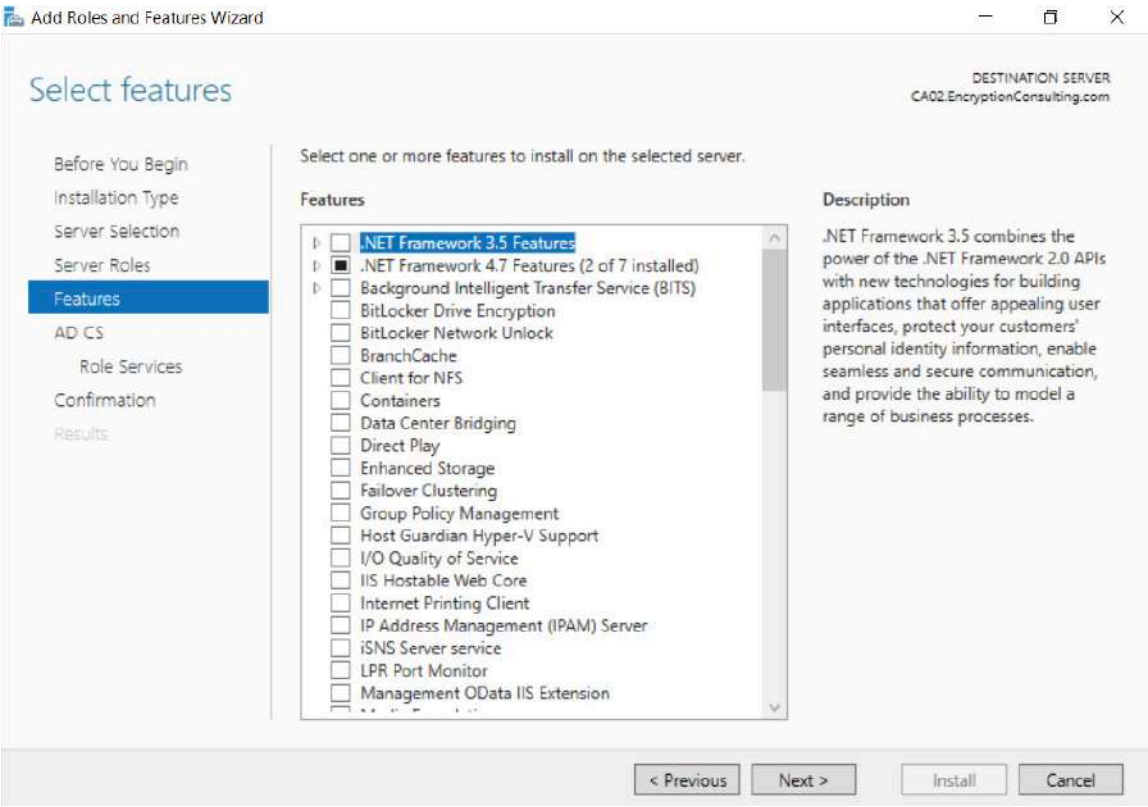
1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsulting\Administrator.
2. Open **Server Manager.**
3. Right-click **Roles** and then select **Add Roles.**
4. On the **Before You Begin** page select **Next.**



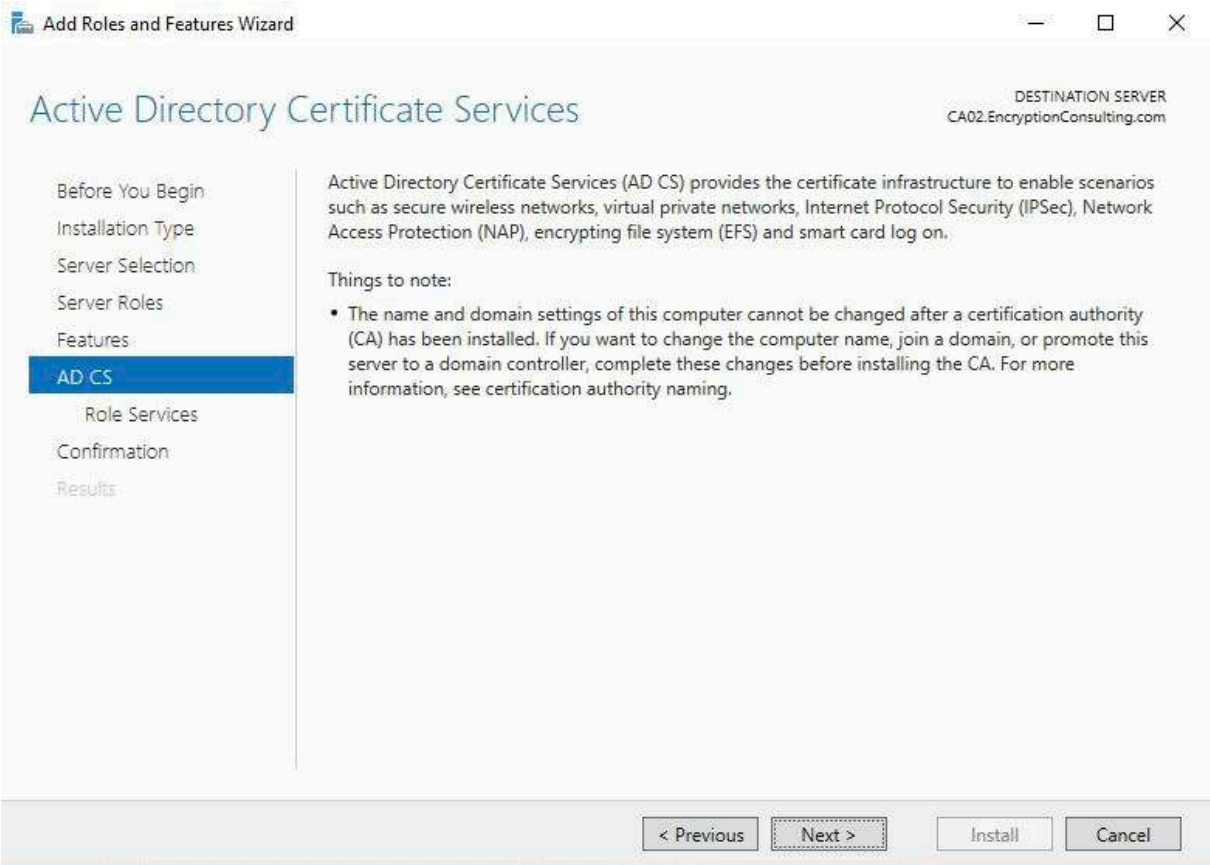
5. On the **Installation Type** page, choose **Role based or Featured based installation** and then click **Next.**
6. On the **server selection** page, click **next.**
7. On the **Select Server Roles** page select **Active Directory Certificate Services,** and then click **Next.**



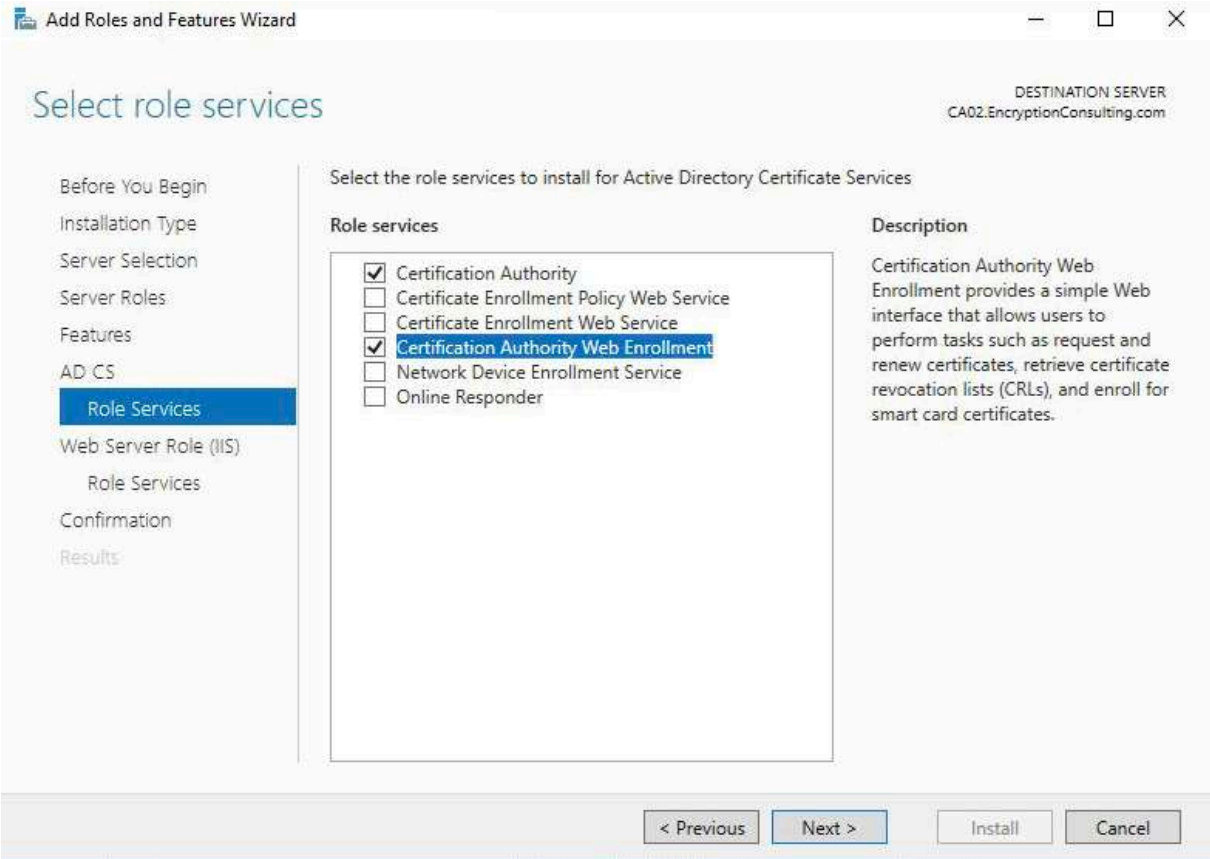
8. On the **Select features** page, click **Next.**



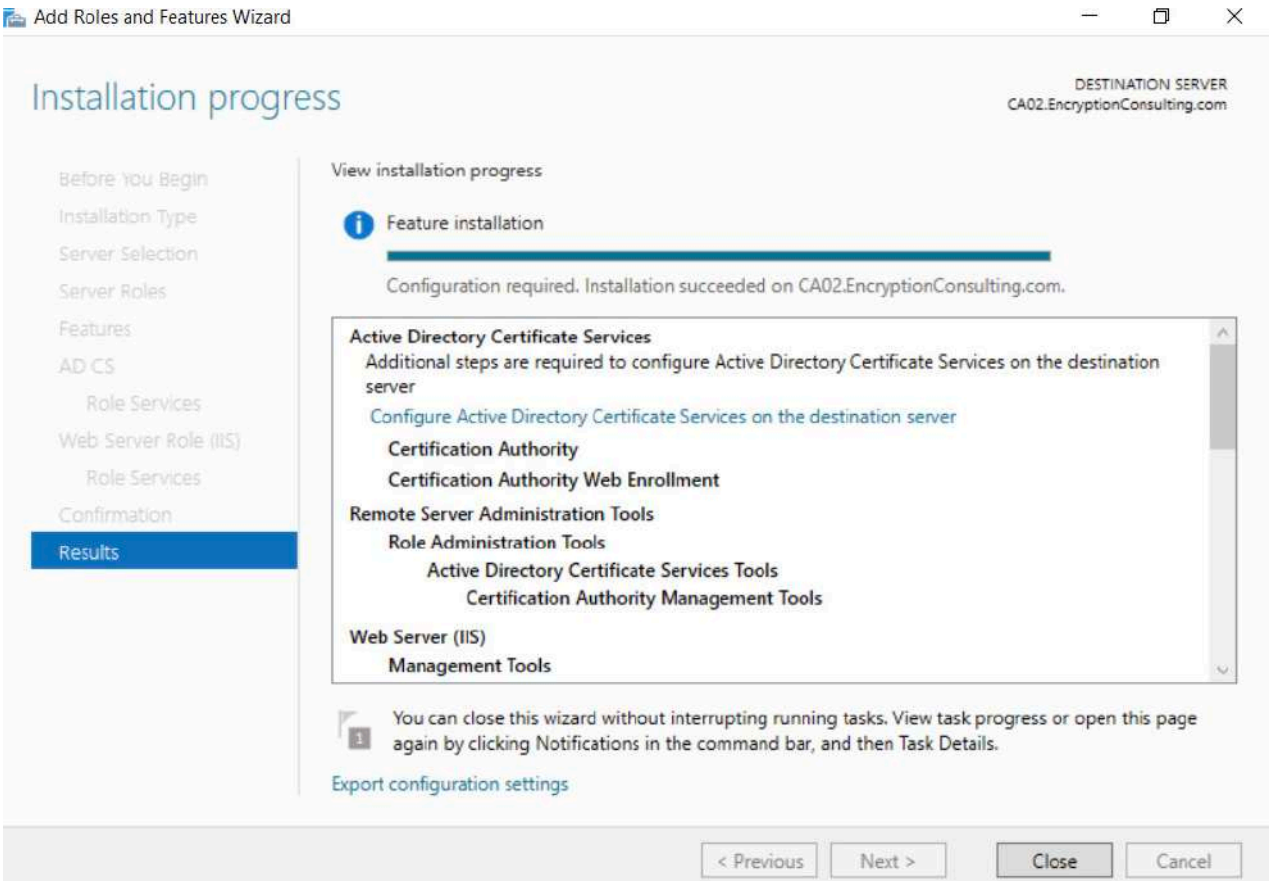
9. On the Introduction to **Active Directory Certificate Services** page, click **Next.**



10. On the **Select Role Services** page, select **Certification Authority** and **Certification Authority Web Enrollment.** If you see the **Add Roles Wizard,** click **Add Required Role Services.** Click **Next.**

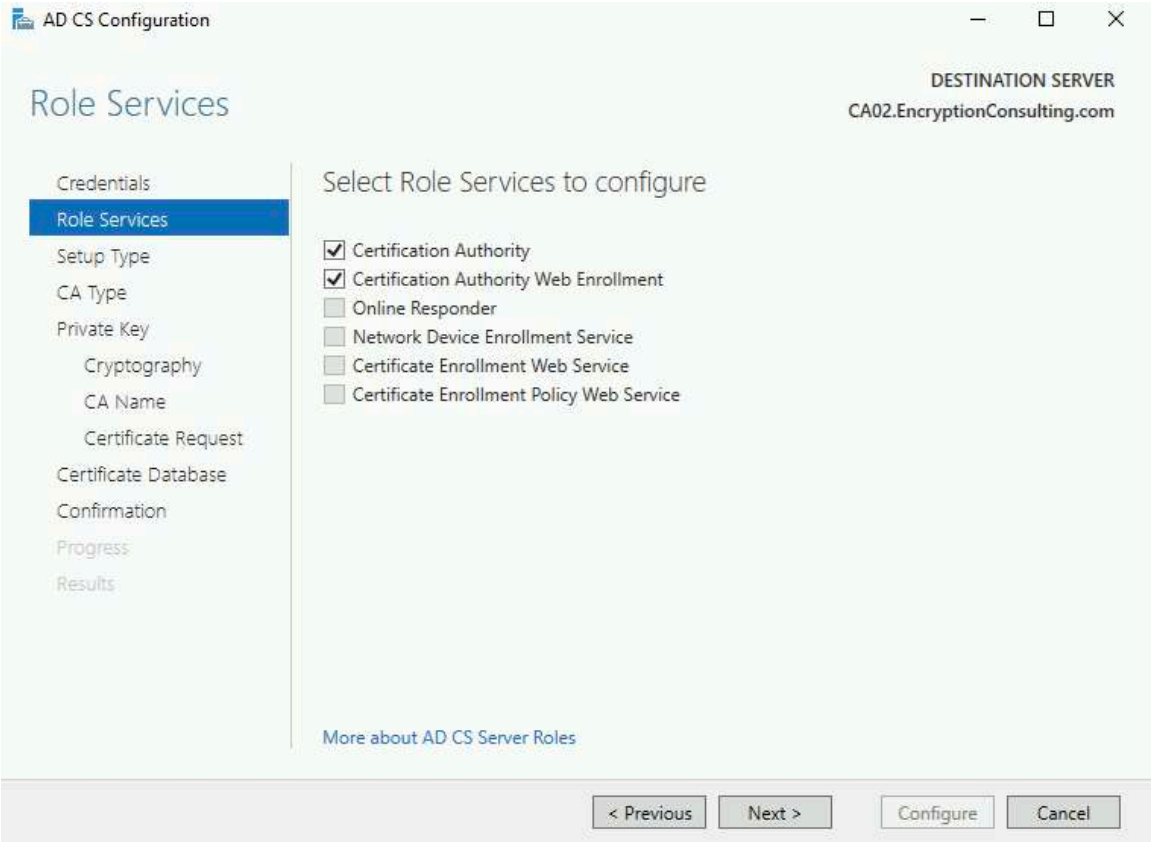


11. On the **Web Server Role IIS** page, click **Next.**
12. Leave the Role Services as default and click Next.
13. On the confirmation page, review the details and click **Install.**

