Implementing Certificate Deployment via Intune and Windows Server (NDES + SCEP)

By Vishnu Vardhan Gollapudi

Introduction

Certificate-based authentication is crucial for securing modern enterprise environments. Using Microsoft Intune alongside Windows Server's Network Device Enrollment Service (NDES) and Simple Certificate Enrollment Protocol (SCEP) enables seamless certificate deployment to devices for enhanced security.
In this article, I will walk you through the process of setting up certificate deployment using Intune and Windows Server, sharing key configurations and best practices from my hands-on experience.

Prerequisites

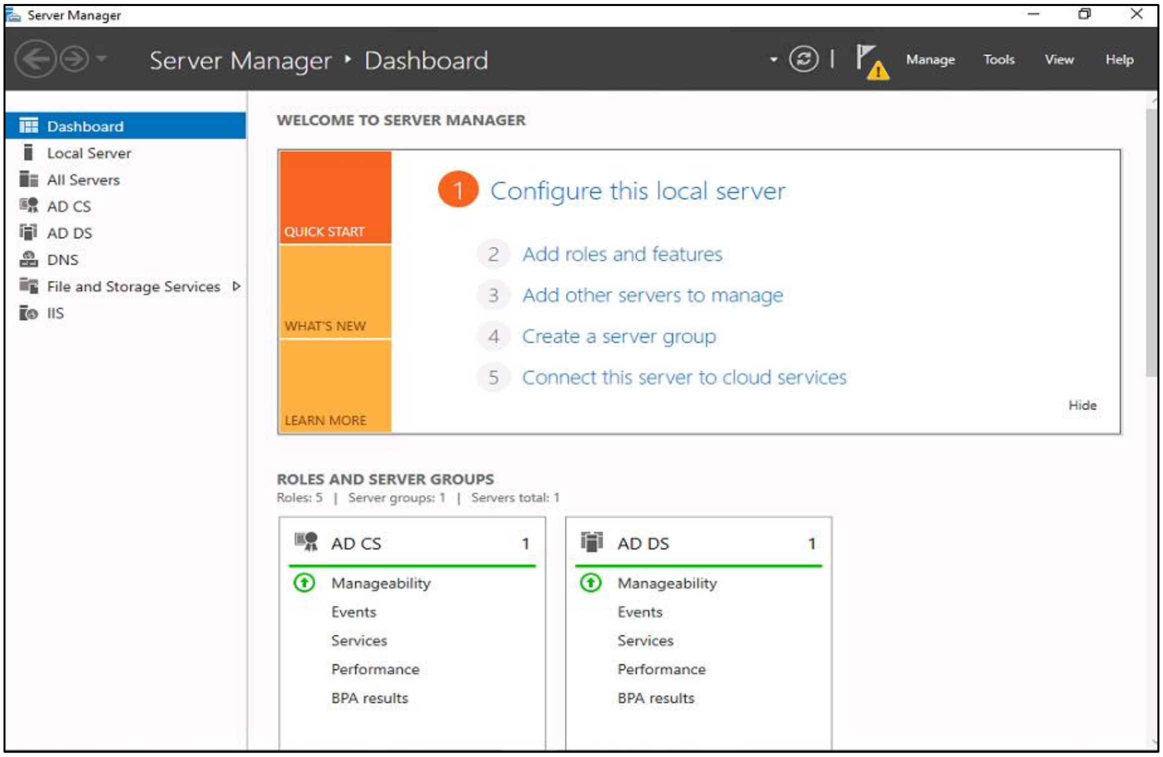
Before starting, ensure you have:

- Windows Server 2019
- Active Directory and Azure AD Connect configured
- Enterprise Certificate Authority (CA)
- Domain-joined NDES server
- Microsoft Intune and Azure AD tenant
- Administrative privileges (including temporary Enterprise Admin rights)

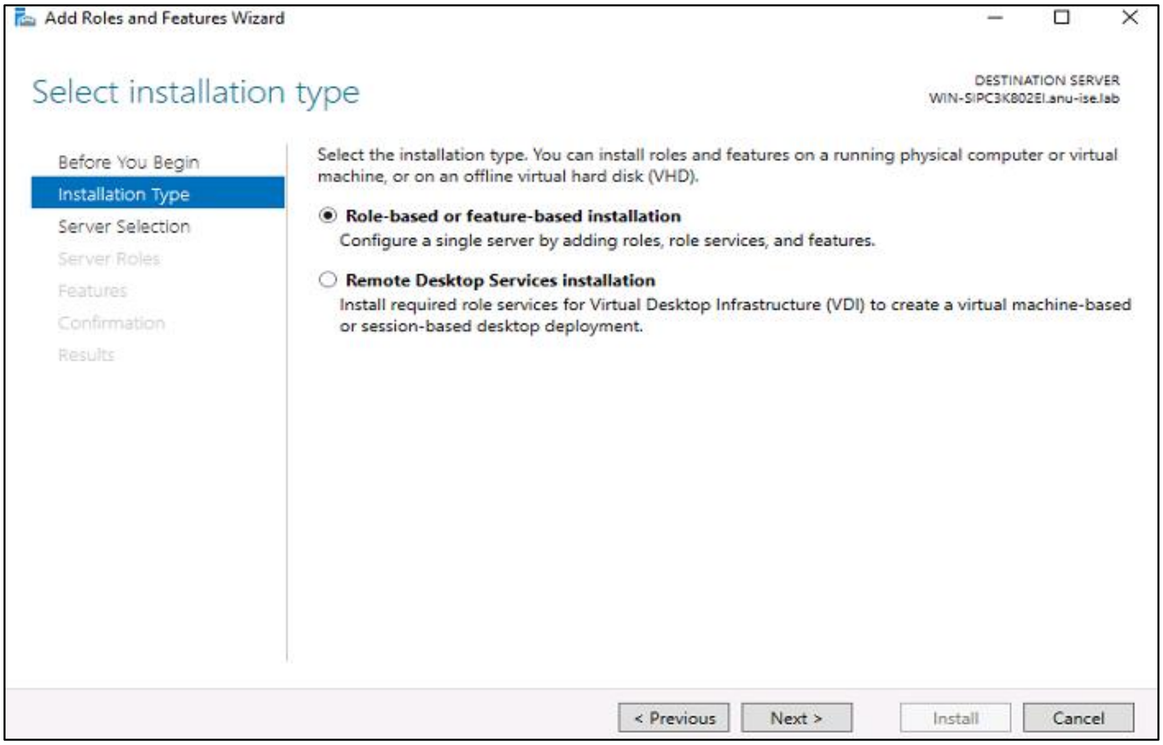
Step 1: Installing and Configuring Active Directory Certificate Services (AD CS)

Follow these steps to install and configure AD CS:

- Open Server Manager from the Start menu.
- Click on 'Add roles and features'.



- Choose 'Role-based or feature-based installation.

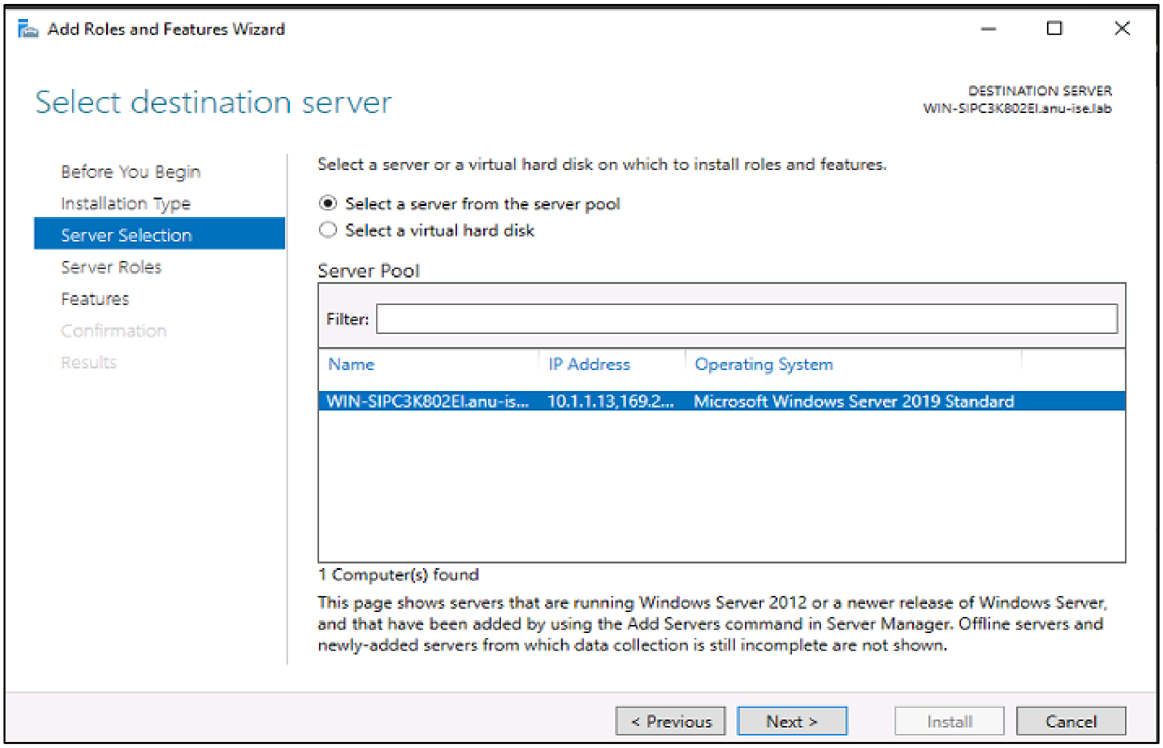


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

- Select the local server.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-SIPC3K802EI.anu-ise.lab

