Konfigurieren von SCEP für die Bereitstellung lokal bedeutender Zertifikate auf 9800 WLC

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie den 9800 Wireless LAN Controller (WLC) für die Anmeldung bei Locally Significant Certificate (LSC) für die Verbindung von Access Points (AP) über die Microsoft Network Device Enrollment Service (NDES)- und Simple Certificate Enrollment Protocol (SCEP)-Funktionen in Windows Server 2012 R2 Standard konfigurieren.

Voraussetzungen

Um SCEP mit dem Windows-Server erfolgreich ausführen zu können, muss der 9800 WLC die folgenden Anforderungen erfüllen:

- Der Controller und der Server müssen erreichbar sein.
- Der Controller und der Server werden mit demselben NTP-Server synchronisiert oder verwenden dieselbe Datums- und Zeitzone (wenn die Uhrzeit zwischen dem CA-Server und der Uhrzeit vom Access Point abweicht, hat der Access Point Probleme mit der Zertifikatsvalidierung und -installation).

Bei Windows Server müssen die Internetinformationsdienste (IIS) zuvor aktiviert sein.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Technologien zu verfügen:

- 9800 Wireless LAN Controller, Version 16.10.1 oder höher.
- Microsoft Windows Server 2012 Standard.
- Private Key Infrastructure (PKI) und Zertifikate.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Version 17.2.1 der WLC-Software 9800-L.
- Windows Server 2012 Standard R2.
- 3802 Access Points

> **Hinweis**: Die serverseitige Konfiguration in diesem Dokument ist insbesondere WLC SCEP. Weitere Informationen zu verstärkten, sicheren und Zertifikatsserverkonfigurationen finden Sie in Microsoft TechNet.

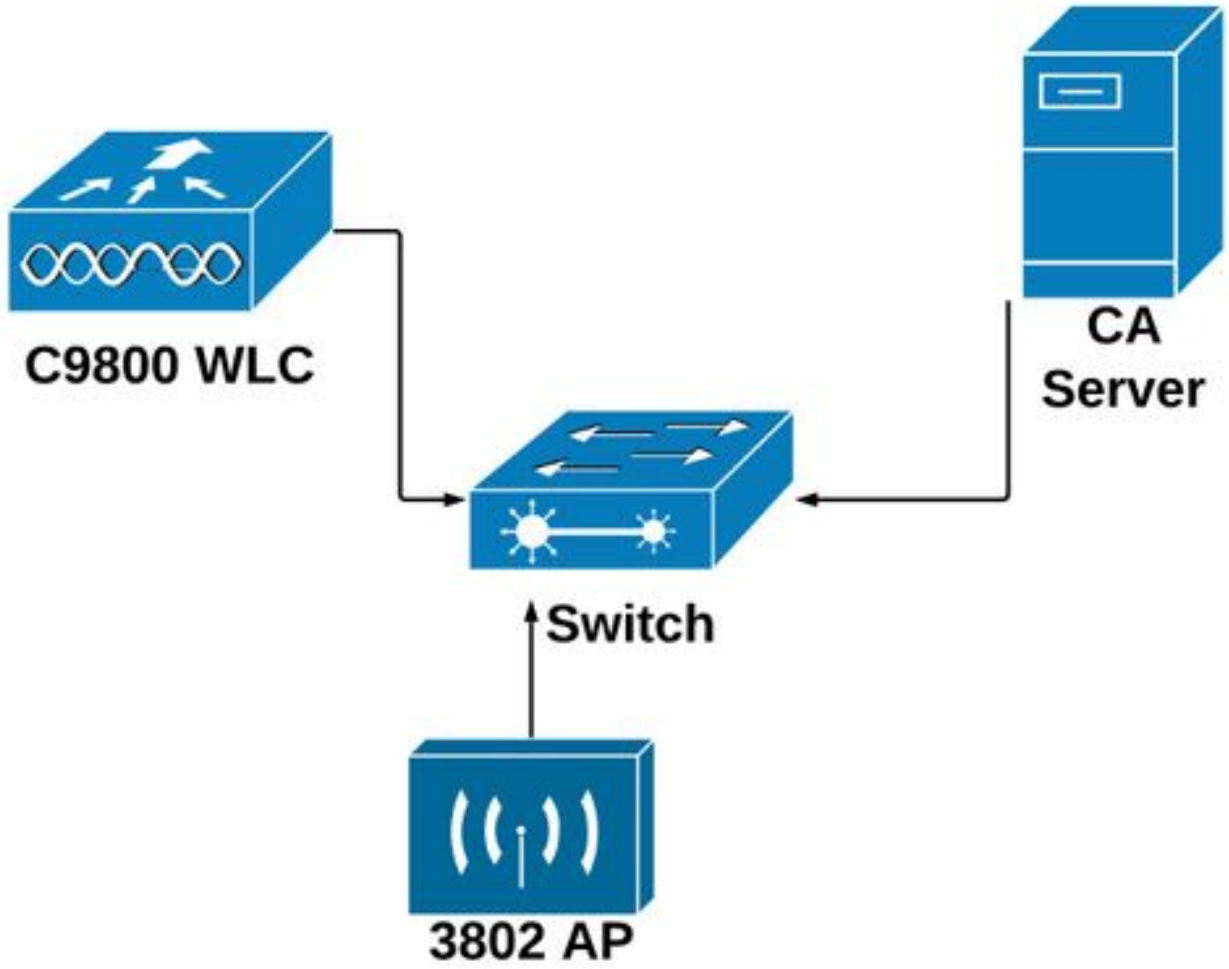
Hintergrundinformationen

Die neuen LSC-Zertifikate, sowohl das Root-Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) als auch das Gerätezertifikat, müssen auf dem Controller installiert sein, um sie schließlich in die Access Points herunterzuladen. Mit SCEP werden die CA- und Gerätezertifikate vom CA-Server empfangen und später automatisch im Controller installiert.

Der gleiche Zertifizierungsprozess findet bei der Bereitstellung von LSCs durch die APs statt. Dabei fungiert der Controller als CA-Proxy und unterstützt dabei, die (selbst generierte) Zertifikatsanforderung für den Access Point von der Zertifizierungsstelle zu signieren.

Konfigurieren

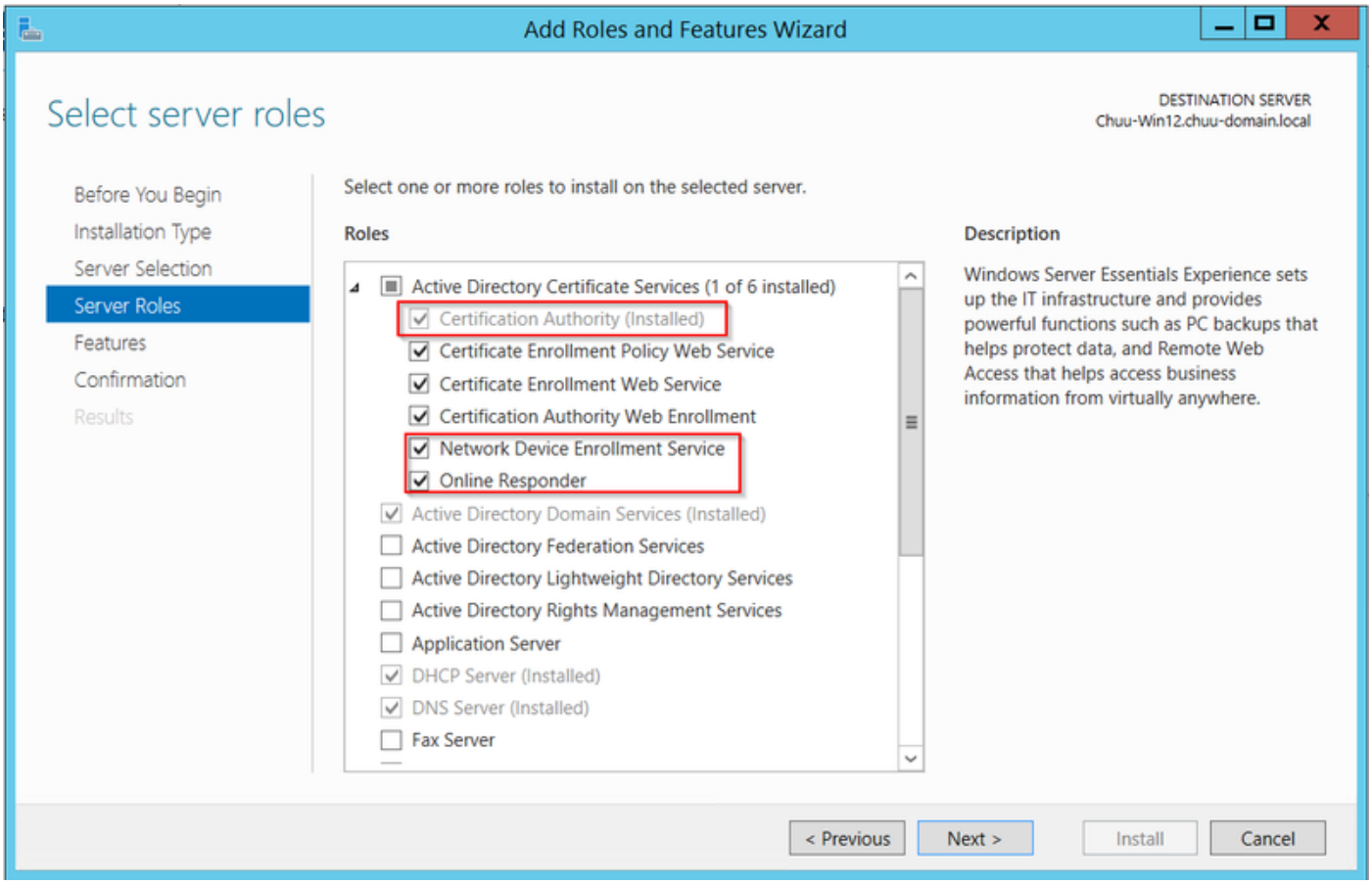
Netzwerkdiagramm



Aktivieren von SCEP-Diensten in Windows Server

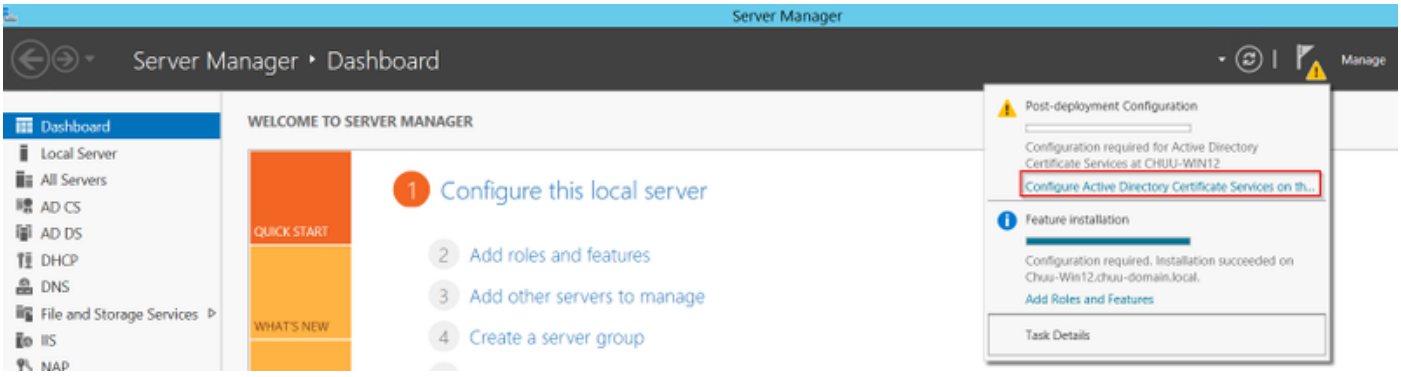
Schritt 1: Wählen Sie in der **Server Manager-**Anwendung das Menü **Verwalten** aus, und wählen Sie dann die Option **Rollen und Funktionen hinzufügen aus,** um die Rolle Konfigurationsassistent für Rollen und Funktionen hinzufügen zu öffnen. Wählen Sie von dort die Serverinstanz aus, die für die SCEP-Serverregistrierung verwendet wird.

