NASLORD

LDAP CONFIGURATION GUIDE (SUPER-USERS)

NASLORD 3.0.0

LDAP Configuration Guide (Super-Users)

Version: 3.0.0
Date: 2026-07-14
Product: NASLord
Vendor: Gallium Inc.
Audience: Super-users (NASLord administrators)

TABLE OF CONTENTS

1. CONFIGURE DNS ON THE NASLORD INSTANCE (SKIP IF DNS IP ADDRESS IS ALREADY CONFIGURED):

a. Open a web console on NASLord instance through your Hypervisor, login and enter *configure* to execute the configuration script.

b. Type *Y* on the *change network configuration prompt and hit Enter.*

c. *Type N* on *enable DHCP and hit enter.*

d. Enter the FQDN, IPs and DNS IPs.

e. Once the configure script is done, reboot the instance.

2. CREATE REQUIRED GROUPS AND USERS ON THE DOMAIN CONTROLLER:

a. Create allowed-users security group in the DC Organizational Unit

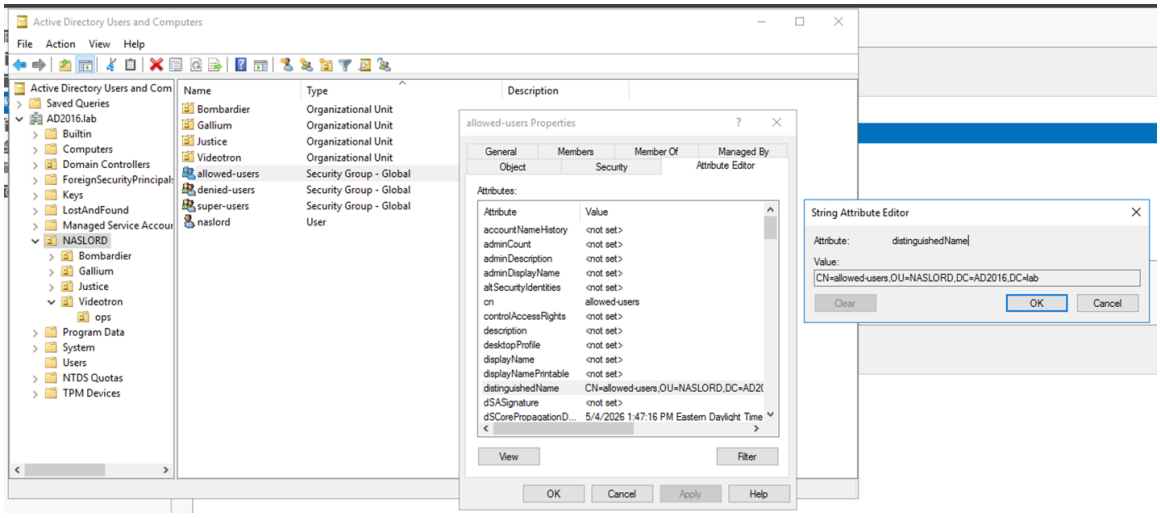
b. Create denied-users security group in the DC Organizational Unit

c. Create super-users security group in the DC Organizational Unit

d. Create a user used as service account to link the NASLord instance to the DC LDAPS server.

e. Gather the previously created groups/user *distinguished names* and save for later for the NASLord instance LDAPS configuration.

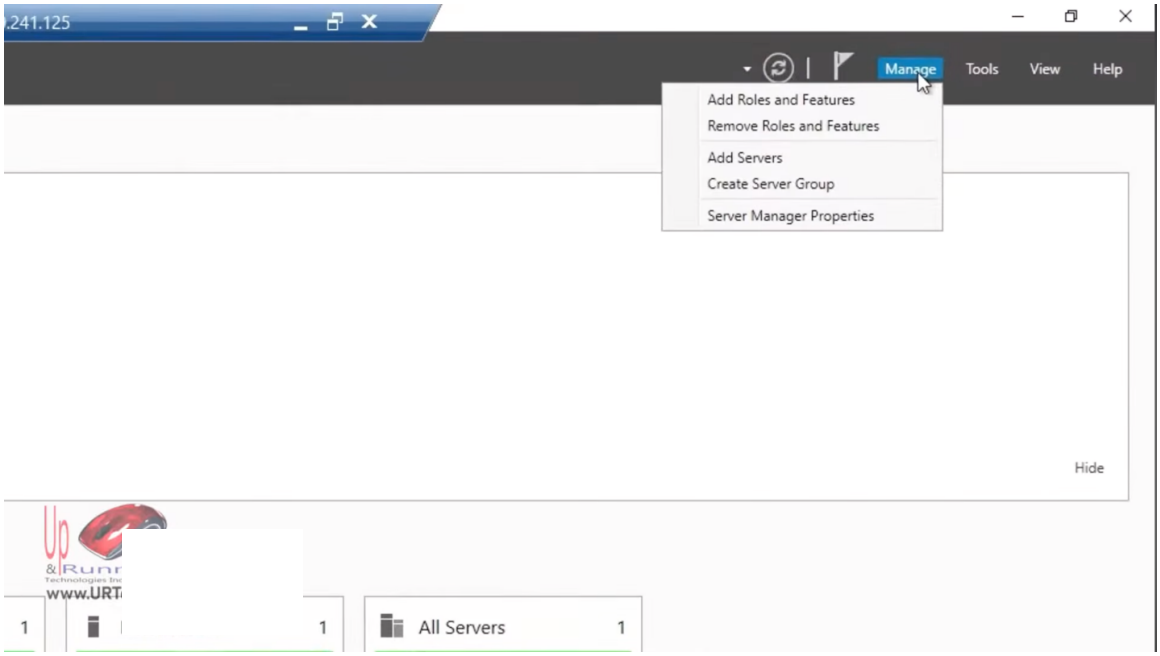
Ex.



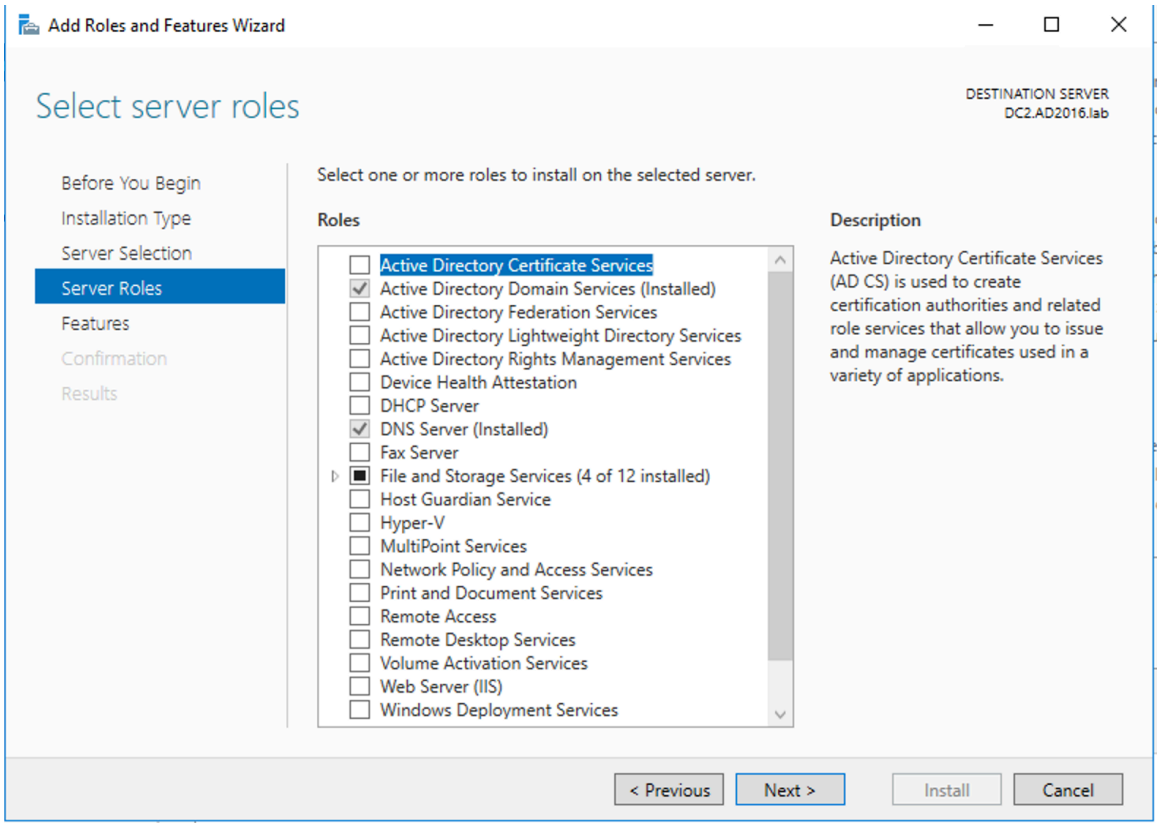
3. CONFIGURE CERTIFICATE CA SERVICES ON THE DOMAIN CONTROLLER:

Skip to step 4 if you already have a Certificate CA on you Domain Controller.

a. Add Roles and Features:



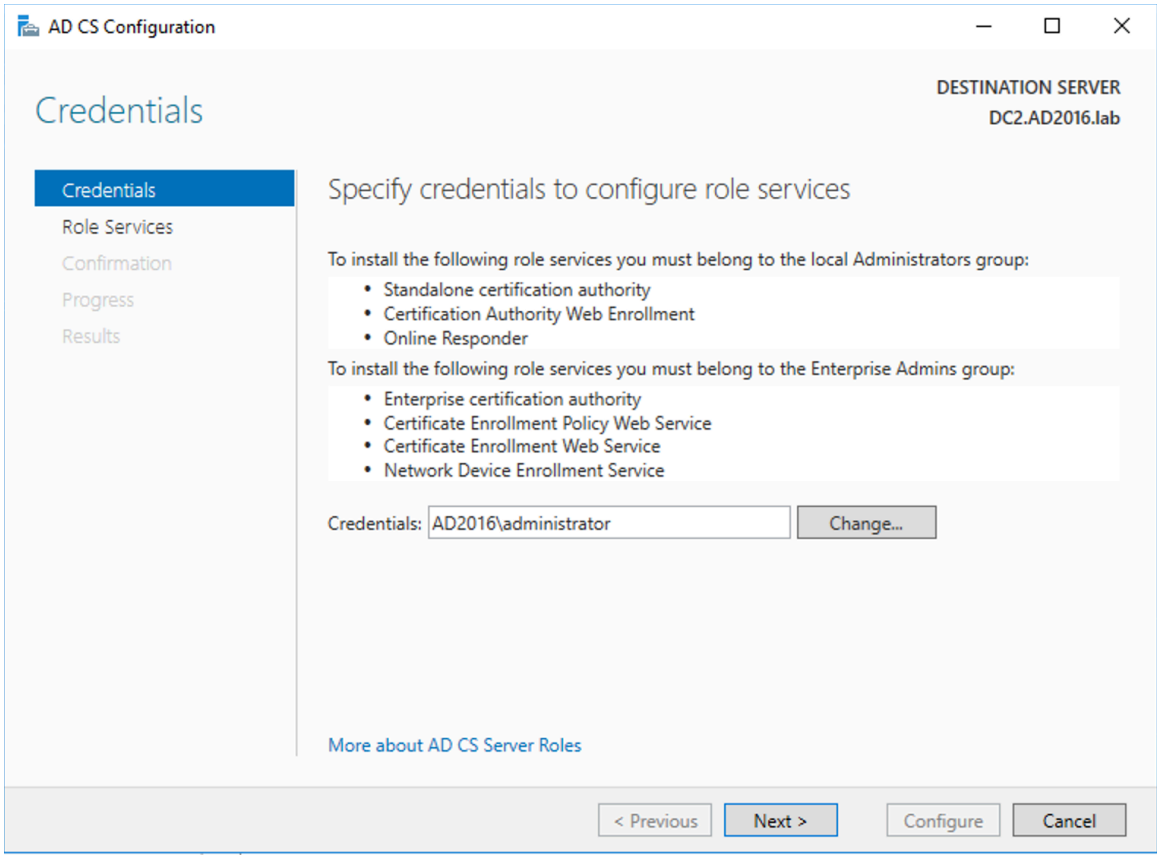
b. Select Active Directory Certificate Services:



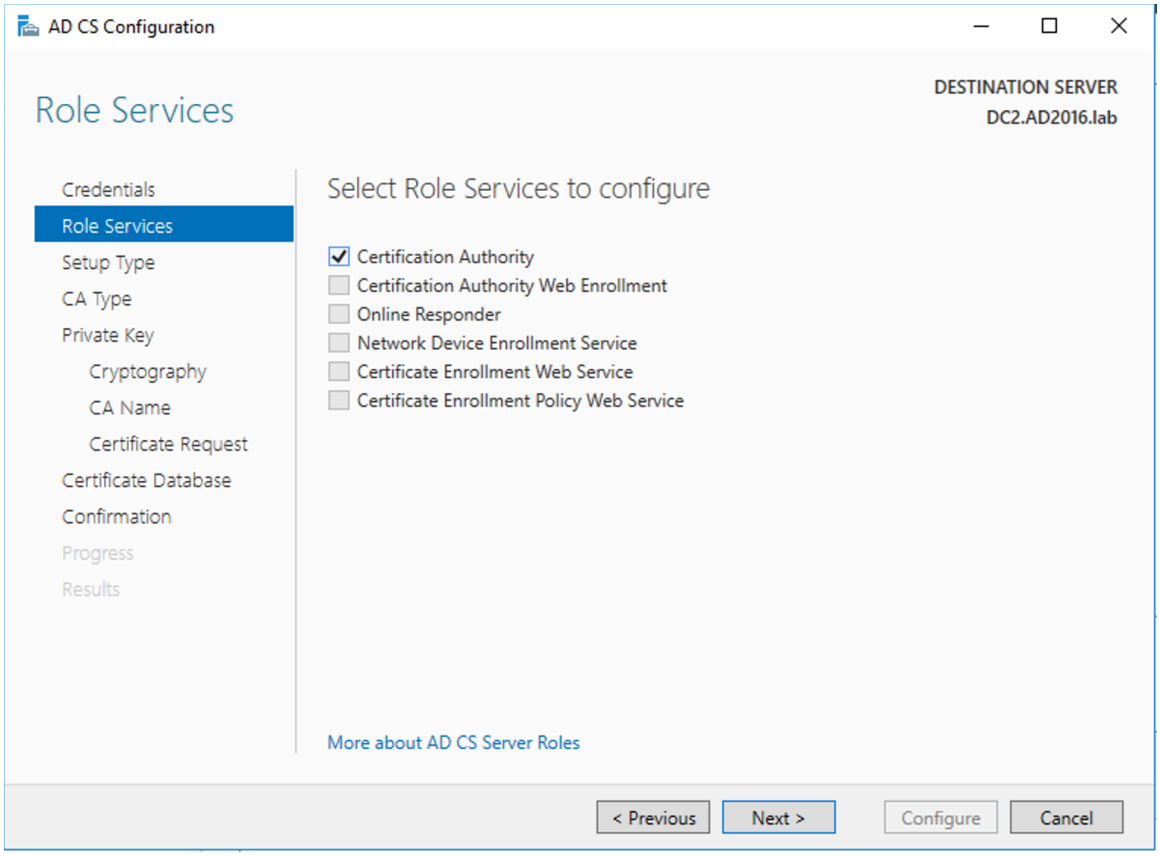
c. Hit *Add Features* when prompted.

d. Follow the Wizard steps and hit *Install* to install the services on the Domain Controller.

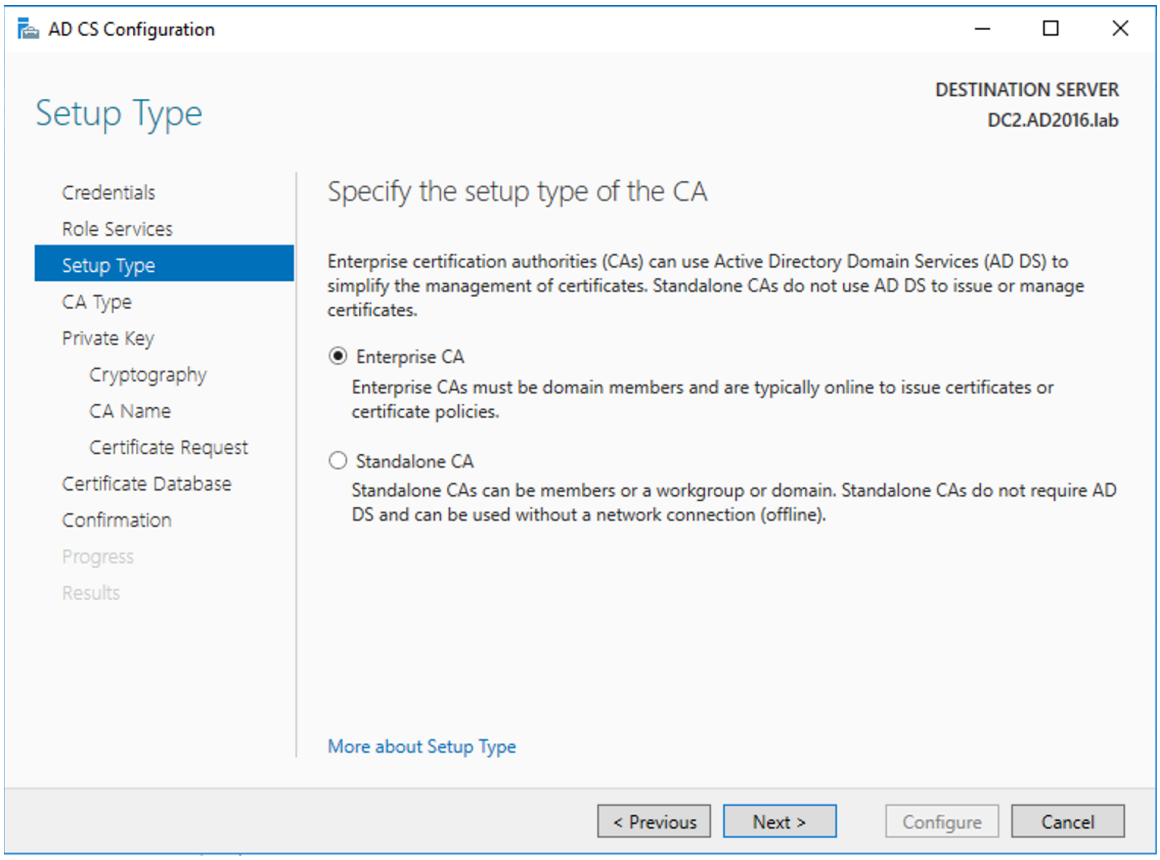
e. Under Roles and Features, select AD CS Configuration and use Wizard to configure CA:



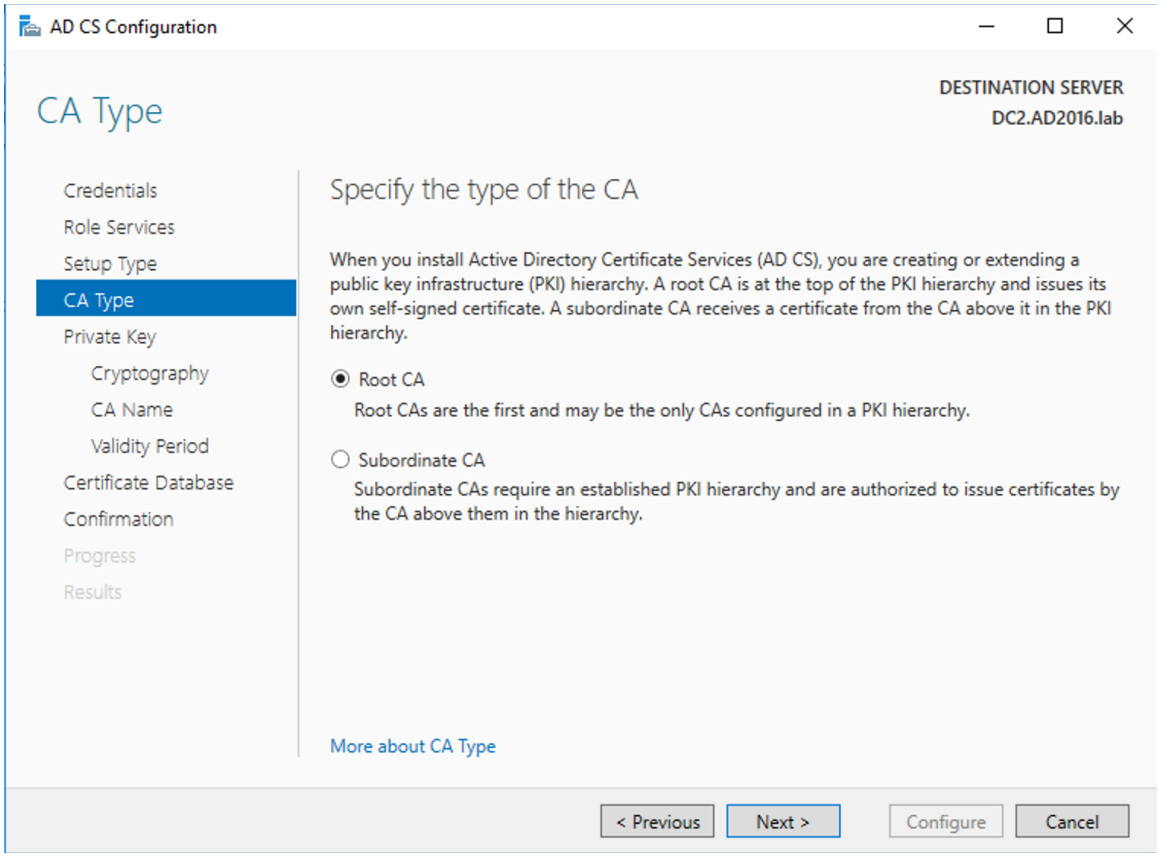
f. Select *Certification Authority* Role services and hit Next:



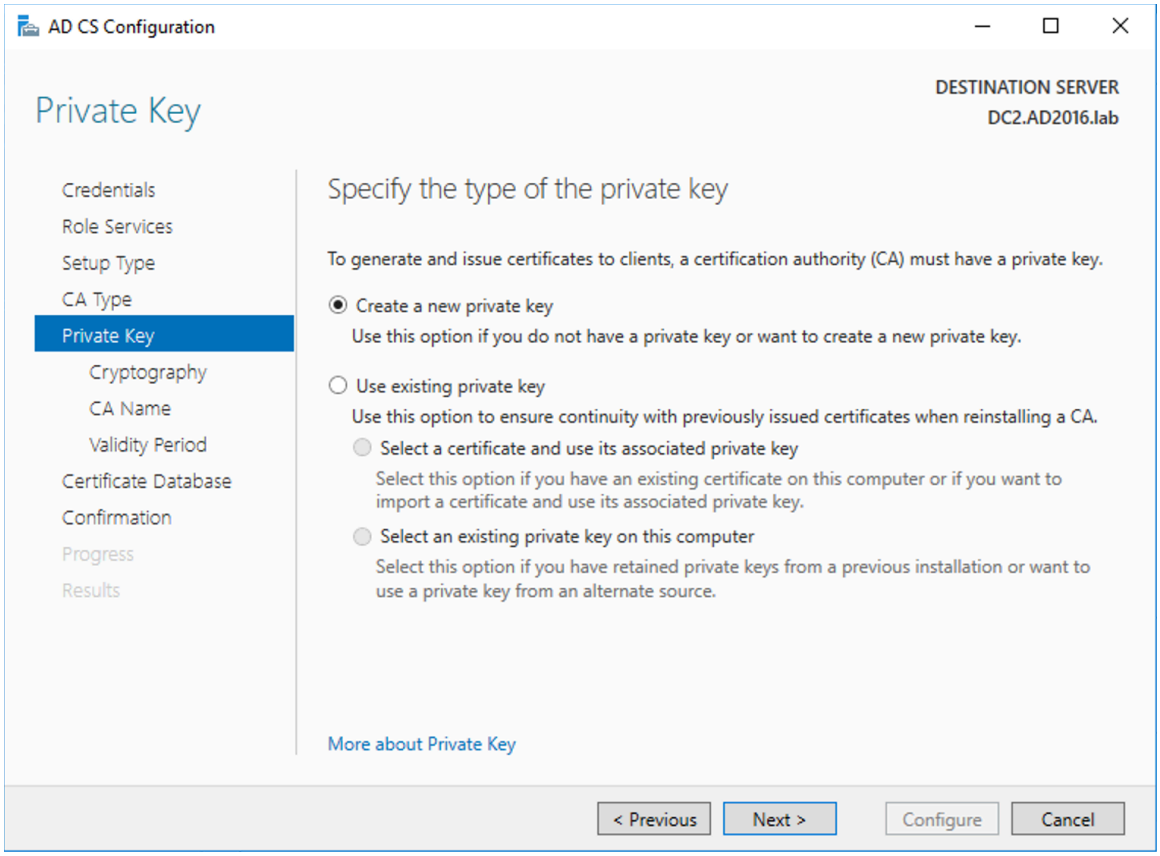
g. Select *Enterprise CA* and hit Next:



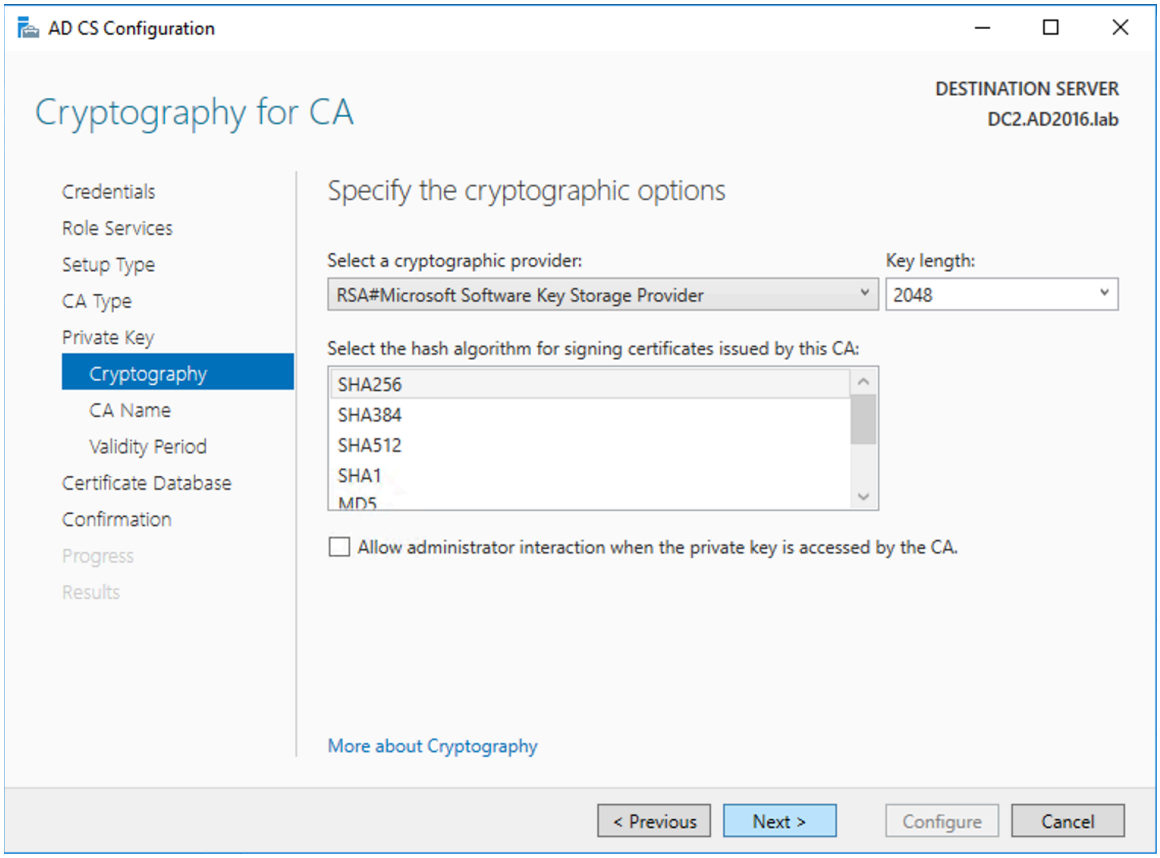
h. Select *Root CA* and hit next:



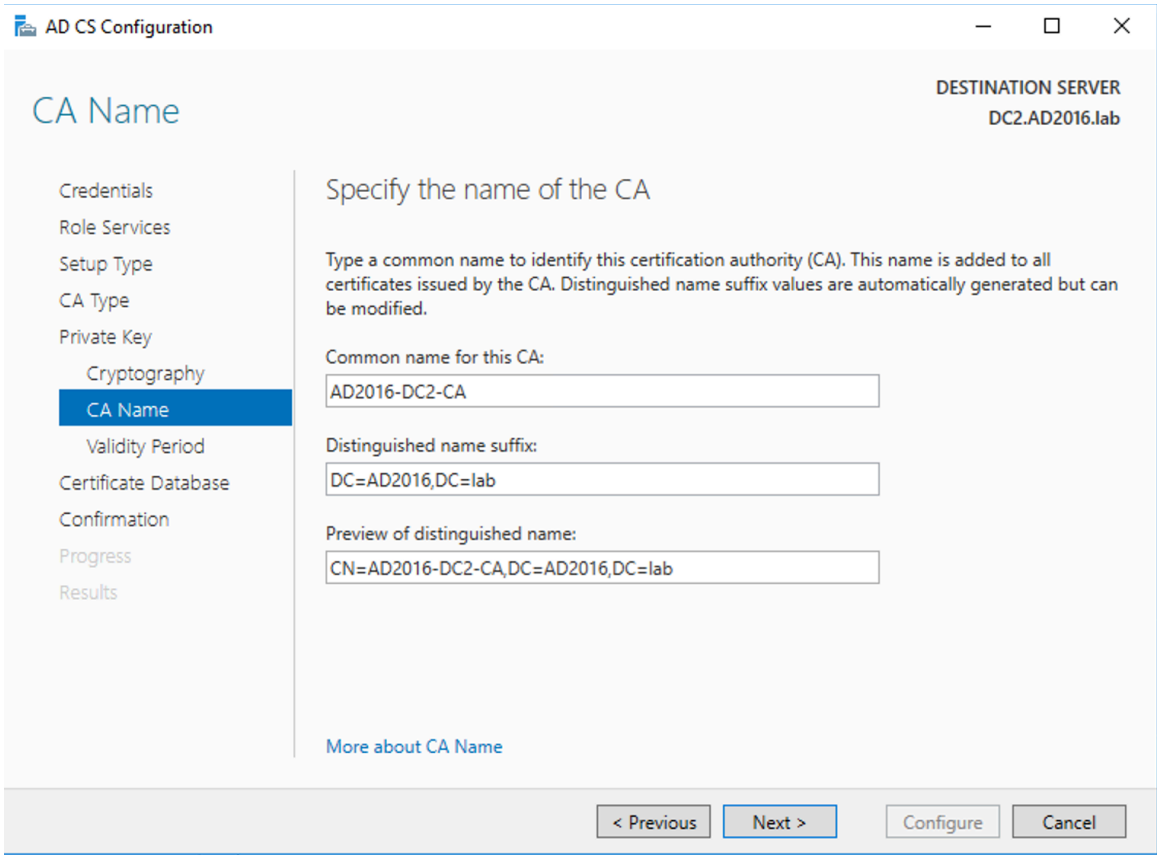
i. Select *Create a new Private Key* and hit next:



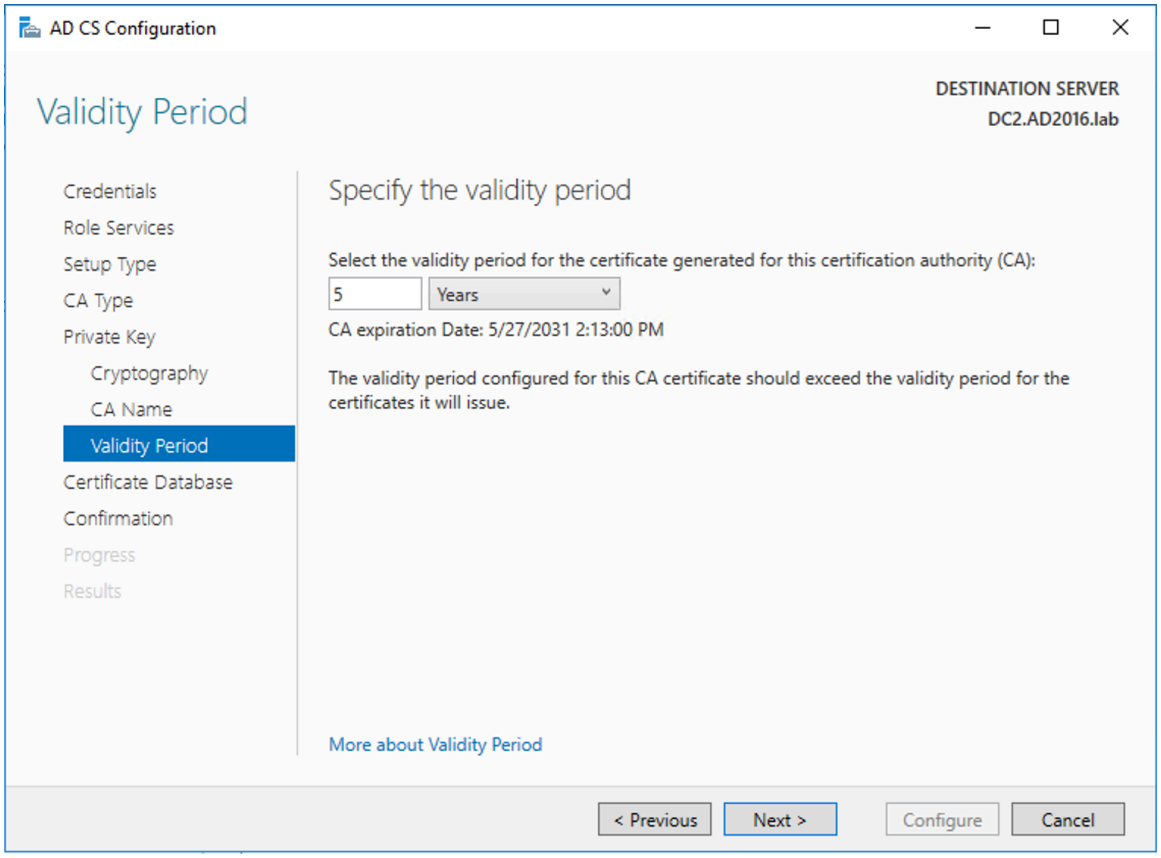
j. Select *SHA256* Algorithm and hit next:



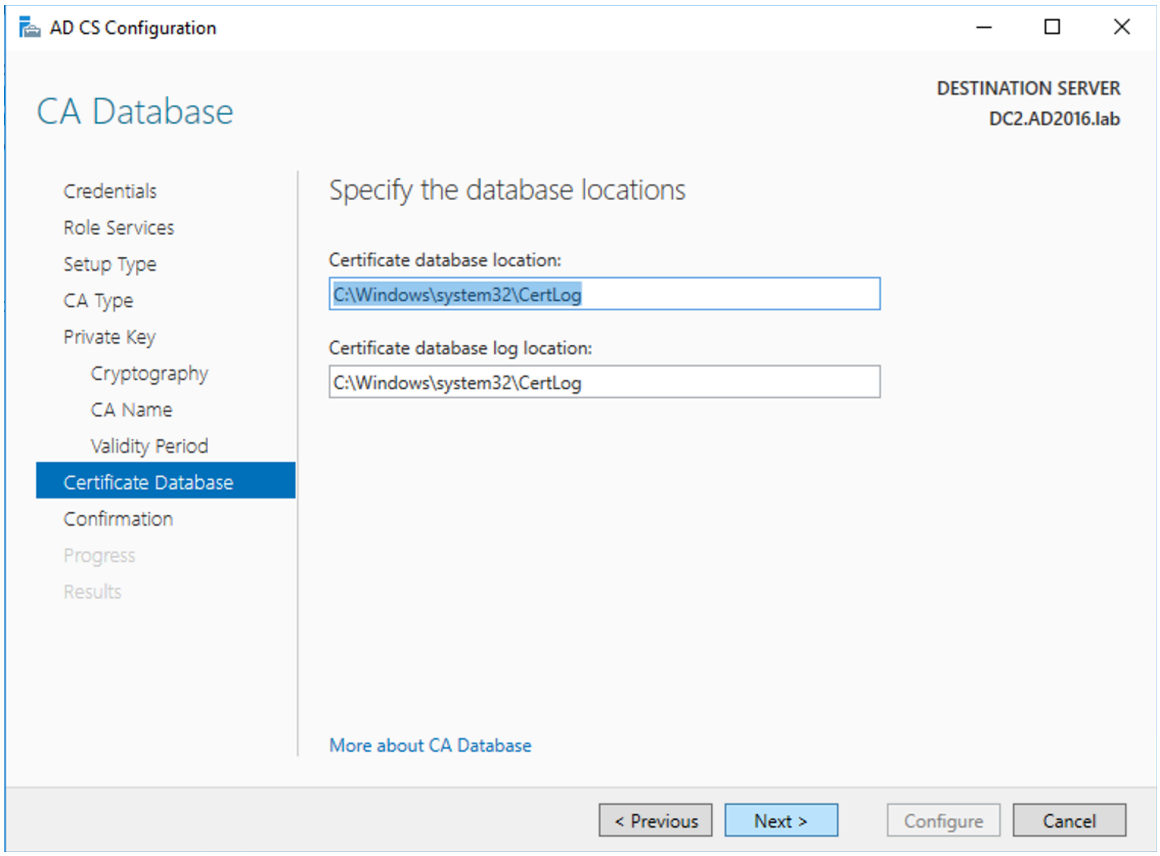
k. Type the name of your CA and hit next:



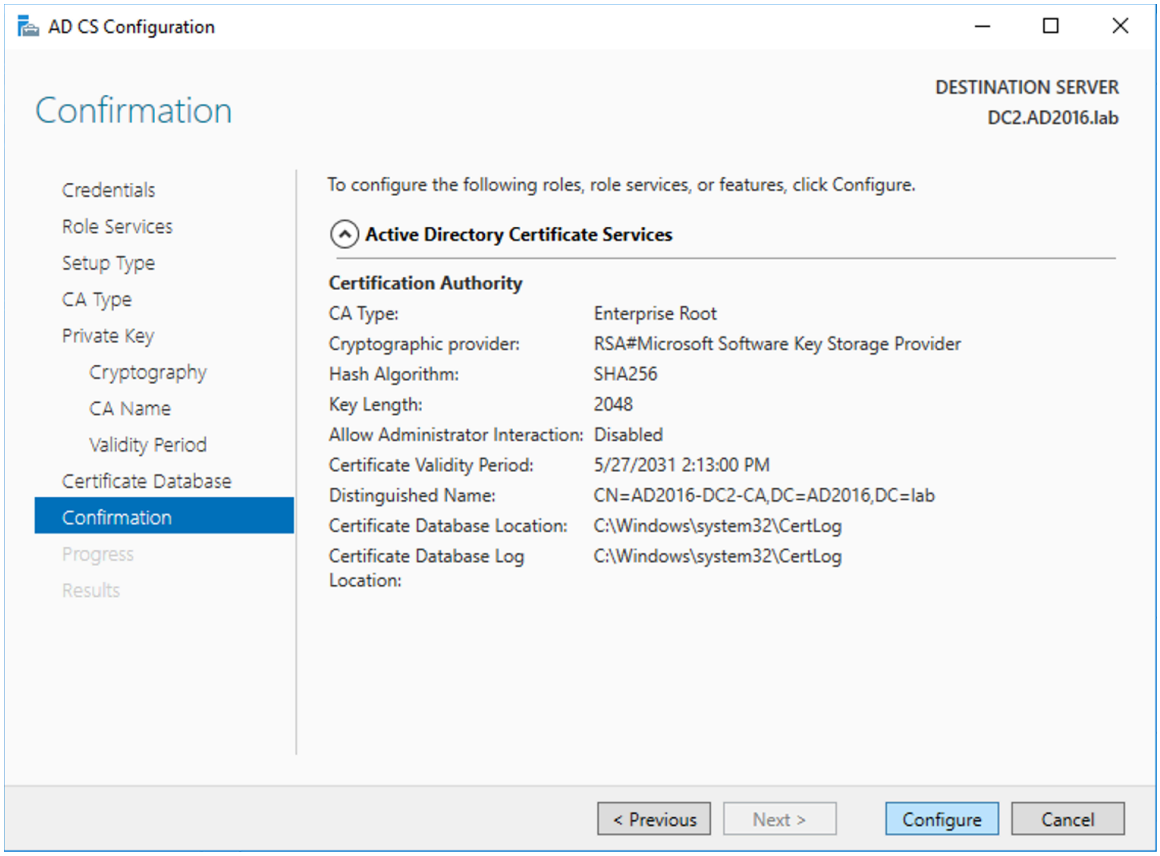
1. Select the validity period of the CA and hit next:



m. Specify the database locations (use default) and hit next:



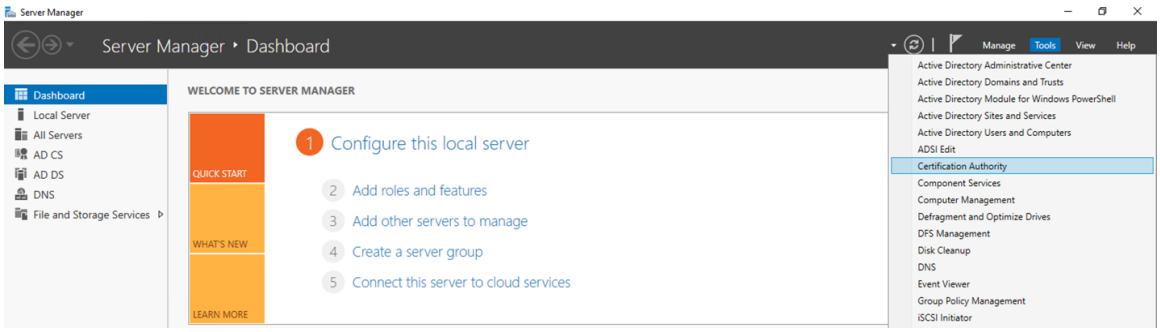
n. Validate configurations and hit *Configure*:



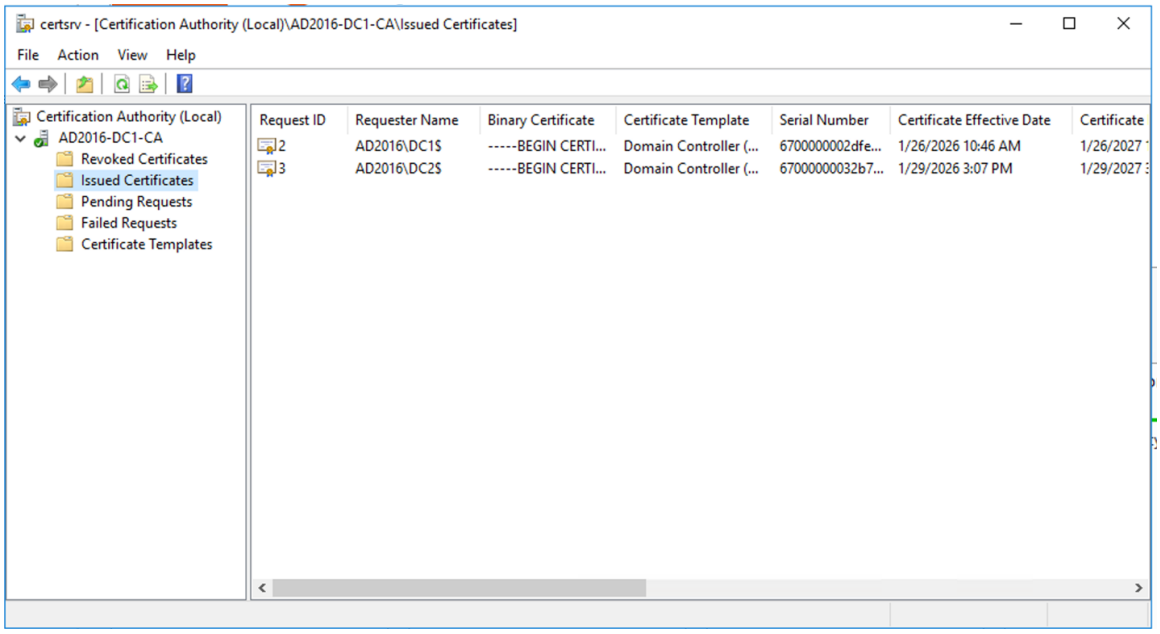
o. Reboot the Windows Server to generate a certificate.

4.VALIDATE CERTIFICATE AND LDAP CONNECTION:

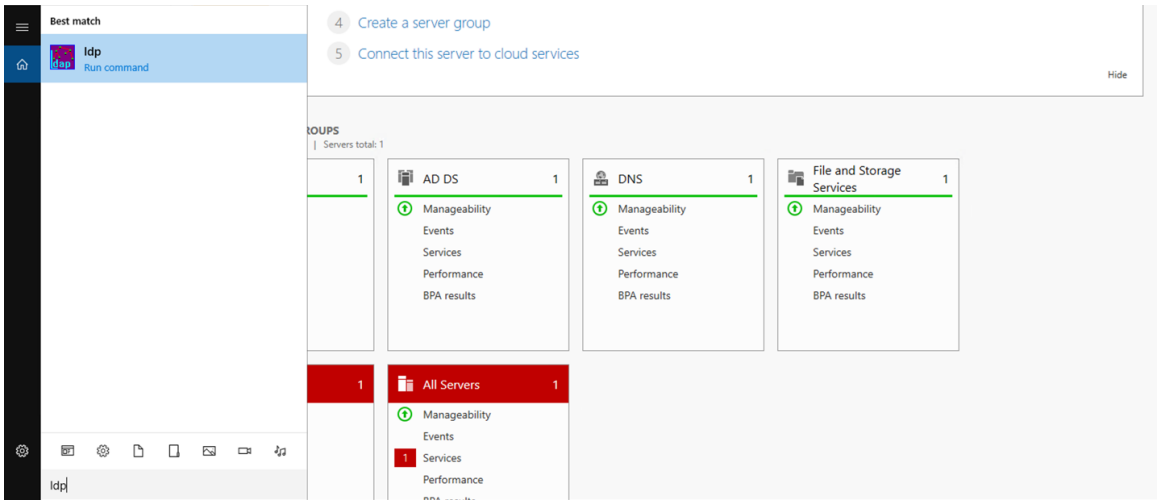
a. Open the *Certification Authority* manager:



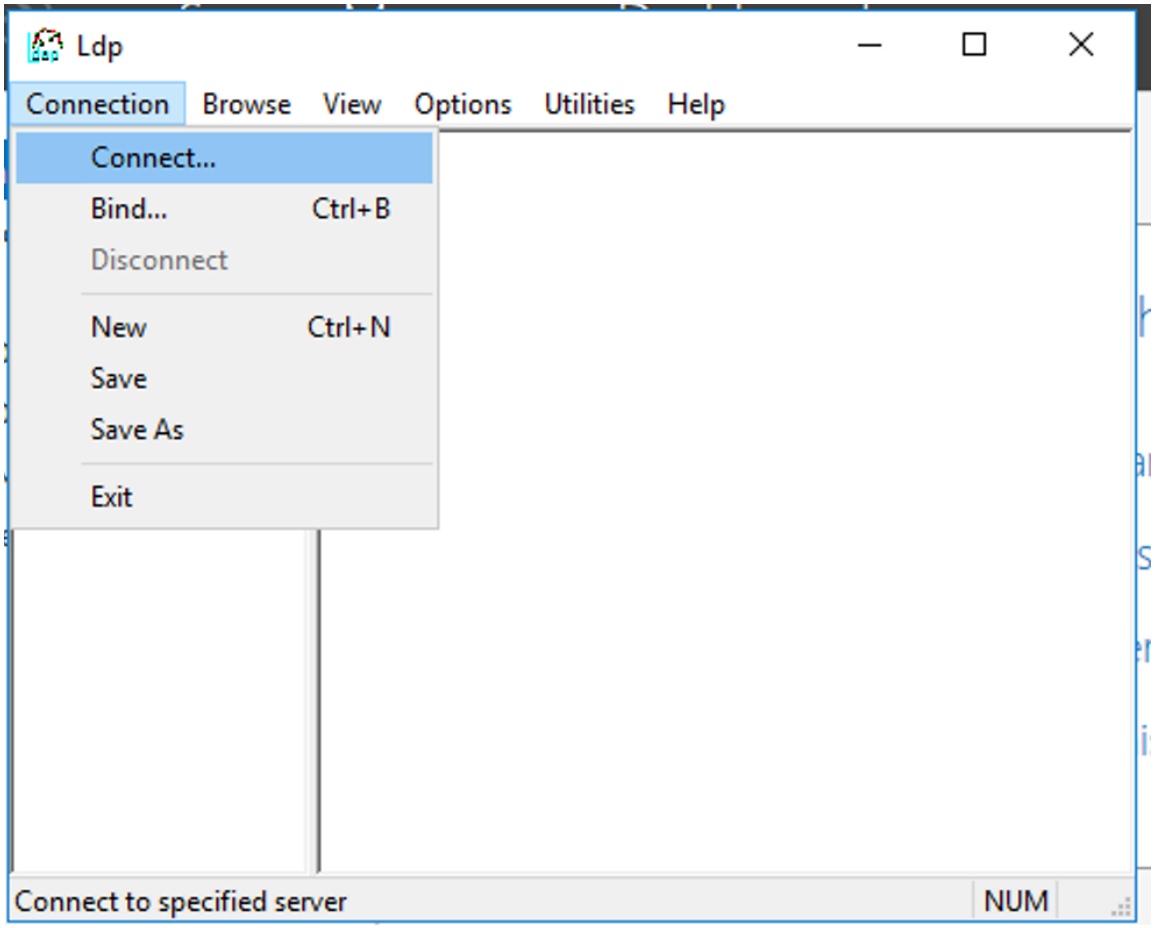
b. Open the *Issued Certificates* folder. There should be one issued certificate to the Domain Controller:



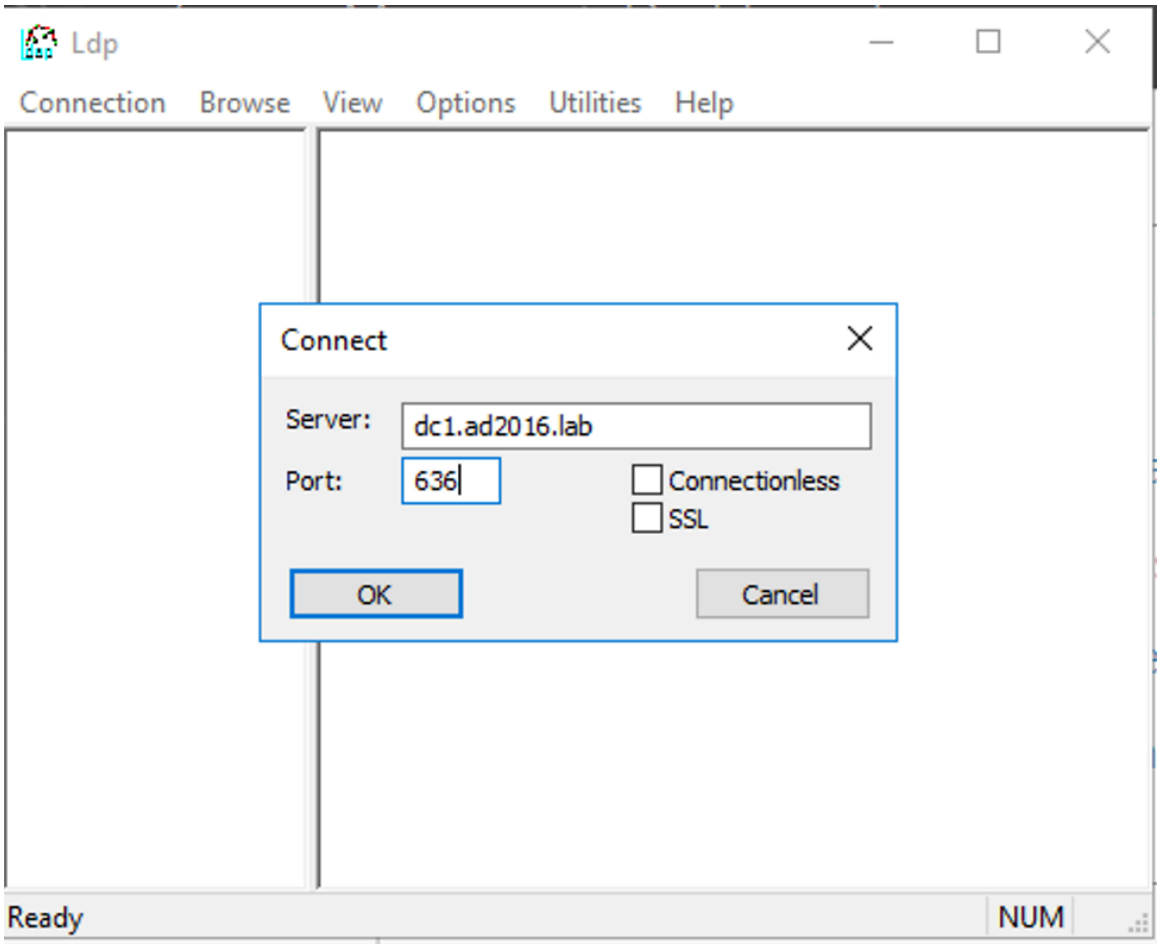
c. Open *ldp* console to test the LDAP connection:



d. Hit *Connection* and *connect*:



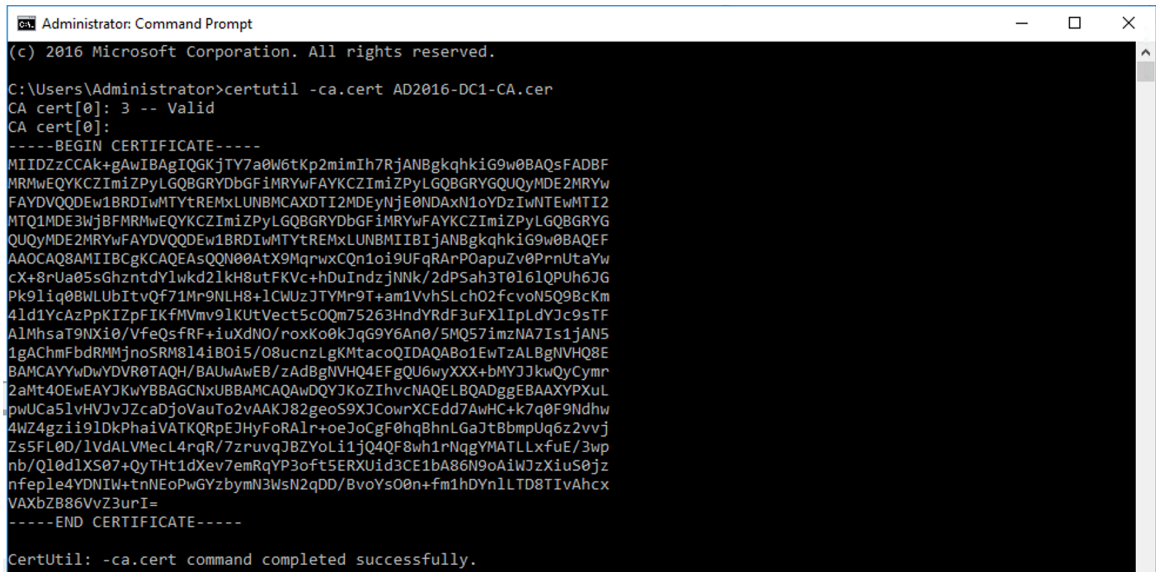
e. Type the server FQDN and type port 636 and hit OK:



f. Confirm the connection is established:

5. GET THE CERTIFICATE USING CMD (COMMAND PROMPT) – METHOD 1:

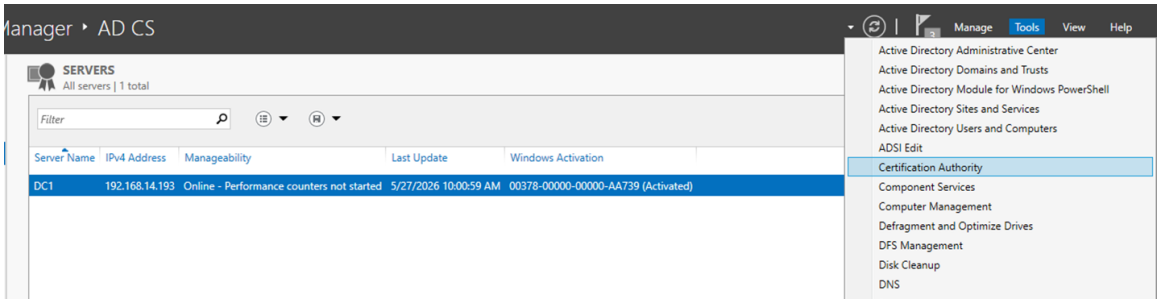
a. Open CMD and enter the certutil -ca.cert [certificate name}.cer



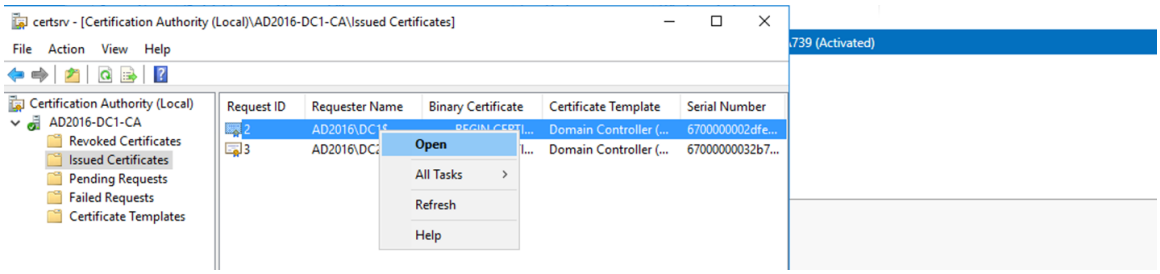
b. Copy and save the certificate plain text for later for the NASlord LDAP authentication services configuration.

6. GET THE CERTIFICATE USING AD CS AND CERTIFICATE EXPORT – METHOD 2:

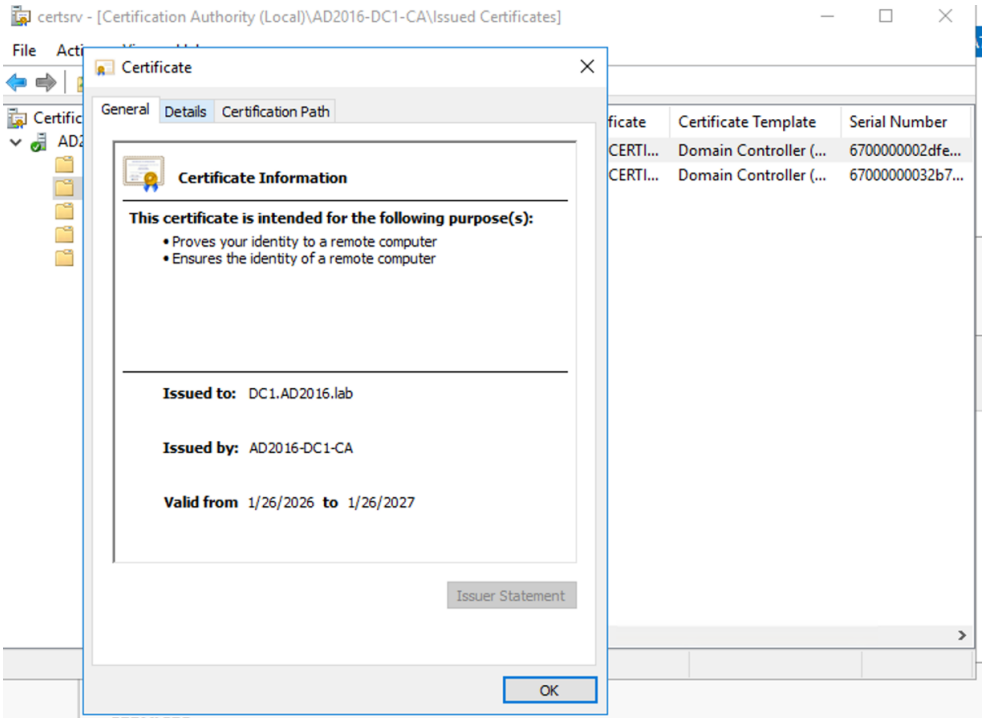
a. Go to *Certification Authority*:



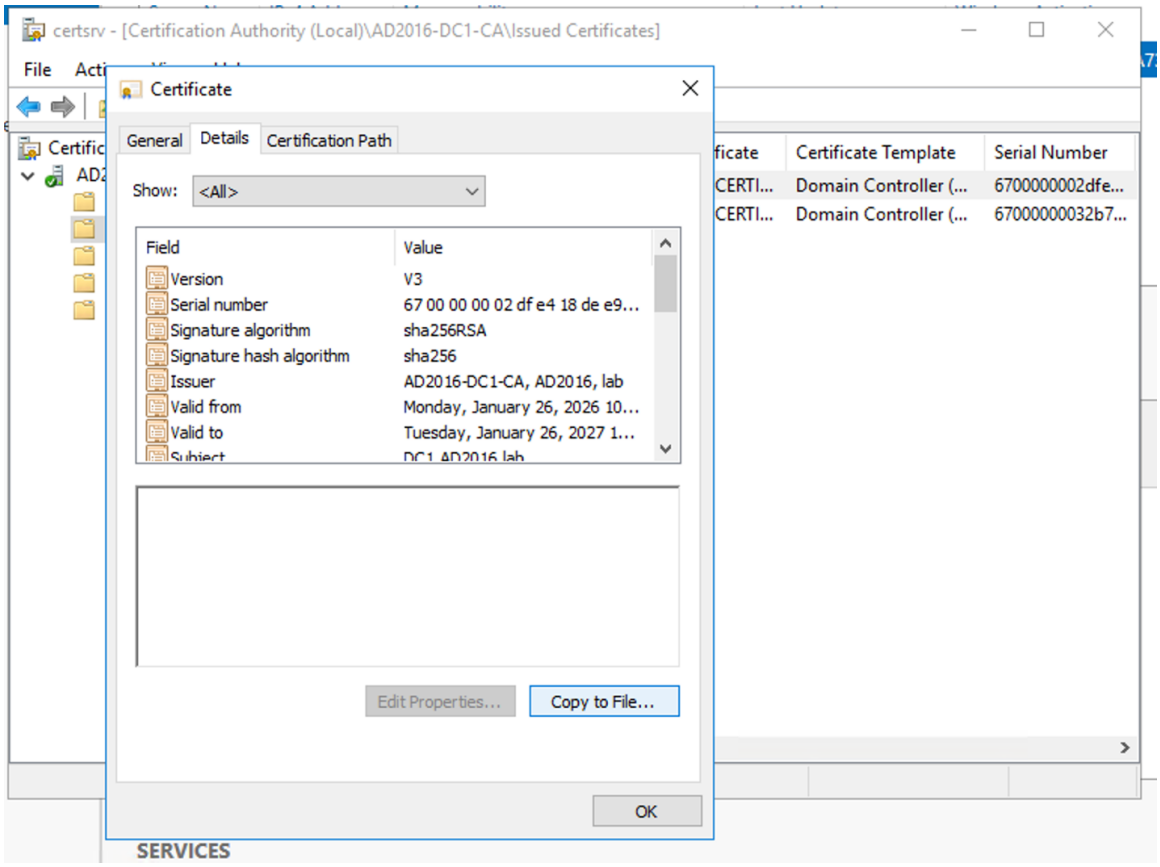
b. Pull down the CA instance, hit *Issued Certificates*, right-click on the first issued Certificate and hit Open:



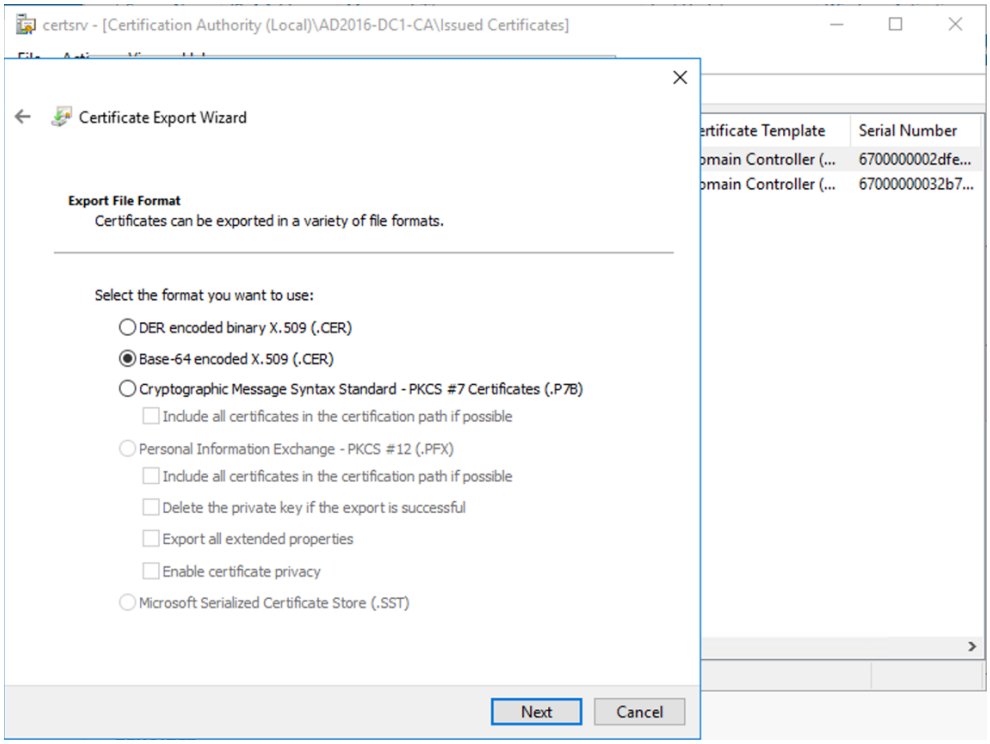
a. Hit *details:*



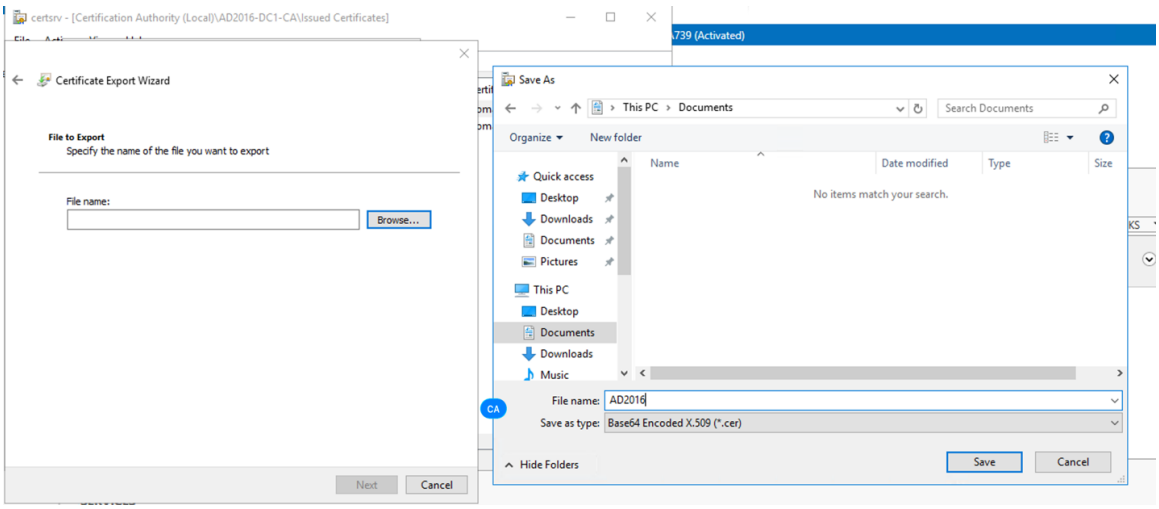
c. Hit *Copy to File…*:



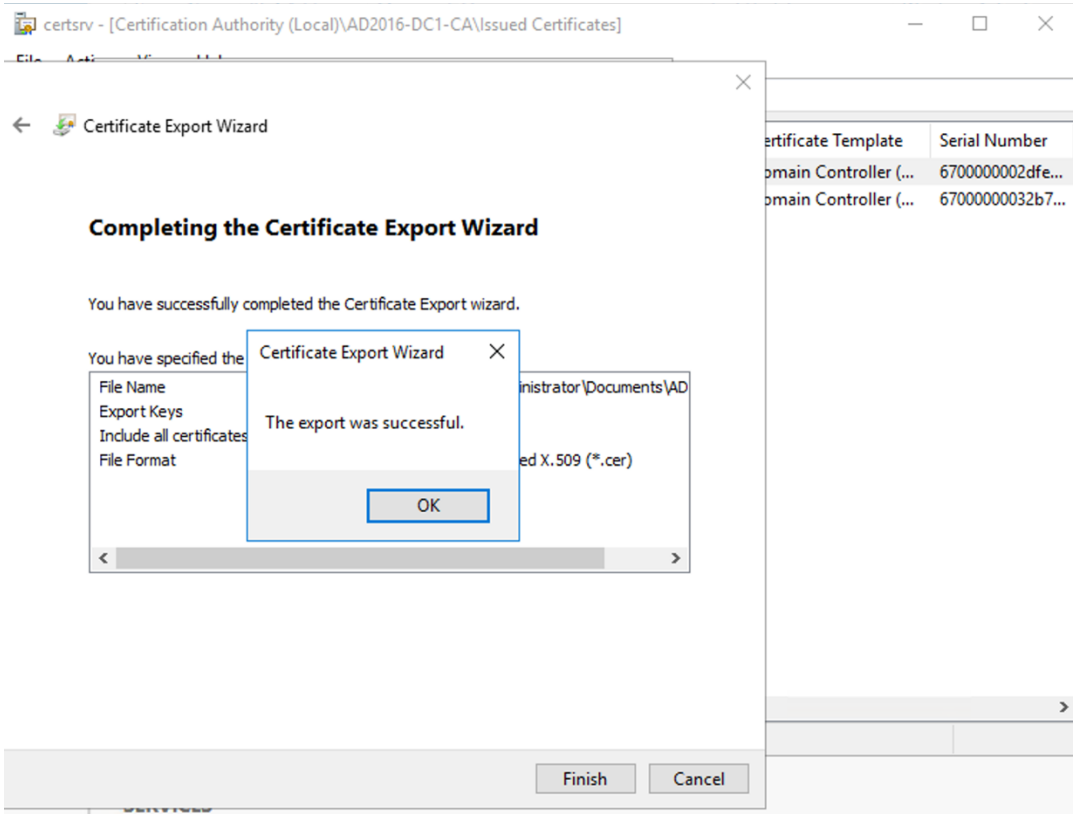
d. Choose *Base-64 encoded X.509* certificate:



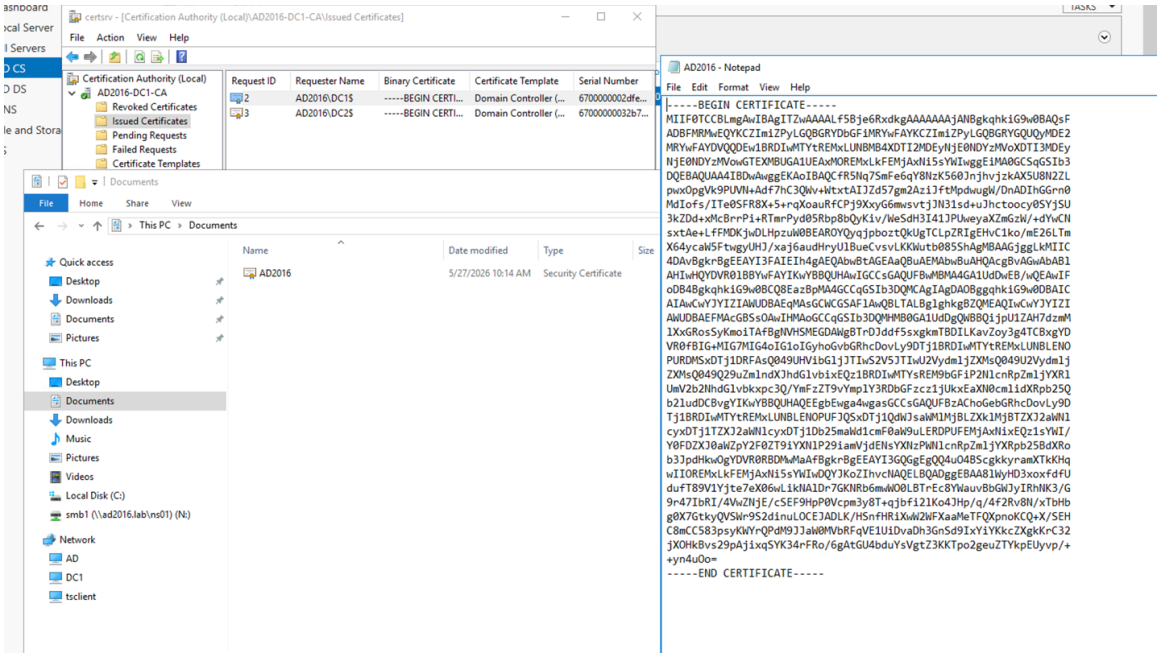
e. Hit *Browse*, name and save the certificate:



f. Hit *next* until the end of the Wizard and hit *Finish*:



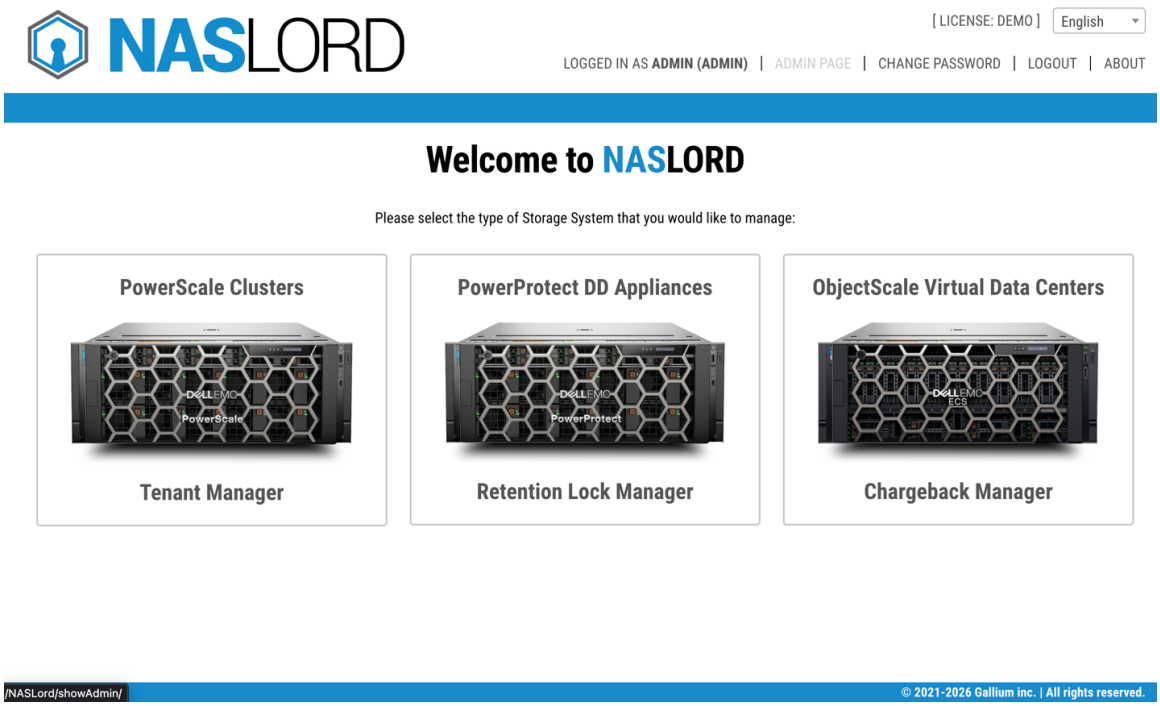
g. Go to the certificate location, right click on the previously saved certificate and choose *open with* > *Notepad*:



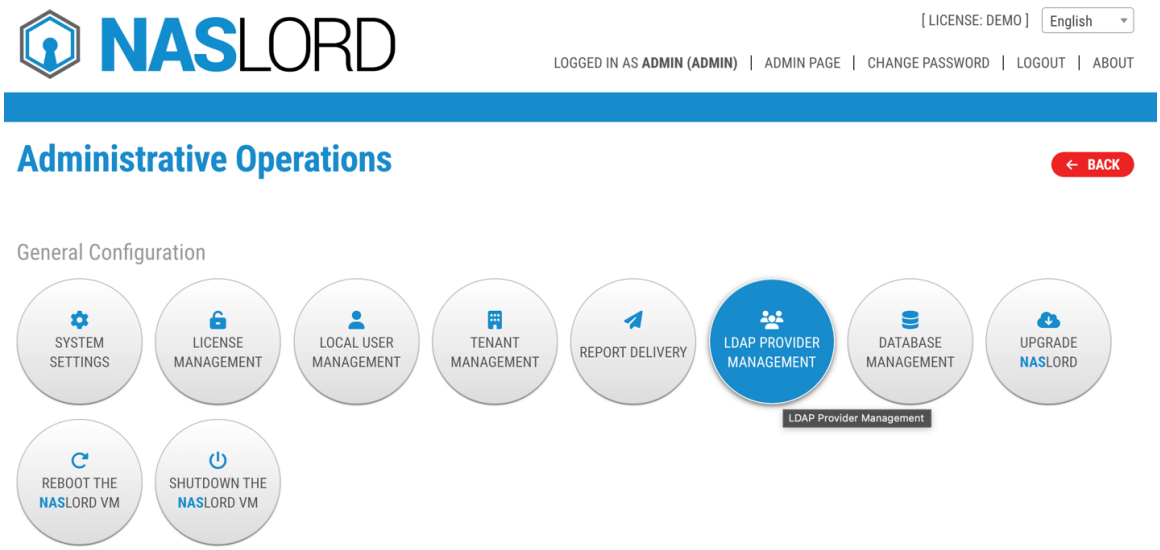
h. Copy and save the certificate plain text for later for the NASlord LDAP authentication services configuration.

7. NASLORD LDAP CONFIGURATION:

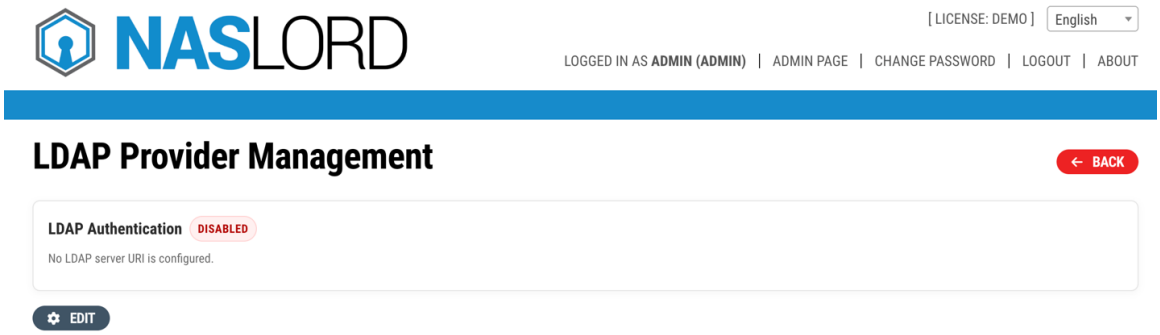
a. Go to *Admin Page*:



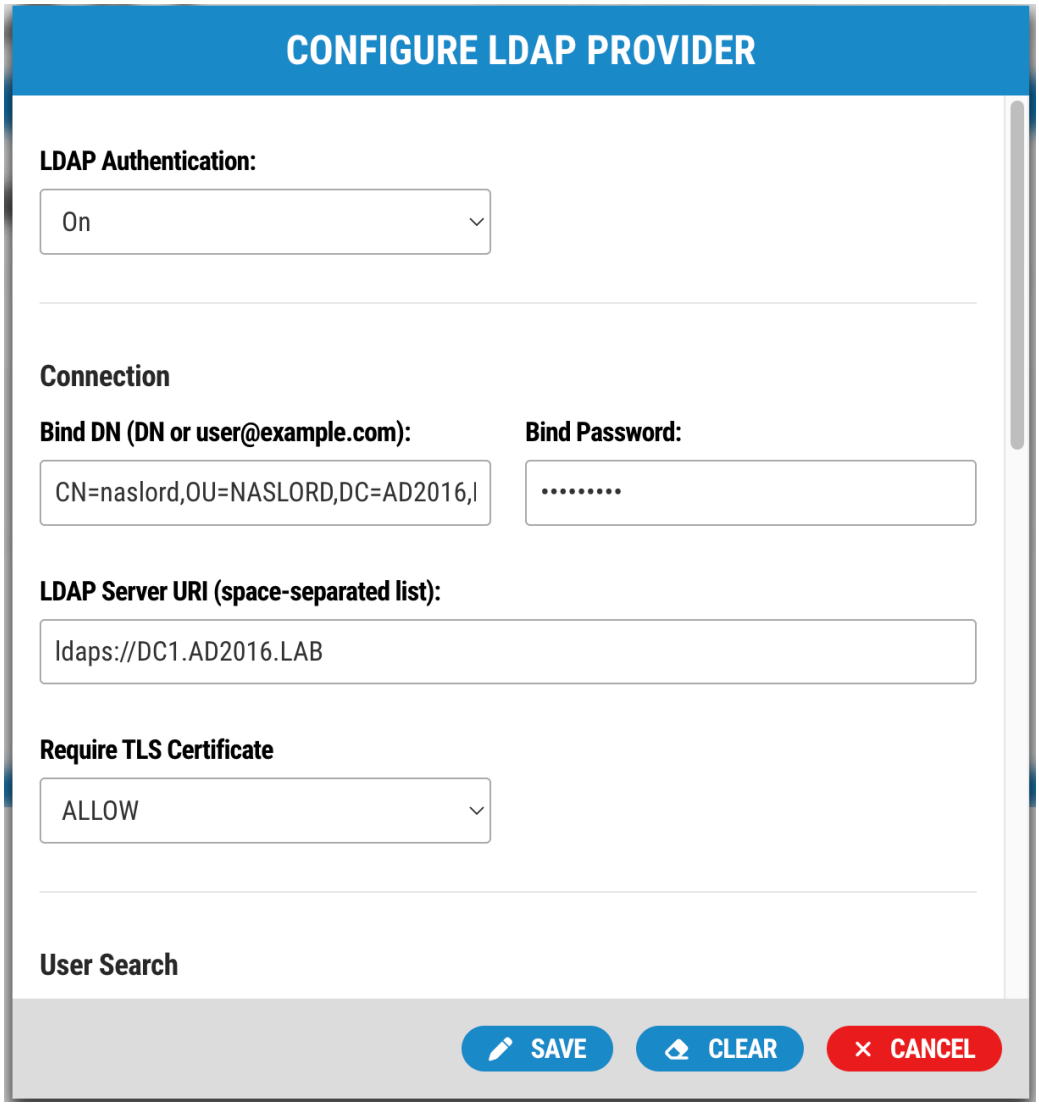
b. Hit *LDAP Provider Management*:

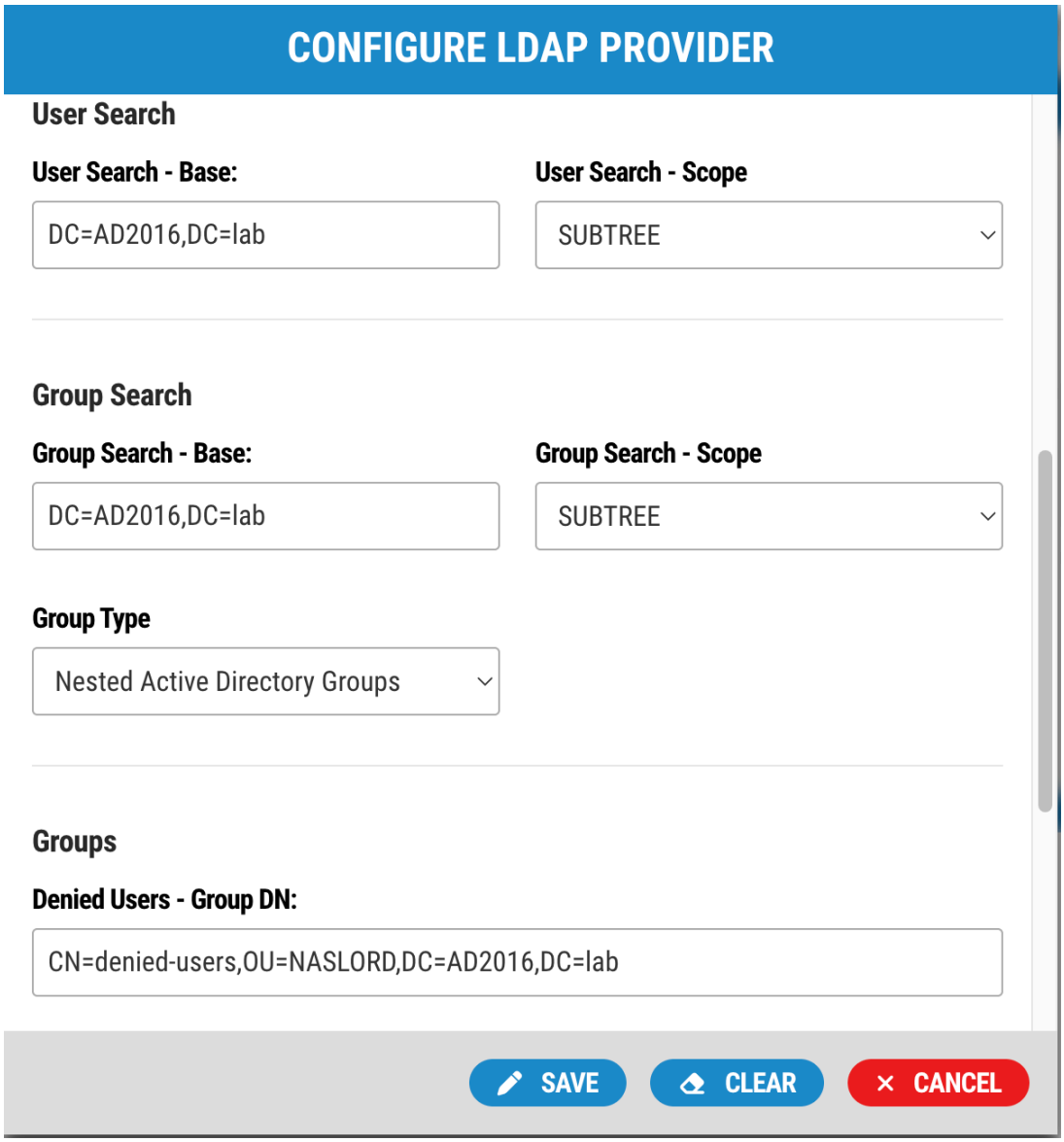


c. Hit *Edit*:

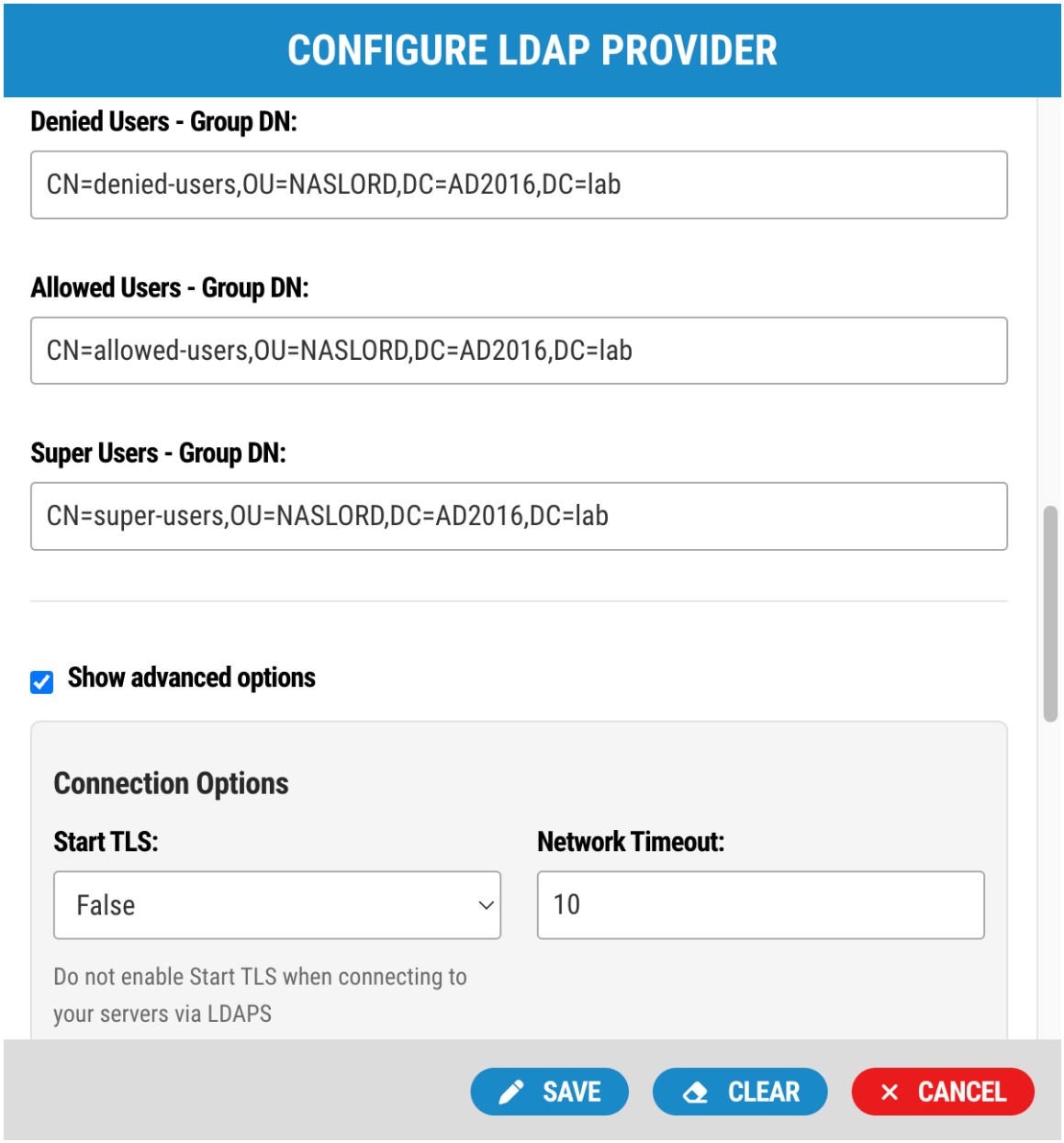


d. Enter the LDAP information using distinguished name form (Under AD user/group attributes) saved previously:

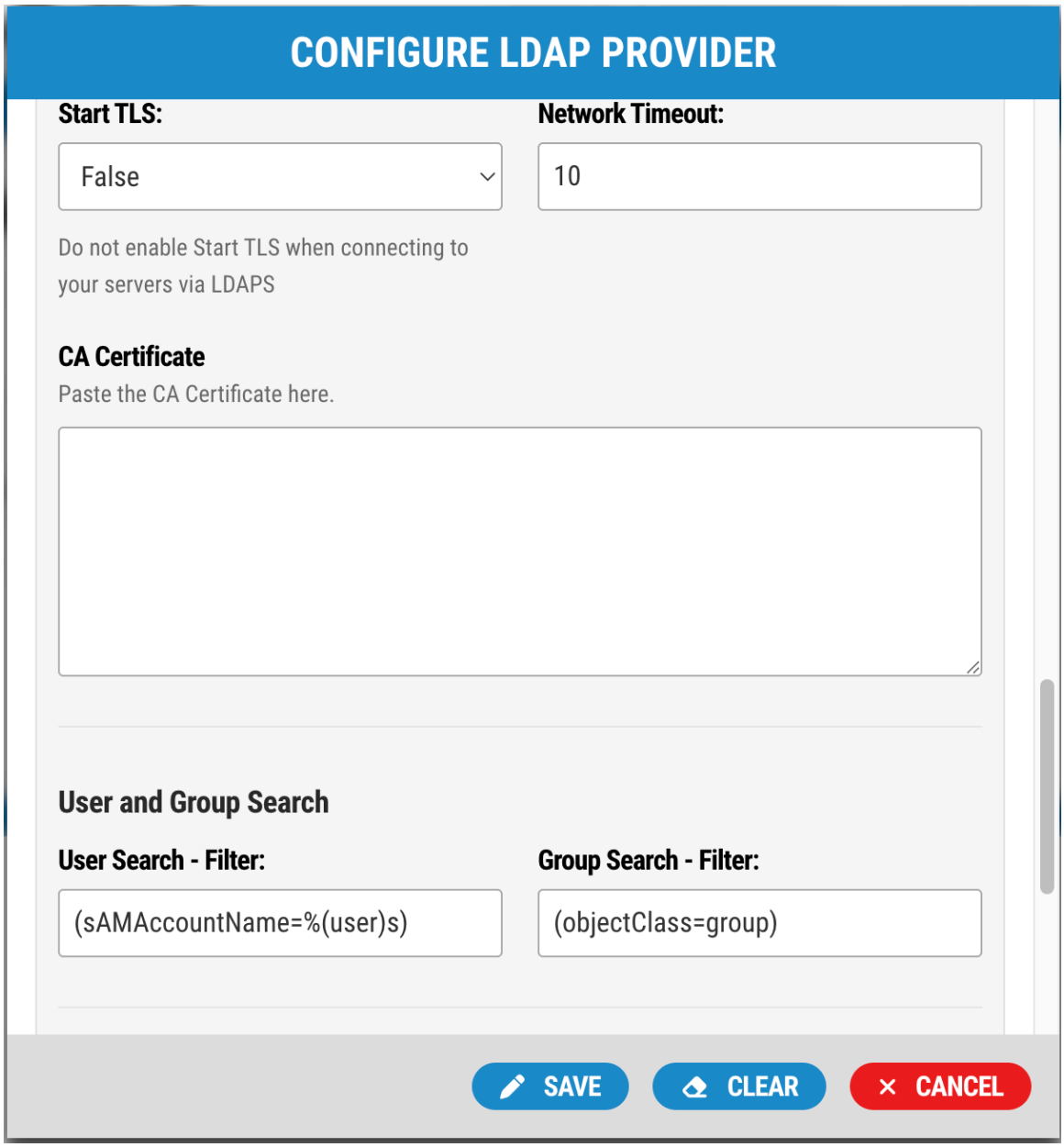



CONFIGURE LDAP PROVIDER
User Search
User Search - Base:
DC=AD2016,DC=lab
User Search - Scope
SUBTREE
Group Search
Group Search - Base:
DC=AD2016,DC=lab
Group Search - Scope
SUBTREE
Group Type
Nested Active Directory Groups
Groups
Denied Users - Group DN:
CN=denied-users,OU=NASLORD,DC=AD2016,DC=lab
SAVE
CLEAR
CANCEL

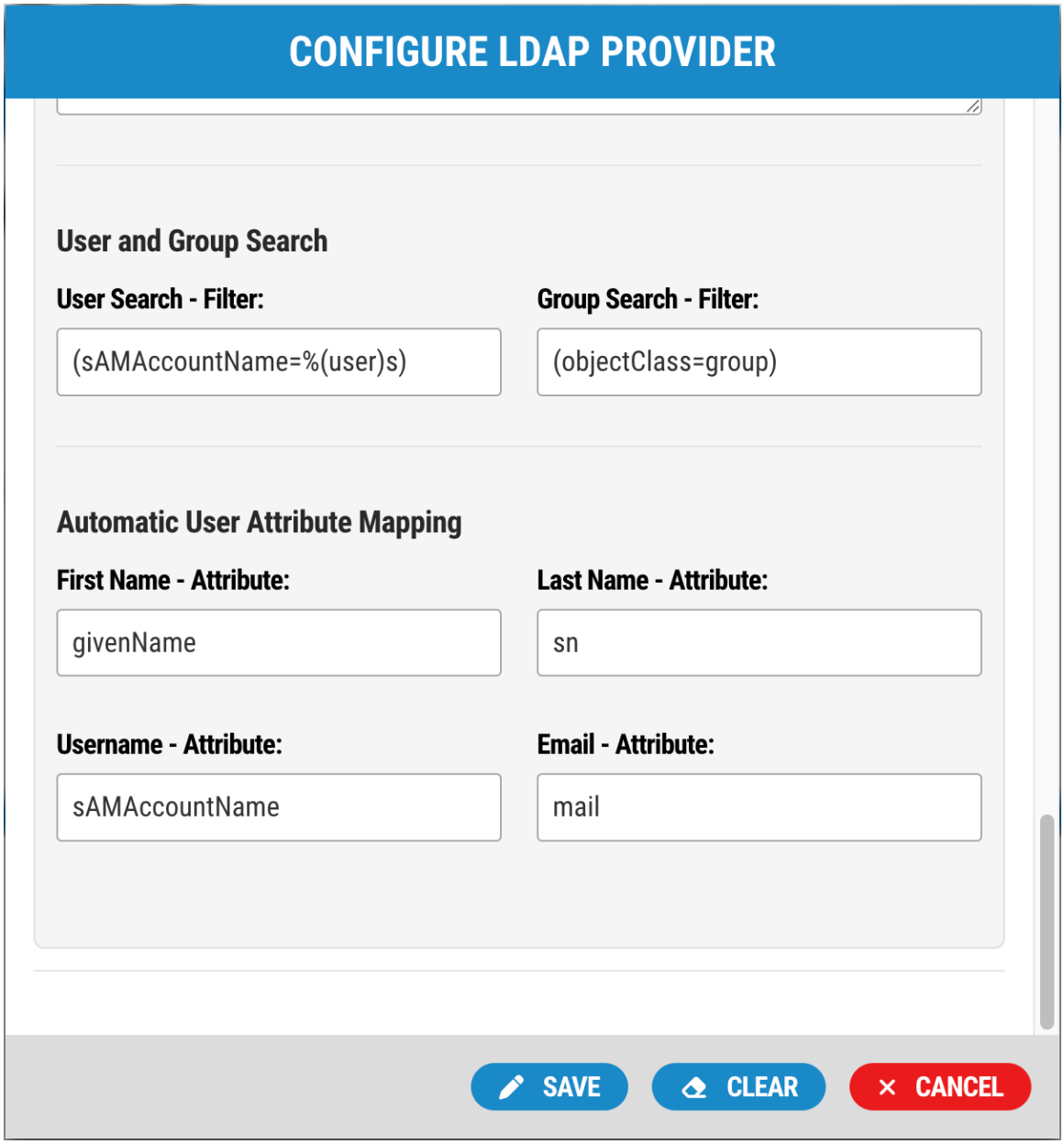
e. Check the *Show advanced options* box. Leave *Start TLS* to *False* and scroll further down:



f. Copy the CA Certificate plain text previously saved from the AD:



g. We recommend to leave these options to default unless you need to customize them. Hit *Save* once the configuration is completed:



h. Confirm the connection and bind are successful: