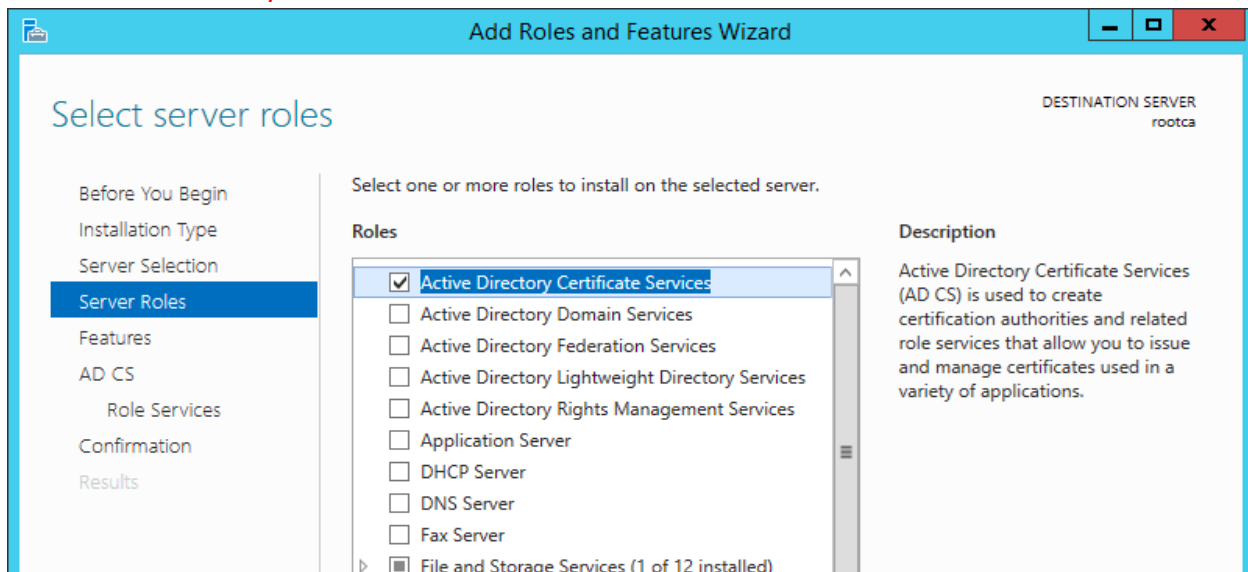
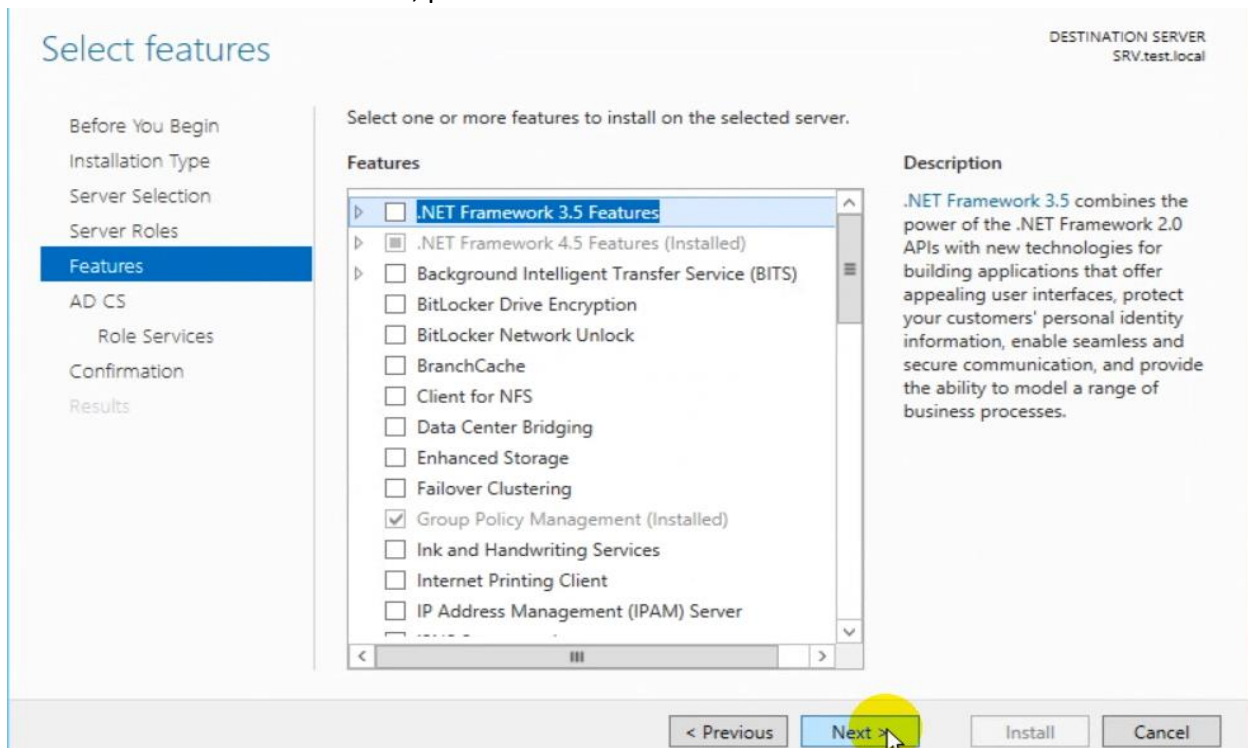


## CA Server in Windows 2012:

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



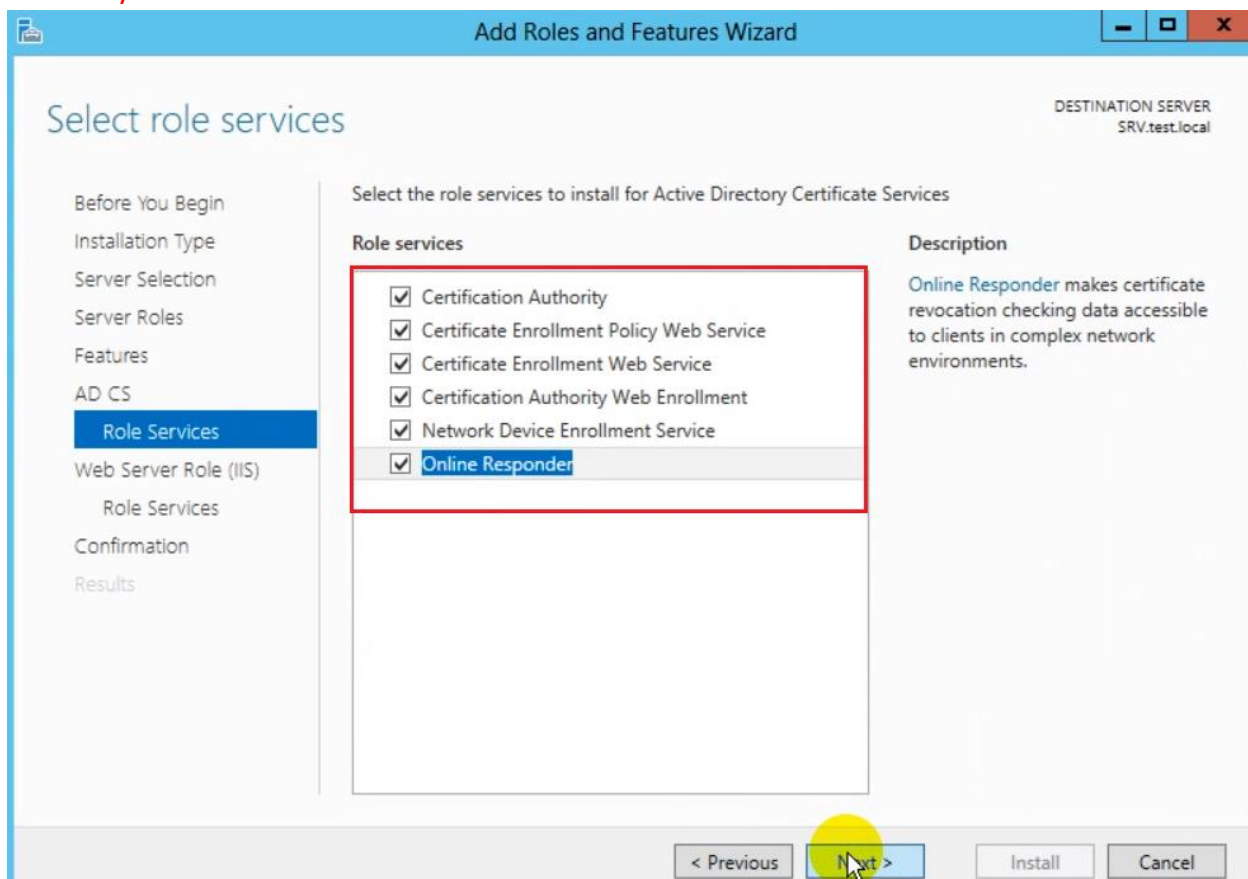
In the **Select Features** interface, proceed with **Next...**



