Configure 802.1X on APs for PEAP or EAP-TLS with LSC

Contents

Introduction

This document describes how to authenticate Cisco access points on their switchport using 802.1X PEAP or EAP-TLS methods.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireless Controller
- Access Point
- Switch

- ISE server
- Certificate Authority.

Components Used

The information in this document is based on these software and hardware versions:

- Wireless controller: C9800-40-K9 running 17.09.02
- Access Point: C9117AXI-D
- Switch: C9200L-24P-4G running 17.06.04
- AAA server: ISE-VM-K9 running 3.1.0.518
- Certificate Authority: Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background information

If you want your access points (APs) to authenticate with their switchport using 802.1X, by default they use the EAP-FAST authentication protocol which does not require certificates. If you want the APs to use the PEAP-mschapv2 method (which uses credentials on the AP side but a certificate on the RADIUS side) or the EAP-TLS method (which uses certificates on both sides), you have to configure LSC first. It is the only way to provision a trusted/root certificate onto an access point (and also a device certificate in the case of EAP-TLS). It is not possible for the AP to do PEAP and ignore the server side validation. This document first covers configuring LSC and then the 802.1X configuration side.

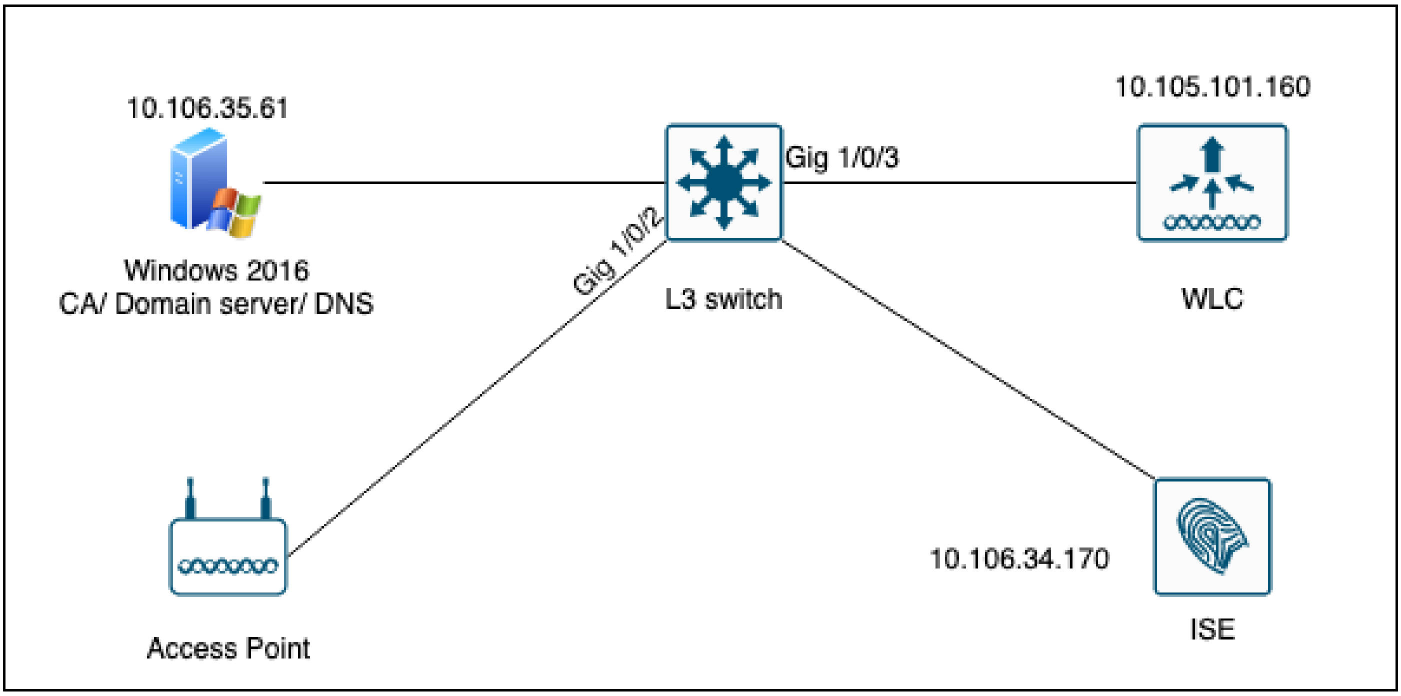
Use a LSC if you want your PKI to provide better security, have control of your Certificate Authority (CA), and define policies, restrictions, and usages on the generated certificates.

With LSC, the controller gets a certificate issued by the CA. An AP does not communicate directly with the CA server but the WLC requests certificates on behalf of the joining APs. The CA server details must be configured on the controller and must be accessible.

The controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

The SCEP is a certificate management protocol that the PKI clients and CA servers use to support certificate enrollment and revocation. It is widely used in Cisco and supported by many CA servers. In SCEP, HTTP is used as the transport protocol for the PKI messages. The primary goal of SCEP is the secure issuance of certificates to network devices.

Network Diagram



Configure

There are two things to configure mainly : the SCEP CA and the 9800 WLC.

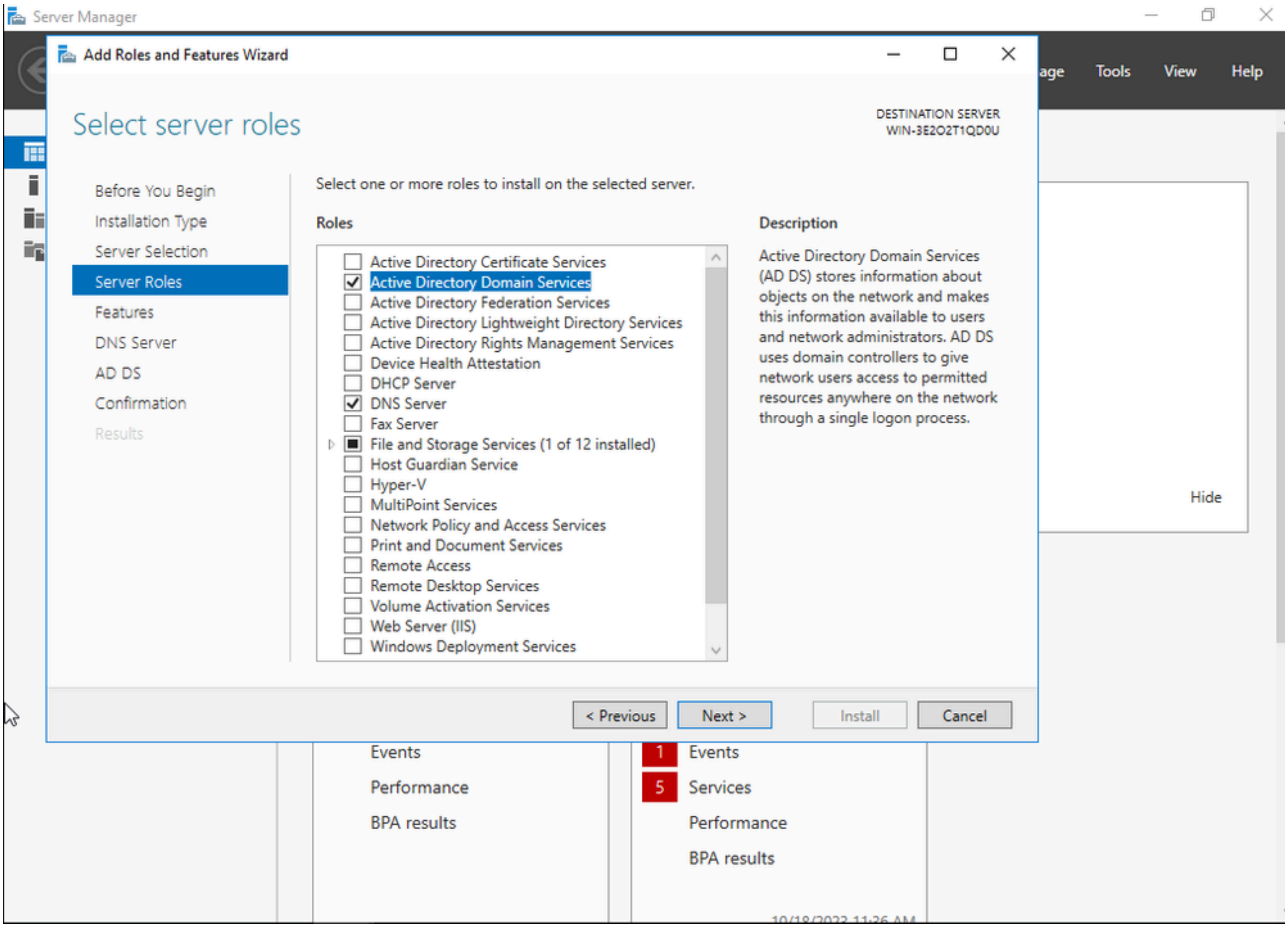
Windows Server 2016 SCEP CA

This document covers a basic install of a Windows Server SCEP CA for lab purposes. An actual production-grade Windows CA must be configured securely and appropriately for enteprise operations. This section is meant to help you test it in the lab as well as take inspiration from the required settings to make this configuration work. Here are the steps :

Step 1. Install a fresh Windows Server 2016 Desktop Experience.

Step 2. Make sure your server is configured with a static IP address.

Step 3.nstall a new role and service, start with Active Directory Domain services and DNS server.



Server Manager

Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-3E2O2T1QD0U

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- DNS Server
- AD DS
- Confirmation
- Results

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

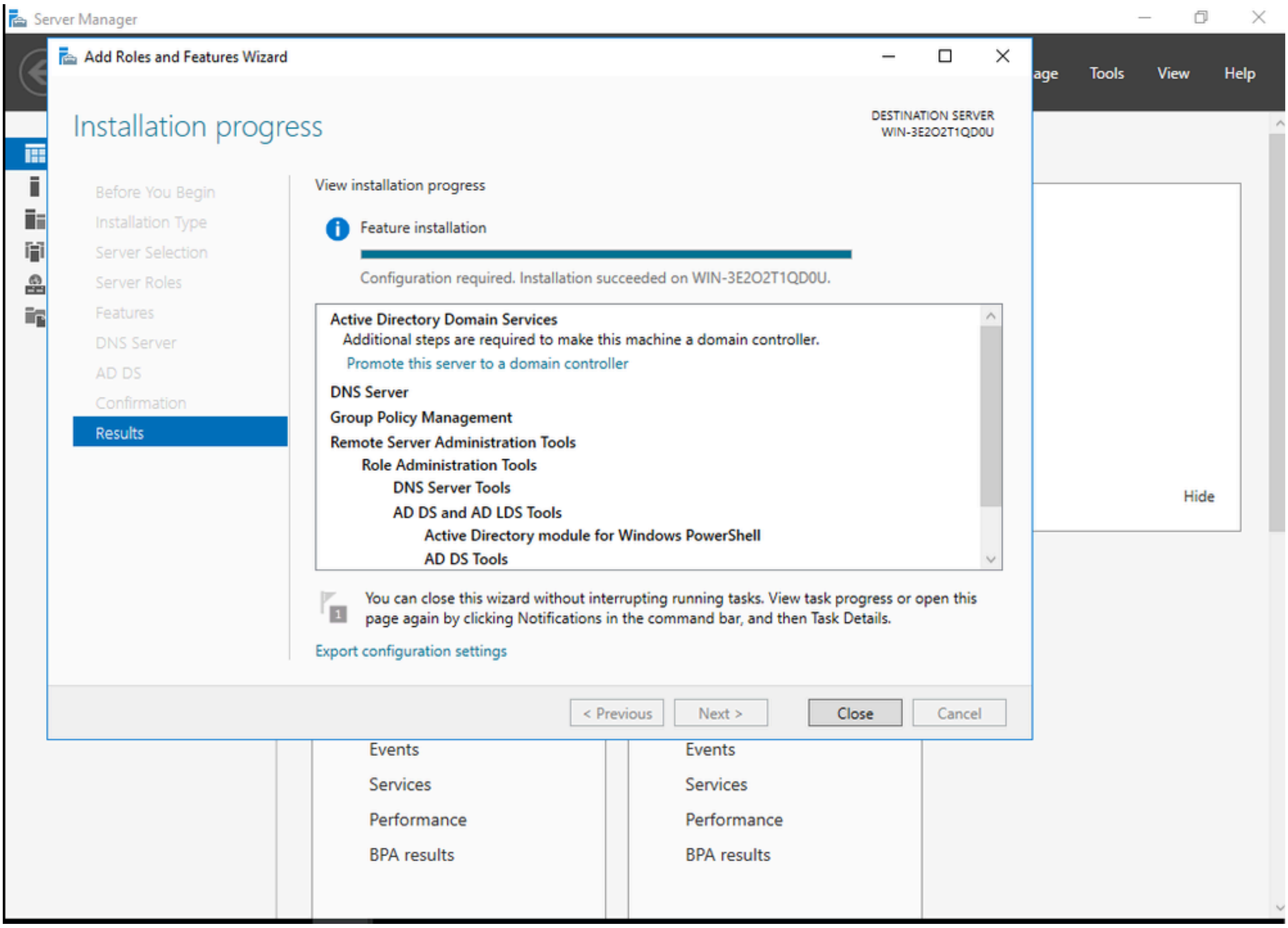
Roles

☐ Active Directory Certificate Services
☑ Active Directory Domain Services
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Device Health Attestation
☐ DHCP Server
☑ DNS Server
☐ Fax Server
■ File and Storage Services (1 of 12 installed)
☐ Host Guardian Service
☐ Hyper-V
☐ MultiPoint Services
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☐ Web Server (IIS)
☐ Windows Deployment Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Active Directory installation



Installation progress

DESTINATION SERVER
WIN-3E2O2T1QD0U

View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-3E2O2T1QD0U.

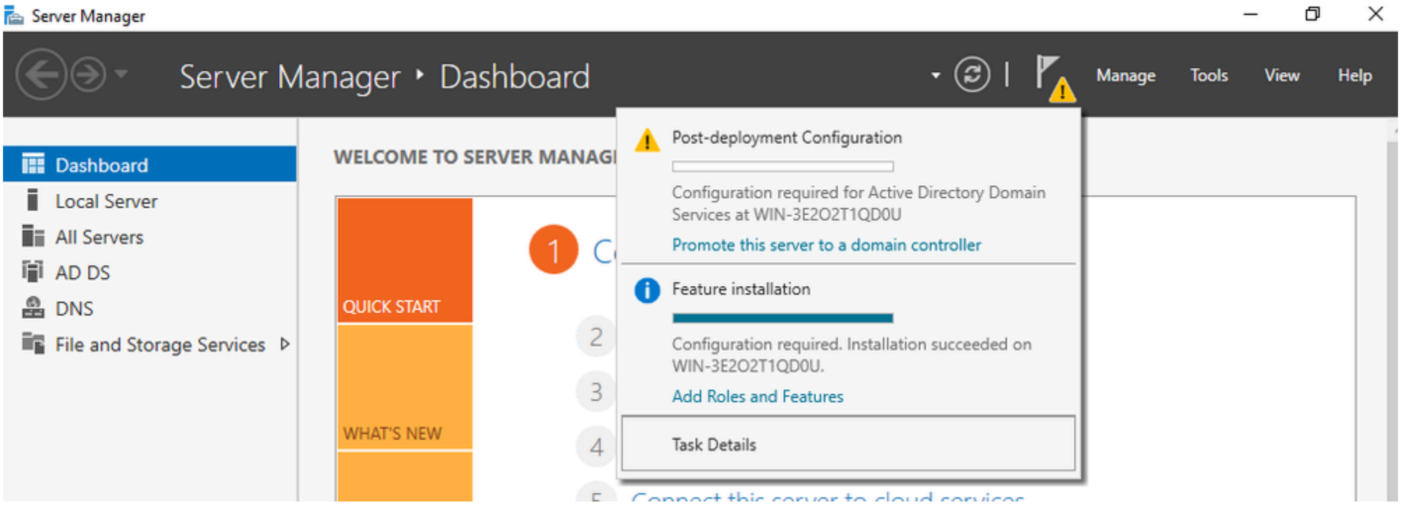
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
DNS Server
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
DNS Server Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

End of AD installation

Step 4. Once done, click in the dashboard on **Promote this server to a domain controller.**



Post-deployment Configuration

Configuration required for Active Directory Domain Services at WIN-3E2O2T1QD0U

Promote this server to a domain controller

Feature installation

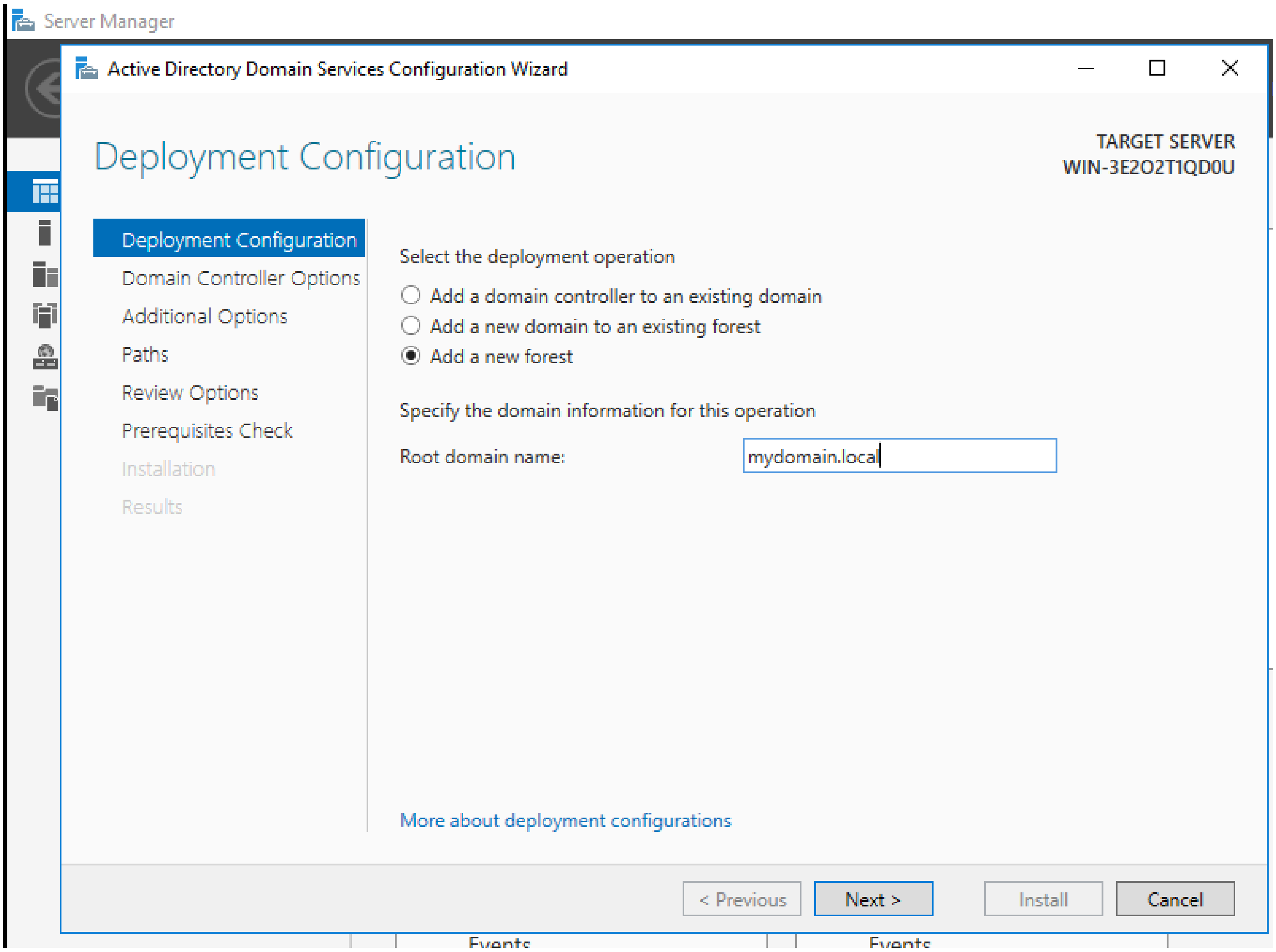
Configuration required. Installation succeeded on WIN-3E2O2T1QD0U.

Add Roles and Features

Task Details

Configure the AD services

Step 5. Create a new forest and chose a domain name.


