為9800 WLC上的本地重要證書調配配置SCEP

目錄

簡介

本檔案介紹如何透過Windows Server 2012 R2 Standard中的Microsoft網路裝置註冊服務(NDES)和簡易憑證註冊通訊協定(SCEP)功能，為存取點(AP)加入的本地重要憑證(LSC)註冊設定9800無線LAN控制器(WLC)。

必要條件

若要成功在Windows Server上執行SCEP，9800 WLC必須滿足以下要求：

- 控制器和伺服器之間必須存在可達性。
- 控制器和伺服器同步到同一個NTP伺服器，或者共用相同的日期和時區（如果CA伺服器與來自AP的時間的時間不同，則AP存在證書驗證和安裝問題）。

Windows Server必須先前已啟用Internet資訊服務(IIS)。

需求

思科建議您瞭解以下技術：

- 9800無線LAN控制器版本16.10.1或更高版本。

- Microsoft Windows Server 2012標準版。
- 私鑰基礎架構(PKI)和憑證。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800-L WLC軟體版本17.2.1。
- Windows Server 2012 Standard R2。
- 3802無線接入點。

> **附註**：本檔案中的伺服器端組態特定為WLC SCEP，如需其他強化、安全和憑證伺服器組態，請參閱Microsoft TechNet。

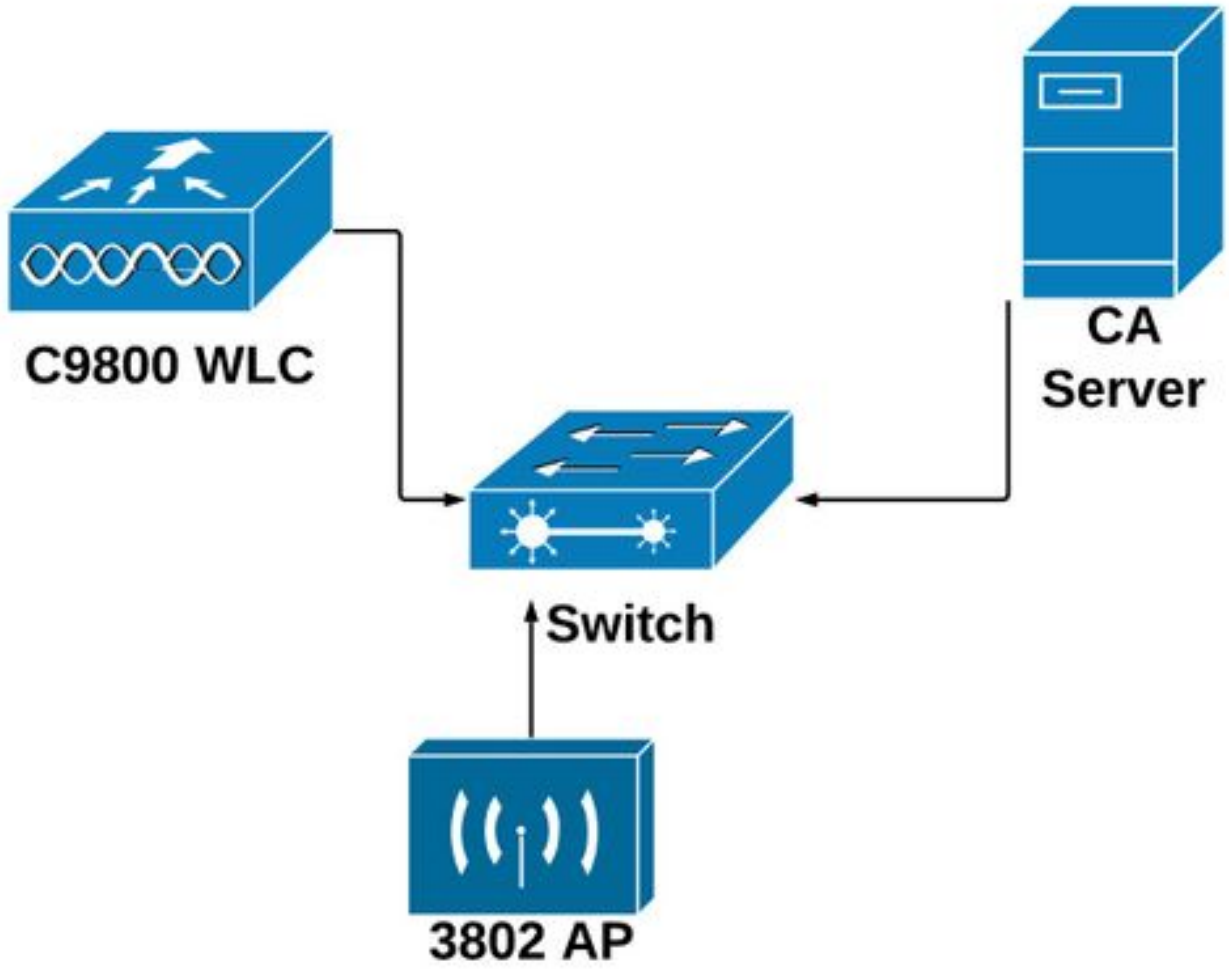
背景資訊

必須在控制器上安裝新的LSC證書(包括證書頒發機構(CA)根證書和裝置證書)，以便最終將其下載到AP中。透過SCEP，系統會從CA伺服器接收CA和裝置憑證，稍後會自動將其安裝到控制器中。

為AP調配LSC時，會出現相同的認證過程；為此，控制器充當CA代理，並幫助取得CA為AP簽署的憑證請求（自生）。

設定

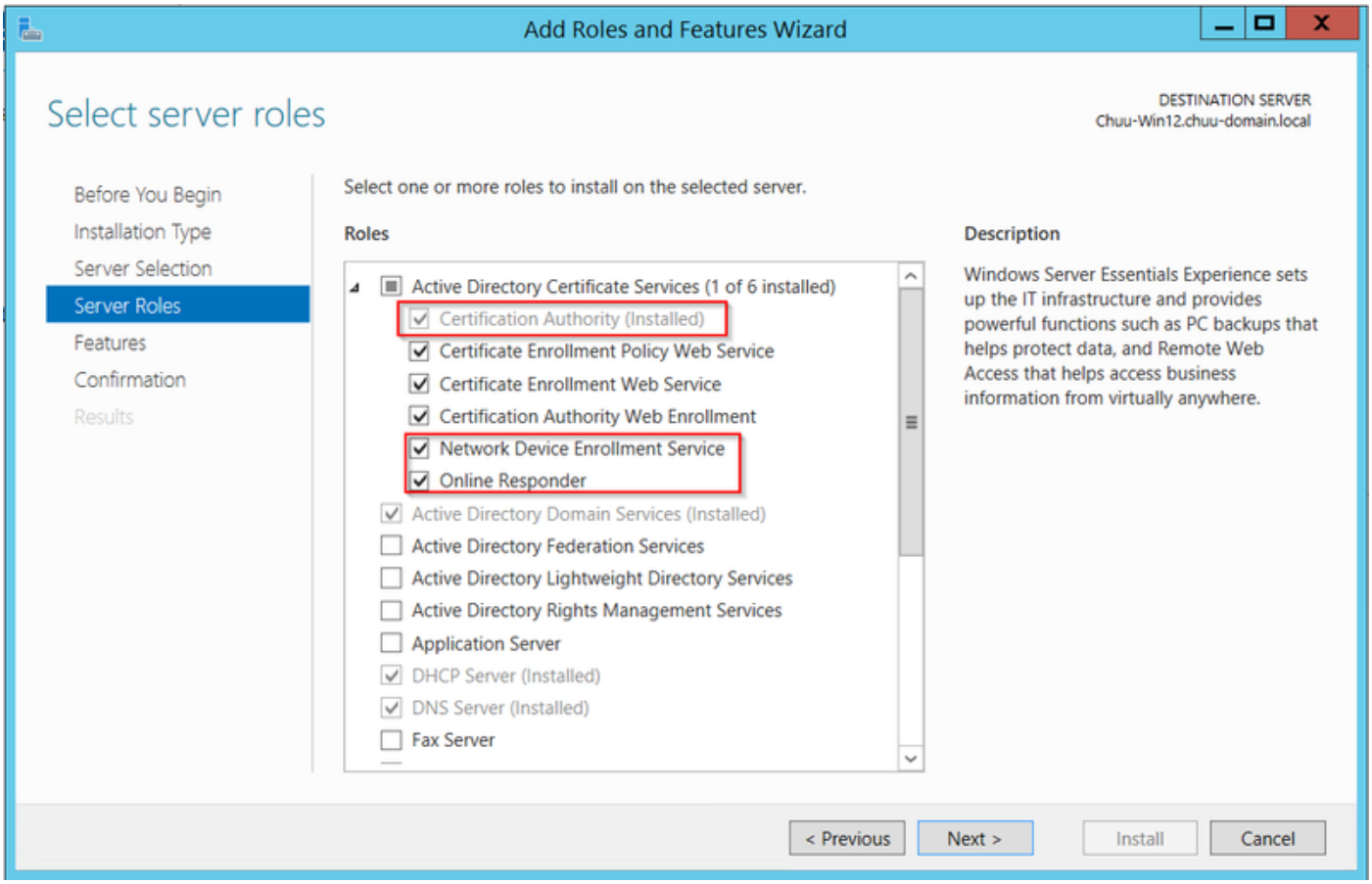
網路圖表



在Windows伺服器中啟用SCEP服務

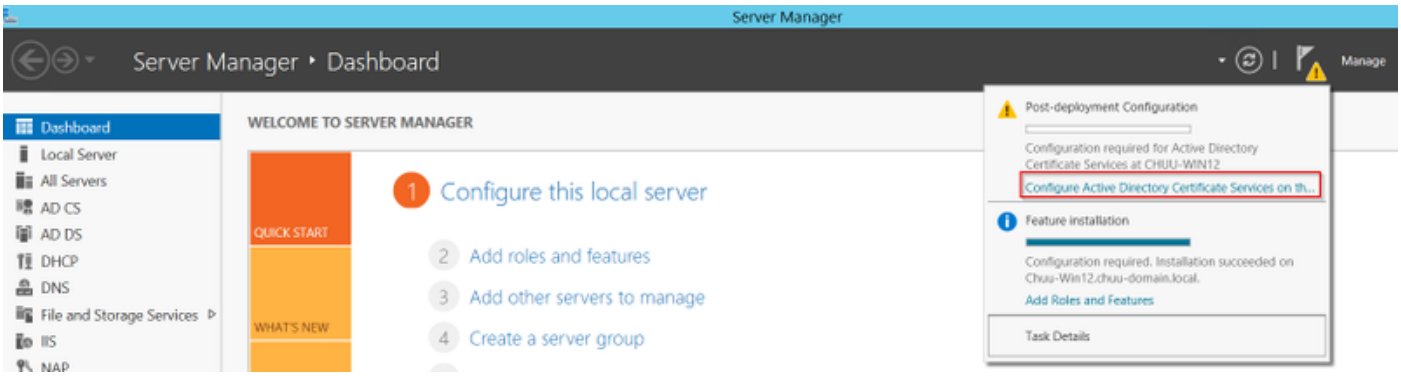
步驟1.在Server Manager**應用程**序中，選擇**Manage 選單，然後選擇**Add Roles and Features**選項以開啟角色**Add Roles and Features Configuration Wizard。從中選擇用於SCEP伺服器註冊的伺服器例項。

