

Esempio di certificati LSC (Locally Significant Certificates) con WLC e configurazione di Windows Server 2012

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione server di Microsoft Windows](#)

[Configurare il WLC](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare i certificati LSC (Locally Significant Certificates) con un controller WLC (Wireless LAN Controller) e un nuovo Microsoft Windows Server 2012 R2 installato.

Nota: Le distribuzioni reali possono presentare differenze in molti punti e occorre avere il controllo completo e la conoscenza delle impostazioni in Microsoft Windows Server 2012. Questo esempio di configurazione viene fornito solo come modello di riferimento per i clienti Cisco per implementare e adattare la configurazione di Microsoft Windows Server in modo da consentire il funzionamento di LSC.

Prerequisiti

Requisiti

Cisco consiglia di comprendere tutte le modifiche apportate in Microsoft Windows Server e di consultare la documentazione Microsoft pertinente, se necessario.

Nota: LSC su WLC non è supportato con intermediate-CA, in quanto la CA radice non è presente nel WLC poiché il controller ottiene solo la CA intermedia.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- WLC versione 7.6
- Microsoft Windows Server 2012 R2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione server di Microsoft Windows

Questa configurazione viene visualizzata come eseguita su un nuovo sistema operativo Microsoft Windows Server 2012. È necessario adattare i passaggi al dominio e alla configurazione.

Passaggio 1. Installare Servizi di dominio Active Directory per la procedura guidata relativa a ruoli e funzionalità.

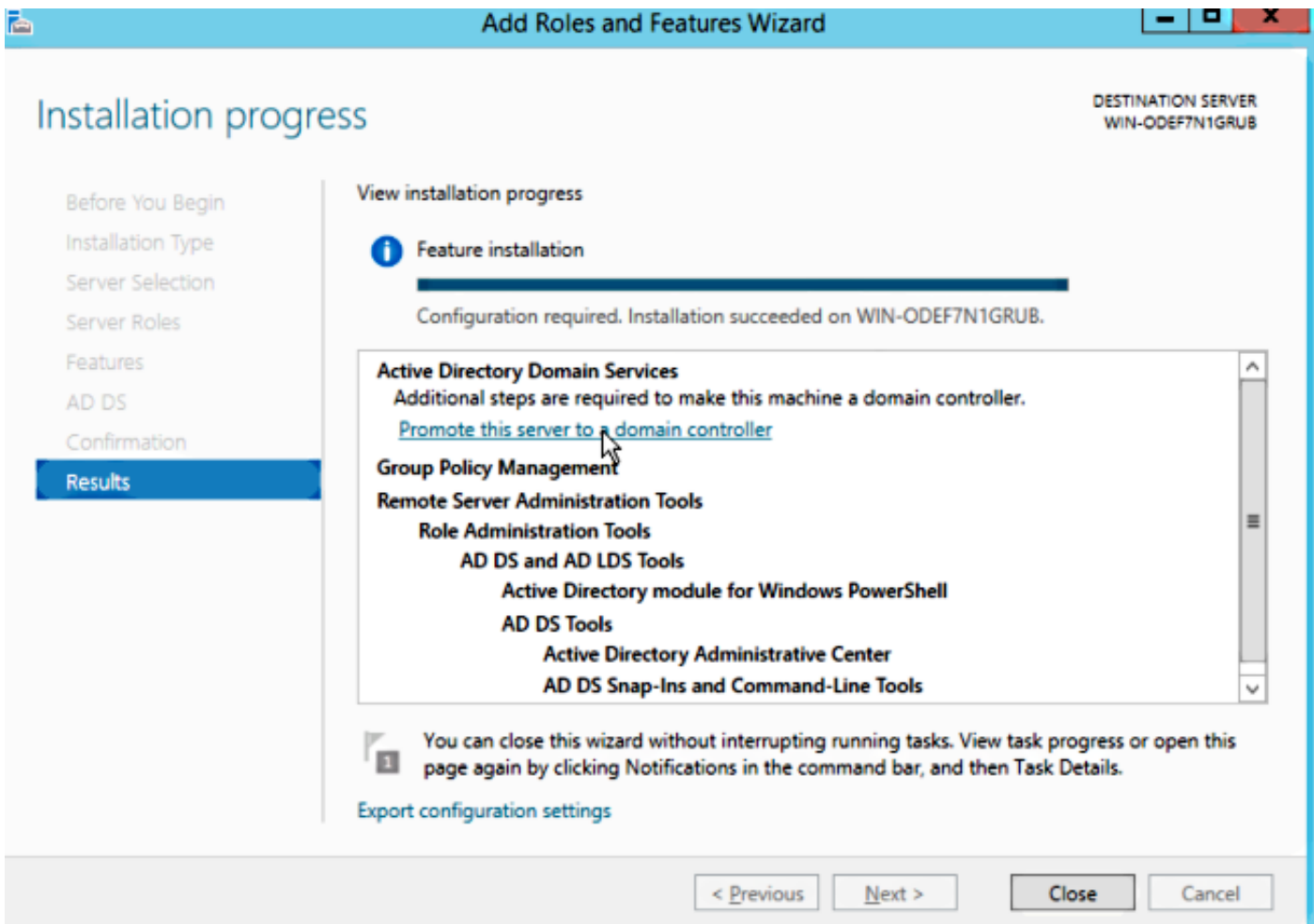
Select server roles DESTINATION SERVER
WIN-ODEF7N1GRUB

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Select one or more roles to install on the selected server.

