Configuratievoorbeeld voor lokale belangrijke certificaten (LSC) met WLC en Windows Server 2012

Inhoud

Inleiding

Dit document beschrijft hoe u lokaal belangrijke certificaten (LSC) kunt configureren met een draadloze LAN-controller (WLC) en een nieuw geïnstalleerd Microsoft Windows Server 2012 R2.

> Opmerking: Reële implementaties kunnen op veel punten verschillen. U dient volledige controle en kennis te hebben over de instellingen op Microsoft Windows Server 2012. Dit configuratievoorbeeld wordt alleen geleverd als een referentiesjabloon voor Cisco-klanten om hun Microsoft Windows Server-configuratie te implementeren en aan te passen om LSC te laten werken.

Voorwaarden

Vereisten

Cisco raadt u aan elke wijziging te begrijpen die in Microsoft Windows Server is gemaakt en indien nodig de relevante Microsoft documentatie te controleren.

> Opmerking: LSC op WLC wordt niet ondersteund met intermediair-CA, omdat de basis-CA wordt gemist vanuit WLC omdat de controller alleen de intermediaire CA krijgt.

Gebruikte componenten

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

- WLC versie 7.6

- Microsoft Windows Server 2012 R2

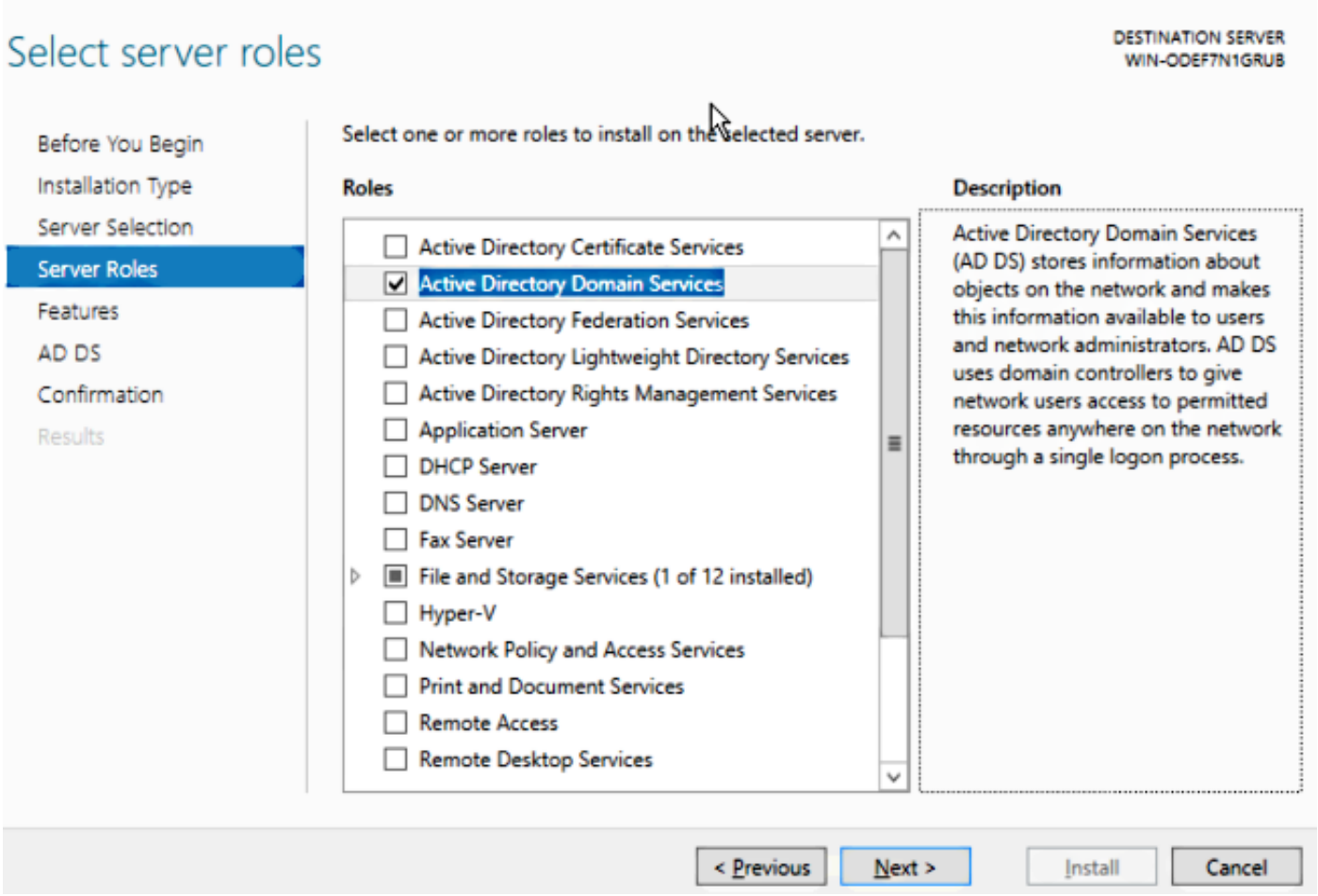
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

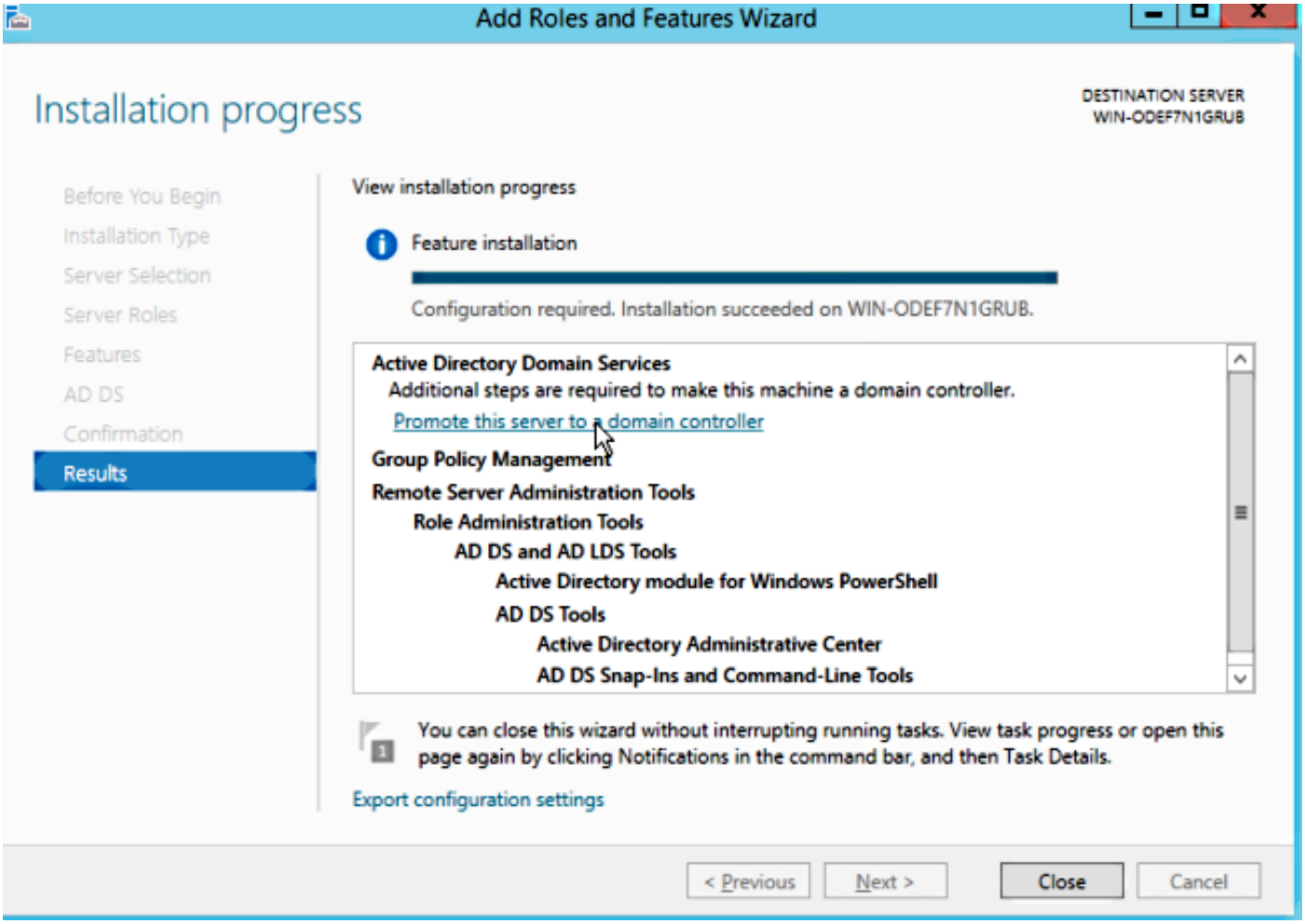
Configuratie Microsoft Windows-server

Deze configuratie wordt weergegeven zoals uitgevoerd op een nieuw geïnstalleerd Microsoft Windows Server 2012. U moet de stappen aan uw domein en uw configuratie aanpassen.

Stap 1. Installeer de actieve Domeinservices van de Map voor de rollen en eigenschappen wizard.

