

# Configurazione di 802.1X sui punti di accesso per PEAP o EAP-TLS con LSC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[CA SCEP di Windows Server 2016](#)

[Configurare il modello di certificato e il Registro di sistema](#)

[Configurazione di LSC su 9800](#)

[Procedura di configurazione GUI di AP LSC](#)

[Passi di configurazione CLI di AP LSC](#)

[Verifica LSC AP](#)

[Risoluzione dei problemi di provisioning LSC](#)

[Autenticazione 802.1X cablata AP tramite LSC](#)

[Passi di configurazione dell'autenticazione 802.1x per dispositivi cablati AP](#)

[Configurazione GUI autenticazione 802.1x cablata AP](#)

[Configurazione CLI autenticazione 802.1x cablata AP](#)

[Configurazione switch di autenticazione 802.1x cablato AP](#)

[Installazione certificato server RADIUS](#)

[Verifica autenticazione 802.1x cablata AP](#)

[Risoluzione dei problemi di autenticazione 802.1X](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come autenticare i Cisco Access Point sulla porta dello switch con i metodi 802.1X PEAP o EAP-TLS.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Controller wireless

- Access Point
- Interruttore
- server ISE
- Autorità di certificazione.

## Componenti usati

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

- Controller wireless: C9800-40-K9 con esecuzione il 17.09.02
- Access point: C9117AXI-D
- Switch: C9200L-24P-4G con versione 17.06.04
- Server AAA: ISE-VM-K9 con 3.1.0.518
- Autorità di certificazione: Windows Server 2016

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.

## Premesse

Se si desidera che i punti di accesso eseguano l'autenticazione con la porta dello switch utilizzando 802.1X, per impostazione predefinita utilizzano il protocollo di autenticazione EAP-FAST che non richiede certificati. Se si desidera che gli access point utilizzino il metodo PEAP-mschapv2 (che usa le credenziali sul lato AP ma un certificato sul lato RADIUS) o il metodo EAP-TLS (che usa i certificati su entrambi i lati), è necessario prima configurare LSC. È l'unico modo per effettuare il provisioning di un certificato di attendibilità/radice su un punto di accesso (e anche di un certificato di dispositivo nel caso di EAP-TLS). Non è possibile che l'access point esegua PEAP e ignori la convalida lato server. Questo documento descrive inizialmente la configurazione di LCS e quindi il lato configurazione 802.1X.

Utilizzare un LSC se si desidera che l'infrastruttura a chiave pubblica (PKI) fornisca una maggiore protezione, che abbia il controllo dell'Autorità di certificazione (CA) e che definisca criteri, restrizioni e utilizzi per i certificati generati.

