# Konfigurationsbeispiel für LSC (Locally Significant Certificates) mit WLC und Windows Server 2012

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie Sie Locally Significant Certificates (LSC) mit einem Wireless LAN Controller (WLC) und einem neu installierten Microsoft Windows Server 2012 R2 konfigurieren.

> **Hinweis**: Die tatsächlichen Bereitstellungen können sich in vielen Punkten unterscheiden, und Sie sollten über vollständige Kontrolle und Kenntnisse der Einstellungen in Microsoft Windows Server 2012 verfügen. Dieses Konfigurationsbeispiel wird nur als Referenzvorlage für Cisco Kunden bereitgestellt, um ihre Microsoft Windows Server-Konfiguration zu implementieren und anzupassen, damit LSC funktioniert.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie alle Änderungen in Microsoft Windows Server verstehen und ggf. die entsprechende Microsoft-Dokumentation überprüfen.

> **Hinweis**: LSC auf dem WLC wird nicht von einer intermediären CA unterstützt, da die Root-CA vom WLC nicht unterstützt wird, da der Controller nur die mittlere CA empfängt.

### Verwendete Komponenten

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

- WLC-Version 7.6
- Microsoft Windows Server 2012 R2

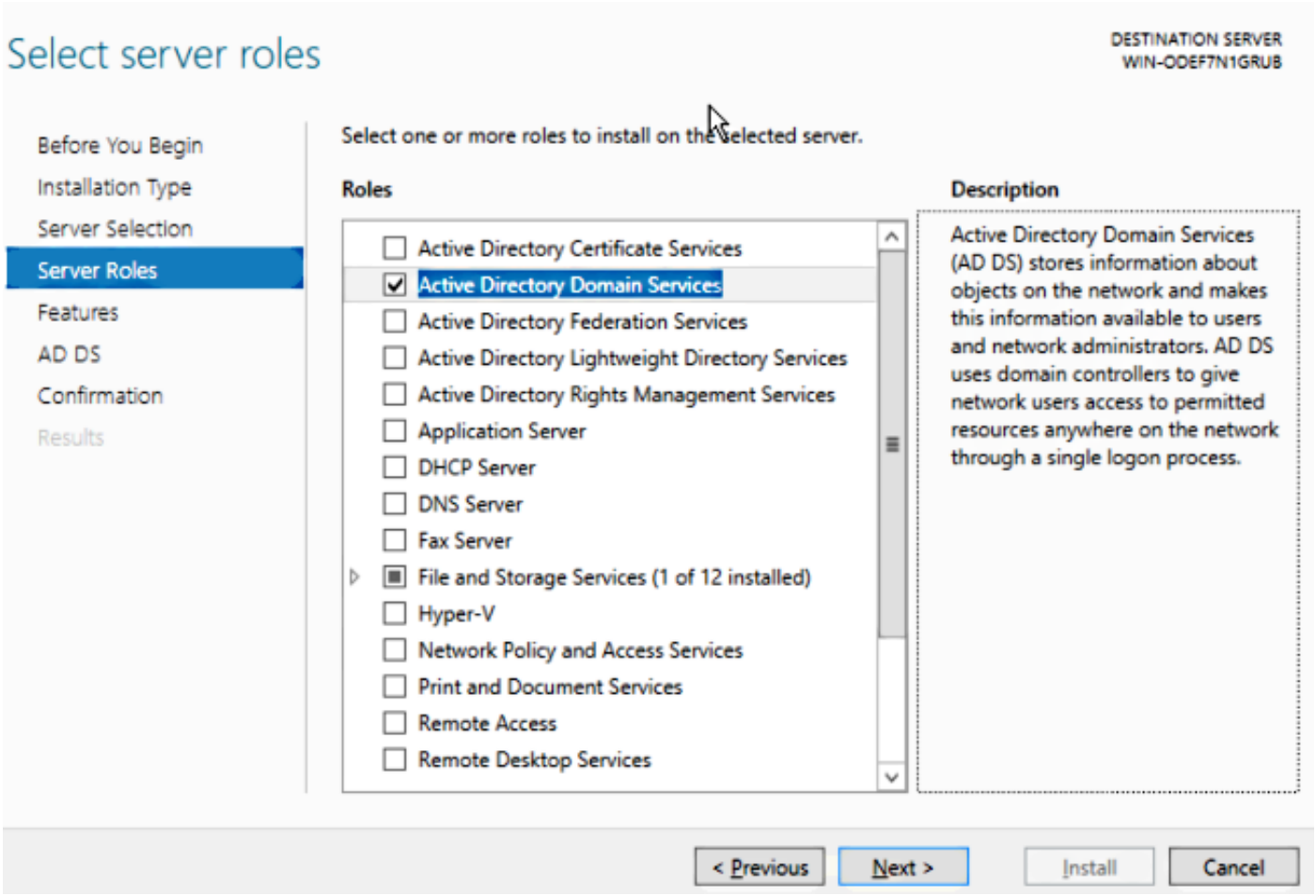
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Konfigurieren

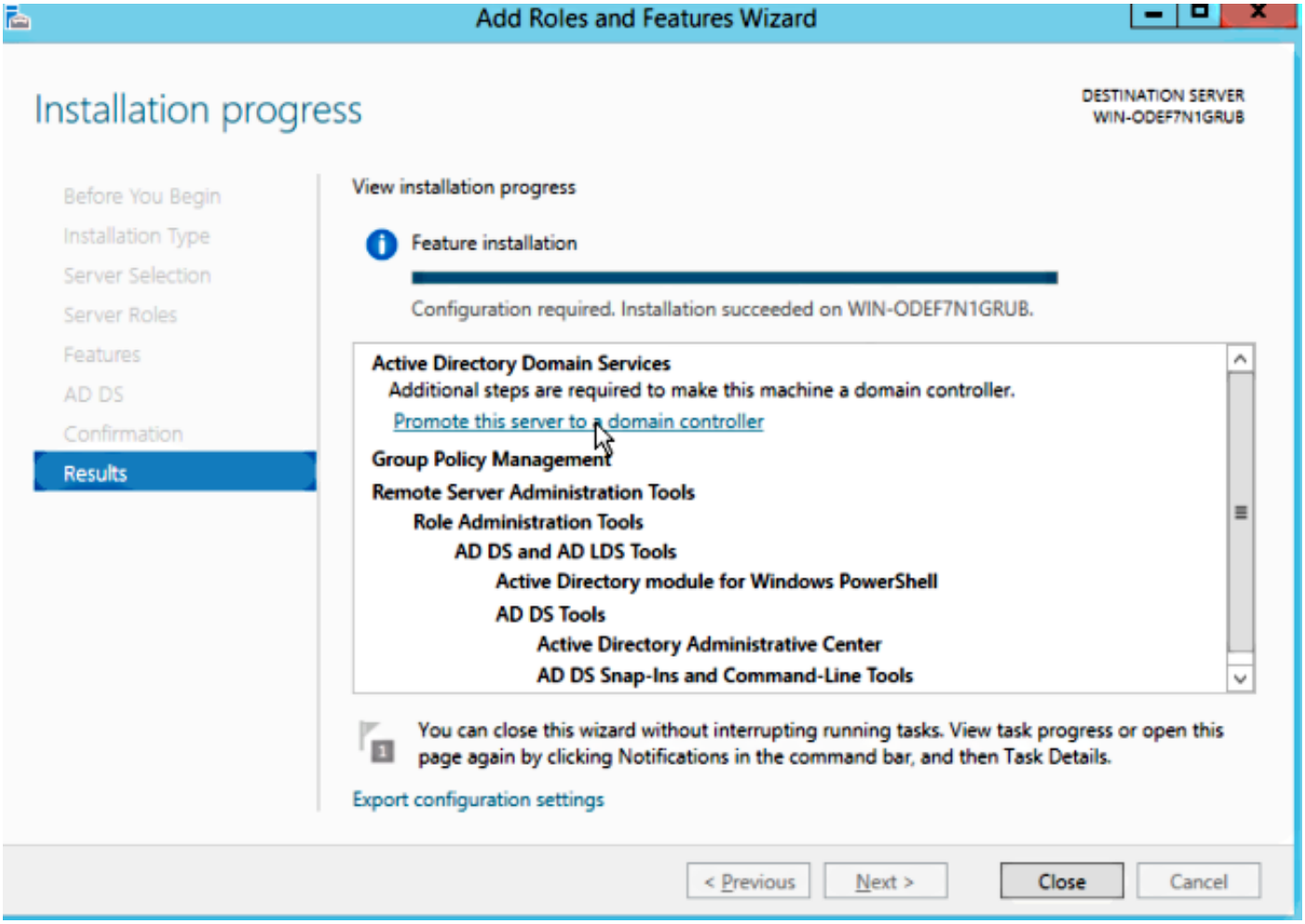
## Microsoft Windows Server-Konfiguration

Diese Konfiguration wird als mit einem neu installierten Microsoft Windows Server 2012 ausgeführt angezeigt. Sie müssen die Schritte an Ihre Domäne und Ihre Konfiguration anpassen.

