Configure SCEP for Locally Significant Certificate Provisioning on 9800 WLC

Contents

Introduction

This document describes how to configure the 9800 Wireless LAN Controller (WLC) for Locally Significant Certificate (LSC) enrollment for Access Point (AP) join purposes through the Microsoft Network Device Enrollment Service (NDES) and Simple Certificate Enrollment Protocol (SCEP) features within Windows Server 2012 R2 Standard.

Prerequisites

In order to successfully perform SCEP with the Windows Server, the 9800 WLC must meet these requirements:

- There must be reachability between the controller and the server.
- The controller and the server are synchronized to the same NTP server, or share the same date and timezone (If the time is different between the CA server and the time from the AP, the AP has issues with certificate validation and installation).

The Windows Server must have the Internet Information Services (IIS) previously enabled.

Requirements

Cisco recommends that you have knowledge of these technologies:

- 9800 Wireless LAN Controller version 16.10.1 or higher.
- Microsoft Windows Server 2012 Standard.
- Private Key Infrastructure (PKI) and certificates.

Components Used

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

- 9800-L WLC software version 17.2.1.
- Windows Server 2012 Standard R2.
- 3802 Access Points.

> **Note**: The server side configuration in this document is specifically WLC SCEP, for additional strengthten, security, and certificate server configurations please refer to Microsoft TechNet.

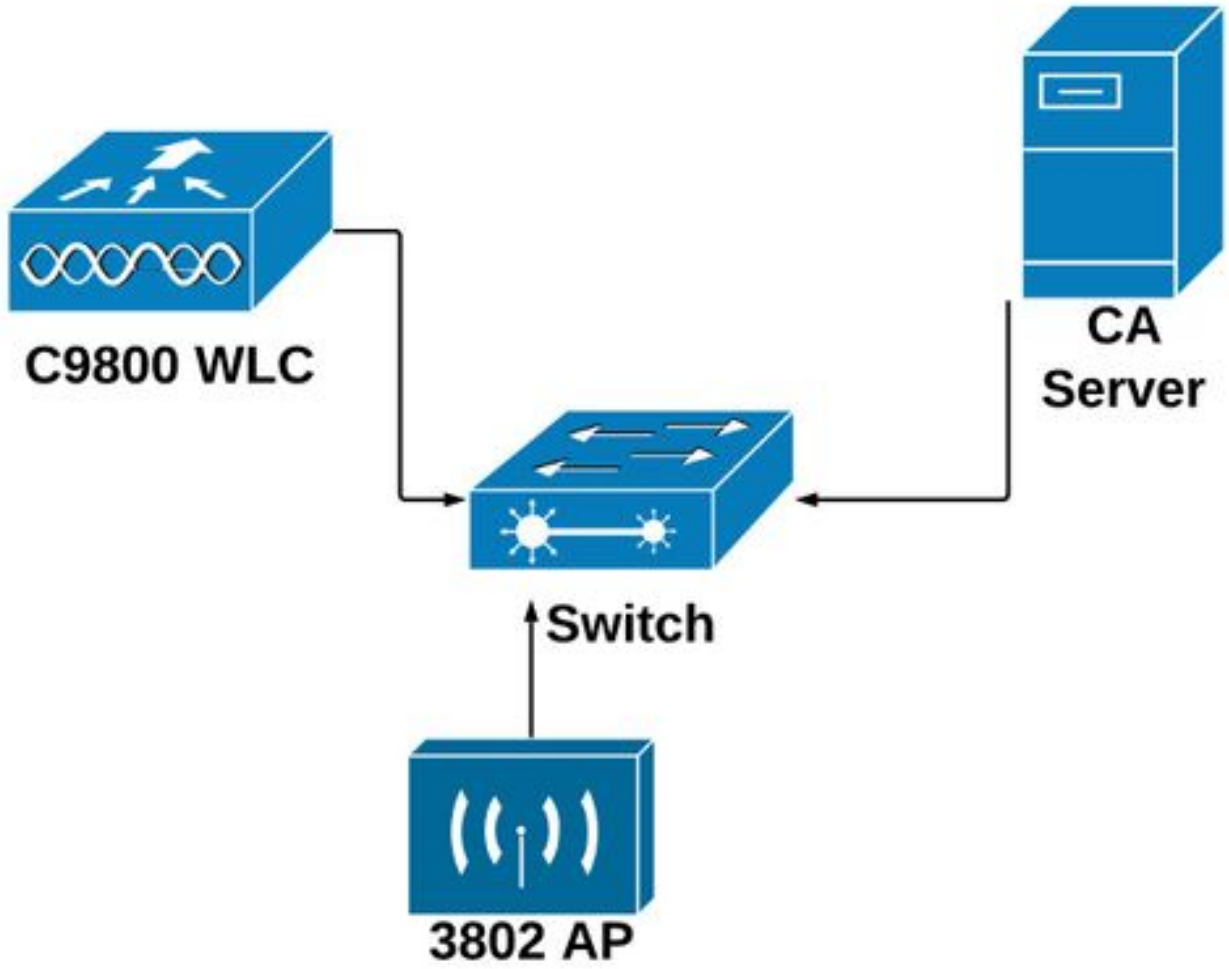
Background Information

The new LSC certificates, both Certificate Authority (CA) root certificate and device certificate, must be installed on the controller to eventually download it in the APs. With SCEP, the CA and device certificates are received from the CA server, and later installed automatically in the controller.

The same certification process takes place when the APs are provisioned with LSCs; to do so, the controller acts as a CA-proxy and help to get the certificate request (self-generated) signed by the CA for the AP.

Configure

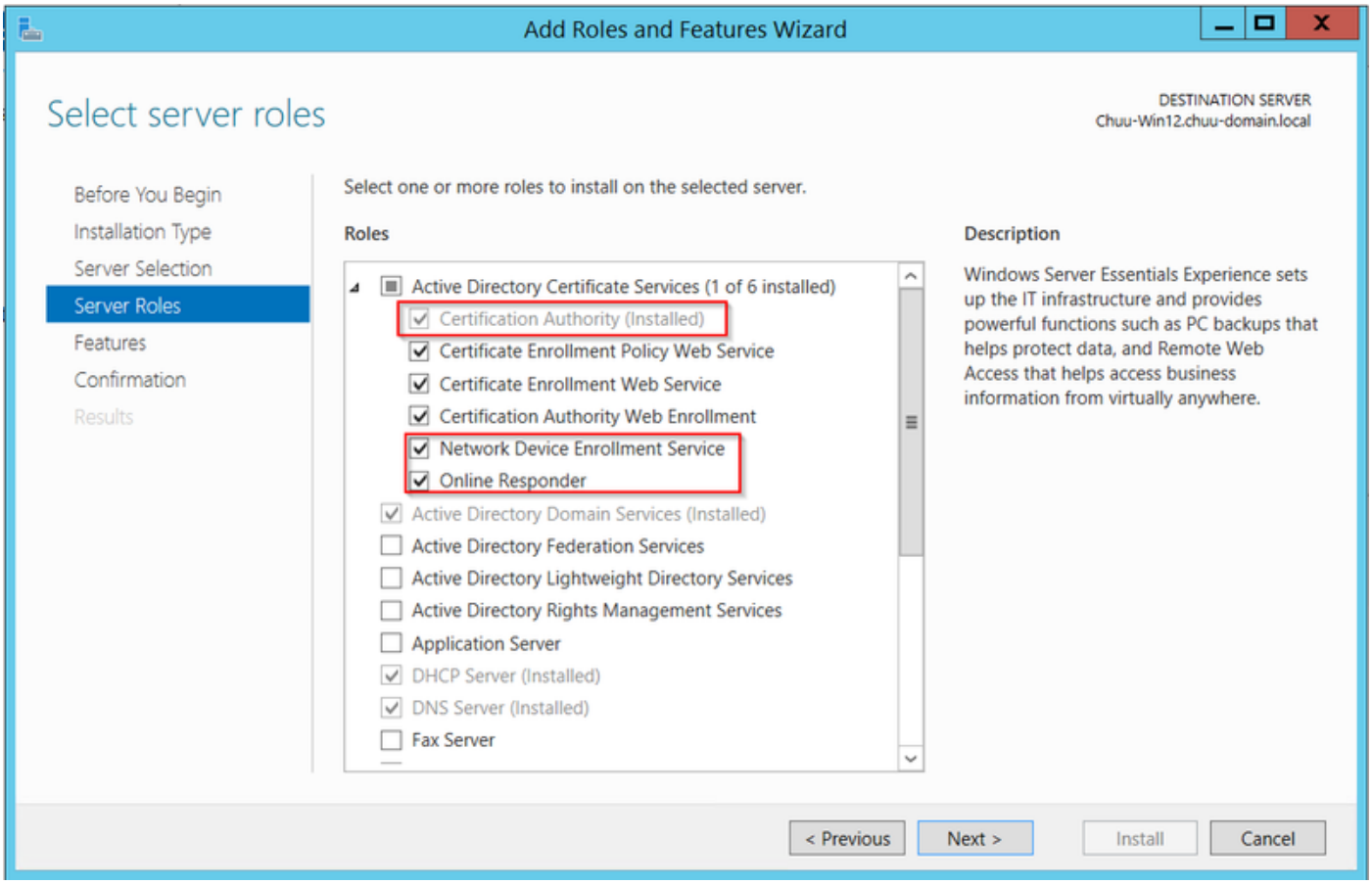
Network Diagram



Enable SCEP Services in the Windows Server

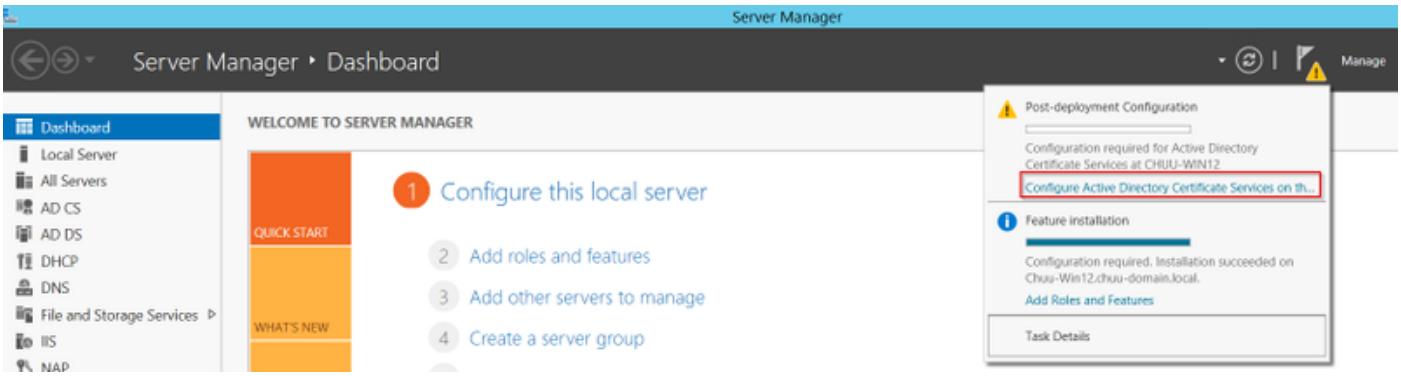
Step 1. In the **Server Manager** application, select the **Manage** menu and then select the **Add Roles and Features** option to open the role Add Roles and Features Configuration Wizard. From there, select the server instance that is used for SCEP server enrollment.