Server Manager

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-3E2O2T1QD0U

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

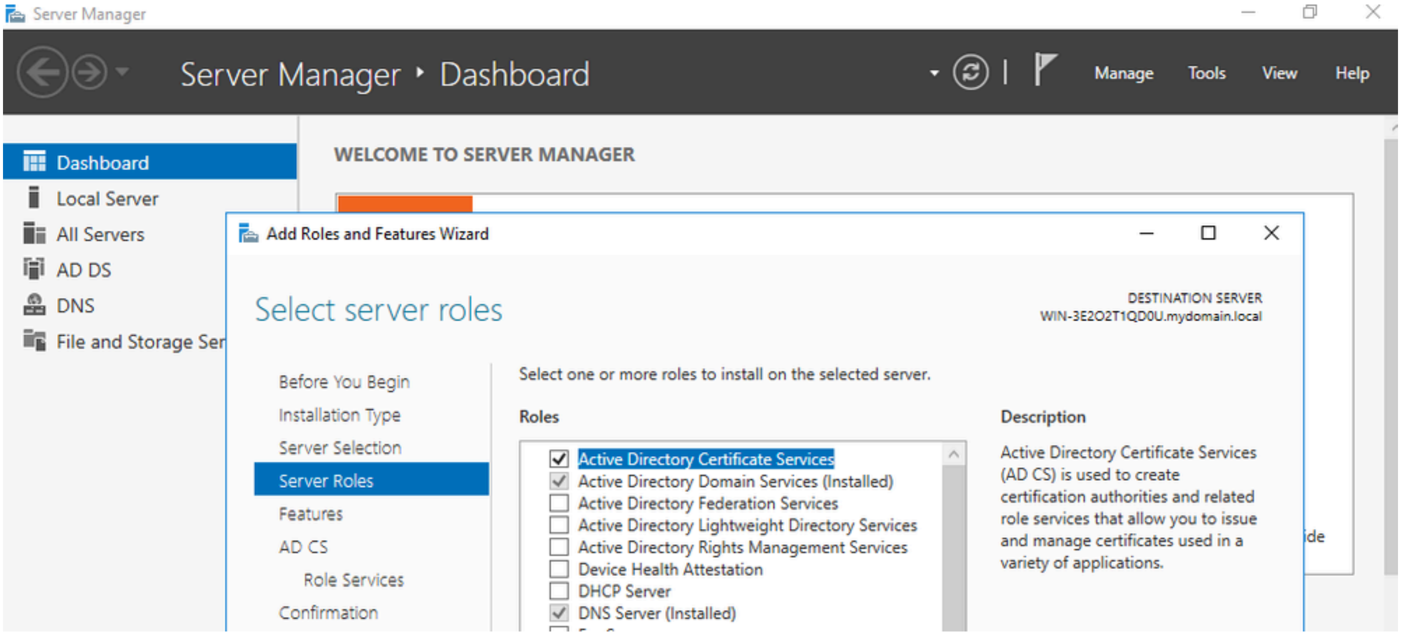
Specify the domain information for this operation

Root domain name: mydomain.local

More about deployment configurations

Chose a forest name

Step 6. Add the Certificate Services role to your server:



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

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

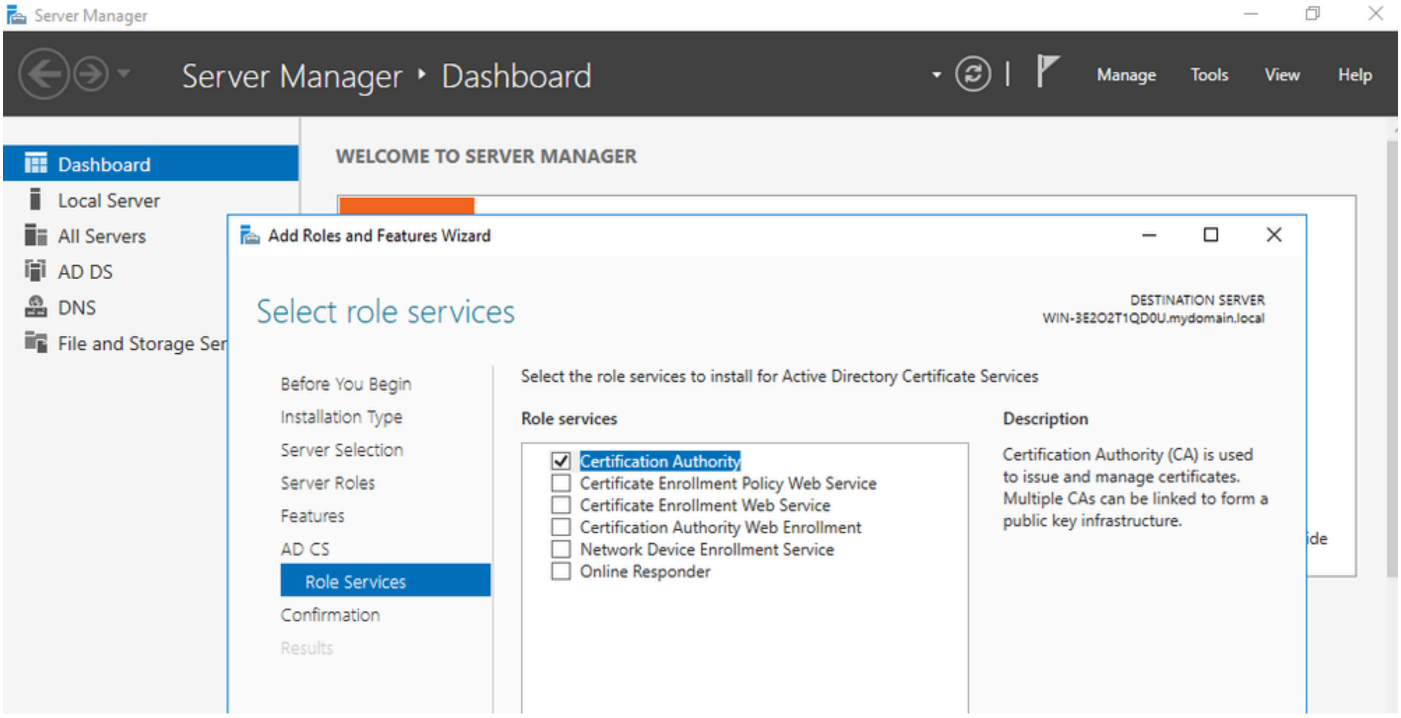
Roles

☑ Active Directory Certificate Services
☑ 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)

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.

Add Certificate services



Select role services

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

Select the role services to install for Active Directory Certificate Services

Role services

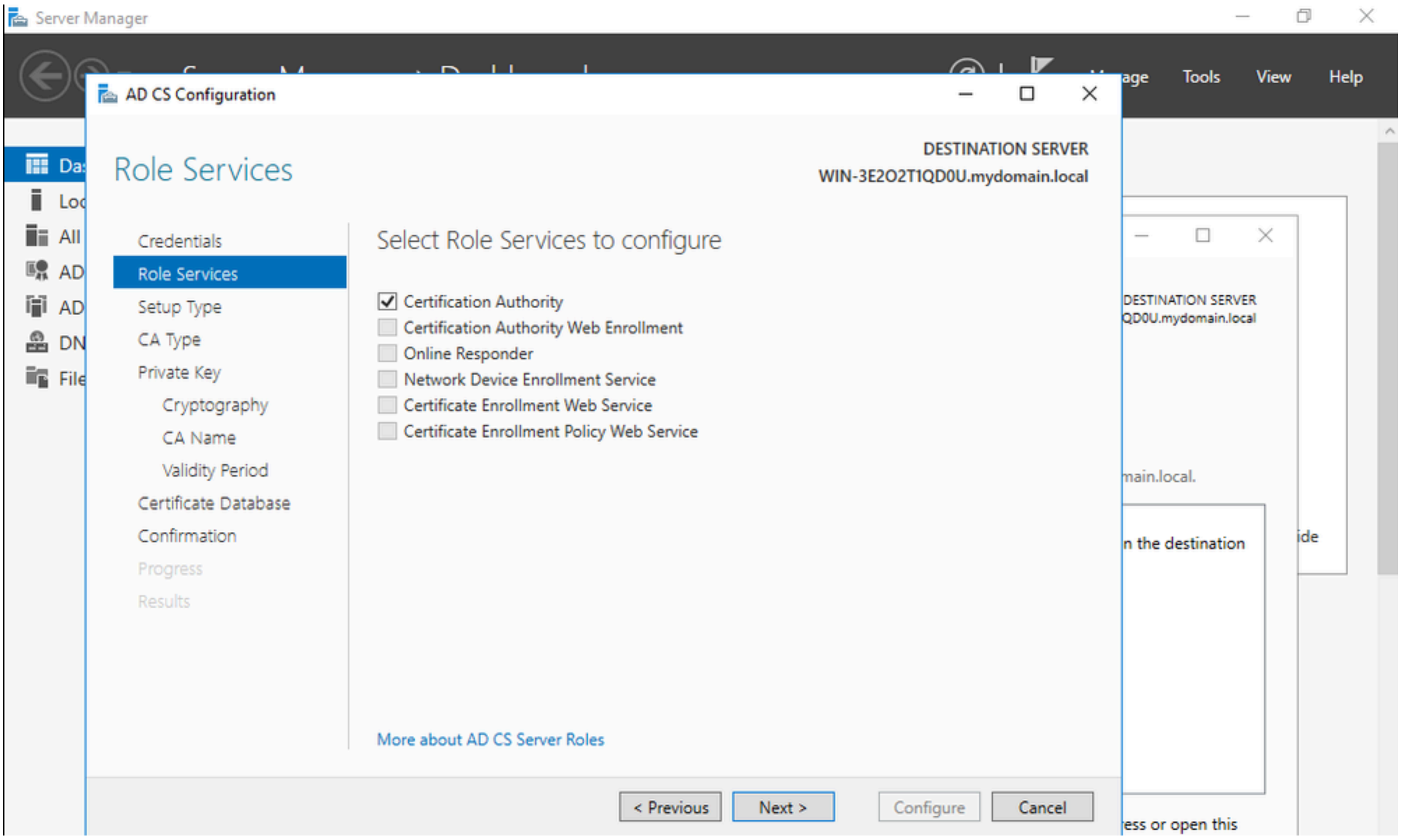
☑ Certification Authority
☐ Certificate Enrollment Policy Web Service
☐ Certificate Enrollment Web Service
☐ Certification Authority Web Enrollment
☐ Network Device Enrollment Service
☐ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

Add just the certification authority

Step 7. Once done, configure your Certification Authority.



Role Services

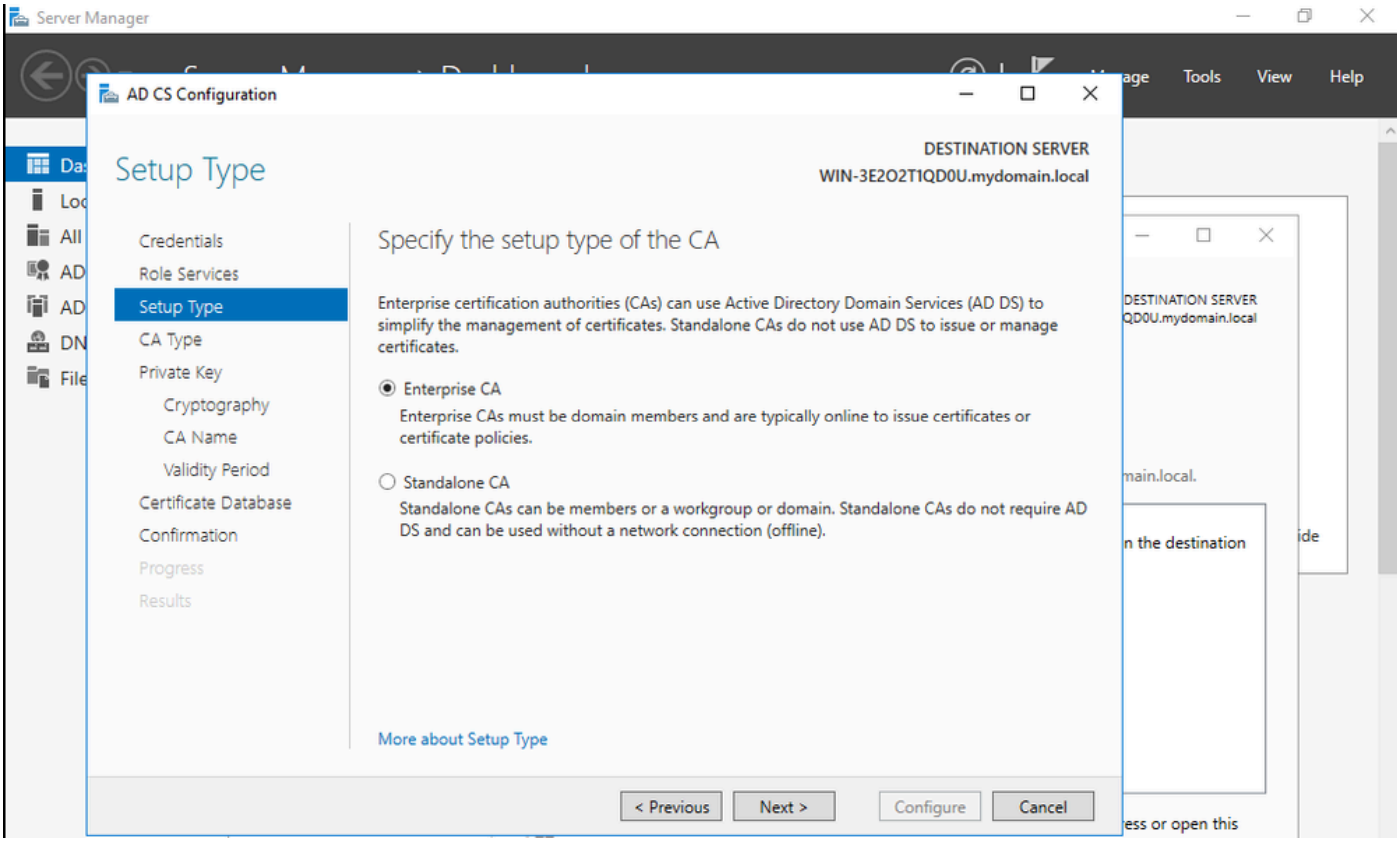
DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

Select Role Services to configure

☑ Certification Authority
☐ Certification Authority Web Enrollment
☐ Online Responder
☐ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

More about AD CS Server Roles

Step 8. Choose Enteprise CA.



Setup Type

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA

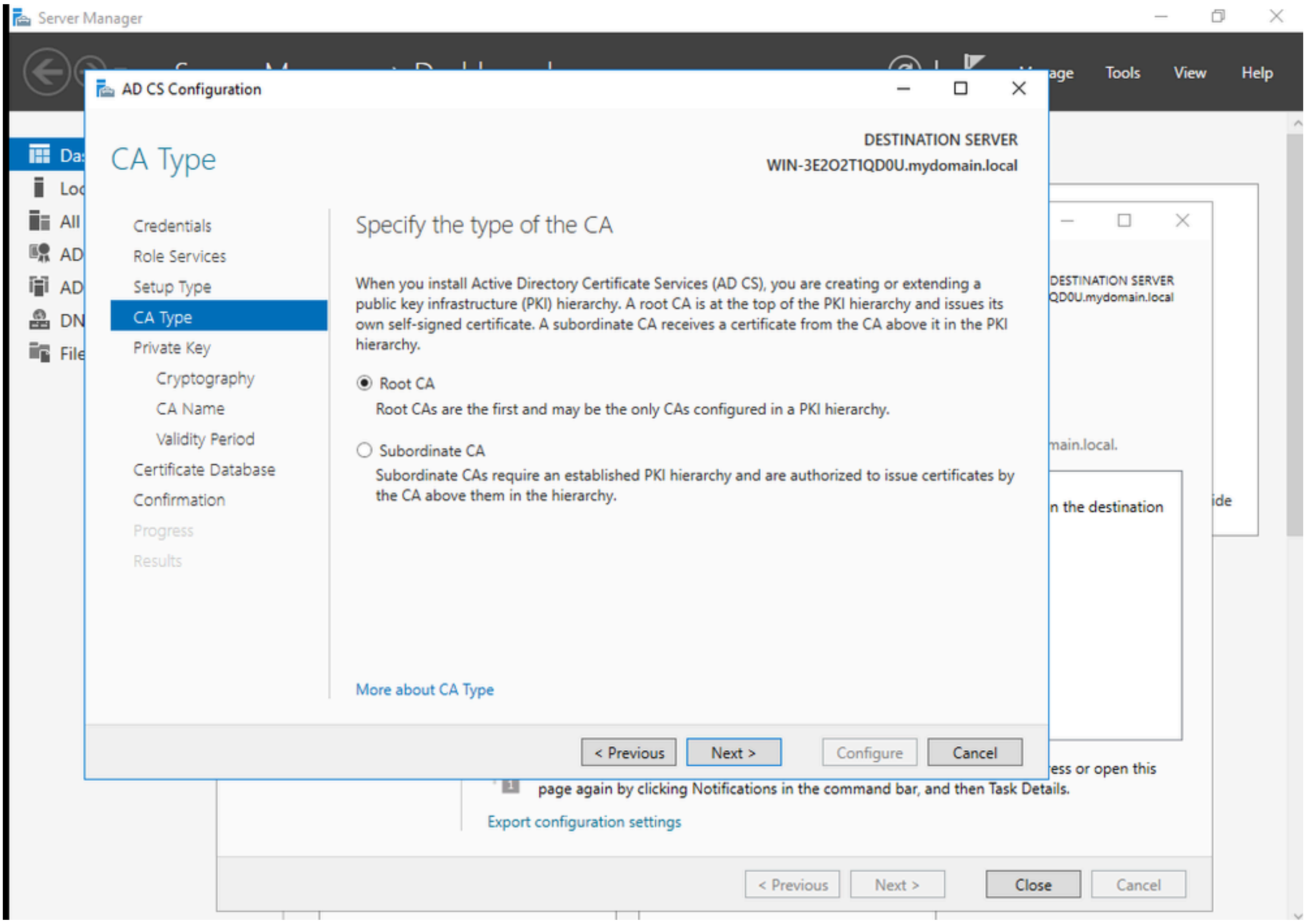
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

Enterprise CA

Step 9. Make it a Root CA. Since Cisco IOS XE 17.6, subordinate CAs are supported for LSC.



CA Type

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA

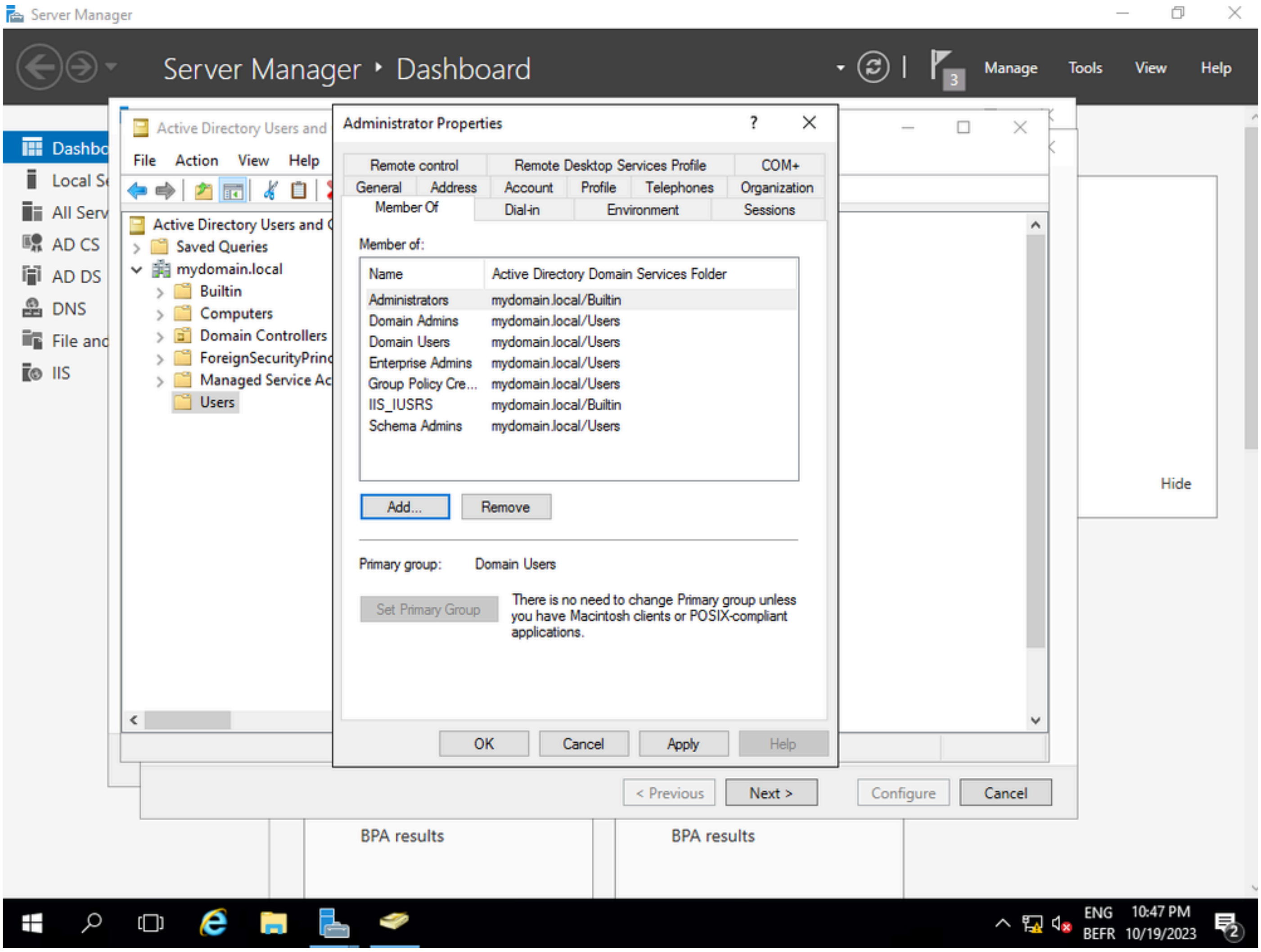
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

Chose a Root CA

It is important to have the account you use for your CA to be part of the IIS_IUSRS group. In this example, you use the Administrator account and go to Active Directory Users and Computers menu to add the Administrator users to the IIS_IUSRS group.