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



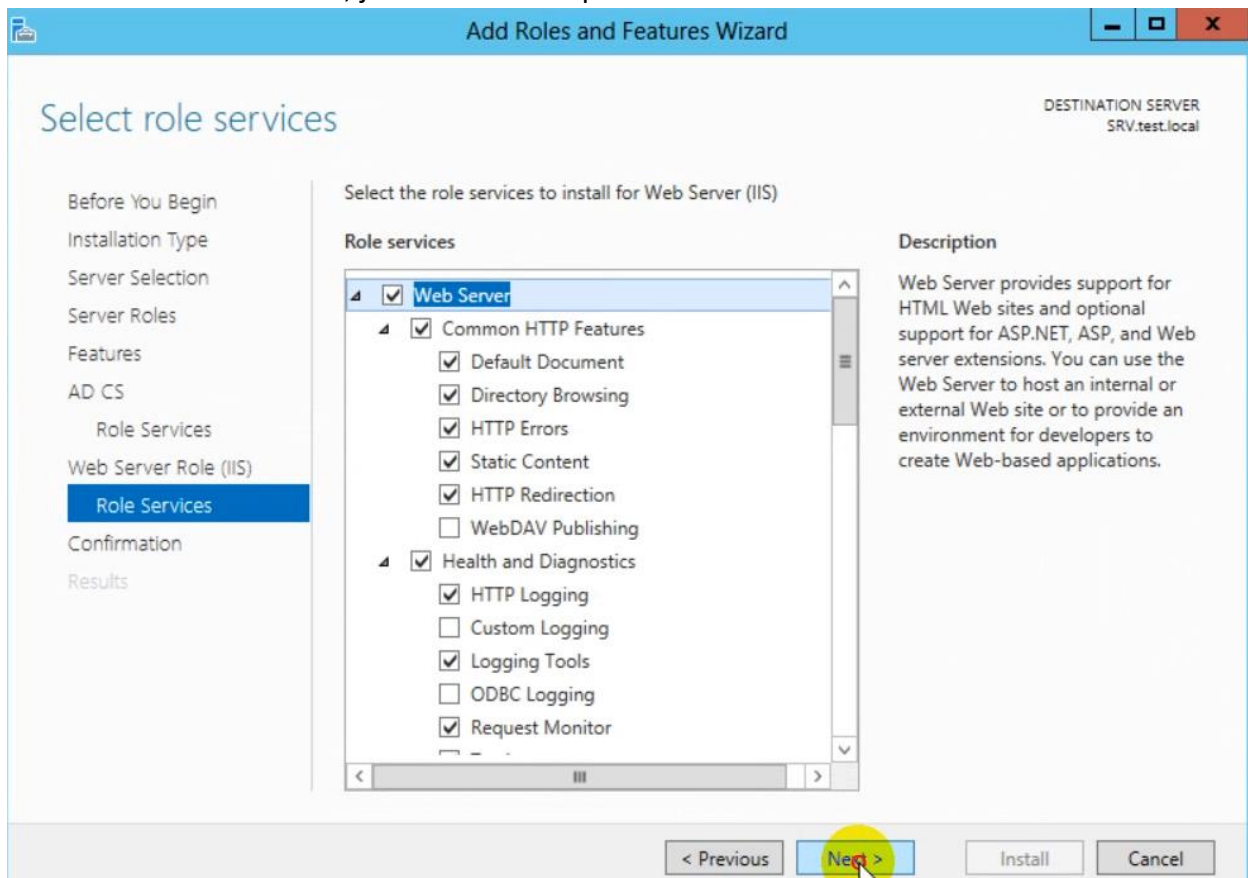
In **Select role services**, make sure you tick all specially, **Certificate Authority** and **Certification Authority Web Enrollment** check box and then click **Next...**



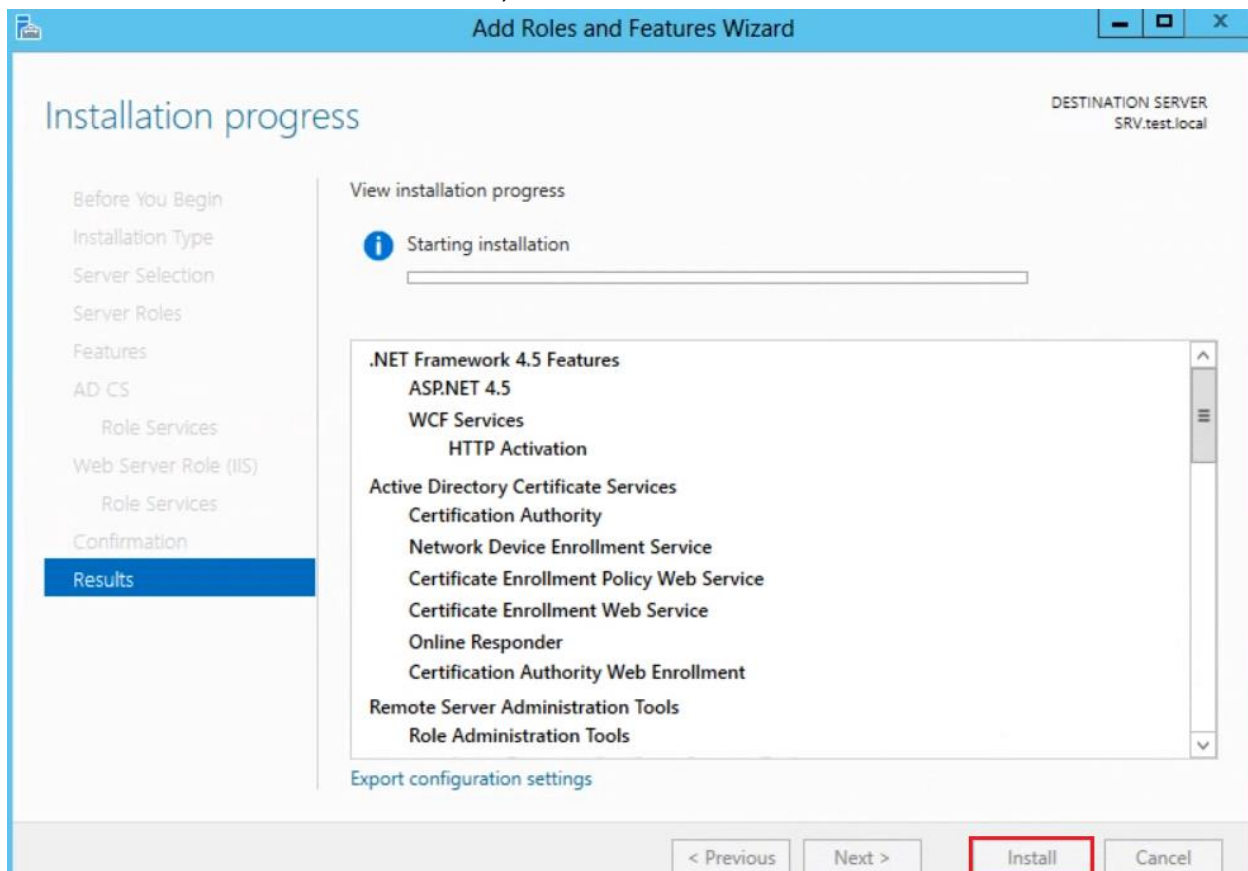
In the **Web Server Role (IIS)** interface, click **Next** to proceed...



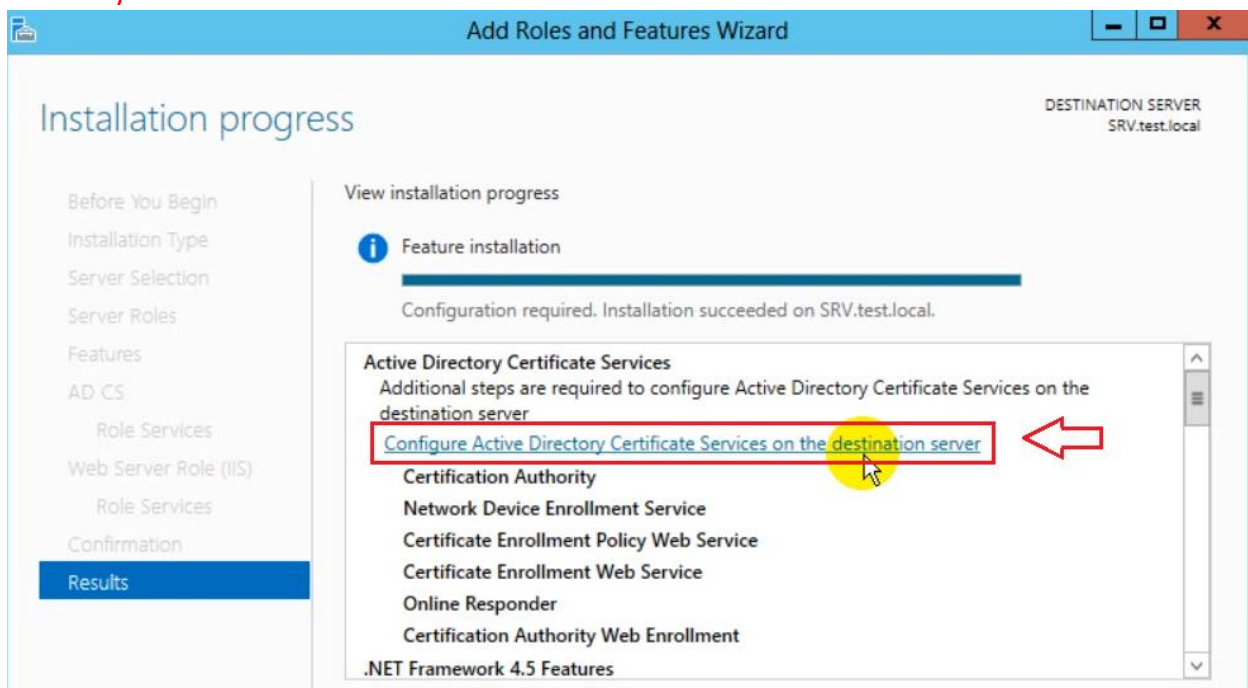
in the **Select Role Services**, just click **Next** to proceed...



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

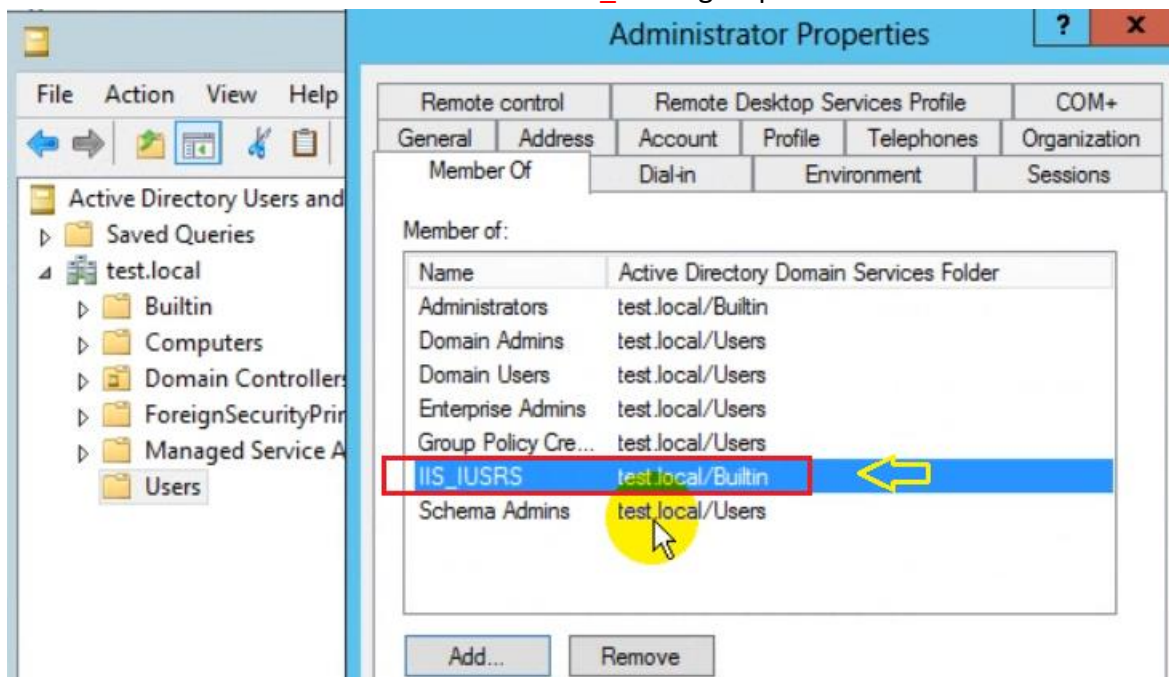


After installation complete, in the Installation progress interface, click **Configure Active Directory Certificate Services on the destination server...**