Step 2. Verify that the **Certification Authority**, **Network Device Enrollment Service**, and **Online Responder** features are selected, and then select **Next**:



Step 3. Select **Next** twice, and then **Finish** to end the configuration Wizard**.** Wait for the server to complete the feature installation process, then select **Close** to close the Wizard.

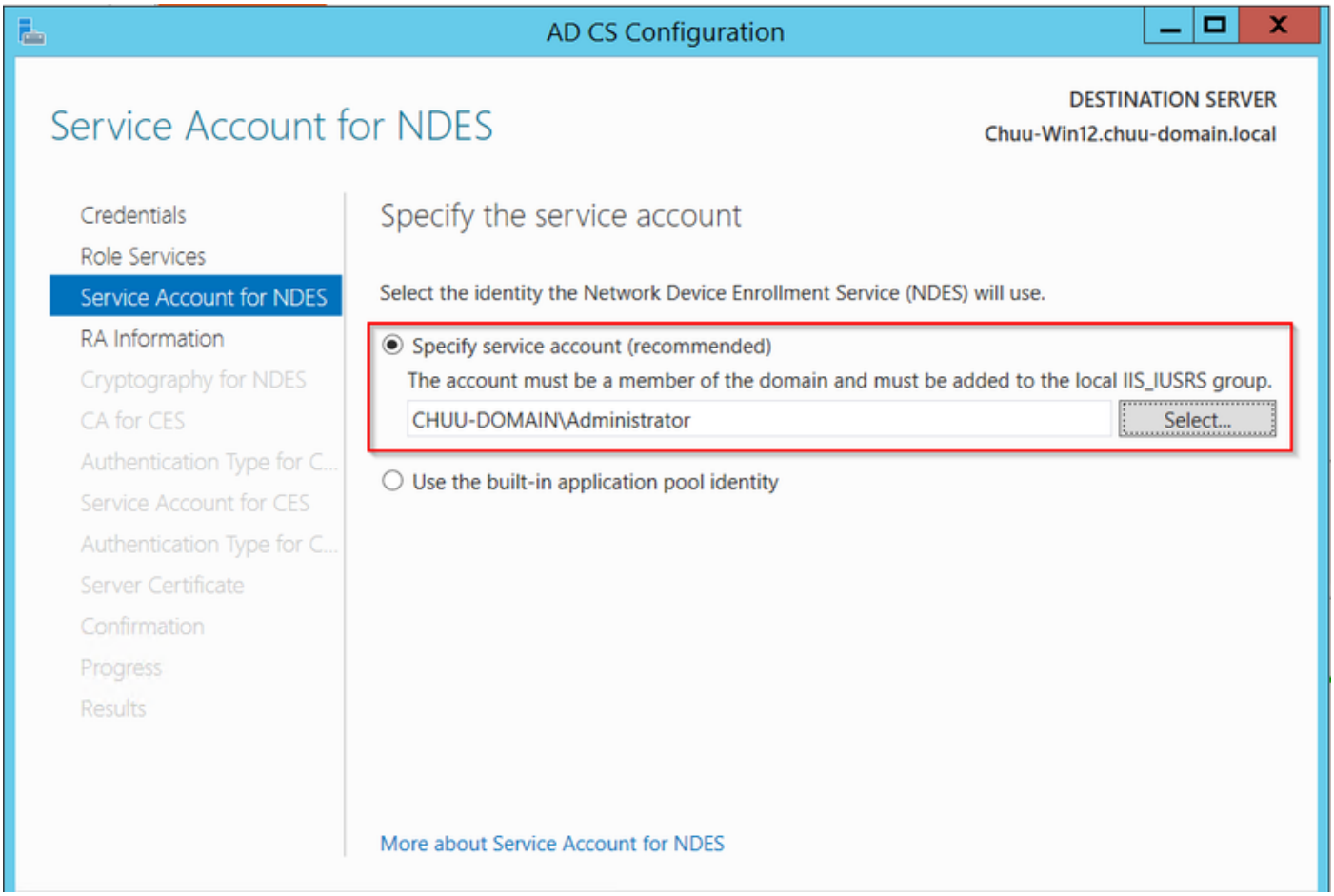
Step 4. Once the installation is done, a warning icon shows in the Server Manager Notification icon. Select it and select the **Configure Active Directory Services on the destination server** option link to lauch the **AD CS Configuration** wizard menu.



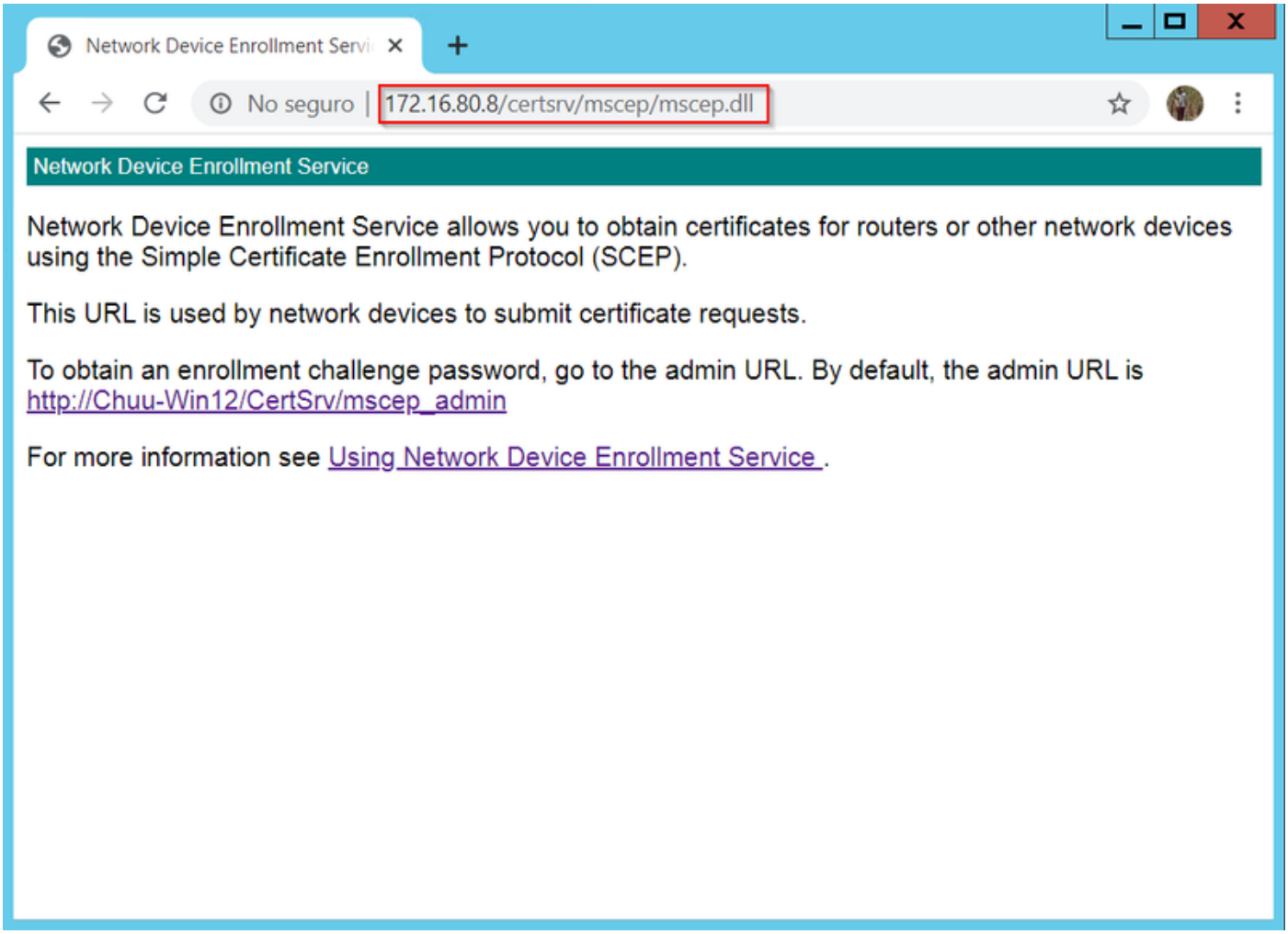
Step 5. Select the **Network Device Enrollment Service**, and **Online Responder** role services to be configured in the menu, then select **Next**.

Step 6. In the **Service Account for NDES** select either option between the built-in application pool or the service account, then select **Next**.

Note: If service account, make sure that the account is part of the **IIS_IUSRS** group.



Step 7. Select **Next** for the next screens, and let the installation process finish. After the installation, the SCEP url is available with any web brower. Navigate to the URL **http://<server ip>/certsrv/mscep/mscep.dll** to verify that the service is available.



