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

Sommario

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

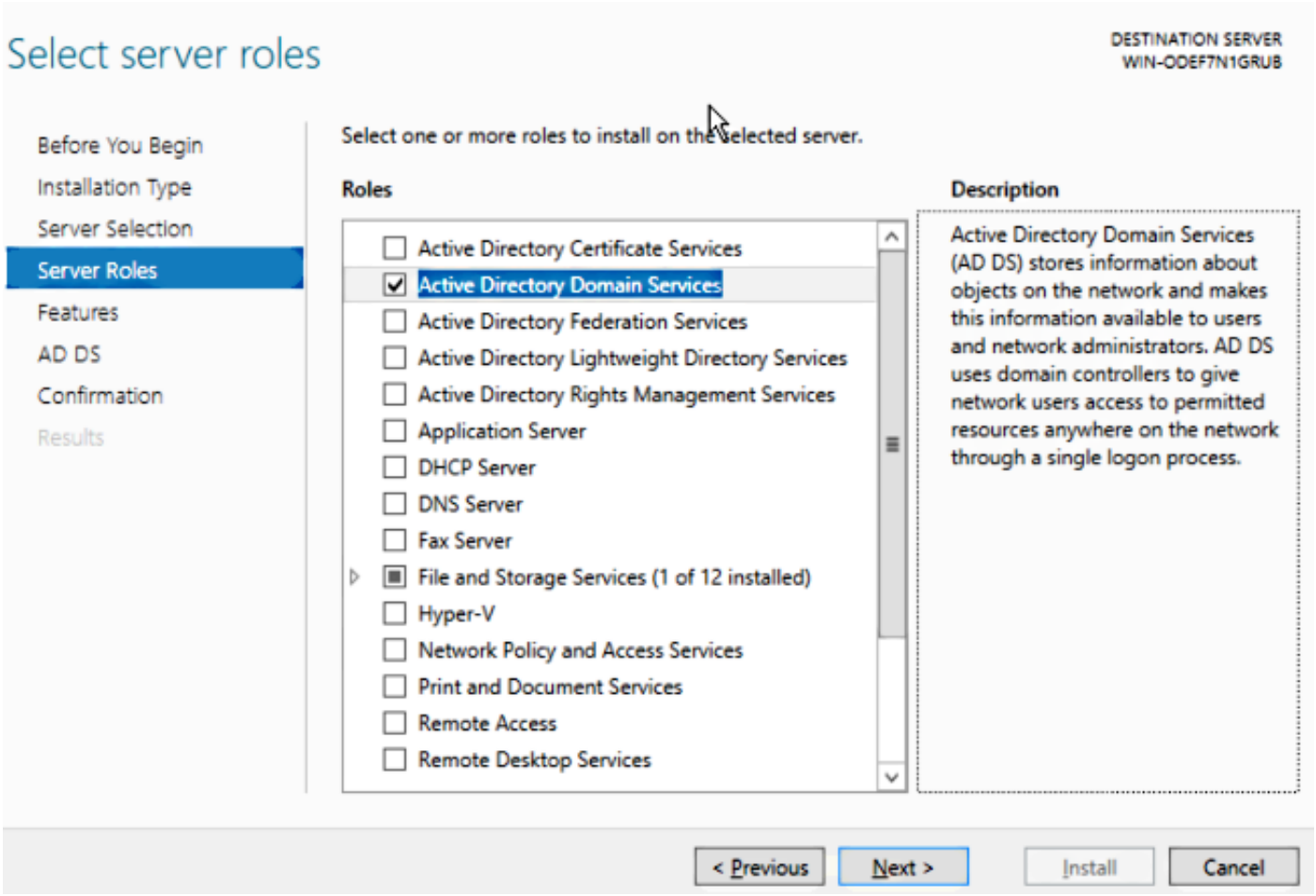
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

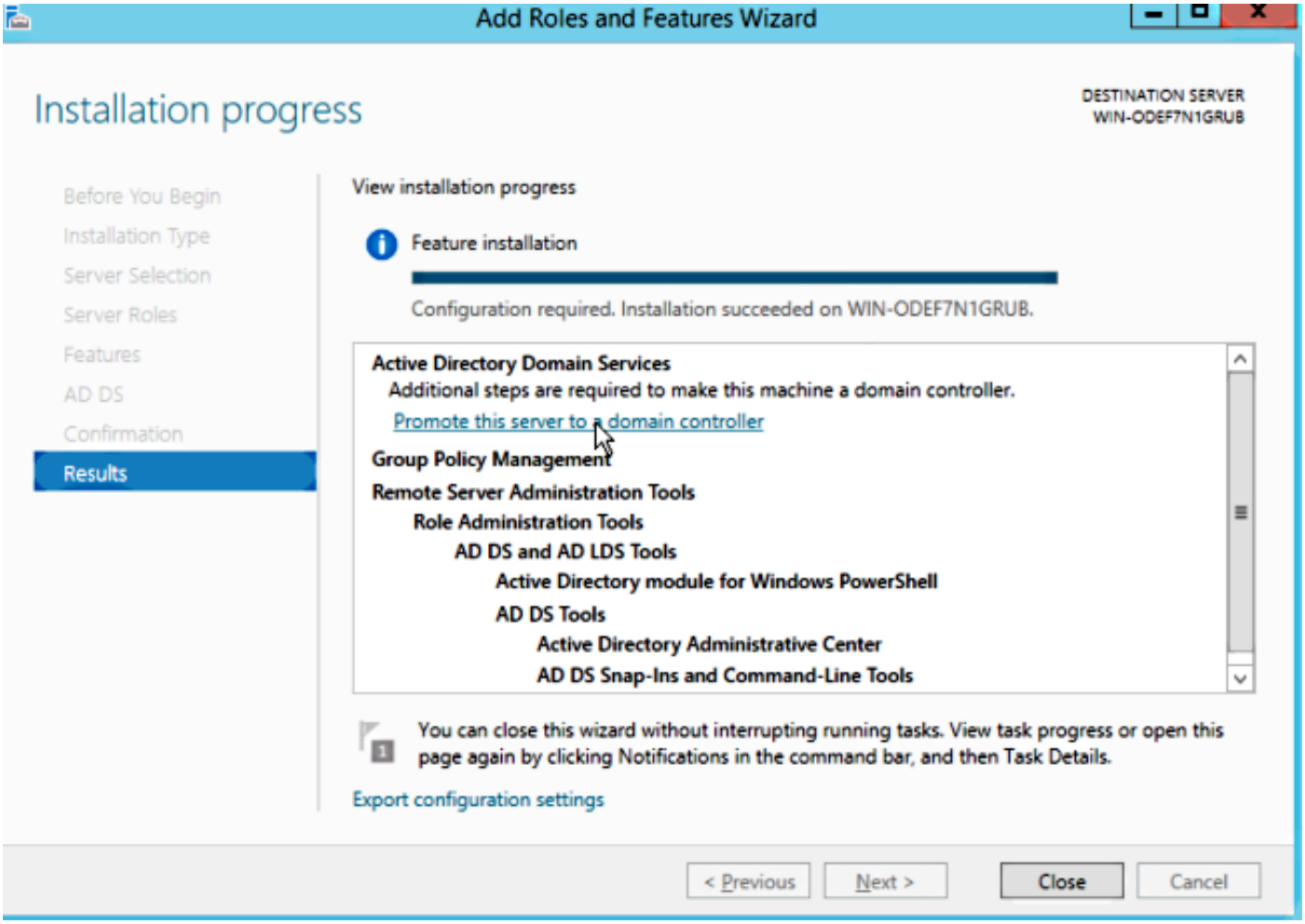
Configurazione server di Microsoft Windows

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.