Schritt 2: Vergewissern Sie sich, dass die Funktionen Zertifizierungsstelle, **Network Device Enrollment Service** und **Online Responder** ausgewählt sind, und wählen Sie **Weiter:**



Schritt 3: Wählen Sie zweimal **Weiter** und dann **Beenden**, um den Konfigurationsassistenten zu beenden**.** Warten Sie, bis der Server die Funktionsinstallation abgeschlossen hat, und wählen Sie dann **Schließen aus,** um den Assistenten zu schließen.

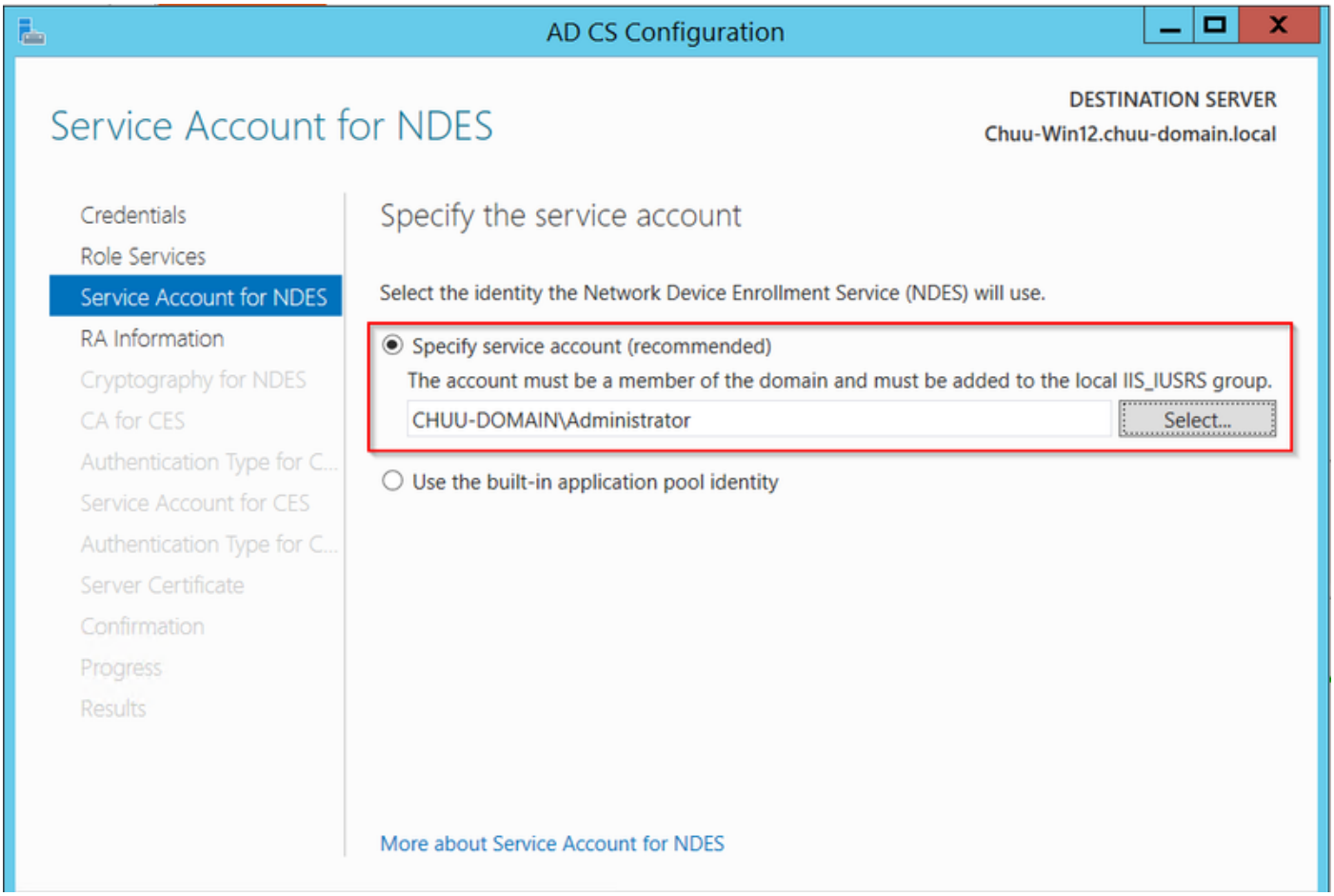
Schritt 4: Nach Abschluss der Installation wird im Server Manager Notification-Symbol ein Warnsymbol angezeigt. Wählen Sie diese Option aus, und wählen Sie den Link **Configure Active Directory Services auf dem Zielserver** aus, um das Assistentenmenü für die **AD CS-Konfiguration** aufzurufen.



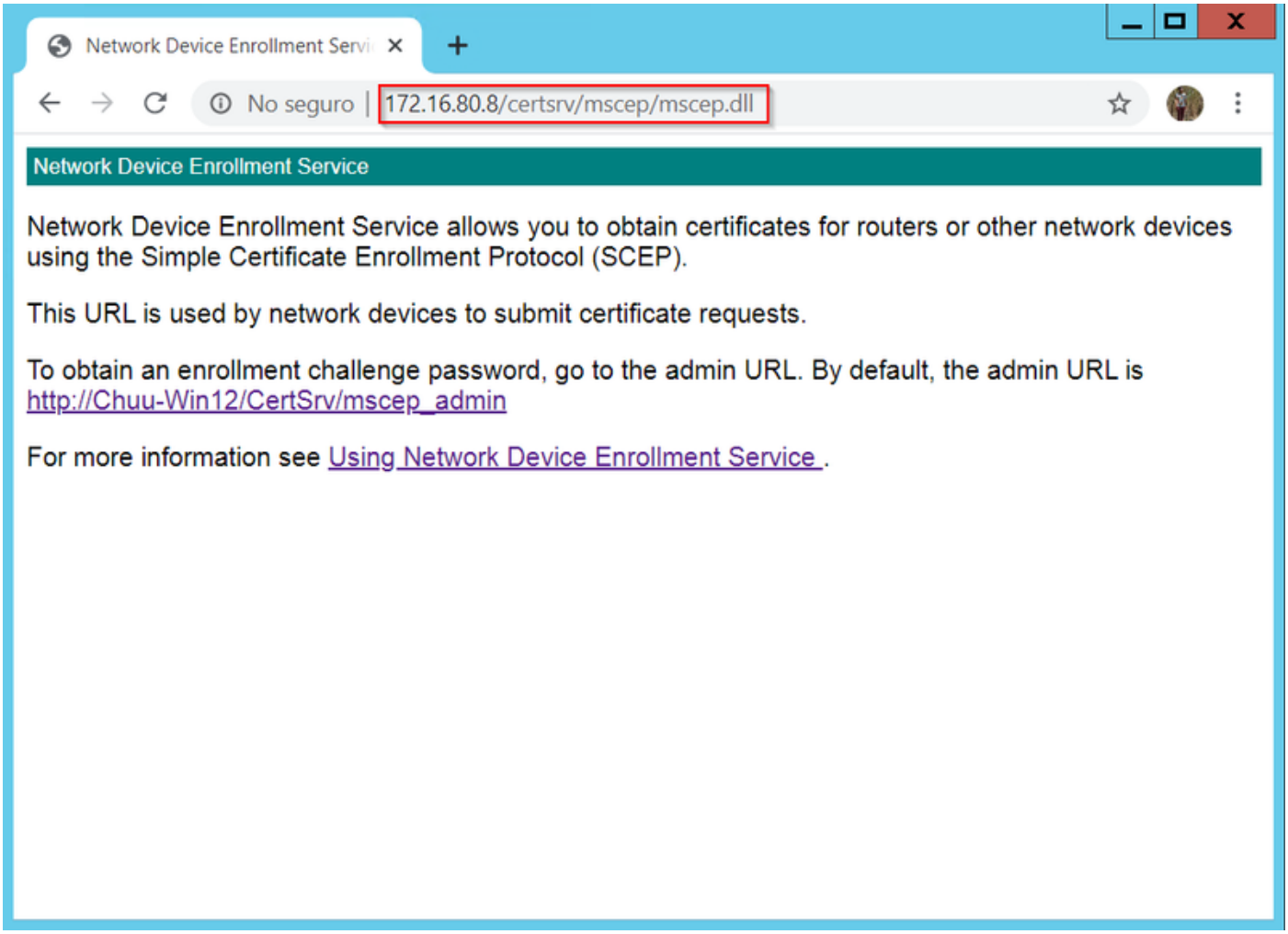
Schritt 5: Wählen Sie den **Network Device Enrollment Service** (Netzwerkgeräteinschreibung) und die im Menü zu konfigurierenden **Online Responder**-Rollendienste aus, und wählen Sie dann **Next (Weiter)**.

Schritt 6: Wählen Sie im **Dienstkonto für NDES** entweder eine Option zwischen dem integrierten Anwendungspool oder dem Dienstkonto aus, und wählen Sie dann **Weiter aus**.

> **Hinweis**: Stellen Sie bei einem Dienstkonto sicher, dass das Konto zur **IIS_IUSRS**-Gruppe gehört.



Schritt 7: Wählen Sie **Weiter** für die nächsten Bildschirme aus, und beenden Sie den Installationsprozess. Nach der Installation ist die SCEP-URL mit jedem Webbrowser verfügbar. Navigieren Sie zur URL **http://<server ip>/certsrv/mscep/mscep.dll**, um zu überprüfen, ob der Service verfügbar ist.



