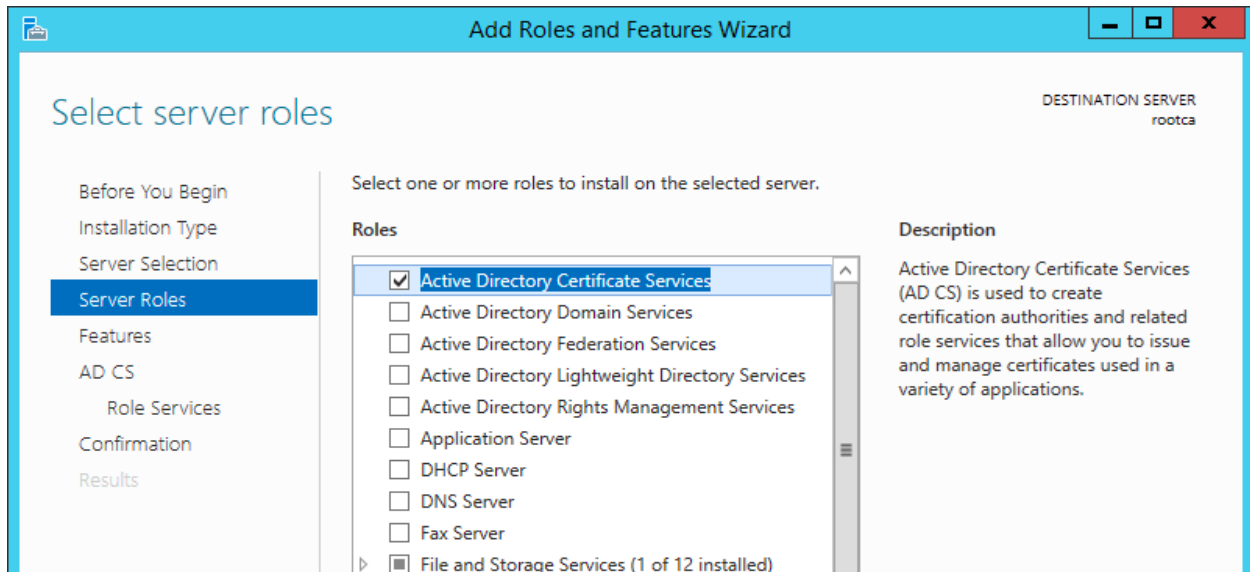
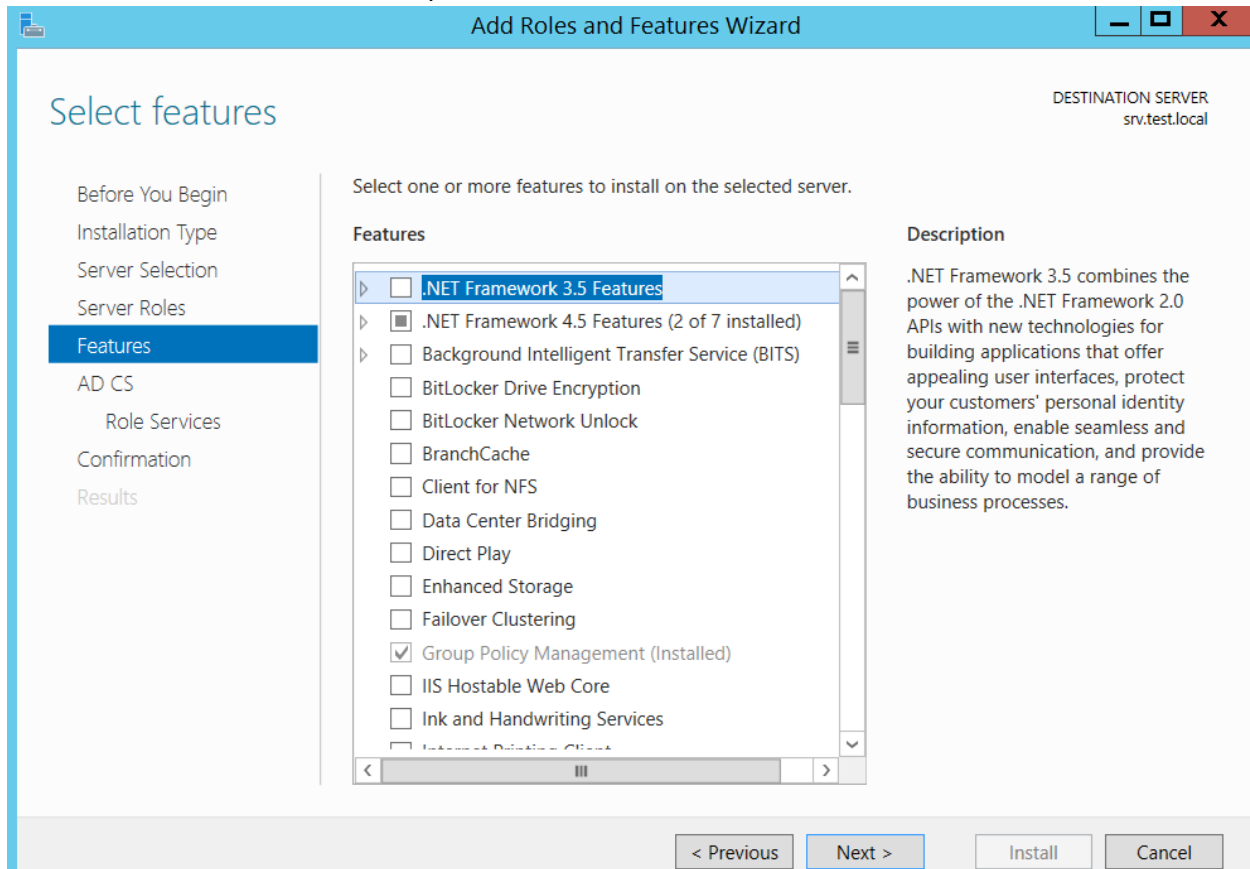


CA Server in Windows 2012:

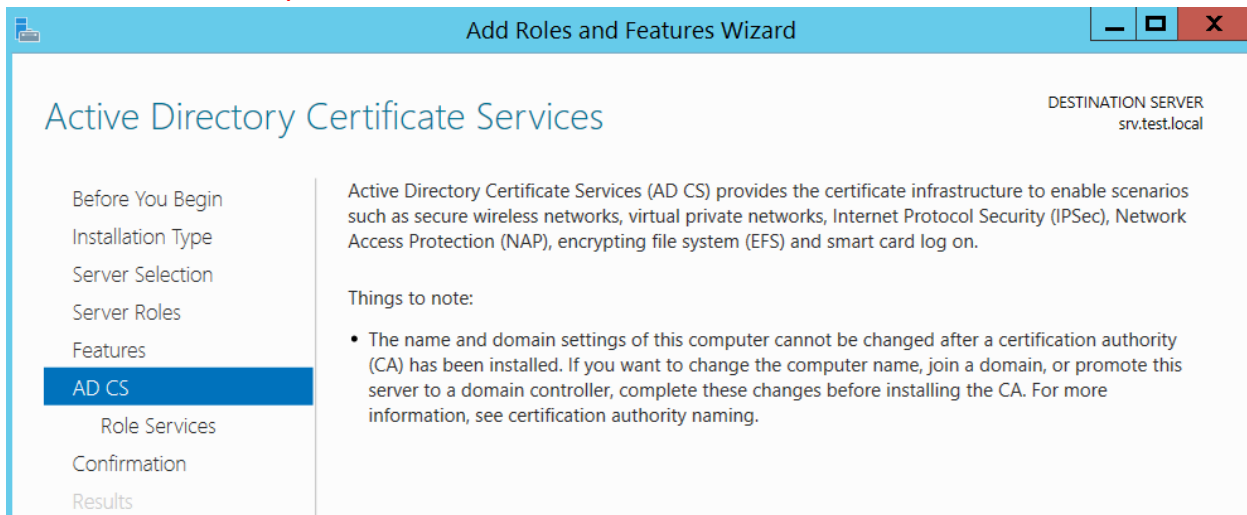
On the domain Server, open **Server Manager** and go through to **Select Server Roles** and click **Active Directory Certificate Services** and then click **Next...**



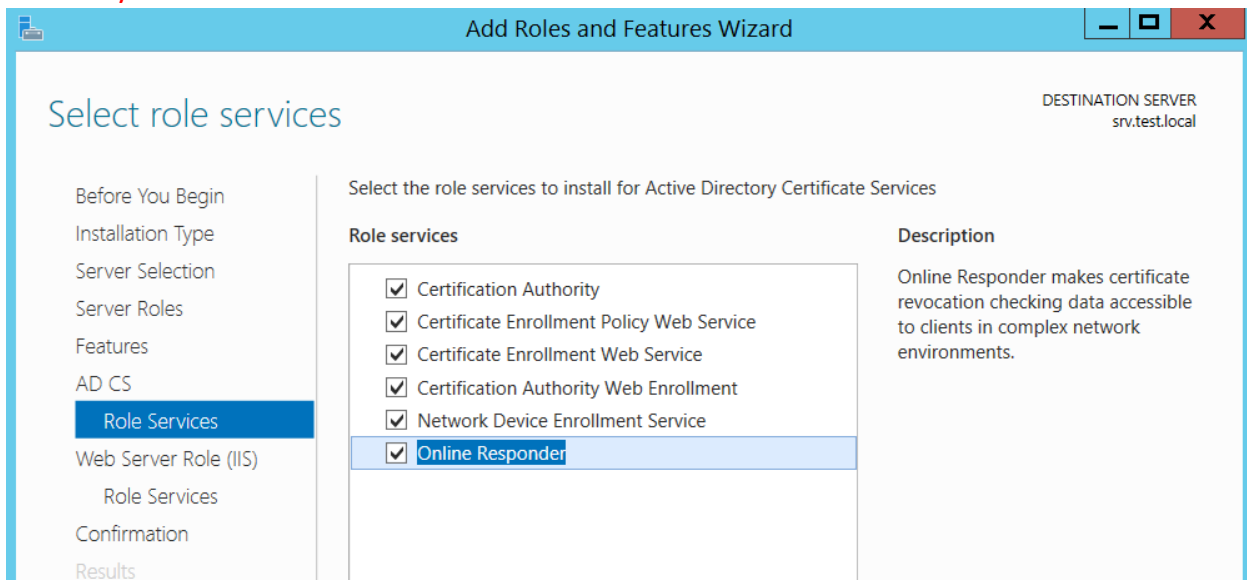
In the **Select Features** interface, proceed with **Next...**