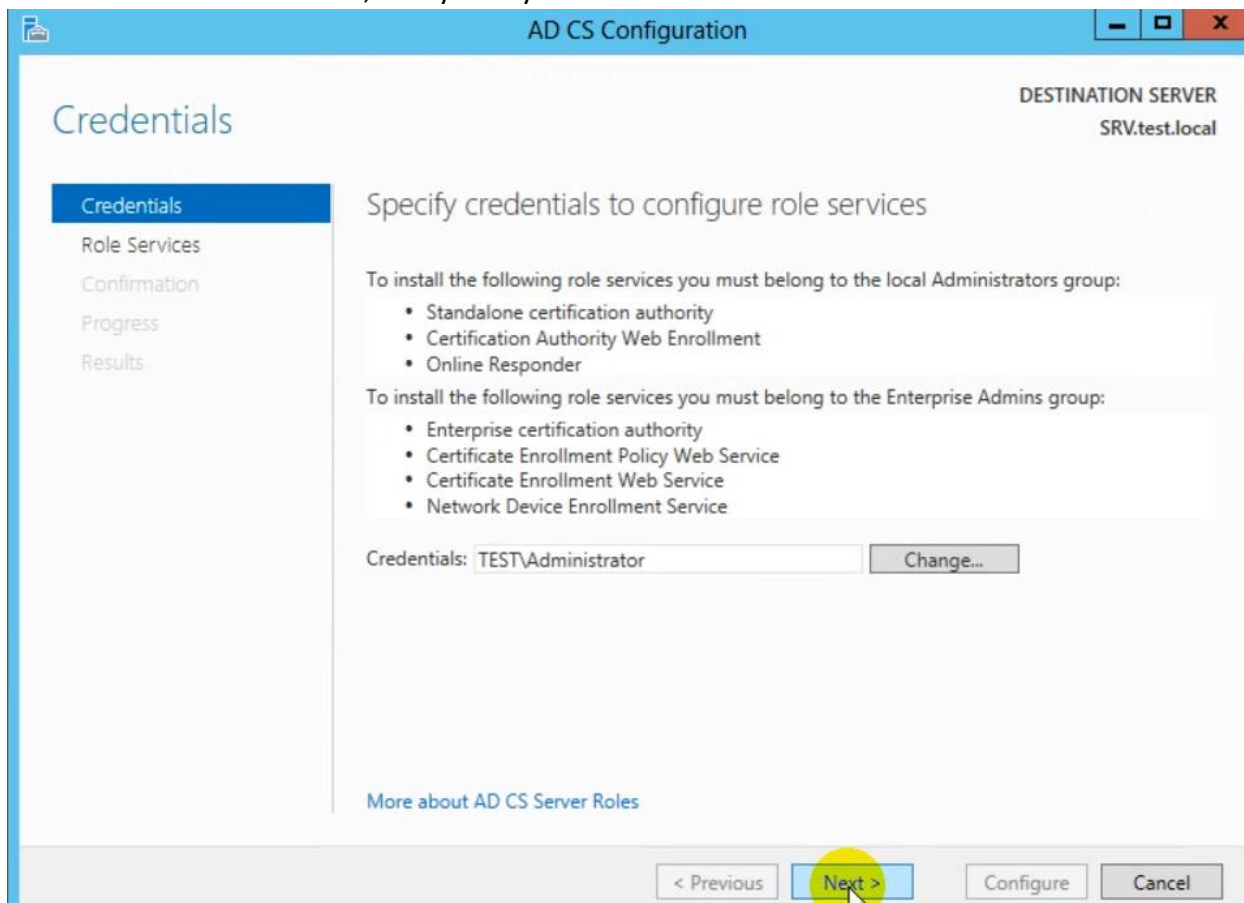




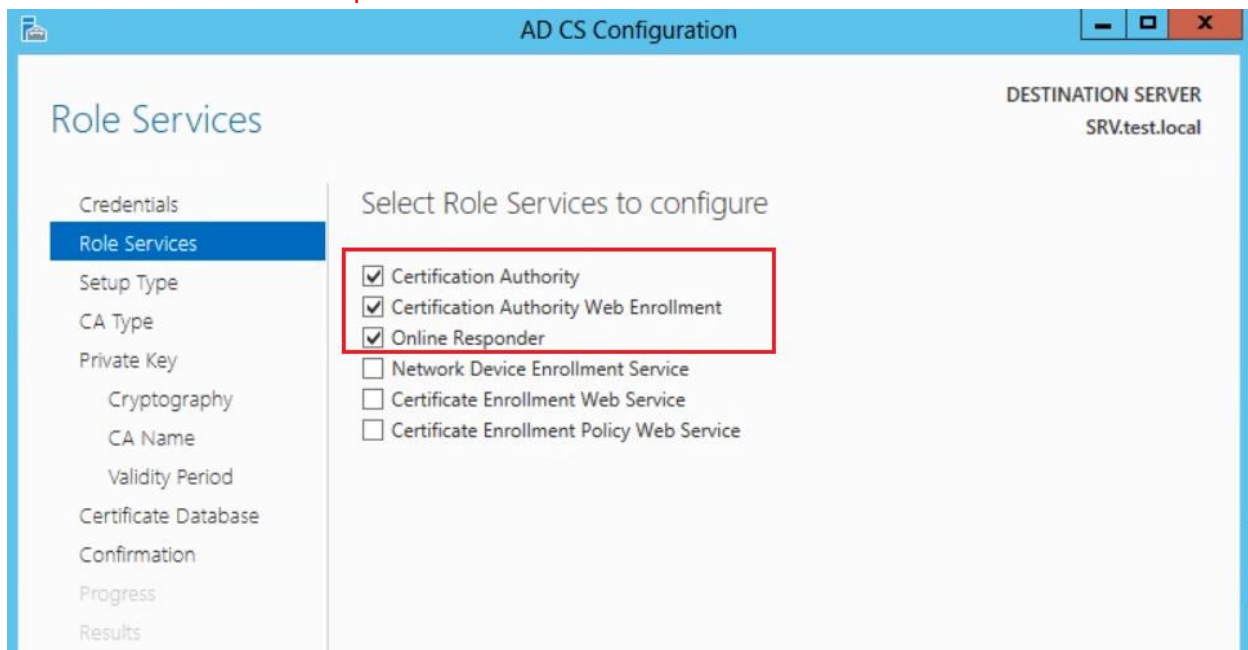
Make sure **Administrator** is the member of **IIS\_IUSRS** group if not add them.



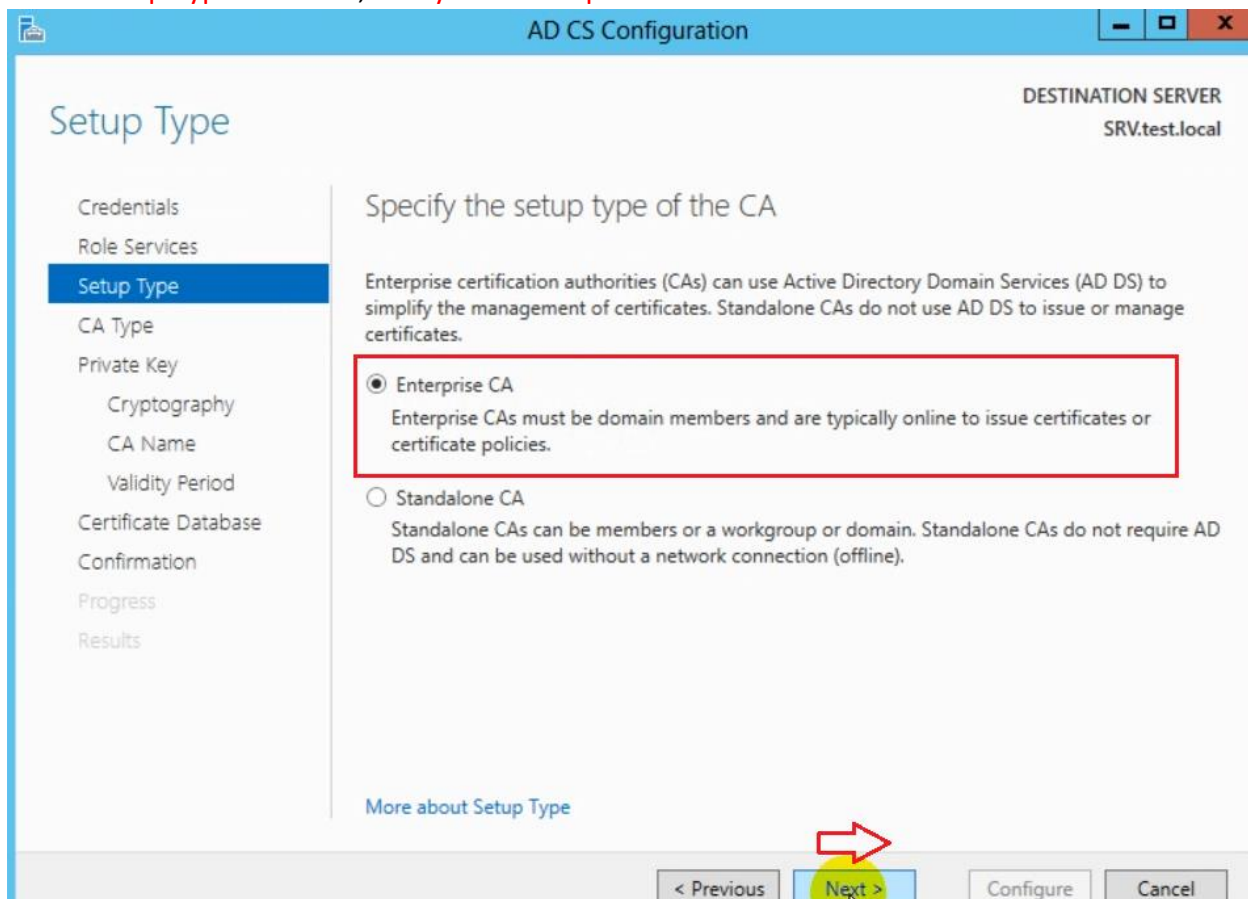
In the **Credentials** interface, verify that your Credentials is **Administrator** and then click **Next...**