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

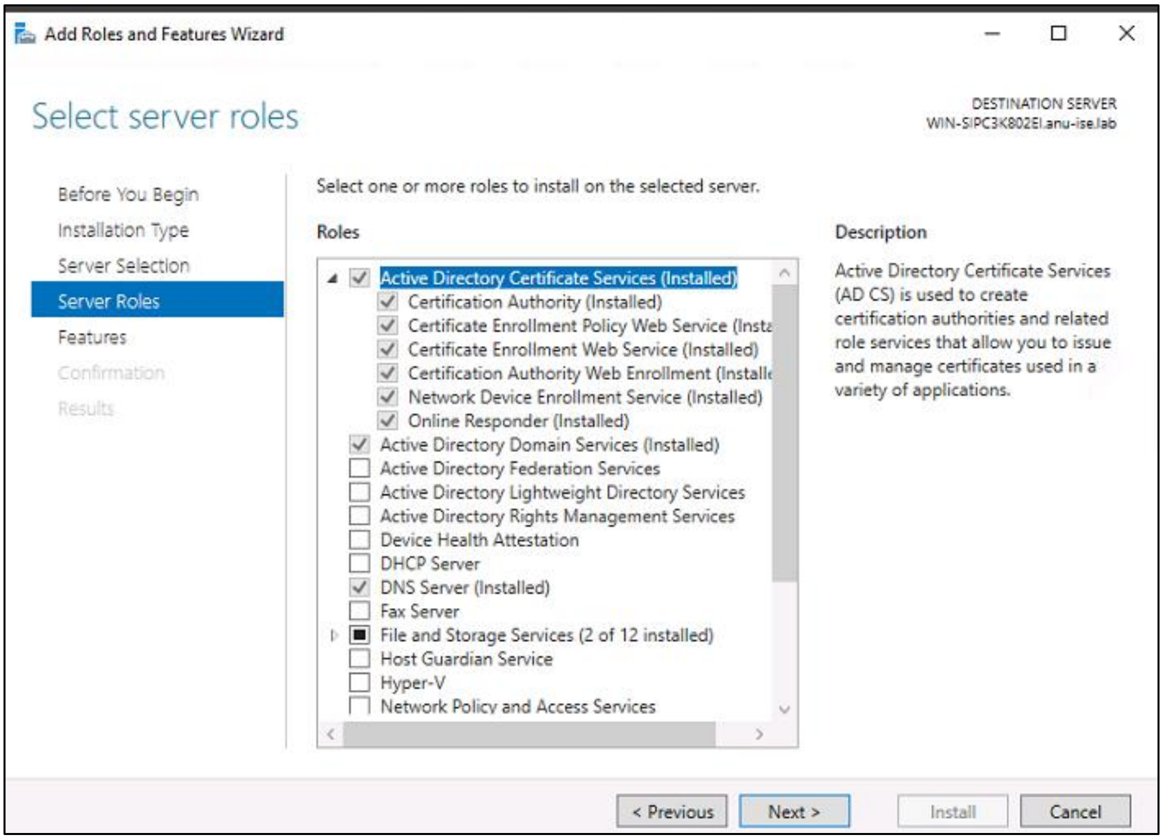
Filter:

Name	IP Address	Operating System
WIN-SIPC3K802EI.anu-is...	10.1.1.13,169.2...	Microsoft Windows Server 2019 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

- In 'Server Roles', select 'Active Directory Certificate Services'.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-SIPC3K802EI.anu-ise.lab

Select one or more roles to install on the selected server.

Roles

☑ Active Directory Certificate Services (Installed)
  ☑ Certification Authority (Installed)
  ☑ Certificate Enrollment Policy Web Service (Insta
  ☑ Certificate Enrollment Web Service (Installed)
  ☑ Certification Authority Web Enrollment (Installe
  ☑ Network Device Enrollment Service (Installed)
  ☑ Online Responder (Installed)
☑ Active Directory Domain Services (Installed)
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☐ DHCP Server
☑ DNS Server (Installed)
☐ Fax Server
■ File and Storage Services (2 of 12 installed)
☐ Host Guardian Service
☐ Hyper-V
☐ Network Policy and Access Services

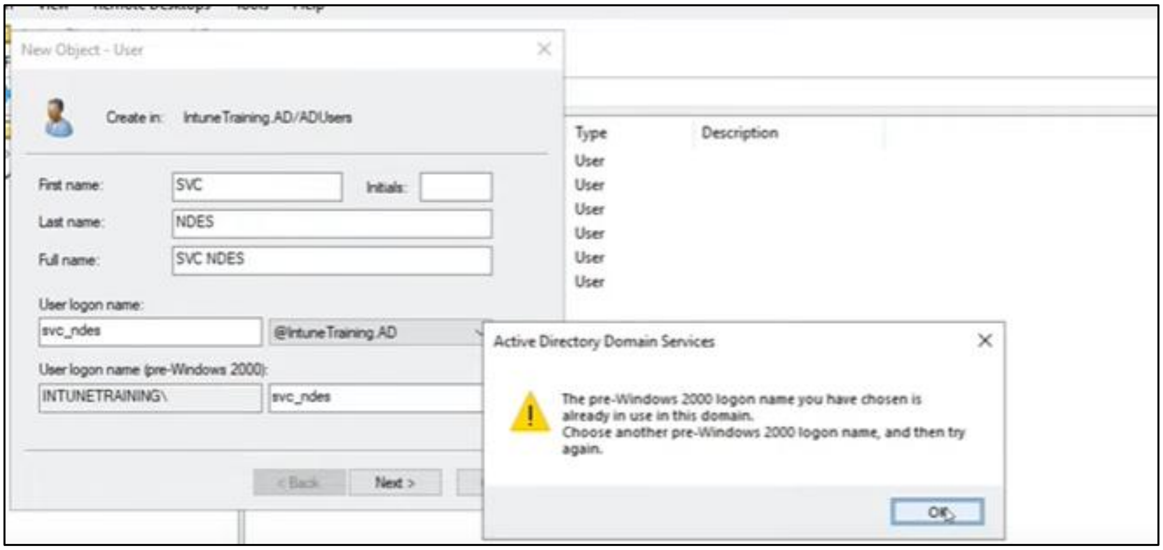
Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

- On the 'Role Services' page, select the following: Certification Authority, Certification Authority Web Enrollment, Certificate Enrollment Web Service, and optionally Online Responder.
- Click Next and then Install.
- After installation, return to Server Manager and click the yellow warning icon indicating 'Configuration required'.
- Launch the AD CS Configuration Wizard:
    - Use Enterprise Admin credentials.
    - Select 'Enterprise CA' and choose 'Root CA' if this is your first CA in the hierarchy.
    - Choose to create a new private key with RSA Microsoft Software Key Storage Provider
    - 2048-bit key length, and SHA256 hash algorithm.
    - Name the CA and set certificate validity (default 5 years).
    - Select Windows Authentication for enrollment and choose the appropriate web enrollment certificate.
    - Review your settings and click Configure, then Close when finished.

Step 2: Creating the NDES Service Account

- Open the Active Directory Users and Computers console.
- Create a new domain service account, e.g., 'svc_NDES'.



Create in: IntuneTraining.AD/ADUsers

First name: SVC

Initials:

Last name: NDES

Full name: SVC NDES

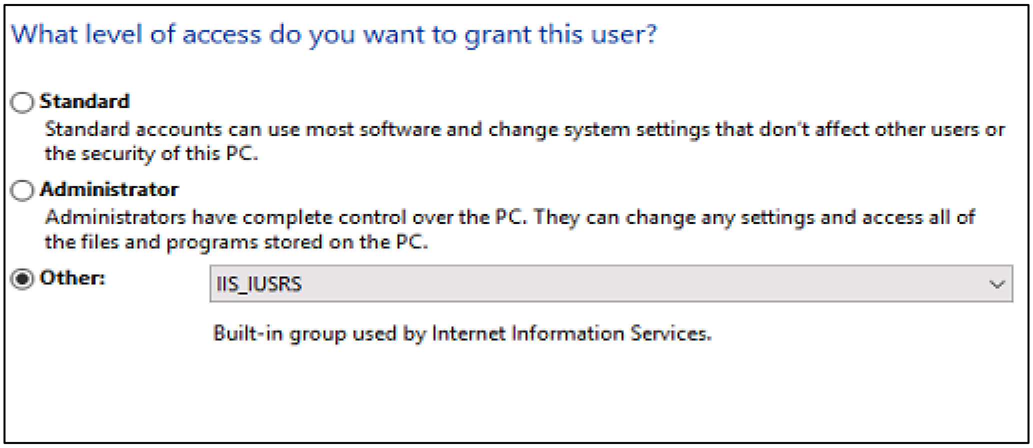
User logon name: svc_ndes @IntuneTraining.AD

User logon name (pre-Windows 2000): INTUNETRAINING\ svc_ndes

Active Directory Domain Services

The pre-Windows 2000 logon name you have chosen is already in use in this domain.
Choose another pre-Windows 2000 logon name, and then try again.

- On the NDES server, open the 'Run' dialog and type 'netplwiz'.
- Navigate to the 'Groups' tab and add 'svc_NDES' to the 'IIS_IUSRS' group.



What level of access do you want to grant this user?