In the **Active Directory Certificate Services** interface, click **Next...**



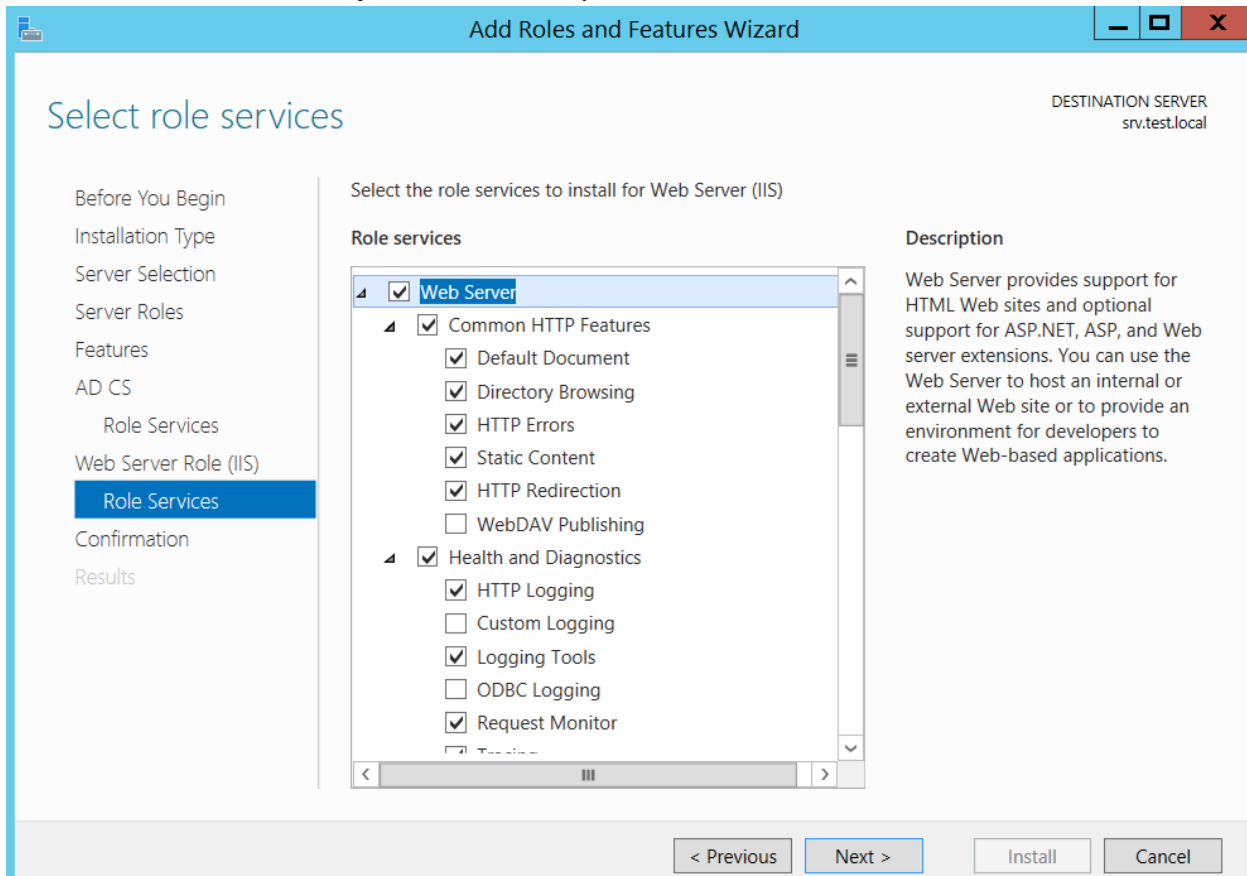
In **Select role services**, make sure you tick all specially, **Certificate Authority** and **Certification Authority Web Enrollment** check box and then click **Next...**



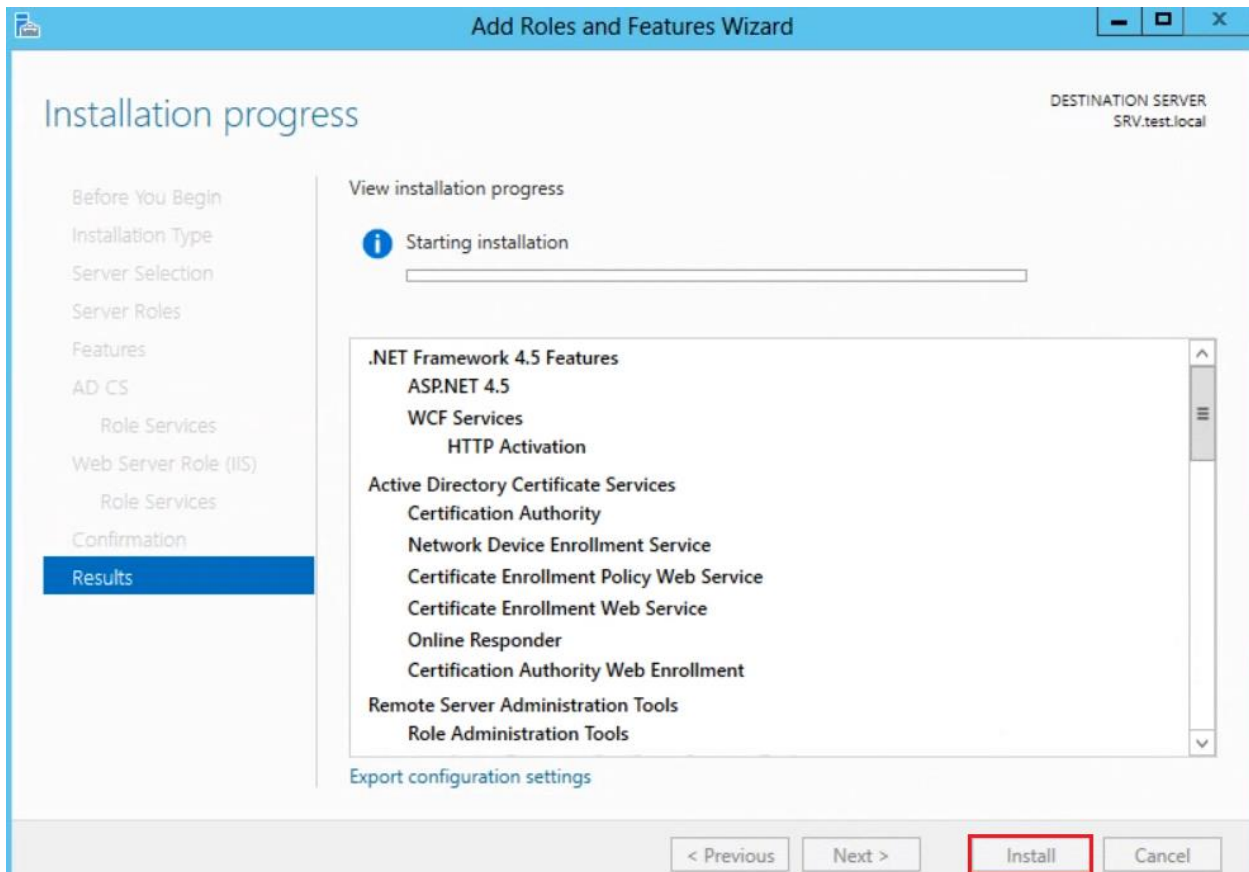
In the **Web Server Role (IIS)** interface, click **Next** to proceed...



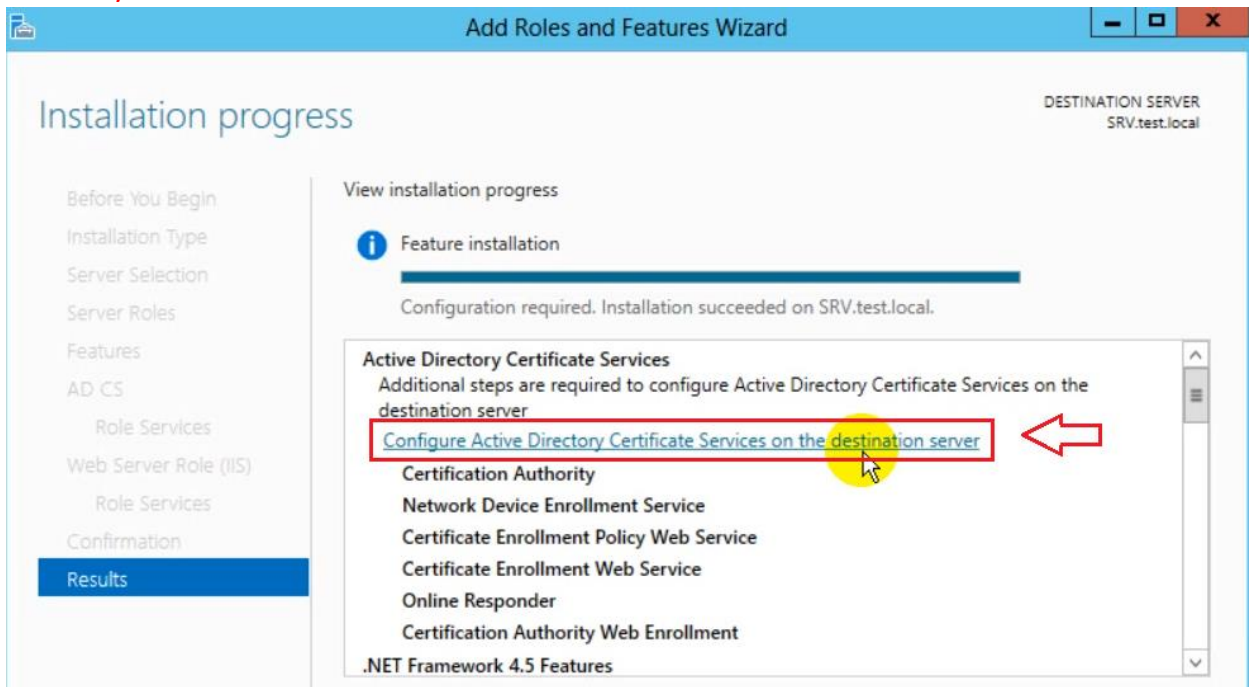
in the **Select Role Services**, just click **Next** to proceed...



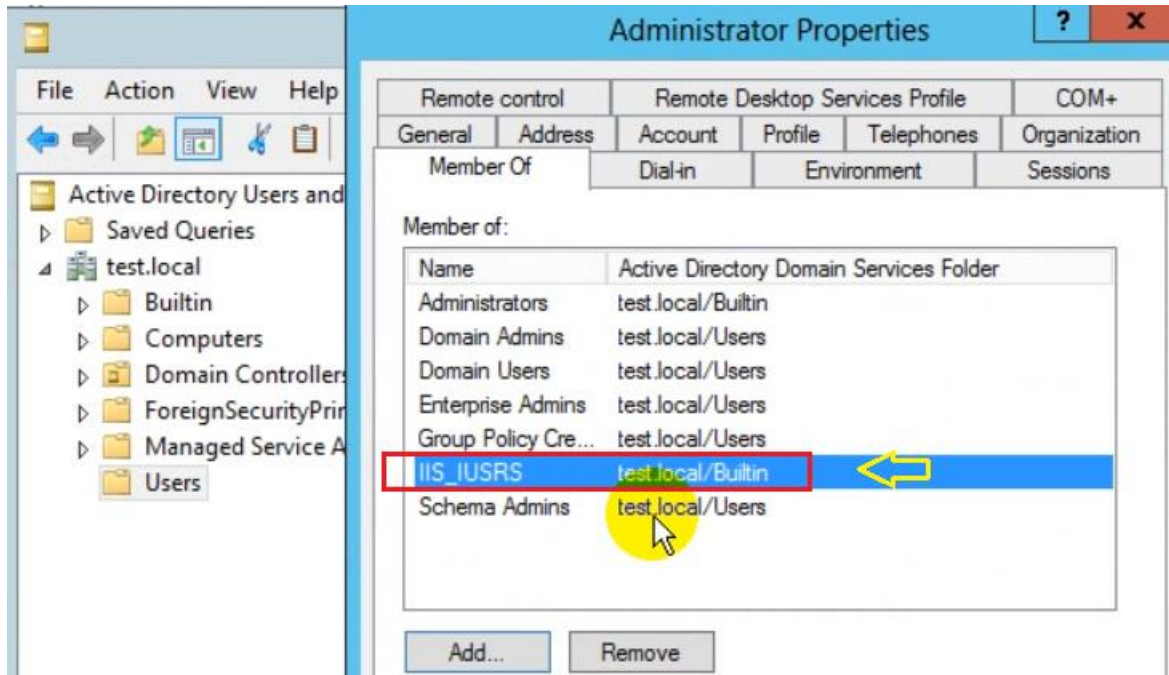
In the installation selections interface, click **Install...**