步驟2.驗證是否已選擇**Certification Authority、Network Device Enrollment Service和Online Responder功能，然後選擇**Next:



步驟3.選擇**Next**兩次，然後選擇**Finish**結束配置嚮導。**等待伺服器完成功能安裝過程，然後選擇關閉**關閉嚮導。

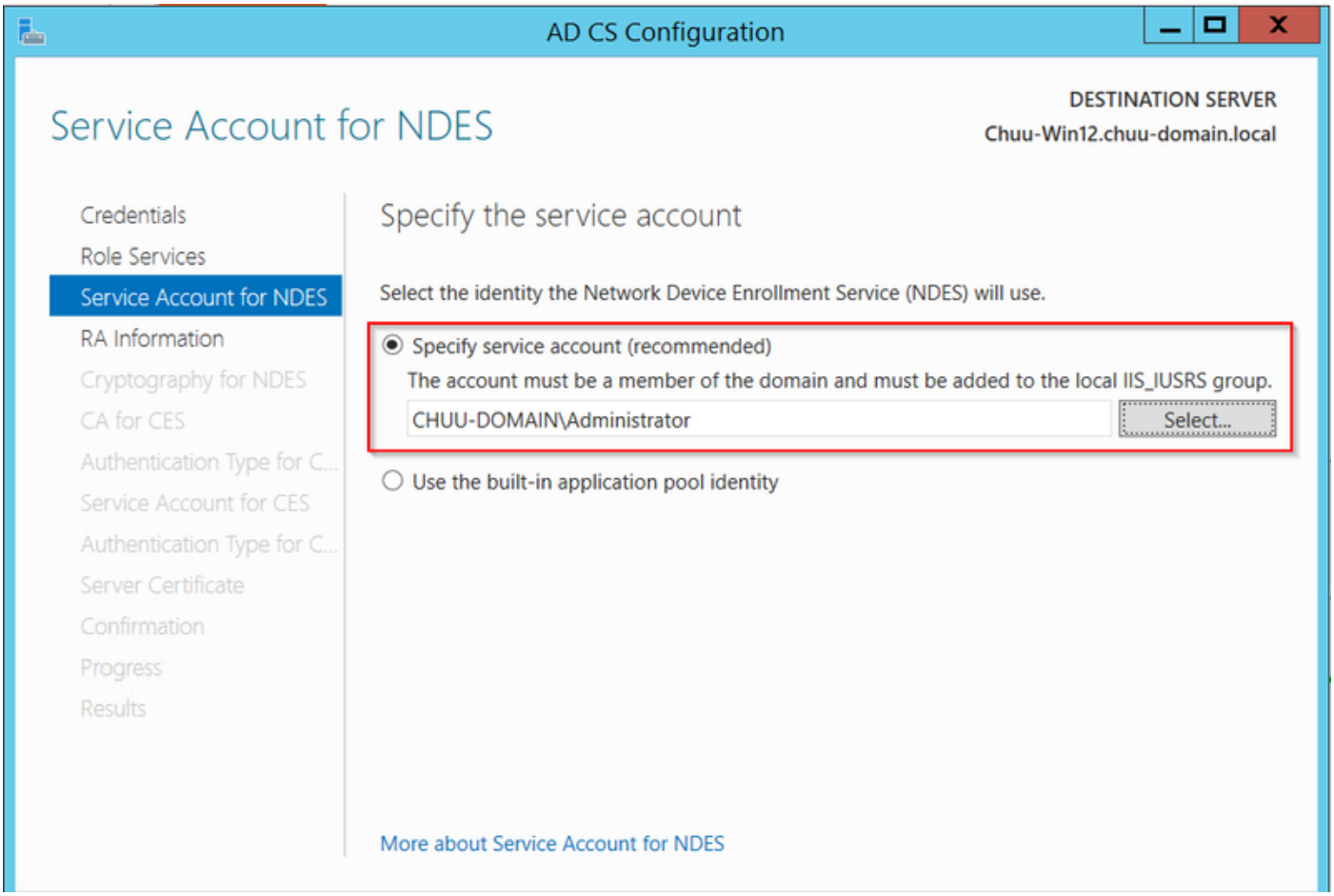
步驟4.安裝完成後，伺服器管理器通知圖示中將顯示一個警告圖示。選擇該選項並選擇**在目標伺服器上配置Active Directory服務**選項鍊接以啟動**AD CS配置**嚮導選單。



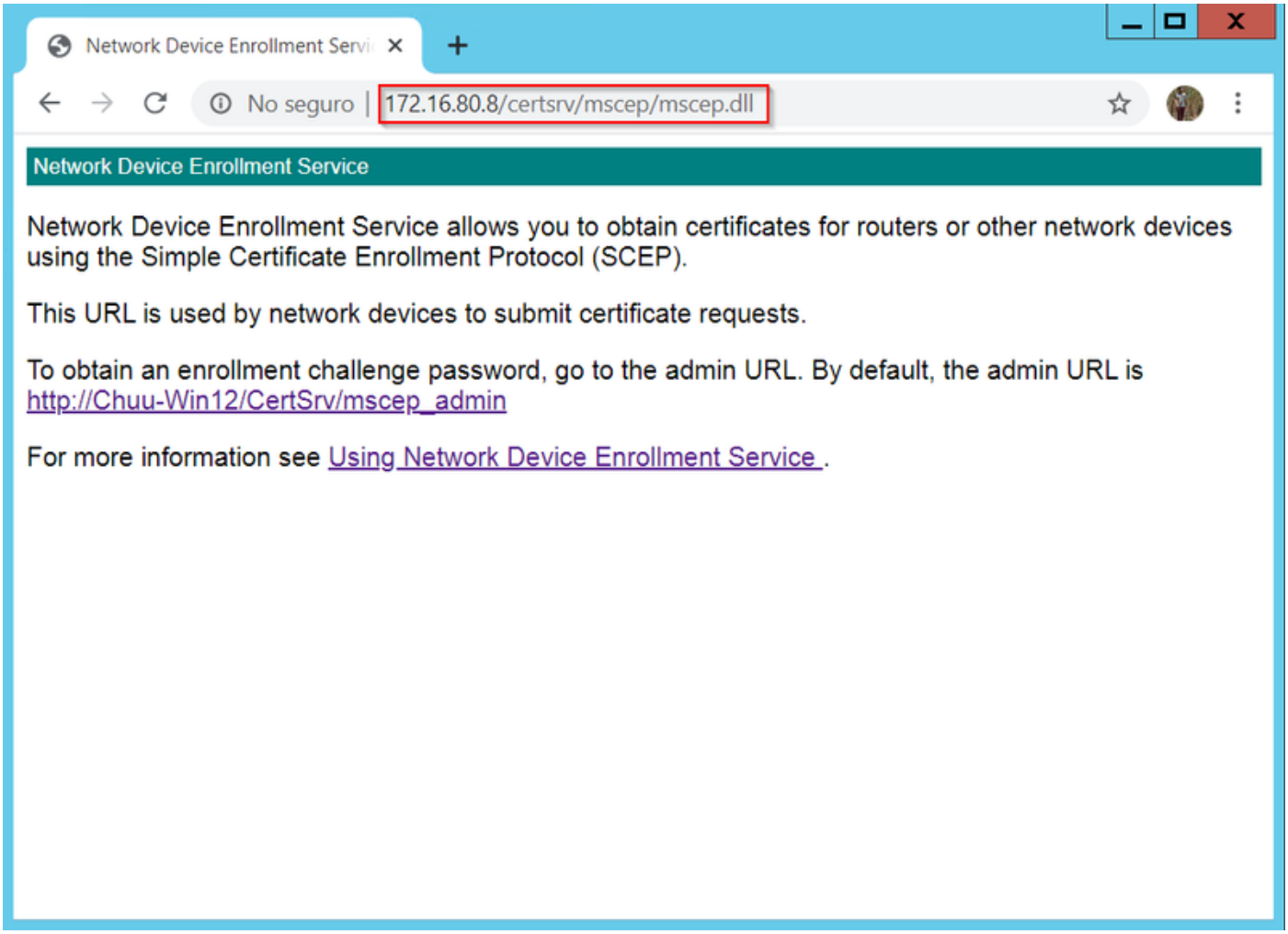
步驟5.選擇要在選單中配置的**網路裝置註冊服務**和**Online Responder**角色服務，然後選擇**下一步**。

步驟6.在NDES的**服務帳戶中**，選擇內建應用程式池或服務帳戶之間的任一選項，然後選擇**下一步**。

附註：如果服務帳戶，請確保該帳戶是**IIS_IUSRS組的**一部分。



步驟7.選擇**Next**進入下一螢幕，完成安裝過程。安裝完成後，任何Web瀏覽器都提供SCEP url。導航到URL **http://<server ip>/certsrv/mscep/mscep.dll**，確認服務是否可用。