○ **Standard**
Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

○ **Administrator**
Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

● **Other:** IIS_IUSRS

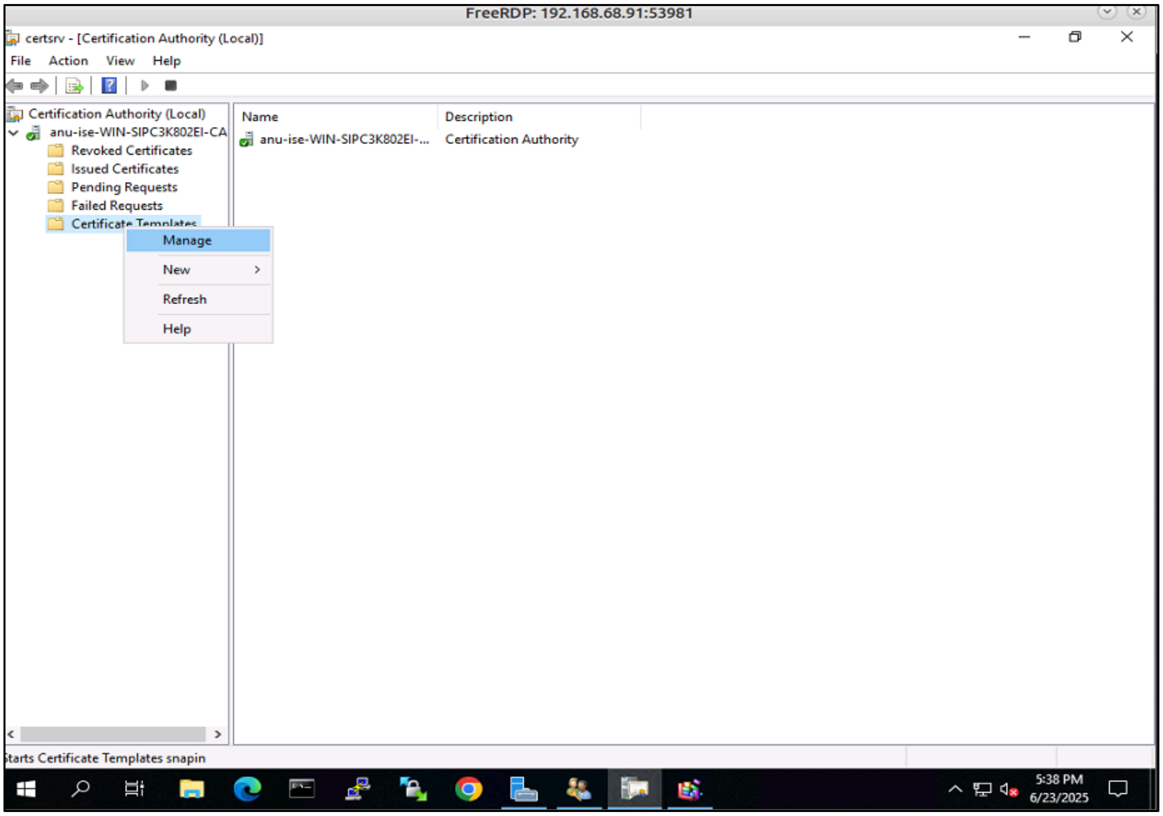
Built-in group used by Internet Information Services.

- In the Certification Authority console, assign the 'Issue and Manage Certificates' permission to 'svc_NDES'.

Step 3: Configuring Certificate Templates

Configure certificate templates for NDES as follows:

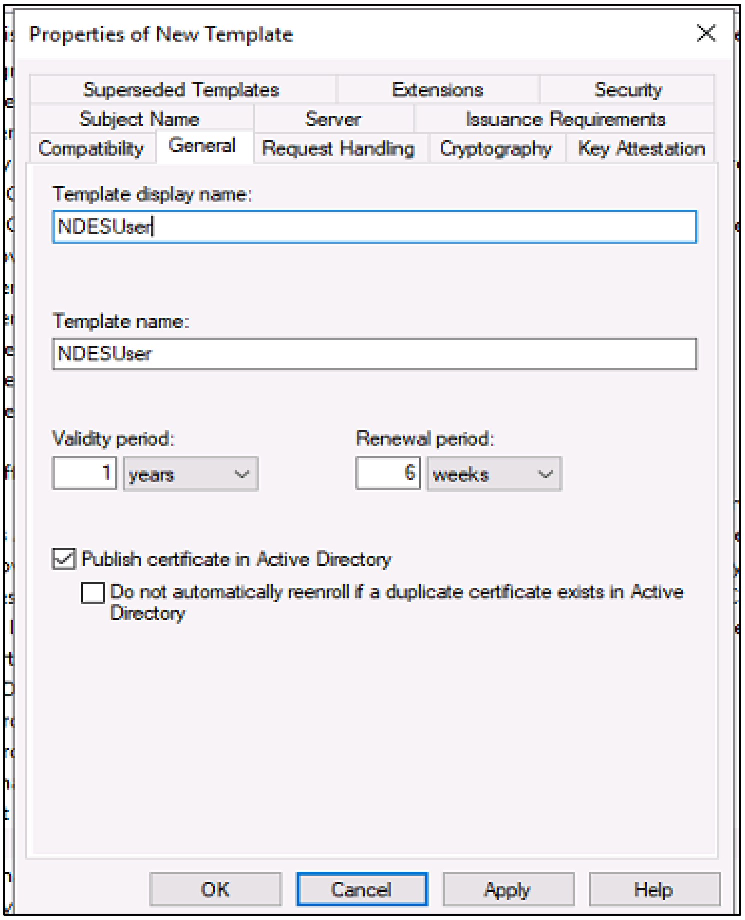
- Open the Certification Authority console.
- Right-click 'Certificate Templates' and select 'Manage'.



FreeRDP: 192.168.68.91:53981
certsrv - [Certification Authority (Local)]
File
Action
View
Help
Certification Authority (Local)
anu-ise-WIN-SIPC3K802EI-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
Refresh
Help
tarts Certificate Templates snapin
5:38 PM
6/23/2025

Name	Description
anu-ise-WIN-SIPC3K802EI-...	Certification Authority

- Duplicate the 'User' template and rename it 'NDESUser'.



Properties of New Template

Template display name:
NDESUser

Template name:
NDESUser

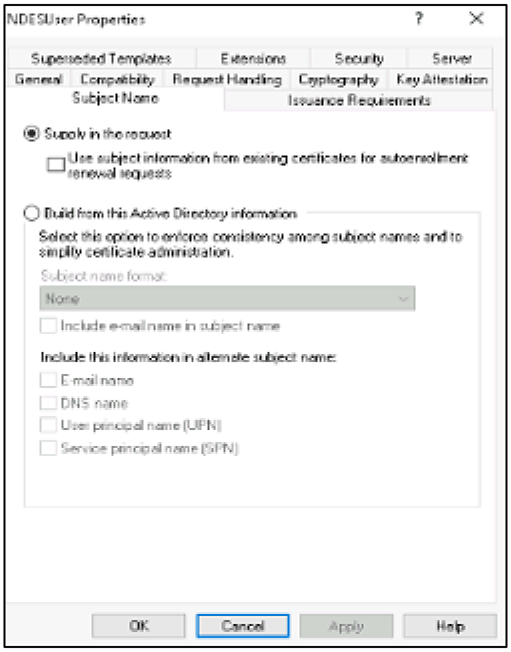
Validity period:
1 years

Renewal period:
6 weeks

☑ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

- Set compatibility to Windows Server 2012 R2 and Windows 10.
- Set the Subject Name to 'Supply in the request'.



NDESUser Properties

● Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:
None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

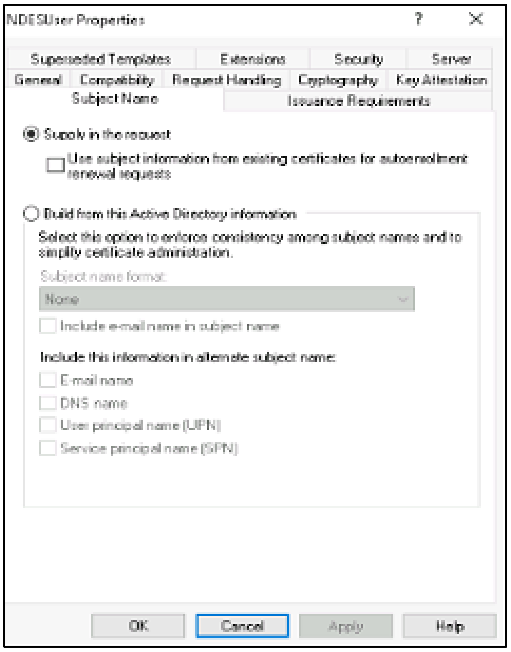
☐ E-mail name

☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

- Under Extensions, add 'Client Authentication' and optionally 'Any Purpose'.
- Under the Security tab, add 'svc_NDES' with Read and Enroll permissions.



● Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

☐ Include e-mail name in subject name

Include this information in alternate subject name:

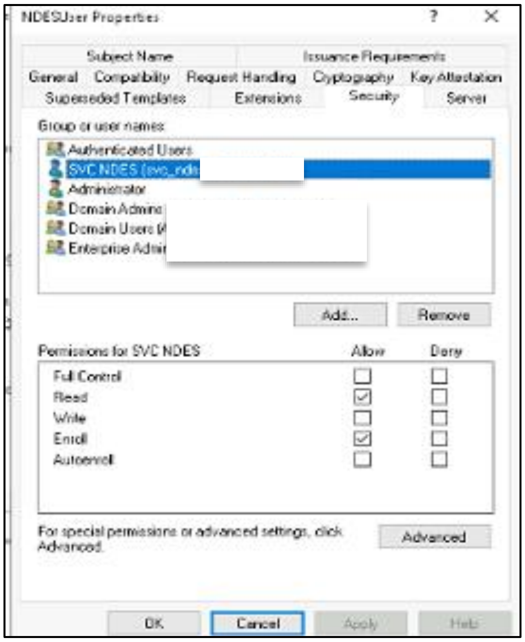
☐ E-mail name

☐ DNS name

☐ User principal name (UPN)

☐ Service principal name (SPN)

- Duplicate the 'Web Server' template as 'NDESWeb' and keep default settings.
- Add the NDES service account and relevant AD devices with Read, Write, and Enroll permissions.