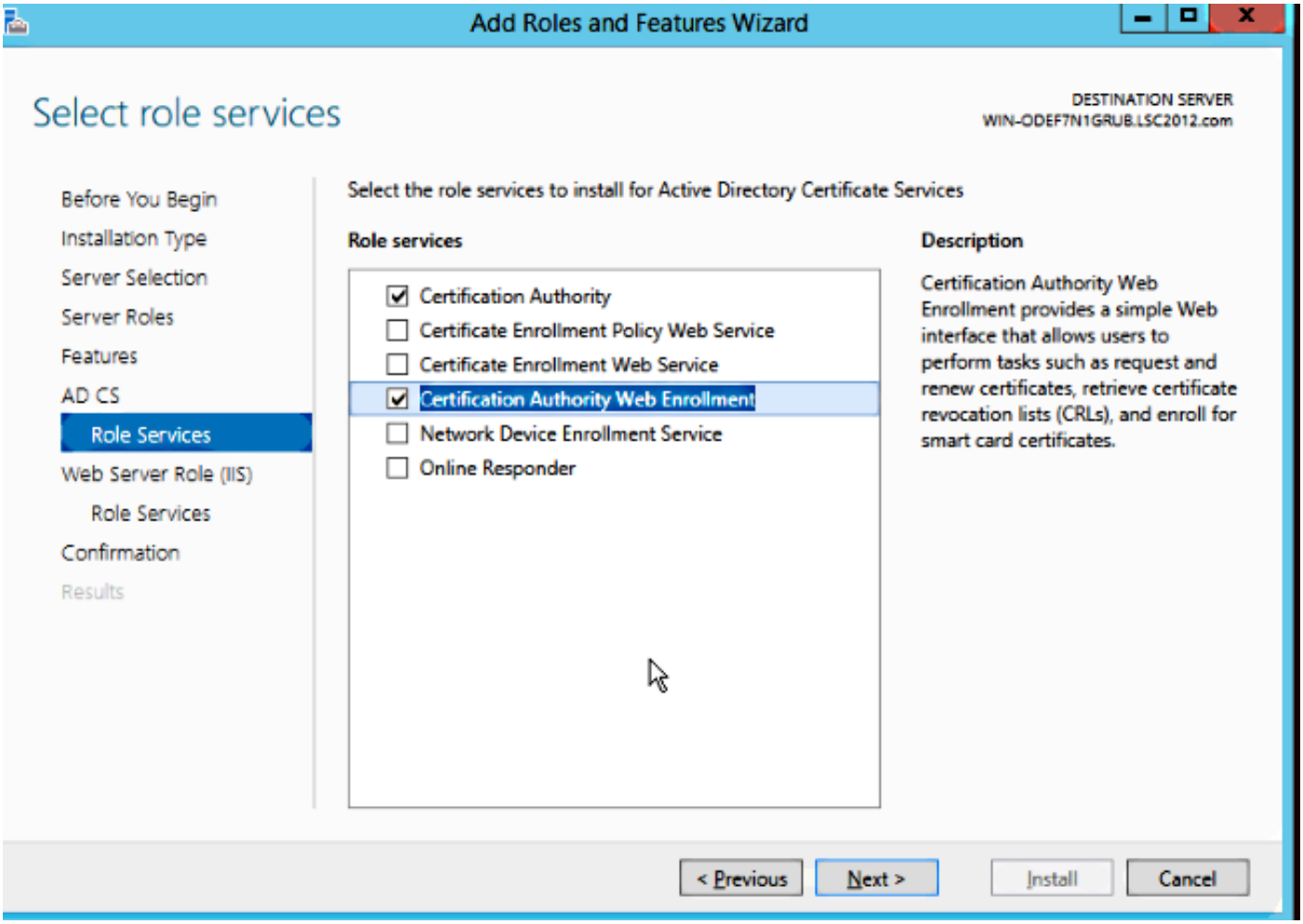


Passaggio 2. Dopo l'installazione, è necessario innalzare di livello il server a controller di dominio.

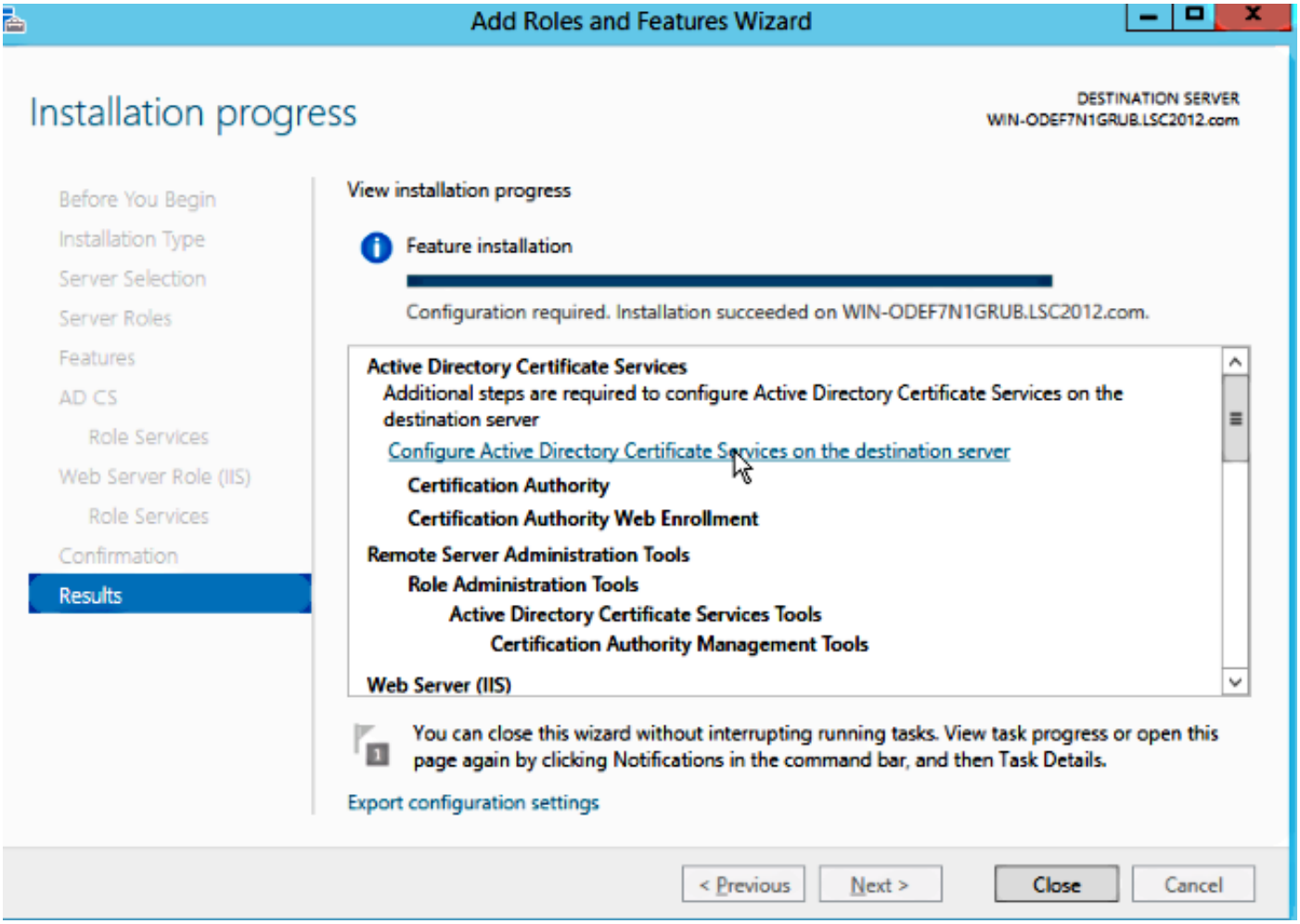


Passaggio 3. Poiché si tratta di una nuova impostazione, è possibile configurare una nuova foresta. ma in genere, nelle implementazioni esistenti, è sufficiente configurare questi punti su un controller di dominio. In questa pagina è possibile scegliere il dominio **LSC2012.com**. In questo modo viene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