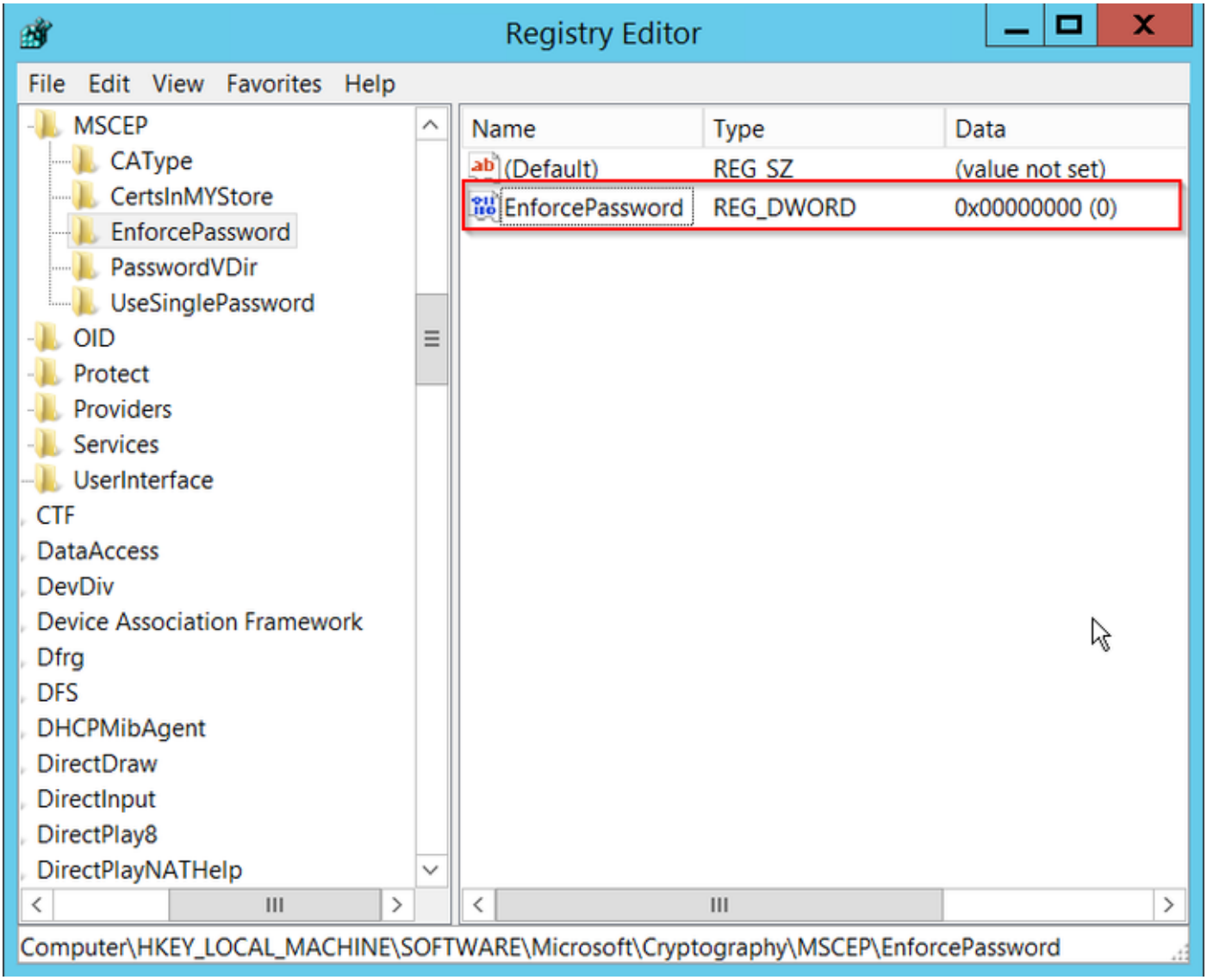
禁用SCEP註冊質詢密碼要求

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：

步驟1.開啟登錄檔編輯器，在「開始」菜**單中**搜尋「**Regedit**」。

步驟2.導航到**Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword**

步驟3.將**EnforcePassword值更**改為0。如果該值已經為0，則保留原樣。



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：

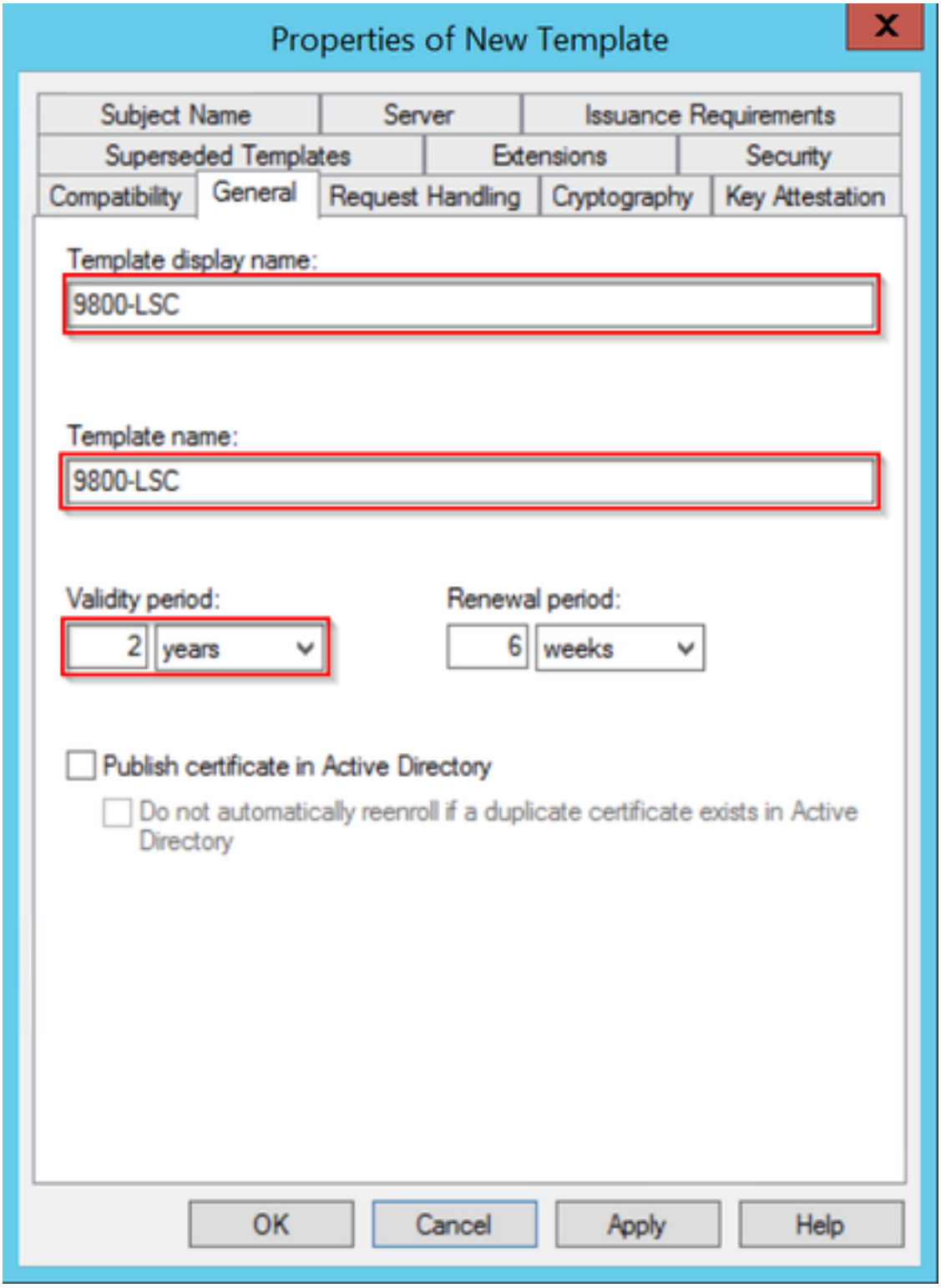
步驟1.導航到**開始>管理工具>證書頒發機構**。

步驟2.展開CA Server資料夾樹，按一下右鍵「證書模板」文**件夾，**然後選擇「**管理**」。

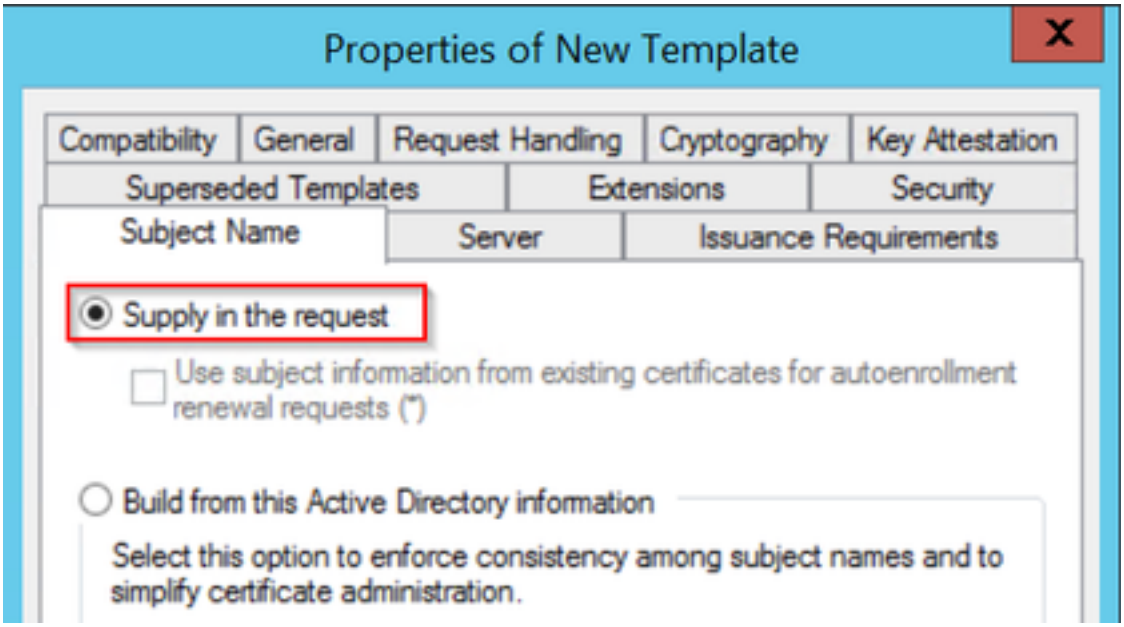
步驟3.按一下右鍵**Users certificate**模板，然後在上下文**選單中**選擇Duplicate Template。