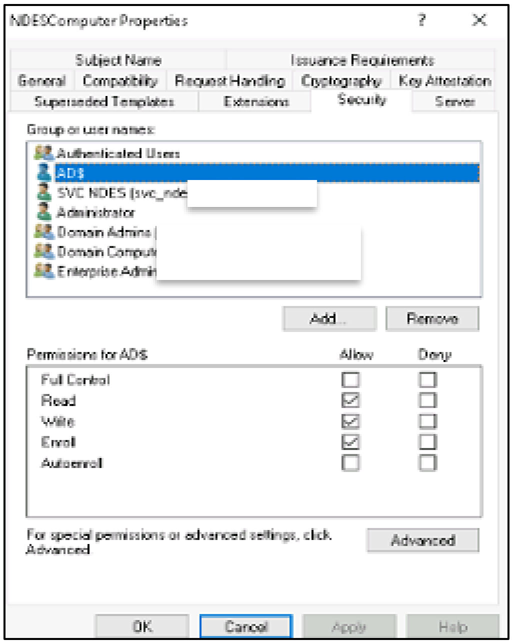


Group or user names:

Authenticated Users
SVC NDES (svc_nde
Administrator
Domain Admins
Domain Users (
Enterprise Admi

Permissions for SVC NDES	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☐	☐
Enroll	☑	☐
Autoenroll	☐	☐

For special permissions or advanced settings, click Advanced.



NDESComputer Properties

Subject Name | Issuance Requirements
General | Compatibility | Request Handling | Cryptography | Key Attestation
Superseded Templates | Extensions | Security | Server

Group or user names:

- Authenticated Users
- AD$
- SVC NDES (svc_nde
- Administrator
- Domain Admins (
- Domain Comput
- Enterprise Admi

Permissions for AD$

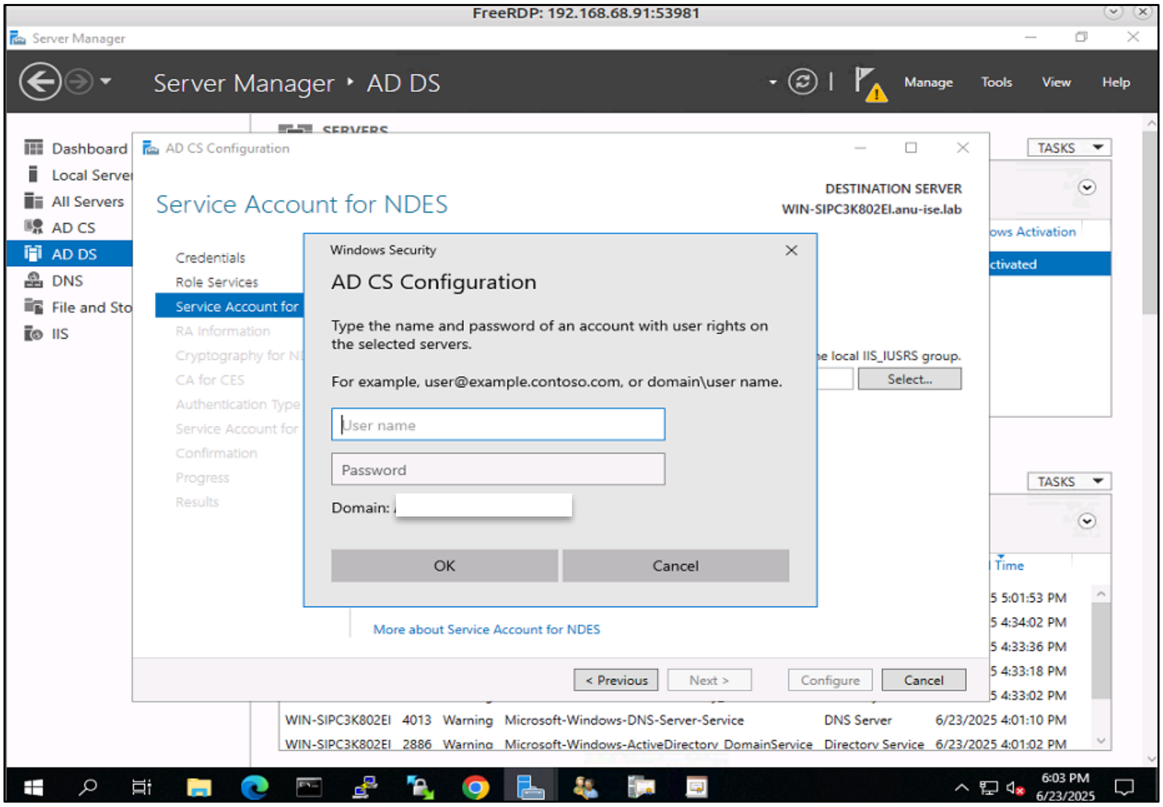
	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☑	☐
Enroll	☑	☐
Autoenroll	☐	☐

For special permissions or advanced settings, click Advanced.

- Publish the 'NDESUser' and 'NDESWeb' templates by right-clicking 'Certificate Templates', selecting 'New' > 'Certificate Template to Issue', then choosing these templates.

Step 4: Configuring the NDES Role and Setting SPN

- In Server Manager, select 'Post-deployment Configuration' and choose 'Configure Active Directory Certificate Services'.
- Select only 'Network Device Enrollment Service (NDES)' and proceed.
- Add the NDES service account when prompted.



Service Account for NDES

DESTINATION SERVER
WIN-SIPC3K802EI.anu-ise.lab

…e local IIS_IUSRS group.

Windows Security

AD CS Configuration

Type the name and password of an account with user rights on the selected servers.

For example, user@example.contoso.com, or domain\user name.

User name

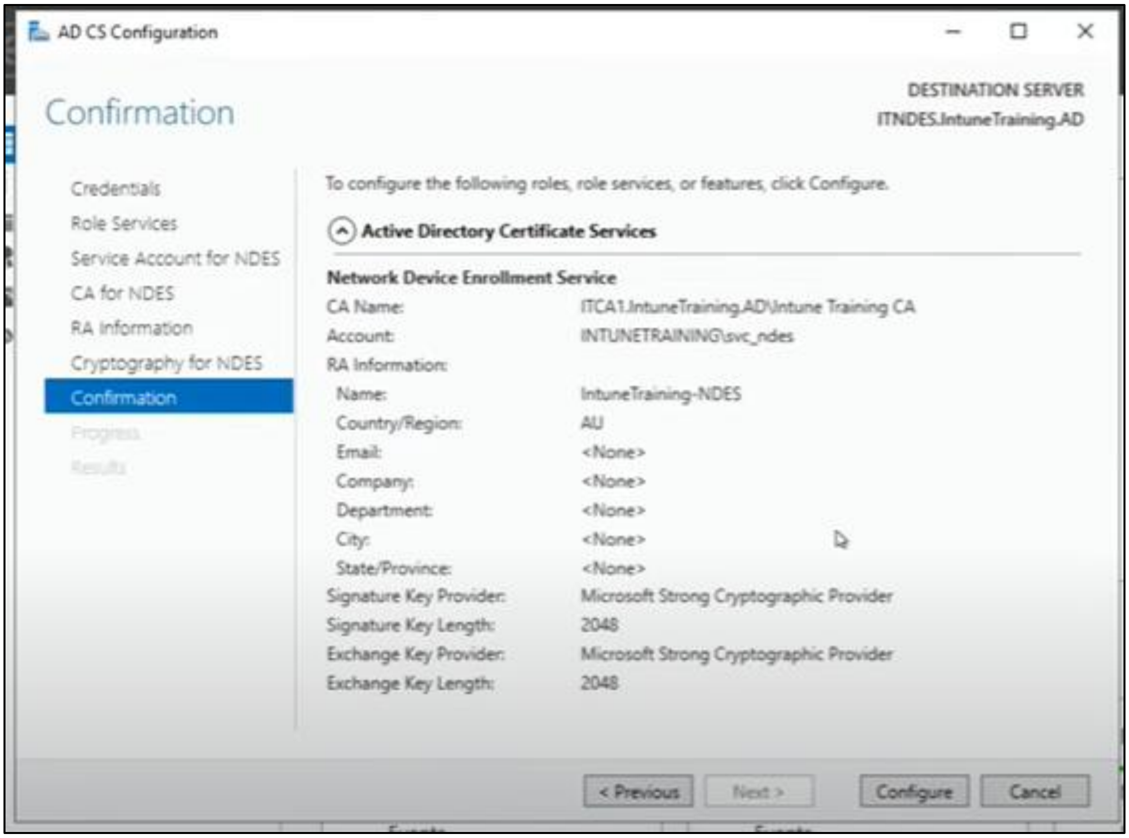
Password

Domain:

OK Cancel

```
5 5:01:53 PM
5 4:34:02 PM
5 4:33:36 PM
5 4:33:18 PM
5 4:33:02 PM
WIN-SIPC3K802EI   4013   Warning   Microsoft-Windows-DNS-Server-Service          DNS Server          6/23/2025 4:01:10 PM
WIN-SIPC3K802EI   2886   Warning   Microsoft-Windows-ActiveDirectory_DomainService   Directory Service   6/23/2025 4:01:02 PM
```

- Specify the CA name, RA Name (friendly identifier), and select 2048-bit key for the CSPs.
- Finish the configuration.