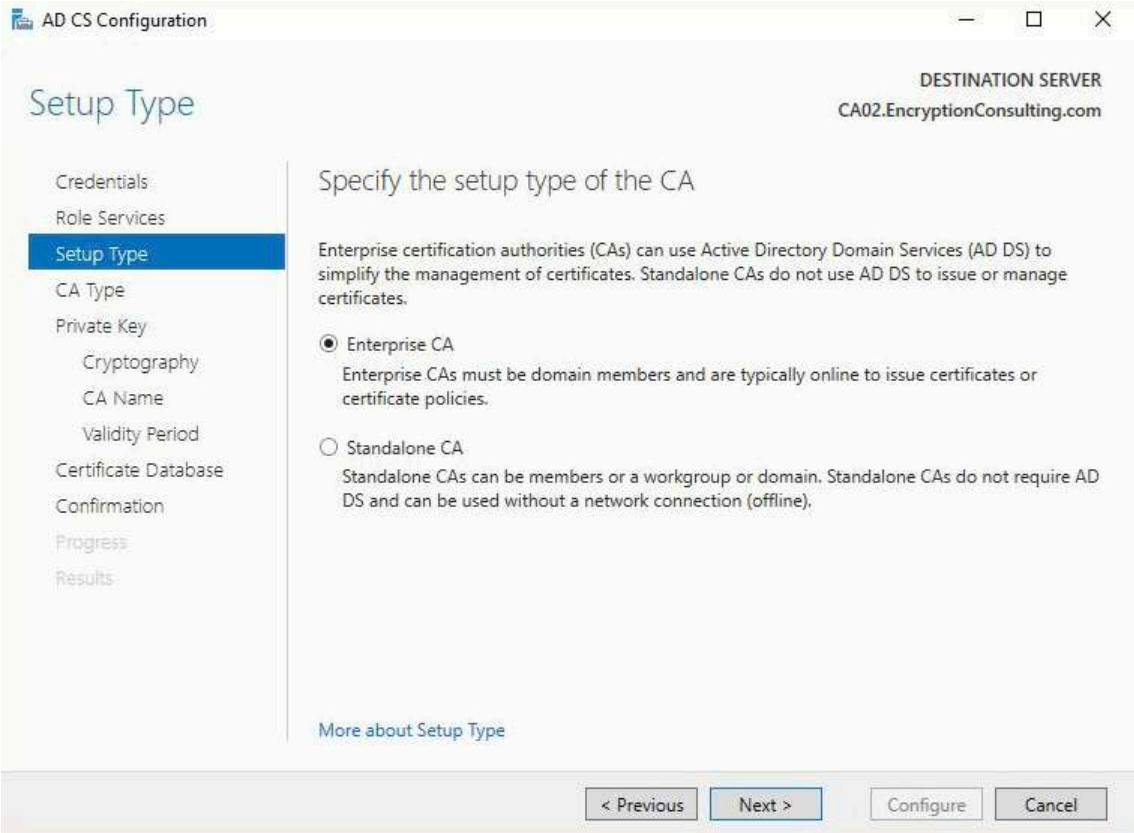


14. Click on **"configure Active Directory Certificate Services on the destination server".**
15. On the Specify Credential to configure roles and services page, credential should be **Encryptionsu\Administrator,** then click **Next.**

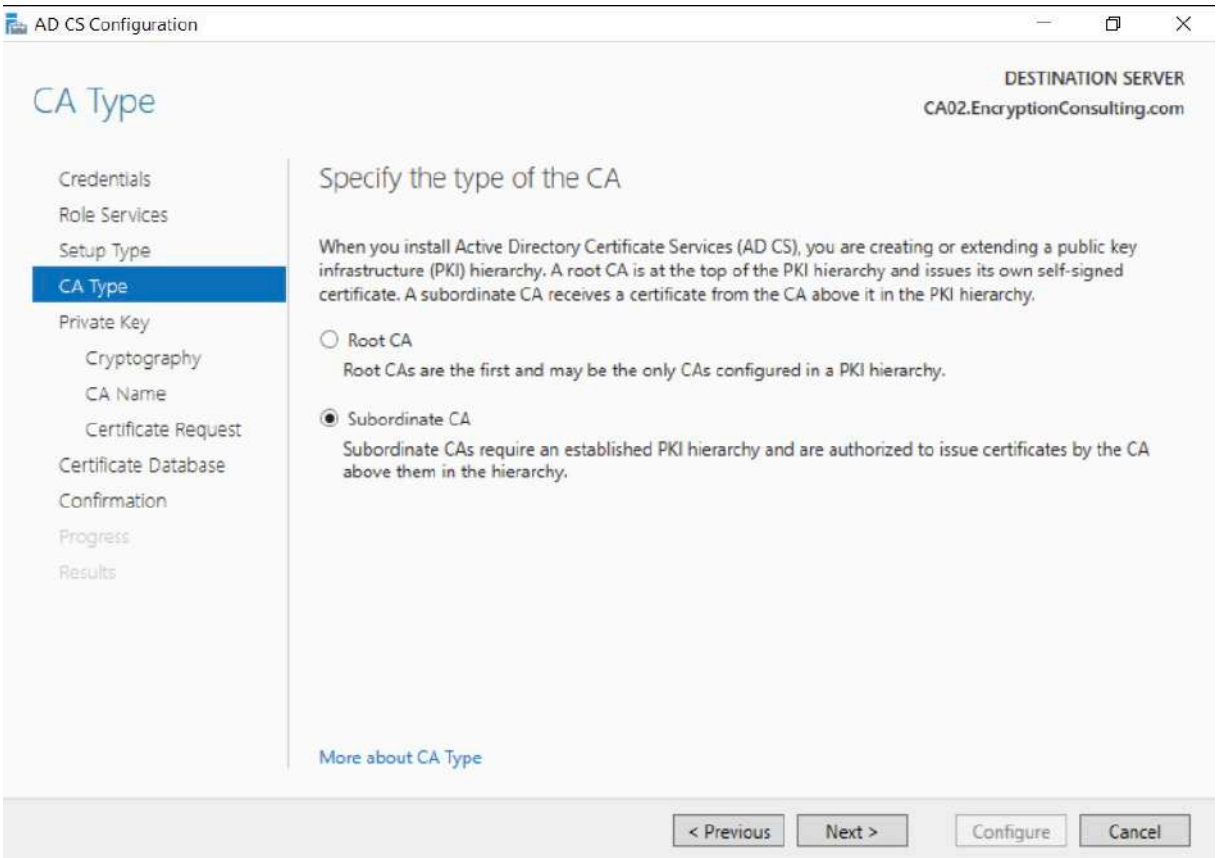
16. On the **Select Role services** to configure page, **select Certificate Authority and Certificate Authority Web Enrollment** then click Next.



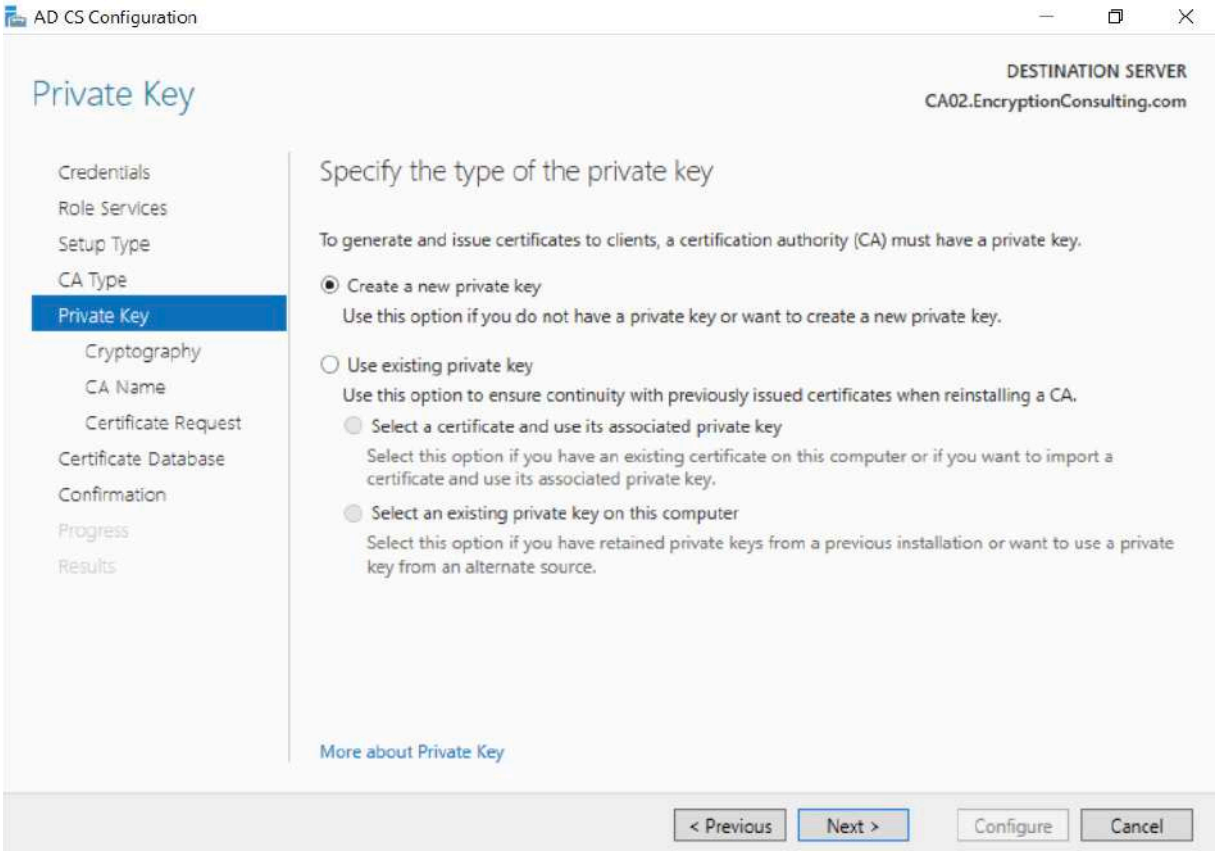
17. On the **Specify Setup Type** page, ensure that **Enterprise** is selected, and then click **Next.**



18. On the **Specify CA Type** page, select **Subordinate CA**, and then click **Next**



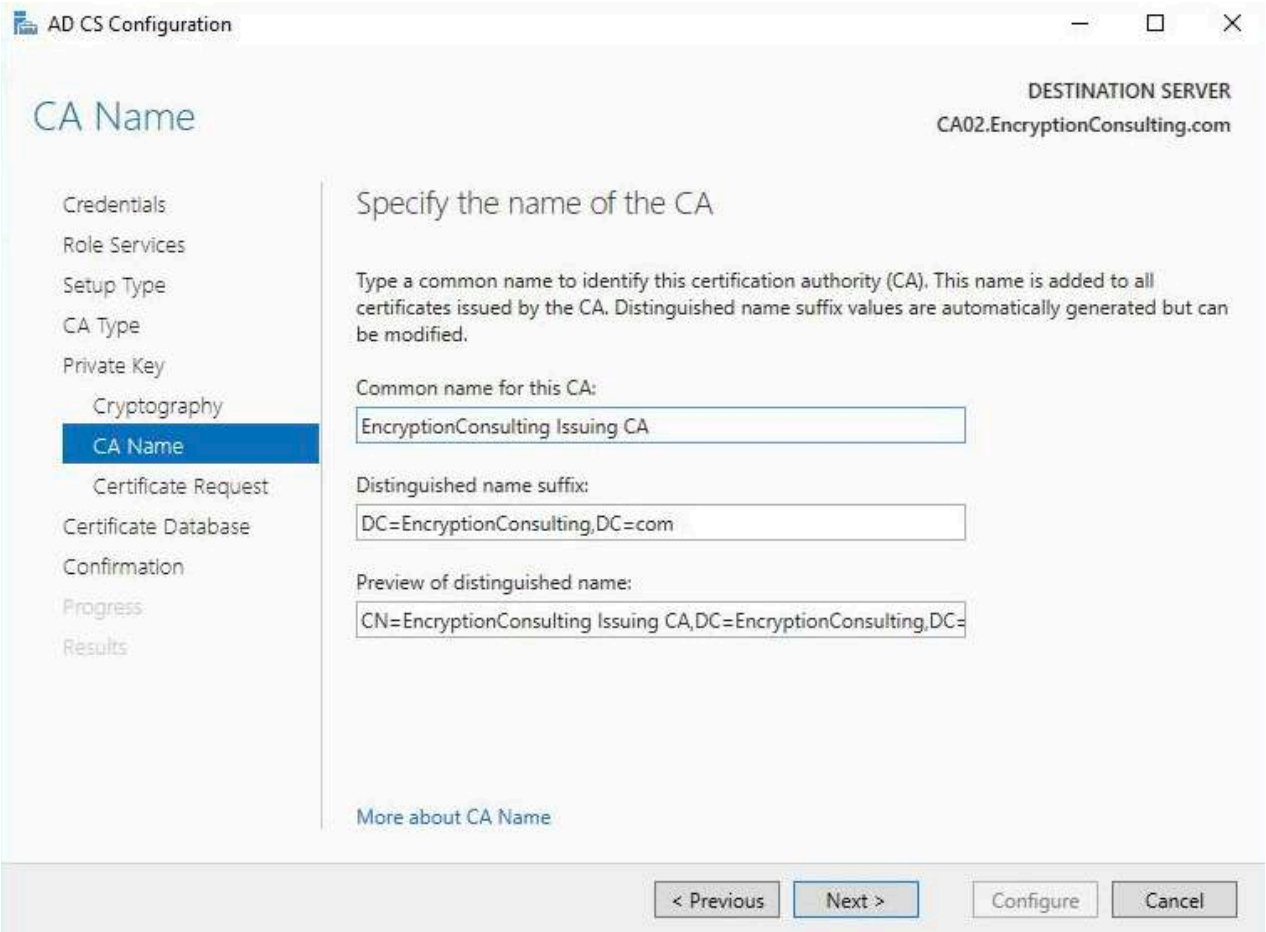
19. On the **Set Up Private Key** page, ensure that **Create a new private key** is selected, and then click **Next.**



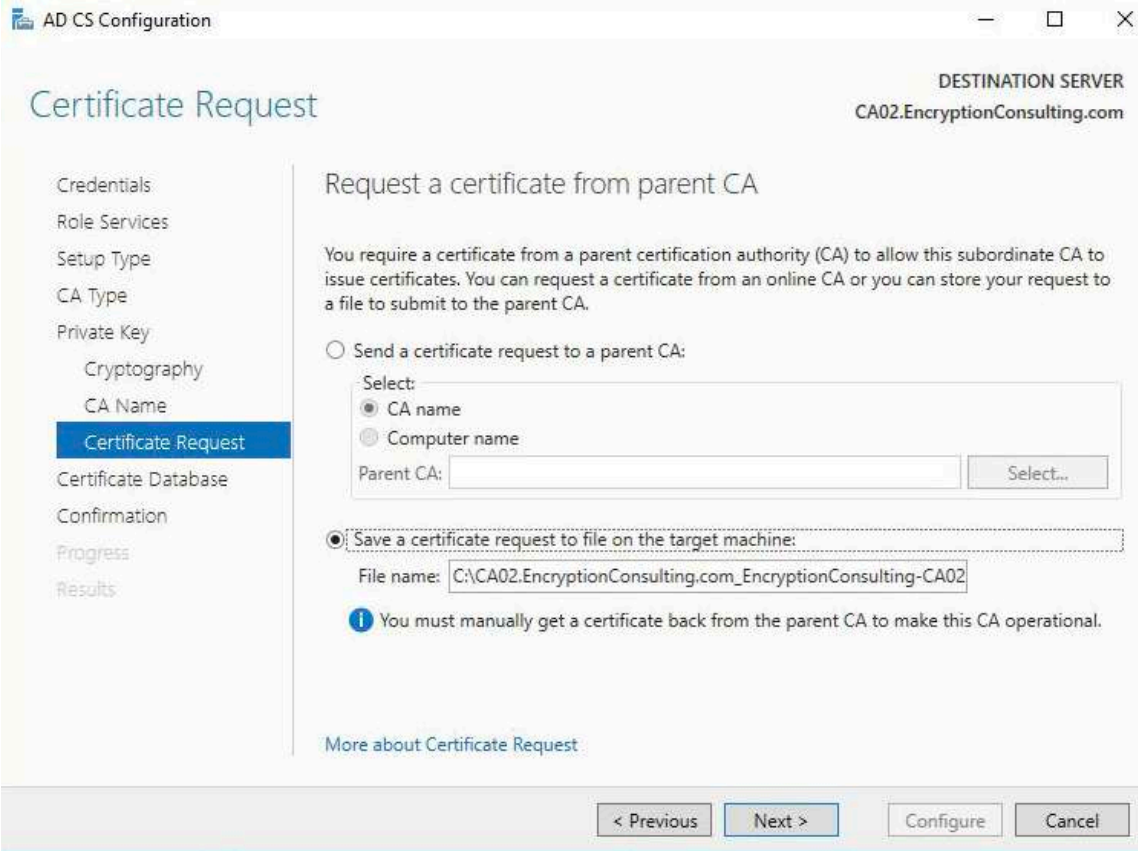
20. Leave the defaults on the **Configure Cryptography for CA** page, then click **Next.**
Important: When installing in a production environment,
the CSP, Hash Algorithm and Key length selected must support application compatibility requirements.

21. On **Configure CA Name** page, clear the existing entry for Common name for this CA box, and enter **EncryptionConsulting Issuing CA,** then select Next.

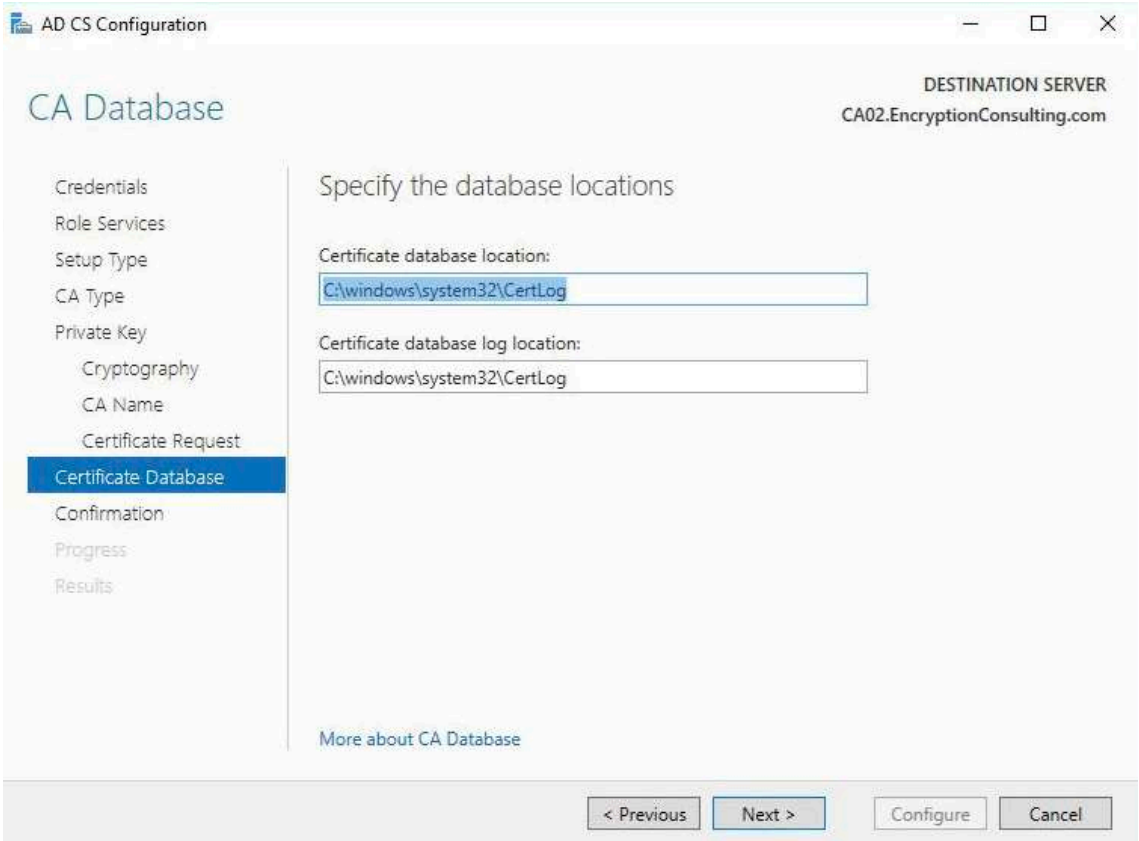
Note - Distinguished Name Suffix is automatically populated and should not be modified.