Member of:

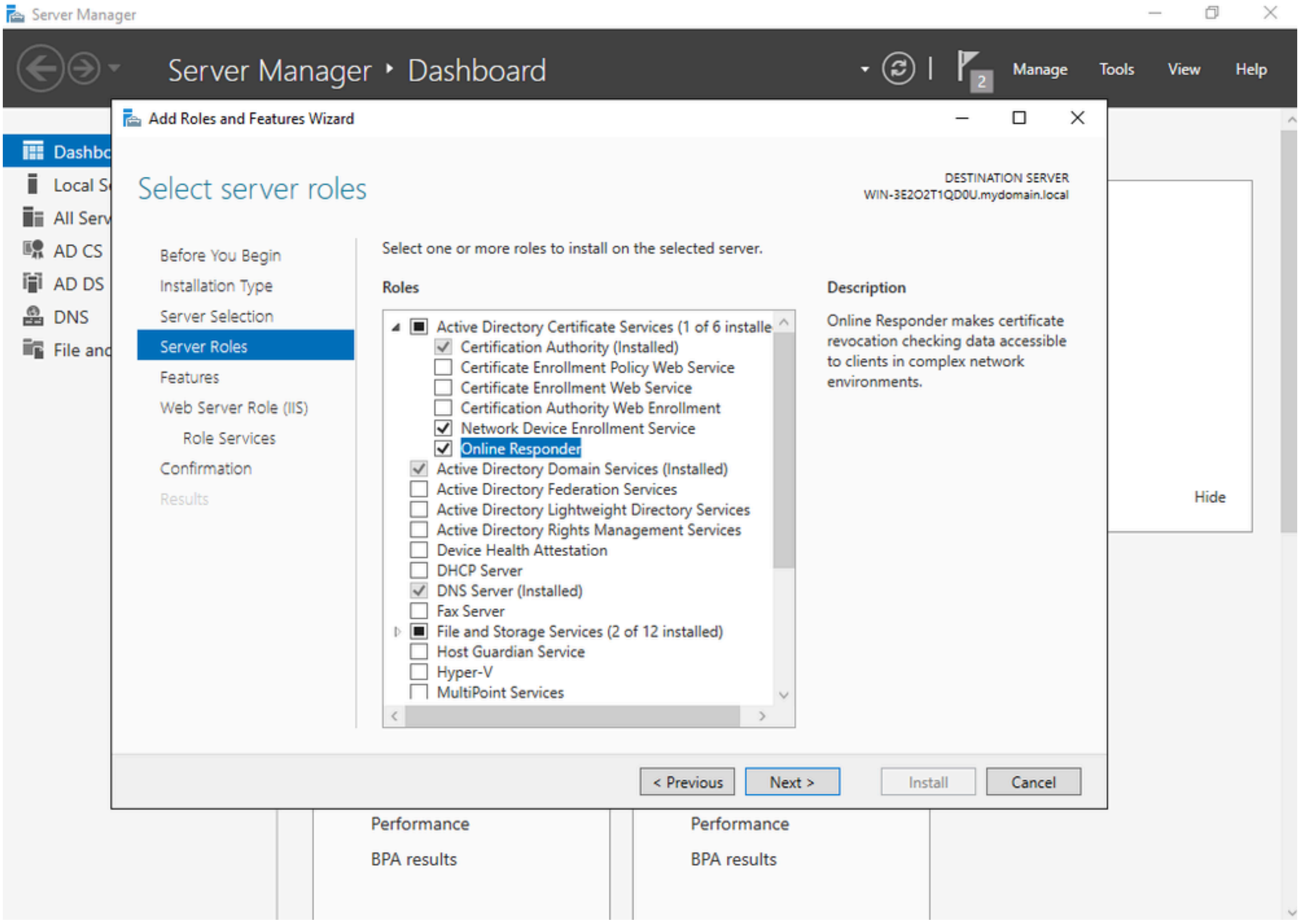
Name	Active Directory Domain Services Folder
Administrators	mydomain.local/Builtin
Domain Admins	mydomain.local/Users
Domain Users	mydomain.local/Users
Enterprise Admins	mydomain.local/Users
Group Policy Cre...	mydomain.local/Users
IIS_IUSRS	mydomain.local/Builtin
Schema Admins	mydomain.local/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Add your admin account to the IIS_USER group

Step 10. Once you have a user in the right IIS group, add roles and services. Then add the Online Responder and NDES services to your Certifiation Authority.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

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

Roles

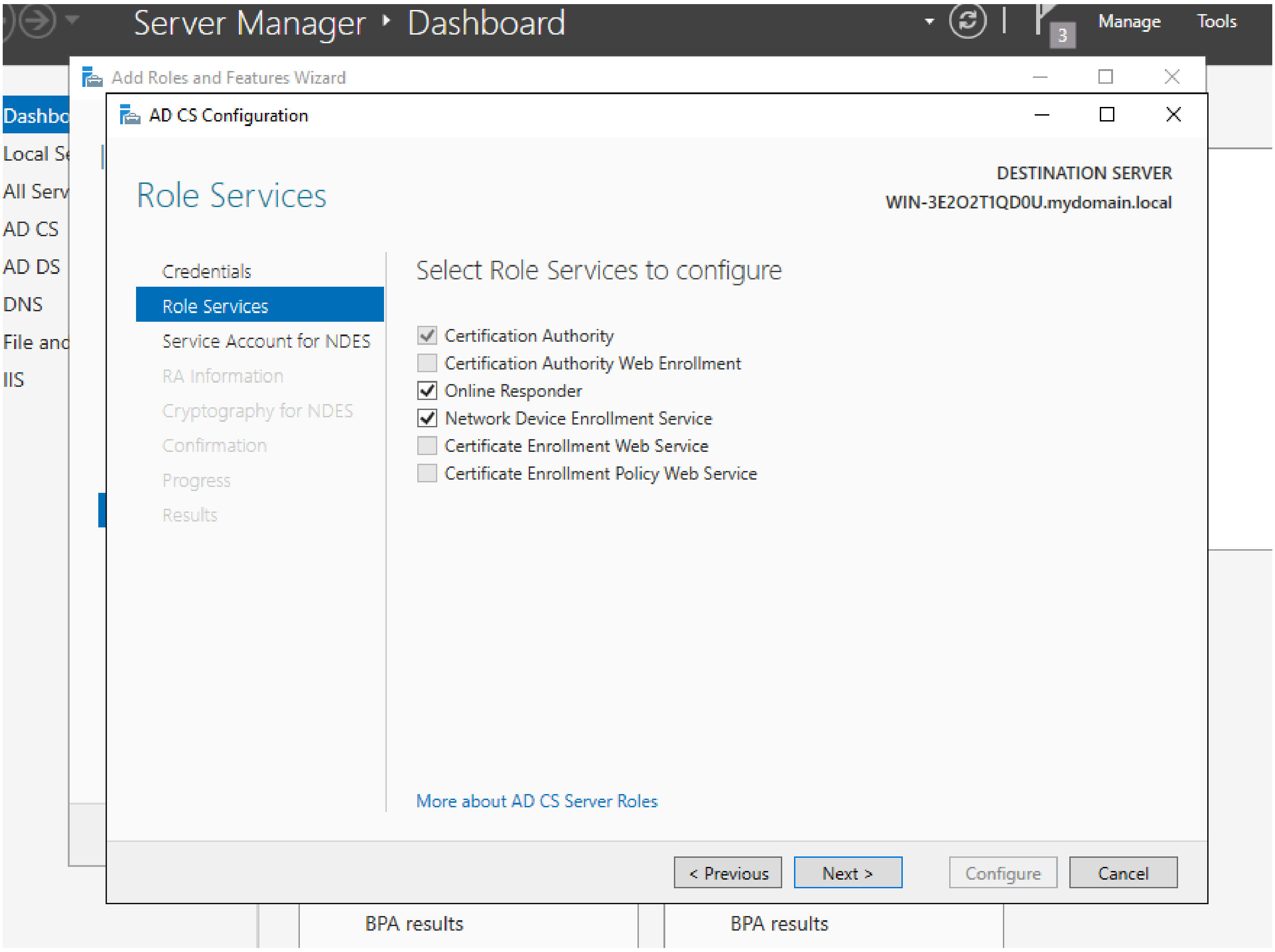
- ■ Active Directory Certificate Services (1 of 6 installe
  - ☑ Certification Authority (Installed)
  - □ Certificate Enrollment Policy Web Service
  - □ Certificate Enrollment Web Service
  - □ Certification Authority Web Enrollment
  - ☑ Network Device Enrollment Service
  - ☑ Online Responder
- ☑ 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
- □ MultiPoint Services

Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Install the NDES and Online responder services

Step 11. Once done, configure those services.



Role Services

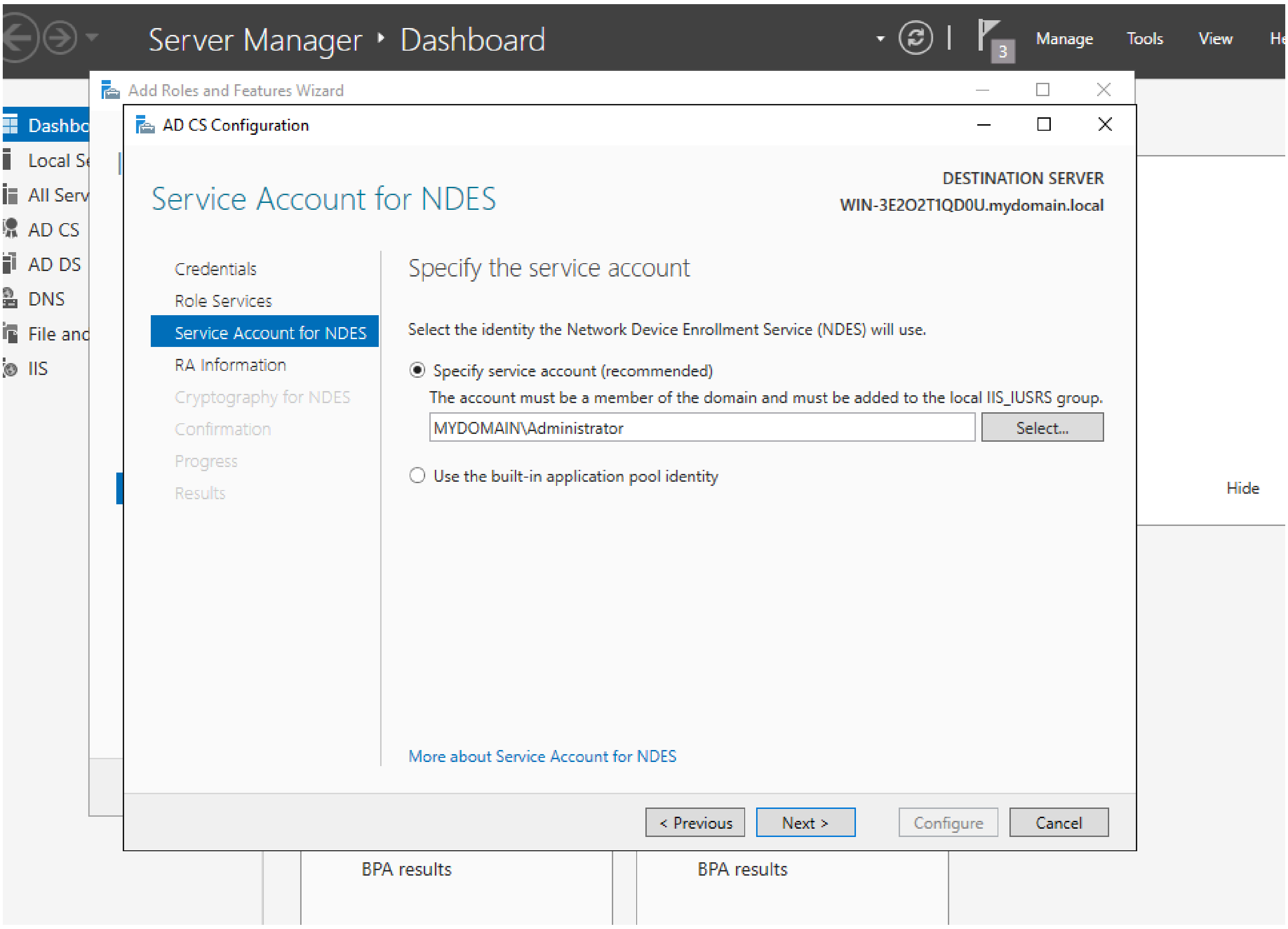
DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

Select Role Services to configure

☑ Certification Authority
☐ Certification Authority Web Enrollment
☑ Online Responder
☑ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

Install the Online responsder and NDES service

Step 12. You are prompted to choose a service account. This is the account that you previously added to the IIS_IUSRS group.



Service Account for NDES

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

Specify the service account

Select the identity the Network Device Enrollment Service (NDES) will use.

● Specify service account (recommended)

The account must be a member of the domain and must be added to the local IIS_IUSRS group.

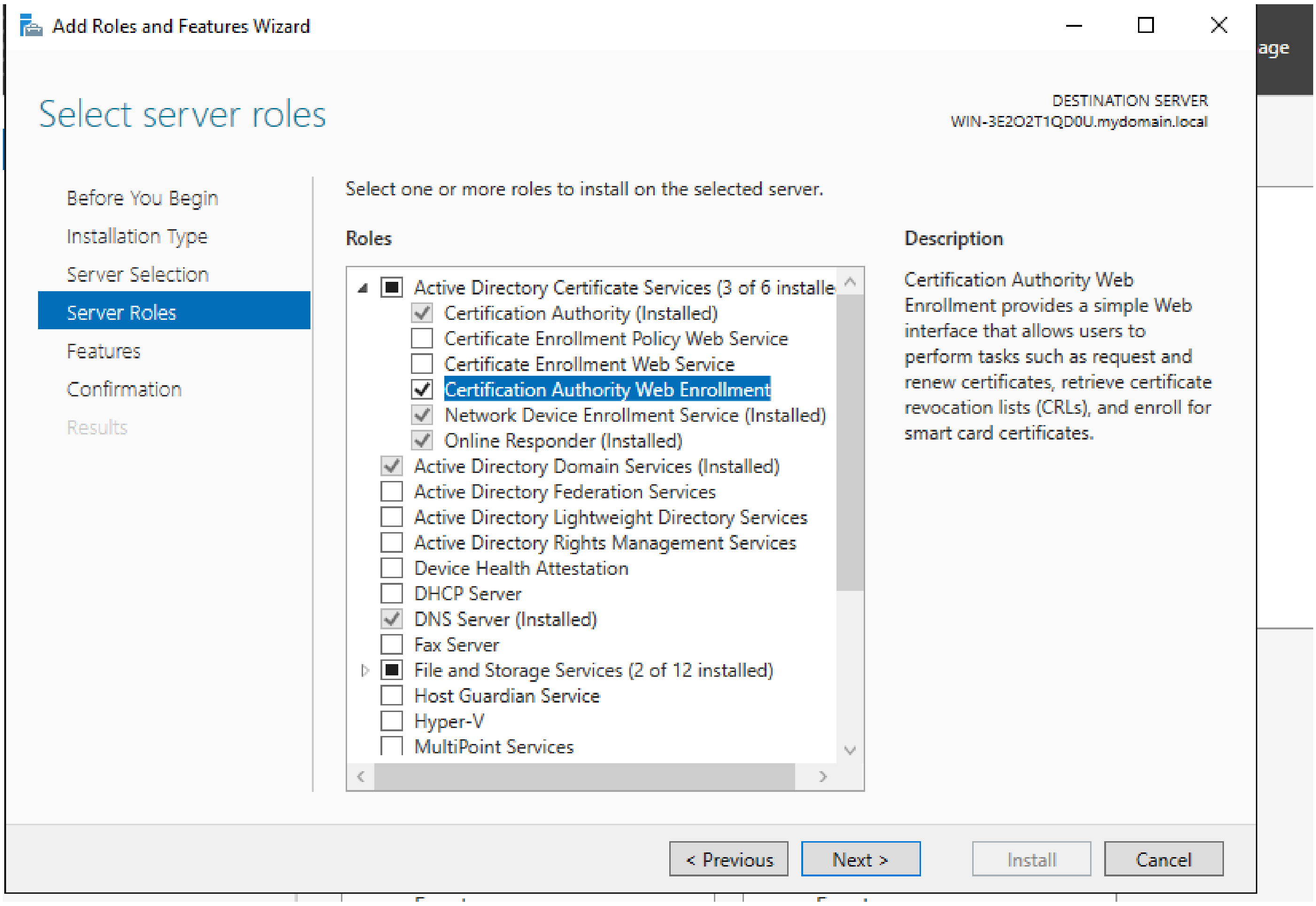
MYDOMAIN\Administrator

○ Use the built-in application pool identity

More about Service Account for NDES

Pick the user that you added to the IIS group

Step 13.This is enough for SCEP operations, but in order to achieve 802.1X authentication, you also need to install a certificate on the RADIUS server. Therefore, for ease, install and configure the web enrollment service in order to be easily able to copy and paste the ISE certificate request on our Windows Server.



Select server roles

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

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

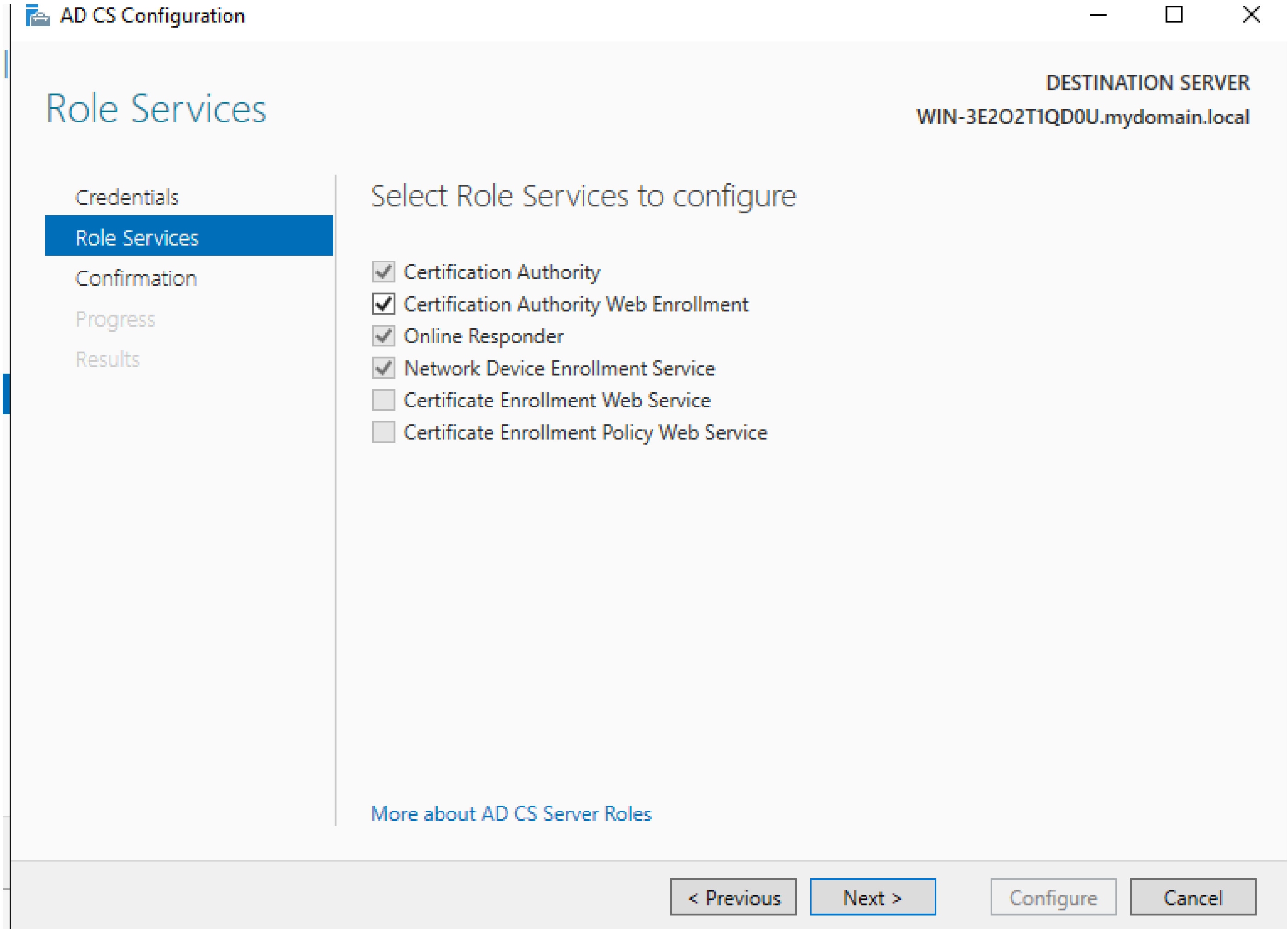
Roles

- ■ Active Directory Certificate Services (3 of 6 installe
  - ☑ Certification Authority (Installed)
  - □ Certificate Enrollment Policy Web Service
  - □ Certificate Enrollment Web Service
  - ☑ Certification Authority Web Enrollment
  - ☑ 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
- □ MultiPoint Services

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

Install the web enrollment service



AD CS Configuration

DESTINATION SERVER
WIN-3E2O2T1QD0U.mydomain.local

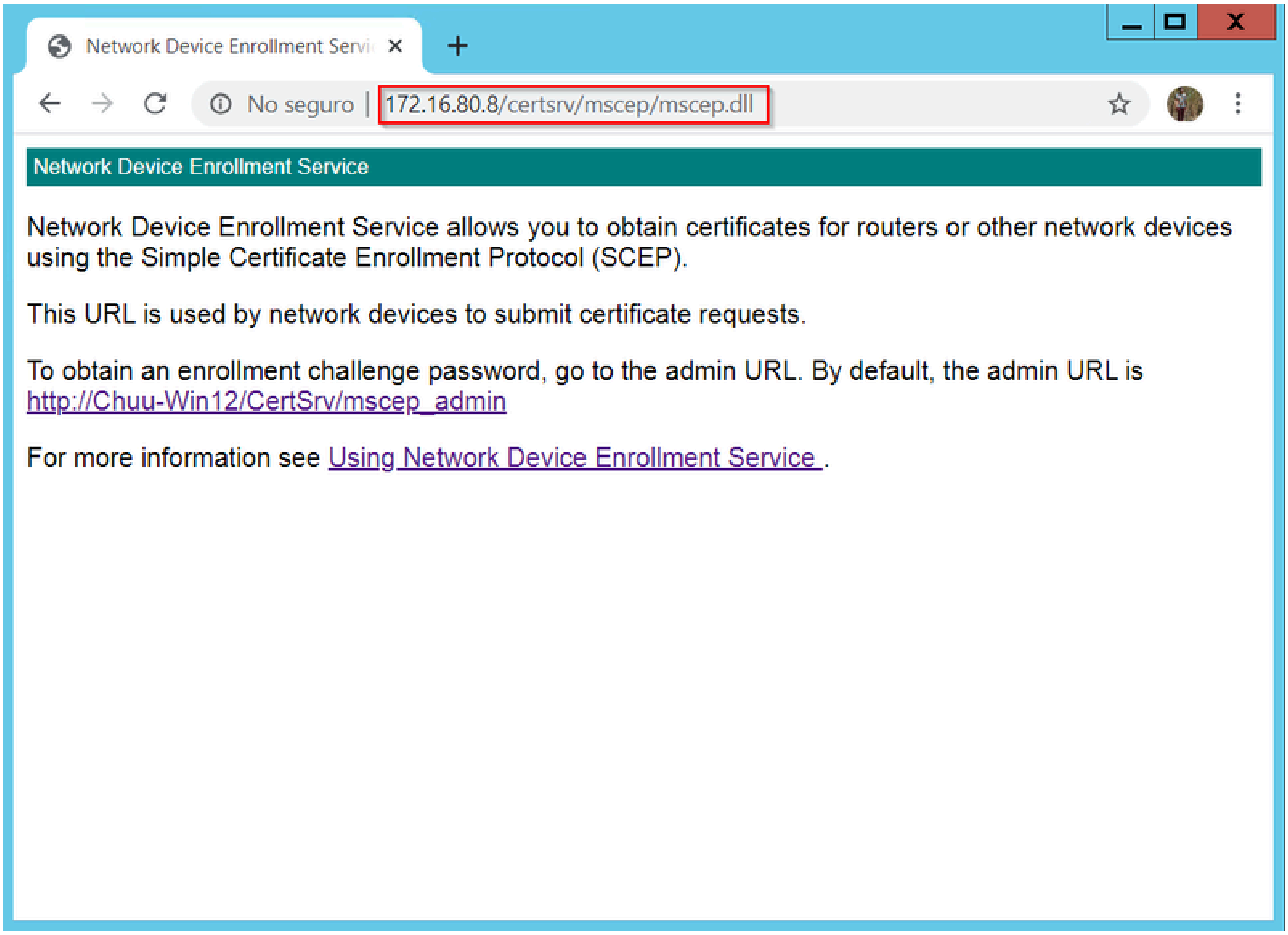
Role Services

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
☑ Online Responder
☑ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

configure the web enrollment service

Step 14. You can verify the SCEP service is operating properly by visiting http://<serverip>/certsrv/mscep/mscep.dll ：



Network Device Enrollment Servi
No seguro
172.16.80.8/certsrv/mscep/mscep.dll

Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

This URL is used by network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is http://Chuu-Win12/CertSrv/mscep_admin

For more information see Using Network Device Enrollment Service .