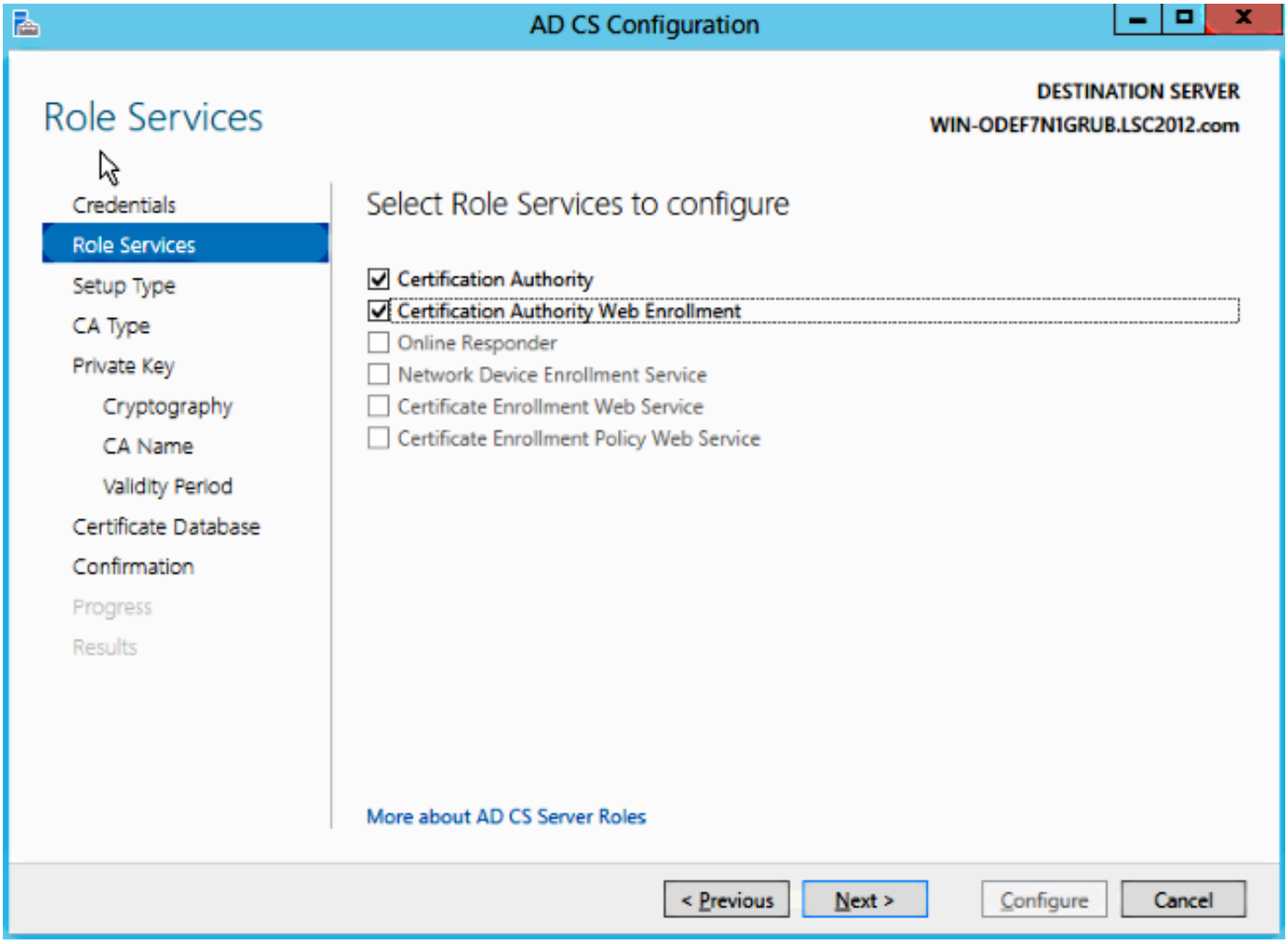
Passaggio 4. Dopo il riavvio, installare il servizio Autorità di certificazione (CA) e la registrazione Web.



Passaggio 5. Configurarle.



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

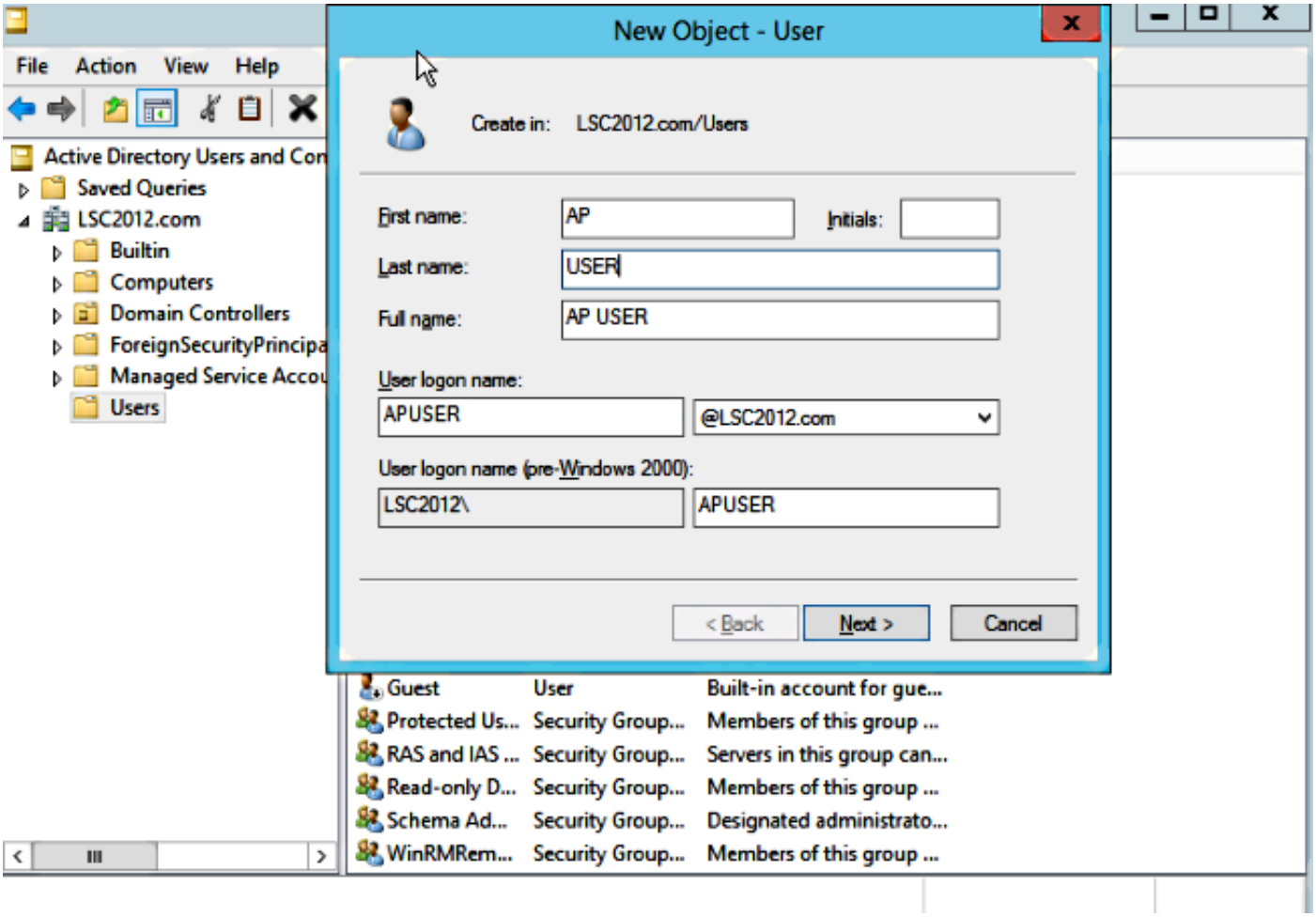


Passaggio 7. Fare clic sul **menu Start di Microsoft Windows**.

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**.



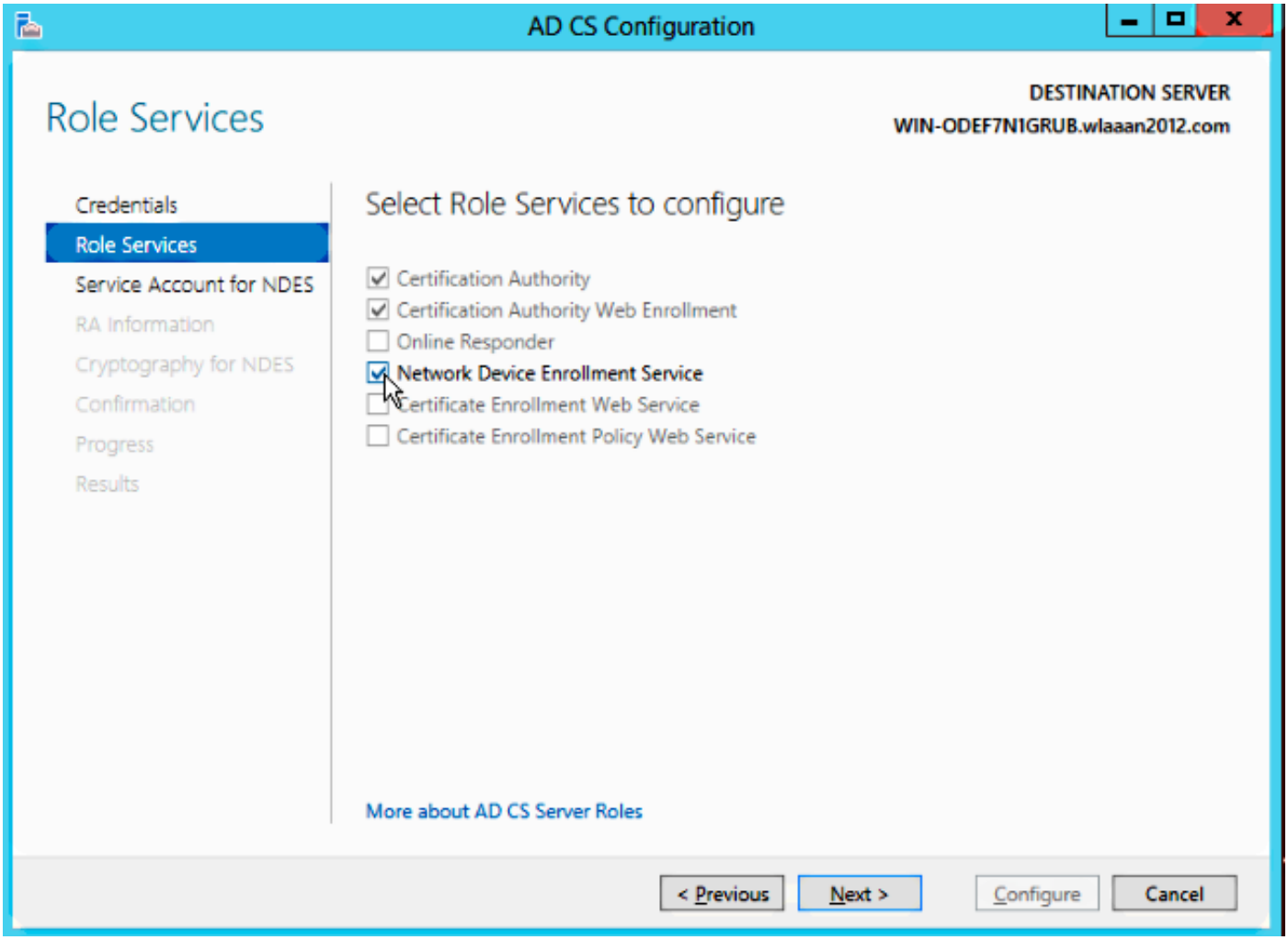
Passaggio 11. In questo esempio, il nome è **APUSER**. Una volta creato, è necessario modificare l'utente, fare clic sulla **scheda MemberOf** e impostarlo come membro del gruppo IIS_IUSRS

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.