**Schritt 1:** Active Directory-Domänendienste für den Assistenten für Rollen und Funktionen installieren.

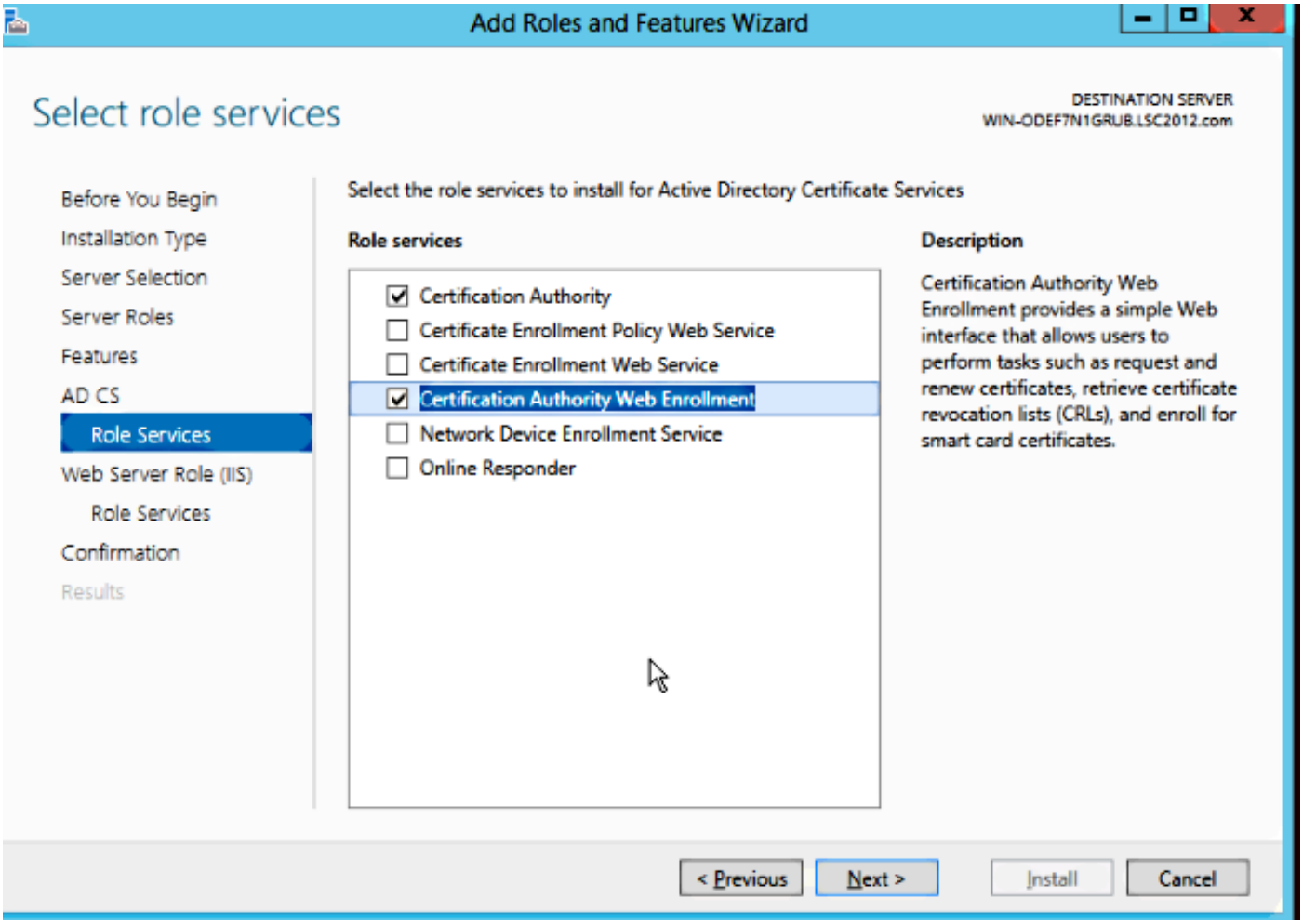



**Schritt 2.** Nach der Installation müssen Sie den Server für den Domänen-Controller bewerben.

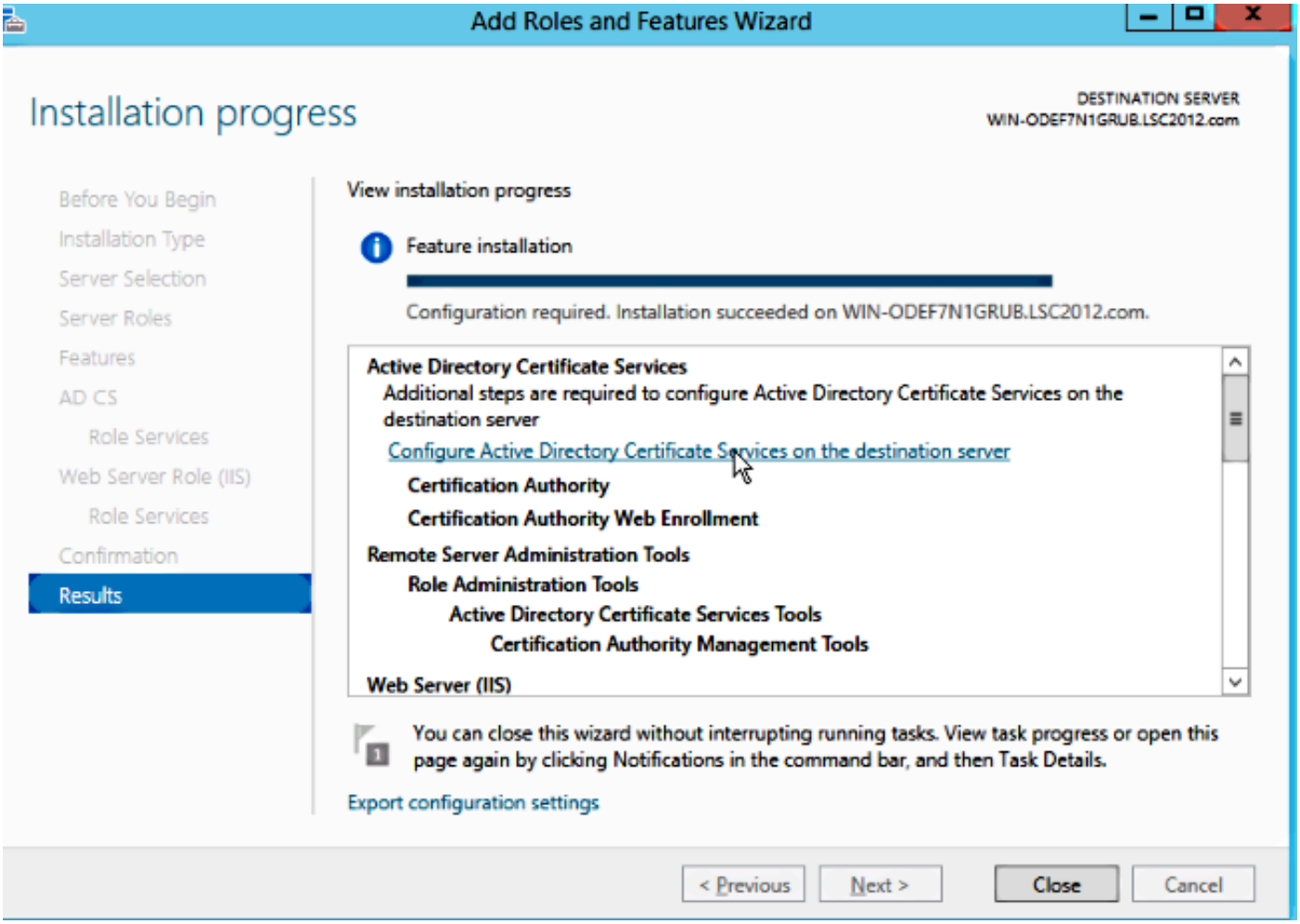



**Schritt 3:** Da es sich um eine neue Konfiguration handelt, konfigurieren Sie einen neuen Wald. konfigurieren Sie diese Punkte jedoch in der Regel in vorhandenen Bereitstellungen einfach auf einem Domänencontroller. Wählen Sie hier die Domäne **LSC2012.com** aus. Dadurch wird auch die Funktion Domain Name Server (DNS) aktiviert.