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。

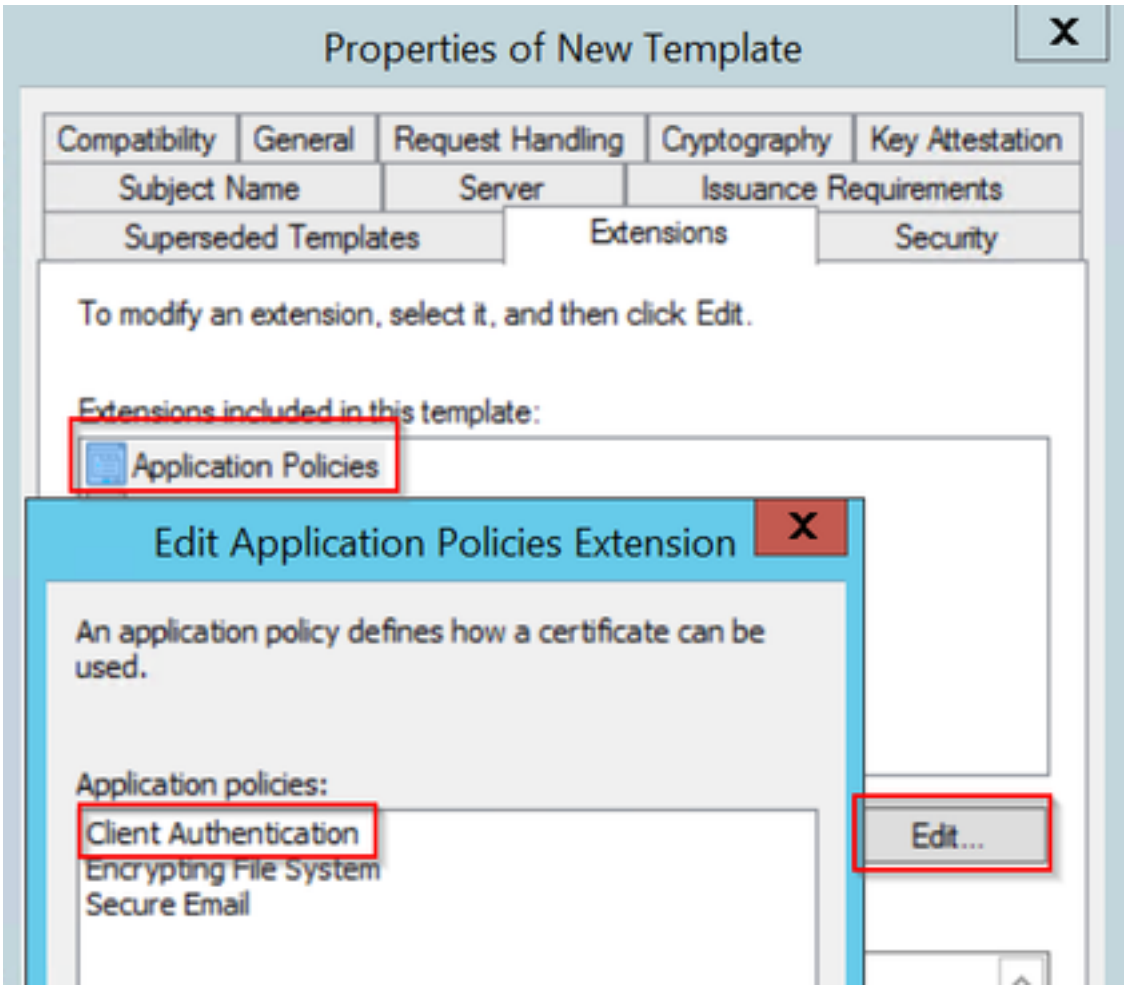
注意：修改有效期時，請確保有效期不超過證書頒發機構的根證書有效性。



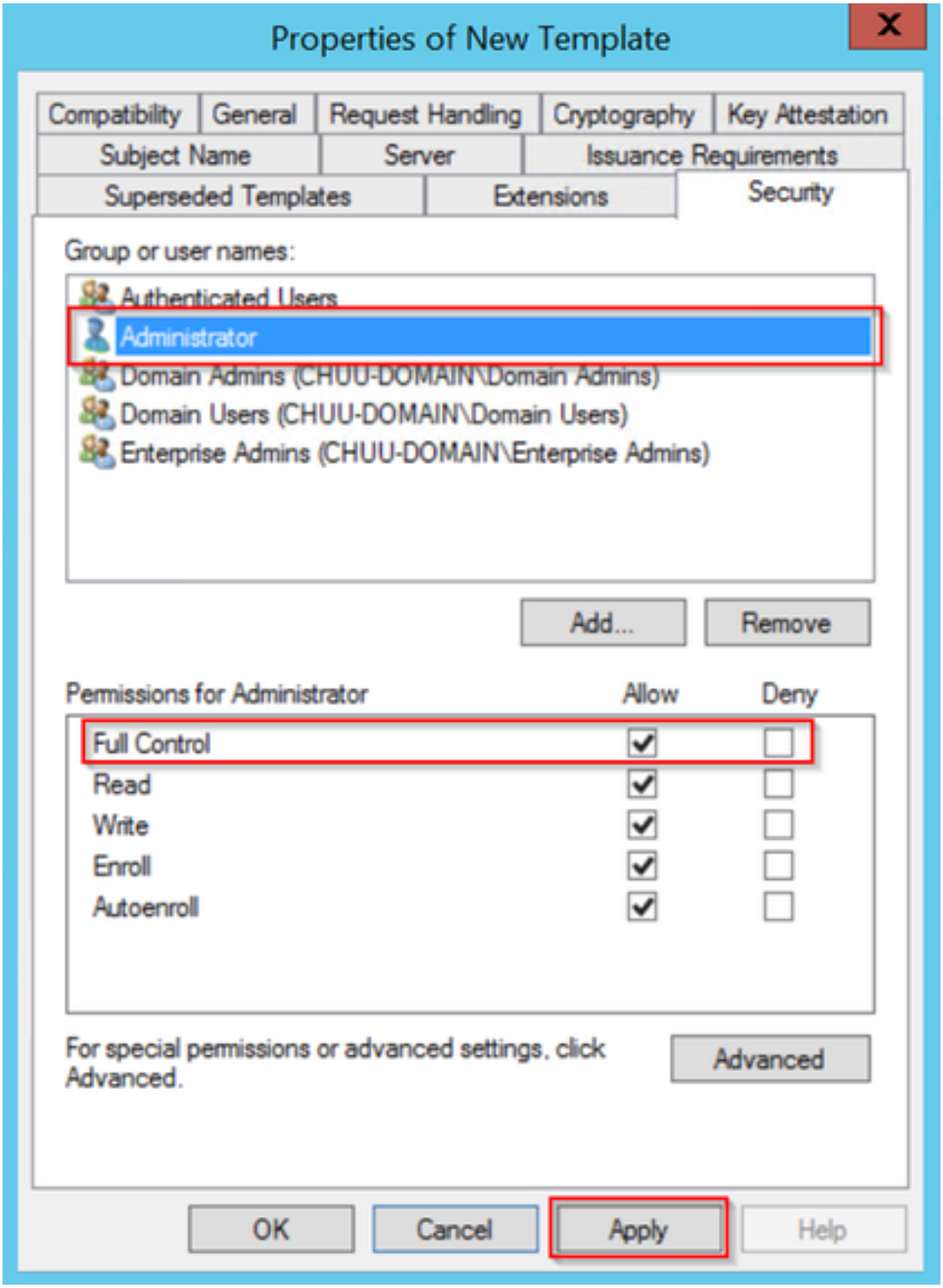
步驟5.定位至「主題**名稱**」標籤，確保已選**擇請求中的**「供應」。系統將顯示一個彈出視窗，指示使用者不需要管理員批准即可簽署其證書，請選擇**OK**。



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，請選擇**Add**並新增它。



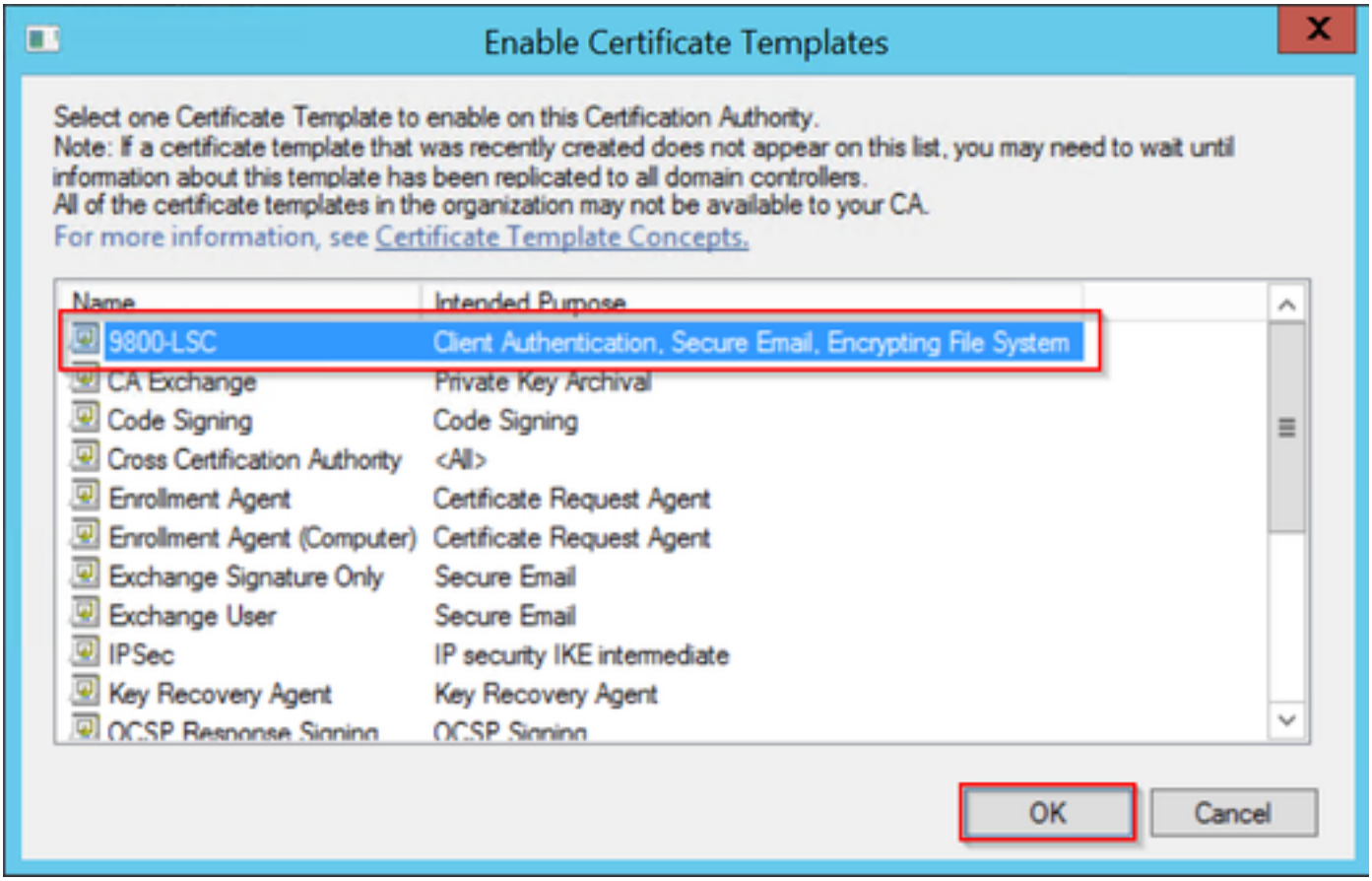
步驟7.導航到**Security**頁籤，確保在**Windows Server**中啟用**SCEP**服務的步驟6中定義的服務帳戶具有模板的完全控制許可權，然後選擇**Apply**和**OK**。



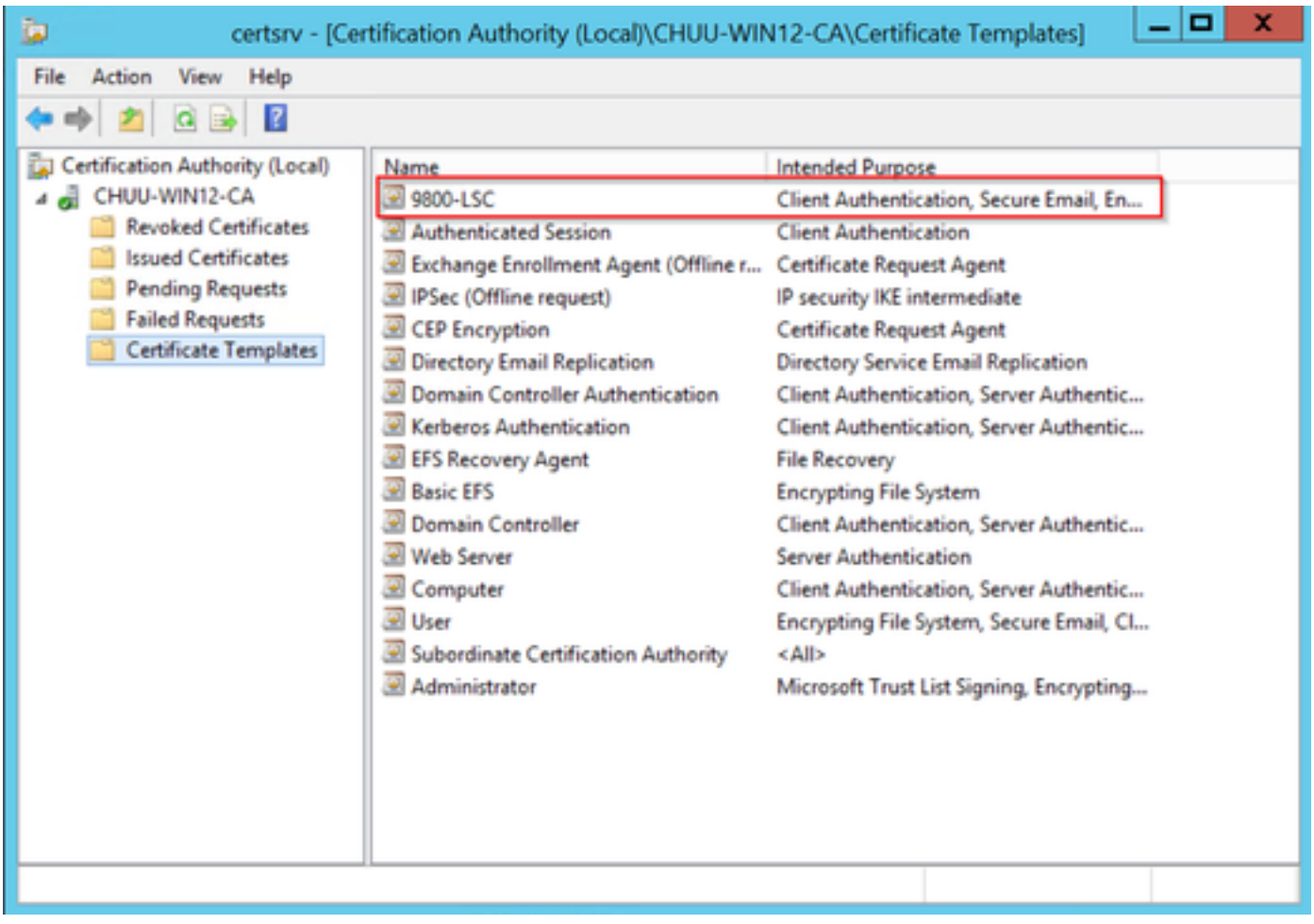
步驟8.返回Certification Authority視窗，在Certificate Templates資料夾中按一下右鍵，然後選擇New > Certificate Template to Issue。