SCEP Portal Verification

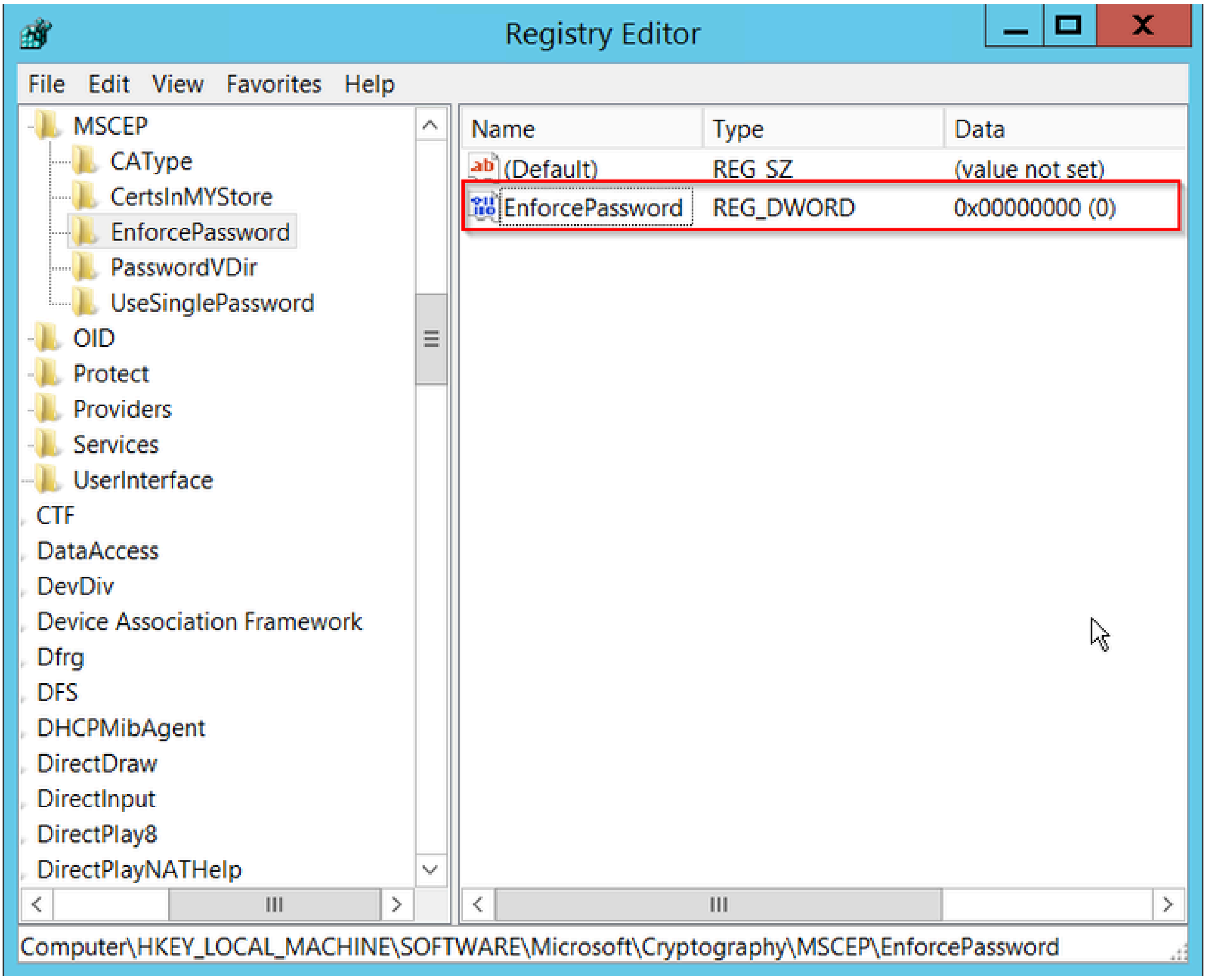
Step 15.

By default, the Windows Server used a dynamic challenge password to authenticate client and endpoint requests before enrollment within Microsoft SCEP (MSCEP). This requires an admin account to browse to the web GUI to generate an on-demand password for each request (the password must be included within the request).The controller is not capable to include this password within the requests it sends to the server. To remove this feature, the registry key on the NDES server needs to be modified:

Open the Registry Editor, search for **Regedit** within the **Start** menu.

Navigate to **Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP** > **EnforcePassword**

Change the **EnforcePassword** value to 0. If it is already 0, then leave it as is.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforcePassword	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

Set the Enforcepassword Value

Configure the certificate template and registry

Certificates and its associated keys can be used in multiple scenarios for different purposes defined by the application policies within the CA Server. The application policy is stored in the Extended Key Usage (EKU) field of the certificate. This field is parsed by the authenticator to verify that it is used by the client for its intended purpose. To make sure that the proper application policy is integrated to the WLC and AP certificates, create the proper certificate template and map it to the NDES registry:

Step 1. Navigate to **Start** > **Administrative Tools** > **Certification Authority**.

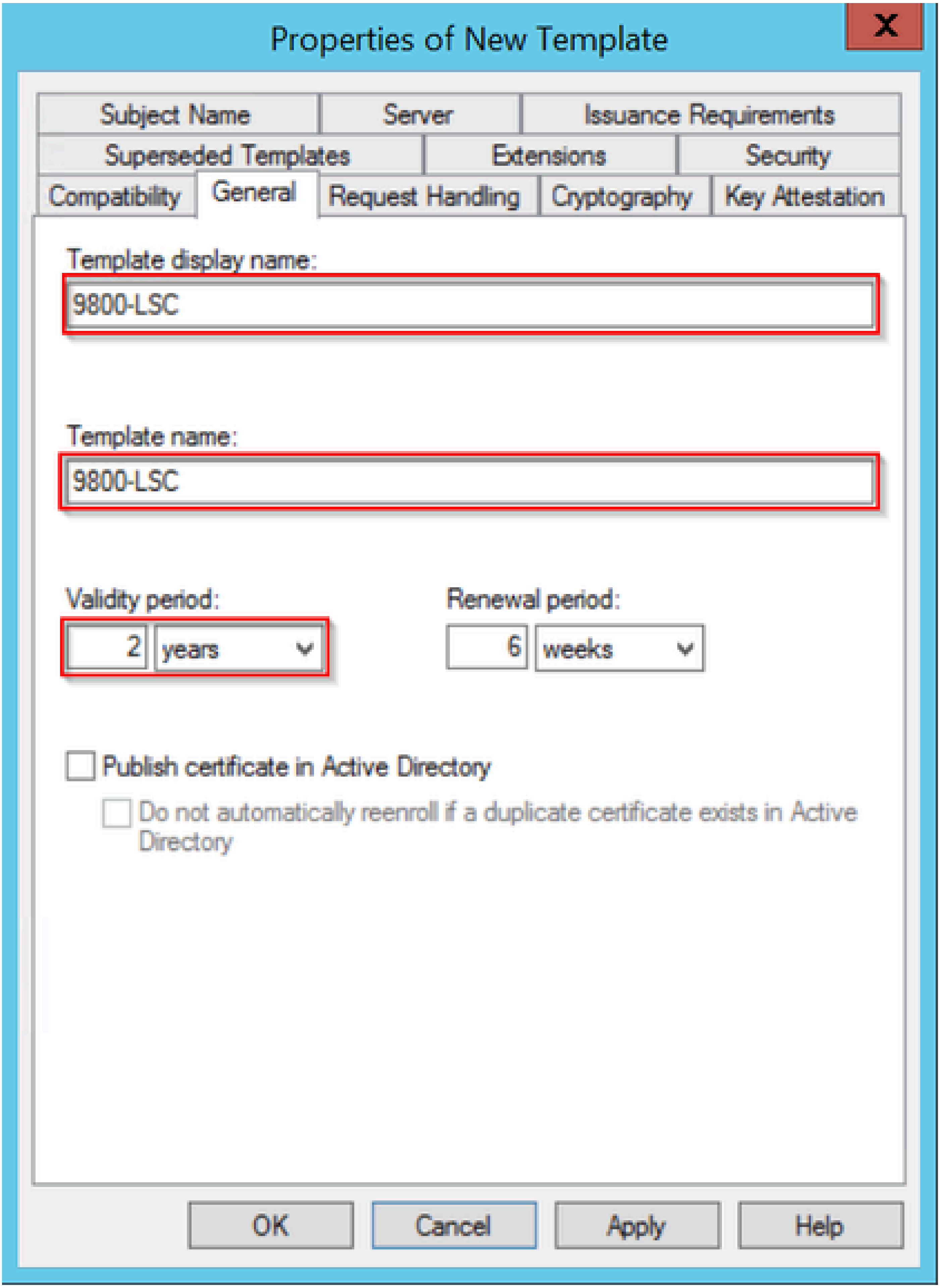
Step 2. Expand the CA Server folder tree, right-click on the **Certificate Templates** folders and select **Manage**.

Step 3. Right-click on the **Users** certificate template, then select **Duplicate Template** in the context menu.

Step 4. Navigate to the **General** tab, change the template name and validity period as desired, leave all other options unchecked.

⚠ **Caution**: When the Validity period is modified, ensure that it is not greater than the Certification

⚠ Authority root certificate validity.



Properties of New Template

Template display name: 9800-LSC

Template name: 9800-LSC

Validity period: 2 years

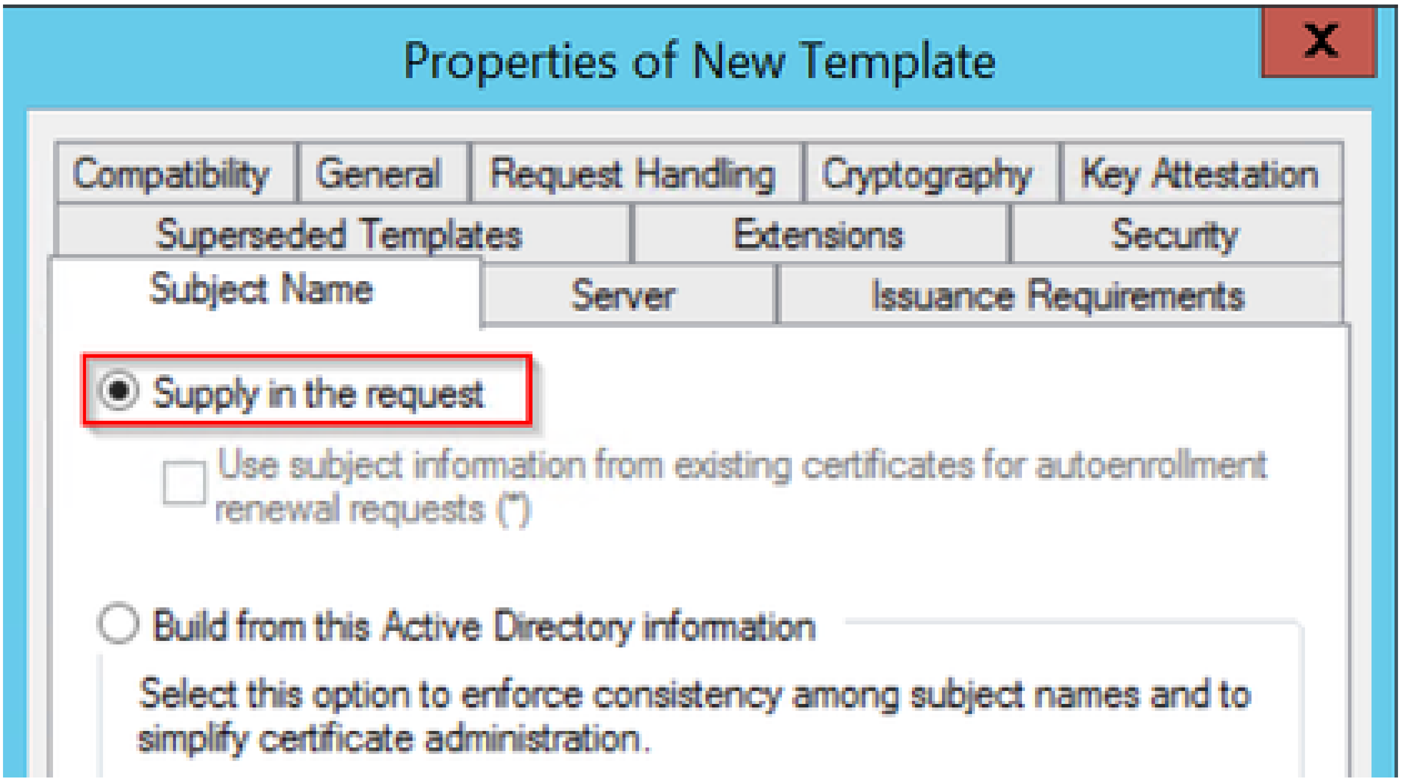
Renewal period: 6 weeks

☐ Publish certificate in Active Directory

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

Configure the Certificate Template

Step 5. Navigate to the **Subject Name** tab, ensure that **Supply in the request** is selected. A pop-up appears to indicate that users do not need admin approval to get their certificate signed, select **OK**.



● Supply in the request

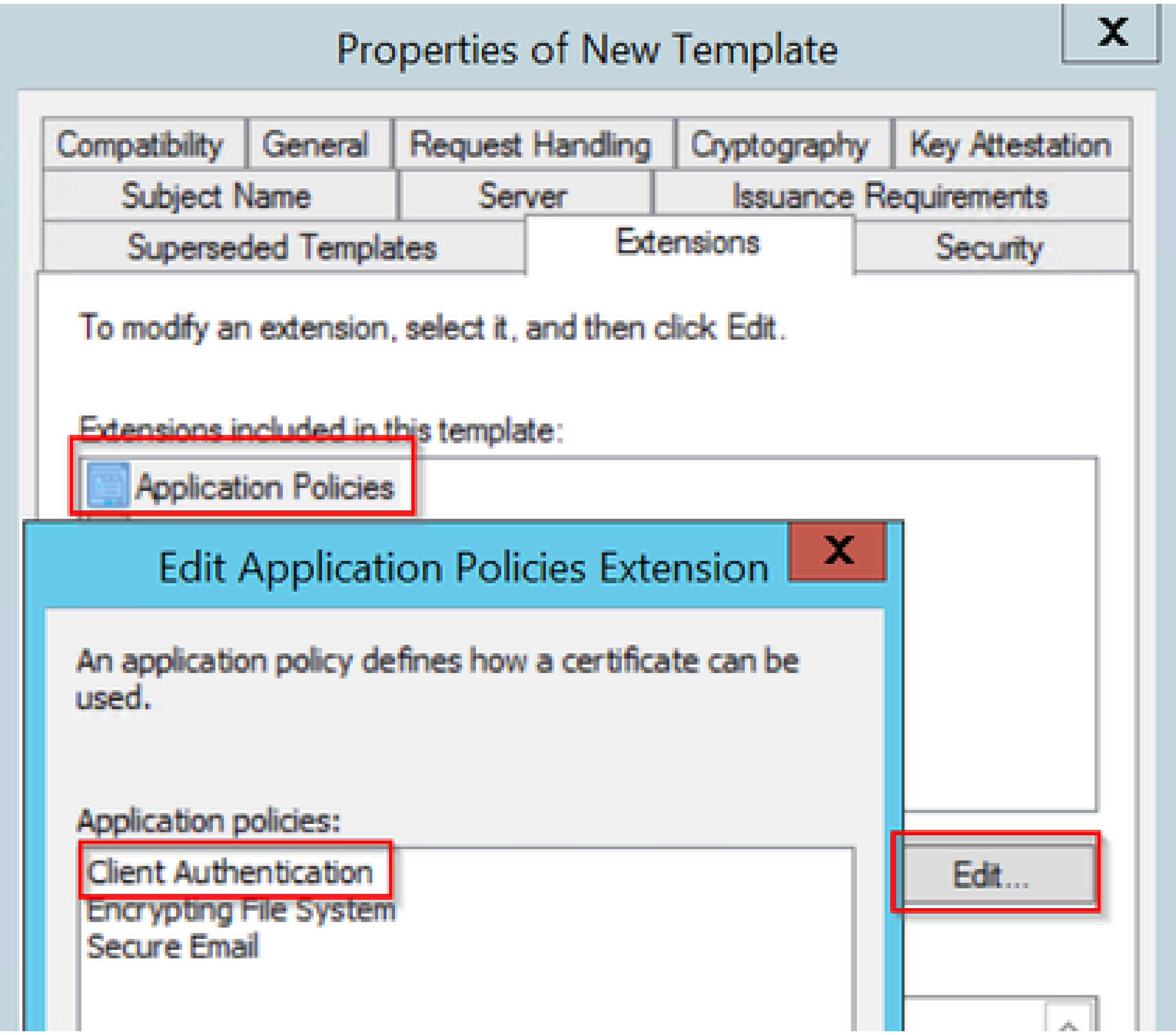
□ Use subject information from existing certificates for autoenrollment renewal requests (*)

○ Build from this Active Directory information

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

Supply in the Request

Step 6. Navigate to the **Extensions** tab, then select the **Application Policies** option and select the **Edit...** button. Ensure that **Client Authentication** is in the **Application Policies** window; otherwise,select **Add** and add it.



To modify an extension, select it, and then click Edit.

Extensions included in this template:

Application Policies

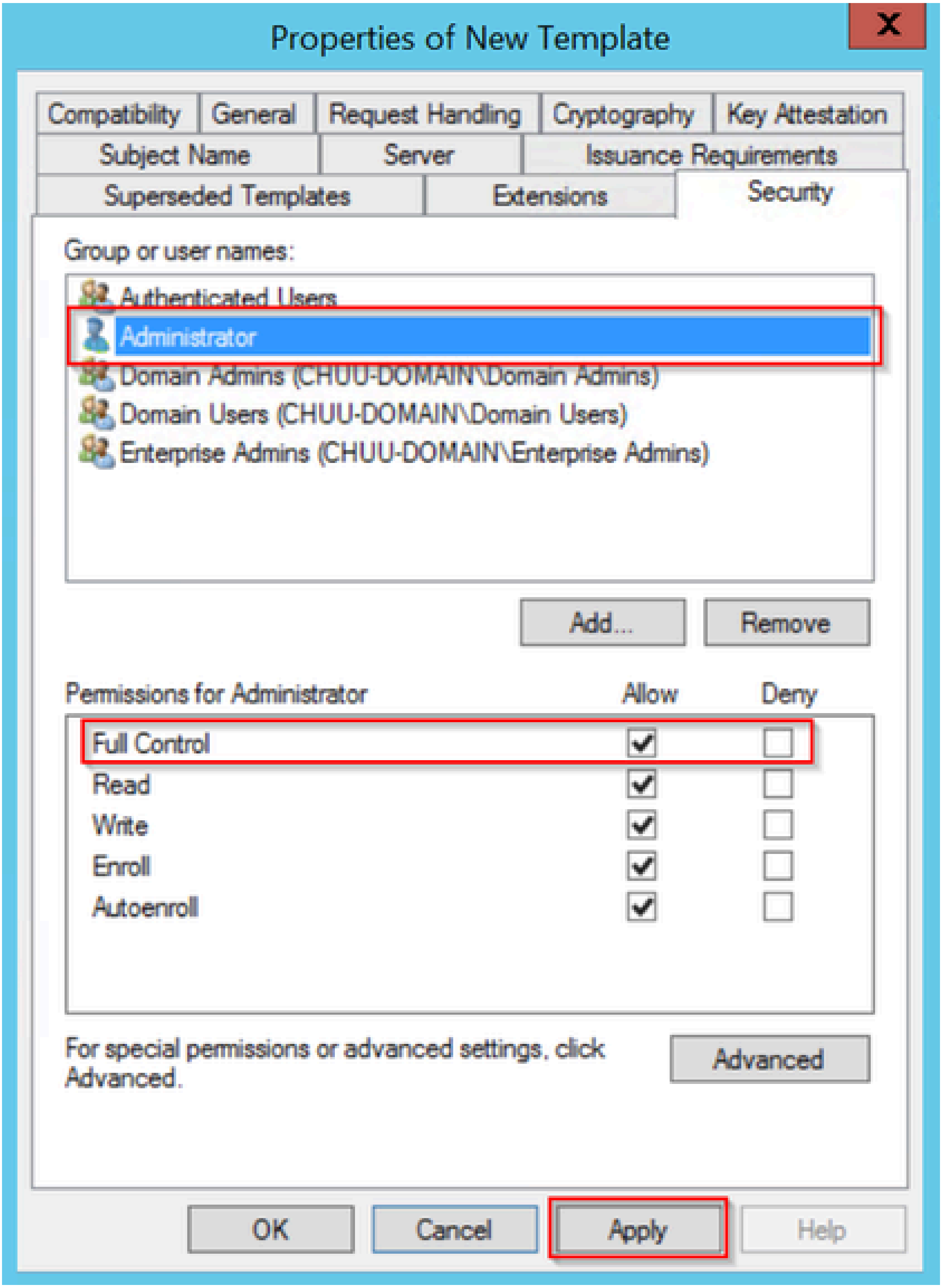
An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Encrypting File System
Secure Email

Verify Extensions

Step 7. Navigate to the **Security** tab, ensure that the service account defined in Step 6 of the **Enable SCEP Services in the Windows Server** has **Full Control** permissions of the template, then select **Apply** and **OK**.



Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (CHUU-DOMAIN\Domain Admins)
- Domain Users (CHUU-DOMAIN\Domain Users)
- Enterprise Admins (CHUU-DOMAIN\Enterprise Admins)

Permissions for Administrator	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	☑	□

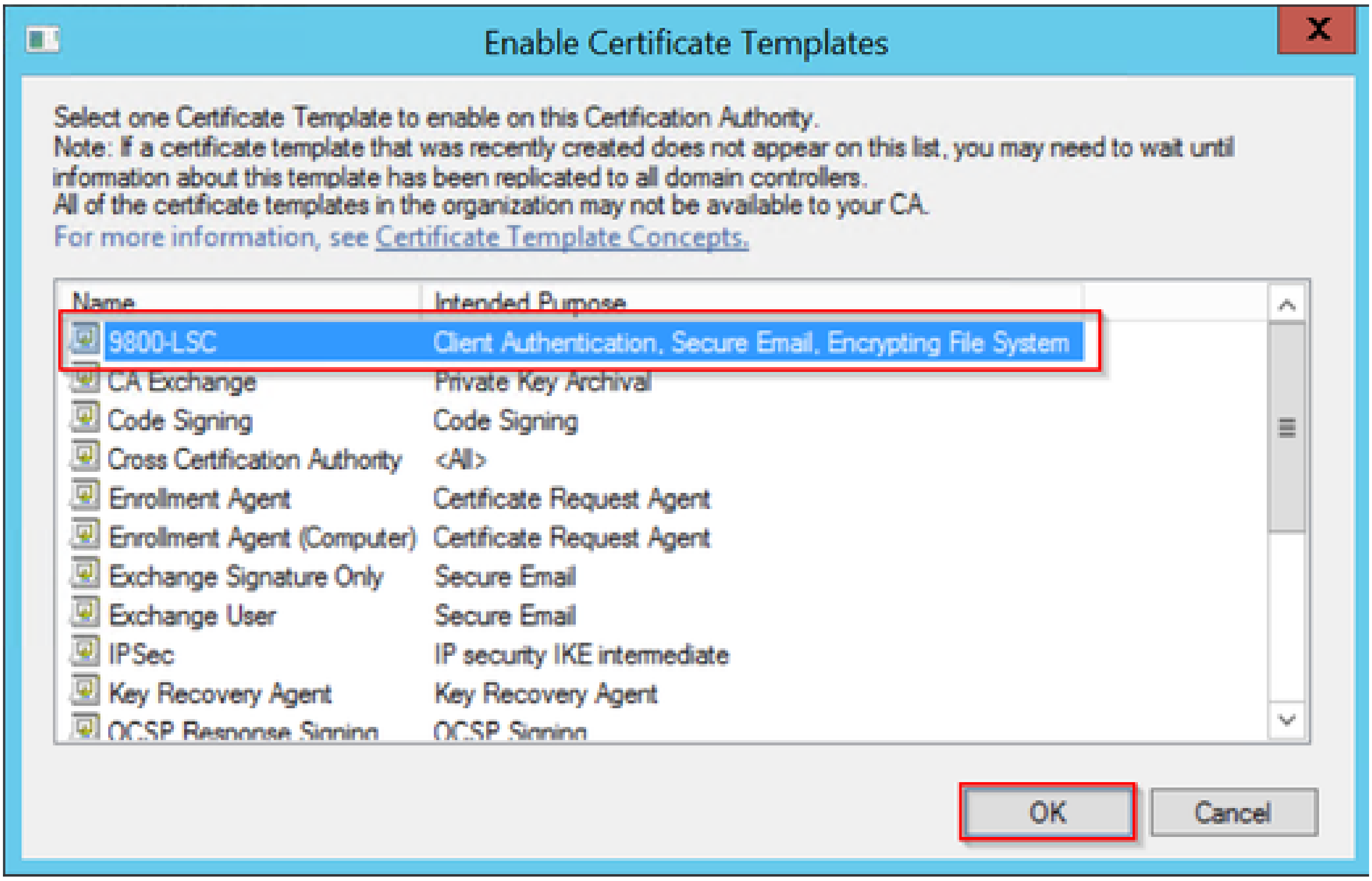
For special permissions or advanced settings, click Advanced.

Give Full Control

Step 8. Return to the **Certification Authority** window, right-click in the **Certificate Templates** folder and select **New > Certificate Template to Issue**.

Step 9. Select the certificate template previously created, in this example is 9800-LSC, and select **OK**.

Note: The newly created certificate template can take longer to be listed in multiple server deployments as it needs to be replicated accross all servers.

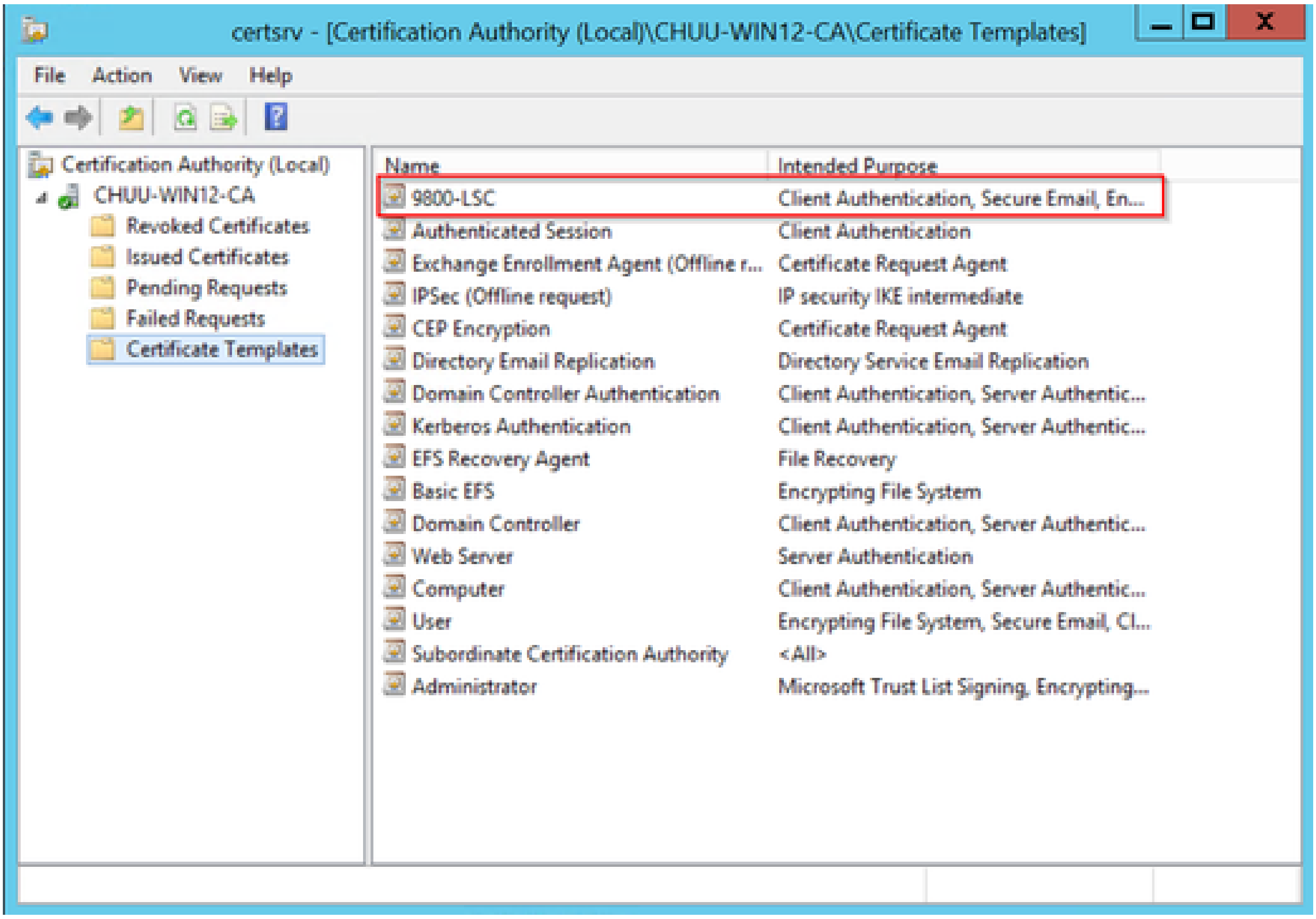


Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
9800-LSC	Client Authentication, Secure Email, Encrypting File System
CA Exchange	Private Key Archival
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
IPSec	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing

Choose the Template

The new certificate template is listed now within the **Certificate Templates** folder content.

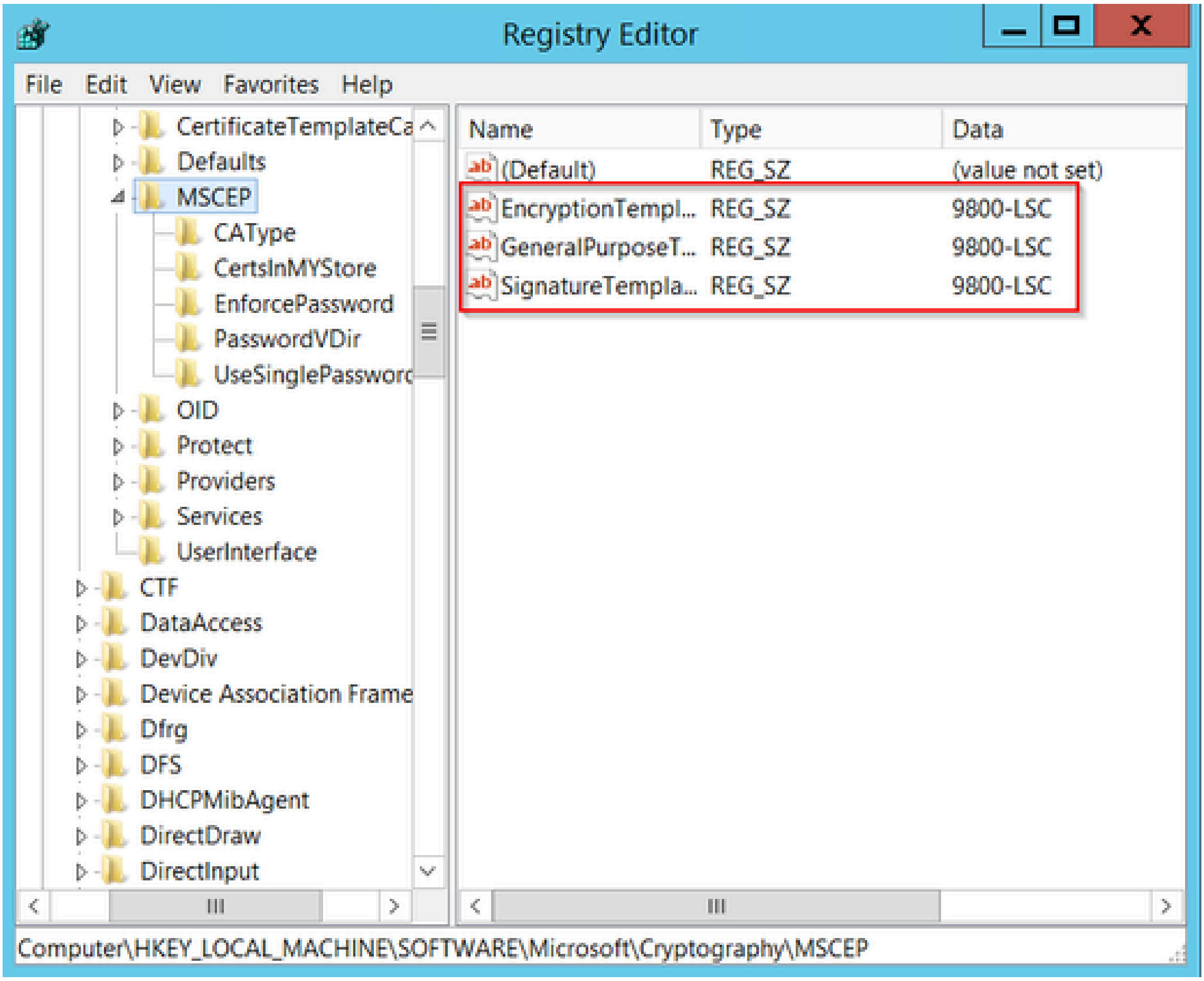


Name	Intended Purpose
9800-LSC	Client Authentication, Secure Email, En...
Authenticated Session	Client Authentication
Exchange Enrollment Agent (Offline r...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
CEP Encryption	Certificate Request Agent
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Select the LSC

Step 10. Return to the **Registry Editor** window and navigate to **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**.

Step 11. Edit the **EncryptionTemplate**, **GeneralPurposeTemplate**, and **SignatureTemplate** registries so that they point to the newly created certificate template.

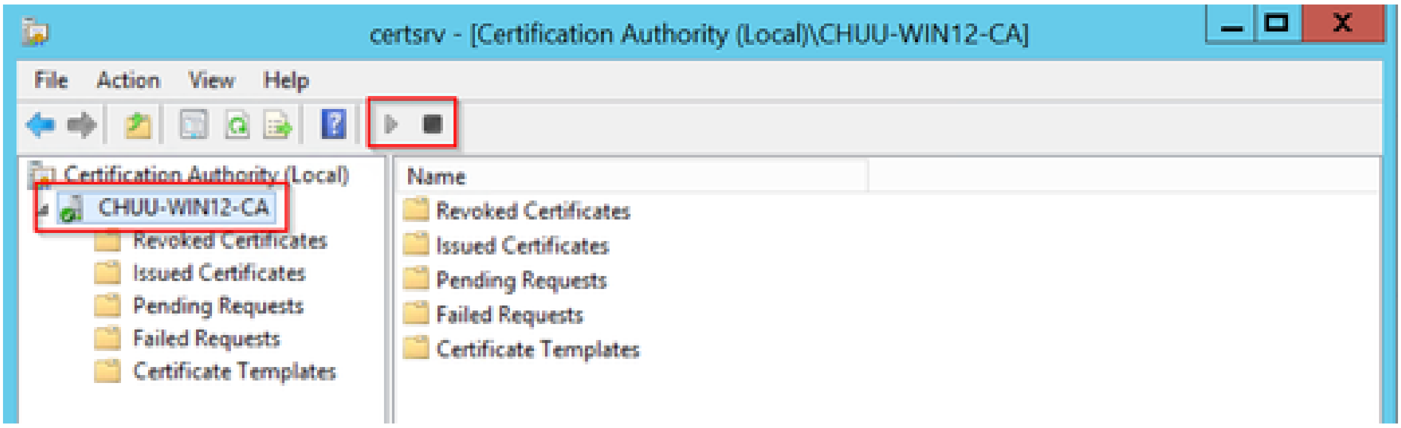


Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTempl...	REG_SZ	9800-LSC
GeneralPurposeT...	REG_SZ	9800-LSC
SignatureTempla...	REG_SZ	9800-LSC

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

Change the Template in the Registry

Step 12. Reboot the NDES server, so return to the **Certification Authority** window, select on the server name, and select the **Stop** and **Play** button succssively.



Configure LSC on the 9800

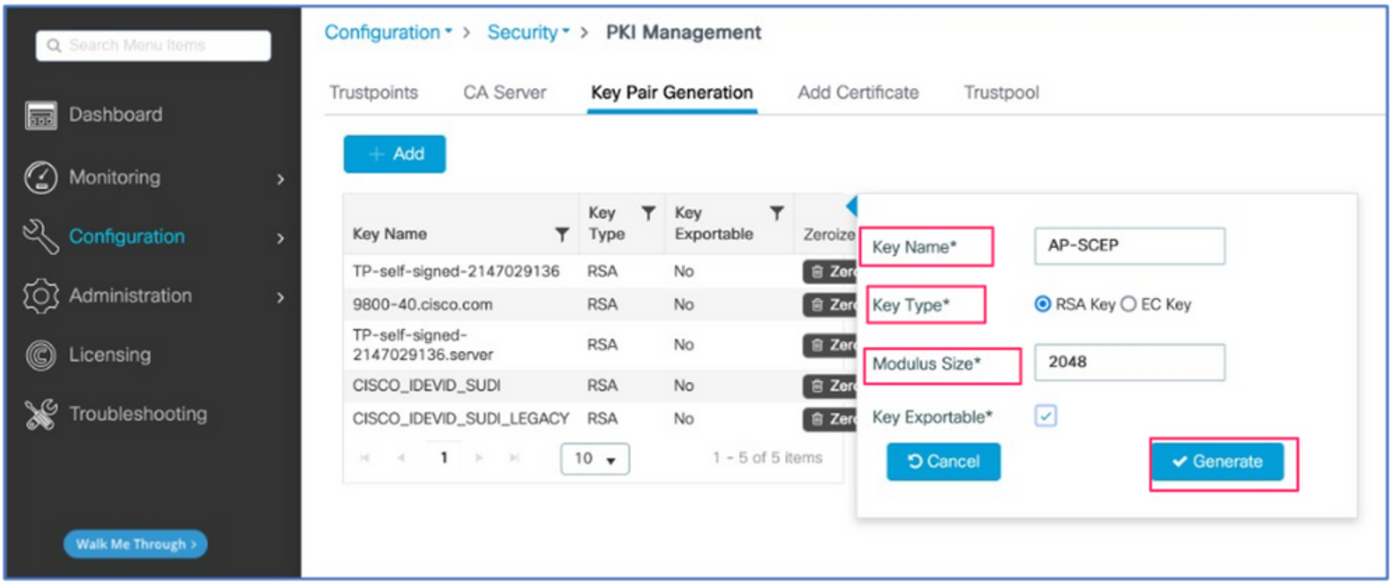
Here are the steps in sequence for configuring LSC for AP in WLC.

1. Create RSA Key. This key is used later for PKI trustpoint.
2. Create a trustpoint and map the RSA key created.
3. Enable LSC provisioning for APs and map the trustpoint.
   1. Enable LSC for all the joined APs.
   2. Enable LSC for selected APs via provision list.
4. Change the Wireless management trustpoint and point to the LSC trustpoint.

AP LSC GUI Configuration Steps

Step 1. Navigate to Configuration > Security > PKI Management > Key Pair Generation.

