

在AP上為PEAP或使用LSC的EAP-TLS配置802.1X

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[Windows Server 2016 SCEP CA](#)

[配置證書模板和登錄檔](#)

[在9800上配置LSC](#)

[AP LSC GUI配置步驟](#)

[AP LSC CLI配置步驟](#)

[AP LSC驗證](#)

[排除LSC調配故障](#)

[使用LSC的AP有線802.1X身份驗證](#)

[AP有線802.1X身份驗證配置步驟](#)

[AP有線802.1X身份驗證GUI配置](#)

[AP有線802.1X身份驗證CLI配置](#)

[AP有線802.1X身份驗證交換機配置](#)

[RADIUS伺服器憑證安裝](#)

[AP有線802.1X驗證驗證](#)

[802.1X身份驗證故障排除](#)

[相關資訊](#)

簡介

本文檔介紹如何使用802.1X PEAP或EAP-TLS方法對交換機埠上的思科接入點進行身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- 無線控制器
- 存取點

- 交換器
- ISE伺服器
- 證書頒發機構。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 無線控制器：運行17.09.02的C9800-40-K9
- 接入點：C9117AXI-D
- 交換機：運行17.06.04的C9200L-24P-4G
- AAA伺服器：運行3.1.0.518的ISE-VM-K9
- 證書頒發機構：Windows Server 2016

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

如果您希望存取點(AP)使用802.1X驗證其交換器連線埠，預設情況下，它們會使用不需要憑證的EAP-FAST驗證通訊協定。如果您希望AP使用PEAP-mschapv2方法（在AP端使用憑證，但在RADIUS端使用證書）或EAP-TLS方法（在兩端使用證書），您必須首先配置LSC。這是將受信任/根證書調配到接入點的唯一方法（在EAP-TLS的情況下也是裝置證書）。AP無法執行PEAP並忽略伺服器端驗證。本文檔首先介紹配置LSC，然後介紹配置802.1X端。

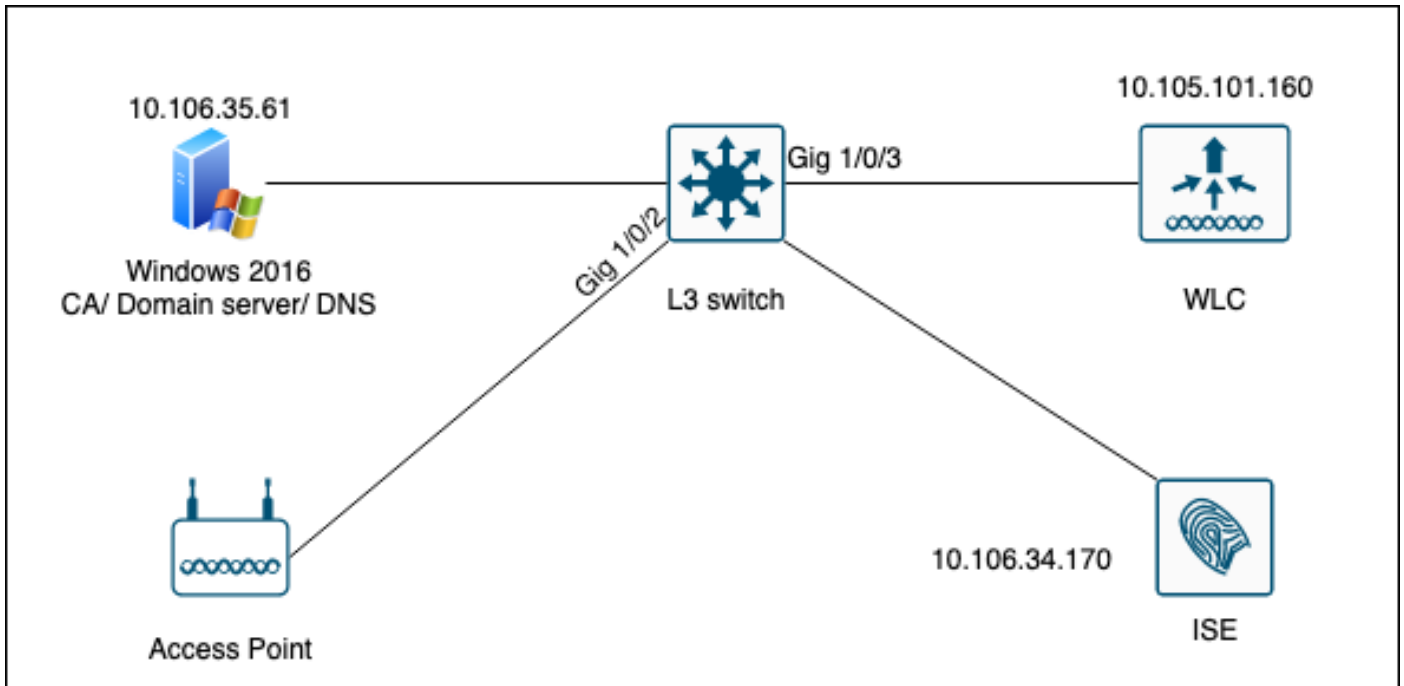
如果您希望PKI提供更好的安全性、控制證書頒發機構(CA)並在生成的證書上定義策略、限制和使用，請使用LSC。

若使用LSC，控制器會取得由CA頒發的憑證。AP不與CA伺服器直接通訊，但WLC代表加入的AP請求證書。CA伺服器詳細資訊必須在控制器上配置並且必須可訪問。

控制器使用Simple Certificate Enrollment Protocol(SCEP)將裝置上生成的certReq轉發到CA，並再次使用SCEP從CA獲取已簽名的證書。

SCEP是PKI客戶端和CA伺服器用於支援證書註冊和撤銷的證書管理協定。它廣泛使用在Cisco中，並且受許多CA伺服器的支援。在SCEP中，HTTP用作PKI消息的傳輸協定。SCEP的主要目標是向網路裝置安全頒發證書。

網路圖表



設定

主要需要設定兩個專案：SCEP CA和9800 WLC。

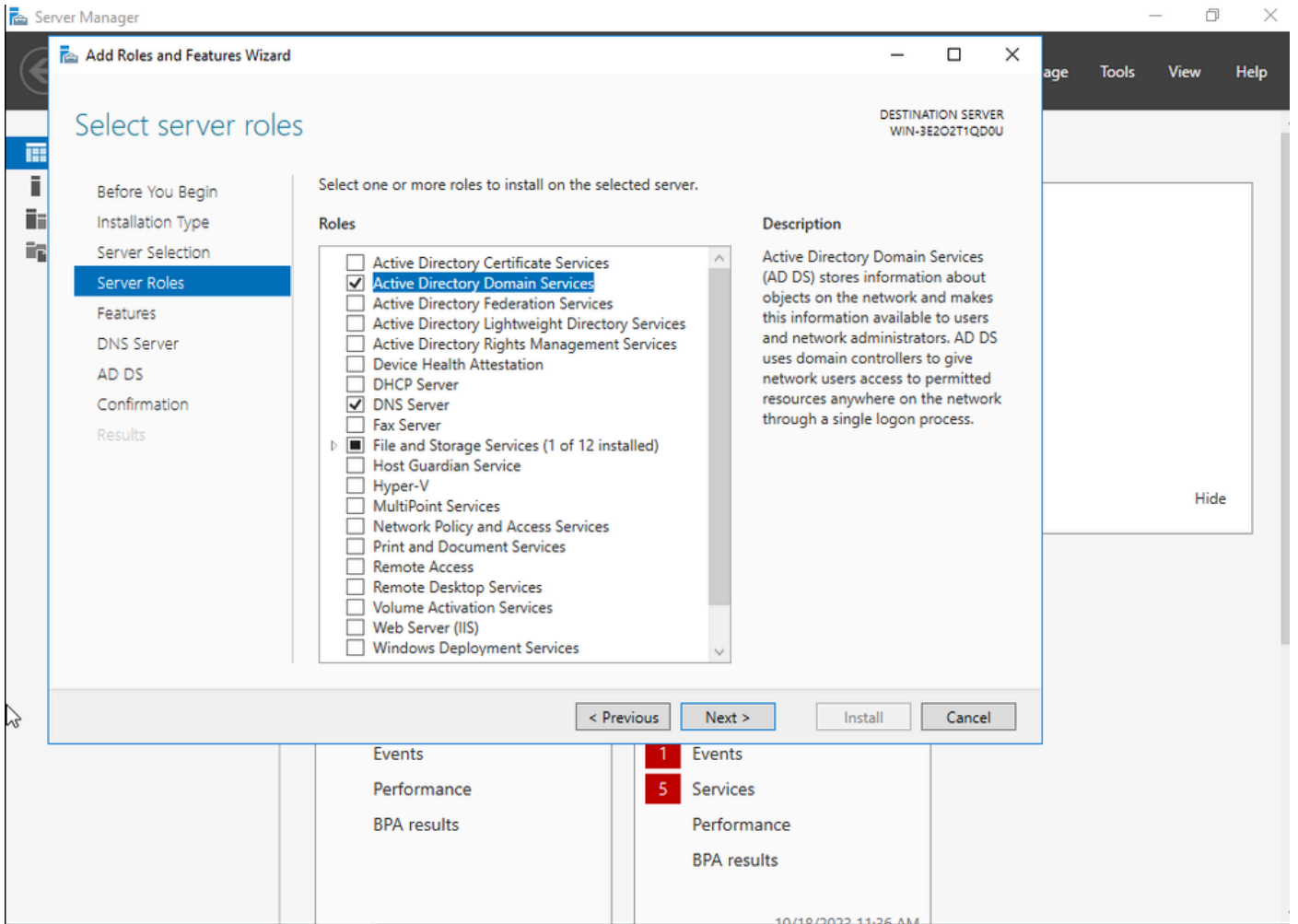
Windows Server 2016 SCEP CA

本文檔介紹用於實驗的Windows Server SCEP CA的基本安裝。對於企業運營，必須安全且適當地配置實際的生產級Windows CA。本節旨在幫助您在實驗室中對其進行測試，並從使此配置正常工作所需的設定中獲得靈感。以下是步驟：

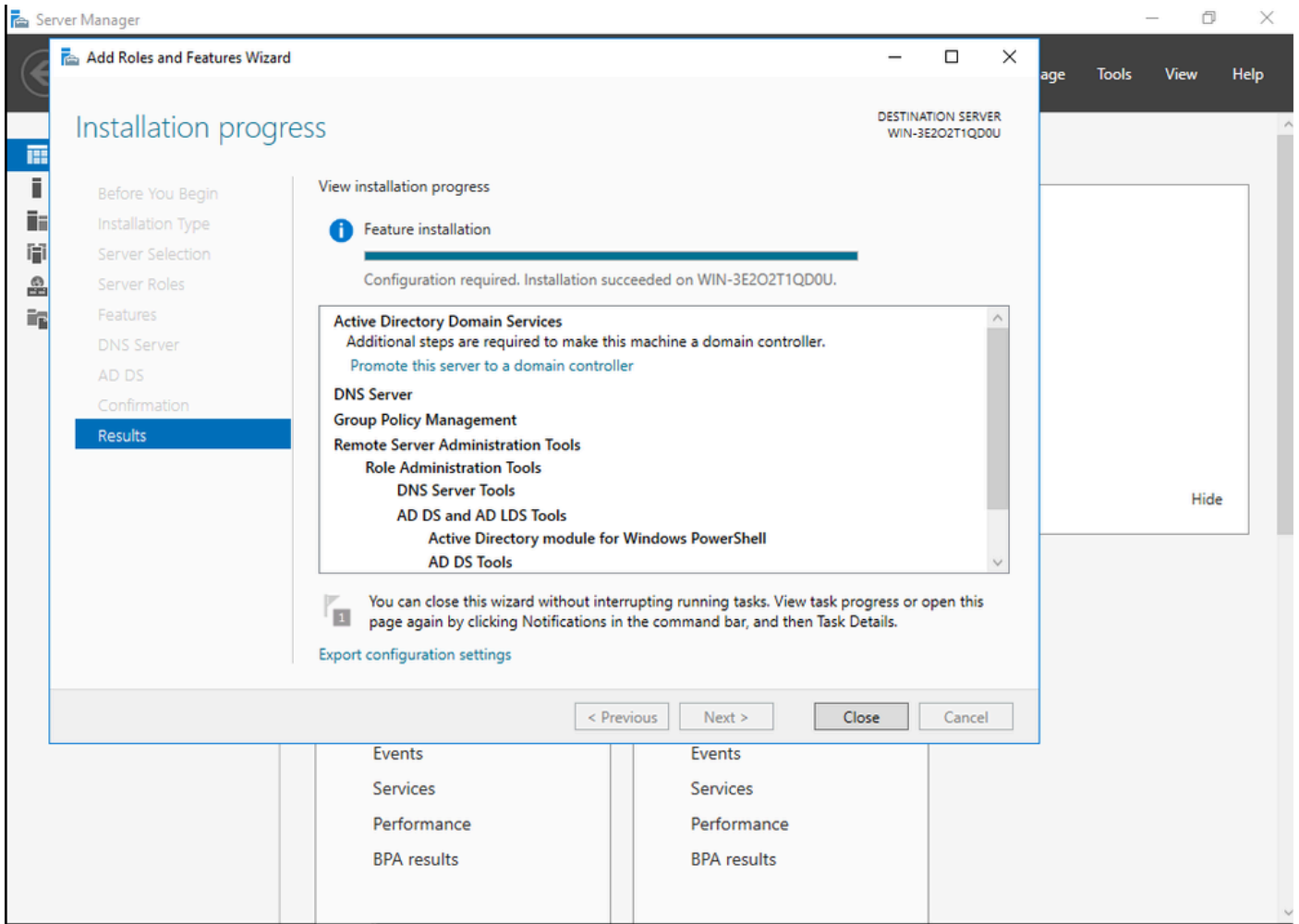
步驟1.安裝全新的Windows Server 2016案頭體驗。

步驟2.確保您的伺服器配置了靜態IP地址。

步驟3.安裝新的角色和服務，從Active Directory域服務和DNS伺服器開始。

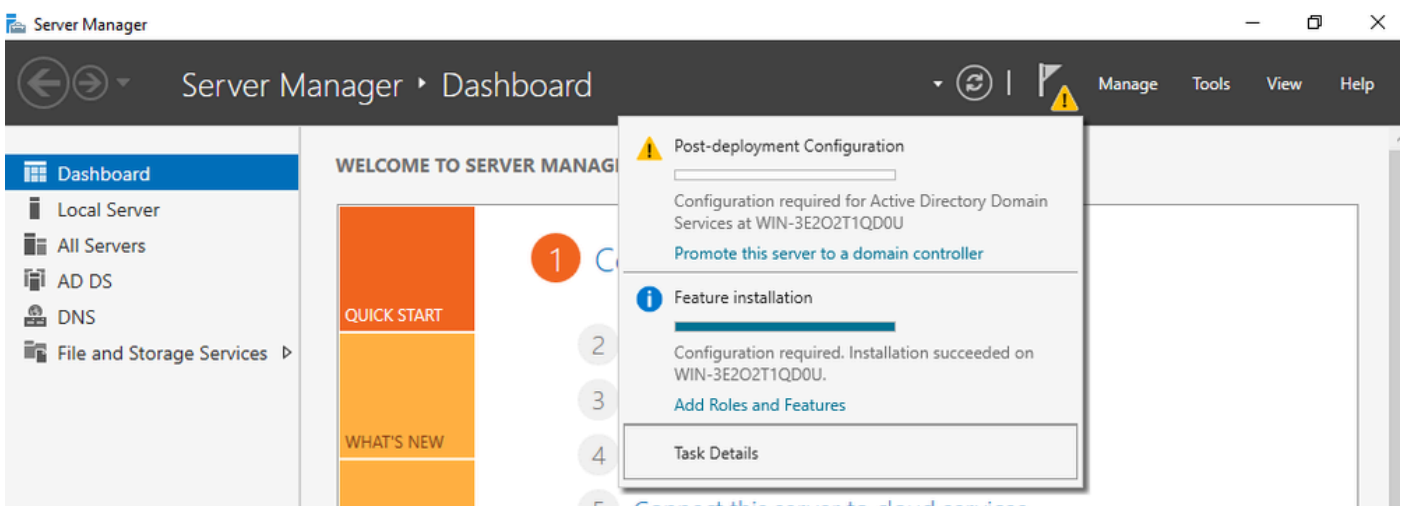


Active Directory安裝



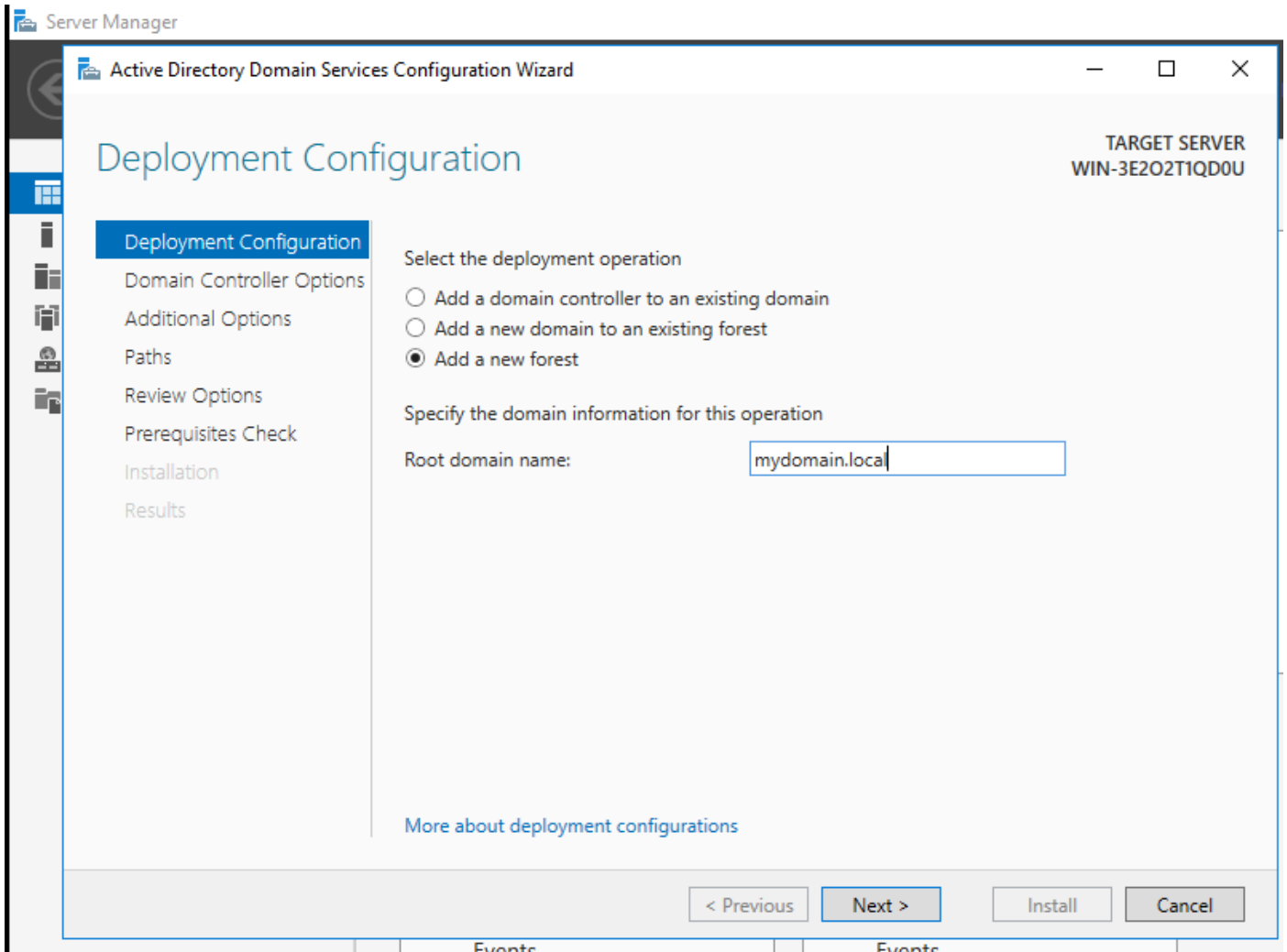
AD安裝結束

步驟4.完成後，在「Promote this server to a domain controller (將此伺服器升級為域控制器)」上按一下控制面板中的按鈕。