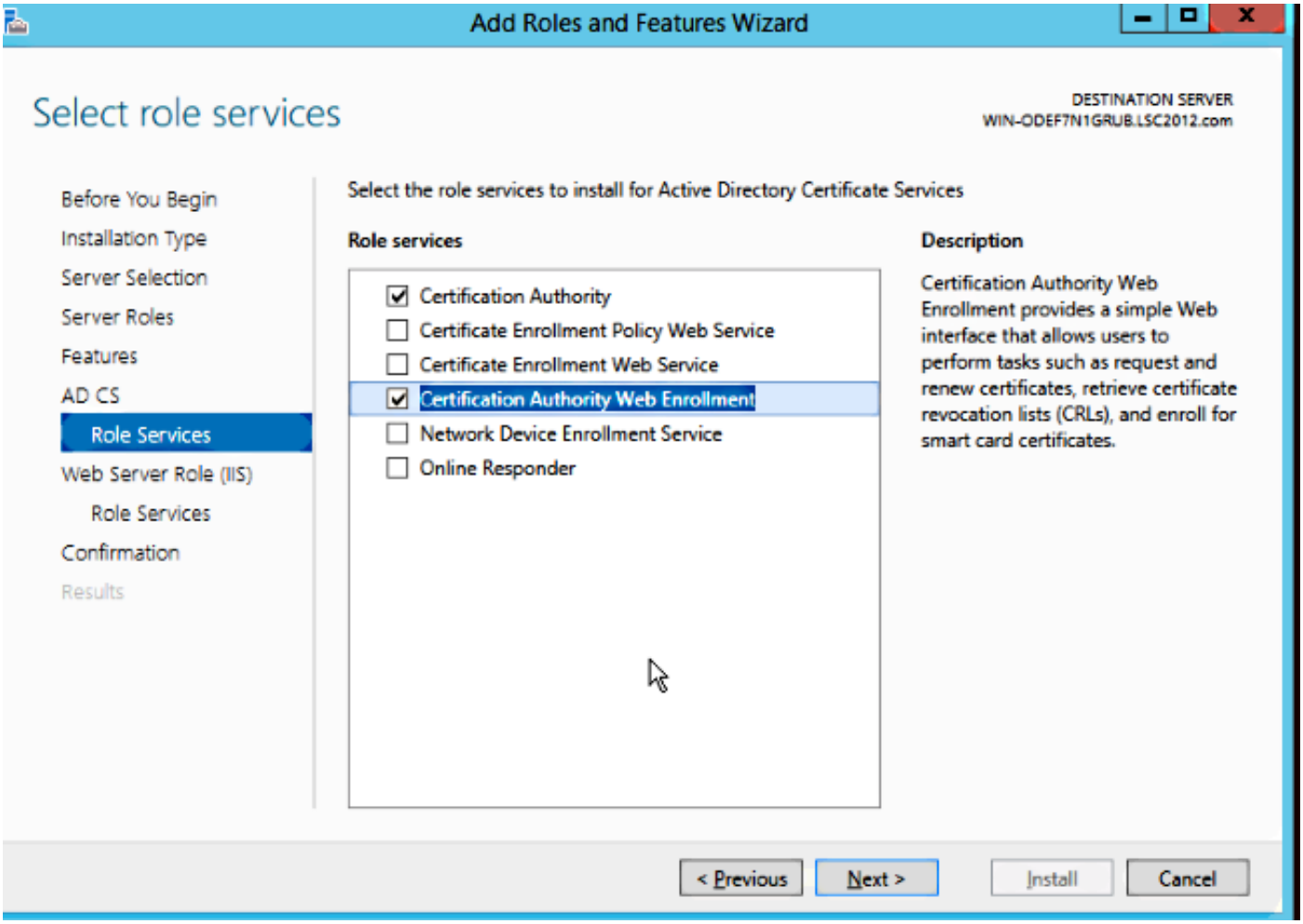


Stap 2. Na de installatie moet u de server naar de domeincontroller promoten.

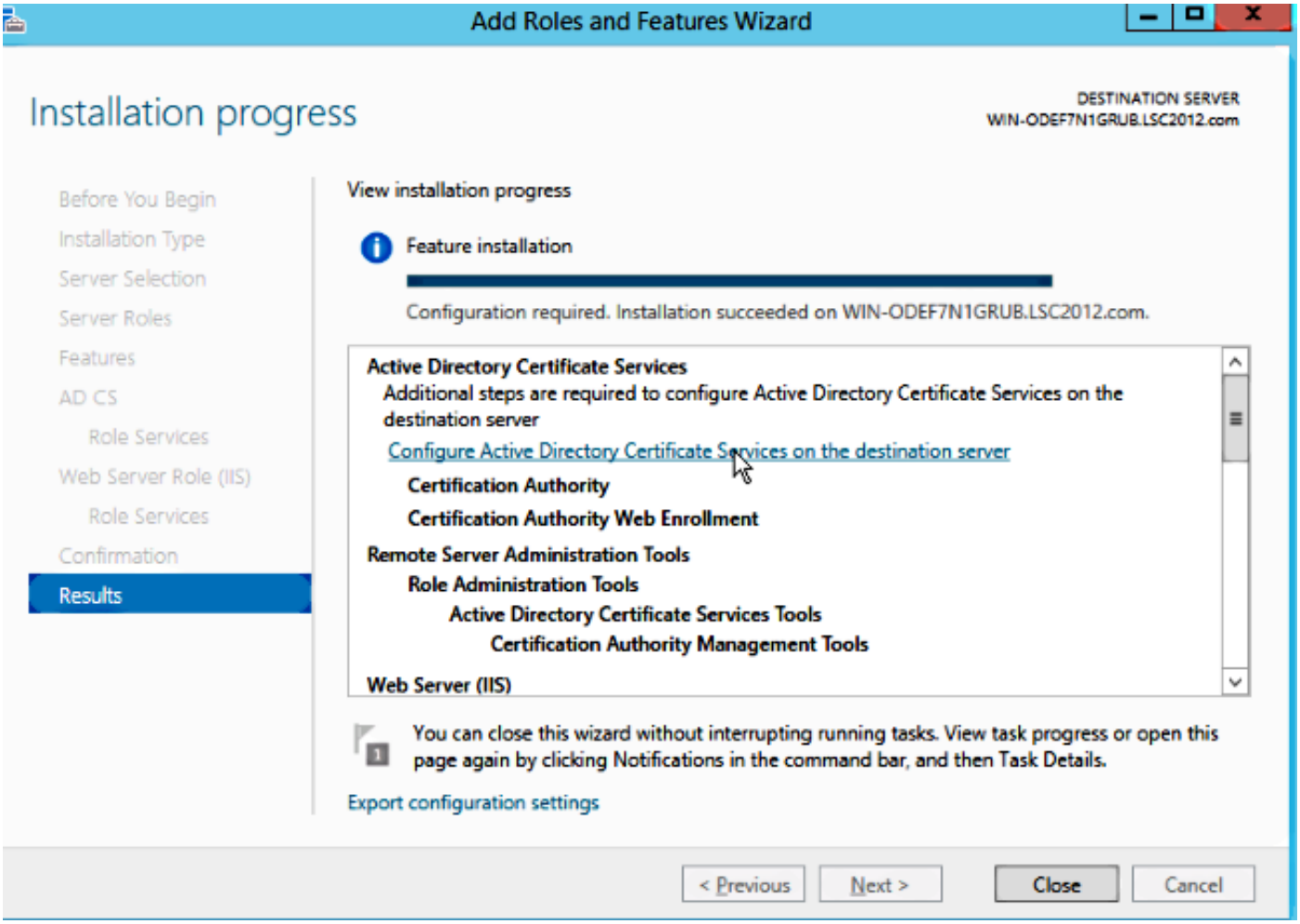


Stap 3. Aangezien dit een nieuwe instelling is, kunt u een nieuw bos configureren. maar meestal in bestaande implementaties, moet u deze punten gewoon op een domeincontroller configureren. Hier kiest u het **LSC2012.com-**domein. Hiermee wordt ook de DNS-functie (Domain Name Server) geactiveerd.