1. Click add and give it a relevant name.
2. Add the RSA key size.
3. The key exportable option is optional. This is only needed if you want to export the key out of the box.
4. Select Generate



Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	Zero
9800-40.cisco.com	RSA	No	Zero
TP-self-signed-2147029136.server	RSA	No	Zero
CISCO_IDEVID_SUDI	RSA	No	Zero
CISCO_IDEVID_SUDI_LEGACY	RSA	No	Zero

1 10 1 - 5 of 5 items

Key Name* AP-SCEP

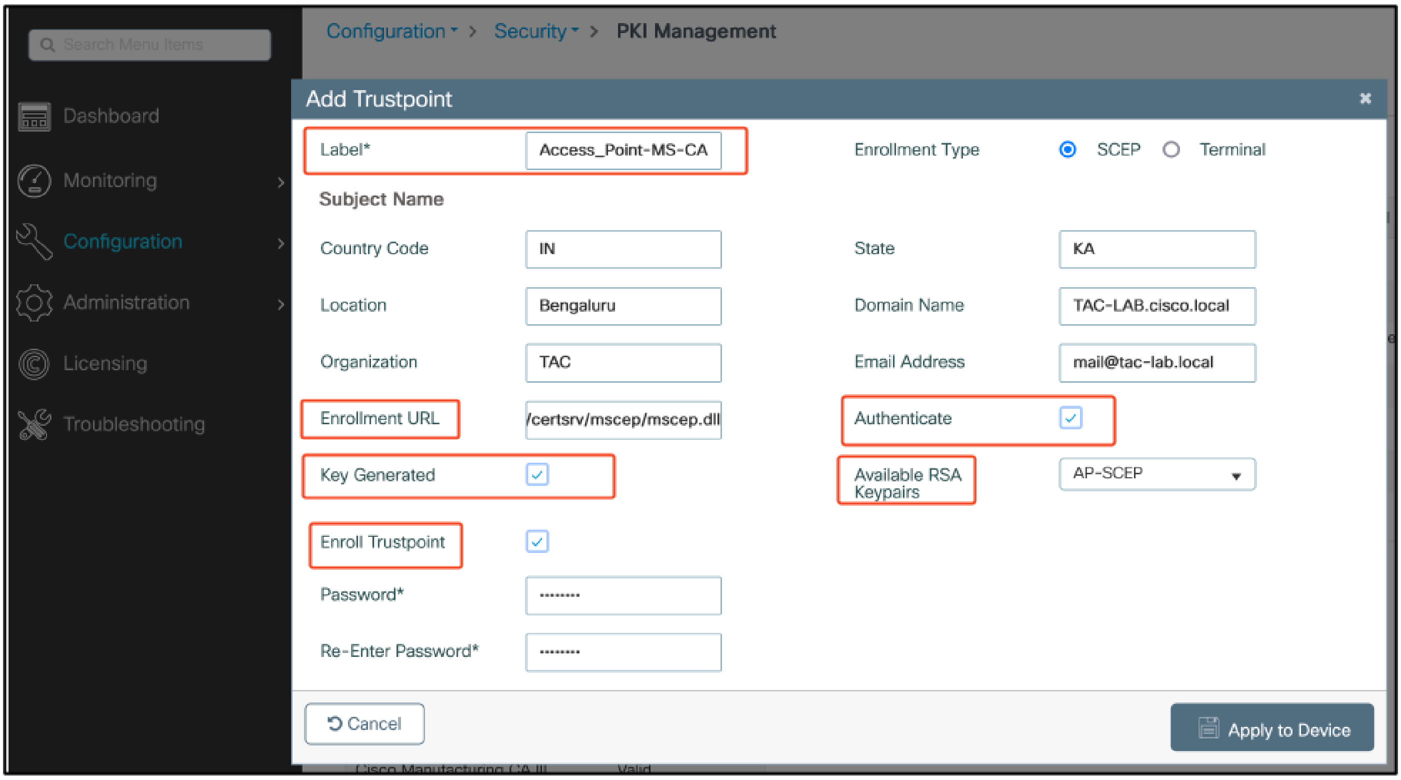
Key Type* ● RSA Key ○ EC Key

Modulus Size* 2048

Key Exportable* ☑

Step 2. Navigate to Configuration > Security > PKI Management > Trustpoints

1. Click add and give it a relevant name.
2. Enter the enrollment URL (Here the URL is http://10.106.35.61:80/certsrv/mscep/mscep.dll) and the rest of the details.
3. Select RSA keypairs created in step 1.
4. Click on **Authenticate**.
5. Click enroll trustpoint and enter a password.
6. Click **Apply to Device.**



Add Trustpoint

Label*	Access_Point-MS-CA	Enrollment Type	● SCEP ○ Terminal

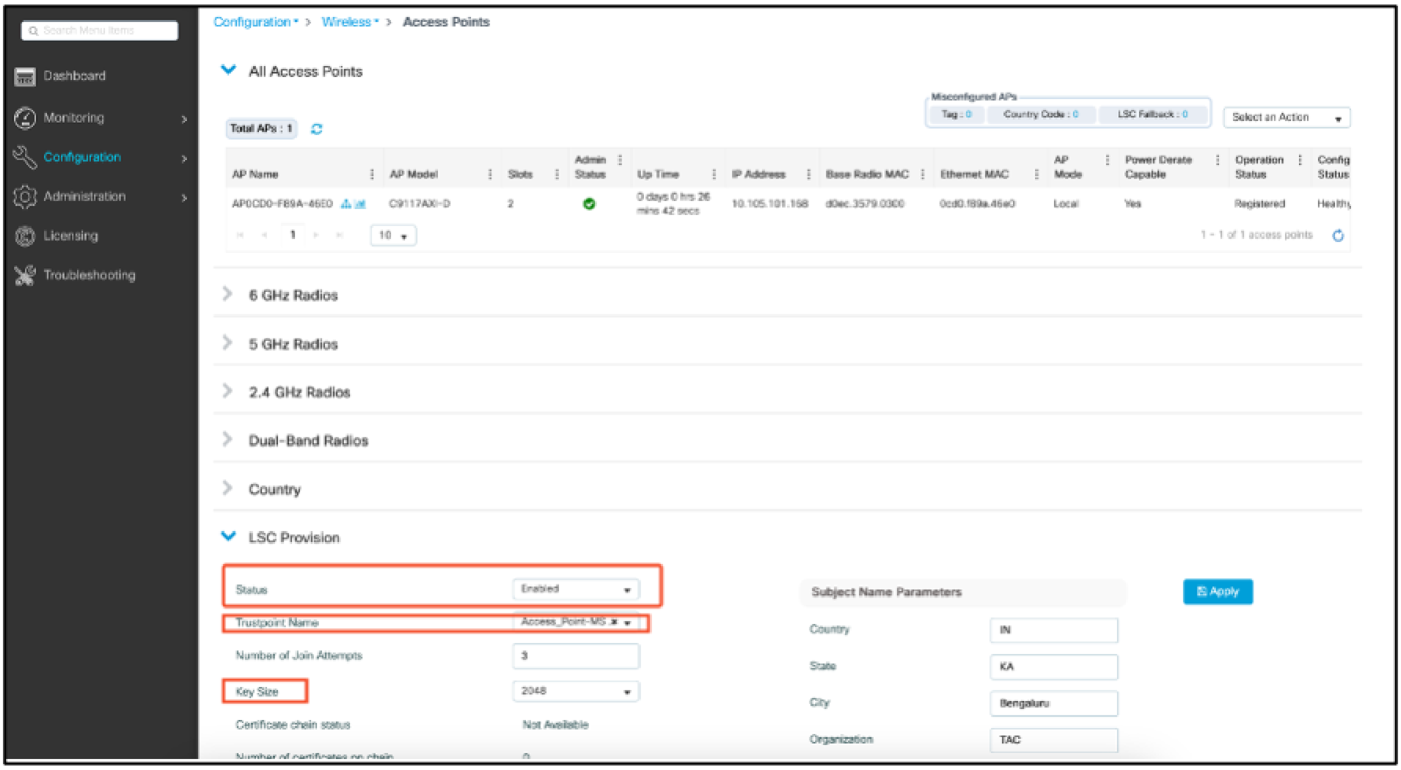
Subject Name

Country Code	IN	State	KA
Location	Bengaluru	Domain Name	TAC-LAB.cisco.local
Organization	TAC	Email Address	mail@tac-lab.local
Enrollment URL	/certsrv/mscep/mscep.dll	Authenticate	☑
Key Generated	☑	Available RSA Keypairs	AP-SCEP
Enroll Trustpoint	☑		
Password*	••••••••		
Re-Enter Password*	••••••••		

Step 3. Navigate to **Configuration > Wireless > Access Points**. Scroll down and select LSC Provision.

1. Select status as enabled. This enables LSC for all the APs that are connected to this WLC.
2. Select the trustpoint name that we created in Step 2.

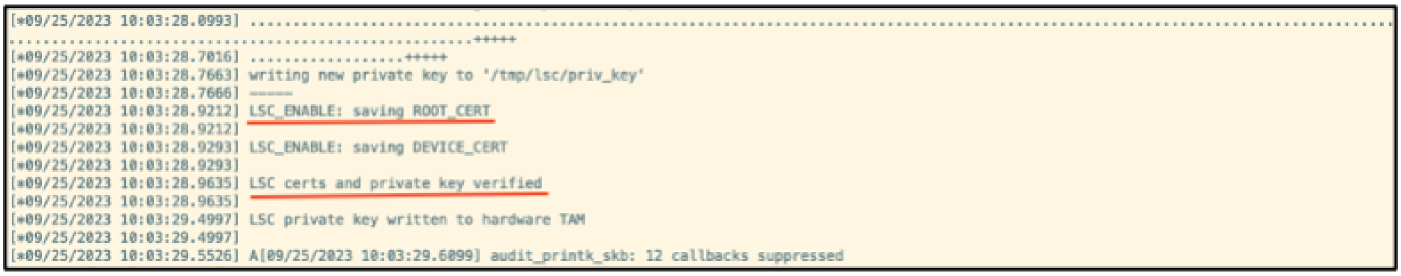
Fill out the rest of the details according to your needs.



AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP0CD0-F89A-46E0	C9117AXI-D	2	✓	0 days 0 hrs 26 mins 42 secs	10.105.101.168	d0ec.3579.0300	0cd0.f89a.46e0	Local	Yes	Registered	Healthy

Status	Enabled	Subject Name Parameters	
Trustpoint Name	Access_Point-MS	Country	IN
Number of Join Attempts	3	State	KA
Key Size	2048	City	Bengaluru
Certificate chain status	Not Available	Organization	TAC
Number of certificates on chain	0		

Once you enable LSC, APs download the certificate via WLC and reboot. In the AP console session, you then see something like this snippet.

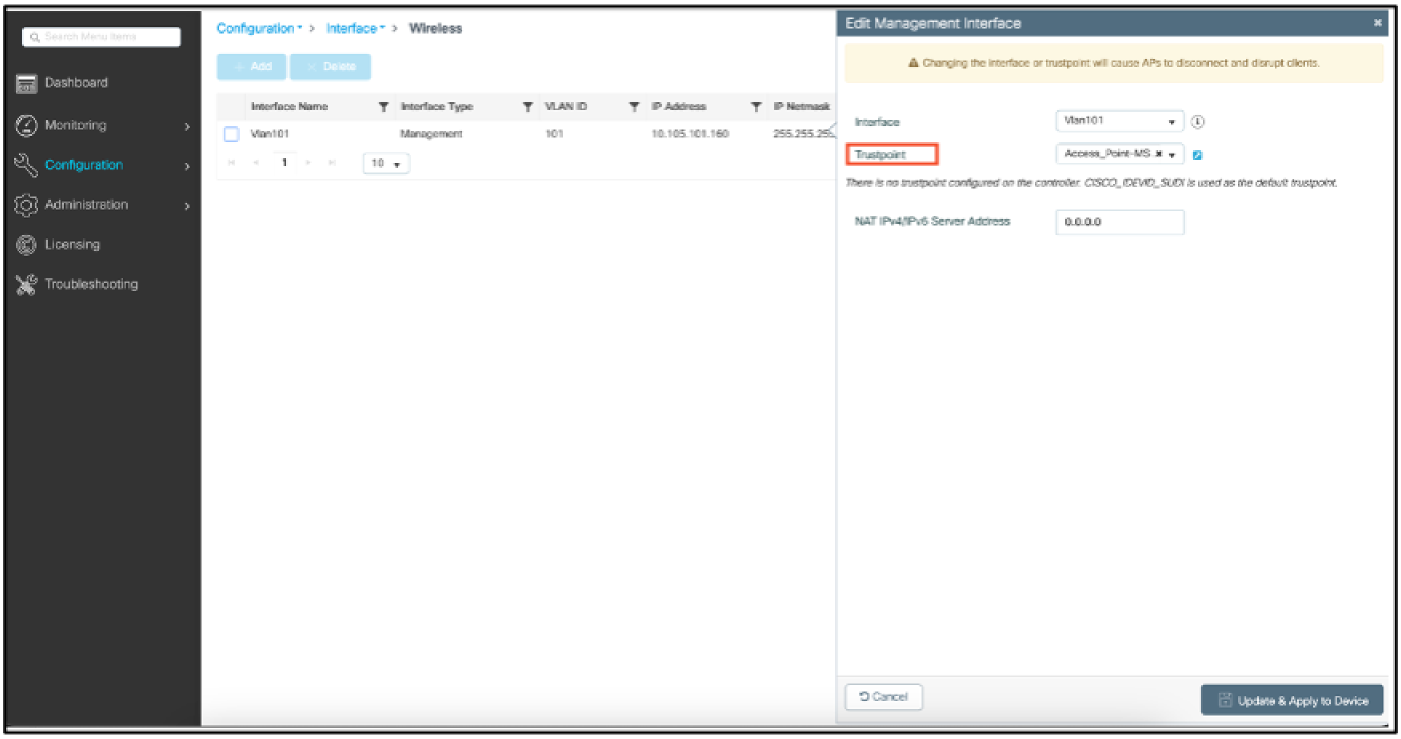


```
[*09/25/2023 10:03:28.0993] ...............................................................................................................................
.............................................................+++++
[*09/25/2023 10:03:28.7016] ..................+++++
[*09/25/2023 10:03:28.7663] writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:03:28.7666] -----
[*09/25/2023 10:03:28.9212] LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:03:28.9212]
[*09/25/2023 10:03:28.9293] LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:03:28.9293]
[*09/25/2023 10:03:28.9635] LSC certs and private key verified
[*09/25/2023 10:03:28.9635]
[*09/25/2023 10:03:29.4997] LSC private key written to hardware TAM
[*09/25/2023 10:03:29.4997]
[*09/25/2023 10:03:29.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed
```

Step 4. Once LSC is enabled, you can change the Wireless Management certificate to match the LSC trustpoint. This makes APs join with their LSC certificates and the WLC use its LSC certificate for AP join. This is an optional step if your only interested is to do 802.1X authentication of your APs.

1. Go to **Configuration** > **Interface** > **Wireless** and click on **Management Interface**.
2. Change the Trustpoint to match the trustpoint we created in step 2.

This concludes the LSC GUI configuration part. APs must be able to join the WLC using the LSC cert now.



Interface Name	Interface Type	VLAN ID	IP Address	IP Netmask
Vlan101	Management	101	10.105.101.160	255.255.25

⚠ Changing the interface or trustpoint will cause APs to disconnect and disrupt clients.

Interface: Vlan101

Trustpoint: Access_Point-MS

There is no trustpoint configured on the controller. CISCO_IDEVID_SUDI is used as the default trustpoint.

NAT IPv4/IPv6 Server Address: 0.0.0.0

AP LSC CLI Configuration Steps

1. Create an RSA key using this command.

```
9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP

% You already have RSA keys defined named AP-SCEP.
% They will be replaced
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storag
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Create PKI trustpoint and map the RSA key pair. Enter the enrollment URL and the rest of the details.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Authenticate and enrol the PKI trust point with the CA server using the command **crypto pki authenticate <trustpoint>**. Enter a password in the password prompt.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' commandwill show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4. Configure AP join with LSC certificate.

```
9800-40(config)#ap lsc-provision join-attempt 10
9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L
9800-40(config)#ap lsc-provision key-size 2048
9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA
9800-40(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration
Are you sure you want to continue? (y/n): y
```

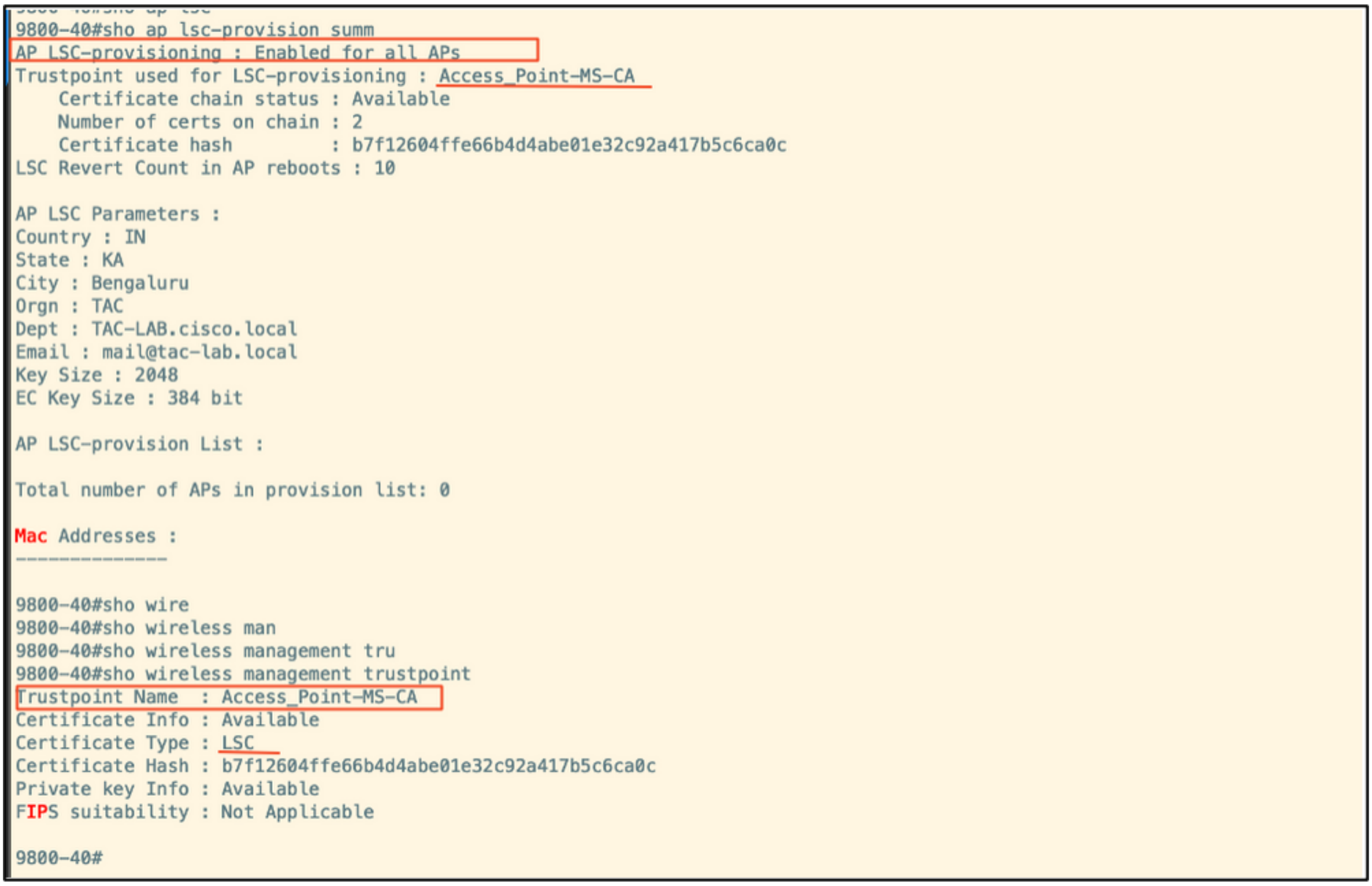
5. Change the Wireless Management Trustpoint to match the trustpoint created above.

```
9800-40(config)#wireless management trustpoint Access_Point-MS-CA
```

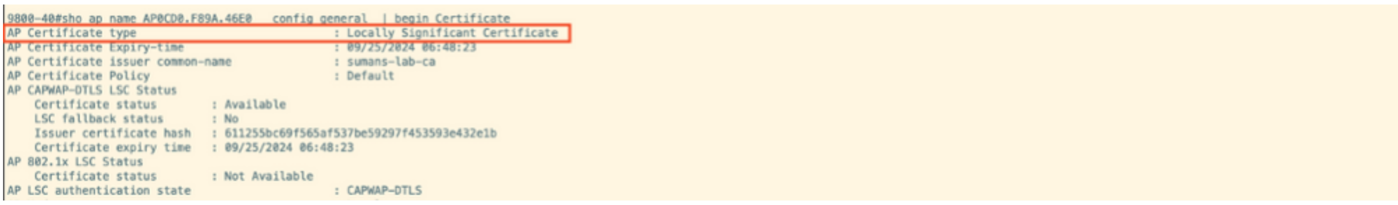
AP LSC Verification

Run these commands on WLC to verify the LSC.

```
#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate
```



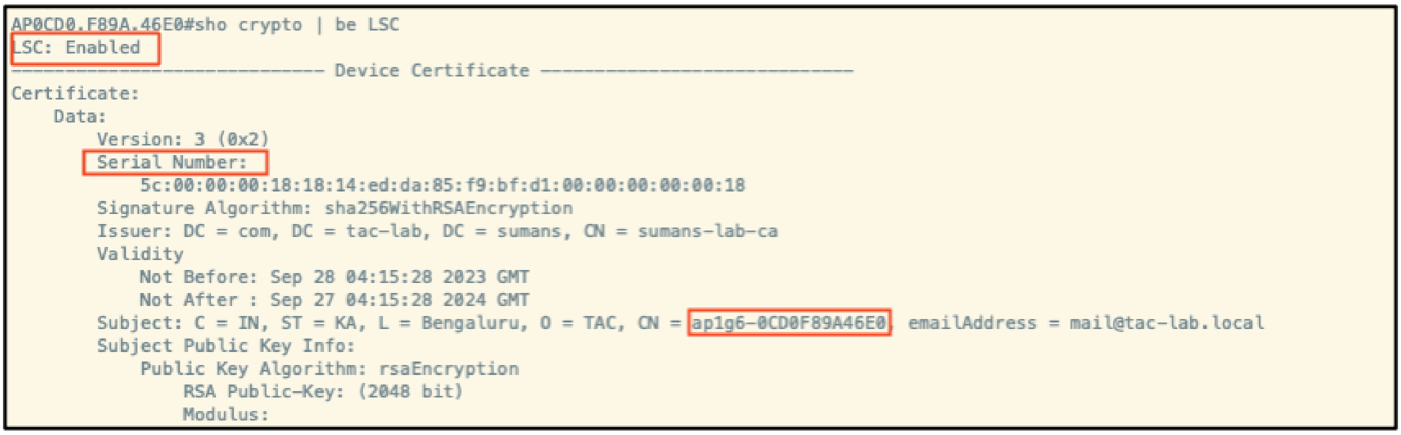
```
9800-40#sho ap lsc
9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
    Certificate chain status : Available
    Number of certs on chain : 2
    Certificate hash         : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
--------------

9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name  : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable

9800-40#
```



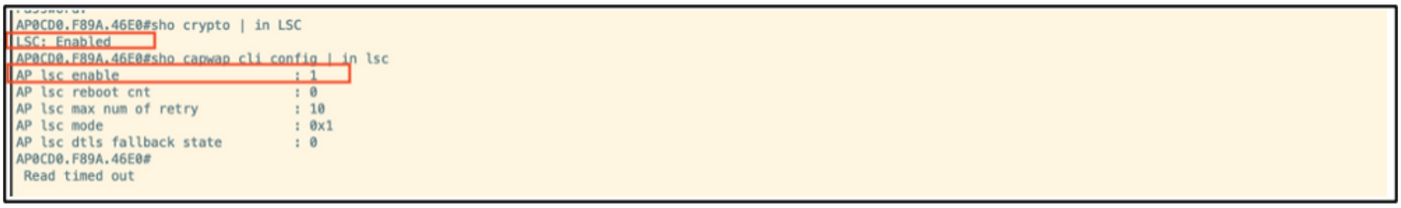
```
9800-40#sho ap name AP0CD0.F89A.46E0   config general  | begin Certificate
AP Certificate type                                    : Locally Significant Certificate
AP Certificate Expiry-time                             : 09/25/2024 06:48:23
AP Certificate issuer common-name                      : sumans-lab-ca
AP Certificate Policy                                  : Default
AP CAPWAP-DTLS LSC Status
    Certificate status        : Available
    LSC fallback status       : No
    Issuer certificate hash   : 611255bc69f565af537be59297f453593e432e1b
    Certificate expiry time   : 09/25/2024 06:48:23
AP 802.1x LSC Status
    Certificate status        : Not Available
AP LSC authentication state                            : CAPWAP-DTLS
```

Once APs are reloaded, login to AP CLI and run these commands to verify LSC configuration.

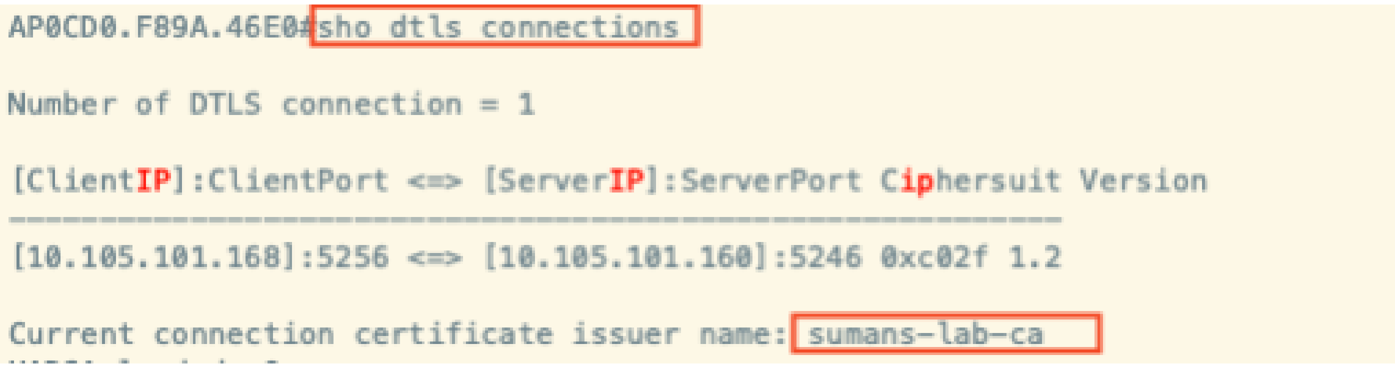
```
#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection
```