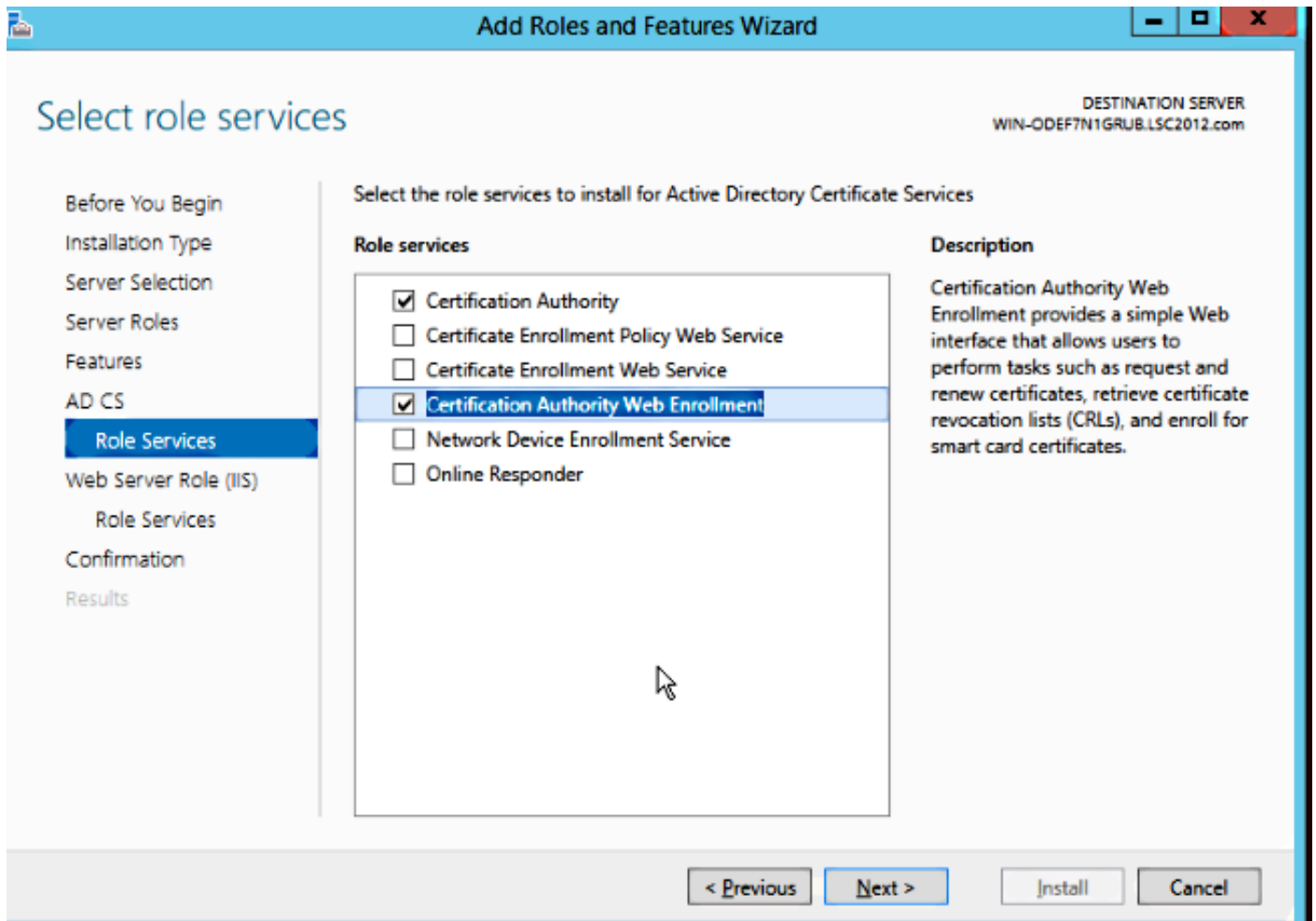
Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	
<input checked="" type="checkbox"/> Active Directory Domain Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. 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	

Passaggio 2. Dopo l'installazione, è necessario innalzare di livello il server a controller di dominio.

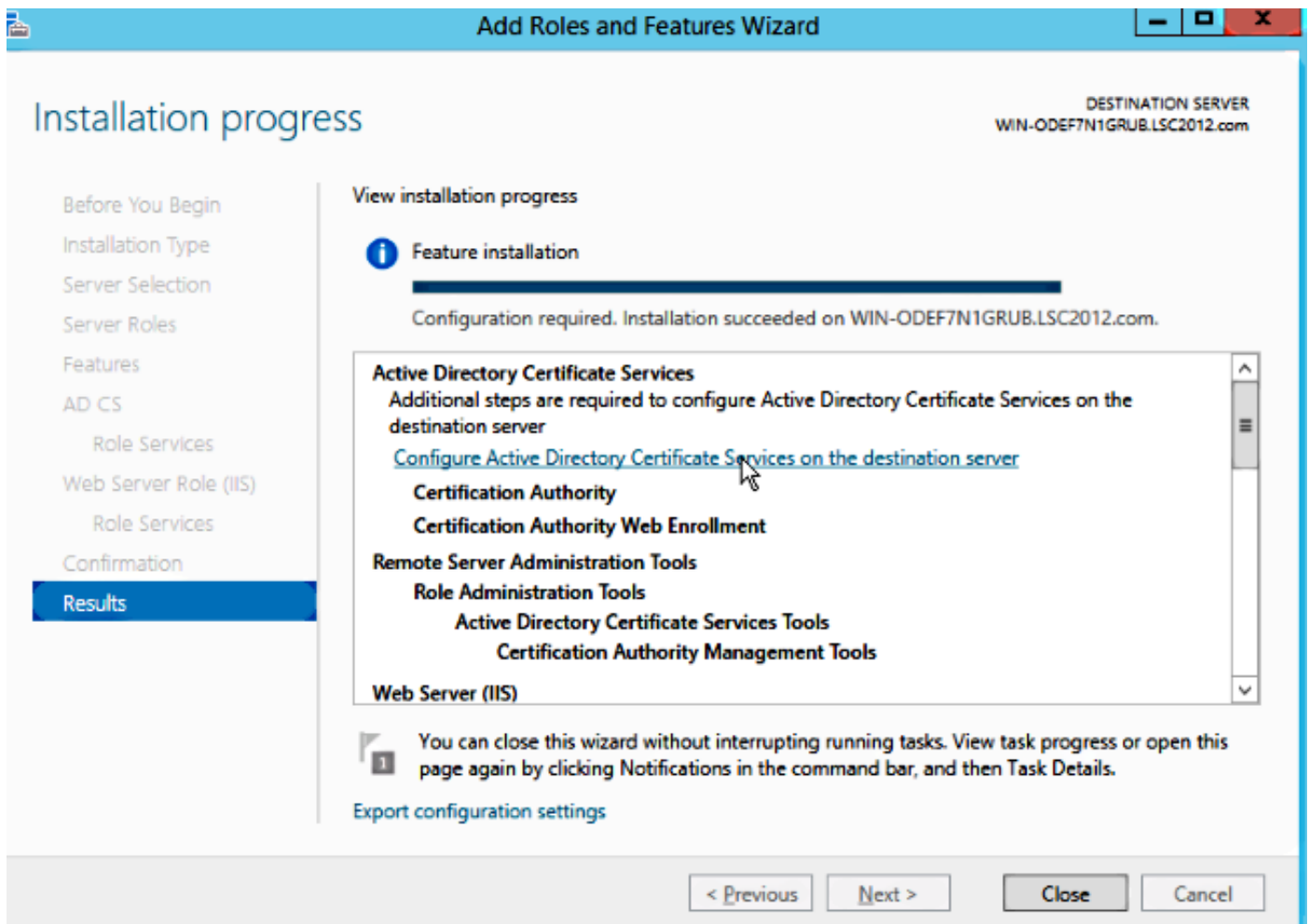


Passaggio 3. Poiché si tratta di una nuova impostazione, è possibile configurare una nuova foresta. ma in genere, nelle implementazioni esistenti, è sufficiente configurare questi punti su un controller di dominio. In questa pagina è possibile scegliere il dominio **LSC2012.com**. In questo modo viene attivata anche la funzionalità DNS (Domain Name Server).

