9800 WLCでのローカルで有効な証明書プロビジョニングのためのSCEPの設定

内容

概要

このドキュメントでは、Windows Server 2012のMicrosoft Network Device Enrollment Service(NDES)およびSimple Certificate Enrollment Protocol(SCEP)機能を使用して、アクセスポイント(AP)のローカルで有効な証明書(LSC)登録を行うように98000ワイヤレス00コントローラ(WLC)を0をする00する00000000000000000000000000000000000000000 r2標準。

前提条件

Windows ServerでSCEPを正常に実行するには、9800 WLCが次の要件を満たしている必要があります。

- コントローラとサーバの間に到達可能性がある必要があります。
- コントローラとサーバは同じNTPサーバに同期されているか、同じ日付とタイムゾーンを共有しています（CAサーバとAPからの時刻が異なる場合、APは証明書の検証とインストールに問題があります）。

Windows Serverでは、インターネットインフォメーションサービス(IIS)が以前に有効になっている必要があります。

要件

次のテクノロジーに関する知識があることが推奨されます。

- 9800 Wireless LAN Controllerバージョン16.10.1以降。
- Microsoft Windows Server 2012 Standard.
- 秘密キーインフラストラクチャ(PKI)と証明書。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9800-L WLCソフトウェアバージョン17.2.1。
- Windows Server 2012 Standard R2。
- 3802アクセスポイント

> **注**：このドキュメントのサーバ側の設定は、特にWLC SCEPです。詳細、セキュリティ、および証明書サーバの設定については、Microsoft TechNetを参照してください。

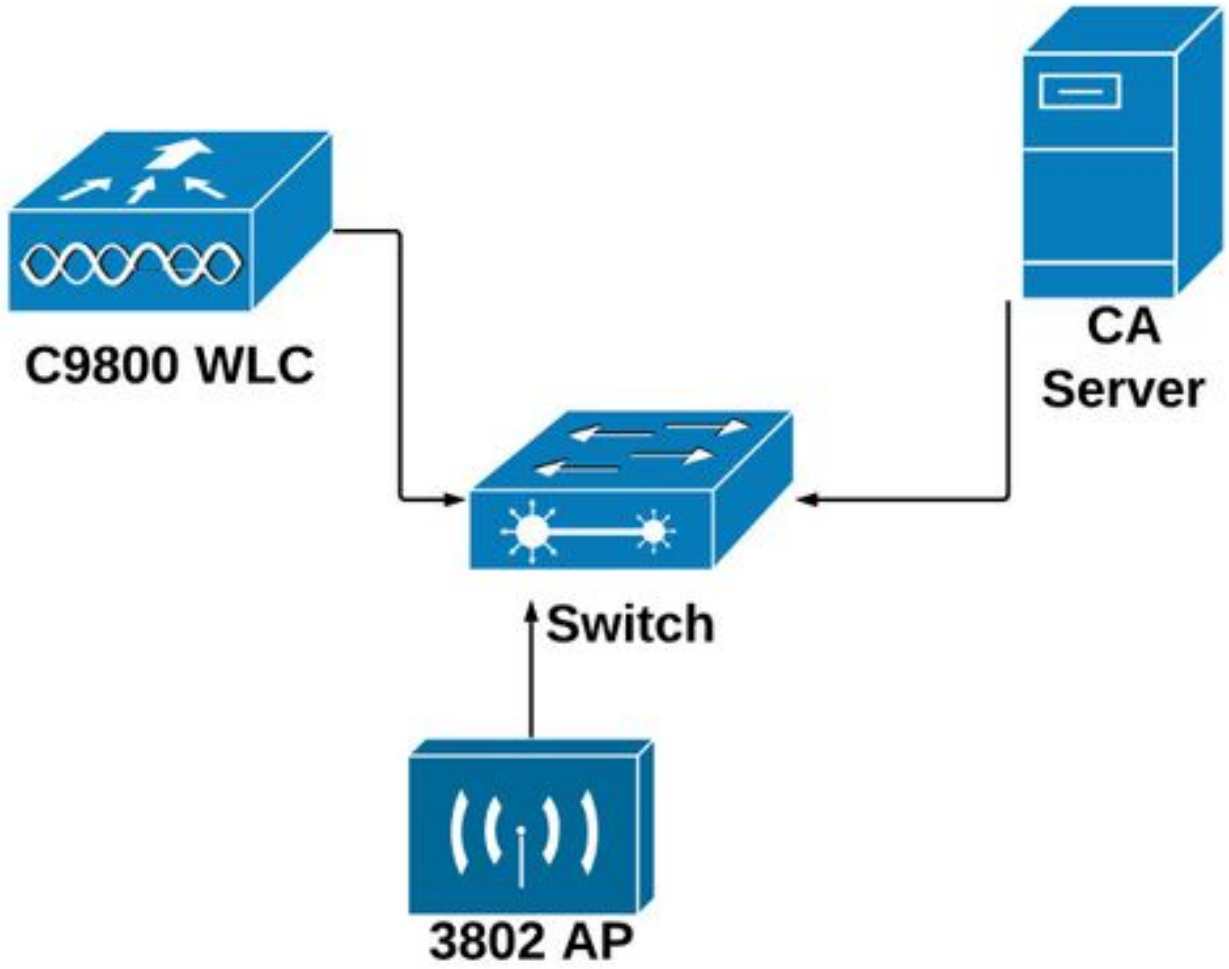
背景説明

新しいLSC証明書(認証局(CA)ルート証明書とデバイス証明書の両方)をコントローラにインストールして、最終的にAPにダウンロードする必要があります。SCEPでは、CA証明書とデバイス証明書がCAサーバから受信され、後でコントローラに自動的にインストールされます。

APがLSCでプロビジョニングされると、同じ認証プロセスが実行されます。そのためには、コントローラがCAプロキシとして機能し、CAによって署名されたAPの証明書要求（自己生成）を取得するのに役立ちます。

設定

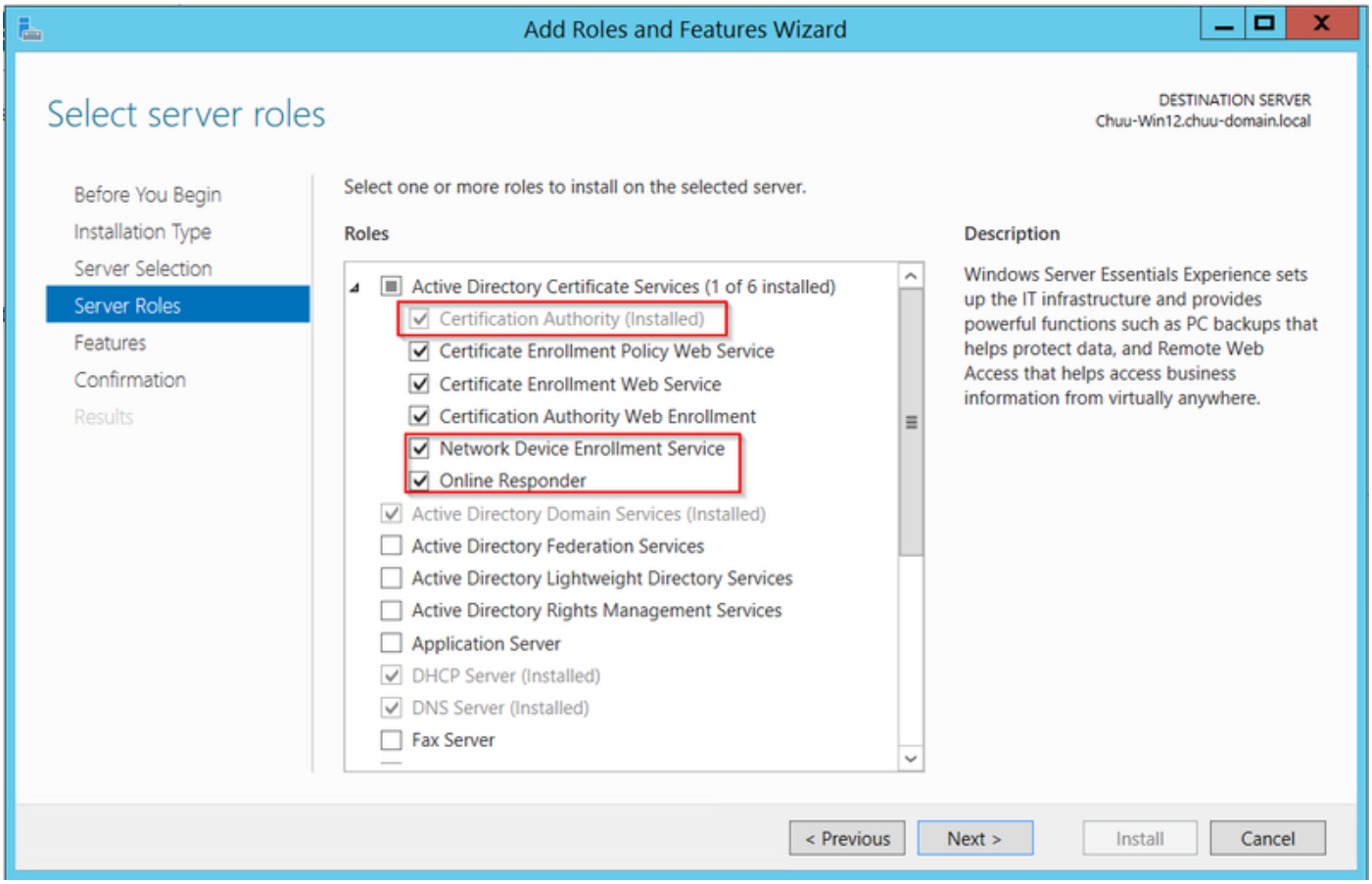
ネットワーク図



Windows ServerでのSCEPサービスの有効化

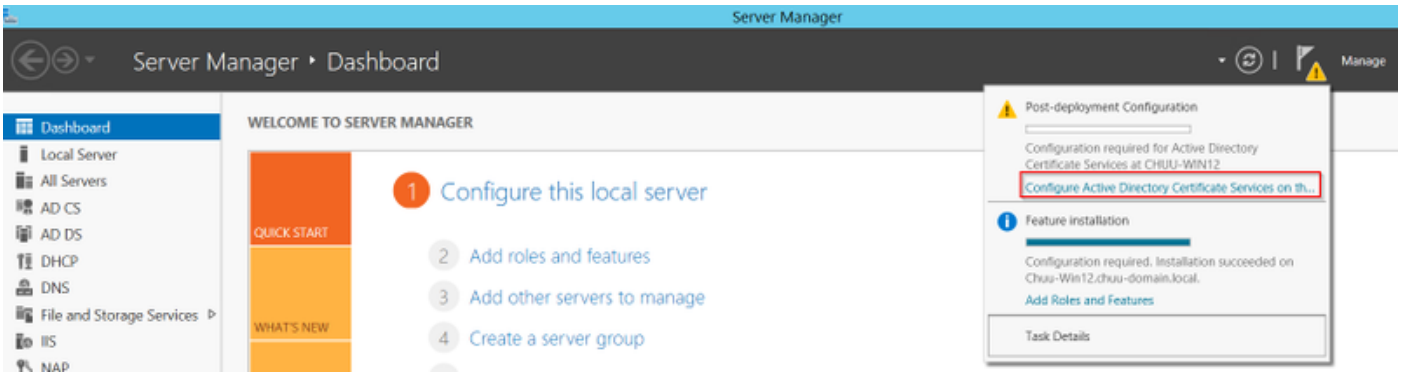
ステップ1：サーバマネージャアプリケーションで、[管理]メ**ニューを選択**し、[役割と機能の追**加]オプションを選択**して、役割の役割と機能構成ウィザードを開きます。そこから、SCEPサーバ登録に使用されるサーバインスタンスを選択します。

