

# Exemple de configuration de certificats d'importance locale (LSC) avec WLC et Windows Server 2012

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configuration de Microsoft Windows Server](#)

[Configurer le WLC](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit comment configurer des certificats d'importance locale (LSC) avec un contrôleur de réseau local sans fil (WLC) et un Microsoft Windows Server 2012 R2 récemment installé.

**Note:** Les déploiements réels peuvent différer sur plusieurs points et vous devez avoir un contrôle et une connaissance complets des paramètres de Microsoft Windows Server 2012. Cet exemple de configuration n'est fourni qu'en tant que modèle de référence permettant aux clients Cisco de mettre en oeuvre et d'adapter leur configuration Microsoft Windows Server afin de faire fonctionner LSC.

## Conditions préalables

### Conditions requises

Cisco vous recommande de comprendre toutes les modifications apportées à Microsoft Windows Server et de consulter la documentation Microsoft appropriée si nécessaire.

**Note:** LSC sur WLC n'est pas pris en charge avec l'autorité de certification intermédiaire, car l'autorité de certification racine sera manquée du WLC puisque le contrôleur obtient seulement l'autorité de certification intermédiaire.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC version 7.6
- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configuration

### Configuration de Microsoft Windows Server

Cette configuration s'affiche comme effectuée sur un Microsoft Windows Server 2012 récemment installé. Vous devez adapter les étapes à votre domaine et à votre configuration.

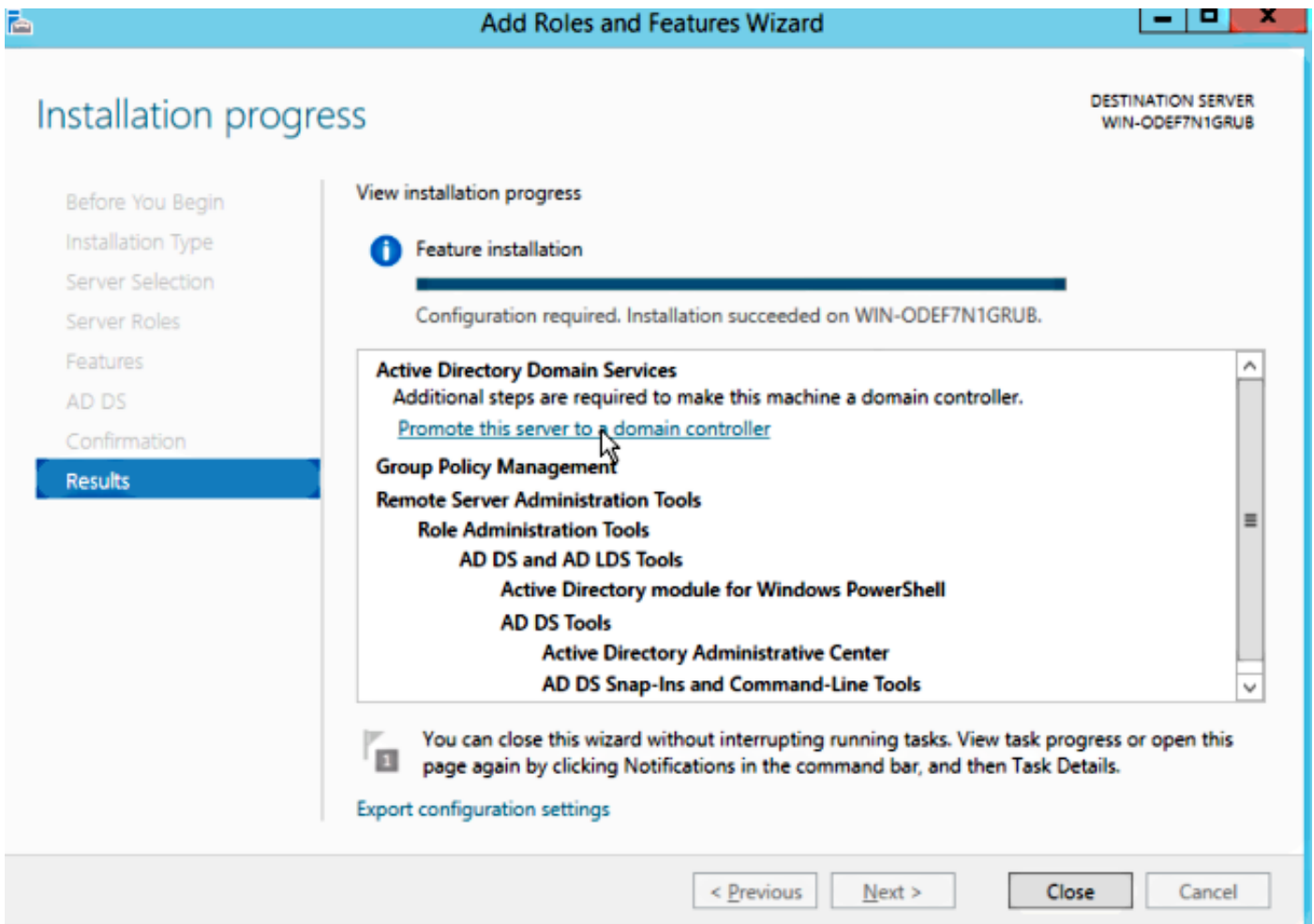
**Étape 1.** Installer les services de domaine Active Directory pour l'Assistant Fonctions et rôles.

The screenshot shows the 'Select server roles' wizard in Windows Server 2012. The title bar indicates the destination server is 'WIN-ODEF7N1GRUB'. The left sidebar shows the installation progress, with 'Server Roles' selected. The main area displays a list of roles to install on the selected server. The 'Active Directory Domain Services' role is checked. A description box on the right provides details about AD DS.

Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	
<input checked="" type="checkbox"/> Active Directory Domain Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Application Server	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	