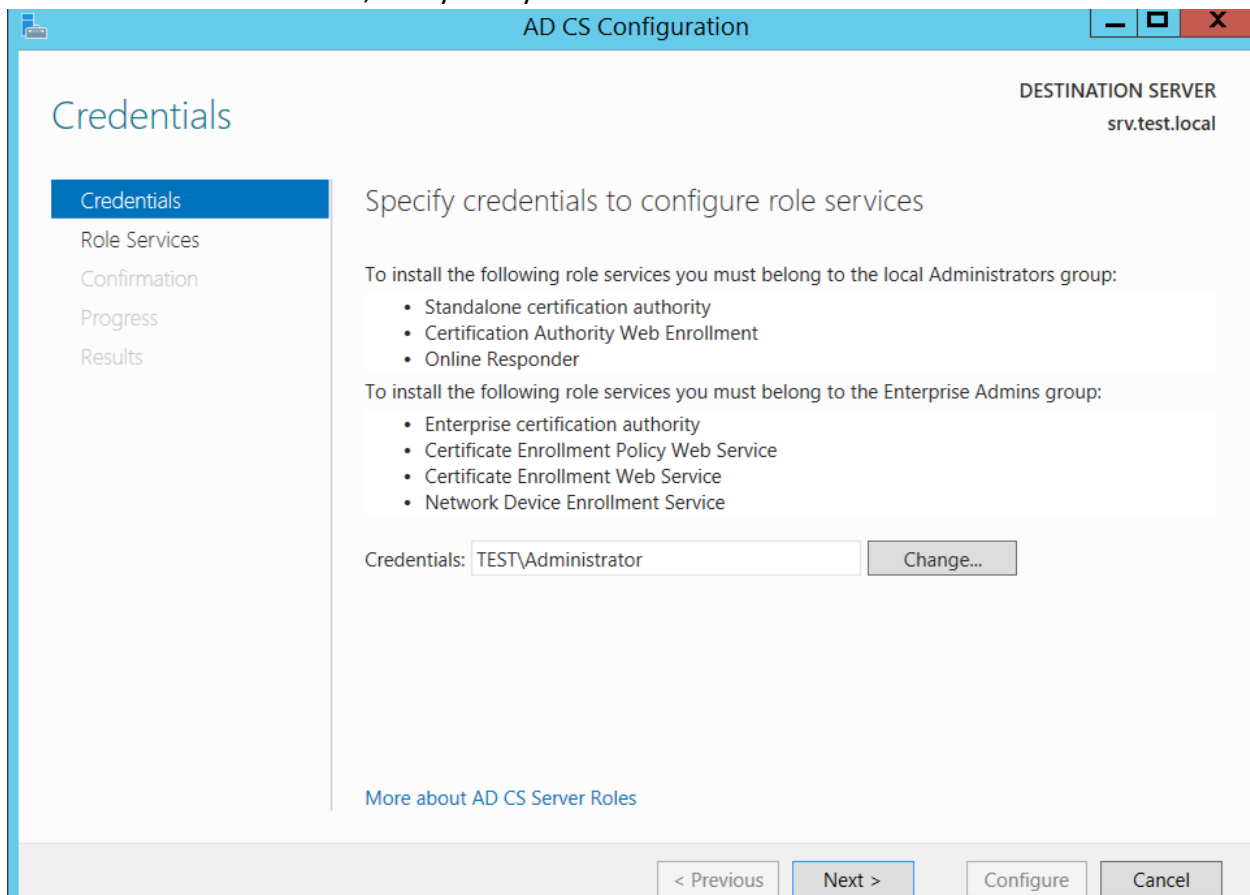
After installation complete, in the Installation progress interface, click **Configure Active Directory Certificate Services on the destination server...**



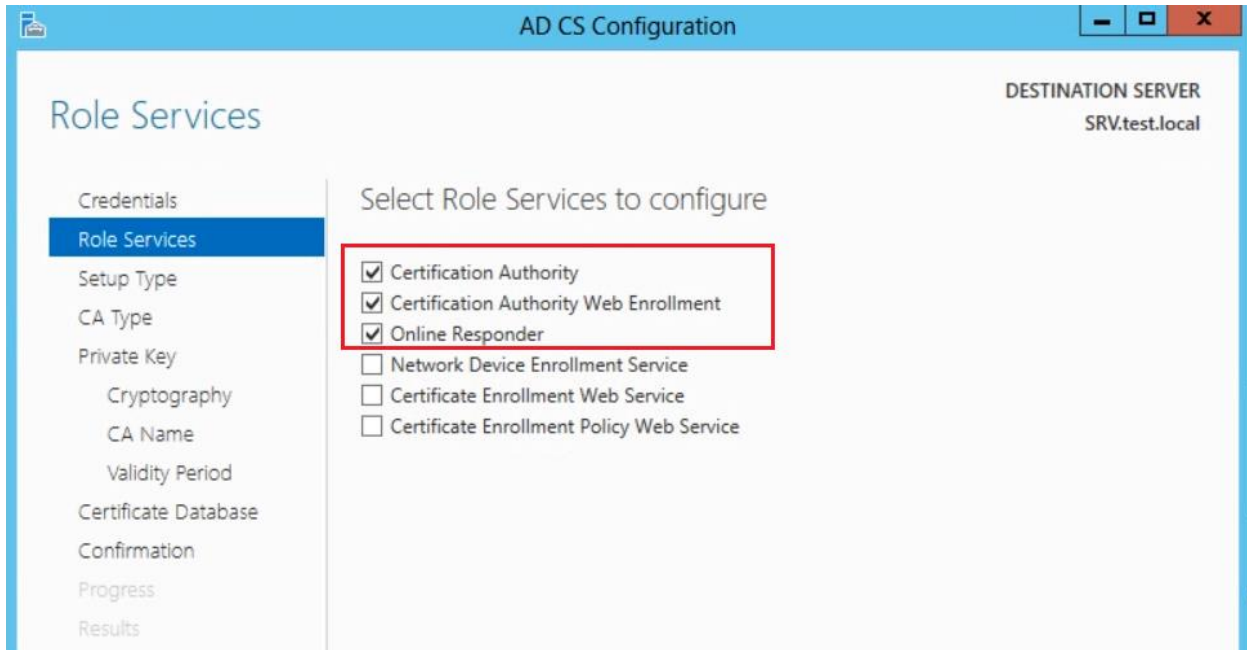
Make sure **Administrator** is the member of **IIS_IUSRS** group if not add them.



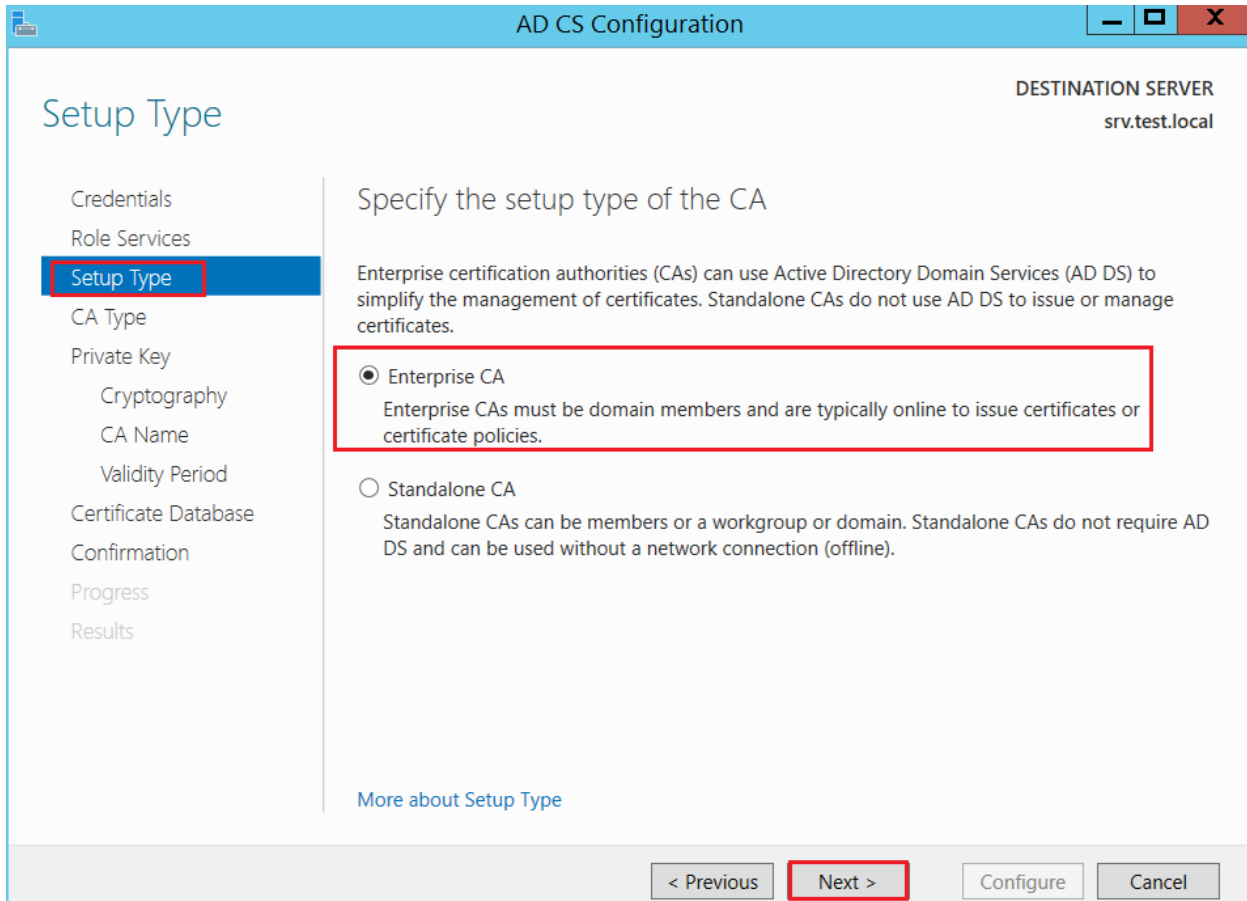
In the **Credentials** interface, verify that your Credentials is **Administrator** and then click **Next...**



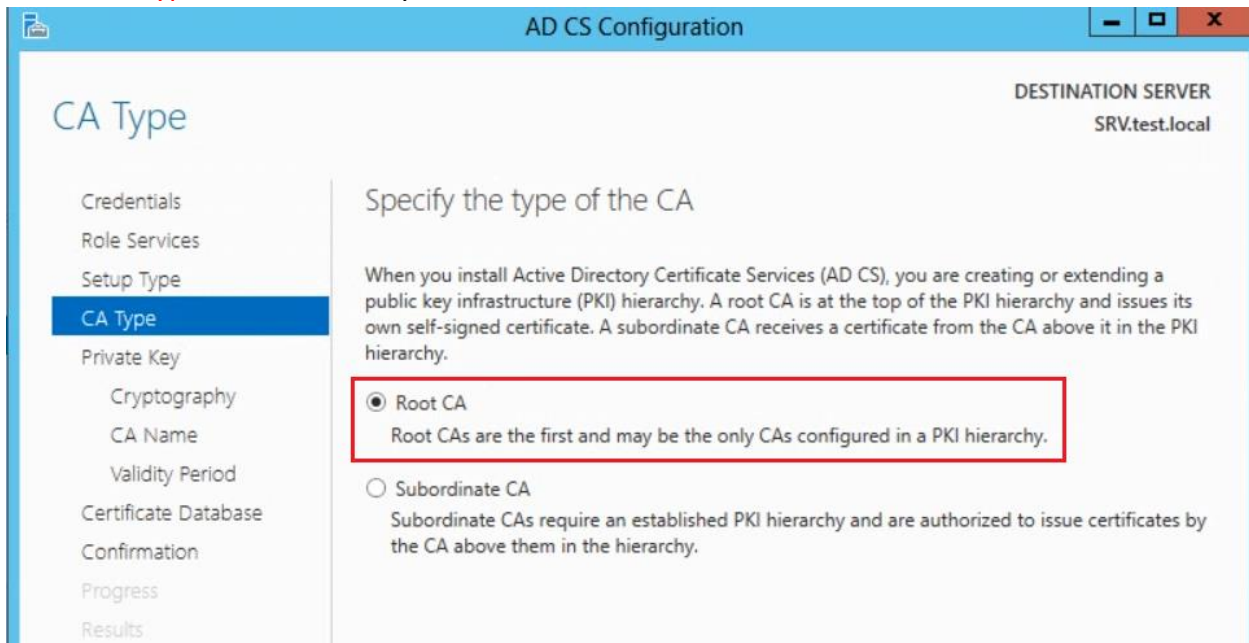
In the **Role Services** interface, tick **Certification Authority**, **Certification Authority Web Enrollment** and **Online Responder** and then click **Next...**



