

# 802.1X op AP's configureren voor PEAP of EAP-TLS met LSC

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Windows Server 2016 SCEP CA](#)

[Het certificaatsjabloon en het register configureren](#)

[LSC op de 9800 configureren](#)

[Configuratiestappen AP LSC GUI](#)

[Configuratiestappen AP LSC CLI](#)

[AP LSC-verificatie](#)

[Probleemoplossing voor LSC-provisioning](#)

[AP-bekabelde 802.1X-verificatie met LSC](#)

[Configuratiestappen voor AP Wired 802.1x-verificatie](#)

[Configuratie van bekabelde AP-802.1x-verificatie en GUI](#)

[CLI-configuratie voor AP-bekabelde 802.1x-verificatie](#)

[Configuratie van bekabelde AP-Switch 802.1x-verificatie](#)

[Installatie van RADIUS-servercertificaat](#)

[Verificatie van bekabelde AP-802.1x-verificatie](#)

[Probleemoplossing 802.1X-verificatie](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u Cisco-access points op hun switchpoort moet verifiëren met behulp van de 802.1X PEAP- of EAP-TLS-methoden.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Draadloze controller

- Access point
- Switch
- ISE-server
- Certificaatautoriteit.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze controller: C9800-40-K9 met 17.09.02
- Access point: C9117AXI-D
- Switch: C9200L-24P-4G met 17.06.04
- AAA-server: ISE-VM-K9 met 3.1.0.518
- Certificaatinstansie: Windows Server 2016

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Als u wilt dat uw access points (AP's) met hun switchport verifiëren met 802.1X, gebruiken zij standaard het EAP-FAST-verificatieprotocol waarvoor geen certificaten nodig zijn. Als u wilt dat de AP's de PEAP-mschappv2 methode (die referenties aan de AP-kant gebruikt maar een certificaat aan de RADIUS-kant) of de EAP-TLS methode (die certificaten aan beide kanten gebruikt) gebruiken, moet u LSC eerst configureren. Het is de enige manier om een vertrouwd/wortelcertificaat op een toegangspunt (en ook een apparaatcertificaat in het geval van EAP-TLS) te verstrekken. Het is niet mogelijk voor het toegangspunt om PEAP uit te voeren en de validatie aan serverzijde te negeren. Dit document behandelt eerst het configureren LSC en vervolgens de 802.1X-configuratiezijde.

Gebruik een LSC als u wilt dat uw PKI betere beveiliging biedt, controle heeft over uw certificaatautoriteit (CA) en beleid, beperkingen en gebruik definieert op de gegenereerde certificaten.

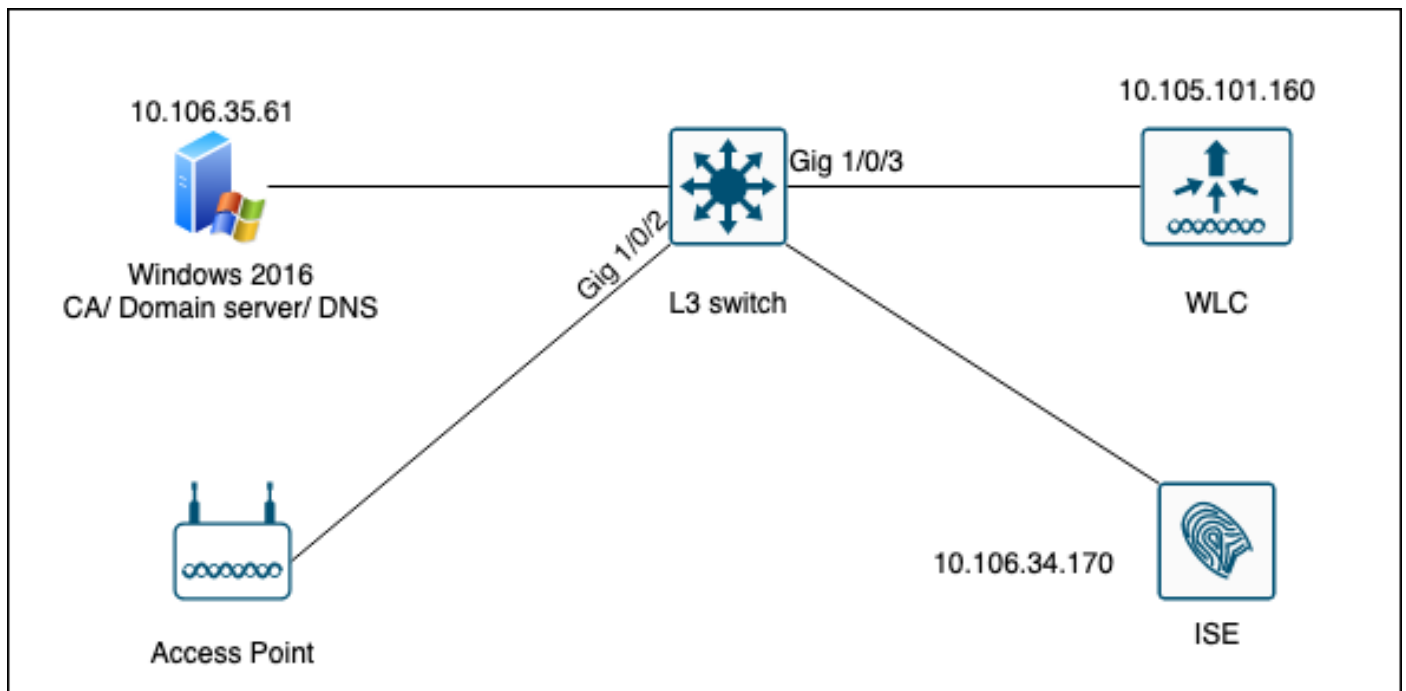
Met LSC krijgt de controller een certificaat van de CA. Een AP communiceert niet direct met de CA-server, maar de WLC vraagt certificaten aan namens de toetredende AP's. De CA-servergegevens moeten op de controller zijn geconfigureerd en toegankelijk zijn.

De controller maakt gebruik van het Simple Certificate Enrollment Protocol (SCEP) om bepaaldeReqs die op de apparaten zijn gegenereerd door te sturen naar de CA en maakt opnieuw gebruik van SCEP om de ondertekende certificaten van de CA te verkrijgen.

SCEP is een protocol voor certificaatbeheer dat de PKI-clients en CA-servers gebruiken om certificaatinschrijving en herroeping te ondersteunen. Het wordt veel gebruikt in Cisco en ondersteund door veel CA-servers. In SCEP wordt HTTP gebruikt als het transportprotocol voor

de PKI-berichten. Het primaire doel van SCEP is de veilige afgifte van certificaten aan netwerkapparaten.

## Netwerkdigram



## Configureren

Er zijn twee dingen om voornamelijk te configureren: de SCEP CA en de 9800 WLC.

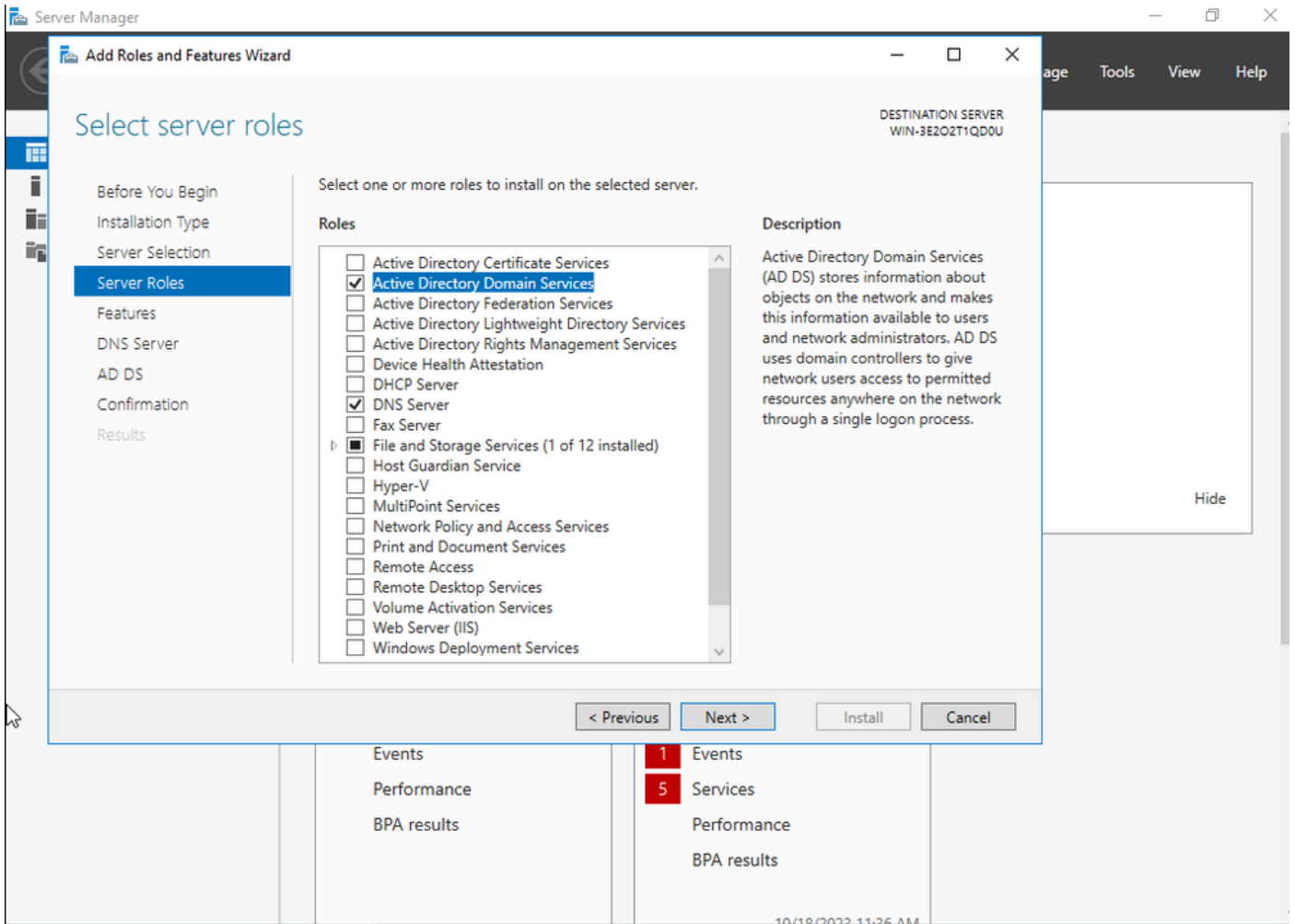
### Windows Server 2016 SCEP CA

Dit document behandelt een fundamentele installatie van een Windows Server SCEP CA voor laboratoriumdoeleinden. Een echte productie-grade Windows CA moet veilig en geschikt worden geconfigureerd voor bedrijfsactiviteiten. Deze sectie is bedoeld om u te helpen het in het laboratorium testen en inspiratie te halen uit de vereiste instellingen om deze configuratie te laten werken. Dit zijn de stappen :

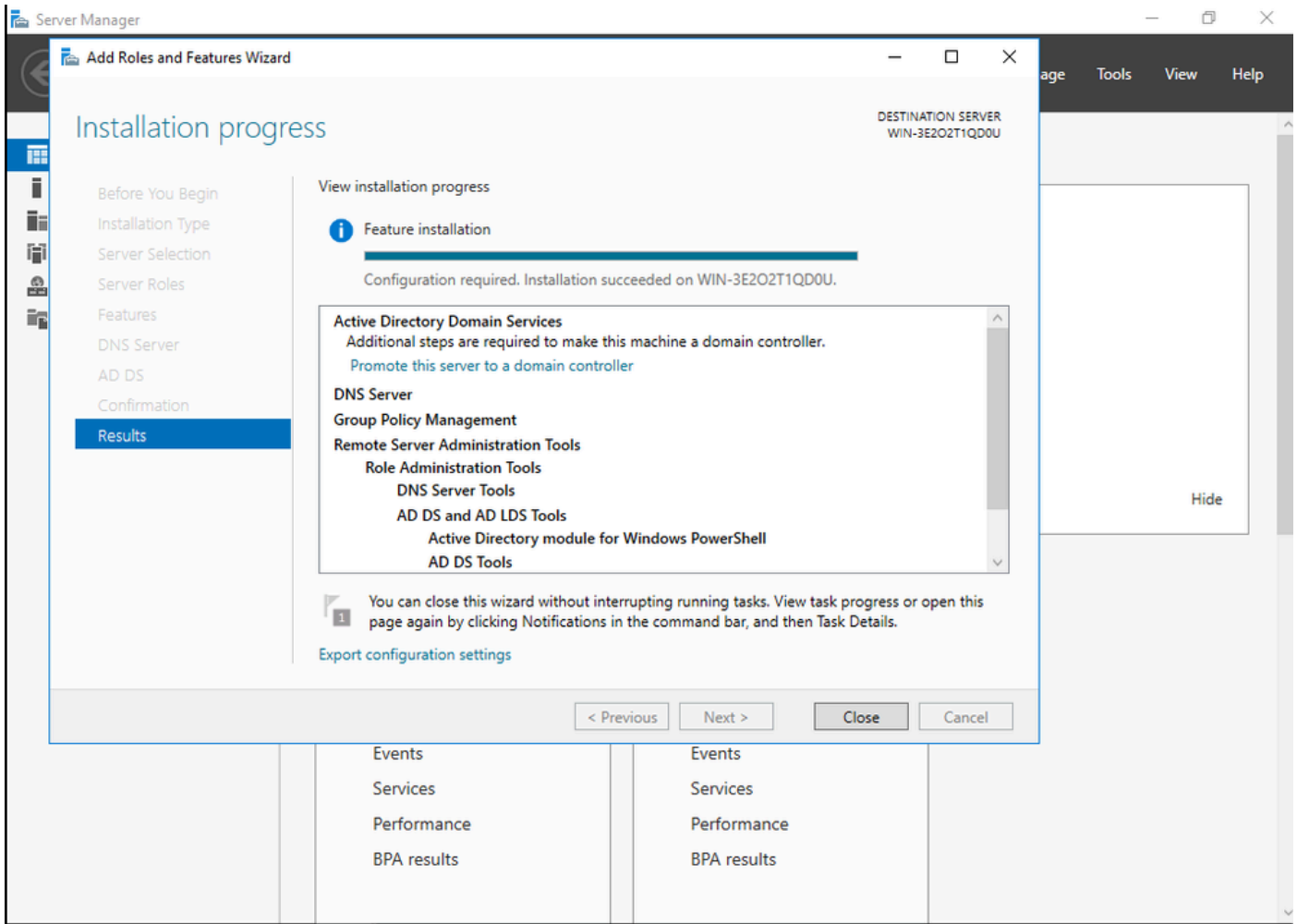
Stap 1. Installeer een nieuwe Windows Server 2016 Desktop Experience.

Stap 2. Controleer of de server is geconfigureerd met een statisch IP-adres.

Stap 3. Installeer een nieuwe rol en service, start met Active Directory Domain services en DNS server.

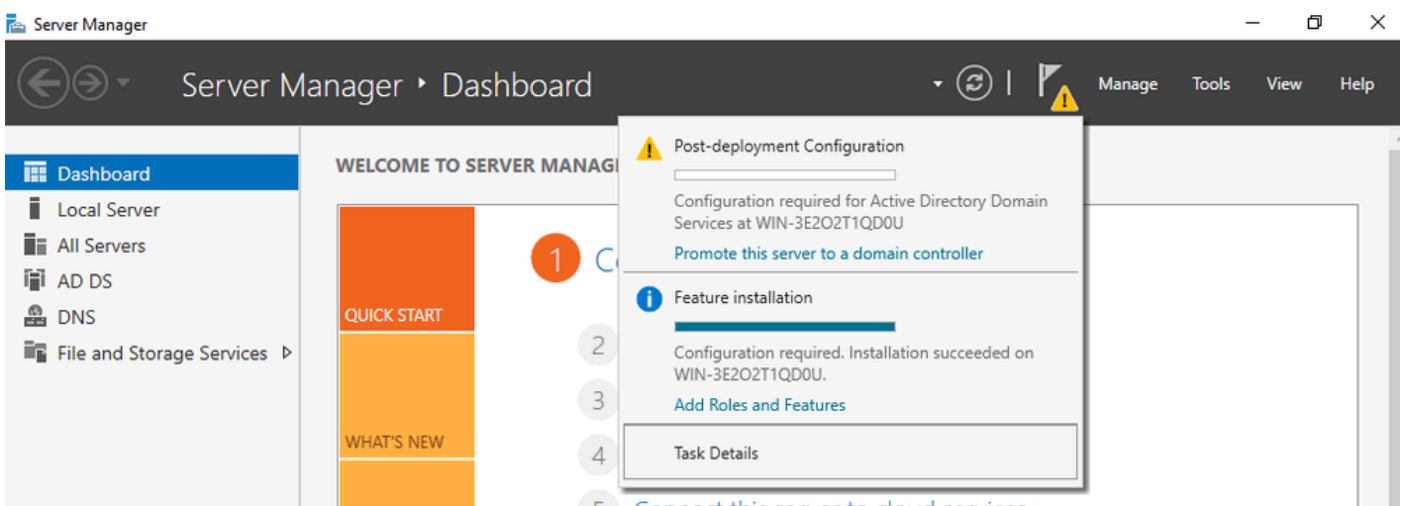


Active Directory-installatie



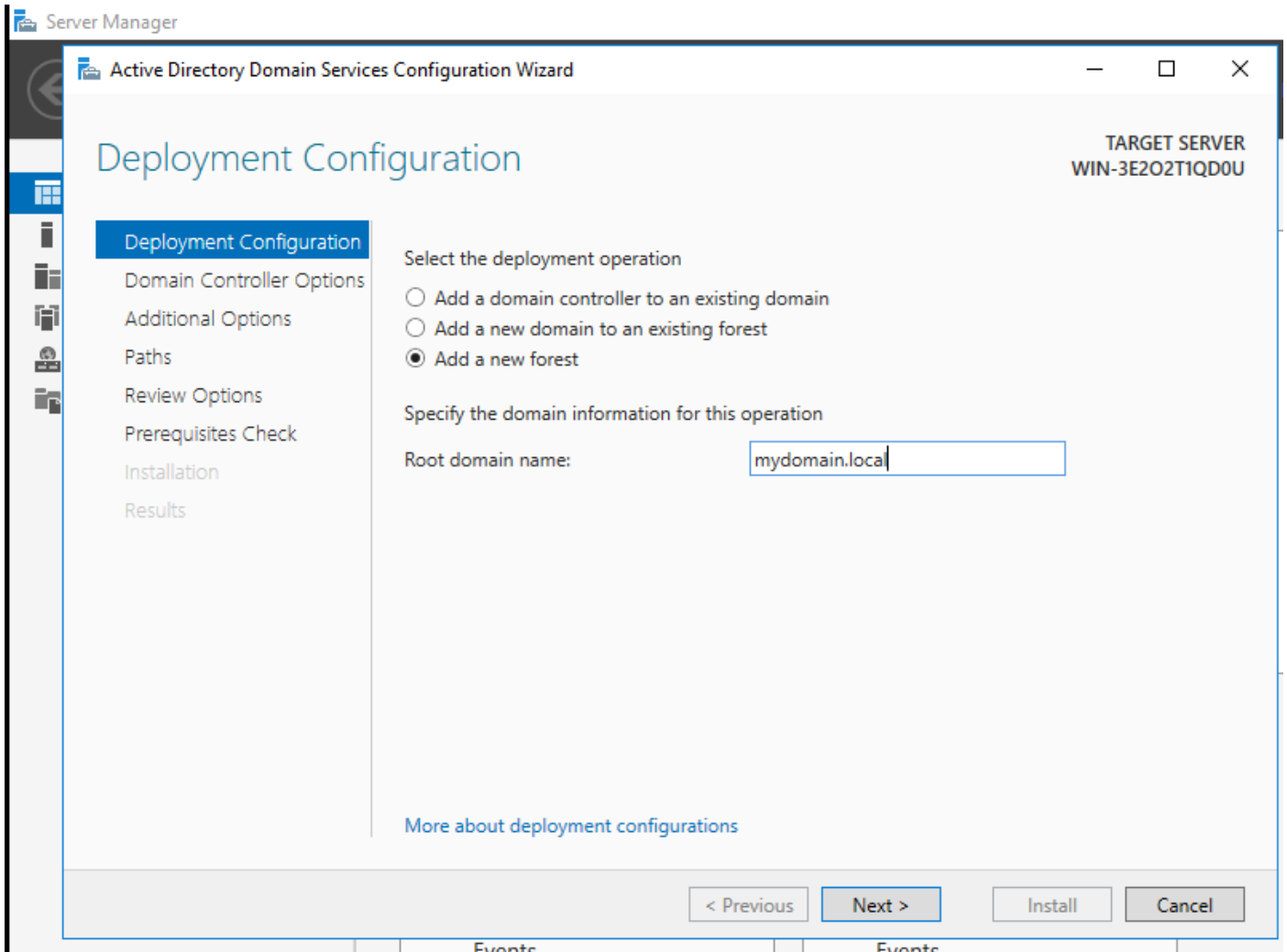
Einde AD-installatie

Stap 4. Als u klaar bent, klikt u op het dashboard op Promoot deze server naar een domeincontroller.



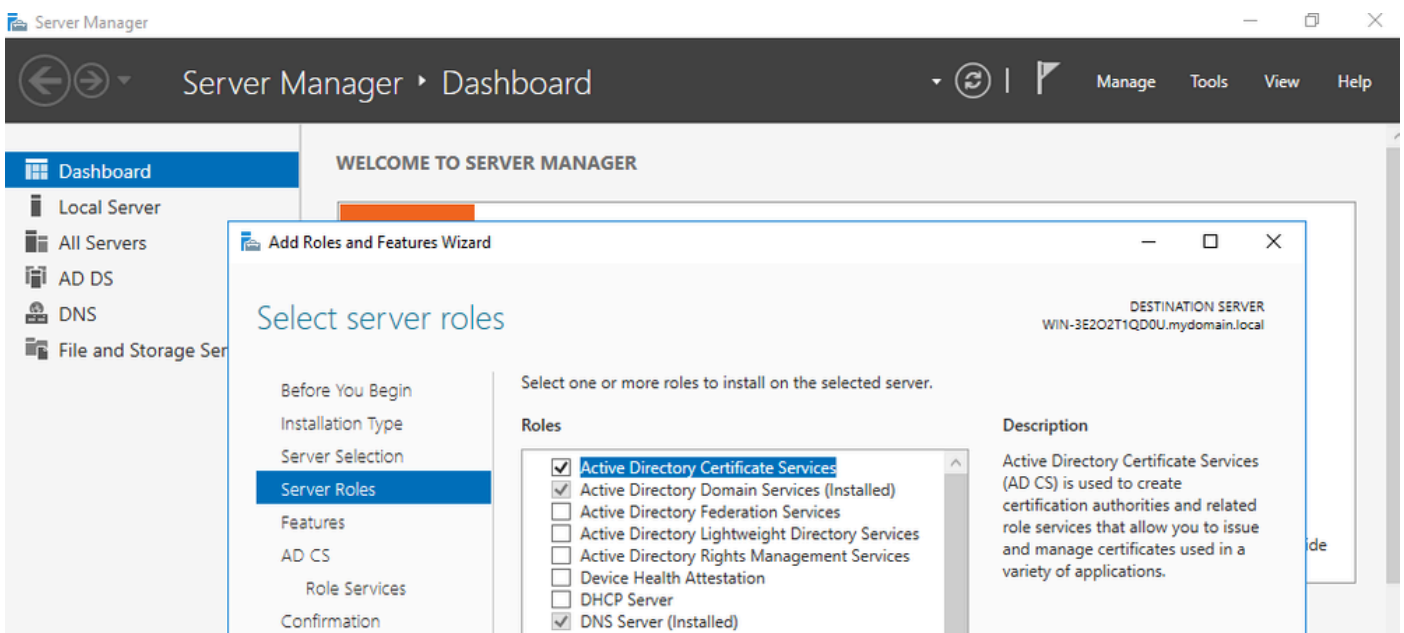
De AD-services configureren

Stap 5. Maak een nieuw bos en kies een domeinnaam.

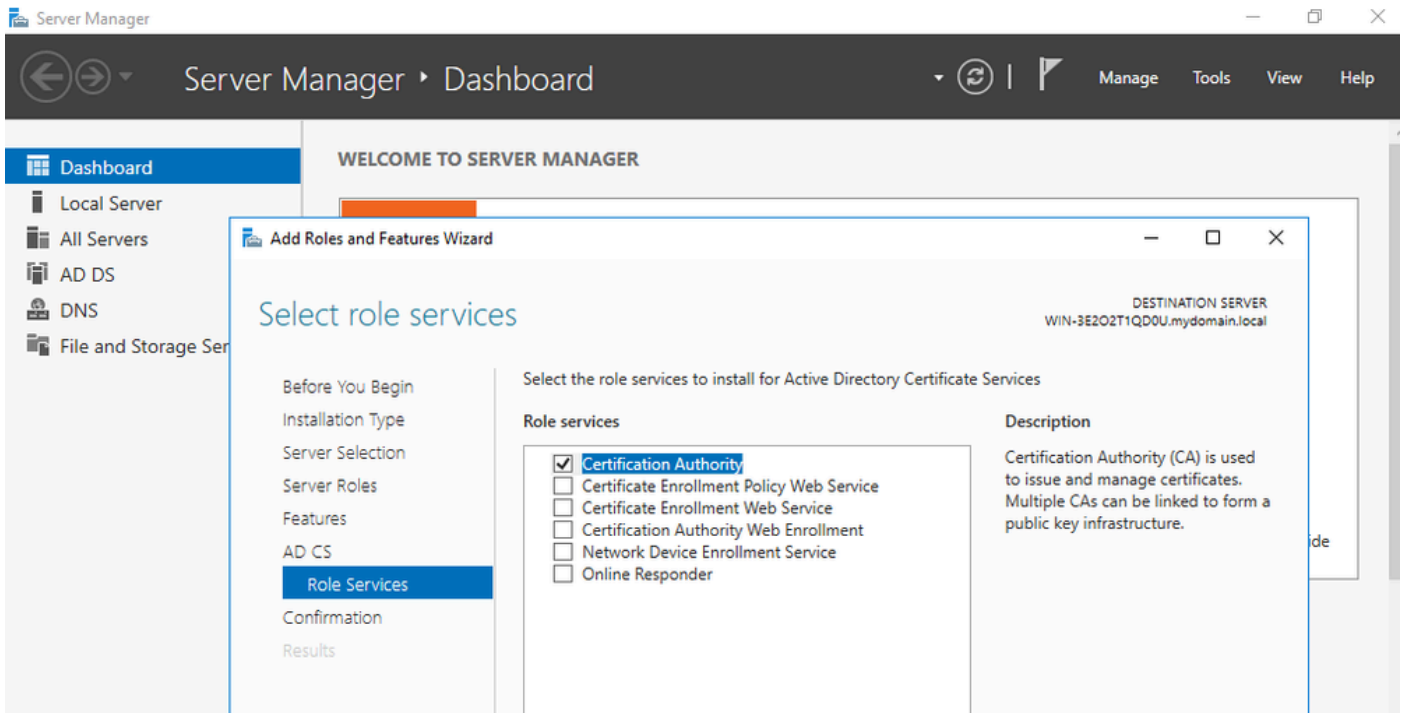


Kies een bosnaam

Stap 6. Voeg de rol Certificaatservices toe aan uw server:

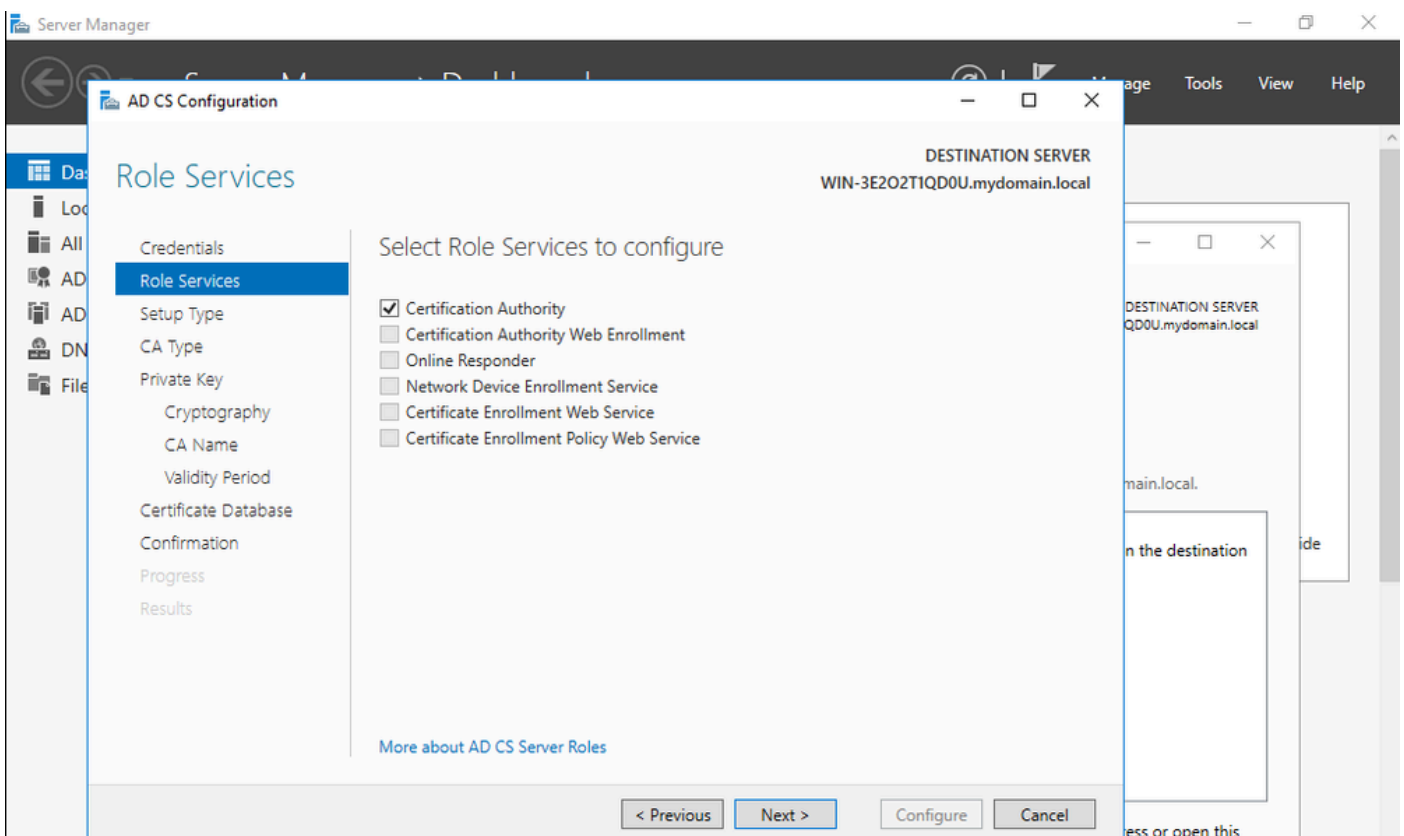


Certificaatservices toevoegen

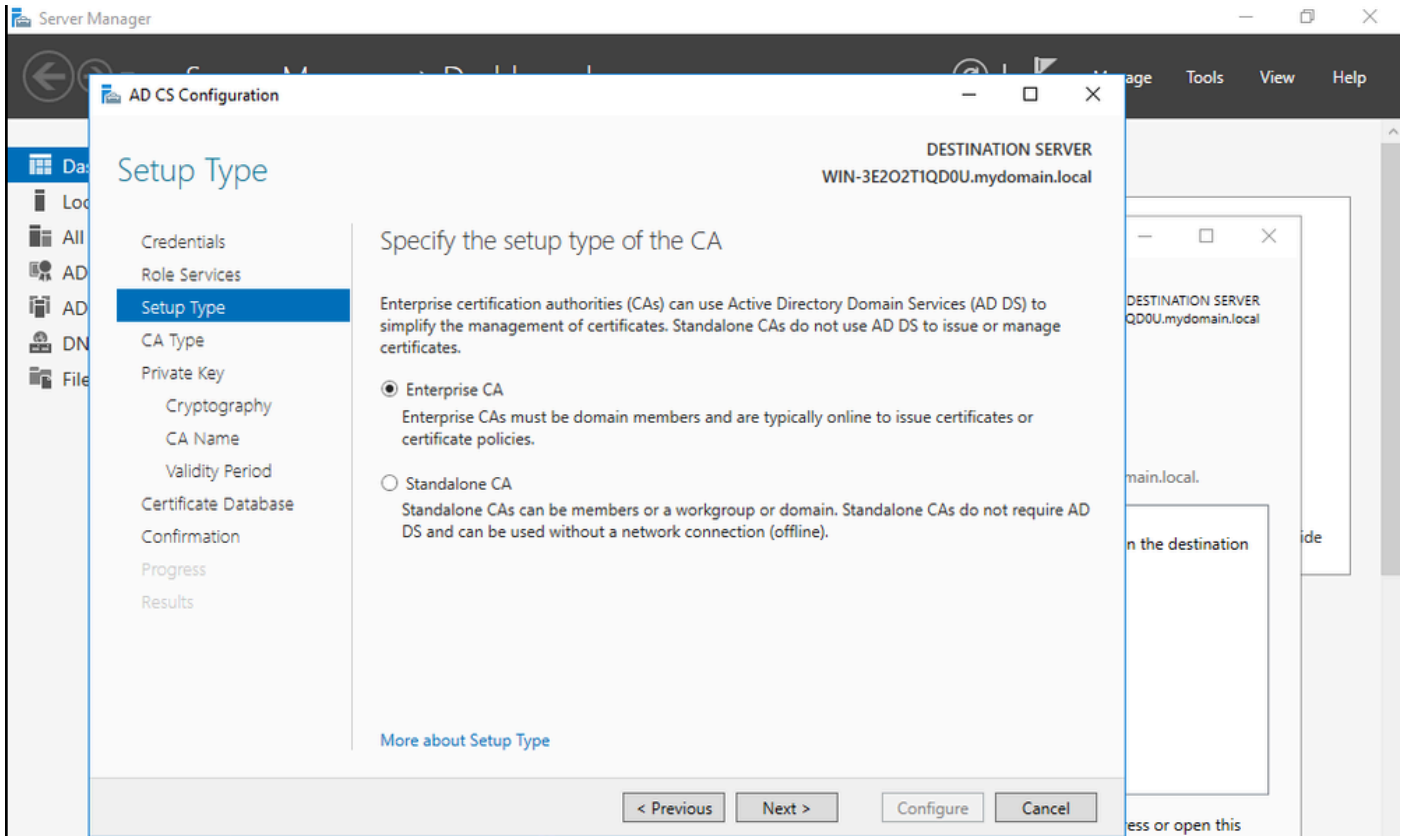


Alleen de certificeringsinstantie toevoegen

Stap 7. Nadat u dit hebt gedaan, configureert u uw certificeringsinstantie.



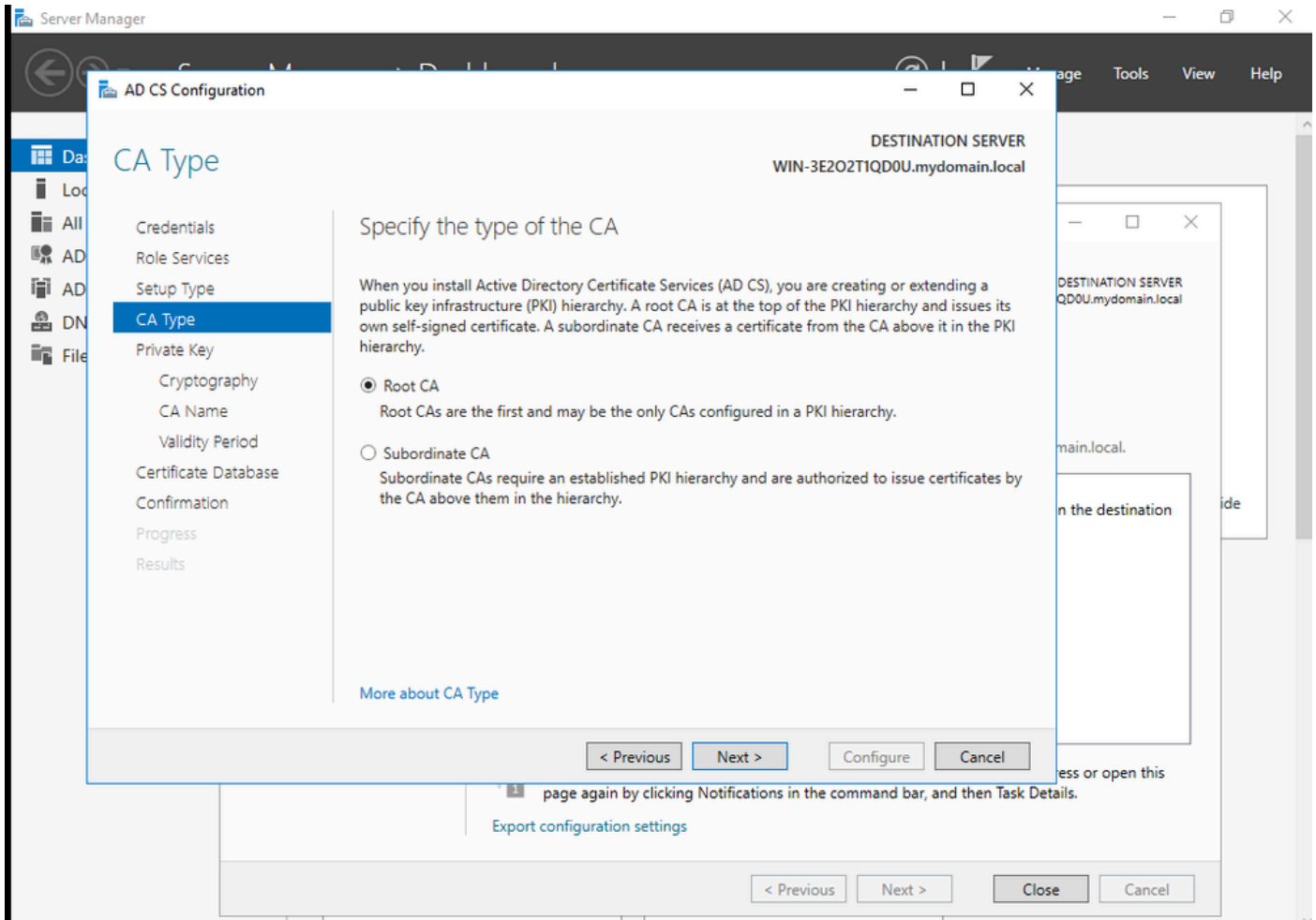
Stap 8. Kies Enterprise CA.



CA voor ondernemingen

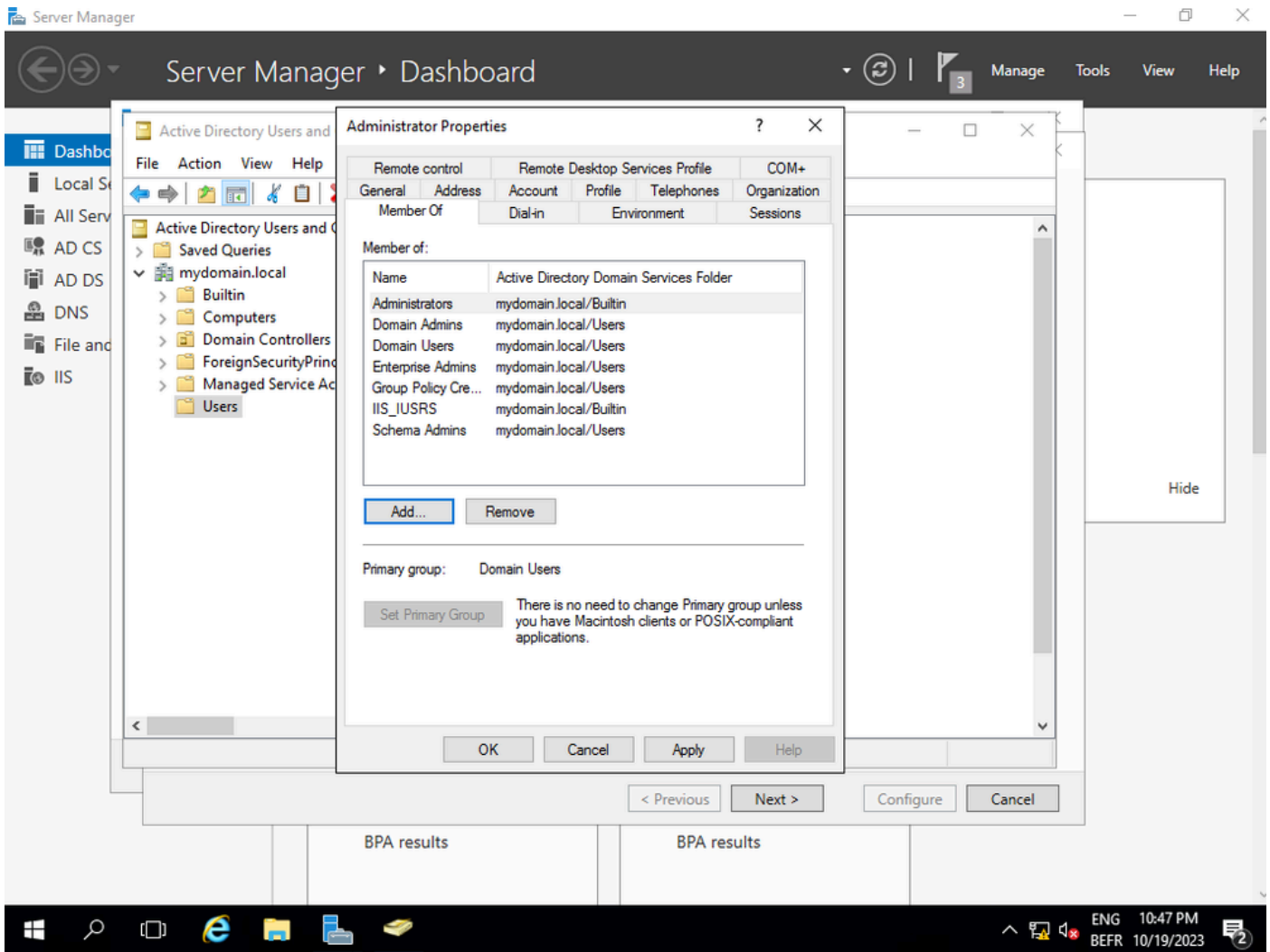
Stap 9. Maak er een root-CA van. Sinds Cisco IOS XE 17.6 worden ondergeschikte CA's ondersteund voor LSC.





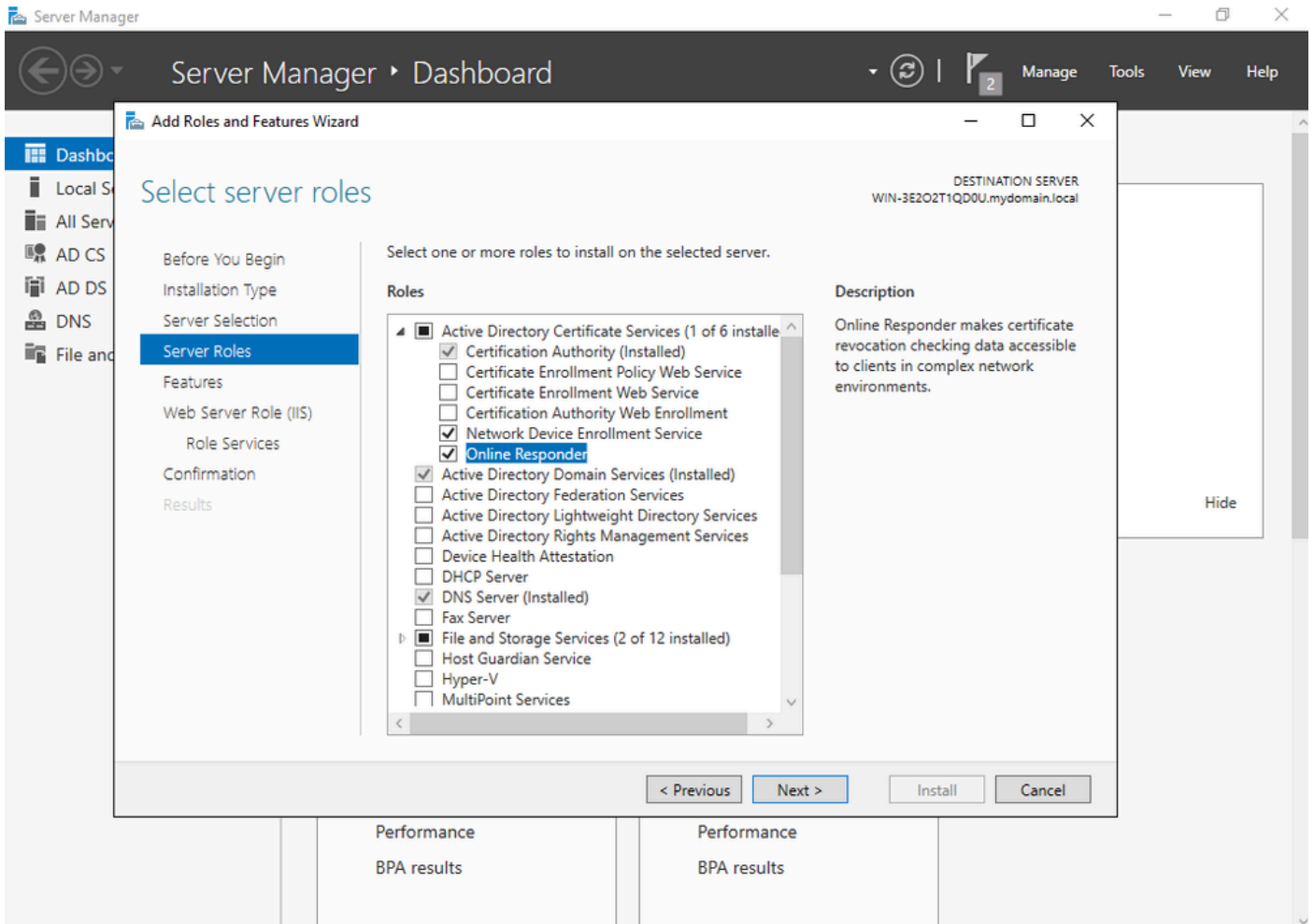
Kies een root-CA

Het is belangrijk dat de account die u gebruikt voor uw CA deel uitmaakt van de groep IIS\_IUSRS. In dit voorbeeld, gebruikt u de rekening van de Beheerder en gaat naar het Actieve menu van de Gebruikers en van Computers van de Folder om de gebruikers van de Beheerder aan de groep toe te voegen IIS\_IUSRS.



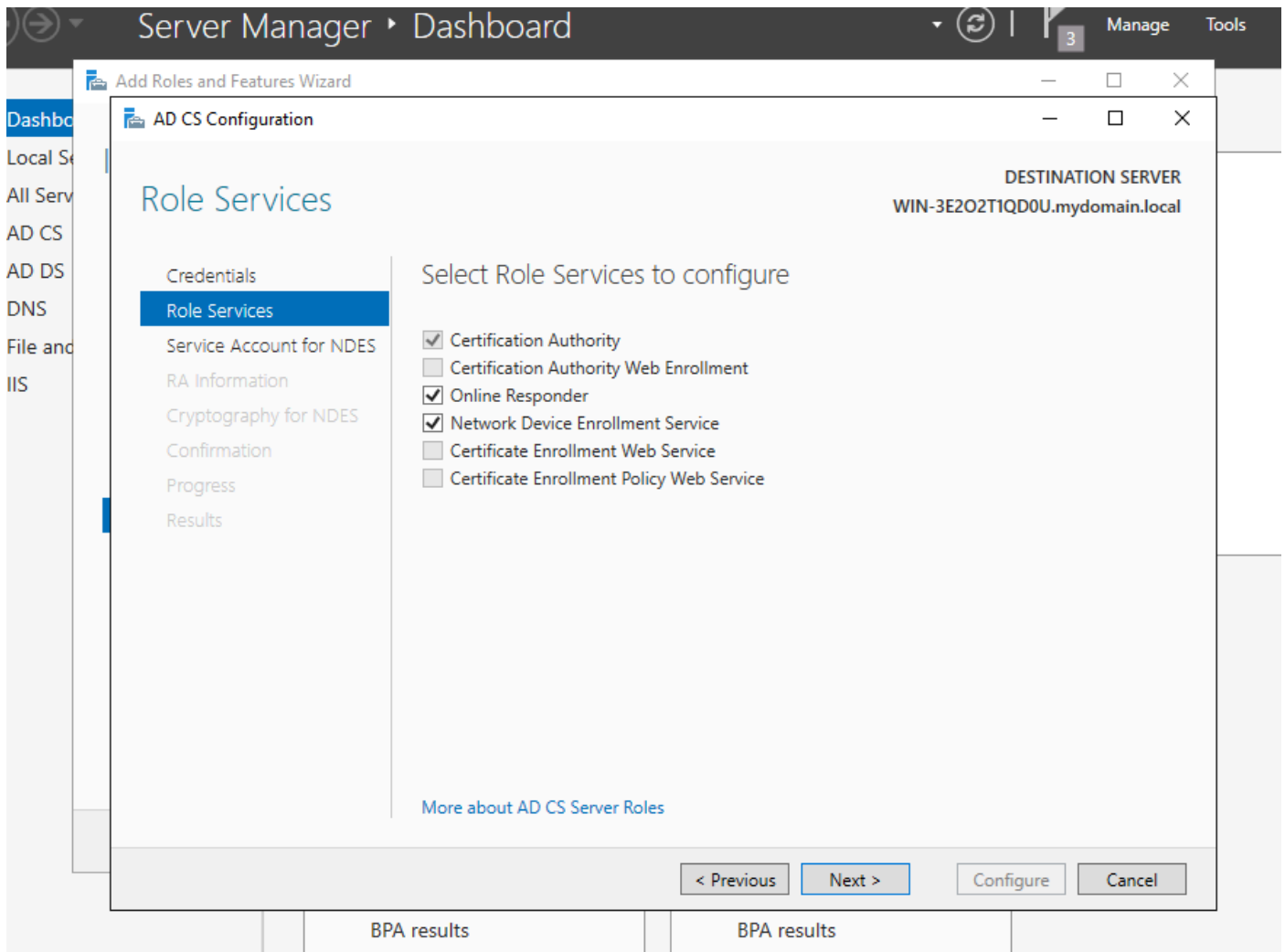
Voeg je admin account toe aan de IIS\_USER groep

Step 10. Zodra u een gebruiker in de juiste IIS-groep hebt, voeg rollen en services toe. Voeg vervolgens de Online Responder- en NDES-services toe aan uw certificeringsinstantie.



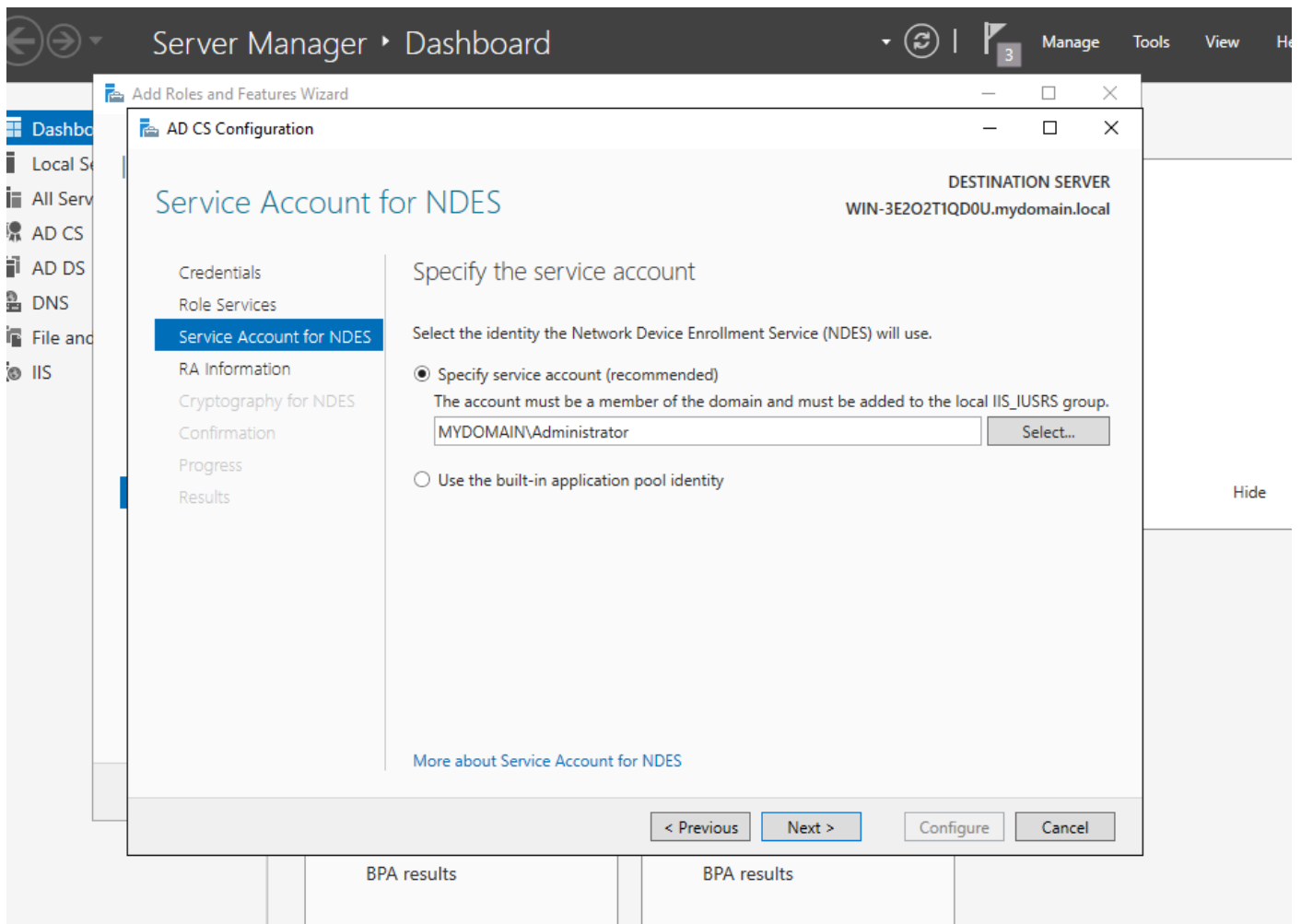
Installeer de NDES- en Online Responder-services

Stap 11. Zodra u klaar bent, configureer deze services.



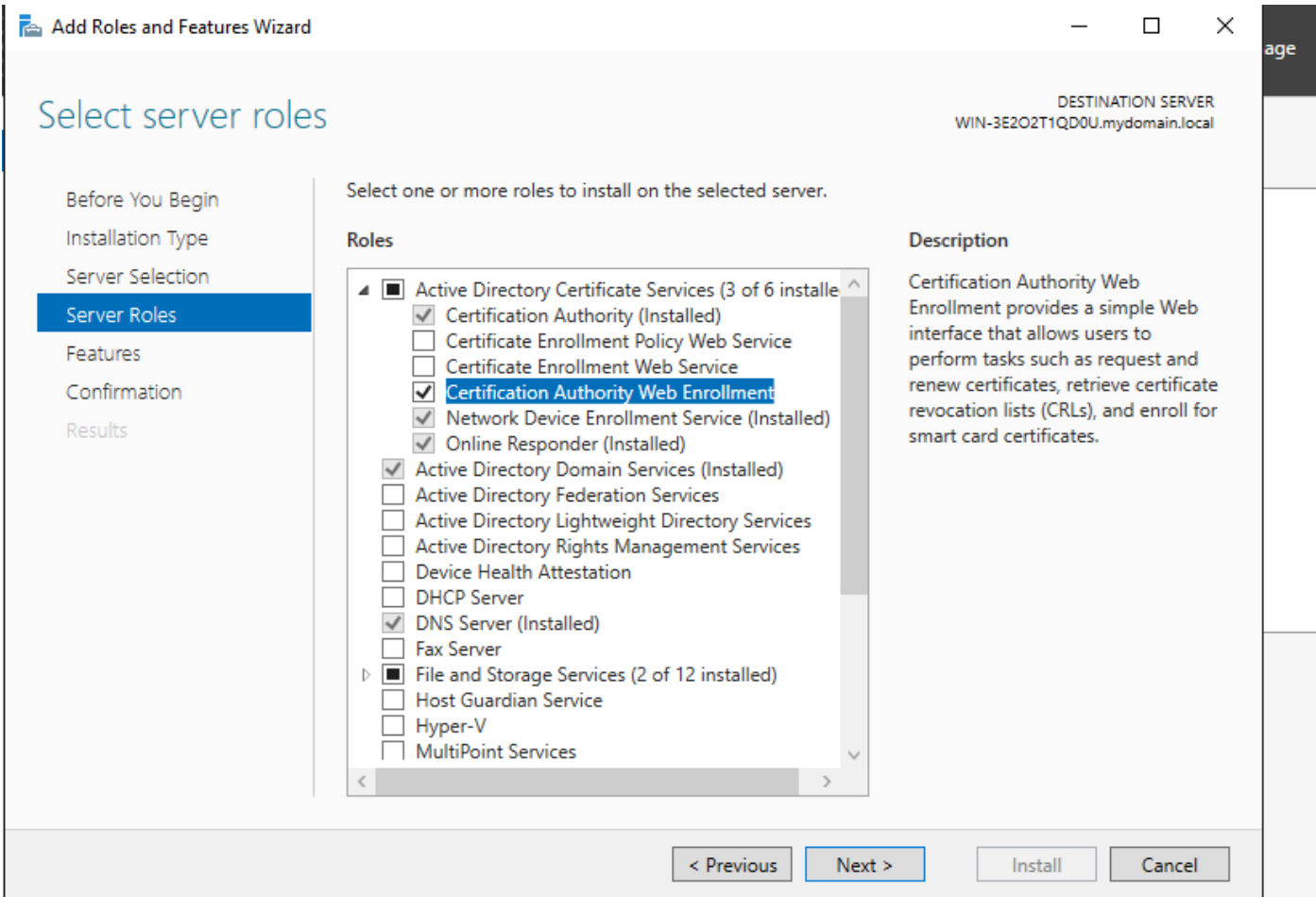
Installeer de Online responder en de NDES-service.

Stap 12. U wordt gevraagd een serviceaccount te kiezen. Dit is de account die u eerder aan de groep IIS\_IUSRS hebt toegevoegd.

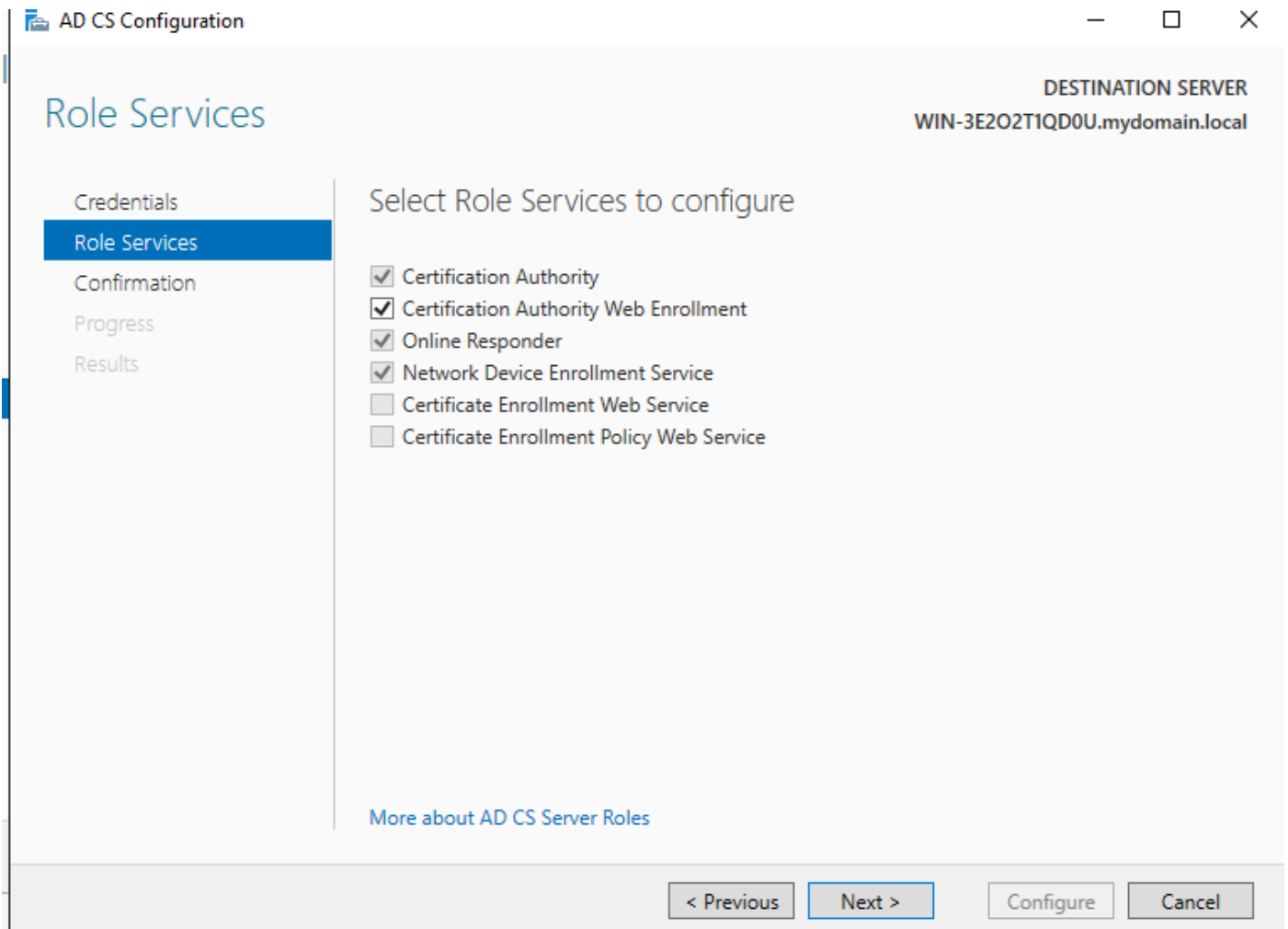


Selecteer de gebruiker die u aan de IIS-groep hebt toegevoegd

Stap 13. Dit is genoeg voor SCEP-bewerkingen, maar om 802.1X-verificatie te kunnen realiseren, moet u ook een certificaat op de RADIUS-server installeren. Daarom, voor gemak, installeer en vorm de dienst van de Webinschrijving om het ISE- certificaatverzoek op onze Server van Windows gemakkelijk te kunnen kopiëren en klevend.

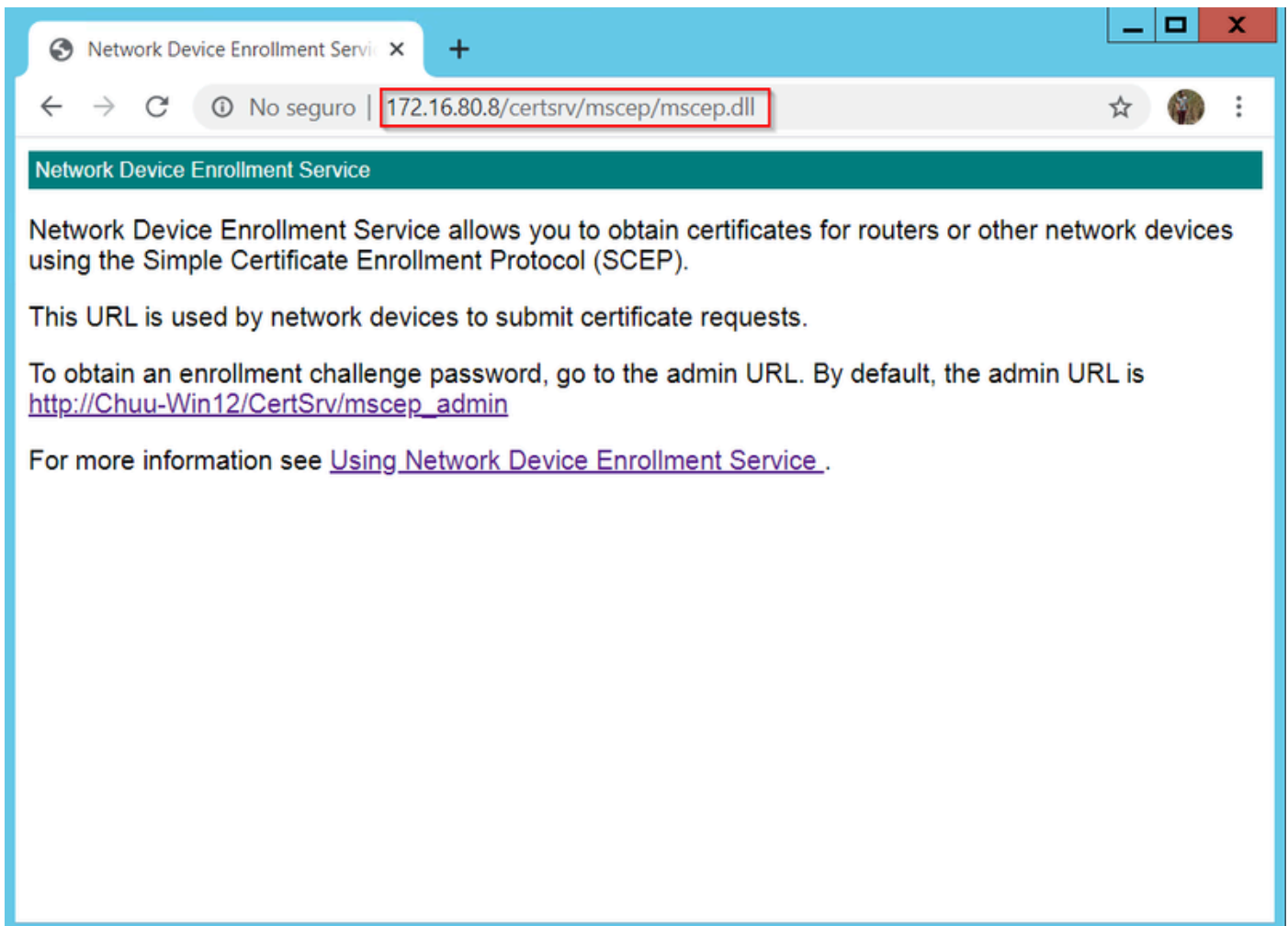


Installeer de webinschrijvingservice



de webinschrijvingservice configureren

Stap 14. U kunt controleren of de SCEP-service correct werkt door te gaan naar <http://<serverip>/certsrv/mscep/mscep.dll> :



Verificatie van SCEP-portal

## Stap 15.

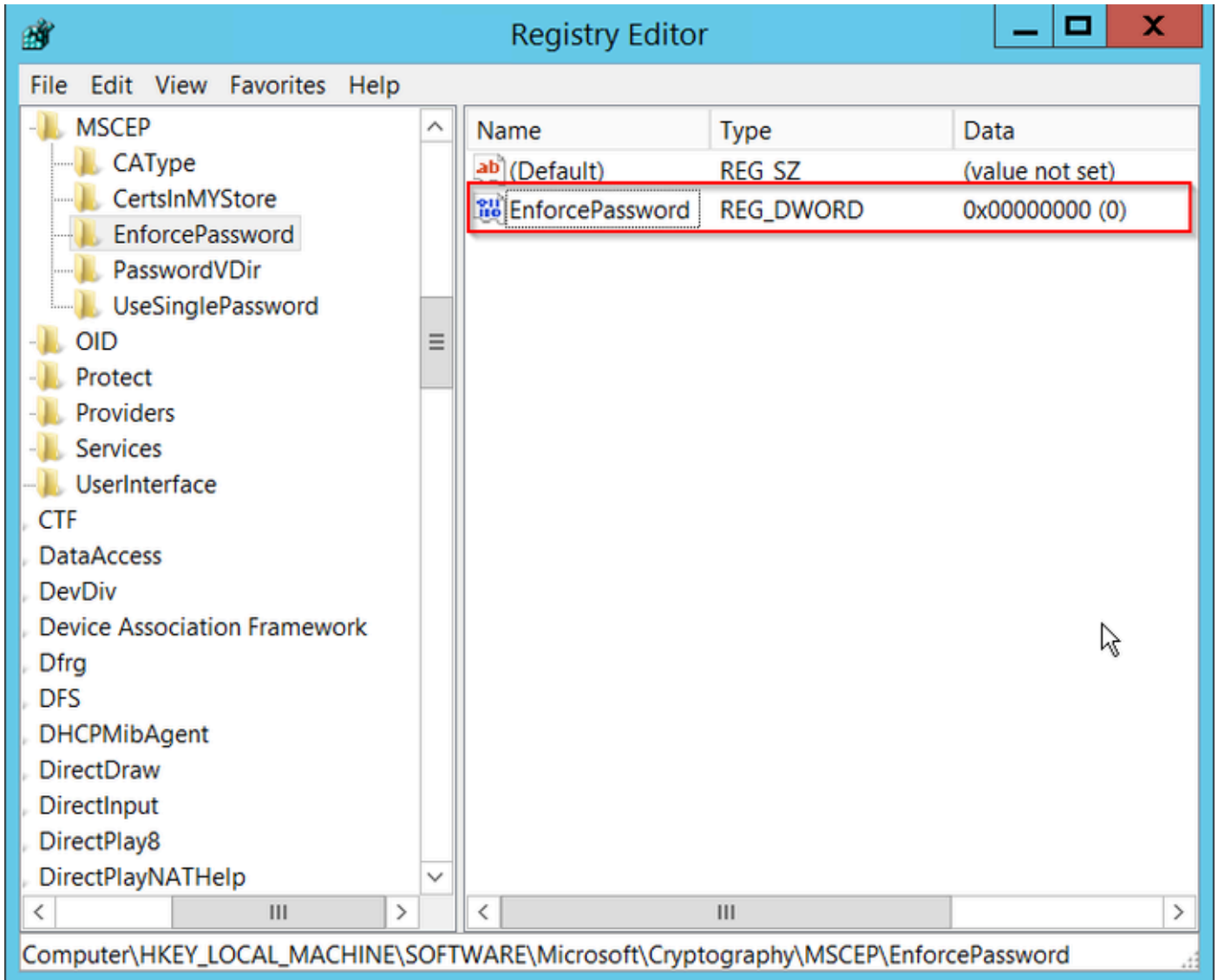
Standaard gebruikt de Windows Server een dynamisch wachtwoord om client- en endpointverzoeken te verifiëren voordat u zich inschrijft bij Microsoft SCEP (MSCEP). Dit vereist een admin-account om naar de web GUI te bladeren om een on-demand wachtwoord voor elk verzoek te genereren (het wachtwoord moet in het verzoek worden opgenomen). De controller is niet in staat om dit wachtwoord op te nemen in de verzoeken die het naar de server stuurt. Om deze functie te verwijderen, moet de registersleutel op de NDES-server worden gewijzigd:

Open de Register-editor, zoek naar Regedit in het menu Start.

Ga naar Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptografie > MSCEP > EnforcePassword

Verander de EnforcePassword waarde in 0. Als het al 0 is, laat het dan zoals het is.





De waarde van het handhavingswachtwoord instellen

## Het certificaatsjabloon en het register configureren

Certificaten en bijbehorende sleutels kunnen worden gebruikt in meerdere scenario's voor verschillende doeleinden die worden gedefinieerd door het toepassingsbeleid binnen de CA-server. Het toepassingsbeleid wordt opgeslagen in het veld Uitgebreide sleutelgebruik (EKU) van het certificaat. Dit veld wordt door de vericator geparseerd om te controleren of de client het voor het beoogde doel gebruikt. Om ervoor te zorgen dat het juiste toepassingsbeleid wordt geïntegreerd in de WLC- en AP-certificaten, maakt u de juiste certificaatsjabloon en brengt u deze in het NDES-register in kaart:


Stap 1. Ga naar Start > Administratieve tools > Certificeringsinstantie.

Stap 2. Breid de mappenstructuur van CA Server uit, klik met de rechtermuisknop op de mappen Certificaatsjablonen en selecteer Beheren.

Stap 3. Klik met de rechtermuisknop op de certificaatsjabloon Gebruikers en selecteer Sjabloon dupliceren in het contextmenu.

Stap 4. Navigeer naar het tabblad Algemeen, verander de naam van de sjabloon en de geldigheidsperiode zoals gewenst, laat alle andere opties onaangevinkt.

---

 Waarschuwing: als de geldigheidsperiode wordt gewijzigd, zorg er dan voor dat deze niet langer is dan de basisgeldigheid van het certificaat van de certificeringsinstantie.

---

## Properties of New Template



Subject Name	Server	Issuance Requirements		
Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation

Template display name:

Template name:

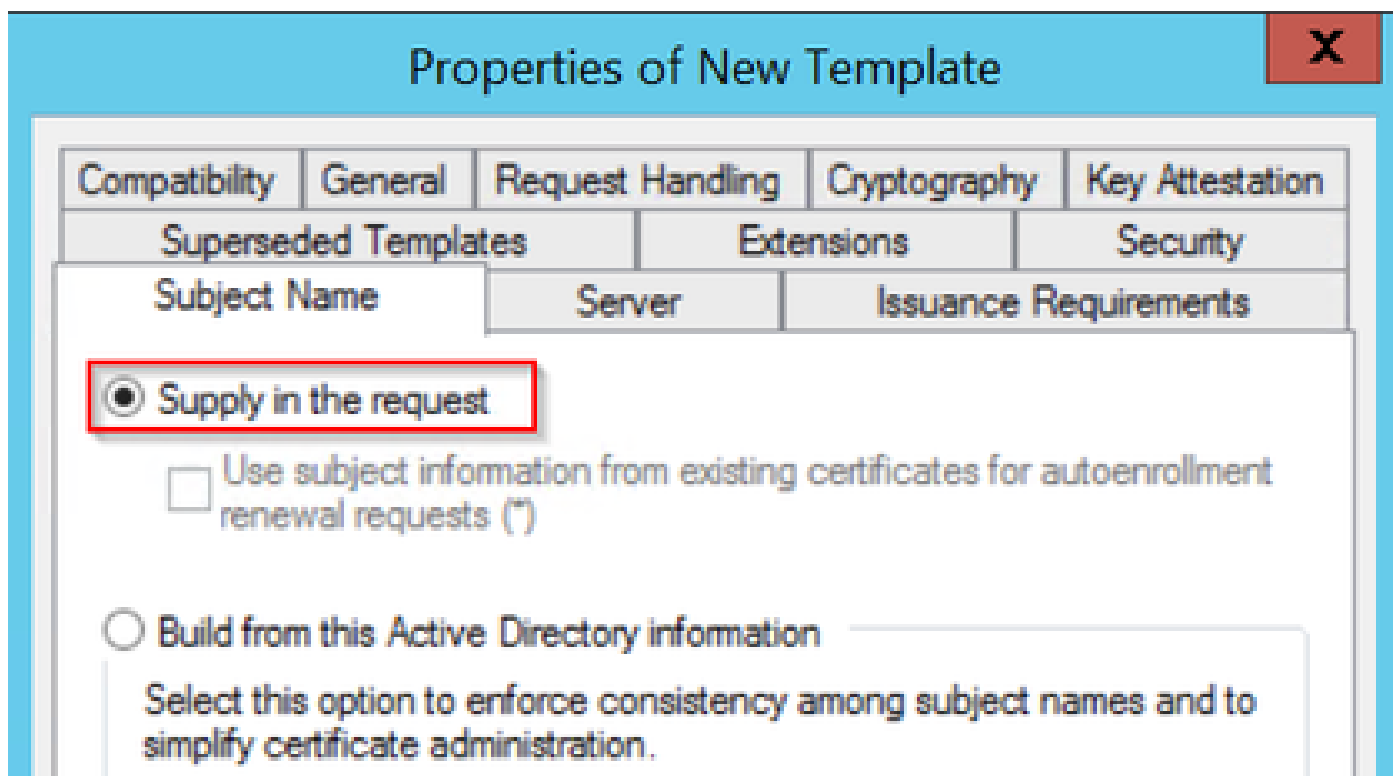
Validity period:  
 years

Renewal period:  
 weeks

Publish certificate in Active Directory

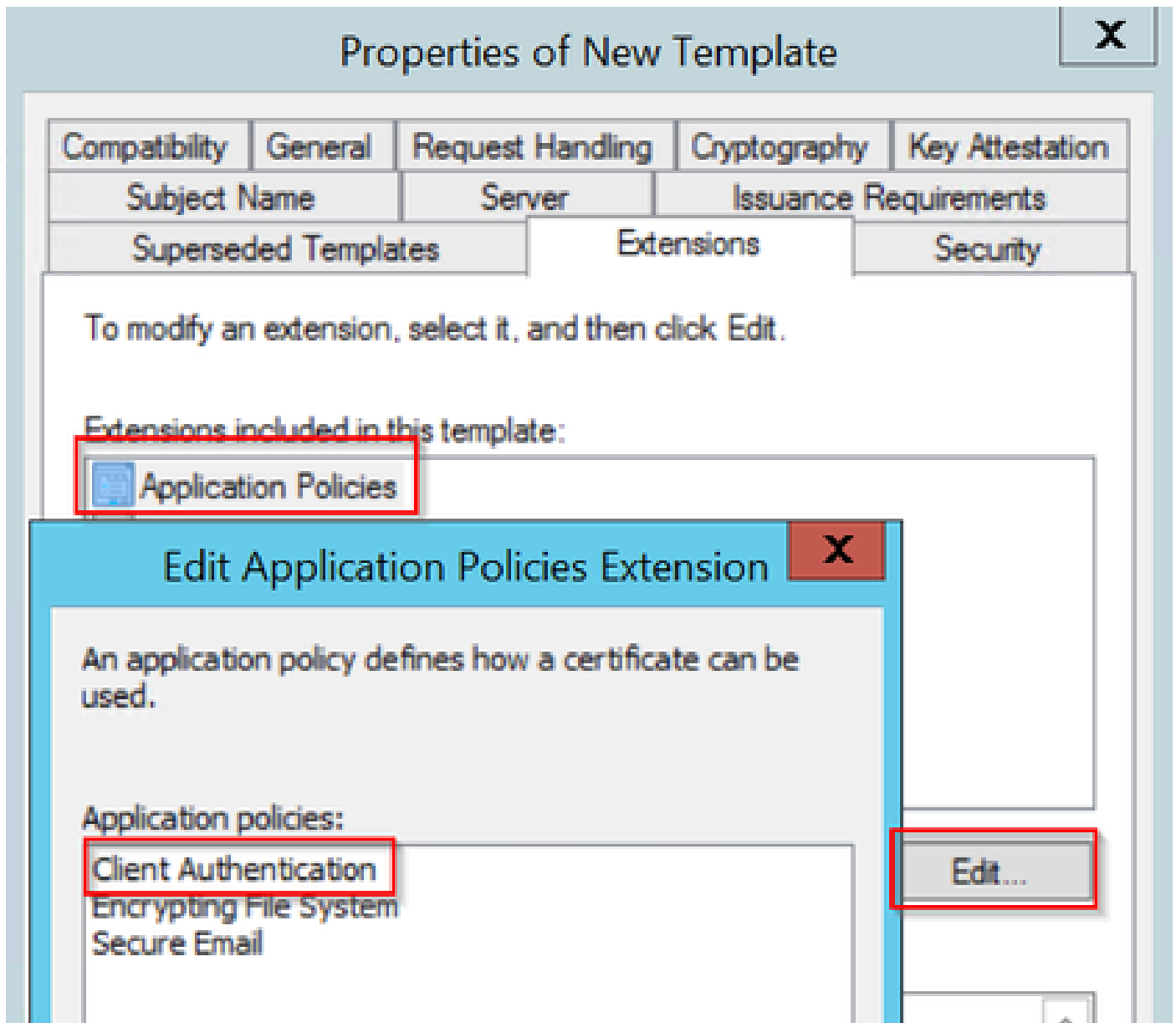
Do not automatically reenroll if a duplicate certificate exists in Active Directory

Stap 5. Navigeer naar het tabblad Onderwerpnaam en zorg ervoor dat Levering in het verzoek is geselecteerd. Een pop-up lijkt aan te geven dat gebruikers geen admin goedkeuring nodig hebben om hun certificaat ondertekend te krijgen, OK selecteren.



Levering in het verzoek

Stap 6. Navigeer naar het tabblad Uitbreidingen en selecteer vervolgens de optie Toepassingsbeleid en selecteer de knop Bewerken.... Zorg ervoor dat de Clientverificatie in het venster Toepassingsbeleid staat; anders selecteert u Toevoegen en voegt u deze toe.



Controleer de uitbreidingen

Stap 7. Navigeer naar het tabblad Security en zorg ervoor dat de serviceaccount die is gedefinieerd in Stap 6 van het tabblad Enable SCEP Services in de Windows Server beschikt over volledige controle-rechten van de sjabloon, en selecteer vervolgens Toepassen en OK.

# Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security

Group or user names:

- Authenticated Users
- Administrator**
- Domain Admins (CHUU-DOMAIN\Domain Admins)
- Domain Users (CHUU-DOMAIN\Domain Users)
- Enterprise Admins (CHUU-DOMAIN\Enterprise Admins)

Add... Remove

Permissions for Administrator


	Allow	Deny
<b>Full Control</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

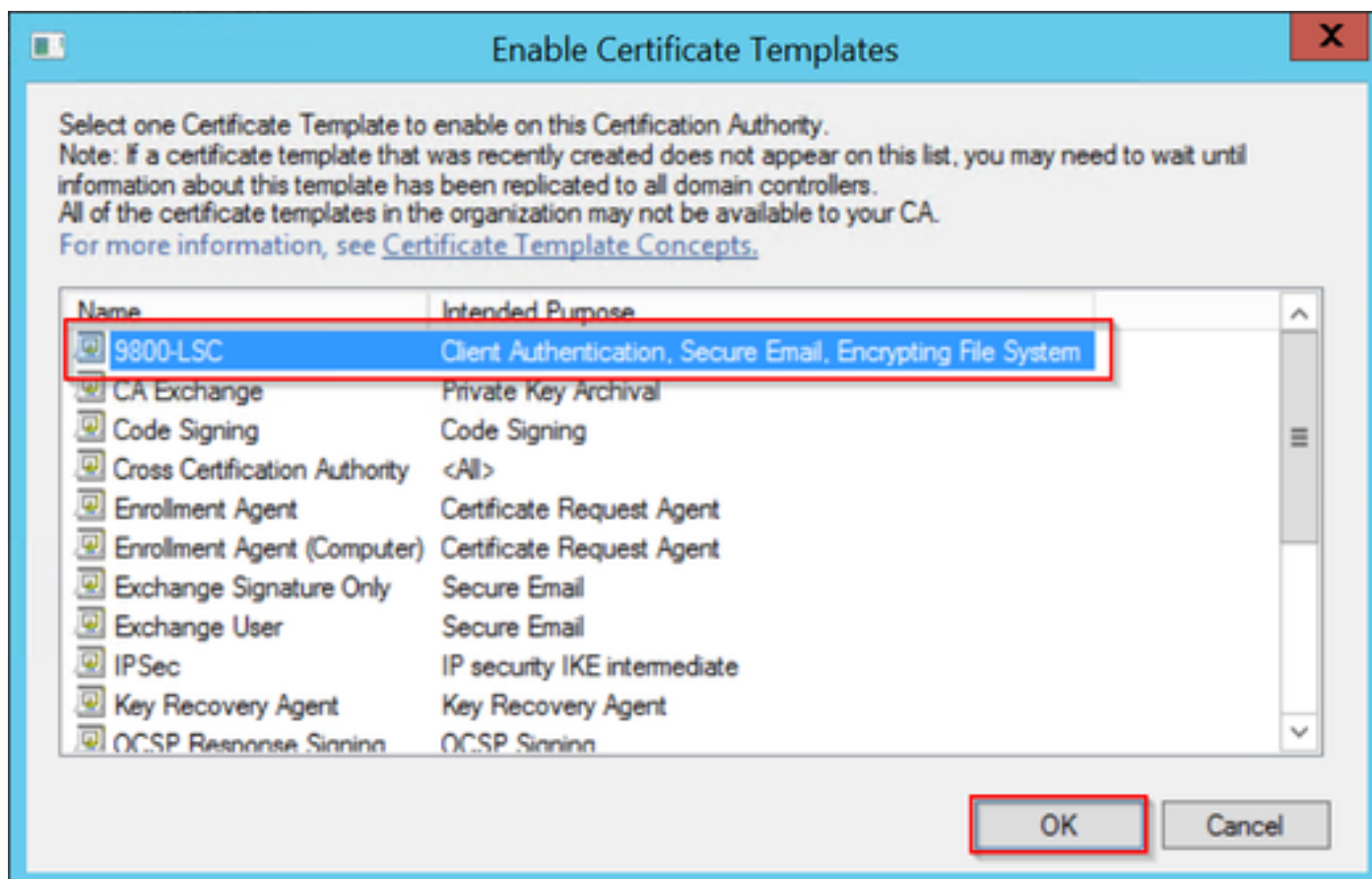
For special permissions or advanced settings, click **Advanced**.

OK Cancel **Apply** Help

Stap 8. Ga terug naar het venster Certificatie-instantie, klik met de rechtermuisknop in de map Certificaatsjablonen en selecteer Nieuw > Certificaatsjabloon voor afgifte.

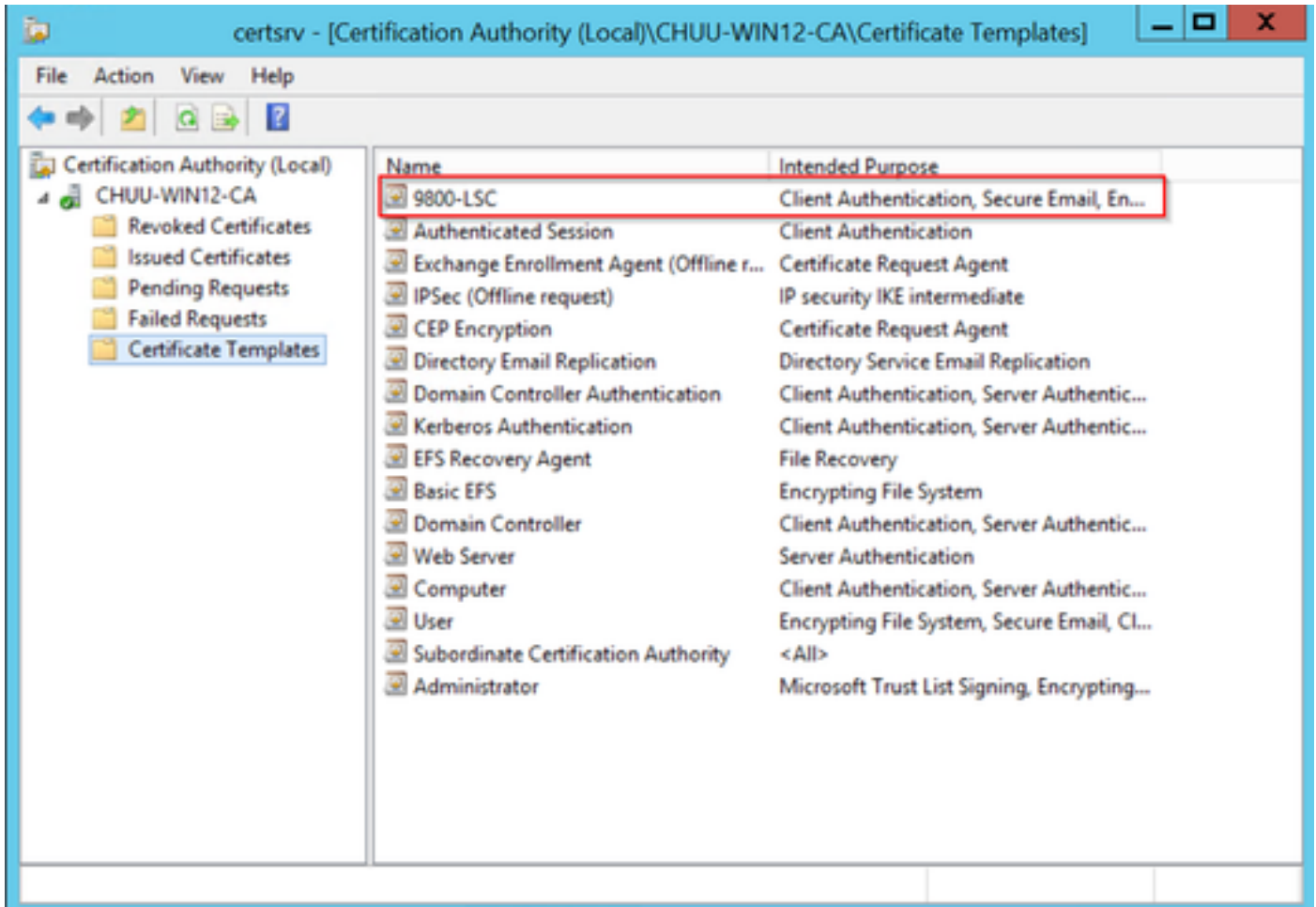
Stap 9. Selecteer de certificaatsjabloon die eerder is gemaakt. In dit voorbeeld is 9800-LSC en selecteer OK.

 Opmerking: het kan langer duren voordat de nieuw gemaakte certificaatsjabloon in meerdere serverimplementaties wordt vermeld, aangezien deze op alle servers moet worden gerepliceerd.



De sjabloon kiezen

De nieuwe certificaatsjabloon is nu opgenomen in de inhoud van de map Certificaatsjablonen.

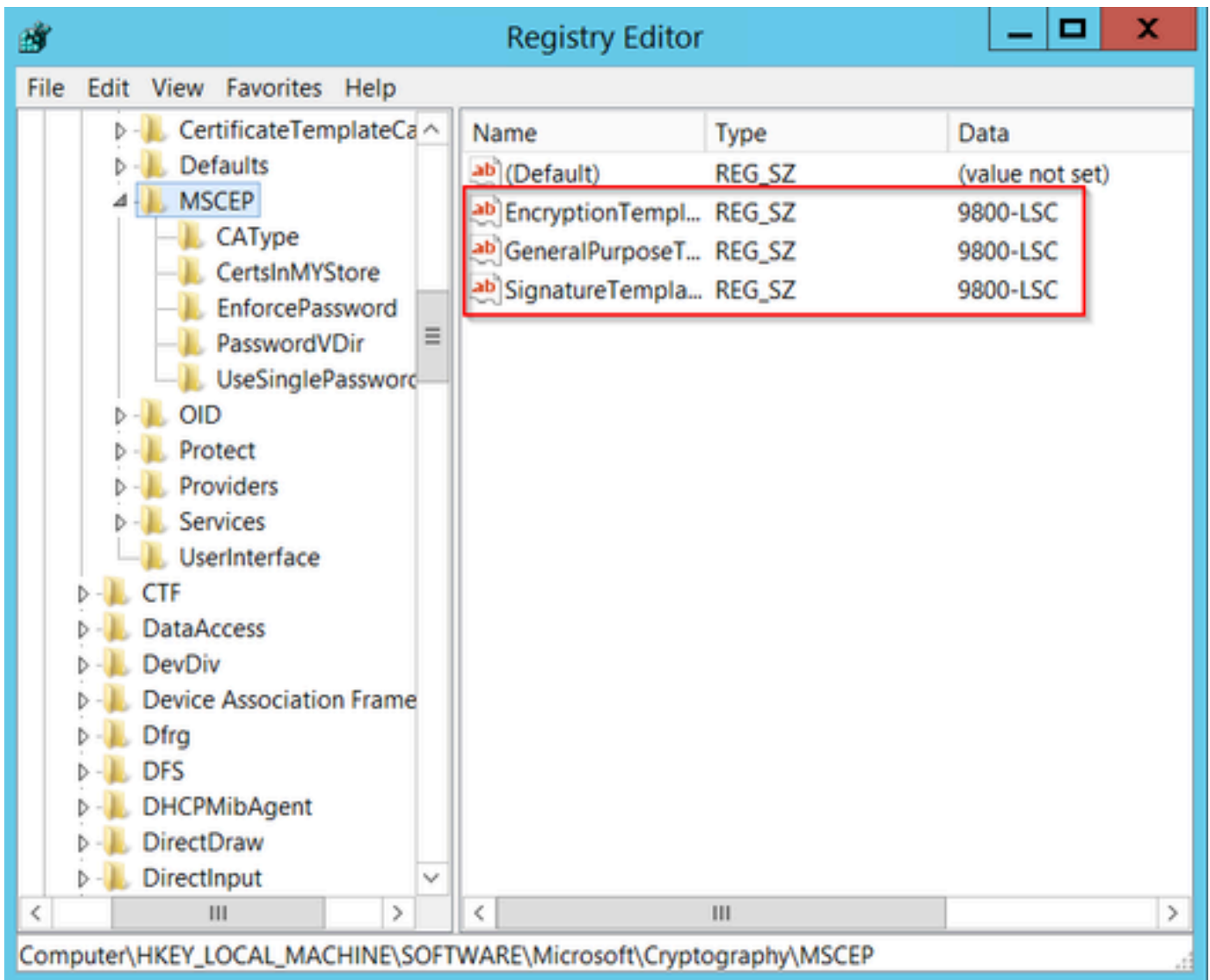


Selecteer de LSC

Stap 10. Ga terug naar het venster Registry Editor en navigeer naar Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

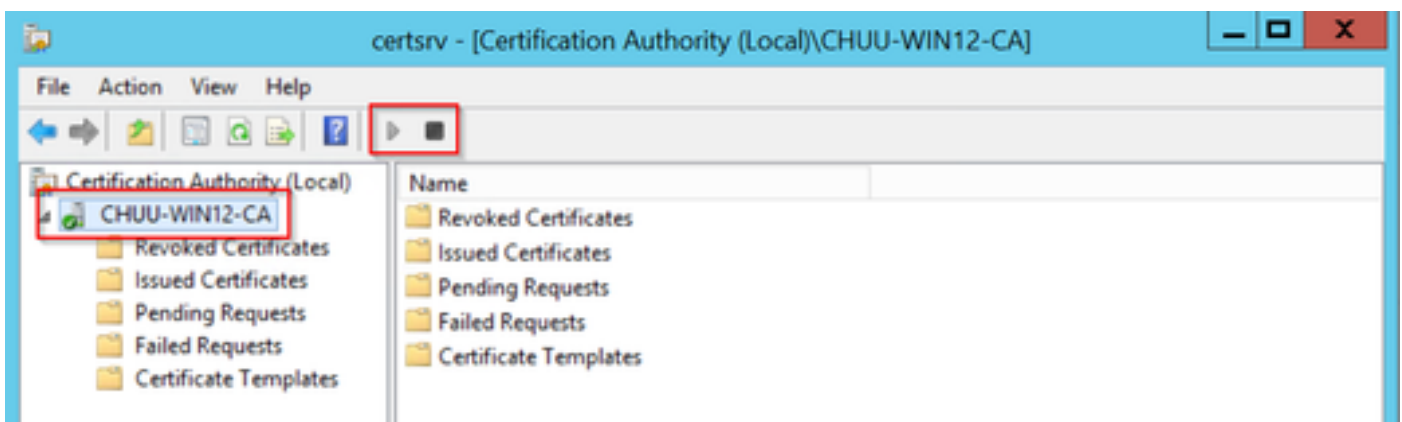
Stap 11. Bewerk de registraties EncryptionTemplate, GeneralPurposeTemplate, en SignatureTemplate zodat ze naar het nieuw gemaakte certificaatsjabloon verwijzen.





De sjabloon in het register wijzigen

Stap 12. Start de NDES-server opnieuw op, ga dus terug naar het venster Certificatie-instansie, selecteer de servernaam en selecteer achtereenvolgens de knop Stop en Play.



## LSC op de 9800 configureren

Hier volgen de stappen voor het configureren van LSC voor AP in WLC.

1. Maak een RSA-sleutel. Deze sleutel wordt later gebruikt voor PKI trustpoint.
2. Maak een trustpoint en breng de gemaakte RSA-sleutel in kaart.
3. Laat LSC levering voor APs toe en breng trustpoint in kaart.
  1. LSC inschakelen voor alle aangesloten AP's.
  2. LSC voor geselecteerde AP's inschakelen via voorzieningslijst.
4. Verander het Draadloze beheer trustpoint en punt aan LSC trustpoint.

## Configuratiestappen AP LSC GUI

Stap 1. Navigeer naar configuratie > Beveiliging > PKI-beheer > genereren van sleutelparen.

1. Klik op Add en geef het een relevante naam.
2. Voeg de RSA-sleutelgrootte toe.
3. De belangrijkste exporteerbare optie is optioneel. Dit is alleen nodig als u de sleutel uit het vak wilt exporteren.
4. Selecteer Generate

The screenshot shows the Cisco PKI Management interface. The breadcrumb navigation is Configuration > Security > PKI Management. The 'Key Pair Generation' tab is active. A table lists existing key pairs, and a modal form is open for adding a new one. The form fields are highlighted with red boxes:

Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	<input type="checkbox"/>
9800-40.cisco.com	RSA	No	<input type="checkbox"/>
TP-self-signed-2147029136.server	RSA	No	<input type="checkbox"/>
CISCO_IDEVID_SUDI	RSA	No	<input type="checkbox"/>
CISCO_IDEVID_SUDI_LEGACY	RSA	No	<input type="checkbox"/>

The configuration form fields are:

- Key Name\*: AP-SCEP
- Key Type\*:  RSA Key  EC Key
- Modulus Size\*: 2048
- Key Exportable\*:

Buttons: Cancel, Generate

Stap 2. Navigeren naar configuratie > Beveiliging > PKI-beheer > Trustpoints

1. Klik op Add en geef het een relevante naam.
2. Voer de URL van de inschrijving in (hier is de URL <http://10.106.35.61:80/certsrv/mscep/mscep.dll>) en de rest van de gegevens.
3. Selecteer RSA-sleutelparen die in stap 1 zijn gemaakt.
4. Klik op Verifiëren.
5. Klik op Inschrijven op trustpoint en voer een wachtwoord in.
6. Klik op Toepassen op apparaat.

Configuration > Security > PKI Management

### Add Trustpoint

Label\*  Enrollment Type  SCEP  Terminal

**Subject Name**

Country Code  State

Location  Domain Name

Organization  Email Address

Enrollment URL  Authenticate

Key Generated  Available RSA Keypairs

Enroll Trustpoint

Password\*

Re-Enter Password\*

Step 3. Navigeer naar Configuration > Wireless > Access points. Scroll naar beneden en selecteer LSC Provision.

1. Selecteer de status zoals deze is ingeschakeld. Dit laat LSC voor alle APs toe die aan deze WLC worden aangesloten.
2. Selecteer de trustpoint naam die we in Stap 2 gecreëerd hebben.

Vul de rest van de gegevens in volgens uw behoeften.

Configuration > Wireless > Access Points

All Access Points

Total APs: 1

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP000-F89A-46E0	C9117AXI-D	2	Enabled	0 days 0 hrs 26 mins 42 secs	10.105.101.158	80ec.3579.0300	0cd0.f99a.46e0	Local	Yes	Registered	Healthy

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Status

Trustpoint Name

Number of Join Attempts

Key Size

Certificate chain status

Subject Name Parameters

Country

State

City

Organization

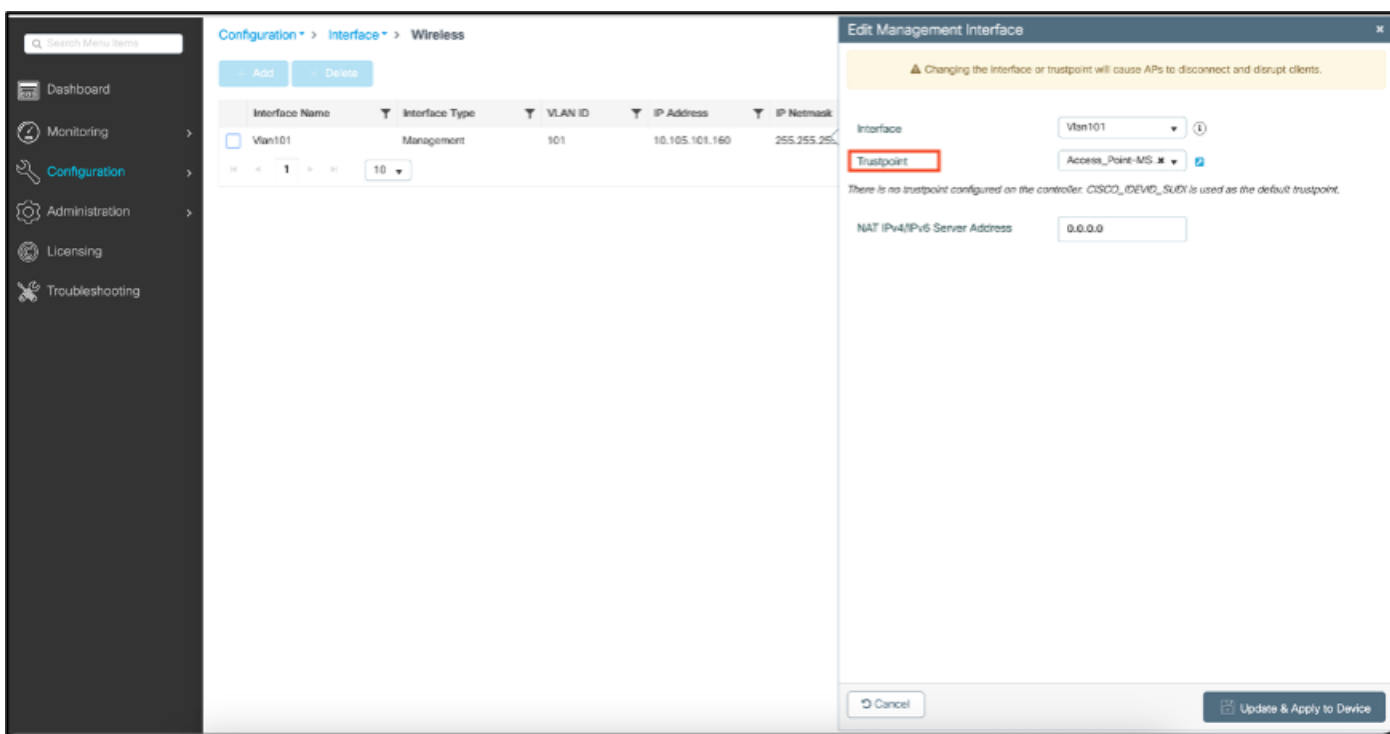
Zodra u LSC inschakelt, downloaden AP's het certificaat via WLC en rebooten. In de AP console sessie, zie je dan iets als dit fragment.

```
[*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
```

Stap 4. Zodra LSC is ingeschakeld, kunt u het certificaat voor draadloos beheer wijzigen in overeenstemming met het LSC-betrouwbaarheidspunt. Dit maakt AP's samenvoegen met hun LSC-certificaten en de WLC gebruikt zijn LSC-certificaat voor AP-samenvoegen. Dit is een optionele stap als uw enige interesse is om 802.1X-verificatie van uw AP's te doen.

1. Ga naar Configuration > Interface > Wireless en klik op Management Interface.
2. Verander het Trustpoint om het trustpoint aan te passen dat we in stap 2 hebben gemaakt.

Hiermee is het configuratieonderdeel van de LSC GUI voltooid. AP's moet zich bij WLC kunnen nu aansluiten met behulp van de LSC cert.



## Configuratiestappen AP LSC CLI

1. Maak een RSA-toets met deze opdracht.

```
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 storage
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Maak PKI-trustpoint en breng het RSA-sleutelpaar in kaart. Voer de URL van de inschrijving en de rest van de gegevens in.

```
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)#rsaakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Verifieer en registreer het PKI-vertrouwenspunt met de CA-server met behulp van de opdracht `crypto pki authenticate <trustpoint>`. Voer een wachtwoord in als om het wachtwoord wordt gevraagd.

```
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' command will 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. AP-verbinding configureren met LSC-certificaat.

```
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-L
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. Verander het Draadloze Management Trustpoint om het trustpoint aan te passen dat hierboven is gemaakt.

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

### AP LSC-verificatie

Voer deze opdrachten op WLC uit om de LSC te verifiëren.

```
#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 AP@CD0.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-OTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP @02.lx LSC Status
Certificate status : Not Available
AP LSC authentication state : CAPWAP-OTLS

```

Zodra APs worden herladen, meld u aan bij AP CLI en voer deze opdrachten uit om LSC-configuratie te verifiëren.

```

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

```

```

AP@CD0.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
```

## Probleemoplossing voor LSC-provisioning

U kunt een EPC-opname maken van de WLC of AP uplink switch poort om te controleren of het certificaat dat AP gebruikt om de CAPWAP- te vormen. Controleer vanuit de PCAP of de DTLS-tunnel met succes is gebouwd.

```
▼ 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: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d_ (pkcs-9-at-emailAddress=mail@tac-lab.local,id-at-commonName=
  ▼ 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)
  ▼ RDNSSequence item: 1 item (dc=com)
  ▼ RelativeDistinguishedName item (dc=com)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: com
  ▼ RDNSSequence item: 1 item (dc=tac-lab)
  ▼ RelativeDistinguishedName item (dc=tac-lab)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: tac-lab
  ▼ RDNSSequence item: 1 item (dc=sumans)
  ▼ RelativeDistinguishedName item (dc=sumans)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: sumans
  ▼ RDNSSequence 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)
```

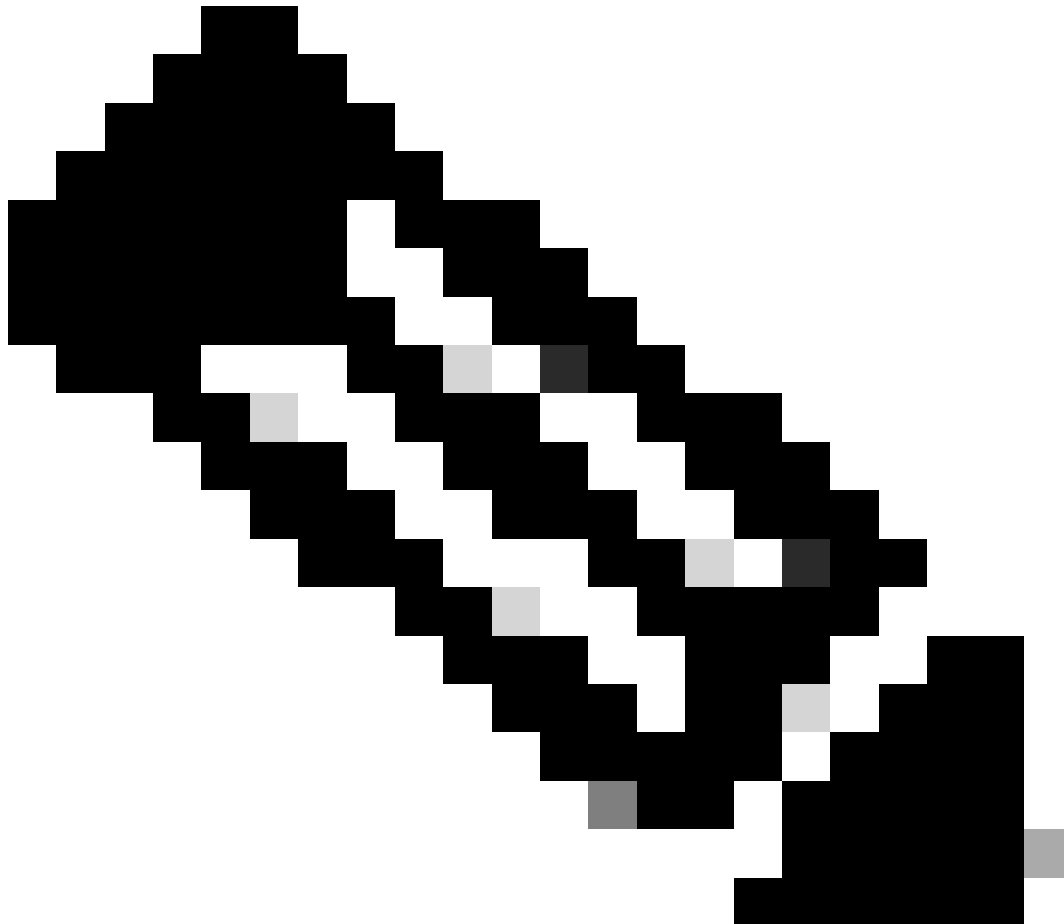
DTLS-debuggs kunnen worden uitgevoerd op AP en WLC om het certificaatprobleem te begrijpen.



## AP-bekabelde 802.1X-verificatie met LSC

AP is ingesteld om hetzelfde LSC-certificaat te gebruiken voor verificatie. AP fungeert als 802.1X aanvrager en wordt door de switch geverifieerd op basis van de ISE-server. ISE-server praat met de AD in het backend.

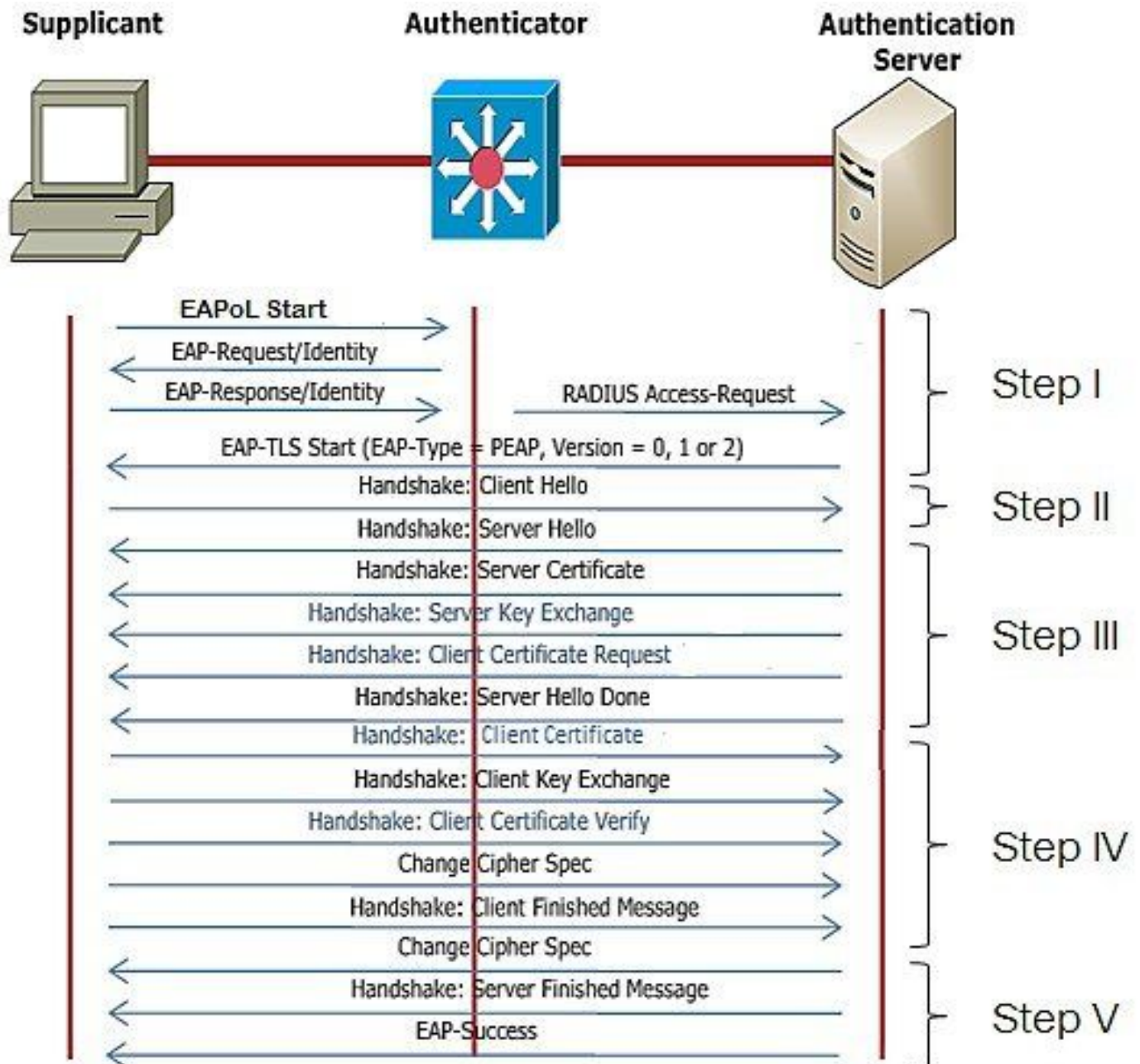
---



Opmerking: als dot1x-verificatie is ingeschakeld op de poort van de AP uplink-switch, kunnen AP's geen verkeer doorsturen of ontvangen totdat de verificatie is doorgegeven. Als u AP's met onsuccesvolle verificatie wilt herstellen en toegang tot AP wilt krijgen, schakelt u dot1x auth uit op de bekabelde AP-switch poort.

---

EAP-TLS-verificatie, werkstroom en berichtenuitwisseling

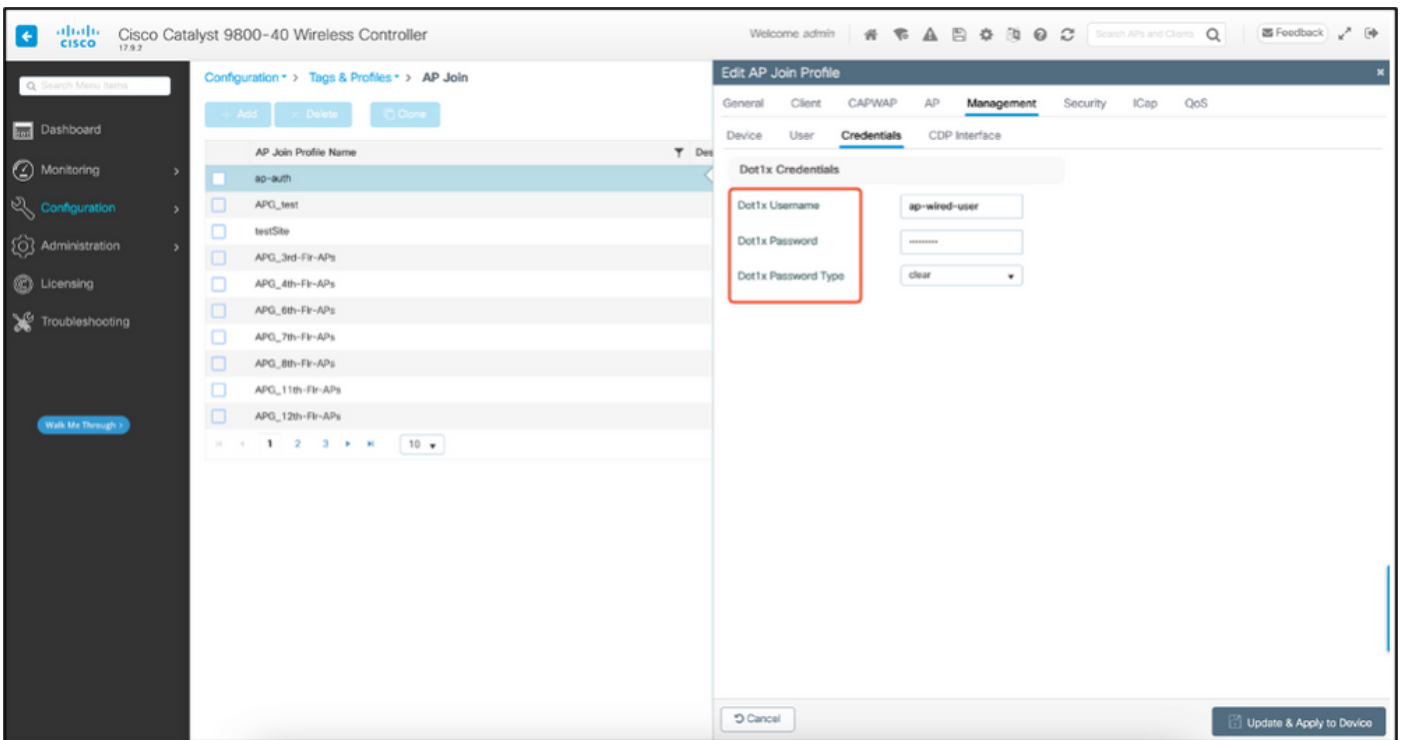
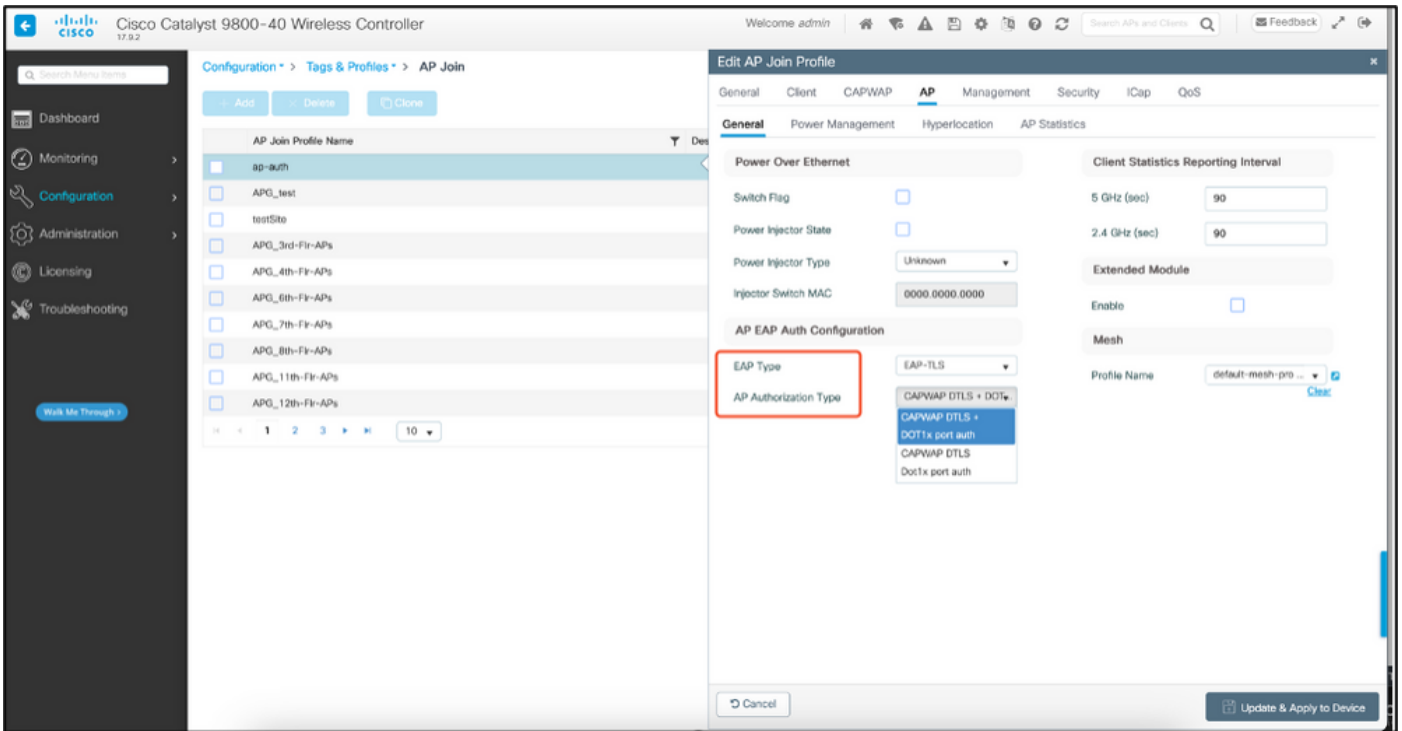


## Configuratiestappen voor AP Wired 802.1x-verificatie

1. Schakel dot1x-poortadapter in samen met CAPWAP DTLS en selecteer het EAP-type.
2. Creeer dot1x geloofsbrieven voor APs.
3. Schakel dot1x in op de switch.
4. Installeer een vertrouwd certificaat op de RADIUS-server.

## Configuratie van bekabelde AP-802.1x-verificatie en GUI

1. Navigeer naar het toetredingspartnersprofiel van het toegangspunt en klik op het profiel.
  1. Klik op AP > Algemeen. Selecteer het EAP-type en het AP-autorisatietype als "CAPWAP DTLS + dot1x port auth".
  2. Navigeer naar Beheer > Credentials en voer een gebruikersnaam en wachtwoord in voor AP dot1x-verificatie.



## CLI-configuratie voor AP-bekabelde 802.1x-verificatie

Gebruik deze opdrachten om dot1x voor AP's vanuit de CLI in te schakelen. Dit maakt alleen bekabelde verificatie mogelijk voor AP's die gebruik maken van het specifieke Joed-profiel.

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

## Configuratie van bekabelde AP-Switch 802.1x-verificatie

Deze switch configuraties worden gebruikt in LAB om bekabelde AP-verificatie in te schakelen. U kunt verschillende configuratie hebben op basis van ontwerp.

```
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
```

## Installatie van RADIUS-servercertificaat

De verificatie vindt plaats tussen het toegangspunt (dat fungeert als de aanvrager) en de RADIUS-server. Beiden moeten elkaar vertrouwen. De enige manier om het AP-vertrouwen in het RADIUS-servercertificaat te hebben, is om de RADIUS-server een certici-certificaat te laten gebruiken dat is afgegeven door de SCEP CA die ook het AP-certificaat heeft afgegeven.

In ISE, ga naar Administratie > Certificaten > Generate Certificaat Ondertekeningsaanvragen

Genereer een CSR en vul de velden met de informatie van uw ISE-knooppunt.

### Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

**ISE Identity Certificates:**

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.
- Data Connect Certificate - Connect to Oracle Database

**ISE Certificate Authority Certificates:**

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

**Usage**

Certificate(s) will be used for **EAP Authentication**

Allow Wildcard Certificates

**Node(s)**

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ISE99	ISE99#EAP Authentication

**Subject**

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Nadat u deze hebt gegenereerd, kunt u deze exporteren en ook kopiëren en plakken als tekst.

Navigeer naar uw Windows CA IP-adres en voeg /certsrv/ toe aan de URL

Klik op Certificaat aanvragen

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

Microsoft Active Directory Certificate Services – mydomain-WIN-3E202T1QD0U-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Klik op Een certificaataanvraag indienen met een base-64 ....

← Non sécurisé | 192.168.1.98/certsrv/certrqad.asp

Microsoft Active Directory Certificate Services – mydomain-WIN-3E2021QD0U-CA

### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

Plakt de MVO-tekst in het tekstvak. Kies de sjabloon voor het webservercertificaat.

← Non sécurisé | 192.168.1.98/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – mydomain-WIN-3E2021QD0U-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

**Certificate Template:**

(No templates found) ▾

**Additional Attributes:**

Attributes:

U kunt dit certificaat vervolgens op ISE installeren door terug te gaan naar het menu Certificaat-ondertekeningsaanvraag en klik op Bindcertificaat. U kunt vervolgens het certificaat uploaden dat u bij uw Windows C hebt verkregen.

≡ Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority >

## Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.

🔍 View 📄 Export 🗑️ Delete 🔗 Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ISE99#EAP Authentication	CN=ISE99.mydomain.local	4096		Mon, 30 Oct 2023	ISE99

Verificatie van bekabelde AP-802.1x-verificatie

Neem consoletoegang tot AP en voer de opdracht uit:

```
#show ap authentication status
```

Ap-verificatie is niet ingeschakeld:

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

Console logt vanaf AP na het inschakelen van ap auth:

```
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 is geverifieerd:

```
AP0CD0.F89A.46E0#sho ap authentication status
vay mgmt IEEE 802.1X (no WPA)
vpa state=COMPLETED
address=0c:d0:f8:9a:46:e0
supplicant PAK state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
cap_tls_version=TLSv1.2
EAP TLS cipher=ECDSA-RSA-AES256-GCM-SHA384
tls_session_reused=0
cap_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ca2bdd11f40494a4325dc98d1919af48b9f33ce526f18eda11effcb2ea0238cf95244aaf5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

WLC-verificatie:

```
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
```

SwitchPort-interfacestatus na succesvolle verificatie:

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
-----
G11/0/2 0cd0.f89a.46e0 dot1x DATA Auth 9765690A0000005CCEED0FBF
```

Dit is een voorbeeld van logbestanden van de AP-console die wijzen op een succesvolle verificatie:

```
[*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 comp1

## Probleemoplossing 802.1X-verificatie

Neem PCAP op de AP uplink en controleer de radius authenticatie. Hier is een fragment van succesvolle verificatie.

479.	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, Identity[Packet size limited during capture]
479.	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP...	TLSh1.2	Encrypted Handshake Message
479.	07:47:17.256975	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.267976	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.270982	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.274979	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.277983	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.311988	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.324988	Cisco_9a:46:e0	Nearest-non-TP...	TLSh1.2	Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, (Change Cipher Spec, Encrypted Handshake M...
479.	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.376979	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Accept id=251

TCPdump verzamelt van ISE-opnamen van de verificatie.

80	07:47:18.171005	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
80	07:47:18.184982	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
80	07:47:18.197978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
79	07:47:18.210982	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
79	07:47:18.223978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
79	07:47:18.236978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
79	07:47:18.249978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
79	07:47:18.262978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
79	07:47:18.275978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
79	07:47:18.288978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
79	07:47:18.301978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
80	07:47:18.314978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
80	07:47:18.327978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
80	07:47:18.340978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
80	07:47:18.353978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
82	07:47:01.945978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Accept id=251

Als er een probleem wordt geobserveerd tijdens de verificatie, is er een gelijktijdige pakketopname van de bekabelde AP-uplink en de ISE-zijde nodig.

Debug opdracht voor AP:

```
#debug ap authentication packet
```

## Gerelateerde informatie

- [Cisco Technical Support en downloads](#)
- [802.1X configureren op AP met AireOS](#)
- [9800 configuratiehandleiding voor LSC](#)
- [LSC-configuratievoorbeeld voor 9800](#)
- [802.1X configureren voor AP's op 9800](#)



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.