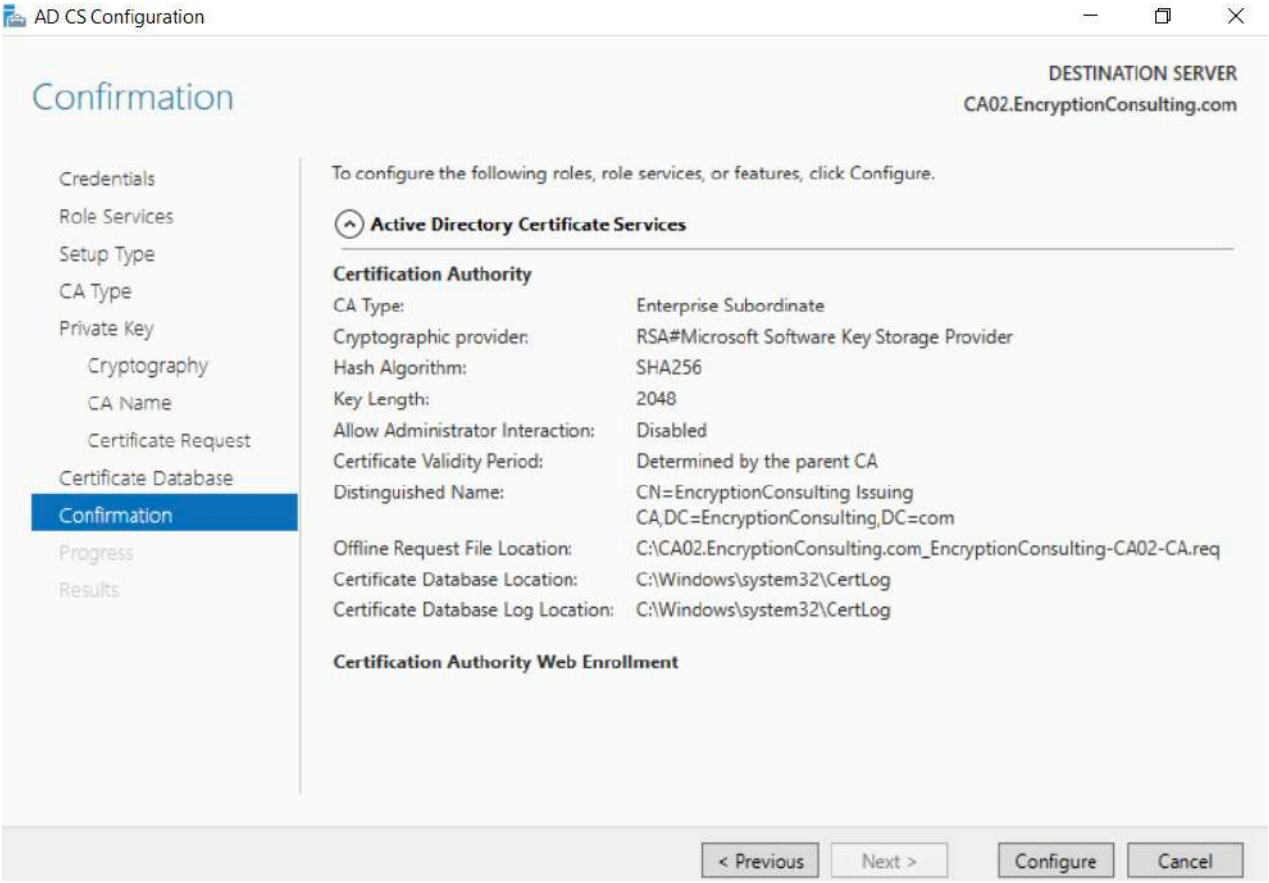
22. On the **Request certificate from a parent CA** page, select **Save a certificate request to file on the target machine** option then click **Next.**



23. Leave the defaults on the **Configure Certificate Database** page, and then click **Next.**

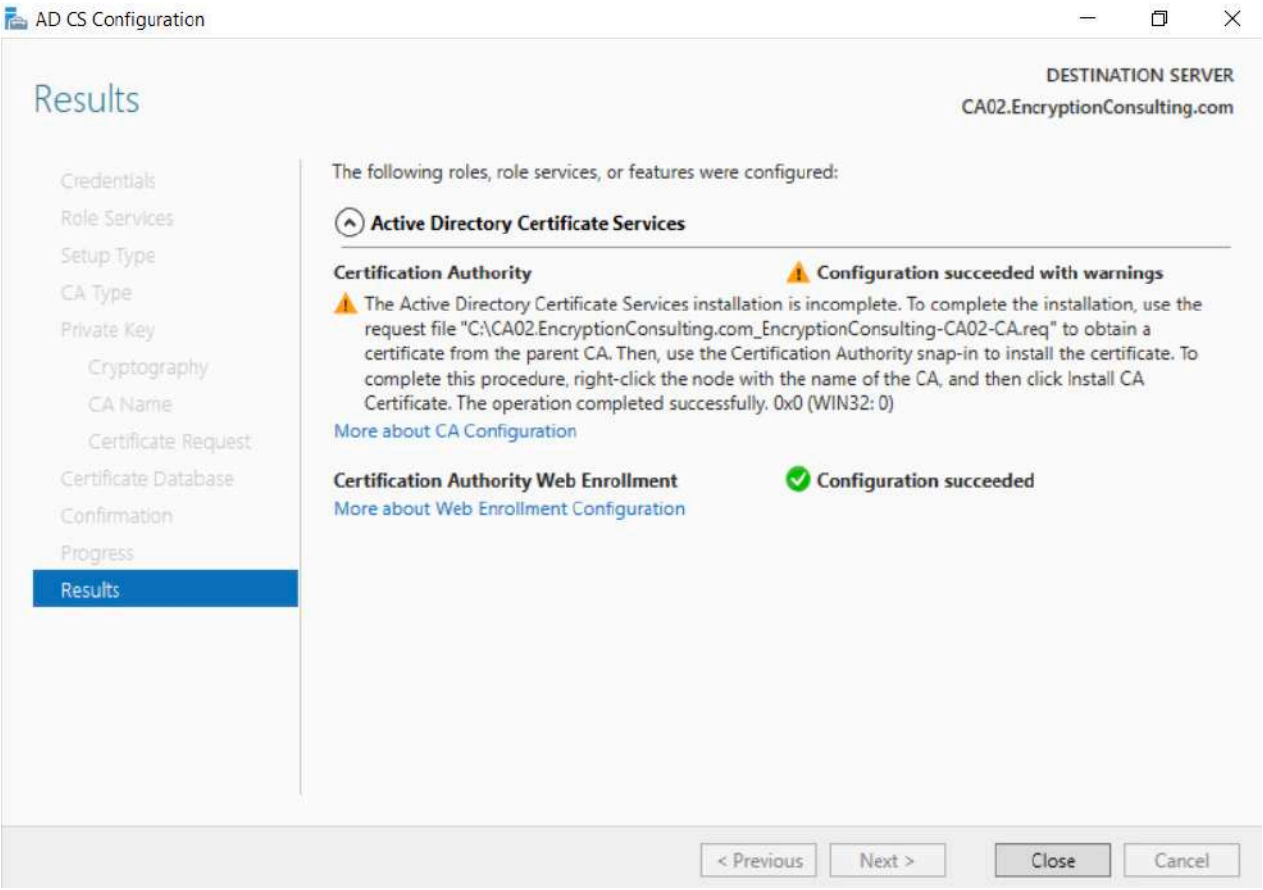


24. On the **Confirm Installation Selections** page, click **configure.**



25. Review the information on the **Installation Results** page to verify that the installation is successful and then click **Close.**

- The following warning message is expected: "The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req" to obtain a certificate from the parent CA. Then, use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)."



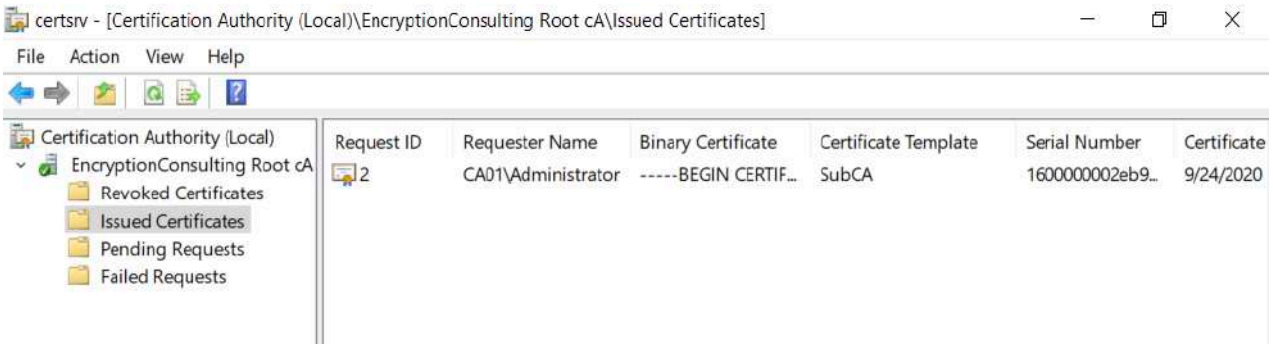
26. Copy C:\ CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req to your removable media. For example, if you want to copy to a floppy disk drive using the drive letter A:, you would run the following command from a command prompt:

- **copy "C:\CA02. EncryptionConsulting.com_ EncryptionConsulting Issuing CA.req" A:**

Task 1: Submit the Request and Issue EncryptionConsulting Issuing CA Certificate

To submit the certificate request and issue the requested certificate:

1. Ensure that you are logged on to CA01 as CA01\Administrator. Place the removable media with the certificate request into CA01.
2. On CA01, open an administrative command prompt. Then, submit the request using the following command (assuming that A:\ is your removable media drive letter):
    - **certreq -submit "A:\CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req"**
    - Note: Pay attention to the **RequestID** number that is displayed after you submit the request. You will use this number when retrieving the certificate.
3. In the **Certification Authority List** dialog box, ensure that **EncryptionConsulting Root CA** is selected and then click **OK**
4. Open the Certification Authority console. To do so, click **Start,** click **Administrative Tools,** click **Certification Authority.**
5. In the **certsrv [Certification Authority (Local)]** dialog box, in the console tree, expand **EncryptionConsulting Root CA.**
6. Click **Pending Requests.** In the details pane, right-click the request you just submitted, click **All Tasks,** and then click **Issue.**



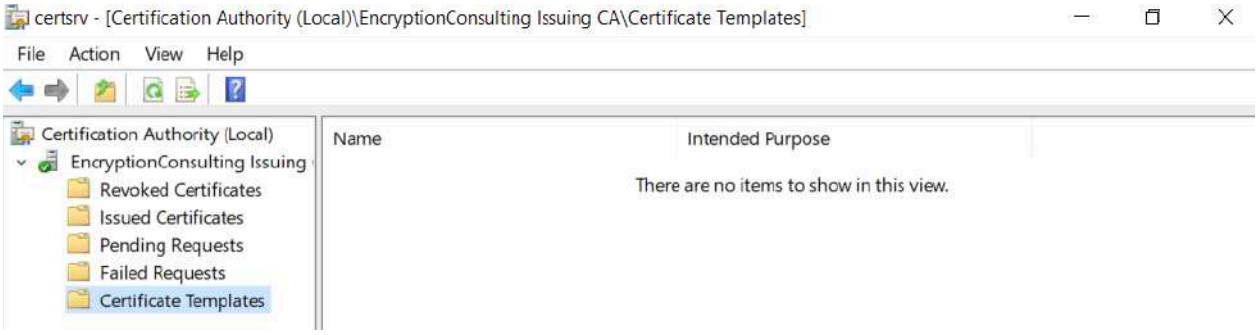
7. Return to the administrative command prompt to accept the issued certificate by running the following command. Ensure that you substitute the appropriate drive letter of your removable media for **A**: as well as the correct RequestID for **2:**
    - **certreq -retrieve 2 "A:\ CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.crt"**
8. In the **Certification Authority List** dialog box, ensure that **EncryptionConsulting Root CA** is selected and then click **OK.**

Task 2: Install the Encryption Consulting Issuing CA Certificate on CA02

To install the certificate and start the Certification Authority service on CA02:

1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsu\Administrator. Place the removable media with the issued certificate for CA02. EncryptionConsulting.com into CA02.
2. Open the Certification Authority console.
3. In the **Certification Authority** console tree, right-click **EncryptionConsulting Issuing CA,** and then click **Install CA Certificate.**
4. In the **Select file to complete CA installation,** navigate to your removable media. Ensure that you are displaying **All Files (*.*)** and click the **CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA** certificate. Click **Open.**

5. In the console tree, right-click **EncryptionConsulting Issuing CA,** click All Tasks, and then click **Start Service.**
6. In the console tree, expand **EncryptionConsulting Issuing CA** and then click **Certificate Templates.** Notice there are no certificates shown in the details pane. This is because the CAPolicy.inf specified not to install the default templates in the line **LoadDefaultTemplates=0.**



Activity 6: Perform Post Installation Configuration Tasks on the Subordinate Issuing CA

There are multiple settings to configure to complete the installation of the issuing CA. These are like the tasks that were needed to complete the configuration of the root CA.

Task 1: Configure Certificate Revocation and CA Certificate Validity Periods

To configure certificate revocation and CA certificate validity periods:

1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsu\Administrator.
2. Configure the CRL and Delta CRL settings by running the following command from an administrative command prompt:
   - **Certutil -setreg CA\CRLPeriodUnits 1**
   - **Certutil -setreg CA\CRLPeriod "Weeks"**
   - **Certutil -setreg CA\CRLDeltaPeriodUnits 1**
   - **Certutil -setreg CA\CRLDeltaPeriod "Days"**
3. Define CRL overlap settings by running the following command from an administrative command prompt:
   - **Certutil -setreg CA\CRLOverlapPeriodUnits 12**
   - **Certutil -setreg CA\CRLOverlapPeriod "Hours"**
4. The default setting for Validity Period is 2 years in registry. Adjust this setting accordingly to meet your needs of entity certificate's lifetime issued from EncryptionConsulting Issuing CA. It is recommended that you do not configure validity periods that are longer than half of total lifetime of EncryptionConsulting Issuing CA certificate, which was issued to be valid for 10 years. To limit issued certificates to 5 years, run the following commands from an administrative command prompt:
   - **Certutil -setreg CA\ValidityPeriodUnits 5**
   - **Certutil -setreg CA\ValidityPeriod "Years"**

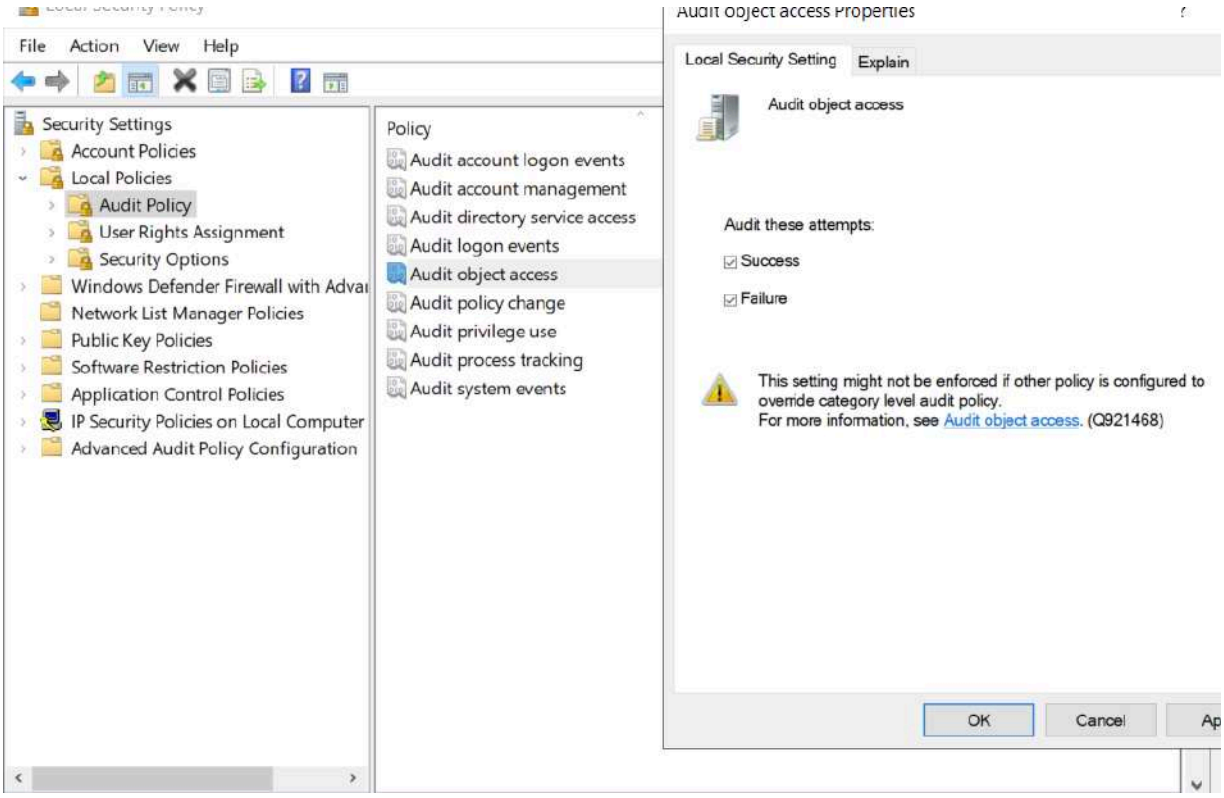
Task 2: Enable Auditing on the Issuing CA

CA auditing depends on system **Audit Object Access** to be enabled. The following instructions describe how to use Local Security Policy to enable object access auditing.

