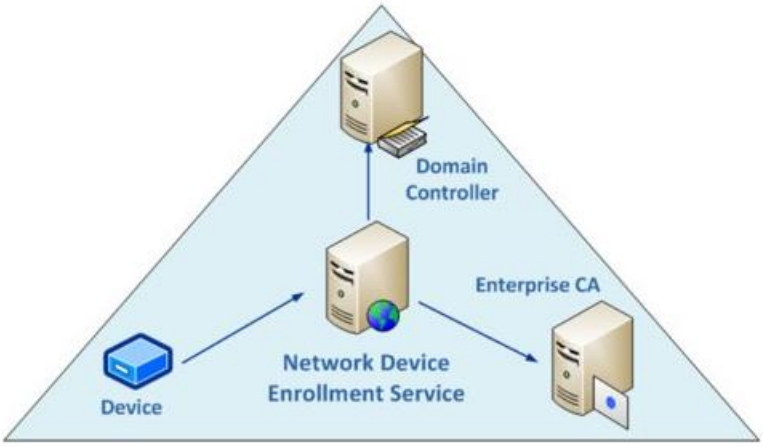
Network Device Enrollment Service (NDES) Installation Guide

Contents

Network Device Enrollment Service (NDES)

Network Device Enrollment Service (NDES) – Microsoft's implementation of SCEP



Prerequisites

The following are the prerequisites to install NDES server.

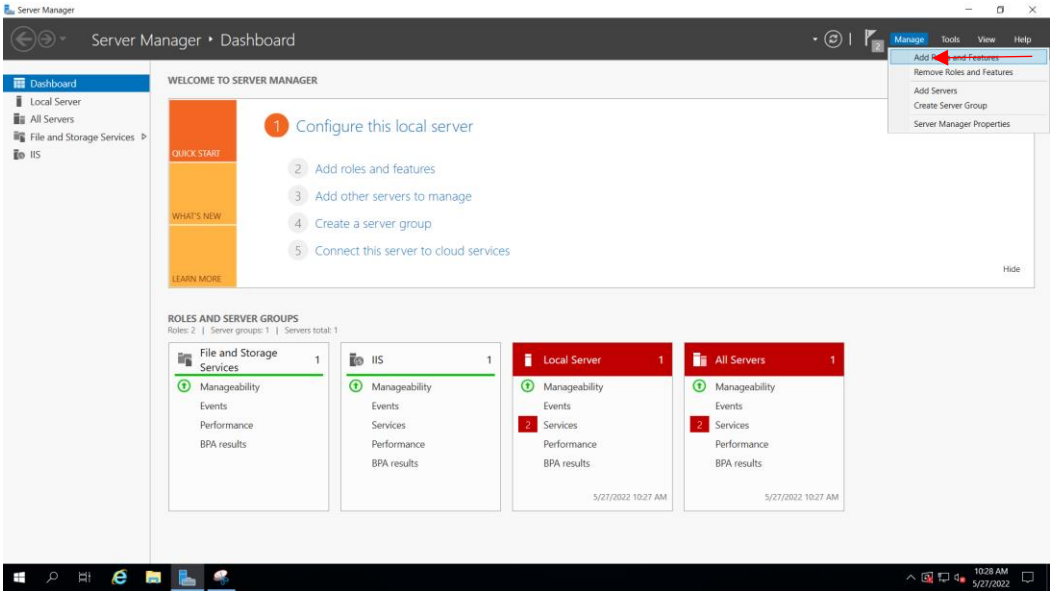
- A service account for NDES server
  - New user to be created (Example: ndesadmin@[redacted].com)
  - Must be a domain user account
  - Must be a member of local IIS_IUSRS group
- Admin user credentials with Enterprise administrator privileges and local administrator privileges to the server where NDES will be installed (i.e. in dev-m[redacted]x.com)

Configuring NDES

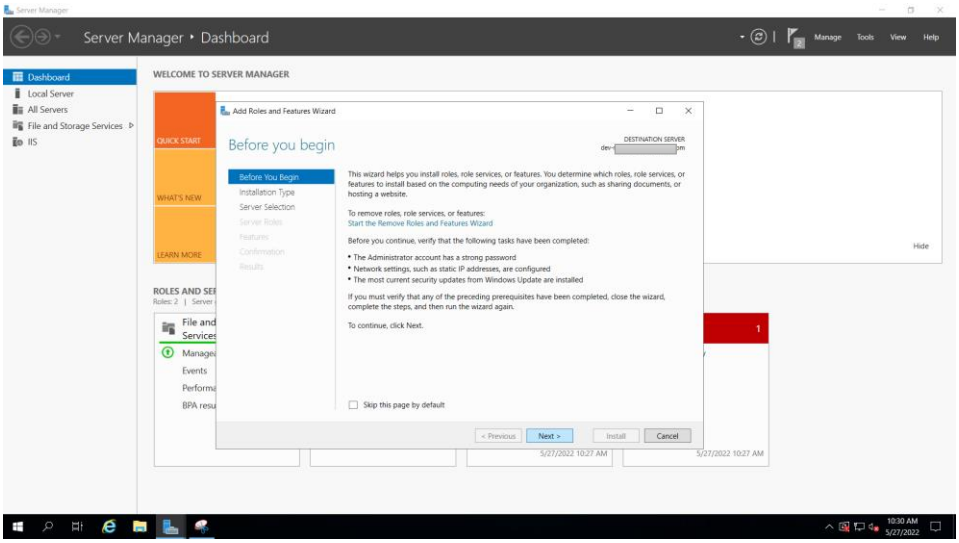
To configure NDES, complete the following steps:

Step 1: Deploy Active Directory Certificate services

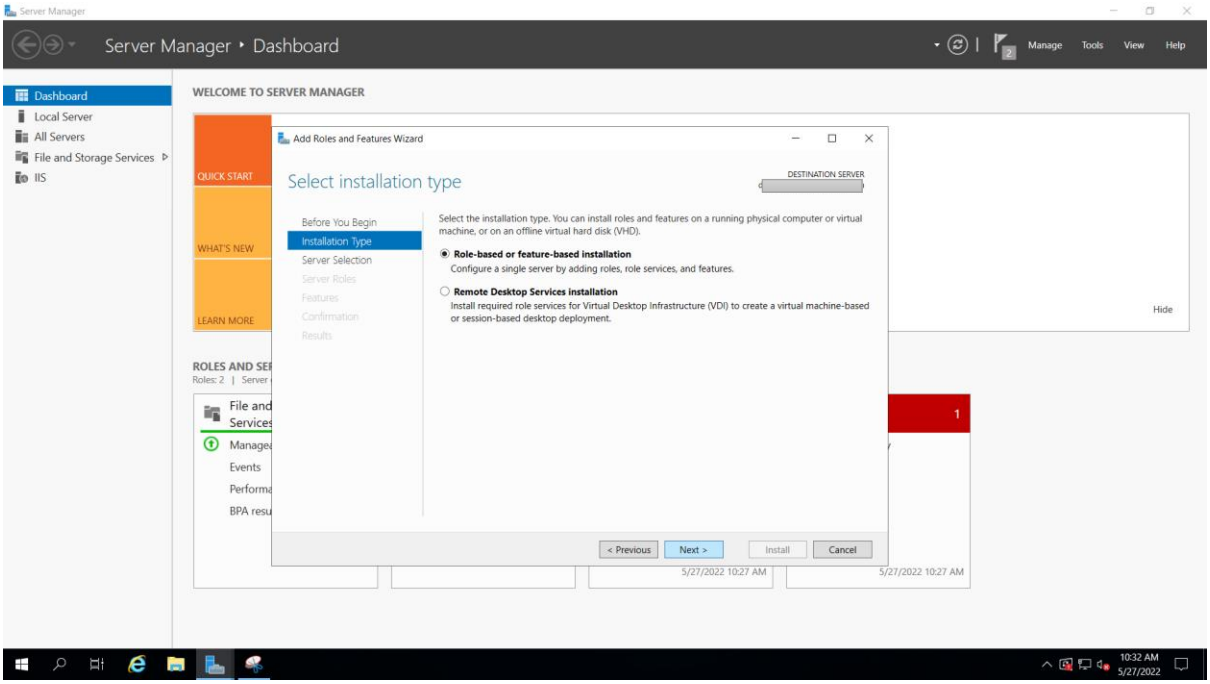
1. From Microsoft Windows Server Manager dashboard, click **Manage** and select **Add Roles and Features**.



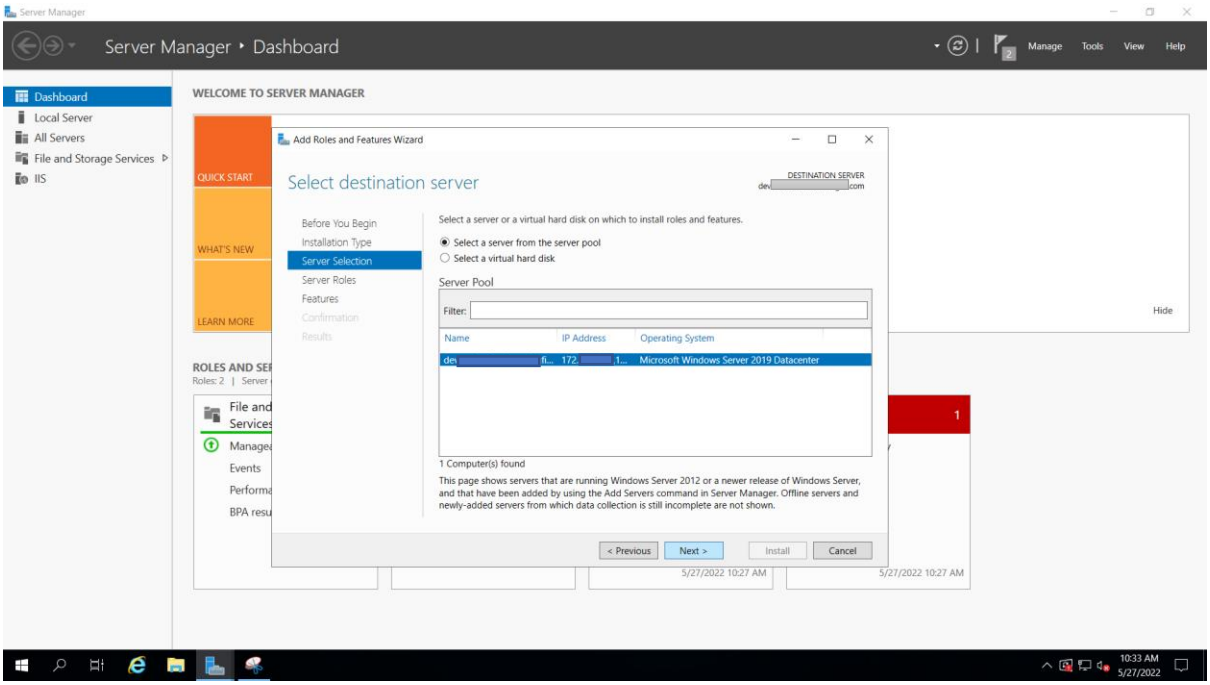
2. Read the content in the **Before You Begin** page and click **Next**.