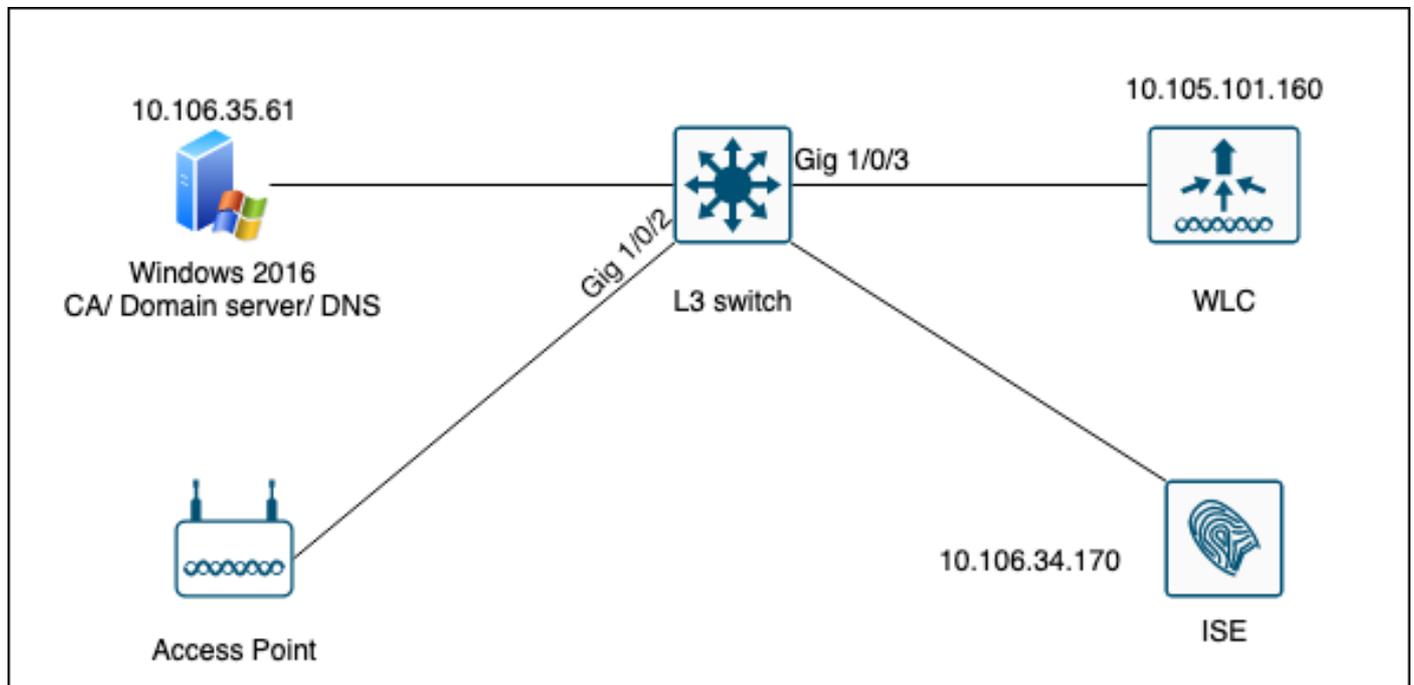
Con LSC, il controller ottiene un certificato rilasciato dalla CA. Un access point non comunica direttamente con il server CA, ma il WLC richiede certificati per conto degli access point che vengono aggiunti. I dettagli del server CA devono essere configurati sul controller e devono essere accessibili.

Il controller utilizza il protocollo SCEP (Simple Certificate Enrollment Protocol) per inoltrare alla CA le richieste di certificati generate sui dispositivi e utilizza nuovamente SCEP per ottenere i certificati firmati dalla CA.

SCEP è un protocollo di gestione dei certificati utilizzato dai client PKI e dai server CA per

supportare la registrazione e la revoca dei certificati. È ampiamente utilizzato in Cisco e supportato da molti server CA. In SCEP, HTTP viene utilizzato come protocollo di trasporto per i messaggi PKI. L'obiettivo principale di SCEP è il rilascio sicuro di certificati ai dispositivi di rete.

## Esempio di rete



## Configurazione

Ci sono due cose da configurare principalmente: SCEP CA e il 9800 WLC.