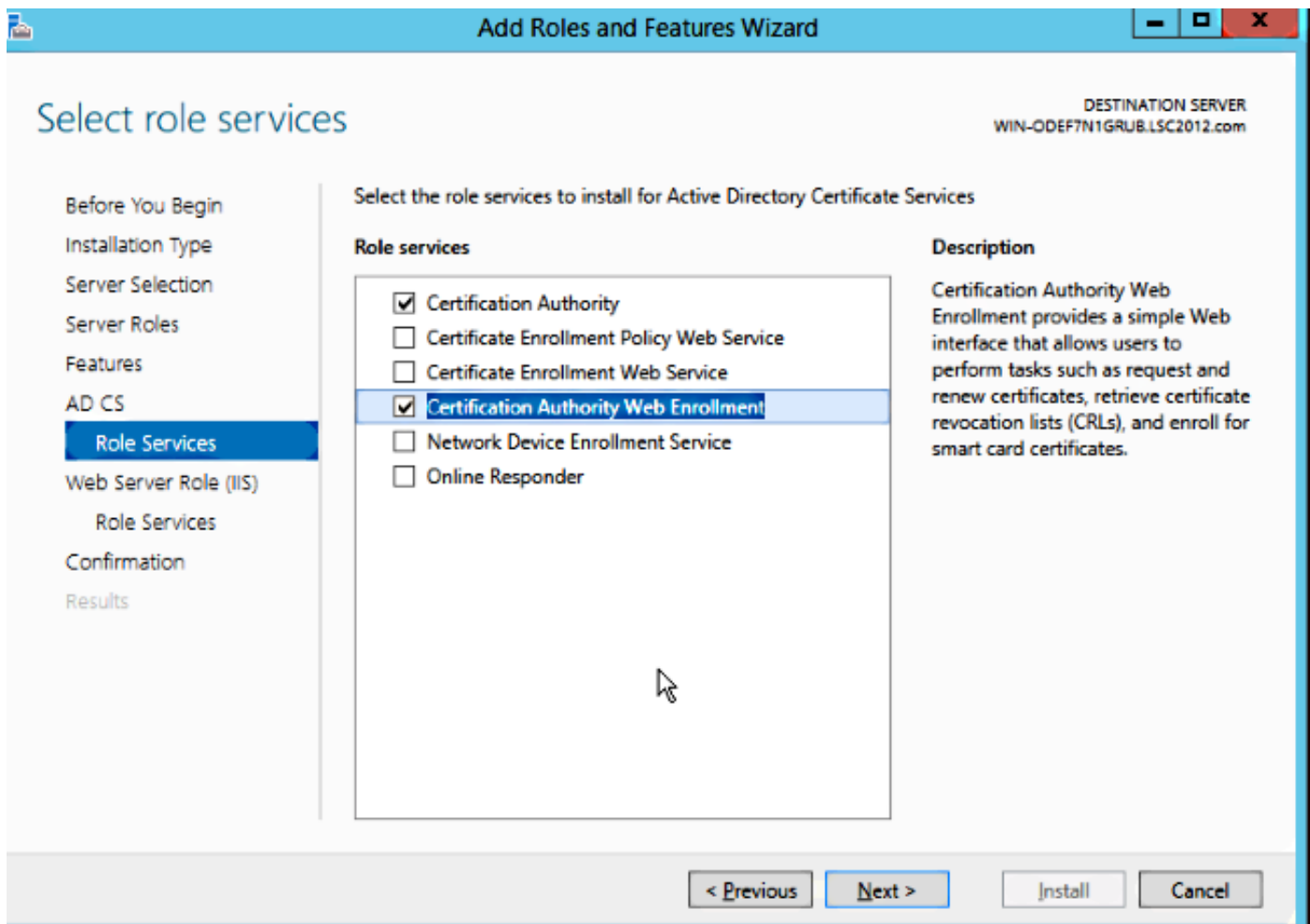
At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

**Étape 2.** Après l'installation, vous devez promouvoir le serveur au contrôleur de domaine.

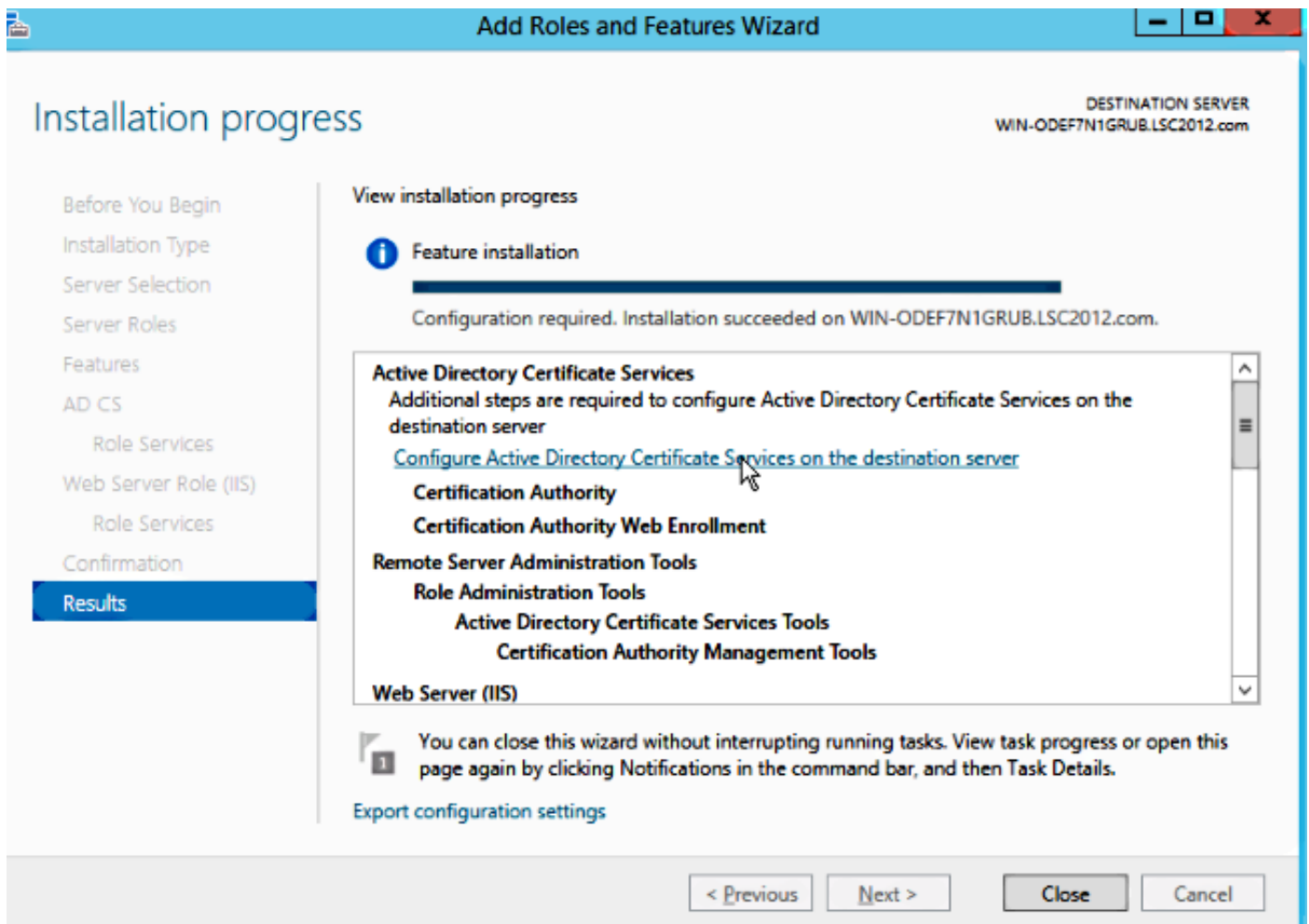


**Étape 3.** Comme il s'agit d'une nouvelle configuration, vous configurez une nouvelle forêt ; mais généralement dans les déploiements existants, il suffit de configurer ces points sur un contrôleur de domaine. Choisissez ici le domaine **LSC2012.com**. Ceci active également la fonctionnalité DNS (Domain Name Server).