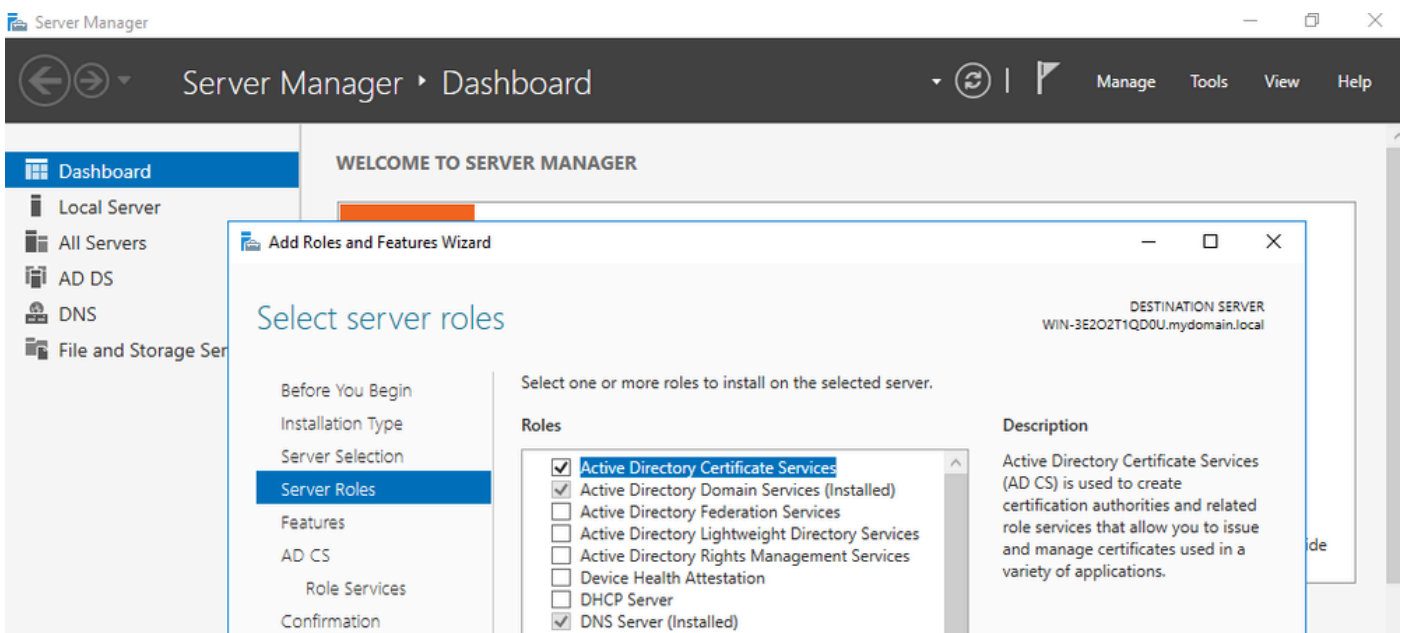
配置AD服務

步驟5.建立新林並選擇域名。

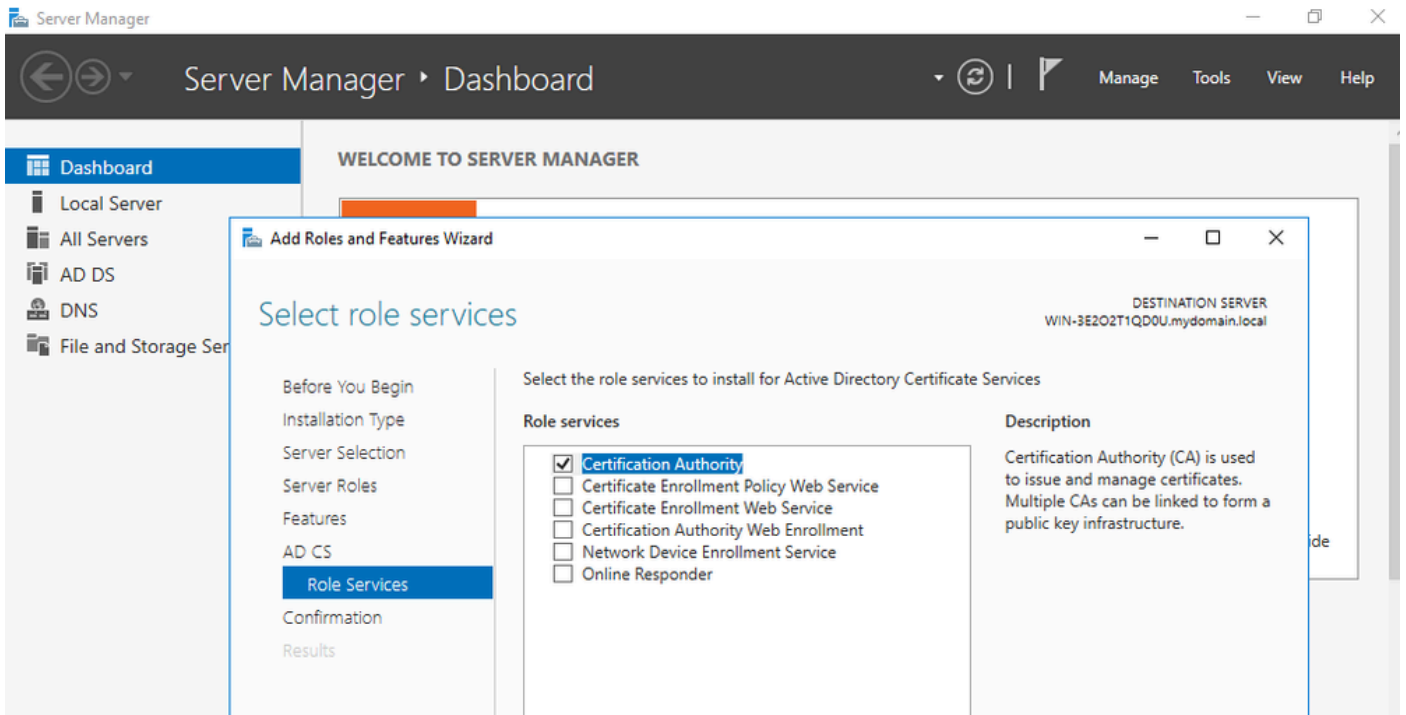


選擇林名稱

步驟6.將Certificate Services角色新增到伺服器：

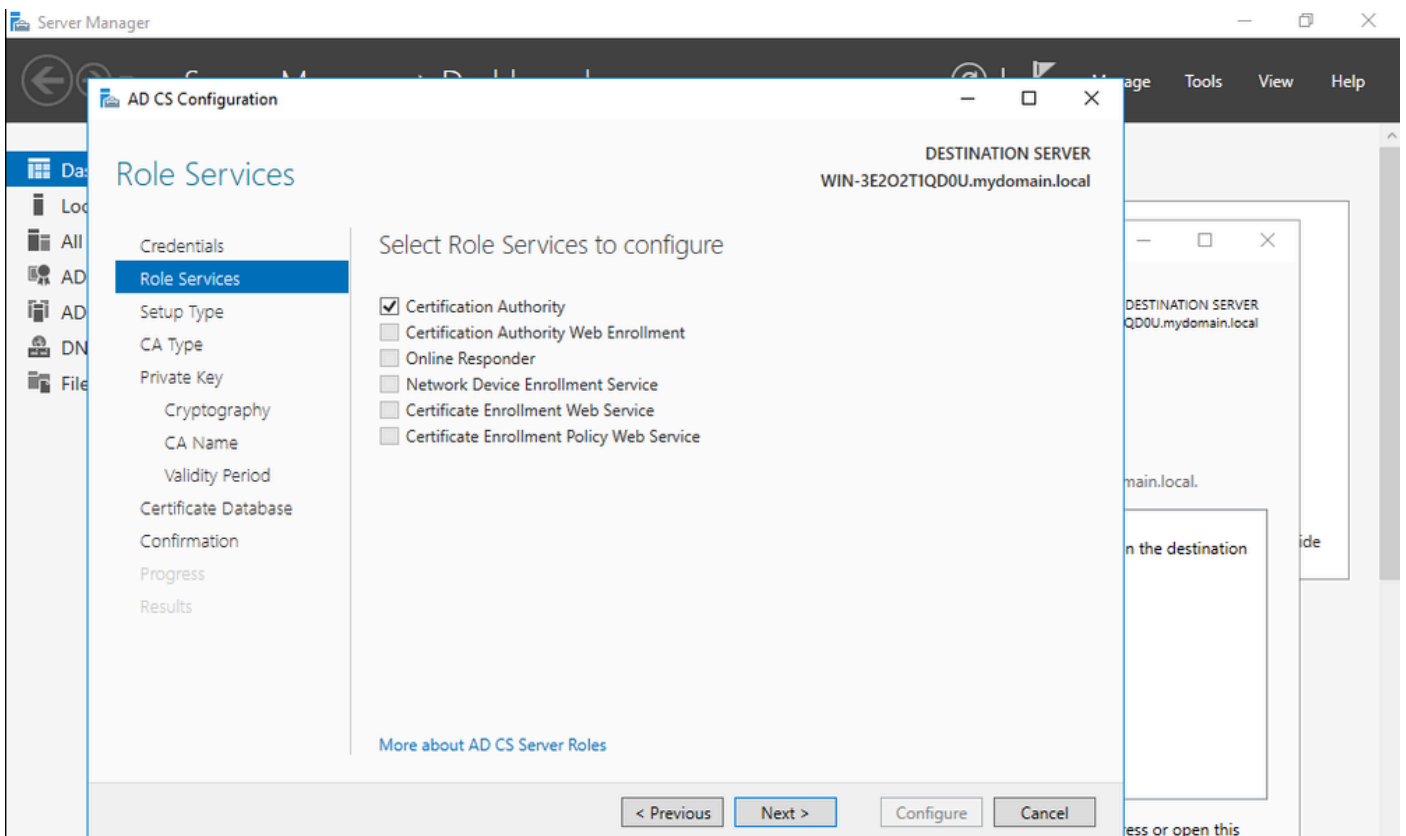


新增證書服務

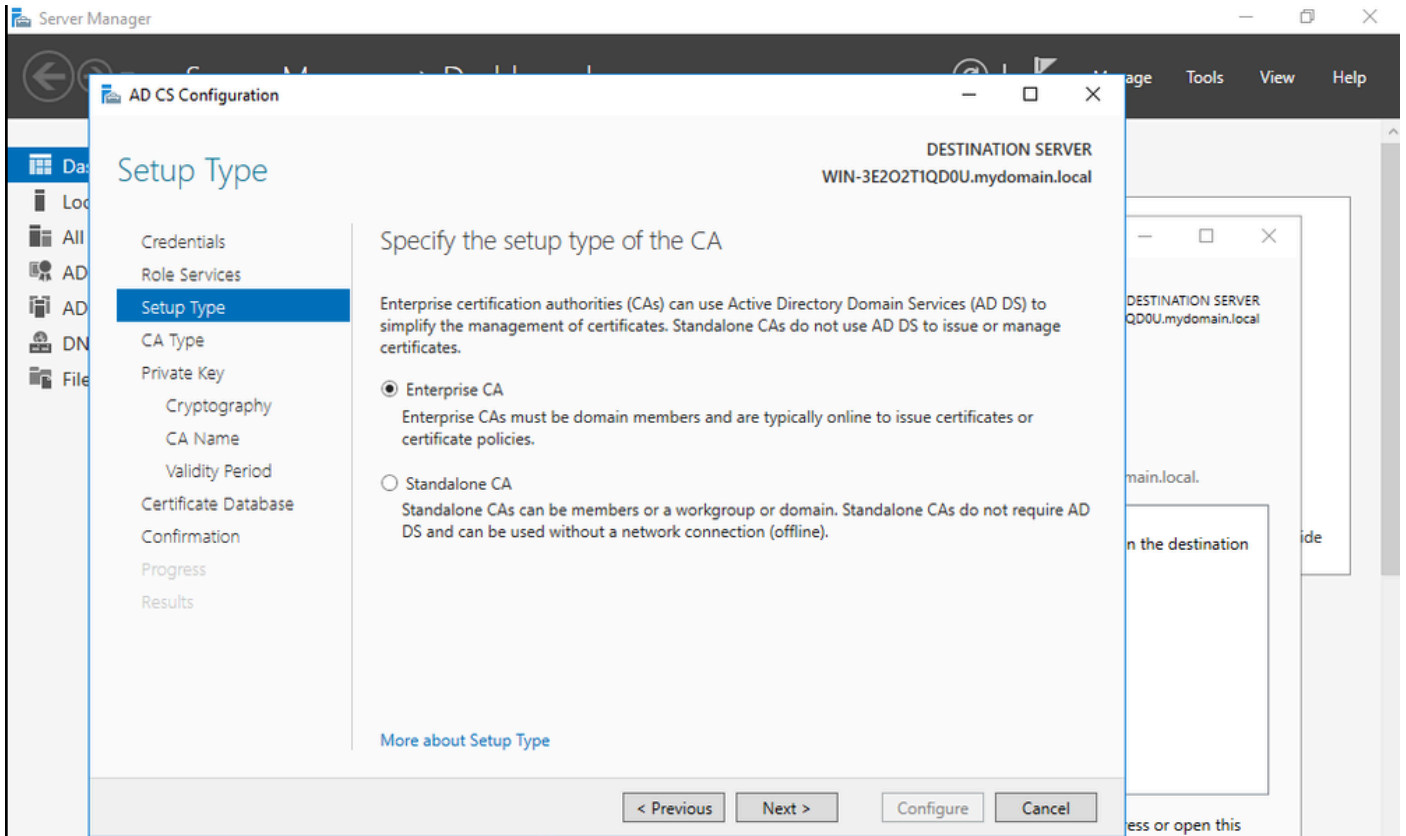


僅新增證書頒發機構

步驟7.完成之後，配置證書頒發機構。

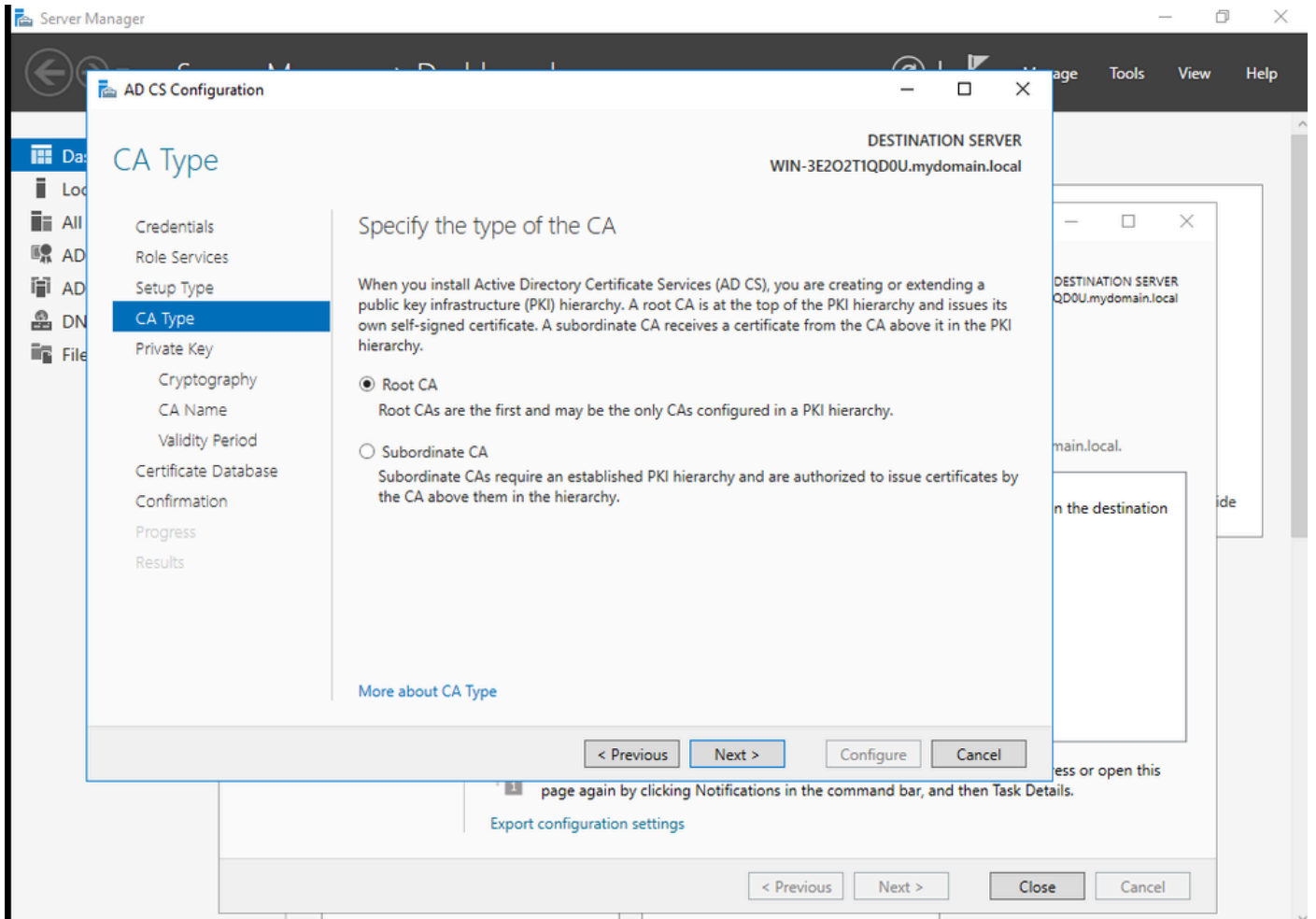


步驟8.選擇企業CA。



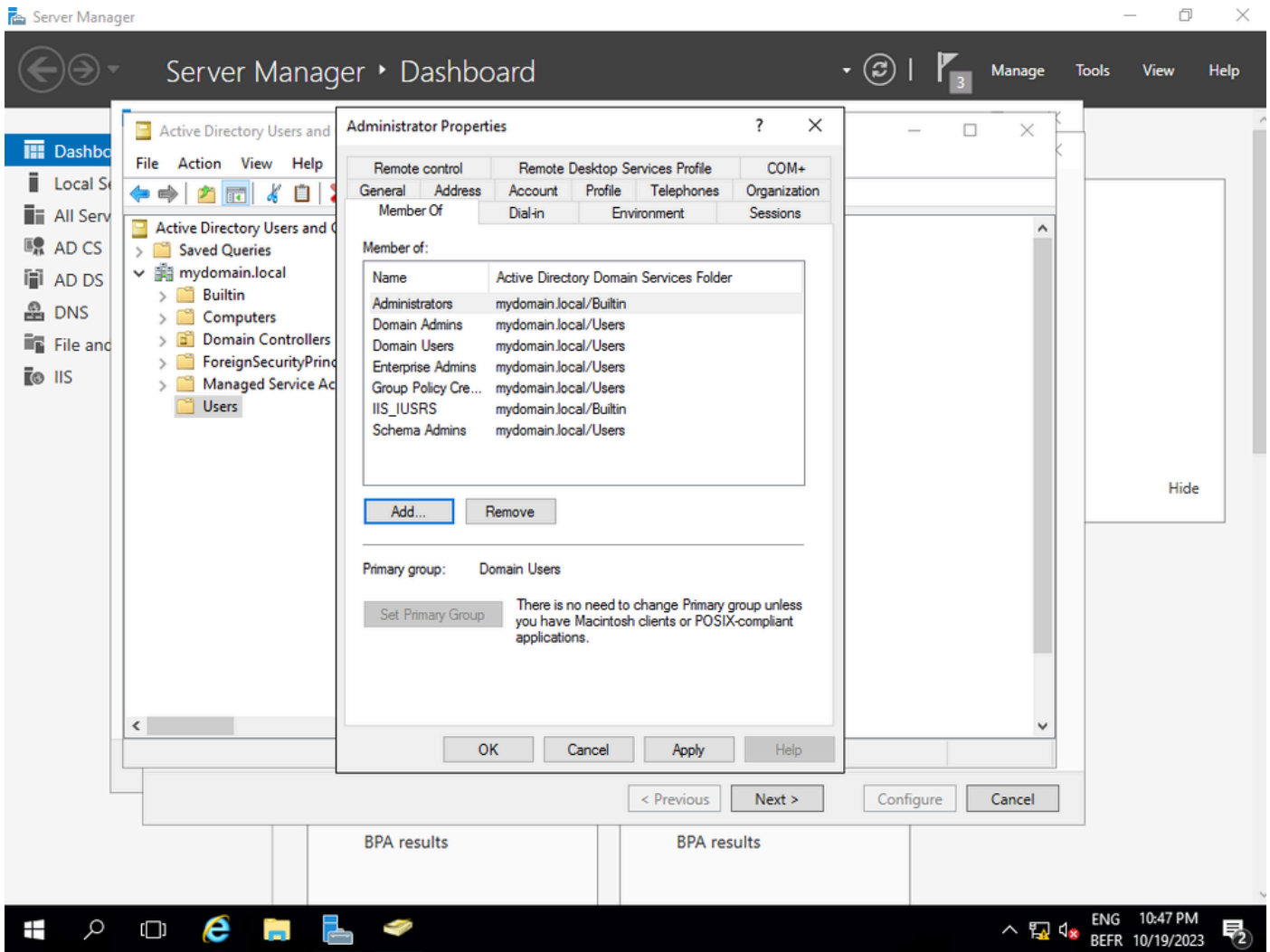
企業CA

步驟9.使其成為根CA。自Cisco IOS XE 17.6以來，LSC支援從屬CA。



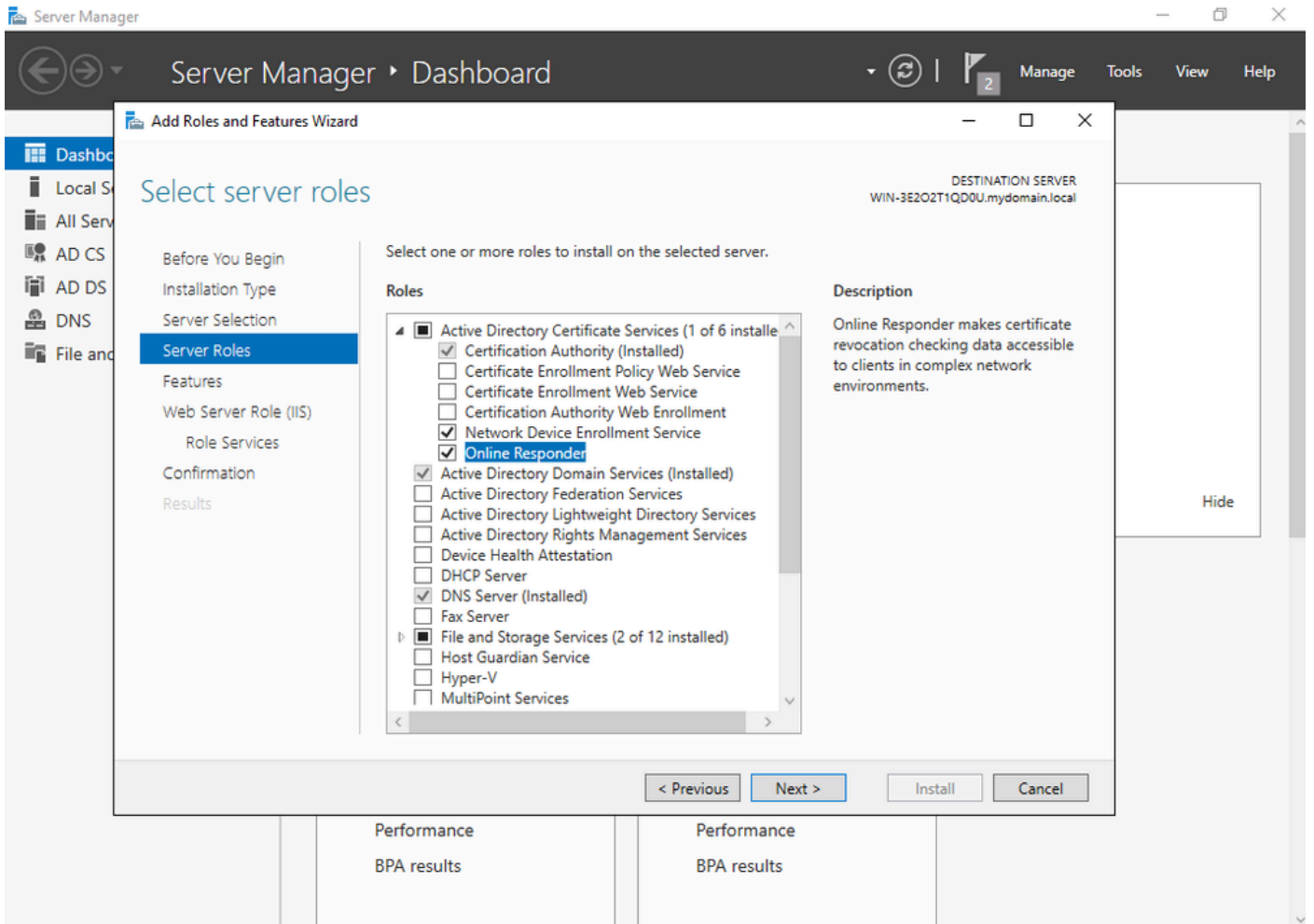
選擇根CA

請務必將用於CA的帳戶設為IIS_IUSRS組的一部分。在本示例中，您使用管理員帳戶並轉到Active Directory使用者和電腦選單，將管理員使用者新增到IIS_IUSRS組中。