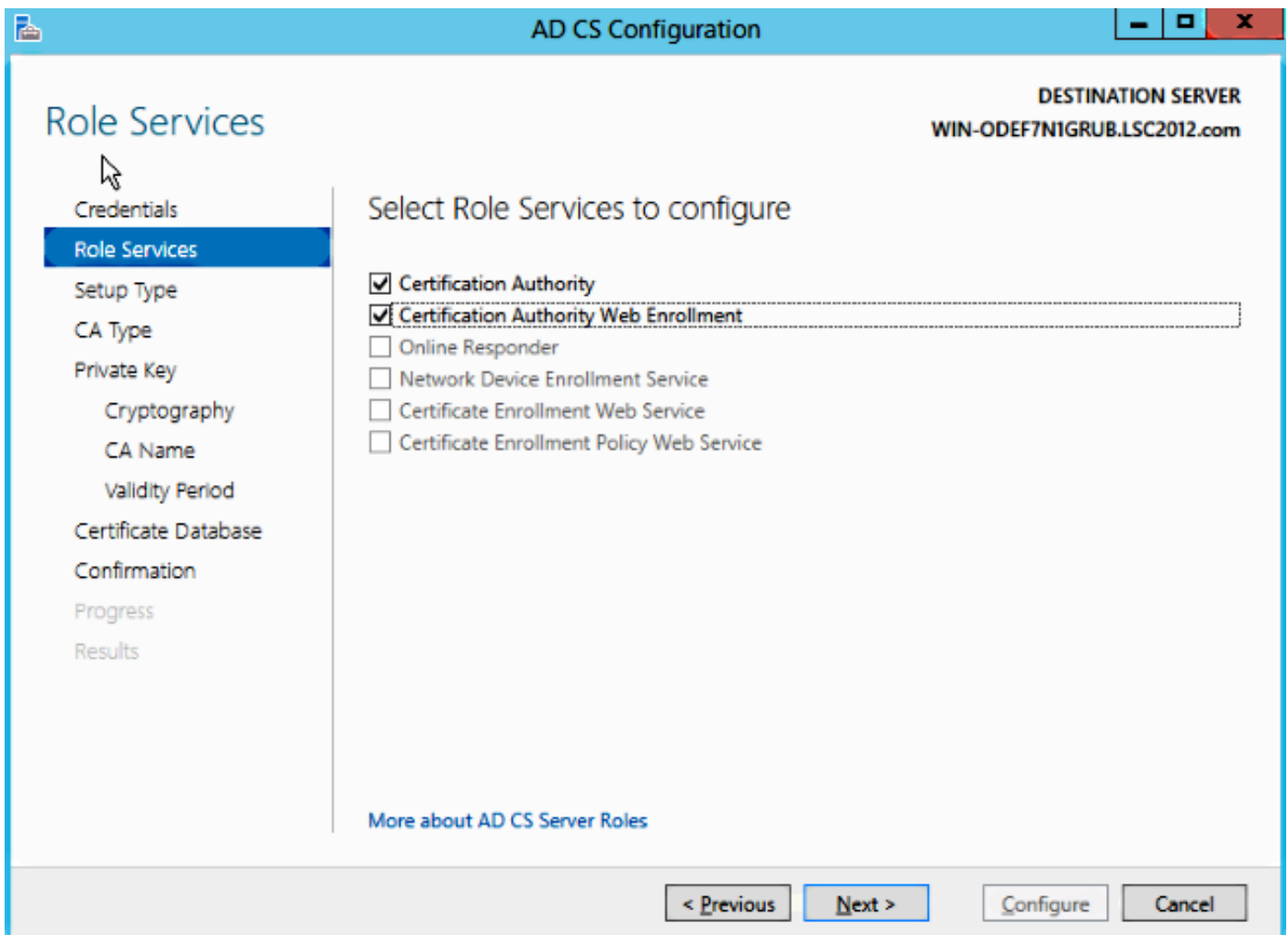
Passaggio 4. Dopo il riavvio, installare il servizio Autorità di certificazione (CA) e la registrazione Web.



Passaggio 5. Configurarle.



Passaggio 6. Scegliere CA organizzazione (Enterprise) e lasciare tutto come valore predefinito.

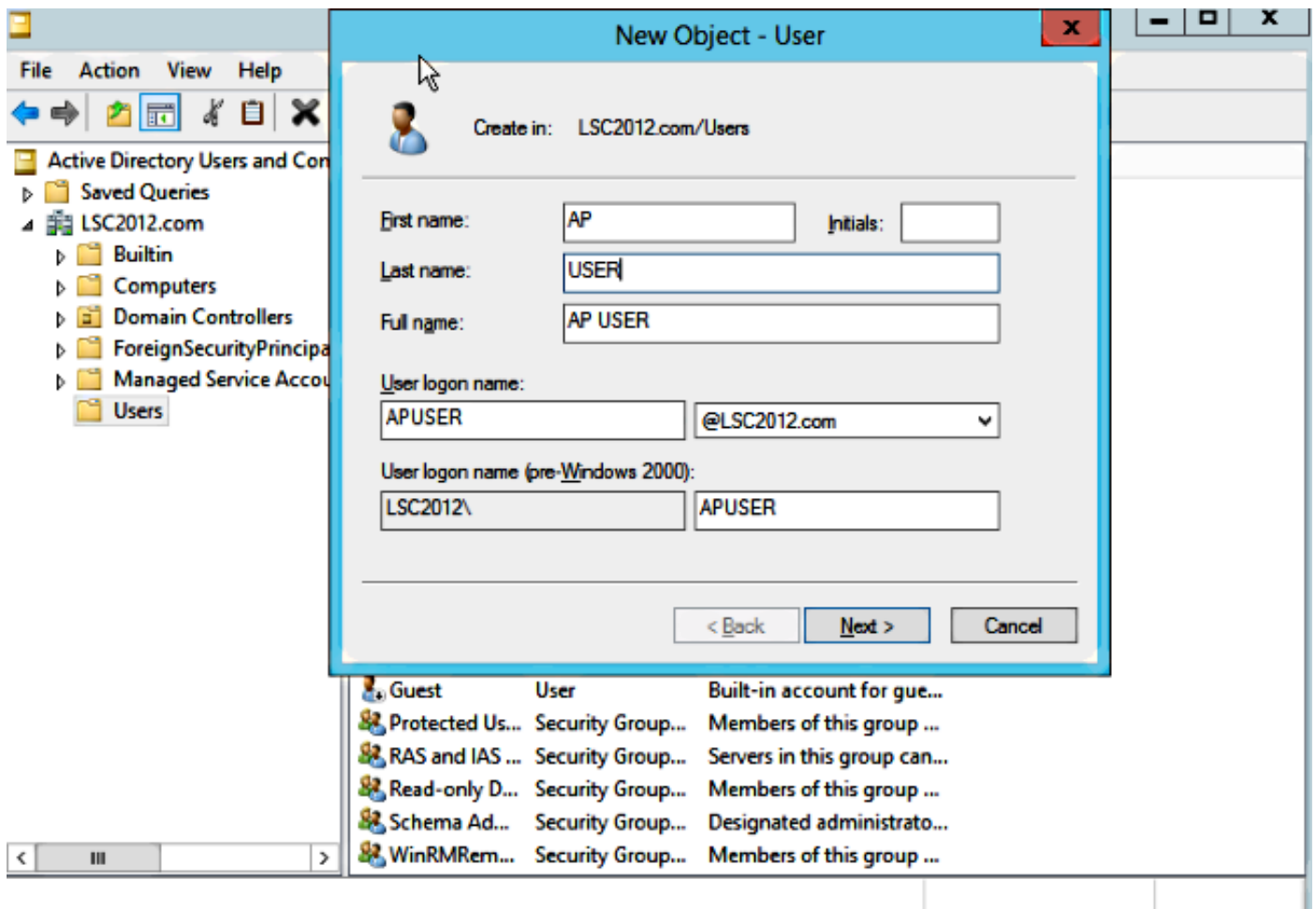


Passaggio 7. Fare clic sul menu **Start** di Microsoft Windows.