```
AP0CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
------------------------------ Device Certificate ------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
        Validity
            Not Before: Sep 28 04:15:28 2023 GMT
            Not After : Sep 27 04:15:28 2024 GMT
        Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0, emailAddress = mail@tac-lab.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
```



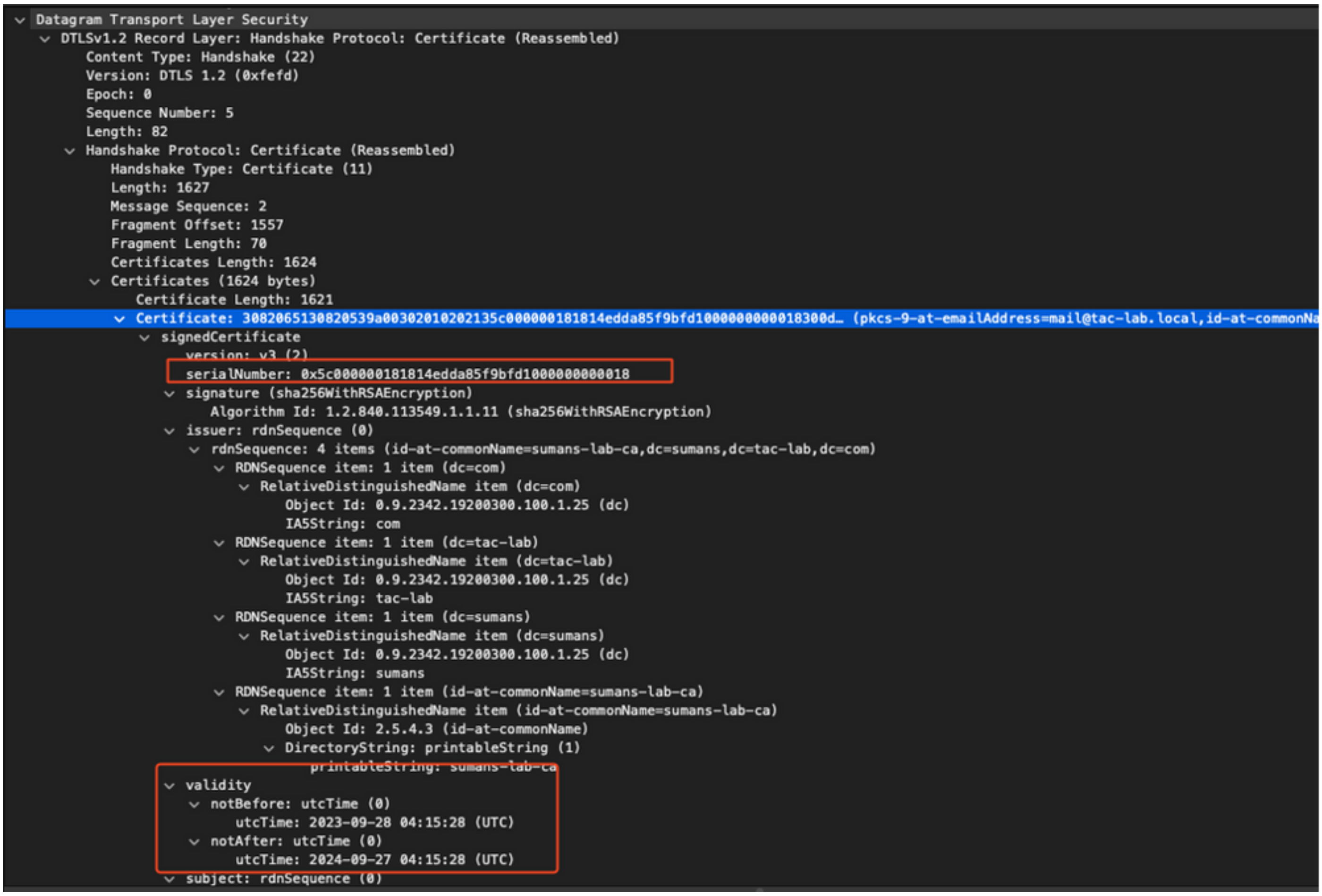
```
AP0CD0.F89A.46E0#sho crypto | in LSC
LSC: Enabled
AP0CD0.F89A.46E0#sho capwap cli config | in lsc
AP lsc enable                          : 1
AP lsc reboot cnt                      : 0
AP lsc max num of retry                : 10
AP lsc mode                            : 0x1
AP lsc dtls fallback state             : 0
AP0CD0.F89A.46E0#
 Read timed out
```



```
AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
-----------------------------------------------------------------
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca
```

Troubleshoot the LSC Provisioning

You can take an EPC capture from the WLC or AP uplink switch port to verify the certificate that AP is using to form the CAPWAP tunnel. Verify from the PCAP if the DTLS tunnel is successfully built.



```
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
      Content Type: Handshake (22)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 0
      Sequence Number: 5
      Length: 82
    v Handshake Protocol: Certificate (Reassembled)
        Handshake Type: Certificate (11)
        Length: 1627
        Message Sequence: 2
        Fragment Offset: 1557
        Fragment Length: 70
        Certificates Length: 1624
      v Certificates (1624 bytes)
          Certificate Length: 1621
        v Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd1000000000018300d… (pkcs-9-at-emailAddress=mail@tac-lab.local,id-at-commonNa
          v signedCertificate
              version: v3 (2)
              serialNumber: 0x5c000000181814edda85f9bfd1000000000018
            v signature (sha256WithRSAEncryption)
                Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
            v issuer: rdnSequence (0)
              v rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
                v RDNSequence item: 1 item (dc=com)
                  v RelativeDistinguishedName item (dc=com)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: com
                v RDNSequence item: 1 item (dc=tac-lab)
                  v RelativeDistinguishedName item (dc=tac-lab)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: tac-lab
                v RDNSequence item: 1 item (dc=sumans)
                  v RelativeDistinguishedName item (dc=sumans)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: sumans
                v RDNSequence item: 1 item (id-at-commonName=sumans-lab-ca)
                  v RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
                      Object Id: 2.5.4.3 (id-at-commonName)
                    v DirectoryString: printableString (1)
                        printableString: sumans-lab-ca
            v validity
              v notBefore: utcTime (0)
                  utcTime: 2023-09-28 04:15:28 (UTC)
              v notAfter: utcTime (0)
                  utcTime: 2024-09-27 04:15:28 (UTC)
            v subject: rdnSequence (0)
```

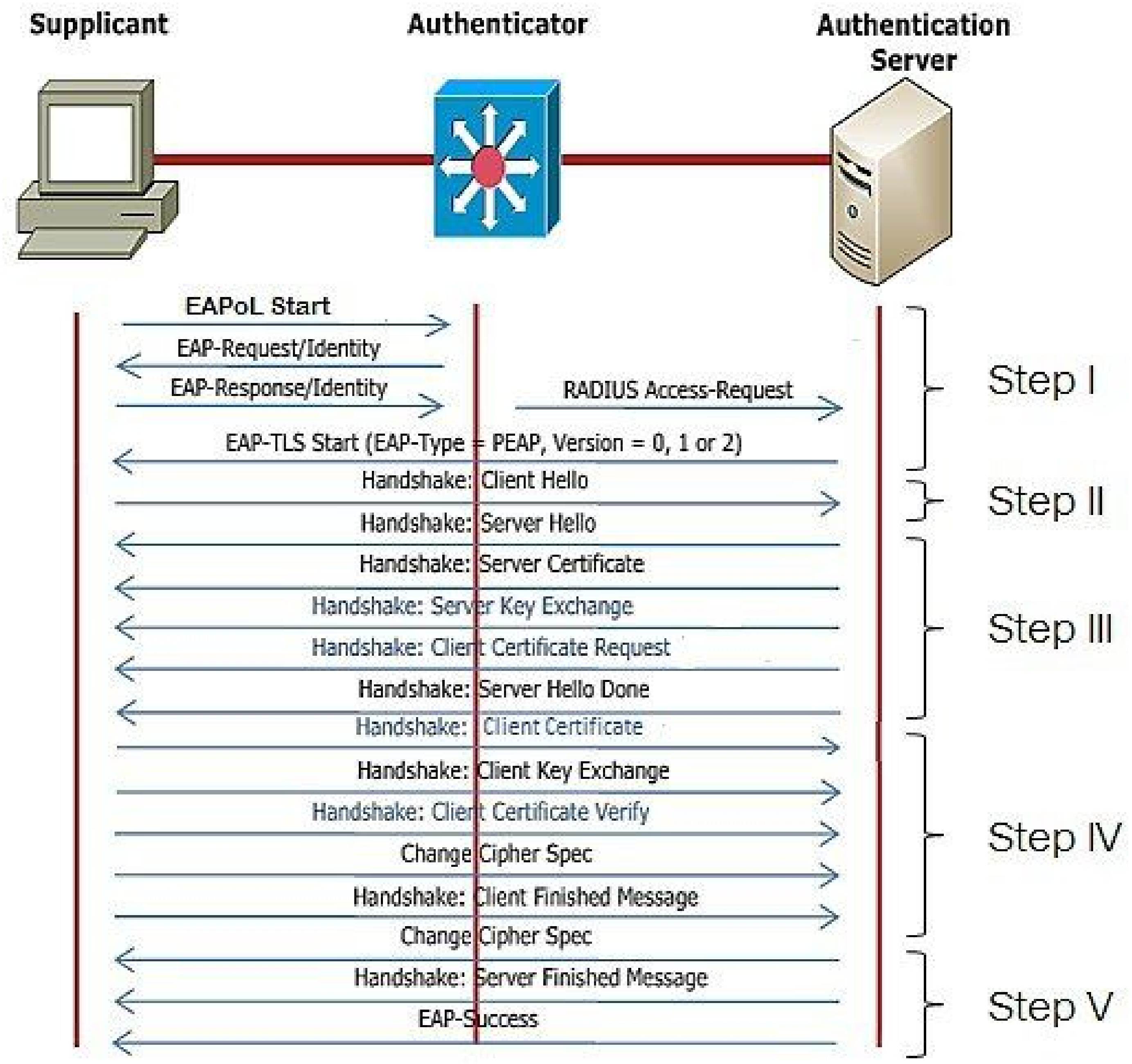
DTLS debugs can be run on AP and WLC to understand the certificate issue.

AP Wired 802.1X Authentication using LSC

AP is configured to use the same LSC certificate to authenticate itself. AP acts as 802.1X supplicant and is authenticated by the switch against the ISE server. ISE server talks to the AD in the backend.

Note: Once dot1x authentication is enabled on the AP uplink switch port, APs is not able to forward or receive any traffic until the authentication is passed. To recover APs with unsuccessful authentication and gain access to AP, disable dot1x auth on the AP wired switch port.

EAP-TLS Authentication Workflow and Message Exchange

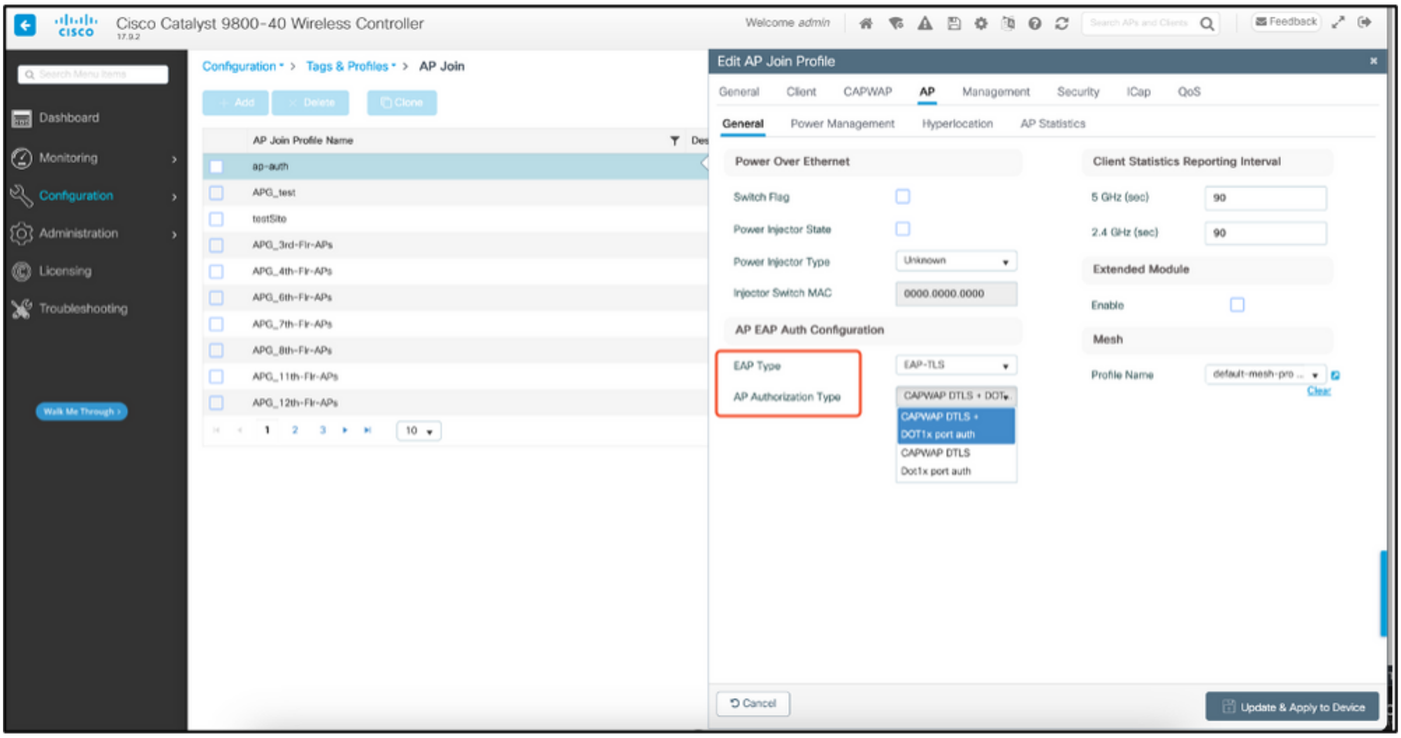

Supplicant
Authenticator
Authentication Server
EAPoL Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS Access-Request
EAP-TLS Start (EAP-Type = PEAP, Version = 0, 1 or 2)
Handshake: Client Hello
Handshake: Server Hello
Handshake: Server Certificate
Handshake: Server Key Exchange
Handshake: Client Certificate Request
Handshake: Server Hello Done
Handshake: Client Certificate
Handshake: Client Key Exchange
Handshake: Client Certificate Verify
Change Cipher Spec
Handshake: Client Finished Message
Change Cipher Spec
Handshake: Server Finished Message
EAP-Success
Step I
Step II
Step III
Step IV
Step V

AP Wired 802.1x Authentication Configuration Steps

1. Enable dot1x port auth along with CAPWAP DTLS and select the EAP type.
2. Create dot1x credentials for APs.
3. Enable dot1x on the switch port.
4. Install a trusted certificate on the RADIUS server.

AP Wired 802.1x Authentication GUI Configuration

1. Navigate to the AP join profile and click on the profile.
    1. Click on AP > General. Select EAP type and AP authorization type as “CAPWAP DTLS + dot1x port auth”.
    2. Navigate to Management > Credentials and create a username and password for AP dot1x auth.



Edit AP Join Profile

AP Join Profile Name
ap-auth
APG_test
testSite
APG_3rd-Flr-APs
APG_4th-Flr-APs
APG_6th-Flr-APs
APG_7th-Flr-APs
APG_8th-Flr-APs
APG_11th-Flr-APs
APG_12th-Flr-APs

Power Over Ethernet

Switch Flag □

Power Injector State □

Power Injector Type: Unknown

Injector Switch MAC: 0000.0000.0000

AP EAP Auth Configuration

EAP Type: EAP-TLS

AP Authorization Type: CAPWAP DTLS + DOT1x port auth

Client Statistics Reporting Interval

5 GHz (sec): 90

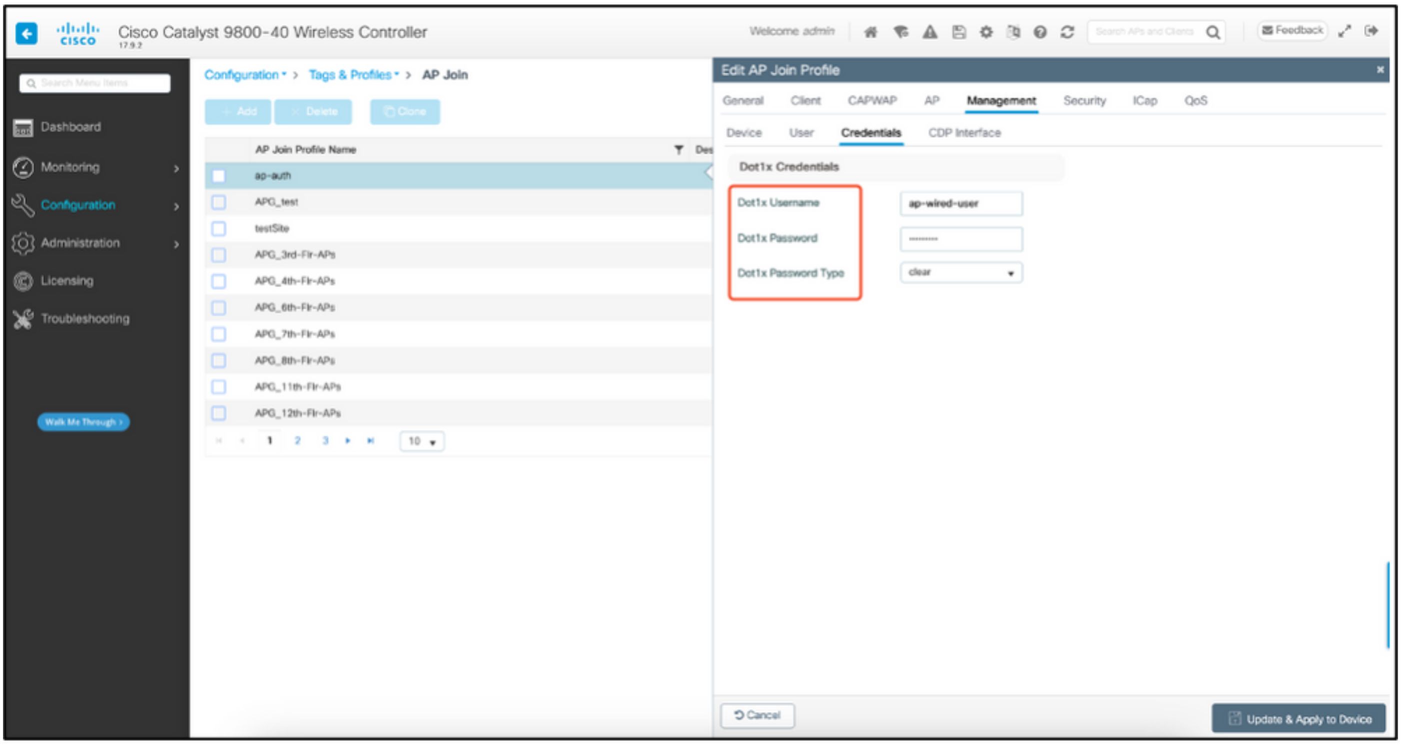
2.4 GHz (sec): 90

Extended Module

Enable □

Mesh

Profile Name: default-mesh-pro...



Edit AP Join Profile

Dot1x Credentials

Dot1x Username: ap-wired-user

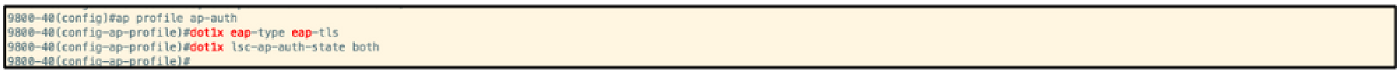
Dot1x Password: ••••••••

Dot1x Password Type: clear

AP Wired 802.1x Authentication CLI Configuration

Use these commands to enable dot1x for APs from the CLI. This only enables wired authentication for APs which are using the specific join profile.

