Konfigurieren von 802.1X auf APs für PEAP oder EAP-TLS mit LSC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Cisco Access Points auf ihrem Switch-Port mithilfe von 802.1X-PEAP- oder EAP-TLS-Methoden authentifiziert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Wireless-Controller

- Access Point
- Switch
- ISE-Server
- Zertifizierungsstelle.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Wireless-Controller: C9800-40-K9 mit 17.09.02
- Access Point: C9117AXI-D
- Switch: C9200L-24P-4G mit 17.06.04
- AAA-Server: ISE-VM-K9 mit 3.1.0.518
- Zertifizierungsstelle: Windows Server 2016

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn Ihre Access Points (APs) sich mit ihrem Switch-Port über 802.1X authentifizieren sollen, verwenden sie standardmäßig das EAP-FAST-Authentifizierungsprotokoll, das keine Zertifikate erfordert. Wenn Sie möchten, dass die APs die PEAP-mschapv2-Methode (bei der die Anmeldeinformationen auf der AP-Seite, aber ein Zertifikat auf der RADIUS-Seite verwendet werden) oder die EAP-TLS-Methode (bei der die Zertifikate auf beiden Seiten verwendet werden) verwenden, müssen Sie zuerst LSC konfigurieren. Nur so kann ein vertrauenswürdiges/Root-Zertifikat auf einem Access Point (und im Fall von EAP-TLS auch ein Gerätezertifikat) bereitgestellt werden. Es ist nicht möglich, dass der Access Point PEAP durchführt und die serverseitige Validierung ignoriert. In diesem Dokument wird zunächst die Konfiguration von LSC und dann die 802.1X-Konfiguration behandelt.

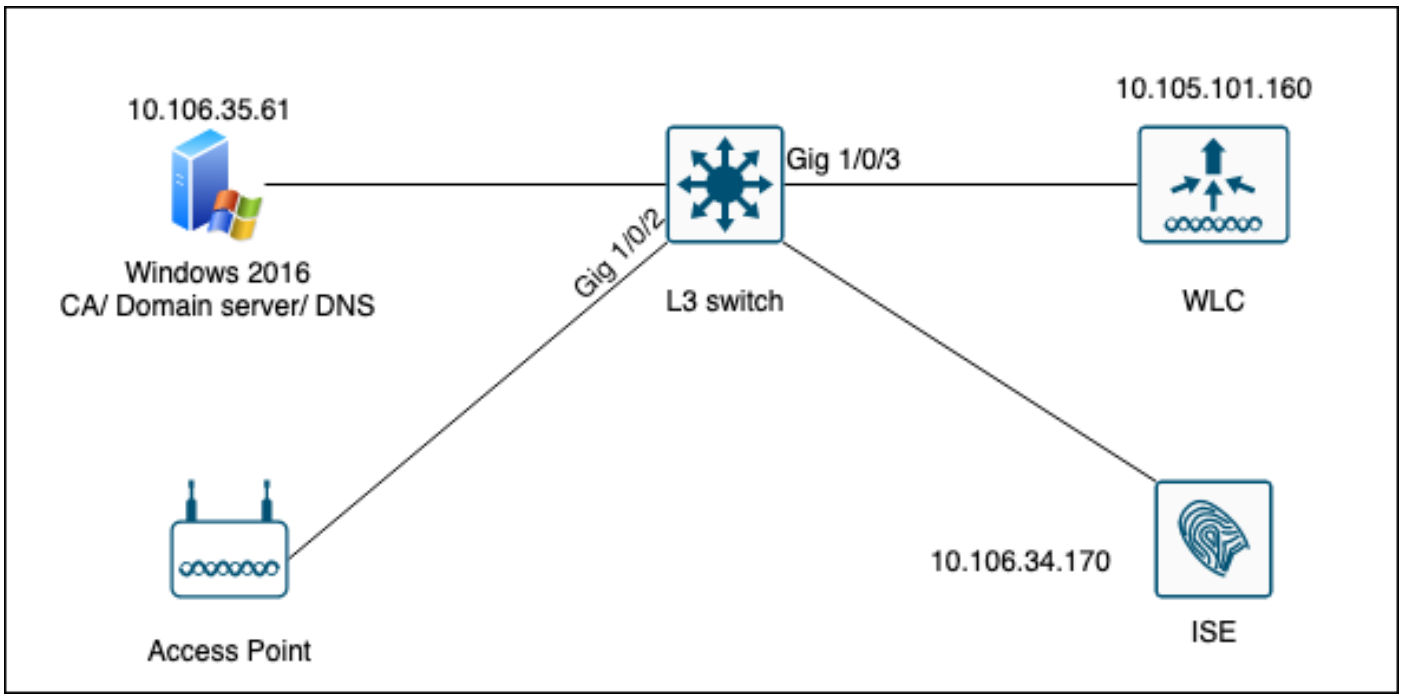
Verwenden Sie ein LSC, wenn Ihre PKI mehr Sicherheit bieten, die Kontrolle über Ihre Zertifizierungsstelle (Certificate Authority, CA) behalten und Richtlinien, Einschränkungen und Verwendungen für die generierten Zertifikate definieren soll.

Mit LSC erhält der Controller ein von der CA ausgestelltes Zertifikat. Ein Access Point kommuniziert nicht direkt mit dem CA-Server, aber der WLC fordert Zertifikate für die beitretenden Access Points an. Die CA-Serverdetails müssen auf dem Controller konfiguriert werden und zugänglich sein.

Der Controller leitet die auf den Geräten generierten certReqs mithilfe des Simple Certificate Enrollment Protocol (SCEP) an die Zertifizierungsstelle weiter und verwendet erneut SCEP, um die signierten Zertifikate von der Zertifizierungsstelle abzurufen.

Das SCEP ist ein Zertifikatverwaltungsprotokoll, das von den PKI-Clients und CA-Servern verwendet wird, um die Zertifikatregistrierung und den Widerruf zu unterstützen. Es wird häufig von Cisco verwendet und von vielen CA-Servern unterstützt. In SCEP wird HTTP als Transportprotokoll für PKI-Nachrichten verwendet. Das Hauptziel von SCEP ist die sichere Ausstellung von Zertifikaten an Netzwerkgeräte.

Netzwerkdiagramm



Konfigurieren

Es müssen hauptsächlich zwei Dinge konfiguriert werden: die SCEP-CA und der 9800 WLC.

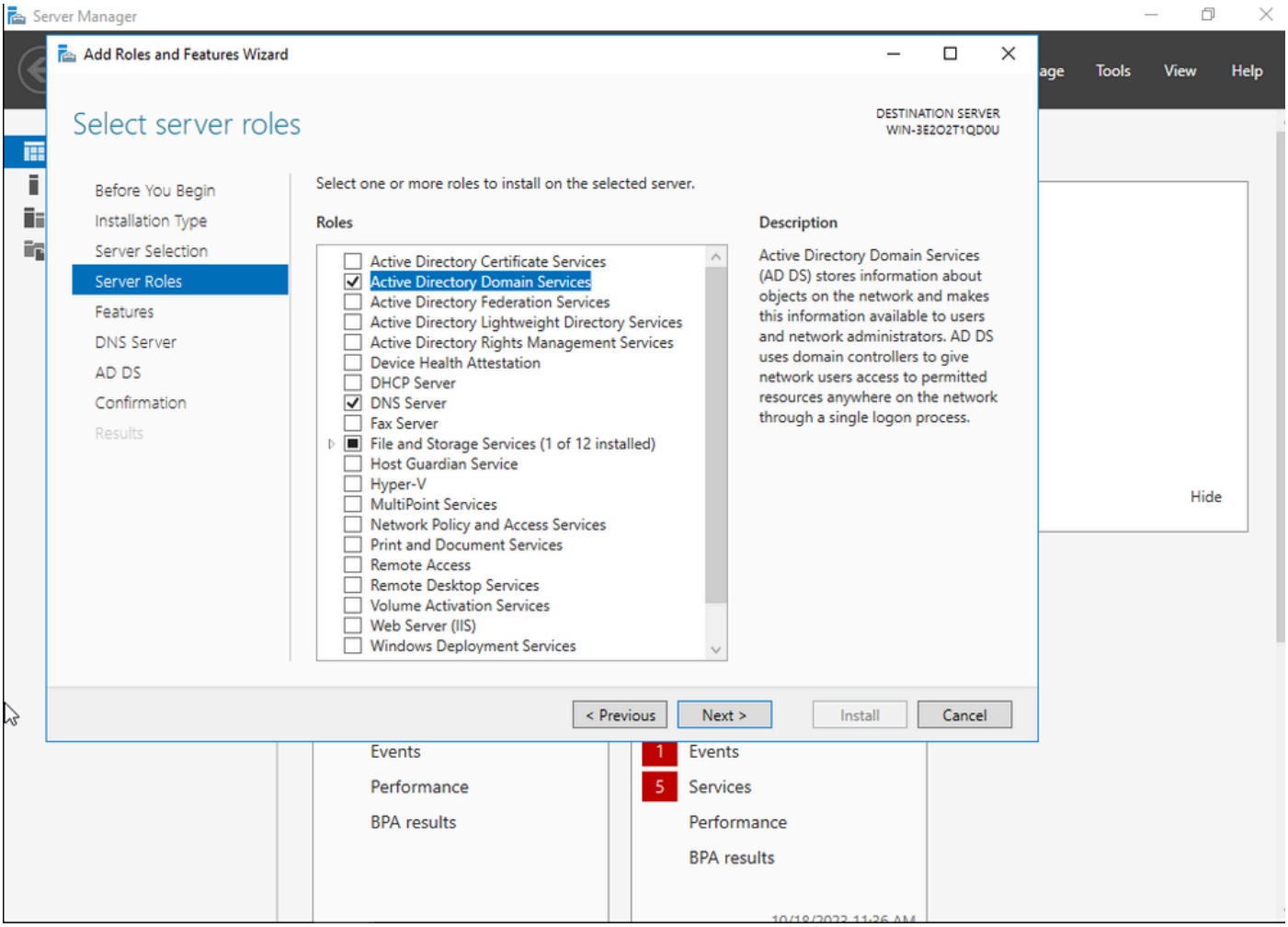
Windows Server 2016 SCEP-CA

In diesem Dokument wird eine grundlegende Installation einer Windows Server SCEP-Zertifizierungsstelle für Übungszwecke behandelt. Eine tatsächliche Windows-Zertifizierungsstelle der Produktionsklasse muss für den Geschäftsbetrieb sicher und angemessen konfiguriert werden. Dieser Abschnitt soll Ihnen helfen, die Konfiguration in der Übung zu testen und sich von den erforderlichen Einstellungen inspirieren zu lassen. So gehen Sie vor:

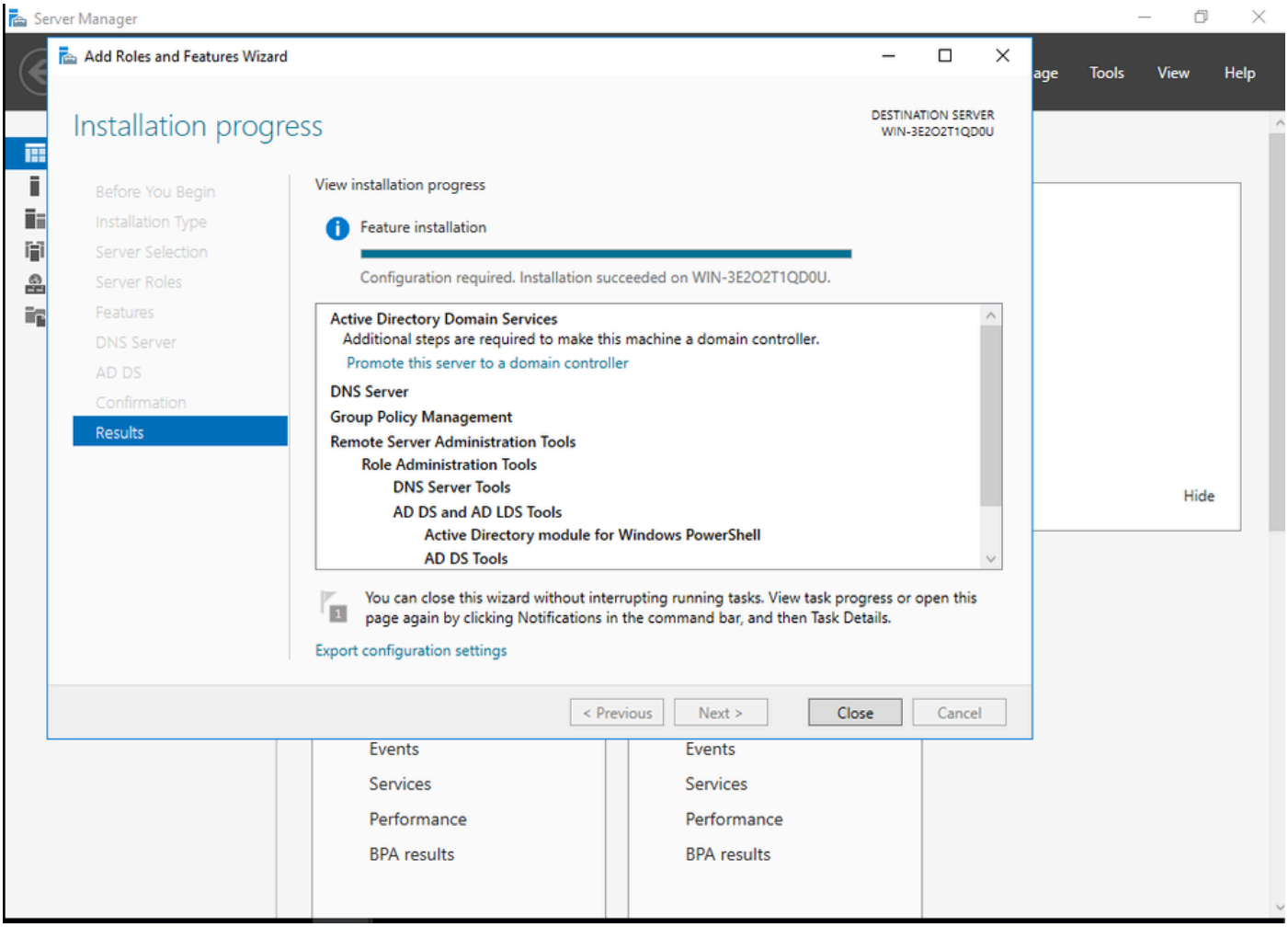
Schritt 1:Installieren Sie ein neues Windows Server 2016 Desktop Experience-Tool.

Schritt 2:Stellen Sie sicher, dass auf Ihrem Server eine statische IP-Adresse konfiguriert ist.

Schritt 3.Installieren Sie eine neue Rolle und einen neuen Dienst, beginnen Sie mit den Active Directory-Domänendiensten und dem DNS-Server.

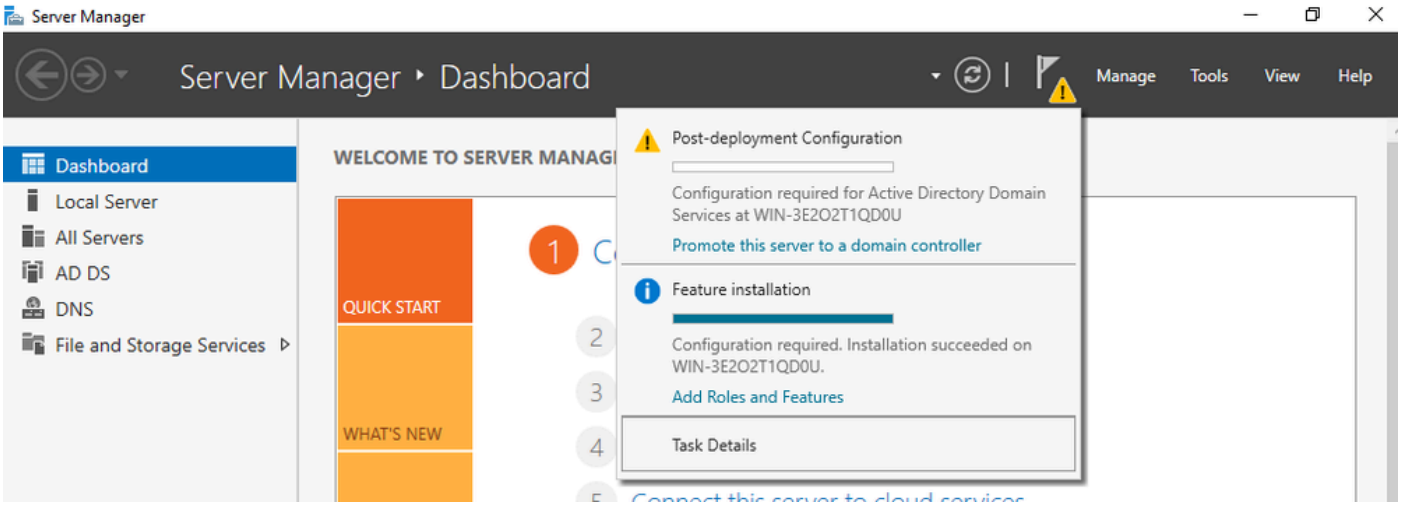


Active Directory-Installation



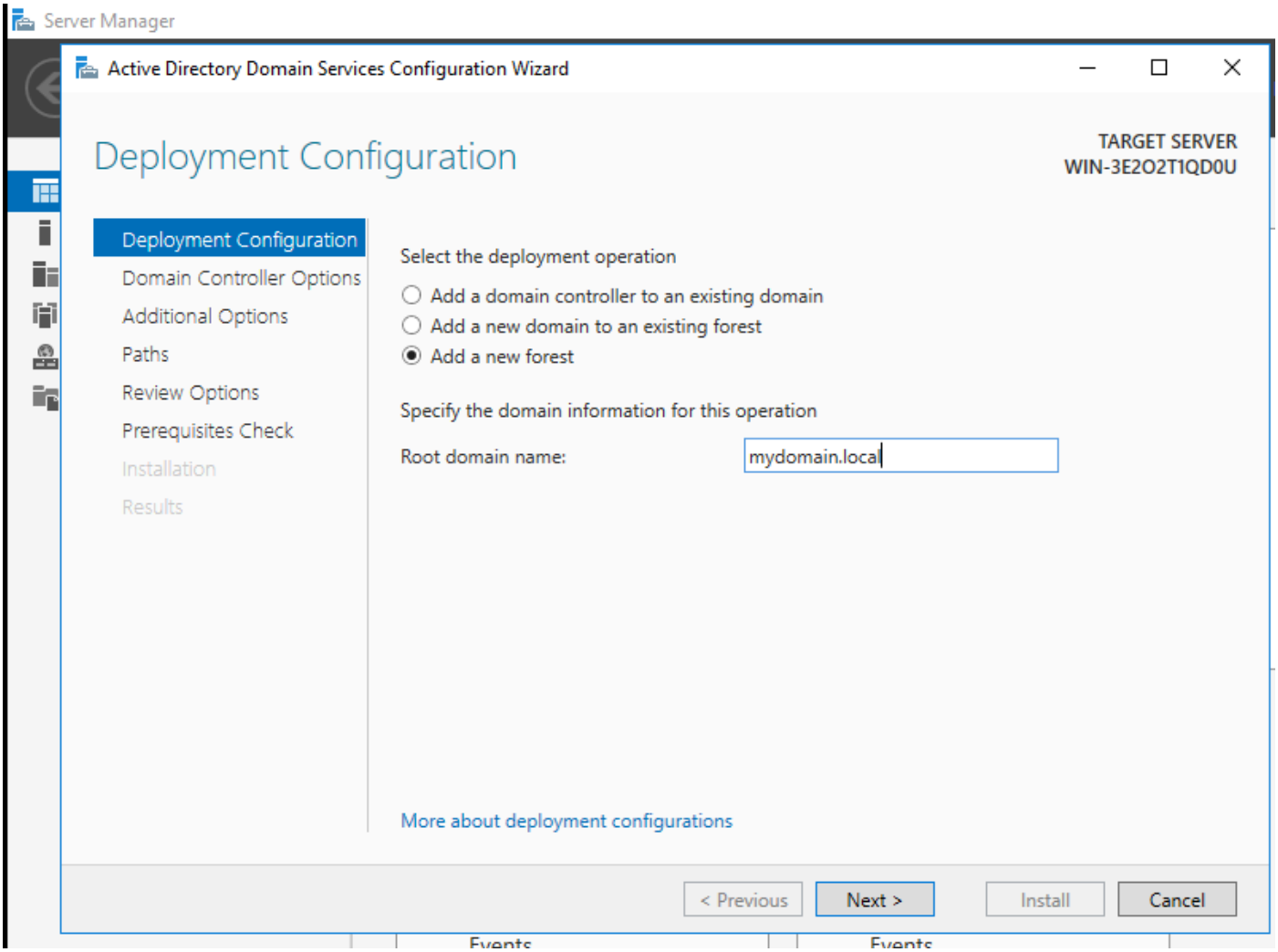
Ende der AD-Installation

Schritt 4.Klicken Sie abschließend im Dashboard auf Diesen Server zu einem Domänencontroller heraufstufen.



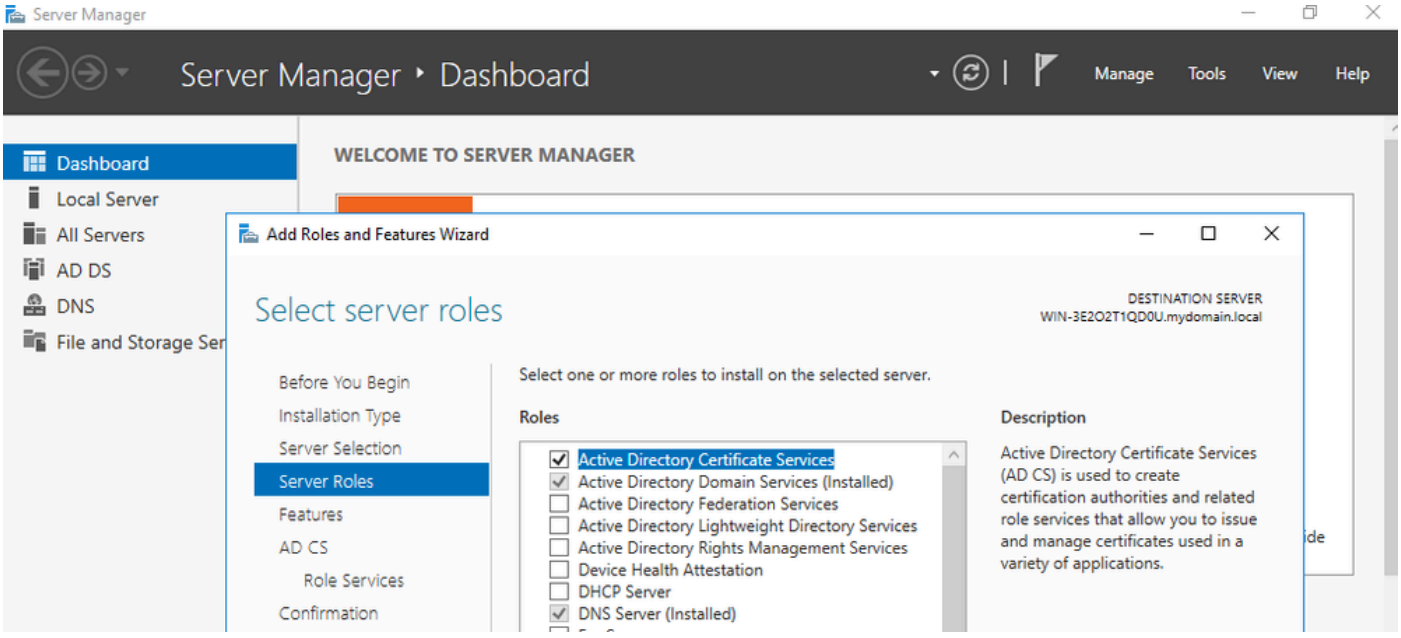
Konfigurieren der AD-Dienste

Schritt 5: Erstellen Sie eine neue Gesamtstruktur, und wählen Sie einen Domänennamen aus.

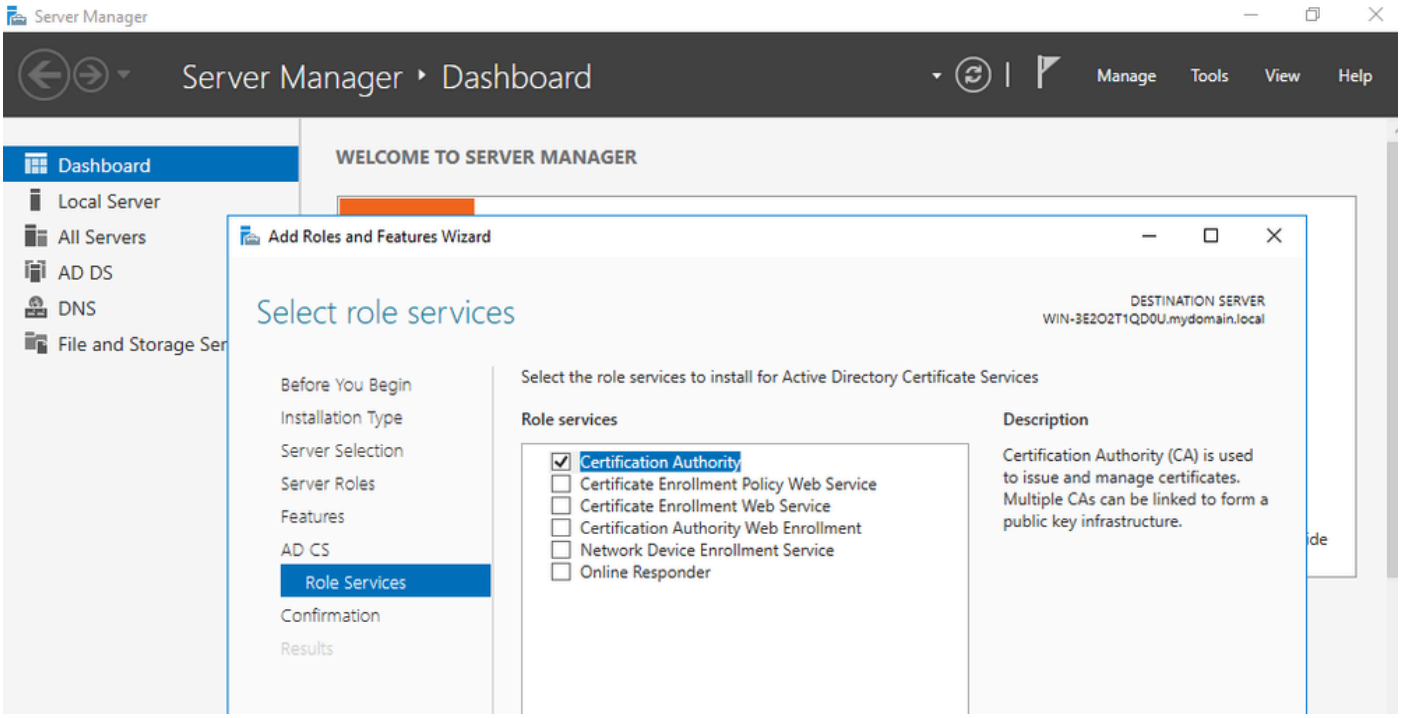


Wählen Sie einen Gesamtstrukturnamen

Schritt 6: Hinzufügen der Zertifikatdienste-Rolle zum Server:

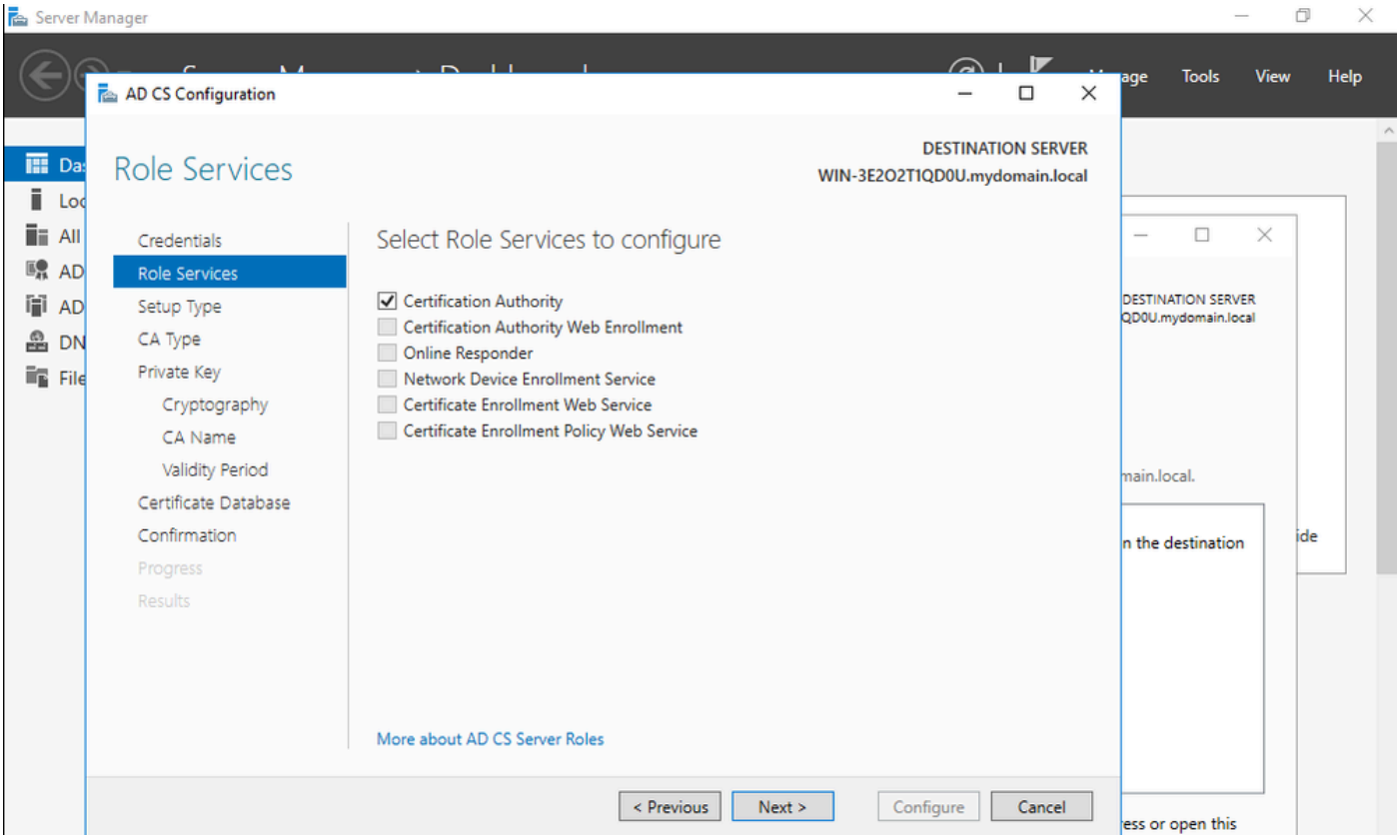


Zertifikatdienste hinzufügen

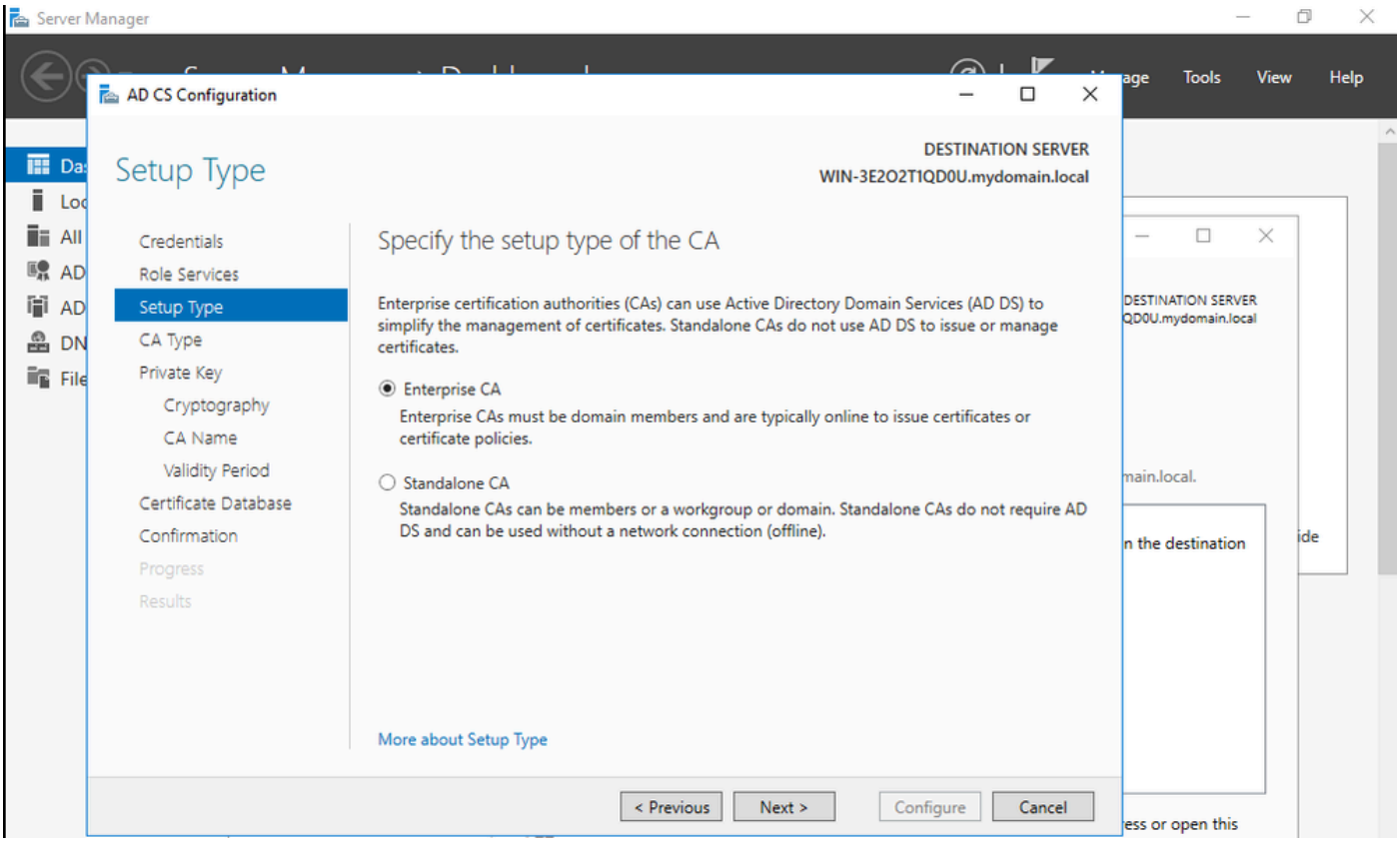


Nur Zertifizierungsstelle hinzufügen

Schritt 7: Konfigurieren Sie anschließend Ihre Zertifizierungsstelle.

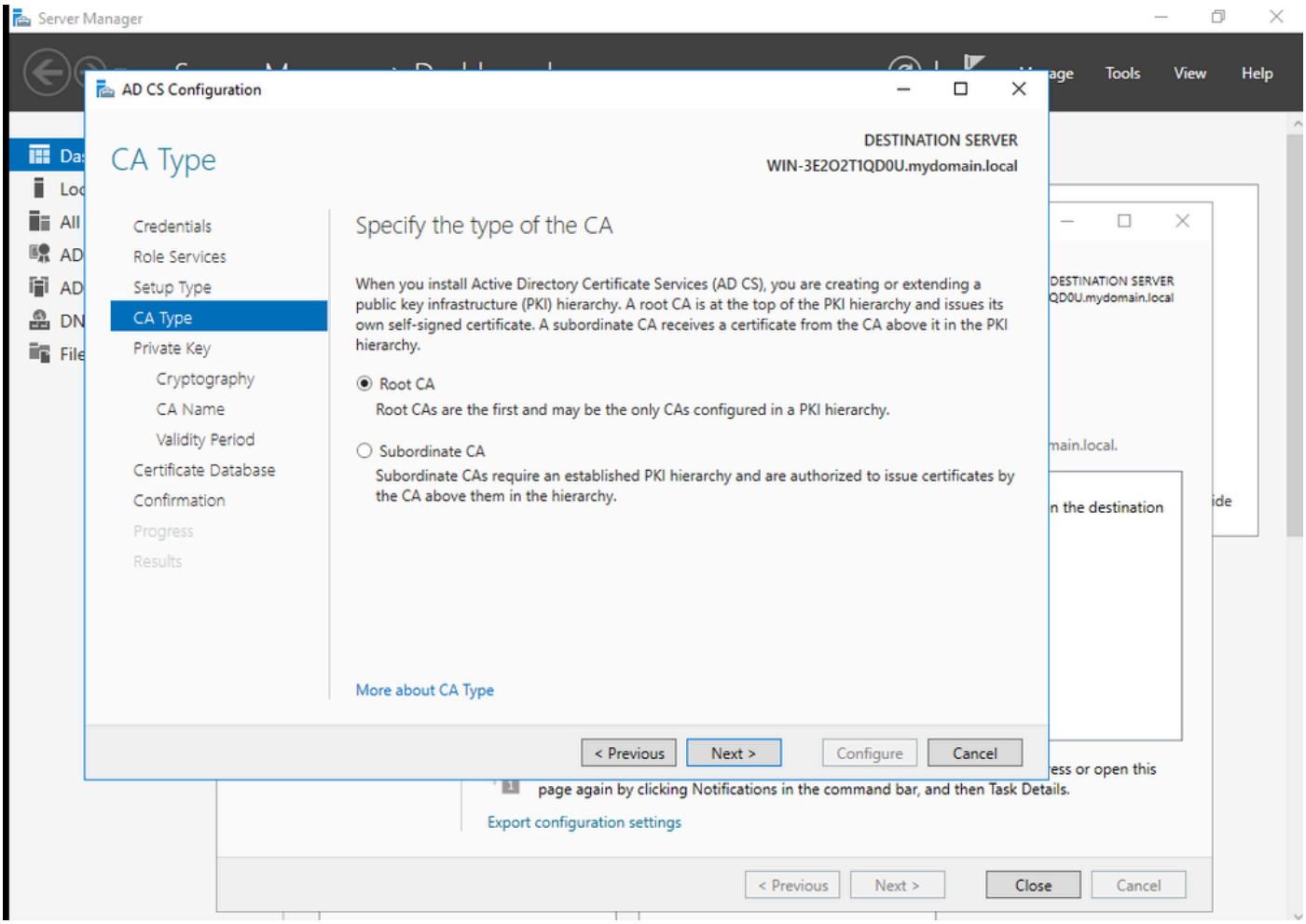


Schritt 8: Wählen Sie eine Enterprise CA aus.



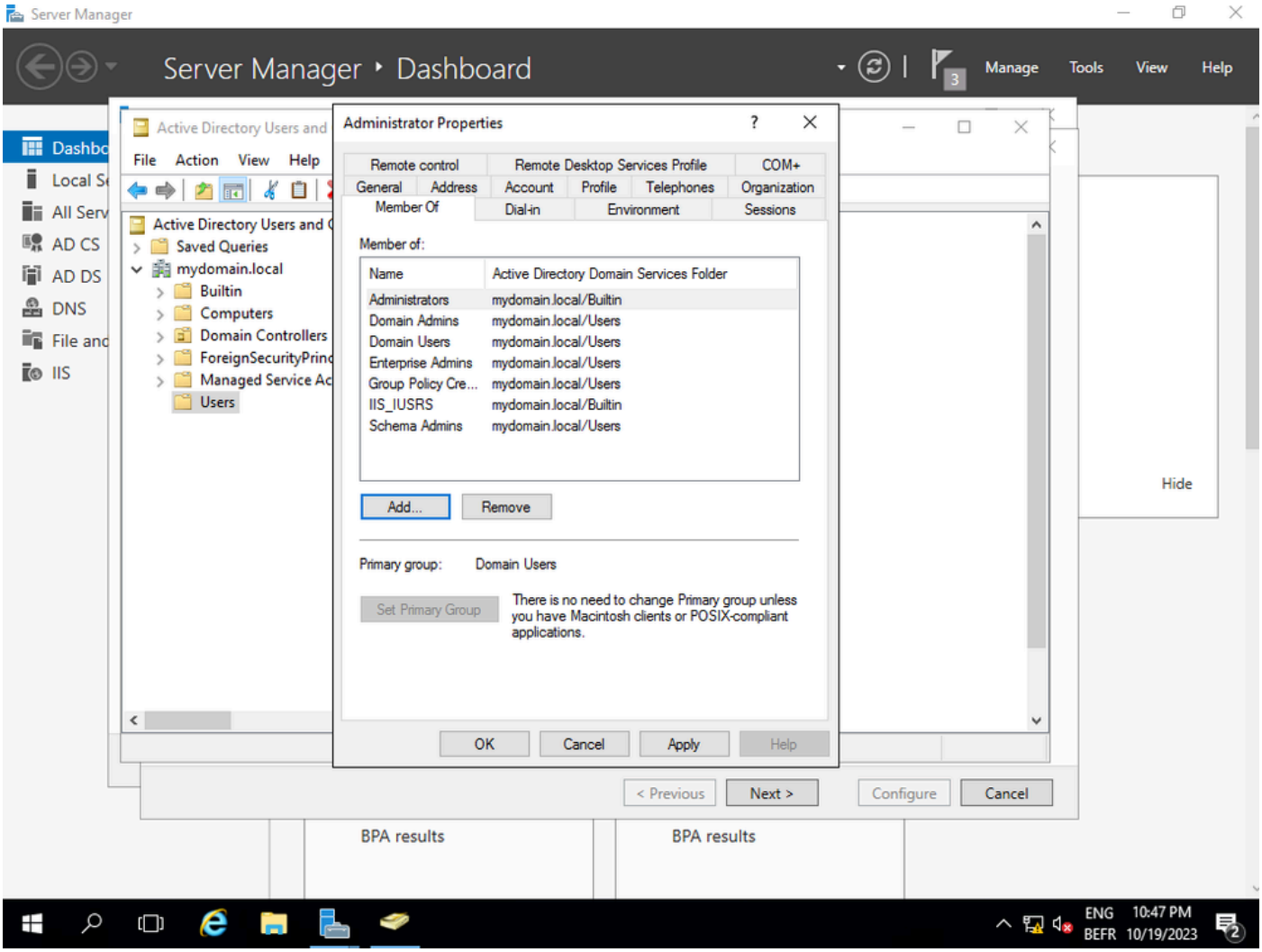
Enterprise-CA

Schritt 9: Erstellen einer Stammzertifizierungsstelle Seit Cisco IOS XE 17.6 werden untergeordnete CAs für LSC unterstützt.



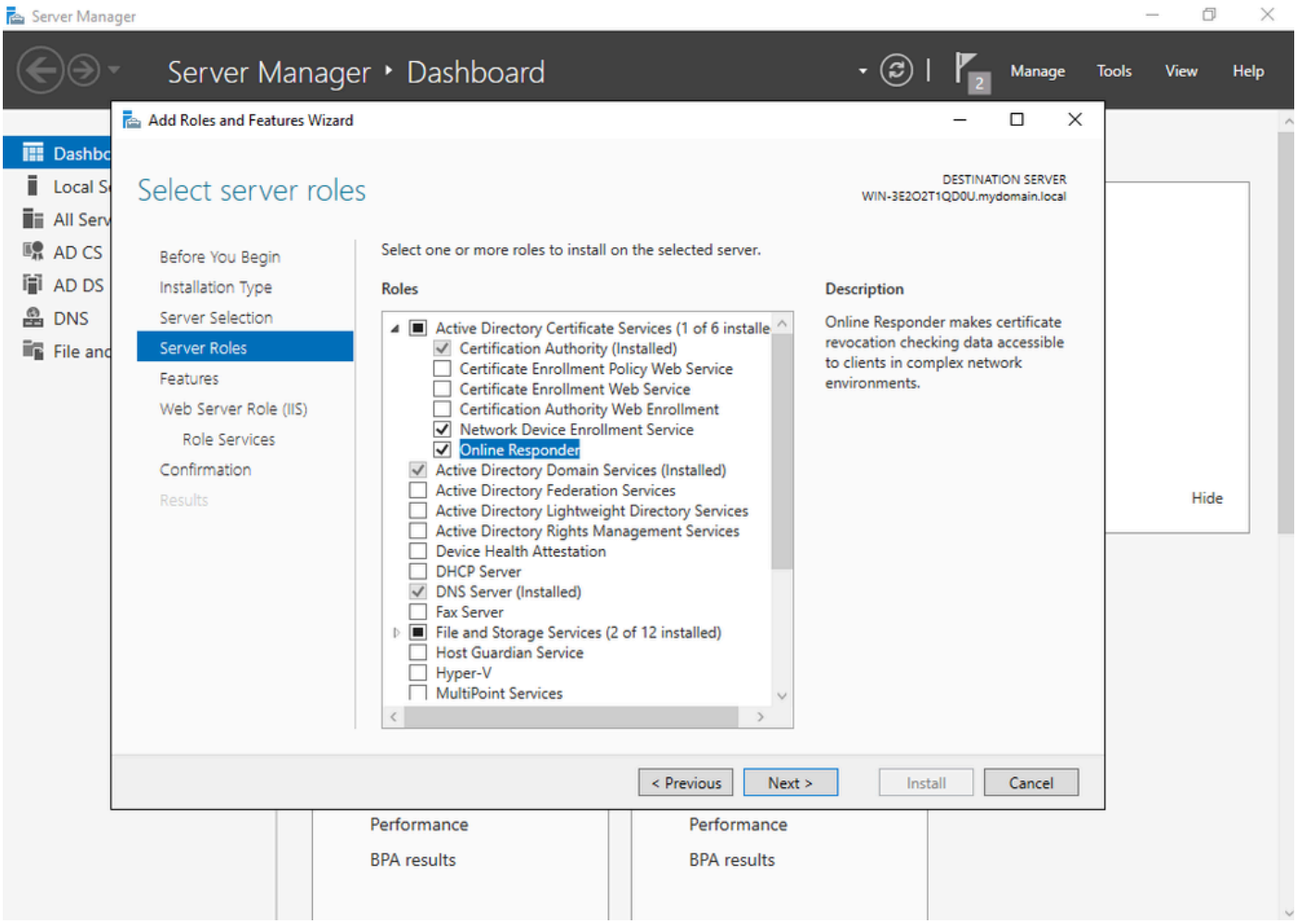
Stammzertifizierungsstelle auswählen

Es ist wichtig, dass das Konto, das Sie für Ihre Zertifizierungsstelle verwenden, Teil der Gruppe IIS_IUSRS ist. In diesem Beispiel verwenden Sie das Administratorkonto und gehen zum Menü Active Directory-Benutzer und -Computer, um die Administratorbenutzer zur Gruppe IIS_IUSRS hinzuzufügen.



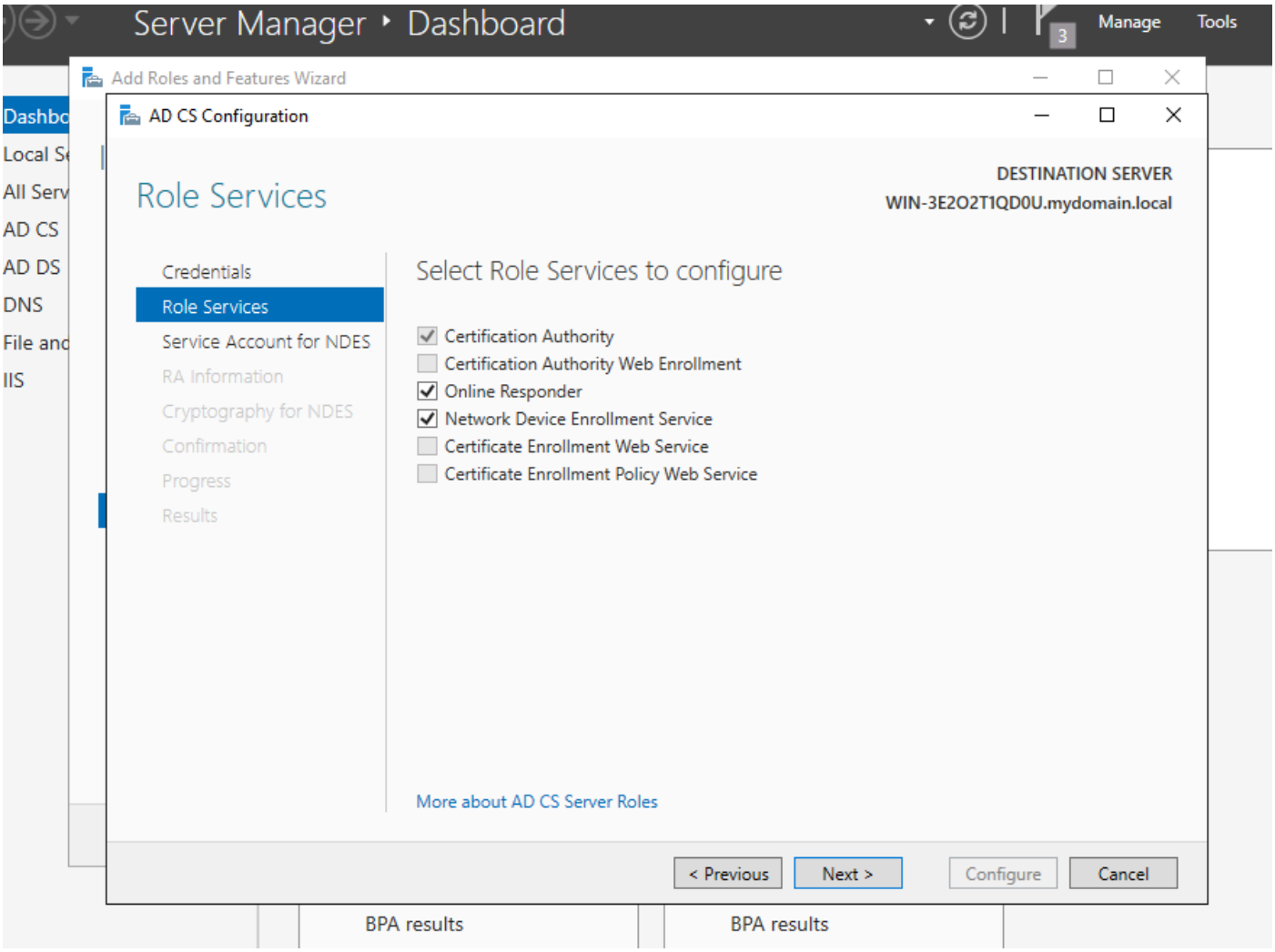
Fügen Sie Ihr Administratorkonto zur Gruppe IIS_USER hinzu.

Schritt 10.Sobald sich ein Benutzer in der richtigen IIS-Gruppe befindet, fügen Sie Rollen und Dienste hinzu. Fügen Sie dann die Online Responder- und NDES-Services Ihrer Zertifizierungsstelle hinzu.



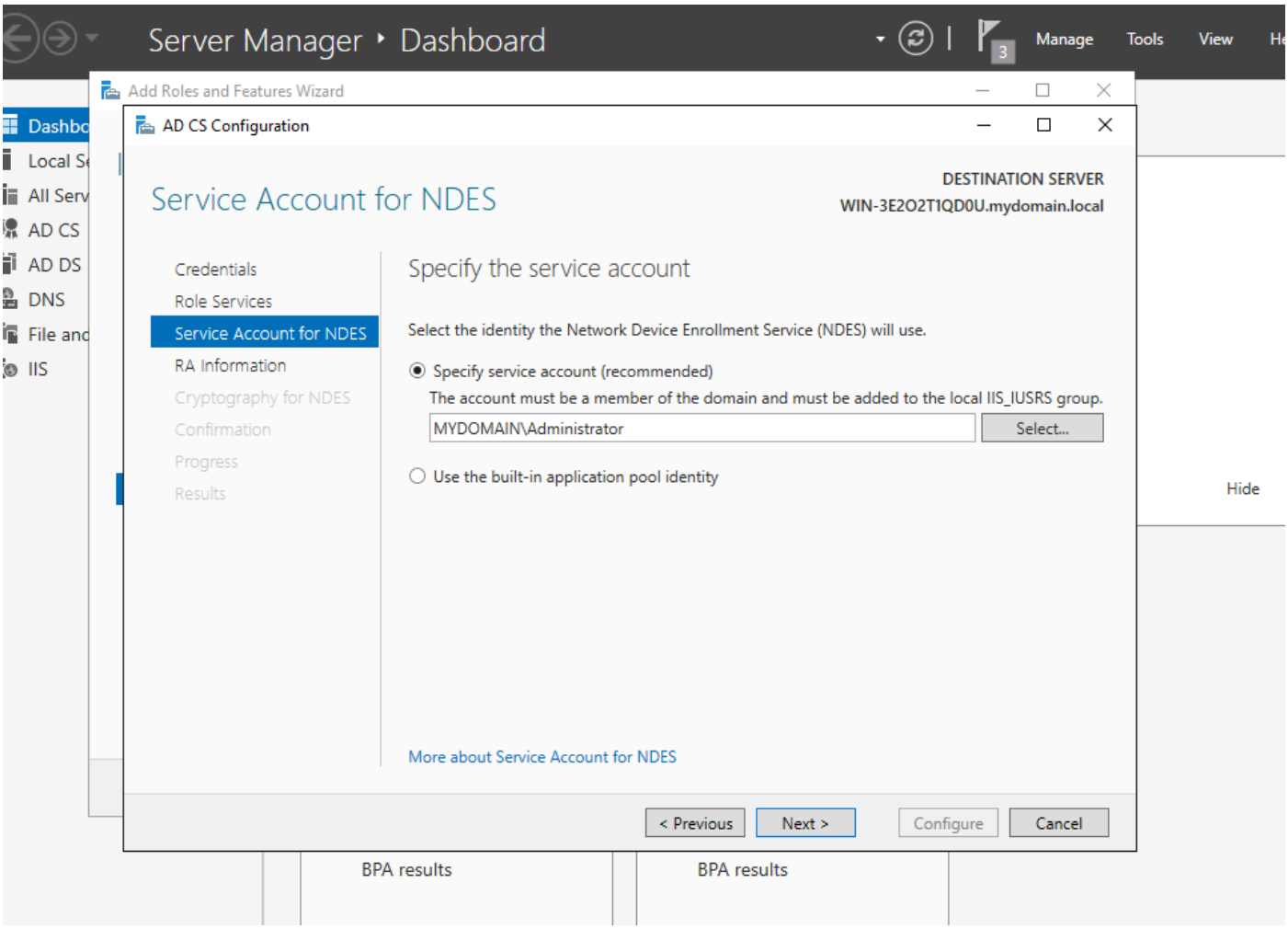
Installation der NDES- und Online-Responder-Services

Schritt 11: Konfigurieren Sie diese Dienste anschließend.



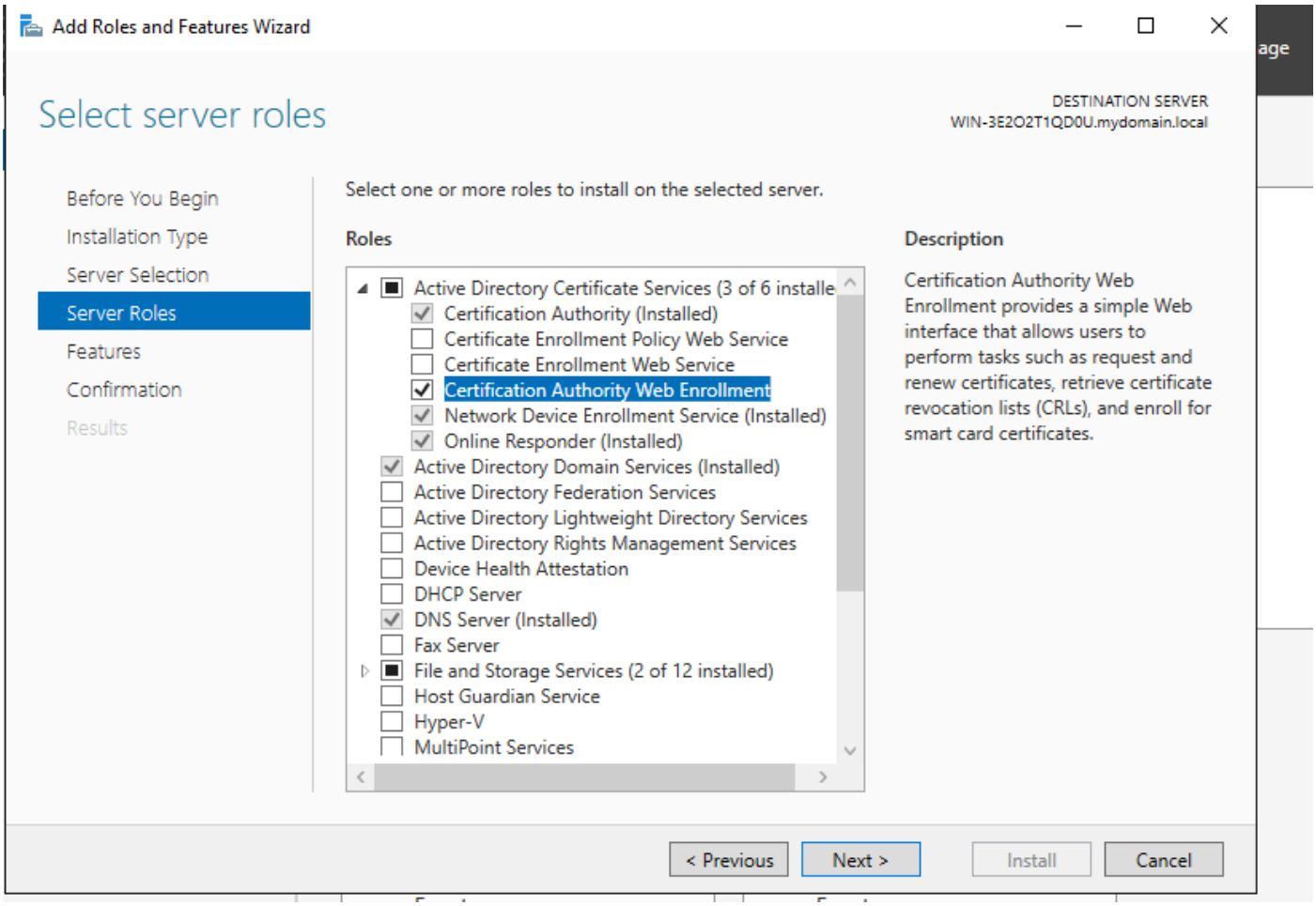
Installation des Online-Responders und des NDES-Service

Schritt 12.Sie werden aufgefordert, ein Dienstkonto auszuwählen. Dies ist das Konto, das Sie zuvor der Gruppe IIS_IUSRS hinzugefügt haben.

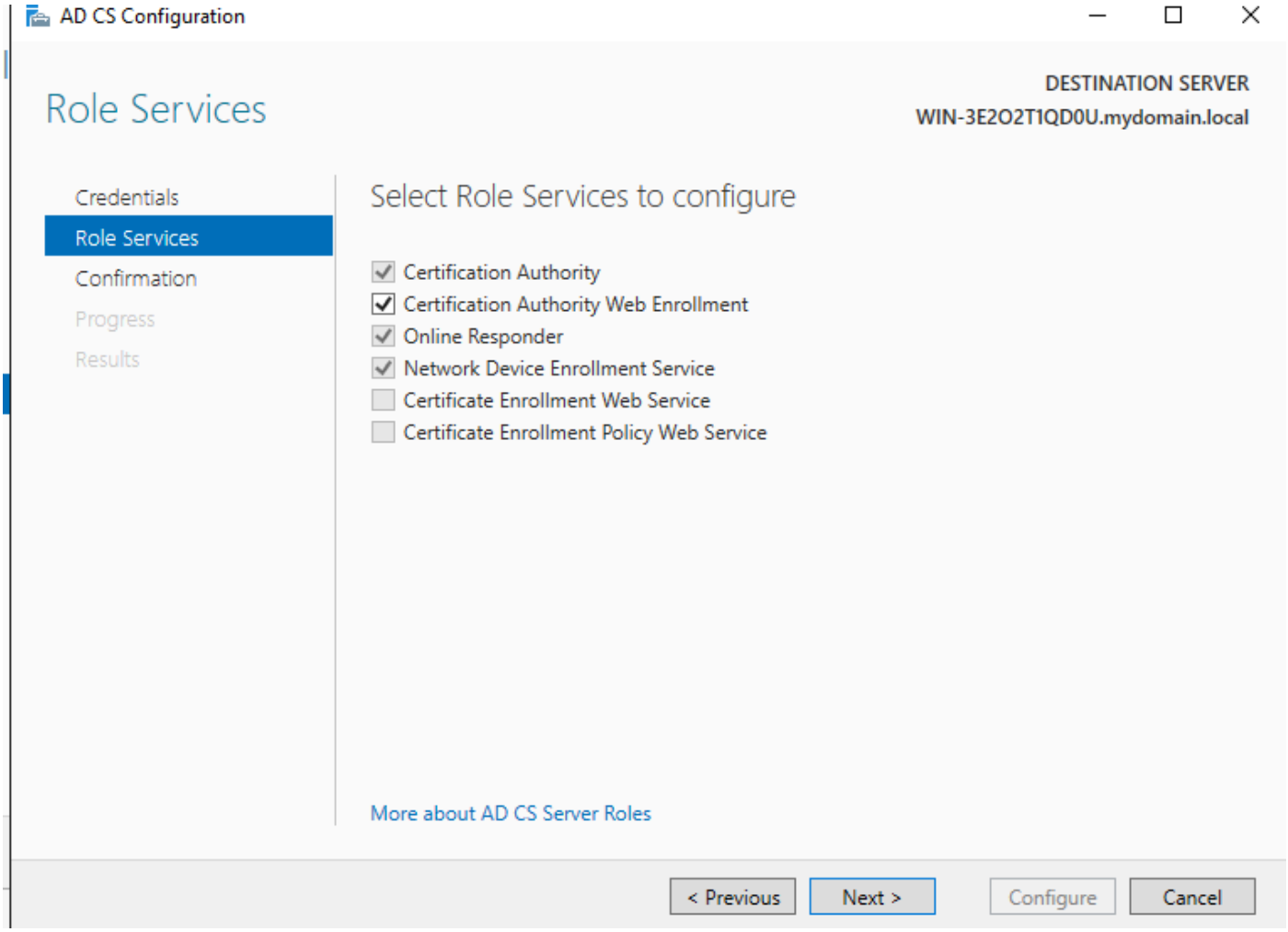


Wählen Sie den Benutzer aus, den Sie der IIS-Gruppe hinzugefügt haben.

Schritt 13.Dies ist für SCEP-Vorgänge ausreichend. Um jedoch eine 802.1X-Authentifizierung zu erreichen, müssen Sie auf dem RADIUS-Server auch ein Zertifikat installieren. Installieren und konfigurieren Sie daher den Webregistrierungsdienst, damit Sie die ISE-Zertifikatanforderung einfach auf unseren Windows Server kopieren und einfügen können.

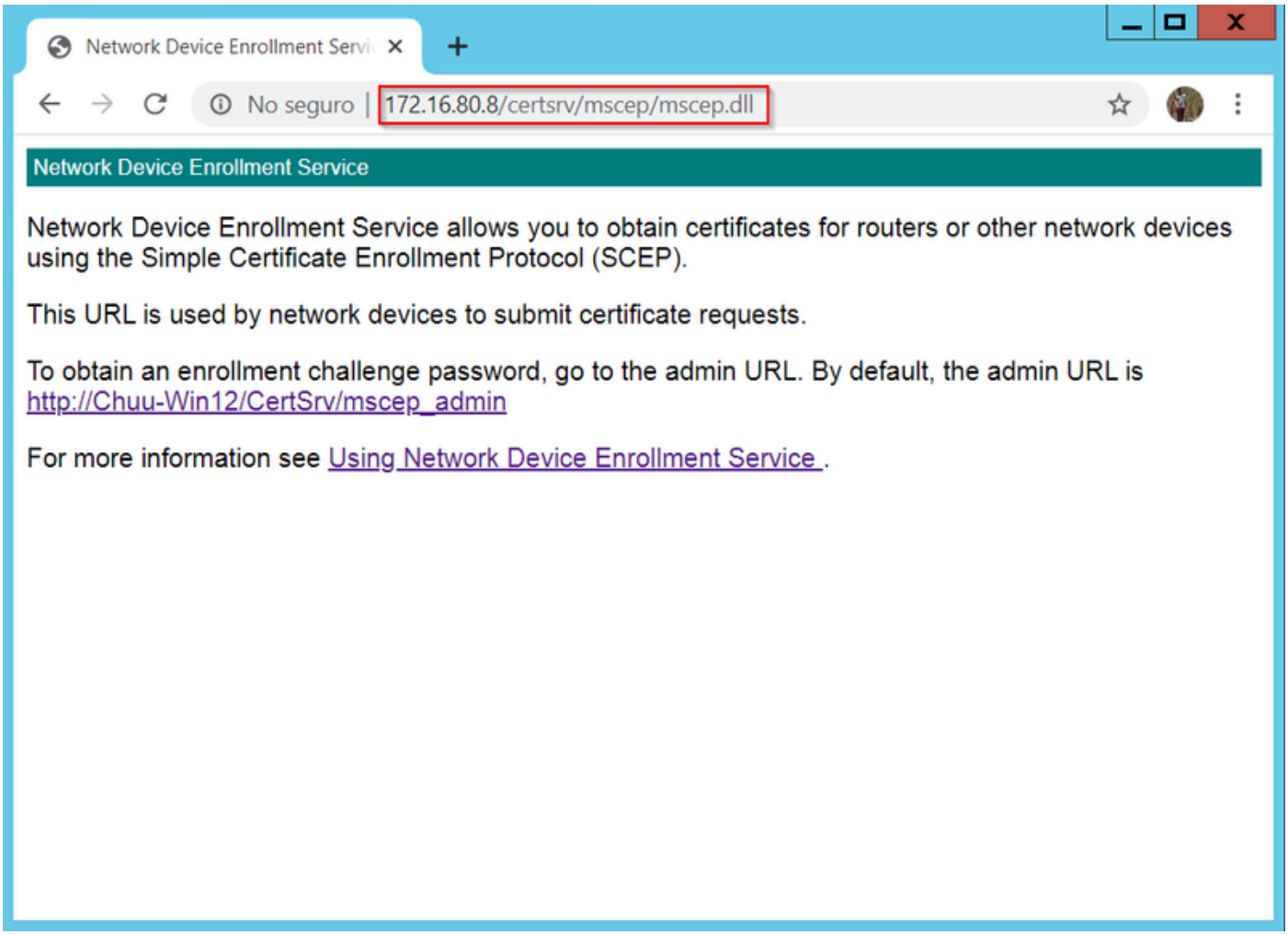


Web-Registrierungsdienst installieren



Konfigurieren des Webregistrierungsdiensts

Schritt 14: Sie können überprüfen, ob der SCEP-Dienst ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter http://<serverip>/certsrv/mscep/mscep.dll :



SCEP-Portalverifizierung

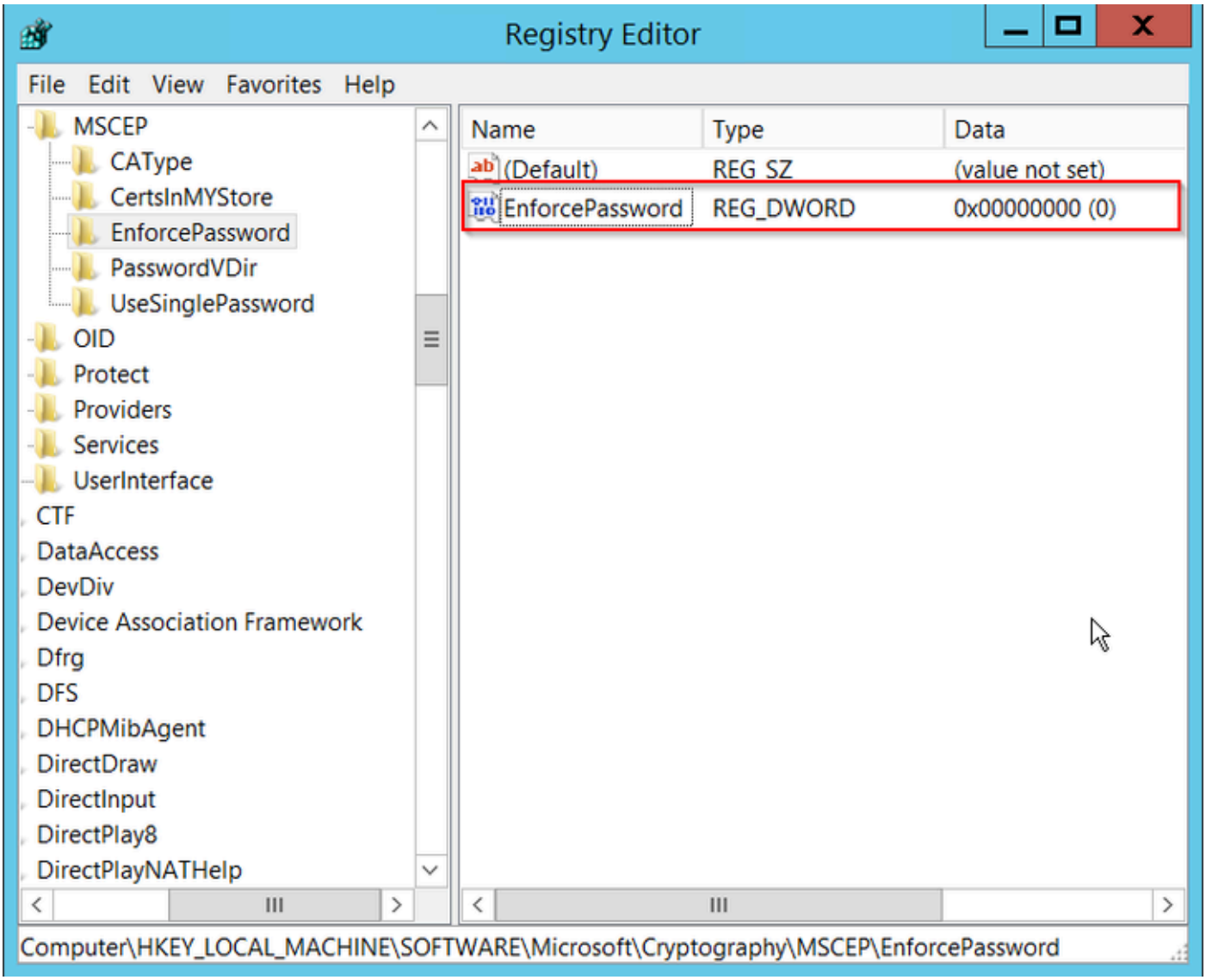
Schritt 15:

Standardmäßig hat Windows Server vor der Registrierung bei Microsoft SCEP (MSCEP) ein dynamisches Challenge-Kennwort zur Authentifizierung von Client- und Endpunktanforderungen verwendet. Hierfür muss ein Admin-Konto in der Web-GUI navigieren, um ein On-Demand-Kennwort für jede Anforderung zu generieren (das Kennwort muss in der Anforderung enthalten sein). Der Controller ist nicht in der Lage, dieses Kennwort in die Anforderungen aufzunehmen, die er an den Server sendet. Um diese Funktion zu entfernen, muss der Registrierungsschlüssel auf dem NDES-Server geändert werden:

Öffnen Sie den Registrierungs-Editor, und suchen Sie im Menü Start nach Regedit.

Navigieren Sie zu Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword.

Ändern Sie den Wert EnforcePassword auf 0. Wenn es bereits 0 ist, dann lassen Sie es wie es ist.



Festlegen des Enforcepassword-Werts

Zertifikatvorlage und Registrierung konfigurieren

Zertifikate und die zugehörigen Schlüssel können in verschiedenen Szenarien für unterschiedliche Zwecke verwendet werden, die durch die Anwendungsrichtlinien innerhalb des Zertifizierungsstellenservers definiert werden. Die Anwendungsrichtlinie wird im Feld Extended Key Usage (EKU) des Zertifikats gespeichert. Dieses Feld wird vom Authentifikator analysiert, um zu überprüfen, ob es vom Client für seinen vorgesehenen Zweck verwendet wird. Um sicherzustellen, dass die richtige Anwendungsrichtlinie in die WLC- und AP-Zertifikate integriert ist, erstellen Sie die richtige Zertifikatvorlage, und ordnen Sie sie der NDES-Registrierung zu:

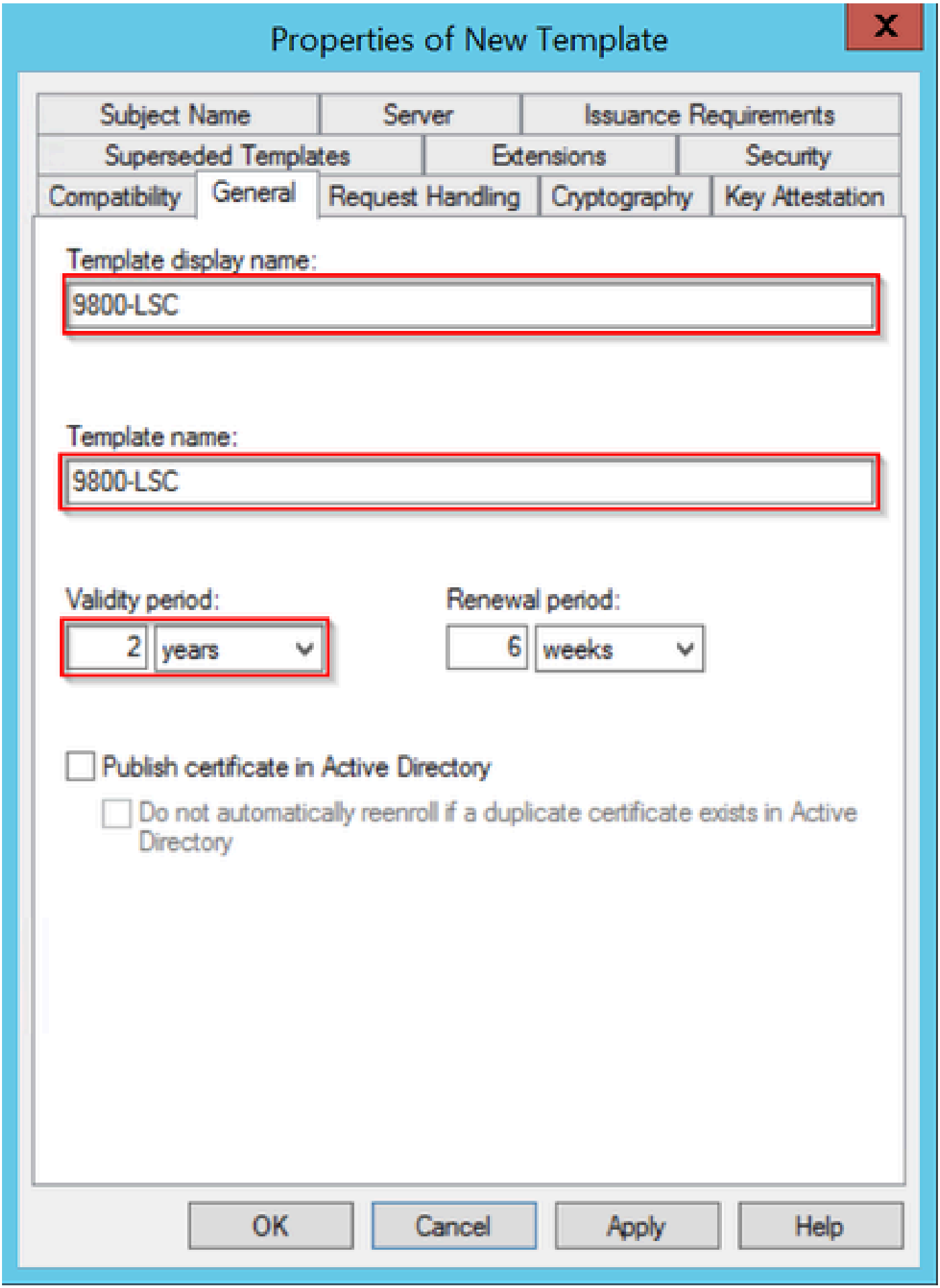
Schritt 1: Navigieren Sie zu Start > Verwaltung > Zertifizierungsstelle.

Schritt 2: Erweitern Sie die Verzeichnisstruktur des CA Servers, klicken Sie mit der rechten Maustaste auf die Ordner Zertifikatvorlagen, und wählen Sie Verwalten.

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

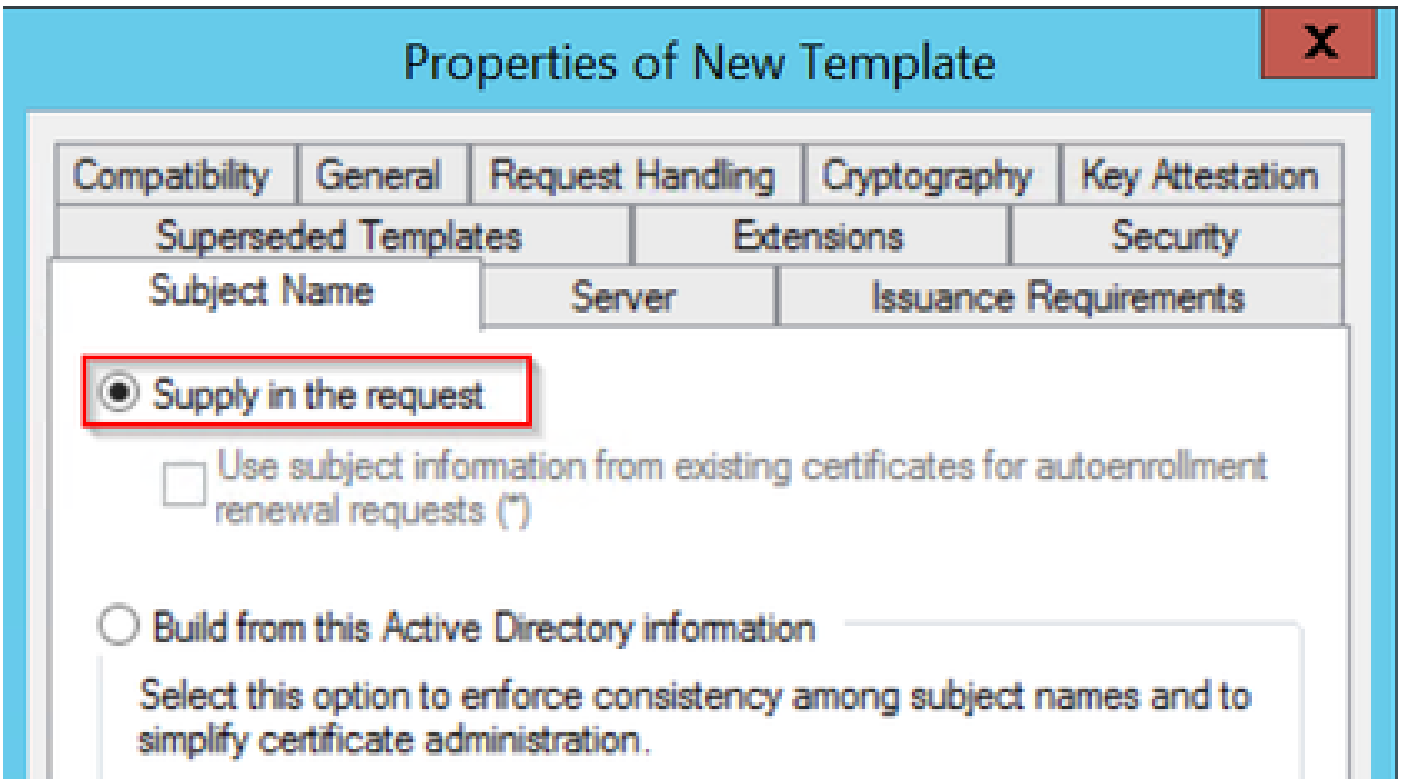
Schritt 4: Navigieren Sie zur Registerkarte Allgemein, ändern Sie den Vorlagennamen und die Gültigkeitsdauer, und lassen Sie alle anderen Optionen deaktiviert.

⚠ Vorsicht: Wenn der Gültigkeitszeitraum geändert wird, stellen Sie sicher, dass er nicht größer als die Stammzertifikatsgültigkeit der Zertifizierungsstelle ist.



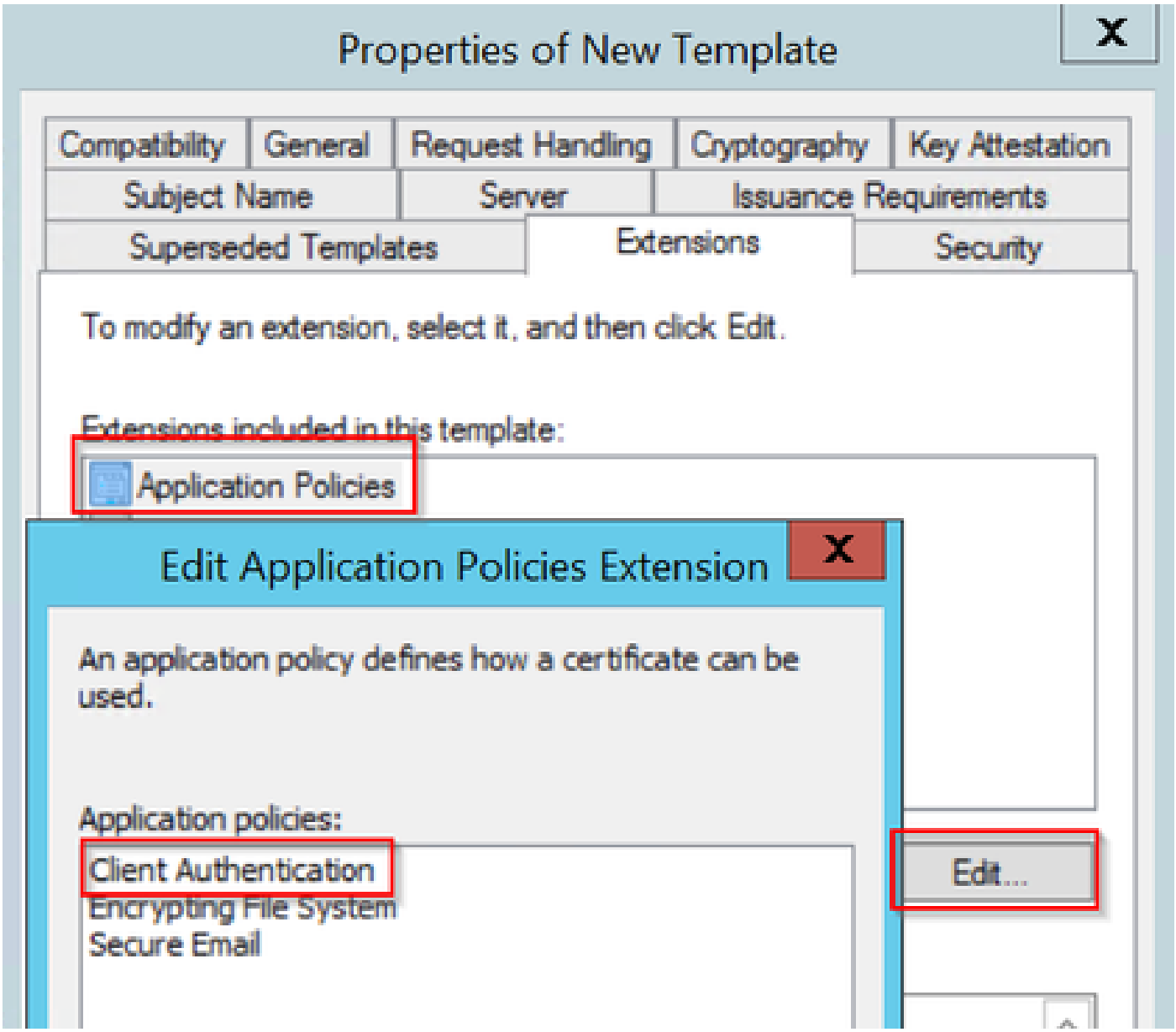
Konfigurieren der Zertifikatvorlage

Schritt 5: Navigieren Sie zur Registerkarte Subject Name (Betreffname), und stellen Sie sicher, dass Supply (Belieferung) in der Anfrage ausgewählt ist. Ein Popup-Fenster zeigt an, dass Benutzer keine Administratorgenehmigung benötigen, um ihr Zertifikat zu signieren. Wählen Sie OK aus.



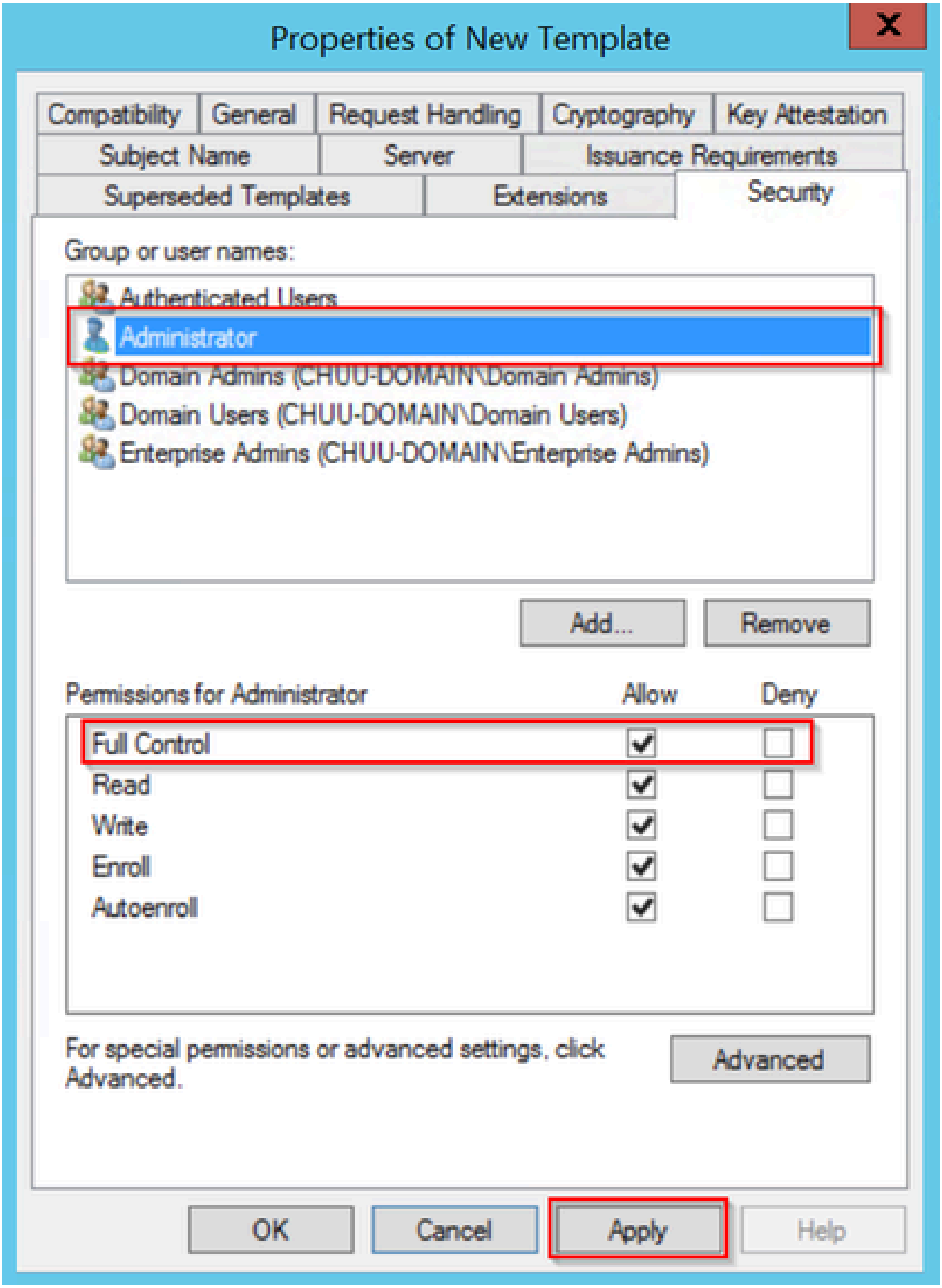
Bereitstellung in der Anforderung

Schritt 6: Navigieren Sie zur Registerkarte Erweiterungen, wählen Sie dann die Option Anwendungsrichtlinien aus, und klicken Sie auf die Schaltfläche Bearbeiten. Stellen Sie sicher, dass sich die Clientauthentifizierung im Fenster Anwendungsrichtlinien befindet. Wählen Sie andernfalls Hinzufügen und fügen Sie sie hinzu.



Durchwahlen überprüfen

Schritt 7. Navigieren Sie zur Registerkarte Sicherheit, und stellen Sie sicher, dass das in Schritt 6 der Option SCEP-Dienste in Windows Server aktivieren definierte Dienstkonto über Vollzugriff-Berechtigungen für die Vorlage verfügt. Wählen Sie anschließend Übernehmen und OK aus.

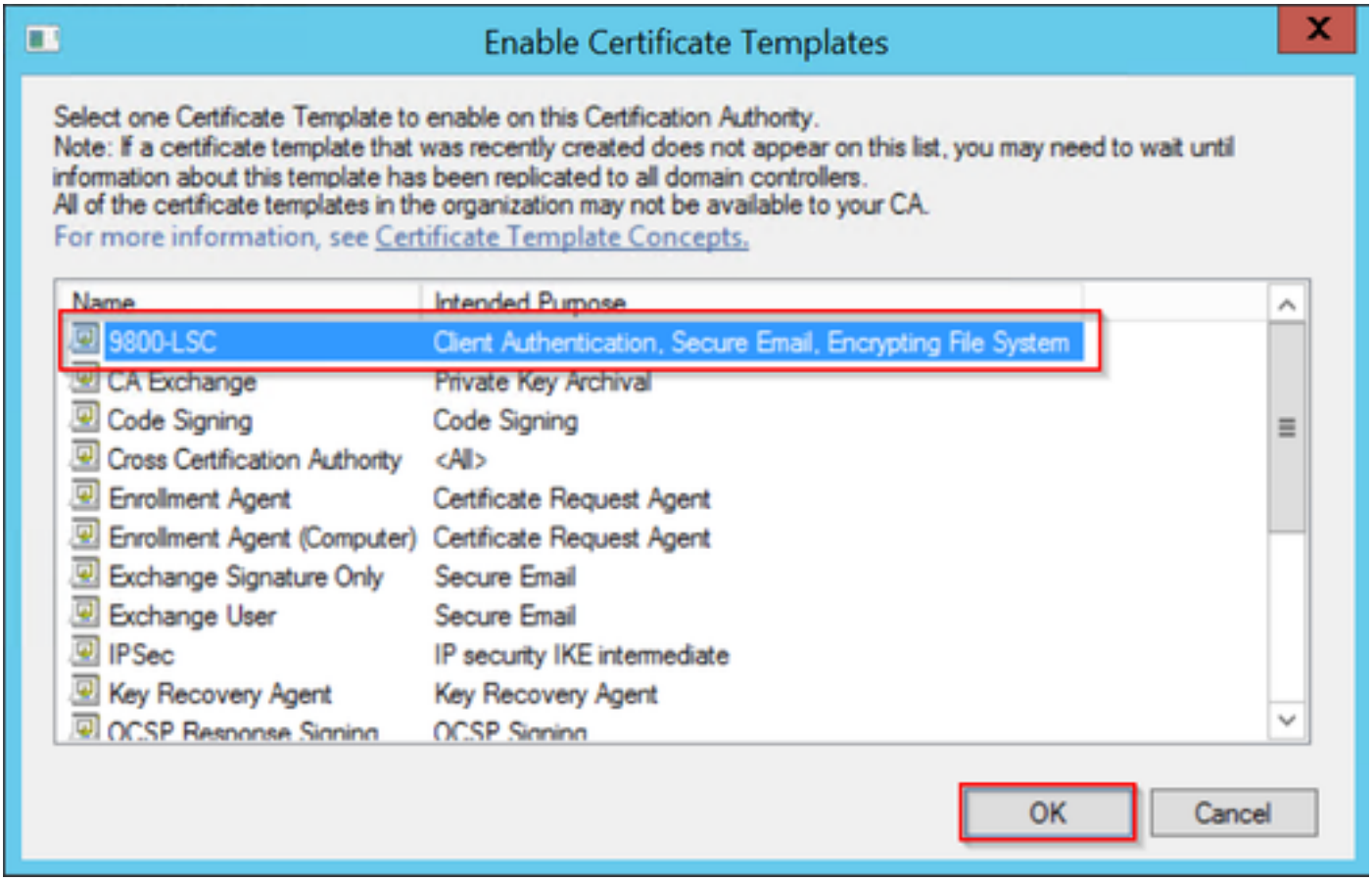


Umfassende Kontrolle

Schritt 8: Kehren Sie zum Fenster Zertifizierungsstelle zurück, klicken Sie mit der rechten Maustaste in den Ordner Zertifikatvorlagen, und wählen Sie Neu > Zertifikatvorlage zur Ausgabe aus.

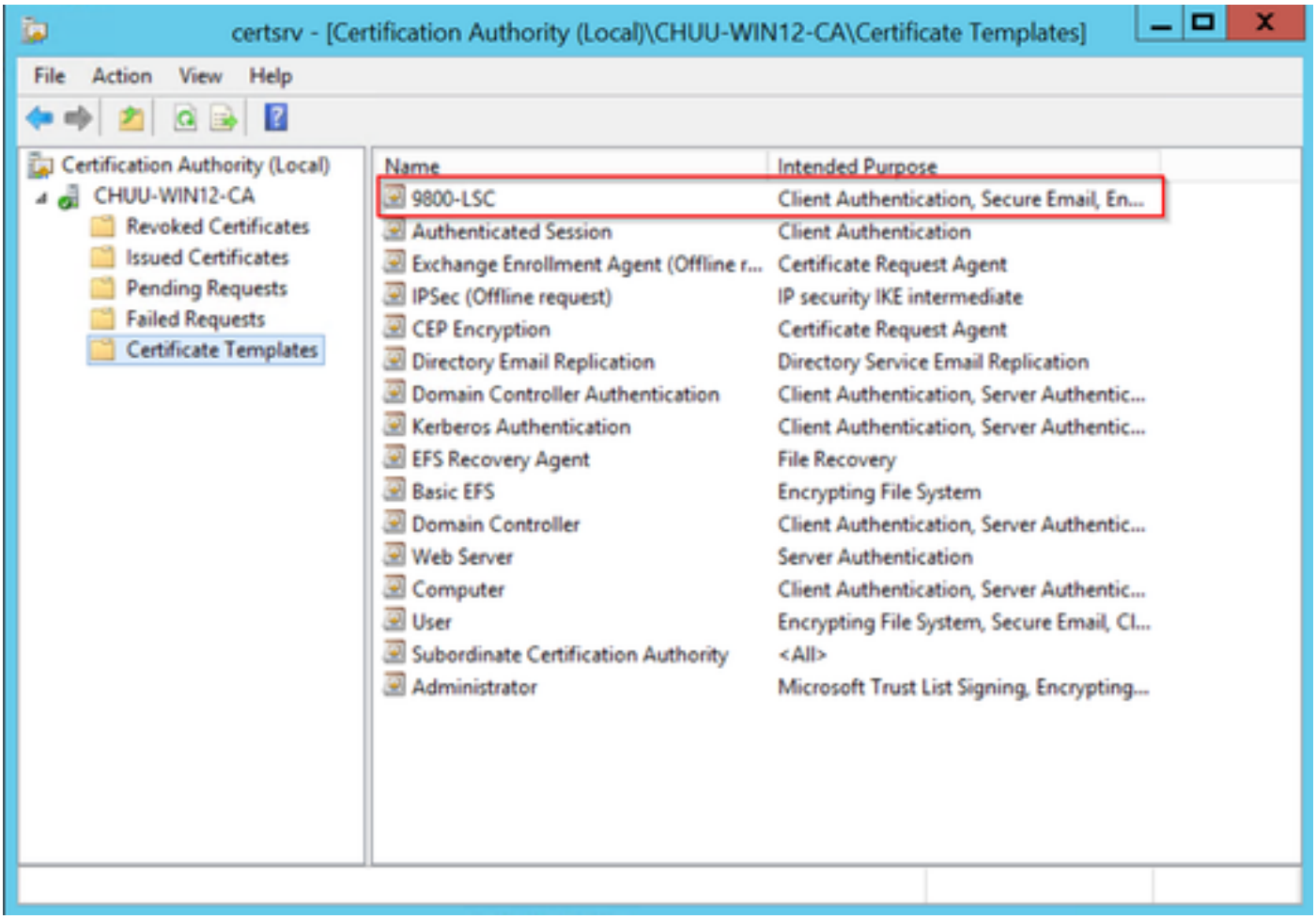
Schritt 9. Wählen Sie die zuvor erstellte Zertifikatvorlage aus (in diesem Beispiel 9800-LSC), und wählen Sie OK aus.

Hinweis: Die neu erstellte Zertifikatvorlage kann länger in mehreren Serverbereitstellungen aufgeführt werden, da sie auf allen Servern repliziert werden muss.



Vorlage auswählen

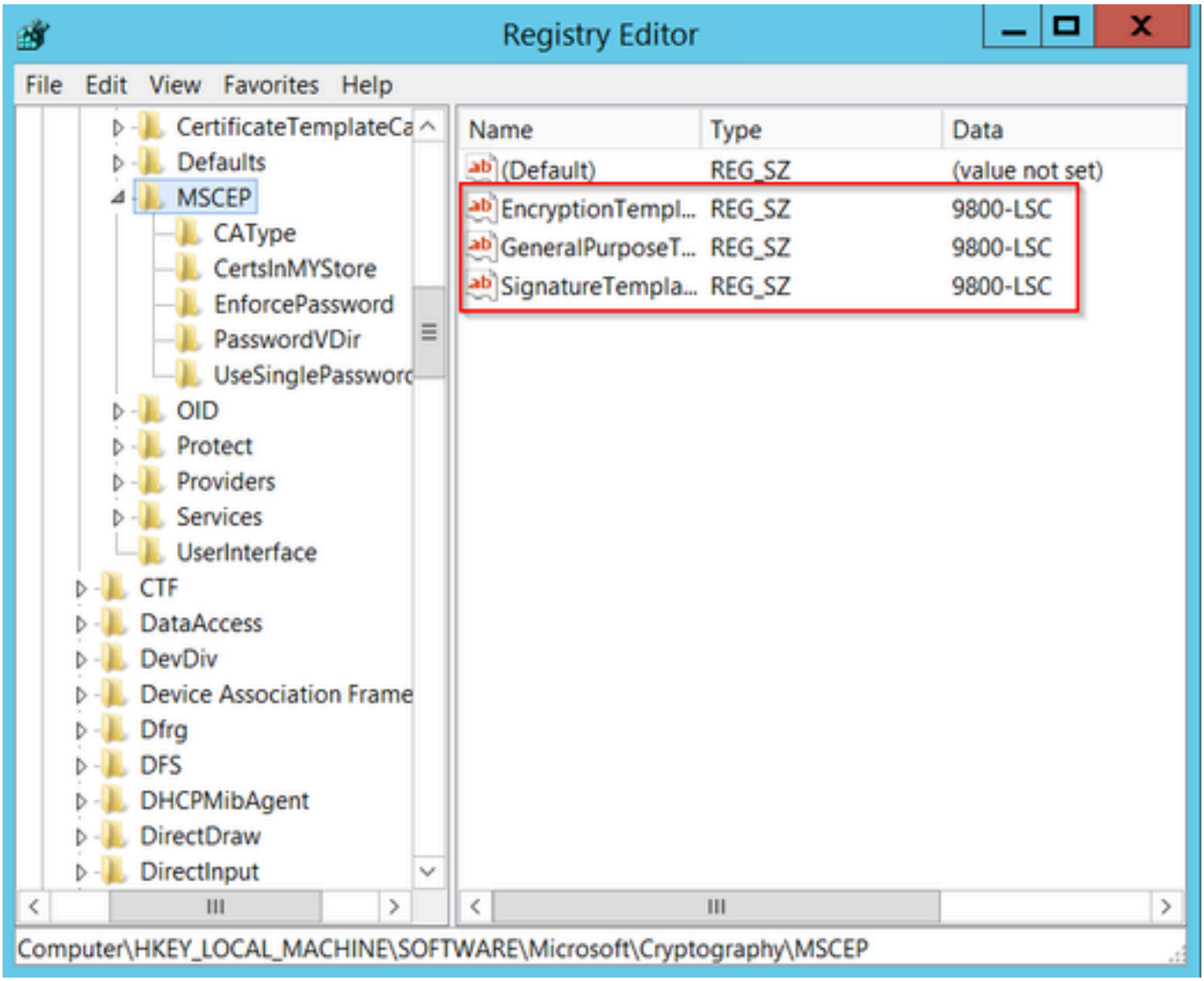
Die neue Zertifikatvorlage wird nun im Ordnerinhalt Zertifikatvorlagen aufgeführt.



Auswahl des LSC

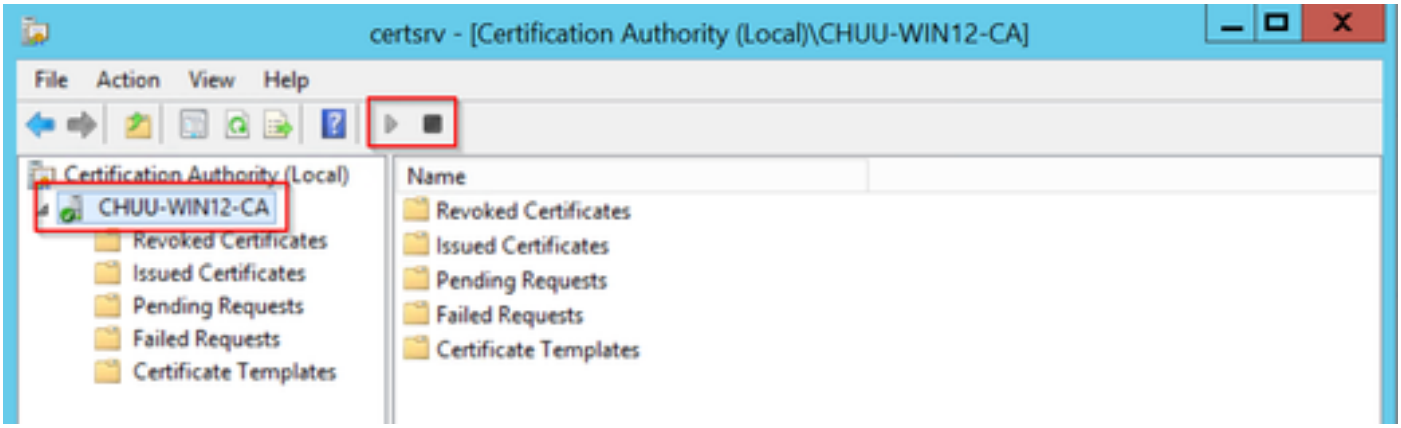
Schritt 10. Kehren Sie zum Fenster Registrierungs-Editor zurück, und navigieren Sie zu Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

Schritt 11. Bearbeiten Sie die Registrierungen EncryptionTemplate, GeneralPurposeTemplate und SignatureTemplate, sodass sie auf die neu erstellte Zertifikatvorlage verweisen.



Ändern der Vorlage in der Registrierung

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



Konfigurieren des LSC auf dem 9800

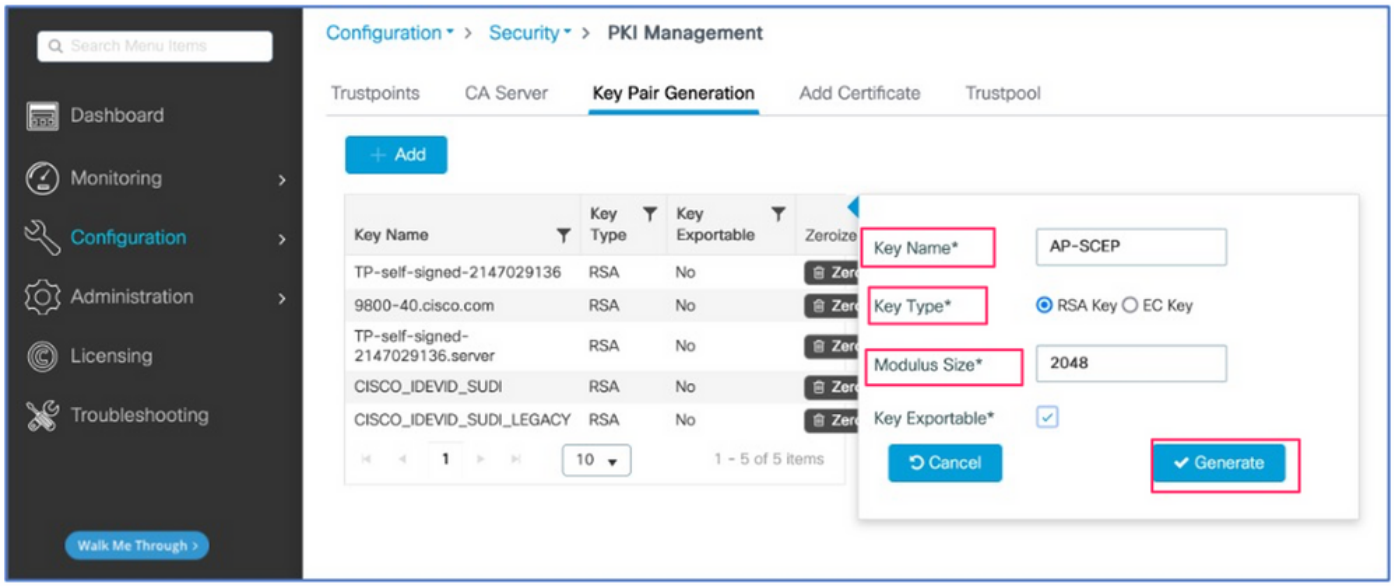
Im Folgenden werden die Schritte zur Konfiguration von LSC für AP im WLC aufgeführt.

1. RSA-Schlüssel erstellen. Dieser Schlüssel wird später für PKI Trustpoint verwendet.
2. Erstellen Sie einen Vertrauenspunkt, und ordnen Sie den erstellten RSA-Schlüssel zu.
3. Aktivieren Sie die LSC-Bereitstellung für APs, und ordnen Sie den Vertrauenspunkt zu.
    1. Aktivieren Sie LSC für alle verbundenen APs.
    2. Aktivieren Sie LSC für ausgewählte APs über die Bereitstellungsliste.
4. Ändern Sie den Wireless-Verwaltungs-Vertrauenspunkt, und verweisen Sie auf den LSC-Vertrauenspunkt.

Konfigurationsschritte für die AP LSC-GUI

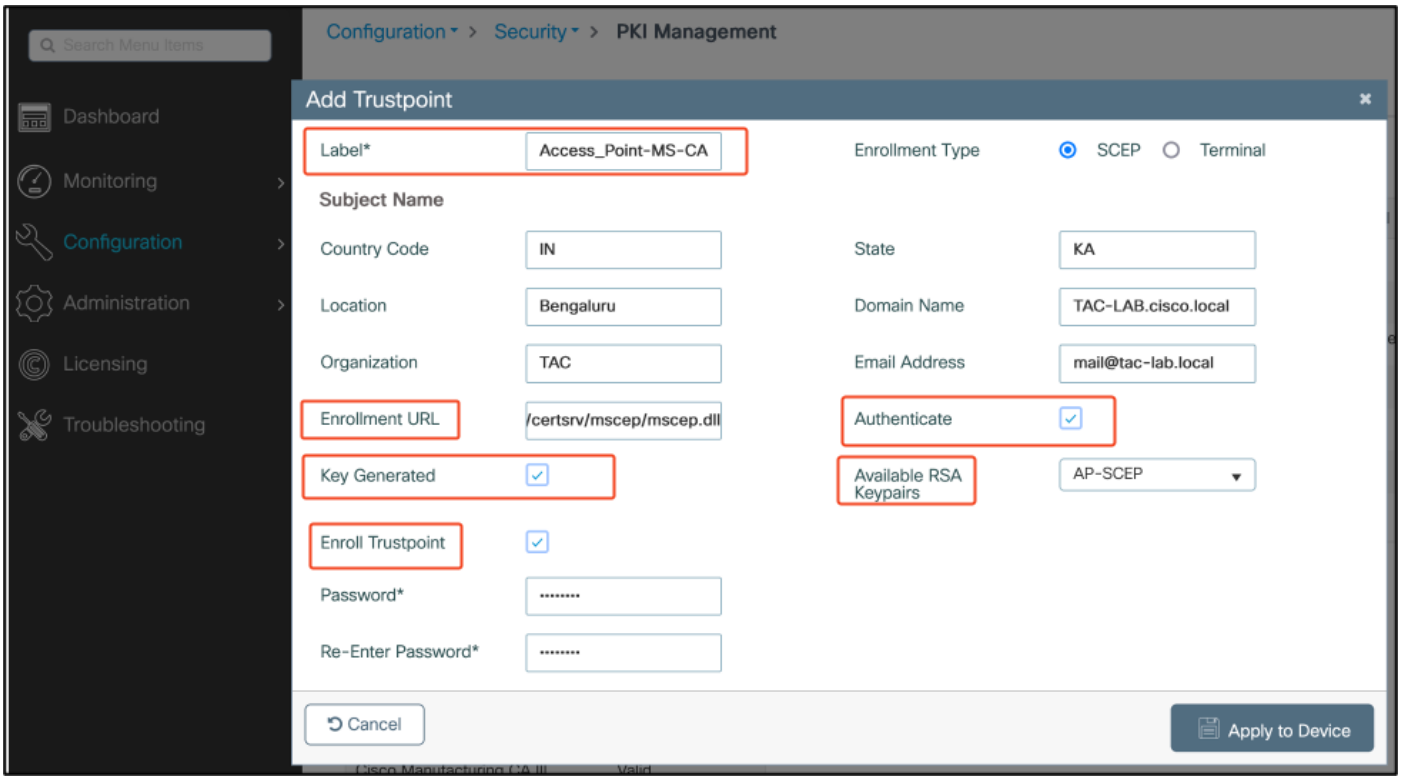
Schritt 1: Navigieren Sie zu Configuration > Security > PKI Management > Key Pair Generation.

1. Klicken Sie auf Hinzufügen, und geben Sie ihm einen relevanten Namen.
2. Fügen Sie die RSA-Schlüsselgröße hinzu.
3. Die Option für den Schlüsselexport ist optional. Dies ist nur erforderlich, wenn Sie den Schlüssel direkt exportieren möchten.
4. Wählen Sie Generieren



Schritt 2: Navigieren Sie zu Konfiguration > Sicherheit > PKI-Verwaltung > Vertrauenspunkte.

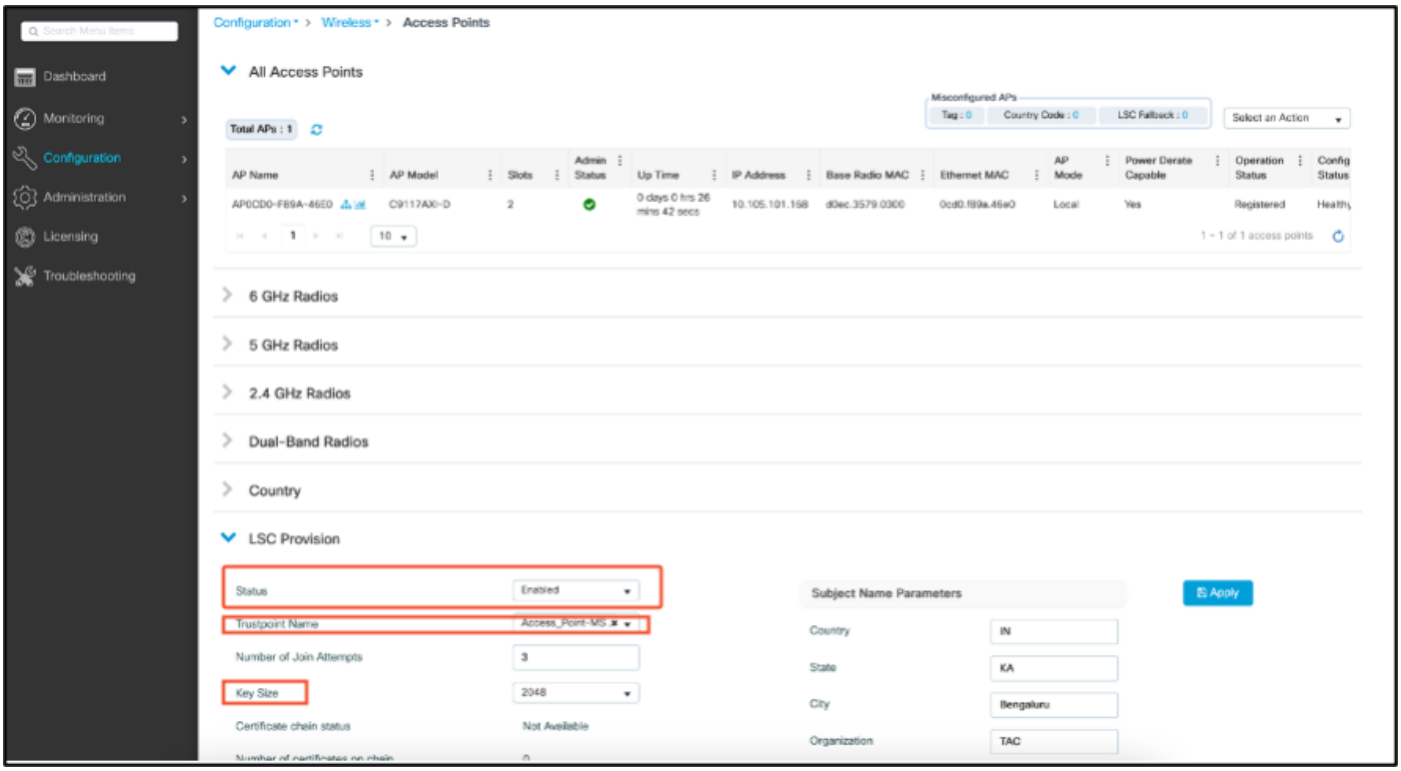
1. Klicken Sie auf Hinzufügen, und geben Sie ihm einen relevanten Namen.
2. Geben Sie die Anmeldungs-URL (hier die URL: http://10.106.35.61:80/certsrv/mscep/mscep.dll) und die übrigen Details ein.
3. Wählen Sie die in Schritt 1 erstellten RSA-Schlüsselpaare aus.
4. Klicken Sie auf Authentifizieren.
5. Klicken Sie auf Vertrauenspunkt registrieren, und geben Sie ein Kennwort ein.
6. Klicken Sie auf Auf Gerät anwenden.



Schritt 3: Navigieren Sie zu Konfiguration > Wireless > Access Points. Blättern Sie nach unten, und wählen Sie LSC Provision aus.

1. Wählen Sie den Status als aktiviert aus. Dadurch wird LSC für alle APs aktiviert, die mit diesem WLC verbunden sind.
2. Wählen Sie den in Schritt 2 erstellten Namen des Vertrauenspunkts aus.

Füllen Sie den Rest der Details nach Ihren Bedürfnissen aus.



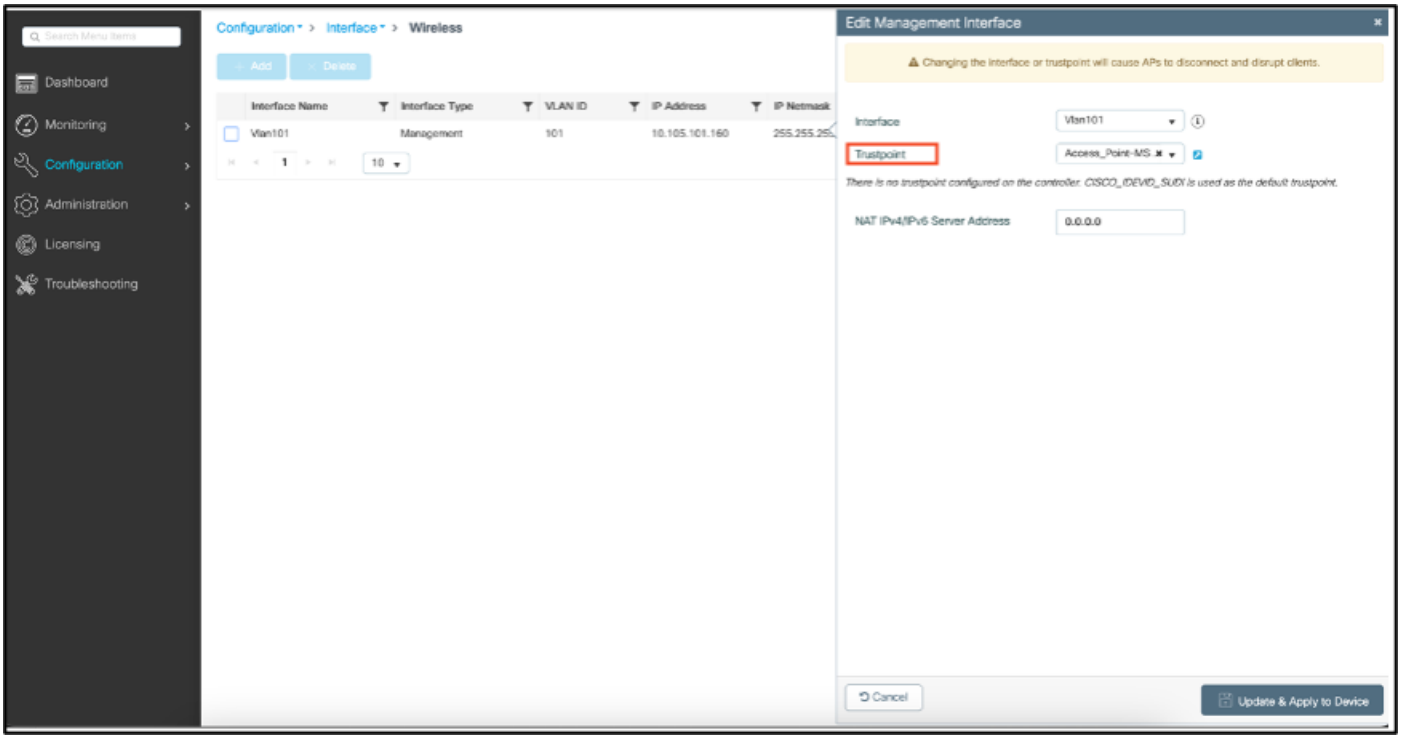
Wenn Sie LSC aktivieren, laden die APs das Zertifikat über WLC herunter und führen einen Neustart durch. In der AP-Konsolensitzung wird dann so etwas wie dieser Ausschnitt angezeigt.

```
[*09/25/2023 10:03:28.0993] .....................................................................................................................
.....................................................+++++
[*09/25/2023 10:03:28.7016] ..................+++++
[*09/25/2023 10:03:28.7663] writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:03:28.7666] -----
[*09/25/2023 10:03:28.9212] LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:03:28.9212]
[*09/25/2023 10:03:28.9293] LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:03:28.9293]
[*09/25/2023 10:03:28.9635] LSC certs and private key verified
[*09/25/2023 10:03:28.9635]
[*09/25/2023 10:03:29.4997] LSC private key written to hardware TAM
[*09/25/2023 10:03:29.4997]
[*09/25/2023 10:03:29.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed
```

Schritt 4: Nach der Aktivierung von LSC können Sie das Zertifikat für die Wireless-Verwaltung entsprechend des LSC-Vertrauenspunkts ändern. Dadurch werden APs mit ihren LSC-Zertifikaten verbunden, und der WLC verwendet sein LSC-Zertifikat für den AP-Beitritt. Dies ist ein optionaler Schritt, wenn Sie nur daran interessiert sind, eine 802.1X-Authentifizierung Ihrer APs durchzuführen.

1. Gehen Sie zu Configuration > Interface > Wireless, und klicken Sie auf Management Interface.
2. Ändern Sie den Vertrauenspunkt in den Vertrauenspunkt, den Sie in Schritt 2 erstellt haben.

Damit ist die LSC-GUI-Konfiguration abgeschlossen. APs müssen in der Lage sein, dem WLC jetzt über das LSC-Zertifikat beizutreten.



Konfigurationsschritte für die AP LSC-CLI

1. Erstellen Sie mit diesem Befehl einen RSA-Schlüssel.

```
9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP
```

```
% You already have RSA keys defined named AP-SCEP.
% They will be replaced
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storag
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Erstellen Sie einen PKI-Vertrauenspunkt, und ordnen Sie das RSA-Schlüsselpaar zu. Geben Sie die Anmeldungs-URL und die übrigen Details ein.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Authentifizieren Sie den PKI-Vertrauenspunkt und registrieren Sie ihn beim Zertifizierungsstellenserver mit dem Befehl crypto pki Authenticate <trustpoint>. Geben Sie an der Eingabeaufforderung für das Kennwort ein Kennwort ein.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' commandwill show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
```

```
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4. Konfigurieren Sie den AP-Beitritt mit einem LSC-Zertifikat.

```
9800-40(config)#ap lsc-provision join-attempt 10
9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-LA
9800-40(config)#ap lsc-provision key-size 2048
9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA
9800-40(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration
Are you sure you want to continue? (y/n): y
```

5. Ändern Sie den Vertrauenspunkt für die Wireless-Verwaltung in den oben erstellten Vertrauenspunkt.

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

AP-LSC-Überprüfung

Führen Sie diese Befehle auf dem WLC aus, um das LSC zu überprüfen.

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

```
9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
    Certificate chain status : Available
    Number of certs on chain : 2
    Certificate hash         : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
---------------

9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name  : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable

9800-40#
```

```
9800-40#sho ap name AP0CD0.F89A.46E0   config general  | begin Certificate
AP Certificate type                          : Locally Significant Certificate
AP Certificate Expiry-time                   : 09/25/2024 06:48:23
AP Certificate issuer common-name            : sumans-lab-ca
AP Certificate Policy                        : Default
AP CAPWAP-DTLS LSC Status
    Certificate status       : Available
    LSC fallback status      : No
    Issuer certificate hash  : 611255bc69f565af537be59297f453593e432e1b
    Certificate expiry time  : 09/25/2024 06:48:23
AP 802.1x LSC Status
    Certificate status       : Not Available
AP LSC authentication state                  : CAPWAP-DTLS
```

Nach dem erneuten Laden der APs melden Sie sich bei der AP-CLI an, und führen Sie diese Befehle aus, um die LSC-Konfiguration zu überprüfen.

```
#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection
```

```
AP0CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
---------------------------- Device Certificate -----------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
        Validity
            Not Before: Sep 28 04:15:28 2023 GMT
            Not After : Sep 27 04:15:28 2024 GMT
        Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0, emailAddress = mail@tac-lab.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
```

```
AP0CD0.F89A.46E0#sho crypto | in LSC
LSC: Enabled
AP0CD0.F89A.46E0#sho capwap cli config | in lsc
AP lsc enable                    : 1
AP lsc reboot cnt                : 0
AP lsc max num of retry          : 10
AP lsc mode                      : 0x1
AP lsc dtls fallback state       : 0
AP0CD0.F89A.46E0#
 Read timed out
```

```
AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
-----------------------------------------------------------------
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca
```

Fehlerbehebung bei der LSC-Bereitstellung

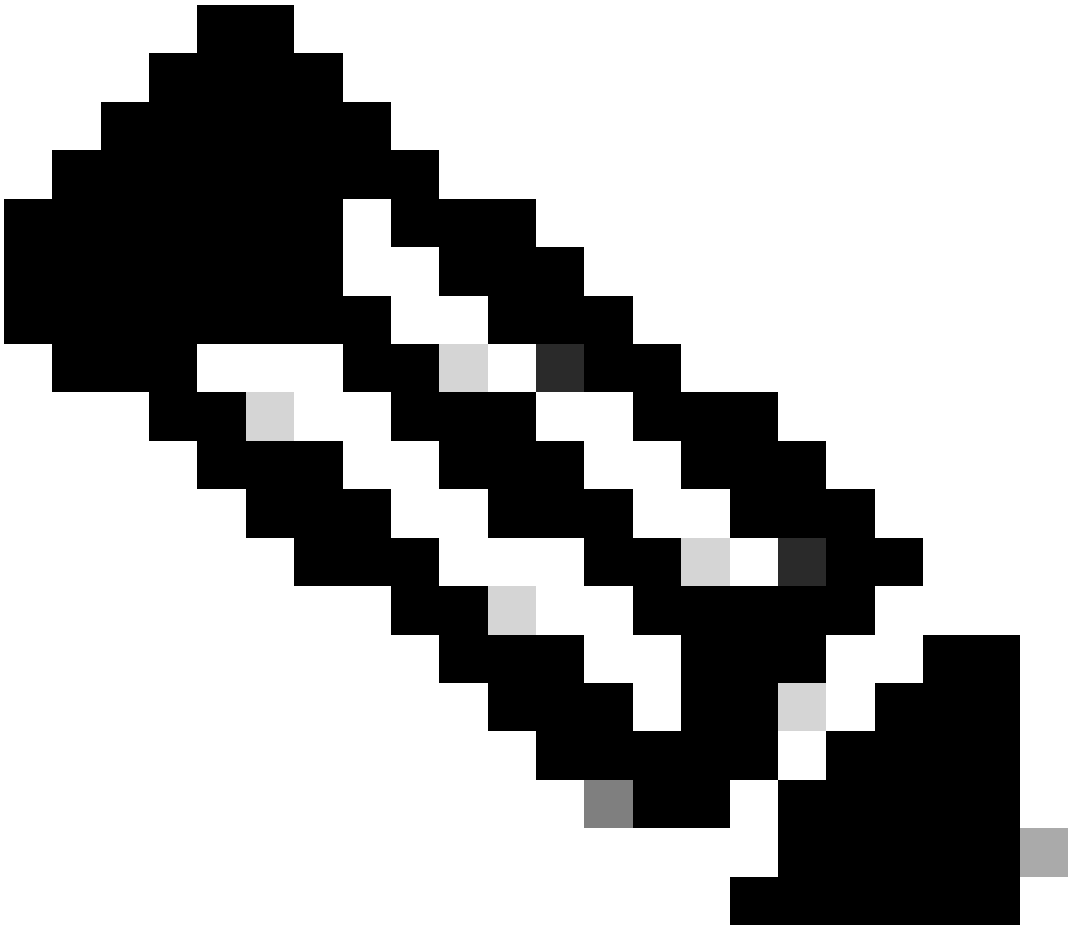
Sie können eine EPC-Erfassung vom WLC- oder AP-Uplink-Switch-Port durchführen, um das Zertifikat zu verifizieren, das der AP zum Bilden des CAPWAP-Tunnels verwendet. Überprüfen Sie anhand des PCAP, ob der DTLS-Tunnel erfolgreich erstellt wurde.

```
Datagram Transport Layer Security
  DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
      Content Type: Handshake (22)
      Version: DTLS 1.2 (0xfefd)
      Epoch: 0
      Sequence Number: 5
      Length: 82
    Handshake Protocol: Certificate (Reassembled)
        Handshake Type: Certificate (11)
        Length: 1627
        Message Sequence: 2
        Fragment Offset: 1557
        Fragment Length: 70
        Certificates Length: 1624
      Certificates (1624 bytes)
          Certificate Length: 1621
        Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd1000000000018300d… (pkcs-9-at-emailAddress=mail@tac-lab.local,id-at-commonNa
          signedCertificate
              version: v3 (2)
              serialNumber: 0x5c000000181814edda85f9bfd1000000000018
            signature (sha256WithRSAEncryption)
                Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
            issuer: rdnSequence (0)
              rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
                RDNSequence item: 1 item (dc=com)
                  RelativeDistinguishedName item (dc=com)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: com
                RDNSequence item: 1 item (dc=tac-lab)
                  RelativeDistinguishedName item (dc=tac-lab)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: tac-lab
                RDNSequence item: 1 item (dc=sumans)
                  RelativeDistinguishedName item (dc=sumans)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: sumans
                RDNSequence item: 1 item (id-at-commonName=sumans-lab-ca)
                  RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
                      Object Id: 2.5.4.3 (id-at-commonName)
                    DirectoryString: printableString (1)
                          printableString: sumans-lab-ca
            validity
              notBefore: utcTime (0)
                  utcTime: 2023-09-28 04:15:28 (UTC)
              notAfter: utcTime (0)
                  utcTime: 2024-09-27 04:15:28 (UTC)
            subject: rdnSequence (0)
```

DTLS-Debugging-Vorgänge können auf dem Access Point und dem WLC ausgeführt werden, um das Zertifikatproblem zu verstehen.

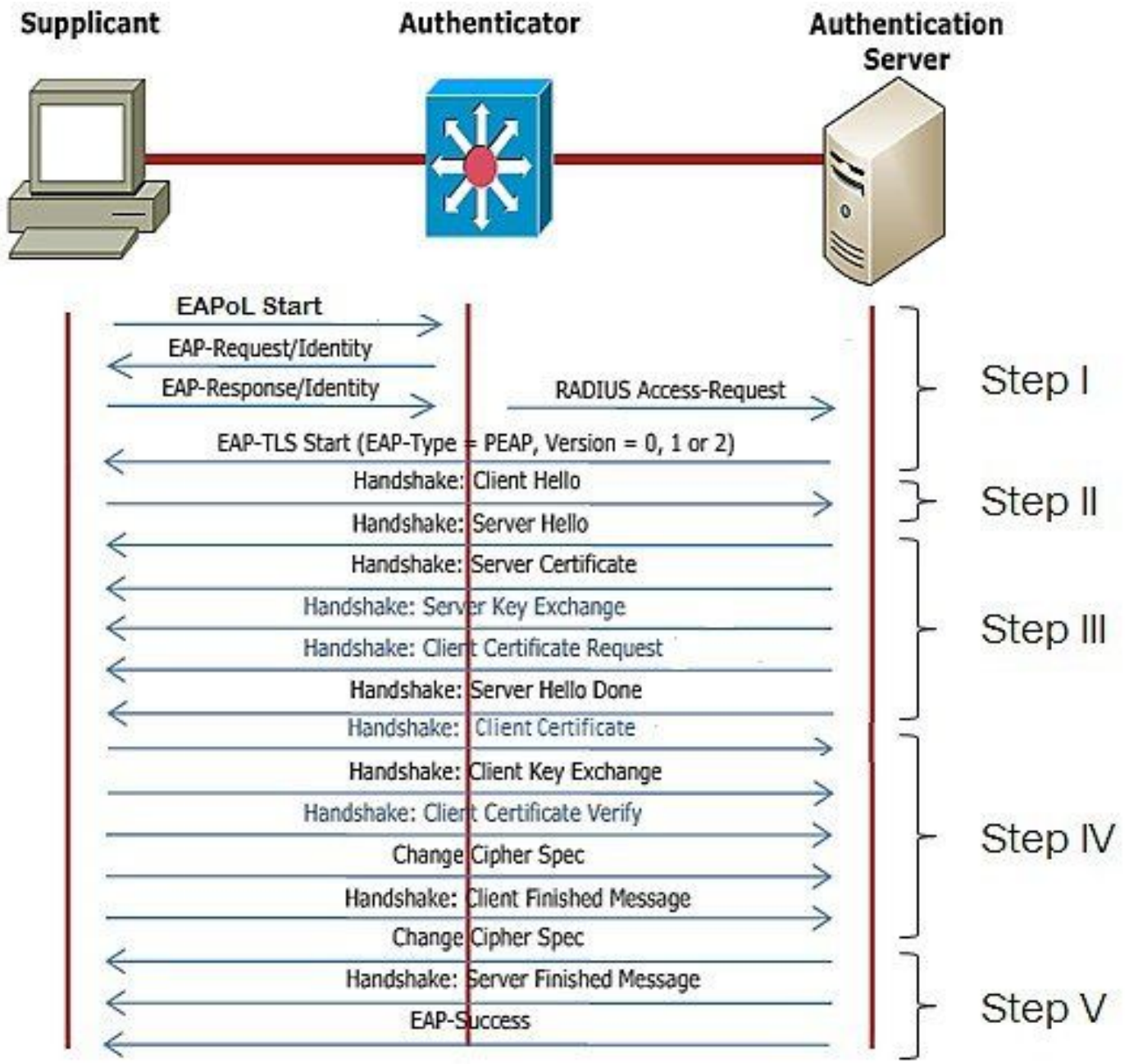
Kabelgebundene AP 802.1X-Authentifizierung mit LSC

Der Access Point ist so konfiguriert, dass er das gleiche LSC-Zertifikat für die Authentifizierung verwendet. Der AP agiert als 802.1X-Komponente und wird vom Switch gegenüber dem ISE-Server authentifiziert. Der ISE-Server kommuniziert mit dem AD im Backend.



> Hinweis: Sobald die 802.1x-Authentifizierung auf dem AP-Uplink-Switch-Port aktiviert ist, können die APs keinen Datenverkehr mehr weiterleiten oder empfangen, bis die Authentifizierung erfolgreich war. Um APs mit erfolgloser Authentifizierung wiederherzustellen und Zugriff auf den AP zu erhalten, deaktivieren Sie die 802.1x-Authentifizierung am Port des kabelgebundenen AP-Switches.

EAP-TLS-Authentifizierungs-Workflow und Nachrichtenaustausch

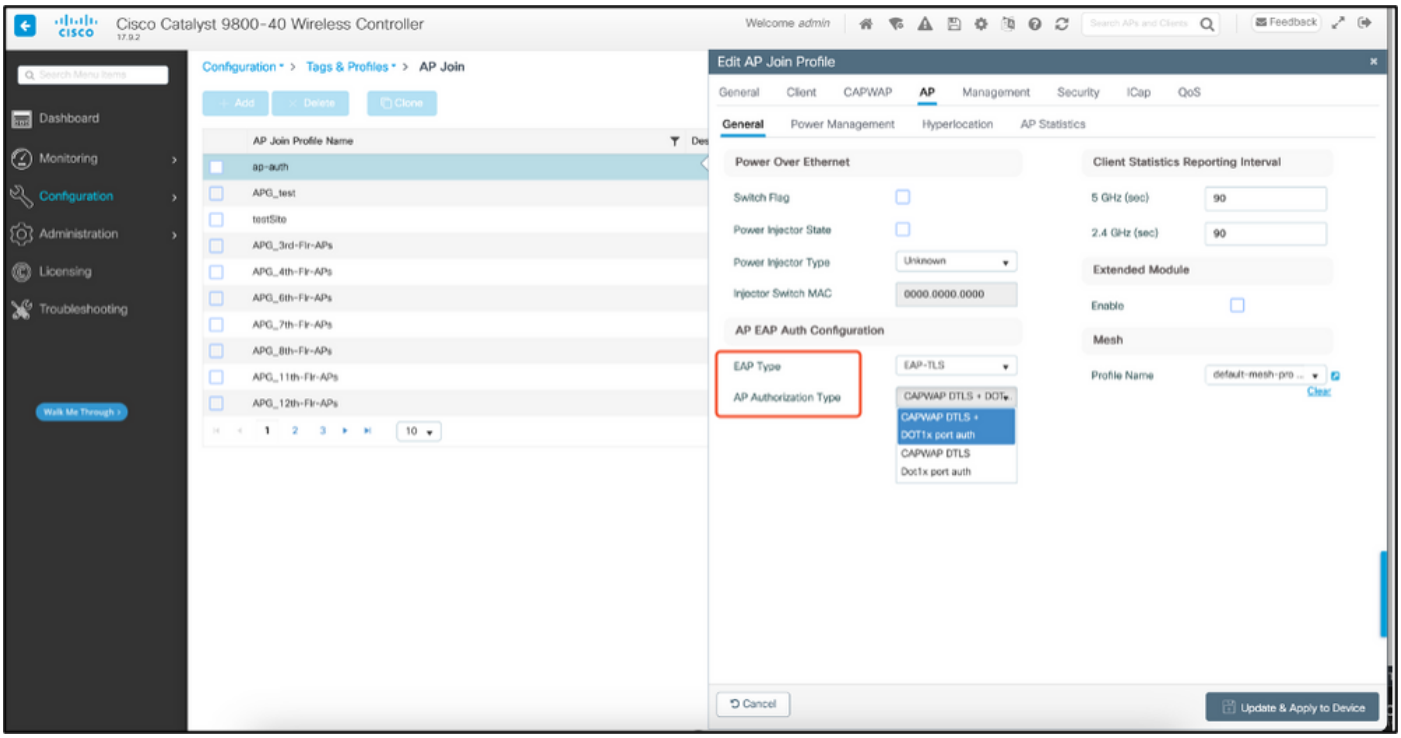


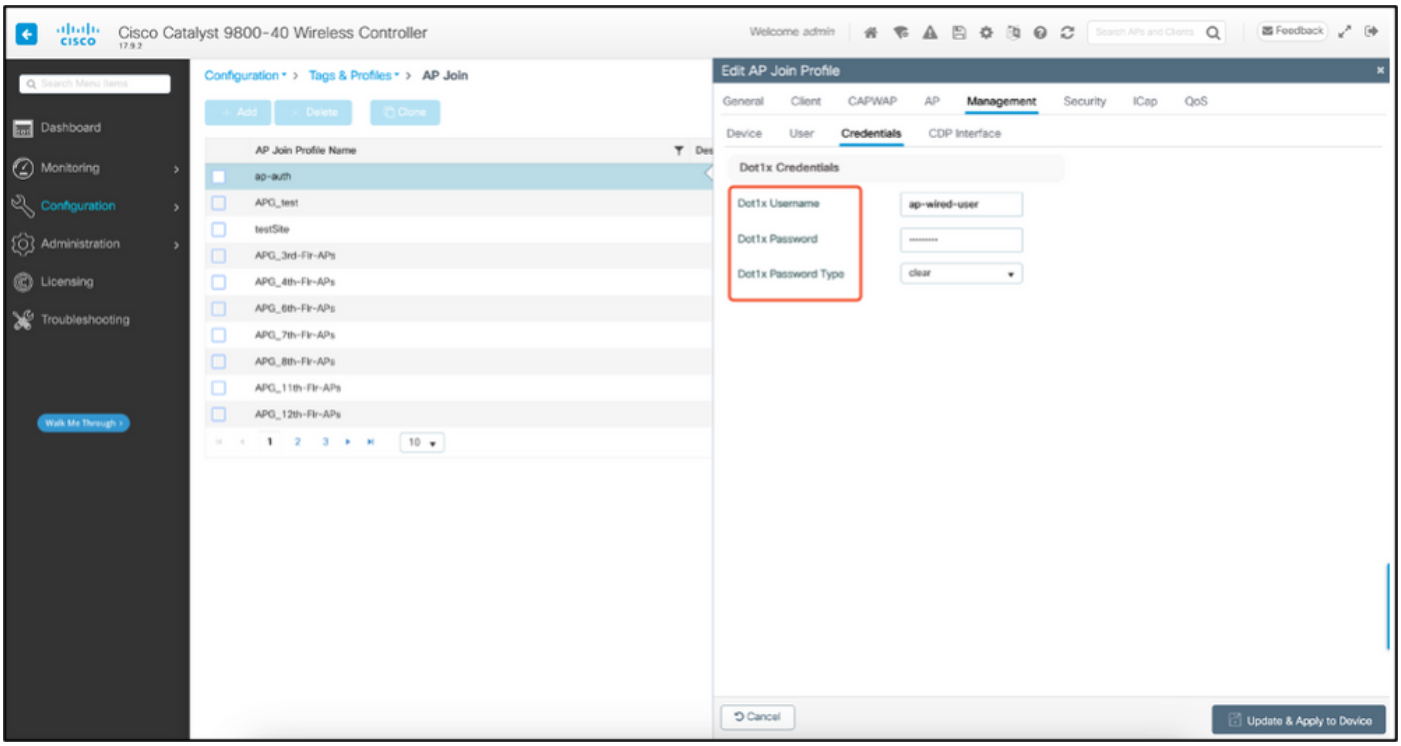
Konfigurationsschritte für die kabelgebundene AP 802.1x-Authentifizierung

1. Aktivieren Sie die dot1x-Port-Authentifizierung zusammen mit CAPWAP DTLS, und wählen Sie den EAP-Typ aus.
2. Erstellen Sie 802.1x-Anmeldeinformationen für APs.
3. Aktivieren Sie dot1x auf dem Switch-Port.
4. Installieren eines vertrauenswürdigen Zertifikats auf dem RADIUS-Server

Konfiguration der kabelgebundenen 802.1x-Authentifizierungs-GUI des AP

1. Navigieren Sie zum AP-Join-Profil, und klicken Sie auf das Profil.
    1. Klicken Sie auf AP > General (Allgemein). Wählen Sie als EAP-Typ und AP-Autorisierungstyp "CAPWAP DTLS + dot1x port auth" aus.
    2. Navigieren Sie zu Management > Anmeldedaten, und erstellen Sie einen Benutzernamen und ein Kennwort für die AP dot1x-Authentifizierung.





Konfiguration der kabelgebundenen 802.1x-Authentifizierungs-CLI des AP

Verwenden Sie diese Befehle, um dot1x für APs über die CLI zu aktivieren. Dadurch wird nur die kabelgebundene Authentifizierung für APs aktiviert, die das spezifische Join-Profil verwenden.

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

```
9800-40(config)#ap profile ap-auth
9800-40(config-ap-profile)#dot1x eap-type eap-tls
9800-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9800-40(config-ap-profile)#
```

Konfiguration des kabelgebundenen AP-802.1x-Authentifizierungs-Switches

Diese Switch-Konfigurationen werden in LAB verwendet, um die drahtgebundene AP-Authentifizierung zu aktivieren. Je nach Design können Sie eine andere Konfiguration verwenden.

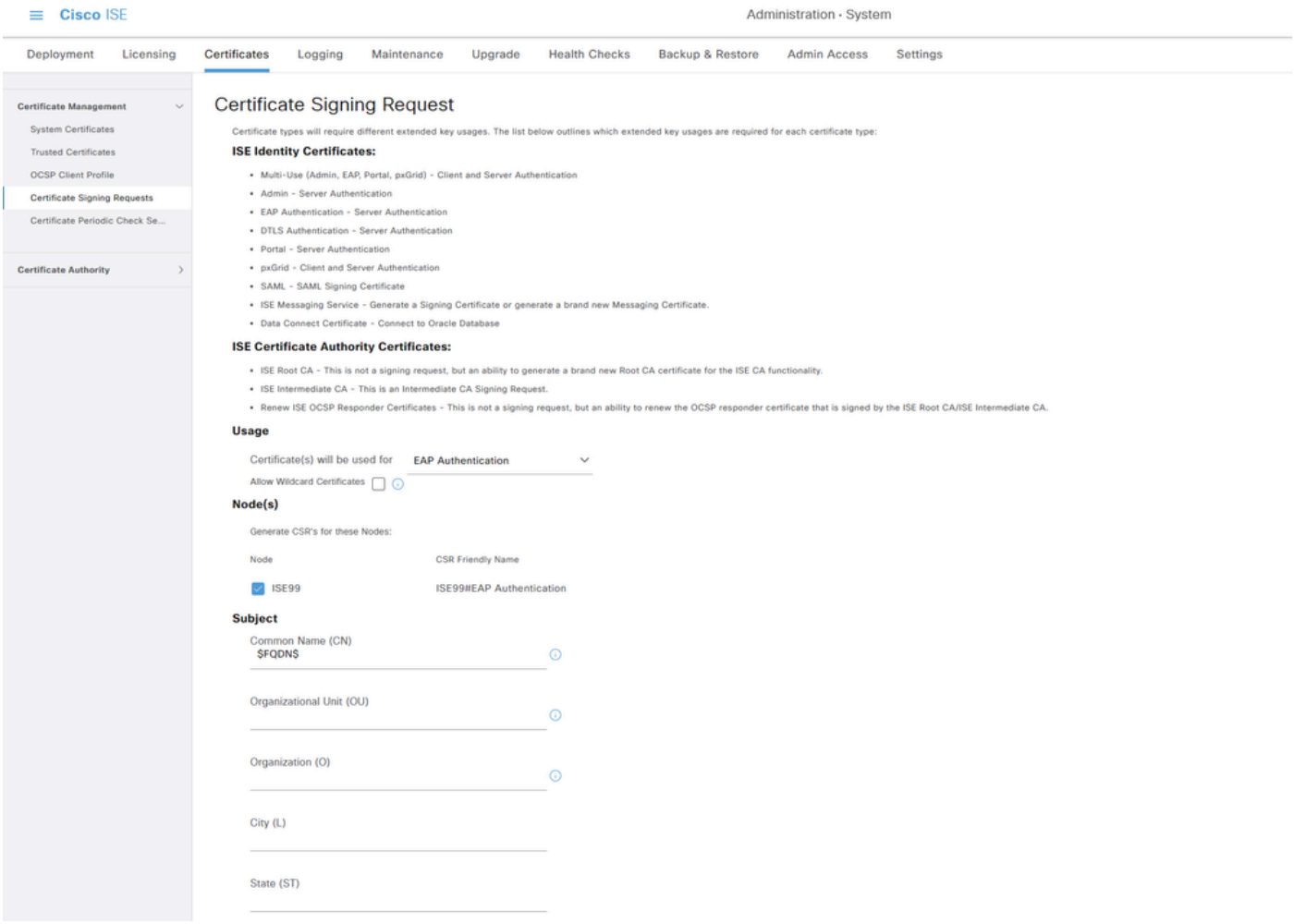
```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

Installation des RADIUS-Serverzertifikats

Die Authentifizierung erfolgt zwischen dem Access Point (der als Supplikant fungiert) und dem RADIUS-Server. Beide müssen sich gegenseitig vertrauen. Der Access Point kann dem RADIUS-Serverzertifikat nur dann vertrauen, wenn der RADIUS-Server ein Zertifikat verwendet, das von der SCEP-Zertifizierungsstelle ausgestellt wurde, die auch das AP-Zertifikat ausgestellt hat.

Gehen Sie in ISE zu Administration > Certificates > Generate Certificate Signing Requests

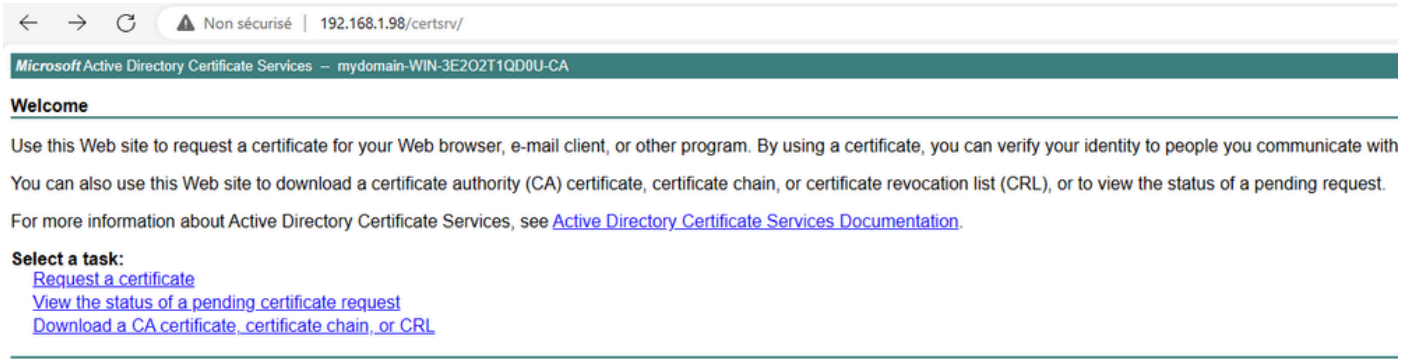
Erstellen Sie eine CSR-Anfrage, und füllen Sie die Felder mit den Informationen Ihres ISE-Knotens aus.



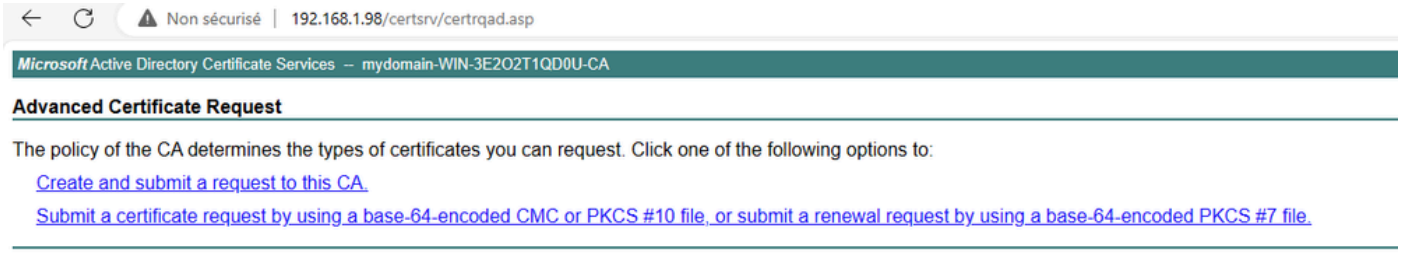
Nach der Generierung können Sie sie exportieren und als Text kopieren und einfügen.

Navigieren Sie zu Ihrer Windows CA-IP-Adresse, und fügen Sie /certsrv/ zur URL hinzu.

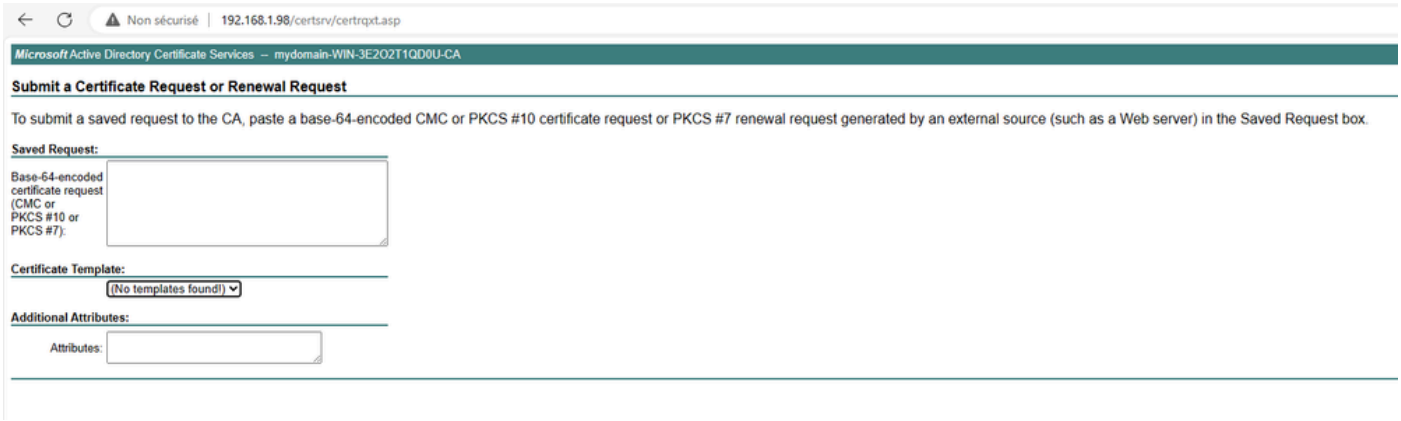
Klicken Sie auf Zertifikat anfordern.



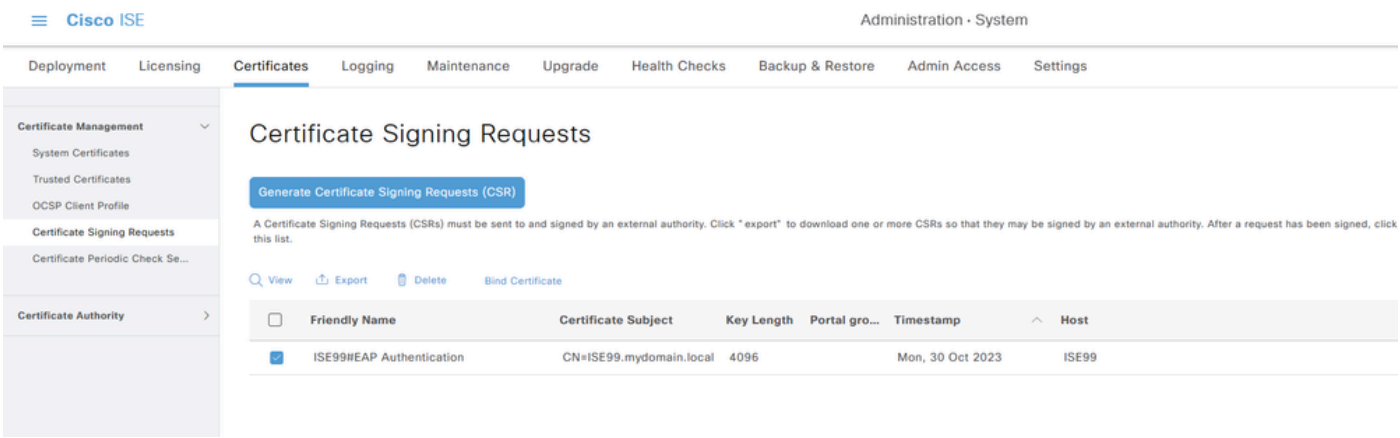
Klicken Sie auf Submit a certificate request by using a base-64 ....



Fügen Sie den CSR-Text in das Textfeld ein. Wählen Sie die Webserver-Zertifikatvorlage aus.



Sie können dieses Zertifikat dann auf der ISE installieren, indem Sie zurück zum Menü "Certificate Signing Request" gehen und auf Bind certificate klicken. Sie können dann das Zertifikat hochladen, das Sie von Ihrem Windows-PC erhalten haben.



AP Wired 802.1x-Authentifizierungsprüfung

Nehmen Sie Konsolenzugriff auf den Access Point, und führen Sie den folgenden Befehl aus:

```
#show ap authentication status
```

Die AP-Authentifizierung ist nicht aktiviert:

```
AP0CD0.F89A.46E0#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E0#
```

Konsolenprotokolle vom Access Point nach Aktivierung der AP-Authentifizierung:

```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

AP erfolgreich authentifiziert:

```
AP0CD0.F89A.46E0#sho ap authentication status
key_mgmt=IEEE 802.1X (no WPA)
wpa_state=COMPLETED
address=0c:d0:f8:9a:46:e0
supplicant_PAE_state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
eap_tls_version=TLSv1.2
EAP TLS cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
eap_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ea2bdd11f40494a4325dc98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aafb5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

WLC-Verifizierung:

```
9800-40#sho ap name AP0CD0.F89A.46E0   config general   | begin Certificate
AP Certificate type                          : Locally Significant Certificate
AP Certificate Expiry-time                   : 09/25/2024 06:48:23
AP Certificate issuer common-name            : sumans-lab-ca
AP Certificate Policy                        : Default
AP CAPWAP-DTLS LSC Status
    Certificate status        : Available
    LSC fallback status       : No
    Issuer certificate hash   : 611255bc69f565af537be59297f453593e432e1b
    Certificate expiry time   : 09/25/2024 06:48:23
AP 802.1x LSC Status
    Certificate status        : Available
    Issuer certificate hash   : 611255bc69f565af537be59297f453593e432e1b
    Certificate expiry time   : 09/25/2024 06:48:23
AP LSC authentication state                  : CAPWAP-DTLS and 802.1x authentication
```

Switch-Port-Schnittstellenstatus nach erfolgreicher Authentifizierung:

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface               MAC Address    Method  Domain  Status Fg  Session ID
---------------------------------------------------------------------------------
Gi1/0/2                 0cd0.f89a.46e0 dot1x   DATA    Auth       9765690A0000005CCEED0FBF
```

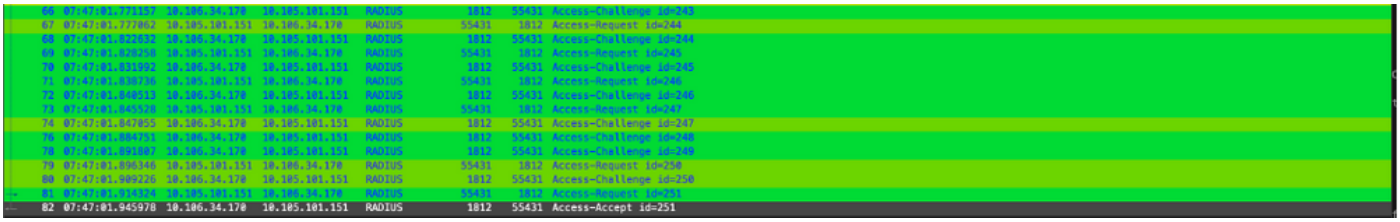
Dies ist ein Beispiel für AP-Konsolenprotokolle, die eine erfolgreiche Authentifizierung anzeigen:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```

Fehlerbehebung: 802.1X-Authentifizierung

Nehmen Sie PCAP für den AP-Uplink, und überprüfen Sie die RADIUS-Authentifizierung. Hier ist ein Ausschnitt der erfolgreichen Authentifizierung.

TCP-Dump erfasst von der ISE die Authentifizierung.



Wenn bei der Authentifizierung ein Problem festgestellt wird, ist eine gleichzeitige Paketerfassung vom verkabelten AP-Uplink und von der ISE-Seite erforderlich.

Debug-Befehl für AP:

```
#debug ap authentication packet
```

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Konfigurieren von 802.1X auf AP mit AireOS
- Konfigurationsanleitung für LSC 9800
- LSC-Konfigurationsbeispiel für 9800
- Konfigurieren von 802.1X für APs auf 9800

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.