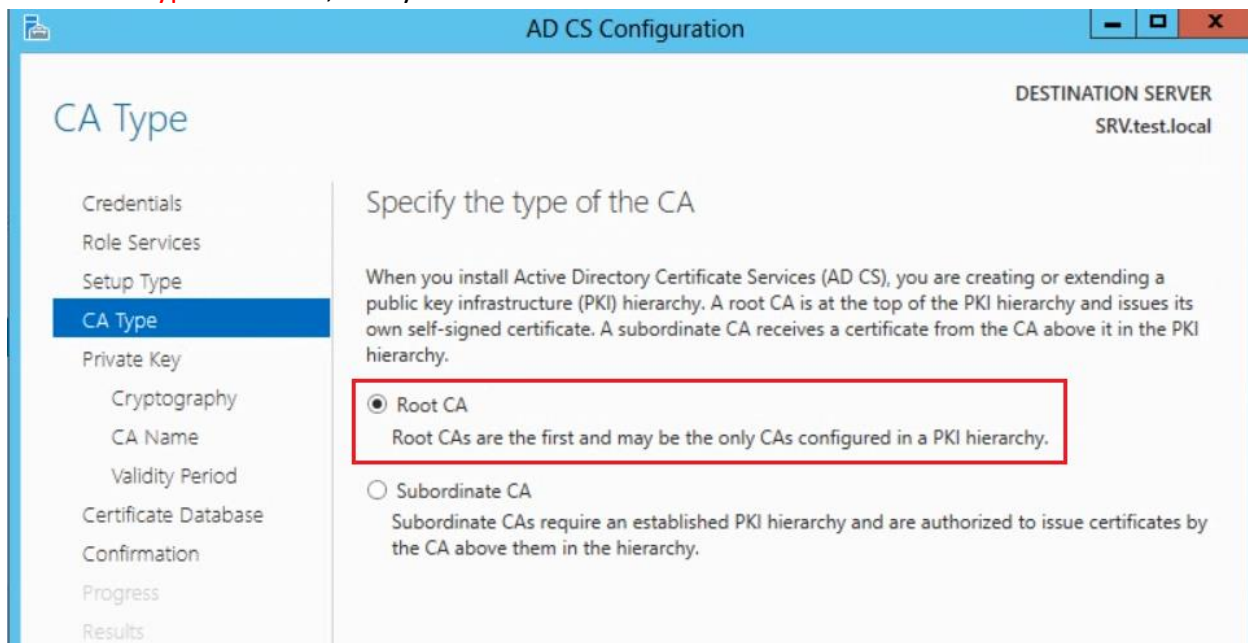
In the **Role Services** interface, tick **Certification Authority**, **Certification Authority Web Enrollment** and **Online Responder** and then click **Next...**



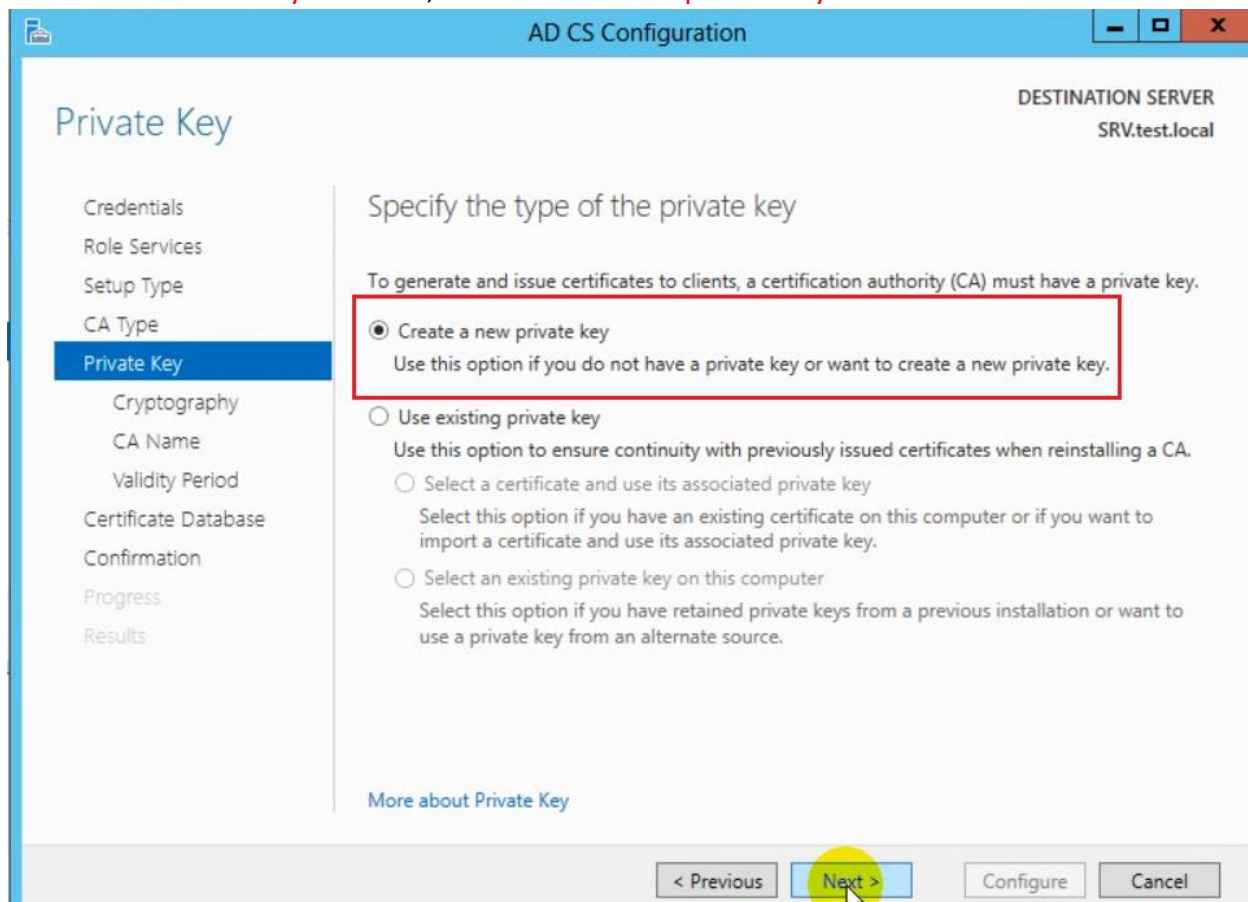
In the **Setup Type** interface, verify that **Enterprise CA** is selected and click **Next...**



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...**

The screenshot shows the 'Cryptography for CA' window in the AD CS Configuration console. The left-hand navigation pane has 'Cryptography' selected. The main area is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' set to 'RSA#Microsoft Software Key Storage Provider' and 'Key length:' set to '2048'. Below these, 'Select the hash algorithm for signing certificates issued by this CA:' is set to 'SHA256', which is highlighted with a red box. A list of other hash algorithms (SHA384, SHA512, SHA1, MD5) is visible below. At the bottom, there is an unchecked checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' The top right corner shows 'DESTINATION SERVER SRV.test.local'.

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

The screenshot shows the 'CA Name' window in the AD CS Configuration console. The left-hand navigation pane has 'CA Name' selected. The main area is titled 'Specify the name of the CA'. It contains a text box for 'Common name for this CA:' with the value 'test-SRV-CA'. Below it, 'Distinguished name suffix:' is set to 'DC=test,DC=local'. At the bottom, 'Preview of distinguished name:' shows 'CN=test-SRV-CA,DC=test,DC=local'. A red box highlights the 'Common name' and 'Distinguished name' fields. The top right corner shows 'DESTINATION SERVER SRV.test.local'. At the bottom, there are buttons for 'Previous', 'Next...', 'Configure', and 'Cancel'.



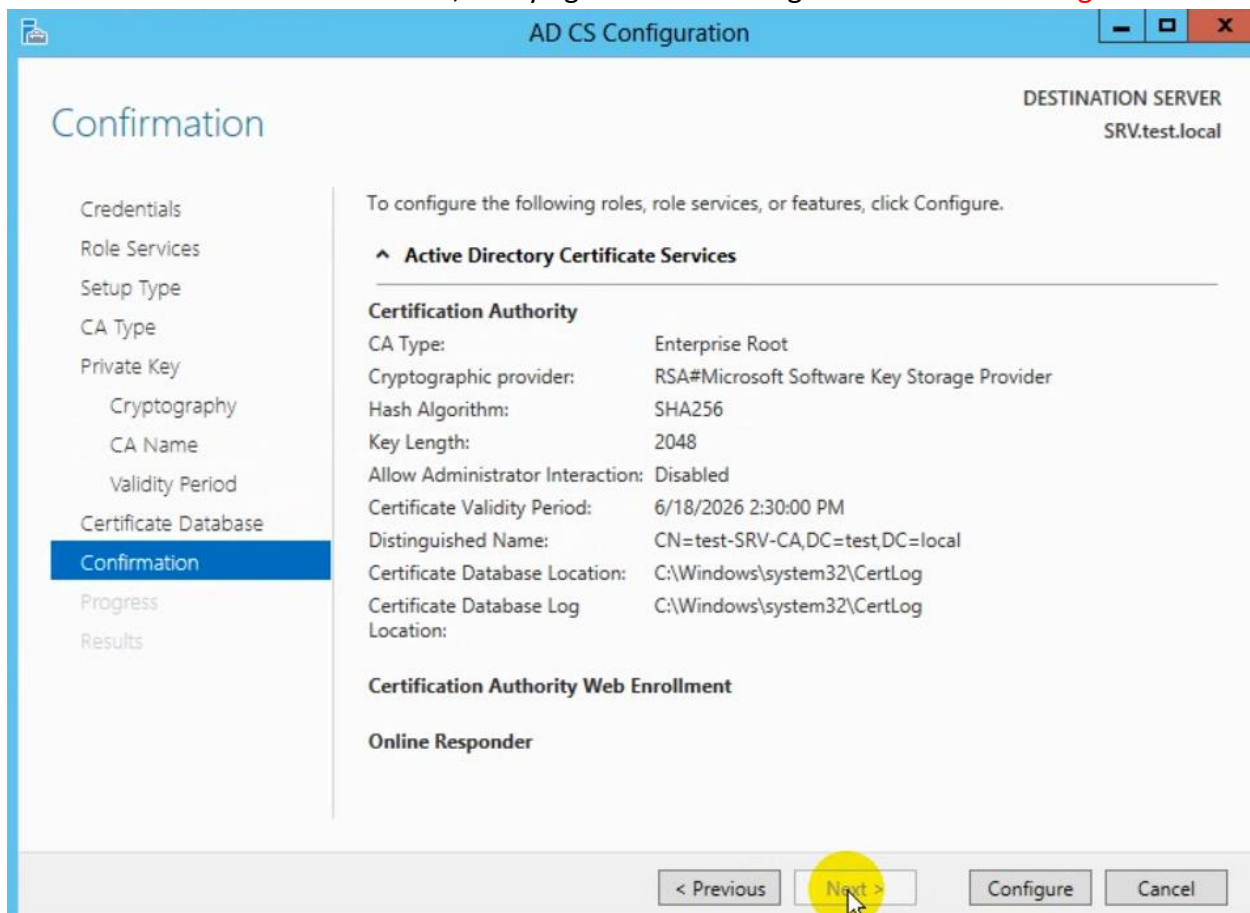
In the **Validity Period**, default should be 5 years, keep the same and then click **Next...**