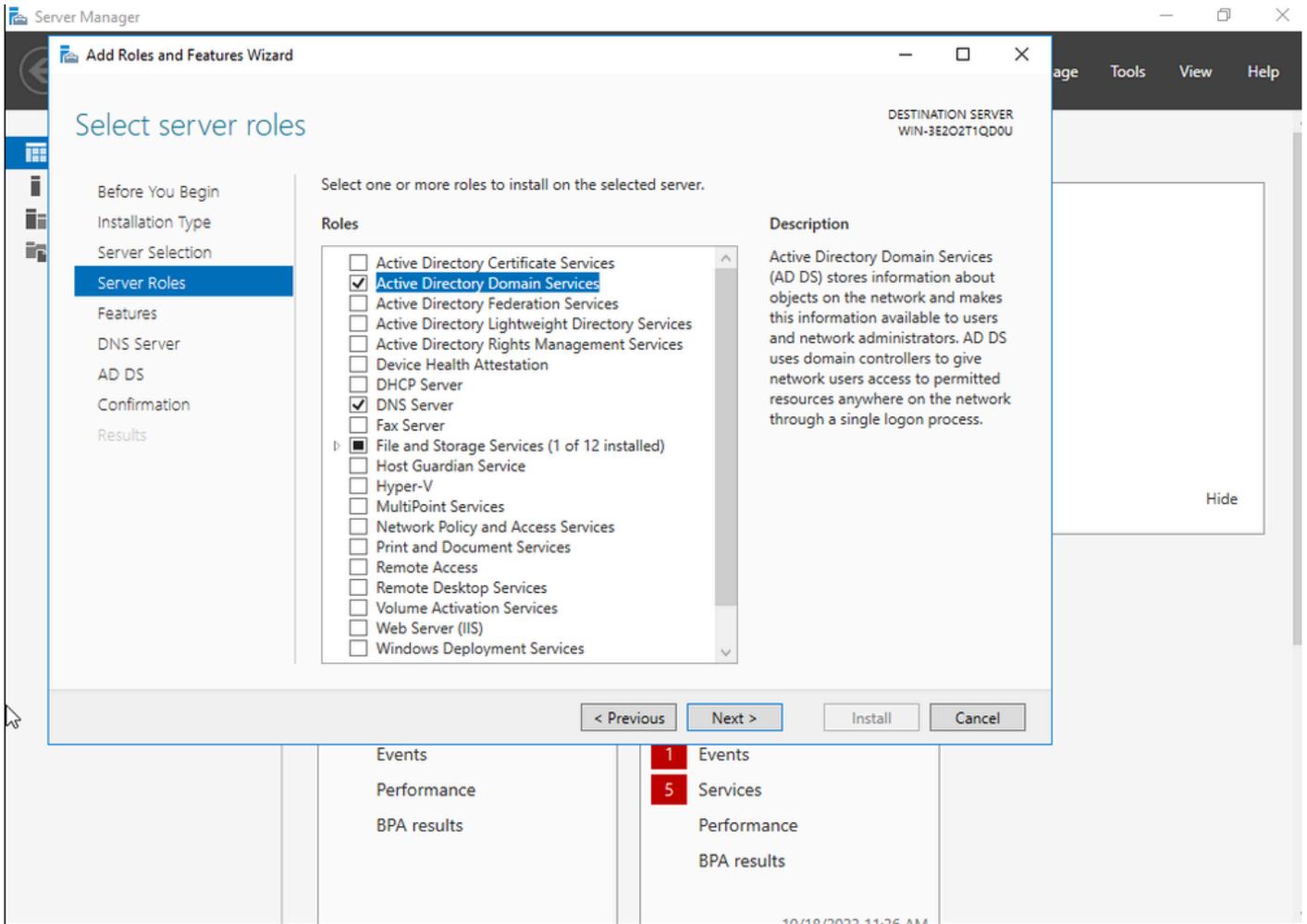
### CA SCEP di Windows Server 2016

In questo documento viene descritta l'installazione di base di una CA SCEP di Windows Server a scopo di laboratorio. È necessario configurare in modo sicuro e appropriato un'autorità di certificazione Windows effettiva per le operazioni aziendali. Questa sezione ha lo scopo di facilitare il test in laboratorio e di trarre ispirazione dalle impostazioni necessarie per il funzionamento della configurazione. Di seguito i passaggi:

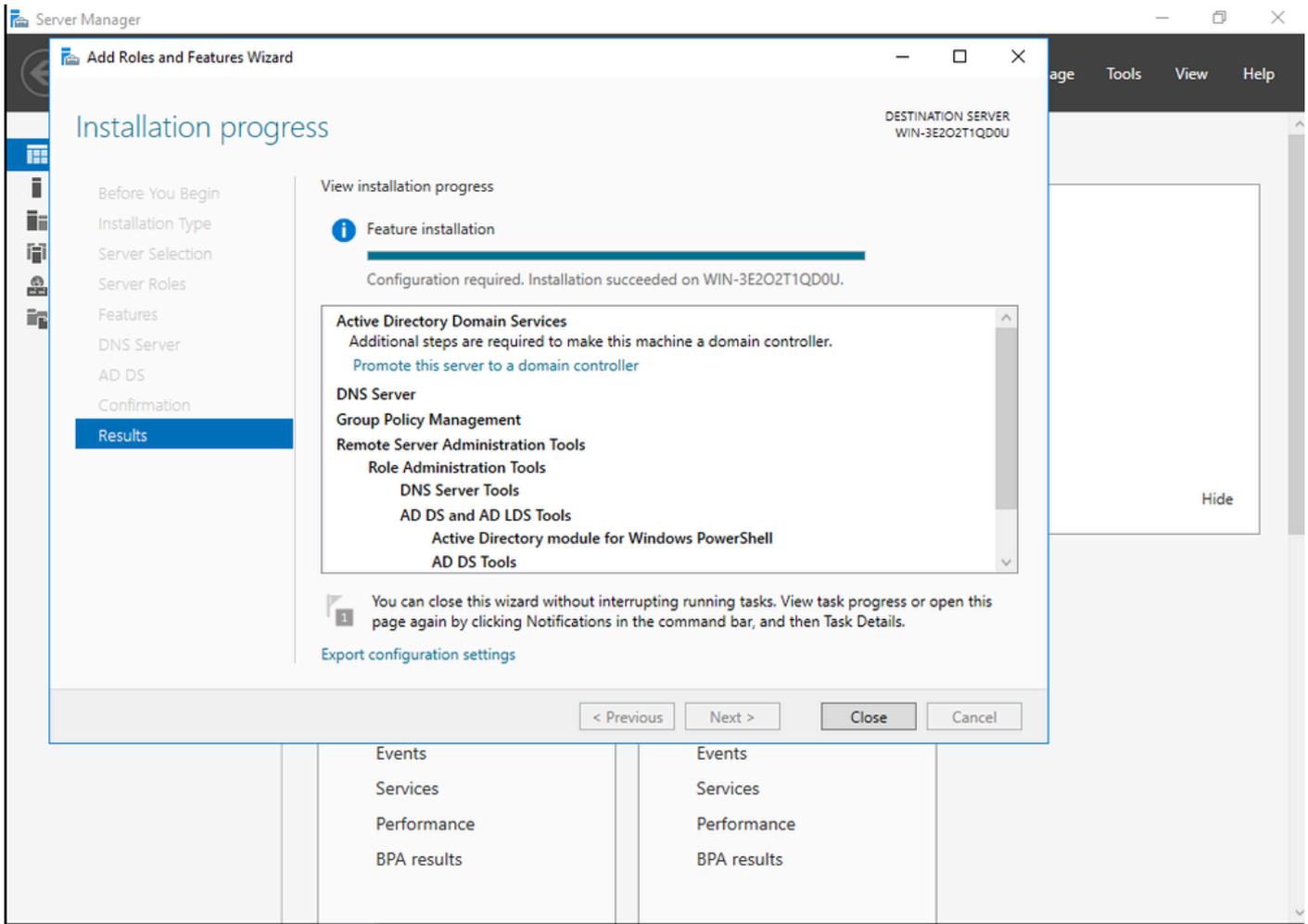
Passaggio 1. Installare un'esperienza desktop di Windows Server 2016 aggiornata.

Passaggio 2. Verificare che il server sia configurato con un indirizzo IP statico.

Passaggio 3. Installare un nuovo ruolo e servizio, iniziare con Servizi di dominio Active Directory e server DNS.