Passaggio 8. Fare clic su **Strumenti di amministrazione**.

Passaggio 9. Fare clic su **Utenti e computer di Active Directory**.

Passaggio 10. Espandere il dominio, fare clic con il pulsante destro del mouse sulla **cartella Utenti**, quindi scegliere **Nuovo oggetto > Utente**.

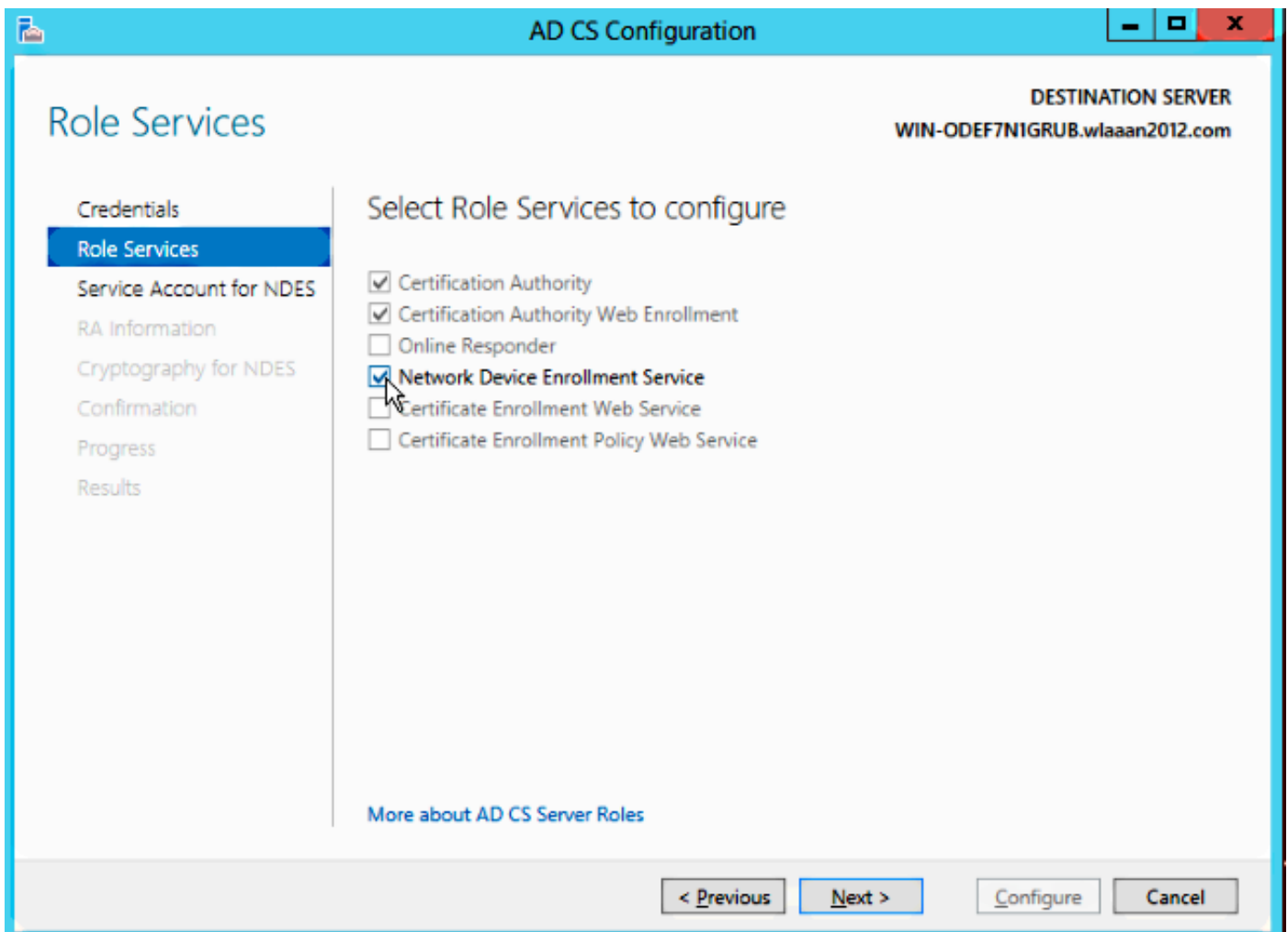


Passaggio 11. In questo esempio, il nome è **APUSER**. Una volta creato, è necessario modificare l'utente, fare clic sulla **scheda MemberOf** e impostarlo come membro del gruppo IIS_IUSRS

Le assegnazioni dei diritti utente richieste sono:

- Consenti accesso locale
- Accedi come servizio

Passaggio 12. Installare il servizio Registrazione dispositivi di rete (NDES).



- Scegliere il membro account del gruppo IIS_USRS, **APUSER** in questo esempio, come account del servizio per NDES.

Passaggio 13. Passare a Strumenti di amministrazione.

Passaggio 14. Fare clic su **Internet Information Services (IIS)**.

Passaggio 15. Espandere **Server > Siti > Sito Web predefinito > Srv certificato**.

Passaggio 16. Per **mscep** e **mscep_admin**, fare clic su **autenticazione**. Verificare che l'autenticazione anonima sia abilitata.

Passaggio 17. Fare clic con il pulsante destro del mouse su **autenticazione di Windows** e scegliere **Provider**. Assicurarsi che NT LAN Manager (NTLM) sia il primo nell'elenco.