ステップ2:[Certification Authority]、[Network Device Enrollment Service]、および[Online Responder]の機能が選択されていることを確認し、[Next]を選択します。



ステップ3:[次へ]を**2回**選択し、[完了]を選択**して構成**ウィザードを終了します。サーバーが機能のインストールプロセスを完了するまで待ってから、[閉じる]を選択し**てウィザ**ードを閉じます。

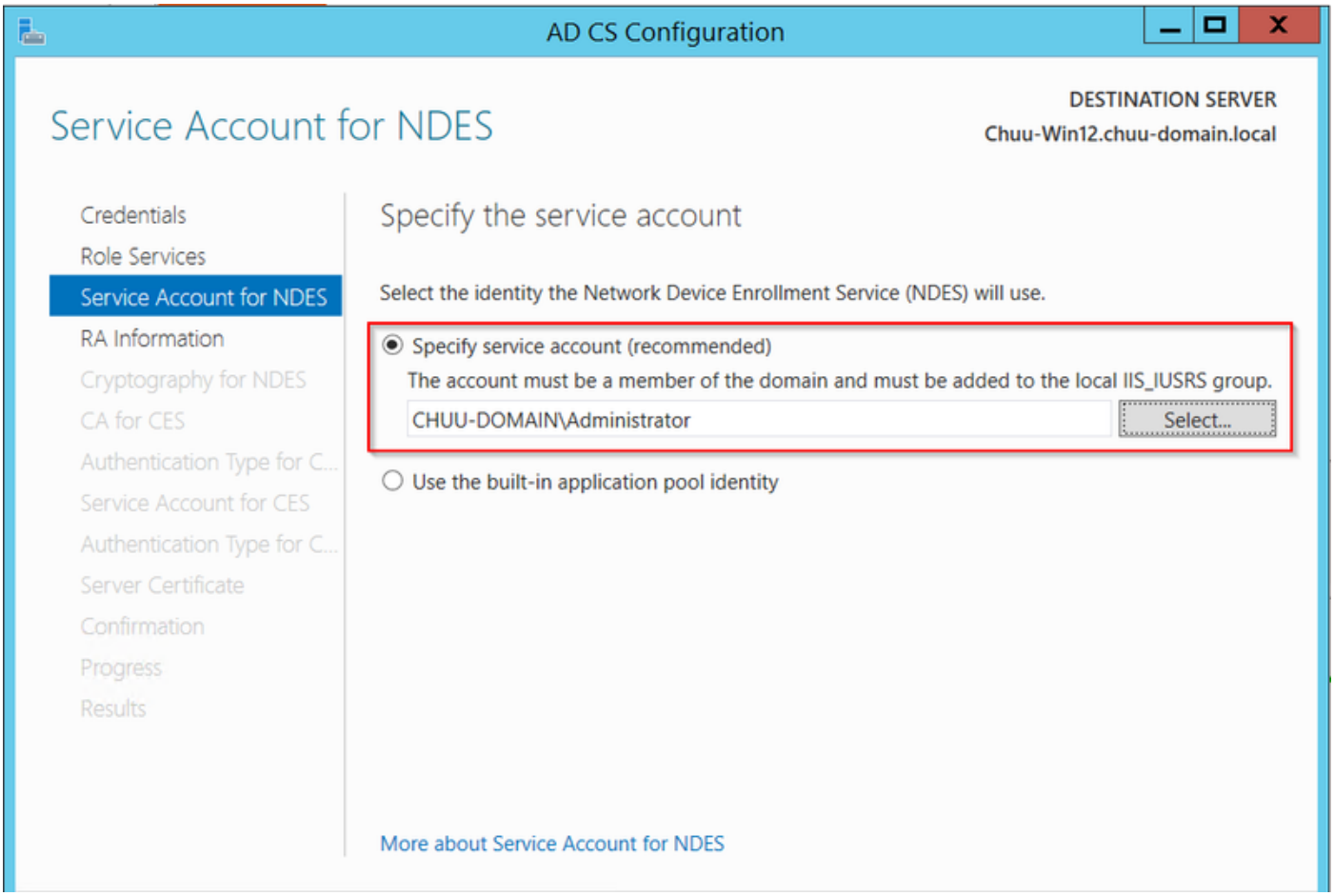
ステップ4：インストールが完了すると、[Server Manager Notification]アイコンに警告アイコンが表示されます。これを選択し、**[AD CS構成ウィザード]メニューを開くには、[接続先サーバー上のActive Directoryサービスの**構成]オプションリンクを選択し**て**ください。



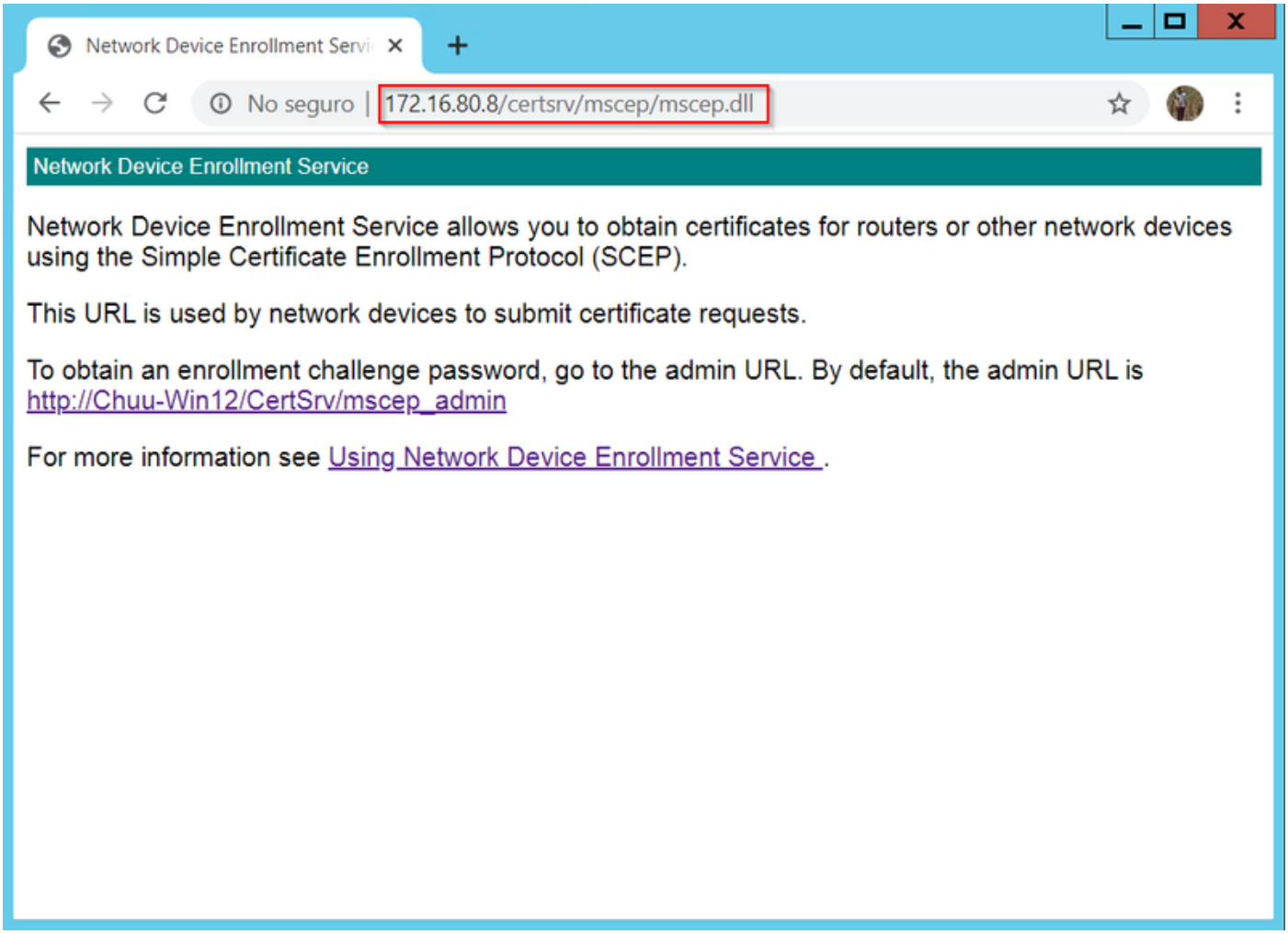
ステップ5：メニューで構成する**Network Device Enrollment Service**と**Online Responder**の役割サービスを選択し、[次へ]を選**択します。**

ステップ6:NDESのサービスアカウントで、組み込みのアプリケーション**プールとサービスアカウントの間のオプションを選択**し、[次へ]を選択**します。**

> **注**：サービスアカウントの場合は、そのアカウントが**IIS**_IUSRSグループに属していることを確認してください。



ステップ7：次の画面で[Next]を選択し、インストール処理を終了します。インストール後、SCEP URLは任意のWebブラウザで使用できます。URL **http://<server ip>/certsrv/mscep/mscep.dll**に移動し、**サービスが利用可能**であることを確認します。