1. Click **Start,** click **Administrative Tools,** and then select **Local Security Policy.**

2. Expand **Local Policies** and then select **Audit Policy.**

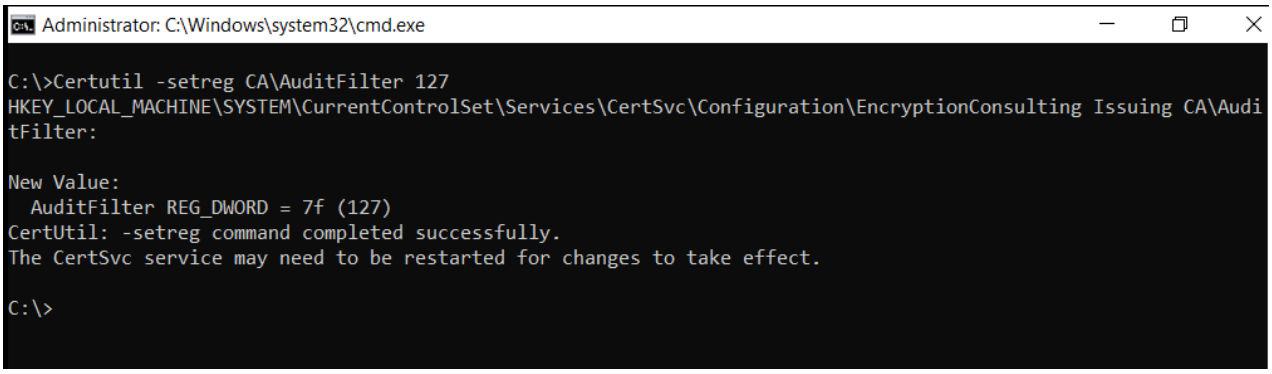
3. Double click **Audit Object Access** and then select **Success** and **Failure** then click **OK.**



4. Close Local Security Policy editor.

5. Enable auditing for the CA by selecting which group of events to audit in the Certificate Authority MMC snap-in or by configuring AuditFilter registry key setting. To configure Auditing for all CA related events, run the following command from an administrative command prompt:

   Certutil -setreg CA\AuditFilter 127



Task 3: Configure the AIA

Using a certutil command is a quick and common method for configuring the AIA. When you run the following certutil command, you will be configuring a static file system location, a lightweight directory access path (LDAP) location, and http location for the AIA. The certutil command to set the AIA modifies the registry, so ensure that you run the command from an command prompt run as Administrator. Run the following command:

certutil -setreg CA\CACertPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA, CN=Public Key Services,CN=Services,%6%11\n2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt"

After you have run that command, run the following command to confirm your settings:
certutil -getreg CA\CACertPublicationURLs

If you look in the registry, under the following

path: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Issuing CA,** you can confirm the CACertPublicationURLs by opening that REG_MULTI_SZ value. You should see the following:

1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt

2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt

You can also see this in the the CA (certsrv) console. To open the console, click **Start,** click **Administrative Tools,** and then click **Certification Authority.** In the navigation pane, expand the **Certificate Authority (Local)**. Right-click **EncryptionConsulting Root CA** and then click **Properties.** On the **Extensions tab**, under **Select extension,** click **Authority Information Access (AIA)** and you will see the graphical representation of the AIA settings.

From an administrative command prompt, run the following command to copy the EncryptionConsulting Issuing CA certificate to the http AIA location:

copy "c:\Windows\System32\certsrv\certenroll\CA02 EncryptionConsulting.com_ EncryptionConsulting Issuing CA.crt" \\srv1.EncryptionConsulting.com\c$\certenroll

Task 4: Configure the CDP

The certutil command to set the CDP modifies the registry, so ensure that you run the command from an command prompt run as Administrator. Run the following command:

certutil -setreg CA\CRLPublicationURLs "65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n79:ldap:///CN=%7%8,CN=%2, CN=CDP,CN=Public Key Services,CN=Services,%6%10\n6:http://pki. EncryptionConsulting.com/CertEnroll/%3%8%9.crl\n65:\\srv1. EncryptionConsulting.com\CertEnroll\%3%8%9.crl"

After you run that command, run the following certutil command to verify your settings:

certutil -getreg CA\CRLPublicationURLs

In the registry

location:**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Issuing CA** you can open the REG_MULTI_SZ value and see the configuration of these values:

65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl

79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

6:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl

65:\\srv1.EncryptionConsulting.com\CertEnroll\%3%8%9.crl

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools**, and then click **Certification Authority.** In the navigation pane, ensure that **Certificate Authority(Local)** is expanded. Right-click **EncryptionConsulting Root CA** and then click **Properties.** On the **Extensions** tab, under **Select extension,** click **CRL Distribution Point (CDP)** and you will see the graphical representation of the CDP settings.

At an administrative command prompt, run the following commands to restart Active Directory Certificate Services and to publish the CRL.

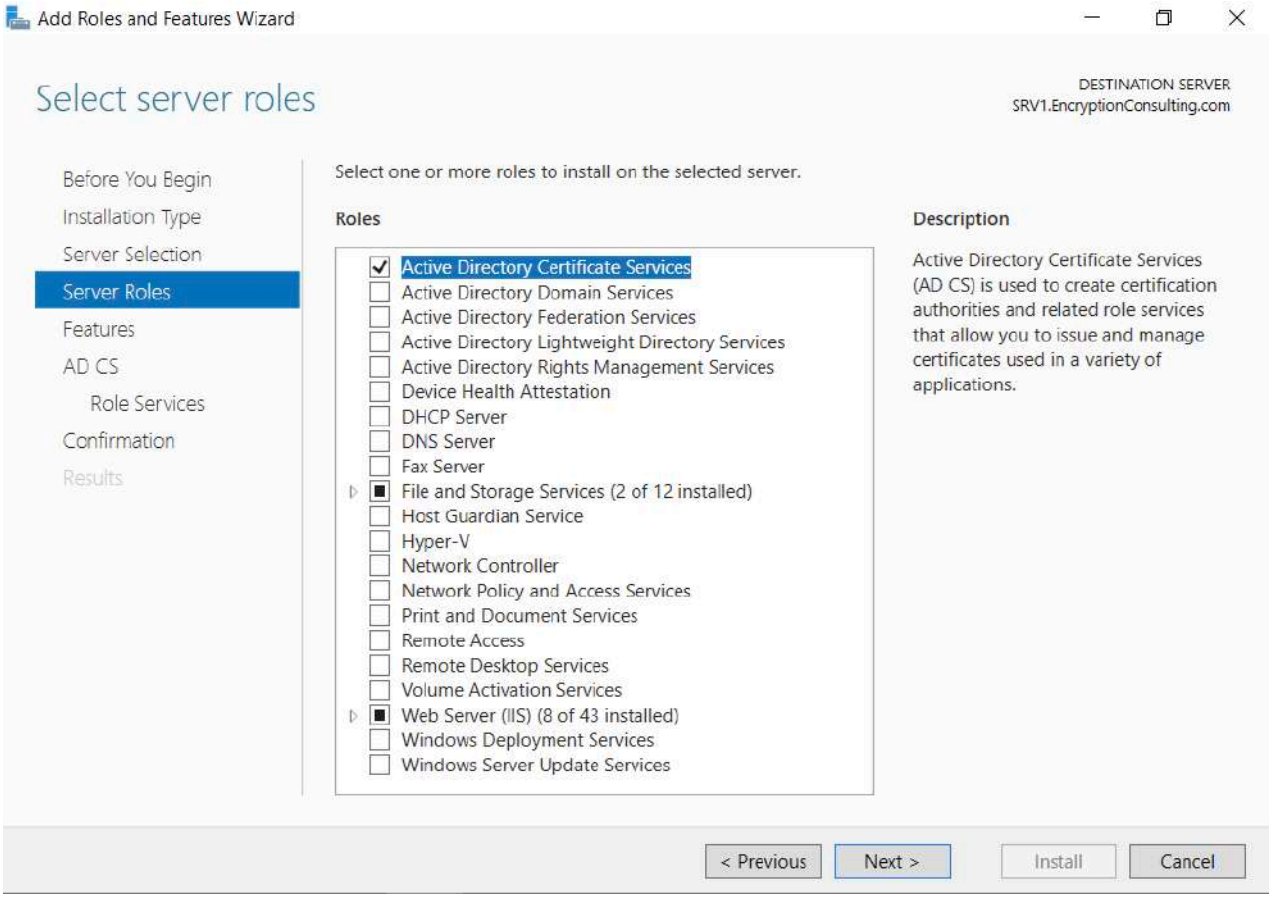
net stop certsvc && net start certsvc

certutil -crl

Activity 7: Install and Configure the Online Responder Role Service

Task 1: Install the Online Responder Role Service on SRV1

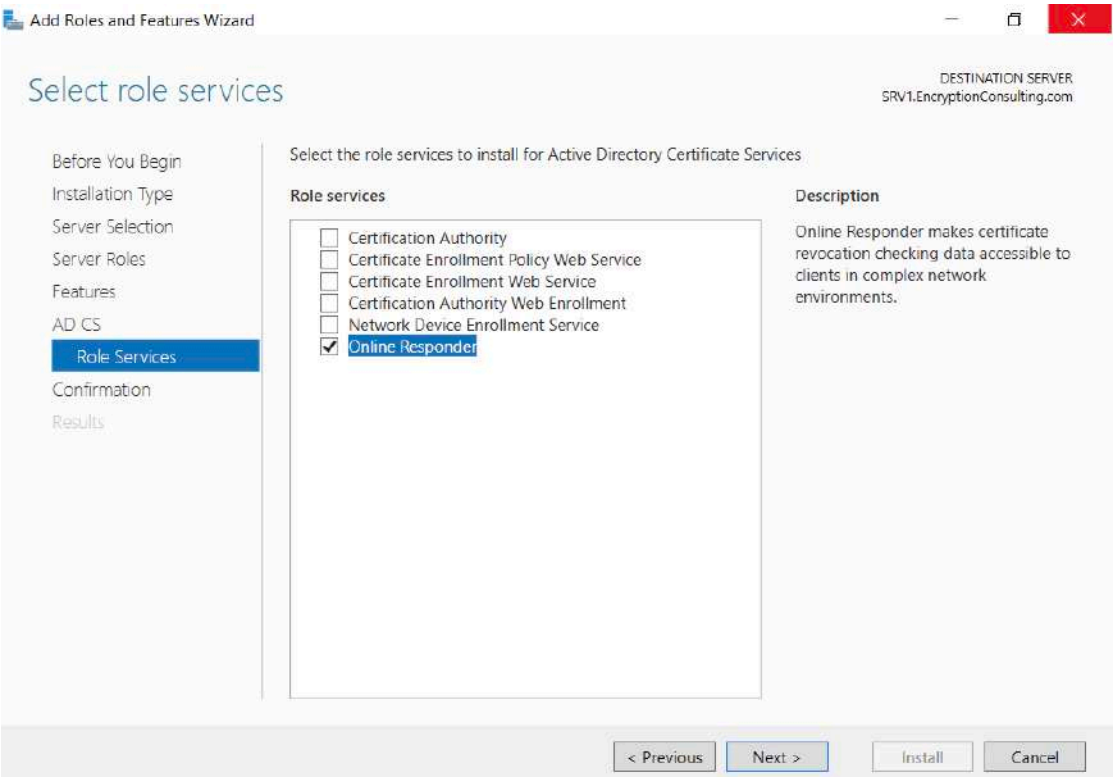
1. Ensure that you are logged on to SRV1. EncryptionConsulting.com as EncryptionConsu\Administrator.
2. Open Server Manager.
3. Right click on **Roles,** and then click **Add Roles.**
4. On the **Before You Begin** page, then select **Next.**
5. On the **Select Installation type** page, select **Role-based or feature-based installation** and then click **Next.**
6. On the **Server Selection** page, click **Next.**
7. On the **Select Server** Roles page, select **Active Directory Certificate Services** and then click **Next.**



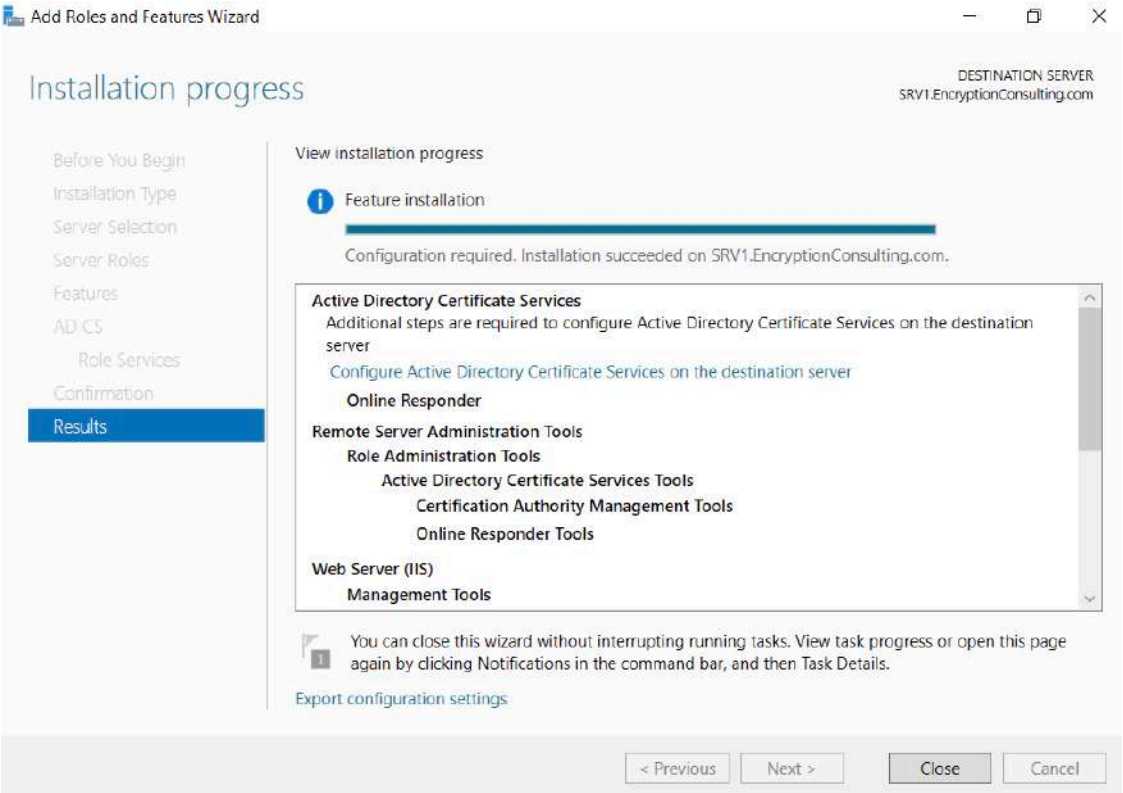
8. On the **Features** page, click **Next.**
9. On **Introduction to Active Directory Certificate Services** page, click **Next.**

10. On the **Select Role Services** page, clear the **Certification Authority,** and then select Online Responder. Click **Next.**

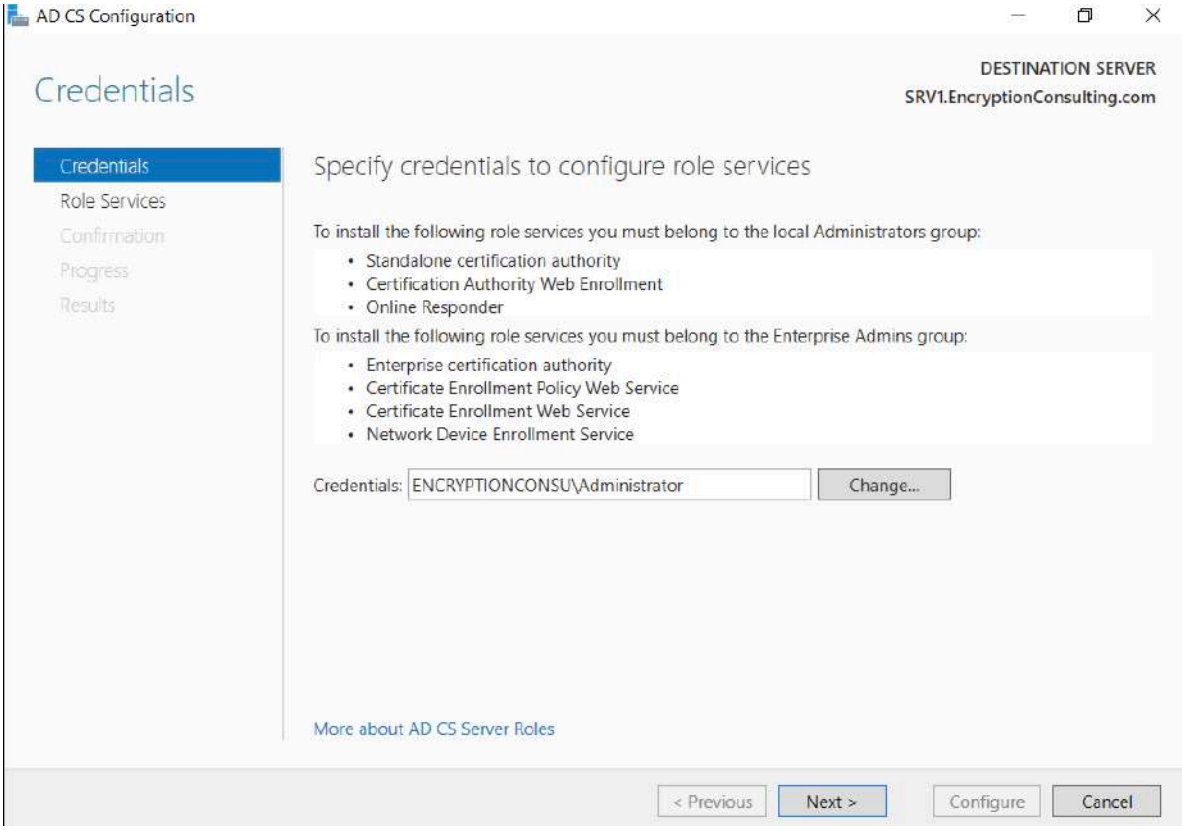
- Note: You do not want to install a Certification Authority on SRV1.EncryptionConsulting.com, so you are clearing that checkbox.
- If the **Add role services and features required for Online Responder** page appears, click **Add Required Role Services** and then click **Next.** Then, on the **Web Server (IIS)**, click **Next.**