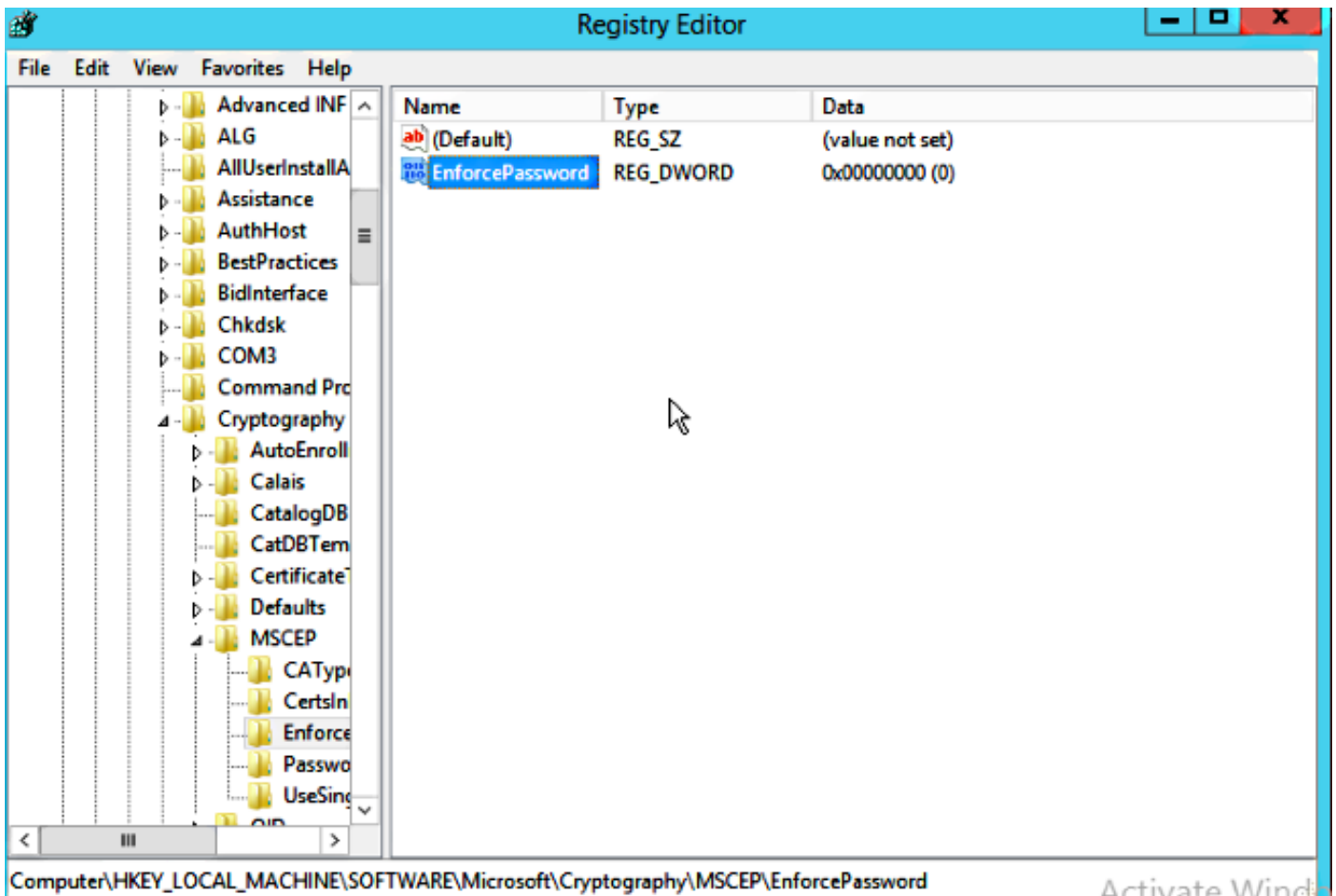
Passaggio 18. Disabilitare la richiesta di verifica dell'autenticazione nelle impostazioni del Registro di sistema. In caso contrario, SCEP (Simple Certificate Enrollment Protocol) prevede

l'autenticazione della richiesta di verifica della password, che non è supportata dal WLC.

Passaggio 19. Aprire l'applicazione regedit.

Passaggio 20. Andare su
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

Passaggio 21. Impostare EnforcePassword su 0.



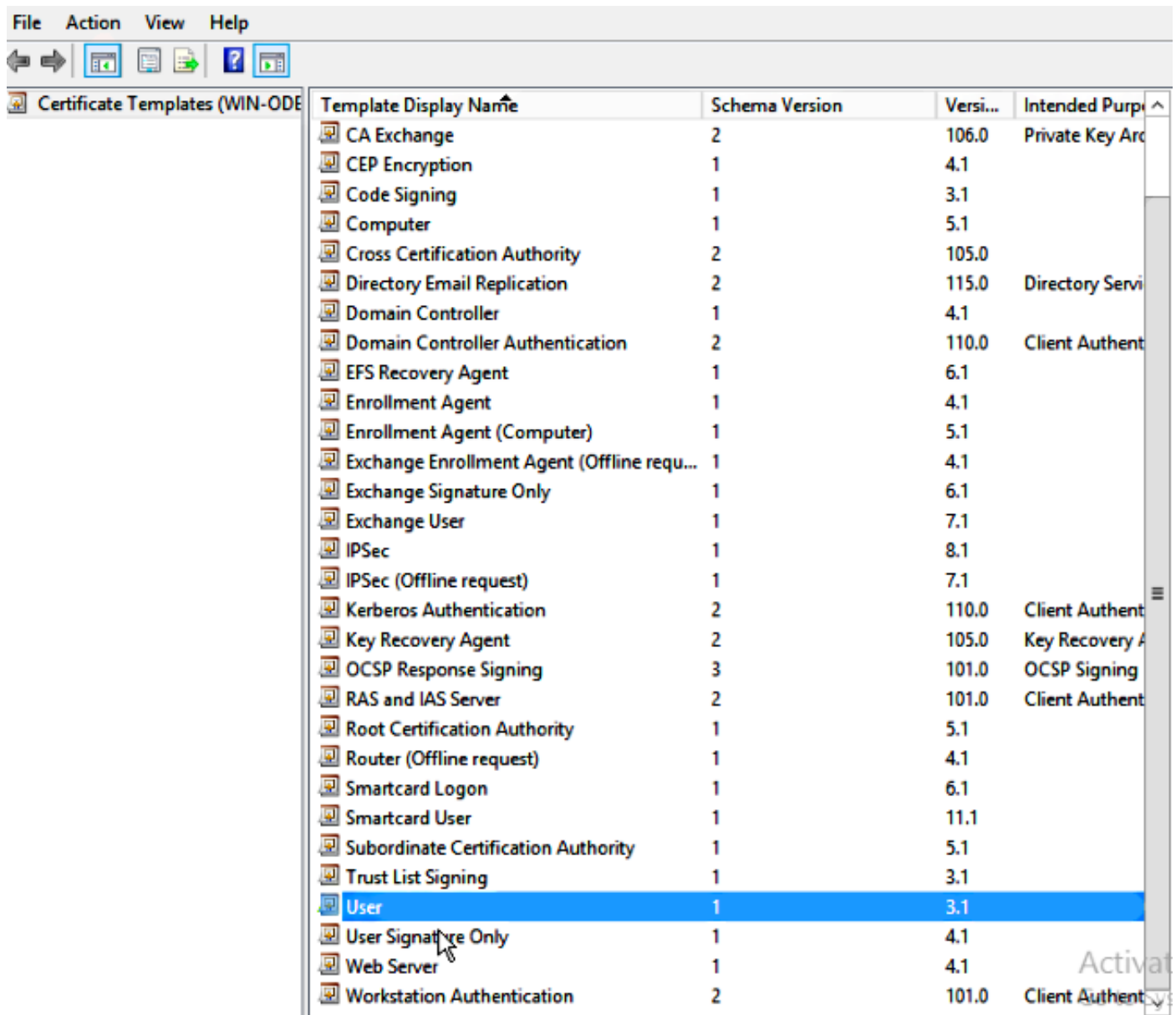
Passaggio 2. Fare clic sul menu Start di Microsoft Windows.

Passaggio 23. Digitare MMC.

Passaggio 24. Scegliere **Aggiungi/Rimuovi snap-in** dal menu File. Scegliere **Autorità di certificazione**.

Passaggio 25. Fare clic con il pulsante destro del mouse sulla **cartella dei modelli di certificato** e scegliere **Gestisci**.