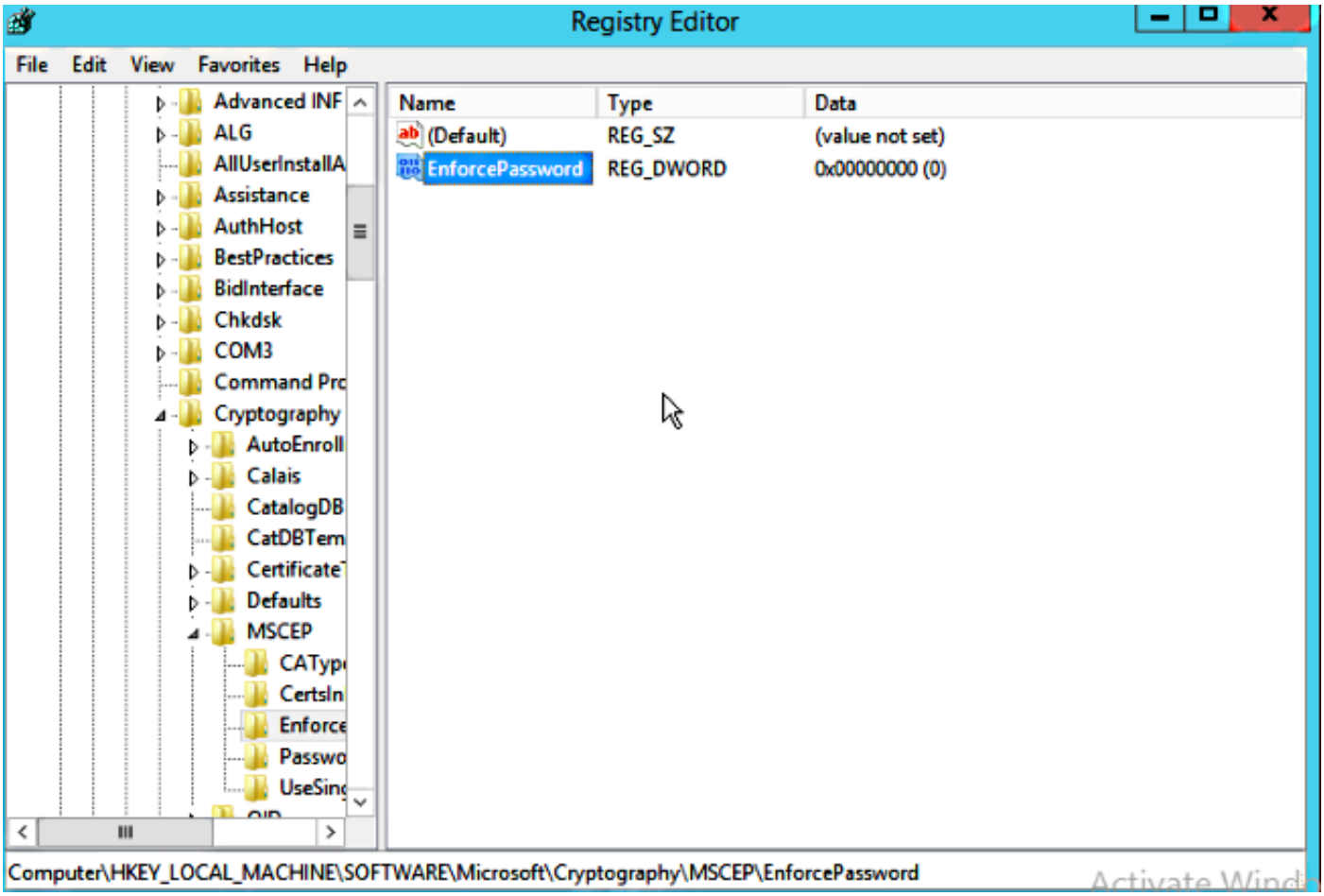
Passaggio 18. Disabilitare la richiesta di verifica dell'autenticazione nelle impostazioni del Registro di sistema. In caso contrario, SCEP (Simple Certificate Enrollment Protocol) prevede

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**.



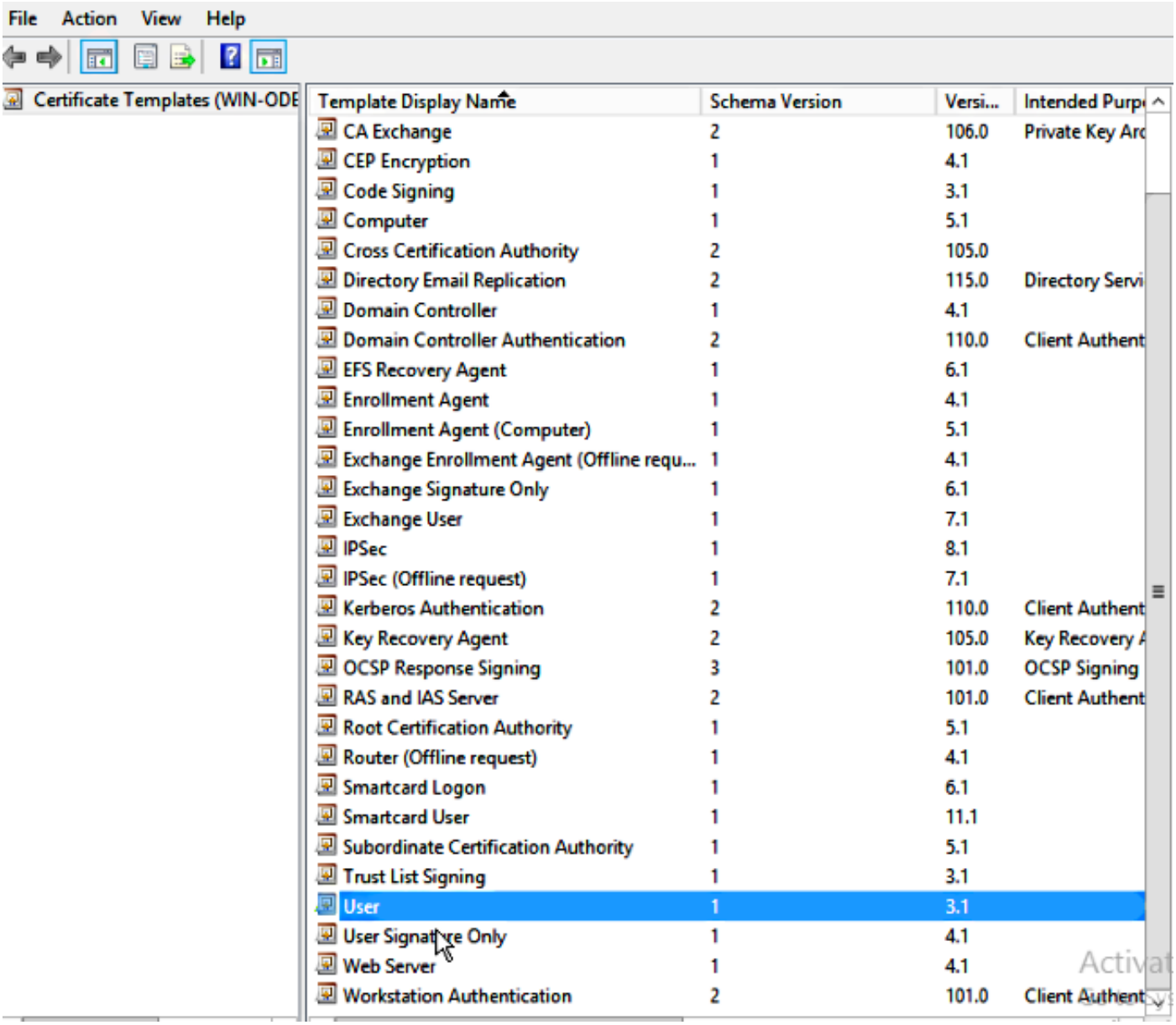
Passaggio 2. Fare clic sul **menu Start di Microsoft Windows**.