Confirmation

DESTINATION SERVER
ITNDES.IntuneTraining.AD

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Network Device Enrollment Service

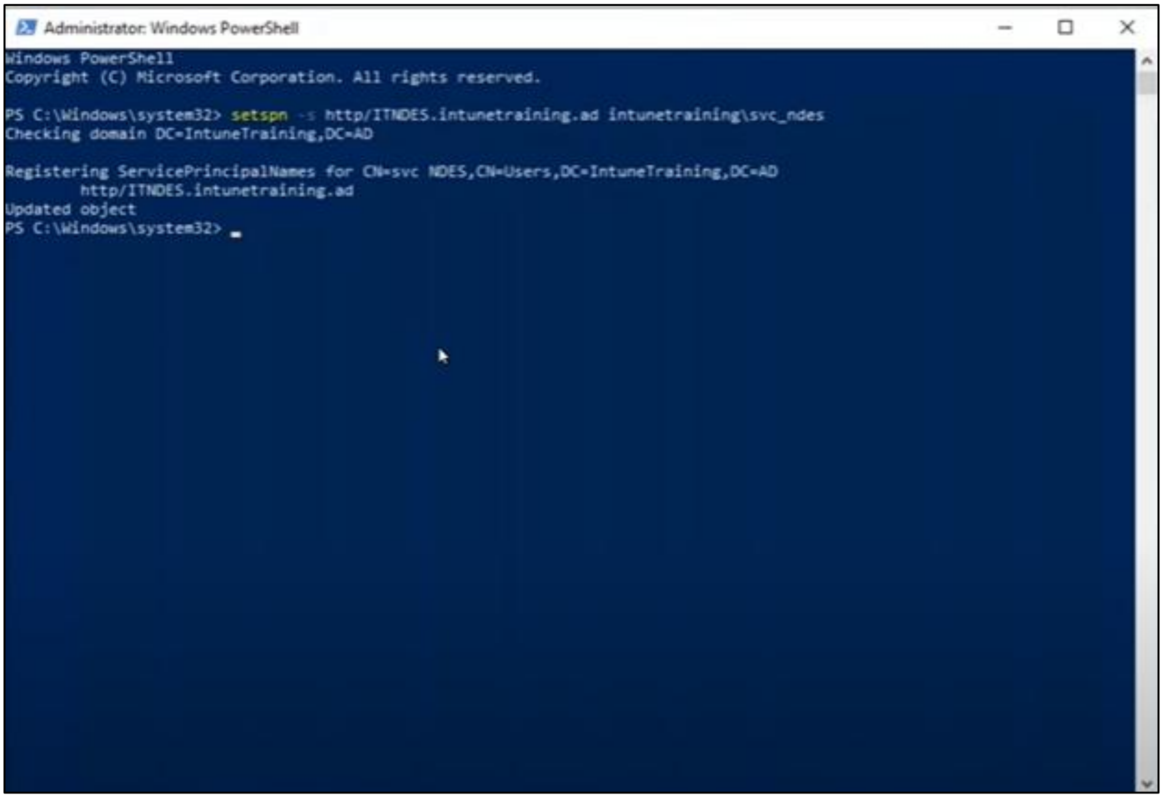
CA Name: ITCA1.IntuneTraining.AD\Intune Training CA
Account: INTUNETRAINING\svc_ndes
RA Information:
Name: IntuneTraining-NDES
Country/Region: AU
Email: <None>
Company: <None>
Department: <None>
City: <None>
State/Province: <None>
Signature Key Provider: Microsoft Strong Cryptographic Provider
Signature Key Length: 2048
Exchange Key Provider: Microsoft Strong Cryptographic Provider
Exchange Key Length: 2048

- Open PowerShell and run the following command to set the Service Principal Name (SPN):

```
setspn -s http/<CA_FQDN> <domain>\<svc_NDES>
```

Example:

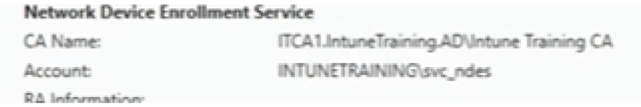
```
setspn -s http/ITNDES.intunetraining.ad intunetraining\svc_ndes
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> setspn -s http/ITNDES.intunetraining.ad intunetraining\svc_ndes
Checking domain DC=IntuneTraining,DC=AD

Registering ServicePrincipalNames for CN=svc NDES,CN=Users,DC=IntuneTraining,DC=AD
        http/ITNDES.intunetraining.ad
Updated object
PS C:\Windows\system32> _
```



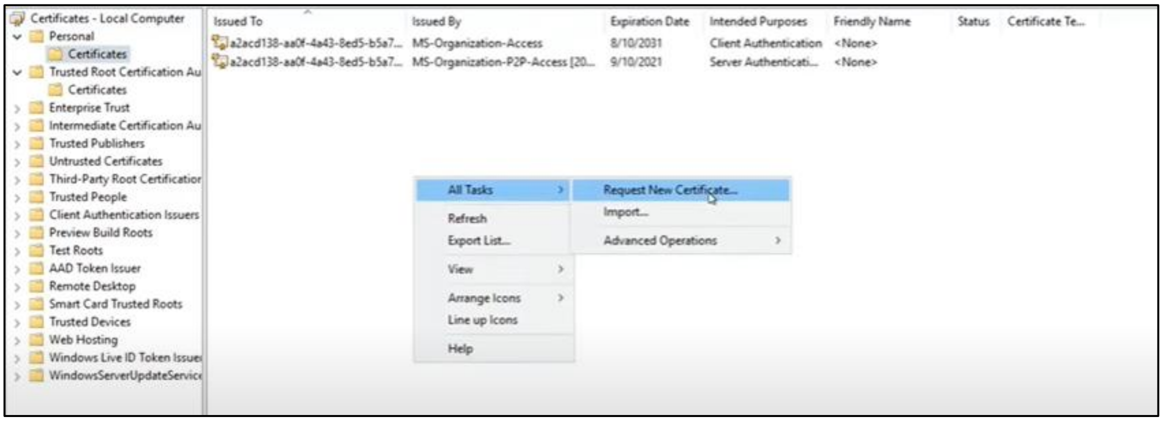
Network Device Enrollment Service

CA Name:	ITCA1.IntuneTraining.AD\Intune Training CA
Account:	INTUNETRAINING\svc_ndes
RA Information:	

- Verify NDES installation by browsing to: `https://localhost/certsrv/mscep/mscep.dll`

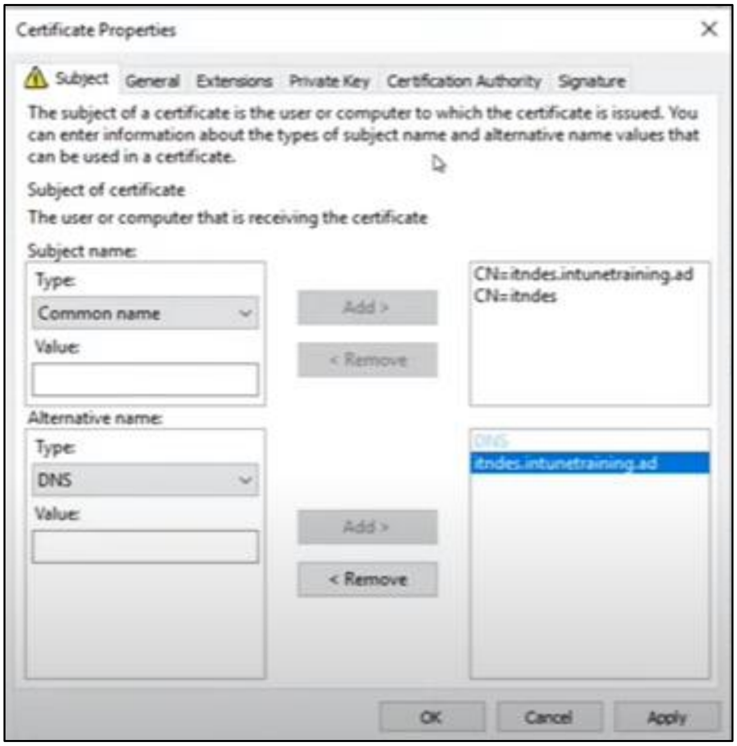
Step 5: Requesting and Binding the Web Server Certificate

- Run 'certlm.msc' to open the Certificates MMC for the local machine.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
a2acd138-aa0f-4a43-8ed5-b5a7...	MS-Organization-Access	8/10/2031	Client Authentication	<None>		
a2acd138-aa0f-4a43-8ed5-b5a7...	MS-Organization-P2P-Access [20...	9/10/2021	Server Authenticati...	<None>		

- Navigate to 'Personal' > 'Certificates' and select 'Request New Certificate'.



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

Value:

CN=itndes.intunetraining.ad
CN=itndes

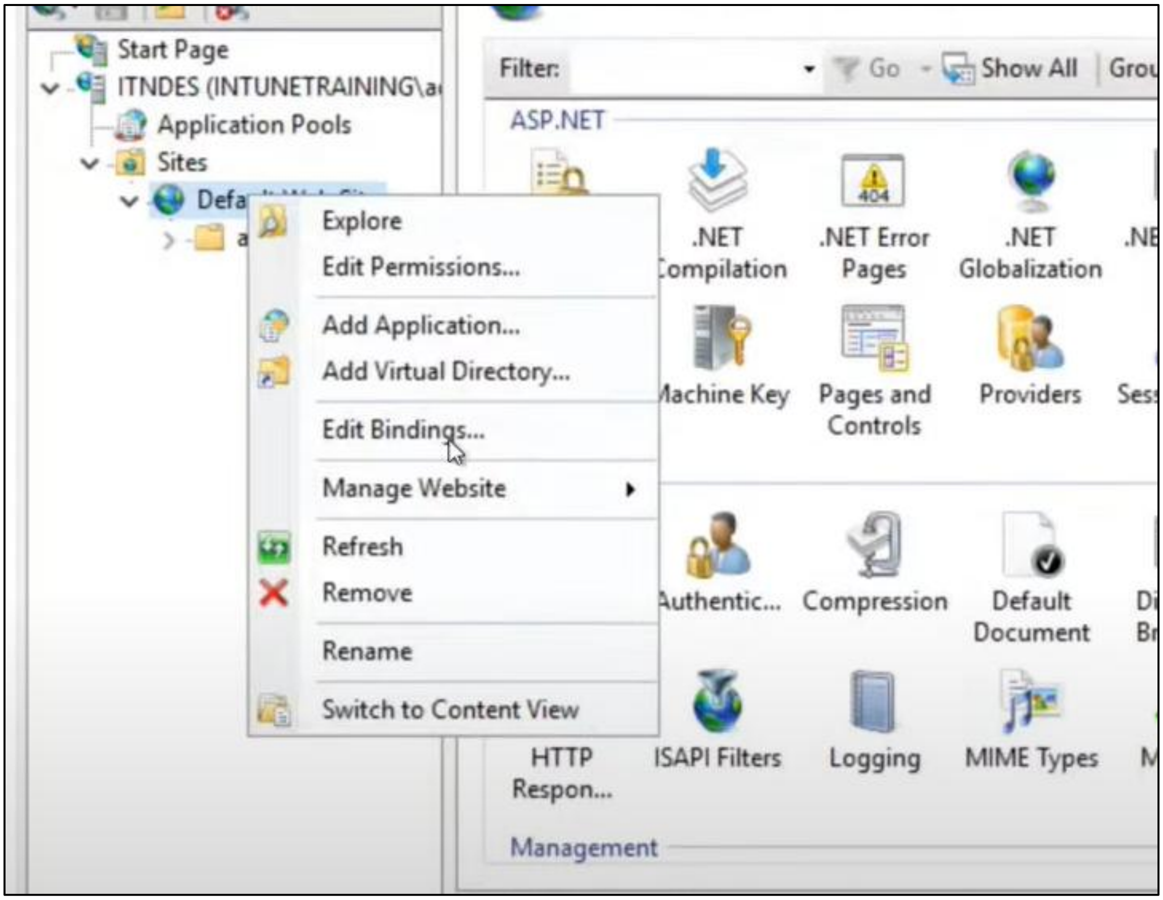
Alternative name:

Type: DNS

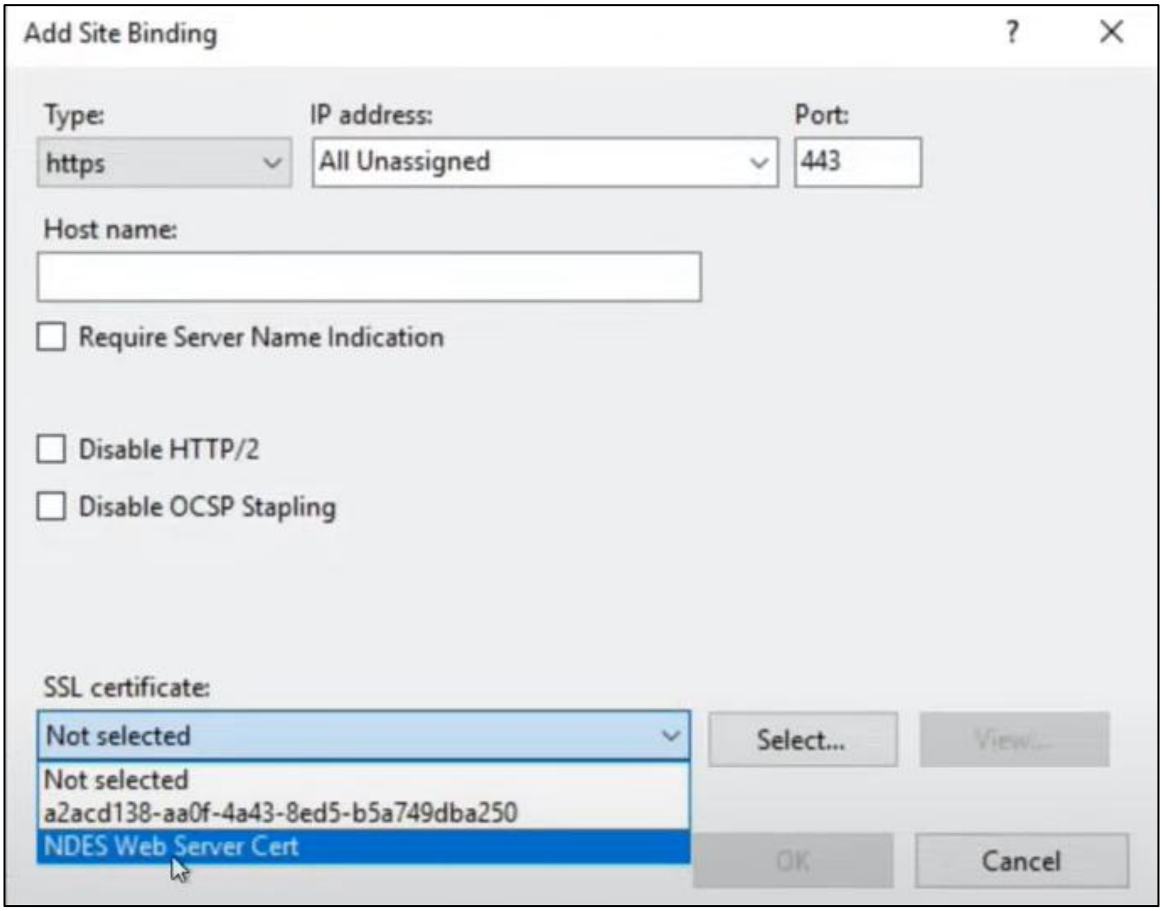
Value:

DNS
itndes.intunetraining.ad

- Choose the 'NDESWeb' template and complete the enrollment process.
- Open IIS Manager, right-click 'Default Web Site', and select 'Edit Bindings'.



- Add a new HTTPS binding using the newly enrolled certificate.



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

□ Disable HTTP/2

□ Disable OCSP Stapling

SSL certificate: Not selected

Not selected
a2acd138-aa0f-4a43-8ed5-b5a749dba250
NDES Web Server Cert

- Click OK to save.

Step 6: Updating the Registry for SCEP Template Mapping

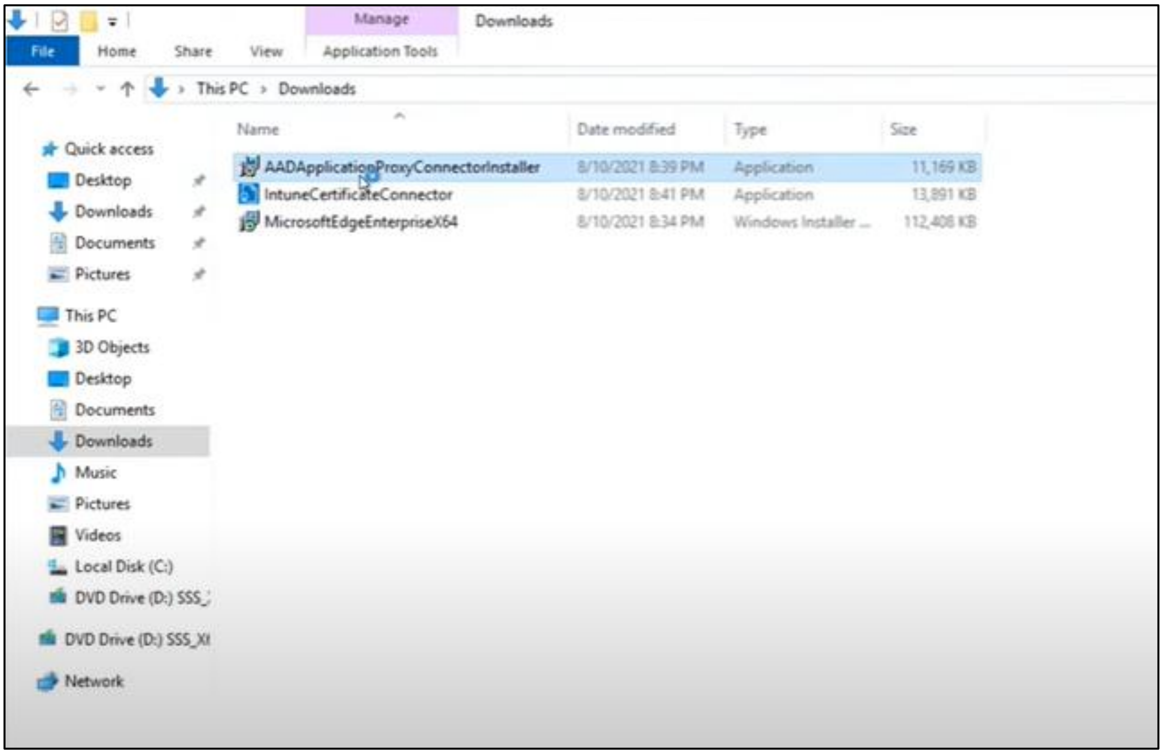
- Open the Registry Editor (regedit).
- Navigate to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP
```

- Modify or add the following string values:
- Encryption Template = NDESUser
- General Purpose Template = NDESUser
- Signature Template = NDESUser
- Restart the server to apply changes.

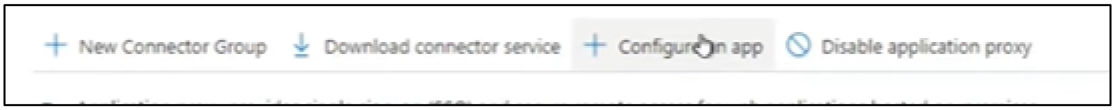
Step 7: Publishing NDES via Azure AD Application Proxy

- In the Azure portal, navigate to Azure AD > Enterprise Applications > Application Proxy.
- Download and install the Application Proxy Connector on the NDES server.

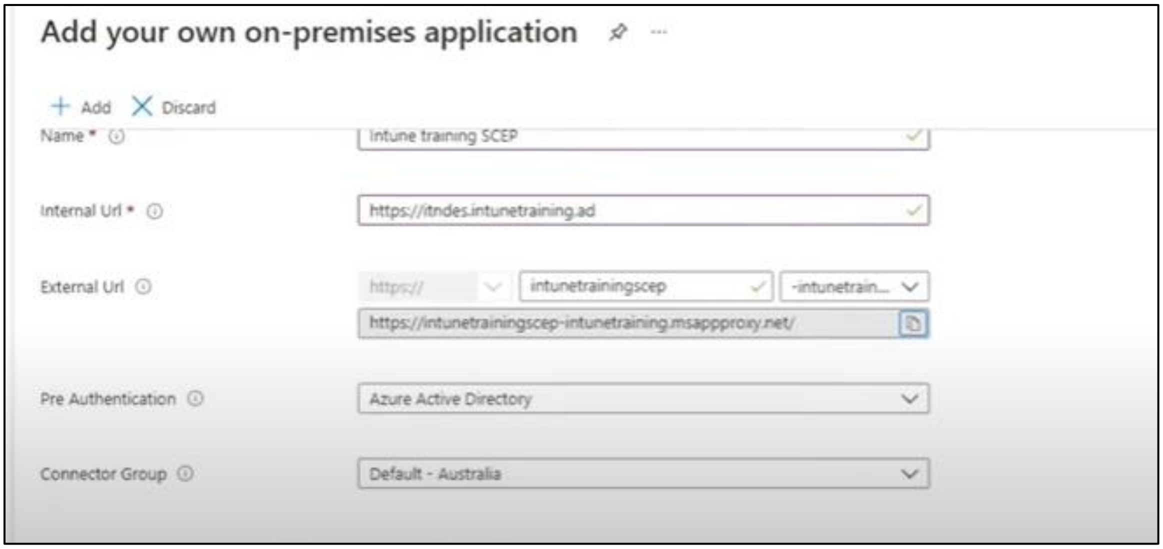


Name	Date modified	Type	Size
AADApplicationProxyConnectorInstaller	8/10/2021 8:39 PM	Application	11,169 KB
IntuneCertificateConnector	8/10/2021 8:41 PM	Application	13,891 KB
MicrosoftEdgeEnterpriseX64	8/10/2021 8:34 PM	Windows Installer ...	112,408 KB

- Create a new Application Proxy application with the following settings:



  - Internal URL: https://<NDES-FQDN>
  - External URL: Auto-generated
  - Pre-authentication: Passthrough



Add your own on-premises application

Name *: Intune training SCEP

Internal Url *: https://itndes.intunetraining.ad

External Url: https:// intunetrainingscep -intunetrain...

https://intunetrainingscep-intunetraining.msappproxy.net/

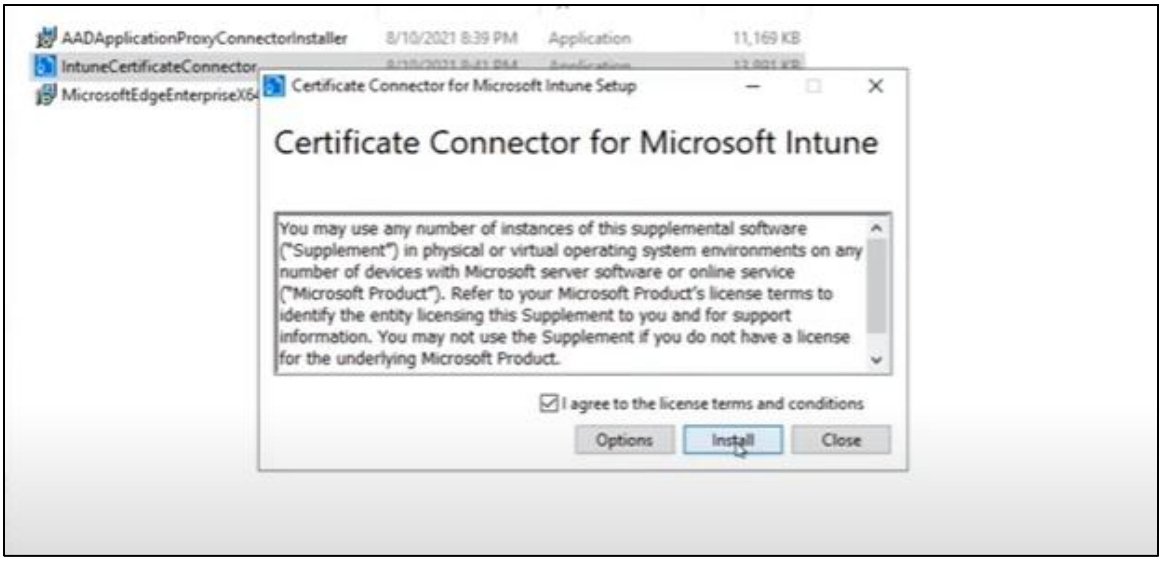
Pre Authentication: Azure Active Directory

Connector Group: Default - Australia

- Test the external URL in a web browser to verify accessibility.

Step 8: Installing the Intune Certificate Connector

- Download the Intune Certificate Connector from the Intune portal under Tenant Admin > Connectors and Tokens.
- Run the installer on the NDES server with Administrator privileges.