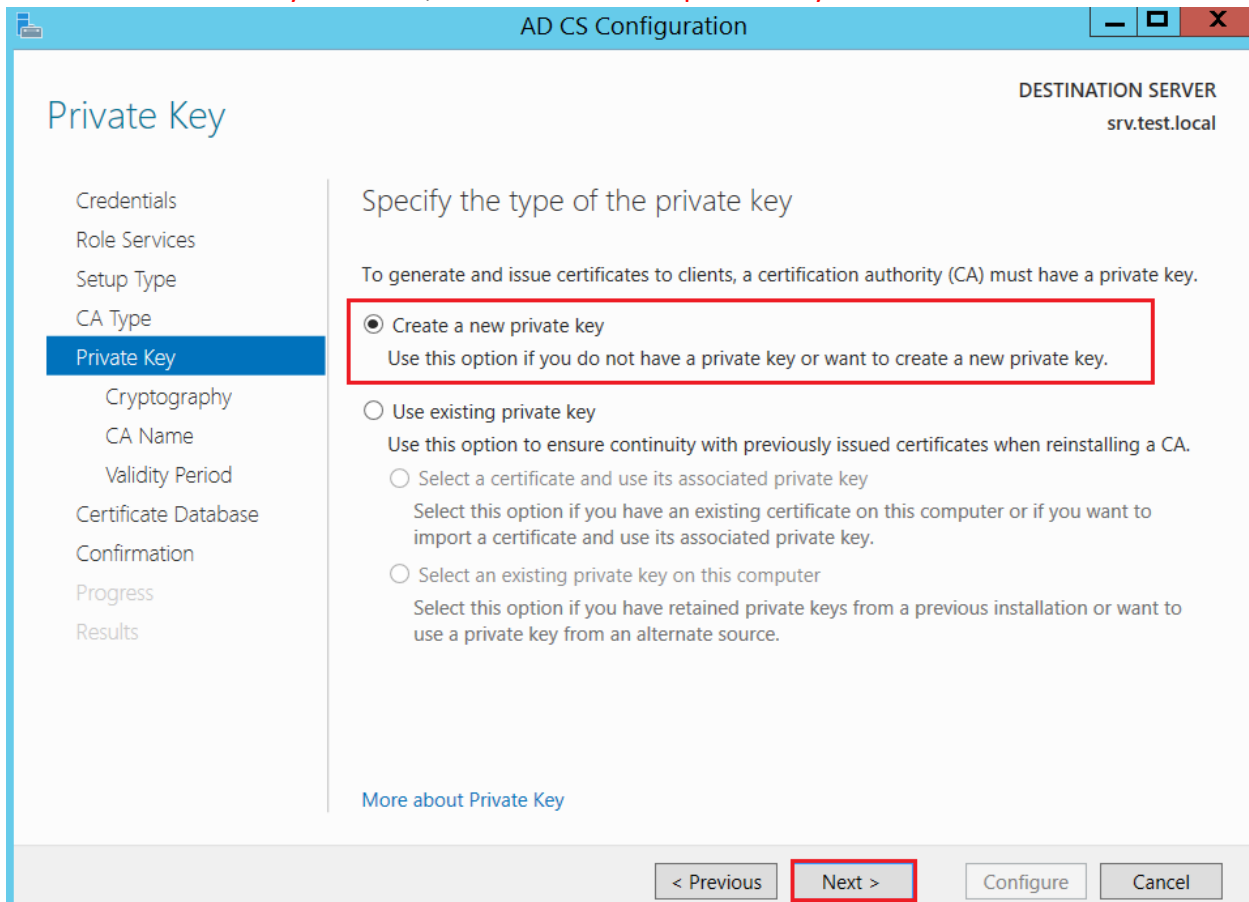
In the **Setup Type** interface, verify that **Enterprise CA** is selected and click **Next...**



In the **CA Type** interface, verify that **Root CA** is selected and then click **Next...**



Next in the **Private Key** interface, click **Create a new private key** and then click **Next...**



In **Cryptography for CA** interface, **setting** which **RSA Cryptography** with **2048 key** length and verify that **SHA256** is selected, and then click **Next...**

AD CS Configuration

DESTINATION SERVER
SRV.test.local

Cryptography for CA

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography**
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256**
- SHA384
- SHA512
- SHA1
- MD5

Allow administrator interaction when the private key is accessed by the CA.

Next in the **CA Name** interface, just proceed with **Next...**

AD CS Configuration

DESTINATION SERVER
srv.test.local

CA Name

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography
- CA Name**
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
test-SRV-CA

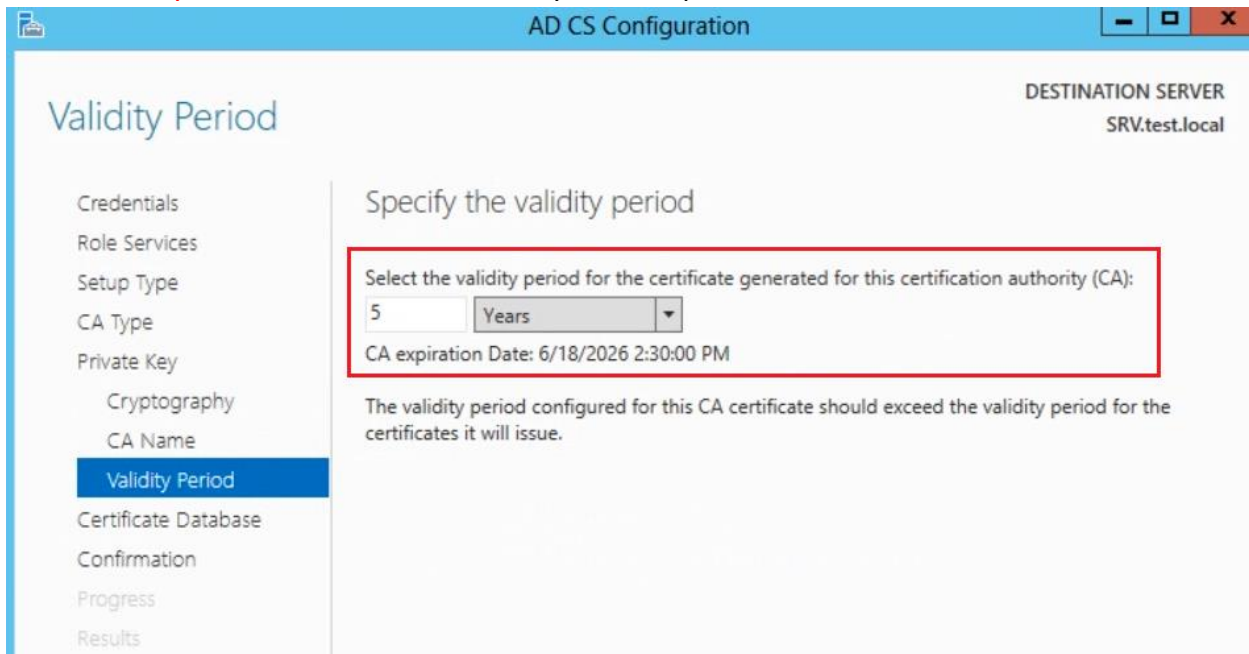
Distinguished name suffix:
DC=test,DC=local

Preview of distinguished name:
CN=test-SRV-CA,DC=test,DC=local

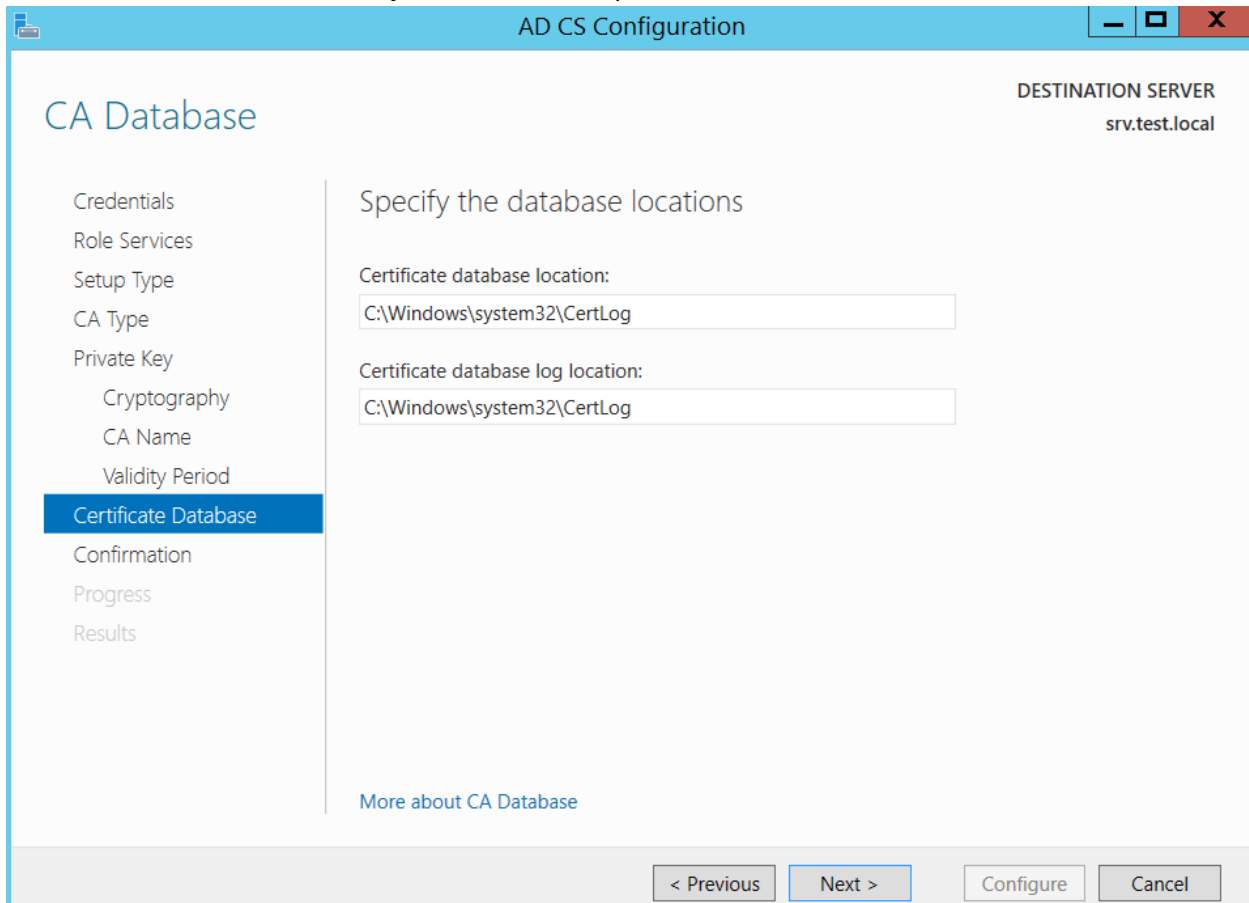
[More about CA Name](#)