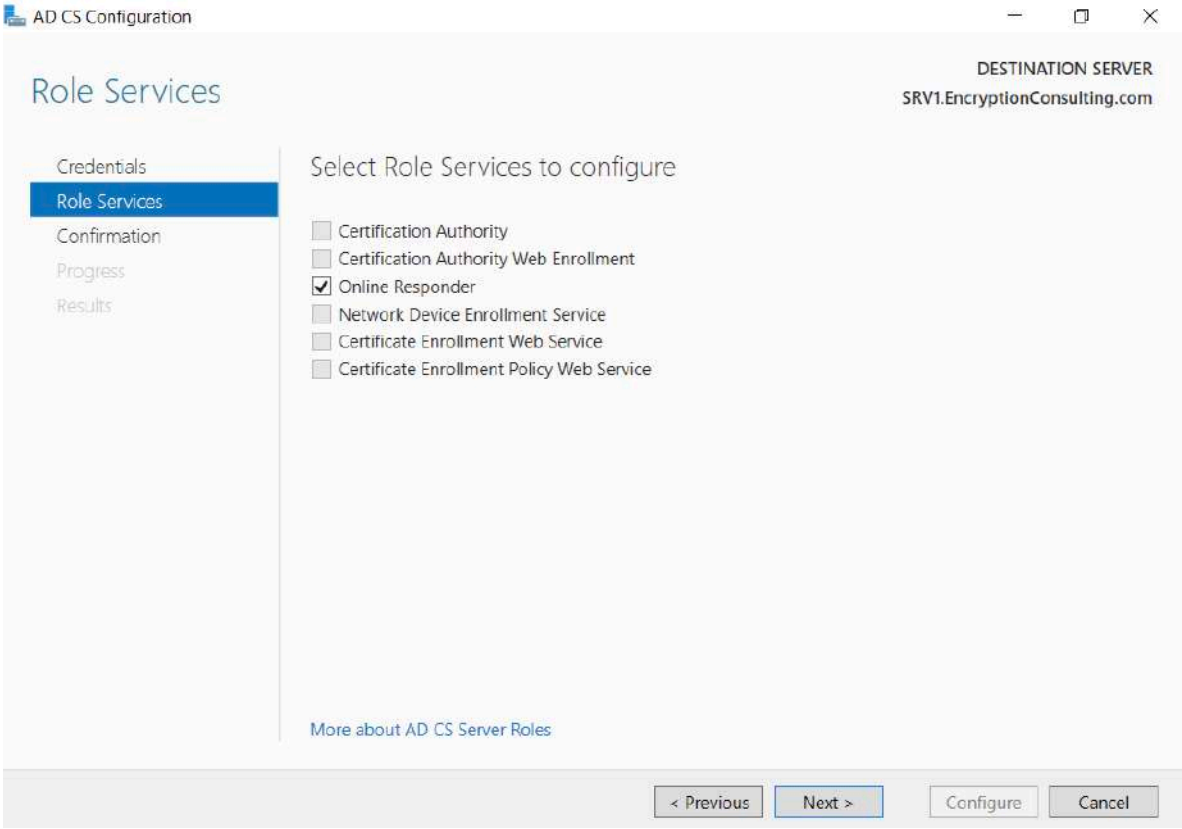


11. On the Confirm Installation Selections page, click Install. Click Close when the installation is complete.

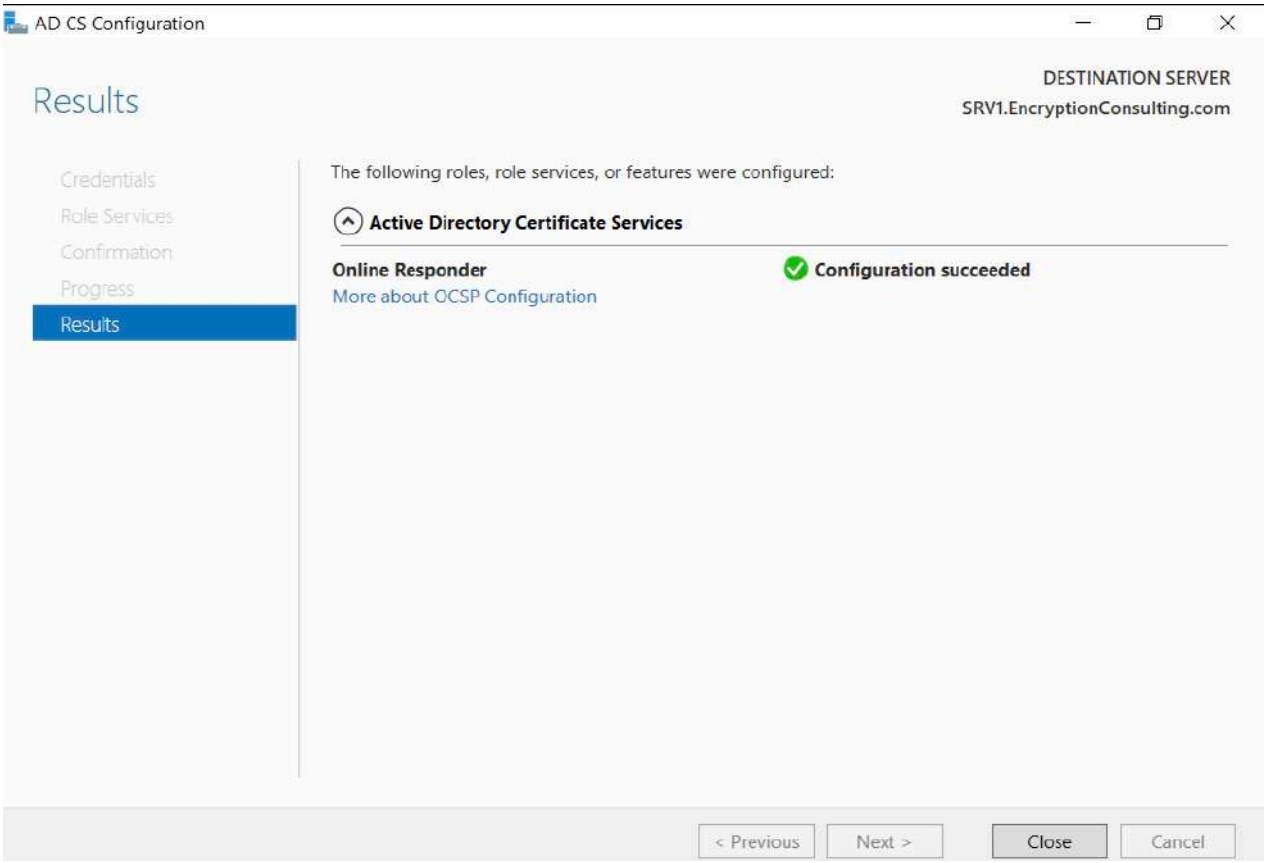


12. Click on **"Configure Active Directory Certificate Services on the destination server"**, on the Credential Page, make sure **Encryptionconsu\Administrator** is mentioned, then click **Next.**





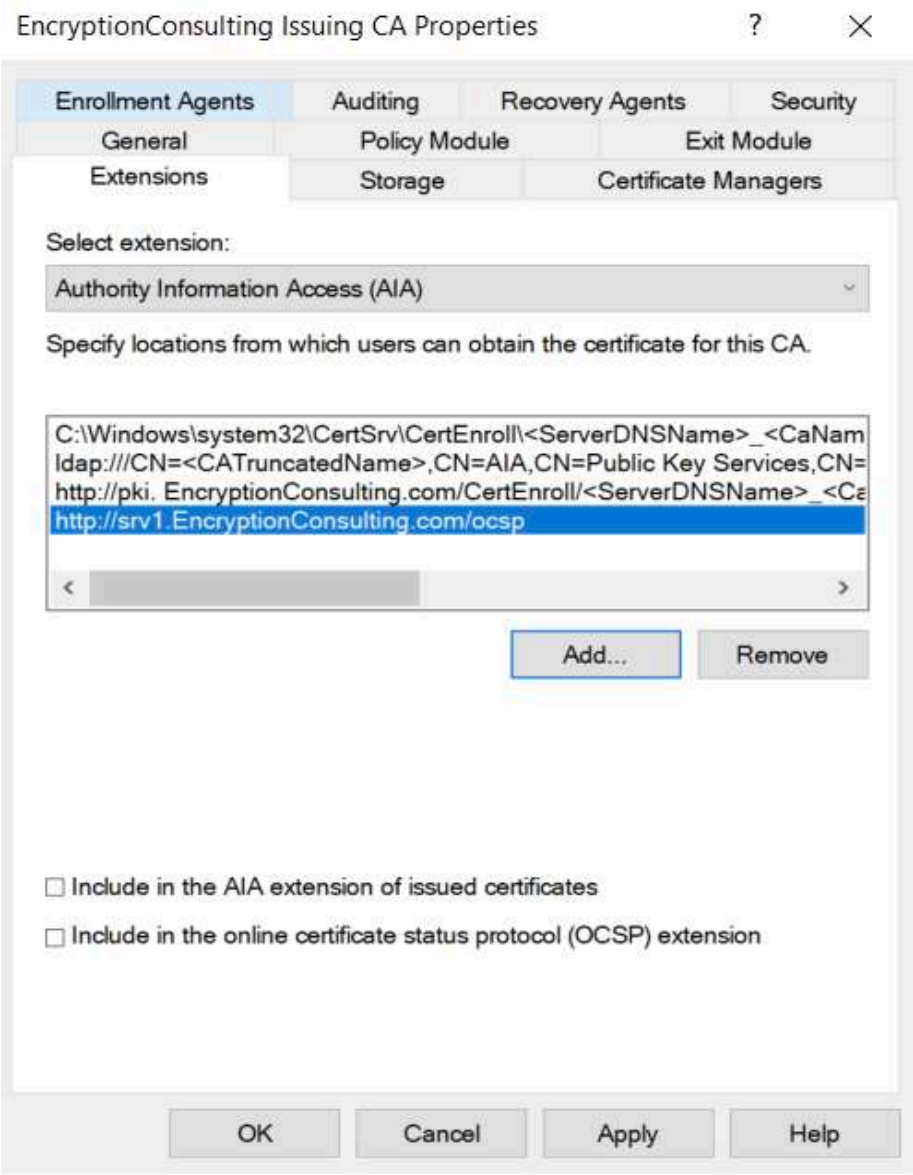
14. On the **confirmation** page, verify the details and click **Next.**



Task 2: Add the OCSP URL to the Encryption Consulting Issuing CA

To add the OCSP URL to the EncryptionConsulting Issuing CA:

1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsu\Administrator
2. In the **Certification Authority** console, in the console tree, right-click EncryptionConsulting **Issuing CA,** and then click **Properties.**
3. On the **Extensions** tab, under **Select extension**, select **Authority Information Access (AIA)**, and then click **Add.**
4. In **Location,** type **http://srv1.EncryptionConsulting.com/ocsp** and then click **OK.**
5. Select **Include in the online certificate status protocol (OCSP) extension.**
    - Note: A common misconfiguration is to select both checkboxes in the Extensions tab, which is incorrect. Ensure that **Include in the online certificate status protocol (OCSP) extension** checkbox is the only one selected.



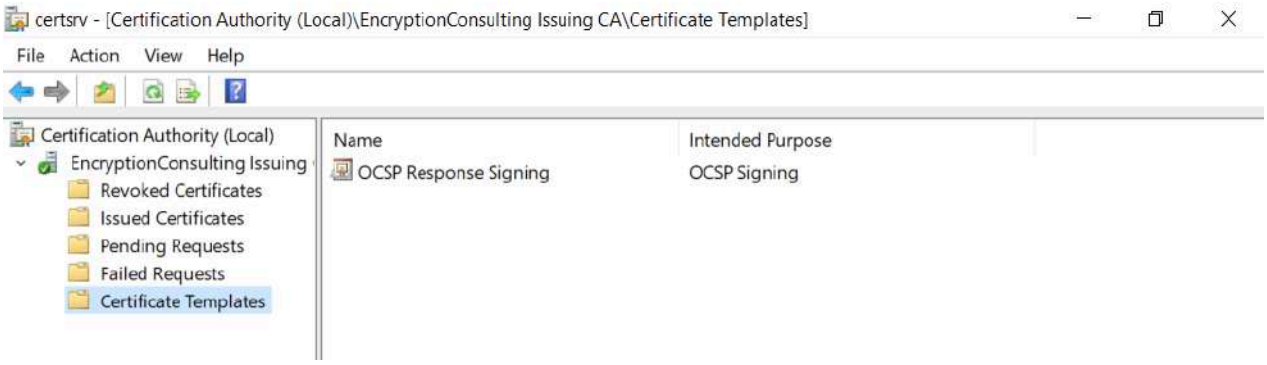
6. Click **OK**. When prompted by the **Certification Authority** dialog box to restart Active Directory Certificate Services, click **Yes.**

Important: The EncryptionConsulting Issuing CA will now include http://srv1. EncryptionConsulting.com/ocsp URL as part of Authority Information Access (AIA) extension in all newly issued certificates issued or renewed or re-enrolled certificates. However, certificates enrolled from EncryptionConsulting Issuing CA prior to this change will not have this URL.

Task 3: Configure and Publish the OCSP Response Signing Certificate on the Encryption Consulting Issuing CA

To configure the OCSP response signing certificate:

1. On CA02. EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
2. In the **Certification Authority** console, ensure that the EncryptionConsulting Issuing CA is expanded in the console tree.
3. Right-click on **Certificate Templates** and then click **Manage. Certificate Templates** opens and displays the certificate templates stored in Active Directory.
4. In the details pane (middle pane) right-click **OCSP Response Signing** and then click **Properties.**
5. On the **Security** tab click **Add.** Click **Object Types.**
6. In the **Object Types** dialog box, select **Computers** and then click **OK.**
7. In **Enter the object names to select,** type **SRV1** and then click **Check Names**. Click **OK.**
8. Ensure that **SRV1** is selected and in the **Allow** column, ensure that the **Read** and **Enroll** permissions are selected. Click **OK.**
9. Close Certificate Templates MMC console.
10. In **certsrv** console, right-click **Certificate Templates**, then select **New** and then select **Certificate Template to Issue.**
11. In the **Enable Certificate Templates** dialog box, click **OCSP Response Signing** and the click **OK.**

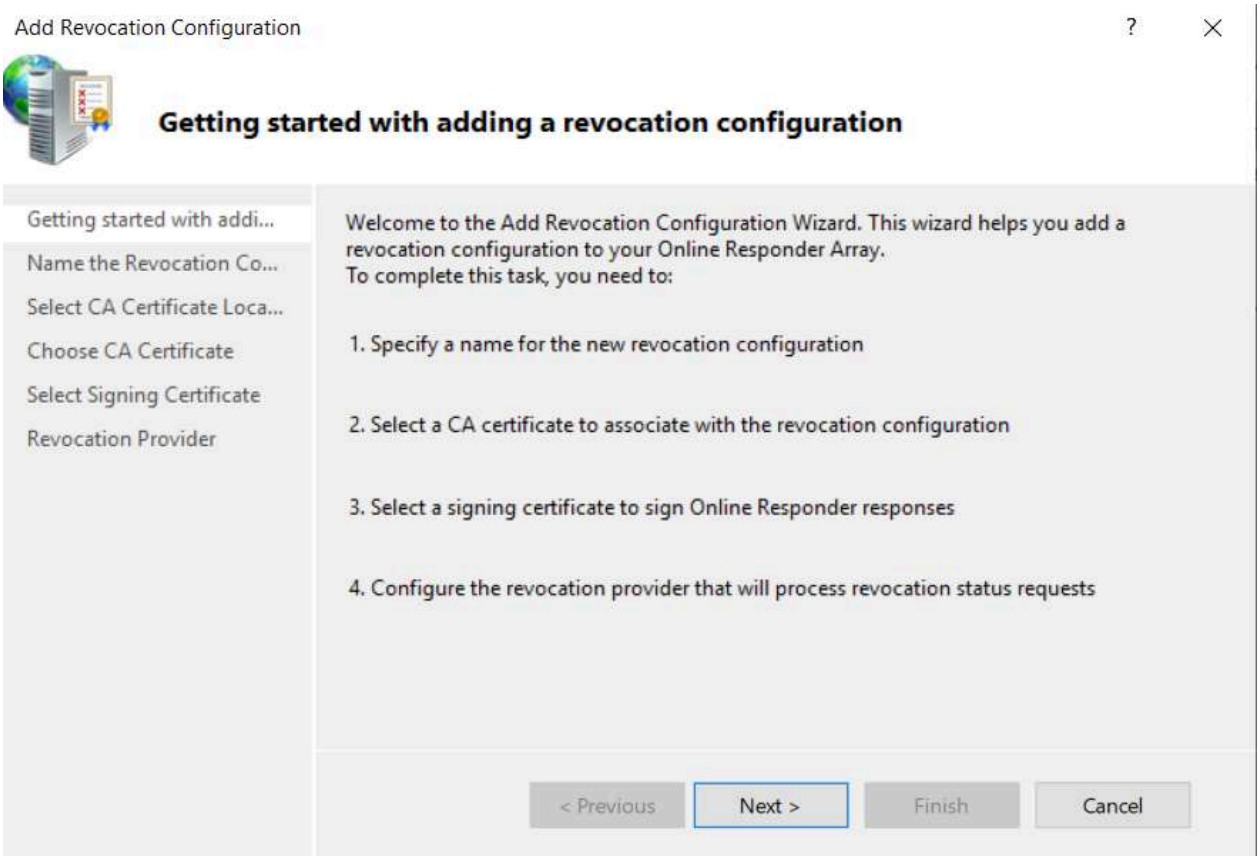


Task 4: Configure Revocation Configuration on the Online Responder

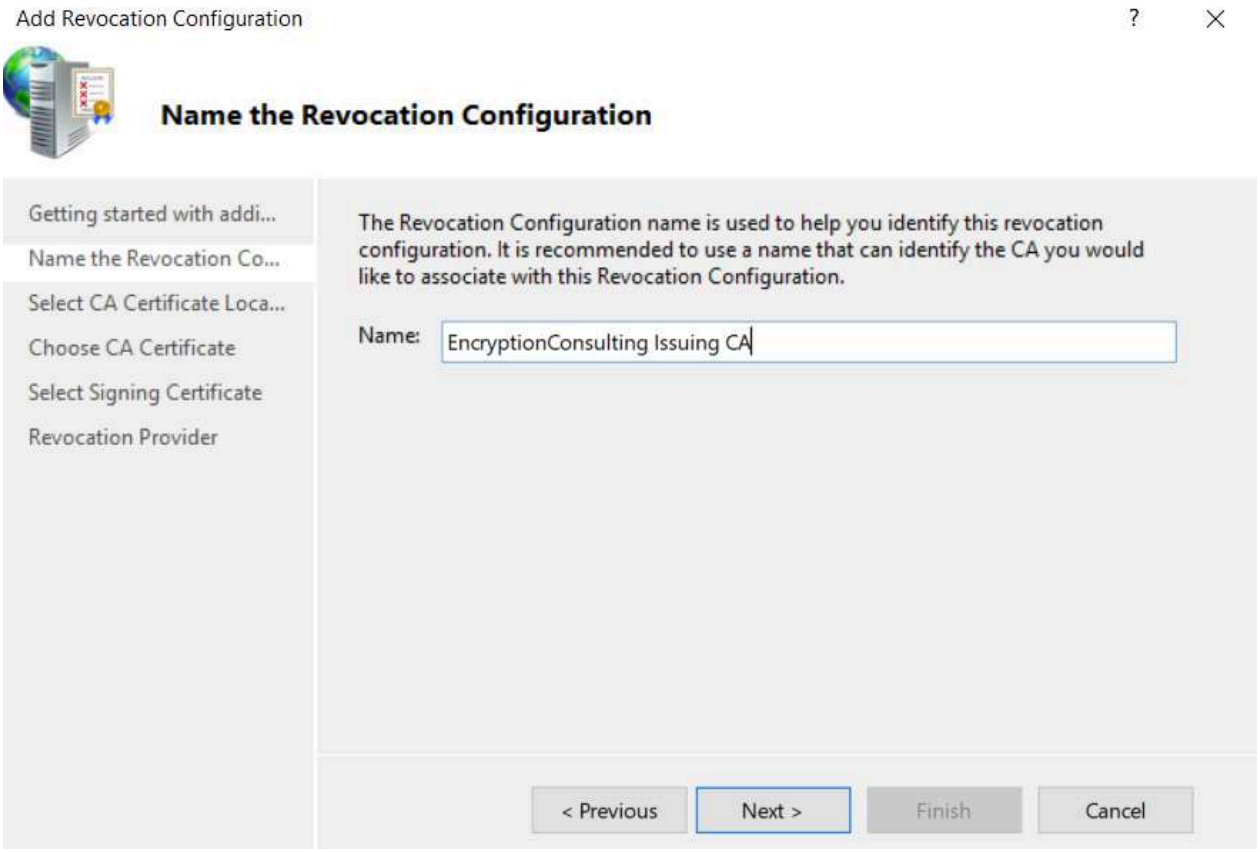
To configure the revocation configuration:

1. On SRV1.EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
2. Open Server Manager navigate to **Tools** and click on **"Online Responder Management".**
3. Right-click **Revocation Configuration** and then click **Add Revocation Configuration.**

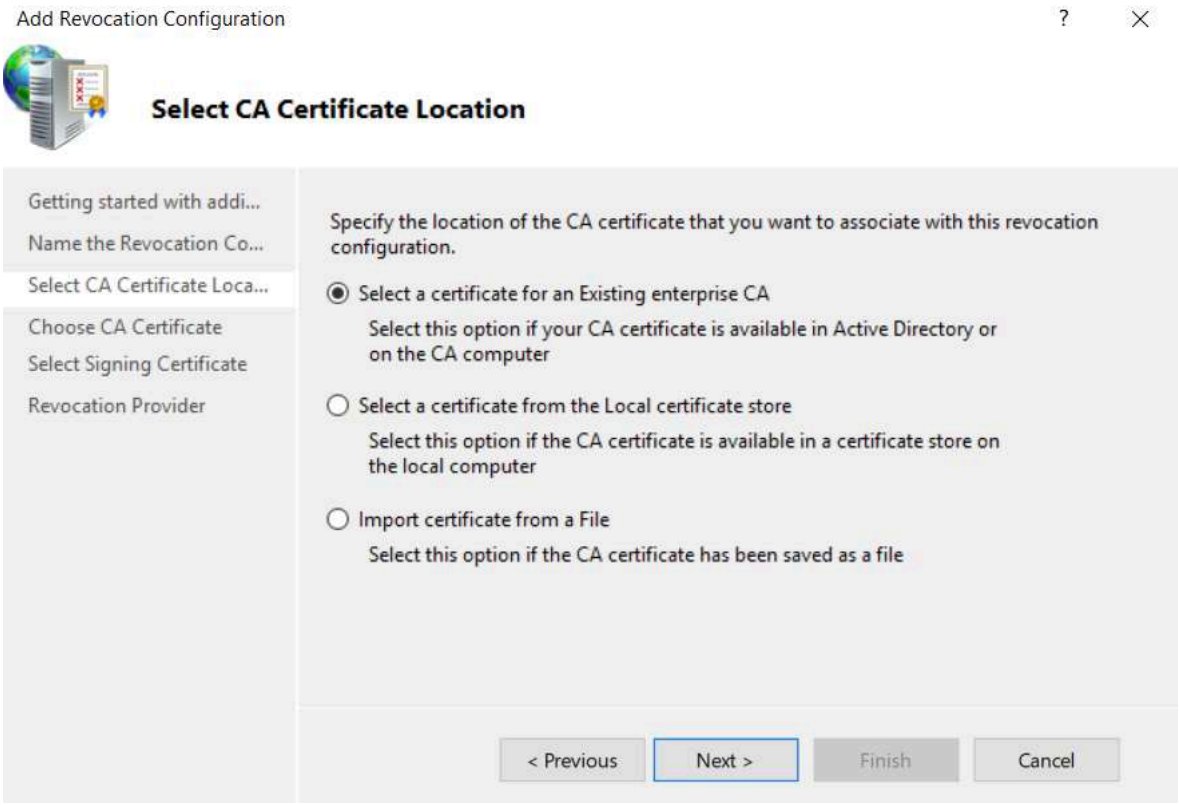
4. On the **Getting Started with Adding a Revocation Configuration** page click **Next.**



5. In **Name**, enter **EncryptionConsulting Issuing CA**, and then click **Next.**

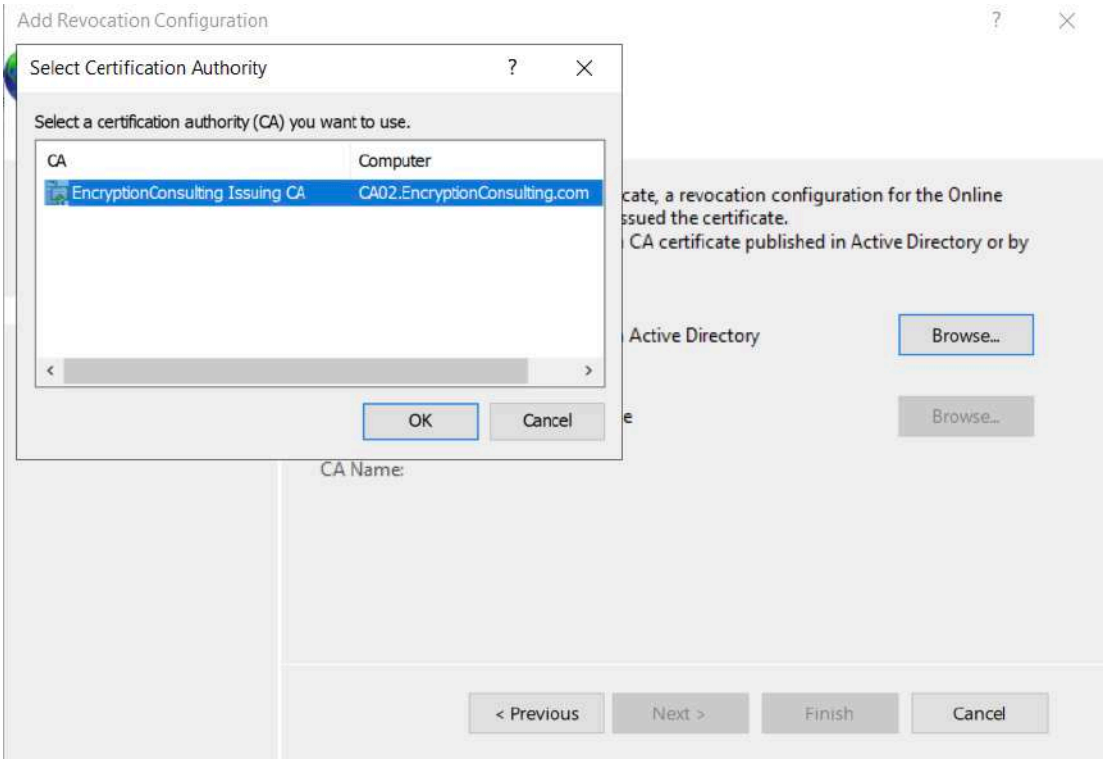


6. On the **Select CA Certificate Location** page ensure that **Select a certificate for an Existing enterprise CA** is selected, then click **Next**.

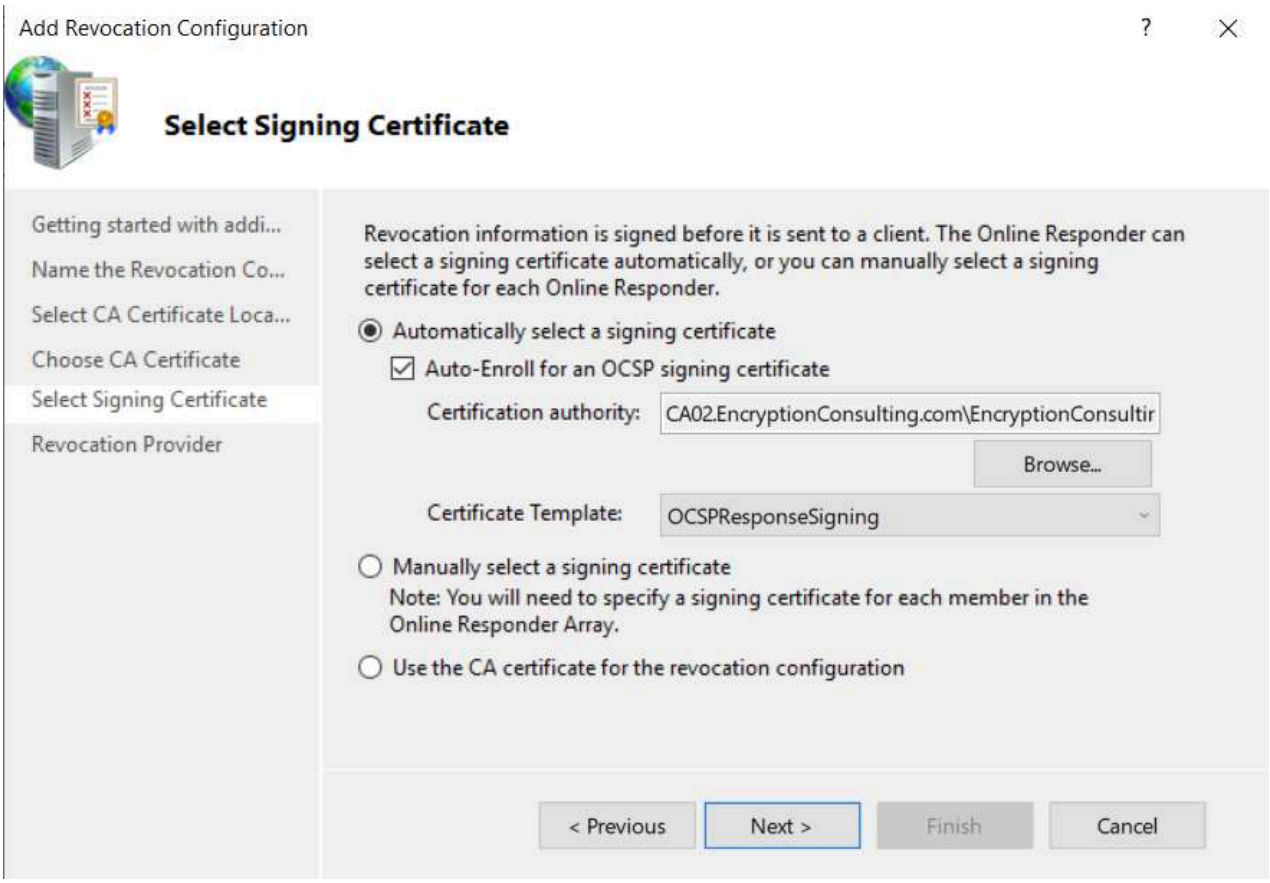


7. On the **Choose CA Certificates** page, ensure that **Browse CA certificates published in Active Directory** is selected, and then click **Browse.**

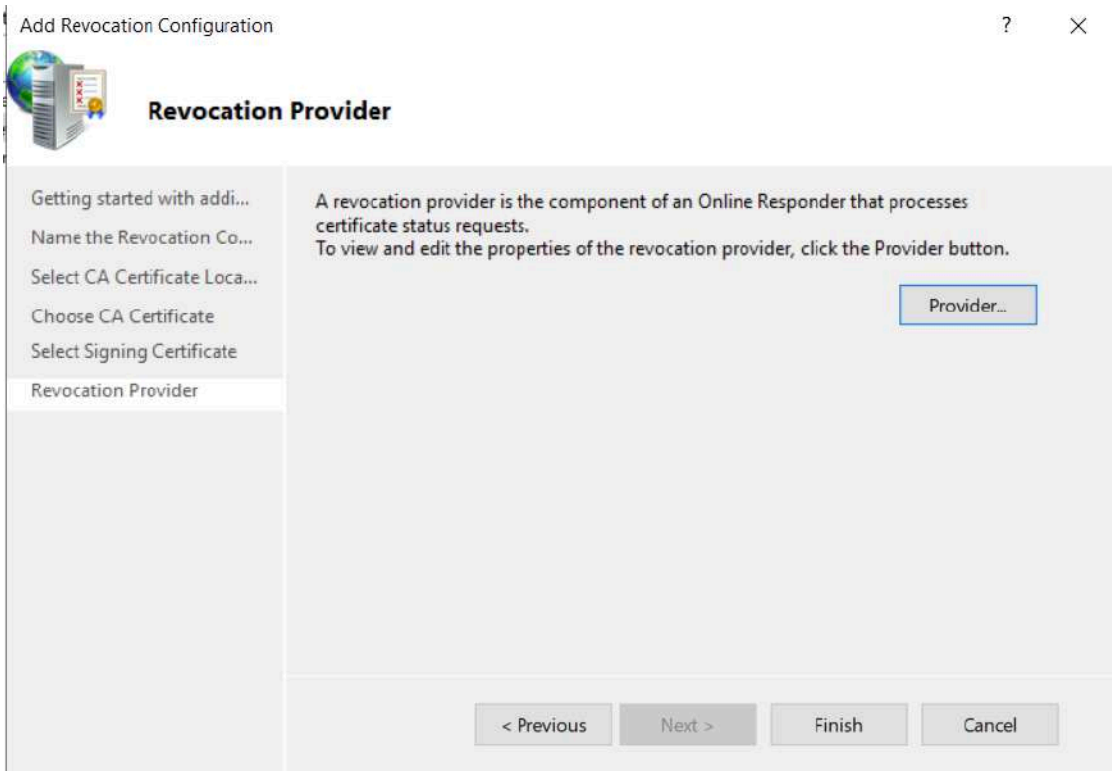
8. On the **Select Certification Authority** dialog box, ensure that **EncryptionConsulting Issuing CA** is selected, and then click **OK**. Click **Next.**



9. Leave the defaults on the **Select Signing Certificate** page, and then click **Next.**



10. On the **Revocation Provider** page, click **Provider.**



11. Review the choices listed for OCSP Responder to down CRLs in the form of LDAP and HTTP locations.
    - Note: Depending on your needs you could select either the LDAP or HTTP as your primary location for OCSP Responder to download CRLs. You can change order for LDAP and HTTP URLs using **Move Up** or **Move Down** button. Leave the defaults as they appear.

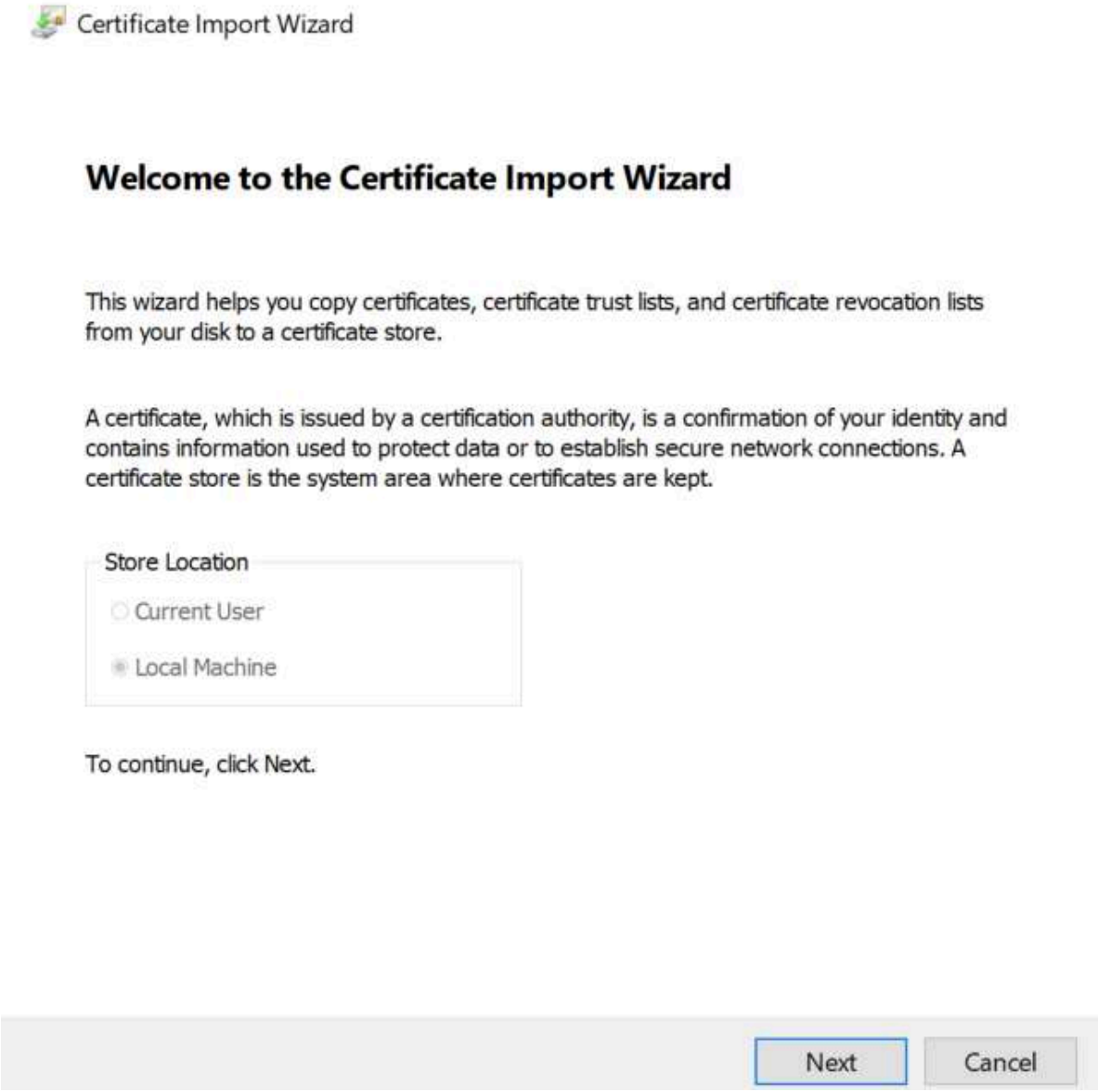
12. Clear the **Refresh CRLs based on their validity periods**. In the **Update CRLs at this refresh interval (min)** box, type **15**, and then click **OK**. Click **Finish.**
    - Note: Modifying this setting to download CRLs at a faster rate than the CRLs normal expiration makes it possible for the OCSP responder to rapidly download new CRLs rather than use the last downloaded CRLs normal expiration date. Pro duction needs may differ from the value chosen here.
13. In the Certification Authority console, expand **Array Configuration** and then click **SRV1.**
14. Review **Revocation Configuration Status** in the middle pane to ensure there is a signing certificate present and the status reports as OK. The provider is successfully using the current configuration.

