Configure the Network Device Enrollment Service In Pictures

The Network Device Enrollment Service performs the following functions

- Generates and provides one-time enrollment passwords to administrators.
- Submits SCEP enrollment requests to the CA.
- Retrieves enrolled certificates from the CA and forwards them to the network device.

To request and enroll for a certificate by using the Network Device Enrollment Service

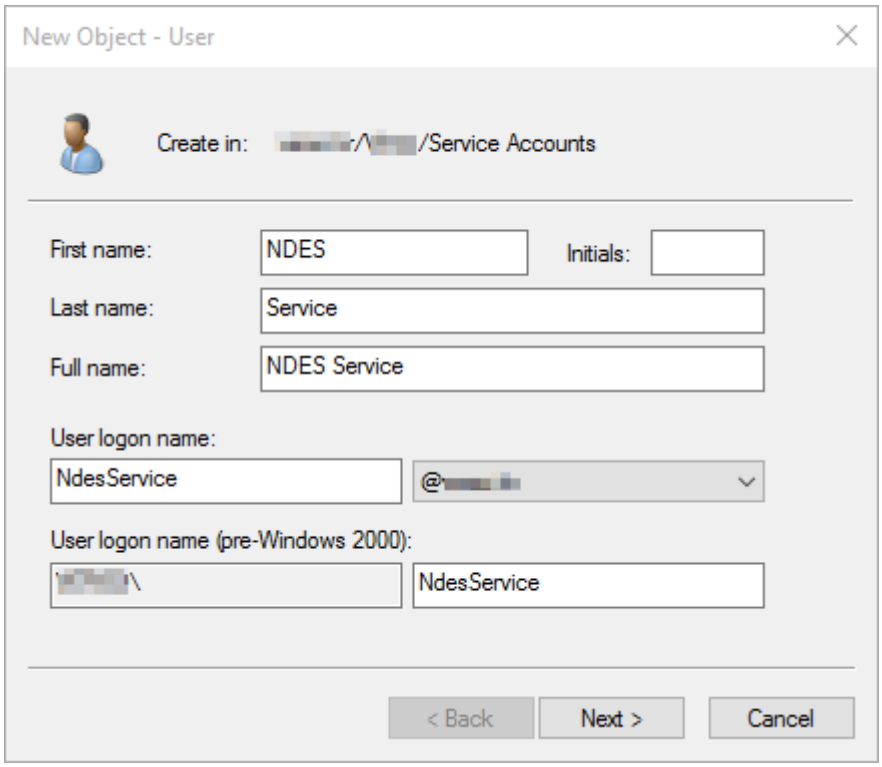
- Run the software used to manage the network device, and use this software to generate an RSA public/private key pair configured for one of the following:
  - Signing and signature verification
  - Encryption and decryption
  - Signing, signature verification, encryption, and decryption
- The service will be available on url: http://localhost/certsrv/mscep_admin
- If the password table is not full, the Network Device Enrollment Service will create a random password and embed it in an HTML page that is returned to the caller.
  - Note: Every time you connect to this URL, a different challenge password is displayed. Each challenge password is valid for 60 minutes and can only be used once.
- Use the device software, along with the password, to submit a certificate request through the Network Device Enrollment Service, which relays the request to the CA.
- If the enrollment request is successful, the requested certificate is returned to the device from the CA through the Network Device Enrollment Service.

By default, the Network Device Enrollment Service can only cache five passwords at a time. If the password cache is full when you submit a password request, you must do one of the following before resubmitting your request:

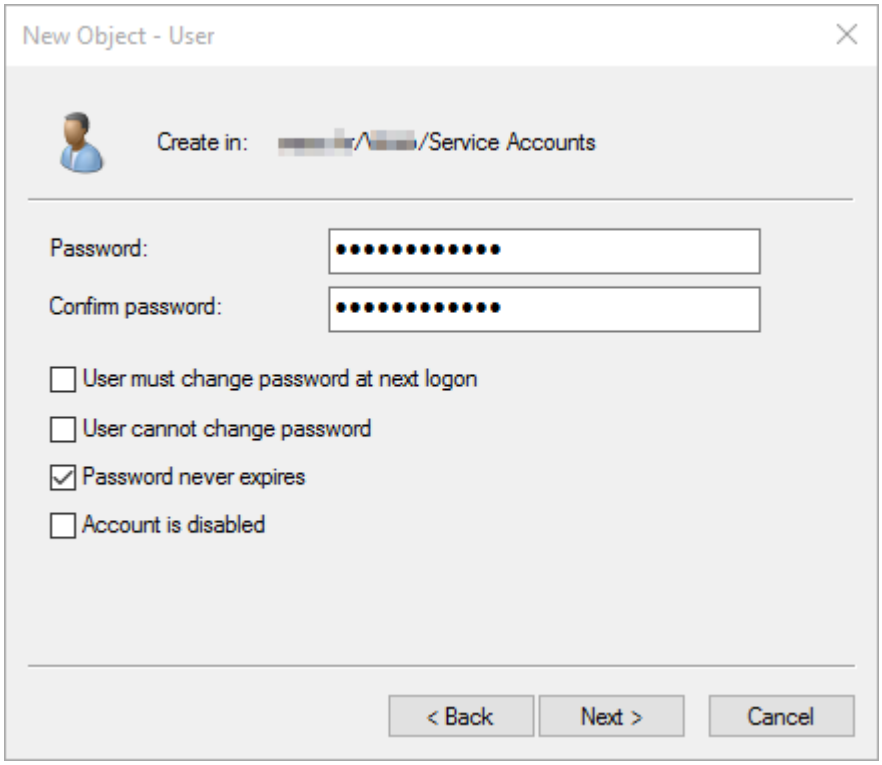
- Wait until one of the passwords has expired before submitting a new request.
- Stop and restart Internet Information Services (IIS) to delete all passwords stored in the cache.
- Configure the service to cache more than five passwords at a time.