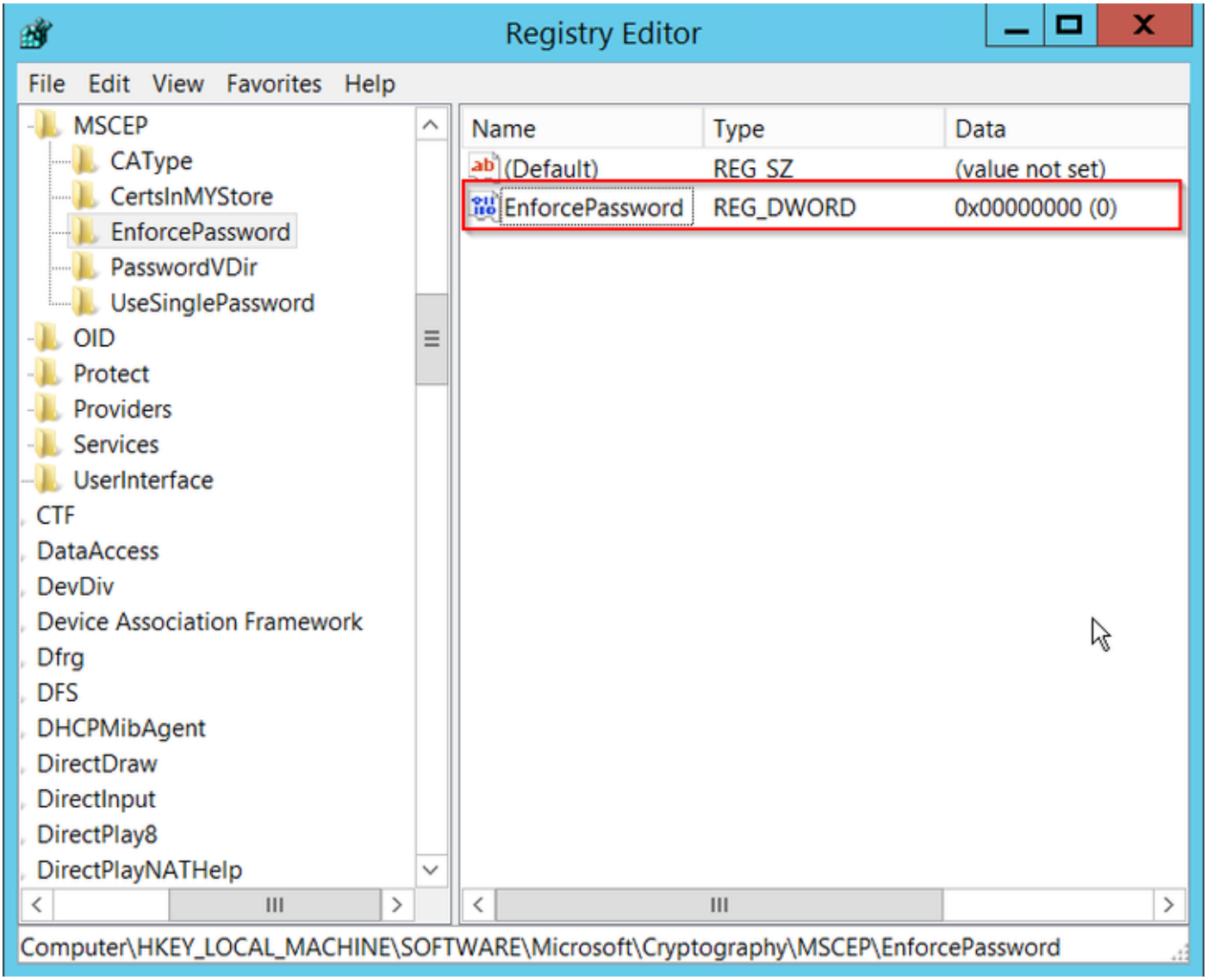
SCEP 登録チャレンジ パスワードの要件の無効化

デフォルトでは、Windows Serverは動的チャレンジパスワードを使用して、Microsoft SCEP(MSCEP)に登録する前にクライアント要求とエンドポイント要求を認証します。 そのためには、管理者アカウントがWeb GUIを参照し、各要求のオンデマンドパスワードを生成する必要があります（パスワードは要求に含める必要があります）。コントローラは、サーバに送信する要求にこのパスワードを含めることはできません。この機能を削除するには、NDESサーバのレジストリキーを変更する必要があります。

ステップ1：レジストリエディットフォームを開き、[スタート]メニューから[Regedit]**を検索**します。

ステップ2:[Computer] > [HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP] > [EnforcePassword]に移動します

ステップ3: EnforcePasswordの値**を0**に変更します。すでに0の場合は、そのまま残します。



証明書テンプレートとレジストリの設定

証明書とその関連キーは、CAサーバ内のアプリケーションポリシーによって定義される異なる目的で、複数のシナリオで使用できます。アプリケーションポリシーは、証明書の拡張キー使用法(EKU)フィールドに保存されます。このフィールドはオーセンティケータによって解析され、意図した目的でクライアントによって使用されていることを確認します。適切なアプリケーションポリシーがWLCおよびAP証明書に統合されていることを確認するには、適切な証明書テンプレートを作成し、それをNDESレジストリにマッピングします。

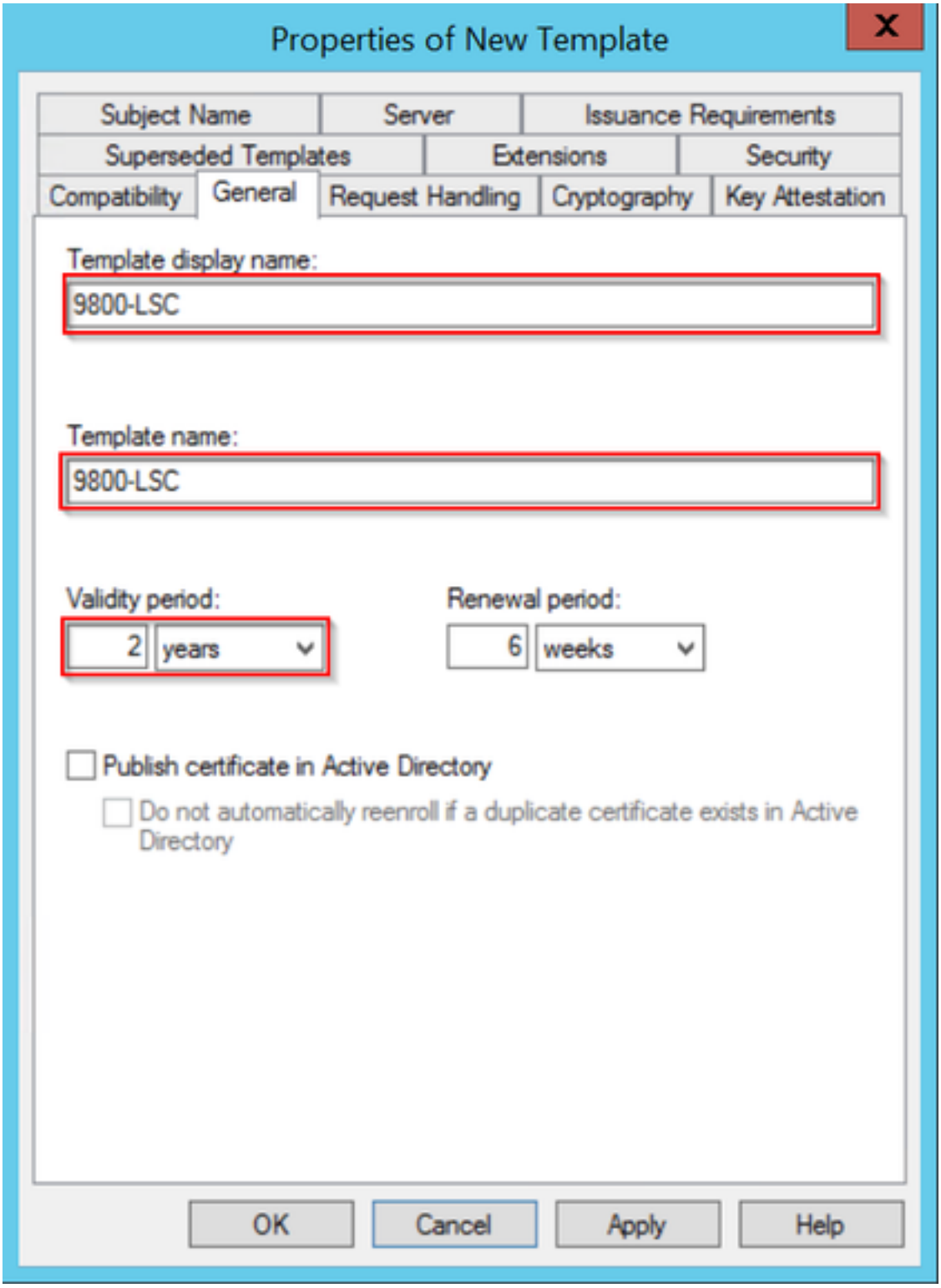
ステップ1:[Start] > **[Administrative Tools] > [Certification Authority]に移動します。**

ステップ2:CA Serverフォルダツリーを展開し、[Certificate Templates]フォルダを右クリックして**[Manage]**を選択**します。**

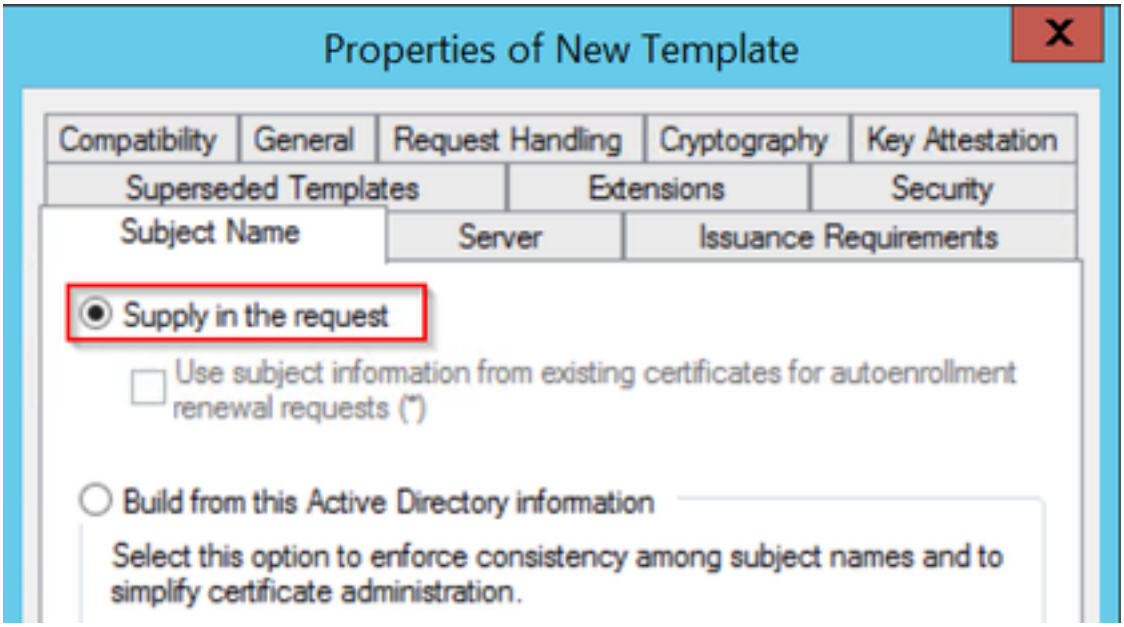
ステップ3：ユーザー証明書テンプレートを右クリックし**て、コン**テキストメニューで**[Duplicate Template]**を選択します。