Task 5: Configure Group Policy to Provide the OCSP URL for the EncryptionConsulting Issuing CA

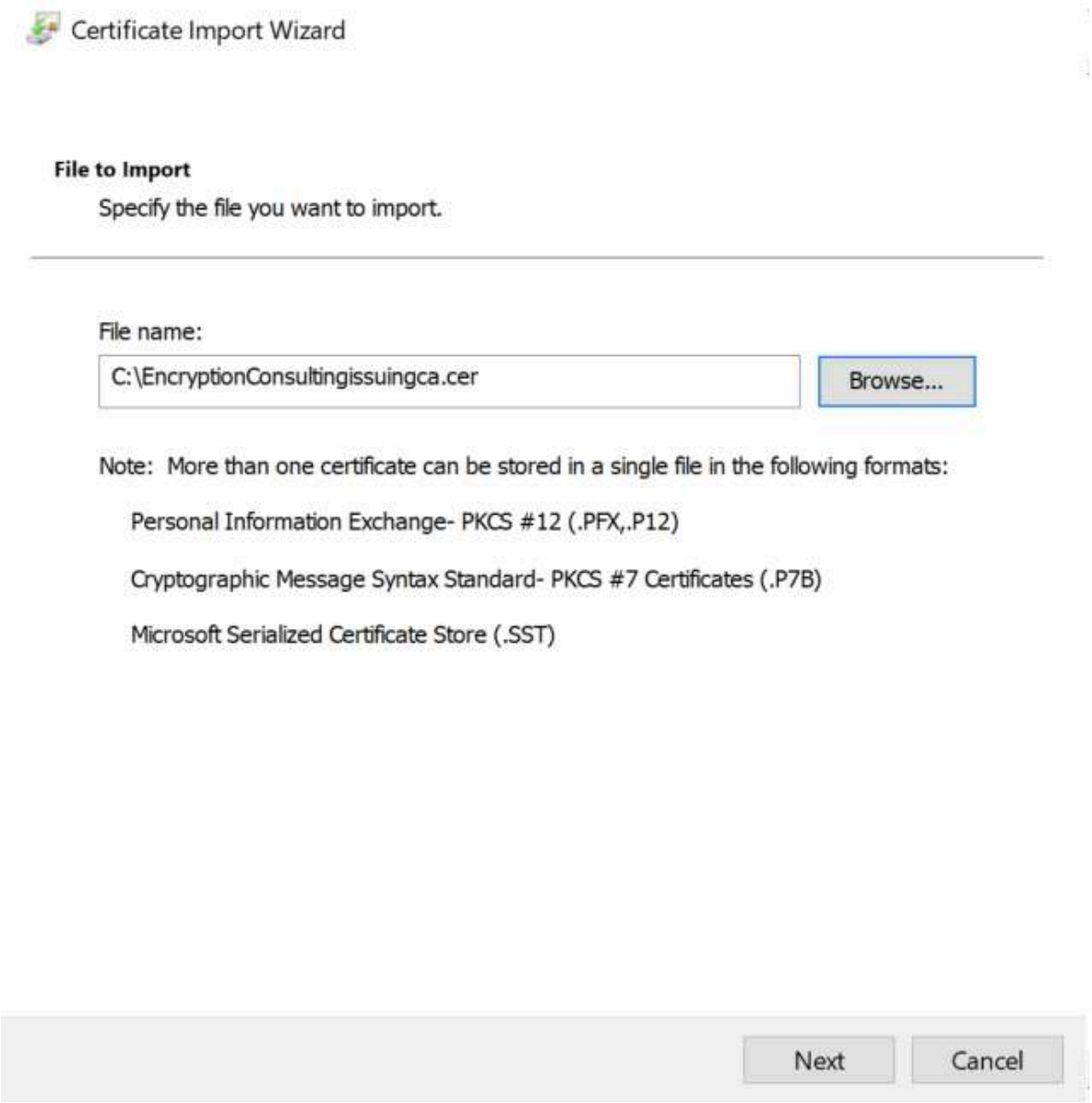
This configuration would only be needed to allow existing certificate holders to take advantage of a new OCSP responder without having to re-enroll new certificates with the required OCSP URL added in them.

1. Ensure you are logged on to DC01. EncryptionConsulting.com as EncryptionConsu\Administrator.
2. Open an administrative command prompt and run the following commands:
    - **cd**
    - **certutil -config "ca02.EncryptionConsulting.com\EncryptionConsulting Issuing CA" -ca.cert EncryptionConsultingissuingca.cer**
3. Click **Start**, click **Run**, and then type **gpmc.msc.** Press **ENTER.**
4. Expand **Forest**, expand **Domains**, expand **EncryptionConsulting.com**, and then expand **Group Policy Objects.**
5. Right click **Default Domain Policy,** then click **Edit.**
6. Under **Computer Configuration,** expand **Policies**, expand **Windows Settings**, expand **Security Settings,** and then expand **Public Key Policies.**
7. Right-click **Intermediate Certification Authorities,** and then click **Import.**

8. On the **Welcome to Certificate Import Wizard** page, click **Next.**

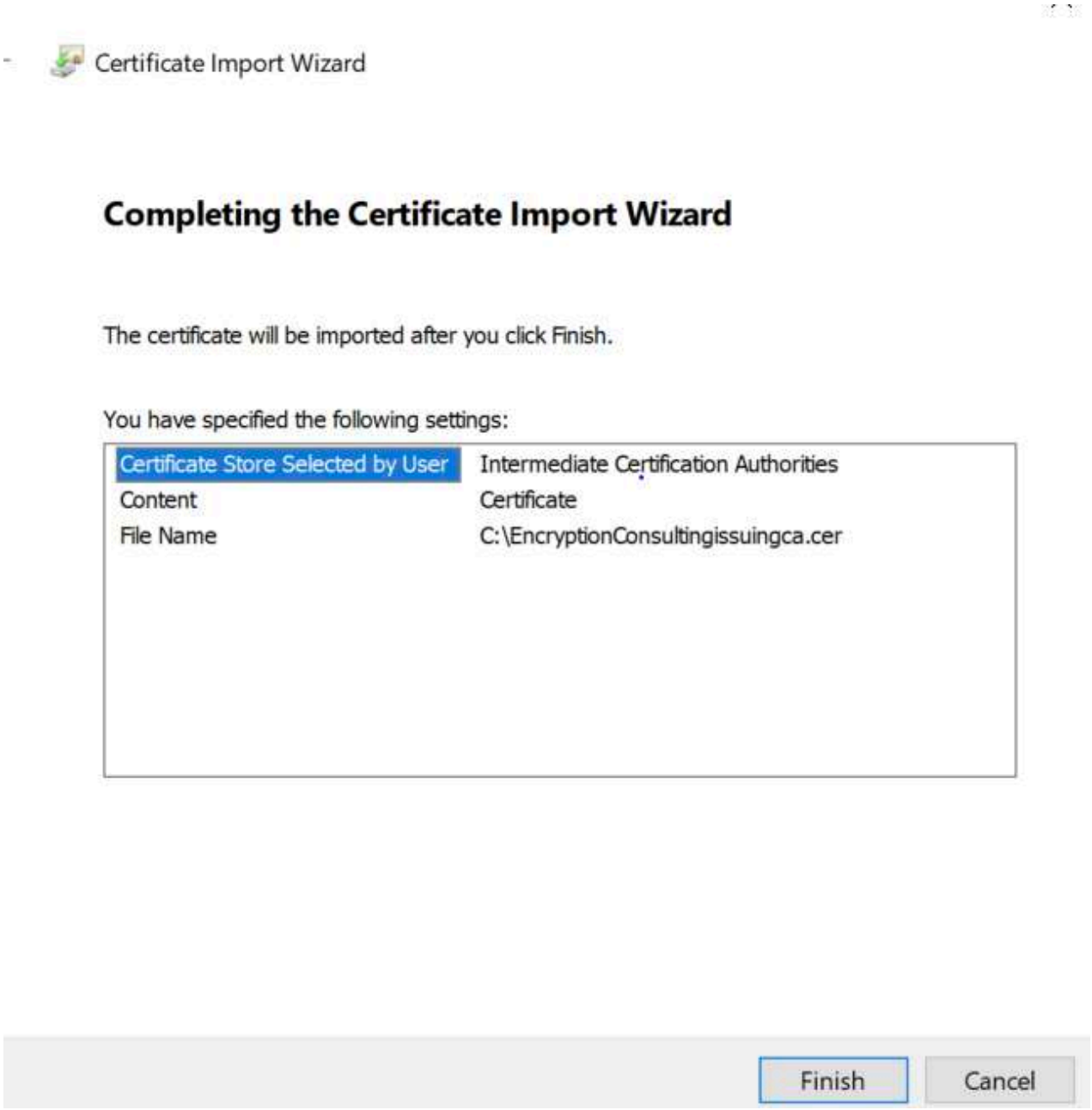


9. In **File name**, type **C:\EncryptionConsultingissuingca.cer**, and then click **Next**.

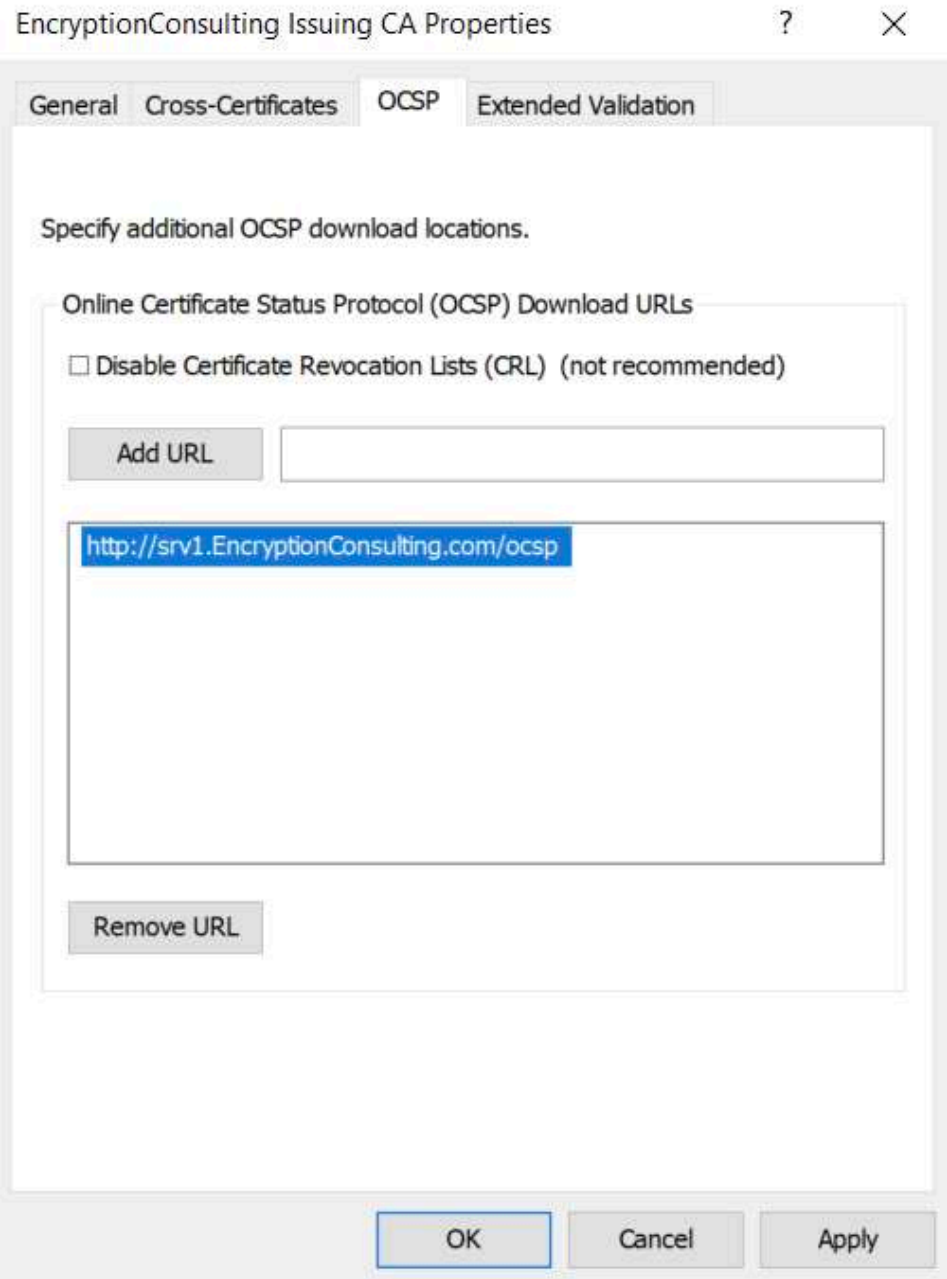


10. On the **Certificate Store** page, click **Next.**

11. On the **Completing the Certificate Import Wizard**, click **Finish**, and then click **OK.**



12. In the console tree, select **Intermediate Certification Authorities.**
13. In the details pane, right-click **EncryptionConsulting Issuing CA certificate**, then click **Properties.**
14. On the **OCSP** tab, in **Add URL** enter **http://srv1.EncryptionConsulting.com/ocsp**, and then click **Add URL**. Click **OK.**



15. Close the Group Policy Management Editor and then close Group Policy Management console.

Activity 8: Verify the PKI Hierarchy Health

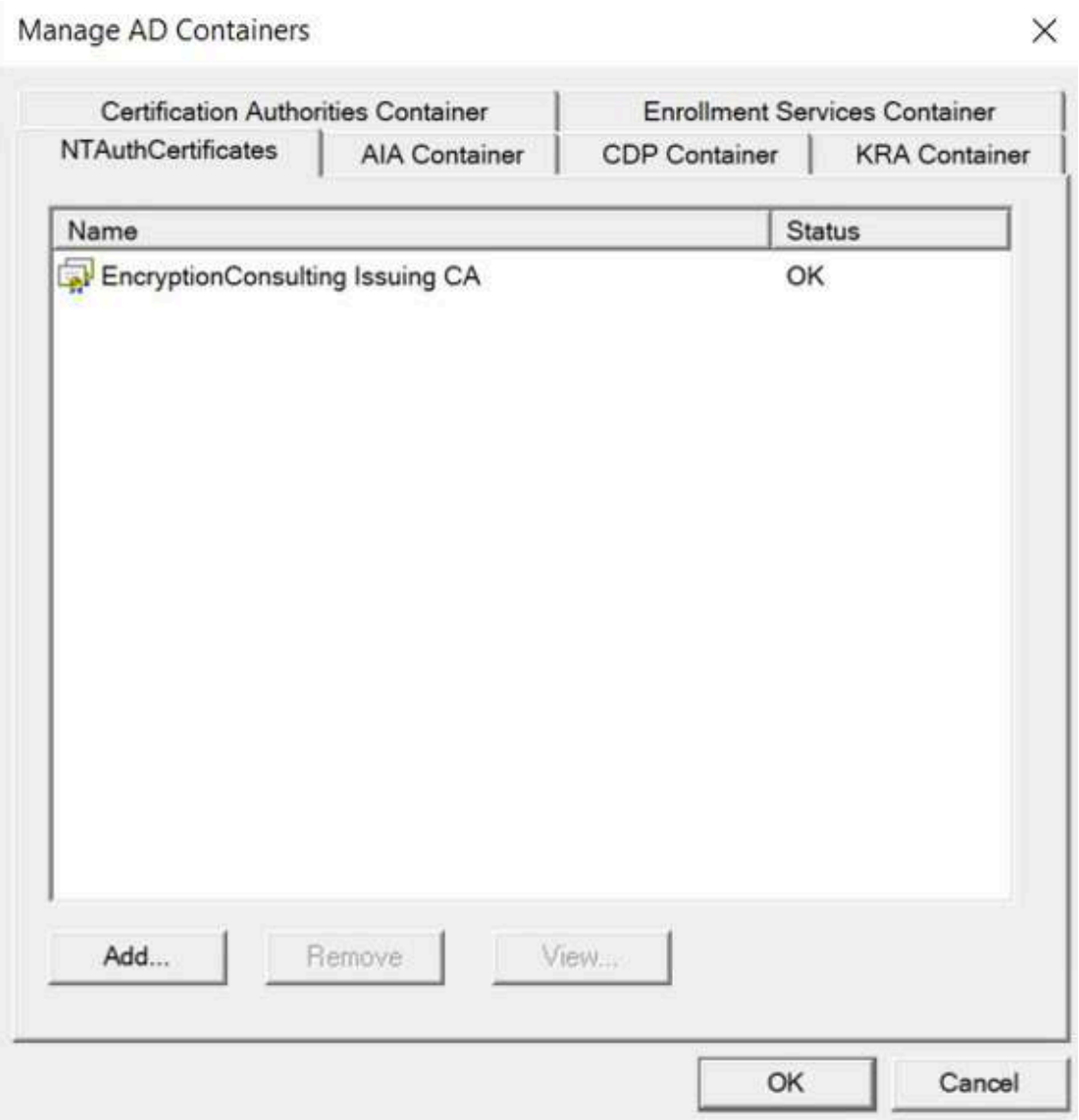
Task 1: Win10

1. Log on to WIN10 as the local administrator.
2. Click **Start**, type **ncpa.cpl** and press **ENTER.**
3. In Network Connections, right-click the **Local Area Connection** and then click **Properties.**
    - If there are more than one Local Area Connection icons in the Network Connections, you want to modify the one that is connected to network segment shared by all the computers that you have installed for this lab.
4. Click the **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties.**
5. Select the **Use the Following IP address**. Configure the **IP address**, **Subnet mask**, and **Default gateway** appropriately for your test network.
    - **IP Address**: 192.168.1.14
    - **Subnet mask**: 255.255.255.0
    - **Default gateway**: <optional>
6. Select the Use the following DNS server address. Configure the P**referred DNS server** as the IP address of your domain controller. Click **OK**. Click **Close.**
    - **Preferred DNS Server**: 192.168.1.10.
7. Click **Start**, type **sysdm.cpl** and press **ENTER**. Click **Change**. (Ensure the computer name is already set to **WIN10** - otherwise change it)
8. In **Member of**, select **Domain**, and then type **EncryptionConsulting.com.** Click **OK.**
9. In **Windows Security**, enter the **Username** and **password** for the domain administrator account. Click **OK.**
10. You should be welcomed to the EncryptionConsulting domain. Click **OK**.
11. When prompted that a restart is required, click **OK**. Click **Close**. Click **Restart Now.**