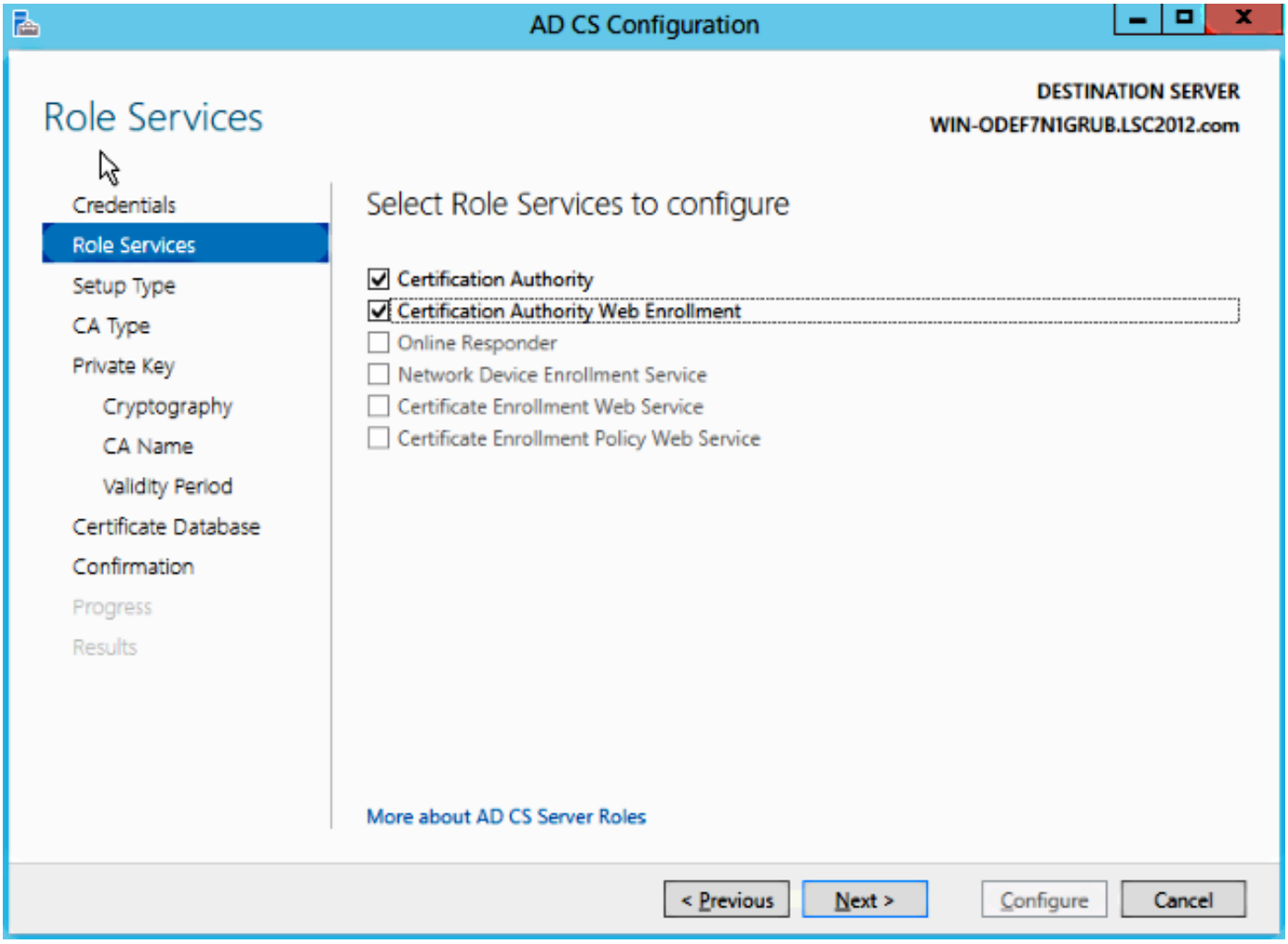
**Schritt 4:** Installieren Sie nach einem Neustart den Service Certificate Authority (CA) sowie die Webregistrierung.




**Schritt 5.** Konfigurieren Sie sie.




**Schritt 6:** Wählen Sie Enterprise CA aus, und belassen Sie alle Standardeinstellungen.

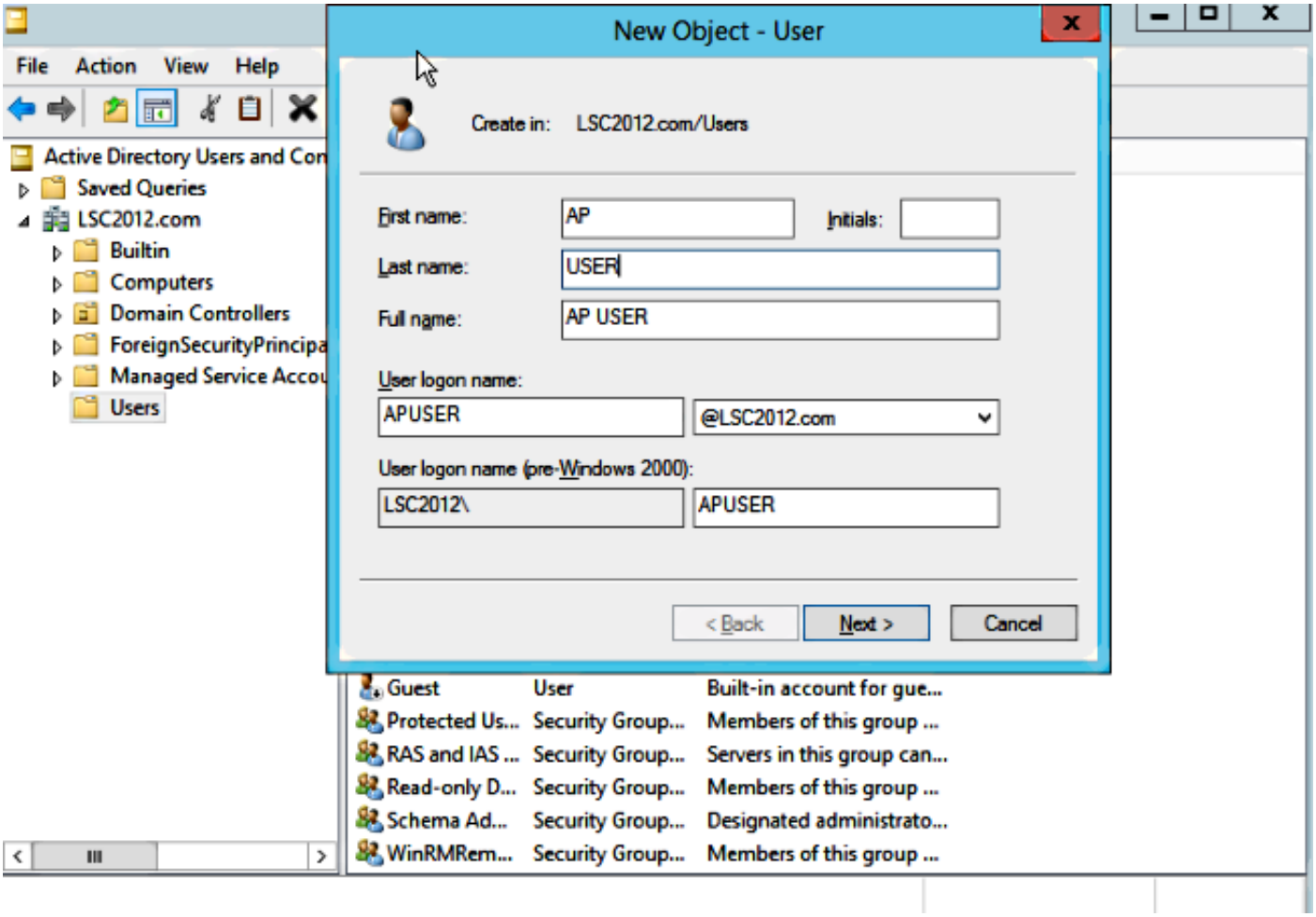



**Schritt 7:** Klicken Sie auf das **Menü Microsoft Windows/Start**.

**Schritt 8:** Klicken Sie auf **Verwaltung**.

**Schritt 9:** Klicken Sie auf **Active Directory-Benutzer und -Computer**.

**Schritt 10:** Erweitern Sie die Domäne, klicken Sie mit der rechten Maustaste auf den **Ordner Benutzer**, und wählen Sie **Neues Objekt > Benutzer aus**.



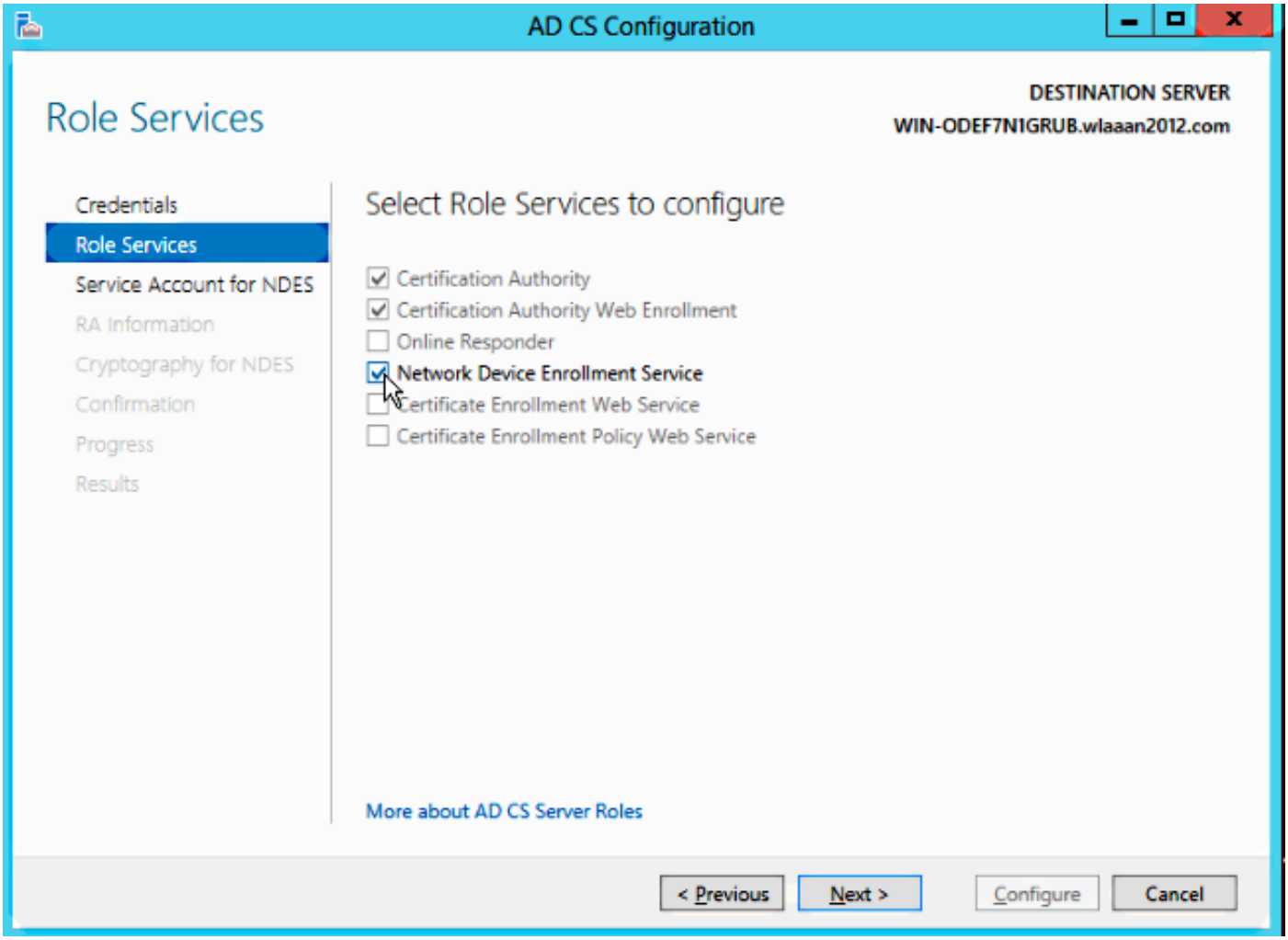

**Schritt 11:** In diesem Beispiel wird es **APUSER** genannt. Nach der Erstellung müssen Sie den Benutzer bearbeiten und auf die **Registerkarte MemberOf** klicken, um ihn zur Gruppe IIS_IUSRS zu machen.