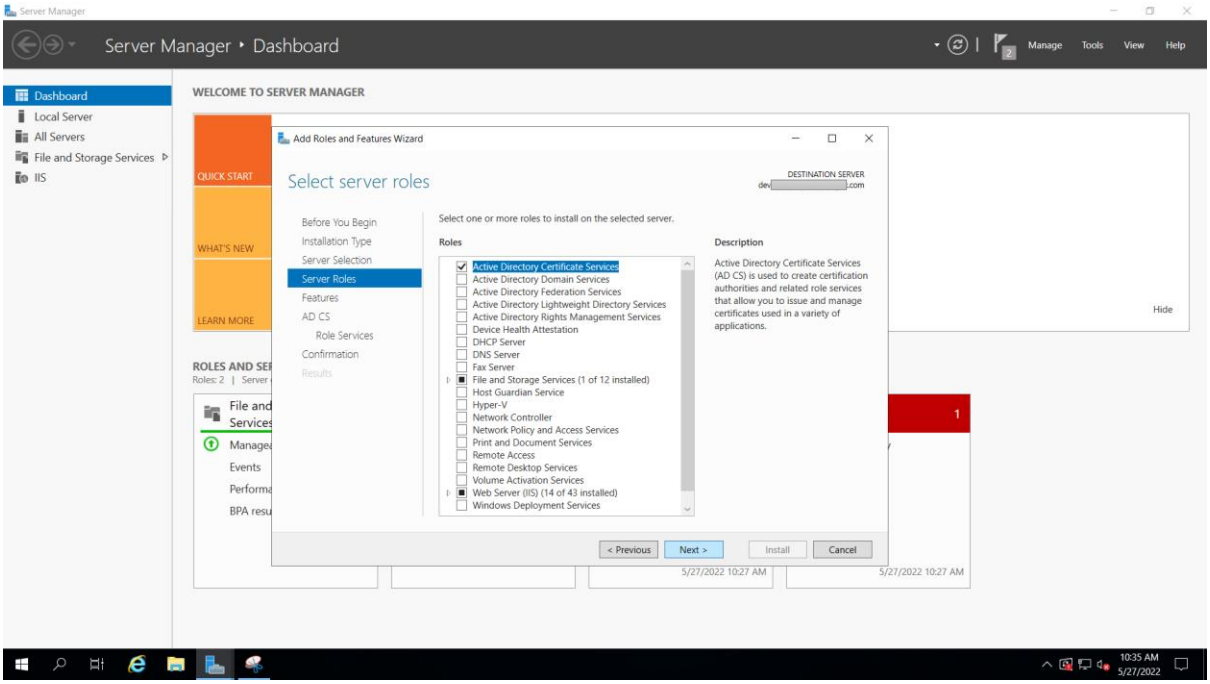
3. For **Installation Type**, select ‘Role-based or feature-based installation’ and click **Next**.



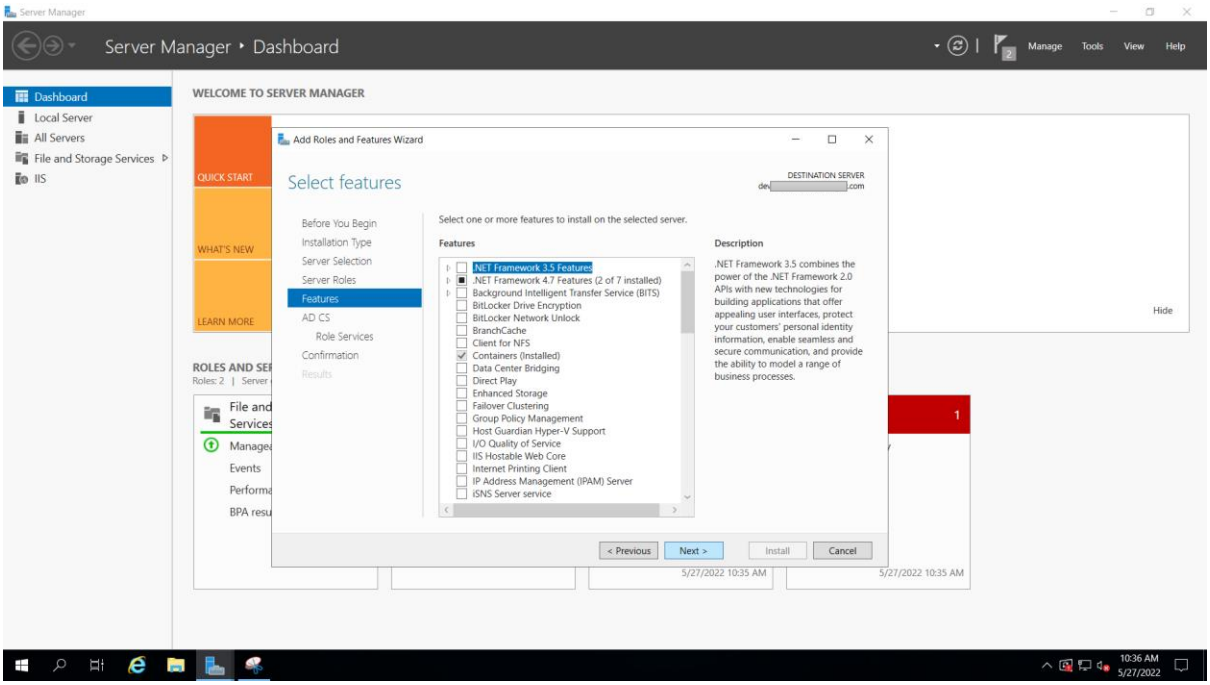
4. In the **Server Selection** section, retain the defaults and click **Next**.



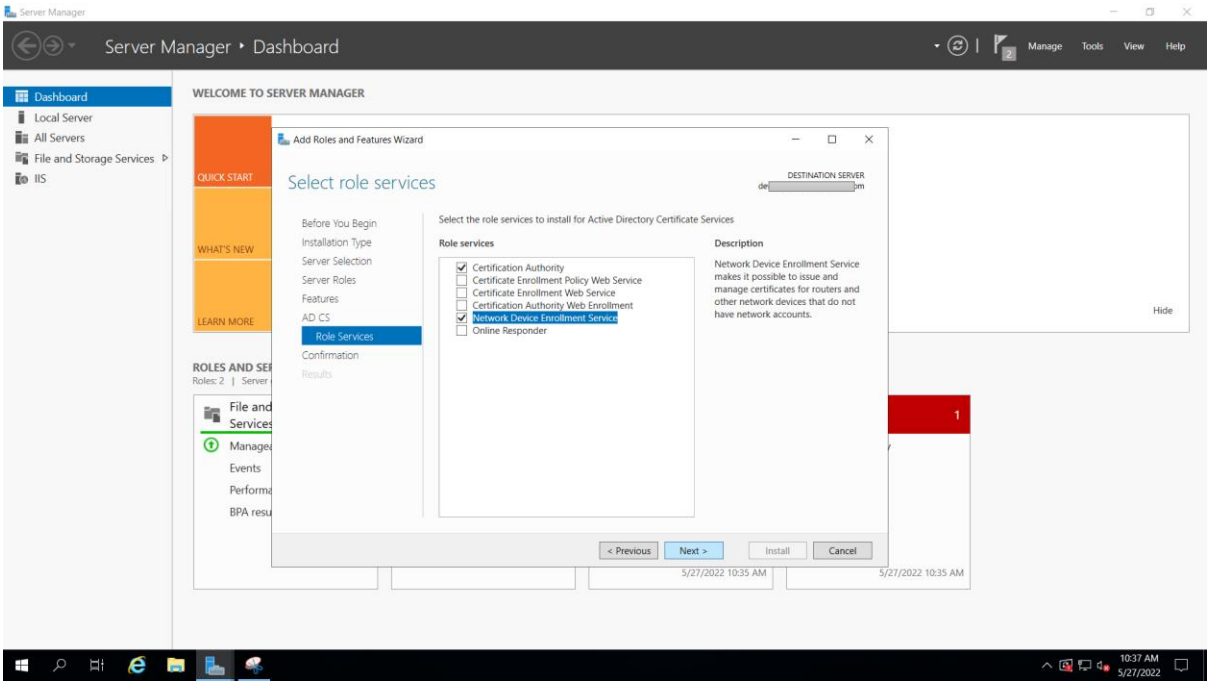
5. In the **Server Roles** section, select ‘Active Directory Certificate Services’ and click **Next**.



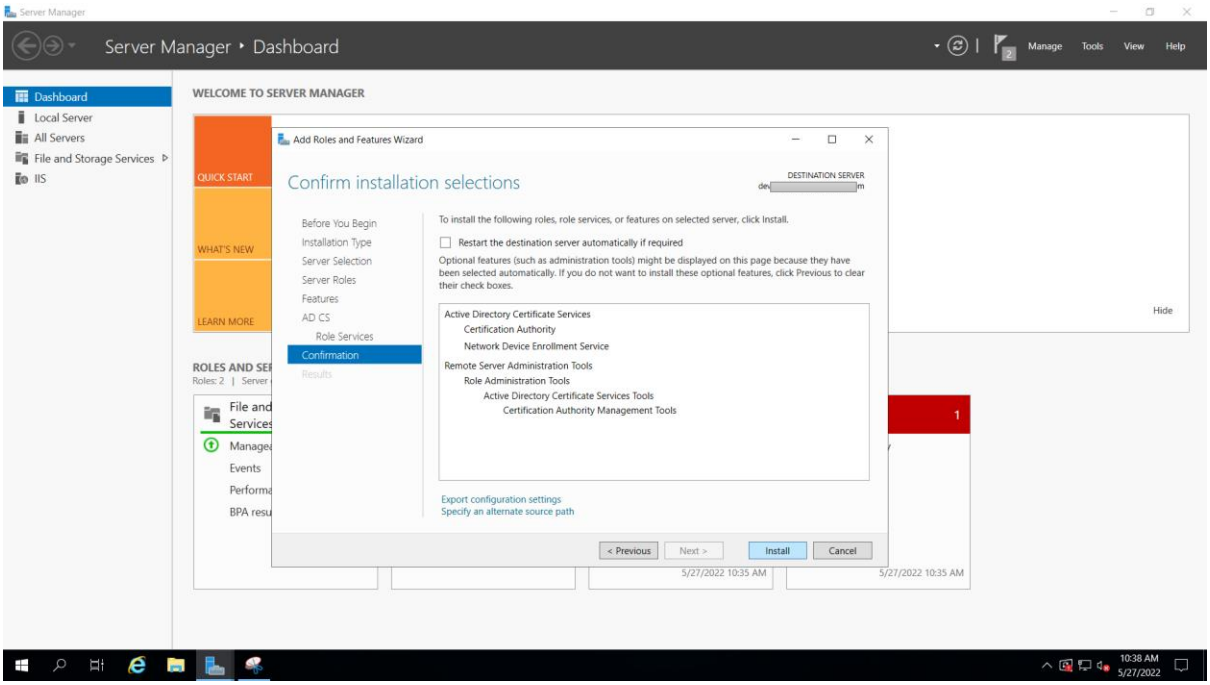
6. In the **Features** section, retain the defaults and click **Next**.