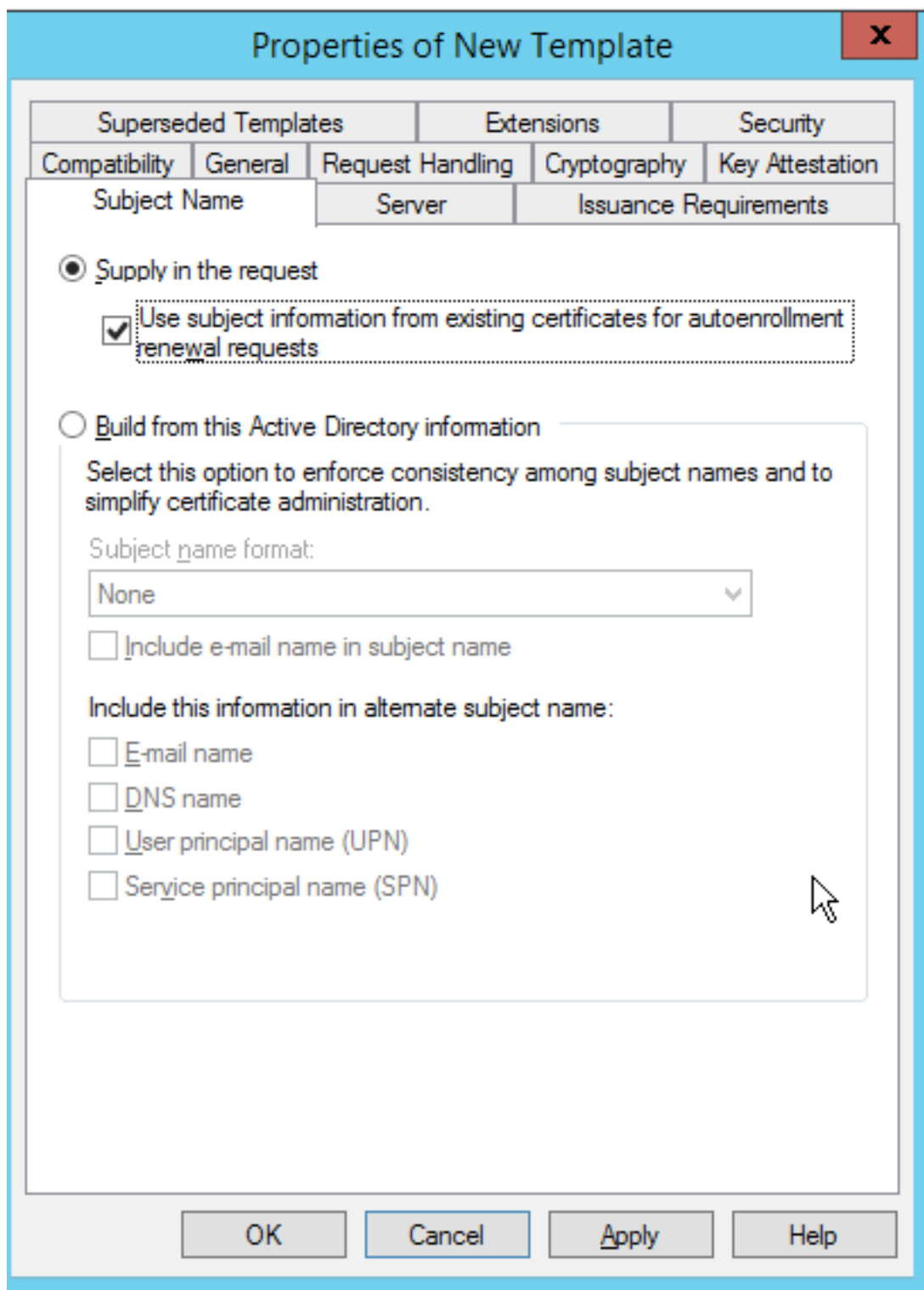
Passaggio 26. Fare clic con il pulsante destro del mouse su un modello esistente, ad esempio **Utente**, e scegliere **Duplica modello**.



Passaggio 27. Scegliere la CA come Microsoft Windows 2012 R2.

Passaggio 28. Nella scheda Generale aggiungere un nome visualizzato, ad esempio WLC, e un periodo di validità.

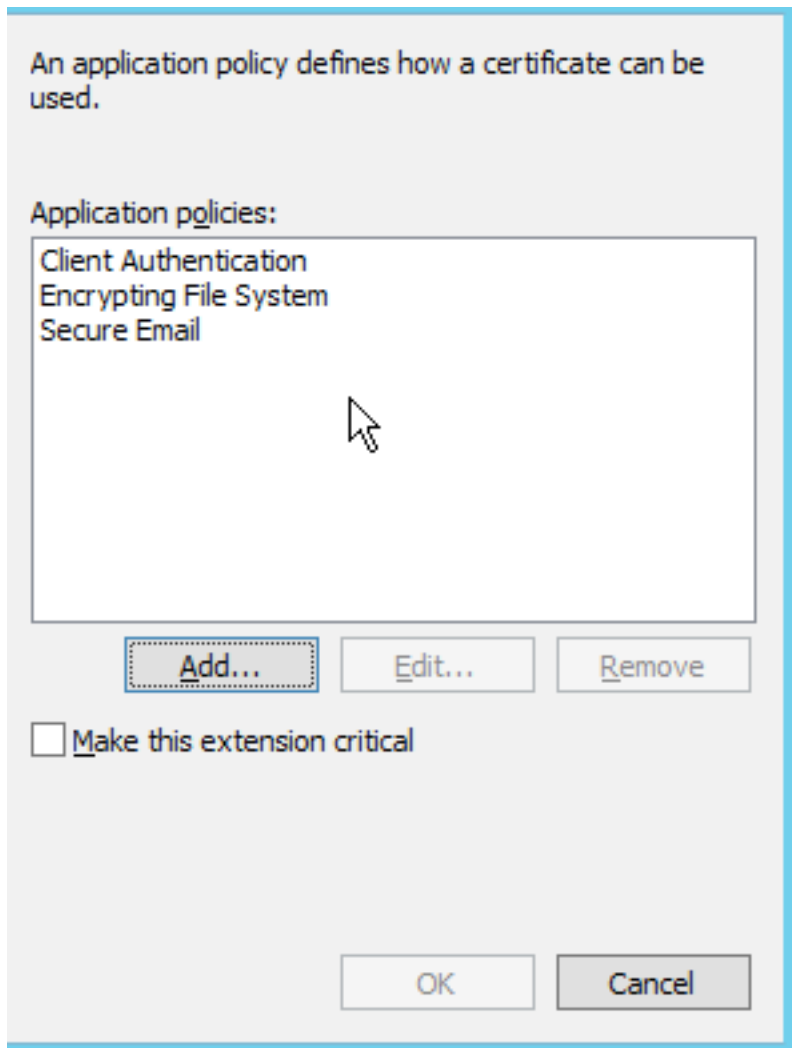
Passaggio 29. Nella scheda Nome soggetto, confermare che **Fornitura nella richiesta** è selezionata.