< Previous Next > Configure Cancel

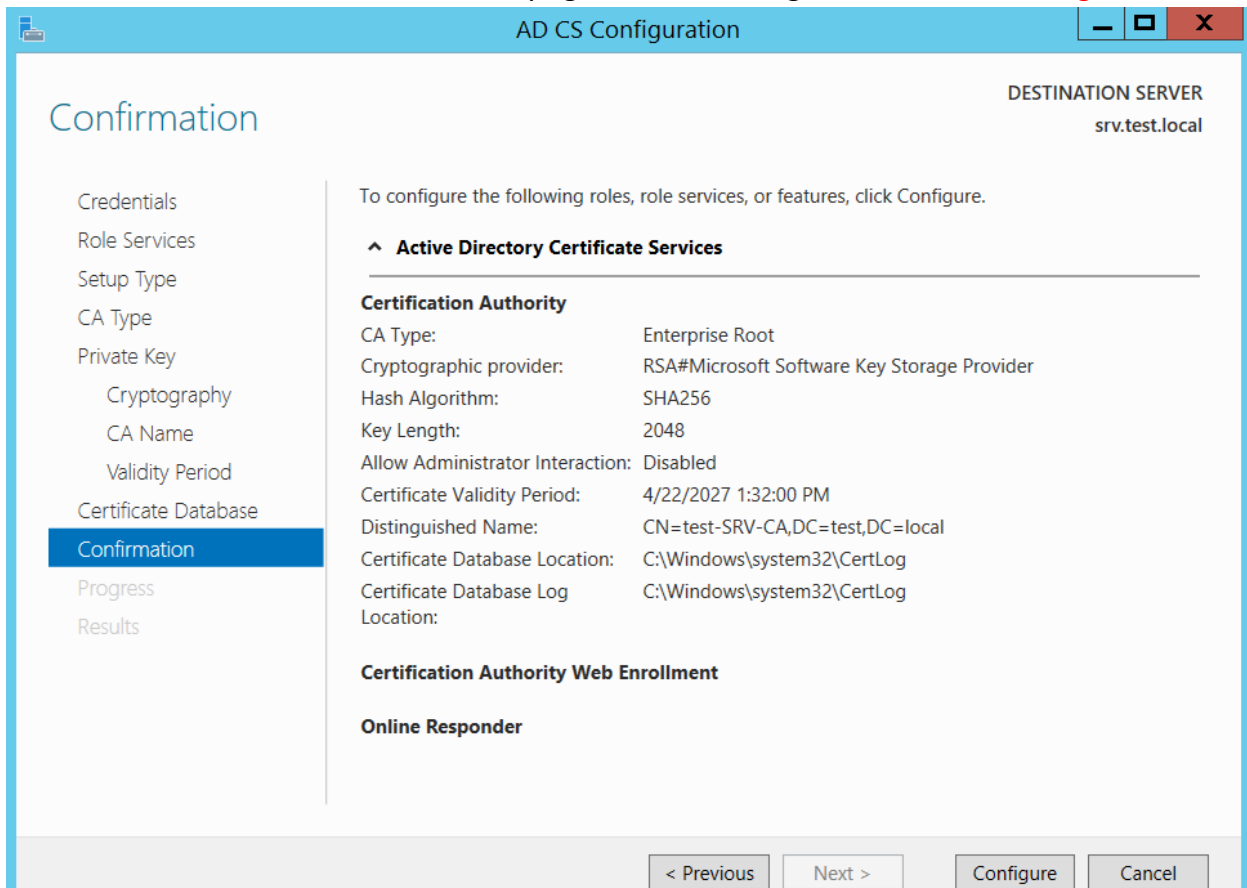
In the **Validity Period**, default should be 5 years, keep the same and then click **Next...**



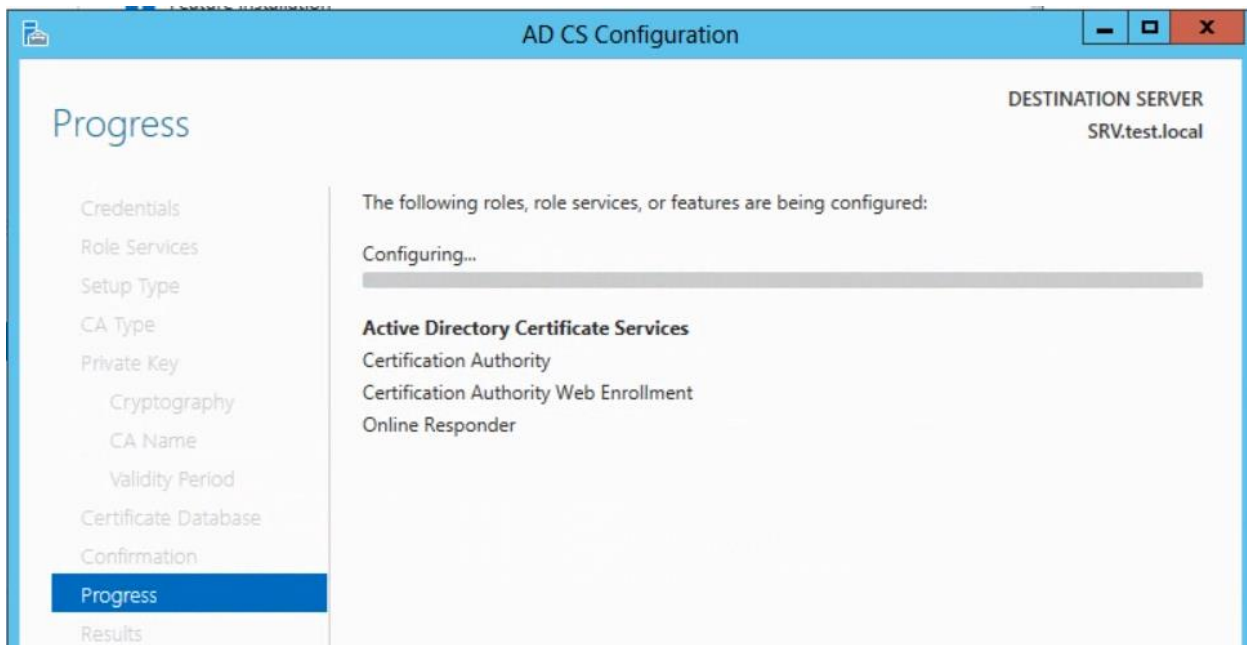
In the **CA Database** interface, just click **Next** to proceed...



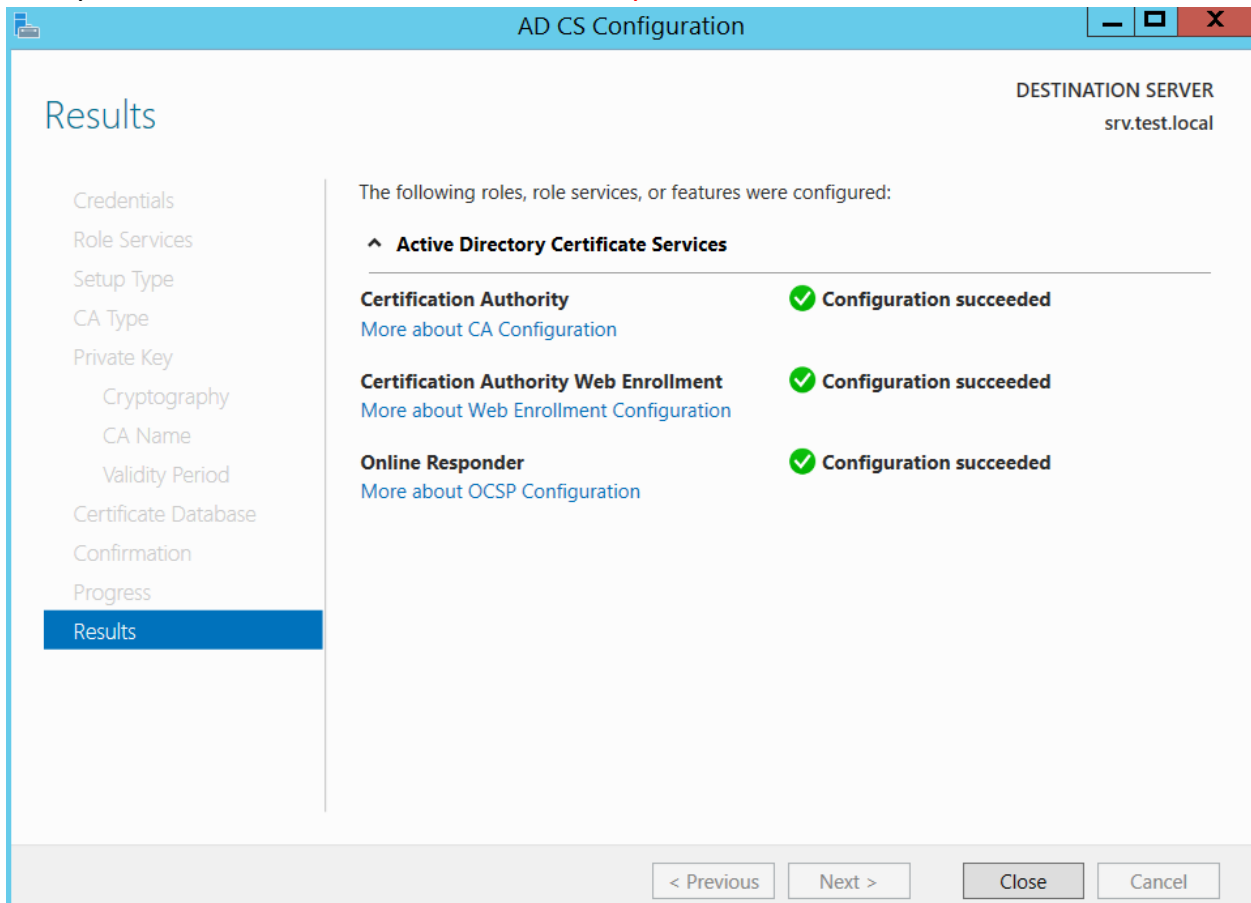
Next in the **Confirmation** interface, verify again all the settings and then click **Configure...**



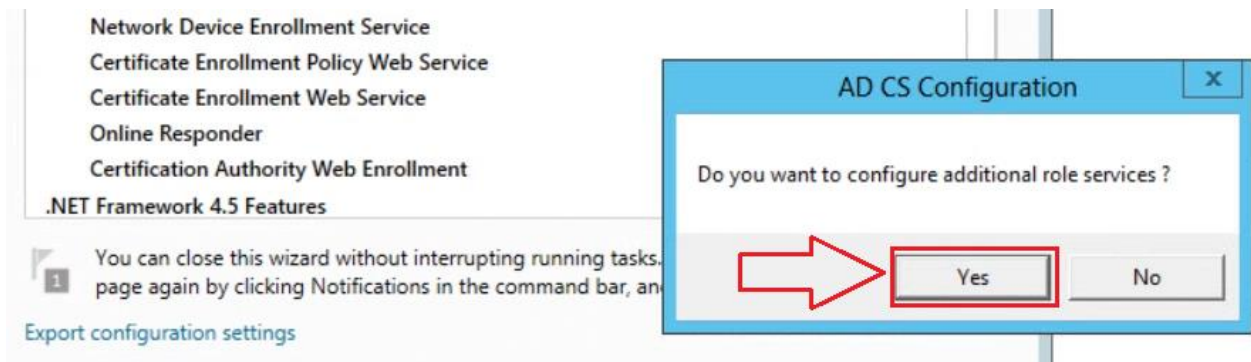
please wait few minutes for the configuration to complete...