```
AADApplicationProxyConnectorInstaller   8/10/2021 8:39 PM   Application   11,169 KB
IntuneCertificateConnector              8/10/2021 8:41 PM   Application   12,001 KB
MicrosoftEdgeEnterpriseX64
```

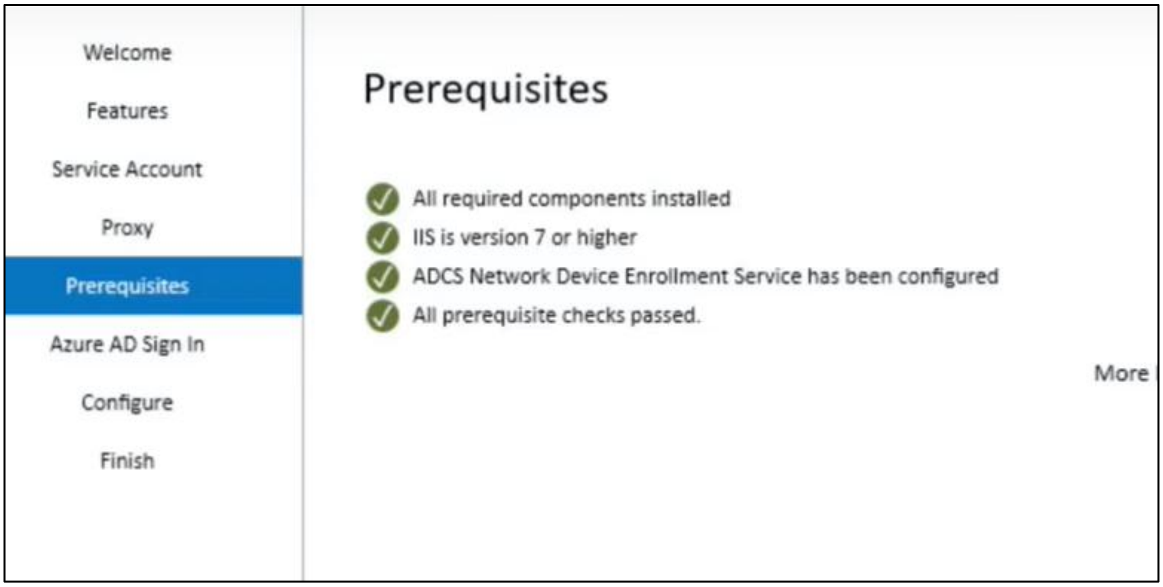
Certificate Connector for Microsoft Intune Setup

Certificate Connector for Microsoft Intune

You may use any number of instances of this supplemental software ("Supplement") in physical or virtual operating system environments on any number of devices with Microsoft server software or online service ("Microsoft Product"). Refer to your Microsoft Product's license terms to identify the entity licensing this Supplement to you and for support information. You may not use the Supplement if you do not have a license for the underlying Microsoft Product.

☑ I agree to the license terms and conditions

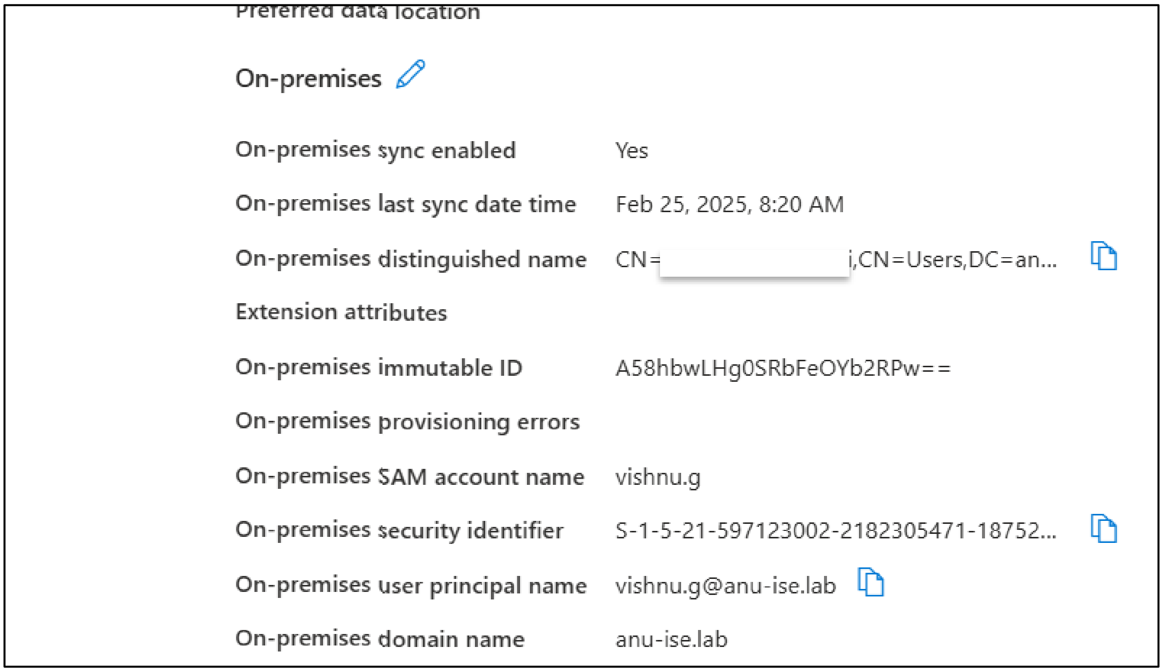
- Select 'SCEP' during the setup wizard and proceed.
- Choose to use the System account and run the prerequisite check.



Prerequisites

- ✓ All required components installed
- ✓ IIS is version 7 or higher
- ✓ ADCS Network Device Enrollment Service has been configured
- ✓ All prerequisite checks passed.

- Select 'Public Commercial Cloud' and sign in with an admin account.
- Ensure the admin account has 'Log on as a service' rights via 'gpedit.msc'.
- The admin account should be in the Azure AD and on-Prem AD



Preferred data location

On-premises

On-premises sync enabled	Yes
On-premises last sync date time	Feb 25, 2025, 8:20 AM
On-premises distinguished name	CN=[redacted]i,CN=Users,DC=an...
Extension attributes	
On-premises immutable ID	A58hbwLHg0SRbFeOYb2RPw==
On-premises provisioning errors	
On-premises SAM account name	vishnu.g
On-premises security identifier	S-1-5-21-597123002-2182305471-18752...
On-premises user principal name	vishnu.g@anu-ise.lab
On-premises domain name	anu-ise.lab

- Complete the installation and click Finish.

Step 9: Validation and Lockdown

- Attempt to access the NDES site; it should return '403 Forbidden' unless proper credentials are used.

- Verify that CA-issued certificates, IIS bindings, and Azure AD App Proxy routing are functioning correctly.

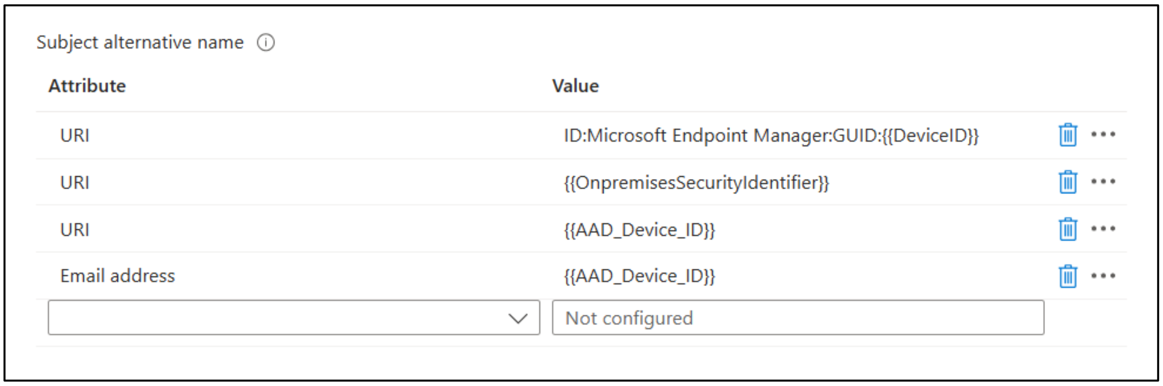
Step 10: Creating Certificate Deployment Profiles in Intune

Trusted Root Certificate Profile:

- Export the root CA certificate in Base64 format.