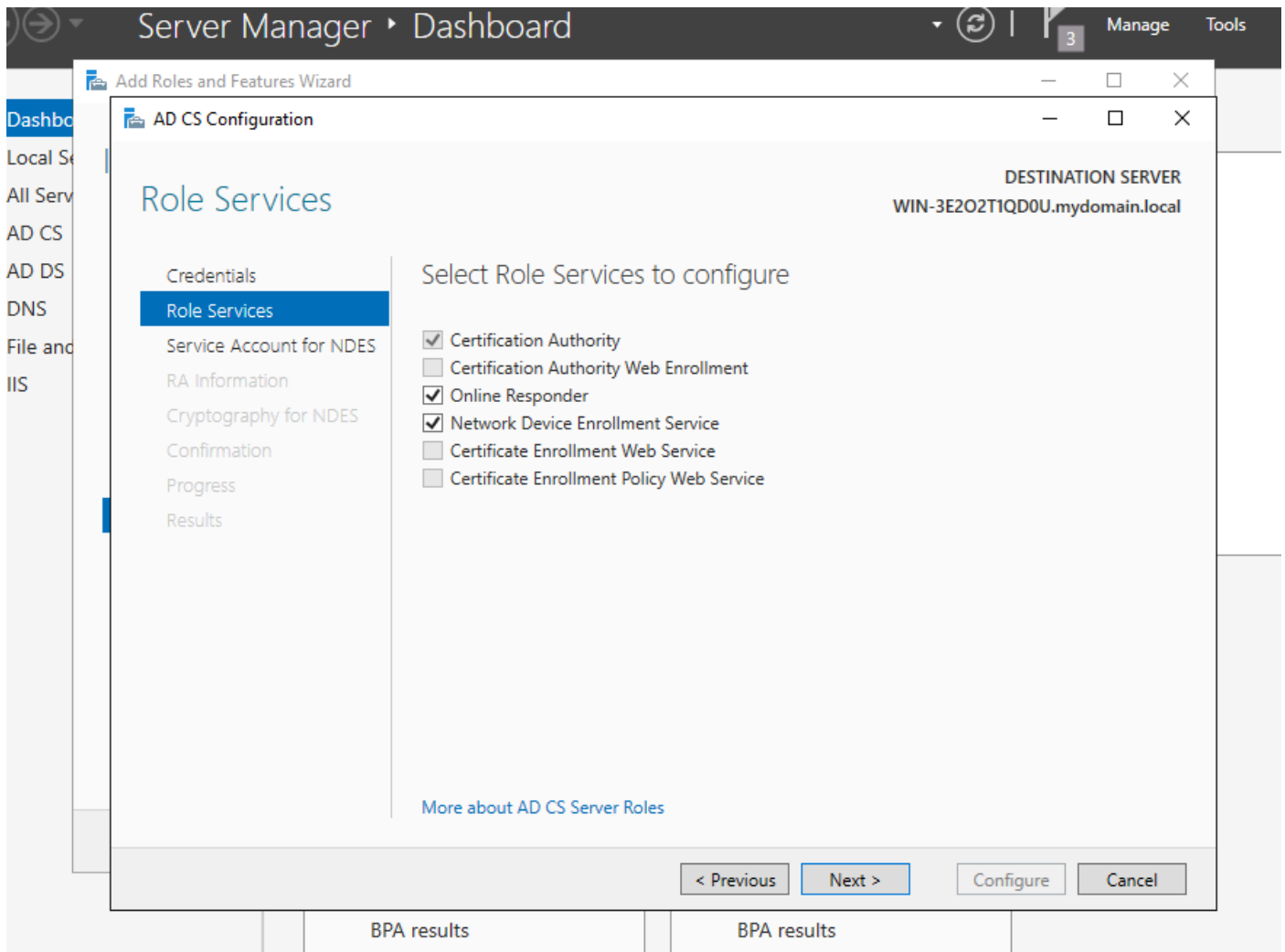
將管理員帳戶新增到IIS_USER組

步驟10.在正確的IIS組中擁有使用者後，新增角色和服務。然後將Online Responder和NDES服務新增到您的認證機構。



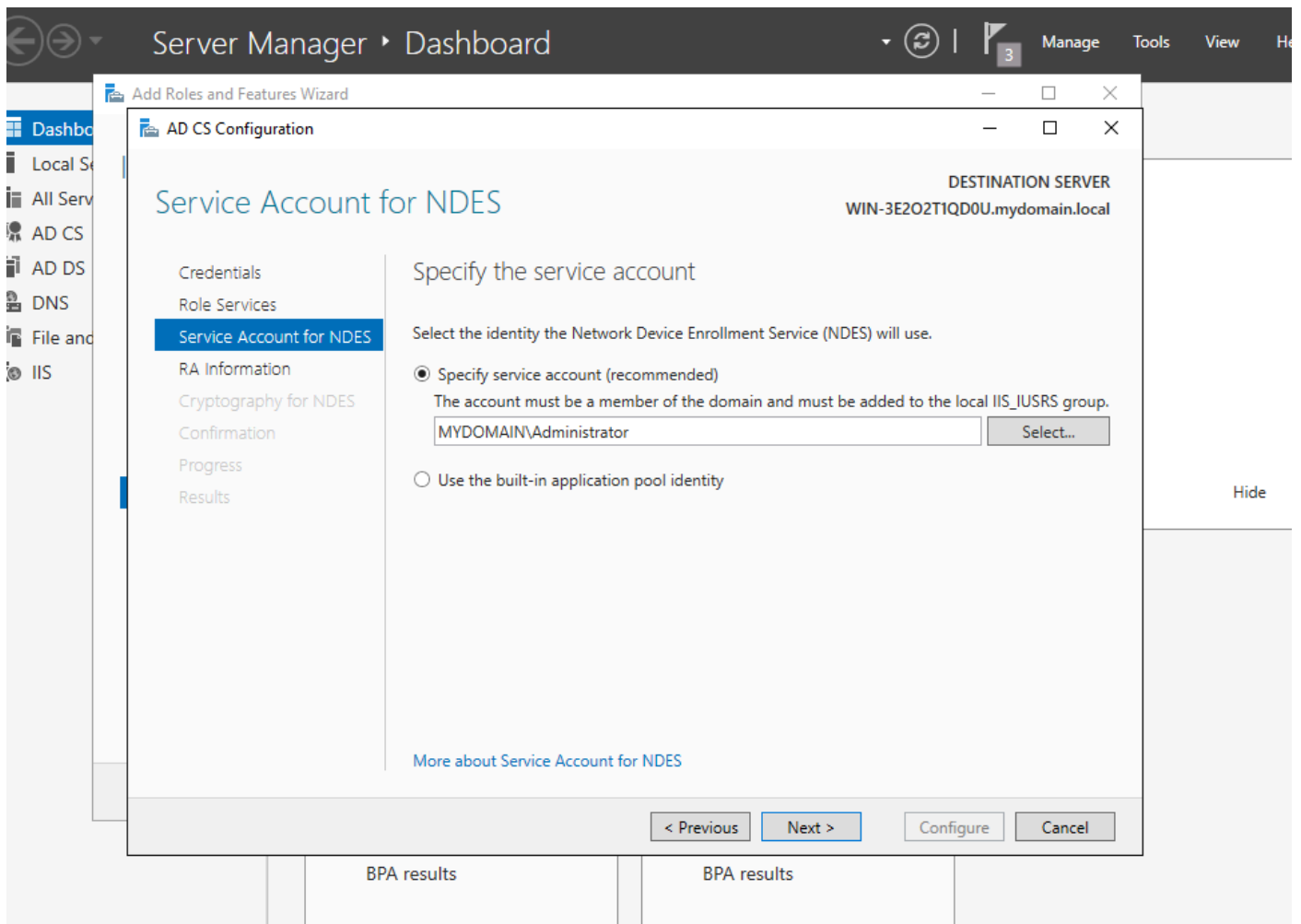
安裝NDES和線上響應程式服務

步驟11.完成後，配置這些服務。



安裝線上響應程式和NDES服務

步驟12.系統提示您選擇服務帳戶。這是您以前新增到IIS_IUSRS組的帳戶。



選擇已新增到IIS組的使用者

步驟13。這足以執行SCEP操作，但為了實現802.1X驗證，您還需要在RADIUS伺服器上安裝憑證。因此，為方便起見，請安裝和配置Web註冊服務，以便在Windows伺服器上輕鬆複製和貼上ISE證書請求。

Select server roles

DESTINATION SERVER
WIN-3E202T1QD0U.mydomain.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

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

Roles

- Active Directory Certificate Services (3 of 6 installed)
 - 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.