ステップ4:[General]タブに移動し、テンプ**レート名**と有効期間を必要に応じて変更し、その他のオプションはすべてオフのままにします。

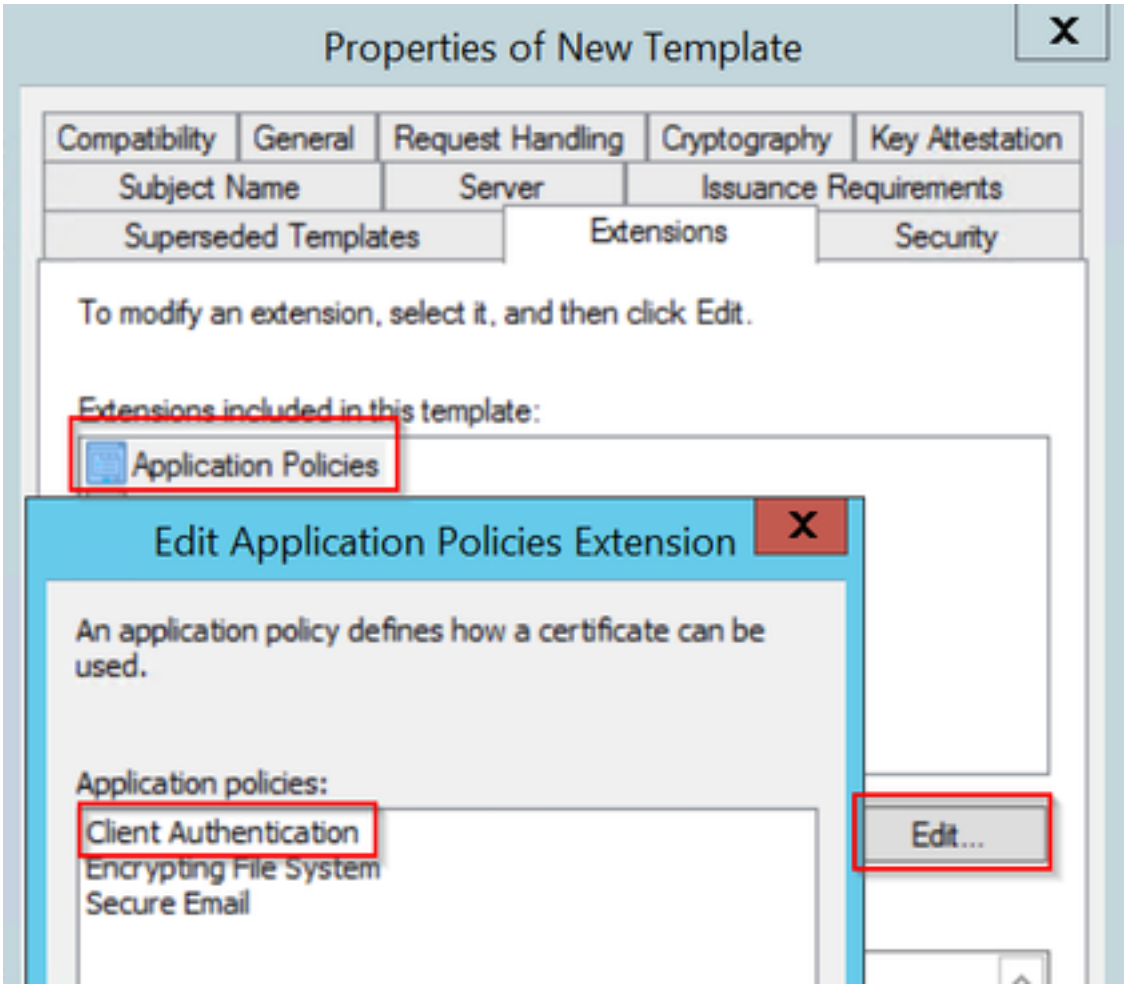
> **注意**：有効期間を変更する場合は、証明機関のルート証明書の有効期間より大きくないことを確認してください。



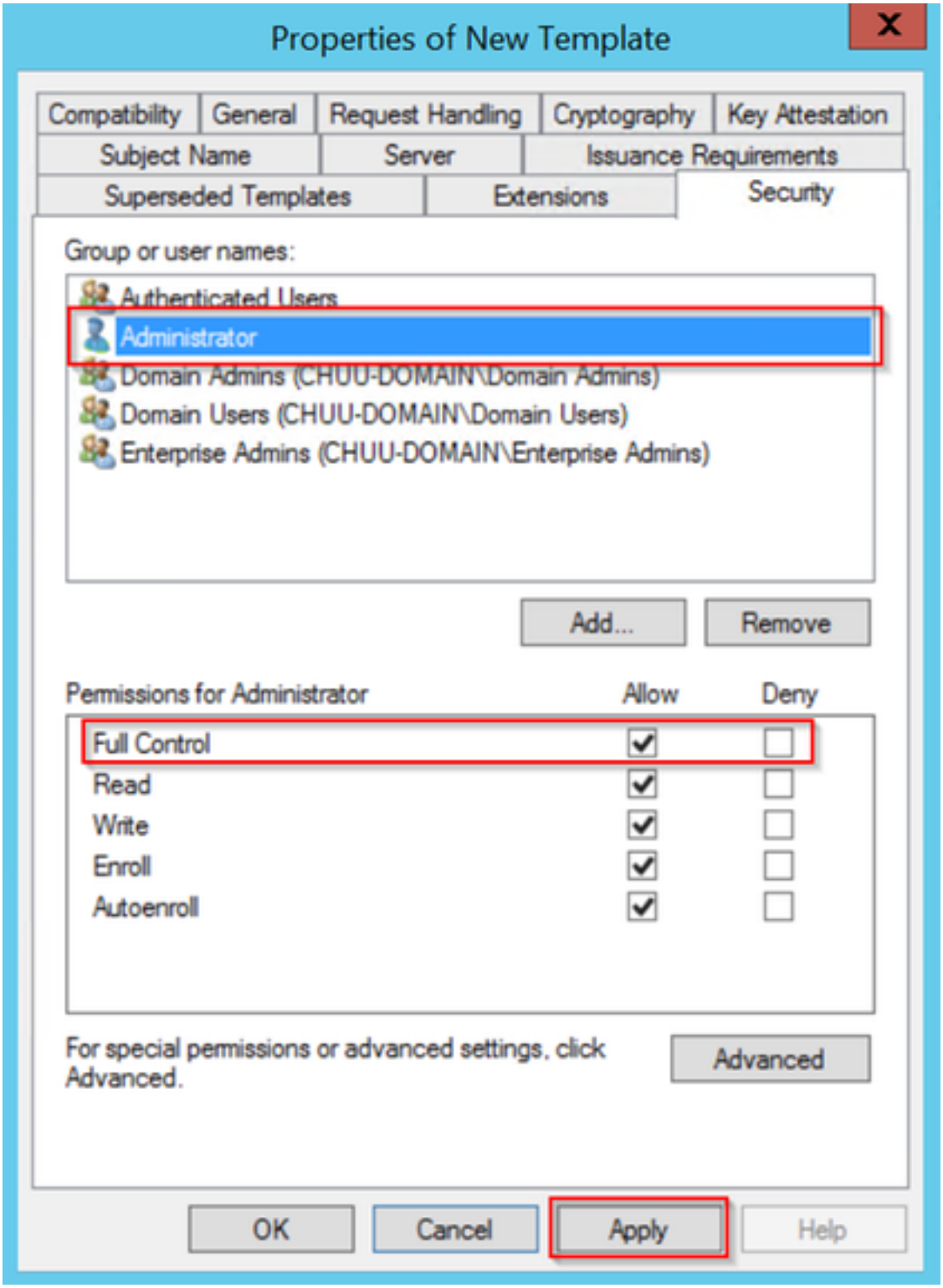
ステップ5:「サブジェクト名」タブに**移動**して、「要求**内の供給」が選択されていることを**確認します。証明書の署名を取得するために管理者の承認が必要ないことを示すポップアップが表示されたら、[OK]を選択**します。**



ステップ6:[Extensions]タブに移動し、[Application Policies]オプションを選択し、[Edit...]ボタンを選択します。[Application Policies]ウィンドウにクライアント認証が表示されていることを確認します。それ以外の場合は、[Add] を選択して追加します。