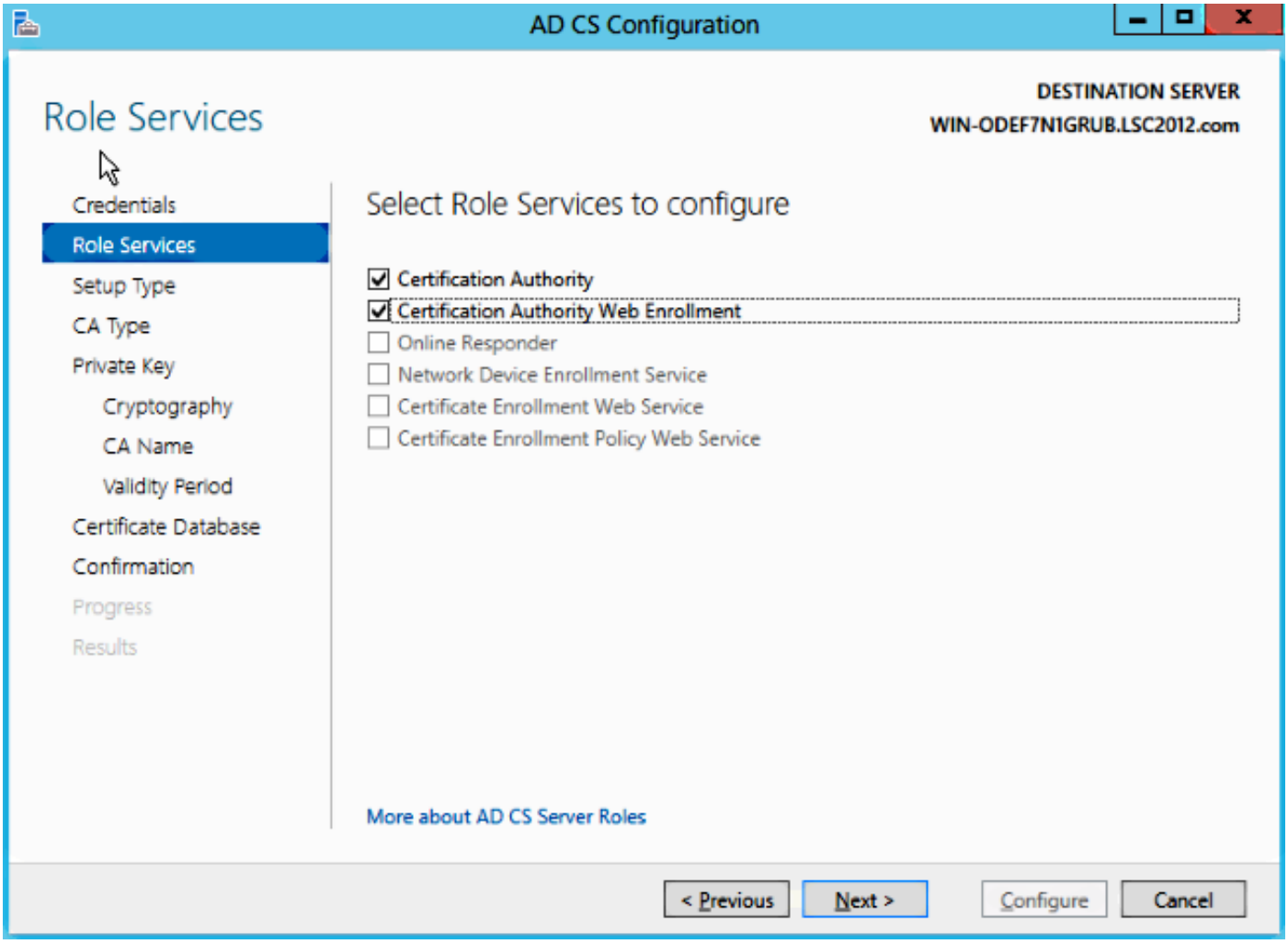
Stap 4. Nadat u het programma opnieuw hebt opgestart, installeert u zowel de certificaatdienst (CA) als de webinschrijving.



Stap 5. Configureer ze.



Stap 6. Kies Enterprise CA en laat alles standaard achter.

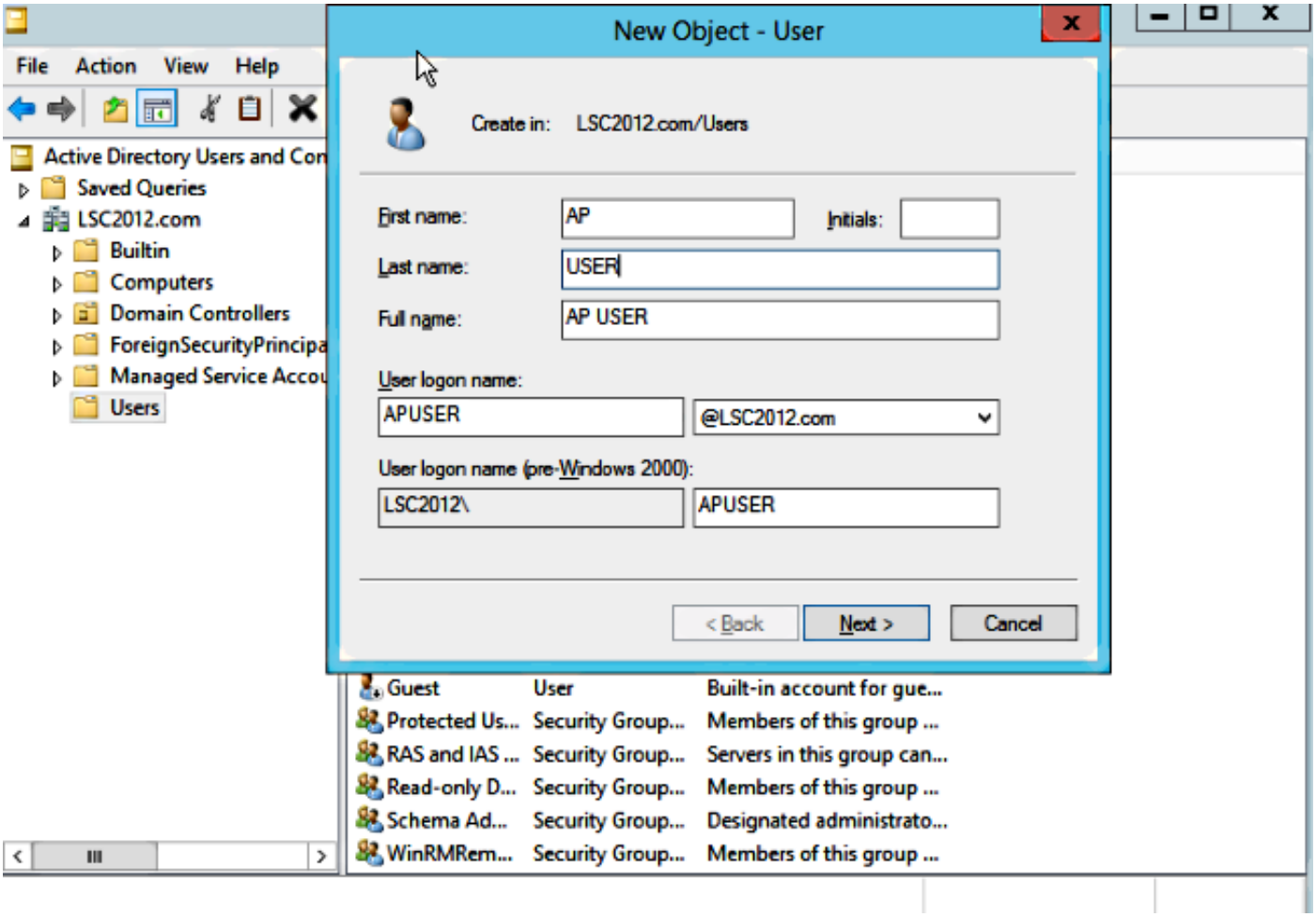


Stap 7. Klik op het **menu Microsoft Windows/Start**.

Stap 8. Klik op **Administratieve hulpmiddelen**.

Stap 9. Klik op **Active Directory Gebruikers en computers**.

Stap 10. Vouw het domein uit, klik met de rechtermuisknop op de **gebruikersmap** en kies **Nieuw object > Gebruiker**.



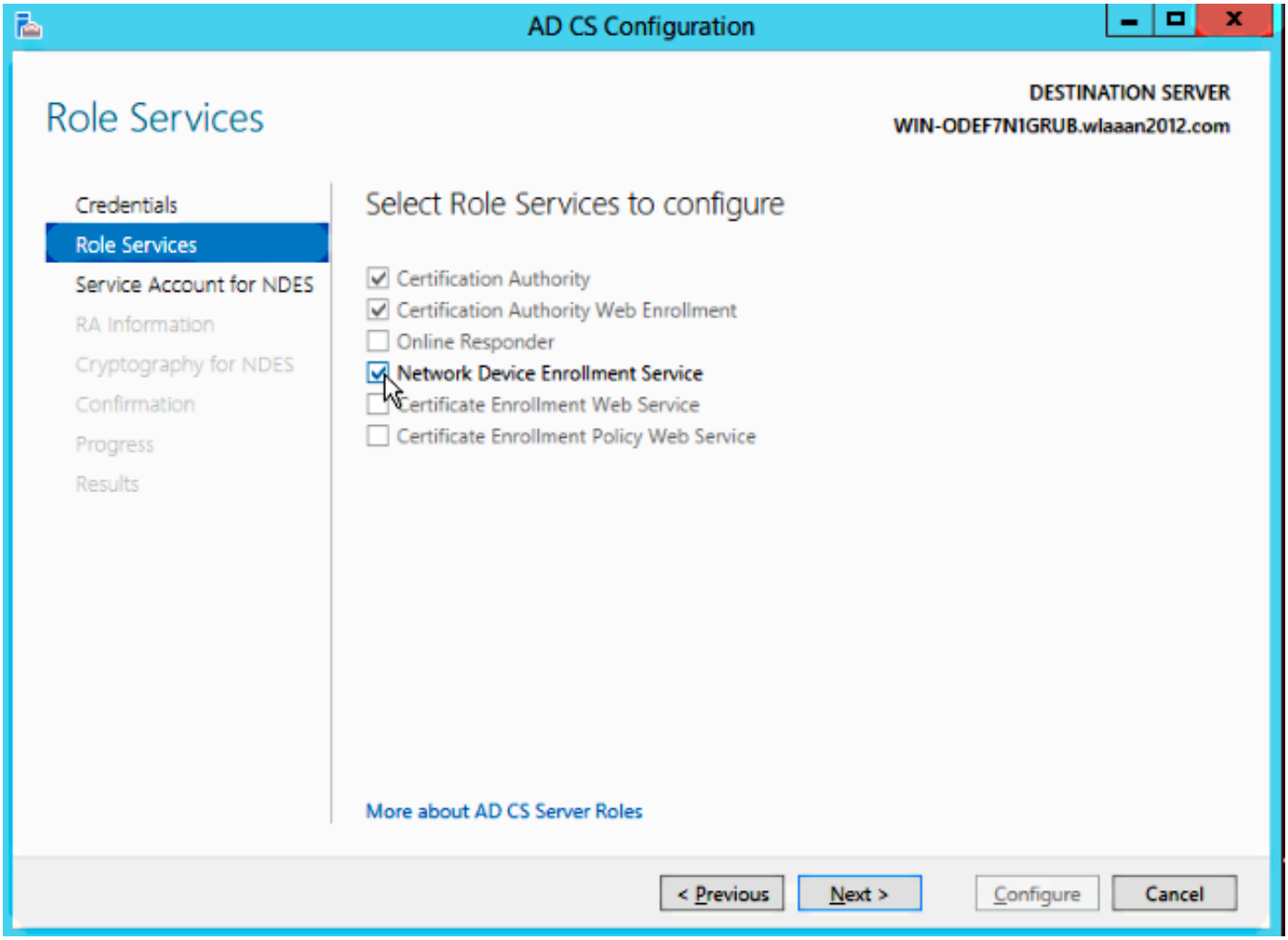
Stap 1. In dit voorbeeld wordt het **APUSER** genoemd. Als deze optie eenmaal is gemaakt, moet u de gebruiker bewerken en op het **tabblad LidOf** klikken, en er een lid van de groep IS_IUSRS van maken