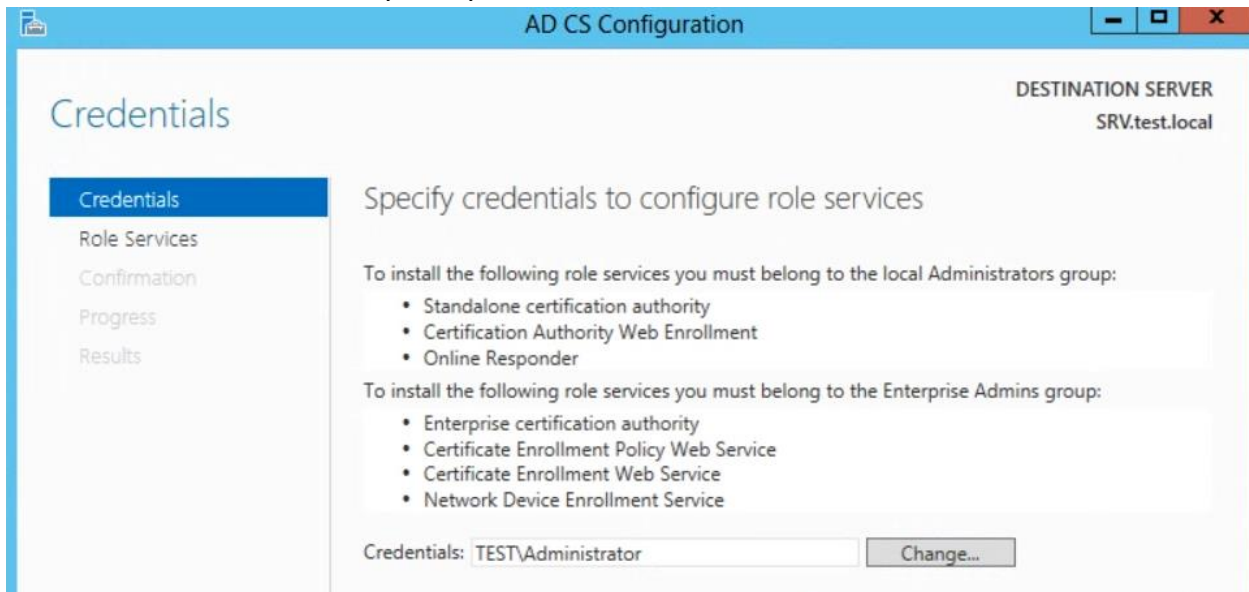
Finally, our CA & CA Web Enrollment successfully installed and click Close



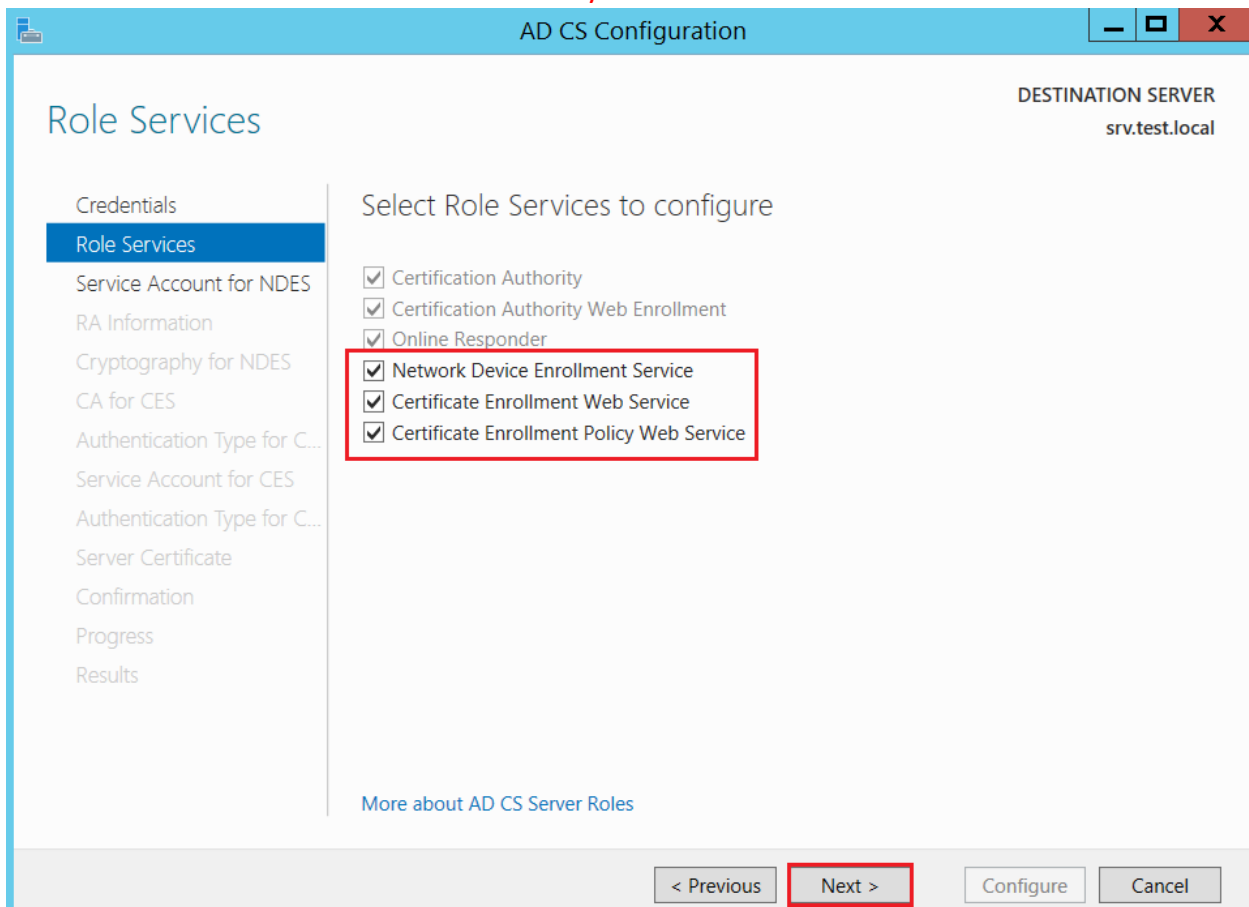
It will prompt you to Do you want to configure additional role services click Yes



In **Credentials** interface, verify that your Credentials is Administrator and then click **Next...**



In the **Role Services** interface, tick **Network Device Enrollment Service**, **Certification Enrollment Web Service** and **Certificate Enrollment Policy Web Service** and then click **Next...**



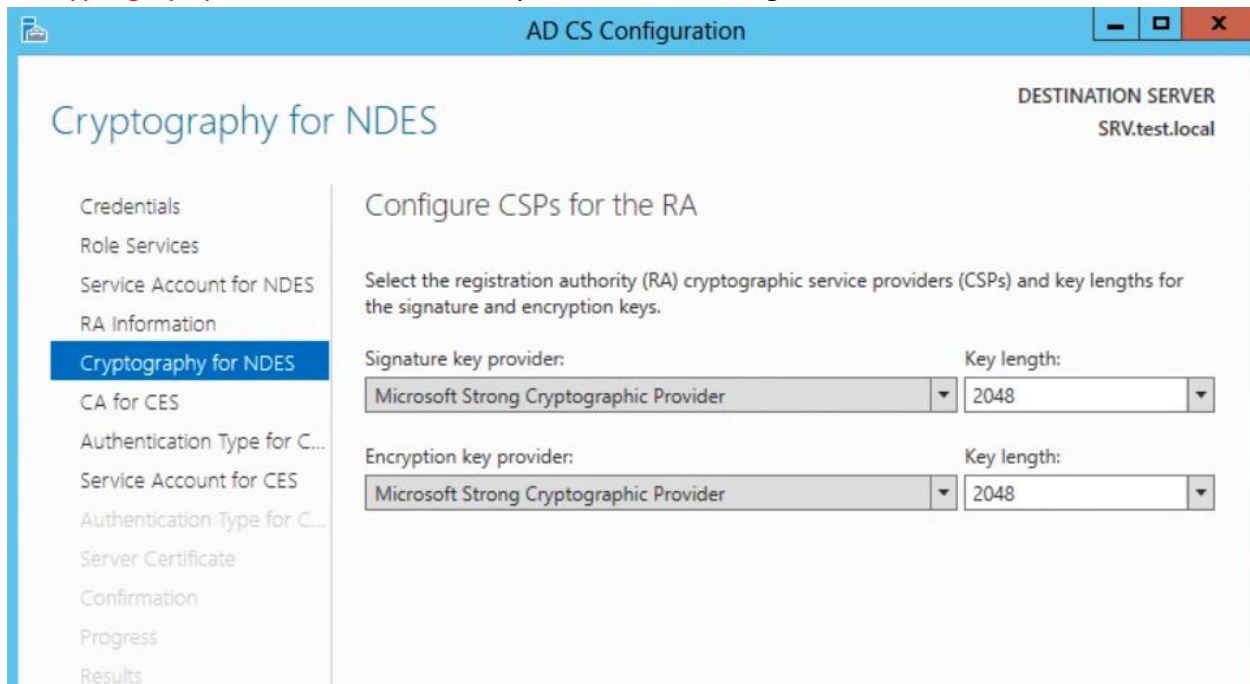
In **Service Account for NDES** interface, verify Credentials is Administrator and then click **Next...**

The screenshot shows the 'Service Account for NDES' configuration window. The title bar reads 'AD CS Configuration'. The main title is 'Service Account for NDES' and the destination server is 'SRV.test.local'. On the left, a navigation pane lists various steps, with 'Service Account for NDES' selected. The main area is titled 'Specify the service account' and contains the instruction: 'Select the identity the Network Device Enrollment Service (NDES) will use.' There are two radio button options: 'Specify service account (recommended)' (which is selected) and 'Use the built-in application pool identity'. Below the first option, a note states: 'The account must be a member of the domain and must be added to the local IIS_IUSRS group.' A text box contains 'TEST\administrator' and a 'Select...' button is to its right.

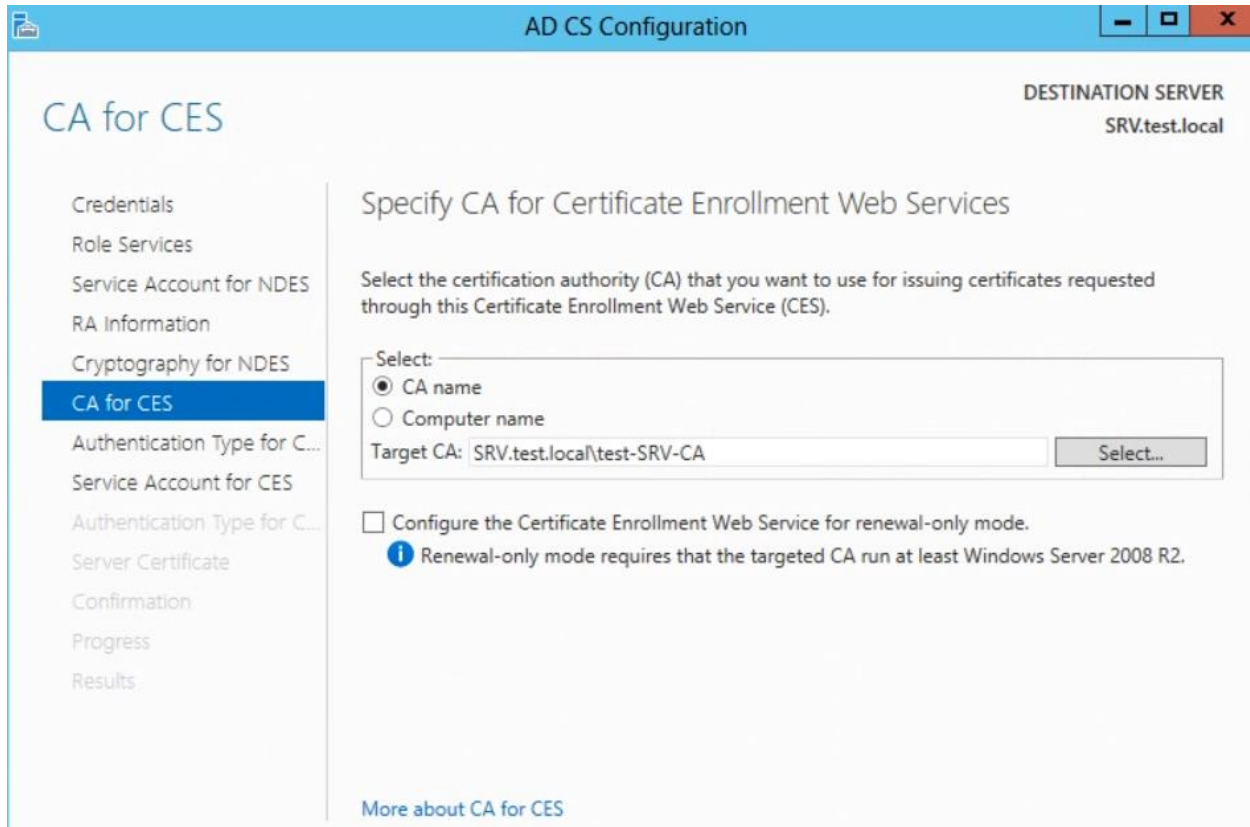
In **RA Information** interface, provide the Optional information and click **Next** to continue.