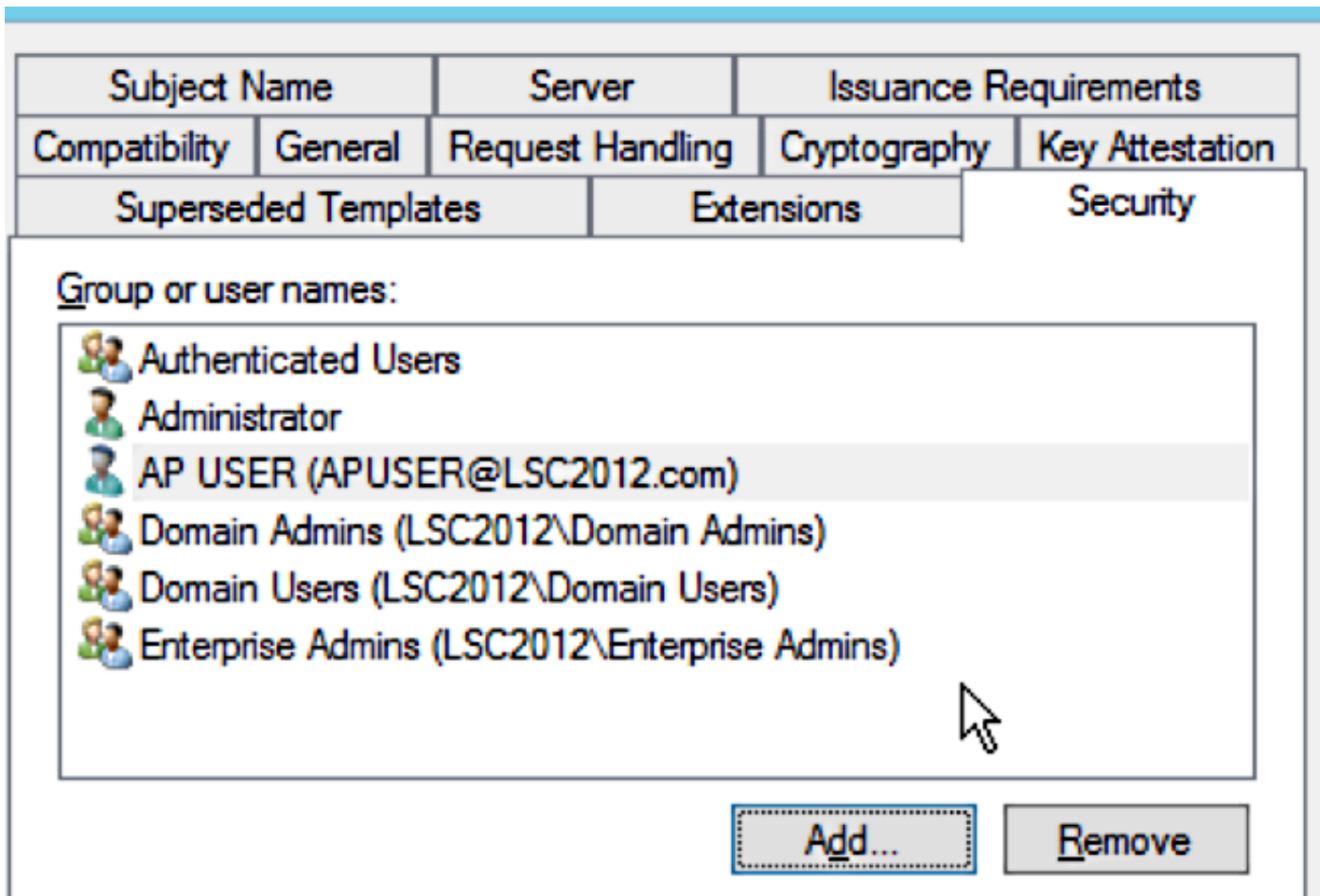
Passaggio 30. Fare clic sulla scheda **Requisiti di rilascio**. Cisco consiglia di lasciare vuoti i criteri di rilascio in un ambiente CA gerarchico tipico:

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"/> <input type="button" value="Add..."/> <input type="button" value="Remove"/></p> <hr/> <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"/>

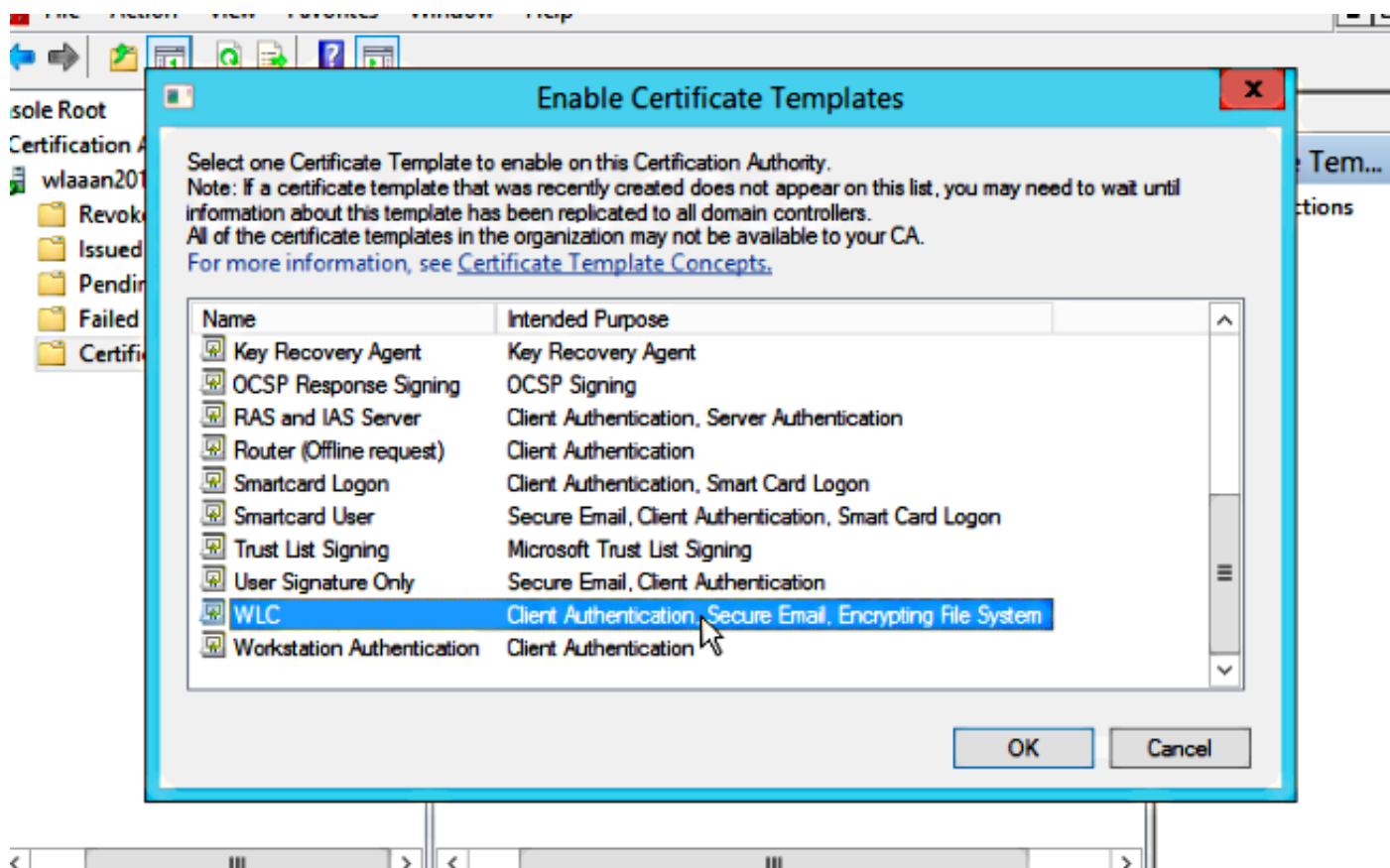
Passaggio 31. Fare clic sulla **scheda Estensioni, Criteri di applicazione**, quindi su **Modifica**. Fare clic su **Aggiungi** e verificare che l'autenticazione client sia stata aggiunta come criterio di applicazione. Fare clic su **OK**.