Task 2: Check PKI Health with Enterprise PKI

To use the Enterprise PKI console to check PKI health:

1. On CA02. EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
2. Open Server Manager.
3. In the console tree, under **Roles** and **Active Directory Certificate Services**, click **Enterprise PKI**.
    - Alternatively, you can run Enterprise PKI by running **PKIView.msc** from an administrative command prompt.
4. Right click **Enterprise PKI** and then click **Manage AD Containers.**

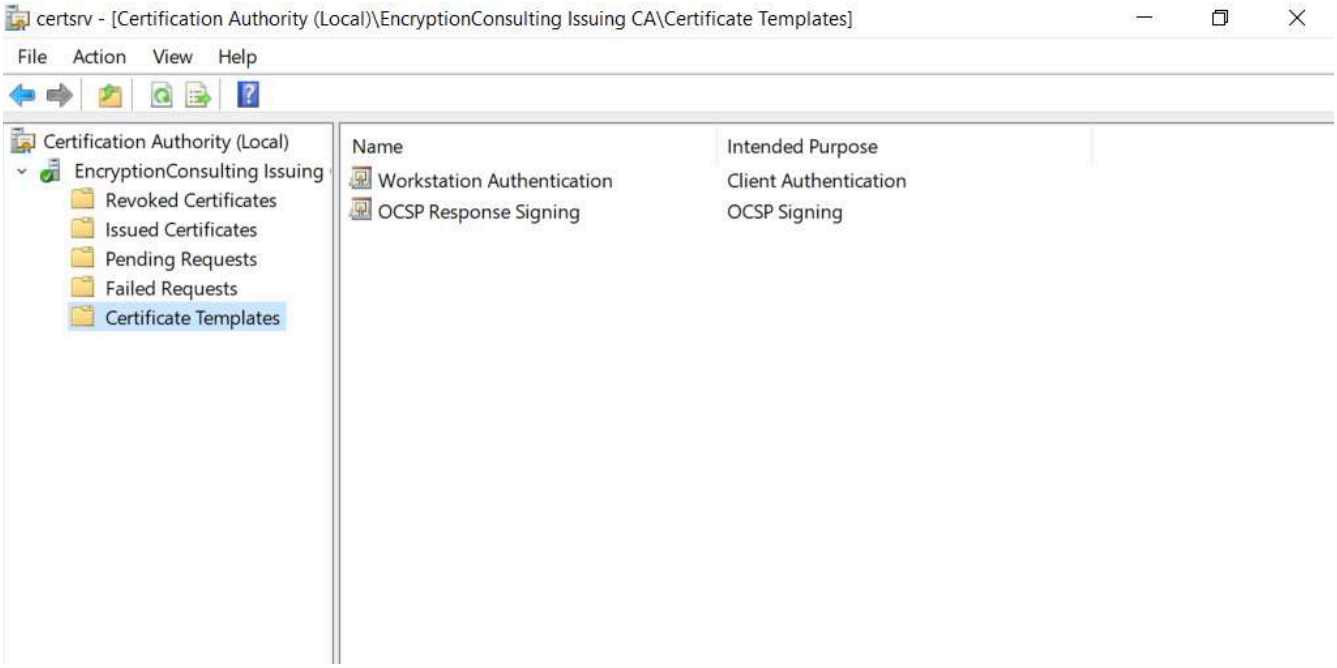


5. On the **NTAuthCertificates** tab, verify the EncryptionConsulting Issuing CA certificate appears with a status of **OK.**
6. On the **AIA Container** tab, verify both the **EncryptionConsulting Root CA** and the **EncryptionConsulting Issuing CA** certificates are present with a status of **OK.**
7. On **CDP Container** tab, verify **EncryptionConsulting Root CA base CRL, EncryptionConsulting Issuing CA base**, and the **Delta CRLs** are present with a status of **OK.**
8. On **Certification Authorities Container,** verify **EncryptionConsulting Root CA** certificate is present with a status of **OK.**
9. On **Enrollment Services Container**, verify **EncryptionConsulting Issuing CA** certificate is present with a status of **OK.**

Task 3: Configure Certificate Distribution on the Encryption Consulting Issuing CA

To publish a certificate for computers in the enterprise:

1. On CA02. EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
2. In the **Certification Authority** console, ensure that **EncryptionConsulting Issuing CA** is expanded.
3. Right-click **Certificate Templates** select **New** and select **Certificate Template to Issue.**
4. On the **Enable Certificate Templates** dialog box, click **Workstation Authentication**, page and then click **OK.**

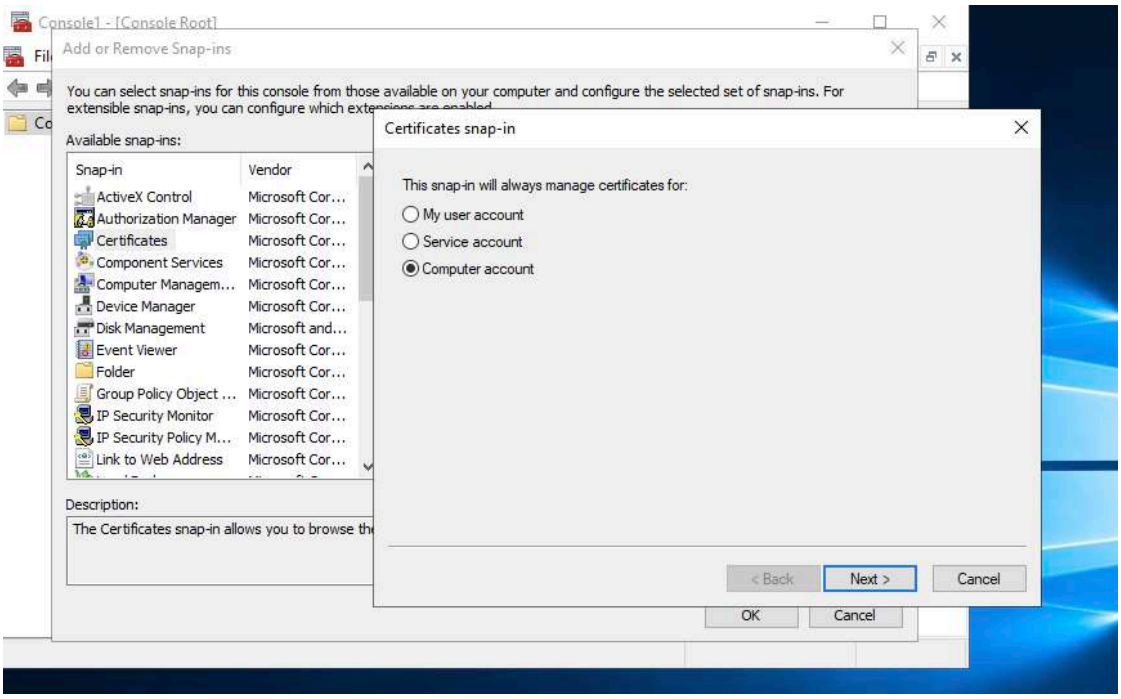


Task 4: Obtain a Certificate Using WIN10 and Verify PKI Health

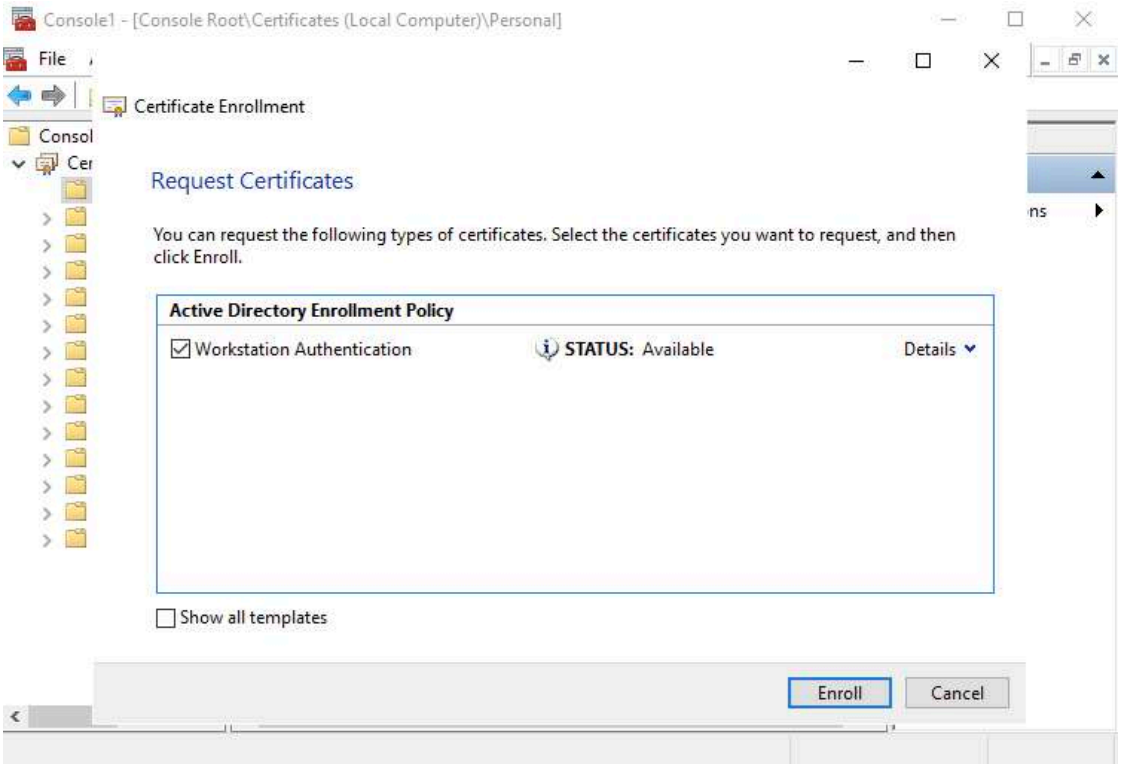
To obtain a certificate for WIN10 and verify PKI health:

1. Log into Win10. EncryptionConsulting.com as EncryptionConsu\Administrator. (Ensure that you switch user to log on as EncryptionConsu\Administrator)
2. Click **Start**, type **mmc** and then press ENTER.
3. Click **File**, and then click **Add/Remove Snap-in.**

4. Click **Certificates**, then click **Add**. Select **Computer Account**, and then click **Finish**. Click **OK.**

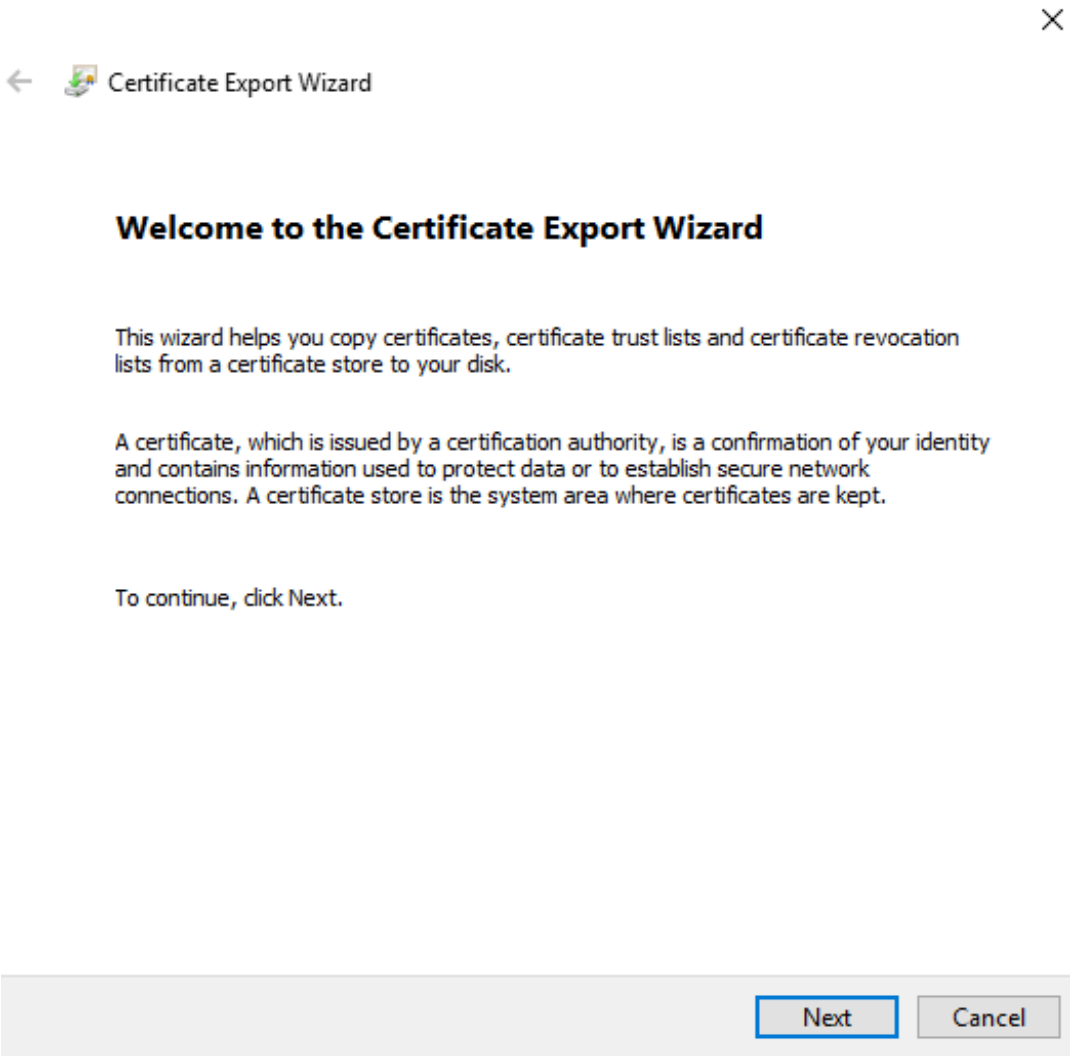


5. Expand **Certificates**, right click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
6. On the **Before you begin** page, click **Next.**
7. On the **Select Certificate Enrollment Policy** page, click **Next**.
8. Select **Workstation Authentication**, click **Enroll**. When the certificate is enrolled, click **Enroll.**

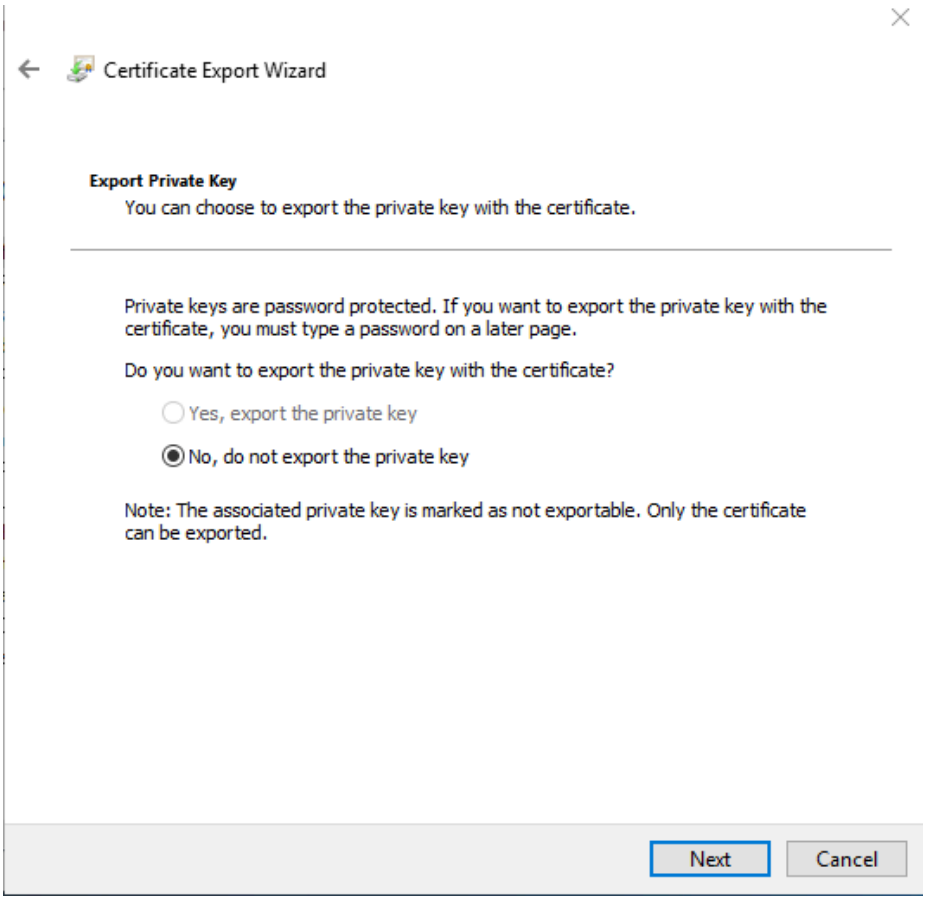


9. In the console tree, expand **Personal**, click **Certificates**. In the details pane, right click the **win10. EncryptionConsulting.com** certificate, click **All Tasks**, and then click **Export.**

10. On the the **Welcome to Certificate Export Wizard** page, click **Next.**



11. On the **Export Private Key**, click **Next.** (No, do not export the private key is selected by default).



12. On the **Export File Format** page, click Next. [DER encoded binary X.509 (.CER) is the default selection].
13. On the **File to Export** page, type **C:\win10**, and then click **Next.**
14. On the **Completing the Certificate Export Wizard** page, click then **Finish**, and then click **OK**.
15. Open a command prompt and run the following commands: (To open a command prompt, click **Start,** type **cmd**, and then press ENTER)
    - **cd**
    - **certutil -URL C:\win10.cer**
16. In the URL Retrieval Tool, perform the following steps, in the **Retrieve** section:
    - Select **OCSP (from AIA)** option and then click **Retrieve**. Confirm that it shows status as **Verified.**
    - Select **CRLs (from CDP)** option and then click **Retrieve.** Confirm that it shows status as **Verified.**
    - Select **Certs (from AIA)** option and then click **Retrieve.** Confirm that it shows status as **Verified.**
17. Click **Exit** to close URL Retrieval Tool.
18. From command prompt run following command to thoroughly verify certificate chain retrieval and revocation status.
    - **certutil -verify -urlfetch c:\win10.cer**
19. Review the output and make sure all the chain retrieval and revocation status successfully verified.