The screenshot shows the 'RA Information' configuration window. The title bar reads 'AD CS Configuration'. The main title is 'RA Information' and the destination server is 'srv.test.local'. On the left, a navigation pane lists various steps, with 'RA Information' selected. The main area is titled 'Type the requested information to enroll for an RA certificate' and contains the instruction: 'A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.' There are two sections: 'Required information' and 'Optional information'. Under 'Required information', there are two fields: 'RA Name' with the value 'SRV-MSCEP-RA' and 'Country/Region' with a dropdown menu showing 'SA (Saudi Arabia)'. Under 'Optional information', there are five fields: 'E-mail' with 'admin@test.local', 'Company' with 'Test', 'Department' with 'IT', 'City' with 'Riyadh', and 'State/Province' with 'Riyadh'.

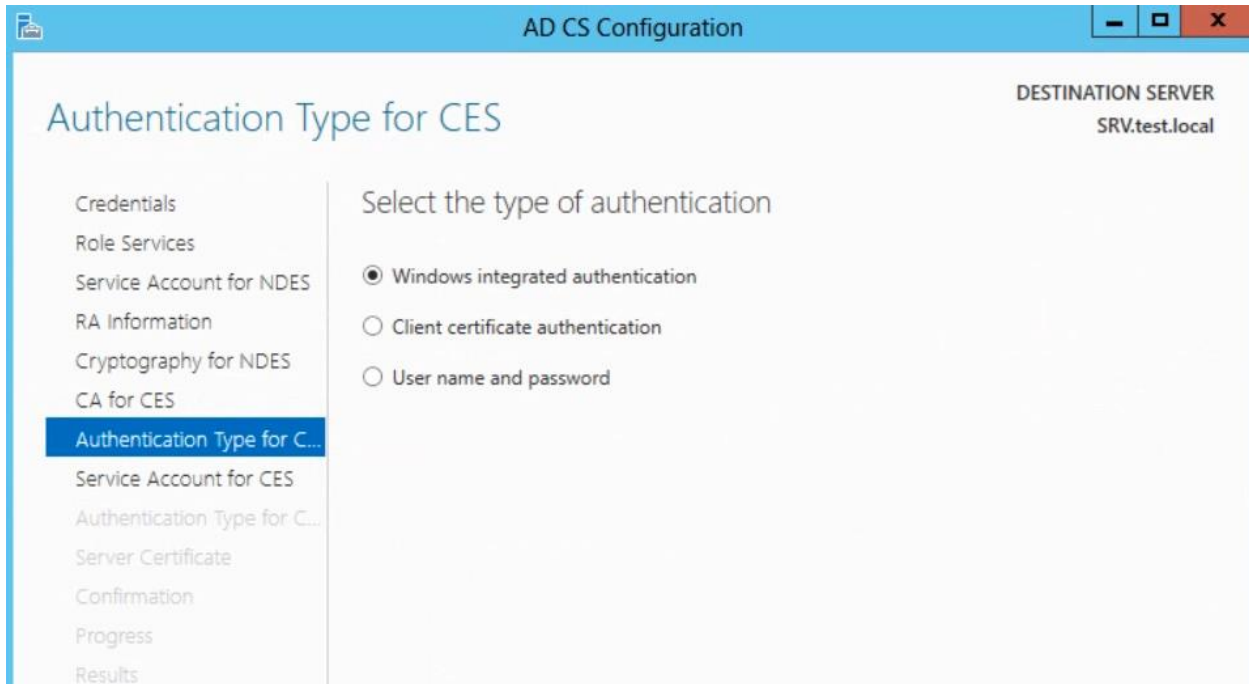
In **Cryptography for NDES** interface keep the default setting and click **Next**...



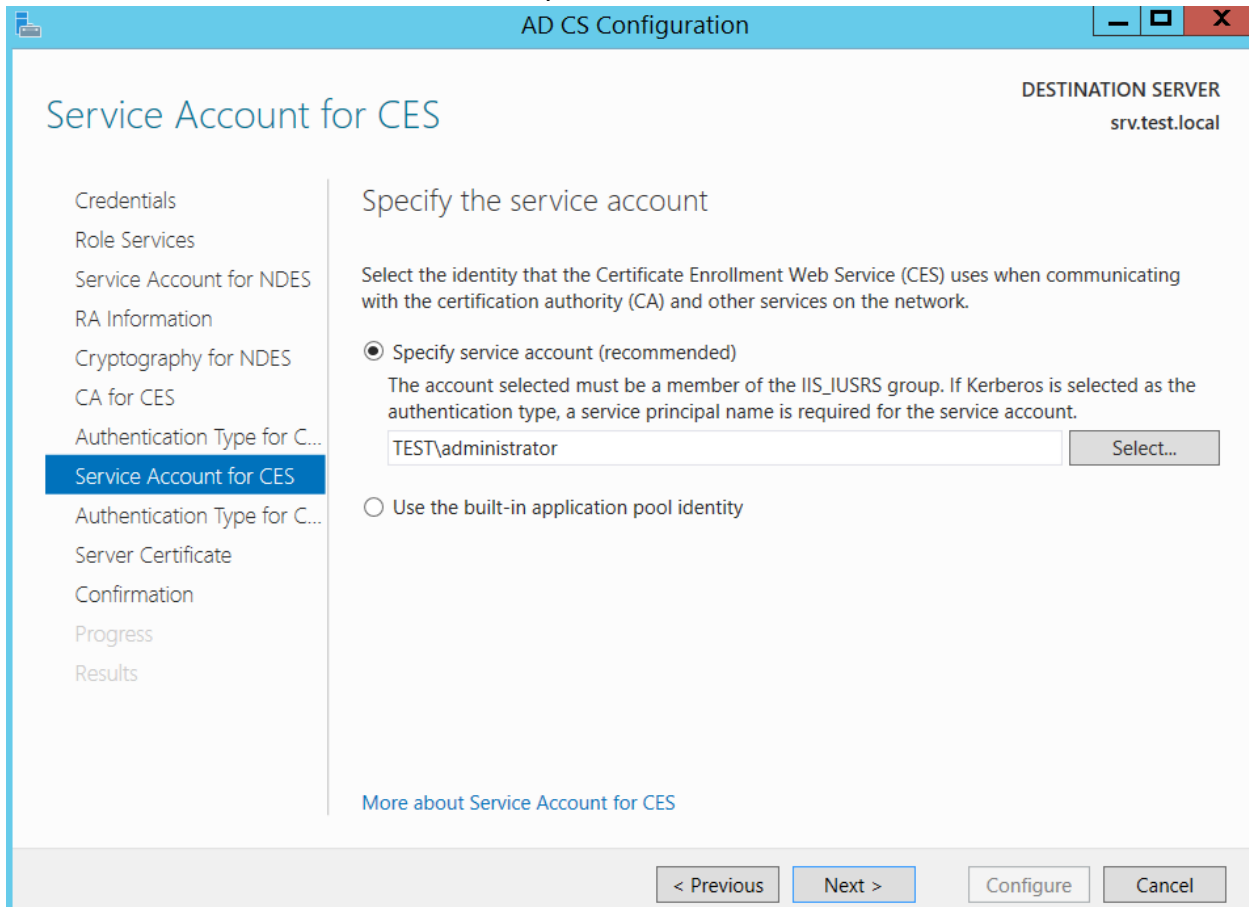
In **CA for CES** interface, keep the default setting just click **Next** to continue



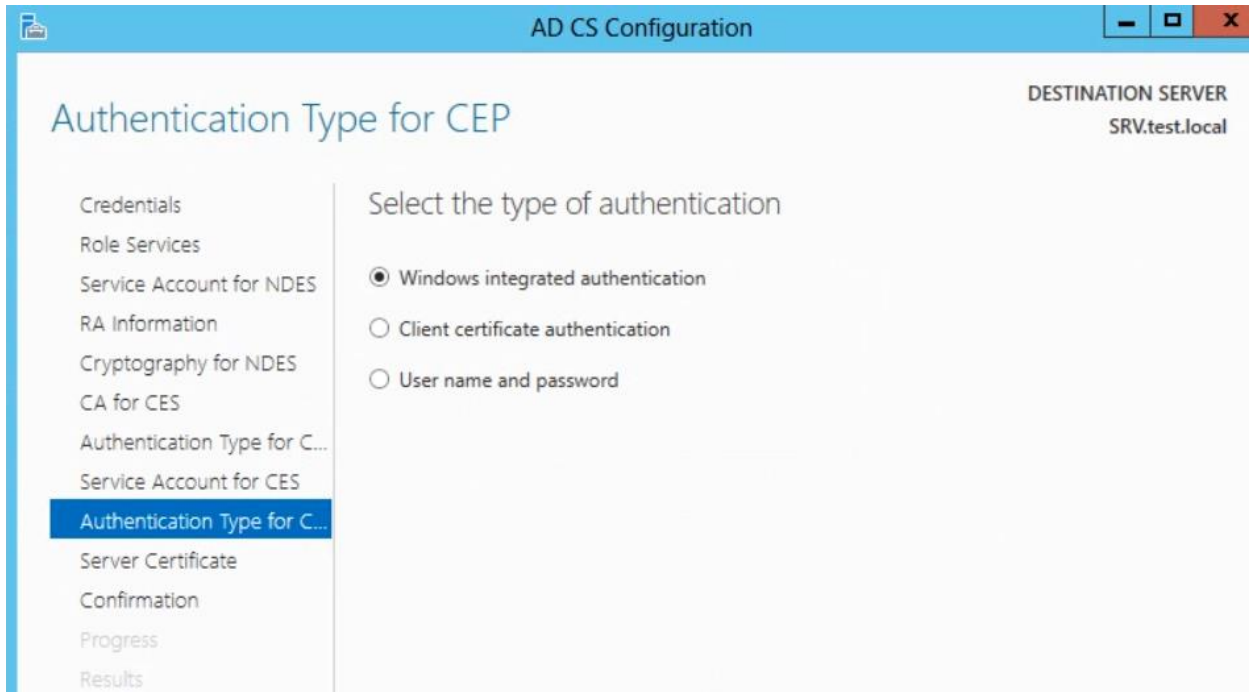
In Authentication Type for CES interface, keep the default **Windows integrated authentication**