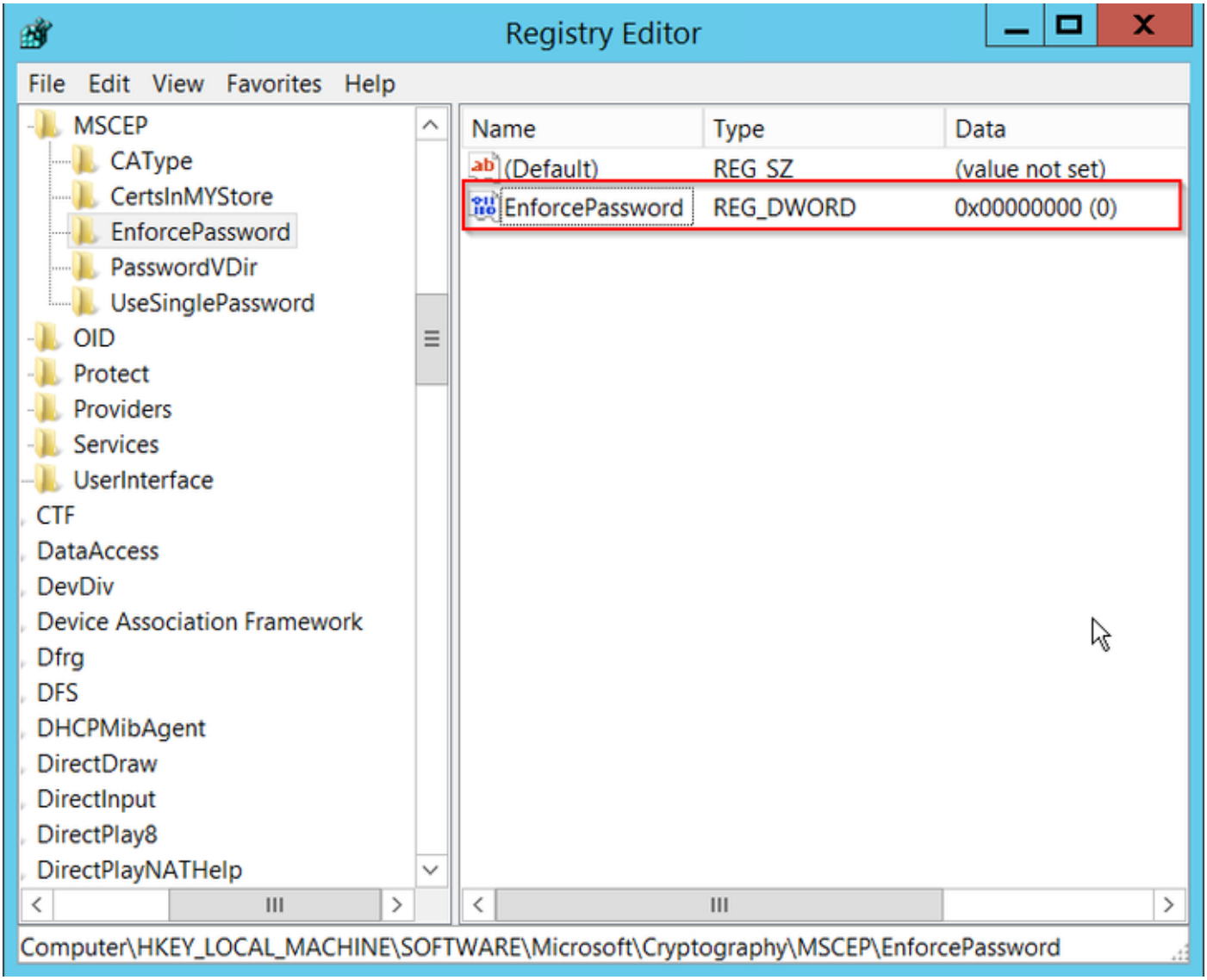
Kennwortanforderung für SCEP-Anmeldung deaktivieren

Standardmäßig verwendet der Windows-Server ein dynamisches Kennwort für die Herausforderung, um Client- und Endpunktanforderungen vor der Anmeldung bei Microsoft SCEP (MSCEP) zu authentifizieren. Dazu muss ein Administratorkonto zur Web-GUI navigieren, um ein On-Demand-Kennwort für jede Anforderung zu generieren (das Kennwort muss in der Anfrage enthalten sein). Der Controller ist nicht in der Lage, dieses Kennwort in die Anforderungen einzubinden, die er an den Server sendet. Um diese Funktion zu entfernen, muss der Registrierungsschlüssel auf dem NDES-Server geändert werden:

Schritt 1: Öffnen Sie den Registrierungseditor, und suchen Sie im **Start**-Menü nach **Regedit**.

Schritt 2: Navigieren Sie zu **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword**

Schritt 3: Ändern Sie den Wert **EnforcePassword** auf 0. Wenn es bereits 0 ist, lassen Sie es so, wie es ist.



Konfigurieren der Zertifikatsvorlage und -registrierung

Zertifikate und die zugehörigen Schlüssel können in mehreren Szenarien für verschiedene Zwecke verwendet werden, die von den Anwendungsrichtlinien im CA-Server definiert werden. Die Anwendungsrichtlinie wird im Feld Extended Key Usage (EKU) des Zertifikats gespeichert. Dieses Feld wird vom Authentifizierer analysiert, um zu überprüfen, ob es vom Client für seinen beabsichtigten Zweck verwendet wird. Um sicherzustellen, dass die richtige Anwendungsrichtlinie in die WLC- und AP-Zertifikate integriert ist, erstellen Sie die entsprechende Zertifikatsvorlage und ordnen diese der NDES-Registrierung zu:

Schritt 1: Navigieren Sie zu **Start > Verwaltung > Zertifizierungsstelle**.

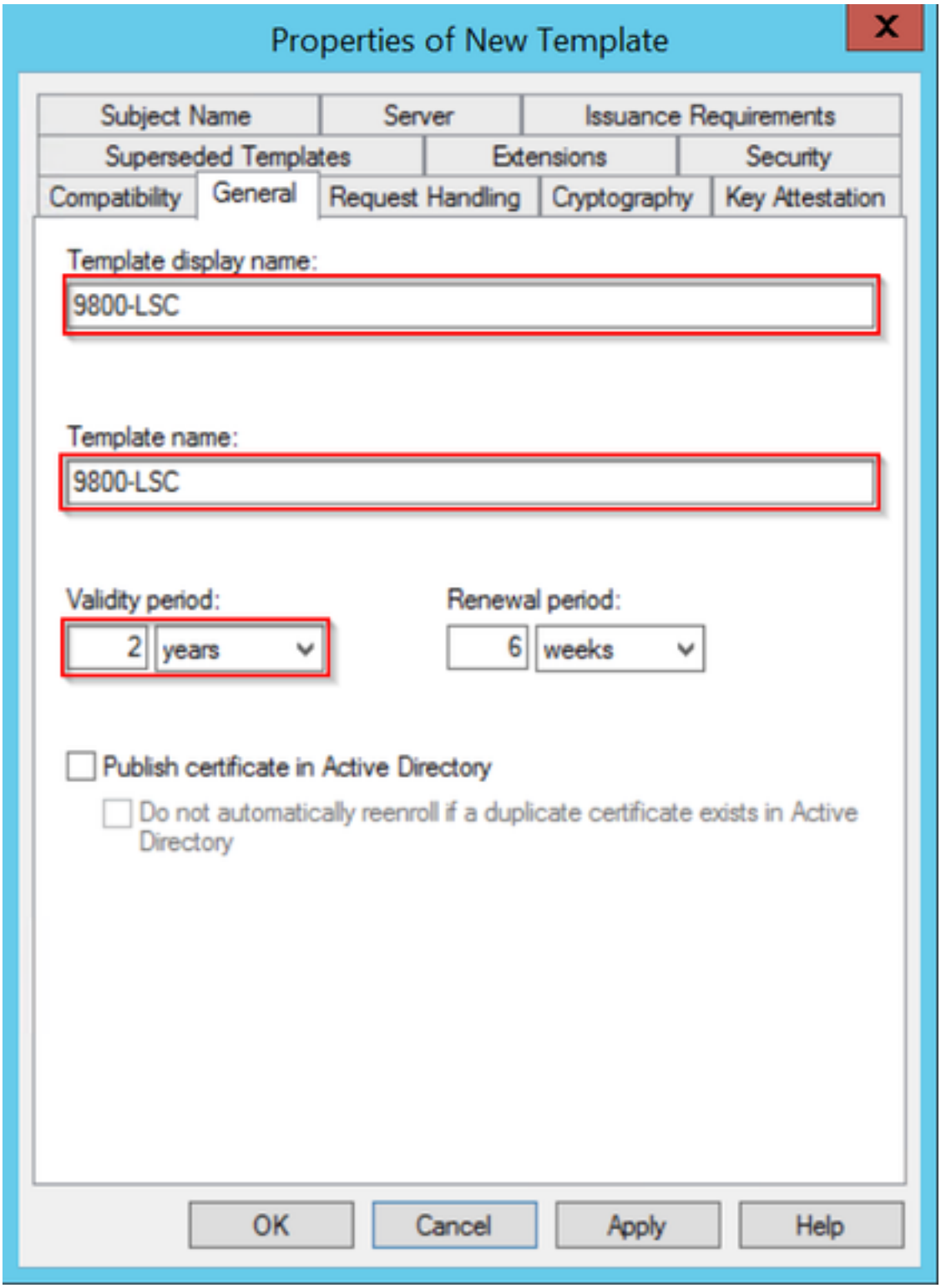
Schritt 2: Erweitern Sie die Verzeichnisstruktur für den CA-Server, klicken Sie mit der rechten Maustaste auf die Ordner **Zertifikatsvorlagen**, und wählen Sie **Verwalten aus**.

Schritt 3: Klicken Sie mit der rechten Maustaste auf die Vorlage **Benutzerzertifikat**, und wählen Sie im Kontextmenü die Option **Vorlage duplizieren**.

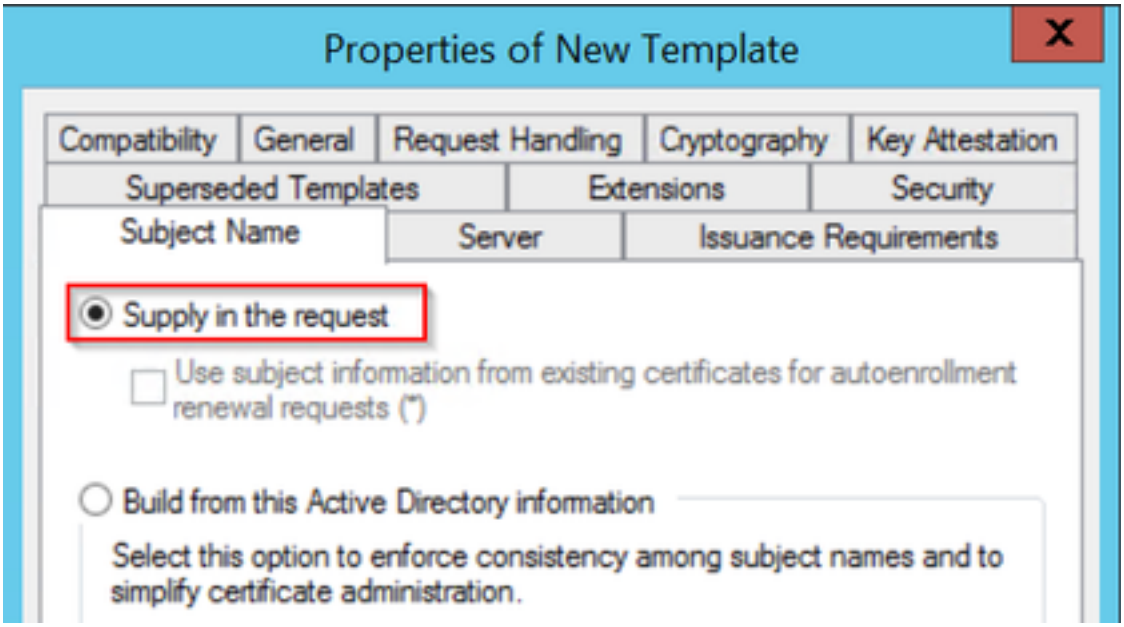
Schritt 4: Navigieren Sie zur Registerkarte **Allgemein**, ändern Sie den Namen und die Gültigkeitsdauer der Vorlage nach Bedarf, und lassen Sie alle anderen Optionen deaktiviert.