De vereiste gebruikersrechten opdrachten zijn:

- Lokaal loggen toestaan

- Log in als service

Stap 12. Installeer de Inschrijvingsservice voor het netwerkapparaat (NDES).



- Kies het rekeninglid van de groep IS_USRS, **APUSER** in dit voorbeeld, als de servicekening voor NDES.

Stap 13. Navigeer naar administratieve hulpmiddelen.

Stap 14. Klik op **Internet Information Services (IS)**.

Stap 15. Uitbreidt de **server > Sites > Standaardwebsite > Cert Srv**.

Stap 16. Klik voor zowel **mscep** als **mscep_admin** op **verificatie**. Zorg ervoor dat anonieme verificatie is ingeschakeld.

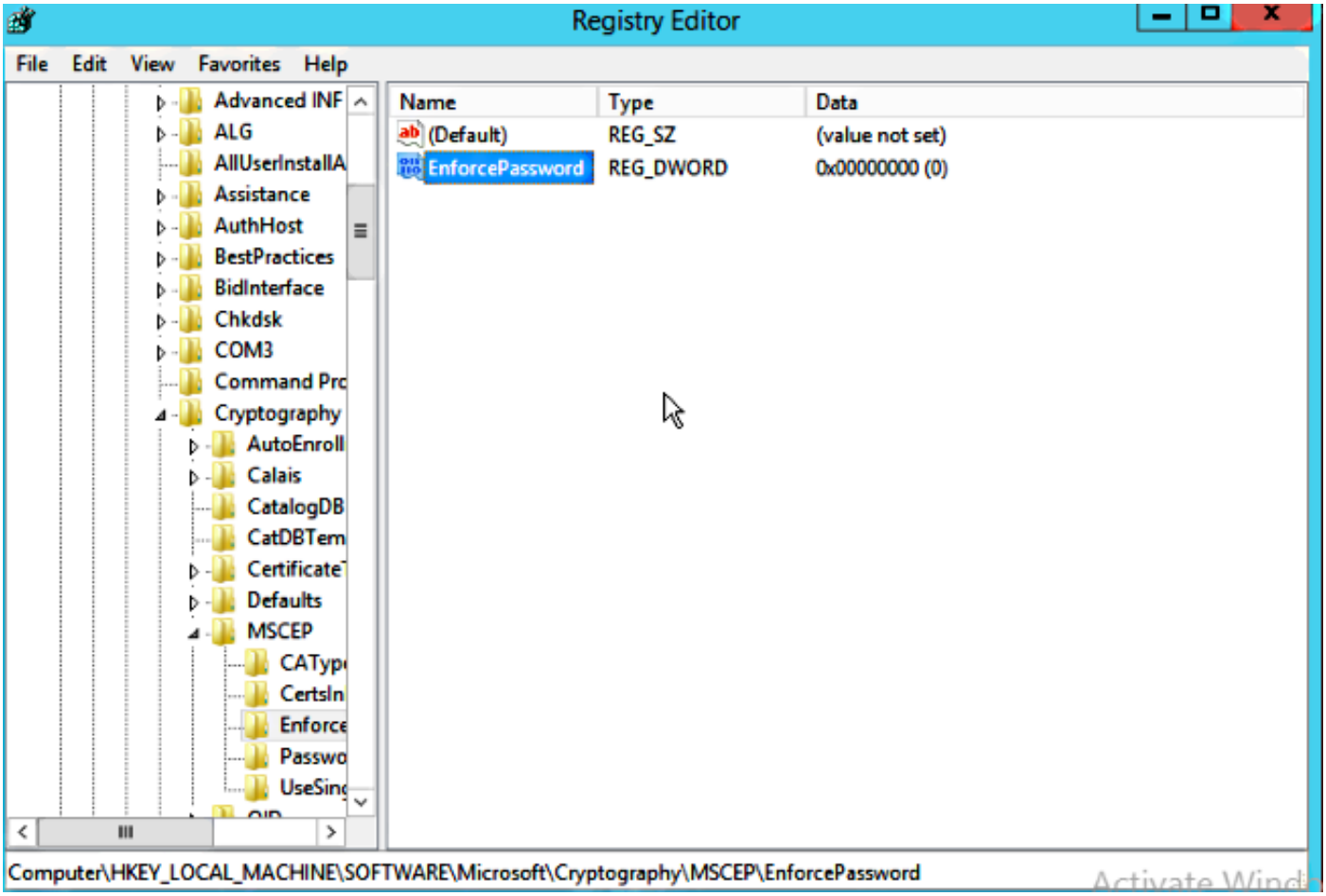
Stap 17. Klik met de rechtermuisknop op **Windows-verificatie** en kies **providers**. Zorg ervoor dat NT LAN Manager (NTLM) eerst in de lijst staat.

Stap 18. Schakel de authenticatie-uitdaging uit in de registerinstellingen, anders verwacht Simple certificaatinschrijving Protocol (SCEP) dat de WLC-versie niet ondersteunt.

Stap 19. Open de **toepassing**.

Stap 20. Ga naar **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP**.

Stap 21. Stel het wachtwoord in op **0**.



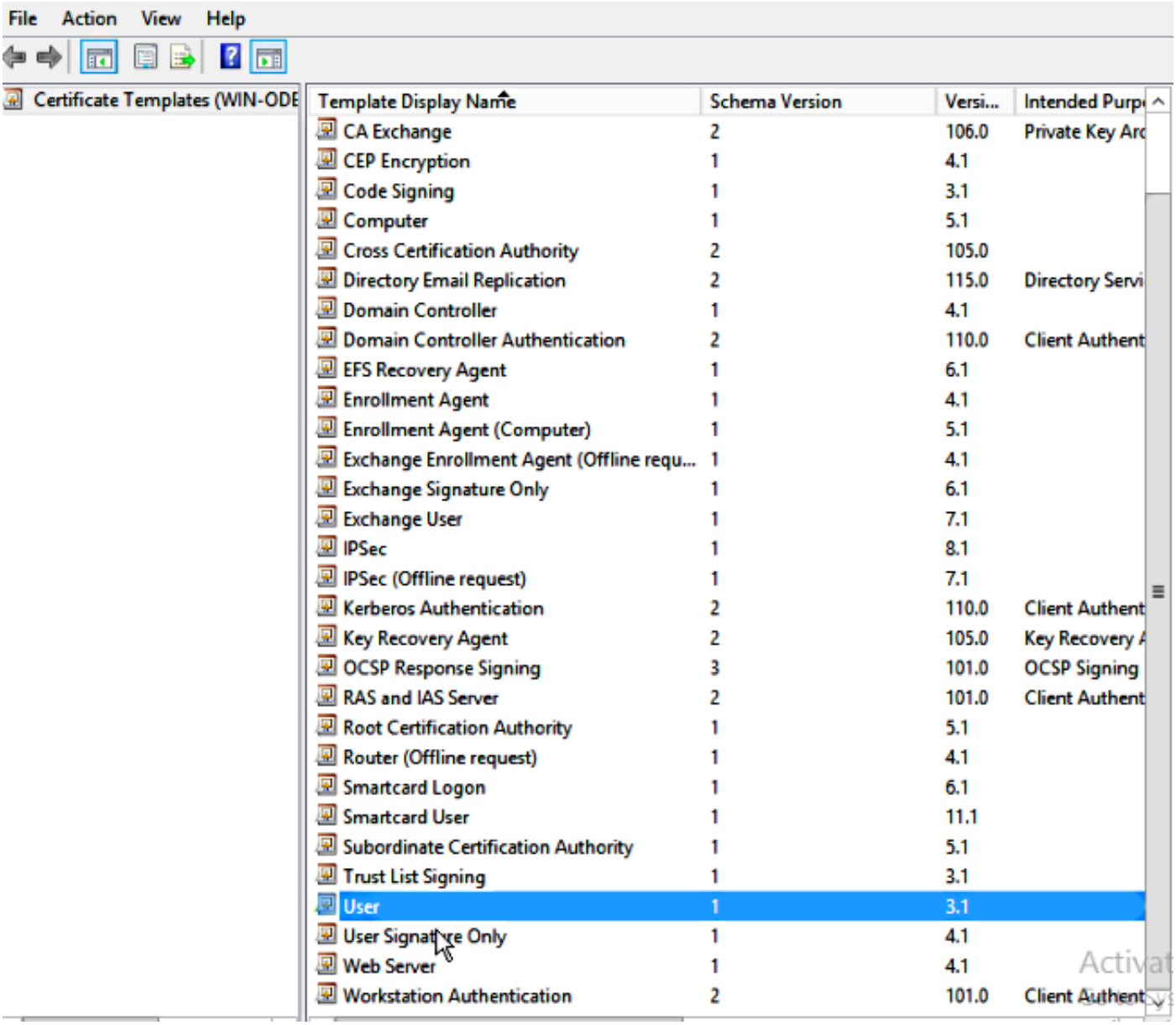
Stap 2. Klik op het **menu Microsoft Windows/Start**.