步驟9.選擇先前建立的證書模板（在此示例中為9800-LSC），然後選擇**確定**。

> **附註**：新建立的證書模板可能需要較長時間才能在多個伺服器部署中列出，因為它需要跨所有伺服器複製。



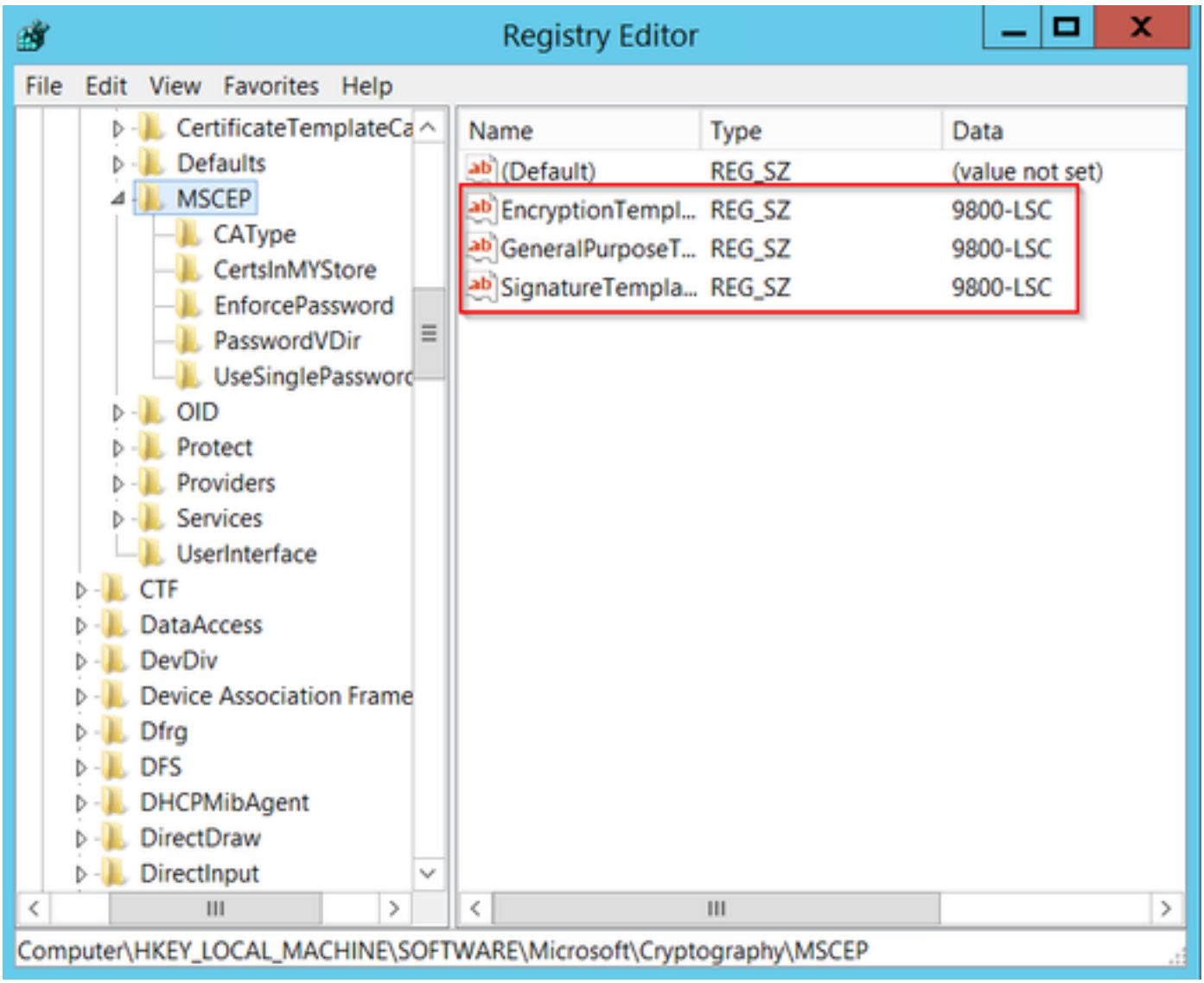
新證書模板現在列在**Certificate Templates**檔案**夾內**容中。



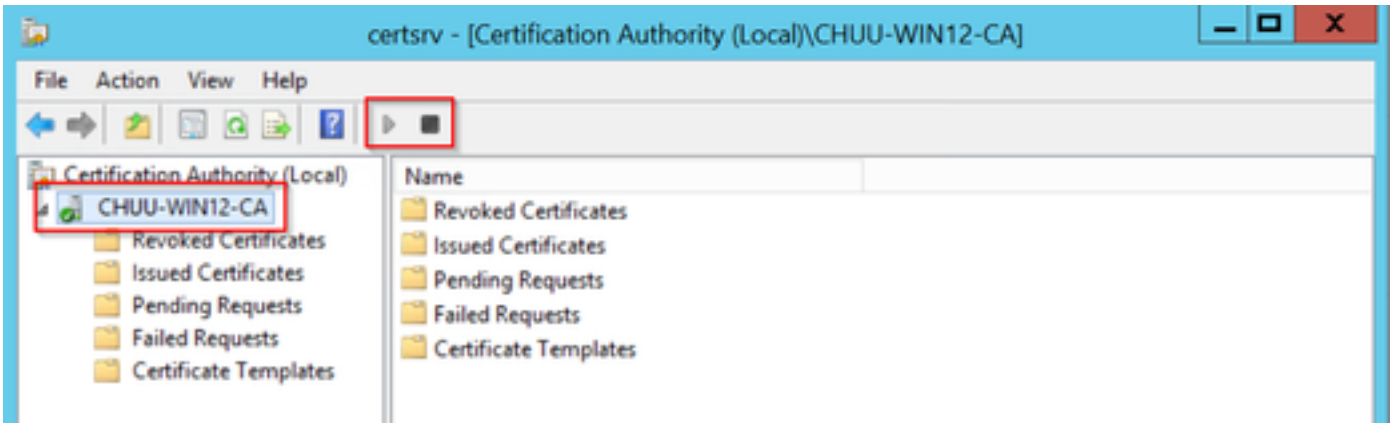
步驟10。返回**Registry Editor視窗，然後導航到Computer > HKEY_LOCAL_MACHINE >**

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。



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



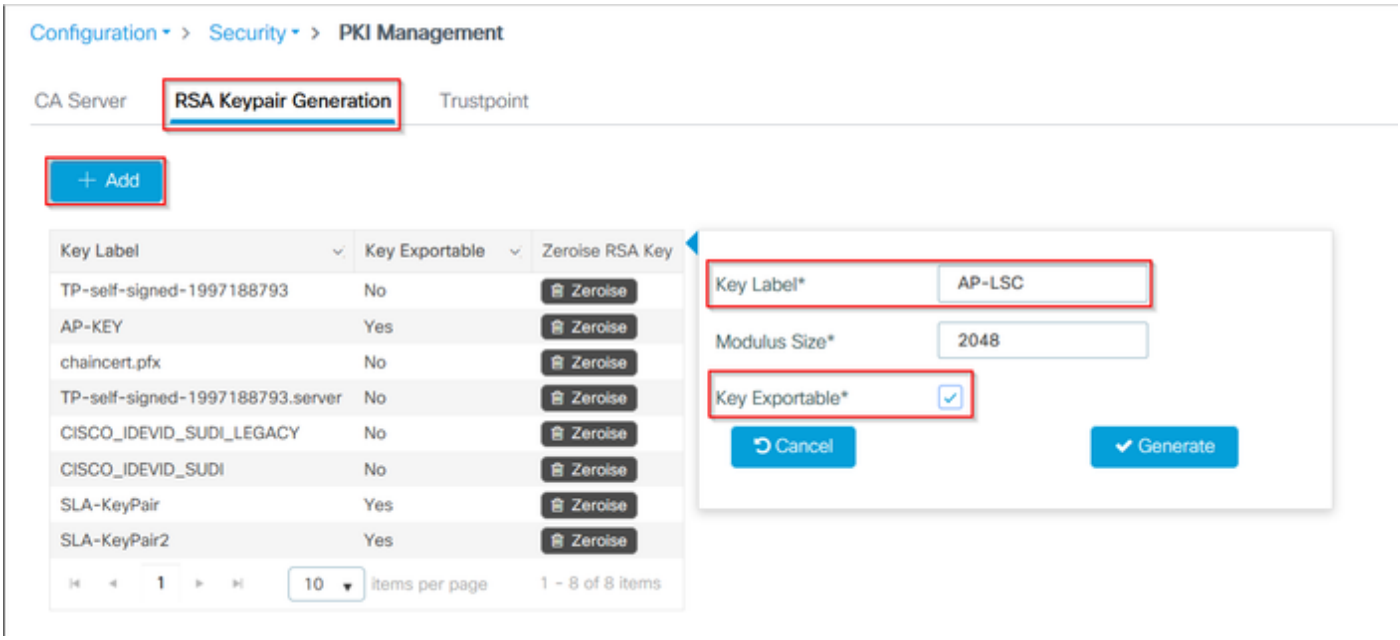
配置9800裝置信任點

控制器需要定義信任點，以便在預配AP後對其進行身份驗證。信任點包括9800裝置證書以及從同一

CA伺服器（本示例中為Microsoft CA）獲取的CA根證書。 對於要安裝在信任點中的證書，它必須包含主題屬性以及與其關聯的一對RSA金鑰。配置通過Web介面或命令列執行。

步驟1.導航到**Configuration > Security > PKI Management**，然後選擇**RSA Keypair Generation選項卡**。選擇**+ Add**按鈕。