**Die erforderlichen Zuweisungen für Benutzerrechte sind:**

- Lokale Anmeldung zulassen

- Melden Sie sich als Service an.

**Schritt 12:** Installieren Sie den Network Device Enrollment Service (NDES).




- Wählen Sie den Kontomember der Gruppe IIS_USRS, **APUSER** in diesem Beispiel, als Dienstkonto für NDES aus.

**Schritt 13:** Navigieren Sie zu Verwaltung.

**Schritt 14:** Klicken Sie auf **Internetinformationsdienste (IIS)**.

**Schritt 15:** Erweitern Sie **Server > Sites > Default website > Cert Srv**.

**Schritt 16:** Klicken Sie für **mscep** und **mscep_admin** auf **Authentifizierung**. Stellen Sie sicher, dass die anonyme Authentifizierung aktiviert ist.

**Schritt 17:** Klicken Sie mit der rechten Maustaste auf **Windows-Authentifizierung**, und wählen Sie **Provider (Anbieter)** aus. Stellen Sie sicher, dass NT LAN Manager (NTLM) der erste in der Liste ist.

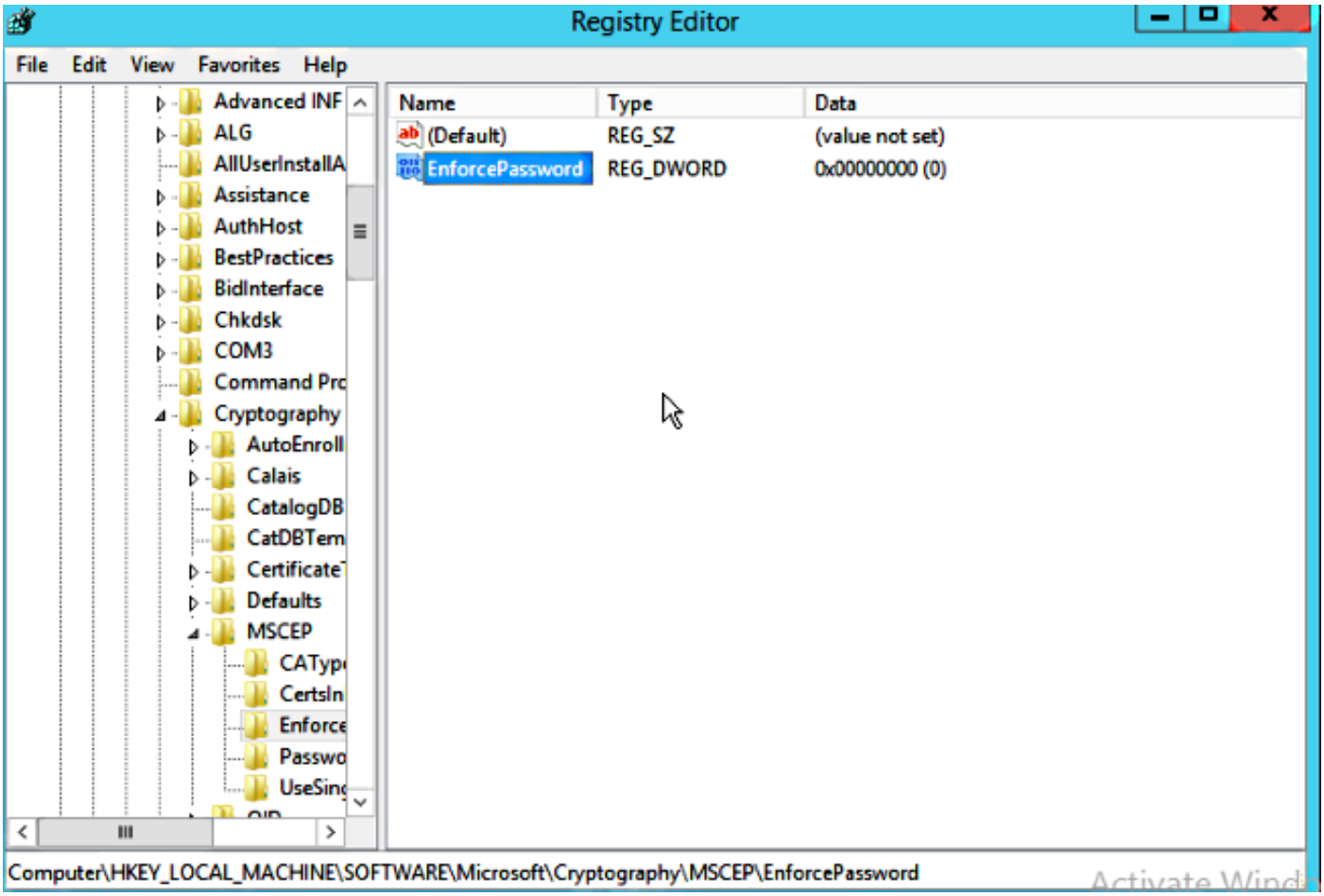
**Schritt 18:** Deaktivieren Sie die Authentifizierungsproblematik in den Registrierungseinstellungen.

Andernfalls erwartet Simple Certificate Enrollment Protocol (SCEP) eine Kennwortauthentifizierung, die vom WLC nicht unterstützt wird.

**Schritt 19:** Öffnen Sie die **Anwendung regedit**.

**Schritt 20:** Besuchen Sie **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP**.

**Schritt 21:** Legen Sie EnforcePassword auf **0 fest**.



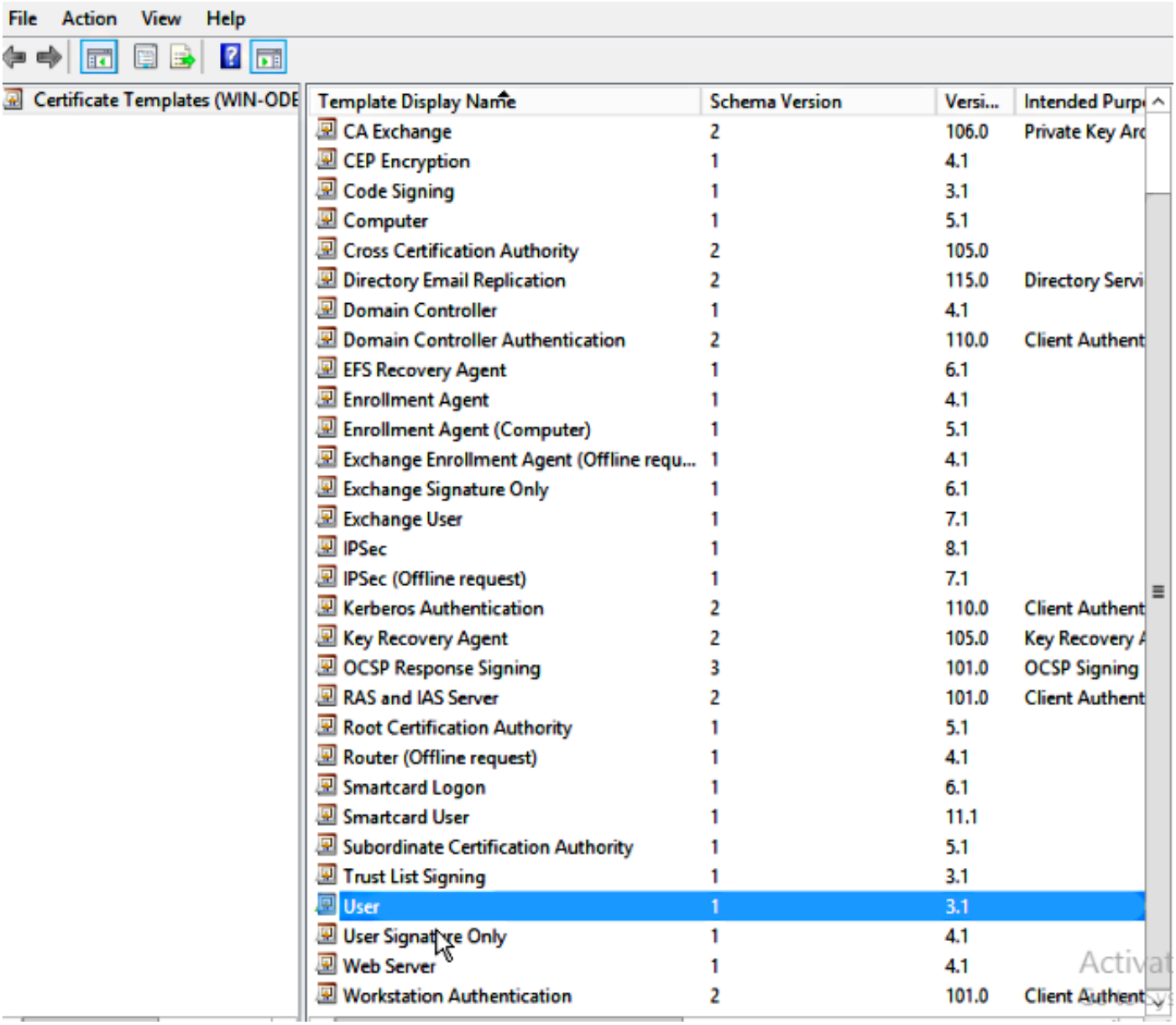

**Schritt 22:** Klicken Sie auf das **Menü Microsoft Windows/Start**.

**Schritt 23:** Geben Sie **MMC ein**.

**Schritt 24:** Wählen Sie im Menü Datei die Option **Snap-In hinzufügen/entfernen**. Wählen Sie **Zertifizierungsstelle aus**.