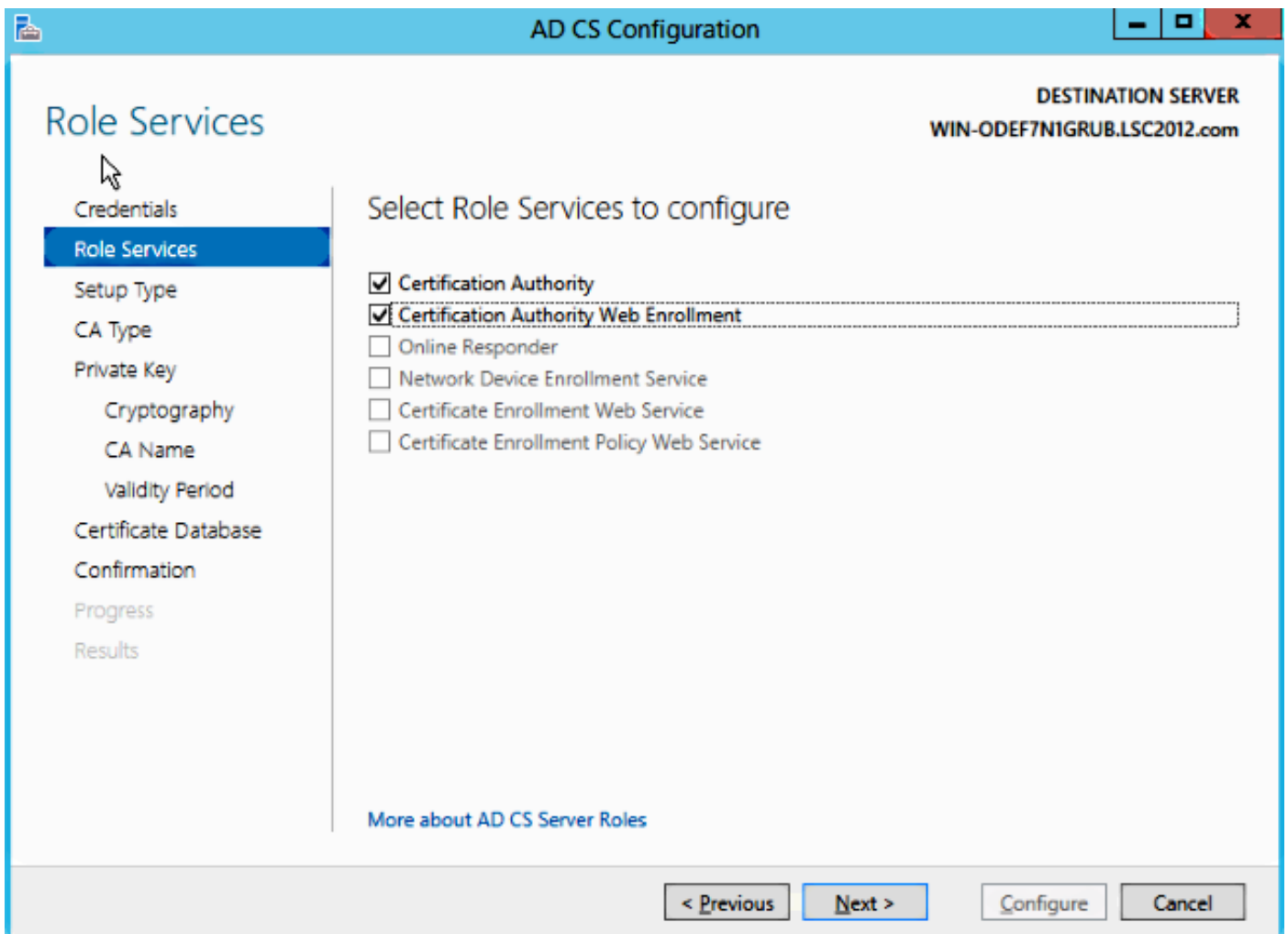
**Étape 4.** Après un redémarrage, installez le service Autorité de certification (CA) ainsi que l'inscription Web.



Étape 5. Configurez-les.



Étape 6. Choisissez Entreprise CA et laissez tout comme valeur par défaut.

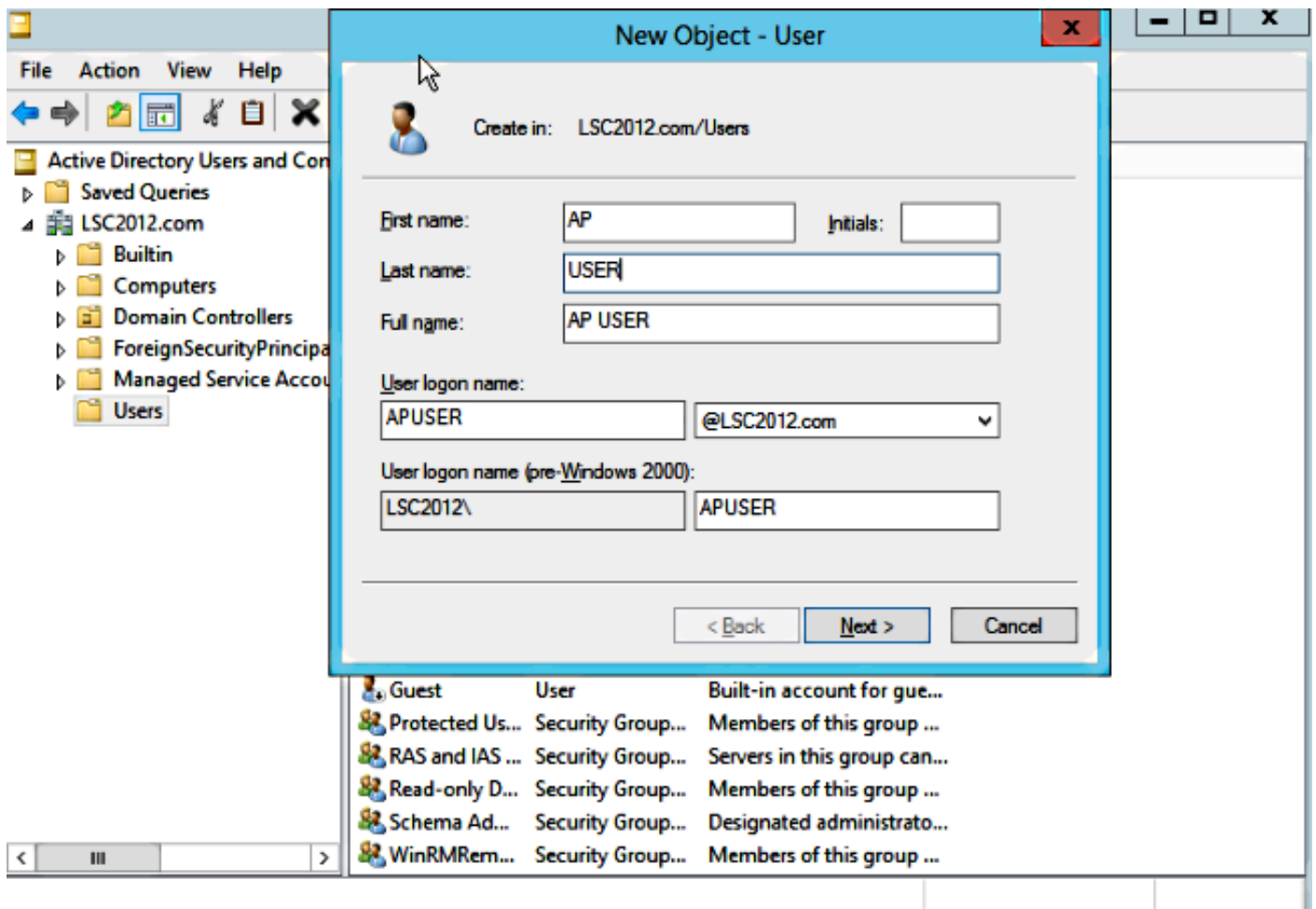


**Étape 7.** Cliquez sur le menu Microsoft Windows/Démarrer.

**Étape 8.** Cliquez sur Outils d'administration.

**Étape 9.** Cliquez sur Utilisateurs et ordinateurs Active Directory.

**Étape 10.** Développez le domaine, cliquez avec le bouton droit sur le dossier Utilisateurs, puis choisissez Nouveau objet > Utilisateur.