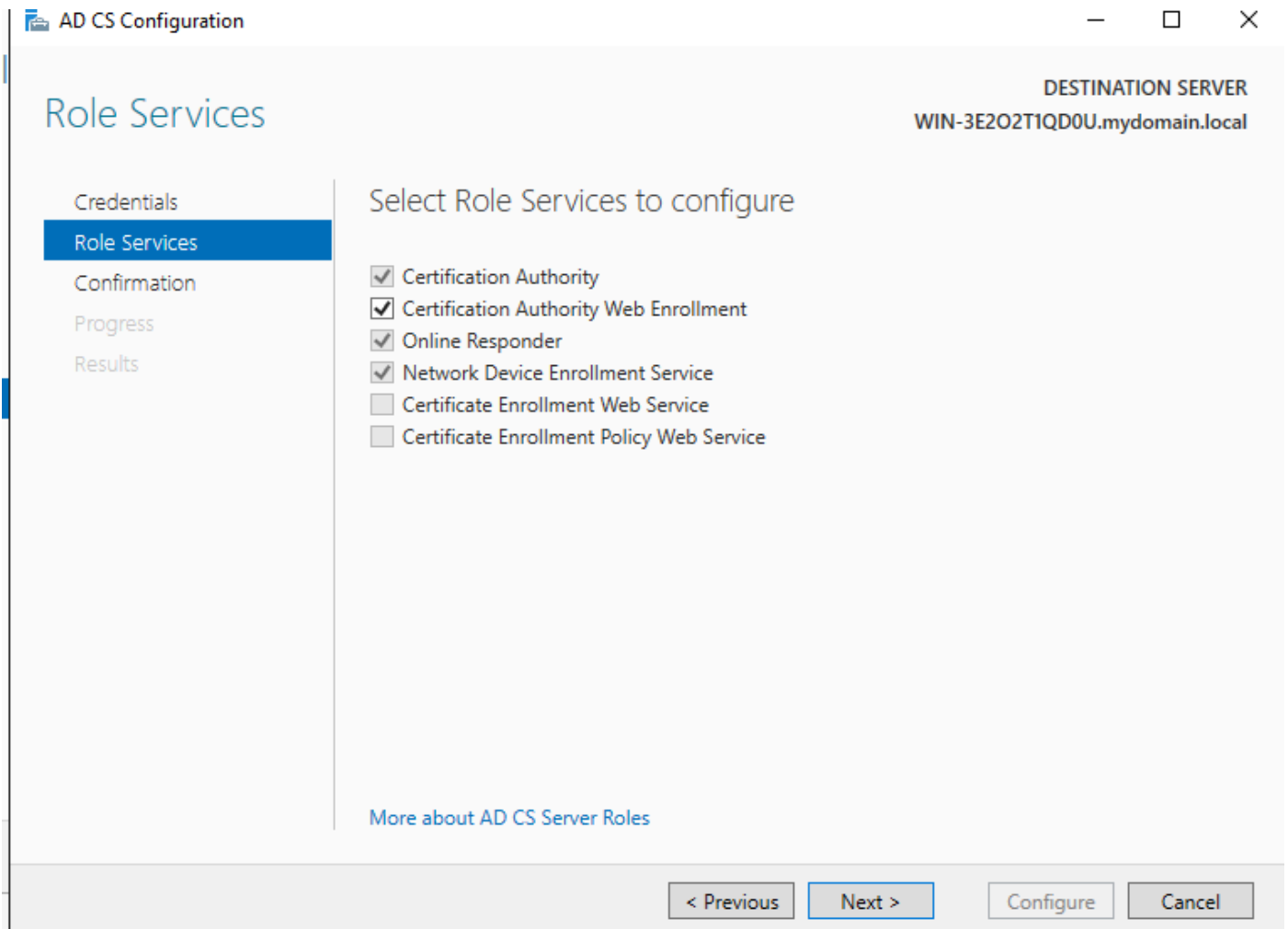
< Previous

Next >

Install

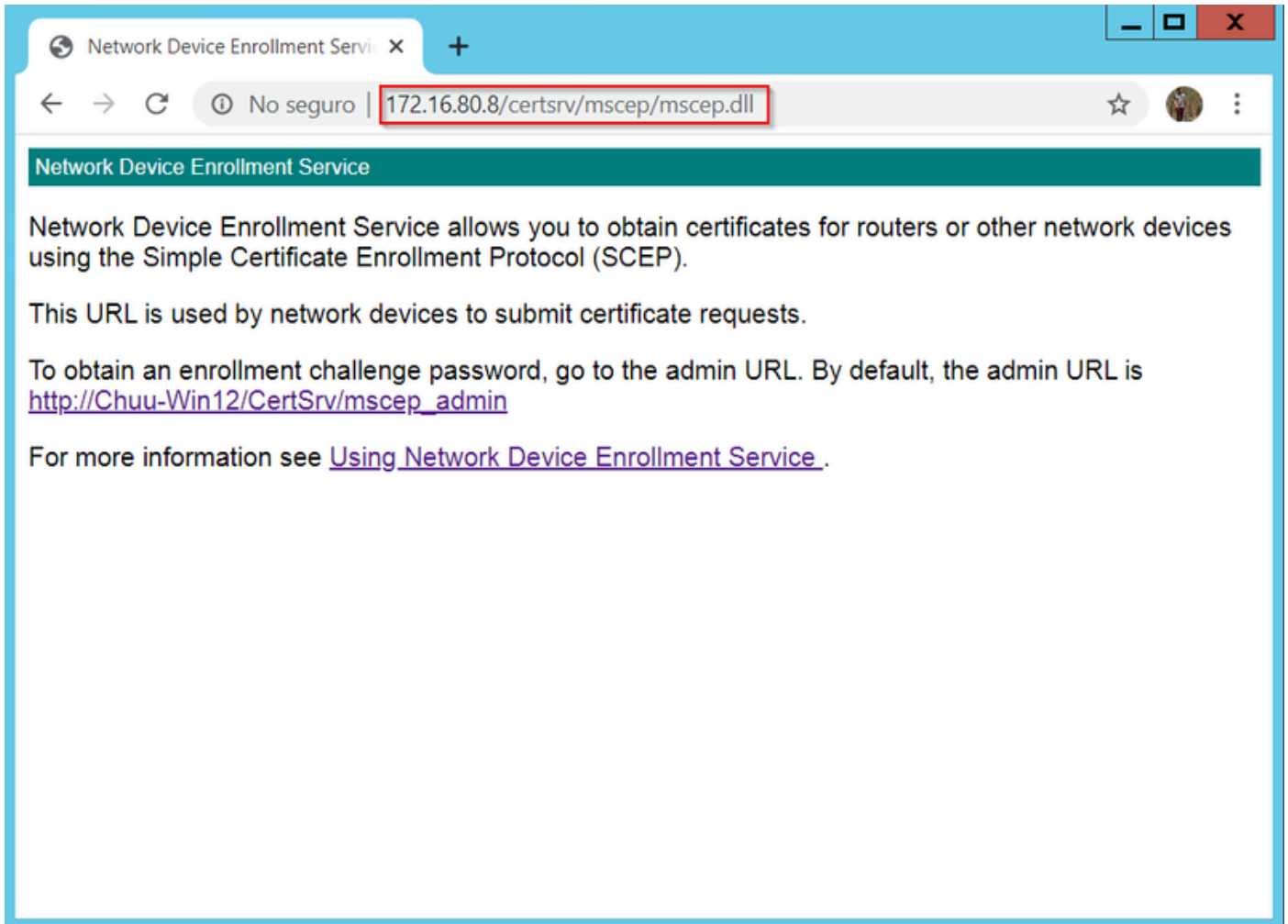
Cancel

安裝Web註冊服務



配置web註冊服務

步驟 14. 您可以訪問<http://<serverip>/certsrv/mscep/mscep.dll>，驗證SCEP服務是否正常運行：



SCEP入口驗證

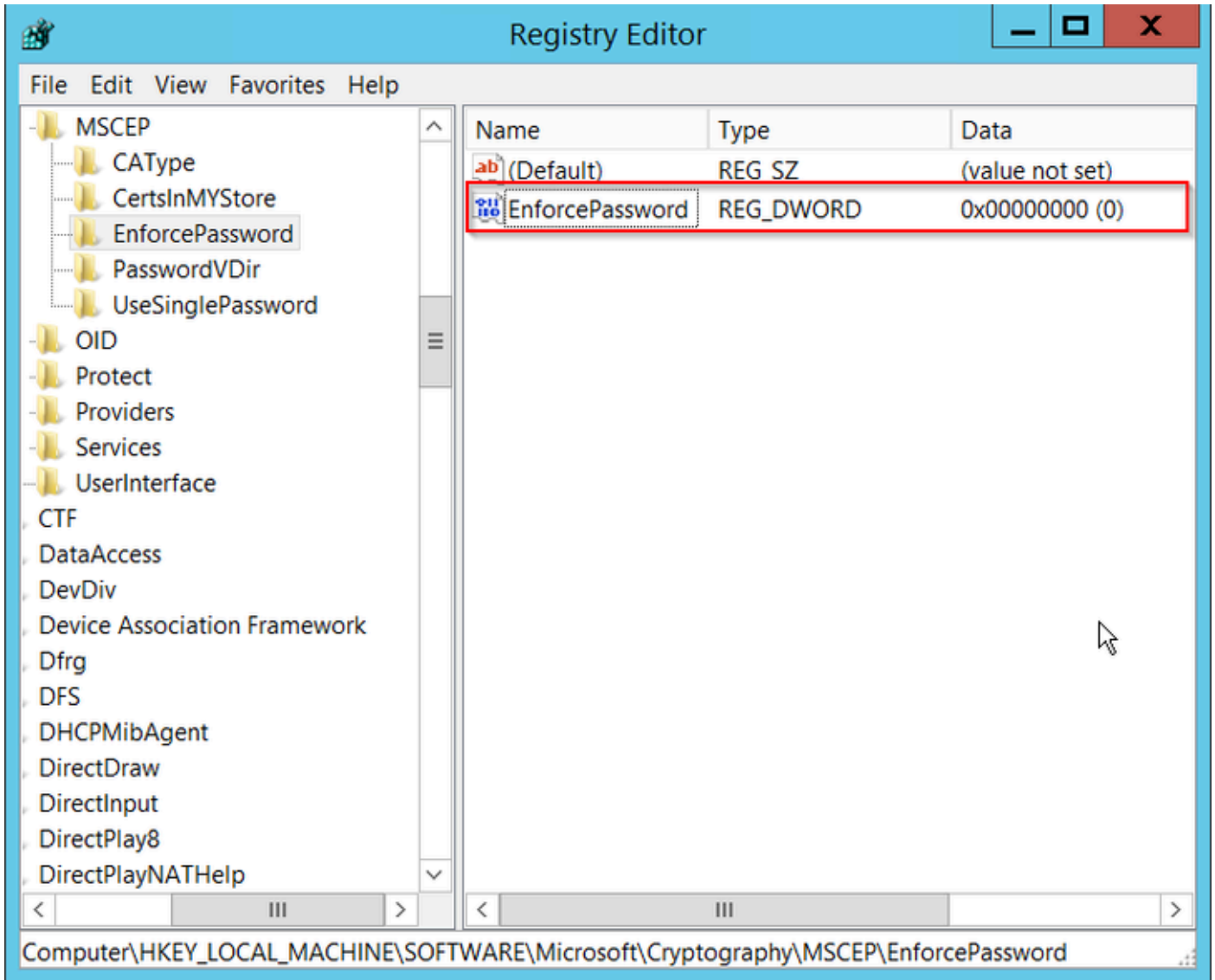
步驟 15.

預設情況下，Windows Server在Microsoft SCEP(MSCEP)註冊之前使用動態質詢密碼對客戶端和終端請求進行身份驗證。這需要管理員帳戶瀏覽到Web GUI為每個請求生成按需密碼（密碼必須包含在請求中）。控制器不能將此密碼包含在傳送給伺服器的請求中。要刪除此功能，需要修改NDES伺服器上的登錄檔項：

開啟登錄檔編輯器，在開始選單中搜尋Regedit。

導航到Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword

將EnforcePassword值更改為0。如果它已經是0，則保留原樣。



設定Enforcepassword值

配置證書模板和登錄檔


證書及其關聯金鑰可以在CA伺服器內的應用程式策略所定義的多個場景中用於不同的用途。應用策略儲存在證書的Extended Key Usage(EKU)欄位中。驗證器會分析此欄位，以驗證客戶端是否將其用於預期目的。要確保將正確的應用程式策略整合到WLC和AP證書，請建立正確的證書模板並將其對映到NDES登錄檔：

步驟 1. 導航到開始>管理工具>證書頒發機構。

步驟 2. 展開「CA伺服器」資料夾樹，按一下右鍵Certificate Templates資料夾並選擇Manage。

步驟 3. 按一下右鍵Users證書模板，然後在上下文選單中選擇Duplicate Template。

步驟 4. 定位至常規標籤，根據需要更改模板名稱和有效期，保留所有其它選項未選定。

 注意：修改有效期時，請確保有效期不超過證書頒發機構的根證書有效性。

Properties of New Template



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

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

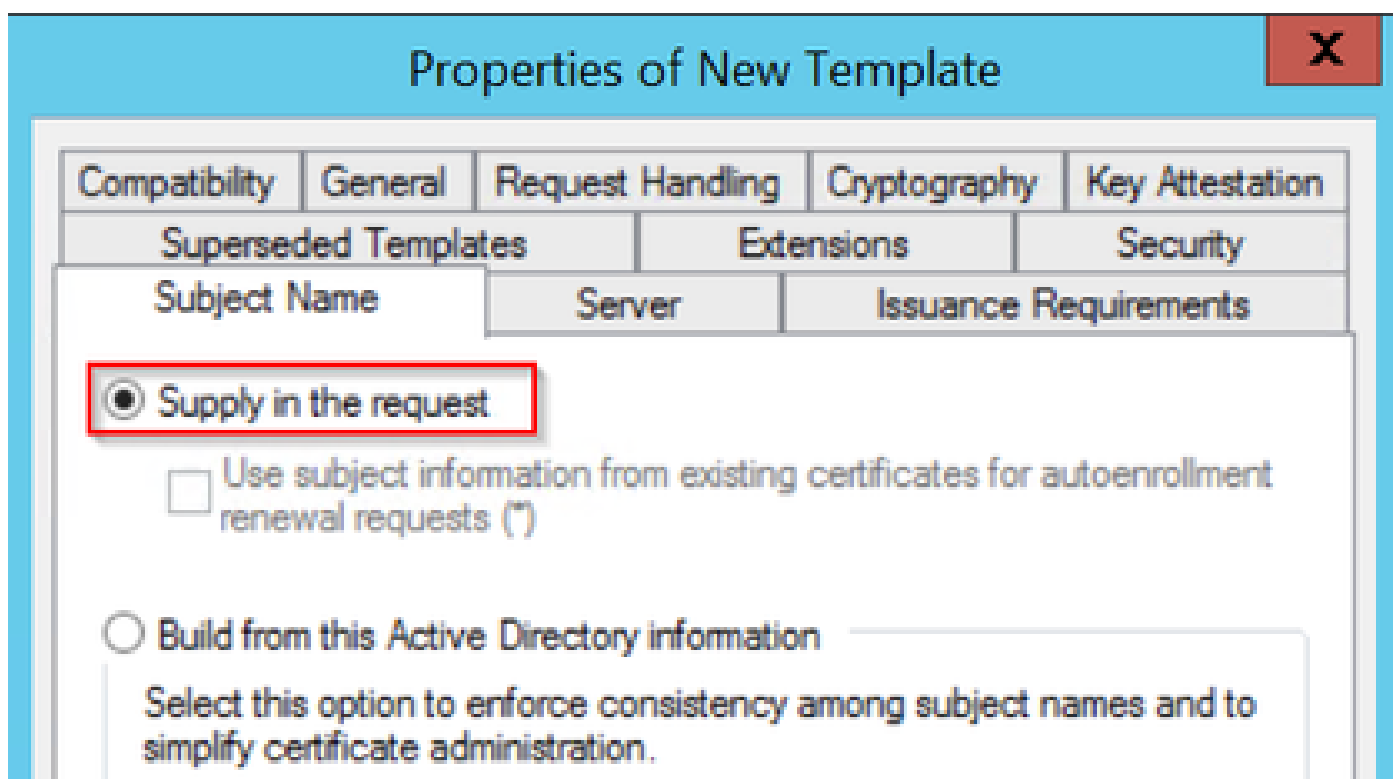
OK

Cancel

Apply

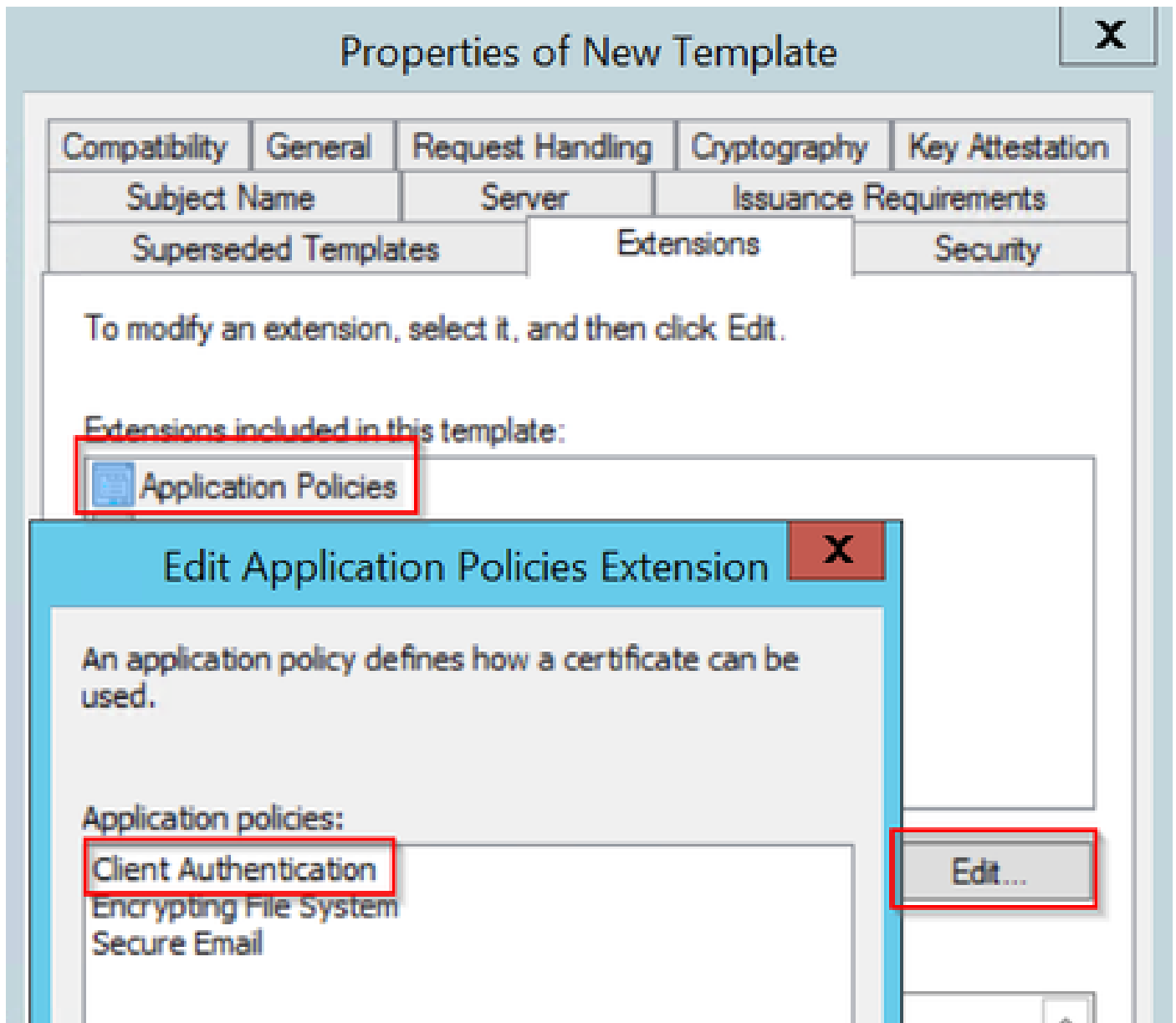
Help

步驟 5. 定位至主題名稱標籤，確保已選擇請求中的「供應」。系統將顯示一個彈出視窗，指示使用者不需要管理員批准即可簽署其證書，請選擇OK。



在請求中提供

步驟 6. 導航到Extensions頁籤，然後選擇Application Policies選項，然後選擇Edit...按鈕。確保Application Policies視窗中的Client Authentication；否則，選擇Add並新增它。



驗證擴展

步驟 7. 導航到 Security 選項卡，確保在 Windows 伺服器中啟用 SCEP 服務的步驟 6 中定義的服務帳戶具有模板的完全控制許可權，然後選擇 Apply 和 OK。

Properties of New Template



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

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)

Add... Remove

Permissions for Administrator

	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>


For special permissions or advanced settings, click Advanced.

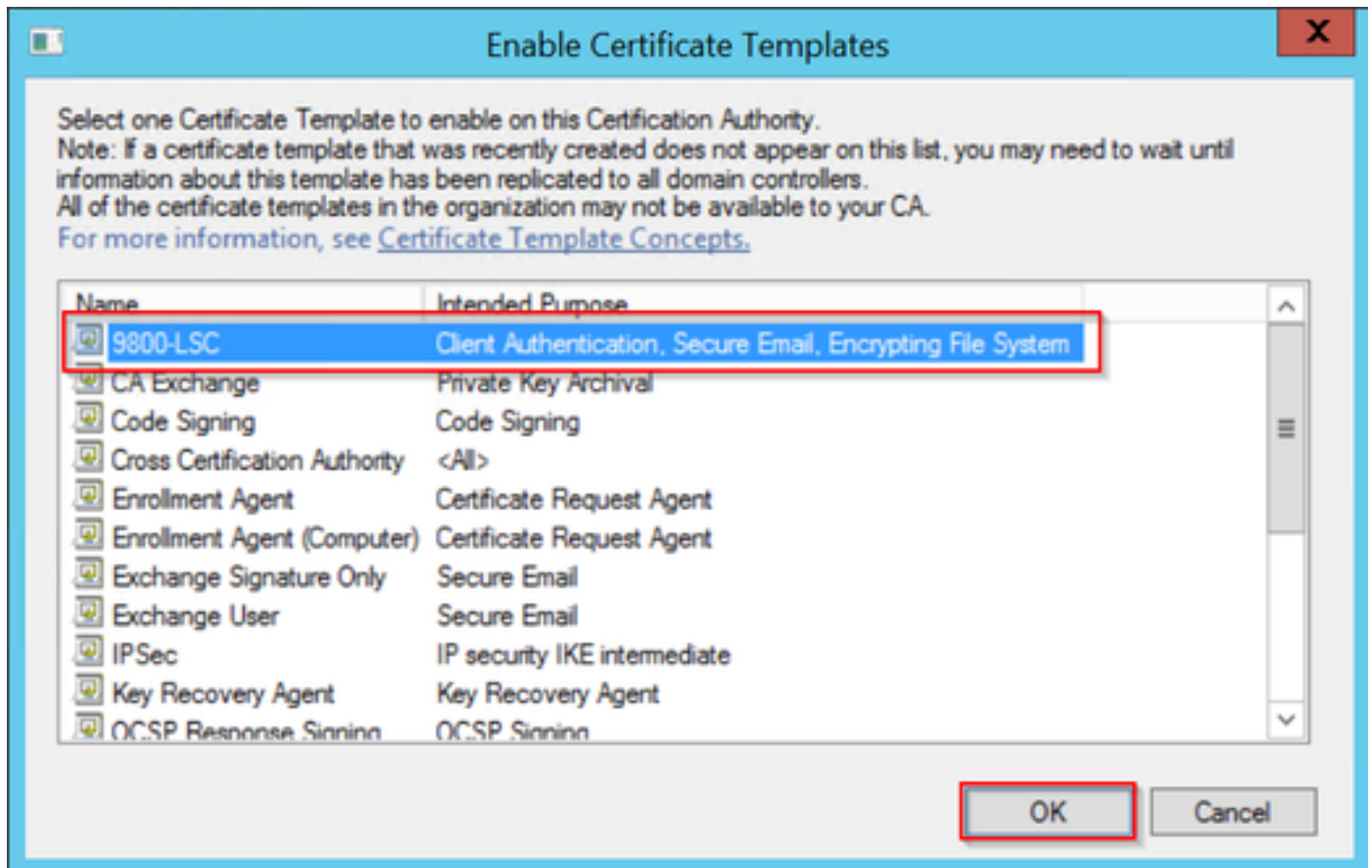
Advanced

OK Cancel **Apply** Help

步驟 8. 返回證書頒發機構視窗，按一下右鍵Certificate Templates資料夾，然後選擇New > Certificate Template to Issue。