—-

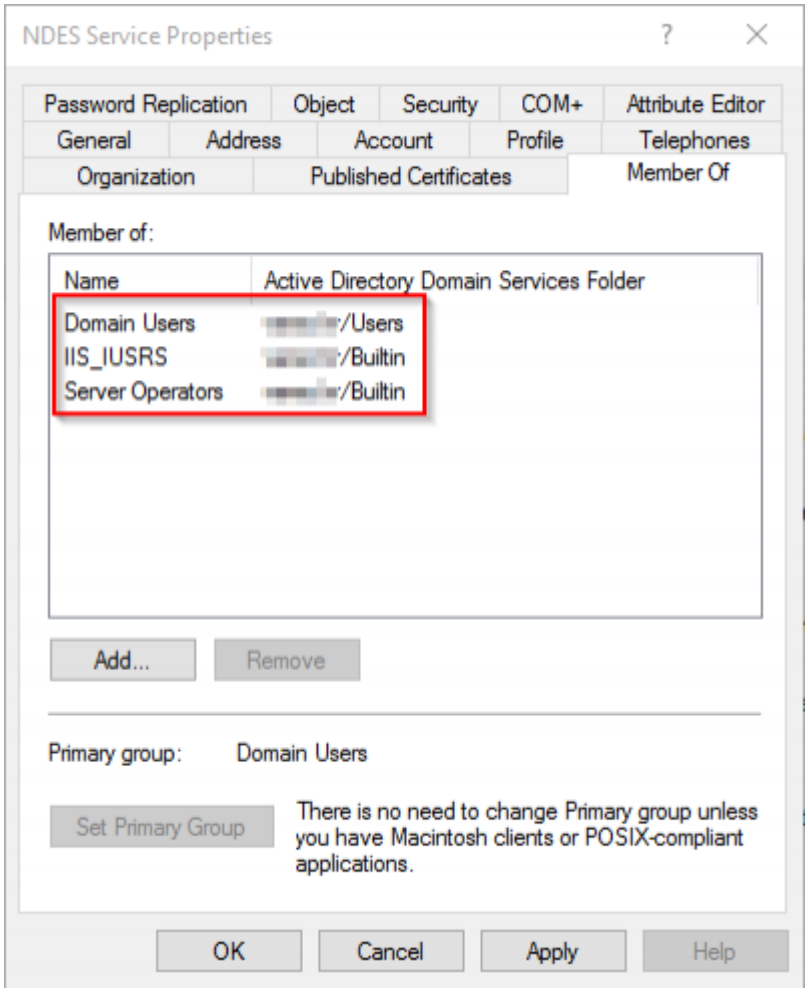
Here is how to configure the feature upon installation:



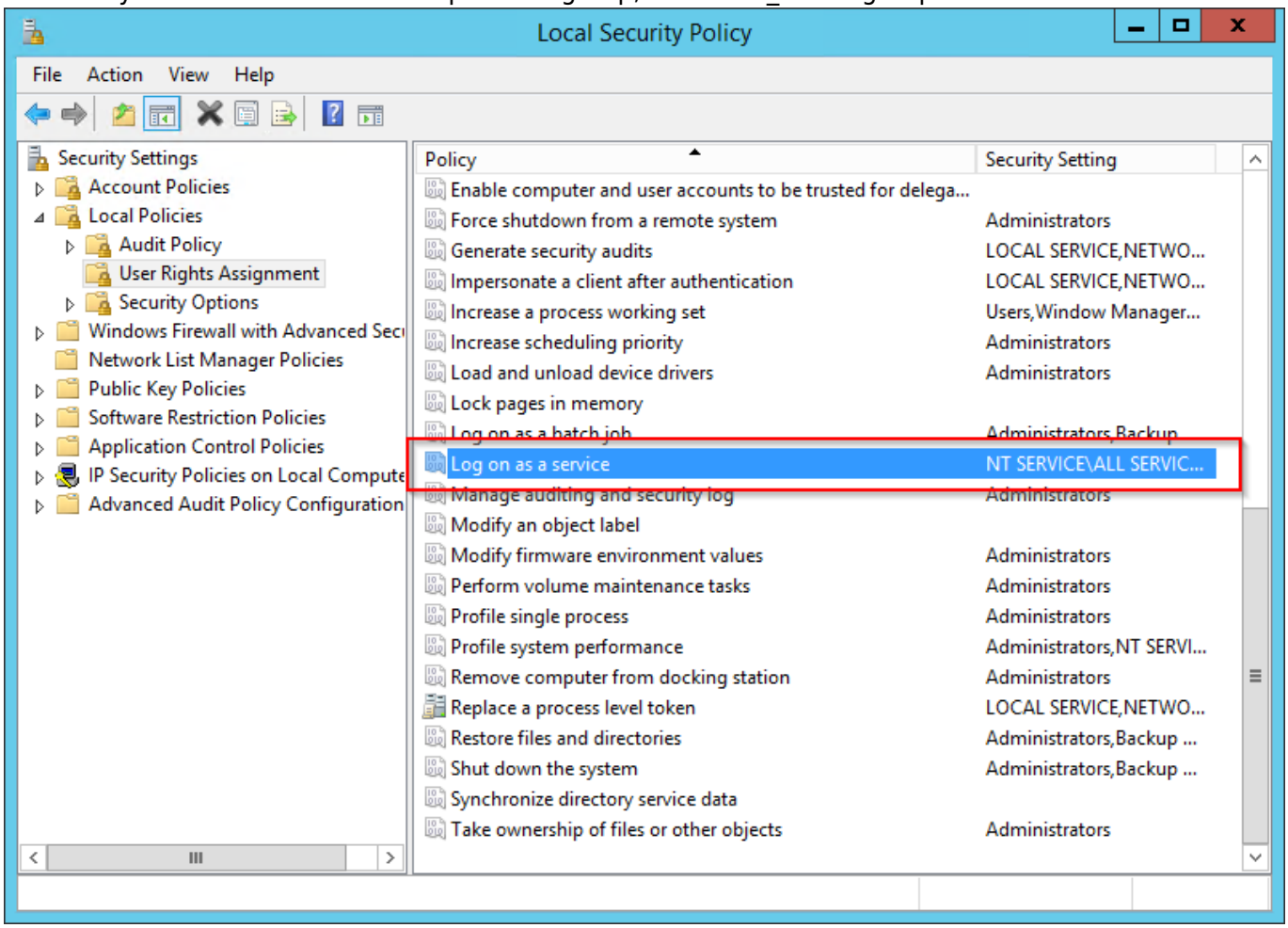
Create a new AD user named NdesService



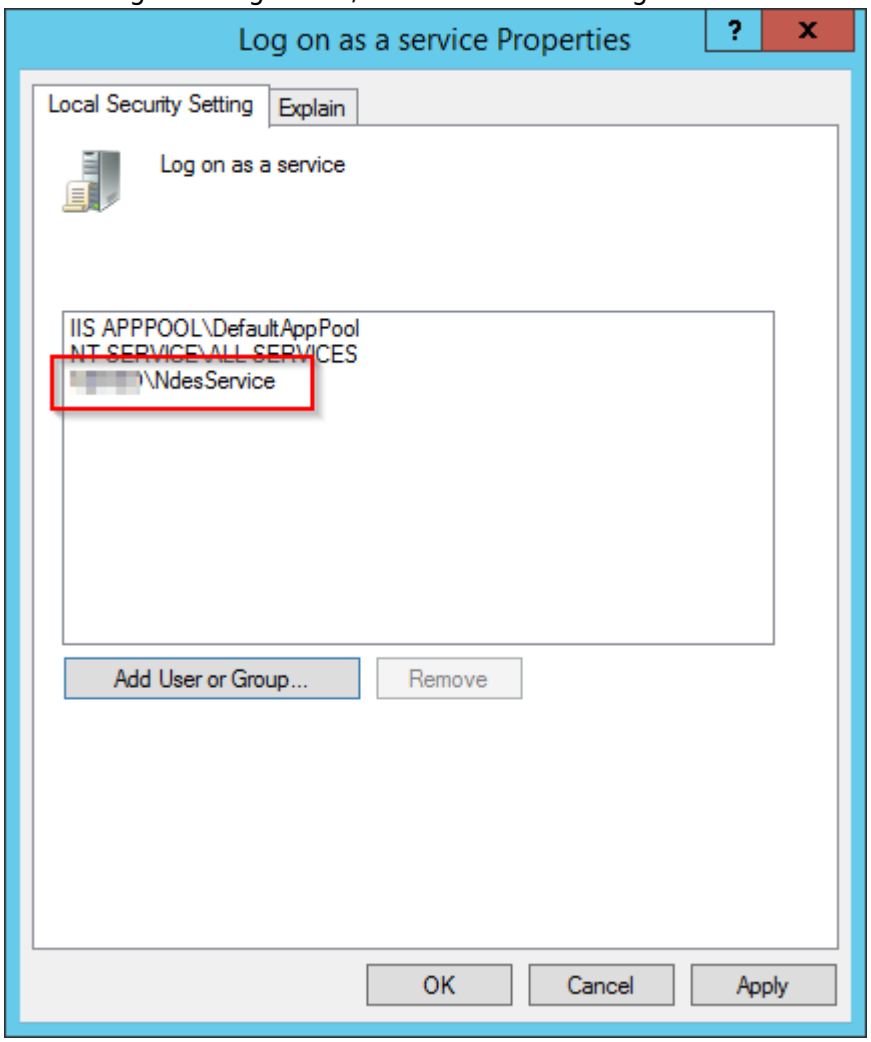
Set a strong password for the user and tick ‘Password never expires’