7. In the **AD CS** section, click Next. From **Role Services**, select ‘Certificate Authority’ and ‘Network Device Enrollment Services’ and click **Next**.

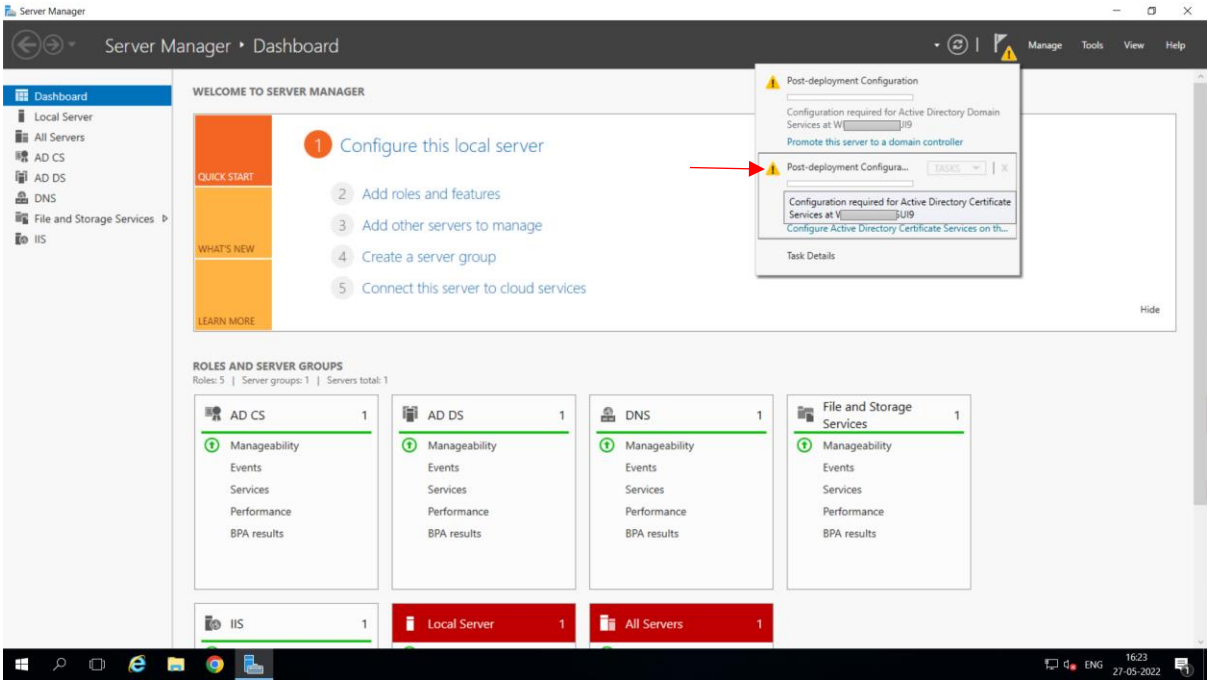


8. In the **Confirmation** section, read and verify the information and click **Install.**

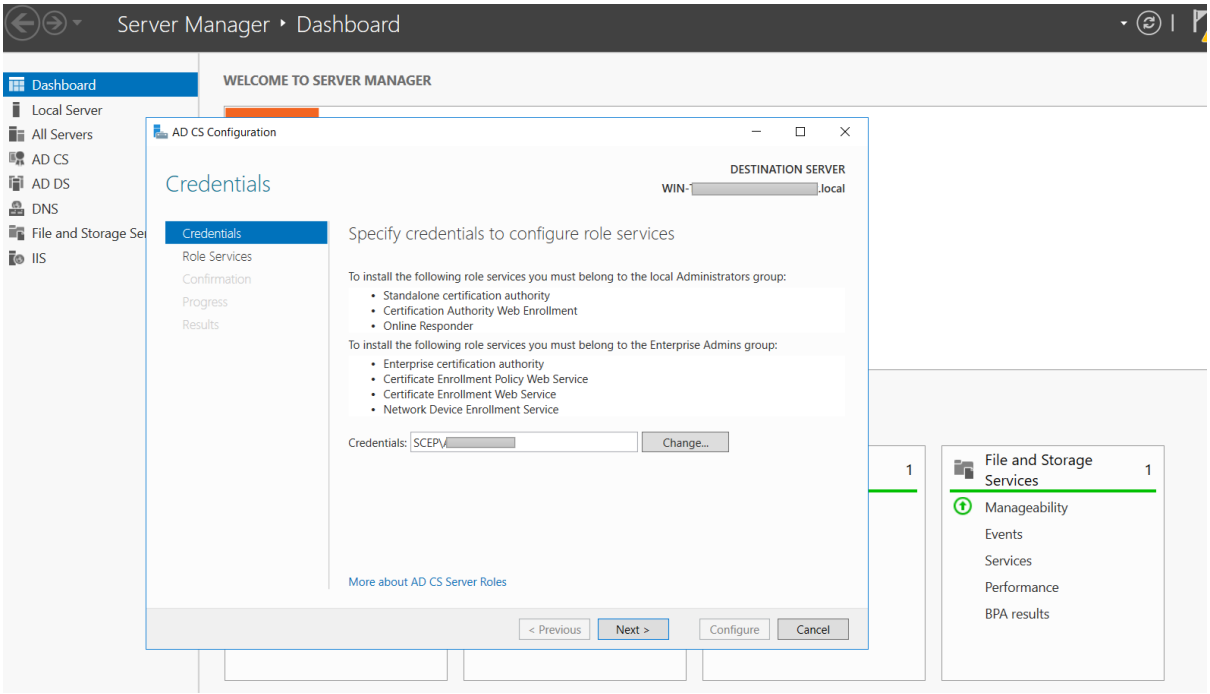


Step 2: Configure Active Directory Certificate services

1. To configure Active Directory Certificate Services, from the Server Manager Dashboard, click  and select **Post-deployment Configuration**.

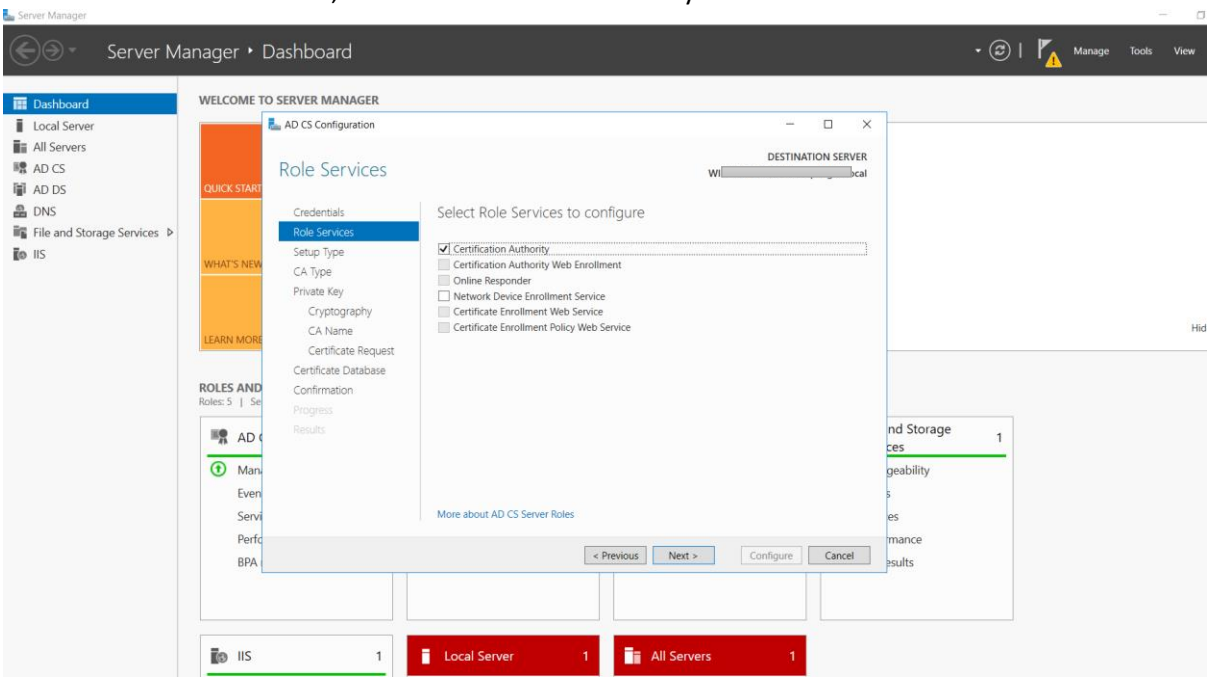


2. Under ROLES AND ERVER GROUPS, select AD CS. In the **Credentials** section, enter the Server Manager Administrator credentials, and click **Next**.