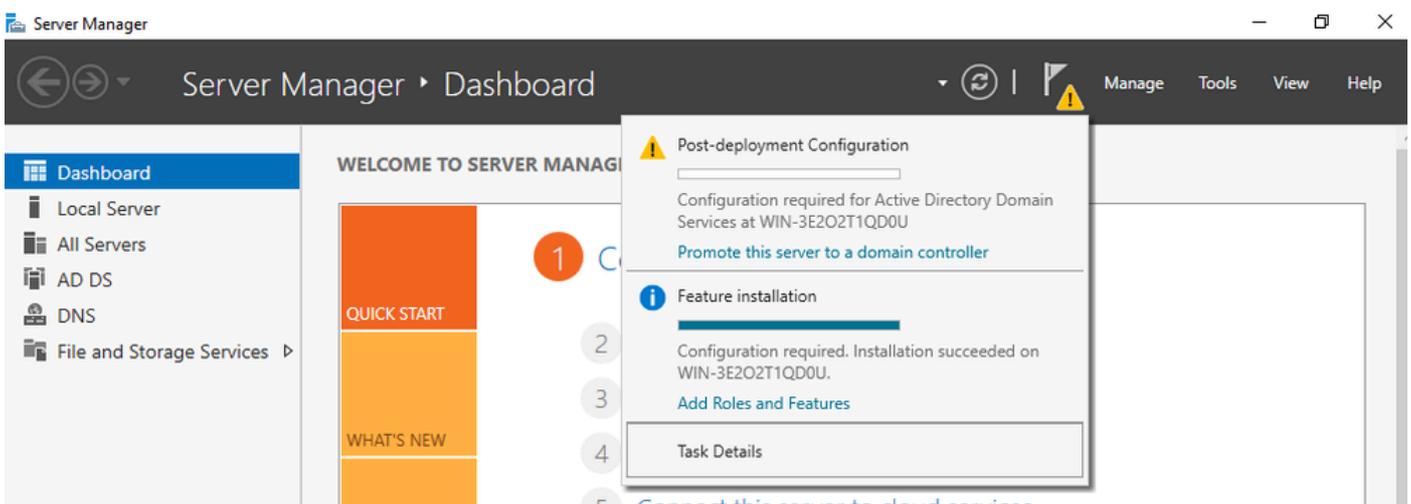


installazione di Active Directory



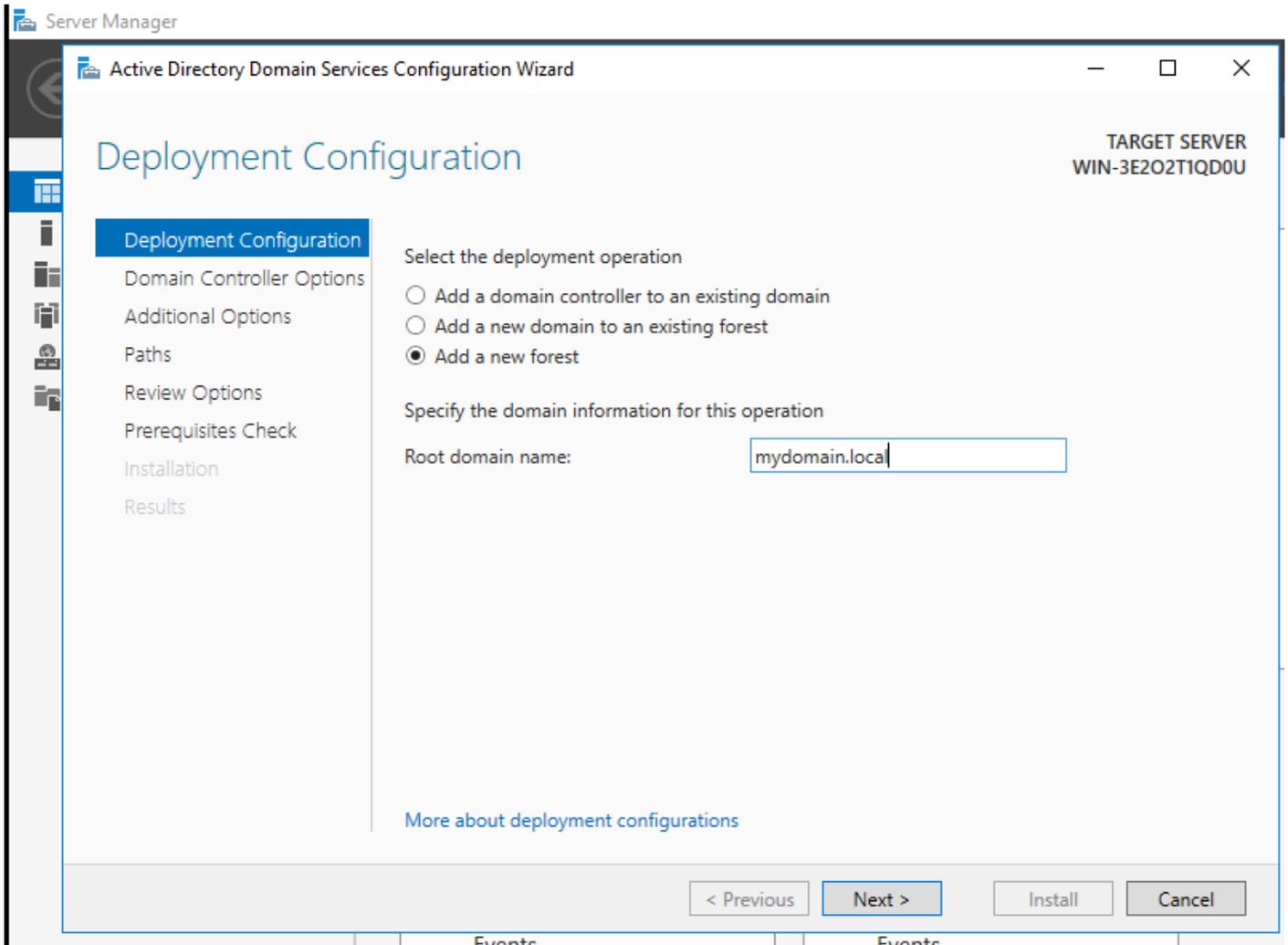
Fine dell'installazione di AD

Passaggio 4. Al termine, fare clic su nel dashboard