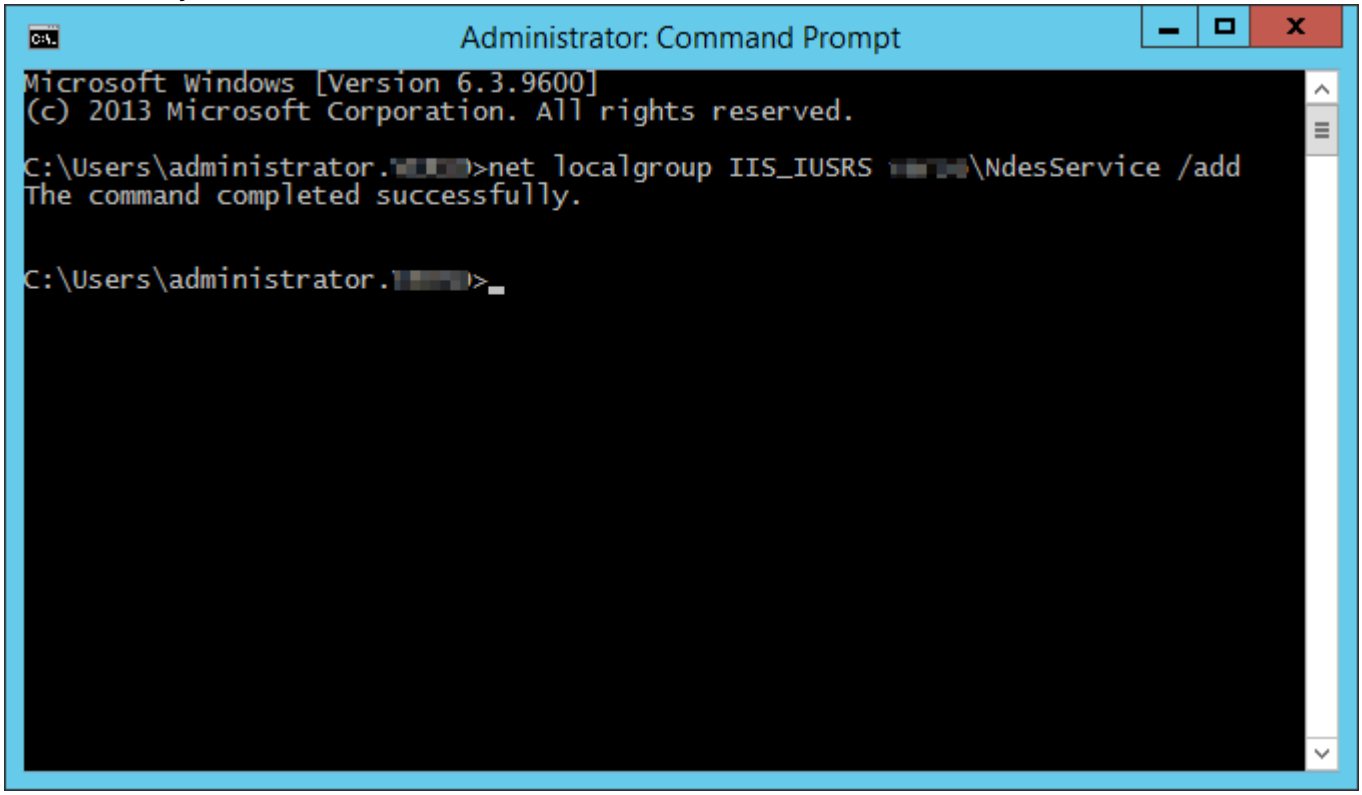
Add newly created user to Server Operators group, and to IIS_IUSRS group



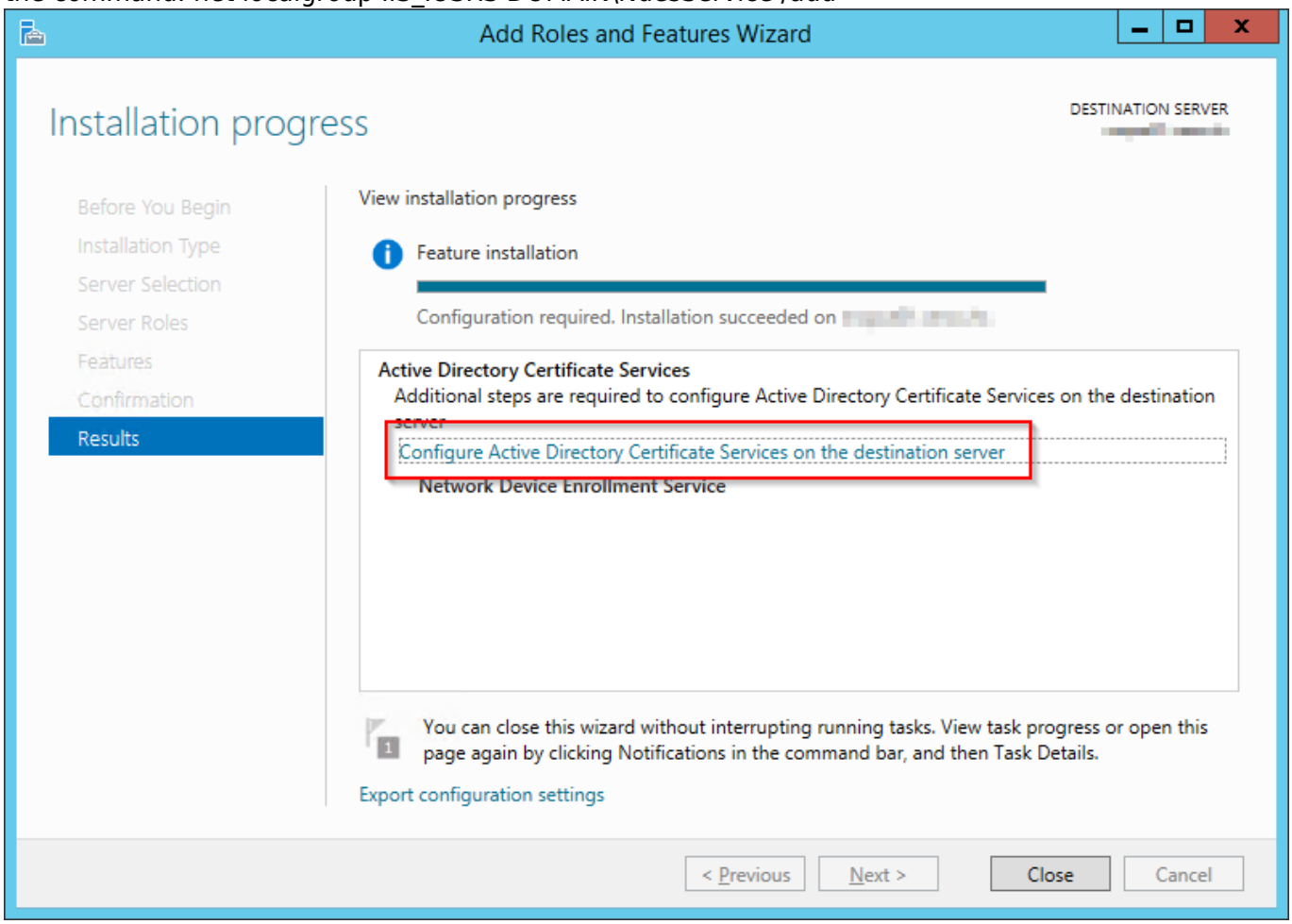
Open ‘Local Security policy’ on the server where you installed the NDES and navigate to Local Policies ⇒ User Rights Assignment, and double-click ‘Log on as a service’