Stap 23. Type **MMC**.

Stap 2. Kies in het menu Bestand de optie **Magnetisch toevoegen/verwijderen**. Kies **certificeringsinstantie**.

Stap 25. Klik met de rechtermuisknop op de **map certificaatsjabloon** en klik op **beheren**.

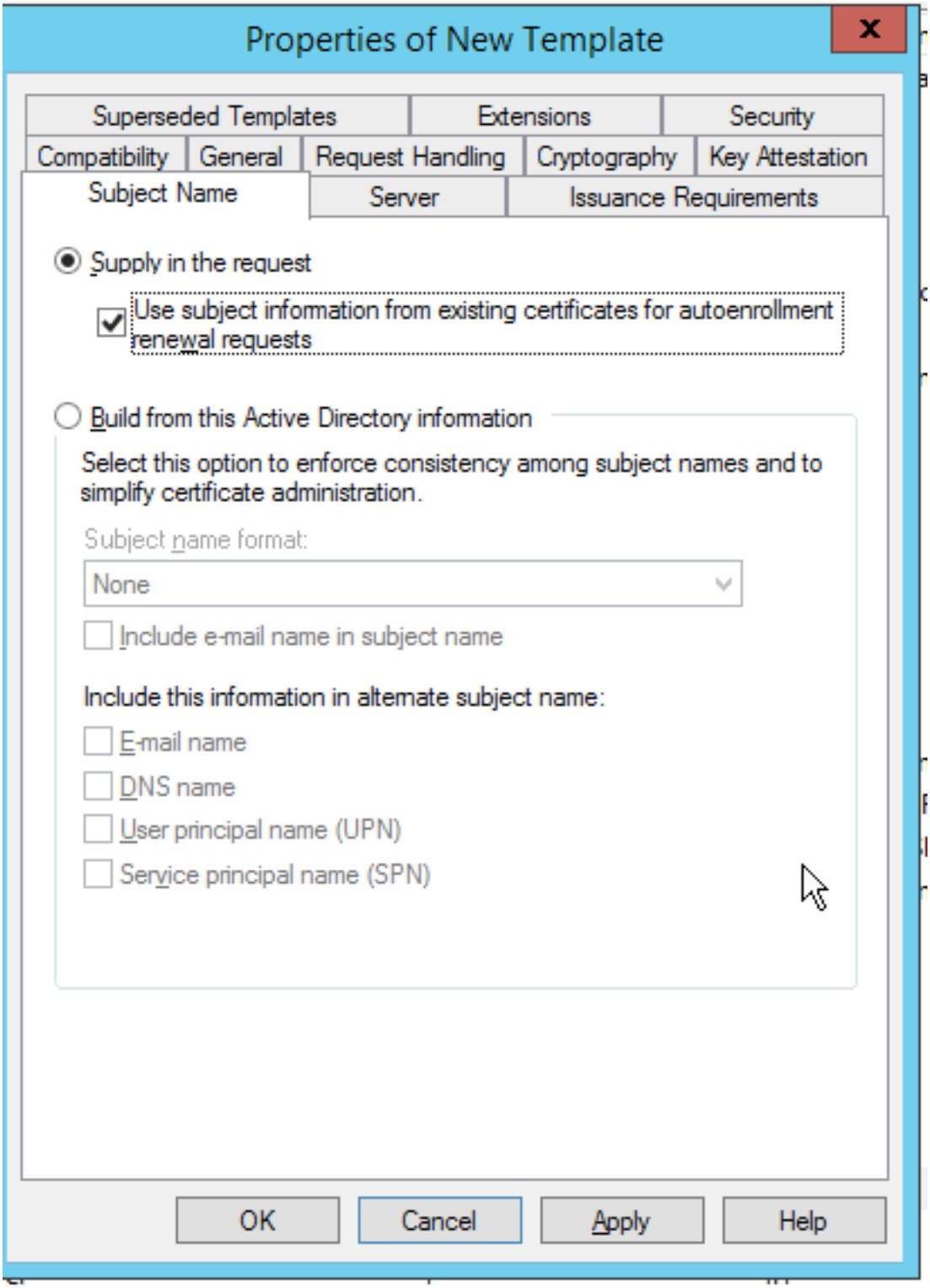
Stap 2. Klik met de rechtermuisknop op een bestaande sjabloon zoals Gebruiker en kies **Dubbele sjabloon**.



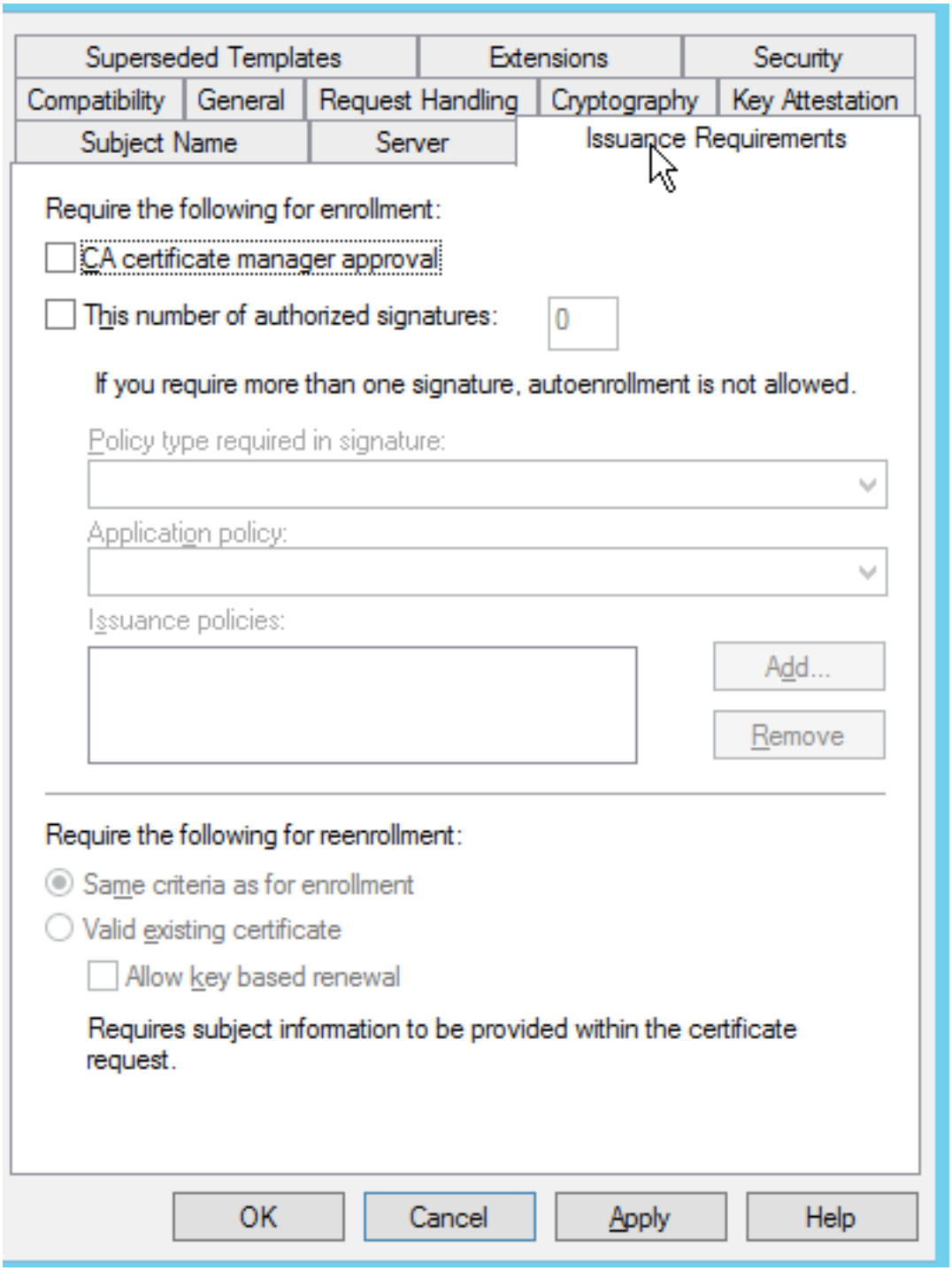
Stap 27. Kies de CA om Microsoft Windows 2012 R2 te zijn.

Stap 28. Voeg in het tabblad Algemeen een weergavenaam toe, zoals WLC, en een validatieperiode.