**Schritt 25:** Klicken Sie mit der rechten Maustaste auf den **Ordner Zertifikatvorlage** und anschließend auf **Verwalten**.

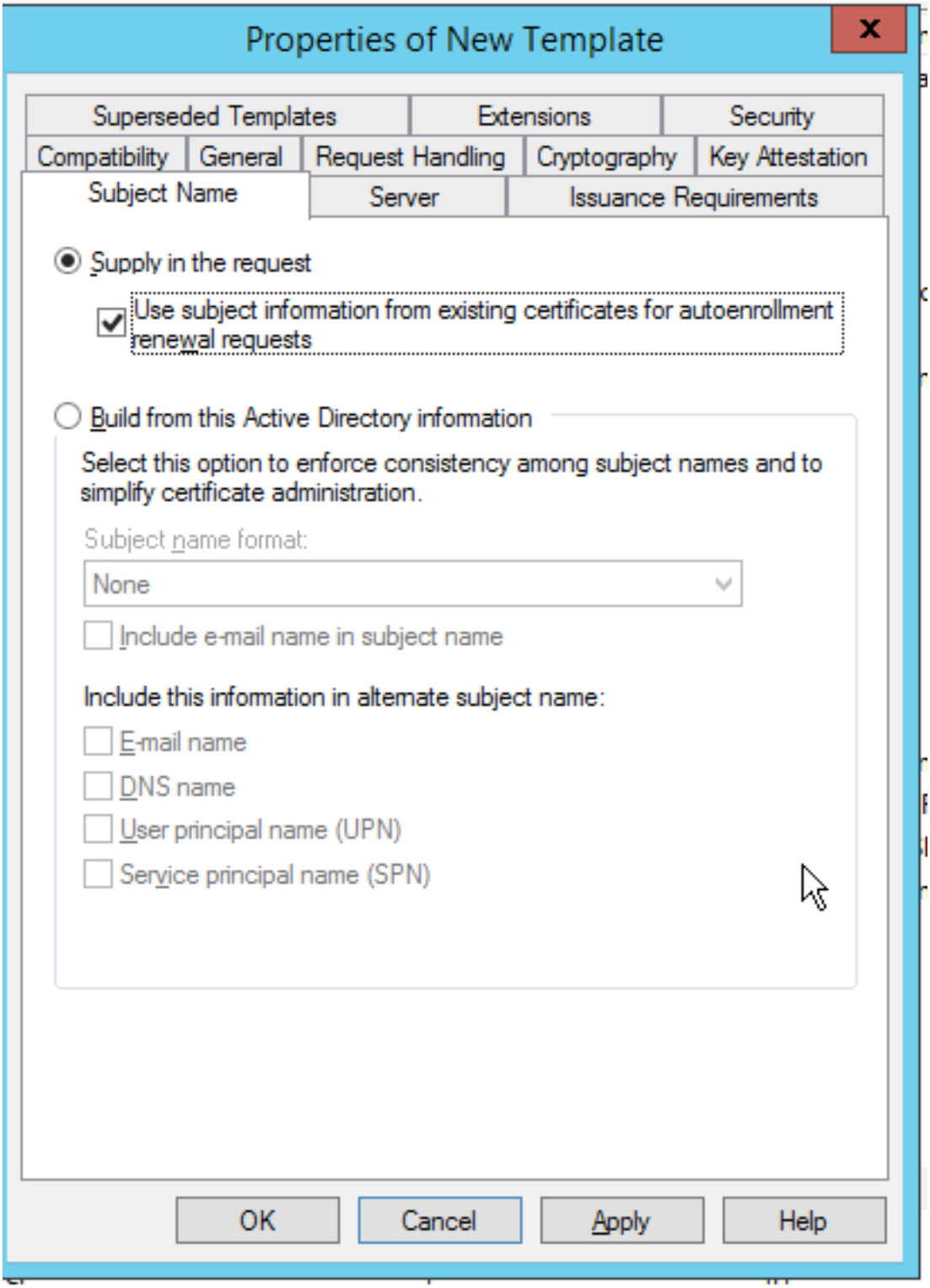
**Schritt 26:** Klicken Sie mit der rechten Maustaste auf eine vorhandene Vorlage, z. B. Benutzer, und wählen Sie **Vorlage duplizieren aus**.