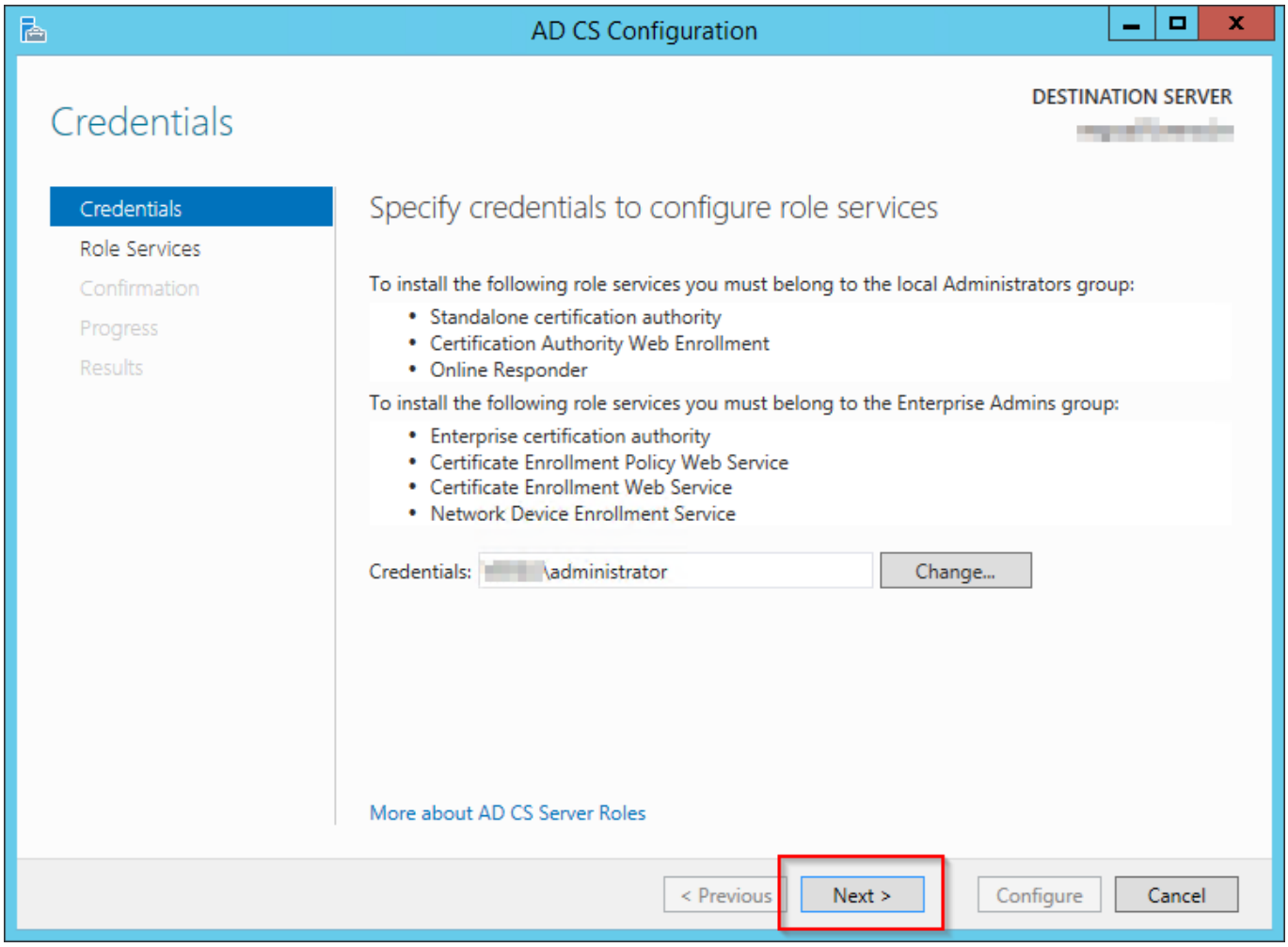
Add the newly created domain user to the list