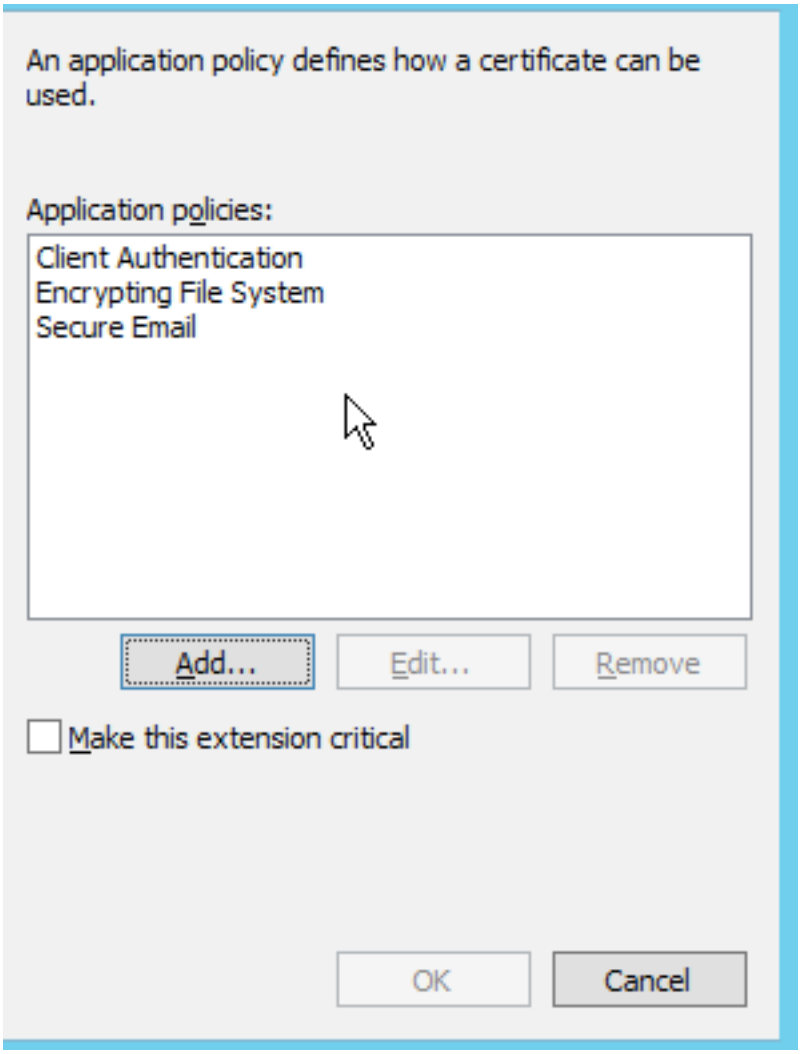
Stap 29. Bevestig in het tabblad Onderwerp dat **Levering in het verzoek** is geselecteerd.



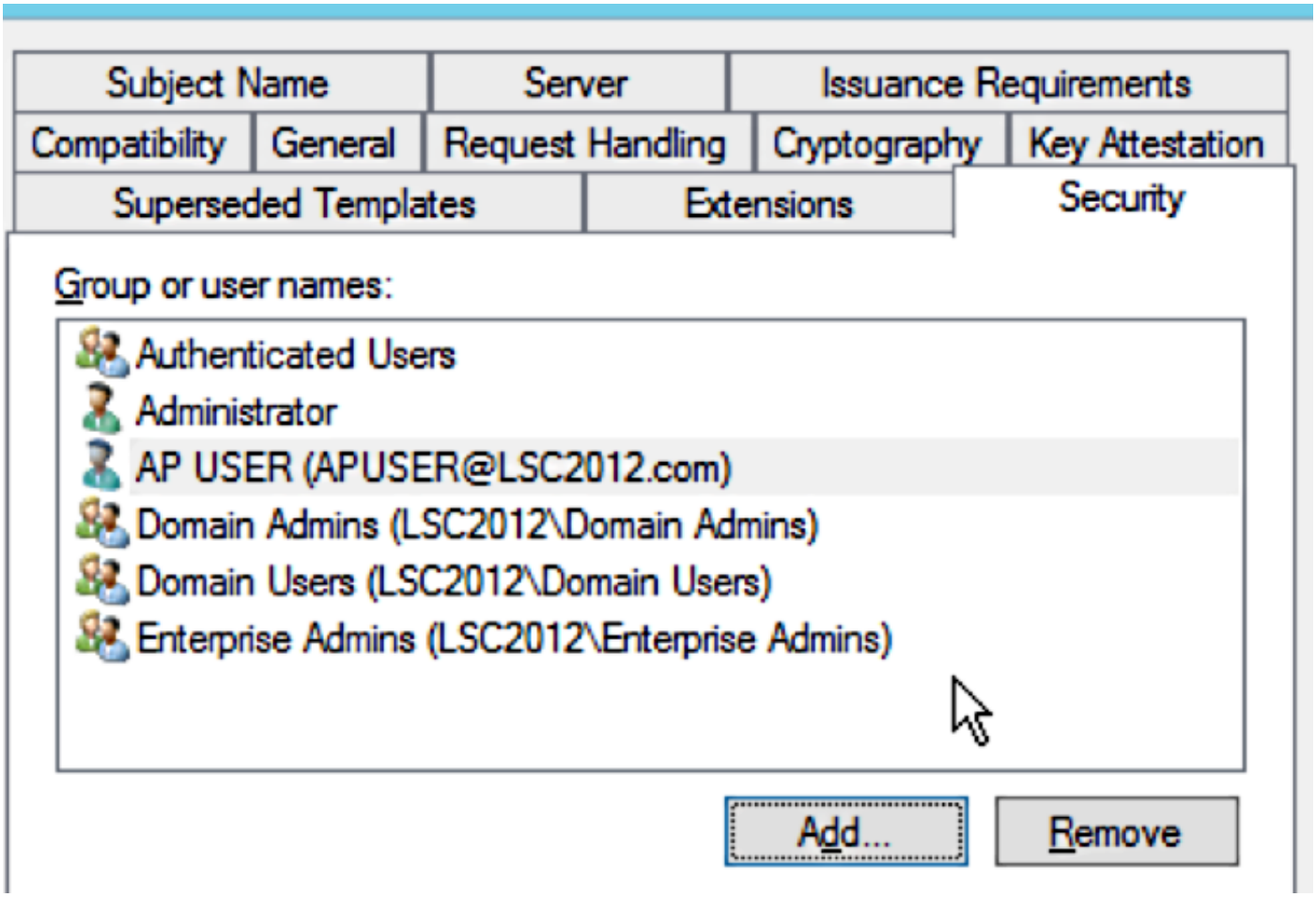
Stap 30. Klik op het tabblad **Eisen** voor **uitgifte**. Cisco raadt aan om uitgiftebeleid leeg te laten in een typische hiërarchische CA-omgeving:



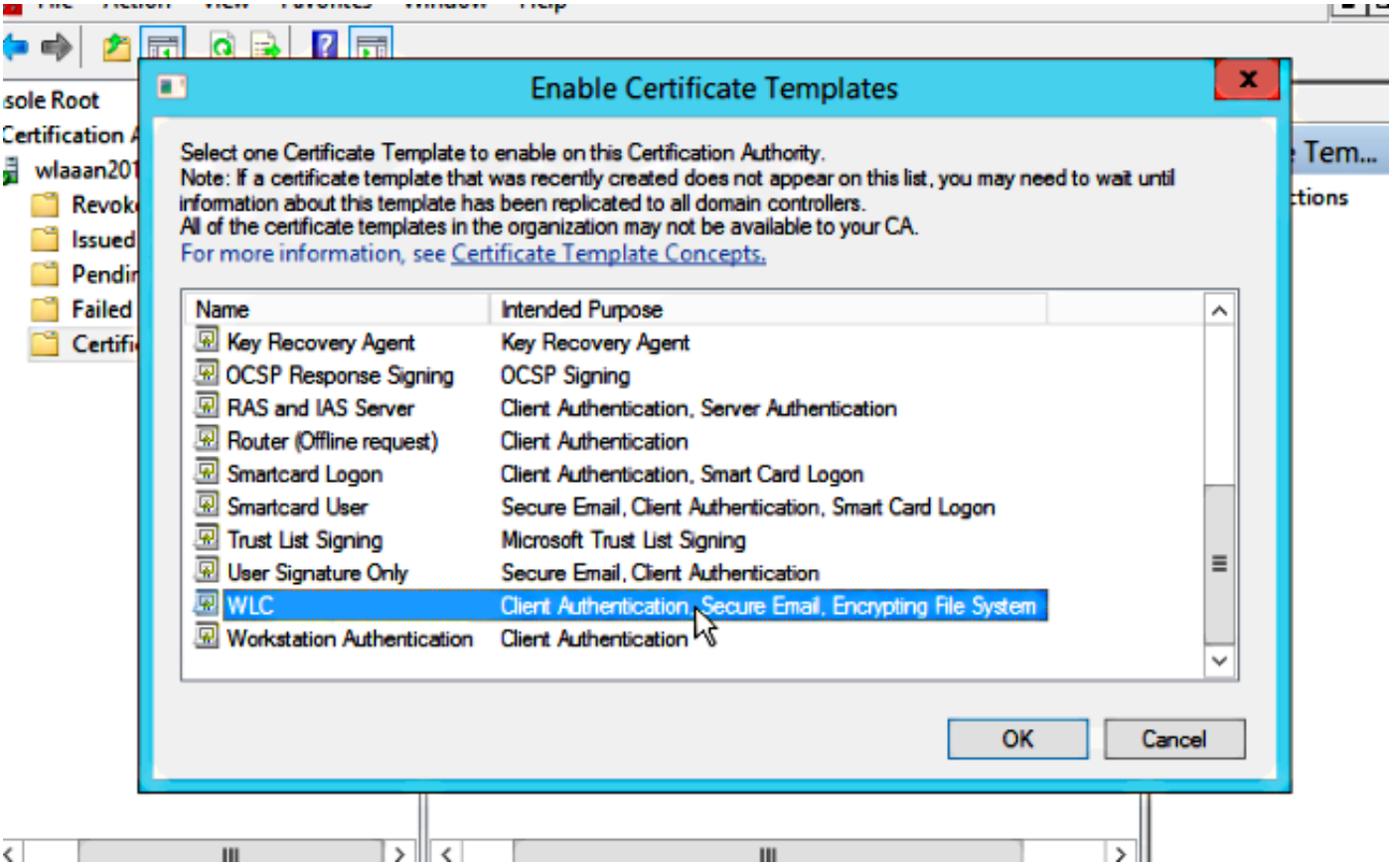
Stap 3 1. Klik op het **tabblad Uitbreidingen**, **Toepassingsbeleid** en **Bewerk**. Klik op **Add** en controleer of clientverificatie wordt toegevoegd als toepassingsbeleid. Klik op **OK**.