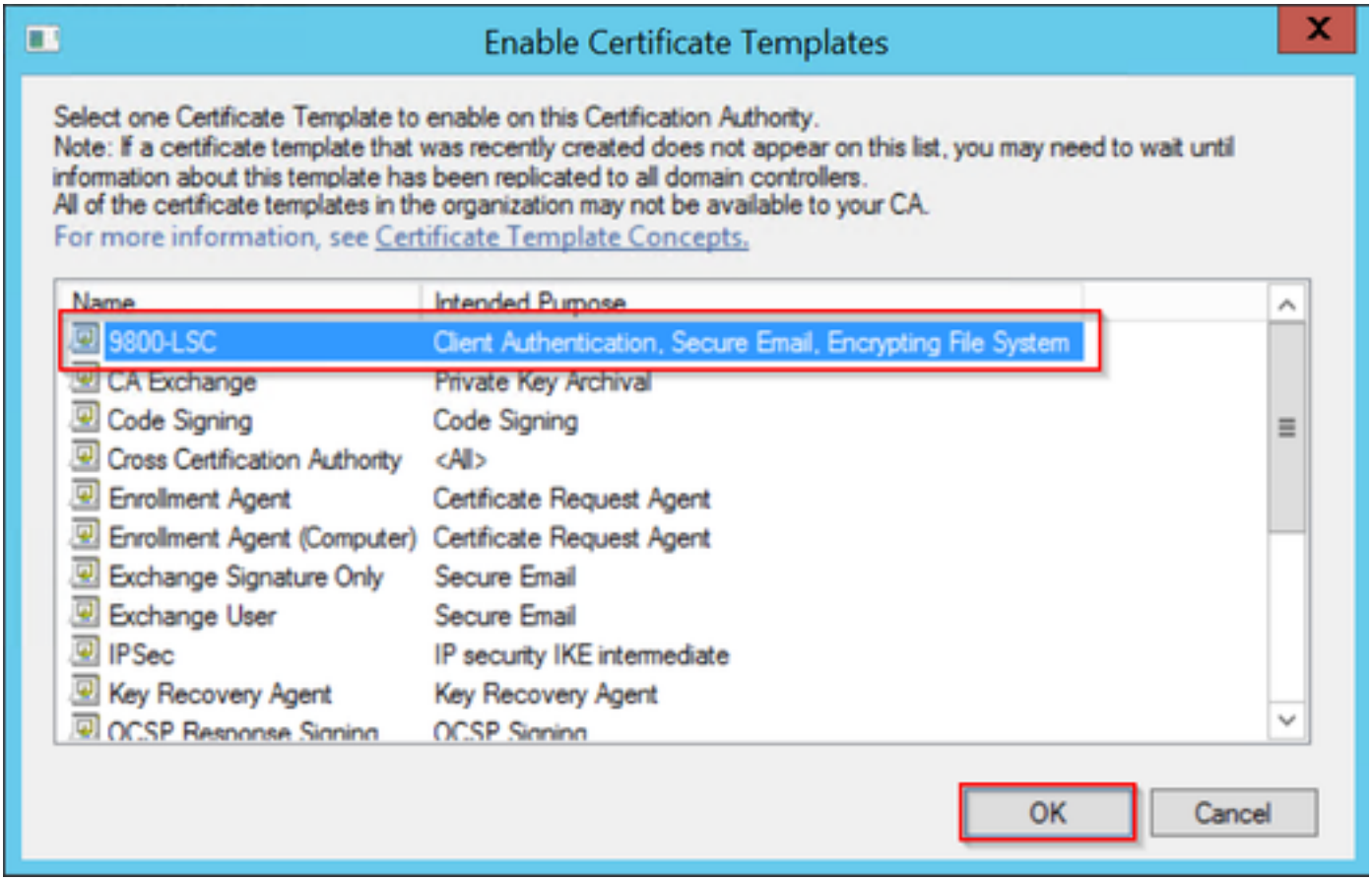
ステップ7:[Security]タブに移動し、Windows ServerでSCEPサービスを有効にするステップ6で定義したサービスアカウントにテンプレートのフルコントロール権限があることを確認して、[Apply]、[OK]を選択します。



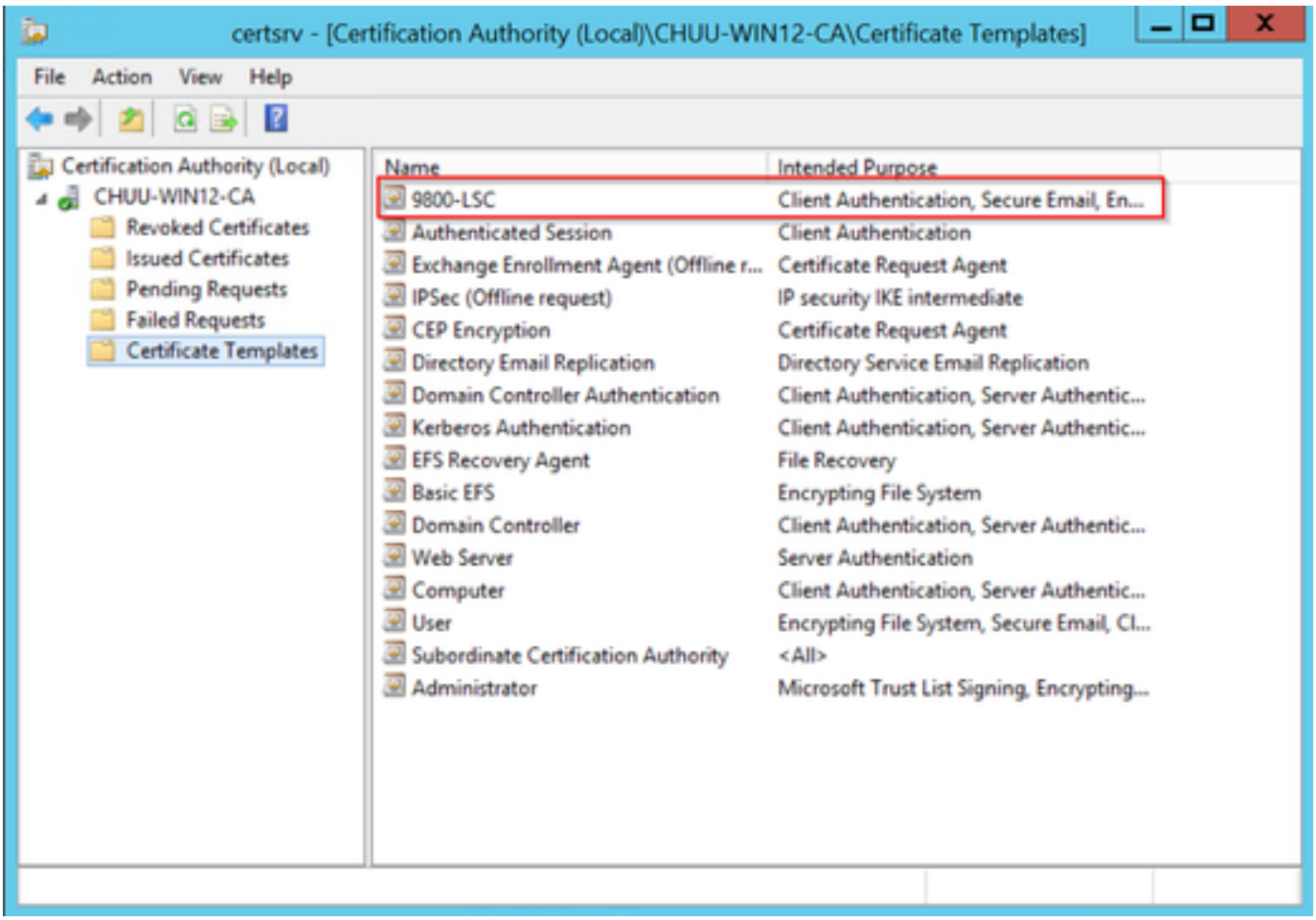
ステップ8:[Certification Authority]ウィンドウに戻り、[Certificate Templates]フォルダを右クリックし、[New] > [Certificate Template to Issue]を選択します。

ステップ9:前に作成した証明書テンプレートを選択します。この例では、9800-LSCです。次に、[OK]を選択します。

> **注：**新しく作成した証明書テンプレートは、すべてのサーバで複製する必要があるため、複数のサーバ展開でリストに表示するには時間がかかる場合があります。



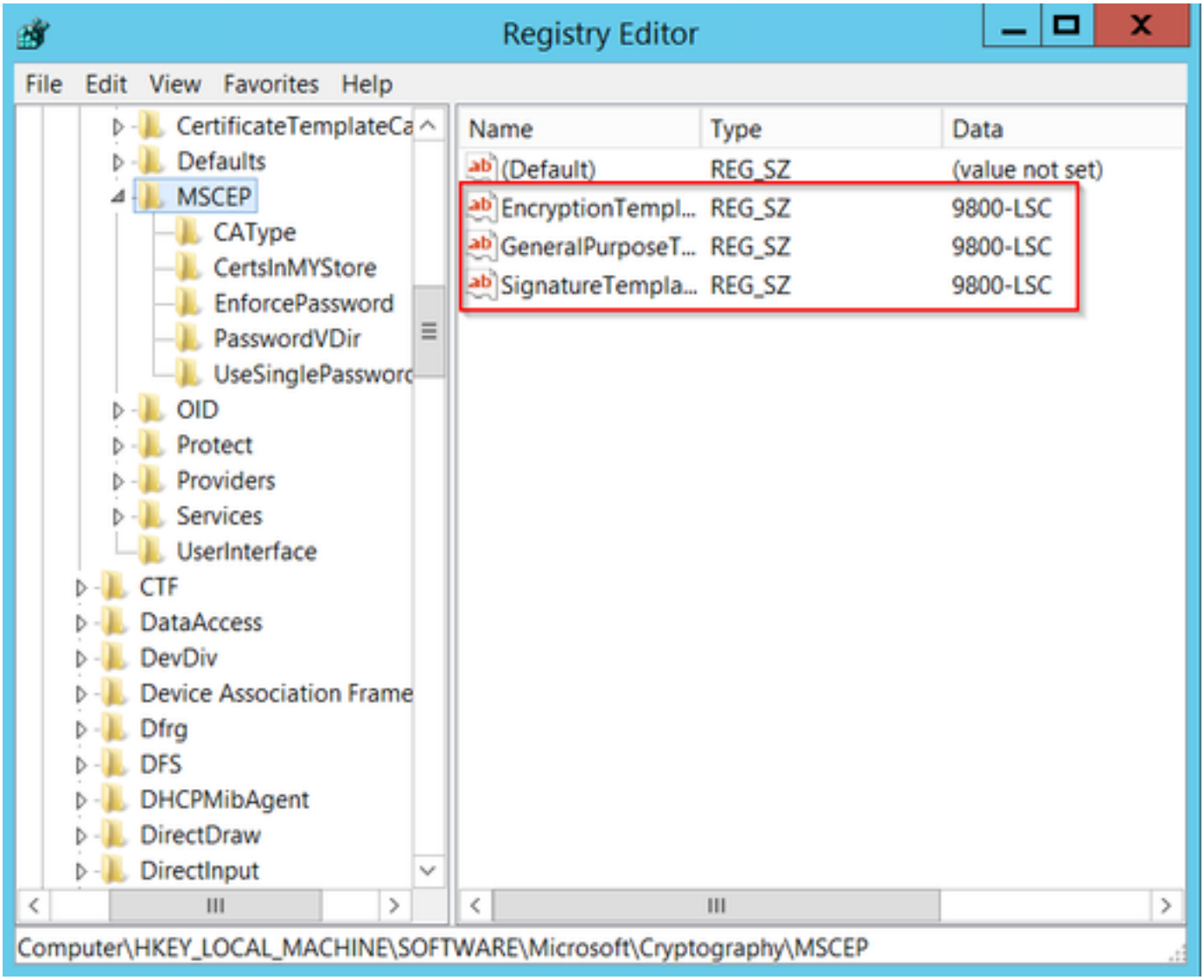
新しい証明書テンプレートが[証明書テンプレート]フォルダの内容にリストされます。