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**.

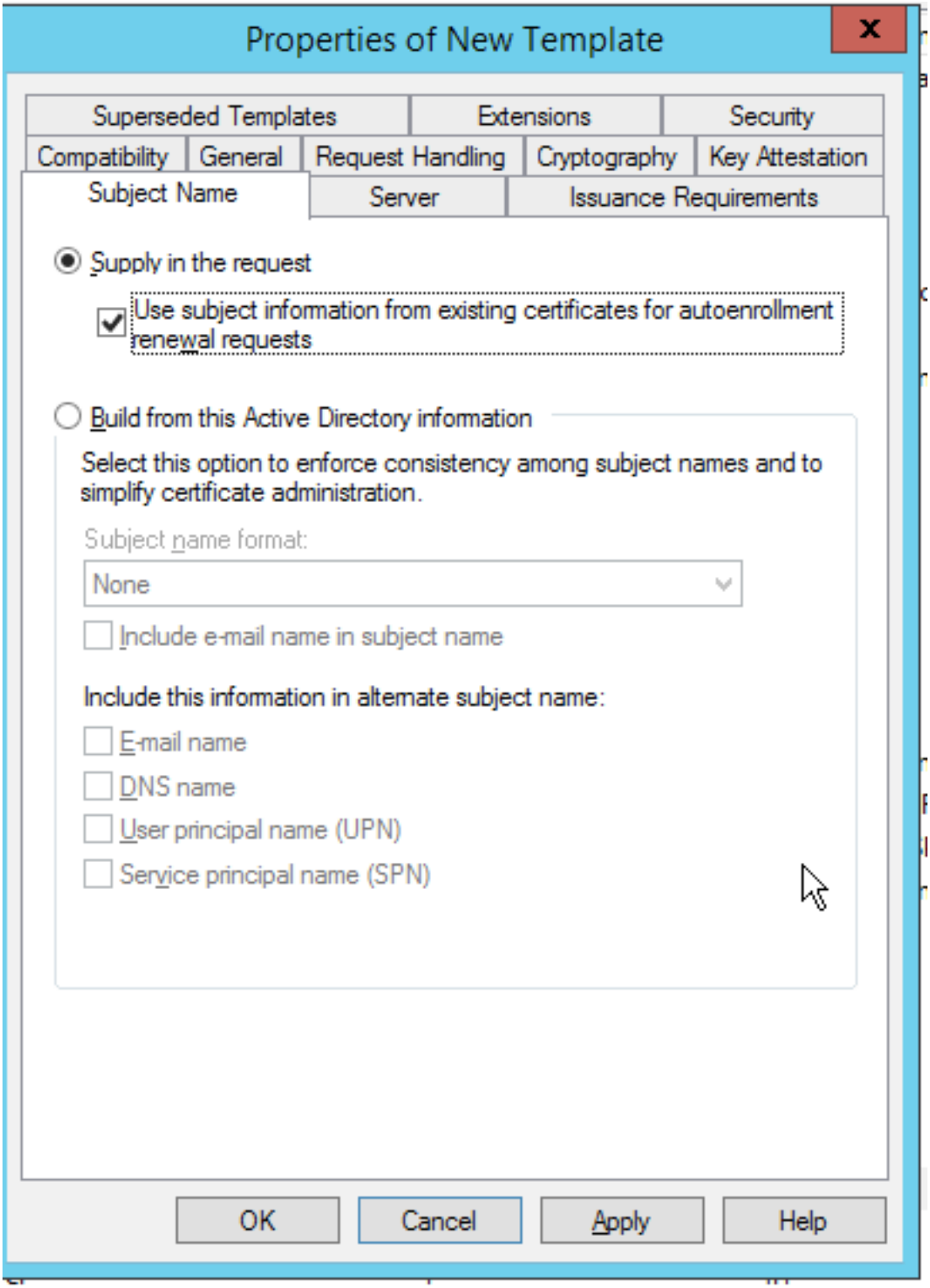
Passaggio 26. Fare clic con il pulsante destro del mouse su un modello esistente, ad esempio Utente, e scegliere **Duplica modello**.



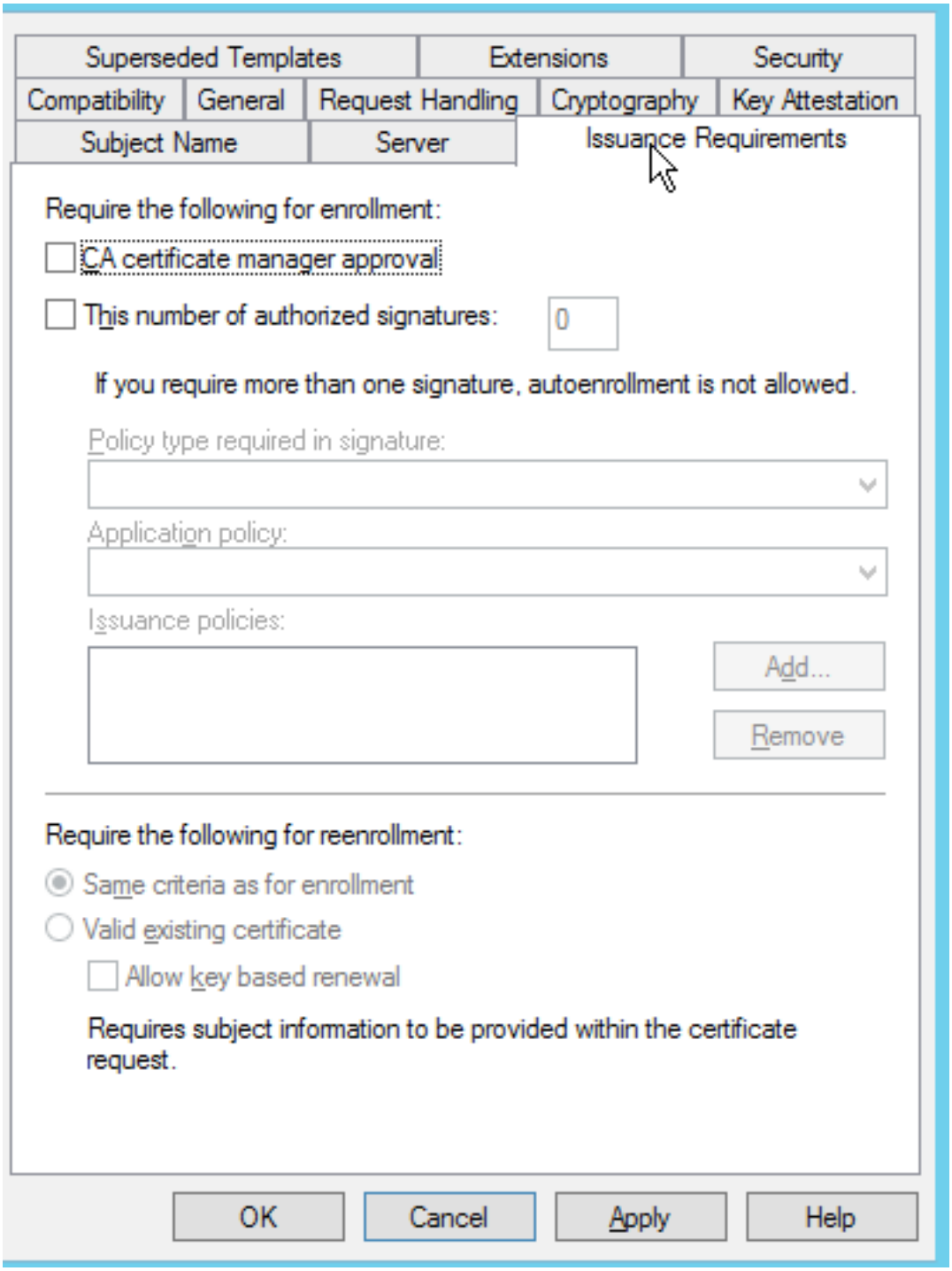
Passaggio 27. Scegliere la CA come Microsoft Windows 2012 R2.