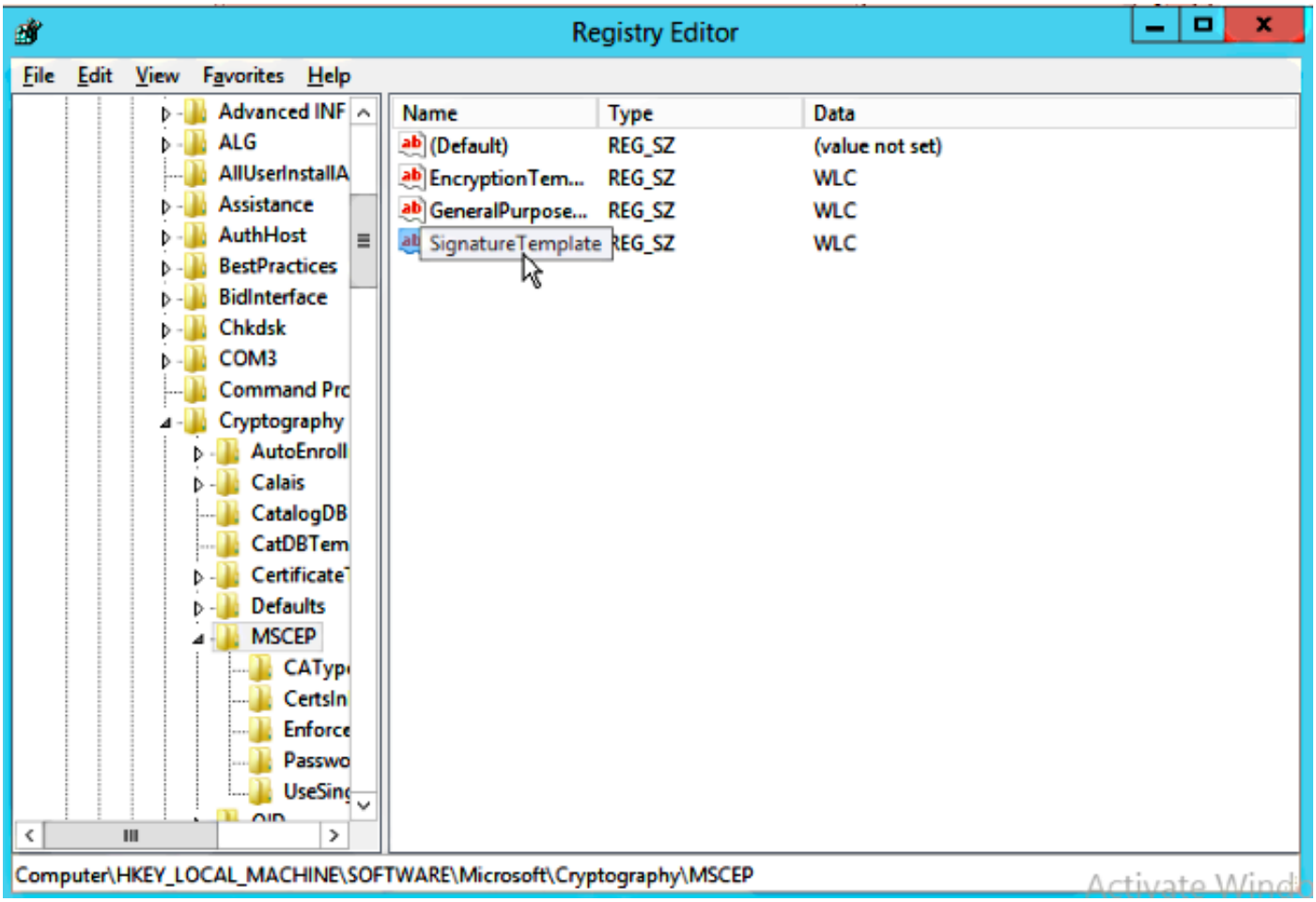
Stap 3 2. Klik op het **tabblad Beveiliging** en vervolgens op **Toevoegen...**. Zorg ervoor dat de SCEP-servicekaart die in de NDES-servicesinstallatie is gedefinieerd, de volledige controle over de sjabloon heeft en klik op **OK**.



Stap 3. Ga terug naar de GUI-interface van de certificeringsinstantie. Klik met de rechtermuisknop op de **map certificaatsjablonen**. Navigeer naar **Nieuw > certificaatsjabloon om uit te geven**. Selecteer de eerder ingesteld WLC-sjabloon en klik op **OK.**



Stap 34. Verander de standaard SCEP-sjabloon in de registratiesystemen onder **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptografie > MSCEP**. Verander de toetsen EncryptionSjabloon, GeneralPurposeSjabloon en SignatureSjabloon van IPsec (Offline aanvraag) naar de eerder gemaakte WLC-sjabloon.



Stap 35. Herstart het systeem.

De WLC configureren

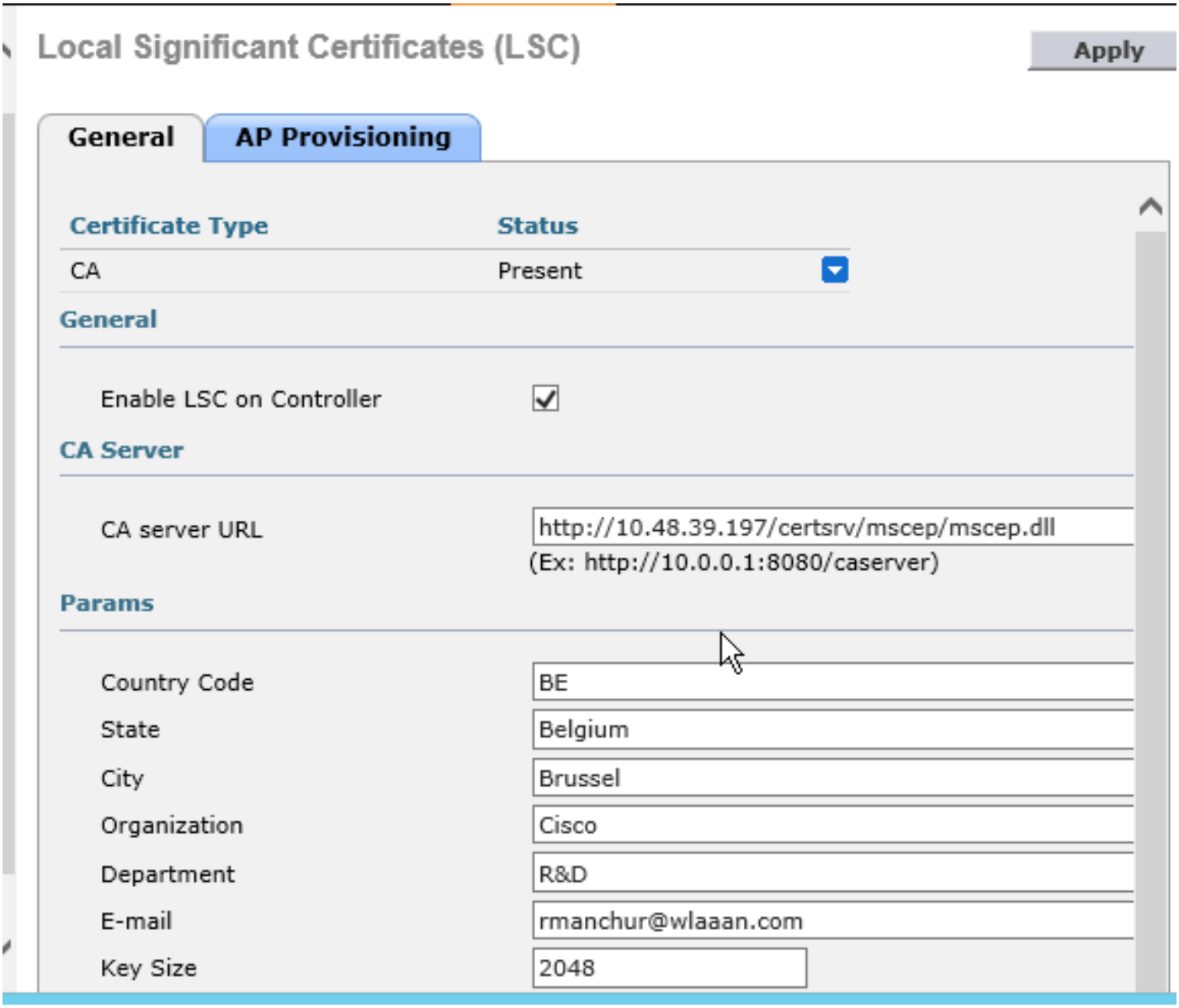
Stap 1. Navigeer in het menu Beveiliging op de WLC. Klik op **Certificaten > LSC**.