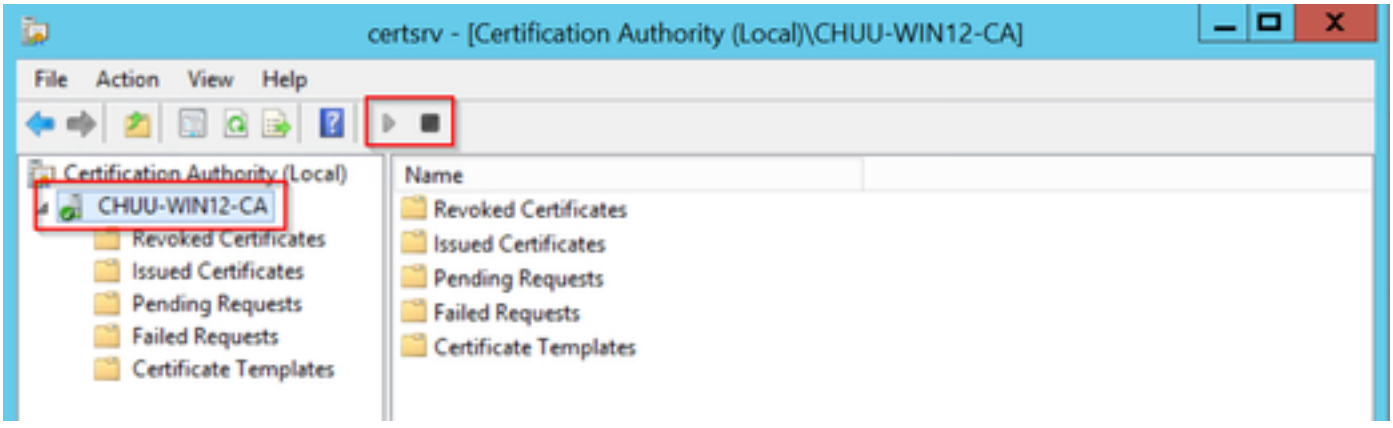
ステップ10：レジストリーエディタ(Registry Editor)ウィンドウに戻り、[Computer] >

[HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP]に移動します。

ステップ11: EncryptionTemplate、GeneralPurposeTemplate、およびSignatureTemplateレジストリを編集して、新しく作成された証明書テンプレートを指定します。



ステップ12:NDESサーバをリブートし、[Certification Authority]ウィンドウに戻り、サーバ名を選択し、[Stop and Play]ボタンを簡潔に選択します。

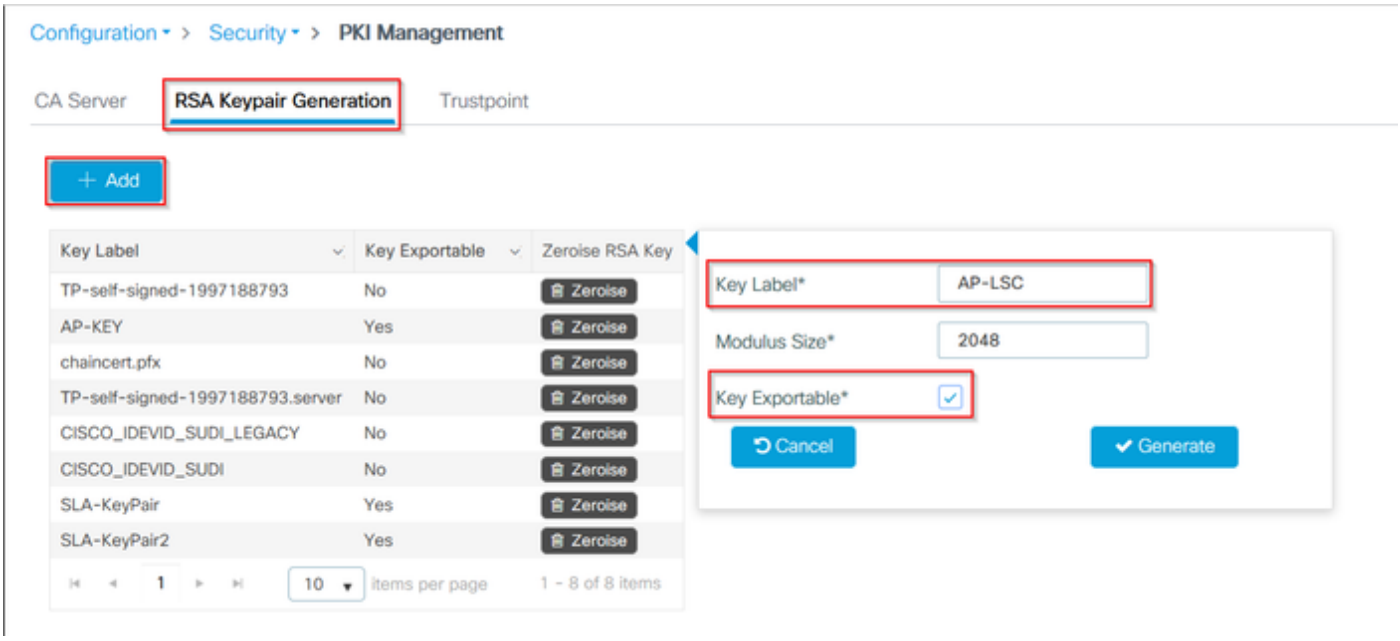


9800デバイスのトラストポイントの設定

コントローラは、APがプロビジョニングされたら、APを認証するためにトラストポイントを定義する必要があります。トラストポイントには、同じCAサーバ（この例ではMicrosoft CA）から取得したCAルート証明書とともに、9800デバイス証明書が含まれます。 証明書をトラストポイントにインストールするには、サブジェクト属性とそれに関連付けられたRSA鍵のペアが含まれている必要があります。設定は、Webインターフェイスまたはコマンドラインを使用して実行されます。

ステップ1:[Configuration] > [Security] > [PKI Management]に移動し、[RSA Keypair Generation]タブを選択します。[+ Add]ボタンを選択します。

ステップ2：キーペアに関連付けられたラベルを定義し、[エクスポート可能(Exportable)]チェックボックスが選択されていることを確認します。



ステップ1と2のCLI設定。この設定例では、ラベルAP-LSCとモジュラスサイズ2048ビットでキーペアが生成されます。

```
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)
```

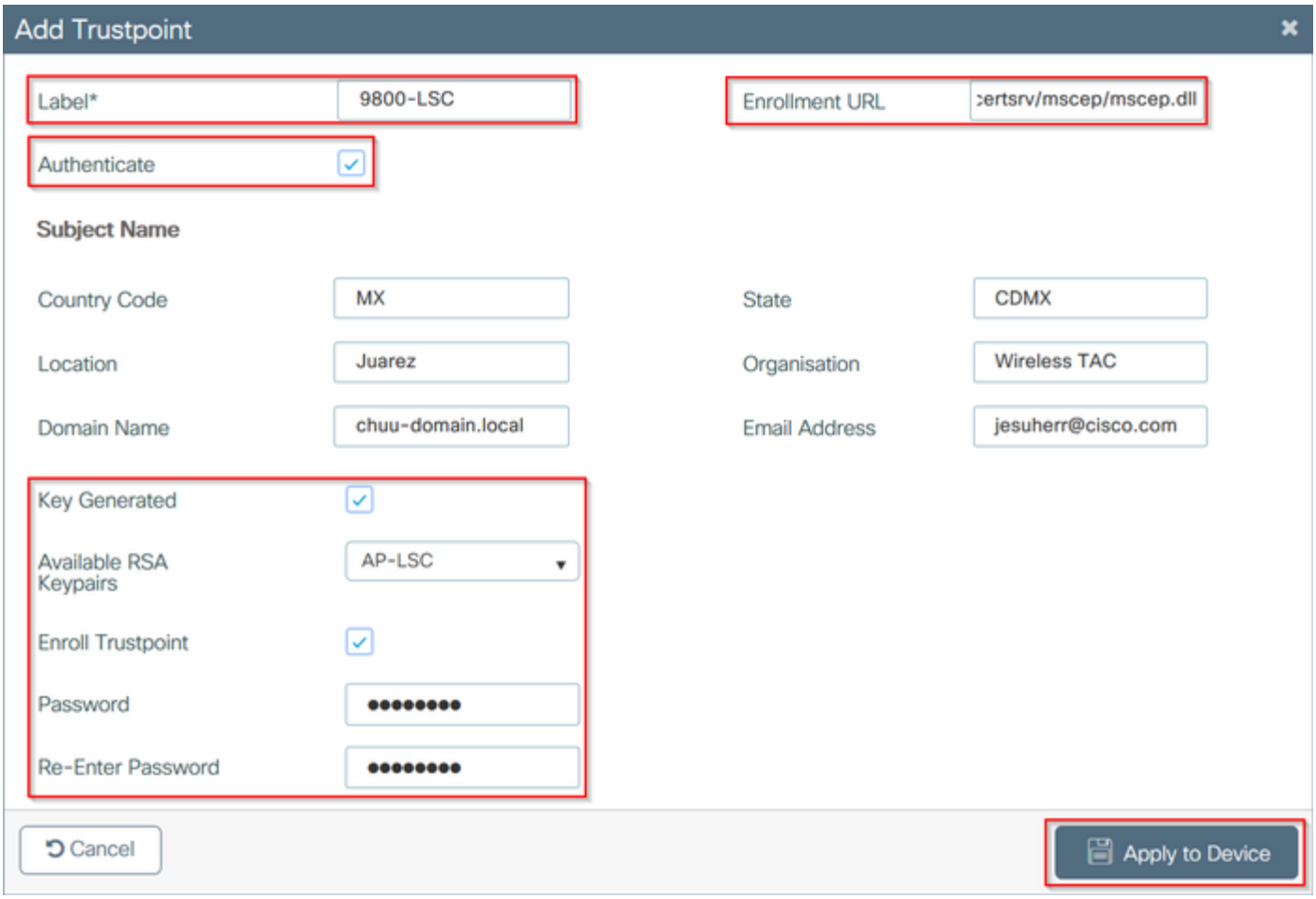
ステップ3:同じセクション内で、[トラストポイント]タブを選択し、[+ Add]ボタンを選択します。