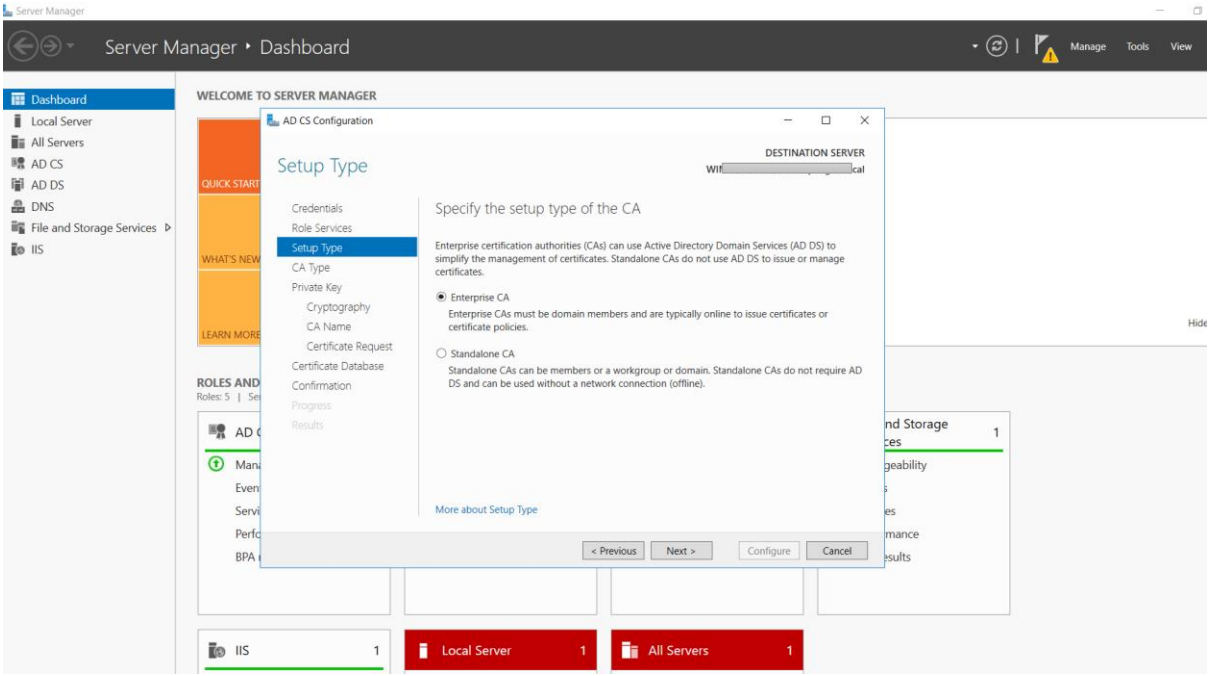


Step 2a: Configure Certification Authority

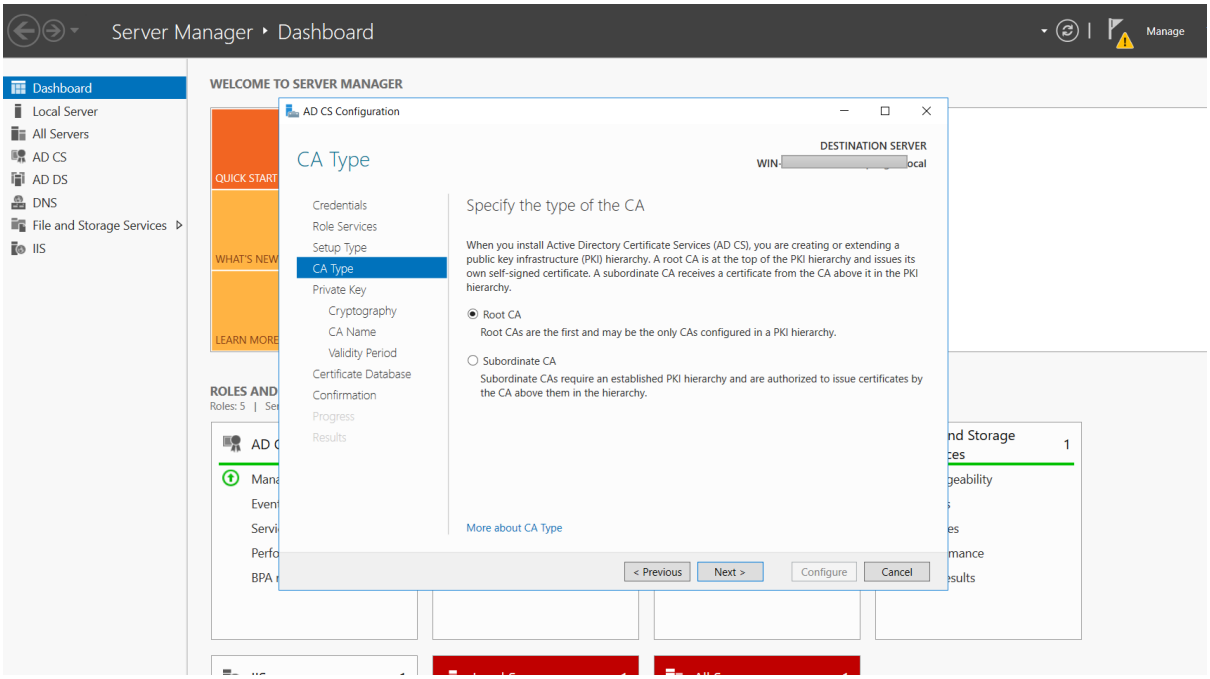
1. In the **Role Services** section, select ‘Certification Authority’ and click **Next**.



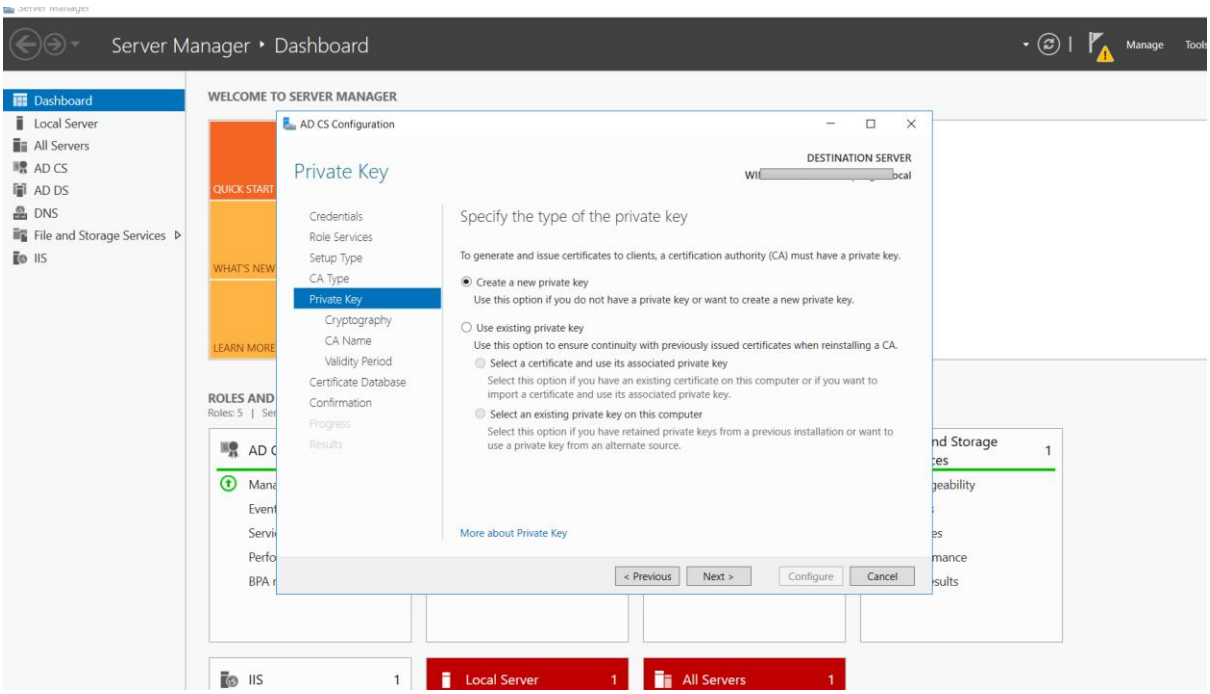
2. For Setup Type, select ‘Enterprise CA’ and click **Next**.



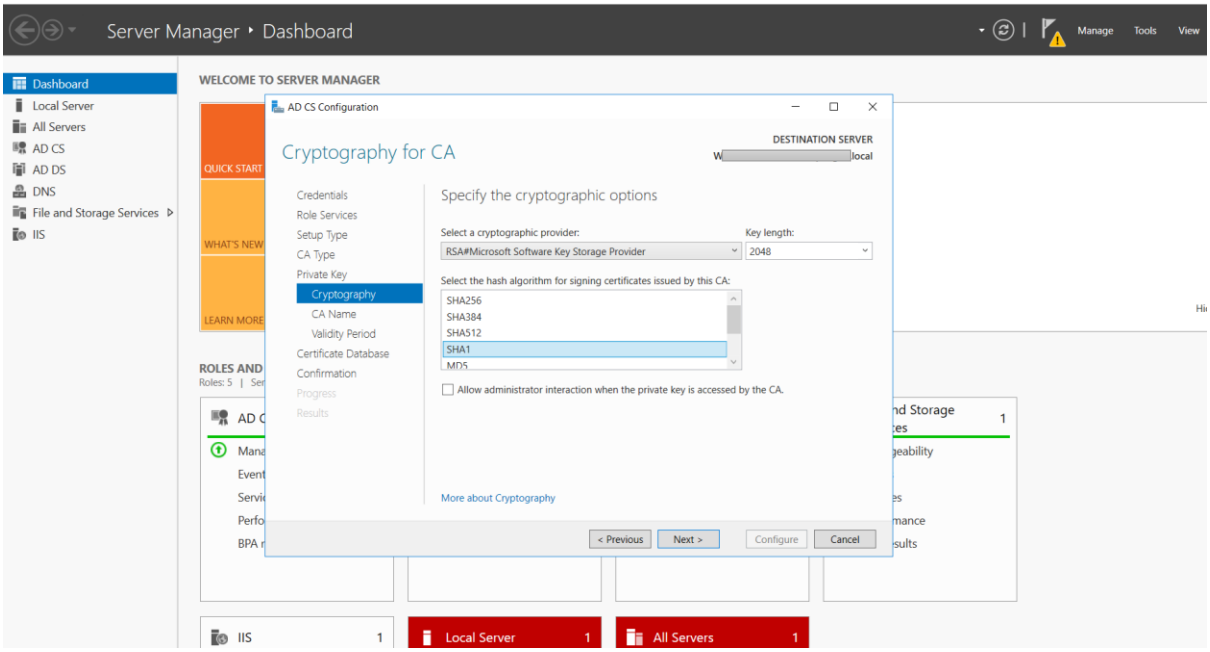
3. For **CA Type**, select ‘Root CA’ and click **Next**.