The screenshot shows the 'AD CS Configuration' window with the 'Validity Period' tab selected. The left sidebar lists various configuration steps, with 'Validity Period' highlighted. The main area is titled 'Specify the validity period'. It contains a text box with the instruction 'Select the validity period for the certificate generated for this certification authority (CA):'. Below this is a numeric input field set to '5' and a dropdown menu set to 'Years'. A red rectangle highlights this section. Below the input fields, it shows 'CA expiration Date: 6/18/2026 2:30:00 PM'. At the bottom, a note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' The top right corner shows 'DESTINATION SERVER: SRV.test.local'.

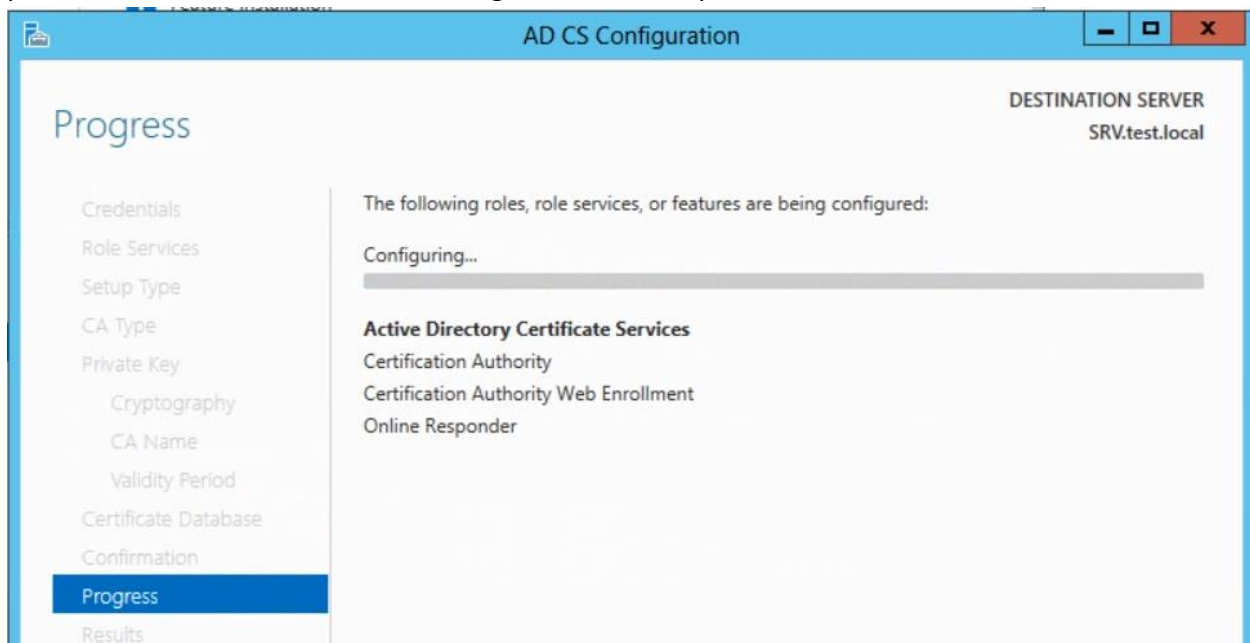
In the **CA Database** interface, just click **Next** to proceed...

The screenshot shows the 'AD CS Configuration' window with the 'CA Database' tab selected. The left sidebar lists various configuration steps, with 'CA Database' highlighted. The main area is titled 'Specify the database locations'. It contains two text input fields: 'Certificate database location:' and 'Certificate database log location:'. Both fields have the value 'C:\Windows\system32\CertLog' entered. At the bottom left, there is a link 'More about CA Database'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'Next >' button is highlighted with a yellow circle and a mouse cursor. The top right corner shows 'DESTINATION SERVER: SRV.test.local'.

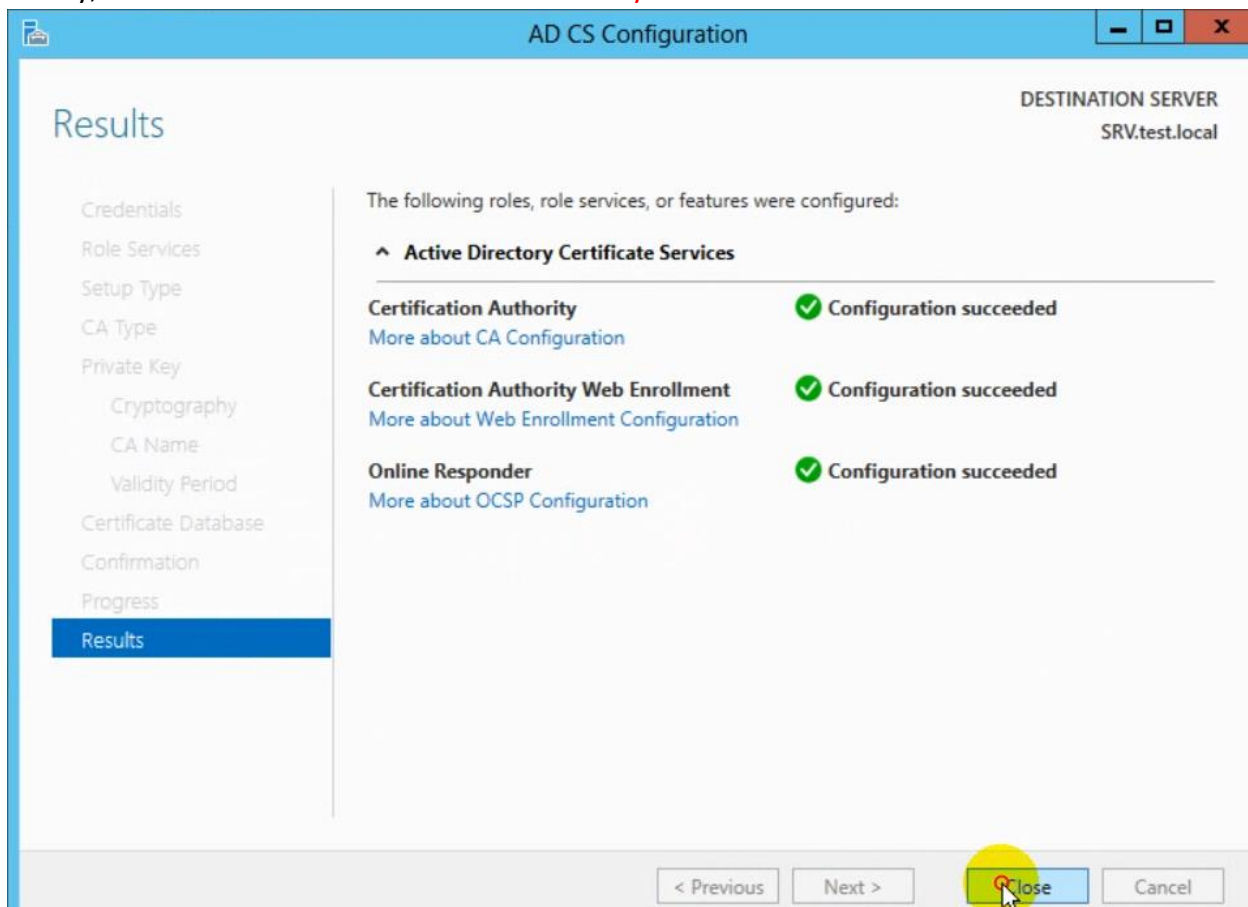
Next in the **Confirmation** interface, verify again all the settings and then click **Configure...**



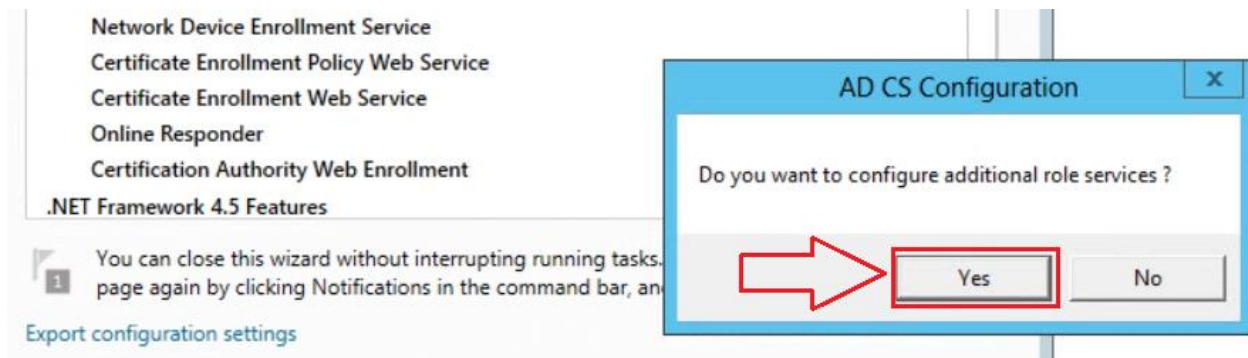
please wait few minutes for the configuration to complete...