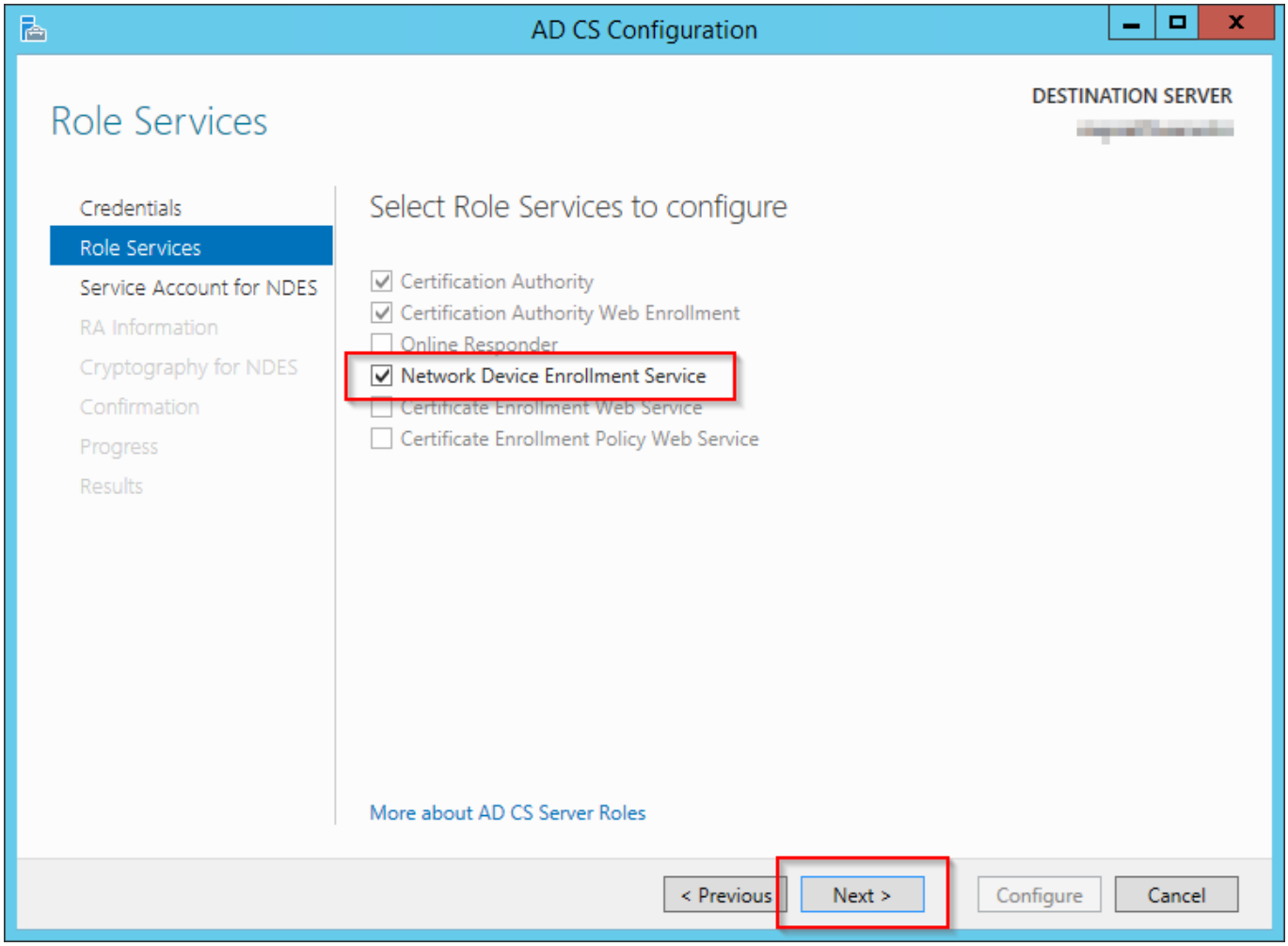
Open command prompt and add the newly created domain user to local IIS_IUSRS group by issuing the command: net localgroup IIS_IUSRS DOMAIN\NdesService /add



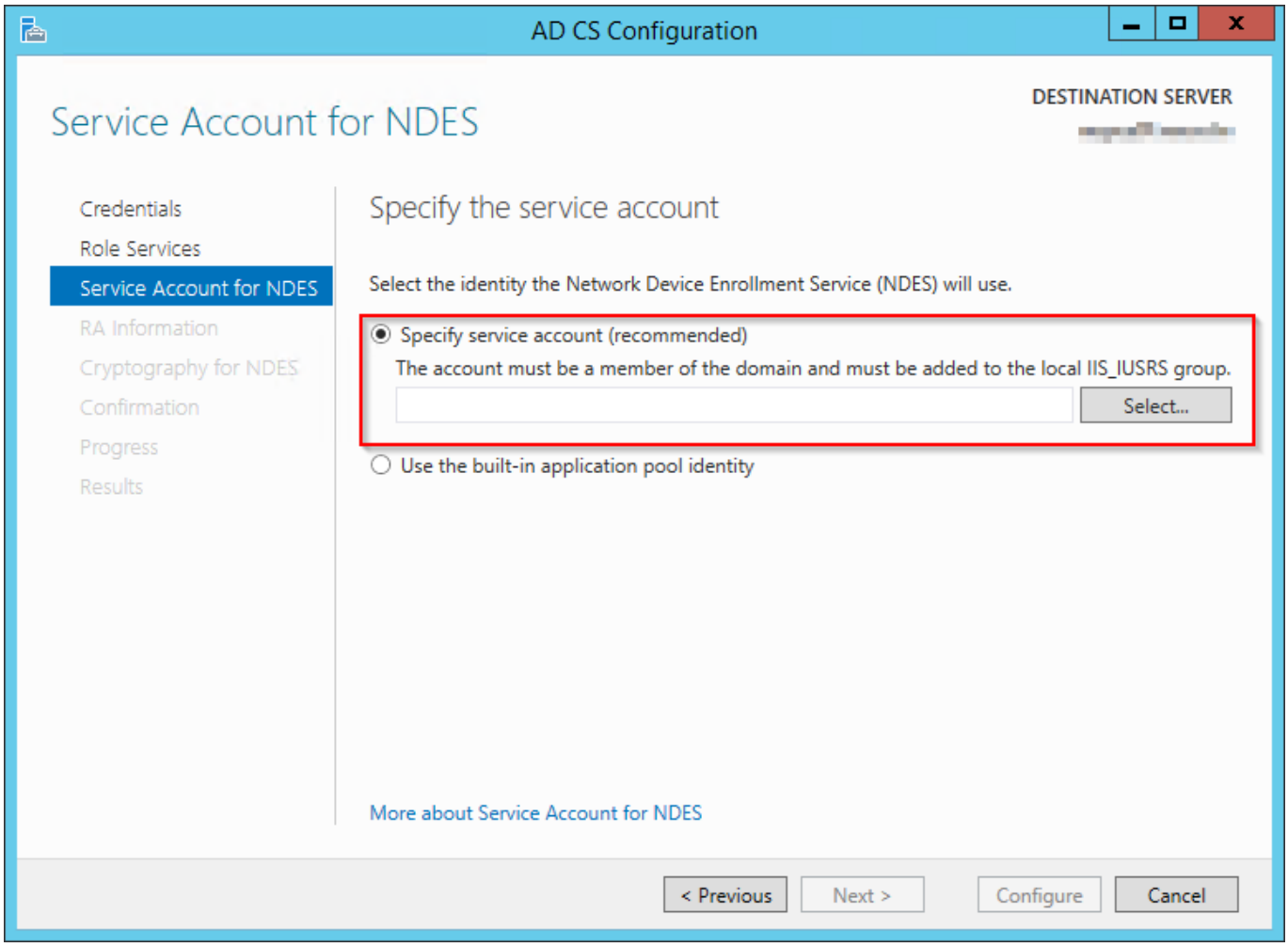
After you have finished installing the Network Device Enrollment Service role, click ‘Configure Active Directory Certificate Services on the destination server’