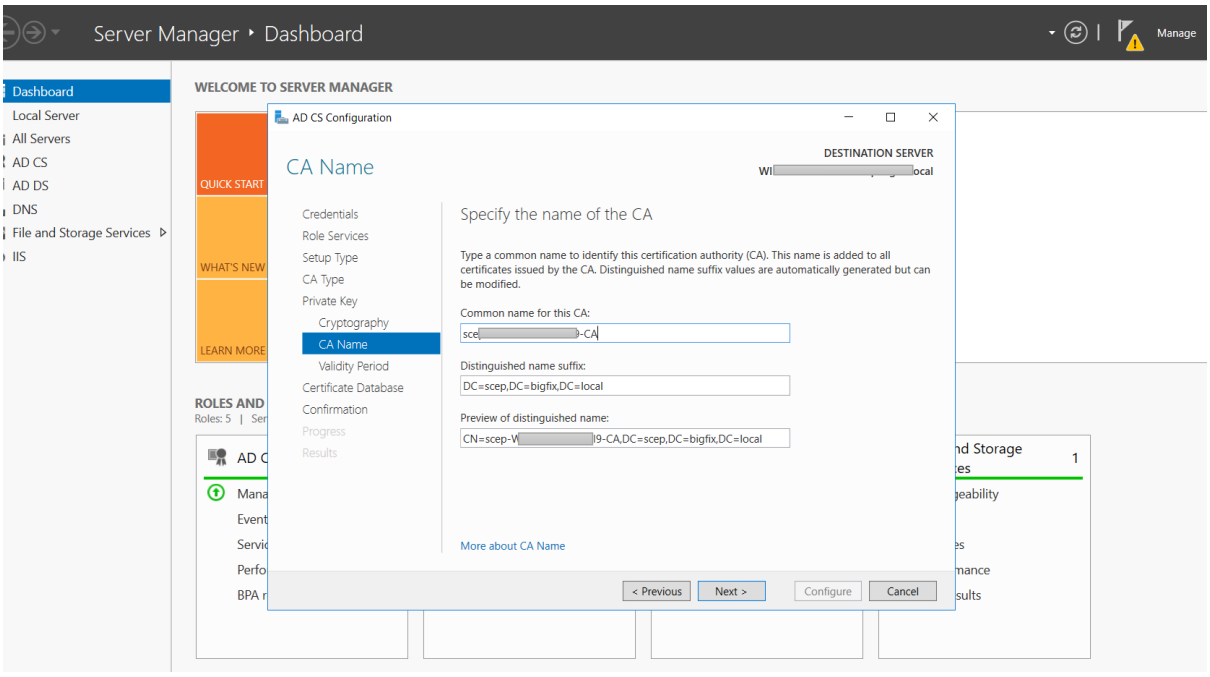
4. For **Private Key**, select ‘Create a new private key’ option and click Next.



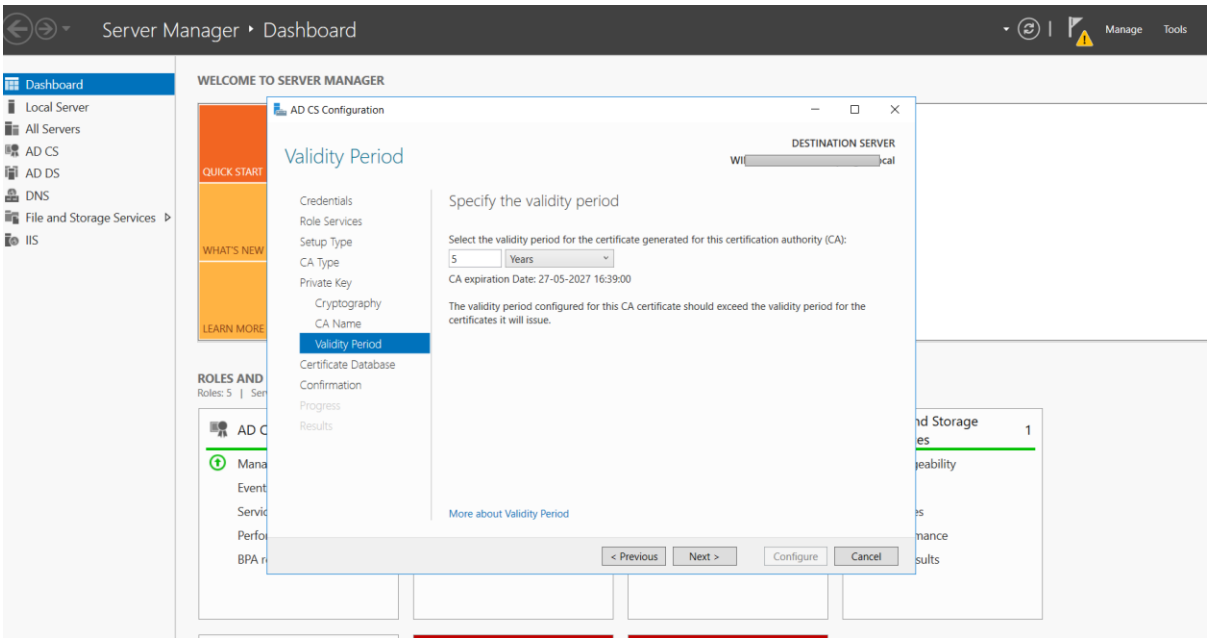
5. **Cryptography**: Specify the cryptographic options as required and click **Next**.



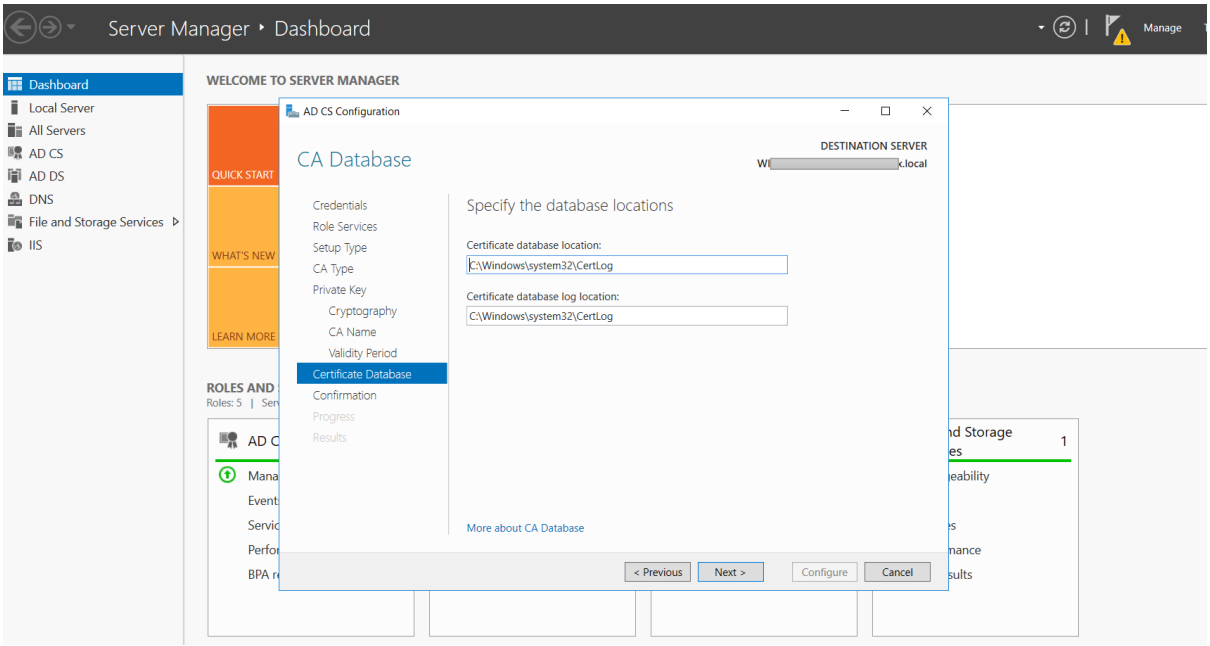
6. For **CA Name**, configure the settings as required and click **Next**.



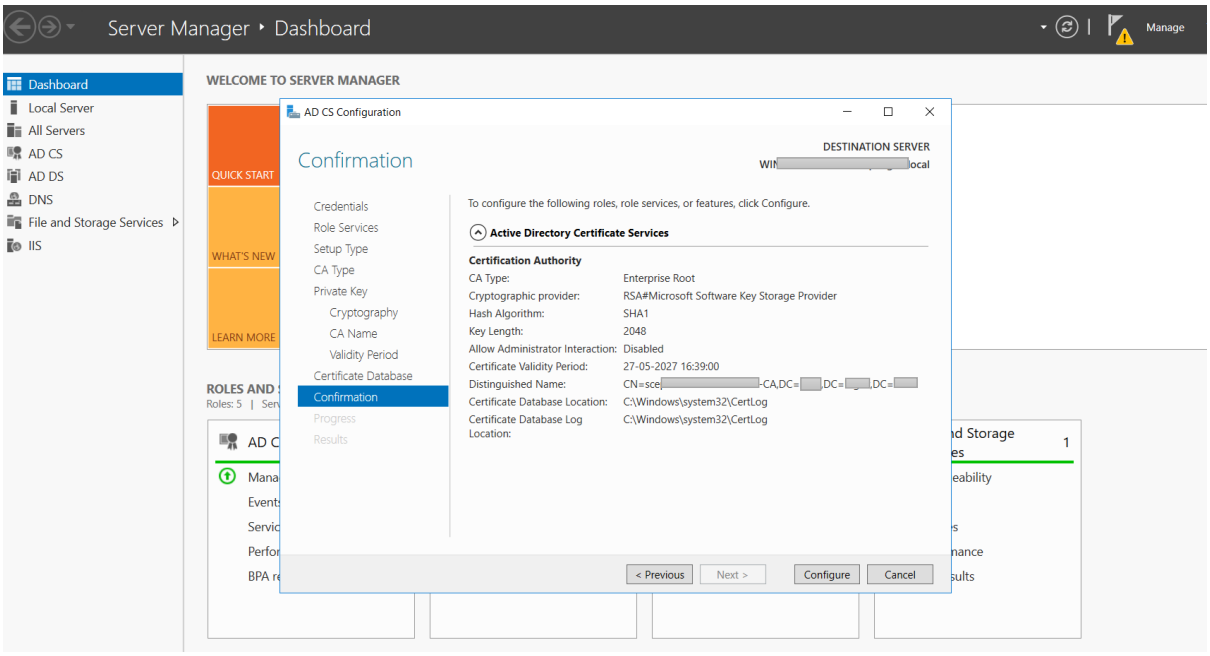
7. **Validity Period**: Configure the CA certificate validity period and click **Next**.