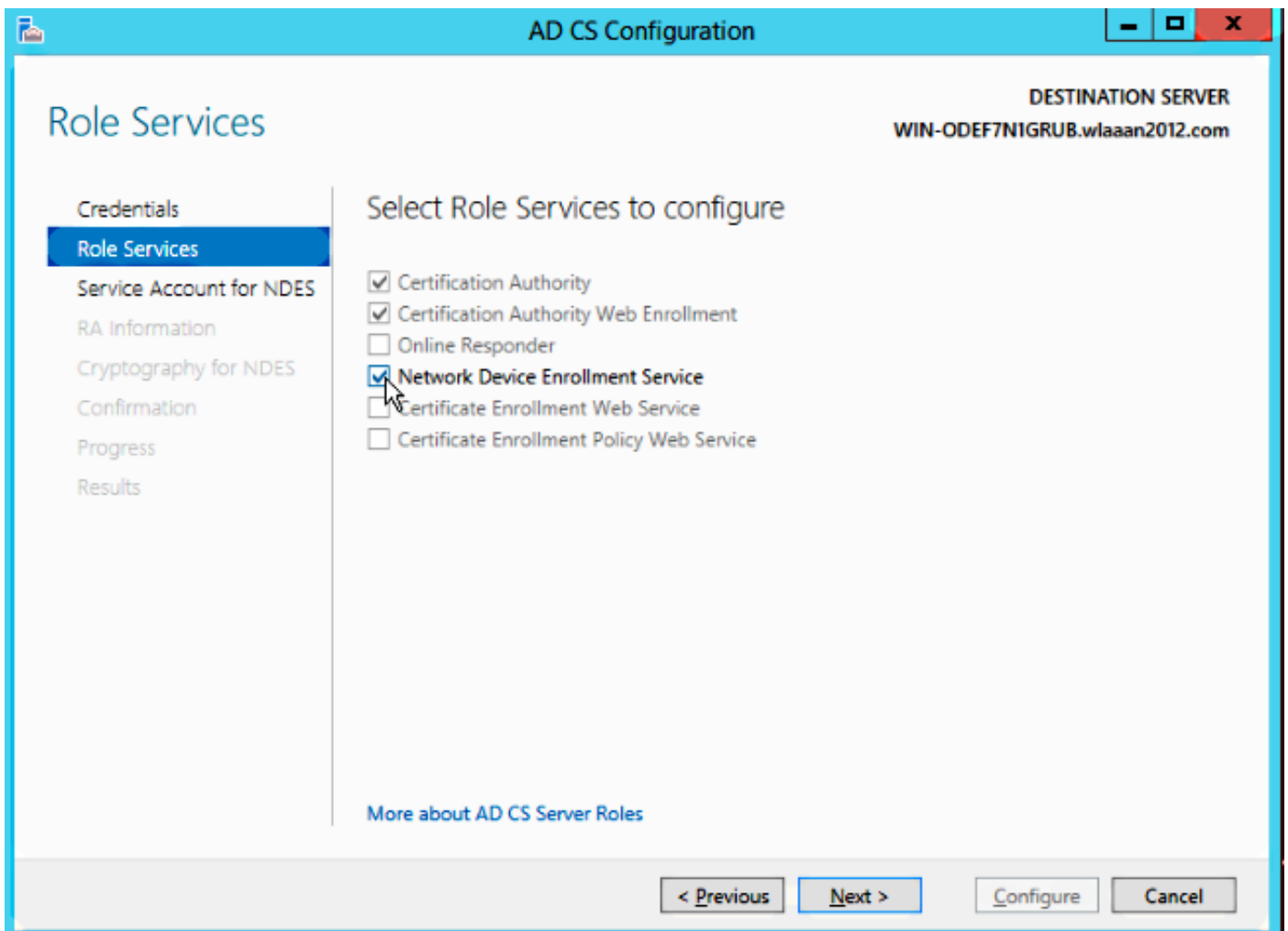


**Étape 11.** Dans cet exemple, il est nommé **APUSER**. Une fois créé, vous devez modifier l'utilisateur et cliquer sur l'onglet **MemberOf**, puis en faire un membre du groupe IIS\_IUSRS.

**Les affectations de droits d'utilisateur requises sont les suivantes :**

- Autoriser la connexion localement
- Se connecter en tant que service

**Étape 12.** Installez le service NDES (Network Device Enrollment Service).



- Choisissez le membre de compte du groupe IIS\_USRS, **APUSER** dans cet exemple, comme compte de service pour NDES.

**Étape 13.** Accédez à Outils d'administration.

**Étape 14.** Cliquez sur IIS (Internet Information Services).

**Étape 15.** Développez Serveur > Sites > Site Web par défaut > Cert Srv.

**Étape 16.** Pour mscep et mscep\_admin, cliquez sur **authentication**. Assurez-vous que l'authentification anonyme est activée.

**Étape 17.** Cliquez avec le bouton droit sur **authentification Windows** et choisissez **Fournisseurs**. Assurez-vous que NT LAN Manager (NTLM) figure en premier dans la liste.

**Étape 18.** Désactivez le défi d'authentification dans les paramètres du Registre, sinon le protocole SCEP (Simple Certificate Enrollment Protocol) attend l'authentification par mot de passe de défi,

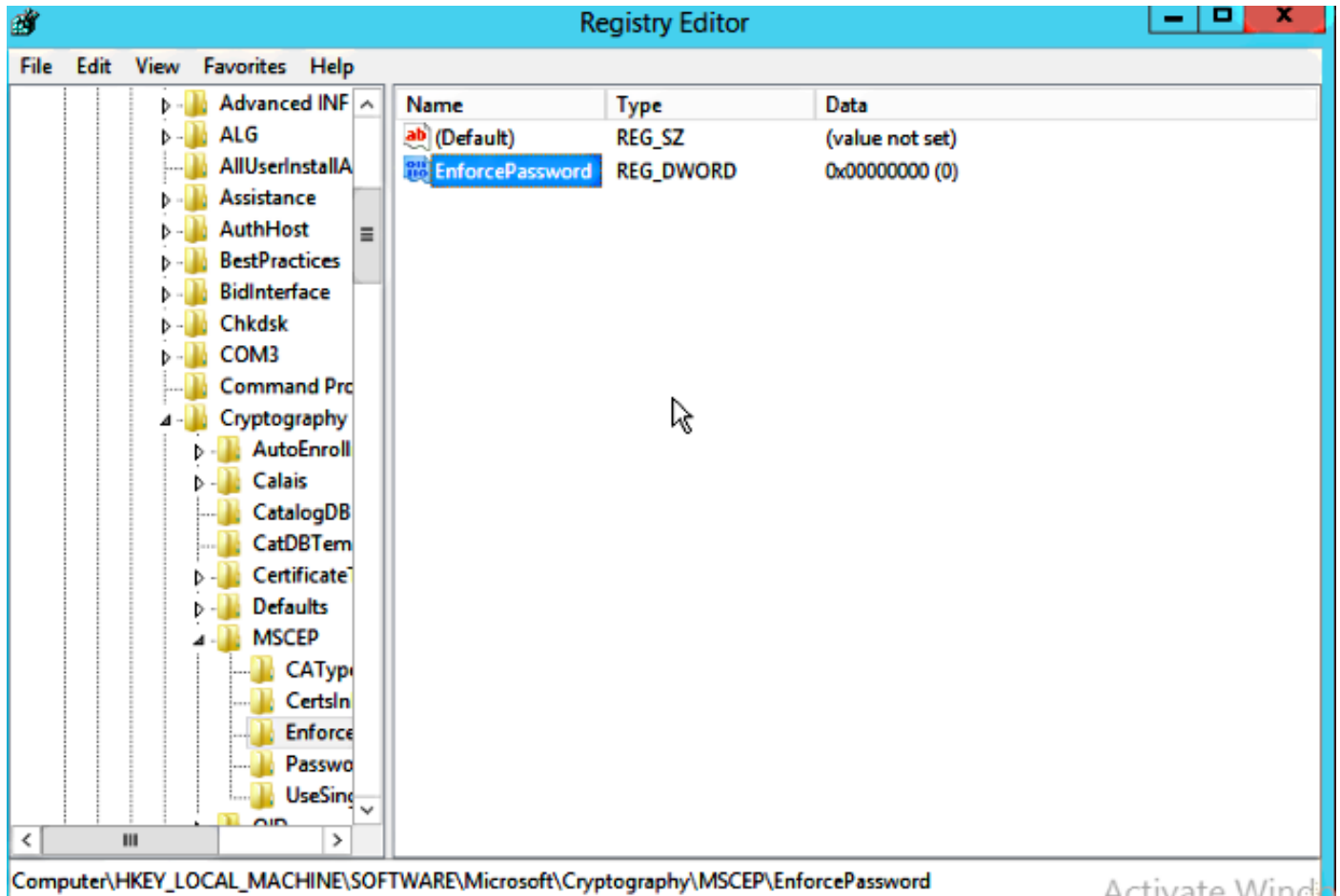


qui n'est pas pris en charge par le WLC.

Étape 19. Ouvrez l'application regedit.

Étape 20. Accédez à  
HKEY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Étape 21. Définissez EnforcePassword sur 0.



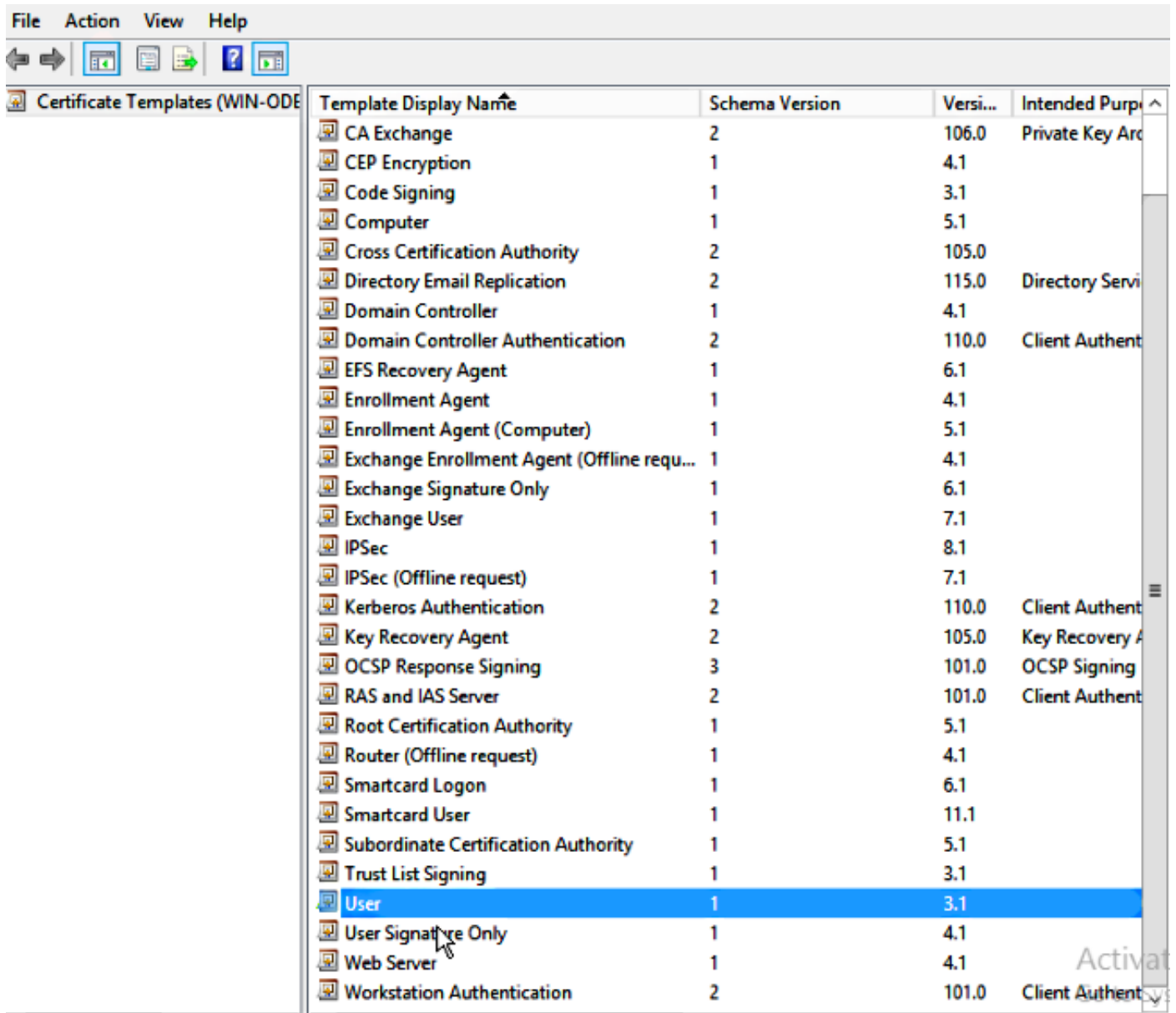
Étape 22. Cliquez sur le menu Microsoft Windows/Démarrer.

Étape 23. Tapez MMC.

Étape 24. Dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**. Sélectionnez **Autorité de certification**.

Étape 25. Cliquez avec le bouton droit sur le dossier **Modèle de certificat** et cliquez sur **Gérer**.

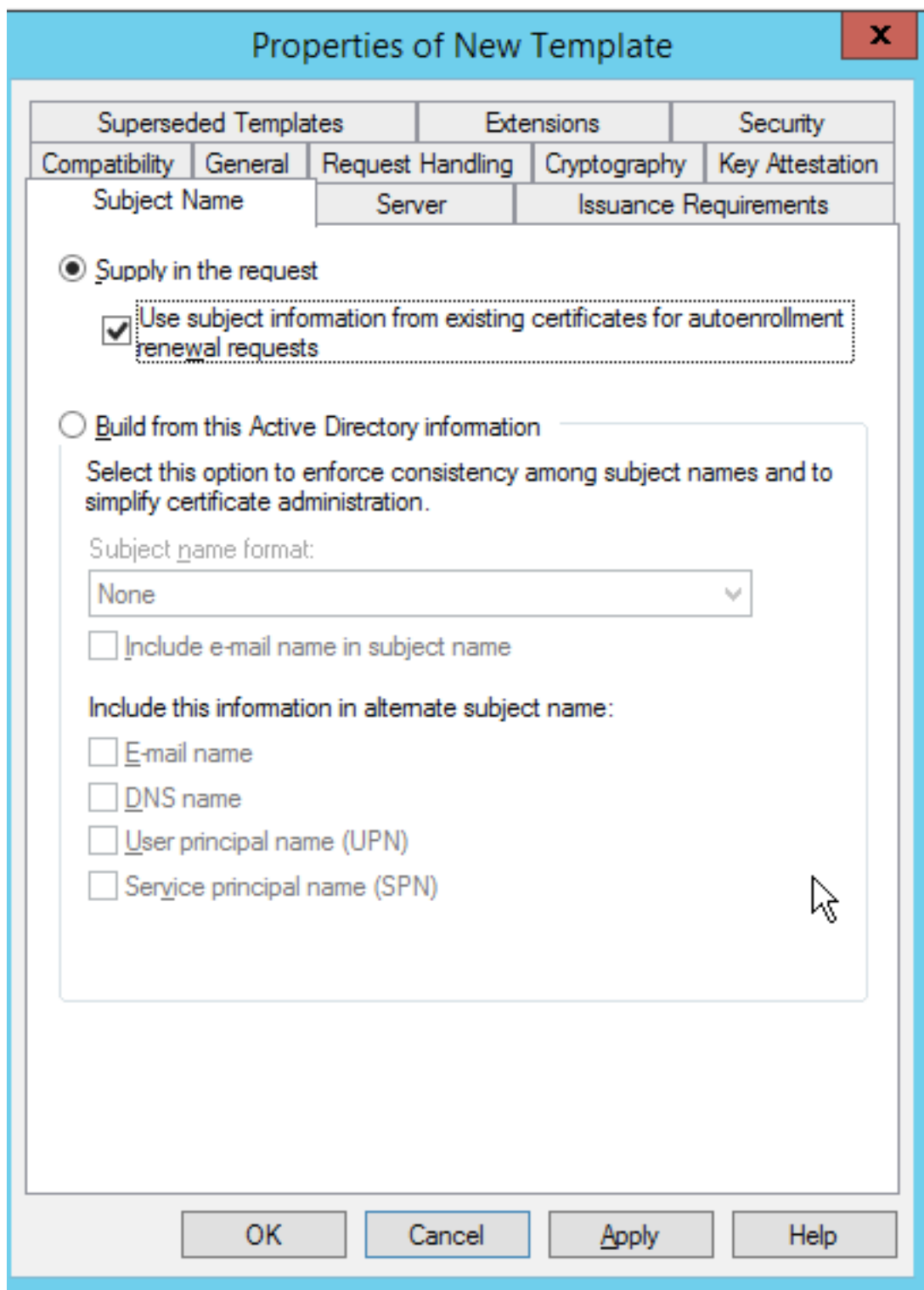
Étape 26. Cliquez avec le bouton droit sur un modèle existant, tel que **Utilisateur**, et choisissez **Modèle en double**.



**Étape 27.** Choisissez l'autorité de certification Microsoft Windows 2012 R2.

**Étape 28.** Dans l'onglet Général, ajoutez un nom d'affichage tel que WLC et une période de validité.

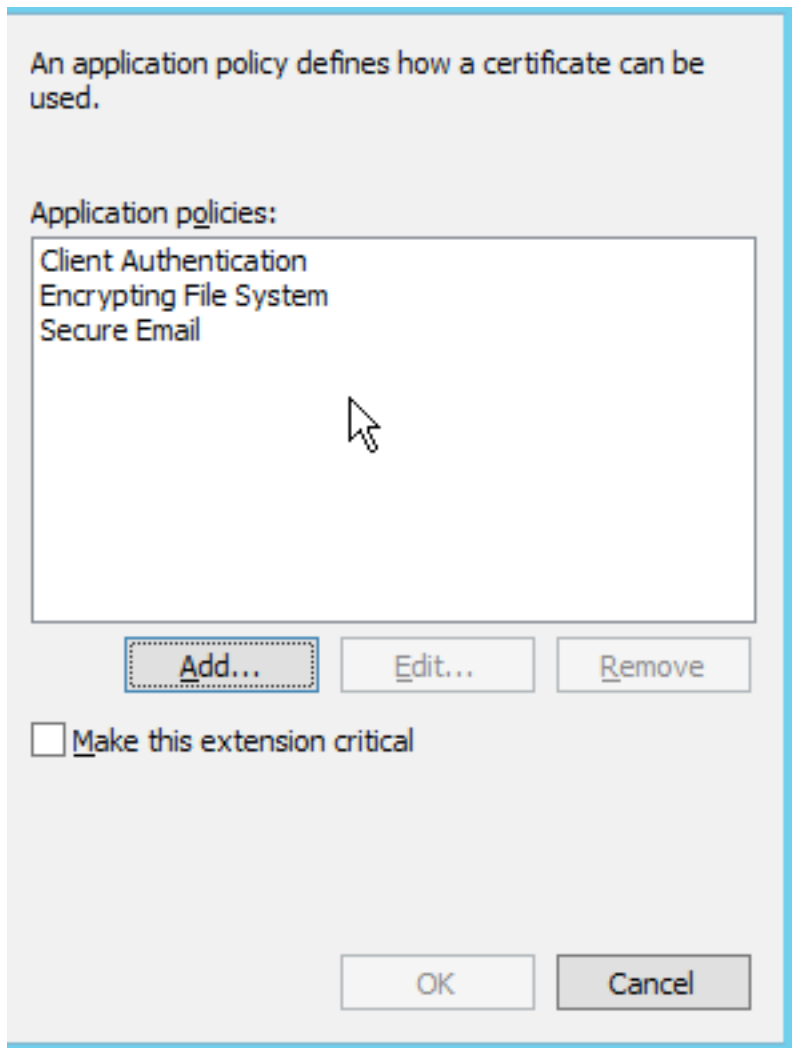
**Étape 29.** Dans l'onglet Nom du sujet, vérifiez que **Approvisionnement dans la demande** est sélectionné.



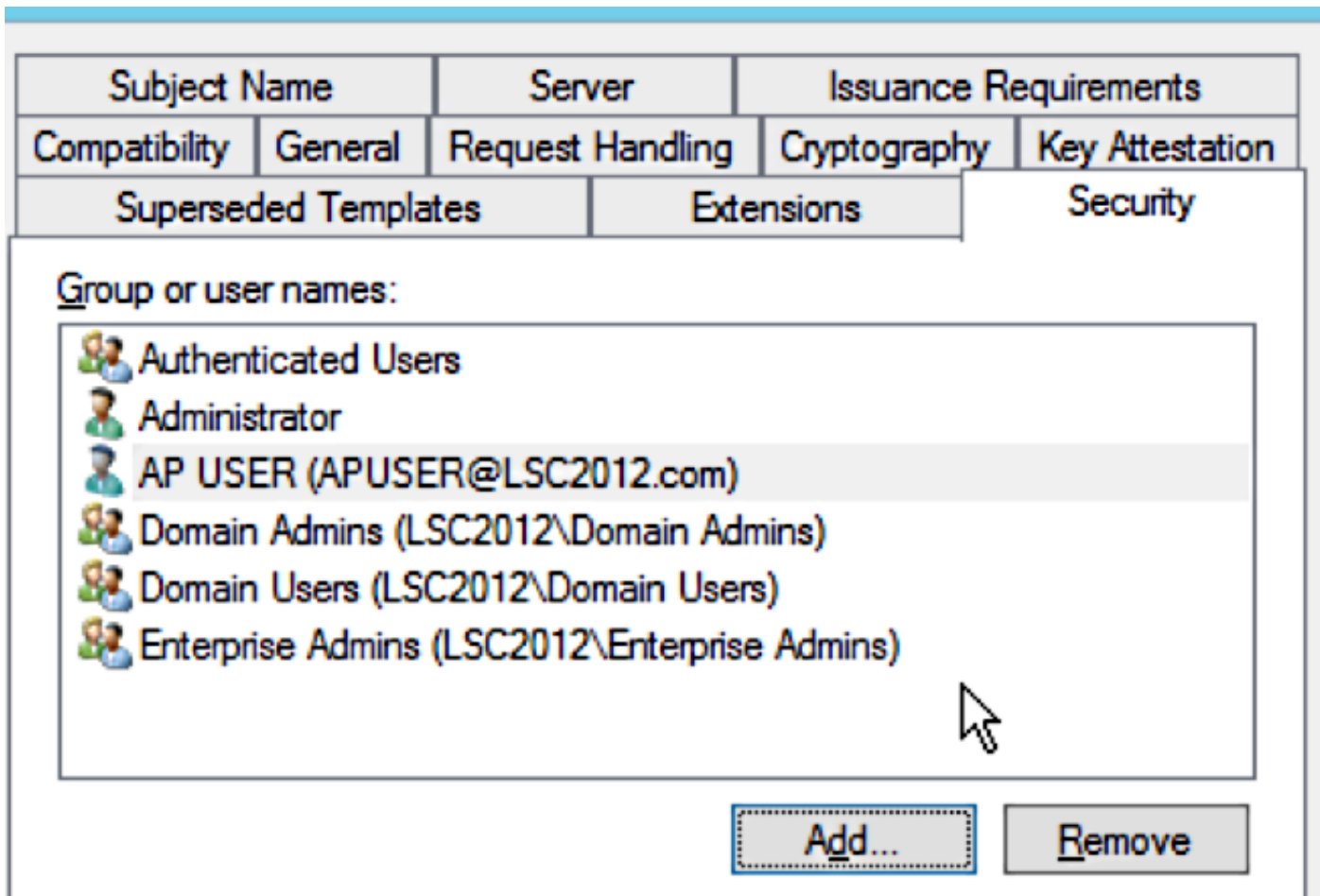
**Étape 30.** Cliquez sur l'onglet **Conditions d'émission**. Cisco recommande de laisser les stratégies d'émission vides dans un environnement CA hiérarchique typique :

Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server		Issuance Requirements
<p>Require the following for enrollment:</p> <p><input type="checkbox"/> CA certificate manager approval</p> <p><input type="checkbox"/> This number of authorized signatures: <input type="text" value="0"/></p> <p>If you require more than one signature, autoenrollment is not allowed.</p> <p>Policy type required in signature: <input type="text"/></p> <p>Application policy: <input type="text"/></p> <p>Issuance policies: <input type="text"/></p> <p><input type="button" value="Add..."/></p> <p><input type="button" value="Remove"/></p>				
<p>Require the following for reenrollment:</p> <p><input checked="" type="radio"/> Same criteria as for enrollment</p> <p><input type="radio"/> Valid existing certificate</p> <p><input type="checkbox"/> Allow key based renewal</p> <p>Requires subject information to be provided within the certificate request.</p>				
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>		<input type="button" value="Apply"/> <input type="button" value="Help"/>

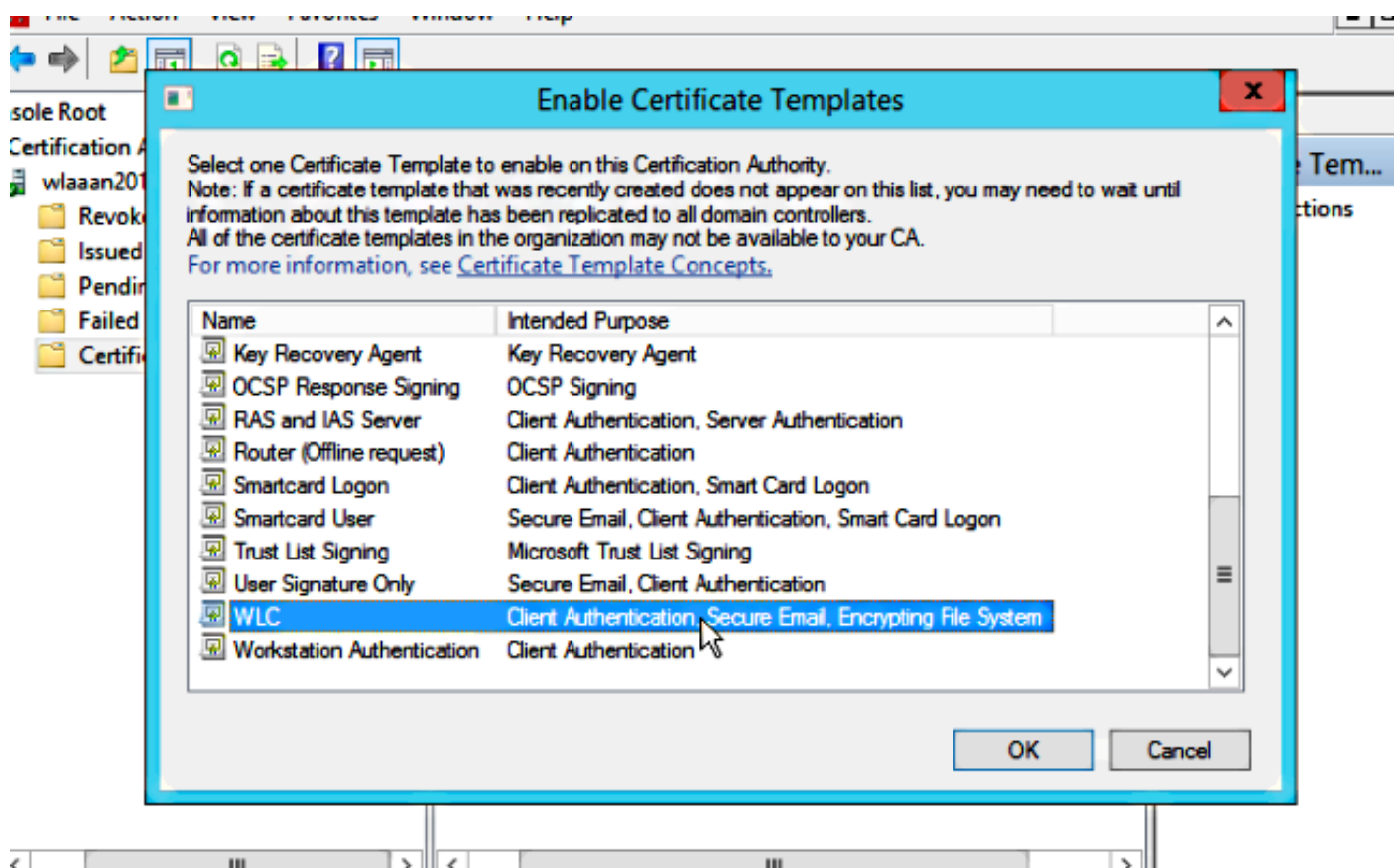
**Étape 31.** Cliquez sur l'onglet **Extensions**, **Stratégies d'application**, puis **Modifier**. Cliquez sur **Add**, et assurez-vous que l'authentification du client est ajoutée en tant que stratégie d'application. Cliquez sur **OK**.



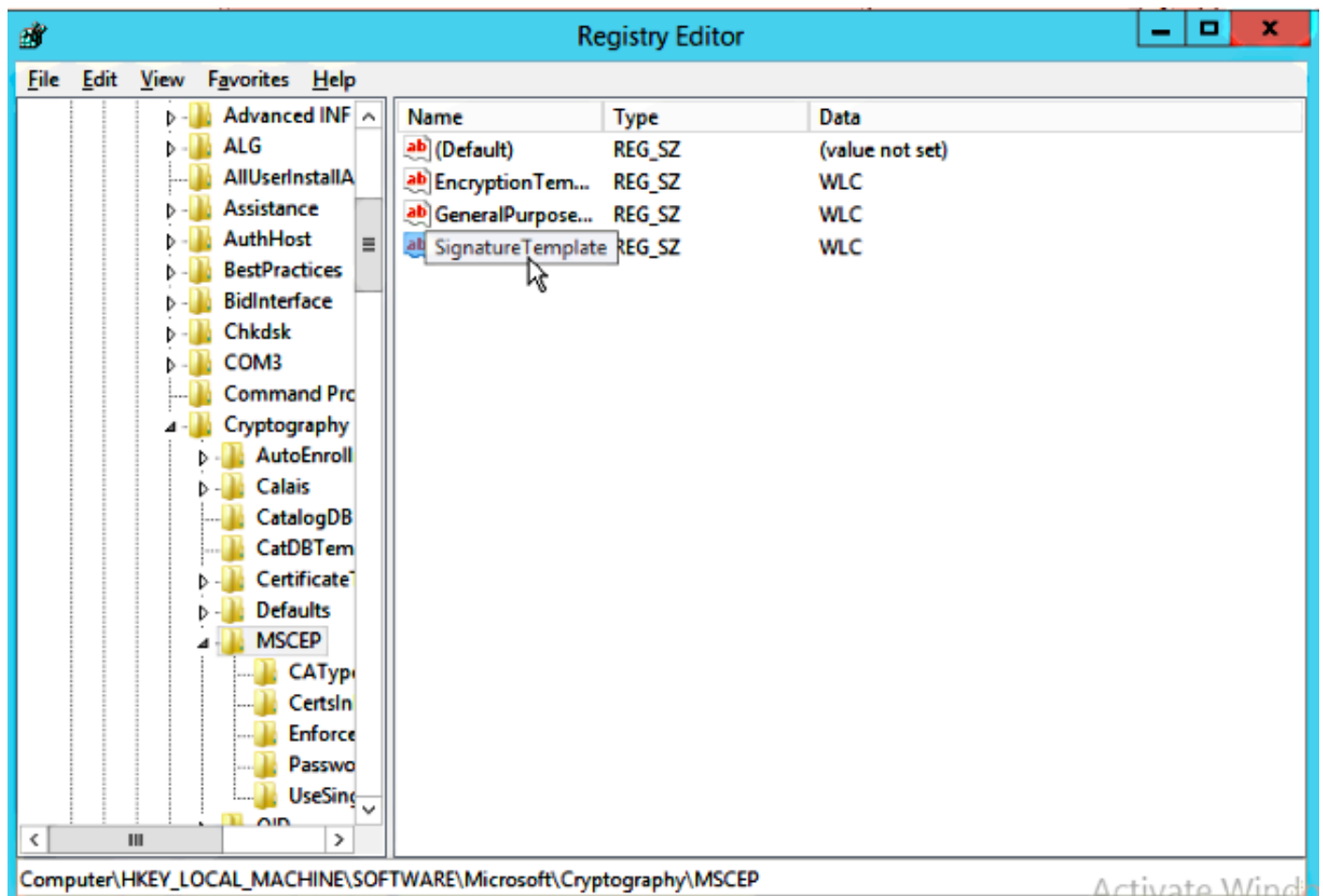
**Étape 32.** Cliquez sur l'onglet **Sécurité**, puis sur **Ajouter....** Assurez-vous que le compte de service SCEP défini dans l'installation du service NDES contrôle entièrement le modèle, puis cliquez sur **OK**.



**Étape 33.** Revenez à l'interface graphique de l'autorité de certification. Cliquez avec le bouton droit de la souris sur le **répertoire Certificate Templates**. Accédez à **Nouveau > Modèle de certificat à émettre**. Sélectionnez le modèle WLC configuré précédemment, puis cliquez sur **OK**.



**Étape 34.** Modifiez le modèle SCEP par défaut dans les paramètres de Registre sous **Ordinateur > HKEY\_LOCAL\_MACHINE > LOGICIEL > Microsoft > Cryptographie > MSCEP**. Modifiez les clés EncryptionTemplate, GeneralPurposeTemplate et SignatureTemplate d'IPsec (Offline Request) au modèle WLC précédemment créé.



**Étape 35.** Redémarrez le système.

## Configurer le WLC

**Étape 1.** Sur le WLC, accédez au menu Sécurité. Cliquez sur **Certificats > LSC**.

**Étape 2.** Cochez la case **Activer LSC sur le contrôleur**.

**Étape 3.** Saisissez votre URL Microsoft Windows Server 2012. Par défaut, il est ajouté à **/certsrv/mscep/mscep.dll**.

**Étape 4.** Entrez vos détails dans la section **Params**.

**Étape 5.** Appliquer la modification.

## Local Significant Certificates (LSC)

Apply

General

AP Provisioning

Certificate Type

Status

CA

Present



General

Enable LSC on Controller



CA Server

CA server URL

http://10.48.39.197/certsrv/mscep/mscep.dll

(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code

BE

State

Belgium

City

Brussel

Organization

Cisco

Department

R&D

E-mail

rmanchur@wlaaan.com

Key Size

2048

**Étape 6.** Cliquez sur la flèche bleue sur la ligne CA supérieure et choisissez **Ajouter**. Il doit changer le statut de **Non présent** à **présent**.

**Étape 7.** Cliquez sur l'onglet **Approvisionnement AP**.



The screenshot shows the Cisco configuration interface for Local Significant Certificates (LSC). The left sidebar contains a navigation menu with categories like AAA, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled 'Local Significant Certificates (LSC)' and has two tabs: 'General' and 'AP Provisioning'. The 'AP Provisioning' tab is active, showing an 'Enable' checkbox that is checked, an 'Update' button, and a text input field for 'Number of attempts to LSC (0 to 255)' with the value '3'. Below this is a section for 'AP Ethernet MAC Addresses' with an empty text input field and an 'Add' button. A 'MAC Address' label is positioned below the input field.

Étape 8. Cochez la case **Activer** sous Approvisionnement AP et cliquez sur **Mettre à jour**.

Étape 9. Redémarrez vos points d'accès s'ils n'ont pas redémarré eux-mêmes.

## Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Le point d'accès, après le redémarrage, se reconnecte et s'affiche avec LSC comme type de certificat dans le menu Wireless.

The screenshot shows the Cisco WLC GUI with the following data in the 'All APs' table:

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode	Certificate Type
<a href="#">CAP15011-1</a>	AIR-CA715011-2-K9	c8:9c:1d:6e:a3:cd	0 d, 00 h 35 m 21 s	Disabled	REG	1	Local	LSC
<a href="#">LAP11421-1</a>	AIR-LAP11421-1-K9	ac:f2:c5:73:33:ce	0 d, 00 h 02 m 35 s	Enabled	REG	1	Local	LSC

**Note:** Après la version 8.3.112, les points d'accès MIC ne peuvent pas se joindre du tout une fois que LSC est activé. Par conséquent, la fonction de comptage « tentatives de LSC » devient d'usage limité.

## Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.