- In Intune portal, navigate to Devices > Windows > Configuration Profiles.
- Create a new Trusted Certificate profile for Windows 10 or later.
- Upload the exported root certificate and set the destination store to 'Computer Certificate Store – Root'.
- Assign the profile to the appropriate user or device groups.

SCEP Certificate Profile:

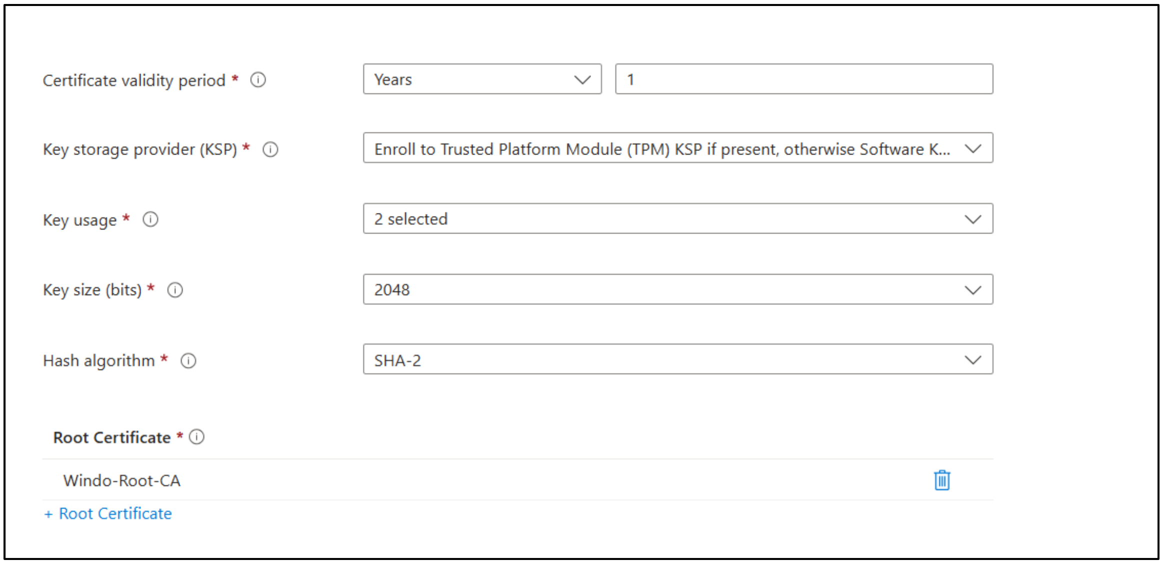
- Create a new SCEP certificate profile in Intune.
- Configure it for Device or User as needed.
- Set the subject name format, e.g., CN={{DeviceName}}.



Subject alternative name

Attribute	Value
URI	ID:Microsoft Endpoint Manager:GUID:{{DeviceID}}
URI	{{OnpremisesSecurityIdentifier}}
URI	{{AAD_Device_ID}}
Email address	{{AAD_Device_ID}}
	Not configured

- Configure the following settings:
- validity period (1 year or less)
- key storage provider (TPM or Software)
- key usage (Digital Signature, Key Encipherment)
- key size (2048-bit), hash algorithm (SHA-2)
- Extended Key Usages matching the template.
- Set the SCEP URL to the Azure AD App Proxy external URL.
- Assign the profile to the same groups as the Trusted Root certificate profile.



Certificate validity period * ⓘ Years 1

Key storage provider (KSP) * ⓘ Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software K...

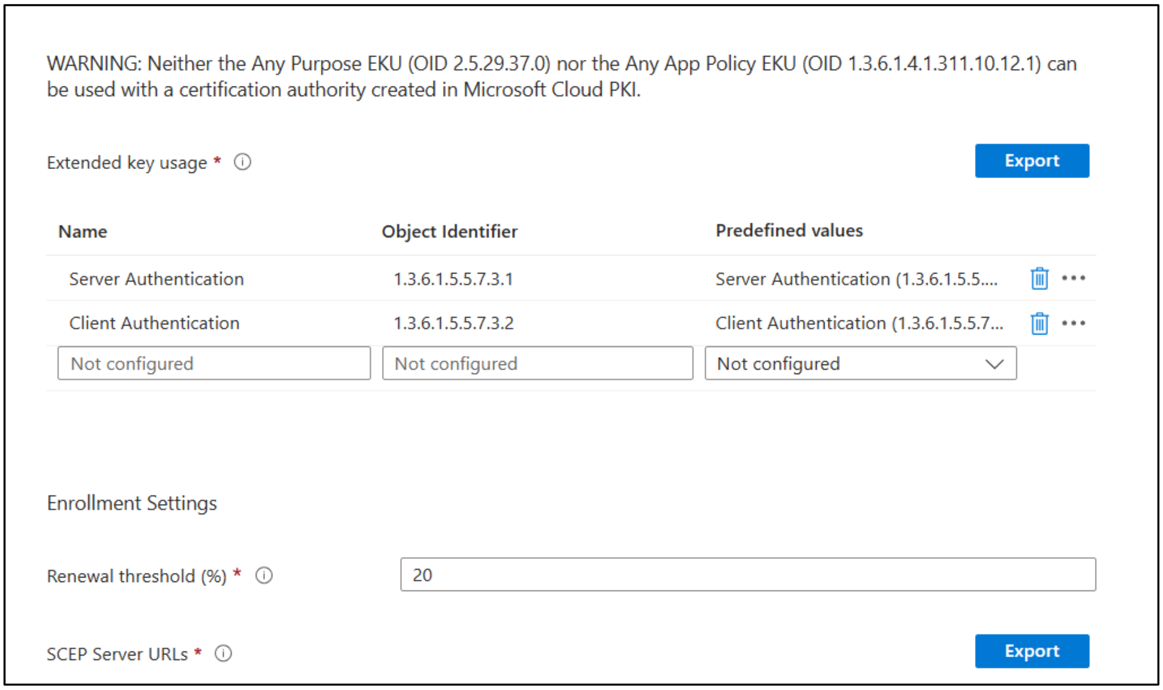
Key usage * ⓘ 2 selected

Key size (bits) * ⓘ 2048

Hash algorithm * ⓘ SHA-2

Root Certificate * ⓘ

Windo-Root-CA



WARNING: Neither the Any Purpose EKU (OID 2.5.29.37.0) nor the Any App Policy EKU (OID 1.3.6.1.4.1.311.10.12.1) can be used with a certification authority created in Microsoft Cloud PKI.

Extended key usage * ⓘ

Name	Object Identifier	Predefined values
Server Authentication	1.3.6.1.5.5.7.3.1	Server Authentication (1.3.6.1.5.5....
Client Authentication	1.3.6.1.5.5.7.3.2	Client Authentication (1.3.6.1.5.5.7...
Not configured	Not configured	Not configured

Enrollment Settings

Renewal threshold (%) * ⓘ 20

SCEP Server URLs * ⓘ

- Save the profile.

Conclusion

Implementing certificate deployment with Intune and Windows Server NDES/SCEP enables secure, scalable device authentication across enterprise environments. The integration with Azure AD Application Proxy ensures secure external accessibility, while Intune simplifies profile management.

I hope this guide helps you in your deployment projects. Feel free to reach out if you have questions or want to discuss further!