步驟2.定義與金鑰對關聯的標籤，並確保選中「**可匯出**」覈取方塊。



第1步和第2步的CLI配置，在此配置示例中，金鑰對是使用標籤AP-LSC和模數大小2048位生成的：

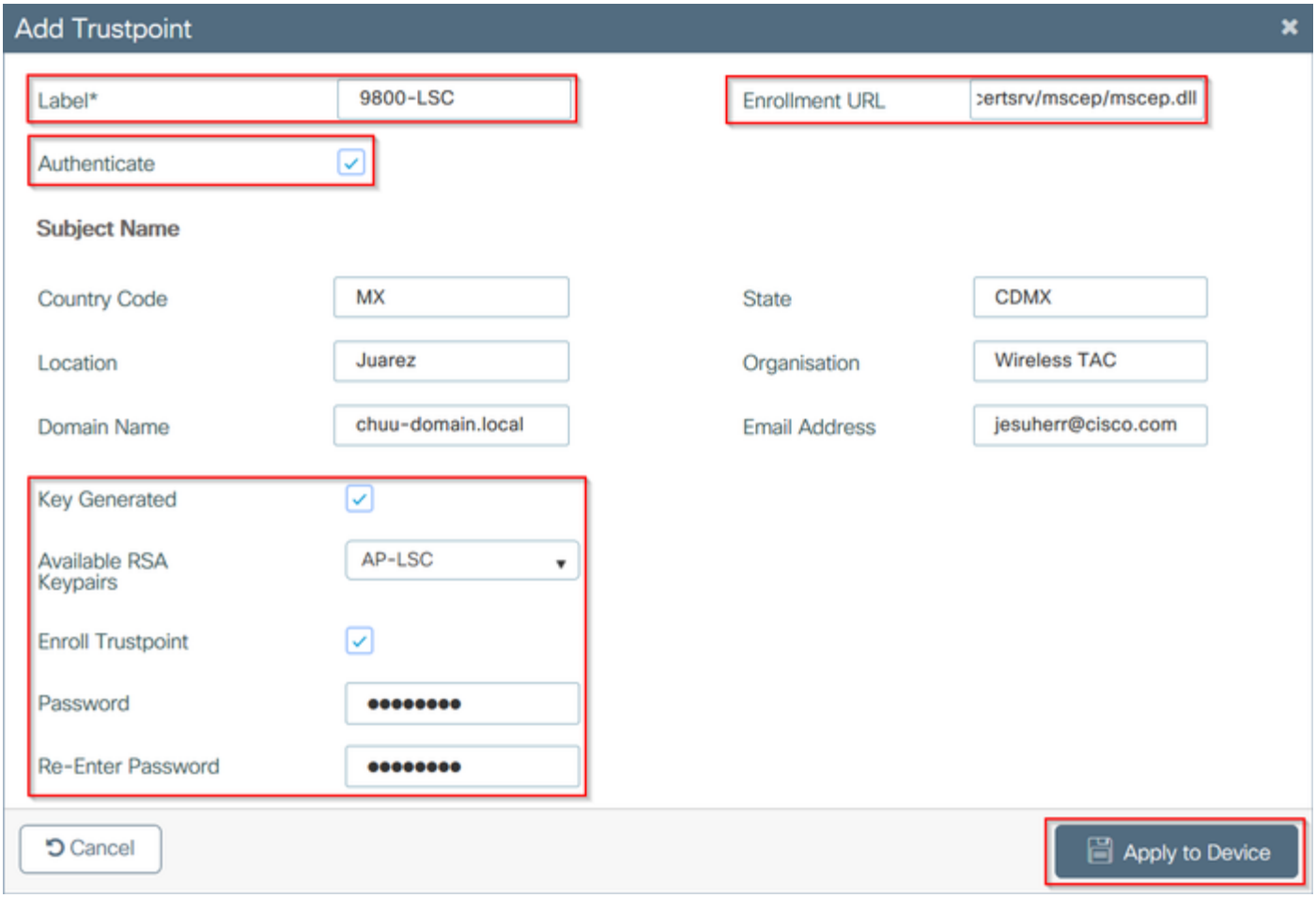
```
9800-L(config)#crypto key generate rsa exportable general-keys modulus


The name for the keys will be: AP-LSC

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
```

步驟3.在同一部分中，選擇**Trustpoint**頁籤，然後選擇**+ Add按鈕**。

步驟4.使用裝置資訊填寫信任點詳細資訊，然後選擇**應用到裝置**：

- **Label**欄位是與信任點關聯的名稱
- 對於**註冊URL**，請使用**在Windows伺服器中啟用SCEP服務**部分的第7步中定義的註冊地址
- 選中**Authenticate**覈取方塊以下載CA證書
- **Domain Name**欄位被放置為證書請求的公用名屬性
- 選中**Key Generated**覈取方塊，即會顯示下拉選單，選擇步驟2中生成的金鑰對
- 選中**Enroll Trustpoint**覈取方塊，將顯示兩個密碼欄位；鍵入密碼。這用於鏈結憑證金鑰與裝置憑證和CA憑證

  警告：9800控制器不支援多層伺服器鏈以安裝LSC，因此根CA必須是簽署控制器和AP的證書請求的CA。



用於步驟3和步驟4的CLI配置：

注意：主題名稱配置行的格式必須採用LDAP語法，否則控制器不會接受它。

```
9800-L(config)#crypto pki trustpoint
```

```
9800-L(ca-trustpoint)#enrollment url http://
```

```
9800-L(ca-trustpoint)#subject-name C=
```

```
9800-L(ca-trustpoint)#rsakeypair
```

```
9800-L(ca-trustpoint)#revocation-check none
9800-L(ca-trustpoint)#exit
```

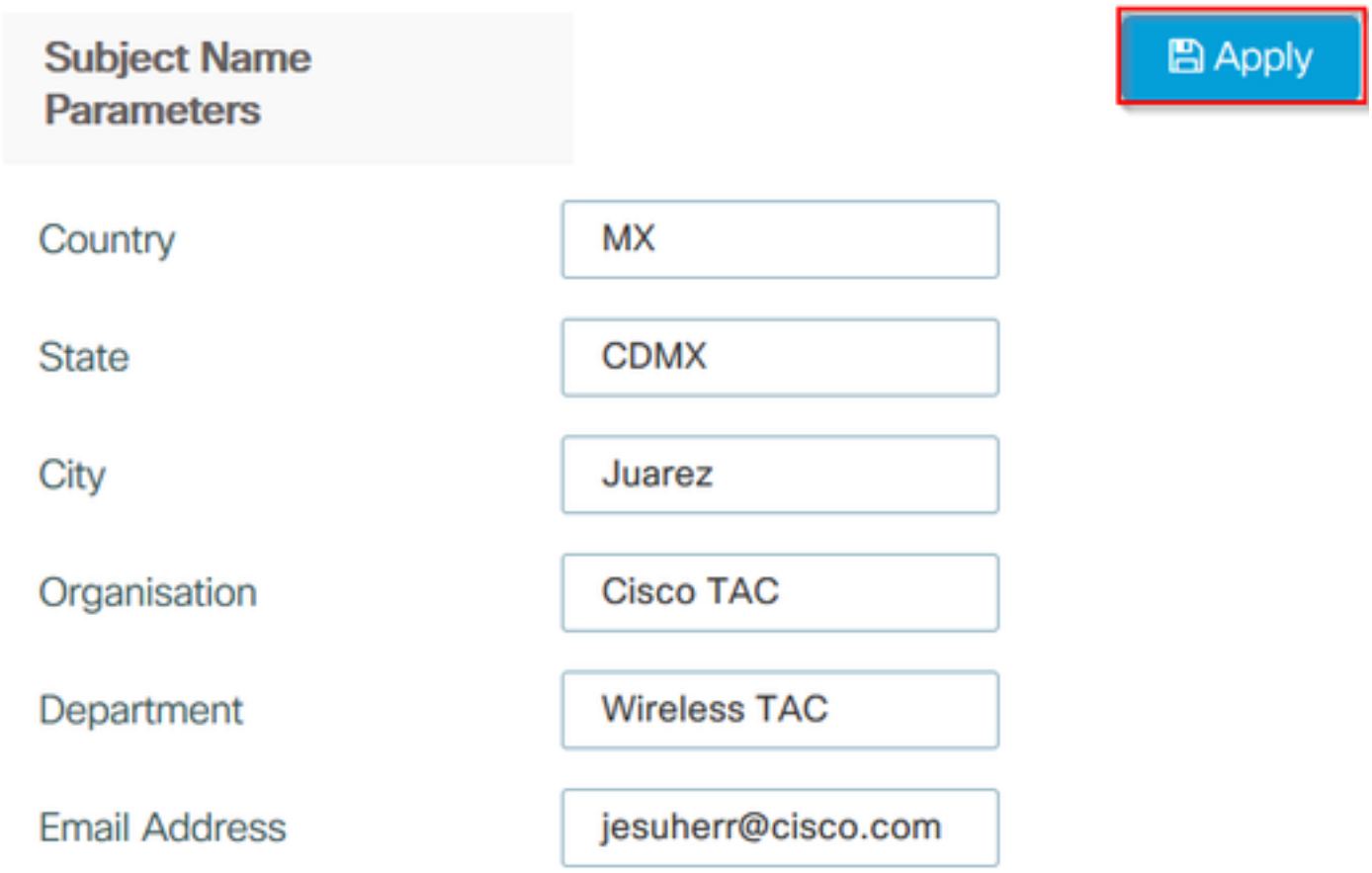
```
9800-L(config)#crypto pki authenticate



Certificate has the following attributes:
       Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
      Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-L(config)#crypto pki enroll <trustpoint name>
%
% 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:
Re-enter password:

% The subject name in the certificate will include: C=MX, ST=CDMX, L=Juarez, O=Wireless TAC,
CN=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
% The subject name in the certificate will include: 9800-L.alzavala.local
% Include the router serial number in the subject name? [yes/no]: no
% 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 AP-LSC' commandwill show the fingerprint.
```

定義AP註冊引數並更新管理信任點

AP註冊使用先前定義的信任點詳細資訊來確定控制器將證書請求轉發到的伺服器詳細資訊。由於控制器用作證書註冊的代理，因此它需要知道證書請求中包含的主題引數。配置通過Web介面或命令列執行。

步驟1.導覽至**Configuration > Wireless > Access Points，然後展開LSC Provision選單。**

步驟2.使用在AP證書請求中填寫的屬性填充**使用者名稱引數，然後選擇應用**。

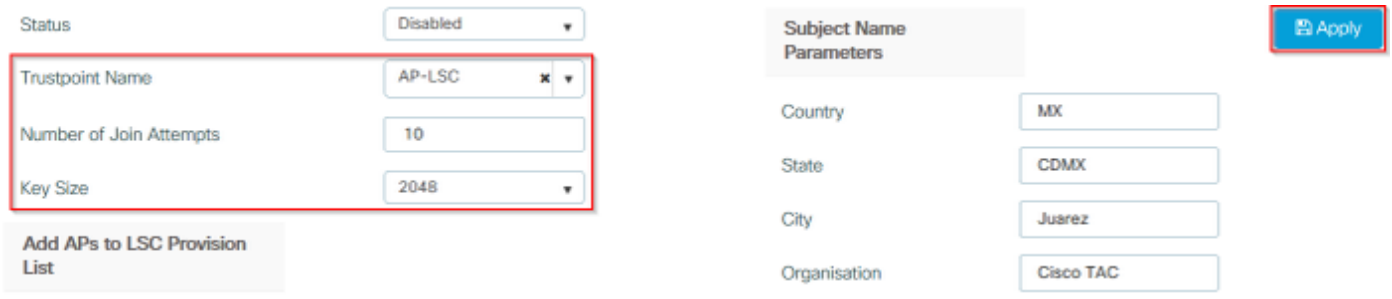


用於步驟1和步驟2的CLI配置：

```
9800-L(config)#ap lsc-provision subject-name-parameter country
```