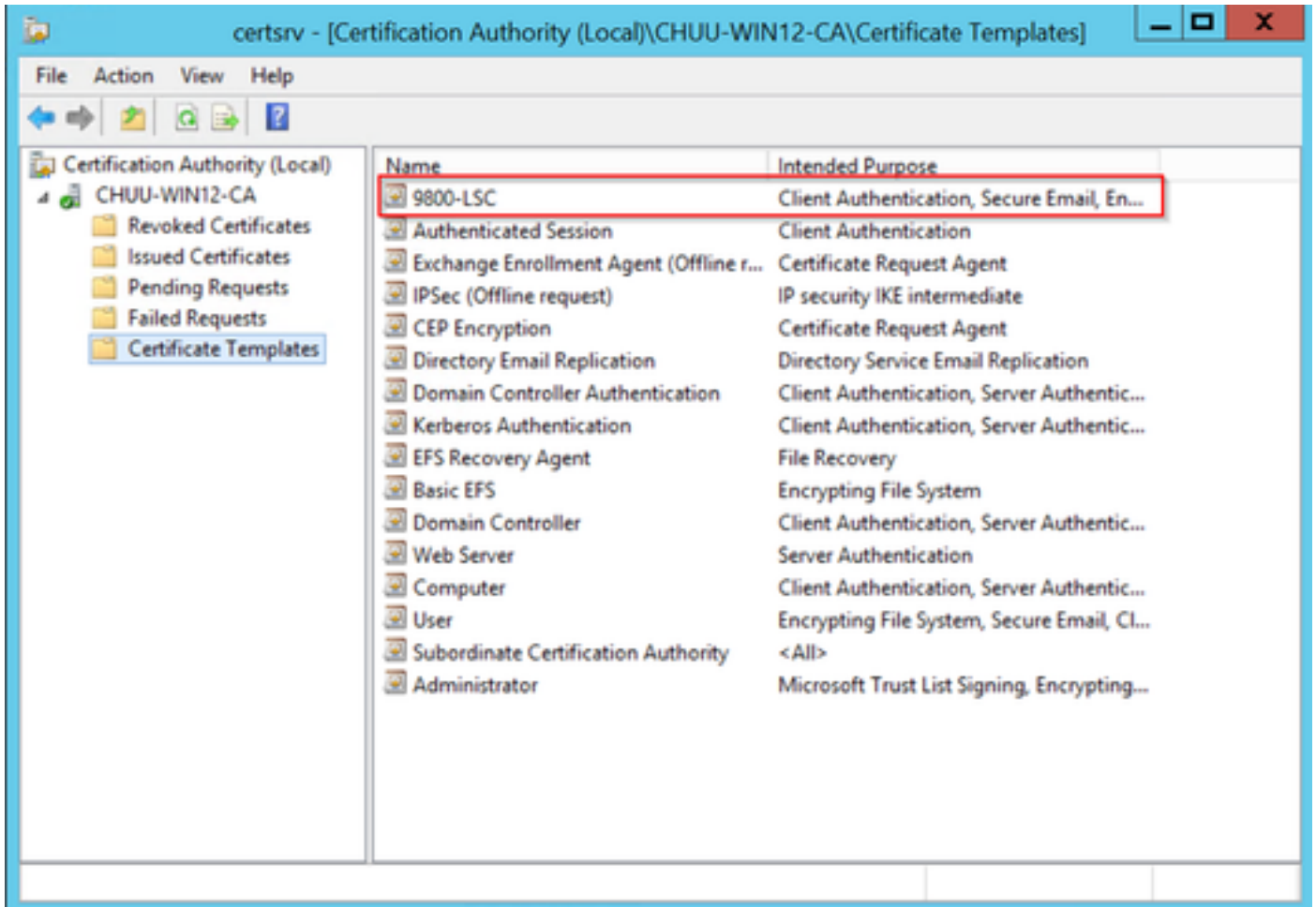
步驟 9. 選擇以前建立的證書模板（在此示例中為9800-LSC），然後選擇OK。

 注意：由於需要在所有伺服器上複製新建立的證書模板，因此在多台伺服器部署中列出該模板可能需要較長時間。



選擇模板

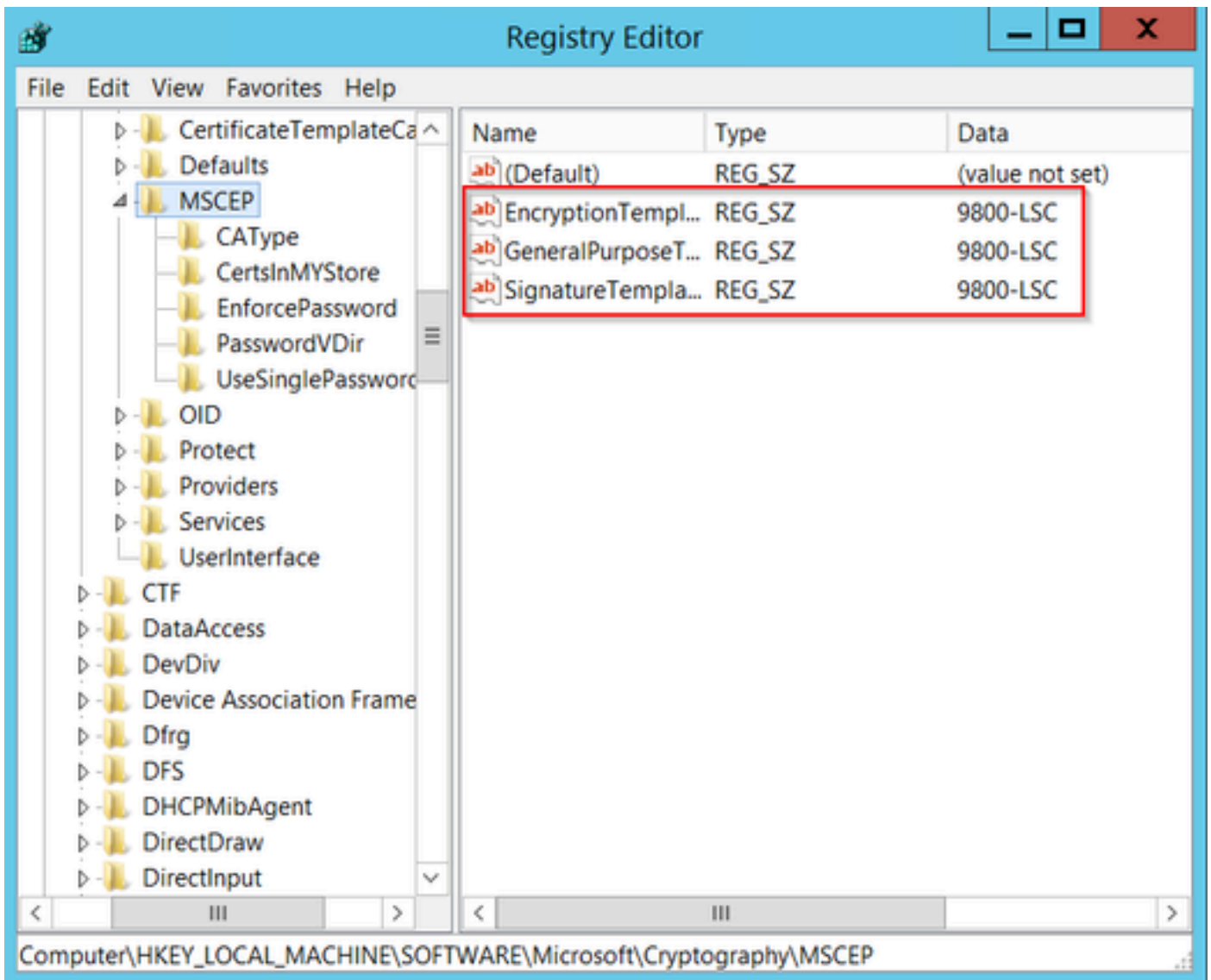
新證書模板現在列在Certificate Templates檔案夾內容中。



選擇LSC

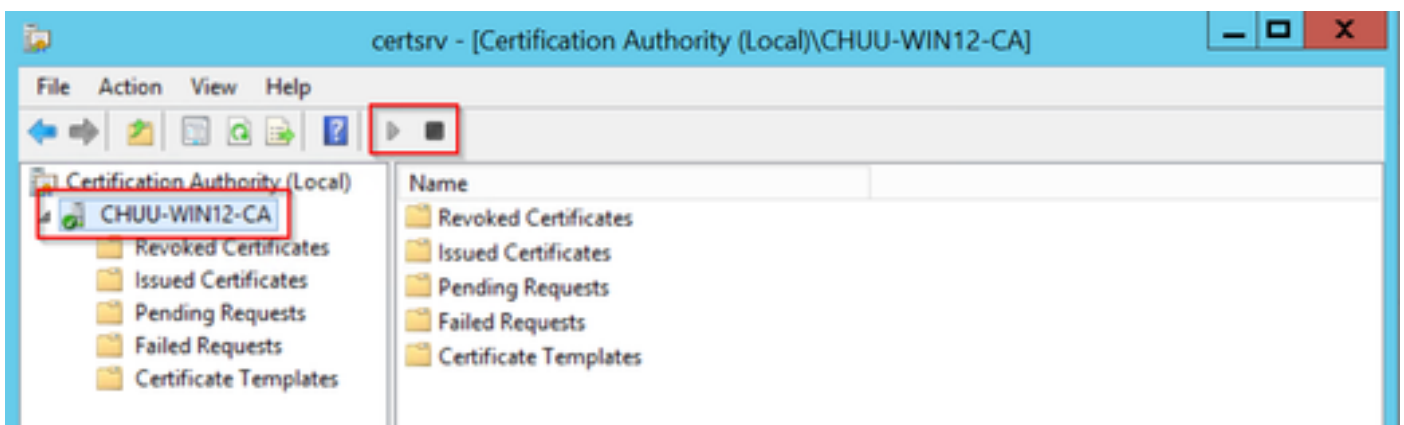
步驟 10. 返回Registry Editor視窗並導航到Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP。

步驟 11. 編輯EncryptionTemplate、GeneralPurposeTemplate和SignatureTemplate登錄檔，使其指向新建立的證書模板。



在登錄檔中更改模板

步驟 12. 重新啟動NDES伺服器，返回到Certification Authority 視窗，選擇伺服器名稱，然後依次選擇Stop 和Play 按鈕。



在9800上配置LSC

以下是在WLC中為AP配置LSC的序列步驟。

1. 建立RSA金鑰。此金鑰稍後用於PKI信任點。
2. 建立信任點並對映建立的RSA金鑰。
3. 為AP啟用LSC調配並對映信任點。
 1. 為所有加入的AP啟用LSC。
 2. 通過預配清單為選定的AP啟用LSC。
4. 更改無線管理信任點並指向LSC信任點。

AP LSC GUI配置步驟

步驟1.導覽至Configuration > Security > PKI Management > Key Pair Generation.

1. 點選add並為其指定相關名稱。
2. 新增RSA金鑰大小。
3. 可匯出金鑰選項是可選的。只有在您想將金鑰從盒子中匯出時才需要這樣做。
4. 選擇生成

The screenshot shows the Cisco ISE GUI for PKI Management. The 'Key Pair Generation' tab is selected. A table lists existing key pairs:

Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	<input type="checkbox"/>
9800-40.cisco.com	RSA	No	<input type="checkbox"/>
TP-self-signed-2147029136.server	RSA	No	<input type="checkbox"/>
CISCO_IDEVID_SUDI	RSA	No	<input type="checkbox"/>
CISCO_IDEVID_SUDI_LEGACY	RSA	No	<input type="checkbox"/>

The modal window for adding a new key pair has the following fields:

- Key Name*: AP-SCEP
- Key Type*: RSA Key EC Key
- Modulus Size*: 2048
- Key Exportable*:

Buttons: Cancel, Generate

步驟 2.導航至Configuration > Security > PKI Management > Trustpoints

1. 點選add並為其指定相關名稱。
2. 輸入註冊URL(此處的URL為<http://10.106.35.61:80/certsrv/mscep/mscep.dll>)及其餘詳細資訊。
3. 選擇在步驟1中建立的RSA金鑰對。
4. 按一下「Authenticate」。
5. 點選註冊信任點並輸入密碼。
6. 按一下Apply to Device (應用到裝置) 。

Configuration > Security > PKI Management

Add Trustpoint

Label* Enrollment Type SCEP Terminal

Subject Name

Country Code State

Location Domain Name

Organization Email Address

Enrollment URL Authenticate

Key Generated Available RSA Keypairs

Enroll Trustpoint

Password*

Re-Enter Password*

步驟3.導覽至Configuration > Wireless > Access Points。向下滾動並選擇LSC Provision。

1. 將狀態選擇為已啟用。這會為連線到此WLC的所有AP啟用LSC。
2. 選擇我們在步驟2中建立的信任點名稱。

根據需要填寫其餘詳細資訊。

Configuration > Wireless > Access Points

All Access Points

Total APs: 1

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
AP0C00-F89A-46E0	C9117AX0-D	2	●	0 days 0 hrs 26 mins 42 secs	10.105.101.158	d8ec.3579.0300	0cd0.f89a.46e0	Local	Yes	Registered	Healthy

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Status Subject Name Parameters

Trustpoint Name

Country

State

City

Organization

Number of Join Attempts

Key Size

Certificate chain status

Number of certificates on chain

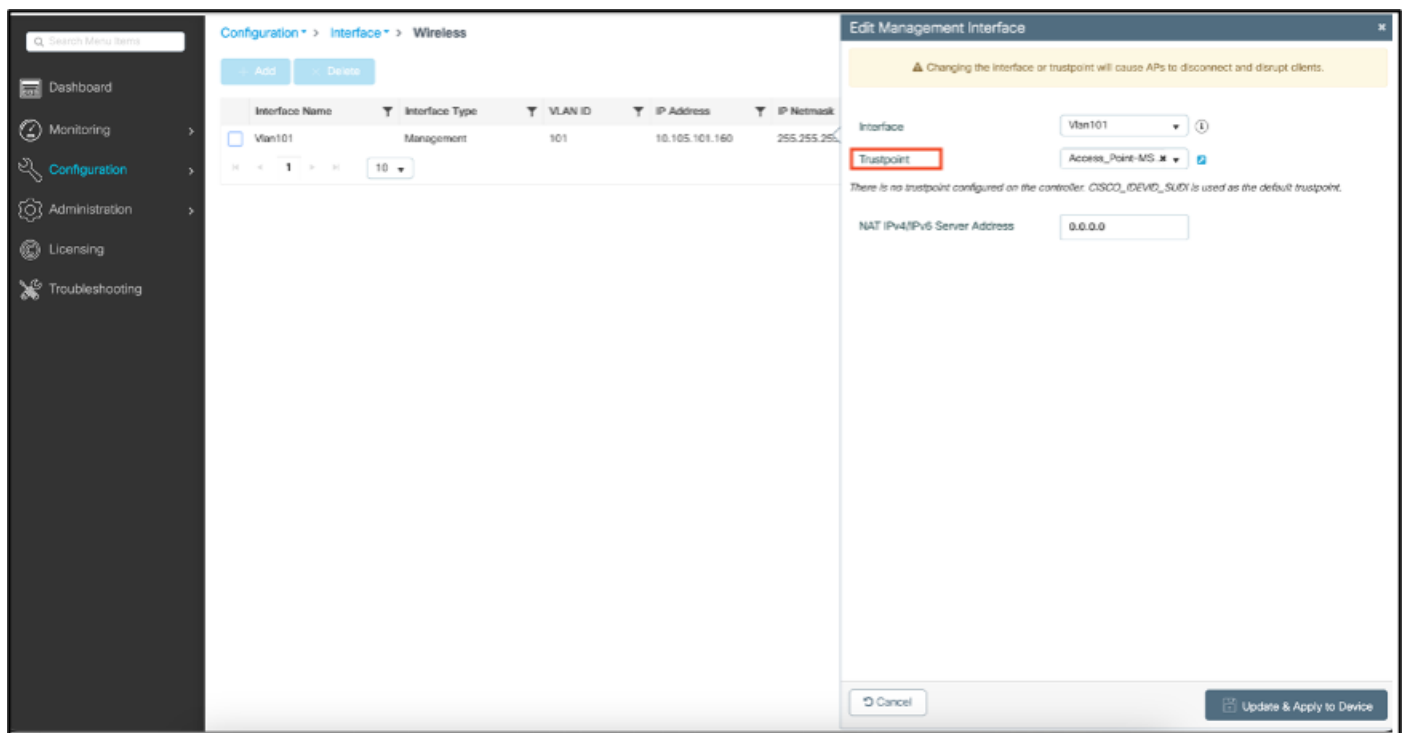
啟用LSC後，AP會通過WLC下載證書並重新啟動。在AP控制檯會話中，您會看到類似以下代碼片段的內容。

```
[*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
```