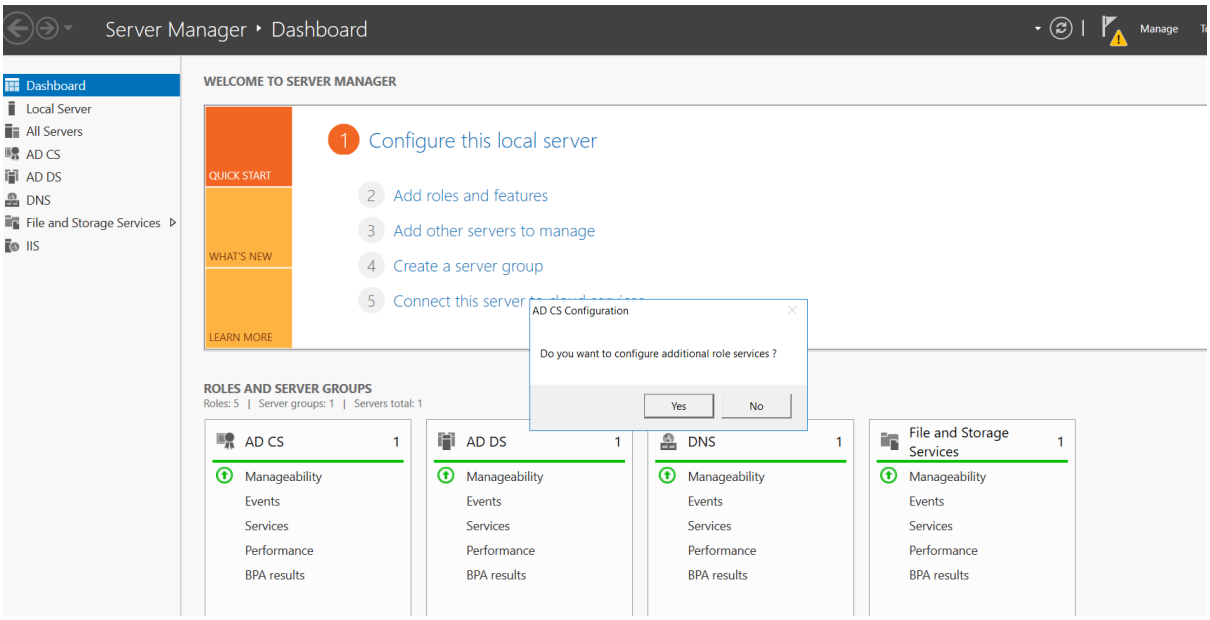
8. **Certificate Database**: Configure the certificate database location and click **Next**.



9. Verify the configuration and click **Configure.**

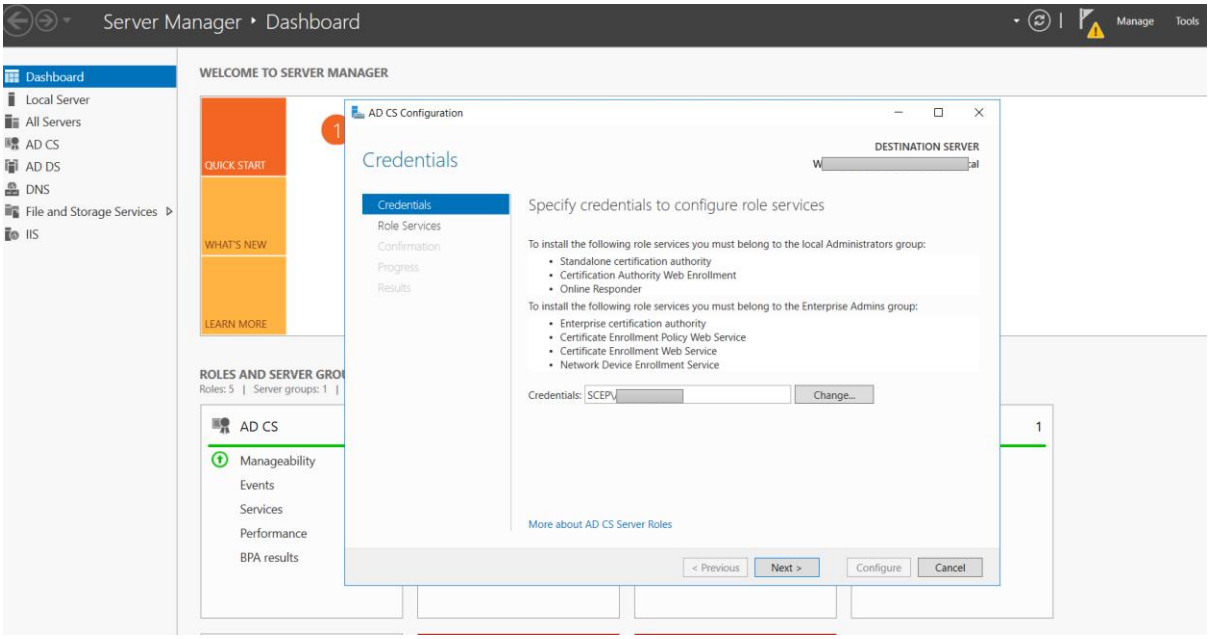


10. Close after configuration succeeds, and click **Yes** to configure additional role services.

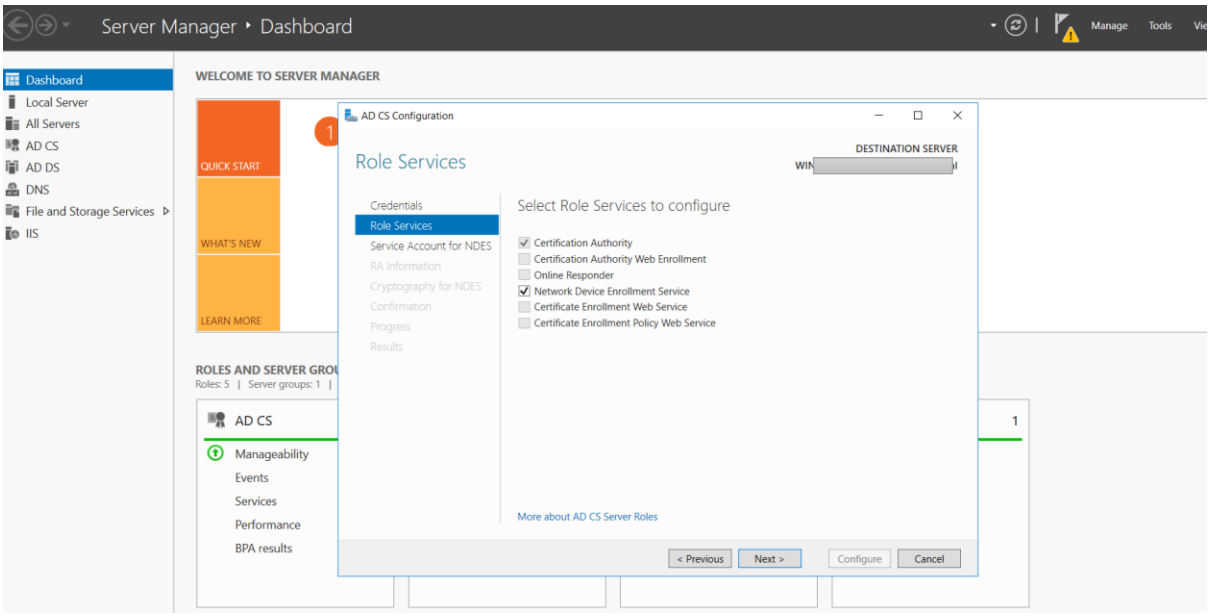


Step 2b: Configure Network Device Enrollment Service (NDES)

1. On the AD CS Configuration page, in the **Credentials** section, verify the logged in Administrator credentials, and click **Next**.

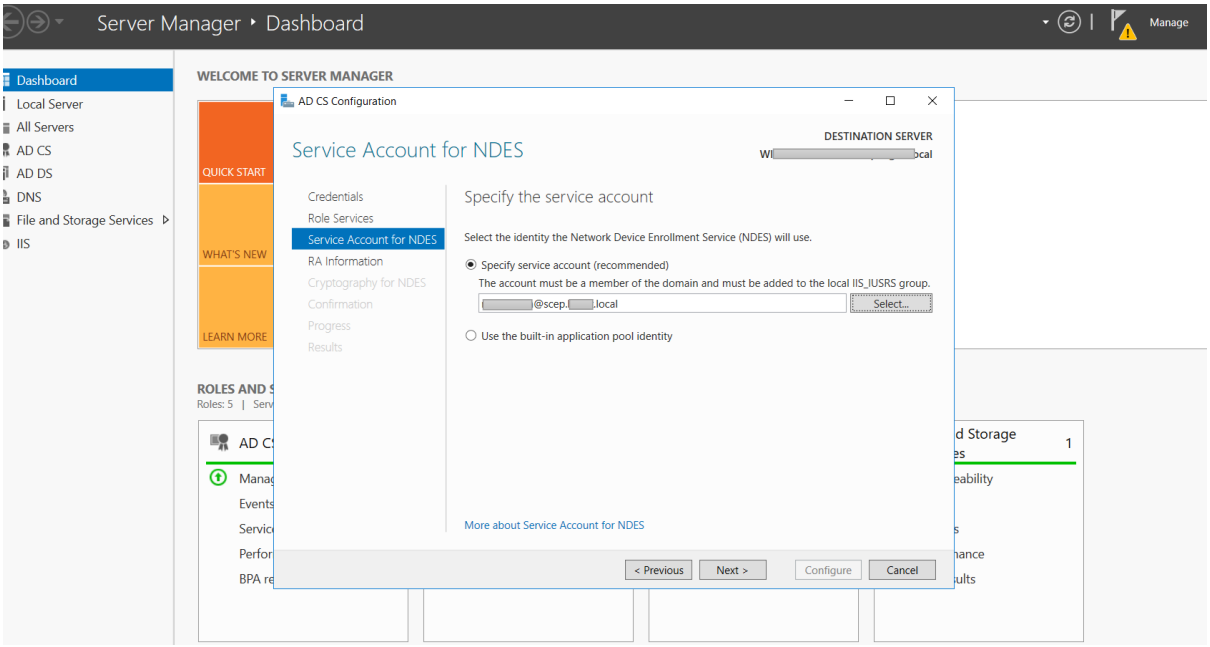


2. From **Role Services**, select 'Network Device Enrollment Service' and click **Next**.

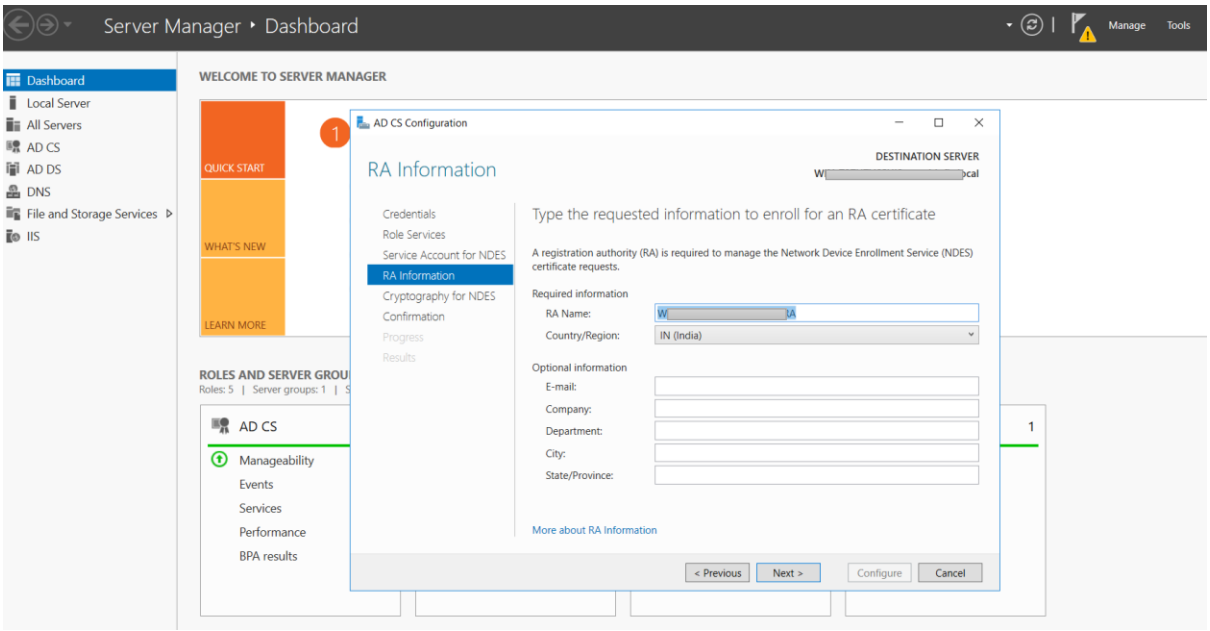


3. In the **Service Account for NDES** section, select the 'Specify service account recommended' option and enter the credentials of the service account created for NDES. Click **Next**.