ステップ4:トラストポイントの詳細にデバイス情報を入力し、[Apply to Device]を選択します。

- [Label] フィールドは、トラストポイントに関連付けられた名前です
- 登録URLの場合は、「Windows ServerでSCEPサービスを有効にする」セクションのステップ7で定義したURLを使用します
- [Authenticate]チェックボックスをオンにし、CA証明書をダウンロードします
- [ドメイン名]フィールドは、証明書要求の共通名属性として配置されます

- [Key Generated]チェックボックスをオンにすると、ドロップダウンメニューが表示され、ステップ2で生成されたキーペアが選択されます
- [Enroll Trustpoint]チェックボックスをオンにすると、2つのパスワードフィールドが表示されます。パスワードを入力します。これは、デバイス証明書とCA証明書で証明書キーをチェーンするために使用されます

警告：9800コントローラはLSCインストールの多層サーバチェーンをサポートしていないため、ルートCAは、コントローラとAPからの証明書要求に署名するルートCAである必要があります。



ステップ3と4のCLI設定：

注意：subject-name設定行は、LDAP構文でフォーマットする必要があります。フォーマットしない場合、コントローラで受け入れられません。

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

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

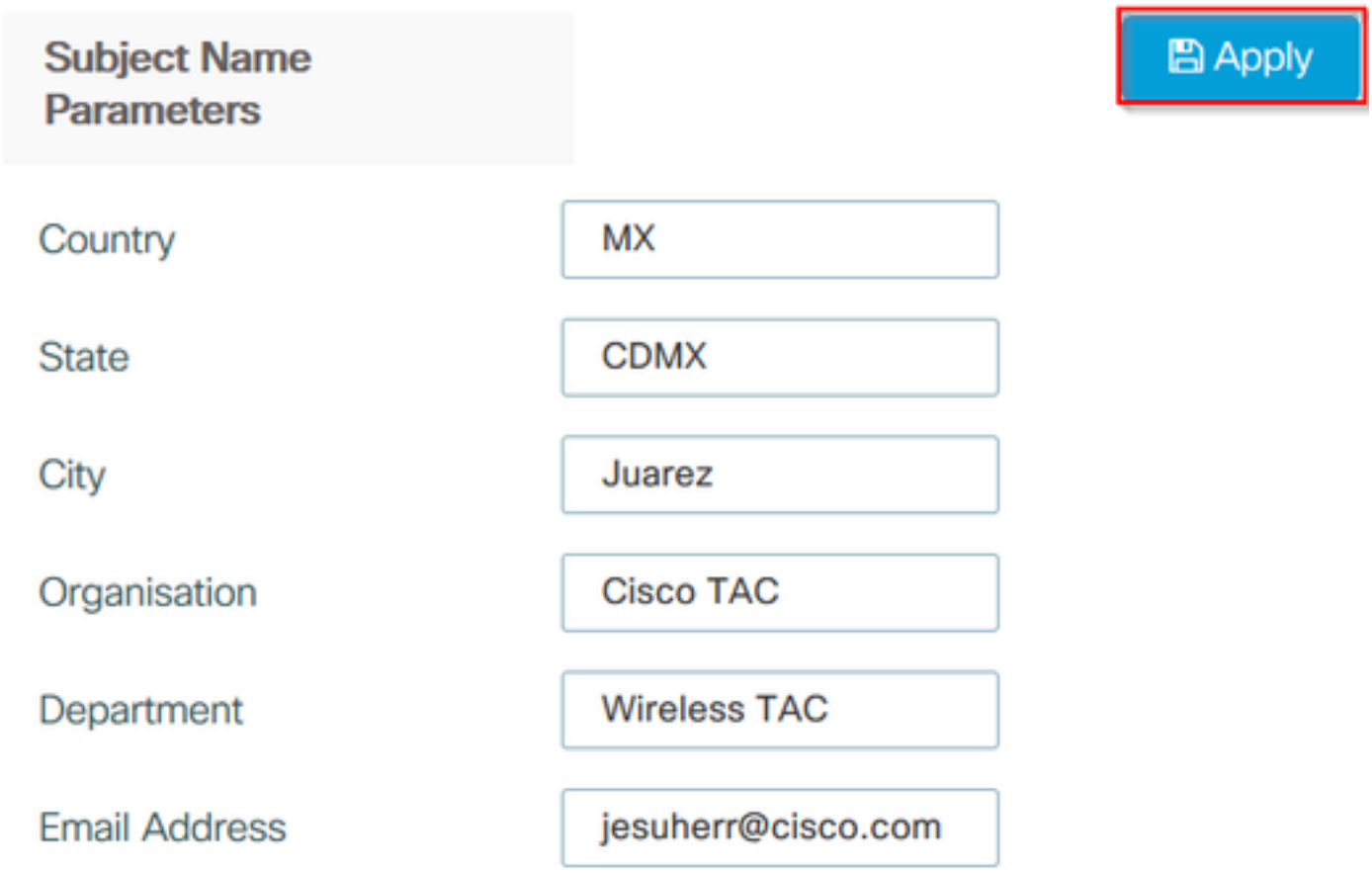
```
9800-L(ca-trustpoint)#subject-name C=



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.
```

AP登録パラメータと更新管理トラストポイントの定義

AP登録では、以前に定義したトラストポイントの詳細を使用して、コントローラが証明書要求を転送するサーバの詳細を決定します。コントローラは証明書登録のプロキシとして使用されるため、証明書要求に含まれるサブジェクトのパラメータを認識する必要があります。設定は、Webインターフェイスまたはコマンドラインを使用して実行されます。

ステップ1:[Configuration] > [Wireless] > [Access Points]に移動し、[LSC Provision]メニューを展開します。

ステップ2:AP証明書要求に**入力された属性**を[Subject Name Parameters]に入力し、[**Apply**]を選択します。

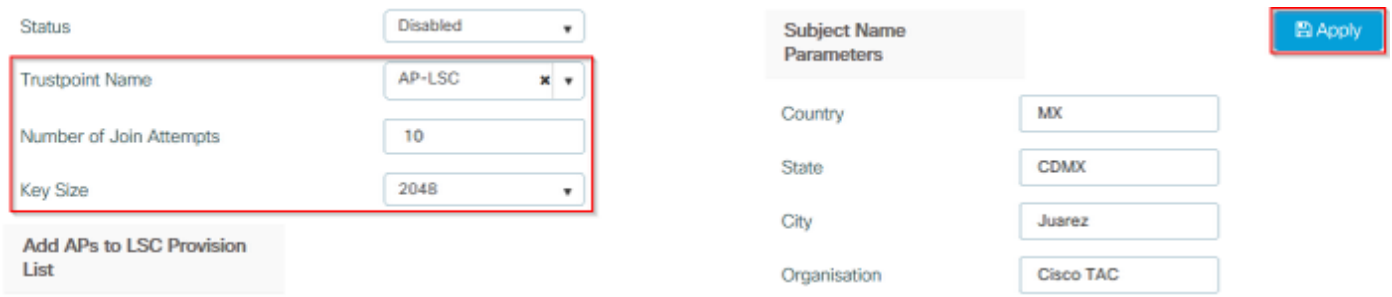


ステップ1と2のCLI設定：

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

> **注**:9800 WLCでは属性が検証されないため、国番号などの2文字に制限されたサブジェクト名パラメータは厳密に尊重する必要があります。
> 詳細については、不具合CSCvo72999を参照してください 参照として

ステップ3：同じメニュー内で、ドロップダウンリストから以前に定義したトラストポイントを選択し、AP加入の試行回数（MICを再度使用する前の加入試行回数を定義します）を指定し、証明書キーサイズを設定します。次に、[Apply] をクリックします。



ステップ3のCLI設定：

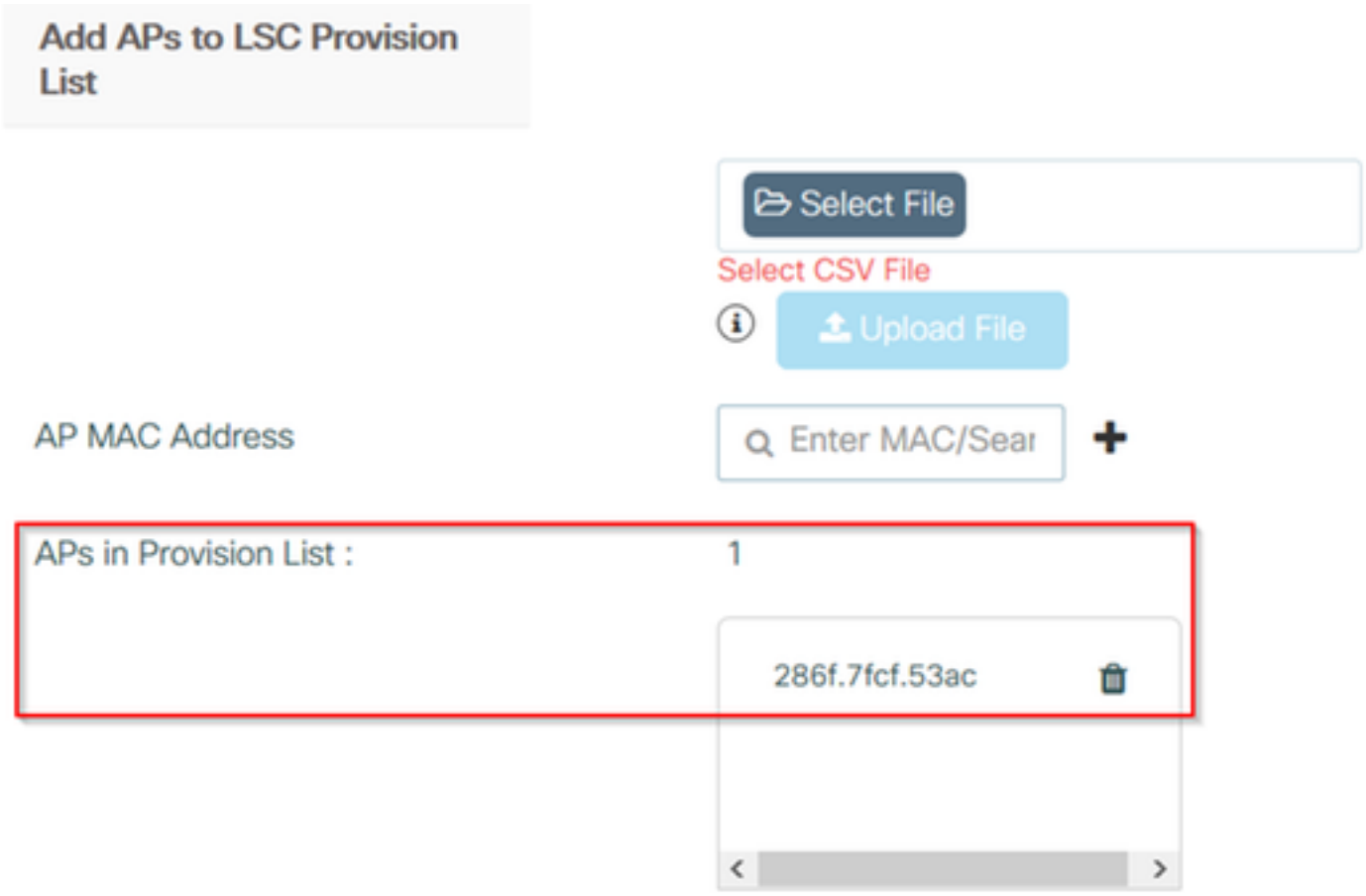
```
9800-L(config)#ap lsc-provision join-attempt
```