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

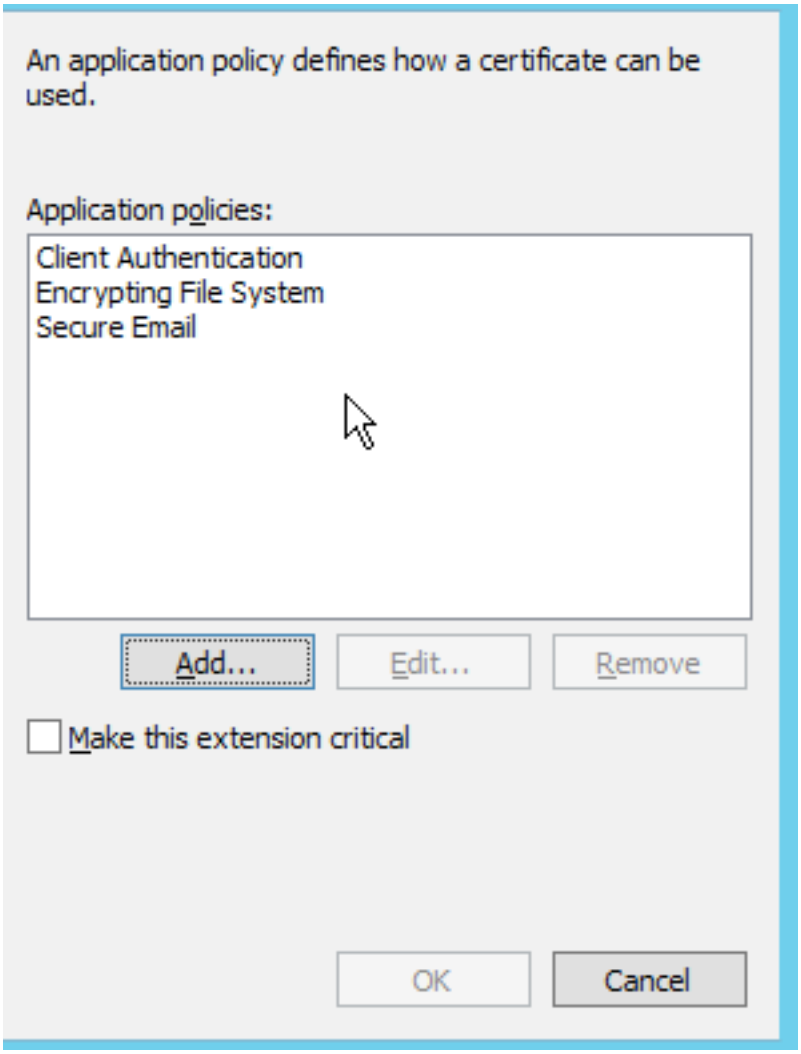
Passaggio 29. Nella scheda Nome soggetto, confermare che **Fornitura nella richiesta** è selezionata.



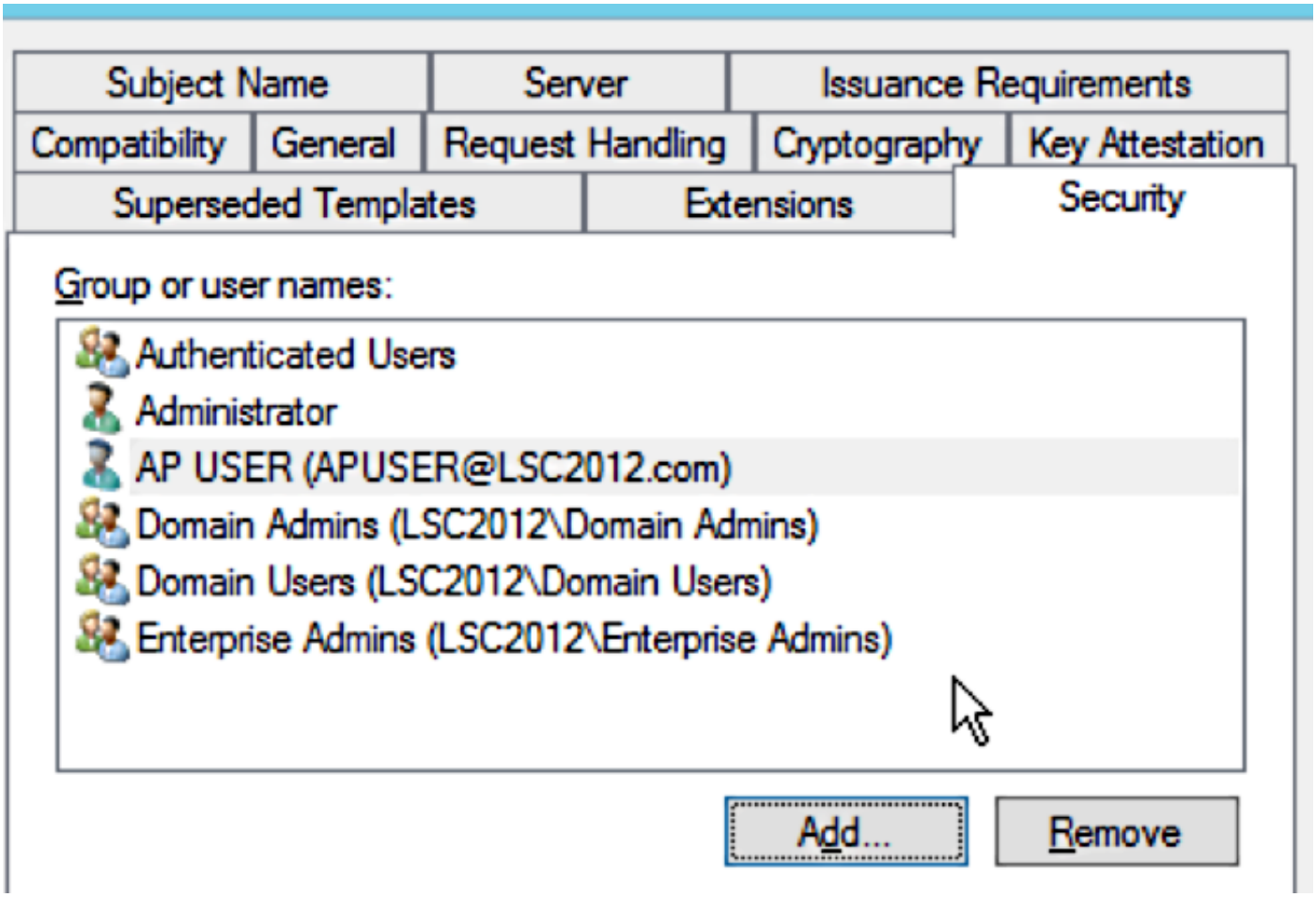
Passaggio 30. Fare clic sulla scheda **Requisiti di rilascio**. Cisco consiglia di lasciare vuoti i criteri di rilascio in un ambiente CA gerarchico tipico:



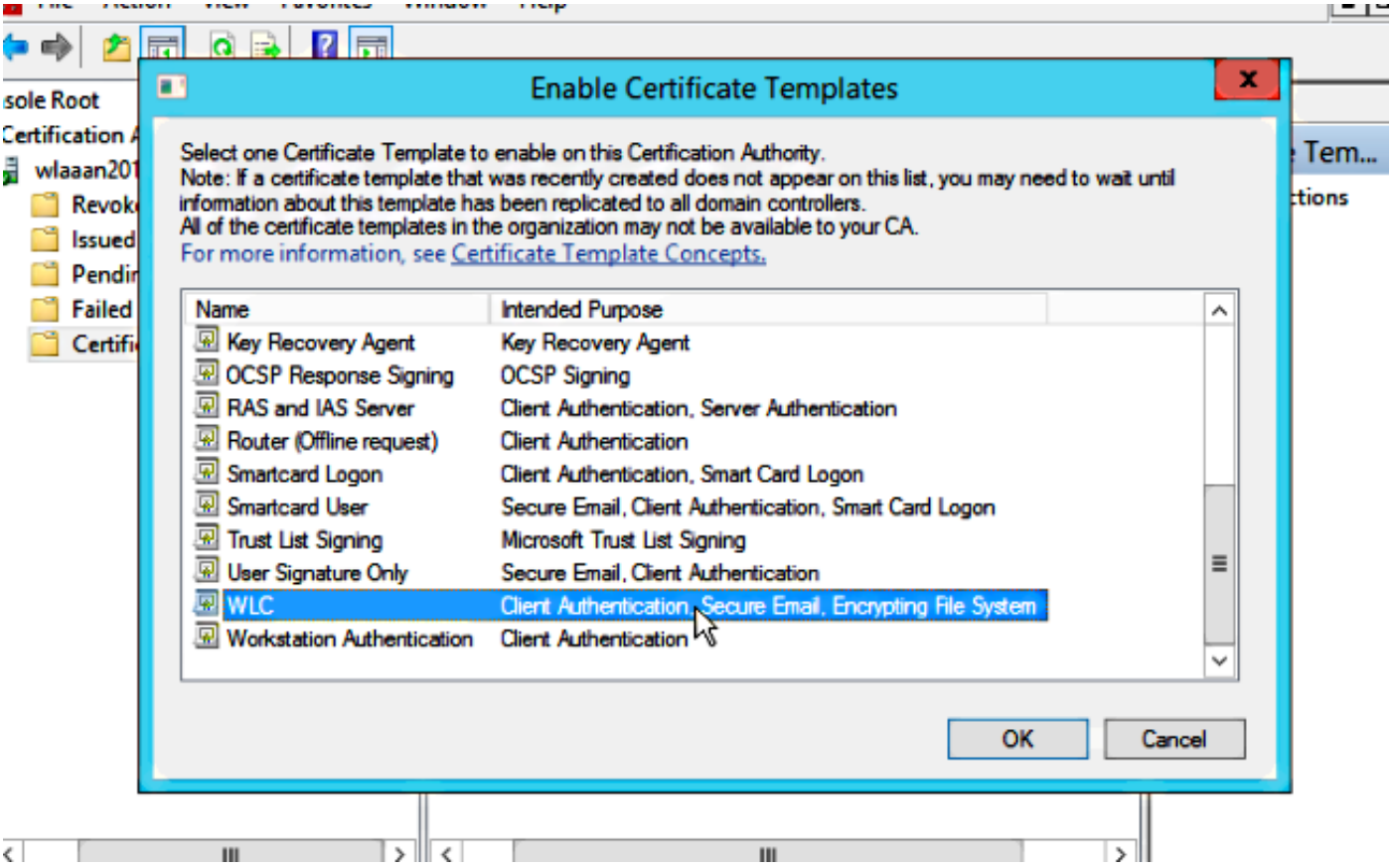
Passaggio 31. Fare clic sulla **scheda Estensioni**, **Criteri di applicazione**, quindi su **Modifica**. Fare clic su **Aggiungi** e verificare che l'autenticazione client sia stata aggiunta come criterio di applicazione. Fare clic su **OK**.