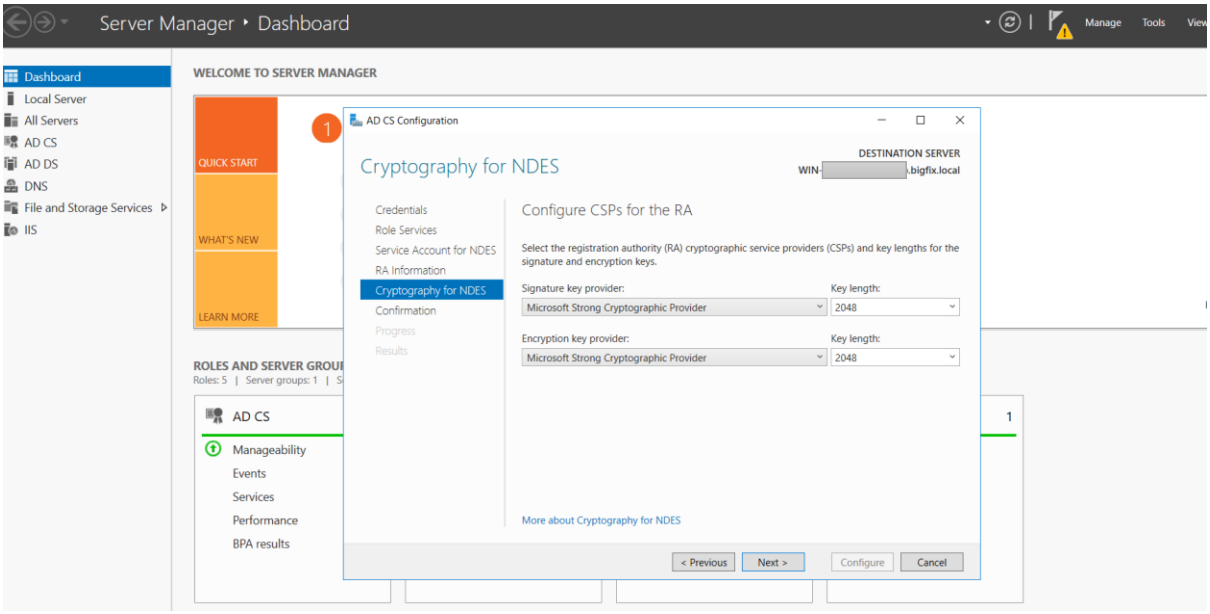
> *Important*: *The service account created must be a part of the local IIS_IUSRS group from Server Manager > Tools > Computer Management > Local Users and Groups > Groups > IIS_USRS > Add to Group menu*.



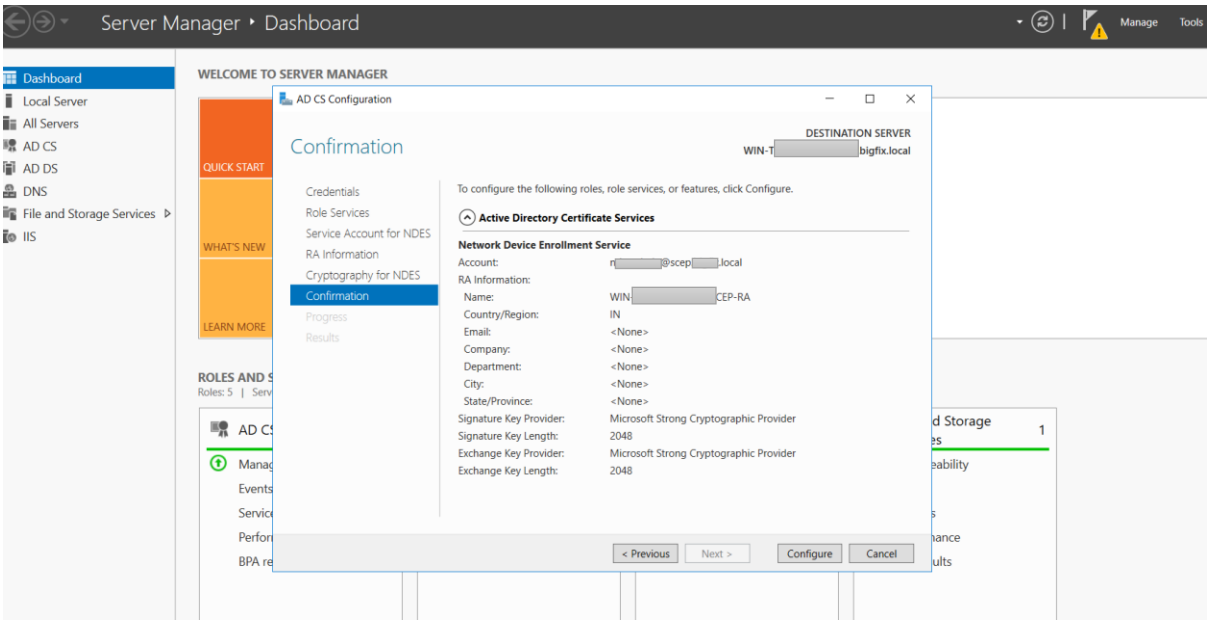
4. **RA Information**: Configure Registration Authority (RA) Information (update only if required) and click **Next**.



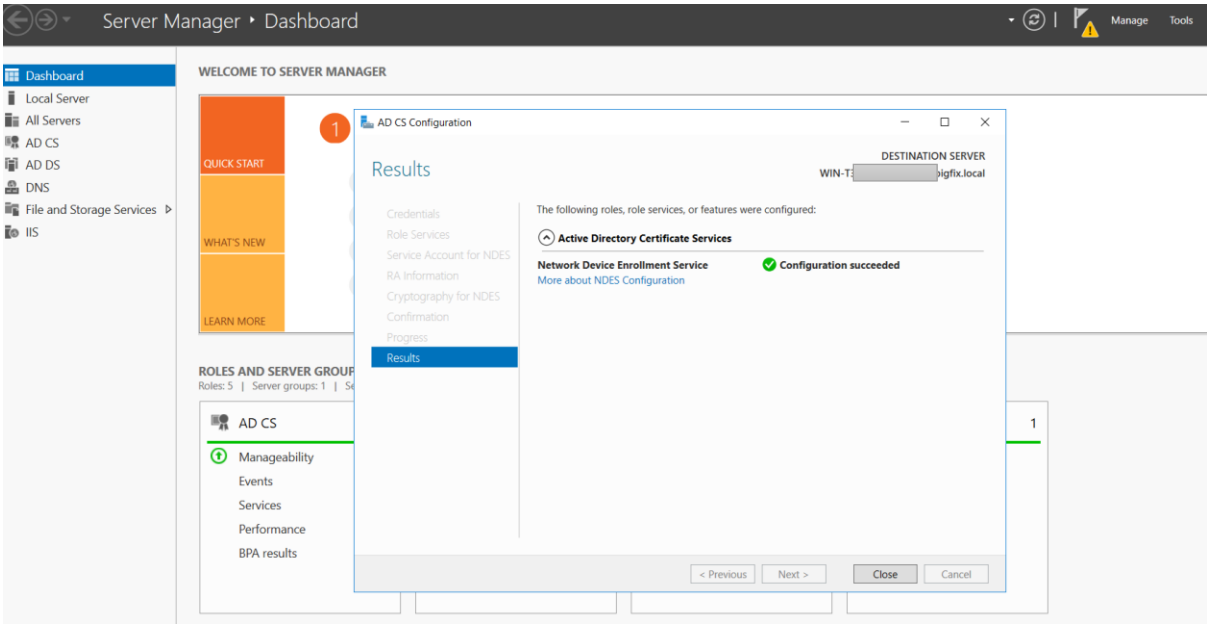
5. **Cryptography for NDES**: Update cryptographic details for NDES (update only if required) and click **Next**.



6. Verify the details and click **Configure.**



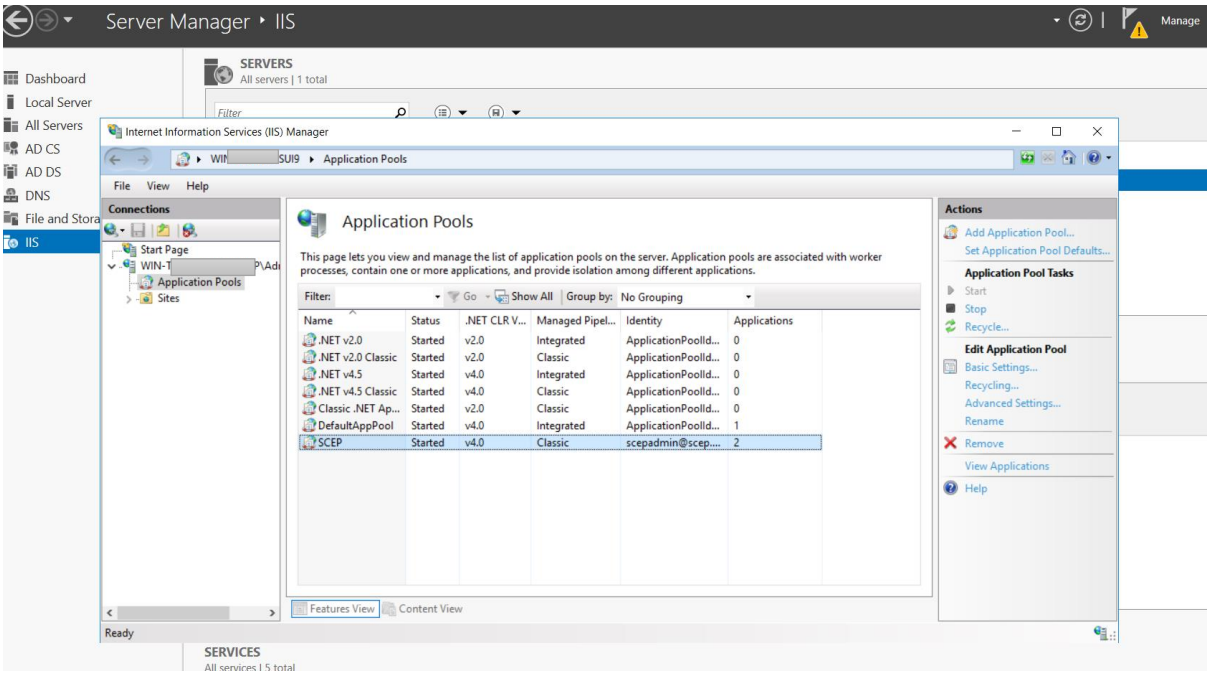
7. Close after configuration succeeds.