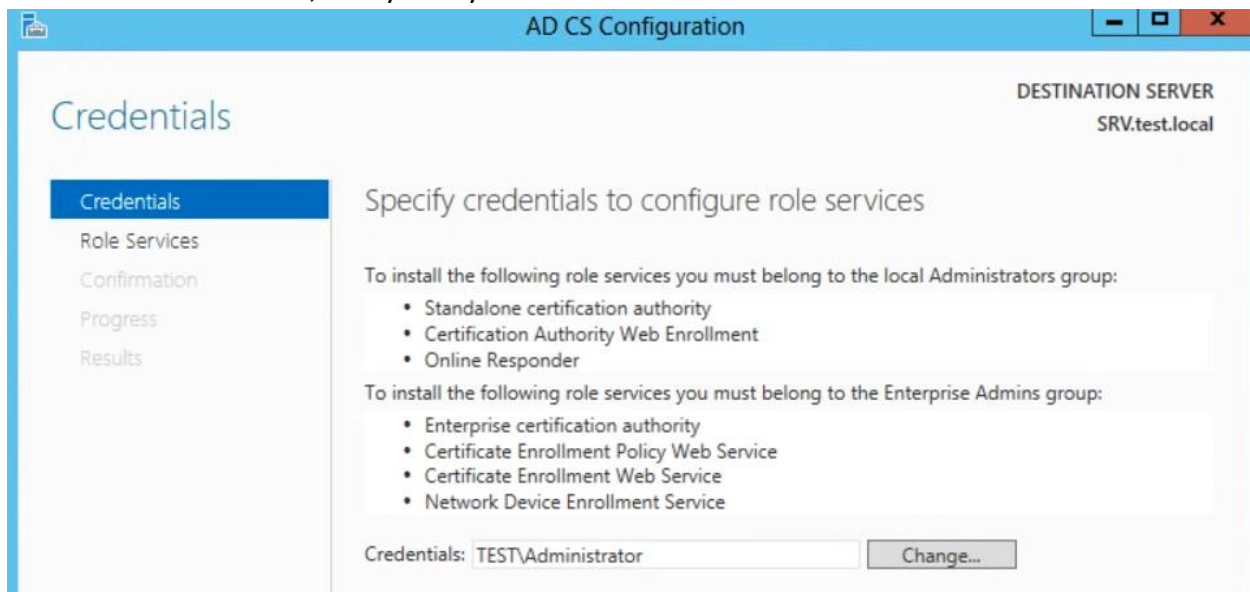
Finally, our CA & CA Web Enrollment successfully installed and click Close



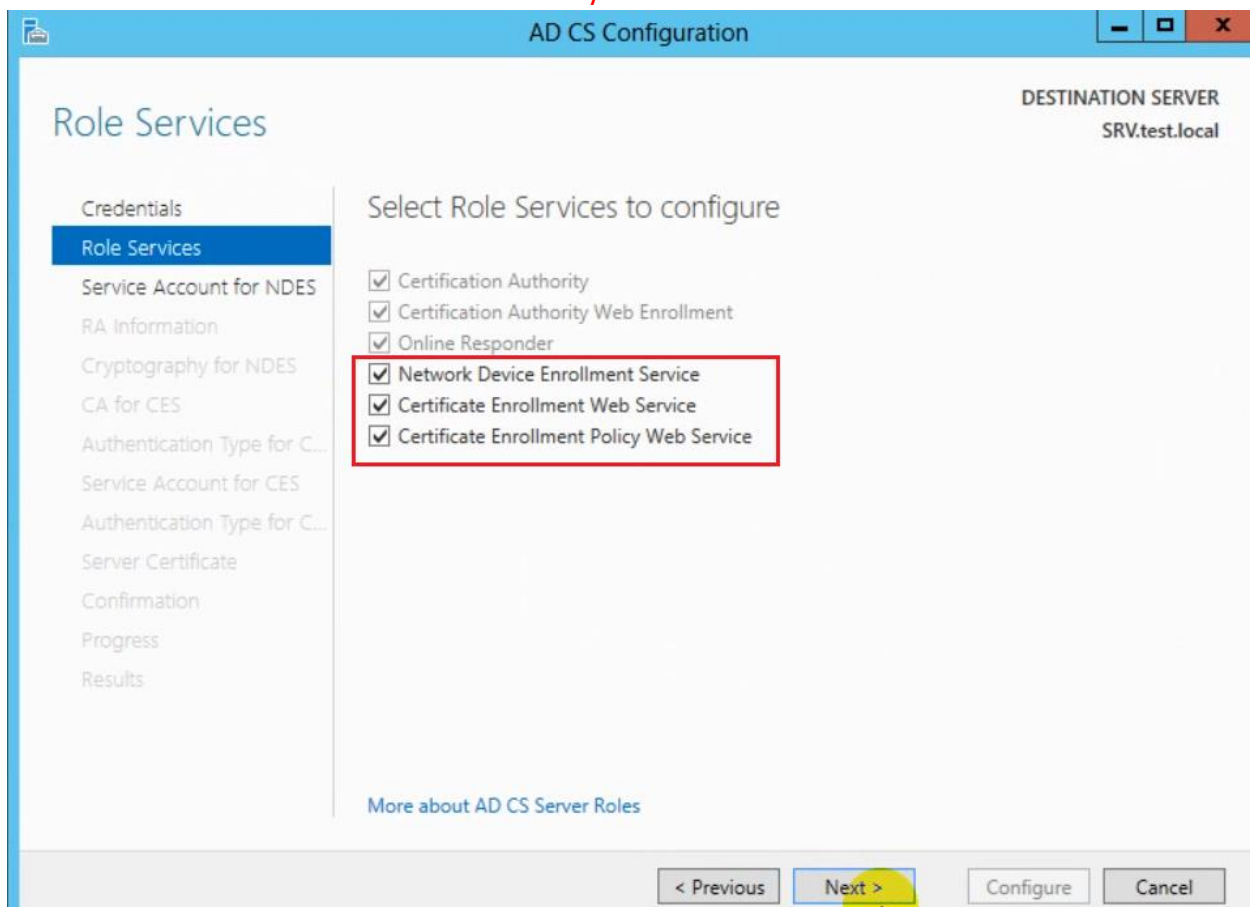
It will prompt you to Do you want to configure additional role services click Yes



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' window. The left sidebar lists steps: Credentials, Role Services, **Service Account for NDES**, RA Information, Cryptography for NDES, CA for CES, Authentication Type for C..., Service Account for CES, Authentication Type for C..., Server Certificate, Confirmation, Progress, and Results. 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 buttons: 'Specify service account (recommended)' (selected) and 'Use the built-in application pool identity'. Below the first option, it 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' window. The left sidebar lists steps: Credentials, Role Services, Service Account for NDES, **RA Information**, Cryptography for NDES, CA for CES, Authentication Type for C..., Service Account for CES, Authentication Type for C..., Server Certificate, Confirmation, Progress, and Results. 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.' It is divided into 'Required information' and 'Optional information' sections. Required information includes 'RA Name' (text box with 'SRV-MSCEP-RA') and 'Country/Region' (dropdown menu with 'US (United States)'). Optional information includes 'E-mail', 'Company', 'Department', 'City', and 'State/Province' (all text boxes). A 'More about RA Information' link is at the bottom left. The bottom navigation bar contains buttons: '< Previous', 'Next >' (highlighted with a yellow circle), 'Configure', and 'Cancel'.

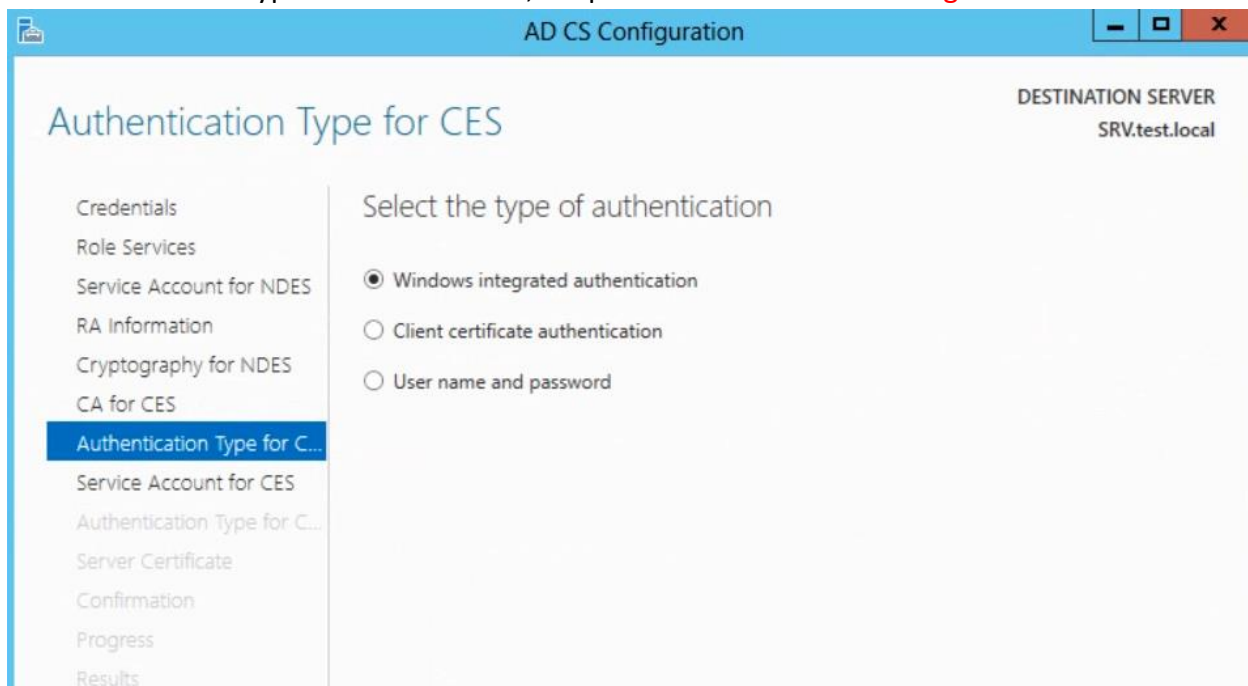
In **Cryptography for NDES** interface keep the default setting and click **Next...**

The screenshot shows the 'Cryptography for NDES' window. The left sidebar lists steps: Credentials, Role Services, Service Account for NDES, RA Information, **Cryptography for NDES**, CA for CES, Authentication Type for C..., Service Account for CES, Authentication Type for C..., Server Certificate, Confirmation, Progress, and Results. The main area is titled 'Configure CSPs for the RA'. It instructs to 'Select the registration authority (RA) cryptographic service providers (CSPs) and key lengths for the signature and encryption keys.' There are two rows of settings. The first row is for the 'Signature key provider', with a dropdown set to 'Microsoft Strong Cryptographic Provider' and a 'Key length' dropdown set to '2048'. The second row is for the 'Encryption key provider', also with a dropdown set to 'Microsoft Strong Cryptographic Provider' and a 'Key length' dropdown set to '2048'. The top right corner shows 'DESTINATION SERVER' as 'SRV.test.local'.

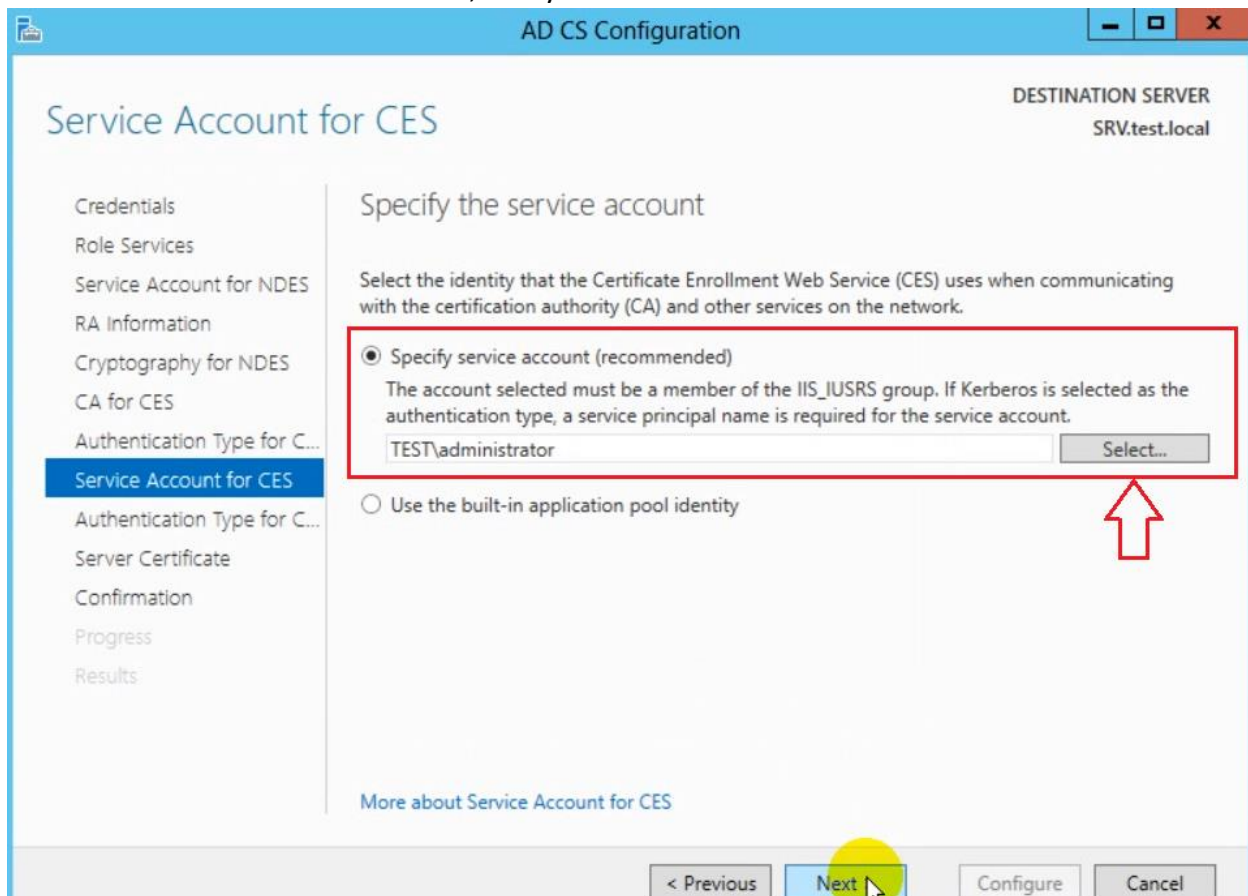
In **CA for CES** interface, keep the default setting just click **Next** to continue

The screenshot shows the 'CA for CES' window. The left sidebar is the same as the previous window, with 'CA for CES' highlighted. The main area is titled 'Specify CA for Certificate Enrollment Web Services'. It instructs to 'Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES)'. There is a 'Select:' section with two radio buttons: 'CA name' (selected) and 'Computer name'. Below this is a 'Target CA:' text box containing 'SRV.test.local/test-SRV-CA' and a 'Select...' button. Below the radio buttons is a checkbox 'Configure the Certificate Enrollment Web Service for renewal-only mode.' which is unchecked. A blue information icon is followed by the text 'Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.' At the bottom left, there is a link 'More about CA for CES'. The top right corner shows 'DESTINATION SERVER' as 'SRV.test.local'.

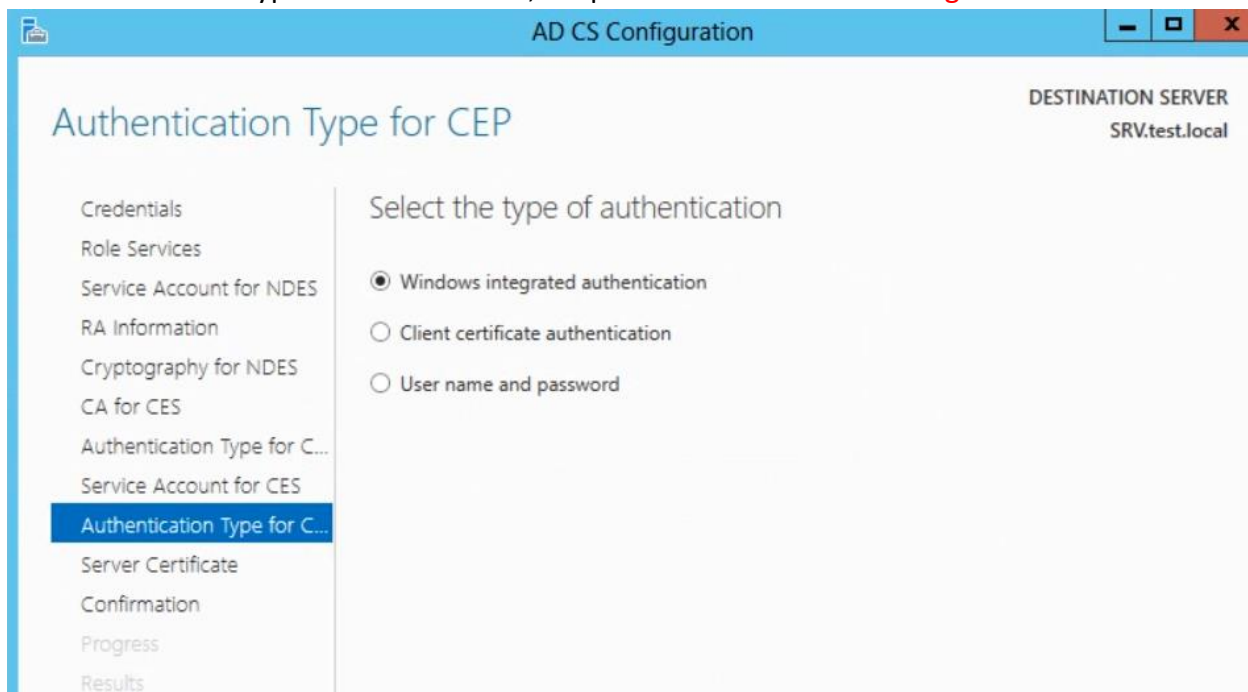
In Authentication Type for CES interface, keep the default **Windows integrated authentication**



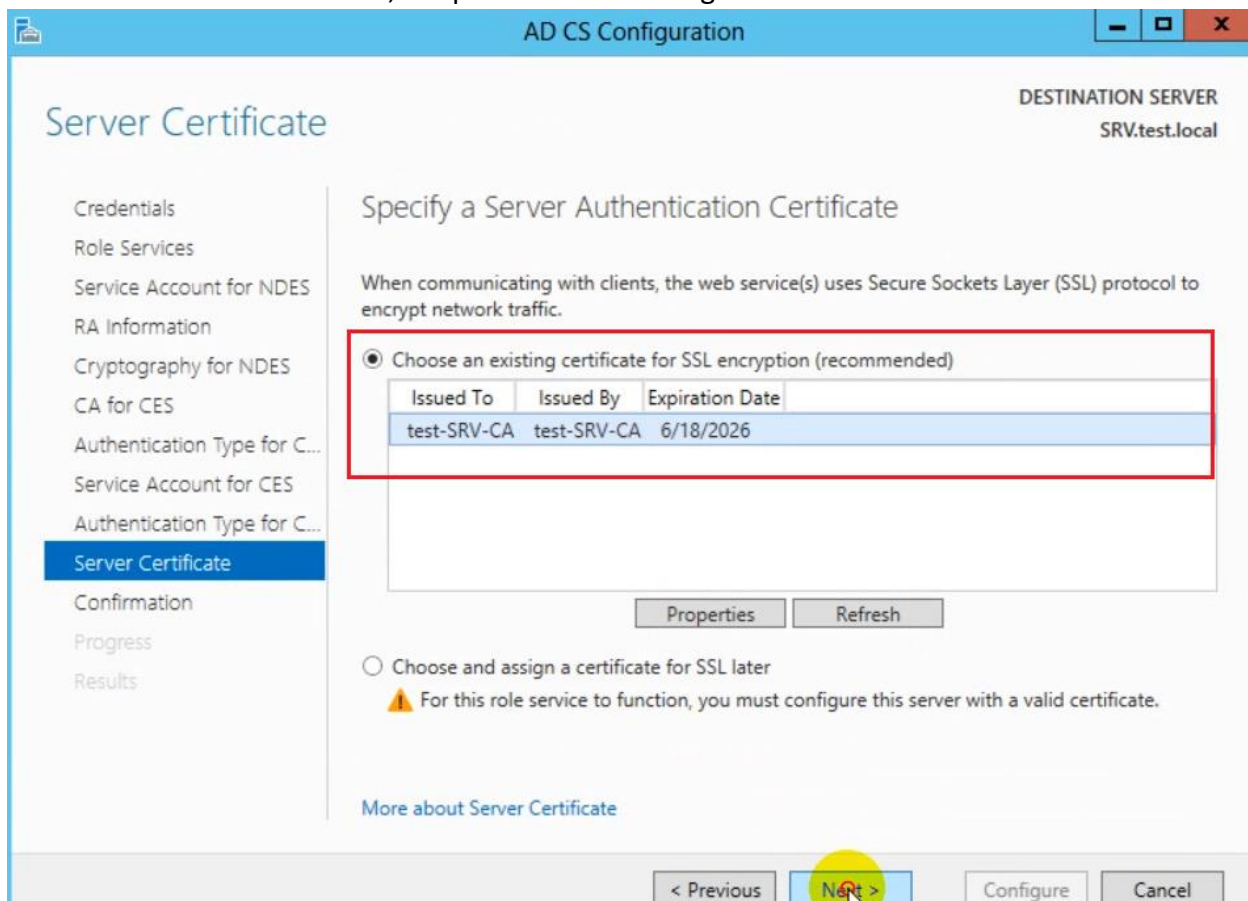
In Service Account for CES interface, verify Credentials is Administrator and then click **Next...**