```
#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123
```



```
9800-40(config)#ap profile ap-auth
9800-40(config-ap-profile)#dot1x eap-type eap-tls
9800-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9800-40(config-ap-profile)#
```

AP Wired 802.1x Authentication Switch Configuration

This switch configurations is used in LAB to enable AP wired authentication. You can have different configuration based on design.

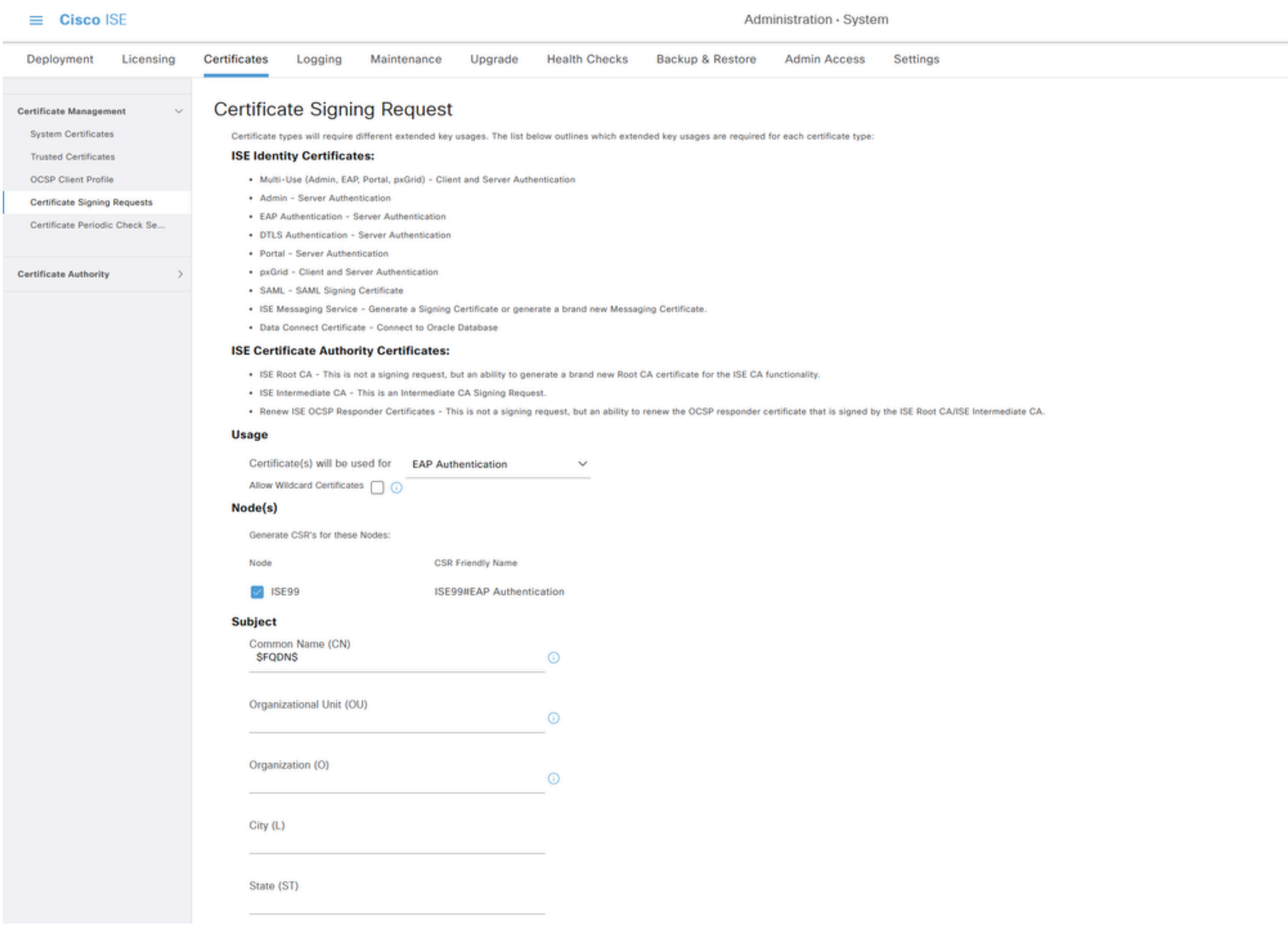
```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

RADIUS Server Certificate Installation

The Authentication occurs between the AP (which is acting as the supplicant) and the RADIUS server. Both must trust each other certificate. The only way to have the AP trust the RADIUS server certificate is to have the RADIUS server use a certificate issued by the SCEP CA which issued the AP certificate as well.

In ISE, go to **Administration > Certificates > Generate Certificate Signing Requests**

Generate a CSR and fill the fields with the information of your ISE node.



Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.
- Data Connect Certificate - Connect to Oracle Database

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: EAP Authentication

Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

	Node	CSR Friendly Name
☑	ISE99	ISE99#EAP Authentication

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

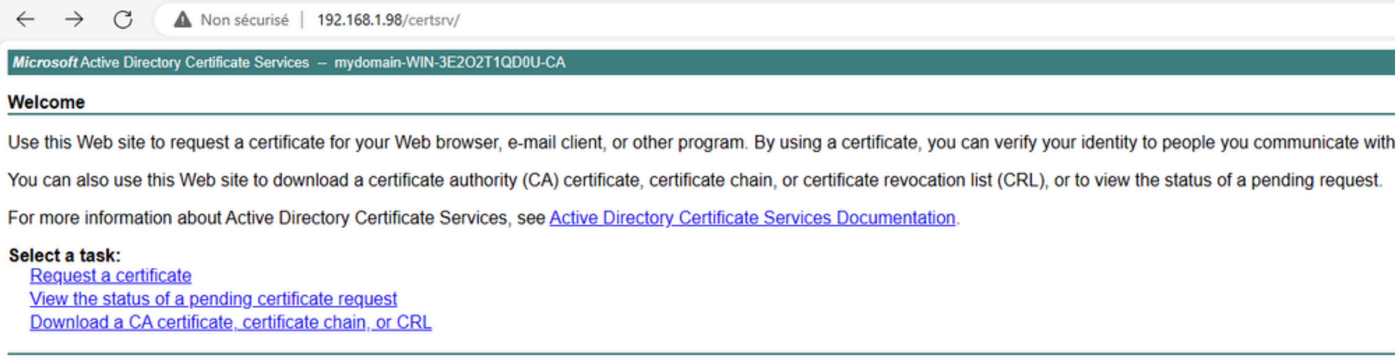
City (L):

State (ST):

Once generated, you can export it and copy-paste it as text as well.

Navigate to your Windows CA IP address and add **/certsrv/** to the URL

Click **Request a certificate**


Non sécurisé | 192.168.1.98/certsrv/
Microsoft Active Directory Certificate Services -- mydomain-WIN-3E2O2T1QD0U-CA

Welcome

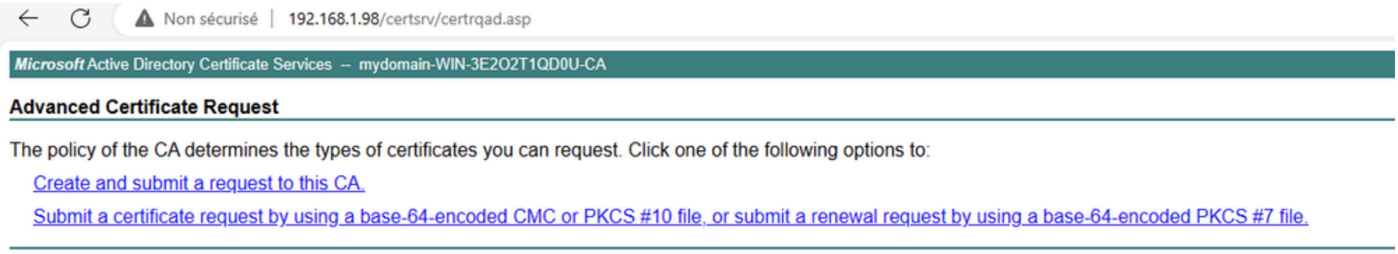
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Click on **Submit a certificate request by using a base-64** ....


Non sécurisé | 192.168.1.98/certsrv/certrqad.asp
Microsoft Active Directory Certificate Services – mydomain-WIN-3E2O2T1QD0U-CA

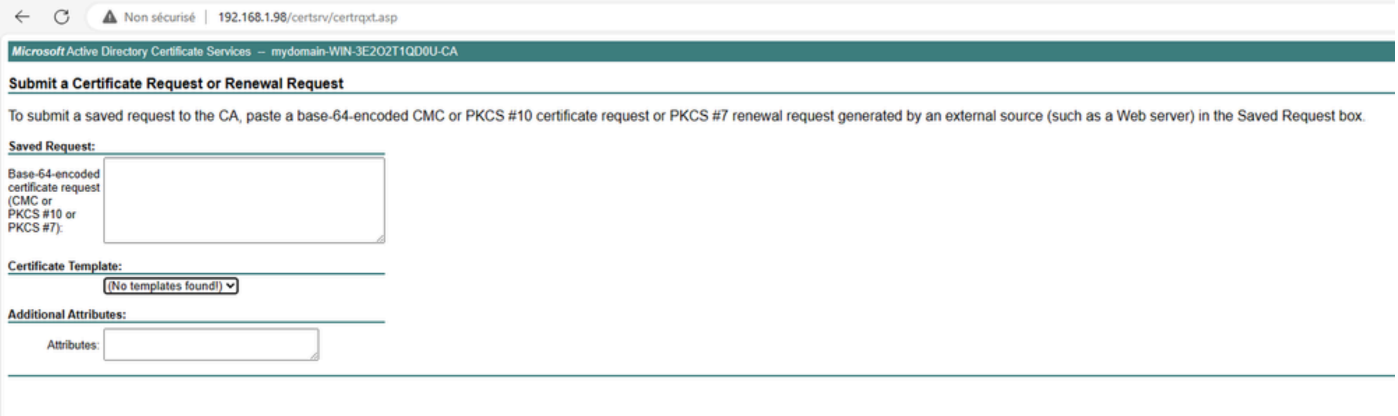
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Paste the CSR text in the textbox. Choose the web server certificate template.


Non sécurisé | 192.168.1.98/certsrv/certrqxt.asp
Microsoft Active Directory Certificate Services – mydomain-WIN-3E2O2T1QD0U-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

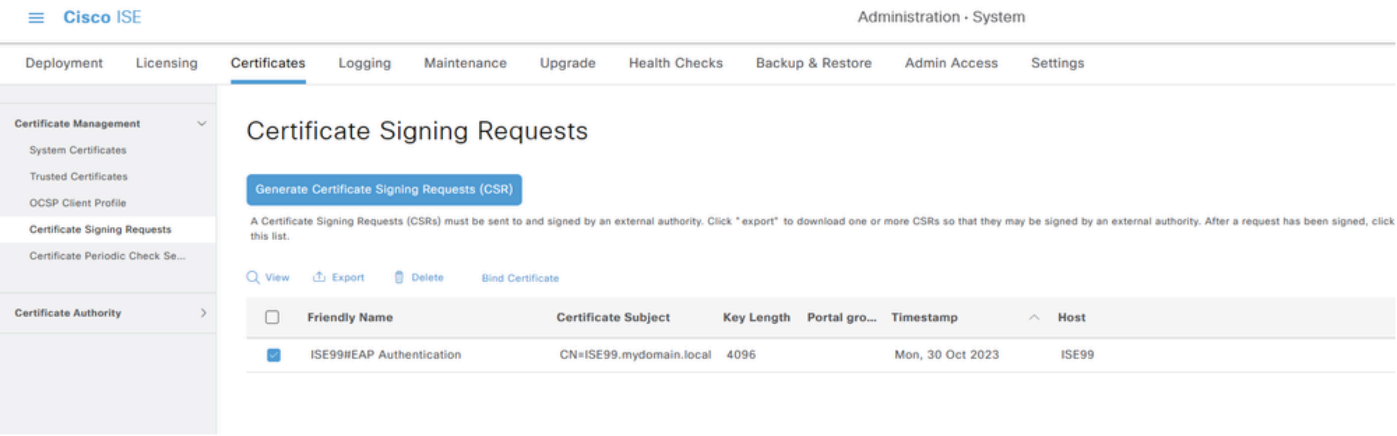
Certificate Template:

(No templates found!)

Additional Attributes:

Attributes:

You can then install this certificate on ISE by going back to the Certificate Signing Request menu and click **Bind certificate.** You can then upload the certificate you obtained from your Windows C.



Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.

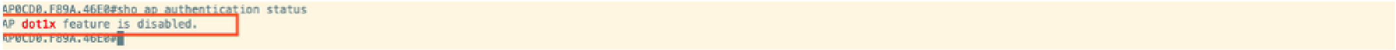
□	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
☑	ISE99#EAP Authentication	CN=ISE99.mydomain.local	4096		Mon, 30 Oct 2023	ISE99

AP Wired 802.1x Authentication Verification

Take console access to AP and run the command:

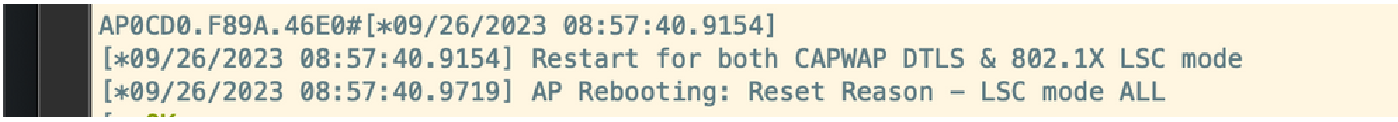
```
#show ap authentication status
```

Ap authentication is not enabled:



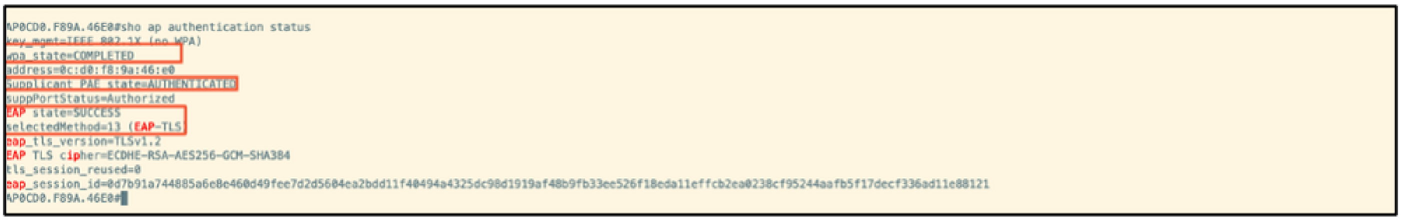
```
AP0CD0.F89A.46E0#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E0#
```

Console logs from AP after enabling ap auth:



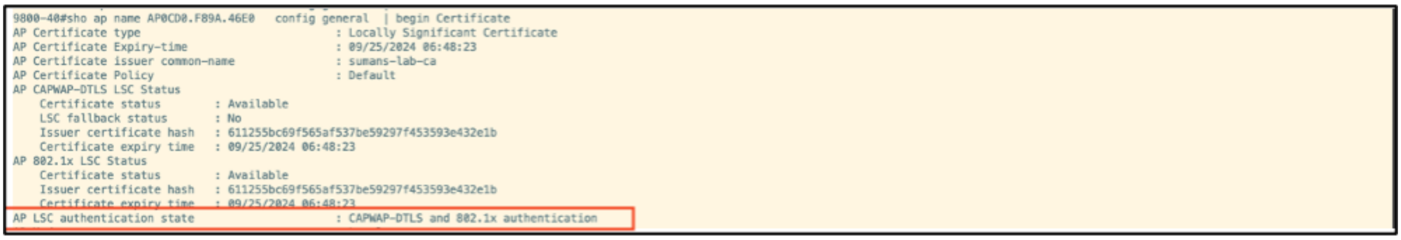
```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

AP successfully authenticated:



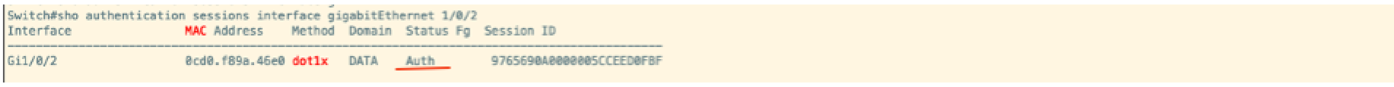
```
AP0CD0.F89A.46E0#sho ap authentication status
key_mgmt=IEEE 802.1X (no WPA)
wpa_state=COMPLETED
address=0c:d0:f8:9a:46:e0
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS
eap_tls_version=TLSv1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
eap_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ea2bdd11f40494a4325dc98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aafb5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

WLC verification:



```
9800-40#sho ap name AP0CD0.F89A.46E0   config general  | begin Certificate
AP Certificate type                              : Locally Significant Certificate
AP Certificate Expiry-time                       : 09/25/2024 06:48:23
AP Certificate issuer common-name                : sumans-lab-ca
AP Certificate Policy                            : Default
AP CAPWAP-DTLS LSC Status
    Certificate status         : Available
    LSC fallback status        : No
    Issuer certificate hash    : 611255bc69f565af537be59297f453593e432e1b
    Certificate expiry time    : 09/25/2024 06:48:23
AP 802.1x LSC Status
    Certificate status         : Available
    Issuer certificate hash    : 611255bc69f565af537be59297f453593e432e1b
    Certificate expiry time    : 09/25/2024 06:48:23
AP LSC authentication state                      : CAPWAP-DTLS and 802.1x authentication
```

Switchport interface status post successful authentication:



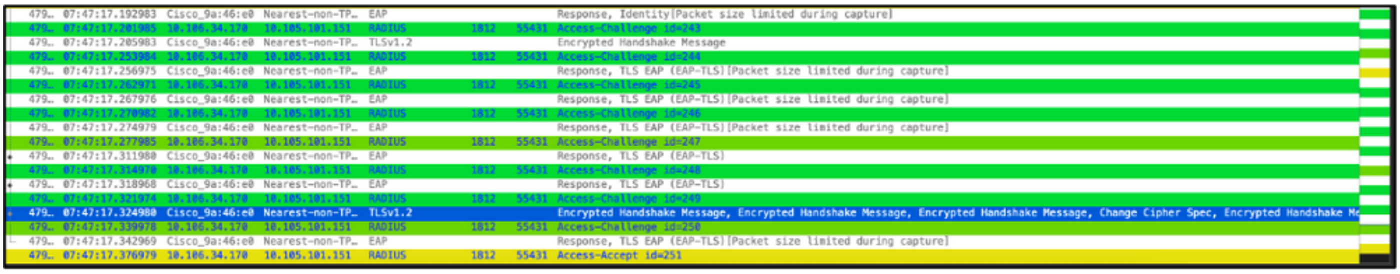
```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface                 MAC Address    Method  Domain  Status Fg  Session ID
------------------------------------------------------------------------------------
Gi1/0/2                   0cd0.f89a.46e0 dot1x   DATA    Auth       9765690A0000005CCEED0FBF
```

This is a sample of AP console logs indicating a successful authentication:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```

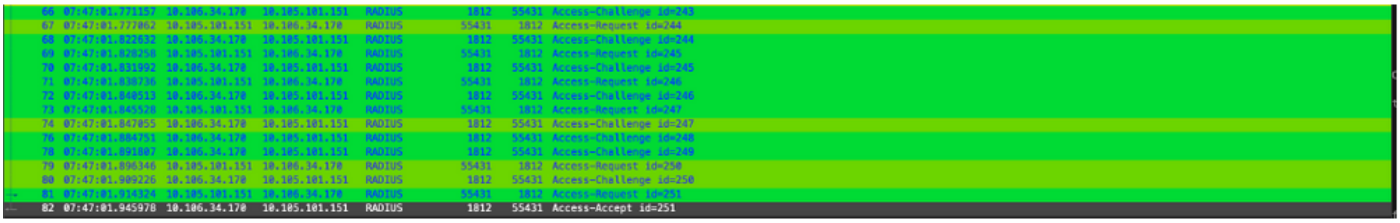
Troubleshoot 802.1X Authentication

Take PCAP on the AP uplink and verify the radius authentication. Here is a snippet of successful authentication.



```
479… 07:47:17.192983 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, Identity[Packet size limited during capture]
479… 07:47:17.201985 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=243
479… 07:47:17.205983 Cisco_9a:46:e0 Nearest-non-TP… TLSv1.2                 Encrypted Handshake Message
479… 07:47:17.253984 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=244
479… 07:47:17.256975 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479… 07:47:17.262971 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=245
479… 07:47:17.267976 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479… 07:47:17.270982 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=246
479… 07:47:17.274979 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479… 07:47:17.277985 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=247
479… 07:47:17.311980 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, TLS EAP (EAP-TLS)
479… 07:47:17.314970 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=248
479… 07:47:17.318968 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, TLS EAP (EAP-TLS)
479… 07:47:17.321974 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=249
479… 07:47:17.324980 Cisco_9a:46:e0 Nearest-non-TP… TLSv1.2                 Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Me
479… 07:47:17.339978 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Challenge id=250
479… 07:47:17.342969 Cisco_9a:46:e0 Nearest-non-TP… EAP                     Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479… 07:47:17.376979 10.106.34.170  10.105.101.151  RADIUS   1812   55431 Access-Accept id=251
```

TCPdump collect from ISE capturing the authentication.



```
66 07:47:01.771157 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=243
67 07:47:01.777062 10.105.101.151 10.106.34.170  RADIUS  55431   1812 Access-Request id=244
68 07:47:01.822632 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=244
69 07:47:01.828258 10.105.101.151 10.106.34.170  RADIUS  55431   1812 Access-Request id=245
70 07:47:01.831992 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=245
71 07:47:01.838736 10.105.101.151 10.106.34.170  RADIUS  55431   1812 Access-Request id=246
72 07:47:01.840513 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=246
73 07:47:01.845528 10.105.101.151 10.106.34.170  RADIUS  55431   1812 Access-Request id=247
74 07:47:01.847055 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=247
76 07:47:01.884751 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=248
78 07:47:01.891807 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=249
79 07:47:01.896346 10.105.101.151 10.106.34.170  RADIUS  55431   1812 Access-Request id=250
80 07:47:01.909226 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Challenge id=250
81 07:47:01.914324 10.105.101.151 10.106.34.170  RADIUS  55431   1812 Access-Request id=251
82 07:47:01.945978 10.106.34.170  10.105.101.151 RADIUS   1812  55431 Access-Accept id=251
```

If there is an issue observed during authentication, simultaneous packet capture from AP wired uplink and ISE side would be needed.

Debug command for AP:

```
#debug ap authentication packet
```

Related Information

- **Cisco Technical Support & Downloads**
- **Configuring 802.1X on AP with AireOS**
- **9800 configuration guide for LSC**
- **LSC configuration example for 9800**
- **Configure 802.1X for APs on 9800**