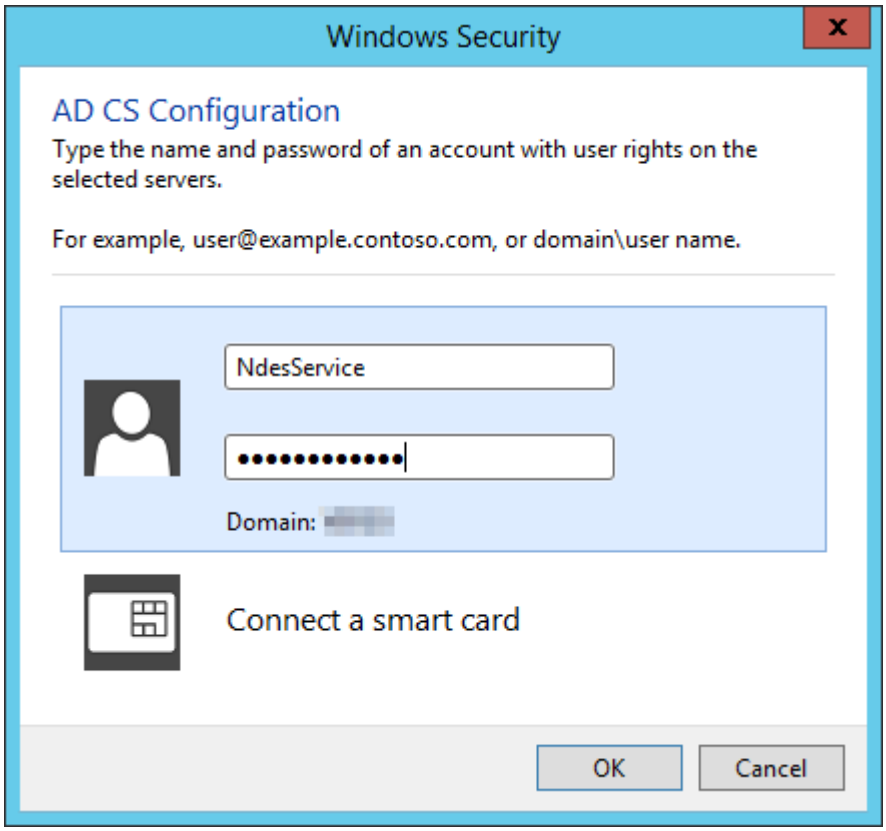
Make sure that you have the adequate credentials and click ‘Next’



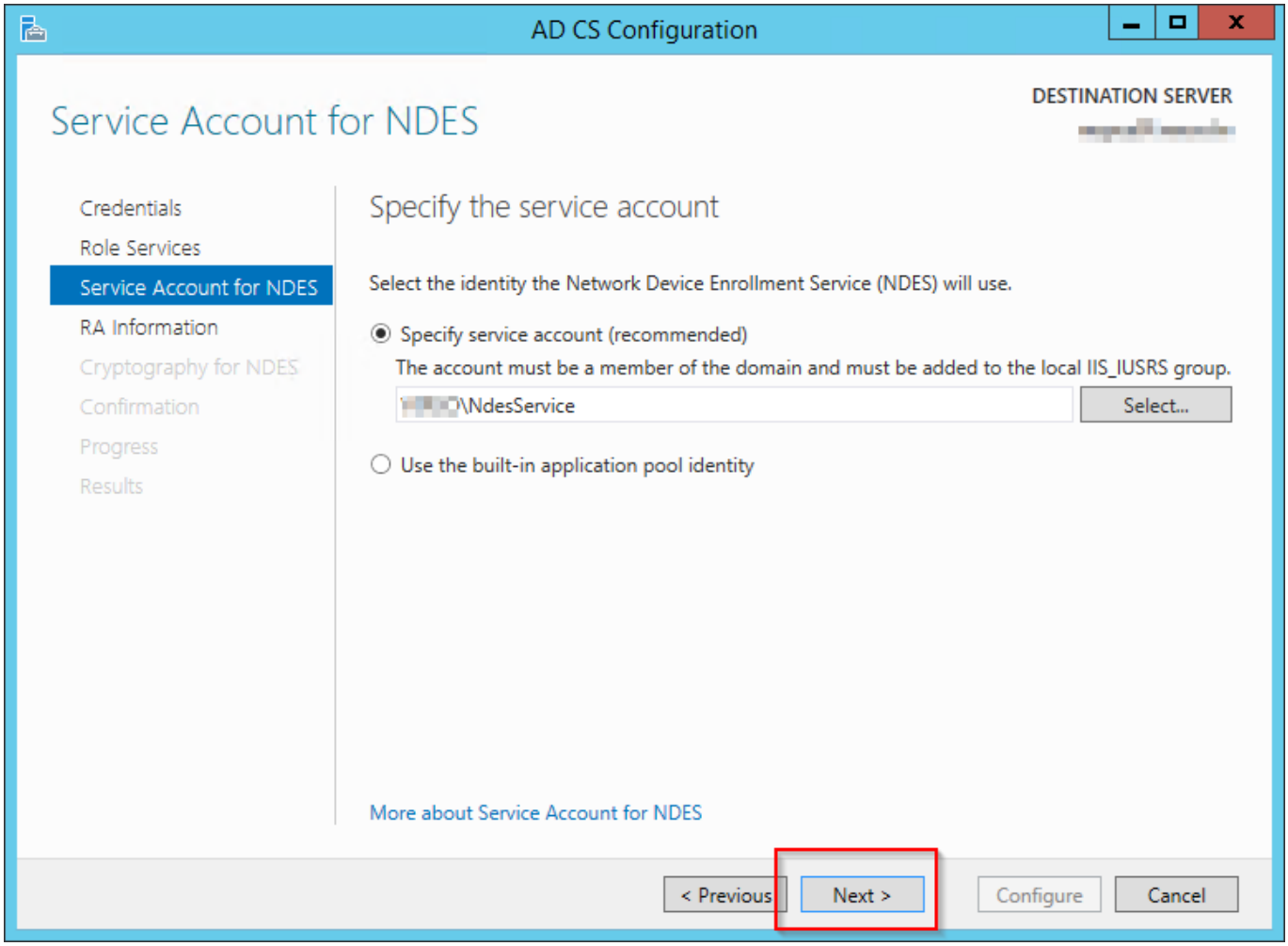
Tick the ‘Network Device Enrollment Service’ and click ‘Next’