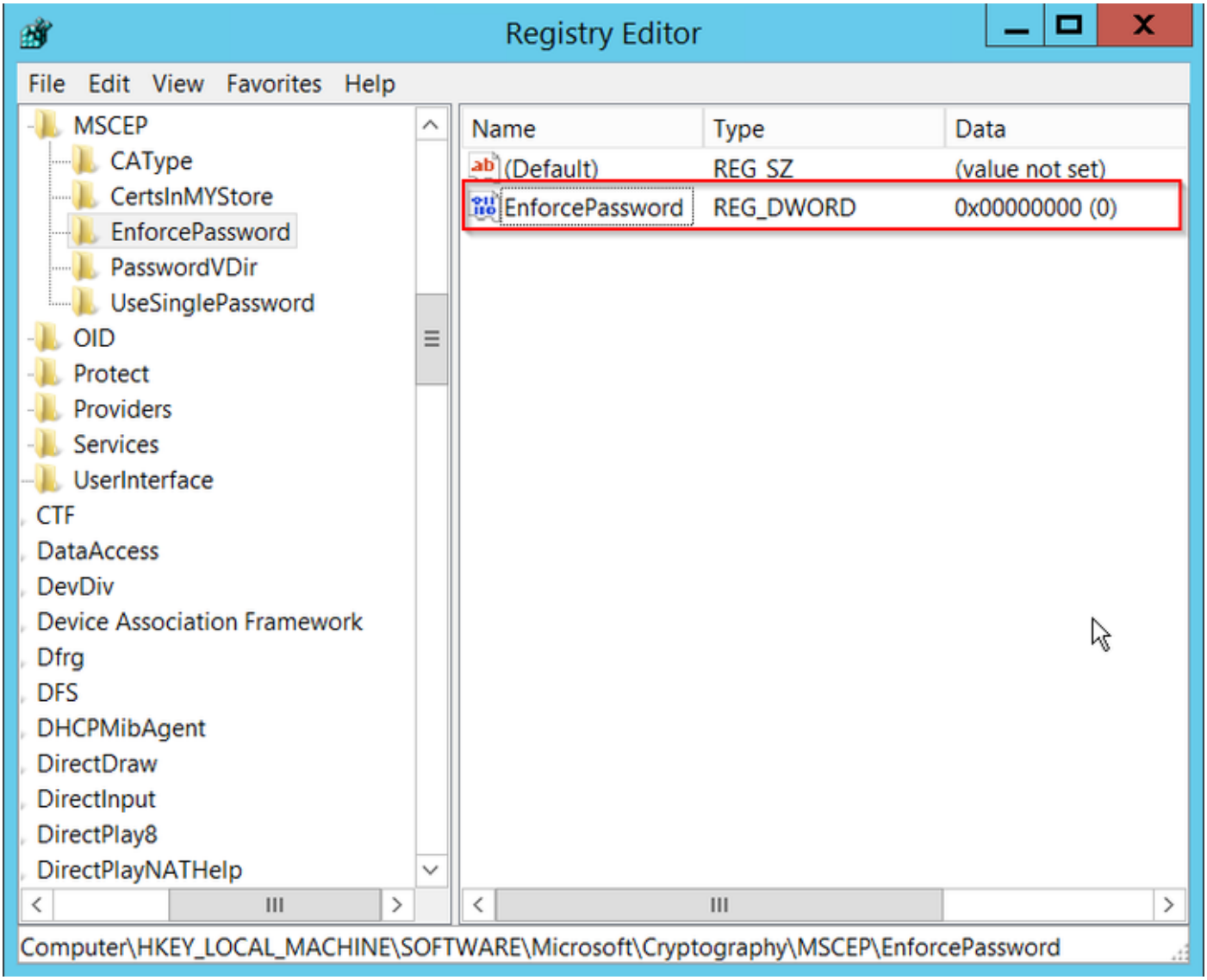
Disable SCEP Enrollment Challenge Password Requirement

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

Step 1. Open the Registry Editorm, search for **Regedit** within the **Start** menu.

Step 2. Navigate to **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword**

Step 3. Change the **EnforcePassword** value to 0. If it is already 0, then leave it as is.



Configure the Certificate Template and Registry

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

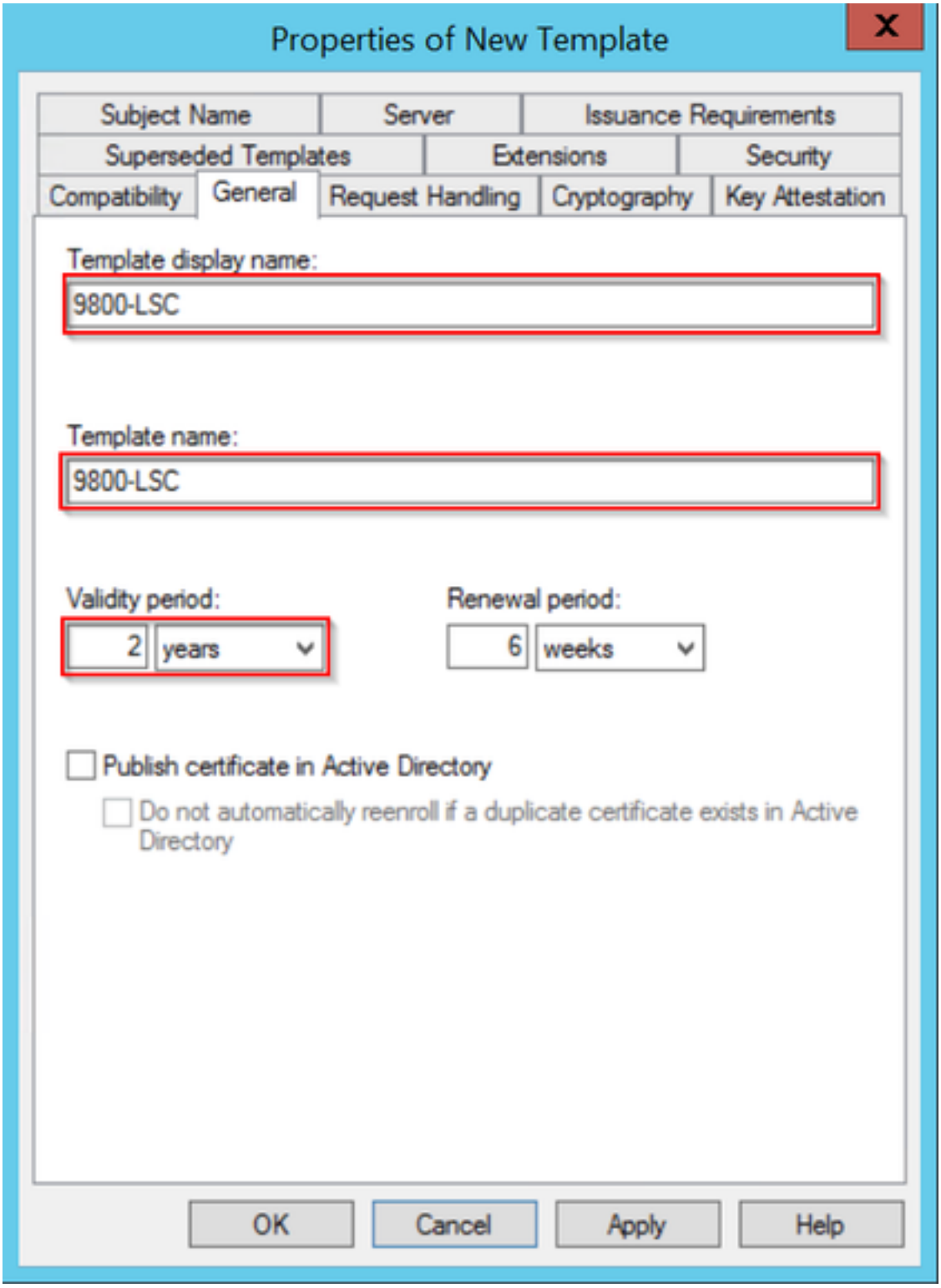
Step 1. Navigate to **Start > Administrative Tools > Certification Authority**.

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

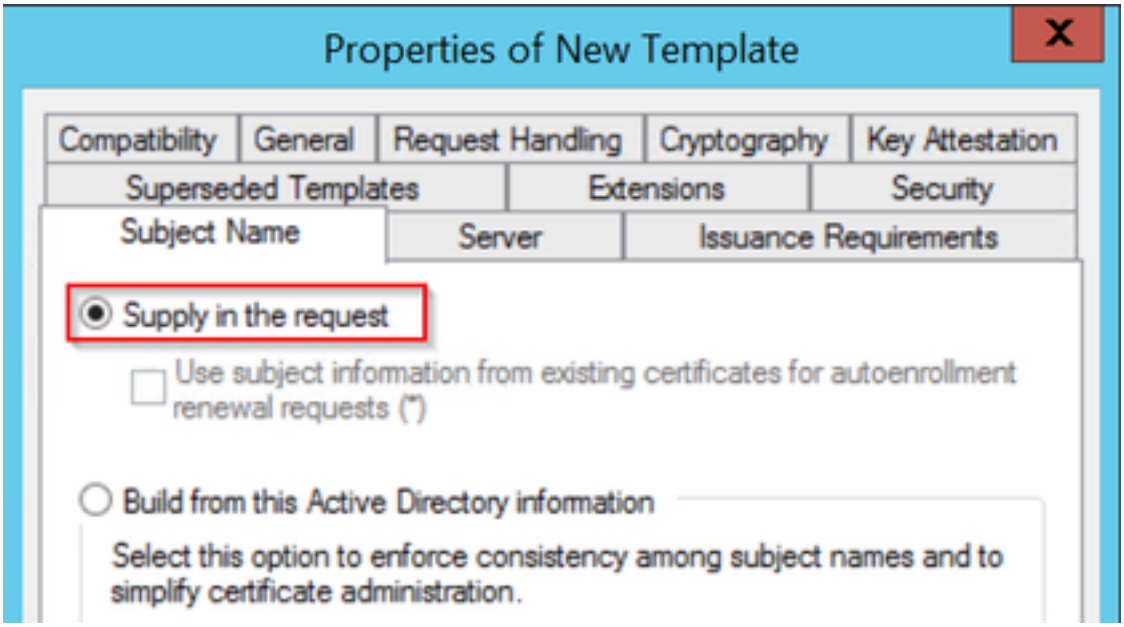
Step 3. Right-click on the **Users** certificate template, then select **Duplicate Template** in the context menu.