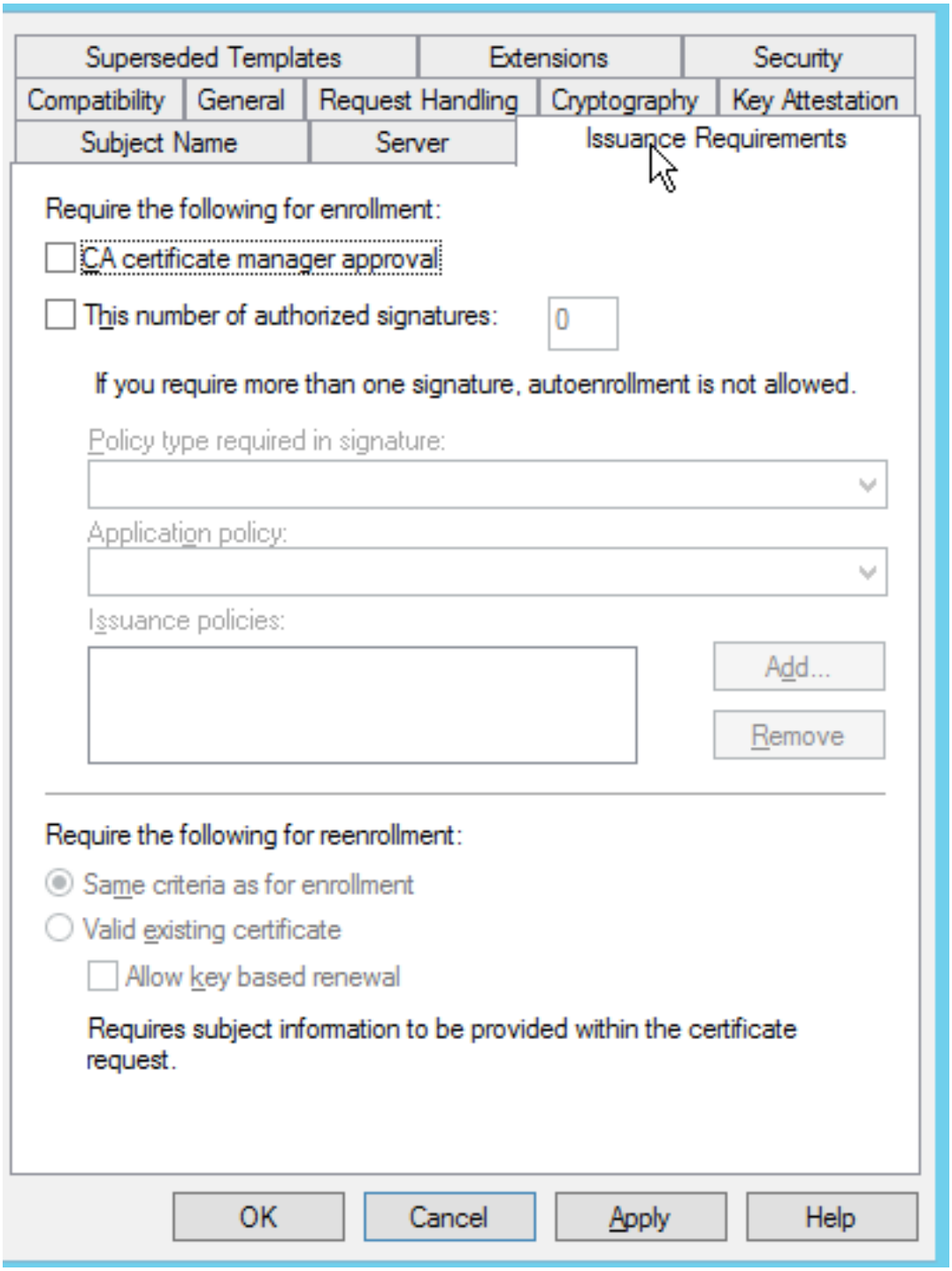

**Schritt 27:** Wählen Sie die CA als Microsoft Windows 2012 R2 aus.

**Schritt 28:** Fügen Sie auf der Registerkarte Allgemein einen Anzeigenamen wie WLC und eine Gültigkeitsdauer hinzu.

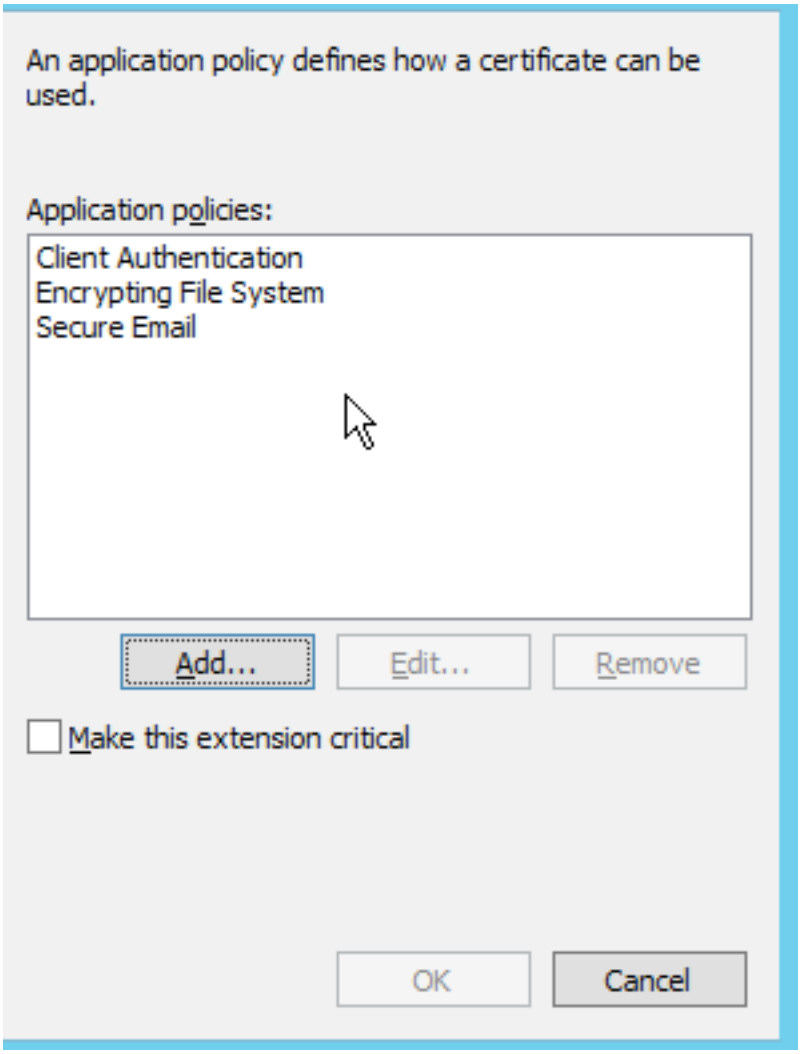
**Schritt 29:** Vergewissern Sie sich auf der Registerkarte Betreffname, dass **die Option Angebot in der Anfrage** ausgewählt ist.



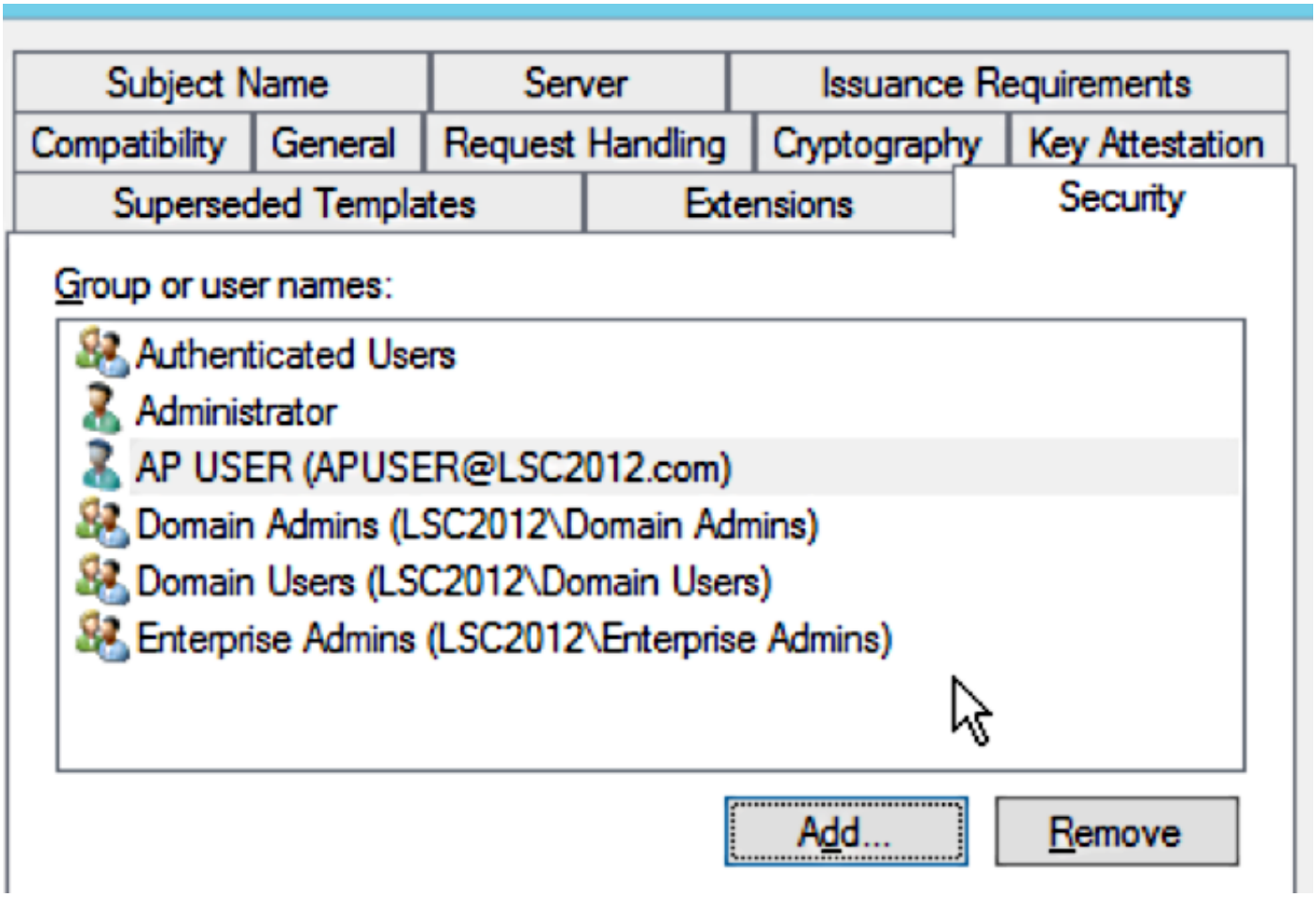

**Schritt 30:** Klicken Sie auf die Registerkarte **Issuance Requirements**. Cisco empfiehlt, Ausgaberichtlinien in einer typischen hierarchischen CA-Umgebung leer zu lassen:



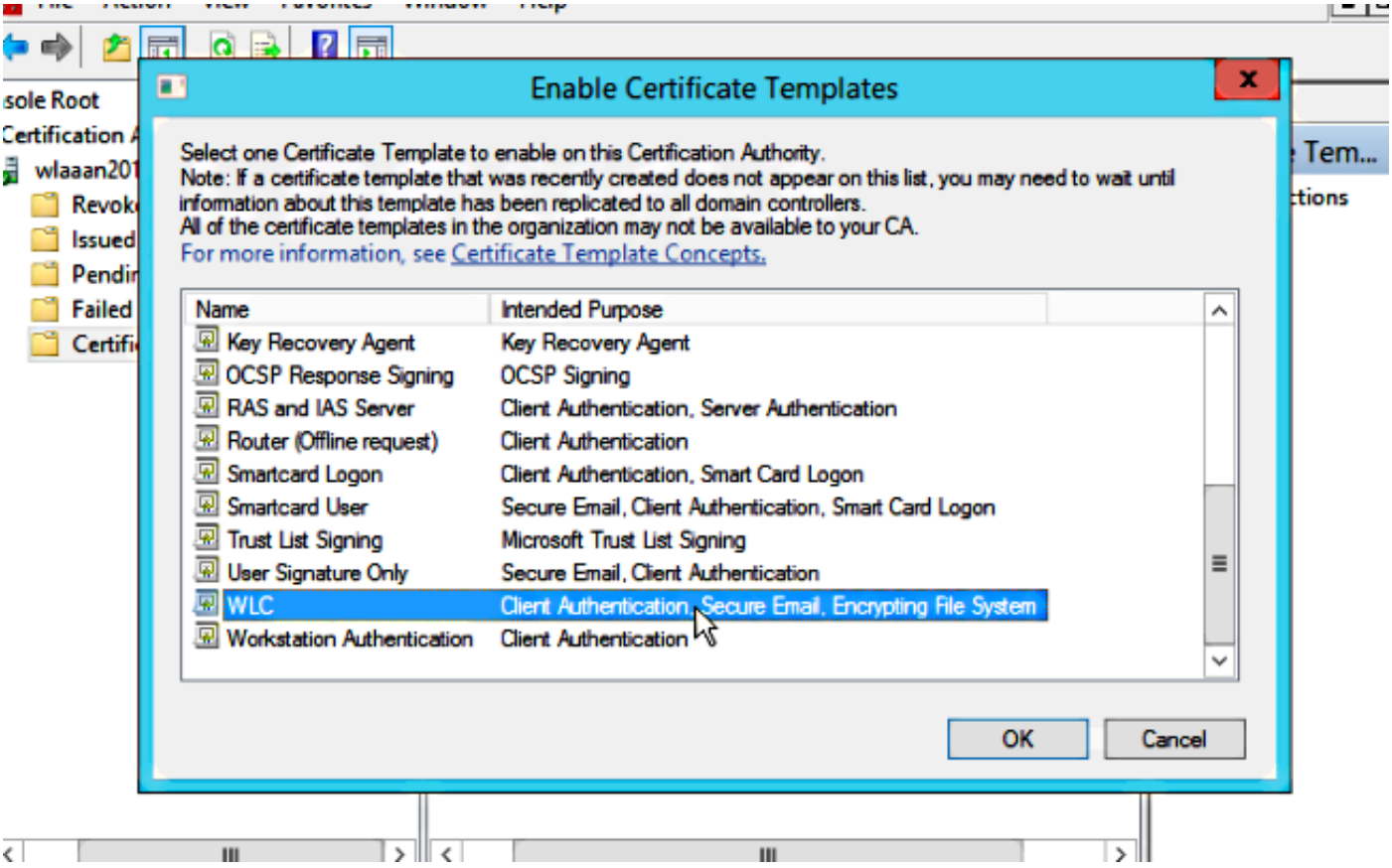

**Schritt 31:** Klicken Sie auf die **Registerkarte Erweiterungen**, **Anwendungsrichtlinien** und dann auf **Bearbeiten**. Klicken Sie auf **Hinzufügen**, und stellen Sie sicher, dass die Client-Authentifizierung als Anwendungsrichtlinie hinzugefügt wird. Klicken Sie auf **OK**.



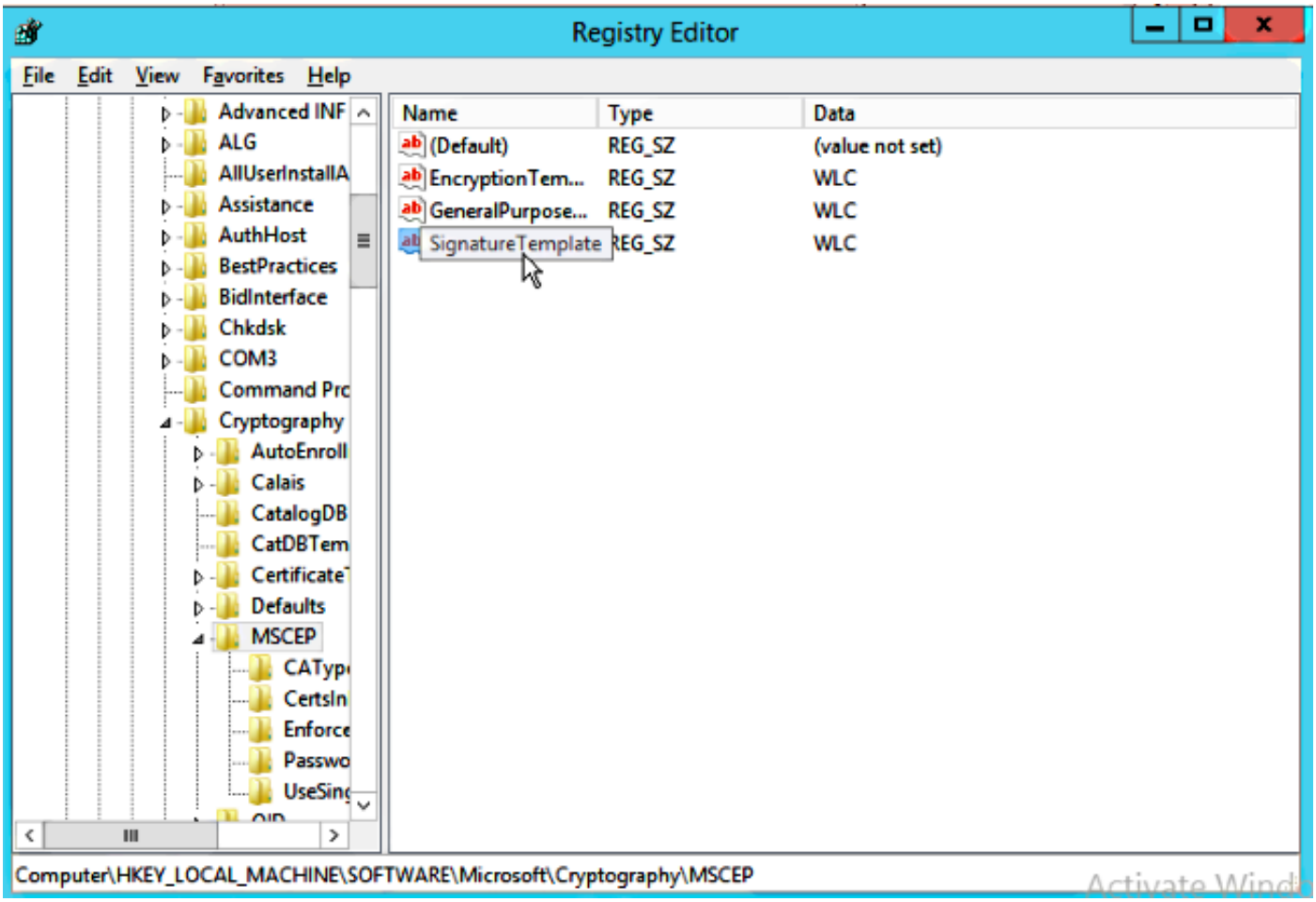

**Schritt 32:** Klicken Sie auf die **Registerkarte Sicherheit** und dann auf **Hinzufügen....**. Stellen Sie sicher, dass das in der NDES-Dienstinstallation definierte SCEP-Dienstkonto über die vollständige Kontrolle über die Vorlage verfügt, und klicken Sie auf **OK**.




**Schritt 33:** Kehren Sie zur GUI-Schnittstelle der Zertifizierungsstelle zurück. Klicken Sie mit der rechten Maustaste auf das **Verzeichnis Zertifikatvorlagen**. Navigieren Sie zu **Neu > Zu erteilende Zertifikatsvorlage**. Wählen Sie die zuvor konfigurierte WLC-Vorlage aus, und klicken Sie auf **OK.**



**Schritt 34:** Ändern Sie die Standard-SCEP-Vorlage in den Registrierungseinstellungen unter **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**. Ändern Sie die Schlüssel für EncryptionTemplate, GeneralPurposeTemplate und SignatureTemplate von IPsec (Offline Request) in die zuvor erstellte WLC-Vorlage.




**Schritt 35:** Starten Sie das System neu.

## Konfigurieren des WLC

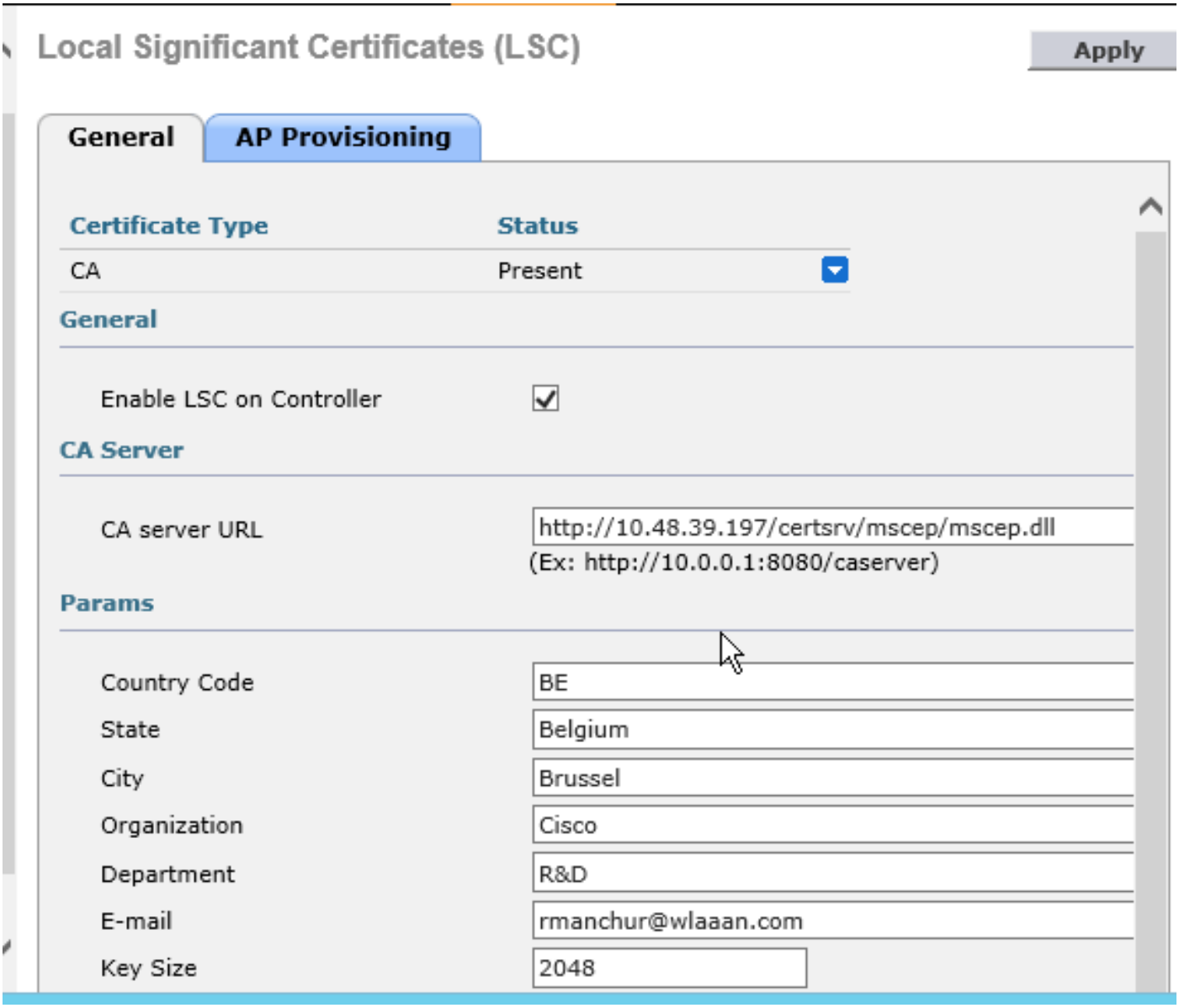
**Schritt 1:** Navigieren Sie im WLC zum Menü Security (Sicherheit). Klicken Sie auf **Certificates > LSC**.

**Schritt 2:** Aktivieren Sie das Kontrollkästchen **LSC auf Controller aktivieren**.

**Schritt 3:** Geben Sie Ihre Microsoft Windows Server 2012-URL ein. Standardmäßig wird sie an **/certsrv/mscep/mscep.dll** angehängt.

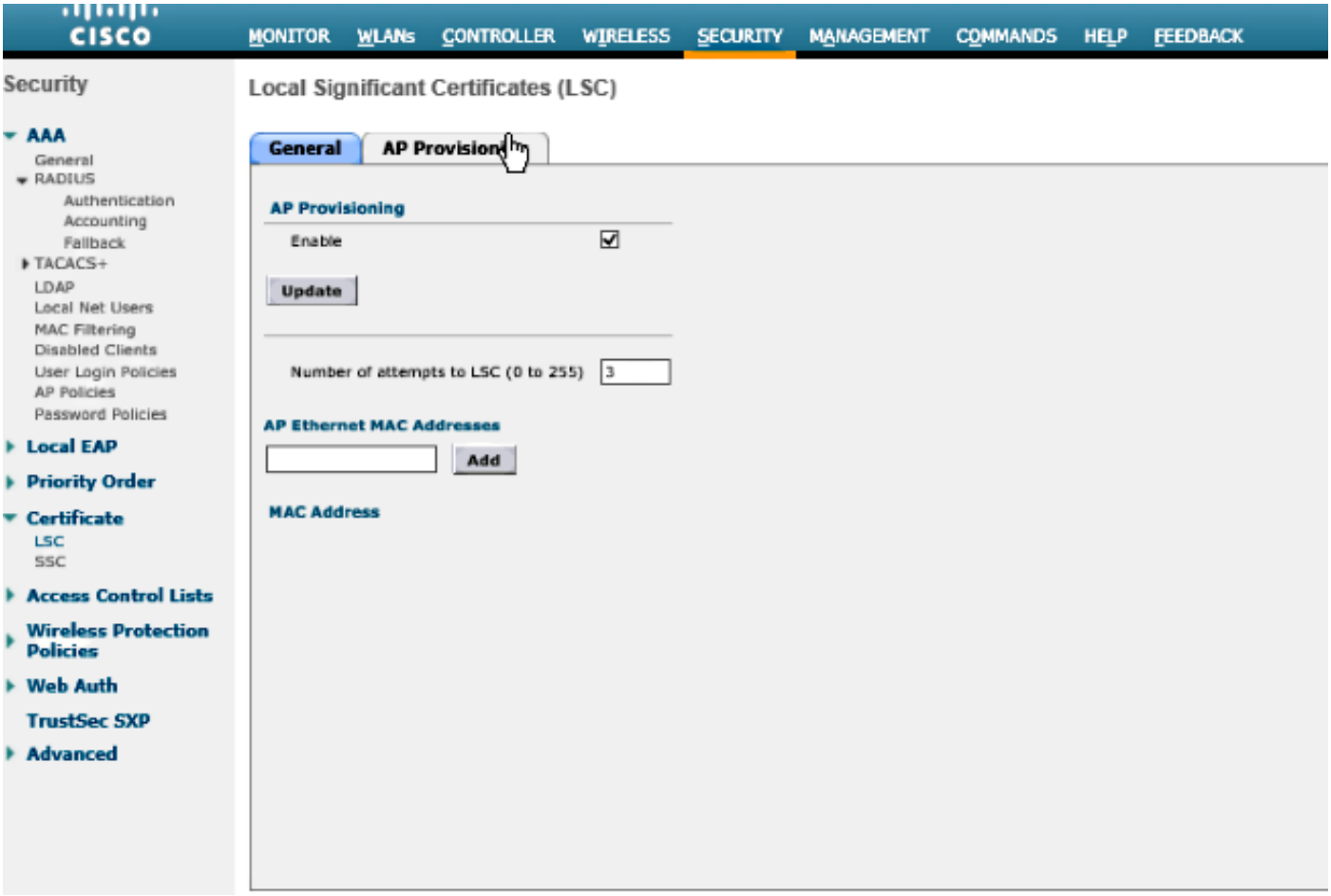
**Schritt 4:** Geben Sie Ihre Daten im Bereich **Params** ein.

**Schritt 5:** Wenden Sie die Änderung an.




**Schritt 6.** Klicken Sie auf den blauen Pfeil in der oberen CA-Zeile, und wählen Sie **Hinzufügen** aus. Sie sollte den Status von **Nicht vorhanden** in **Gegenwart** ändern.

**Schritt 7:** Klicken Sie auf die **Registerkarte AP-Bereitstellung**.



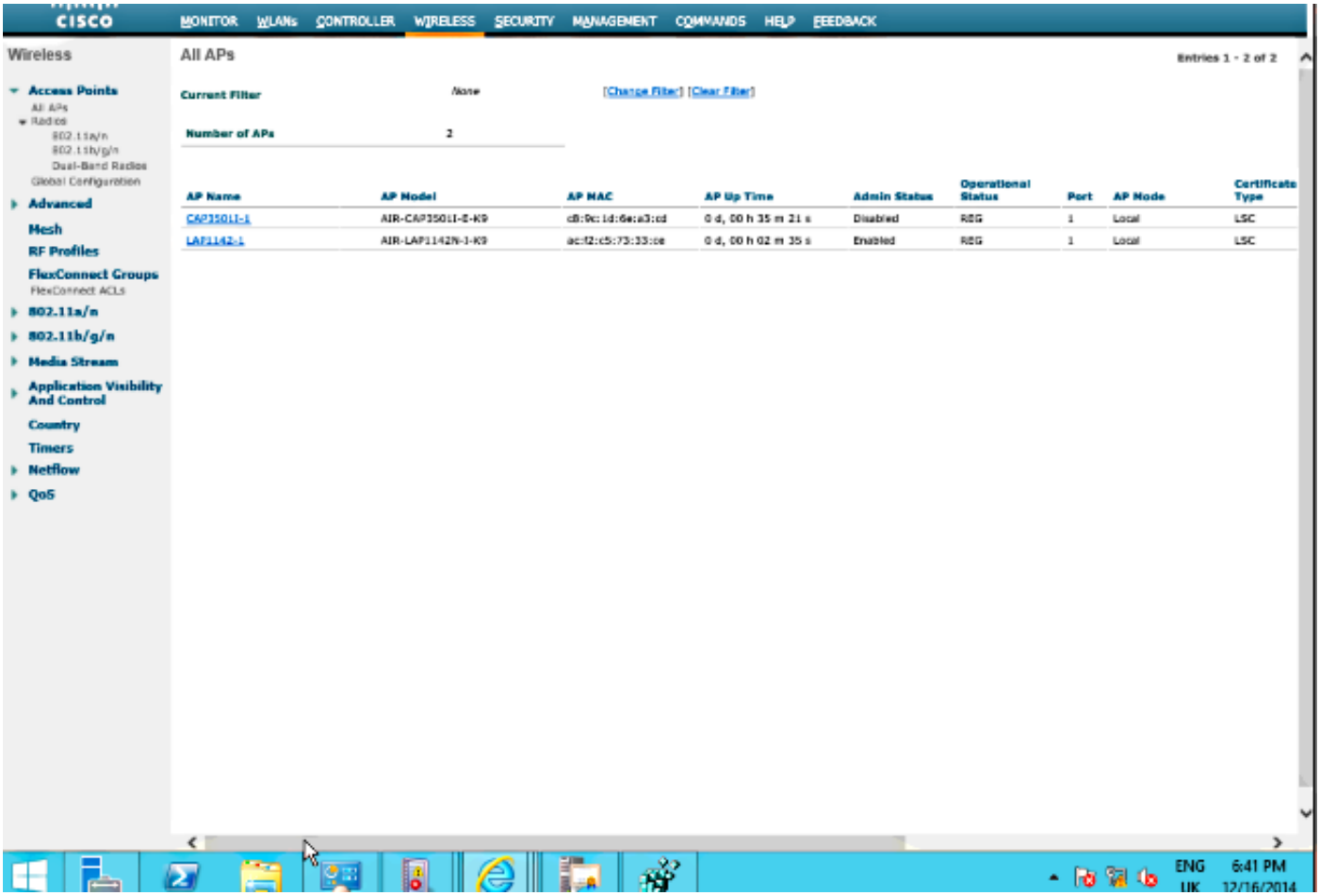

**Schritt 8.**Aktivieren Sie das **Kontrollkästchen Aktivieren** unter AP-Bereitstellung, und klicken Sie auf **Aktualisieren**.

**Schritt 9.** Starten Sie die Access Points neu, wenn sie nicht selbst neu gestartet wurden.

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der Access Point schließt sich nach dem Neustart wieder an und wird im Menü Wireless mit LSC als Zertifikatstyp angezeigt.




**Hinweis**: Nach 8.3.112 können MIC-APs nicht mehr beitreten, wenn LSC aktiviert ist. Daher wird die Funktion "versucht, LSC-Zähler zu erfassen" nur in begrenztem Umfang genutzt.

# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.