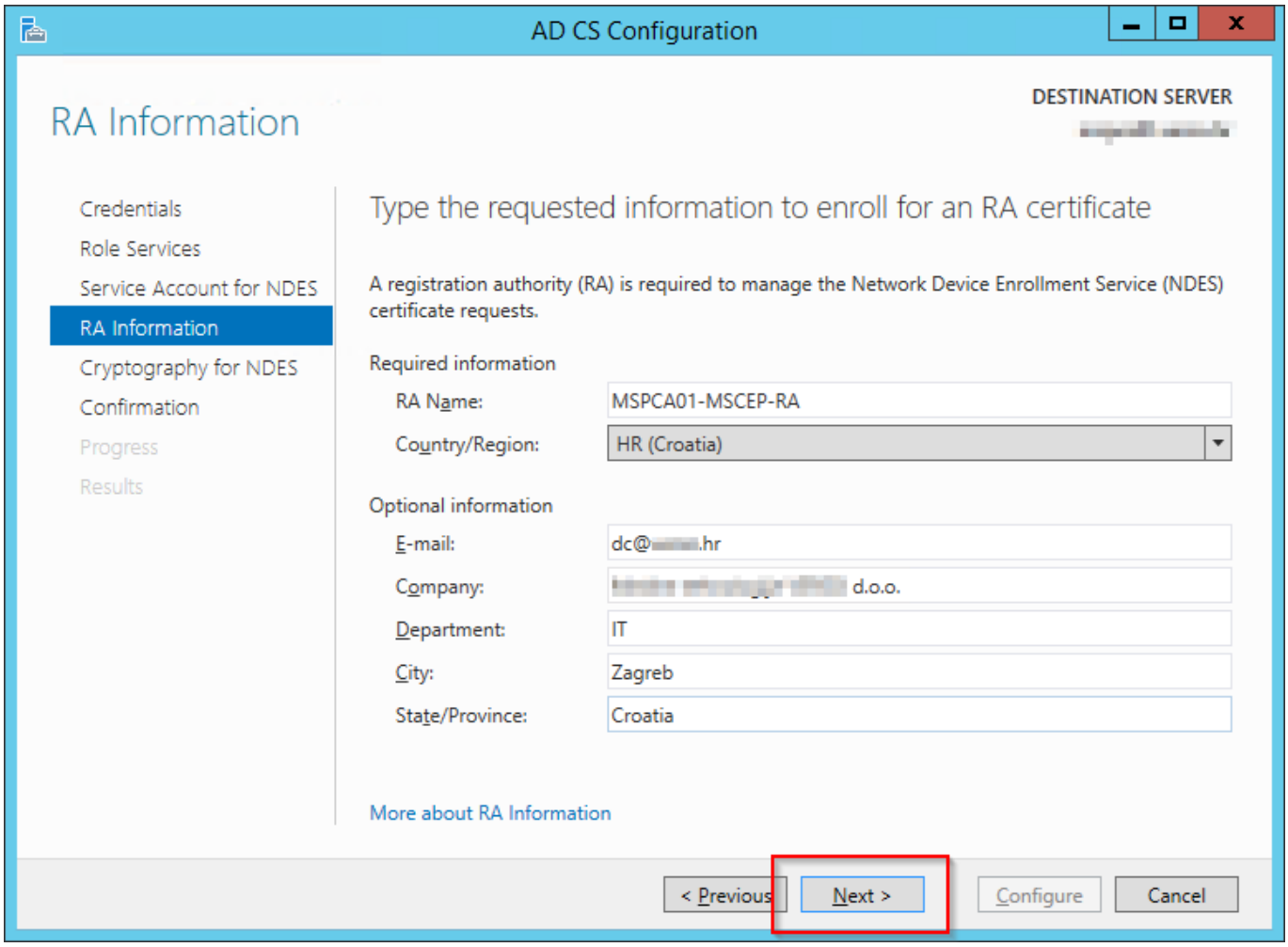
Click ‘Select...’



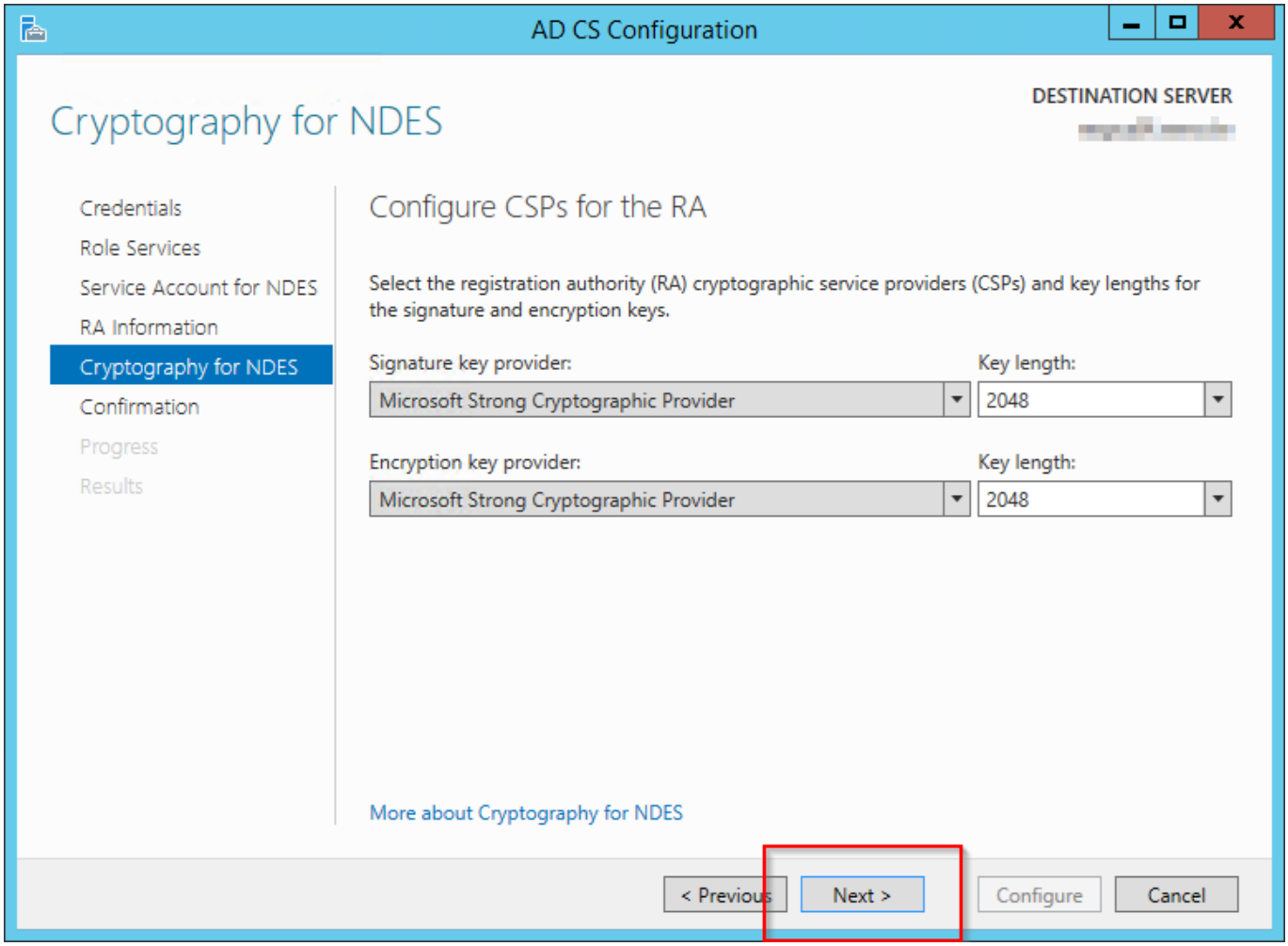
Enter the credentials of the newly created domain user and click ‘OK’