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

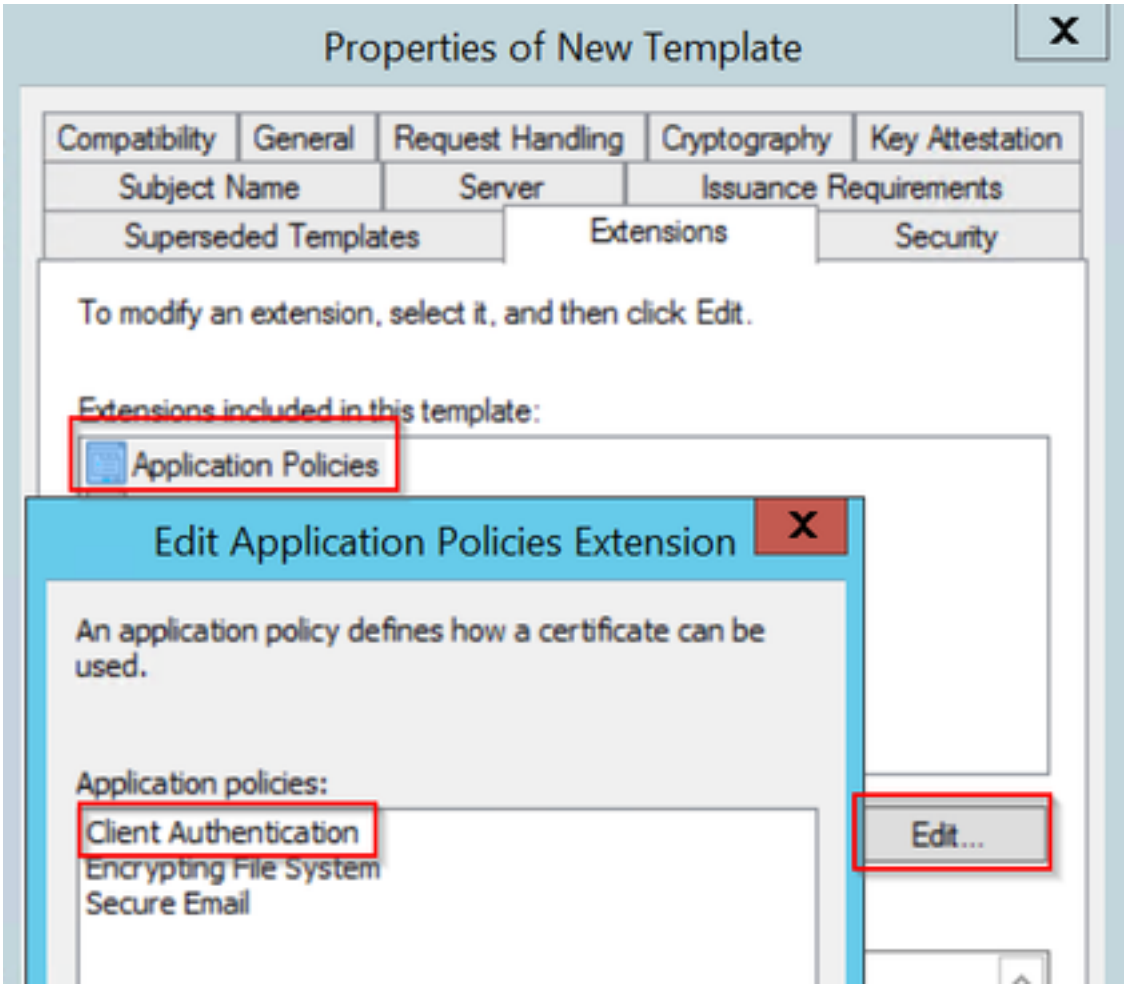
> **Caution**: When the Validity period is modified, ensure that it is not greater than the Certification Authority root certificate validity.



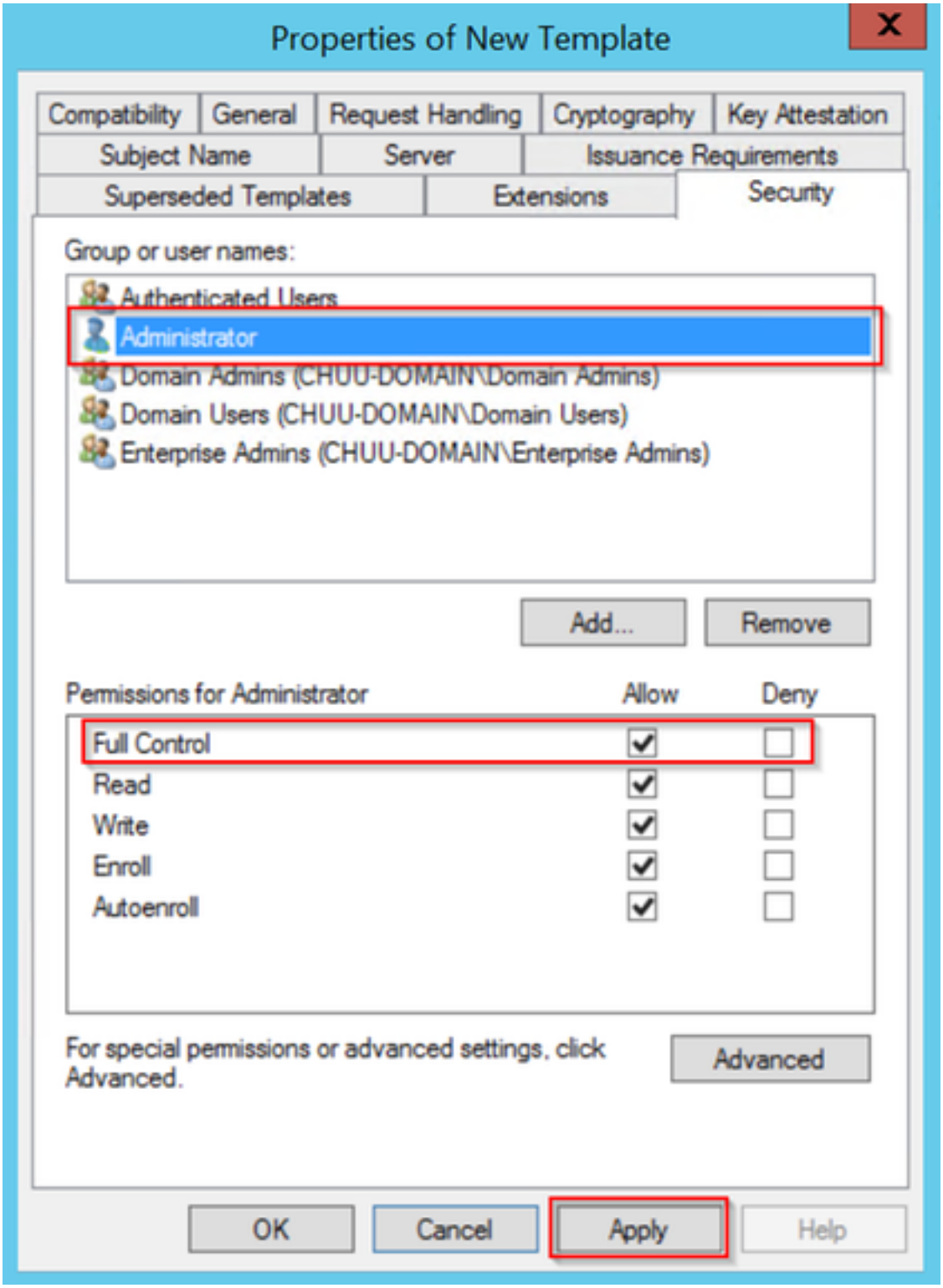
Step 5. Navigate to the **Subject Name** tab, ensure that **Supply in the request** is selected. A pop-up appears to indicate that users do not need admin approval to get their certificate signed, select **OK**.



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



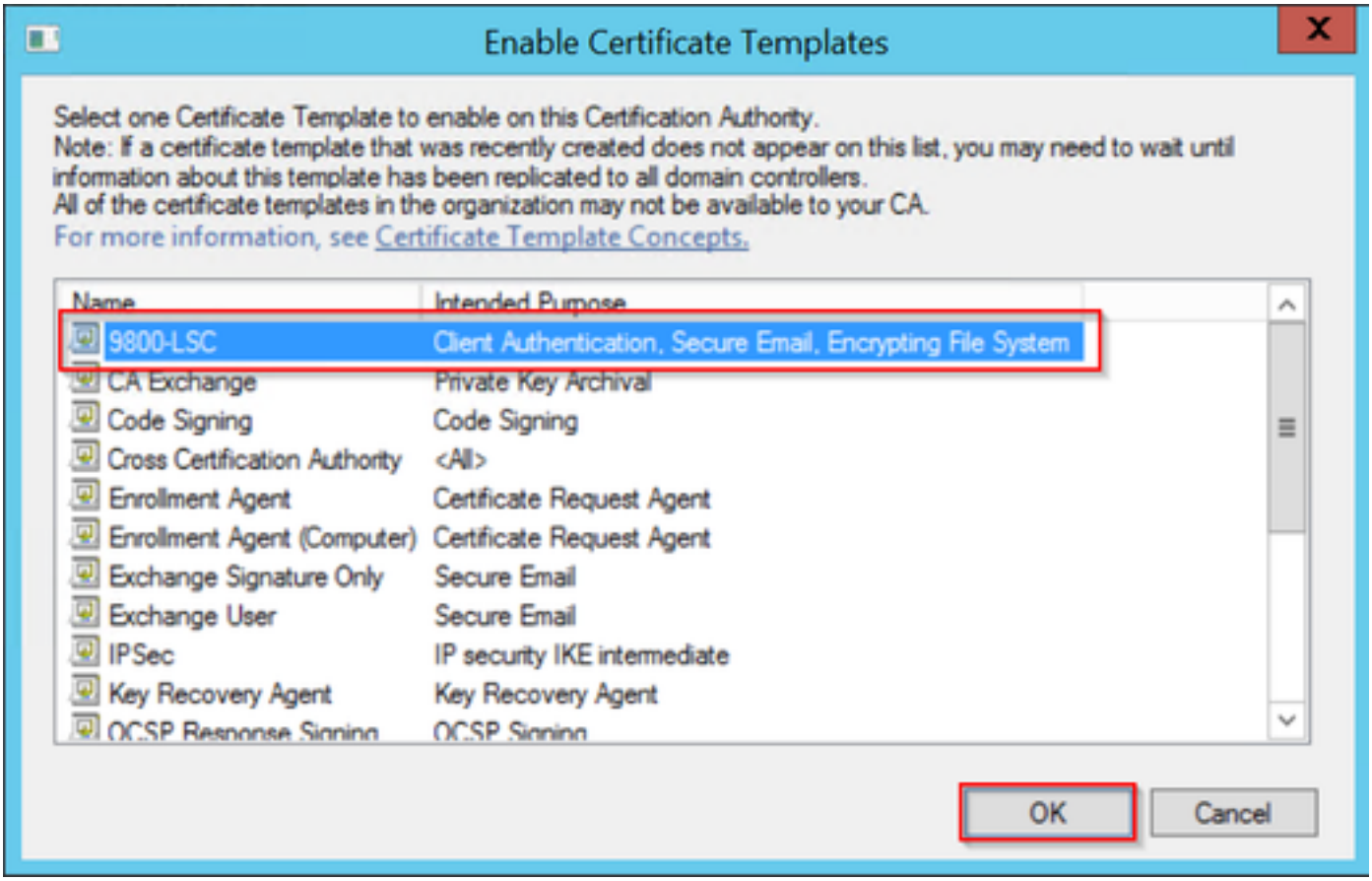
Step 7. Navigate to the **Security** tab, ensure that the service account defined in Step 6 of the **Enable SCEP Services in the Windows Server** has **Full Control** permissions of the template, then select **Apply** and **OK**.



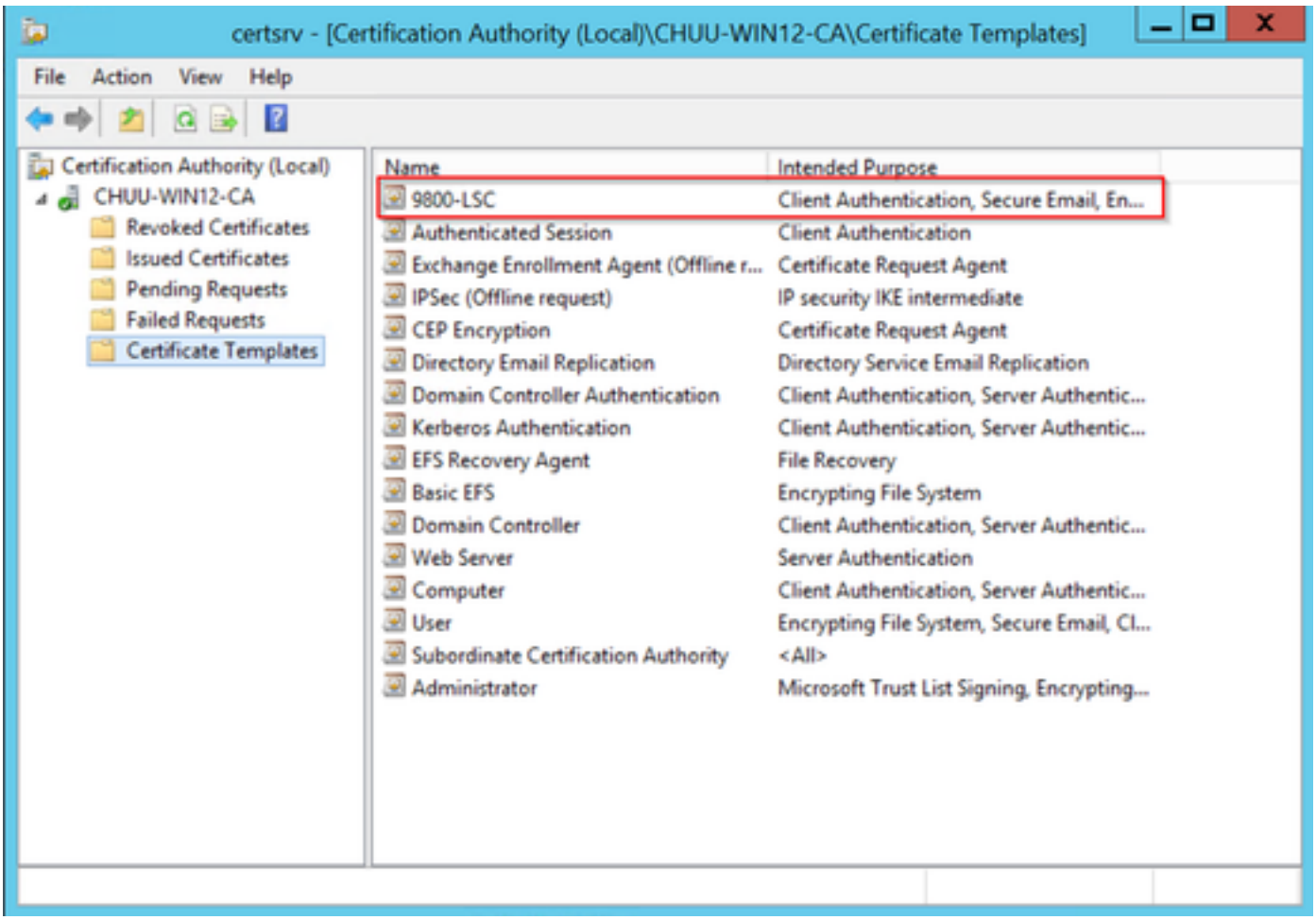
Step 8. Return to the **Certification Authority** window, right-click in the **Certificate Templates** folder and select **New > Certificate Template to Issue**.

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

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



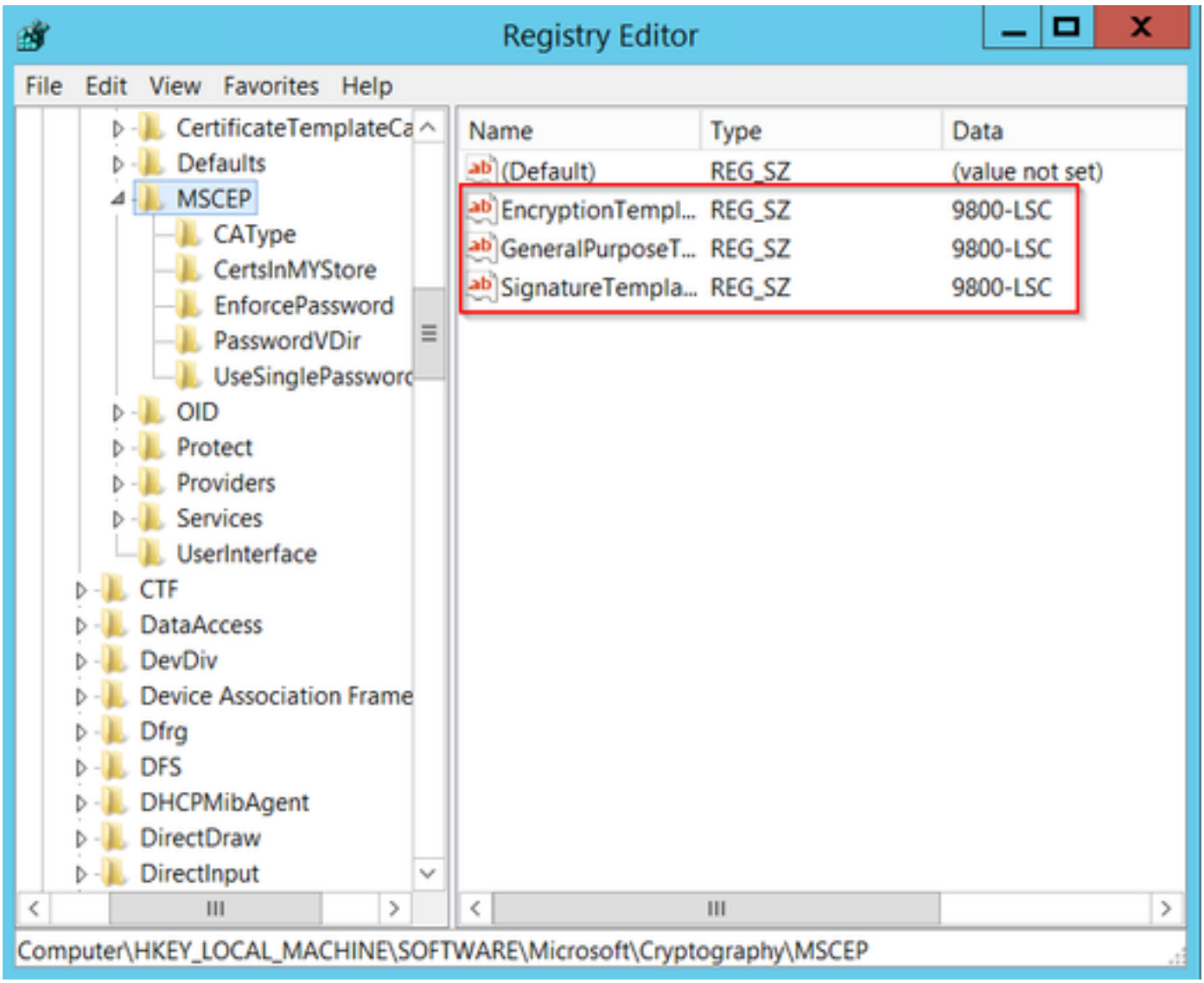
The new certificate template is listed now within the **Certificate Templates** folder content.



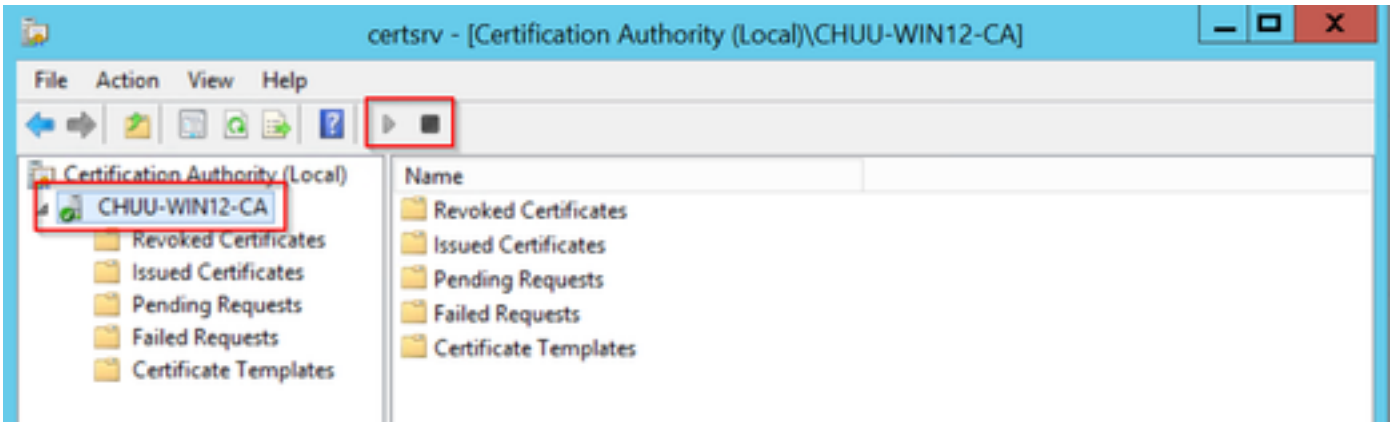
Step 10. Return to the **Registry Editor** window and navigate to **Computer >**

HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

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



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



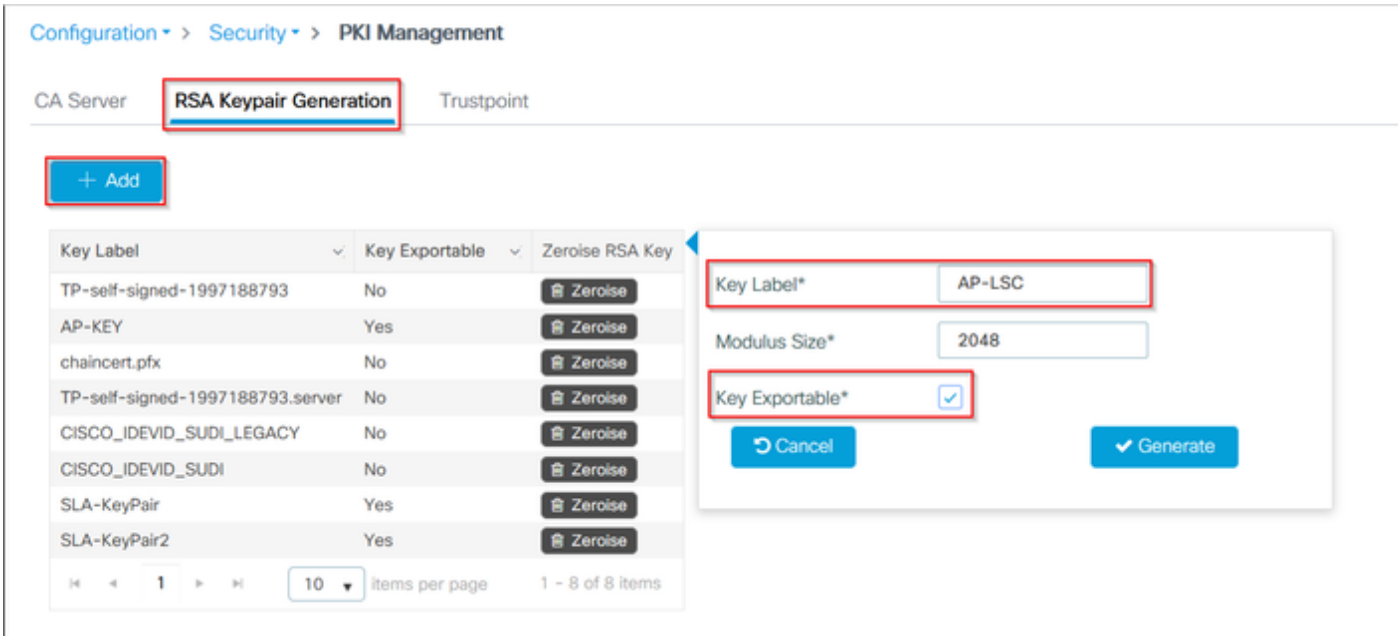
Configure the 9800 Device Trustpoint

The controller needs to have a trustpoint defined to authenticate APs once they have been

provisioned. The trustpoint includes the 9800 device certificate, along with the CA root certificate both obtained from the same CA server (Microsoft CA in this example). For a certificate to be installed in the trustpoint, it must contain the subject attributes along with a pair of RSA keys associated to it. The configuration is performed either throught the web interface or the command line.

Step 1. Navigate to **Configuration > Security > PKI Management** and select the **RSA Keypair Generation** tab. Select the **+ Add** button.

Step 2. Define a label associated with the keypair, and ensure that the **Exportable** checkbox is selected.



CLI configuration for steps one and two, in this configuration example the keypair is generated with label AP-LSC and modulus size of 2048 bits:

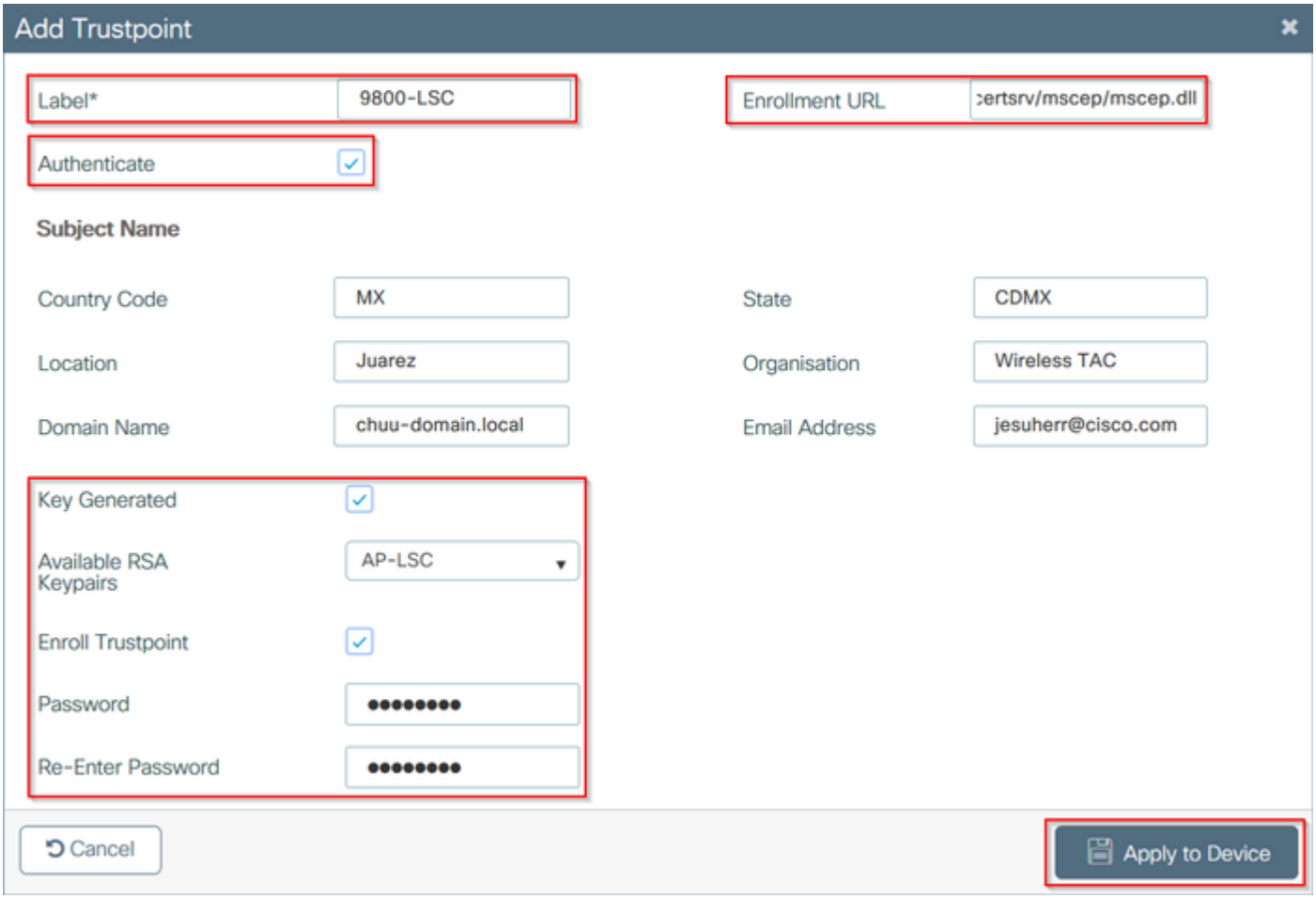
```
9800-L(config)#crypto key generate rsa exportable general-keys modulus <modulus size> label
<label name>
The name for the keys will be: AP-LSC

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

Step 3. Within the same section, select the **Trustpoint** tab, and select the **+ Add** button.

Step 4. Fill out the trustpoint details with the device information, and then select **Apply to Device**:

- The **Label** field is the name associated to the trustpoint
- For **Enrollment URL** use the one defined in Step 7 of the **Enable SCEP Services in the Windows Server** section
- Check the **Authenticate** checkbox is selected so that the CA certificate is downloaded
- The **Domain Name** field is placed as the common name attribute of the certificate request
- Check the **Key Generated** checkbox, a drop down menu shows up, select the keypair generated in Step 2
- Check the **Enroll Trustpoint** checkbox, two password field show up; type a password. This is used to chain the certificate keys with the device certificate and the CA certificate

Warning: The 9800 controller does not support multi-tier server chains for LSC installation, so the root CA must be the one that signs the certificate requests from the controller and the APs.



CLI configuration for steps three and four:

Caution: The subject-name configuration line must be formatted in LDAP syntax, otherwise it is not accepted by the controller.

```
9800-L(config)#crypto pki trustpoint <trustpoint name>
9800-L(ca-trustpoint)#enrollment url http://<CA server IP>/certsrv/mscep/mscep.dll
9800-L(ca-trustpoint)#subject-name C=<country Code>, ST=<state>, L=<location>, O=<organisation>,
CN=<device common name>/emailAddress=<contact e-mail>
9800-L(ca-trustpoint)#rsakeypair <keypair label>
9800-L(ca-trustpoint)#revocation-check none
9800-L(ca-trustpoint)#exit
9800-L(config)#crypto pki authenticate <trustpoint name>
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.
```

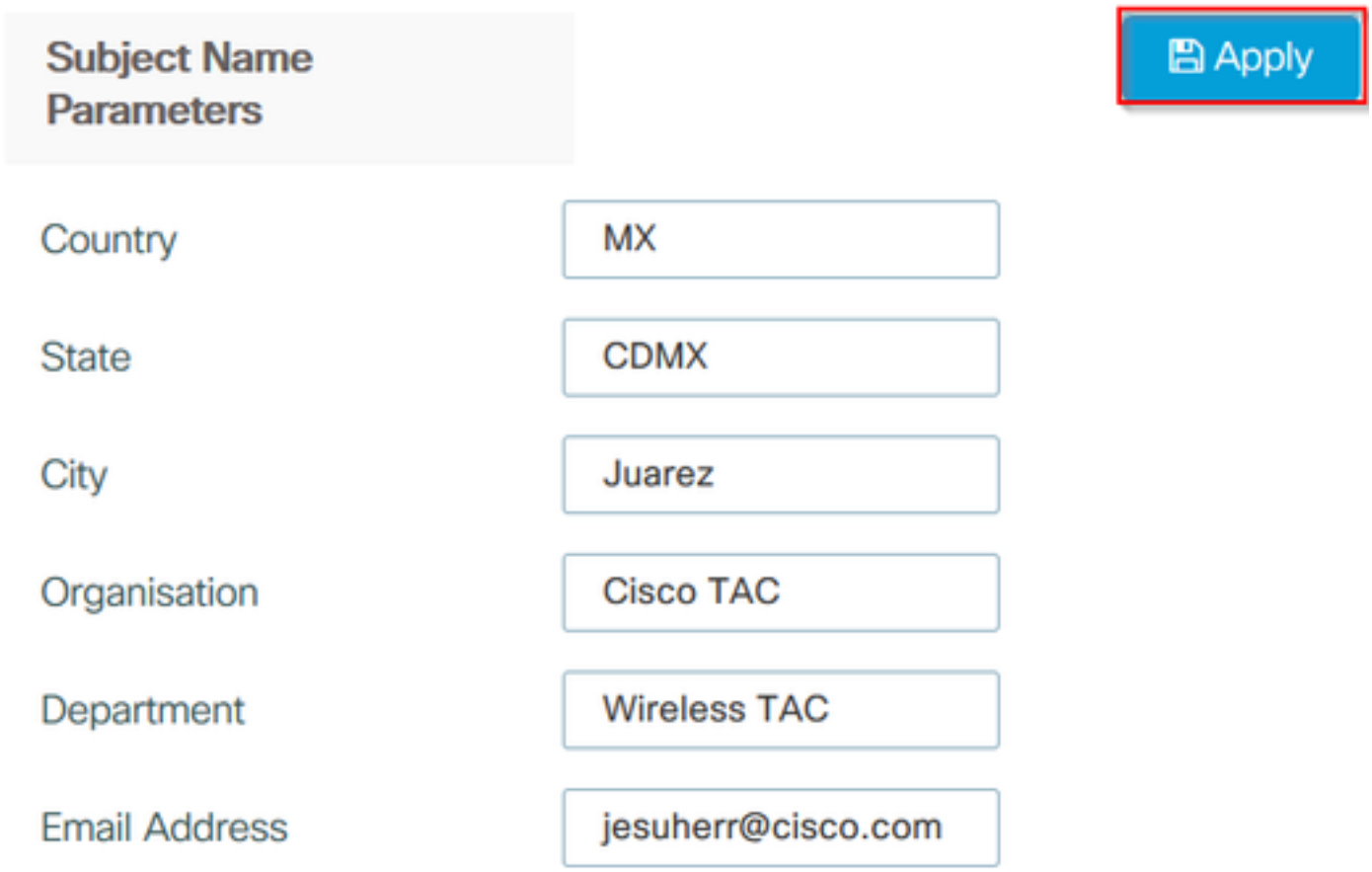
```
   Please make a note of it.

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.
```

Define AP Enrollment Parameters and Update Management Trustpoint

AP enrollment uses the previously defined trustpoint details to determine the server details to which the controller forwards the certificate request. Since the controller is used as a proxy for certificate enrollment, it needs to be aware of the subject parameters included in the certificate request. The configuration is performed either throught the web interface or the command line.

Step 1. Navigate to **Configuration > Wireless > Access Points** and expand the **LSC Provision** menu.

Step 2. Fill the **Subject Name Parameters** with the attributes that are filled in the AP certificate requests, then select **Apply**.



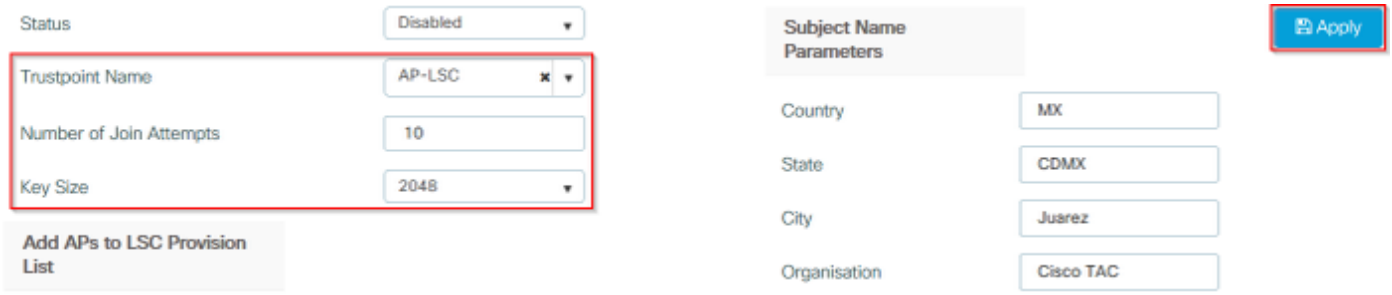
CLI configuration for steps one and two:

```
9800-L(config)#ap lsc-provision subject-name-parameter country <country state <state> city
```

```
<city> domain <department> org <organization> email-address <mail address>
```

> **Note**:Subject-name-parameters restricted to 2 characters like country code must be strictly respected, as the 9800 WLC does not validate those attributes.
> For more information consult the defect CSCvo72999 as a reference.

Step 3. Within the same menu, select the previously defined trustpoint from the drop down list, specify a number of AP join attempts (this defines the number of join attempts before it uses the MIC again), and set the certificate key size. Then, click **Apply**.

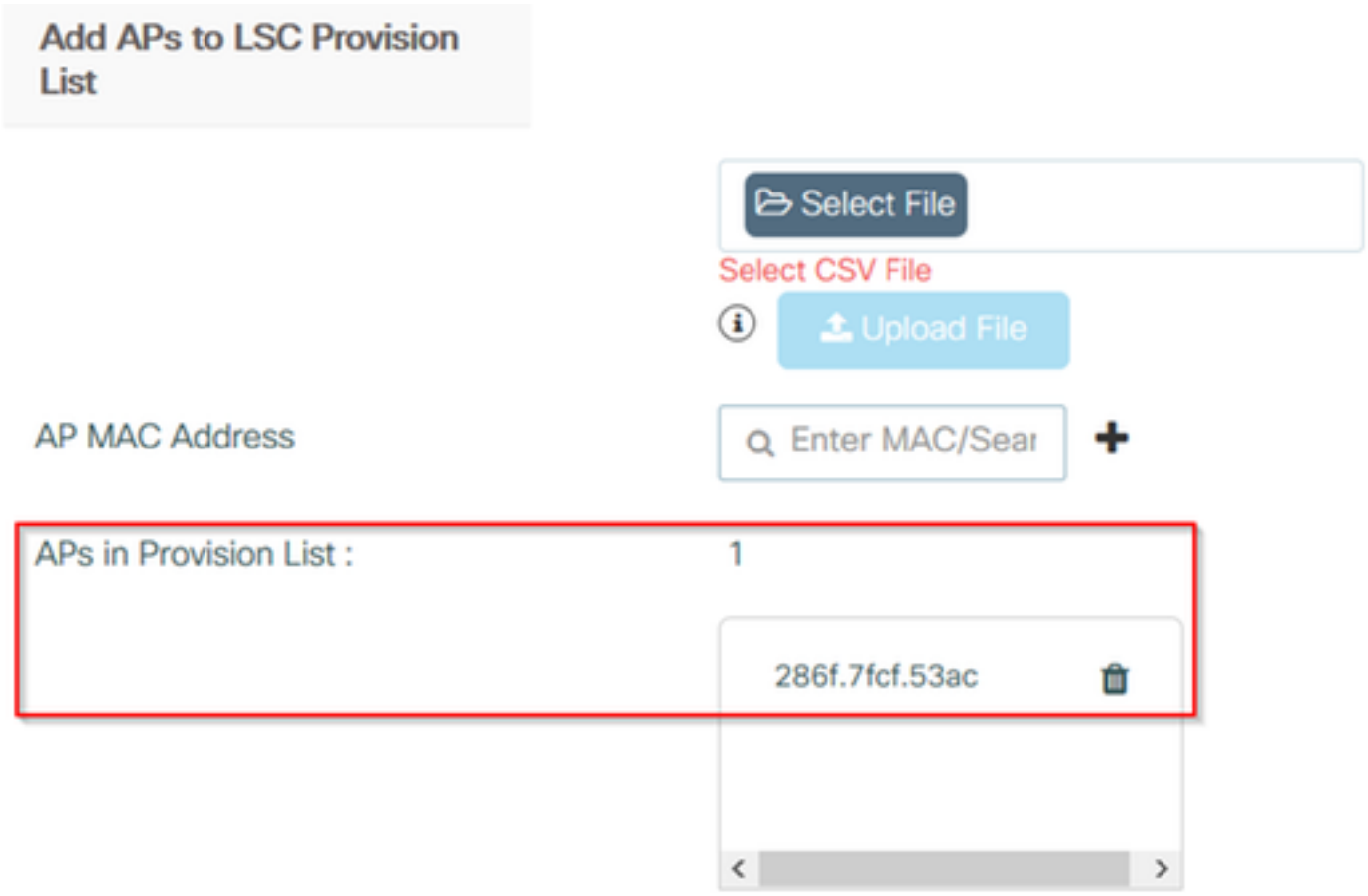


CLI configuration for step three:

```
9800-L(config)#ap lsc-provision join-attempt <number of attempts>
9800-L(config)#ap lsc-provision trustpoint <trustpoint name>
9800-L(config)#ap lsc-provision key-size <key size>
```

Step 4. (Optional) AP LSC provisioning can be triggered for all the APs joined to the controller, or to specific APs defined in a mac address list. Within the same menu, input the AP ethernet mac address in format xxxx.xxxx.xxxx in the text field and click the **+** sign. Alternatively, upload a csv file that contains the AP mac addresses, select the file and then select **Upload File**.

> **Note**: The controller skips any mac address in the csv file that it does not recognize from its joined AP list.



CLI configuration for step four:

```
9800-L(config)#ap lsc-provision mac-address <AP mac in xxxx.xxxx.xxxx format>
```

Step 5. Select **Enabled** or **Provision List** from the drop down menu next to the **Status** label and then click **Apply** to Trigger AP LSC enrollement.

> **Note**: APs begin certificate request, download, and installation. Once the certificate is fully installed, the AP reboots, and starts the join process with the new certificate.

> **Tip**: If AP LSC provisioning is done through a pre-production controller is used along with the provision list, do not remove the AP entries once the certificate is provisioned. If this is done, and the APs fallback to MIC and join the same pre-production controller, their LSC certificates are erased.

CLI configuration for step five:

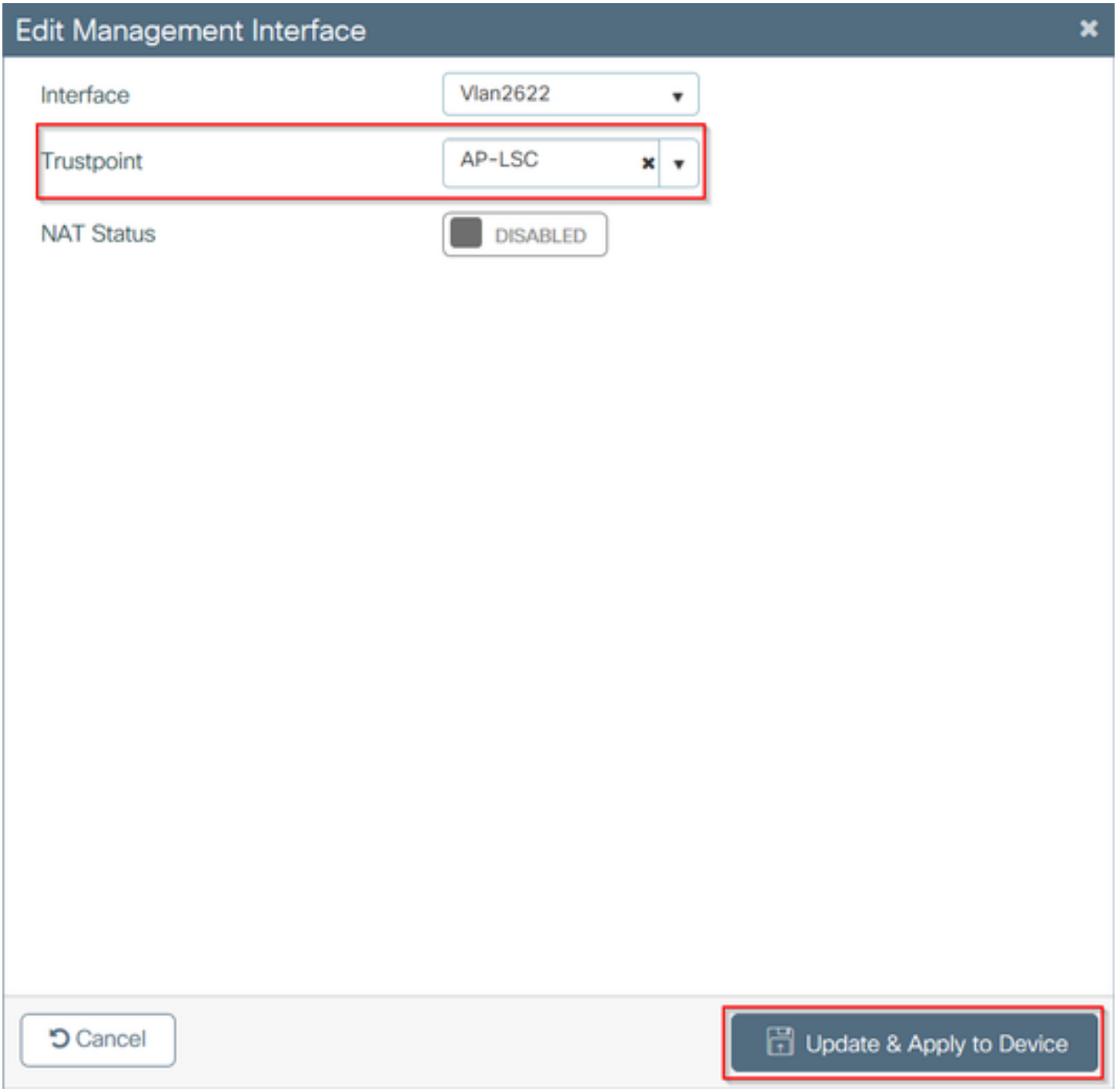
```
9800-L(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size
configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key
by-default or 256 bit key if configured.
Are you sure you want to continue? (y/n):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

use: 9800-L(config)#**ap lsc-provision provision-list**

Step 6. Navigate to **Configuration > Interface > Wireless** and select the management interface. In the **Trustpoint** field, select the new trustpoint from the drop down menu and click **Update & Apply to Device**.

> **Caution**: If LSC is enabled but the 9800 WLC's trustpoint refers to the MIC or an SSC, the APs try to join with the LSC for the configured number of join attempts. Once max attempts limit is reached, the APs fallback to MIC and join again, but since LSC provision is enabled the APs request a new LSC. This leads to a loop where the CA server signs certificates constantly for the same APs and the APs stuck in a join-request-reboot loop.

> **Note**: Once the management trustpoint is updated to use the LSC certificate, new APs are not able to join the controller with the MIC. Currently there is no support to open a provision window. If you need to install new APs, they need to be previously provisioned with an LSC signed by the same CA that the one in the management trustpoint.



CLI configuration for step six:

```
9800-L(config)#wireless management trustpoint <trustpoint name>
```

Verify

Verify Controller Certificate Installation

To verify that the LSC information is present in the 9800 WLC trustpoint issue the command **show crypto pki certificates verbose <trustpoint name>**, two certificates are associated to the trustpoint created for LSC provisioning and enrollment. In this example the trustpoint name is "microsoft-ca" (only relevant output is displayed):

```
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
```

Verify 9800 WLC LSC Configuration

In order to verify the details about the wireless management trustpoint run the **show wireless management trustpoint** command, ensure that the correct trustpoint (the one that contains the LSC details, AP-LSC in this example) is in use and is marked as Available:

```
9800-L#show wireless management trustpoint

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

In order to verify the details about the AP LSC provisioning configuration, along with the list of APs added to the provision list, run the **show ap lsc-provision summary** command. Ensure that the correct proviosion state is shown:

```
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
```

Verify Access Point Certificate Installation

In order to verify the certificates installed in the AP run the **show crypto** command from the AP CLI, ensure that both CA Root certificate and Device certificate are present (the output shows only relevant data):

```
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)
```

If LSC for switch port dot1x authentication is used, from the AP you can verify if port authentication is enabled.

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

> **Note**: To enable port dot1x for the APs, it is needed to define the dot1x credentials for the APs in either the AP profile or the AP configuration itself with dummy values.

Troubleshoot

Common Issues

1. If the templates are not properly mapped in the server registry or if the server requires password challenge, the certificate request for either the 9800 WLC or the APs is rejected.
2. If the IIS default sites are disabled, the SCEP service is disabled as well, therefore the URL defined in the trustpoint is not reachable and the 9800 WLC does not send any certificate request.
3. If time is not synchronized between the server and the 9800 WLC, certificates are not installed since time validity check fails.

Debug and Log Commands

Use these commands to troubleshoot 9800 controller certificate enrollment:

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

In order to troubleshoot and monitor AP enrollment use these commands:

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

From the AP command line, **show logging** shows if the AP had issues with certificate installation, and it provides details about the reason certificate was not installed:

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

Example of a Successful Enrollment Attempt

This is the output from the debugs before mentioned for a successful enrollment for both the controller and its associated APs.

CA root certificate import to 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 device enrollment:

```
[...]
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 enrollment debug output from controller side, this output is repeated multiple times for each AP

that is joined to the 9800 WLC:

```
[...]
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 enrollment debug output from the AP side:

```
[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
```

This concludes the configuration example for LSC enrollment through SCEP.