注意：必須嚴格遵守Subject-name-parameters限制2個字元（如國家/地區代碼），因為9800 WLC不會驗證這些屬性。
如需詳細資訊，請參閱缺陷CSCvo72999 作為參考。

步驟3.在同一選單中，從下拉選單中選擇先前定義的信任點，指定AP加入嘗試次數（這定義了再次使用MIC之前的加入嘗試次數），並設定證書金鑰大小。然後，按一下「**Apply**」。



第三步的CLI配置：

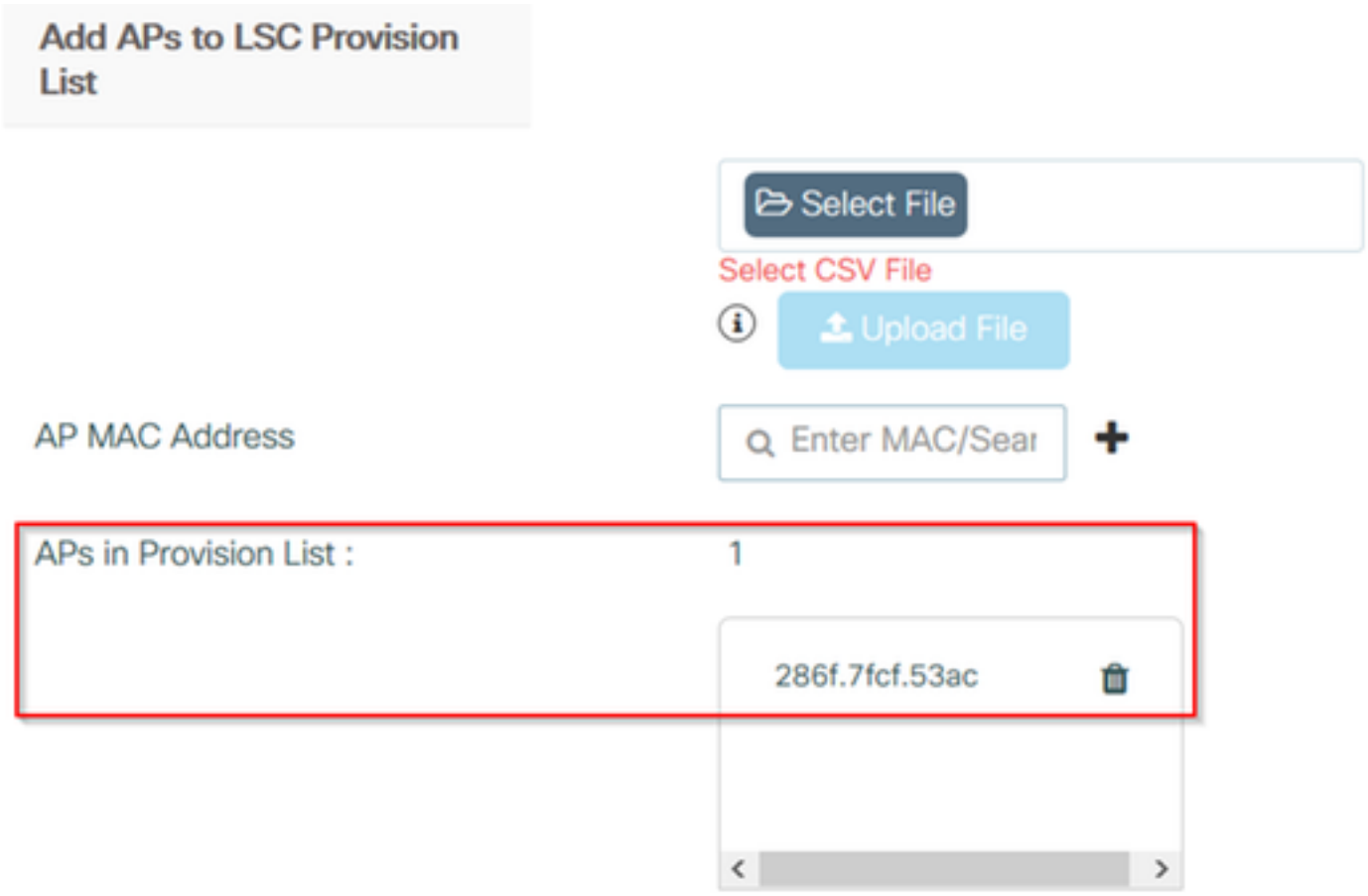
```
9800-L(config)#ap lsc-provision join-attempt
```

```
9800-L(config)#ap lsc-provision trustpoint
```

```
9800-L(config)#ap lsc-provision key-size
```

步驟4.（可選）可以為加入控制器的所有AP或mac地址清單中定義的特定AP觸發AP LSC調配。在同一選單中，在文本欄位中輸入格式為xxxx.xxxx.xxxx的AP乙太網MAC地址，然後按一下**+** 符號。或者，上傳包含AP mac地址的csv檔案，選擇該檔案，然後選擇**上傳檔案**。

附註：控制器跳過csv檔案中它無法從其加入的AP清單中識別的任何mac地址。



用於步驟4的CLI配置：

```
9800-L(config)#ap lsc-provision mac-address
```

步驟5。 從**Status** 標籤旁邊的下拉選單中選擇**Enabled**或**Provision List**，然後按一下**Apply**以觸發AP LSC註冊。

附註：AP開始證書請求、下載和安裝。證書完全安裝後，AP將重新啟動，並使用新證書啟動加入過程。

提示：如果通過預生產控制器完成AP LSC調配，並且使用調配清單，則在調配證書後不要刪除AP條目。如果這樣做，且AP回退到MIC並加入相同的預生產控制器，則擦除其LSC證書。

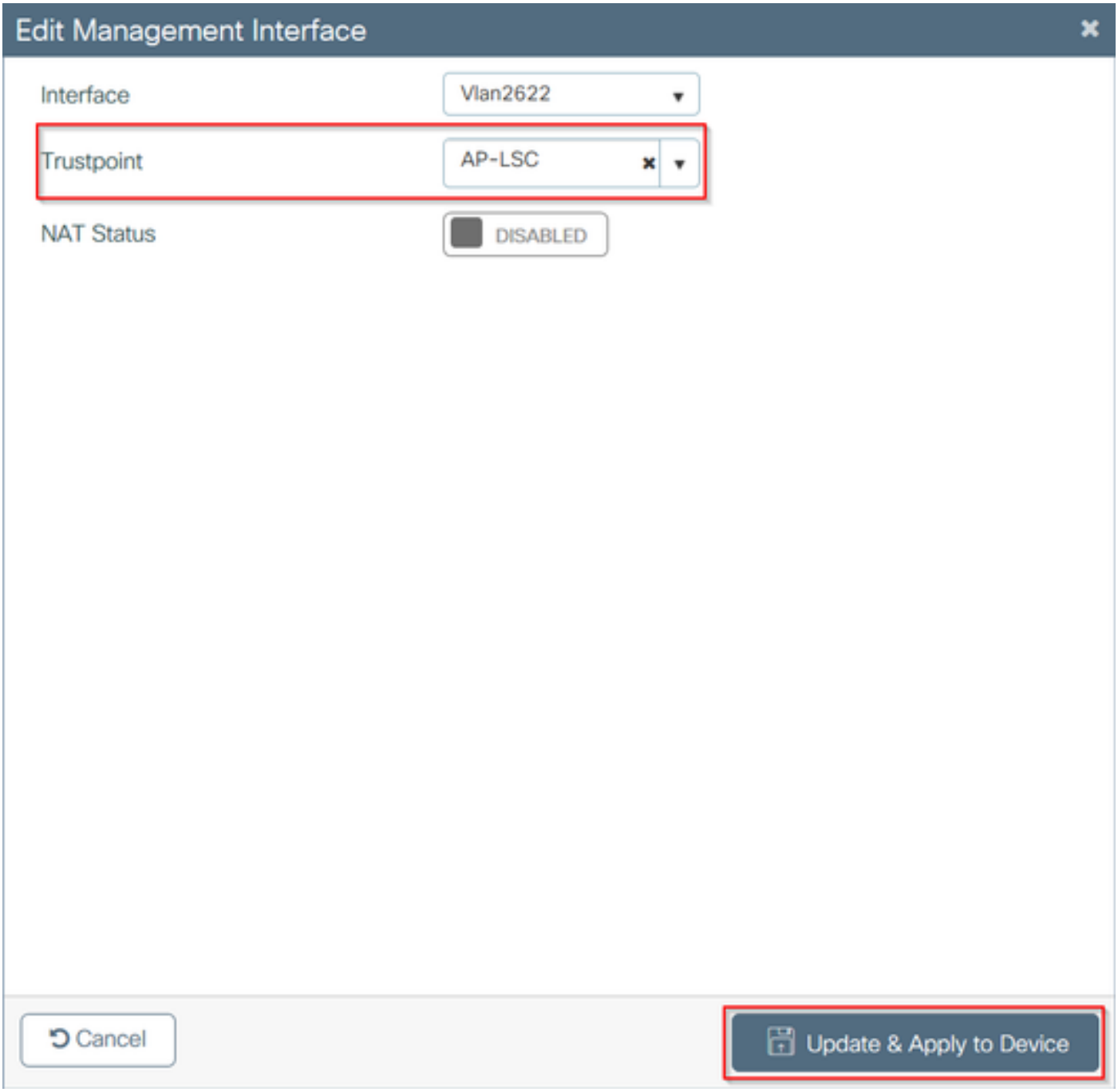
用於步驟5的CLI配置：

```
9800-L(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size
configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key
by-default or 256 bit key if configured.
Are you sure you want to continue? (y/n): y If specific AP list provisioning is preferred then
use: 9800-L(config)#ap lsc-provision provision-list
```

步驟6.導覽至**Configuration > Interface > Wireless，然後選擇management interface。**在**Trustpoint**欄位中，從下拉選單中選擇新信任點，然後按一下**Update & Apply to Device**。

注意：如果已啟用LSC，但9800 WLC的信任點引用MIC或SSC，則AP會嘗試加入LSC以設定嘗試加入的次數。達到最大嘗試次數限制後，AP會回退到MIC並再次加入，但由於啟用了LSC設定，AP會請求新的LSC。這會導致一個環路，其中CA伺服器持續為相同的AP簽署證書，並且AP停滯在join-request-reboot環路中。

附註：管理信任點更新為使用LSC證書後，新AP無法通過MIC加入控制器。當前不支援開啟調配視窗。如果您需要安裝新AP，則需要在之前預配置一個LSC，該LSC由管理信任點中的CA簽署。