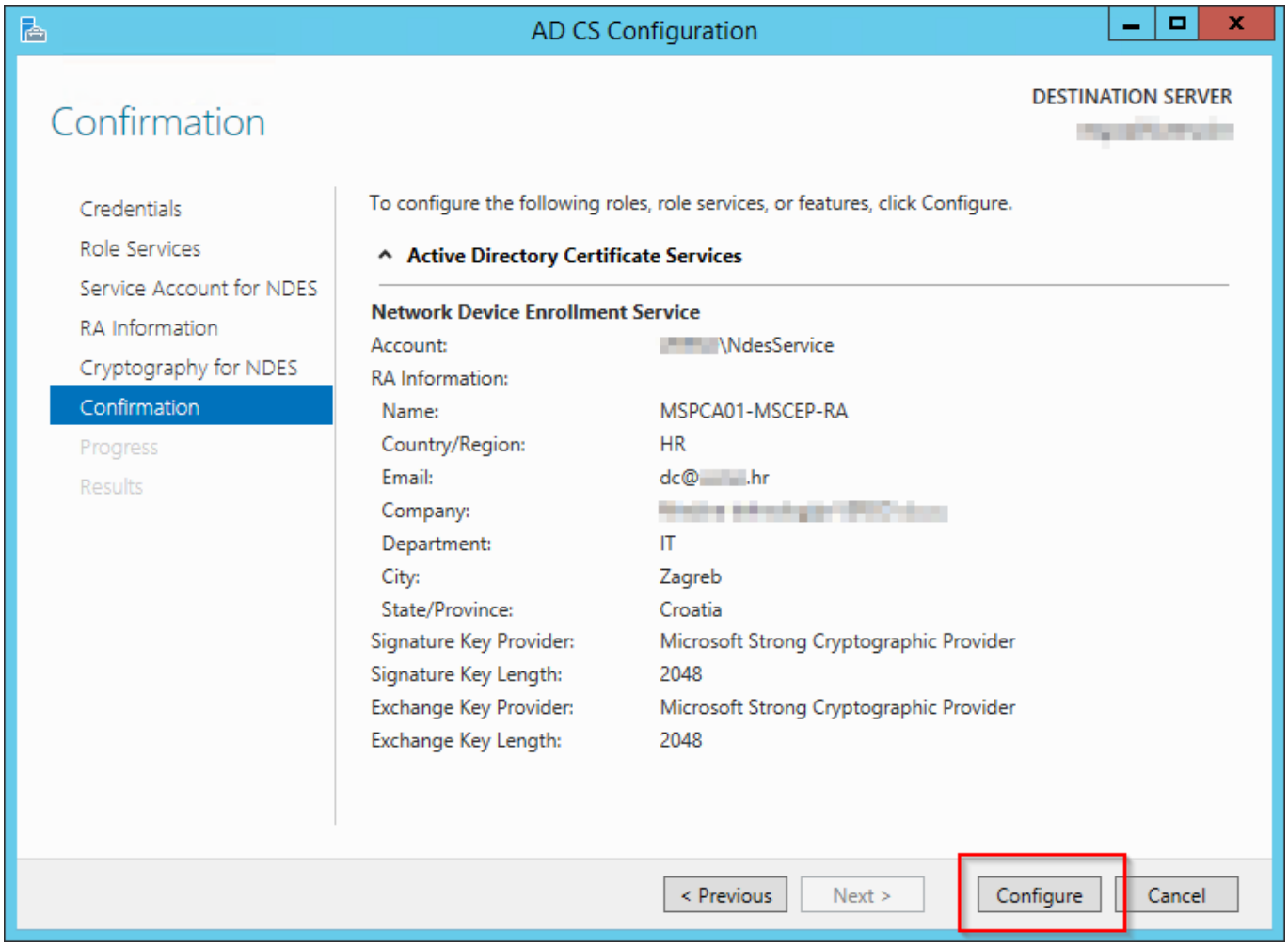
Now that we have selected the user, click ‘Next’



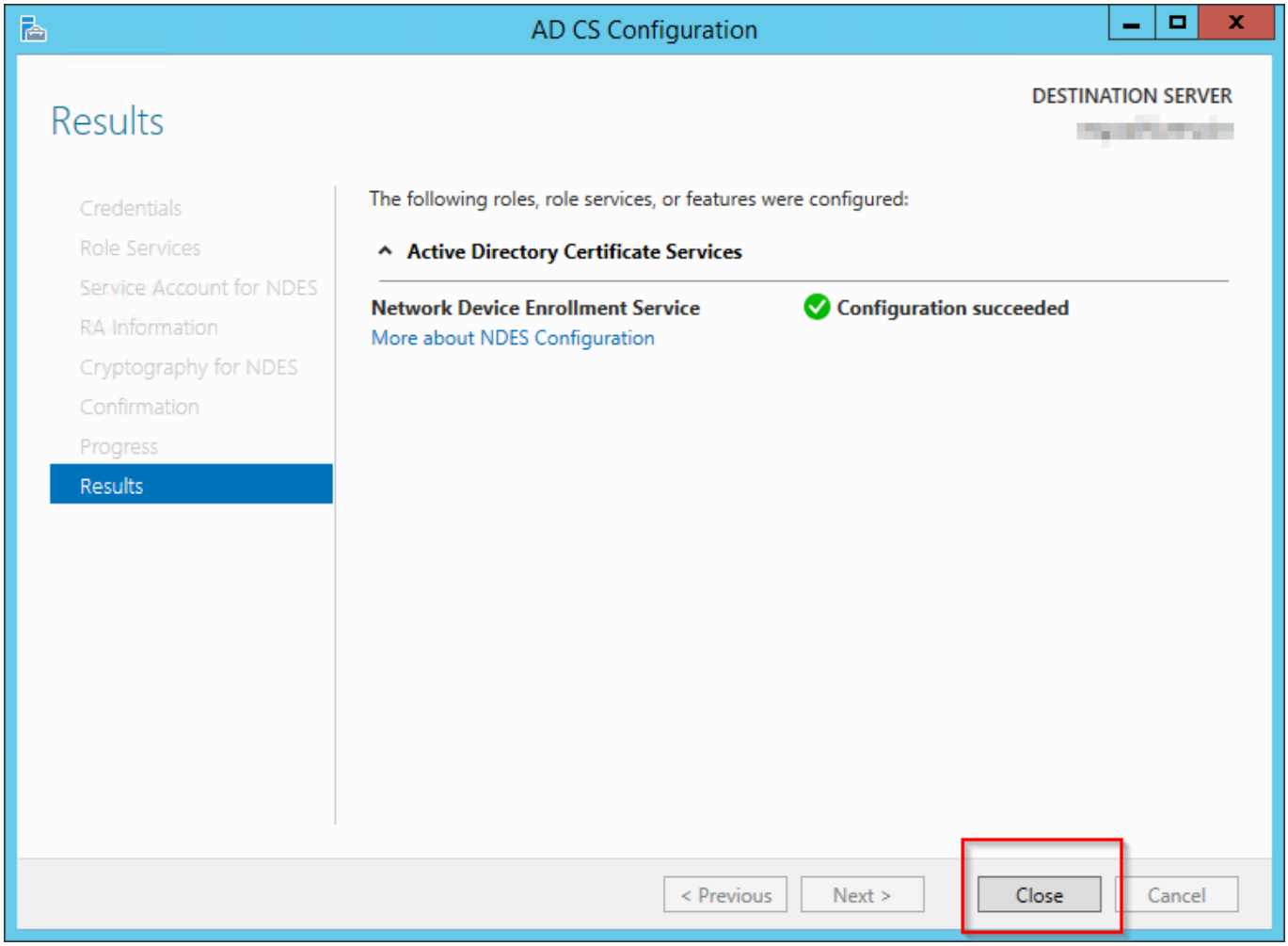
Enter the required details in the form and click ‘Next’



You can leave this as-is and click ‘next’. Or you can change the providers and key lengths, but this is OK



Confirm that all data is correct and click ‘Configure’



Close the wizzard and you’re done!

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=windows:servers:net_data_enrollment_service

Last update: **2019/10/31 09:06**