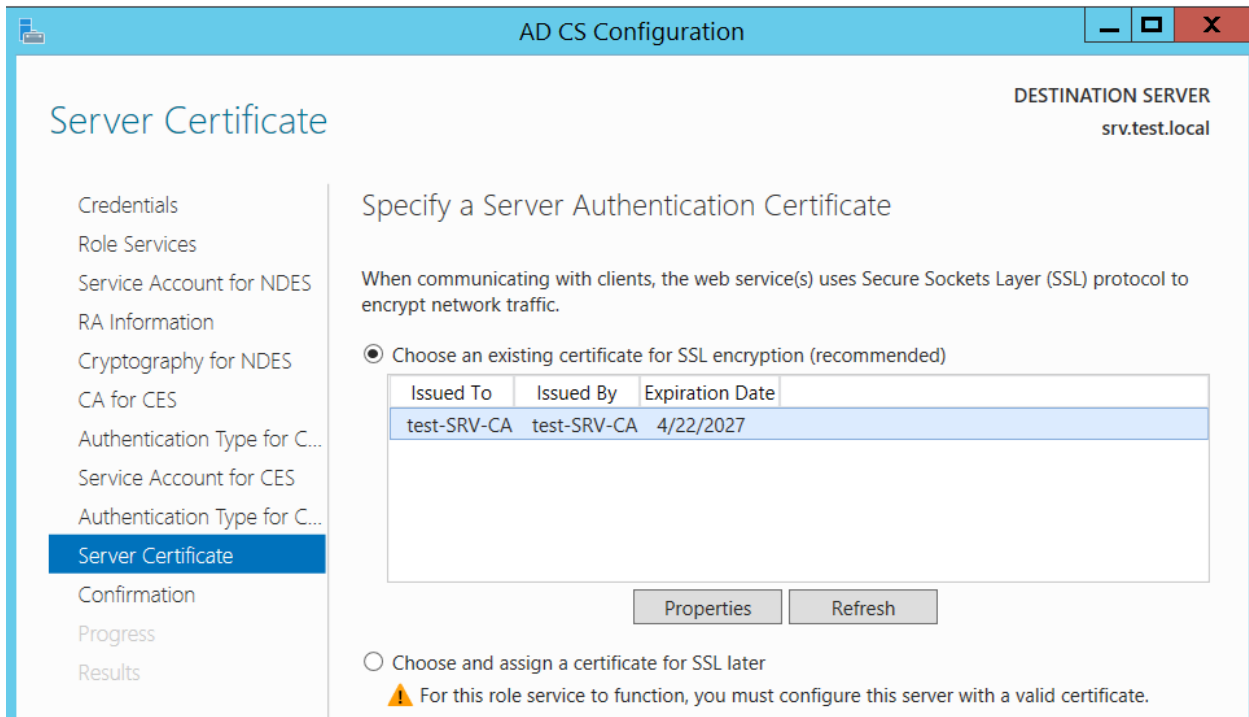
In Service Account for CES interface, verify Credentials is Administrator and then click **Next...**



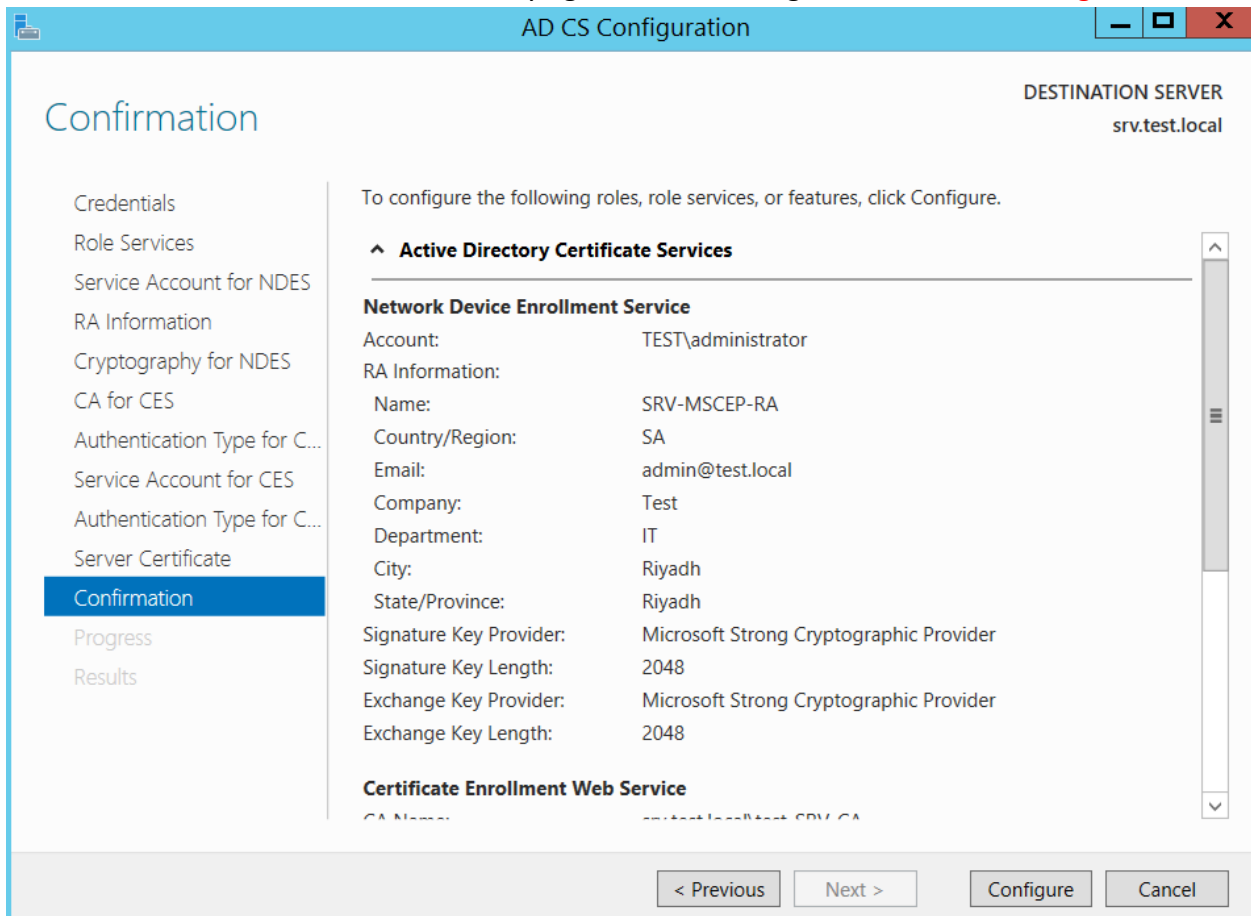
In Authentication Type for CEP interface, keep the default **Windows integrated authentication**



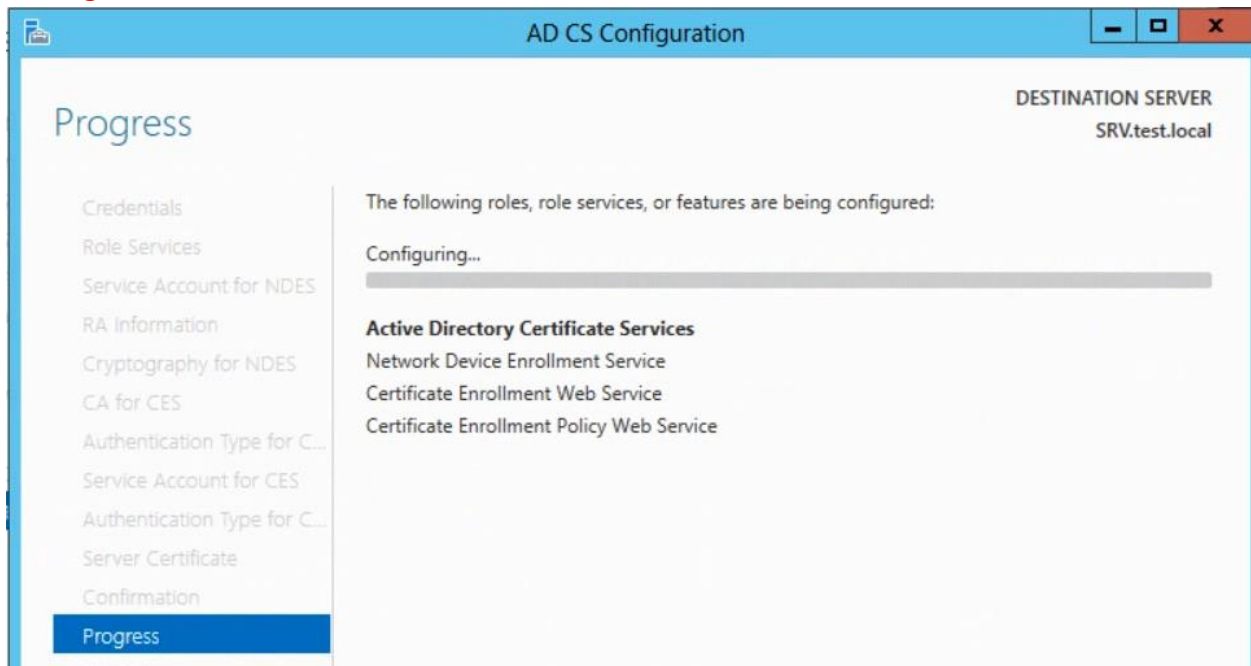
In **Server Certificate** interface, Keep the default setting and click **Next** to continue



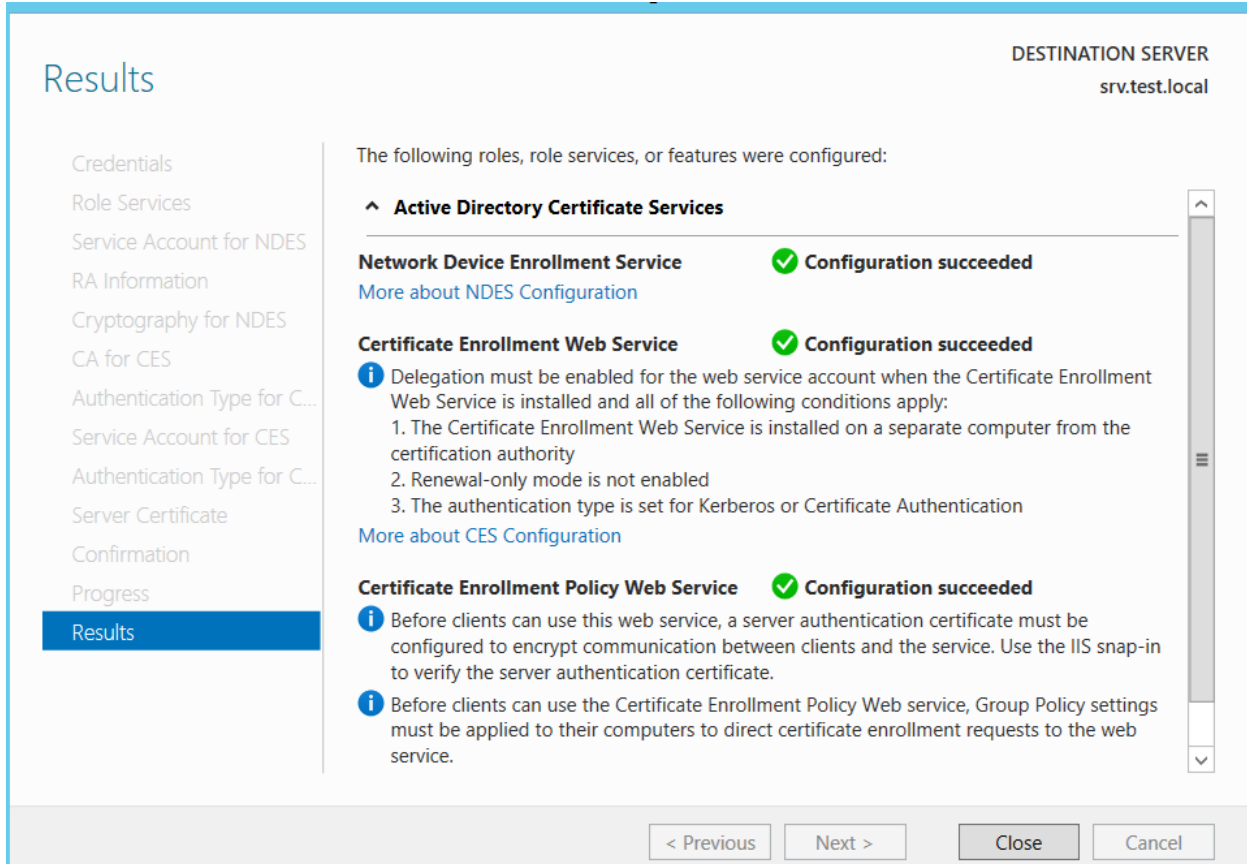
Next in the **Confirmation** interface, verify again all the settings and then click **Configure...**



In **Progress** Interface, wait for moment to install role and features



Finally, all Roles and Features are installed click **Close**



From any server in the domain, you can connect to <http://192.168.100.230/certsrv>. This will launch the Certificate Authority Web Enrollment portal.