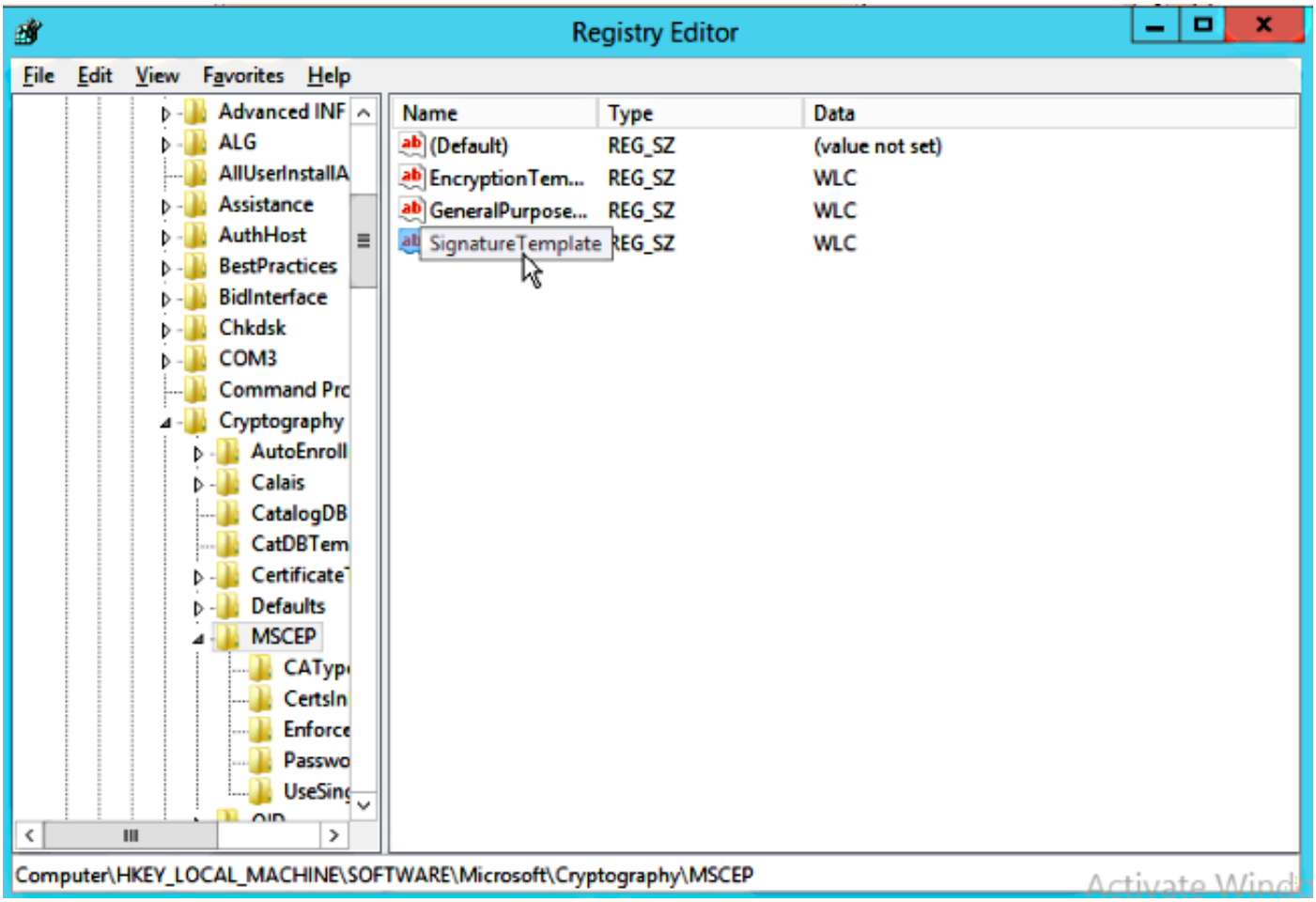
Passaggio 32. Fare clic sulla **scheda Protezione**, quindi su **Aggiungi...**. Verificare che l'account del servizio SCEP definito nell'installazione del servizio NDES disponga del controllo completo del modello e fare clic su **OK**.



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

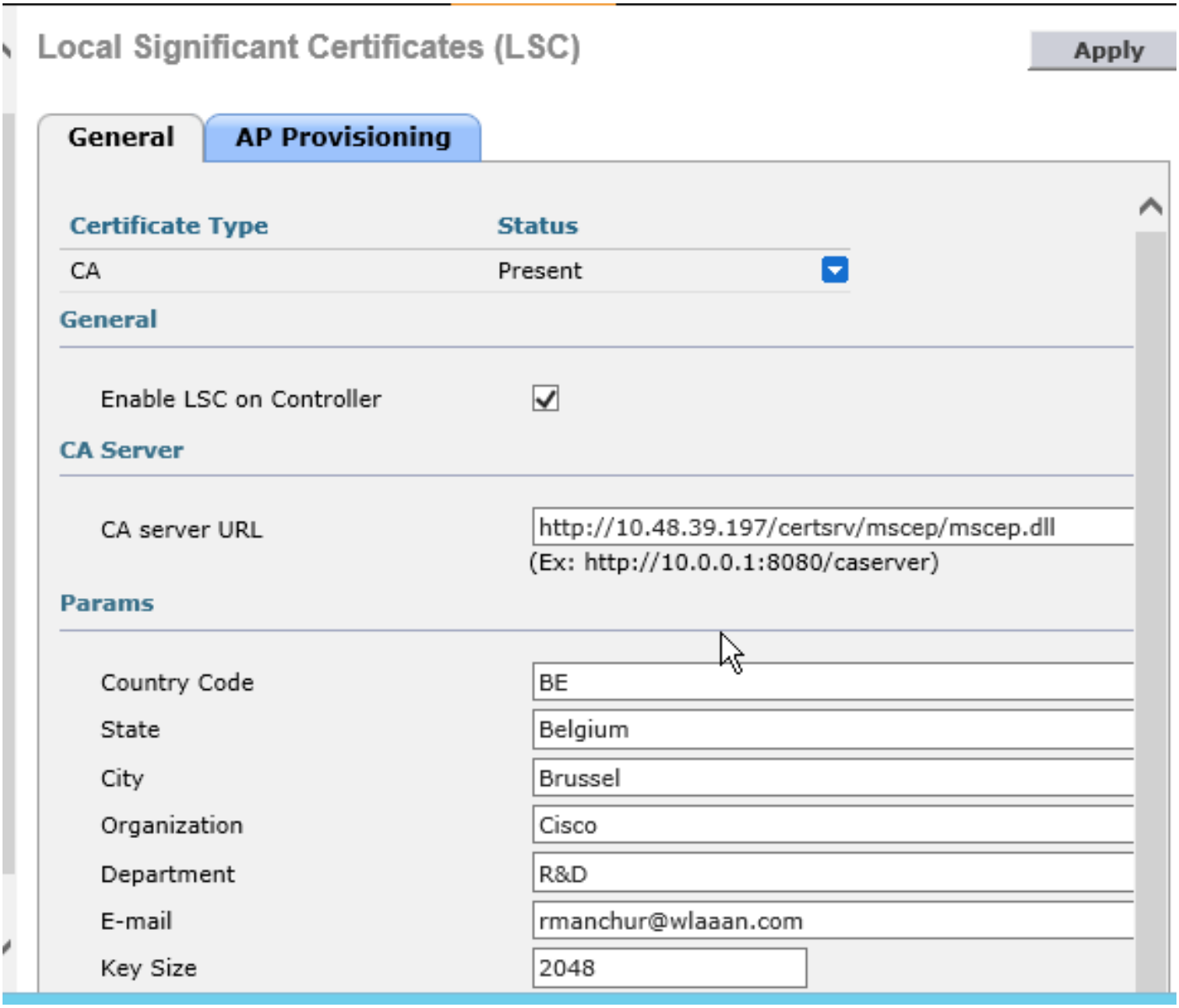
Passaggio 1. Sul WLC, passare al menu Security (Sicurezza). Fare clic su **Certificati > LSC**.