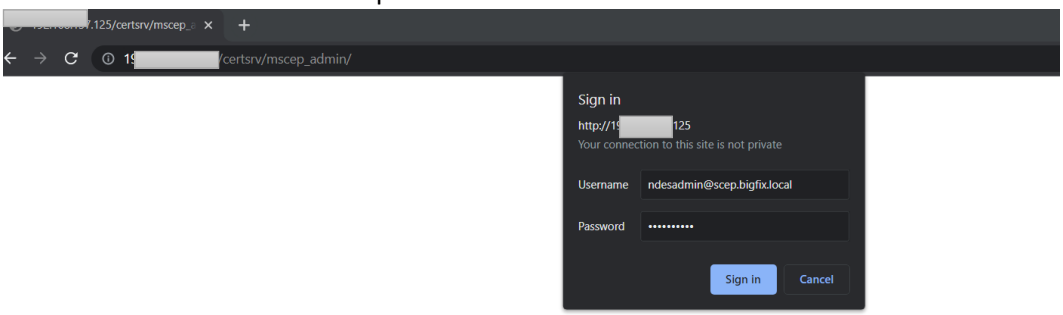
Verify NDES Service configuration

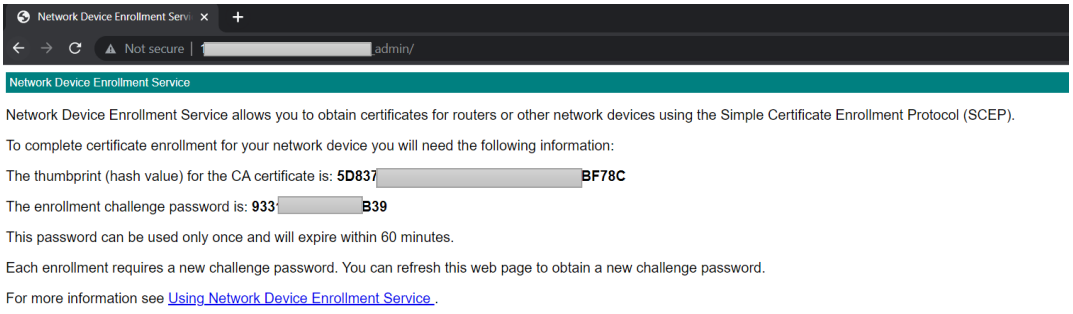
To verify if the SCEP services are running and working as expected, to the following:

1. Open the Internet Information Services (IIS) Manager and check if SCEP service is started.

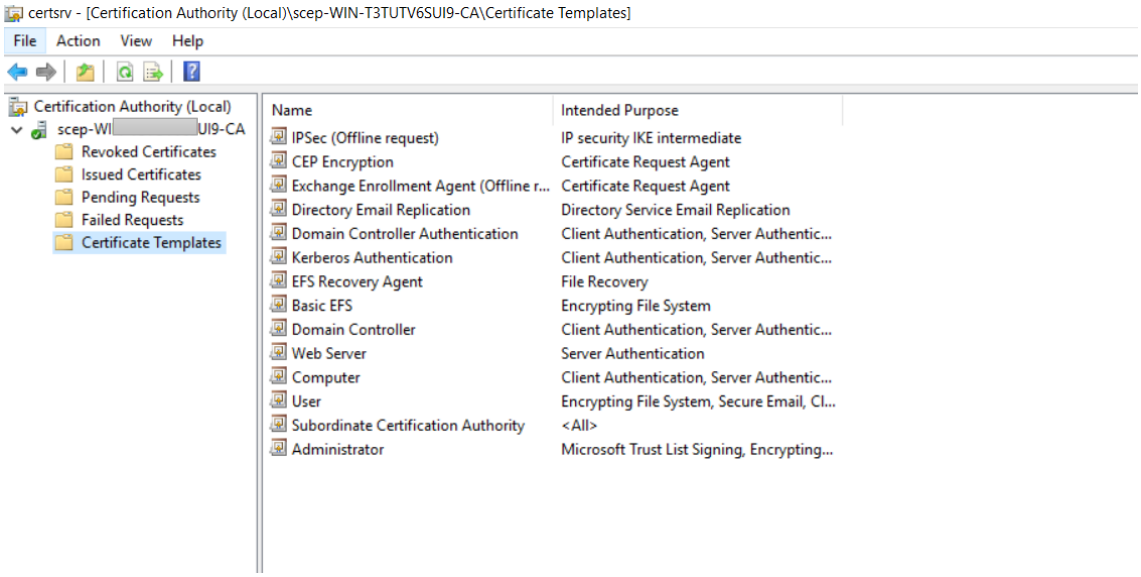


2. Verify SCEP admin app page to get challenge password and CA Thumbprint. Use SCEP service account to authenticate the request.

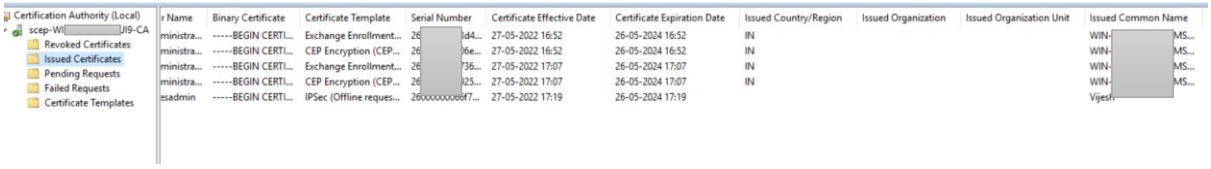




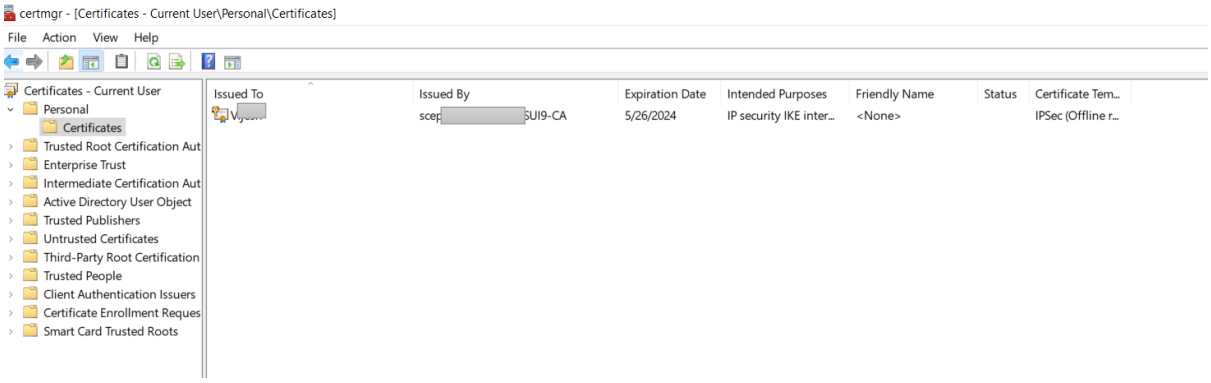
3. CA Certificate templates can be configured from the Certification authority service (Windows > Run > certsrv.msc) > Certificate Templates.



4. You can check the certificates issued from Certification authority service (Windows > Run > certsrv.msc) > Issued Certificates.



5. In the endpoint, you can check the certificates issued from certmgr (Windows > Run > certmgr.msc)



NDES Service Challenge Password configuration

Default behaviors

The following are the default NDES behavior with respect to the challenge password:

- Password cannot be reused for certificate enrollment requests. Every request to the NDES admin service (http://ndes_service/certsrv/mscep_admin) shall generate a new password.
- The maximum number of passwords that will be cached in the server is 5.
- The password validity is 60 minutes.

With the above default behavior, only maximum of 5 certificate enrollment requests per hour can be processed by NDES service.

All of these can be overridden with below registry configurations.

To change the maximum number of passwords cached by NDES (PasswordMax)

You can update the maximum number of passwords that can be cached by NDES through the following steps:

1. Run Registry editor (Regedit)
2. Go to *HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP*
3. Create a new Key named *PasswordMax*
4. Under the *PasswordMax* key, create a new *DWORD* with the same name *PasswordMax* and set the value in decimals. The value will decide the number of passwords that can be cached.
5. Restart IIS

To change the challenge password validity period (PasswordValidity)

You can change the challenge password validity period from 60 minutes through the following steps:

1. Run Registry editor (Regedit)
2. Go to *HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP*
3. Create a new Key named *PasswordValidity*
4. Under the *PasswordValidity* key, create a new *DWORD* with the same name *PasswordValidity* and set the value in decimals. The value will decide the password validity in minutes for which it should be cached.
5. Restart IIS

To reuse the same challenge password (UseSinglePassword)

To allow reusing the same challenge password for every certificate enrollment request, the following registry key needs to be updated. This prevents the NDES admin service from generating new challenge passwords.

1. Run Registry editor (Regedit)
2. Go to *HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP*
3. Modify the value of the key *UseSingePassword* as *1*
4. Restart IIS

Note: If the SCEP services fails to start due to above change, configure the following:

1. Open IIS Manager.
2. In the navigation pane, click *Application Pools.*

3. In Application Pools, click *SCEP.*
4. In the Actions pane, click *Advanced Settings.*
5. Under *Process Model*, click *Load User Profile*. Set to **True**.
6. Click OK to all dialog boxes.
7. Restart IIS

References

- http://everythingaboutintune.com/2020/07/ndes-and-scep-setup-for-intune-a-complete-guide/
- https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-how-to-configure-ndes-for-scep-certificate/ba-p/455125