步驟4.啟用LSC後，可以更改無線管理證書以匹配LSC信任點。這會使AP加入其LSC證書，並且WLC使用其LSC證書加入AP。如果您唯一感興趣的是對AP進行802.1X身份驗證，則這是可選步驟。

1. 前往Configuration > Interface > Wireless，然後按一下Management Interface。
2. 更改Trustpoint以匹配我們在步驟2中建立的信任點。

LSC GUI配置部分到此結束。AP現在必須能夠使用LSC證書加入WLC。



AP LSC CLI配置步驟

1.使用此命令建立RSA金鑰。

```
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 storage
```

```
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. 建立PKI信任點並對映RSA金鑰對。輸入註冊URL及其餘詳細資訊。

```
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)#rsa-keypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. 使用crypto pki authenticate <trustpoint>命令向CA伺服器驗證並註冊PKI信任點。在密碼提示中輸入密碼。

```
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' command will 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.使用LSC證書配置AP加入。

```
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.更改無線管理信任點，使其與上面建立的信任點匹配。

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

AP LSC驗證

在WLC上運行這些命令以驗證LSC。

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

```

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-OTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 002.lx LSC Status
Certificate status : Not Available
AP LSC authentication state : CAPWAP-OTLS

```

重新載入AP後，登入到AP CLI並運行這些命令以驗證LSC配置。

```

#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:d1:00:00:00:00:00:00
  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
```

排除LSC調配故障

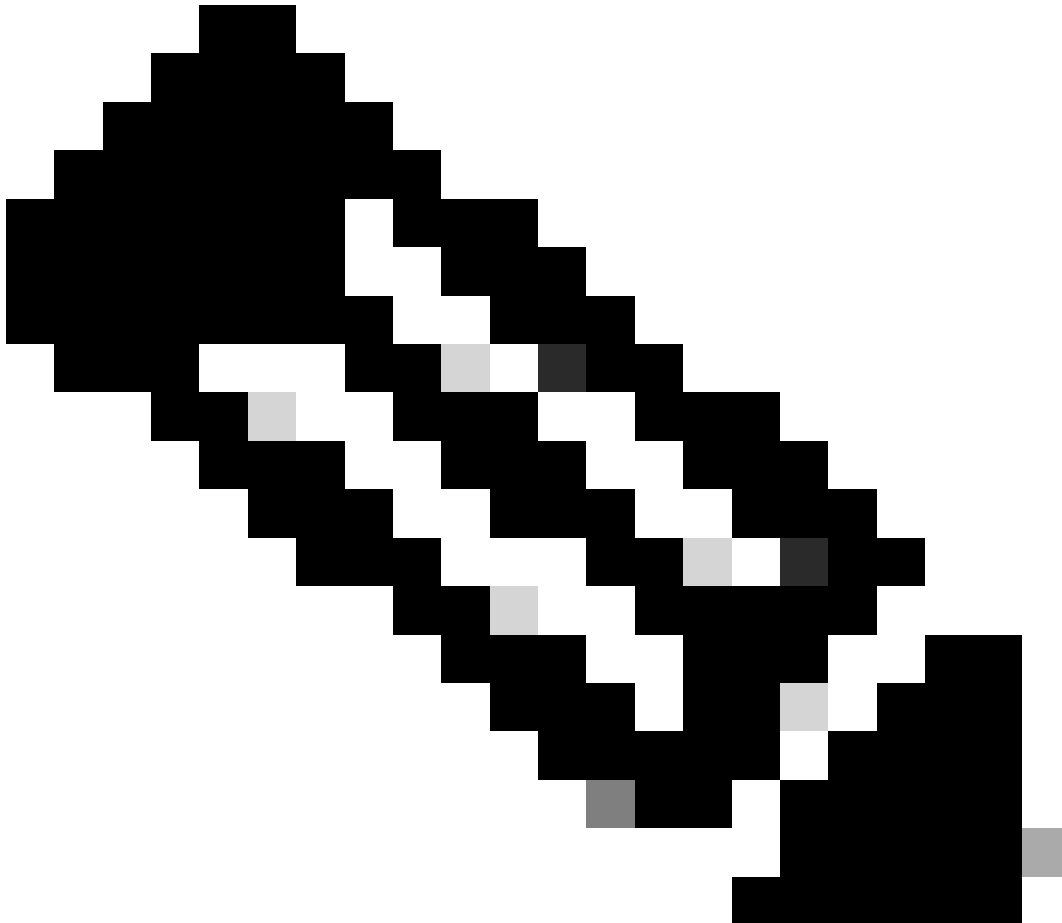
您可以從WLC或AP上行鏈路交換機埠獲取EPC捕獲，以驗證AP用於形成CAPWAP隧道的證書。從PCAP驗證是否成功構建DTLS隧道。

```
▼ Datagram Transport Layer Security
  ▼ DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
    Content Type: Handshake (22)
    Version: DTLS 1.2 (0xfefd)
    Epoch: 0
    Sequence Number: 5
    Length: 82
  ▼ Handshake Protocol: Certificate (Reassembled)
    Handshake Type: Certificate (11)
    Length: 1627
    Message Sequence: 2
    Fragment Offset: 1557
    Fragment Length: 70
    Certificates Length: 1624
  ▼ Certificates (1624 bytes)
    Certificate Length: 1621
  ▼ Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d... (pkcs-9-at-emailAddress=mail@tac-lab.local,id-at-commonName=
    ▼ signedCertificate
      version: v3 (2)
      serialNumber: 0x5c000000181814edda85f9bfd100000000018
      ▼ signature (sha256WithRSAEncryption)
        Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
      ▼ issuer: rdnSequence (0)
        ▼ rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
          ▼ RDNSSequence item: 1 item (dc=com)
            ▼ RelativeDistinguishedName item (dc=com)
              Object Id: 0.9.2342.19200300.100.1.25 (dc)
              IA5String: com
          ▼ RDNSSequence item: 1 item (dc=tac-lab)
            ▼ RelativeDistinguishedName item (dc=tac-lab)
              Object Id: 0.9.2342.19200300.100.1.25 (dc)
              IA5String: tac-lab
          ▼ RDNSSequence item: 1 item (dc=sumans)
            ▼ RelativeDistinguishedName item (dc=sumans)
              Object Id: 0.9.2342.19200300.100.1.25 (dc)
              IA5String: sumans
          ▼ RDNSSequence item: 1 item (id-at-commonName=sumans-lab-ca)
            ▼ RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
              Object Id: 2.5.4.3 (id-at-commonName)
              DirectoryString: printableString (1)
                printableString: sumans-lab-ca
        ▼ validity
          ▼ notBefore: utcTime (0)
            utcTime: 2023-09-28 04:15:28 (UTC)
          ▼ notAfter: utcTime (0)
            utcTime: 2024-09-27 04:15:28 (UTC)
        ▼ subject: rdnSequence (0)
```

可以在AP和WLC上運行DTLS調試以瞭解證書問題。

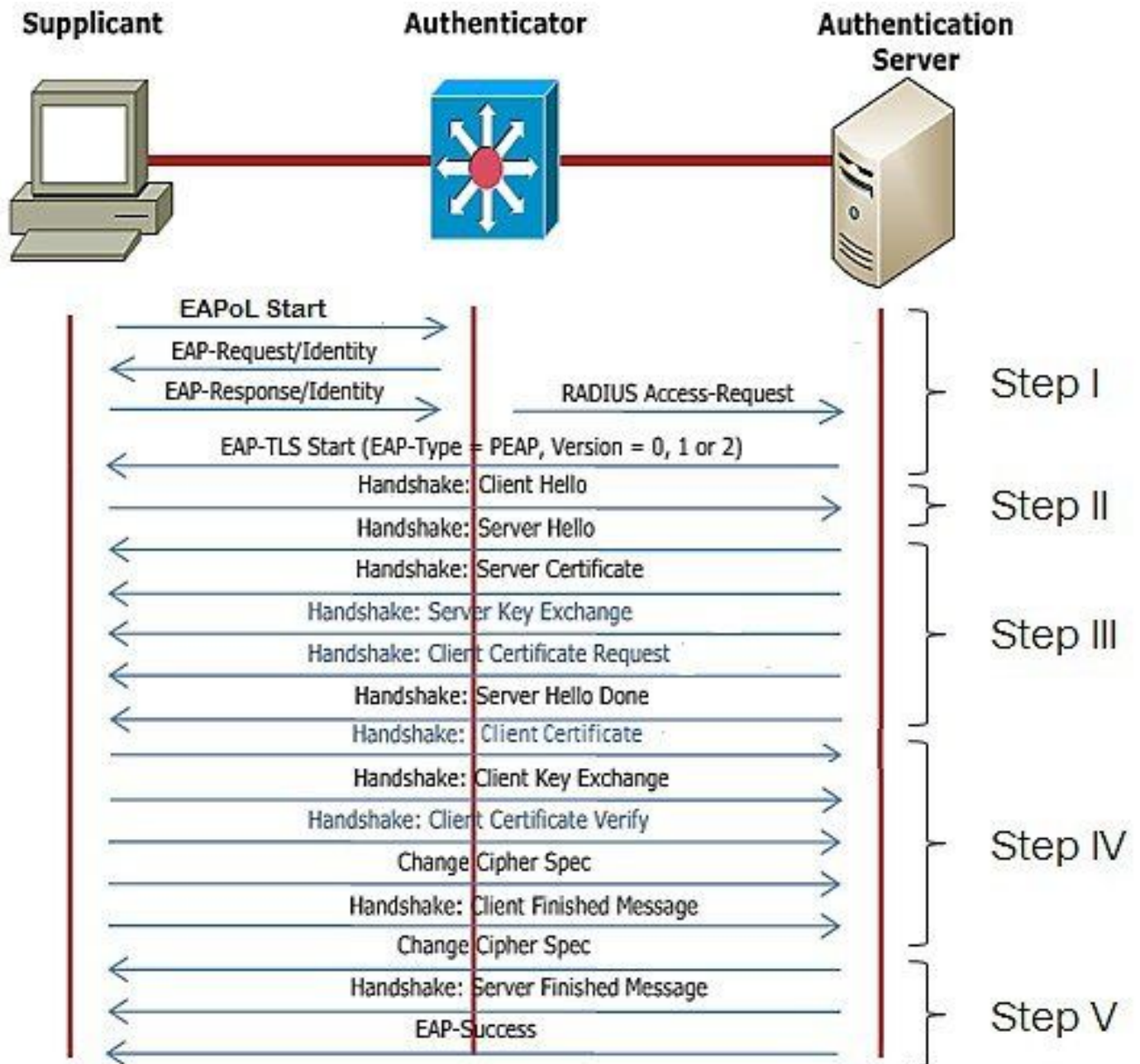
使用LSC的AP有線802.1X身份驗證

AP配置為使用相同的LSC證書進行身份驗證。AP充當802.1X請求方，並由交換機針對ISE伺服器進行身份驗證。ISE伺服器與後端的AD通訊。



註：一旦在AP上行鏈路交換機埠上啟用dot1x身份驗證，AP將無法轉發或接收任何流量，直到身份驗證通過。要恢復身份驗證失敗的AP並獲得AP訪問許可權，請禁用AP有線交換機埠上的dot1x auth。

EAP-TLS身份驗證工作流程和消息交換

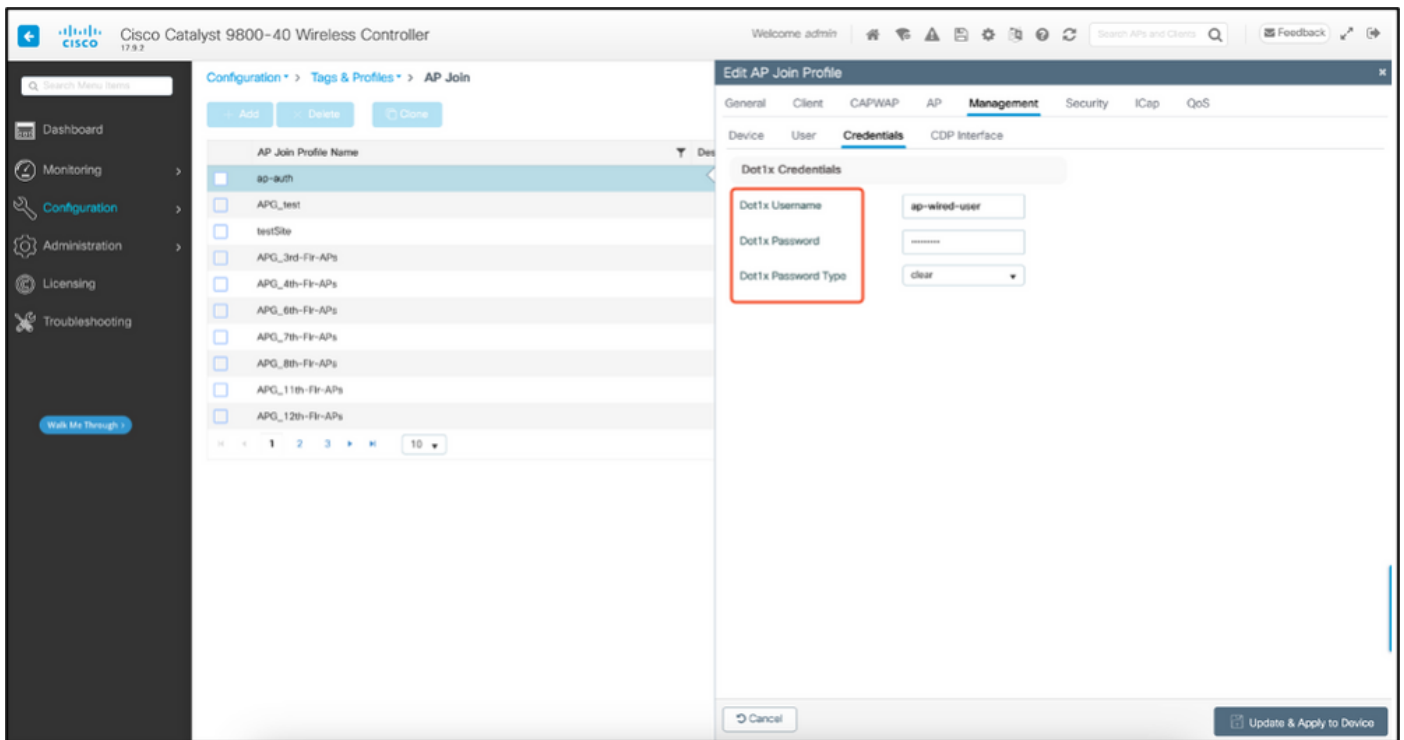
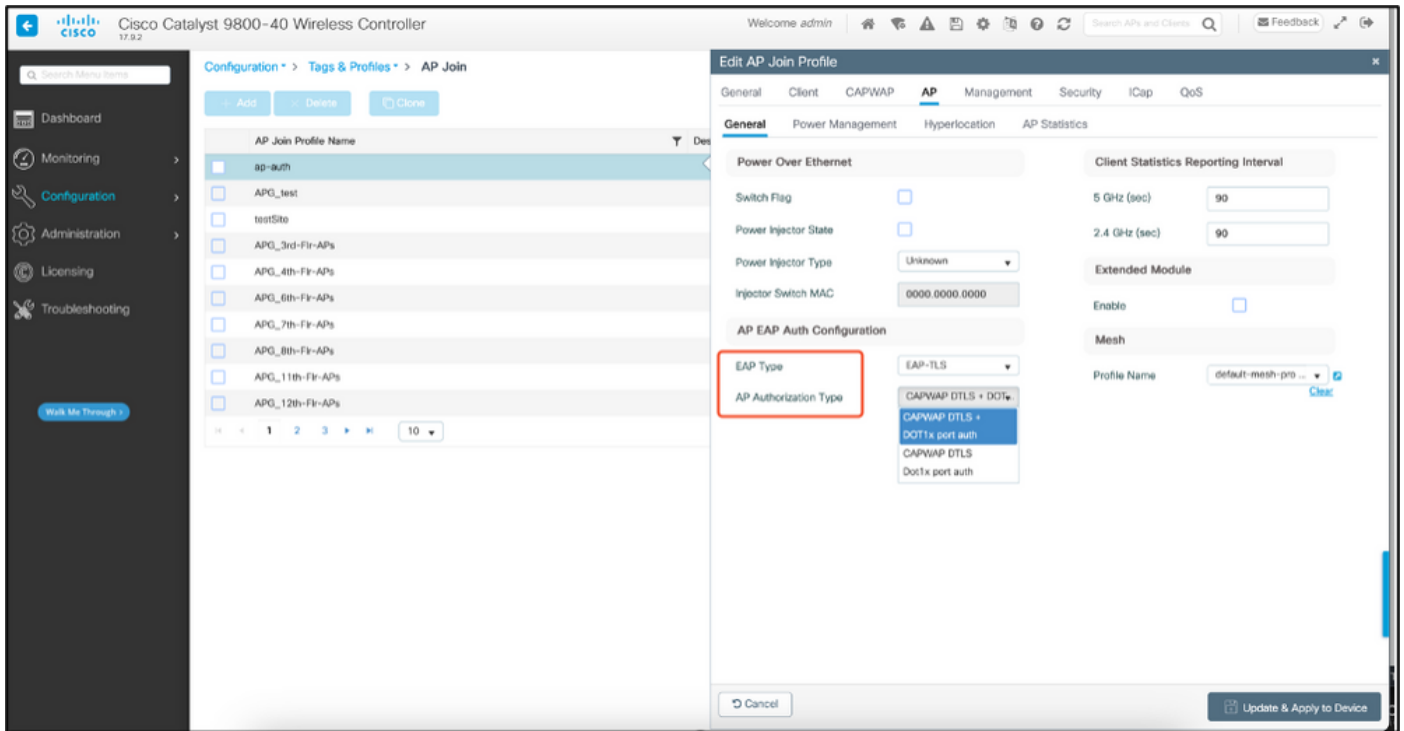