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**.

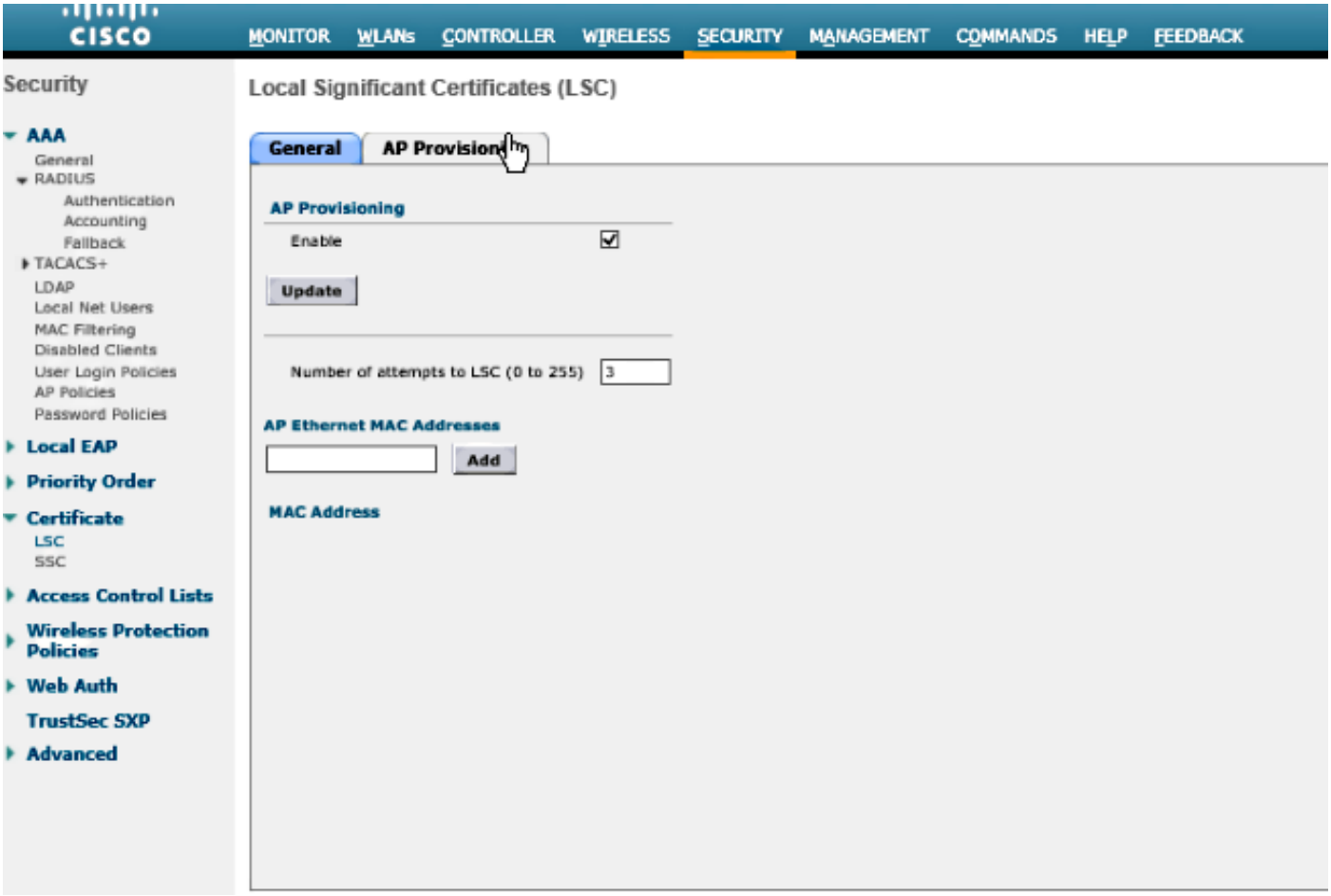
Passaggio 4. Inserire i dettagli nella sezione **Parametri**.

Passaggio 5. Applicare la modifica.



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**.



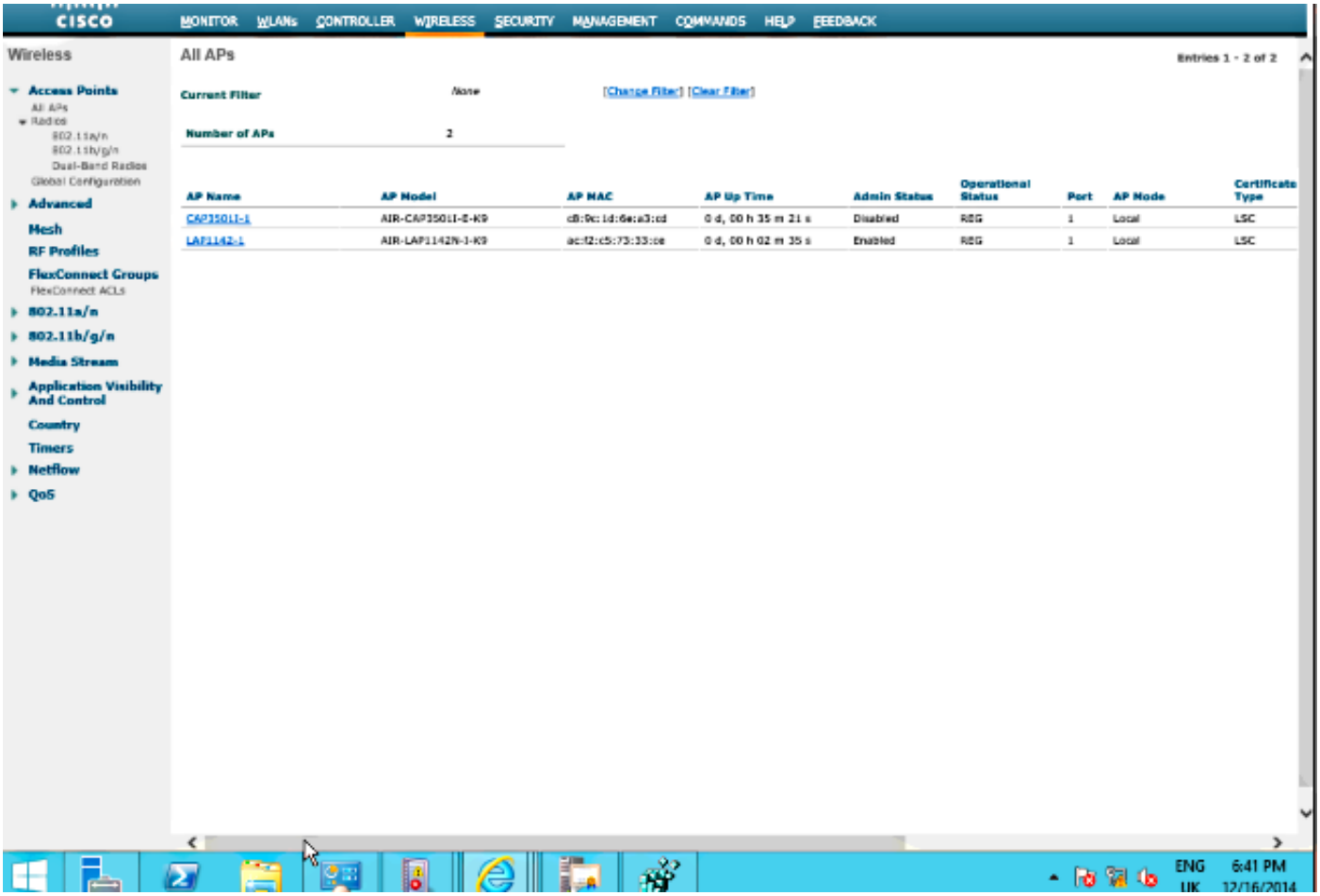
Passaggio 8. Selezionare la casella di controllo **Abilita** in AP Provisioning e fare clic su **Aggiorna**.

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.



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.