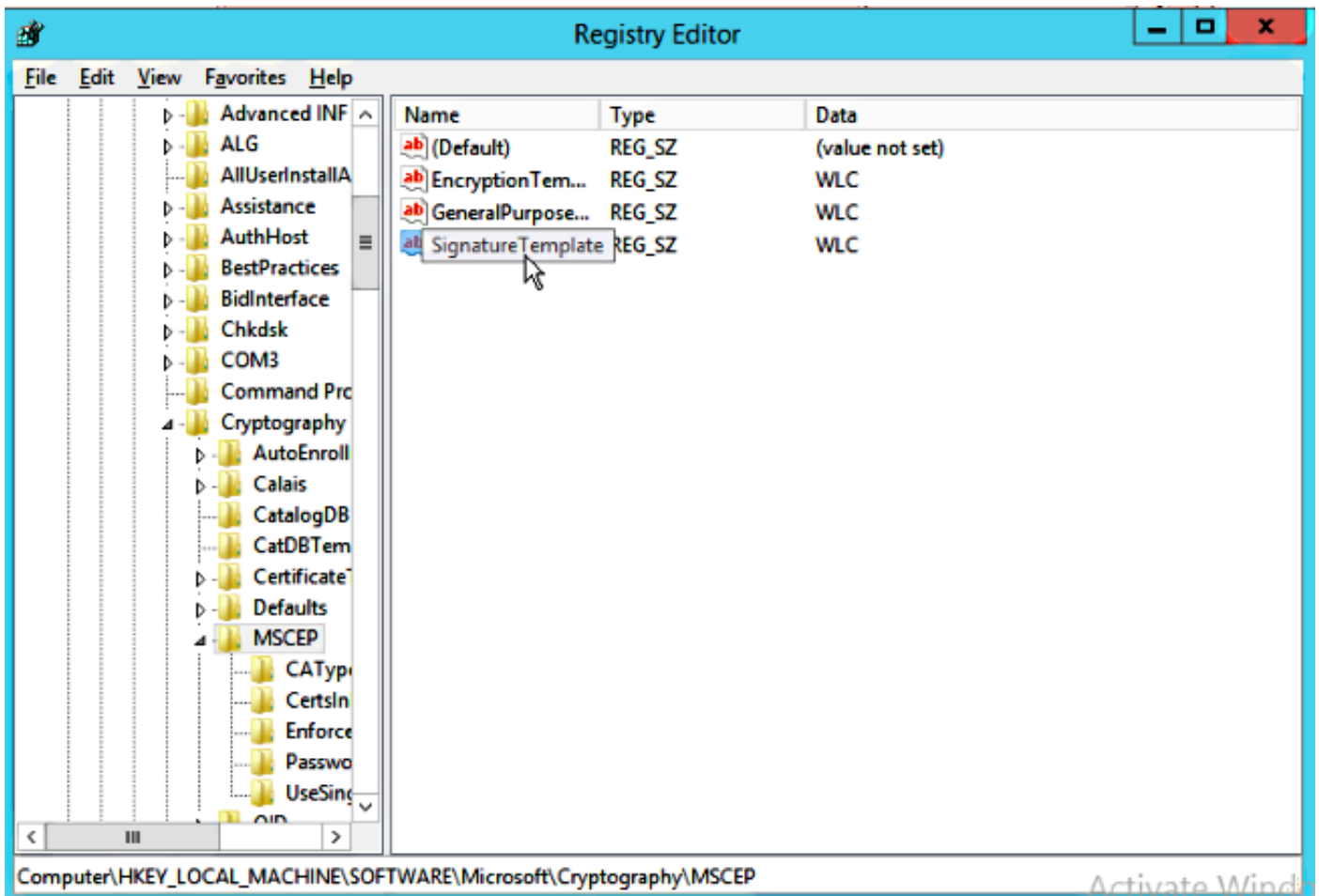
Passaggio 32. Fare clic sulla **scheda Protezione**, quindi su **Aggiungi...** Verificare che l'account del servizio SCEP definito nell'installazione del servizio NDES disponga del controllo completo del modello e fare clic su **OK**.



Passaggio 3. Tornare all'interfaccia GUI dell'Autorità di certificazione. Fare clic con il pulsante destro del mouse sulla **directory dei modelli di certificato**. Passare a **Nuovo > Modello di certificato da emettere**. Selezionare il modello WLC configurato in precedenza e fare clic su **OK**.



Passaggio 34. Modificare il modello SCEP predefinito nelle impostazioni del Registro di sistema in **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP**. Modificare le chiavi EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate da IPsec (richiesta offline) al modello WLC creato in precedenza.



Passaggio 35. Riavviare il sistema.

Configurare il WLC

Passaggio 1. Sul WLC, passare al menu Security (Sicurezza). Fare clic su **Certificati > LSC**.

Passaggio 2. Selezionare la casella di controllo **Abilita LSC** sul controller.

Passaggio 3. Immettere l'URL di Microsoft Windows Server 2012. Per impostazione predefinita, viene aggiunto **/certsrv/mscep/mscep.dll**.

Passaggio 4. Inserire i dettagli nella sezione **Parametri**.

Passaggio 5. Applicare la modifica.

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

Passaggio 6. Fare clic sulla freccia blu sulla linea CA superiore e scegliere **Aggiungi**. Lo stato dovrebbe essere modificato da **Non presente** a **Presente**.

Passaggio 7. Fare clic sulla **scheda Provisioning AP**.

The screenshot shows the Cisco SCA interface for configuring Local Significant Certificates (LSC). The left sidebar lists various security settings, with 'Certificate' expanded to show 'LSC'. 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 the 'AP Ethernet MAC Addresses' section, which includes an empty text input field and an 'Add' button. The 'MAC Address' label is positioned below the input field.

Passaggio 8. Selezionare la casella di controllo **Abilita** in AP Provisioning e fare clic su **Aggiorna**.

Passaggio 9. Riavviare i punti di accesso se non sono stati riavviati.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Il punto di accesso, dopo il riavvio, si unisce e visualizza LSC come tipo di certificato nel menu Wireless.

Wireless

All APs Entries 1 - 2 of 2

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

Number of APs: 2

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

Windows taskbar: ENG 6:41 PM, LUK 12/16/2014

Nota: Dopo la versione 8.3.112, i punti di accesso MIC non possono più unirsi se il protocollo LSC è abilitato. La funzione di conteggio "tentativi di LSC" ha pertanto un utilizzo limitato.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.