第六步的CLI配置：

```
9800-L(config)#wireless management trustpoint
```

驗證

驗證控制器證書安裝

要驗證9800 WLC信任點中是否存在LSC資訊，請發出命令**show crypto pki certificates verbose <trustpoint name>**，兩個證書將關聯到為LSC設定和註冊建立的信任點。在此示例中，信任點名稱為「microsoft-ca」（僅顯示相關輸出）：

```
9800-L#show crypto pki certificates verbose microsoft-ca
Certificate
  Status: Available
  Version: 3
  Certificate Usage: General Purpose
  Issuer:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
  Subject:
    Name: 9800-L.alzavala.local
    cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
    o=Wireless TAC
    l=Juarez
    st=CDMX
    c=MX
    hostname=9800-L.alzavala.local
  CRL Distribution Points:
    ldap:///CN=CHUU-WIN12-CA,CN=Chuu-
Win12,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Coint
Validity Date:
start date: 04:25:59 Central May 11 2020
end date: 04:25:59 Central May 11 2022 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption [...] Authority Info
Access: CA ISSUERS: ldap:///CN=CHUU-WIN12-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=chuu-
domain,DC=local?cACertificate?base?objectClass=certificationAuthority [...] CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 37268ED56080CB974EF3806CCACC77EC
  Certificate Usage: Signature
  Issuer:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
  Subject:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
 Validity Date:
start date: 05:58:01 Central May 10 2019
end date: 06:08:01 Central May 10 2024 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption
```

驗證9800 WLC LSC配置

若要驗證有關無線管理信任點的詳細資訊，請運行show wireless management trustpoint命令，確保使用正確的信任點（此示例中包含LSC詳細資訊的信任點，即AP-LSC）並將其標籤為可用：

```
9800-L#show wireless management trustpoint

Trustpoint  Name : AP-LSC
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
Private key Info : Available
```

若要驗證有關AP LSC調配配置的詳細資訊以及新增到調配清單的AP清單，請運行show ap lsc-provision summary命令。確保顯示正確的設定狀態：

```
9800-L#show ap lsc-provision summary
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : AP-LSC
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : MX
State : CDMX
City : Juarez
Orgn : Cisco TAC
Dept : Wireless TAC
Email : josuvill@cisco.com
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses :
--------------
xxxx.xxxx.xxxx
xxxx.xxxx.xxxx
```

驗證接入點證書安裝

若要驗證安裝在AP中的憑證，請從AP CLI執行show crypto 命令，確保CA根憑證和裝置憑證都存在（輸出僅顯示相關資料）：

```
AP3802#show crypto

[...]
------------------------------------------------------------------------------ LSC: Enabled
----------------------------- Device Certificate -----------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:00:0b
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Validity
            Not Before: May 13 01:22:13 2020 GMT
            Not After : May 13 01:22:13 2022 GMT
        Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC, CN=ap3g3-
286F7FCF53AC/emailAddress=josuvill@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)

----------------------------- Root Certificate ------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Validity
            Not Before: May 10 05:58:01 2019 GMT
            Not After : May 10 05:58:01 2024 GMT
        Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

如果使用交換機埠dot1x身份驗證的LSC，則可以從AP驗證是否啟用了埠身份驗證。

```
AP3802#show ap authentication status
AP dot1x feature is disabled.
```

附註：要為AP啟用埠dot1x，需要在AP配置檔案或AP配置本身中使用虛設值定義AP的dot1x憑證。

疑難排解

常見問題

1. 如果模板在伺服器登錄檔中未正確對映，或者伺服器需要密碼質詢，則會拒絕9800 WLC或AP的證書請求。
2. 如果IIS預設站點被禁用，SCEP服務也會被禁用，因此無法訪問信任點中定義的URL，並且9800 WLC不會傳送任何證書請求。
3. 如果伺服器和9800 WLC之間的時間不同步，則不會安裝證書，因為時間有效性檢查失敗。

Debug和Log命令

使用以下命令排除9800控制器證書註冊故障：

```
9800-L#debug crypto pki transactions
9800-L#debug crypto pki validation
9800-L#debug crypto pki scep
```

要對AP註冊進行故障排除和監控，請使用以下命令：

```
AP3802#debug capwap client payload
AP3802#debug capwap client events
```

在AP命令列中，**show logging**顯示AP是否出現證書安裝問題，並提供有關未安裝證書原因的詳細資訊：

```
[...]
Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.3429] AP has joined controller 9800-L Mar 19
19:39:13 kernel: 03/19/2020 19:39:13.3500] SELinux: initialized (dev mtd_inodefs, type
mtd_inodefs), not configured for labeling Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.5982]
Generating a RSA private key Mar 19 19:39:14 kernel: *03/19/2020 19:39:13.5989]
..................... Mar 19 19:39:15 kernel: *03/19/2020 19:39:14.4179] .. Mar 19 19:39:15
kernel: *03/19/2020 19:39:15.2952] writing new private key to '/tmp/lsc/priv_key' Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.2955] ----- Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5421] cen_validate_lsc: Verification failed for certificate: Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] countryName = MX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421]
stateOrProvinceName = CDMX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] localityName =
Juarez Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] organizationName = cisco-tac Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.5421] commonName = ap3g3- Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] emailAddress = jesuherr@cisco.com Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427] LSC certificates/key failed validation! Mar 19 19:39:15 kernel: *03/19/2020
```

19:39:15.5427]

成功註冊嘗試示例

這是前面提到的成功註冊控制器及其關聯AP的調試輸出。

CA根憑證匯入到9800 WLC:

```
[...]
Certificate has the following attributes: Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B % Do you accept this certificate?
[yes/no]: yes CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA
Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-
LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8
CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened
CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0
(compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC,
refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length
received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length :
(3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0
CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert
Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:47:34 GMT Connection:
close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates.
CRYPTO_PKI_SCEP: Client received CA and RA certificate
CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3
certificates. CRYPTO_PKI:crypto_pkcs7_extract_ca_cert found cert CRYPTO_PKI: Bypassing SCEP
capabilities request 0 CRYPTO_PKI: transaction CRYPTO_REQ_CA_CERT completed CRYPTO_PKI: CA
certificate received. CRYPTO_PKI: CA certificate received. CRYPTO_PKI:
crypto_pki_get_cert_record_by_cert() CRYPTO_PKI: crypto_pki_authenticate_tp_cert() CRYPTO_PKI:
trustpoint AP-LSC authentication status = 0 Trustpoint CA certificate accepted.
```

9800 WLC裝置註冊：

```
[...]
CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI_SCEP: Client sending GetCACert
request CRYPTO_PKI: Sending CA Certificate Request: GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent:
Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint
AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message
CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco
PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked
trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse
content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data
arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header:
HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-
By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 3638 Content-
Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and
RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message
contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs
CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI_SCEP: Client Sending GetCACaps
request with msg = GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACaps&message=AP-LSC
HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI:
locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending
HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE
5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0
CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 171
CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (34) CRYPTO_PKI:
Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply
HTTP header: HTTP/1.1 200 OK Content-Type: text/plain Server: Microsoft-IIS/8.5 X-Powered-By:
ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 34 CRYPTO_PKI:
HTTP header content length is 34 bytes CRYPTO_PKI_SCEP: Server returned capabilities: 92
```

CA_CAP_RENEWAL CA_CAP_S alz_9800(config)#HA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: %PKI-6-CSR_FINGERPRINT: CSR Fingerprint MD5 : 9BFBA438303487562E888087168F05D4 CSR Fingerprint SHA1: 58DC7DB84C632A7307631A97A6ABCF65A3DEFEEF CRYPTO_PKI: Certificate Request Fingerprint MD5: 9BFBA438 30348756 2E888087 168F05D4 CRYPTO_PKI: Certificate Request Fingerprint SHA1: 58DC7DB8 4C632A73 07631A97 A6ABCF65 A3DEFEEF PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E 00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 65 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 66 CRYPTO_PKI: Expiring peer's cached key with key id 66 PKI: Trustpoint AP-LSC has no router cert PKI: Signing pkcs7 with AP-LSC trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2807) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: received msg of 2995 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 2807 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 66 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 67 CRYPTO_PKI: Expiring peer's cached key with key id 67 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (AF58BA9313638026C5DC151AF474723F) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Newly-issued Router Cert: issuer=cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial=1800043245DC93E1D943CA70000043 start date: 21:38:34 Central May 19 2020 end date: 21:38:34 Central May 19 2022 Router date: 21:48:35 Central May 19 2020 %PKI-6-CERT_INSTALL: An ID certificate has been installed under Trustpoint : AP-LSC Issuer-name : cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local Subject-name : cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com,o=Wireless TAC,l=Juarez,st=CDMX,c=MX,hostname=alz_9800.alzavala.local Serial-number: 1800000043245DC93E1D943CA7000000000043 End-date : 2022-05-19T21:38:34Z Received router cert from CA CRYPTO_PKI: Not adding alz_9800.alzavala.local to subject-alt-name field because : Character allowed in the domain name. Calling pkiSendCertInstallTrap to send alert CRYPTO_PKI: All enrollment requests completed for trustpoint AP-LSC

AP註冊調試來自控制器端的輸出，對於加入到9800 WLC的每個AP，此輸出重複多次：

[...]
CRYPTO_PKI: (A6964) Session started - identity selected (AP-LSC) CRYPTO_PKI: Doing re-auth to fetch RA certificate. CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate
CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs
CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 PKCS10 request is compulsory CRYPTO_PKI: byte 2 in key usage in PKCS#10 is 0x5 May 19 21: alz_9800(config)#51:04.985: CRYPTO_PKI: all usage CRYPTO_PKI: key_usage is 4 CRYPTO_PKI: creating trustpoint clone Proxy-AP-LSC8 CRYPTO_PKI: Creating proxy trustpoint Proxy-AP-LSC8 CRYPTO_PKI: Proxy enrollment request trans id = 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: Proxy forwading an enrollment request

CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI: Proxy send CA enrollment request with trans id: 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: No need to re-auth as we have RA in place CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E 00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 67 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 68 CRYPTO_PKI: Expiring peer's cached key with key id 68 PKI: Trustpoint Proxy-AP-LSC8 has no router cert and loaded PKI: Signing pkcs7 with Proxy-AP-LSC8 trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 3 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2727) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: received msg of 2915 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 2727 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 68 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 69 CRYPTO_PKI: Expiring peer's cached key with key id 69 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 alz_9800(config)# verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (7CBB299A2D9BC77DBB1A8716E6474C0C) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Received router cert from CA CRYPTO_PKI: Enrollment poroxy callback status: CERT_REQ_GRANTED CRYPTO_PKI: Proxy received router cert from CA CRYPTO_PKI: Rcvd request to end PKI session A6964. CRYPTO_PKI: PKI session A6964 has ended. Freeing all resources. CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Cleaning RA certificate for TP : AP-LSC CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_CS: removing trustpoint clone Proxy-AP-LSC8

來自AP端的AP註冊調試輸出：

```
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 40 len 407
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: CERTIFICATE_PARAMETER_PAYLOAD(63) vendId 409600
LSC set retry number from WLC: 1

Generating a RSA private key
...
.............................
writing new private key to '/tmp/lsc/priv_key'
-----
[ENC] CAPWAP_WTP_EVENT_REQUEST(9)
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) Len 1135 Total 1135
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 41 len 20
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_CERT_ENROLL_PENDING from WLC

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
Received Capwap watchdog update msg.
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 42 len 1277
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving ROOT_CERT
```

```
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 43 len 2233
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving DEVICE_CERT

SC private key written to hardware TAM

root: 2:  LSC enabled
AP Rebooting: Reset Reason - LSC enabled
```

通過SCEP進行LSC註冊的配置示例到此結束。