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

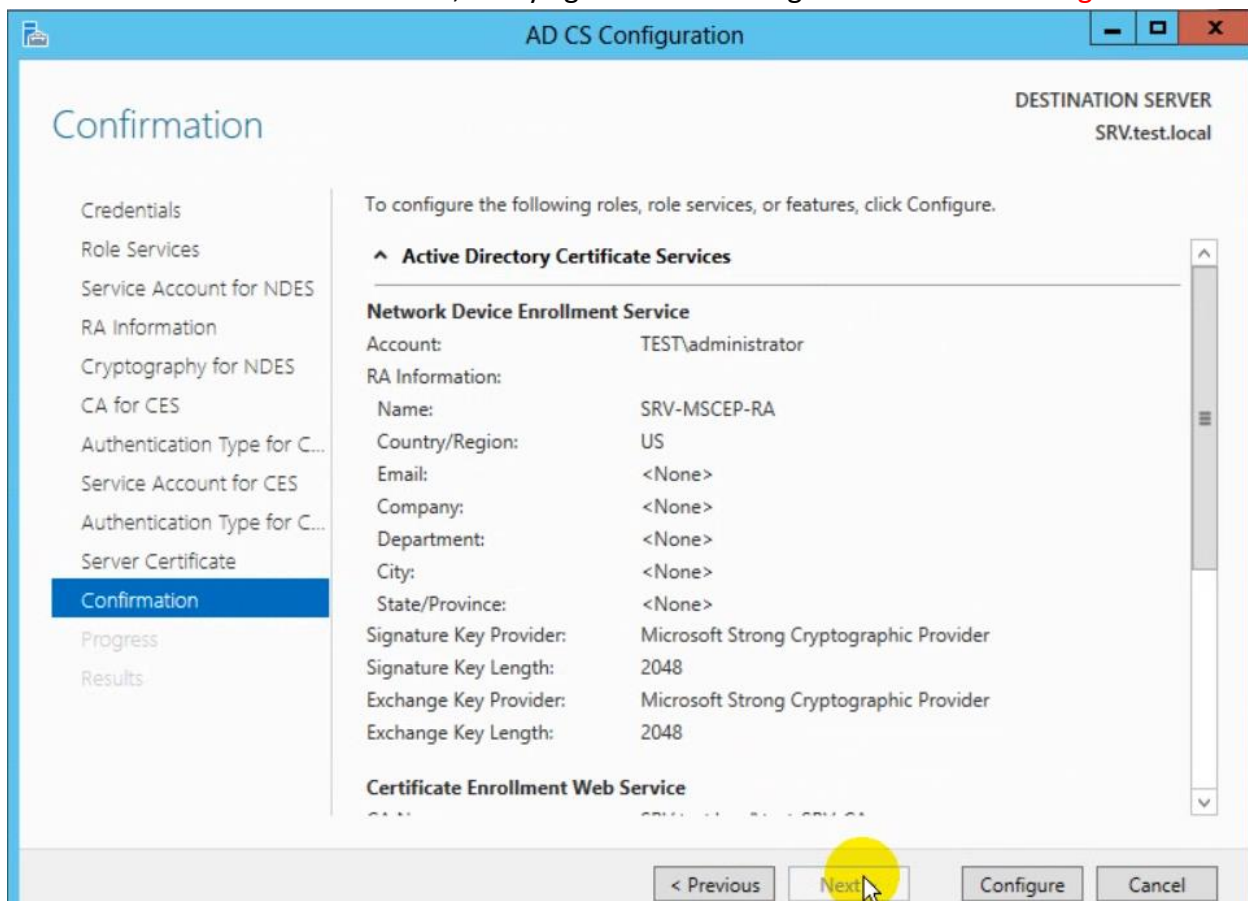


In **Server Certificate** interface, Keep the default setting and click **Next** to continue

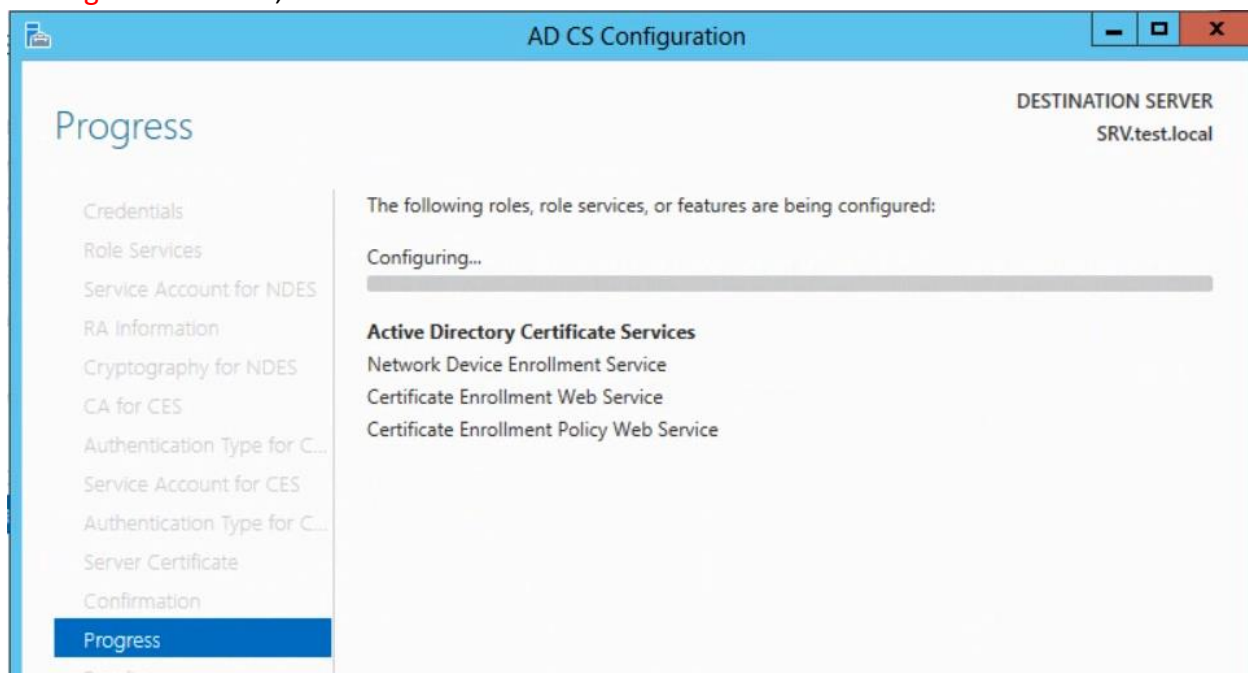




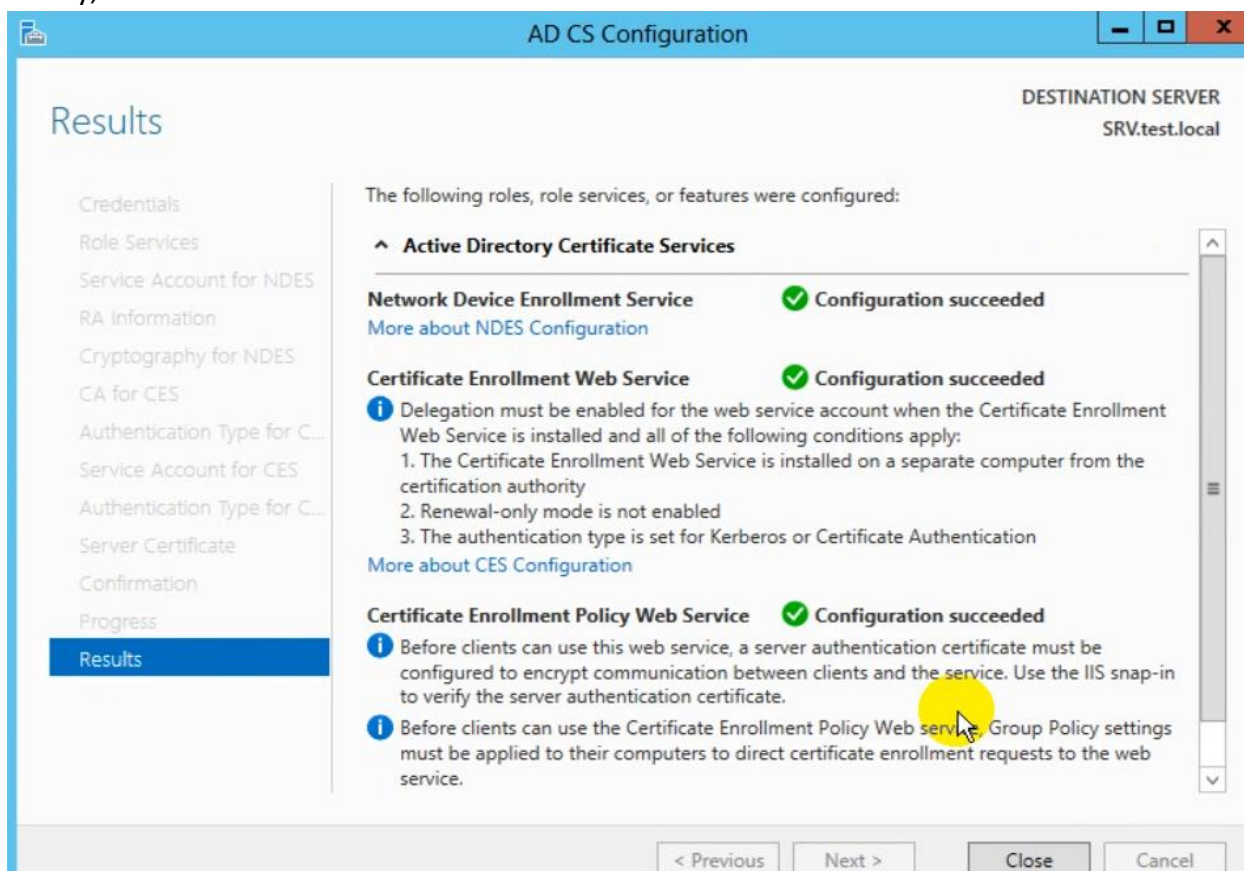
Next in the **Confirmation** interface, verify again all the settings and then click **Configure...**



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.