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

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

ステップ4:（オプション）コントローラに加入しているすべてのAPまたはMACアドレスリストに定義されている特定のAPに対して、AP LSCプロビジョニングをトリガーできます。同じメニューで、テキストフィールドにAPイーサネットMACアドレスをxxxx.xxxx.xxxxの形式で入力し、+記号をクリックします。または、APのMACアドレスを含むcsvファイルをアップロードし、ファイルを選択してから[ファイルのアップロード]を選択します。

> **注**：コントローラは、CSVファイル内で、参加しているAPリストから認識されないMACアドレスをスキップします。



ステップ4のCLI設定：

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

ステップ 5： [Status]ラベルの横のドロップダウンメニューから[Enabled]または[Provision List]を選択して、[Apply to Trigger AP LSC enrollment]をクリックします。

> **注：**APは、証明書要求、ダウンロード、およびインストールを開始します。証明書が完全にインストールされると、APはリブートし、新しい証明書を使用して加入プロセスを開始します。

> **ヒント**：プロビジョンリストとともに実稼働前のコントローラを使用してAP LSCプロビジョニングを行う場合は、証明書がプロビジョニングされたらAPエントリを削除しないでください。これを行い、APがMICにフォールバックして同じ実稼働前コントローラに加入すると、LSC証明書が消去されます。

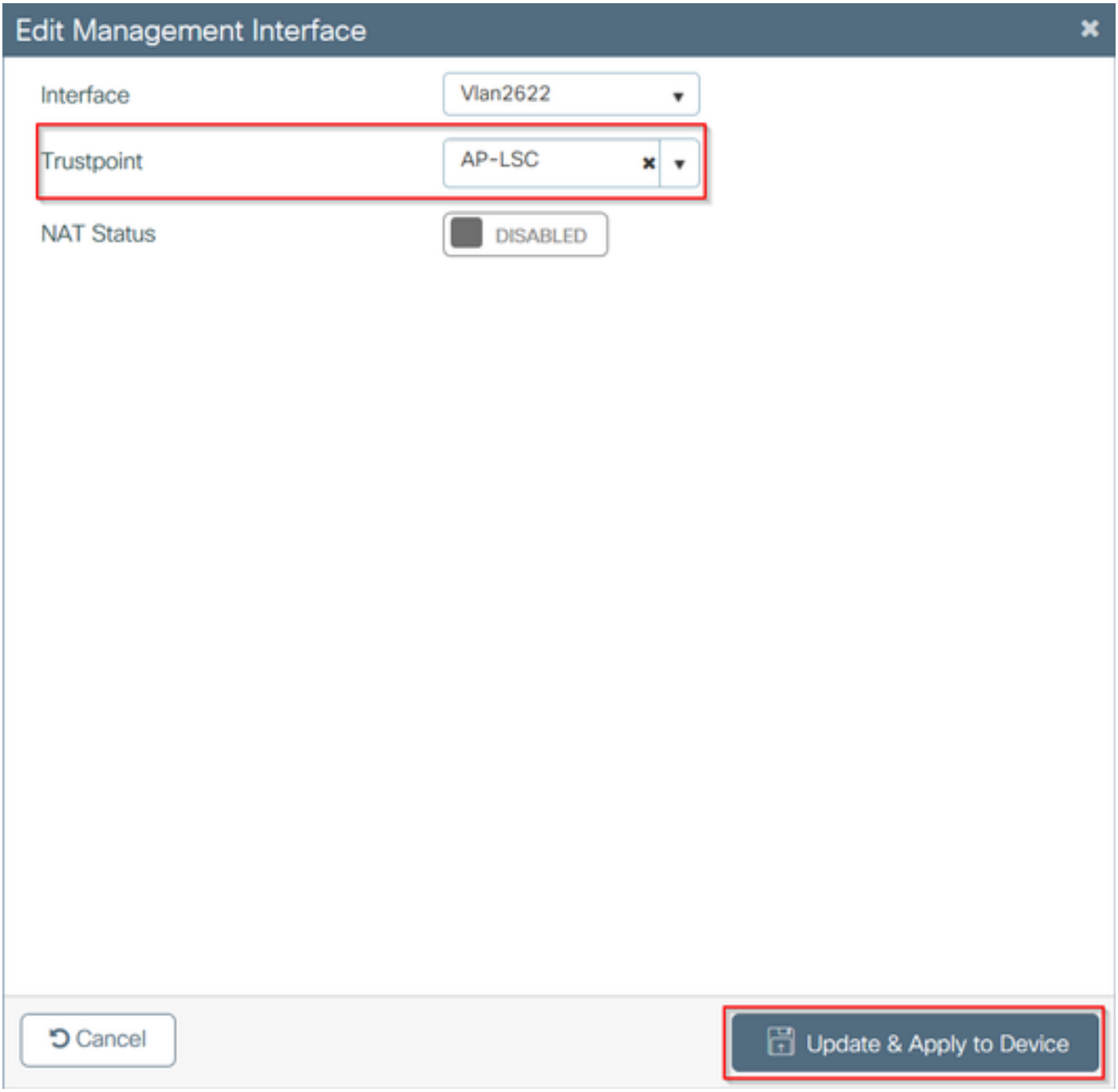
ステップ5のCLI設定：

```
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
```

ステップ6:[Configuration] > [Interface] > [Wireless]に移動して、管理インターフェイスを選択します。[トラストポイント]フィールドで、ドロップダウンメニューから新しいトラストポイントを選択し、[Update & Apply to Device]をクリックします。

> **注意**：LSCが有効で、9800 WLCのトラストポイントがMICまたはSSCを参照している場合、APは設定された数の加入の試行に対してLSCへの加入を試行します。最大試行回数に達すると、APはMICにフォールバックして再度参加しますが、LSCプロビジョニングが有効になっているため、APは新しいLSCを要求します。これにより、CAサーバが同じAPに対して常に証明書に署名し、APがjoin-request-rebootループに留まるというループが発生します。

> **注：**LSC証明書を使用するように管理トラストポイントが更新されると、新しいAPはMICを使用してコントローラに参加できなくなります。現在、プロビジョニングウィンドウを開くサポートはありません。新しいAPをインストールする必要がある場合は、管理トラストポイント内のAPと同じCAによって署名されたLSCを事前にプロビジョニングしておく必要があります。



ステップ6のCLI設定：

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

確認

コントローラ証明書のインストールの確認

9800 WLCトラストポイントにLSC情報があることを確認するために、**show crypto pki certificates verbose <trustpoint name>コマンドを発行します。**2つの証明書が、LSCのプロビジョニングと登録のために作成されたトラストポイントに関連付けられます。この例では、トラスト

ポイント名は「microsoft-ca」です（関連する出力だけが表示されます）。

```
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
```

9800 WLC LSC設定の確認

ワイヤレス管理トラストポイントに関する詳細を確認するには、**show wireless management trustpointコマンドを実行し**て、正しいトラストポイント（LSCの詳細を含むトラストポイント、この例ではAP-LSC）が使用中であり、[Available:

```
9800-L#show wireless management trustpoint

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

AP LSCプロビジョニング設定に関する詳細を、プロビジョンリストに追加されたAPのリストと

ともに確認するには、show ap lsc-provision summaryコマンドを実行します。正しいプロビジョニング状態が表示されていることを確認します。

```
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
```

アクセスポイント証明書のインストールの確認

APにインストールされている証明書を確認するには、AP CLIからshow cryptoコマンドを実行し、CAルート証明書とデバイス証明書の両方が存在することを確認します（出力には関連するデータだけが表示されます）。

```
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)
```

スイッチポートdot1x認証用のLSCが使用されている場合、APからポート認証が有効になっているかどうかを確認できます。

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

> **注**：APのポートdot1xを有効にするには、APプロファイルまたはダミー値を使用したAP設定自体で、APのdot1xクレデンシャルを定義する必要があります。

トラブルシュート

一般的な問題

1. テンプレートがサーバレジストリに正しくマッピングされていない場合、またはサーバにパスワードのチャレンジが必要な場合は、9800 WLCまたはAPの証明書要求は拒否されます。
2. IISのデフォルトサイトが無効になっている場合、SCEPサービスも無効になっているため、トラストポイントで定義されたURLに到達できず、9800 WLCは証明書要求を送信しません。
3. サーバと9800 WLCの間で時刻が同期されていない場合、時刻の妥当性チェックが失敗するため、証明書はインストールされません。

debugおよびlogコマンド

9800コントローラ証明書の登録をトラブルシューティングするには、次のコマンドを使用します。

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

AP登録のトラブルシューティングと監視には、次のコマンドを使用します。

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

APコマンドラインから、**show logging**は、APに証明書のインストールに問題があったかどうかを表示し、証明書がインストールされなかった理由の詳細を表示します。

```
[...]
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]
```

登録の成功例

これは、コントローラとそれに関連するAPの両方の登録が成功した場合の、前述のデバッグの出力です。

9800 WLCへのCAルート証明書のインポート：

```
[...]
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デバイス登録：

```
[...]
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

コントローラ側からのAP登録デバッグ出力では、9800 WLCに加入しているAPごとに、次の出力が複数回繰り返されます。

[...]
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
```

AP側からのAP登録デバッグ出力：

```
[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
```

これで、SCEPによるLSC登録の設定例は終了です。