Vorsicht: Wenn der Gültigkeitszeitraum geändert wird, stellen Sie sicher, dass er die

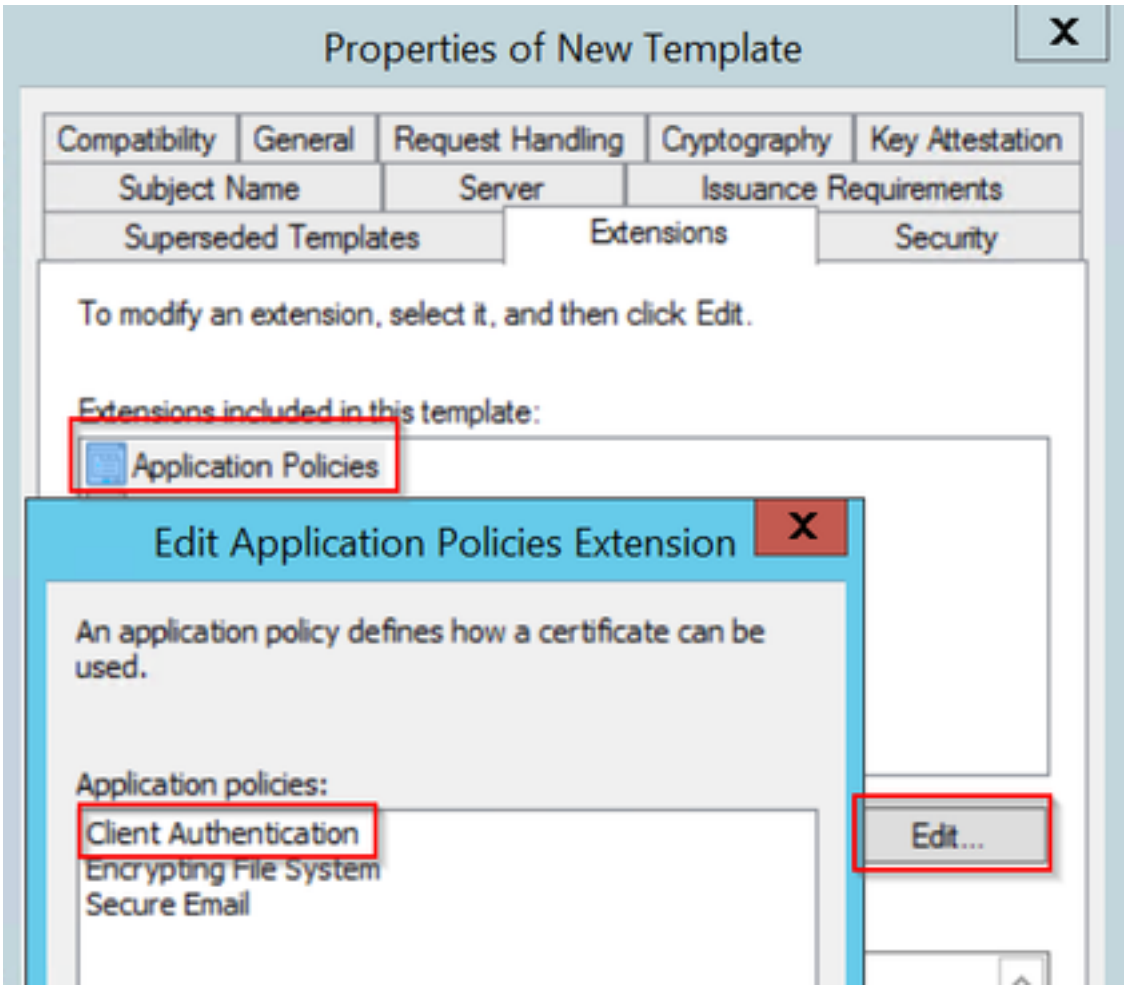
Gültigkeit des Stammzertifikats der Zertifizierungsstelle nicht überschreitet.



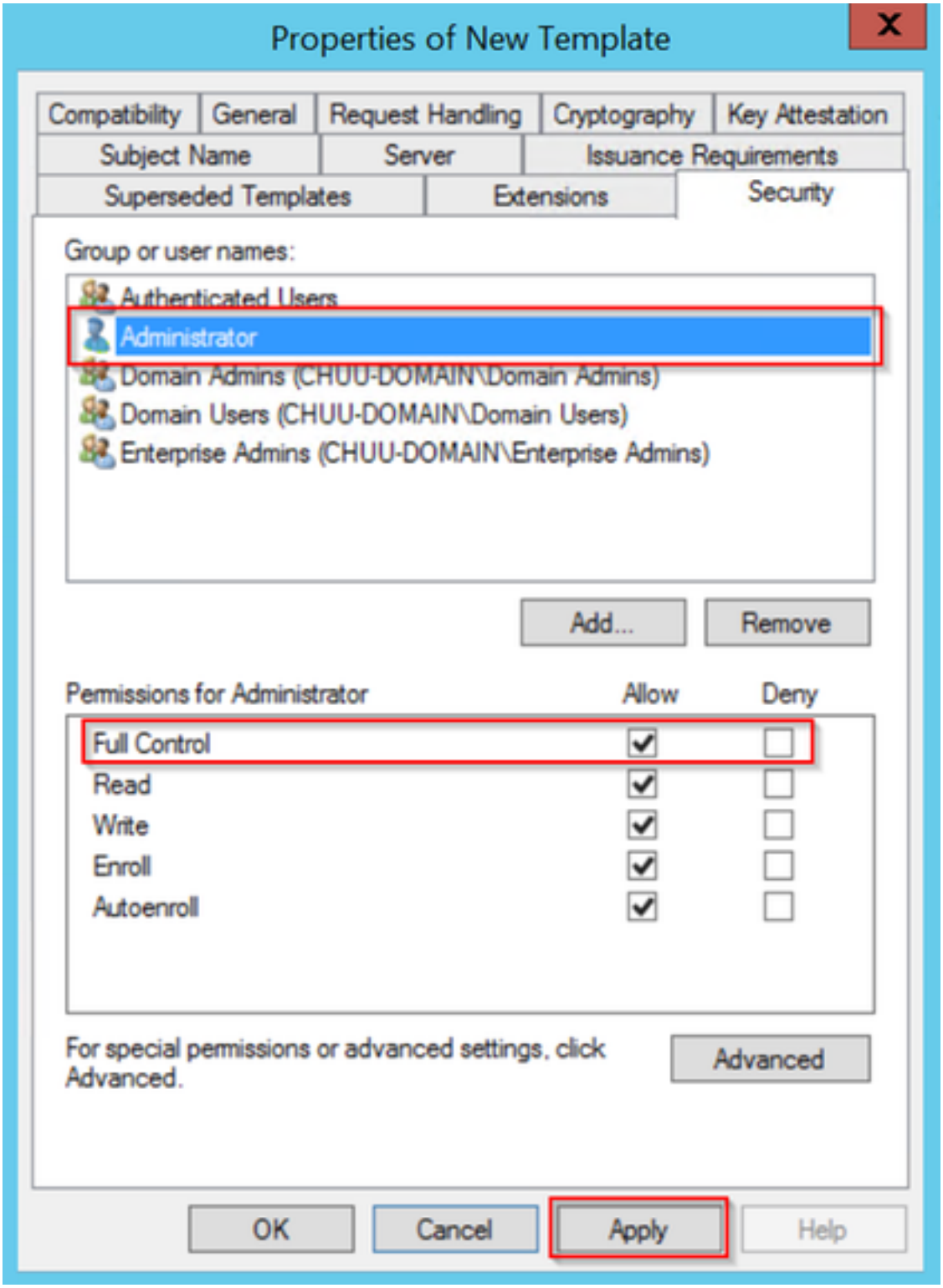
Schritt 5: Navigieren Sie zur Registerkarte **Betreff Name**, und stellen Sie sicher, dass **die Option Angebot in der Anfrage** ausgewählt ist. Ein Popup-Fenster zeigt an, dass Benutzer keine Administratorgenehmigung benötigen, um ihr Zertifikat signieren zu lassen. Wählen Sie **OK**.



Schritt 6: Navigieren Sie zur Registerkarte **Erweiterungen**, wählen Sie dann die Option **Anwendungsrichtlinien** aus, und wählen Sie **Bearbeiten...** -Taste. Stellen Sie sicher, dass sich die **Client-Authentifizierung** im Fenster **Application** Policies (**Anwendungsrichtlinien)** befindet. Andernfalls wählen Sie **Hinzufügen aus**, und fügen Sie es hinzu.



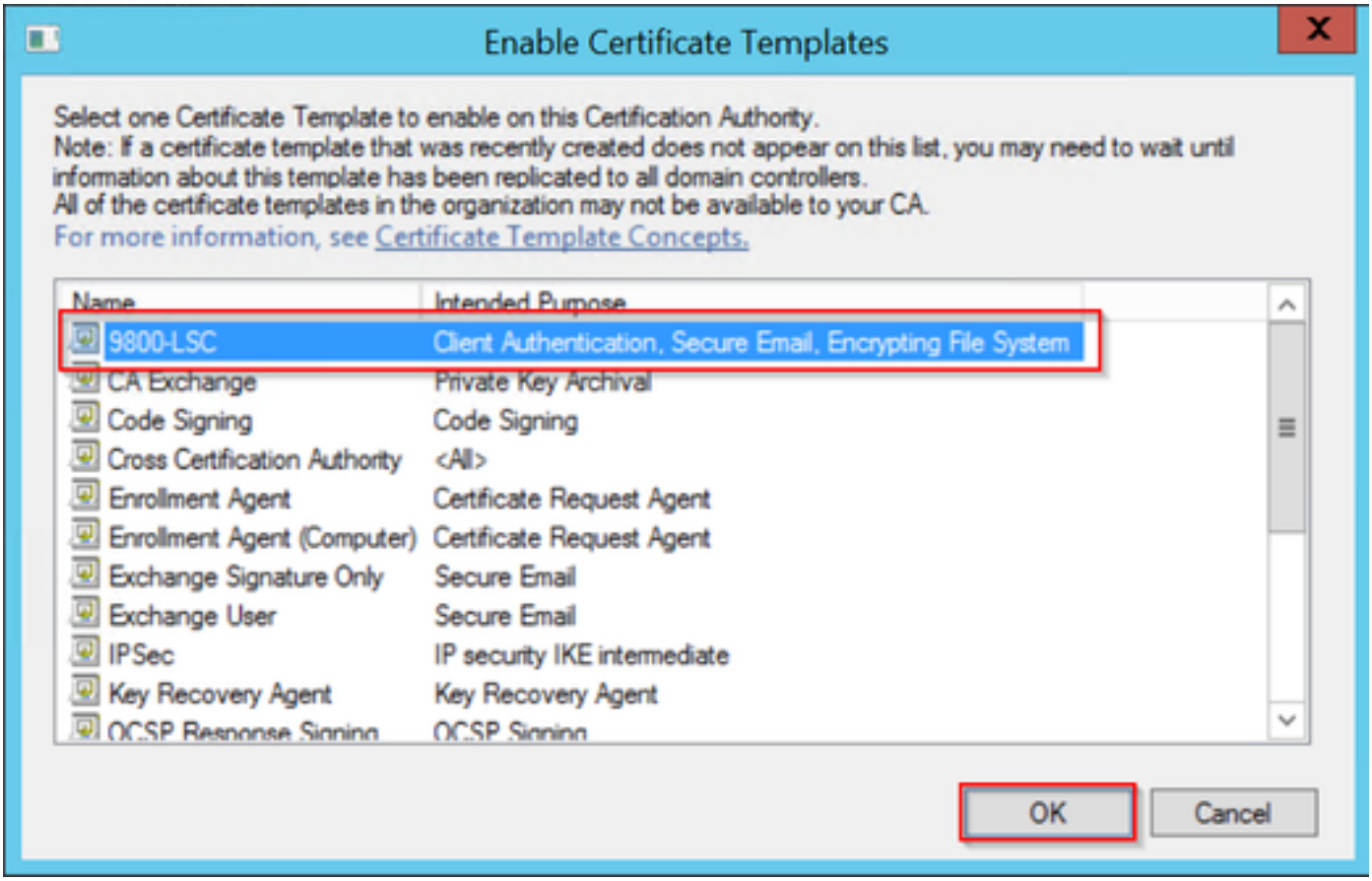
Schritt 7: Navigieren Sie zur Registerkarte **Sicherheit**, stellen Sie sicher, dass das Dienstkonto, das in Schritt 6 der **Enable SCEP Services in the Windows** Server definiert wurde, über **Vollzugriff-**Berechtigungen der Vorlage verfügt, und wählen Sie **Apply und OK aus.**