Stap 2. Controleer het selectieknop **LSC inschakelen op controller**.

Stap 3. Voer uw Microsoft Windows Server 2012 URL in. Standaard wordt deze toegevoegd aan **/certsrv/mscep/mscep.dll**.

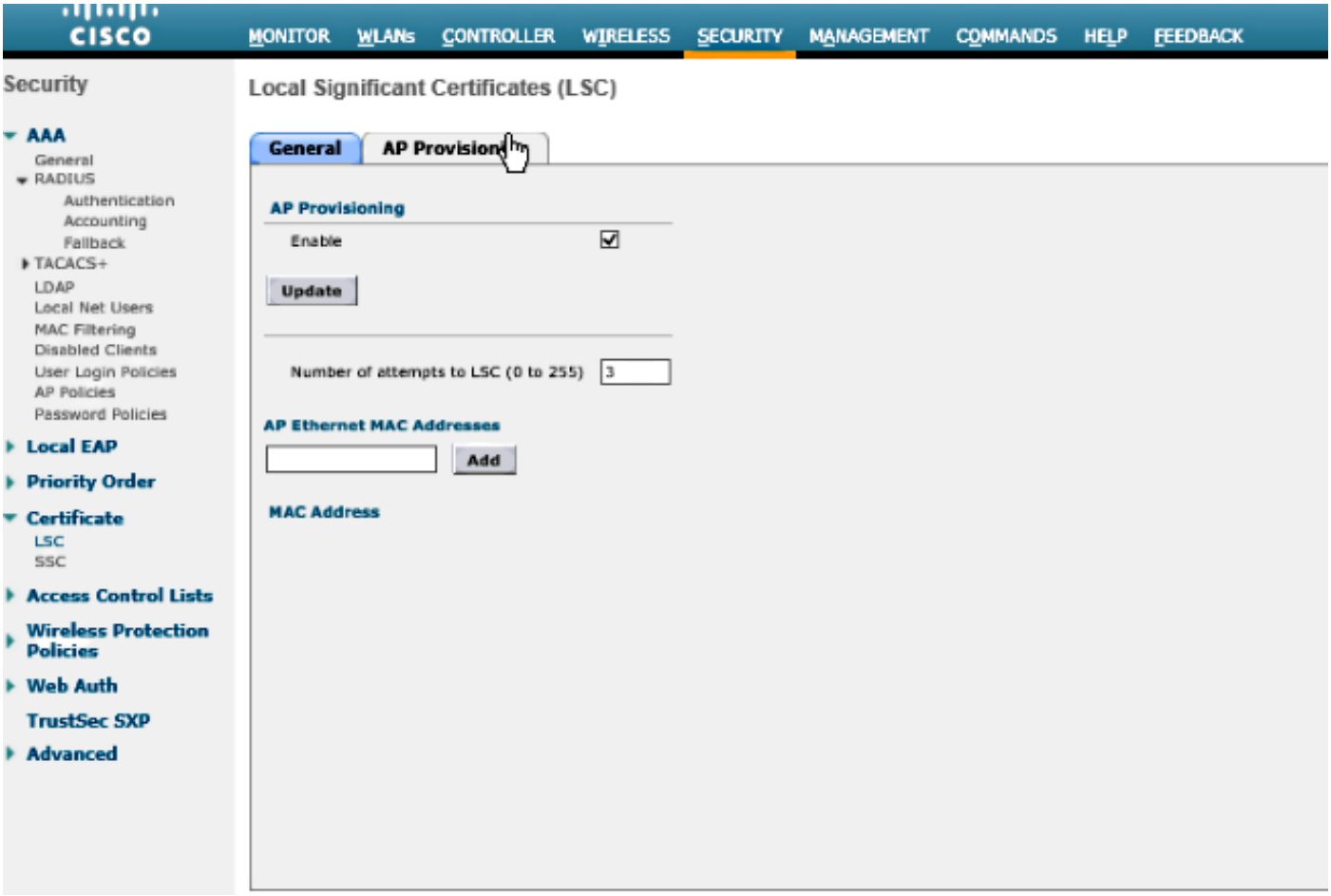
Stap 4. Voer uw gegevens in het gedeelte **Params** in.

Stap 5. Pas de wijziging toe.



Stap 6. Klik op de blauwe pijl op de bovenste CA-lijn en kies **Add**. Het moet de status veranderen van **niet aanwezig** naar **nu**.

Stap 7. Klik op het **tabblad AP-provisioning**.



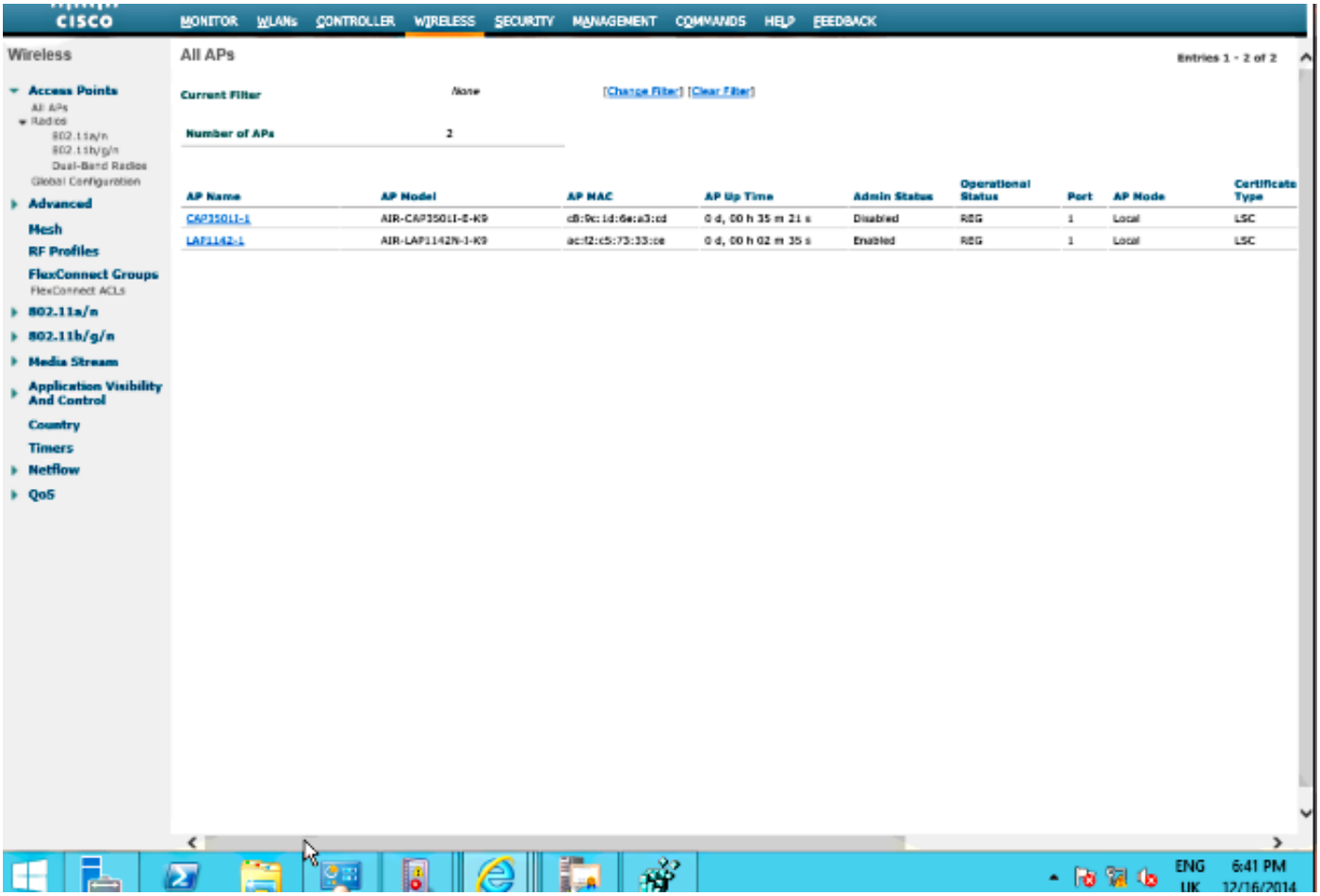
Stap 8. Controleer het selectieteken **Enable** onder AP Provisioning en klik op **Update**.

Stap 9. Herstart uw toegangspunten als ze niet zelf zijn herstart.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het toegangspunt, na het opnieuw opstarten, sluit zich aan bij en toont met LSC als het certificaattype in het menu Draadloos.



Opmerking: Na 8.3.112 kunnen MIC APs zich niet bij allen aansluiten wanneer LSC wordt ingeschakeld. Daarom wordt de optie "pogingen tot LSC" tellen beperkt gebruikt.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.