AP有線802.1x身份驗證配置步驟

1. 啟用dot1x port auth和CAPWAP DTLS，然後選擇EAP型別。
2. 為AP建立dot1x憑據。
3. 在交換機埠上啟用dot1x。
4. 在RADIUS伺服器上安裝受信任的證書。

AP有線802.1x身份驗證GUI配置

1. 導航到AP加入配置檔案，然後按一下該配置檔案。
 1. 按一下AP > General。選擇EAP型別和AP授權型別作為「CAPWAP DTLS + dot1x port auth」。
 2. 導航到Management > Credentials，然後為AP dot1x auth建立使用者名稱和密碼。



AP有線802.1x身份驗證CLI配置

使用以下命令從CLI為AP啟用dot1x。這僅對使用特定加入配置檔案的AP啟用有線身份驗證。

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

```
9808-48(config)#ap profile ap-auth
9808-48(config-ap-profile)#dot1x cap-type cap-tls
9808-48(config-ap-profile)#dot1x lsc-ap-auth-state both
9808-48(config-ap-profile)#
```

AP有線802.1x身份驗證交換機配置

本實驗使用交換機配置來啟用AP有線身份驗證。您可以根據設計採用不同的配置。

```
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伺服器憑證安裝

驗證發生在AP (充當請求方) 和RADIUS伺服器之間。兩者必須信任彼此的證書。使AP信任RADIUS伺服器證書的唯一方法是使RADIUS伺服器使用由也頒發AP證書的SCEP CA頒發的證書。

在ISE中，轉至管理>證書>生成證書簽名請求

生成CSR並使用ISE節點的資訊填充欄位。

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
<input checked="" type="checkbox"/> ISE99	ISE99#EAP Authentication

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

生成後，可以匯出它並將其複製貼上為文本。

導航到您的Windows CA IP地址並將/certsrv/新增到URL

按一下「Request a certificate」

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

Microsoft Active Directory Certificate Services – mydomain-WIN-3E202T1QD0U-CA

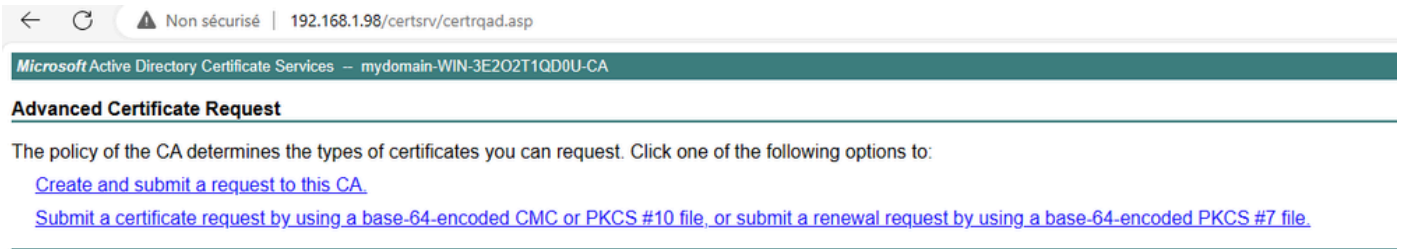
Welcome

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](#).

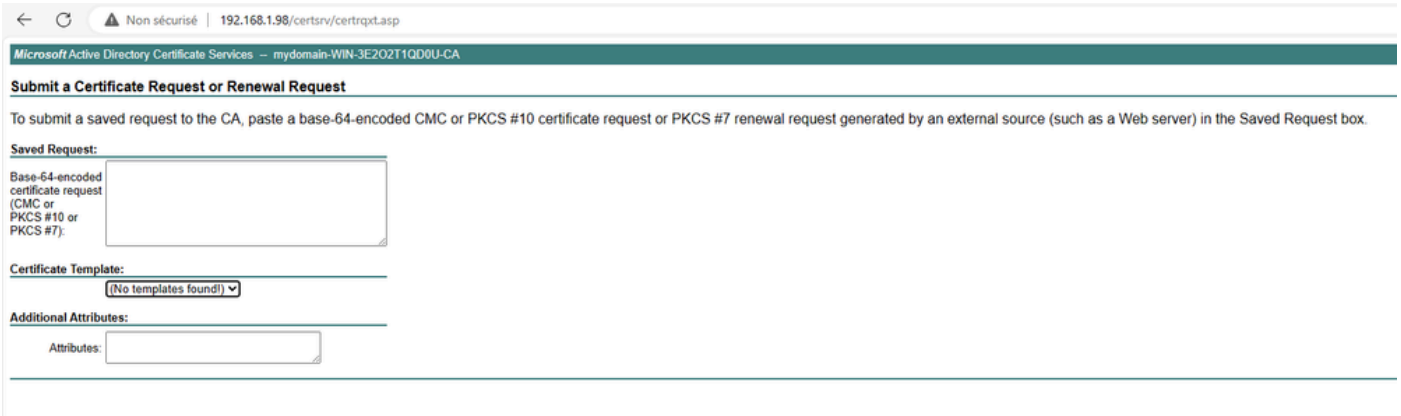
Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

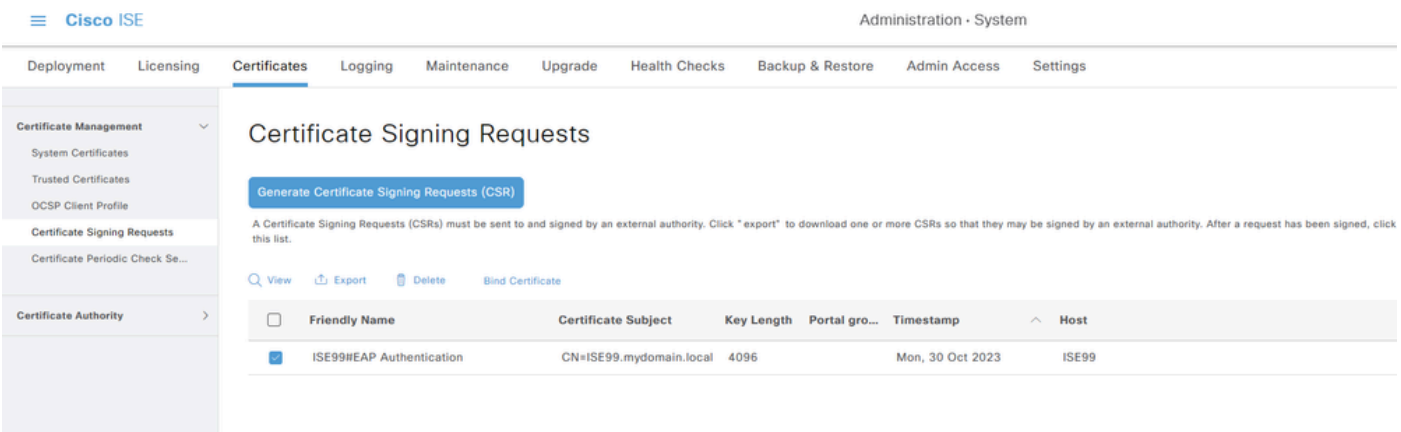
按一下Submit a certificate request by using a base-64



在文本框中貼上CSR文本。選擇Web伺服器證書模板。



然後，通過返回到Certificate Signing Request選單並按一下Bind certificate，可以在ISE上安裝此證書。然後，您可以上傳從Windows C獲得的證書。



AP有線802.1x驗證驗證

通過控制檯訪問AP並運行命令：

```
#show ap authentication status
```

未啟用AP身份驗證：

```
AP0C0B.F89A.46E8#sho ap authentication status
AP dot1x feature is disabled.
AP0C0B.F89A.46E8#
```

啟用ap auth後從AP記錄控制檯日誌：

```
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已成功通過身份驗證：

```
AP0CD0.F89A.46E0#sho ap authentication status
ap_name=IEEE_802.1X (no WPA)
ap_state=COMPLETED
address=c108:f89a:46e0
supplicant_PAE_state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
wap_tls_version=TLSv1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
wap_session_id=8d7b91a744885a6e8e460d49fee7d2d5604ea2bdd11f40494a4325c98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aaf5f17decf336ad1e88121
AP0CD0.F89A.46E0#
```

WLC驗證：

```
9800-48#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
```

成功身份驗證後的交換機埠介面狀態：

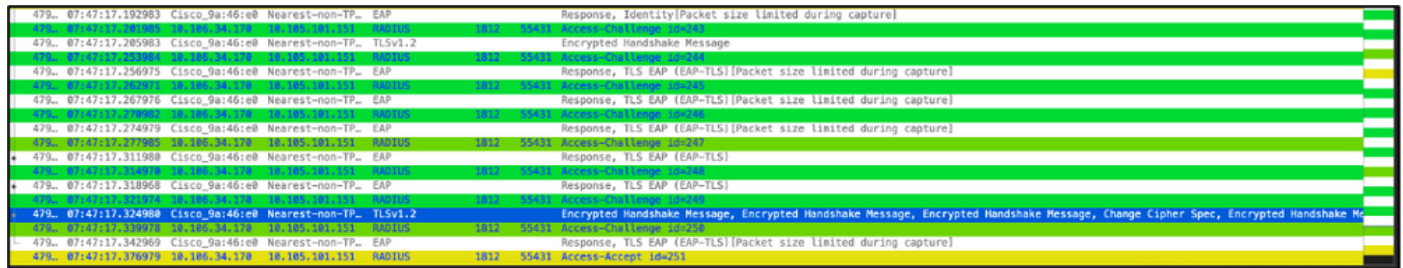
```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
-----
G11/0/2 ecd0.f89a.46e0 dot1x DATA Auth 9765690A000005CCEED8FBF
```

以下是指示身份驗證成功的AP控制檯日誌示例：

```
[*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
```

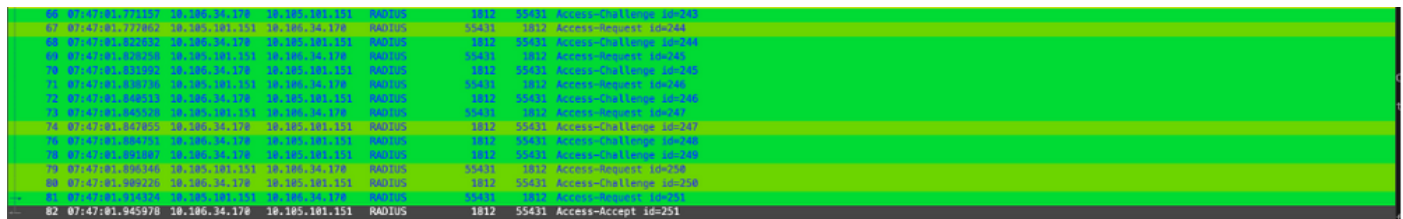
802.1X身份驗證故障排除

在AP上行鏈路上執行PCAP並驗證radius身份驗證。以下是成功驗證的片段。



479.	07:47:17.192983	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, Identity(Packet size limited during capture)
479.	07:47:17.205983	Cisco_9a:46:e0	Nearrest-non-TP...	TLVv1.2	Encrypted Handshake Message
479.	07:47:17.256975	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.267976	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.274979	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.274979	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.311980	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.318968	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.324980	Cisco_9a:46:e0	Nearrest-non-TP...	TLVv1.2	Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
479.	07:47:17.342969	Cisco_9a:46:e0	Nearrest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.376978	10.186.34.178	10.185.101.151	RADIUS	Access-Accept id=251

TCPdump收集來自ISE的身份驗證。



80	07:47:18.113003	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge id=251
82	07:47:18.123002	10.186.34.178	10.185.101.151	RADIUS	Access-Request id=244
88	07:47:18.133002	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge id=244
89	07:47:18.143000	10.186.34.178	10.185.101.151	RADIUS	Access-Request id=240
90	07:47:18.153002	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge id=240
91	07:47:18.163000	10.186.34.178	10.185.101.151	RADIUS	Access-Request id=240
92	07:47:18.173002	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge id=240
93	07:47:18.183000	10.186.34.178	10.185.101.151	RADIUS	Access-Request id=240
94	07:47:18.193002	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge id=240
95	07:47:18.203000	10.186.34.178	10.185.101.151	RADIUS	Access-Request id=240
96	07:47:18.213002	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge id=240
97	07:47:18.223000	10.186.34.178	10.185.101.151	RADIUS	Access-Request id=240
82	07:47:18.945978	10.186.34.178	10.185.101.151	RADIUS	Access-Accept id=251

如果在身份驗證期間發現問題，則需要從AP有線上行鏈路和ISE端同時捕獲資料包。

AP的Debug命令：

```
#debug ap authentication packet
```

相關資訊

- [思科技術支援與下載](#)
- [使用AireOS在AP上配置802.1X](#)
- [適用於LSC的9800組態設定指南](#)
- [9800的LSC配置示例](#)
- [為9800上的AP配置802.1X](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。