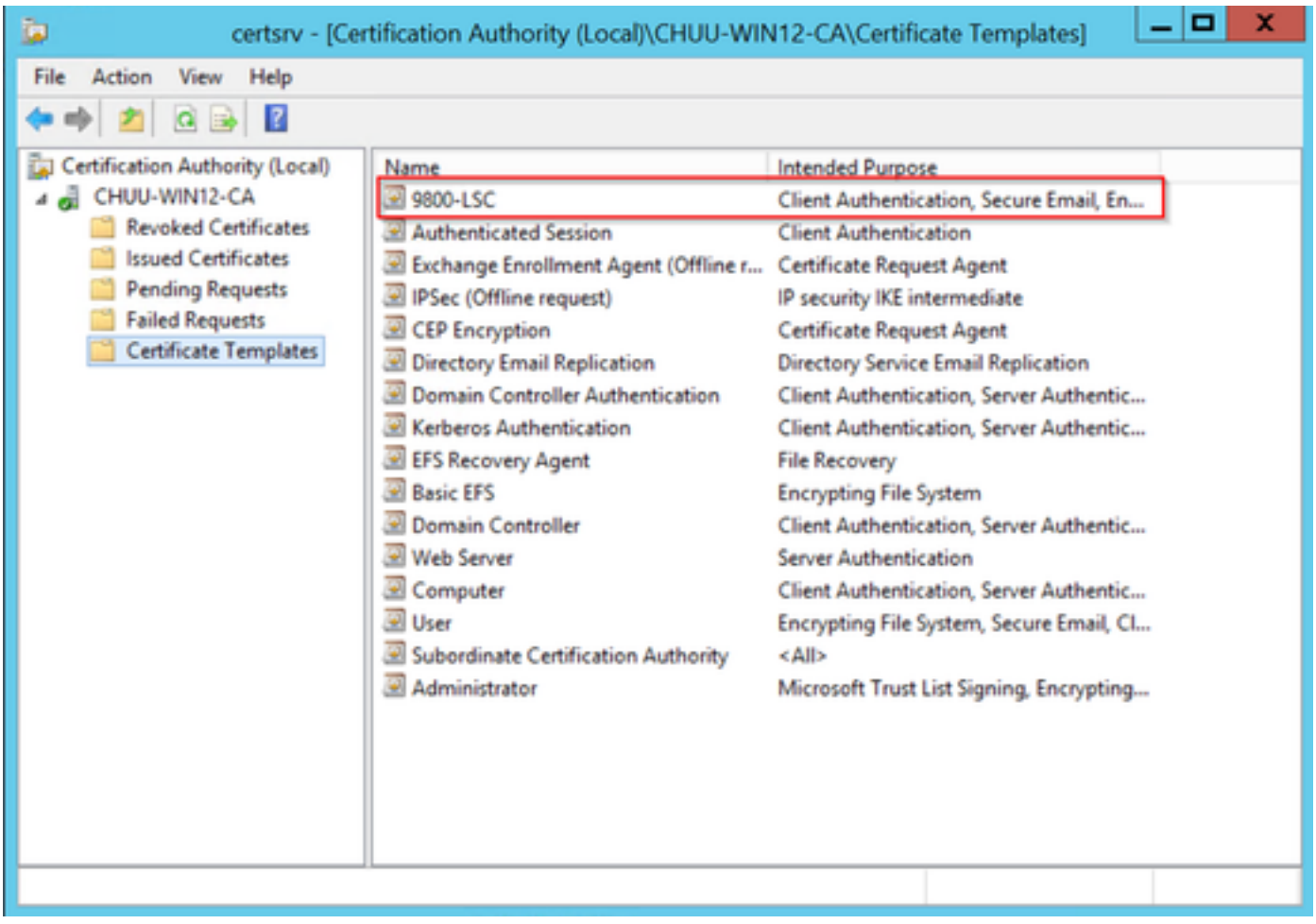
Schritt 8: Kehren Sie zum Fenster der **Zertifizierungsstelle zurück**, klicken Sie mit der rechten Maustaste in den Ordner **Zertifikatsvorlagen**, und wählen Sie **Neu > Zu erteilende Zertifikatsvorlage aus**.

Schritt 9: Wählen Sie die zuvor erstellte Zertifikatsvorlage aus (in diesem Beispiel 9800-LSC), und wählen Sie **OK** aus.

> **Hinweis**: Die Auflistung der neu erstellten Zertifikatsvorlage kann bei mehreren Serverbereitstellungen länger dauern, da sie auf allen Servern repliziert werden muss.



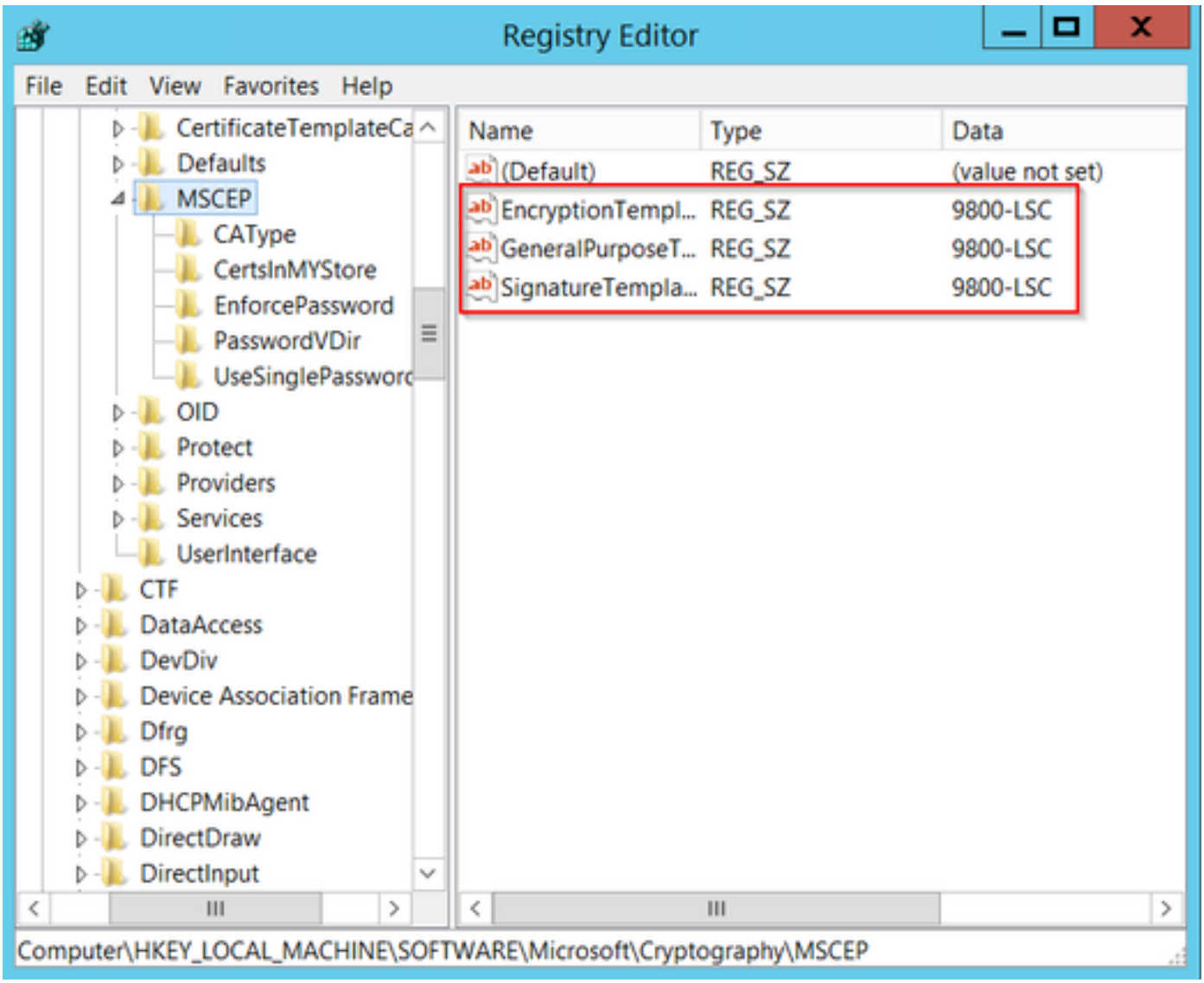
Die neue Zertifikatsvorlage wird jetzt im Ordnerinhalt der **Zertifikatsvorlagen** aufgelistet.



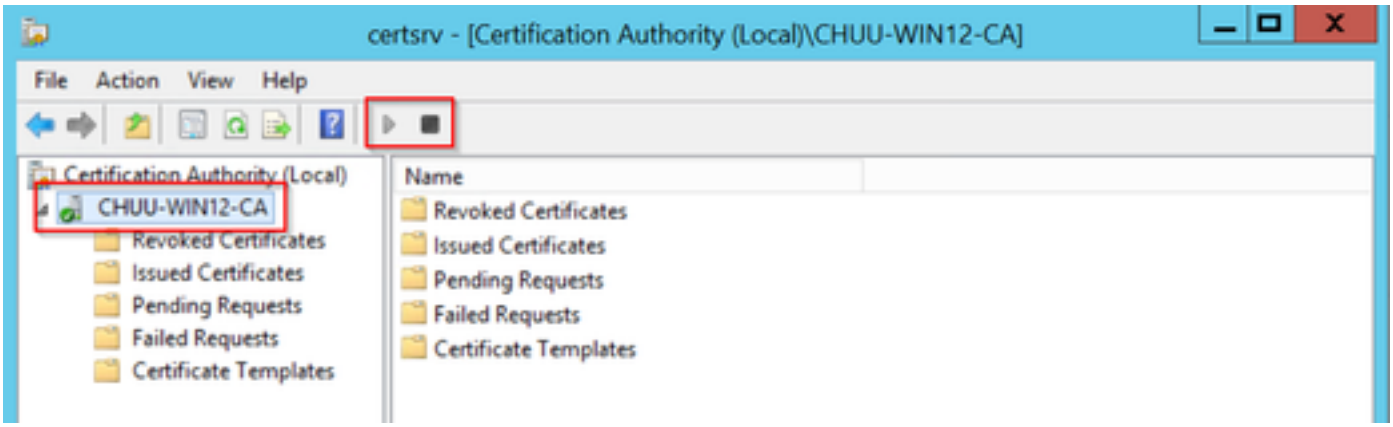
Schritt 10: Kehren Sie zum Fenster **Registrierungs-Editor zurück**, und navigieren Sie zu **Computer**

> HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

Schritt 11: Bearbeiten Sie die Registrierungen **EncryptionTemplate**, **GeneralPurposeTemplate** und **SignatureTemplate** so, dass sie auf die neu erstellte Zertifikatsvorlage zeigen.



Schritt 12: Starten Sie den NDES-Server neu. Kehren Sie also zum Fenster **Certification Authority** zurück, wählen Sie den Servernamen aus, und wählen Sie die Schaltfläche **Stopp** and **Play aus**.



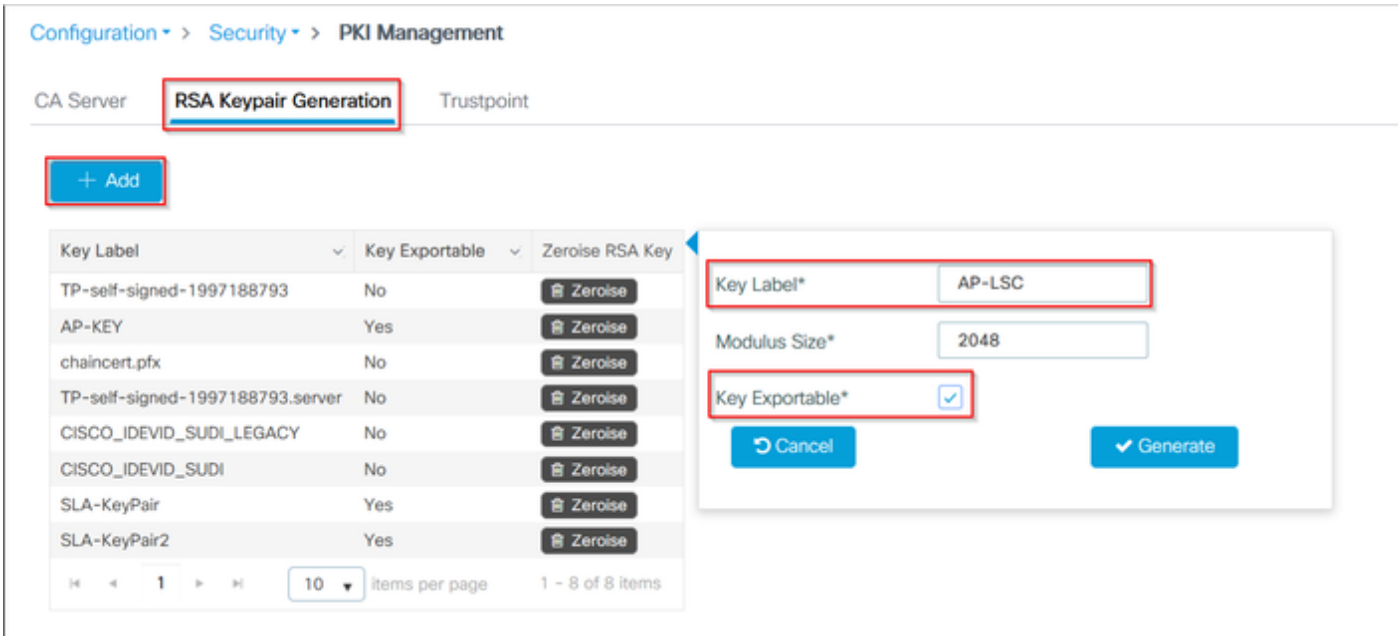
Konfigurieren des 9800-Geräte-Trustpoints

Der Controller muss über einen Trustpoint verfügen, um APs nach ihrer Bereitstellung zu

authentifizieren. Der Trustpoint enthält das Gerätezertifikat 9800 zusammen mit dem Stammzertifikat der CA, das beide vom gleichen CA-Server bezogen wird (in diesem Beispiel Microsoft CA). Damit ein Zertifikat im Trustpoint installiert werden kann, muss es die Betreffattribute sowie ein Paar RSA-Schlüssel enthalten, die ihm zugeordnet sind. Die Konfiguration erfolgt entweder über die Webschnittstelle oder die Befehlszeile.

Schritt 1: Navigieren Sie zu **Konfiguration > Sicherheit > PKI-Management**, und wählen Sie die Registerkarte **RSA-Schlüsselgenerierung aus**. Wählen Sie die Schaltfläche **+ Hinzufügen**.

Schritt 2: Definieren Sie eine dem Tastenfeld zugeordnete Bezeichnung, und stellen Sie sicher, dass das Kontrollkästchen **Exporable** (Exportierbar) aktiviert ist.



CLI-Konfiguration für die Schritte 1 und 2. In diesem Konfigurationsbeispiel wird das Tastenfeld mit dem Label AP-LSC und einer Modulgröße von 2048 Bit generiert:

```
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)
```

Schritt 3: Wählen Sie im gleichen Abschnitt die Registerkarte **Trustpoint** aus, und wählen Sie die Schaltfläche **+ Hinzufügen**.

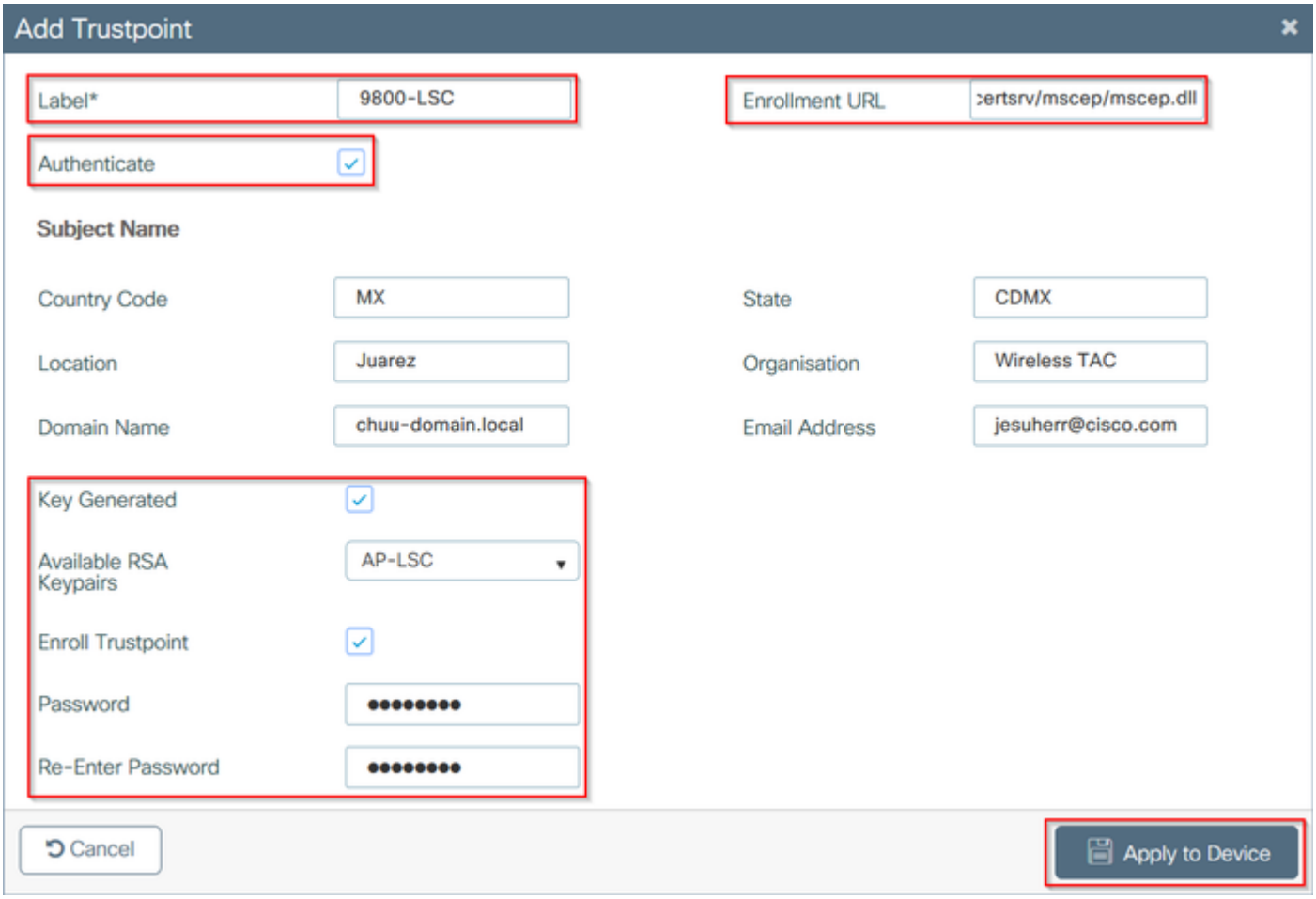
Schritt 4: Füllen Sie die Trustpoint-Details mit den Geräteinformationen aus, und wählen Sie dann **Auf Gerät anwenden aus**:

- Das **Label**-Feld ist der dem Trustpoint zugeordnete Name.
- Für **Registrierungs-URL** verwenden Sie den in Schritt 7 des **Abschnitts "Aktivieren von SCEP-Diensten" im** Abschnitt **Windows Server** definierten **URL**.
- Aktivieren Sie das Kontrollkästchen **Authentifizierung**, um das Zertifizierungsstellenzertifikat

herunterzuladen.

- Das Feld **Domänenname** wird als allgemeines Namensattribut der Zertifikatsanforderung platziert.
- Aktivieren Sie das Kontrollkästchen **Key Generated** (Vom Schlüssel generiert). Ein Dropdown-Menü wird angezeigt. Wählen Sie die in Schritt 2 generierte Tastatur aus.
- Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigkeit registrieren**, und es werden zwei Kennwortfelder angezeigt. Geben Sie ein Kennwort ein. Dies wird verwendet, um die Zertifikatschlüssel mit dem Gerätezertifikat und dem Zertifizierungsstellenzertifikat zu verknüpfen.

Warnung: Der Controller 9800 unterstützt keine mehrstufigen Serverketten für die LSC-Installation. Daher muss die Root-CA die Root-Zertifizierungsstelle sein, die die Zertifikatsanforderungen des Controllers und der APs signiert.



CLI-Konfiguration für die Schritte 3 und 4:

Vorsicht: Die Konfigurationszeile für den Betreffnamen muss in der LDAP-Syntax formatiert sein. Andernfalls wird sie vom Controller nicht akzeptiert.

```
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.
```

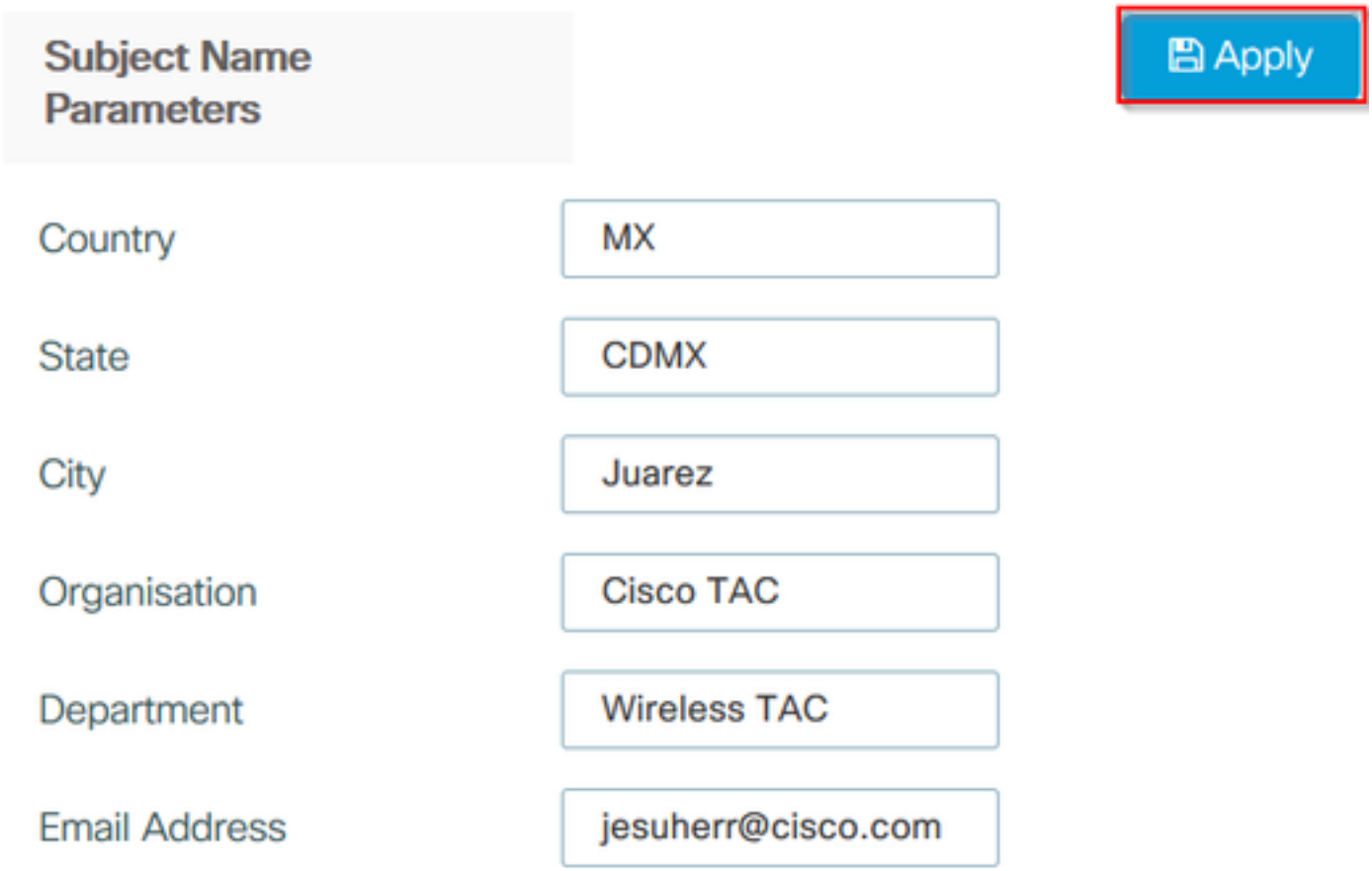
Definieren von AP-Registrierungsparametern und Aktualisieren von Management Trustpoint

Bei der AP-Registrierung werden die zuvor definierten Trustpoint-Details verwendet, um die Serverdetails zu ermitteln, an die der Controller die Zertifikatsanforderung weiterleitet. Da der Controller als Proxy für die Zertifikatsregistrierung verwendet wird, muss er die in der Zertifikatsanforderung enthaltenen Betreffparameter kennen. Die Konfiguration erfolgt entweder über die Webschnittstelle oder die Befehlszeile.

Schritt 1: Navigieren Sie zu **Konfiguration > Wireless > Access Points,** und erweitern Sie das

Menü **LSC Provisioning (LSC-Bereitstellung)**.

Schritt 2: Füllen Sie die **Parameter für den Betreffnamen** mit den Attributen aus, die in den Zertifikatsanforderungen des Access Points ausgefüllt sind, und wählen Sie **Apply** aus.

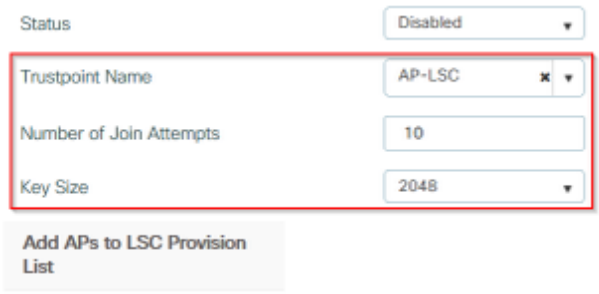


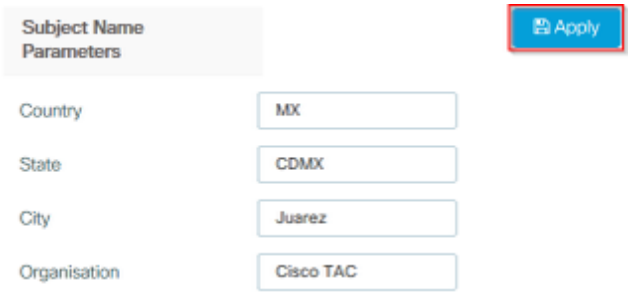
CLI-Konfiguration für die Schritte 1 und 2:

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

> **Hinweis**:Parameter für Betreffnamen, die auf 2 Zeichen beschränkt sind (z. B. Ländercode), müssen strikt eingehalten werden, da diese Attribute vom WLC 9800 nicht validiert werden. Weitere Informationen finden Sie unter dem Fehler CSCvo72999 als Referenz.

Schritt 3: Wählen Sie im gleichen Menü den zuvor definierten Trustpoint aus der Dropdown-Liste aus, geben Sie eine Anzahl von Verbindungsversuchen für den Access Point an (definiert die Anzahl der Verbindungsversuche, bevor der MIC erneut verwendet wird), und legen Sie die Größe des Zertifikatsschlüssels fest. Klicken Sie anschließend auf **Übernehmen**.





CLI-Konfiguration für Schritt drei:

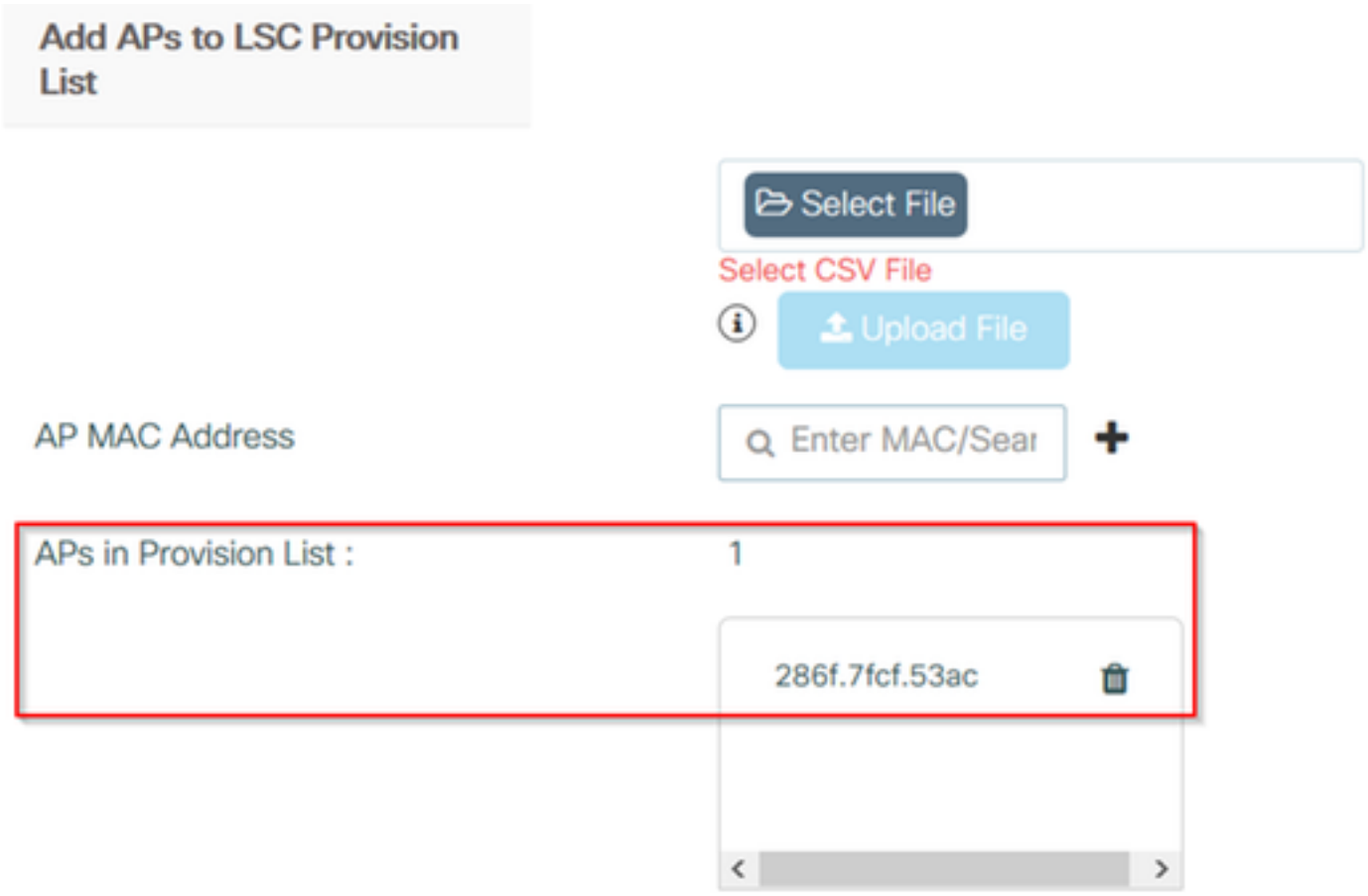
```
9800-L(config)#ap lsc-provision join-attempt
```

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

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

Schritt 4: (Optional) Die AP-LSC-Bereitstellung kann für alle APs ausgelöst werden, die mit dem Controller verbunden sind, oder für bestimmte APs, die in einer MAC-Adressliste definiert sind. Geben Sie im gleichen Menü im Textfeld die MAC-Adresse für das AP-Ethernet im Format xxxx.xxxx.xxxx ein, und klicken Sie auf das **+**-Zeichen. Alternativ können Sie eine CSV-Datei hochladen, die die MAC-Adressen des Access Points enthält, die Datei auswählen und dann **Datei hochladen** auswählen.

> **Hinweis**: Der Controller überspringt jede MAC-Adresse in der CSV-Datei, die er nicht aus der ihm angeschlossenen AP-Liste erkennt.



CLI-Konfiguration für Schritt 4:

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

Schritt 5: Wählen Sie **Enabled (Aktiviert)** oder **Provisioning List (Bereitstellungsliste)** aus dem Dropdown-Menü neben dem Label **Status** aus, und klicken Sie dann auf **Apply** to Trigger AP LSC Enrolllement (AP-LSC-Anmeldung anwenden).

> **Hinweis**: APs beginnen mit der Anforderung, dem Download und der Installation von Zertifikaten. Nach der vollständigen Installation des Zertifikats wird der Access Point neu gestartet, und der Join-Prozess wird mit dem neuen Zertifikat gestartet.

> **Tipp**: Wenn die AP-LSC-Bereitstellung über einen Pre-Production-Controller zusammen mit der Bereitstellungsliste erfolgt, sollten Sie die AP-Einträge nicht entfernen, sobald das Zertifikat bereitgestellt wurde. Wenn dies der Fall ist und die APs auf das MIC zurückfallen und demselben Pre-Production-Controller angehören, werden ihre LSC-Zertifikate gelöscht.

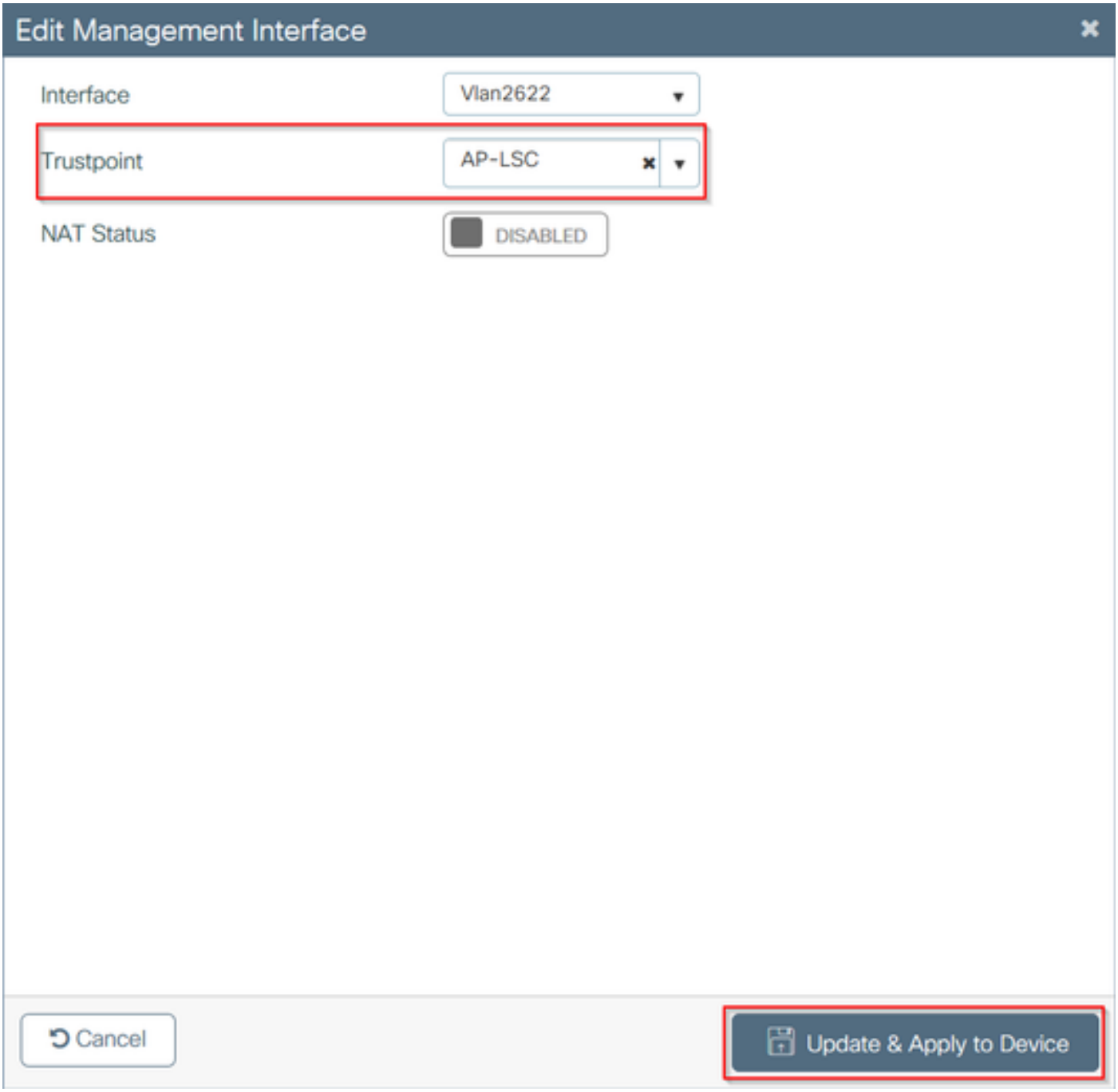
CLI-Konfiguration für Schritt 5:

```
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
```

Schritt 6: Navigieren Sie zu **Konfiguration > Schnittstelle > Wireless,** und wählen Sie die Verwaltungsschnittstelle aus. Wählen Sie im Feld **Trustpoint** den neuen Trustpoint aus dem Dropdown-Menü aus, und klicken Sie auf **Aktualisieren und auf Gerät anwenden**.

Vorsicht: Wenn LSC aktiviert ist, der 9800-WLC-Trustpoint jedoch auf das MIC oder ein SSC verweist, versuchen die Access Points, sich für die konfigurierte Anzahl von Join-Versuchen mit dem LSC zu verbinden. Sobald die maximale Anzahl an Zugriffsversuchen erreicht ist, werden die Access Points auf MIC zurückgesetzt und wieder hinzugefügt. Da die LSC-Bereitstellung jedoch aktiviert ist, fordern die Access Points einen neuen LSC an. Dies führt zu einer Schleife, in der der CA-Server ständig Zertifikate für die gleichen APs signiert und die APs in einer Join-Request-Reboot-Schleife stecken.

Hinweis: Nach der Aktualisierung des Management-Trustpoints zur Verwendung des LSC-Zertifikats können neue APs dem Controller nicht mehr mit dem MIC beitreten. Derzeit wird das Öffnen eines Provisioning-Fensters nicht unterstützt. Wenn Sie neue APs installieren müssen, müssen diese zuvor mit einem LSC versehen sein, der von derselben Zertifizierungsstelle signiert wird, die auch im Verwaltungs-Vertrauenspunkt vorhanden ist.



CLI-Konfiguration für Schritt 6:

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

Überprüfen

Installation des Controller-Zertifikats überprüfen

Um zu überprüfen, ob die LSC-Informationen im 9800-WLC-Vertrauenspunkt vorhanden sind, geben Sie den Befehl **show crypto pki certificate ausführliche <trustpoint name>**, werden zwei Zertifikate dem für die LSC-Bereitstellung und -Registrierung erstellten Vertrauenspunkt

zugeordnet. In diesem Beispiel lautet der Trustpoint-Name "microsoft-ca" (nur relevante Ausgabe wird angezeigt):

```
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
```

Überprüfen der LSC-Konfiguration des 9800 WLC

Um die Details über den Wireless-Management-Trustpoint zu überprüfen, führen Sie den Befehl **show wireless management trustpoint** aus, stellen Sie sicher, dass der richtige Trustpoint (der die LSC-Details enthält, in diesem Beispiel AP-LSC) verwendet wird und als Available gekennzeichnet ist:

```
9800-L#show wireless management trustpoint

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

```
Private key Info : Available
```

Um die Details zur Konfiguration der AP-LSC-Bereitstellung sowie die Liste der APs zu überprüfen, die der Bereitstellungsliste hinzugefügt wurden, führen Sie den Befehl **show ap lsc-provisionierungszusammenfassung aus**. Stellen Sie sicher, dass der richtige Bereitstellungsstatus angezeigt wird:

```
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
```

Installation des Access Point-Zertifikats überprüfen

Um die im Access Point installierten Zertifikate zu überprüfen, führen Sie den Befehl **show crypto** aus der AP-CLI aus, stellen Sie sicher, dass sowohl das CA Root-Zertifikat als auch das Device-Zertifikat vorhanden sind (die Ausgabe enthält nur relevante Daten):

```
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)
```

Wenn LSC für die Switch-Port dot1x-Authentifizierung verwendet wird, können Sie vom Access Point überprüfen, ob die Port-Authentifizierung aktiviert ist.

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

> **Hinweis**: Um Port dot1x für die APs zu aktivieren, müssen die dot1x-Anmeldeinformationen für die APs entweder im AP-Profil oder in der AP-Konfiguration selbst mit Dummy-Werten definiert werden.

Fehlerbehebung

Häufige Probleme

1. Wenn die Vorlagen in der Serverregistrierung nicht korrekt zugeordnet sind oder der Server eine Kennwortprüfung erfordert, wird die Zertifikatsanforderung für den 9800 WLC oder die APs abgelehnt.
2. Wenn die IIS-Standardstandorte deaktiviert sind, ist der SCEP-Dienst ebenfalls deaktiviert. Daher ist der im Trustpoint definierte URL nicht erreichbar, und der 9800-WLC sendet keine Zertifikatsanforderung.
3. Wenn die Zeit zwischen dem Server und dem 9800 WLC nicht synchronisiert wird, werden Zertifikate nicht installiert, da die Überprüfung der Zeitvalidierung fehlschlägt.

Debug- und Protokollbefehle

Verwenden Sie diese Befehle, um bei der Anmeldung für das 9800-Controller-Zertifikat Fehler zu beheben:

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

Verwenden Sie zur Fehlerbehebung und Überwachung der AP-Anmeldung die folgenden Befehle:

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

In der AP-Befehlszeile zeigt die **Protokollierung** an, ob der Access Point Probleme mit der Zertifikatsinstallation hatte. Außerdem enthält sie Details zum Grund, warum das Zertifikat nicht

installiert wurde:

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

Beispiel für einen erfolgreichen Anmeldeversuch

Dies ist die Ausgabe der zuvor erwähnten Debugger für eine erfolgreiche Registrierung für den Controller und die zugehörigen APs.

CA Root-Zertifikatsimport in 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.
```

Anmeldung für 9800 WLC-Geräte:

```
[...]
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

Beim Debugging für die AP-Registrierung wird diese Ausgabe von der Controllerseite mehrmals für jeden AP wiederholt, der dem 9800-WLC hinzugefügt wird:

[...]
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
```

Ausgabe für das Debugging der AP-Registrierung:

```
[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
```

Damit ist das Konfigurationsbeispiel für die LSC-Anmeldung über SCEP abgeschlossen.