per alzare di livello il server a controller di dominio.



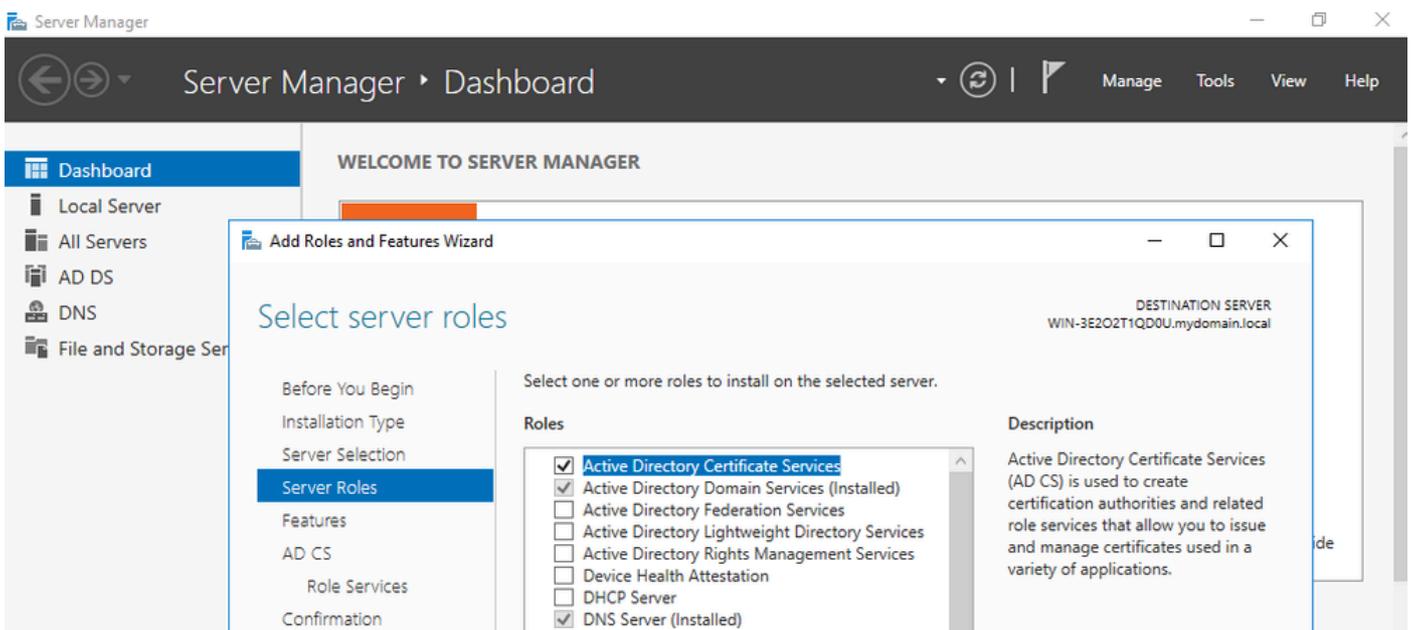
Configurare i servizi AD

Passaggio 5. Creare una nuova foresta e scegliere un nome di dominio.

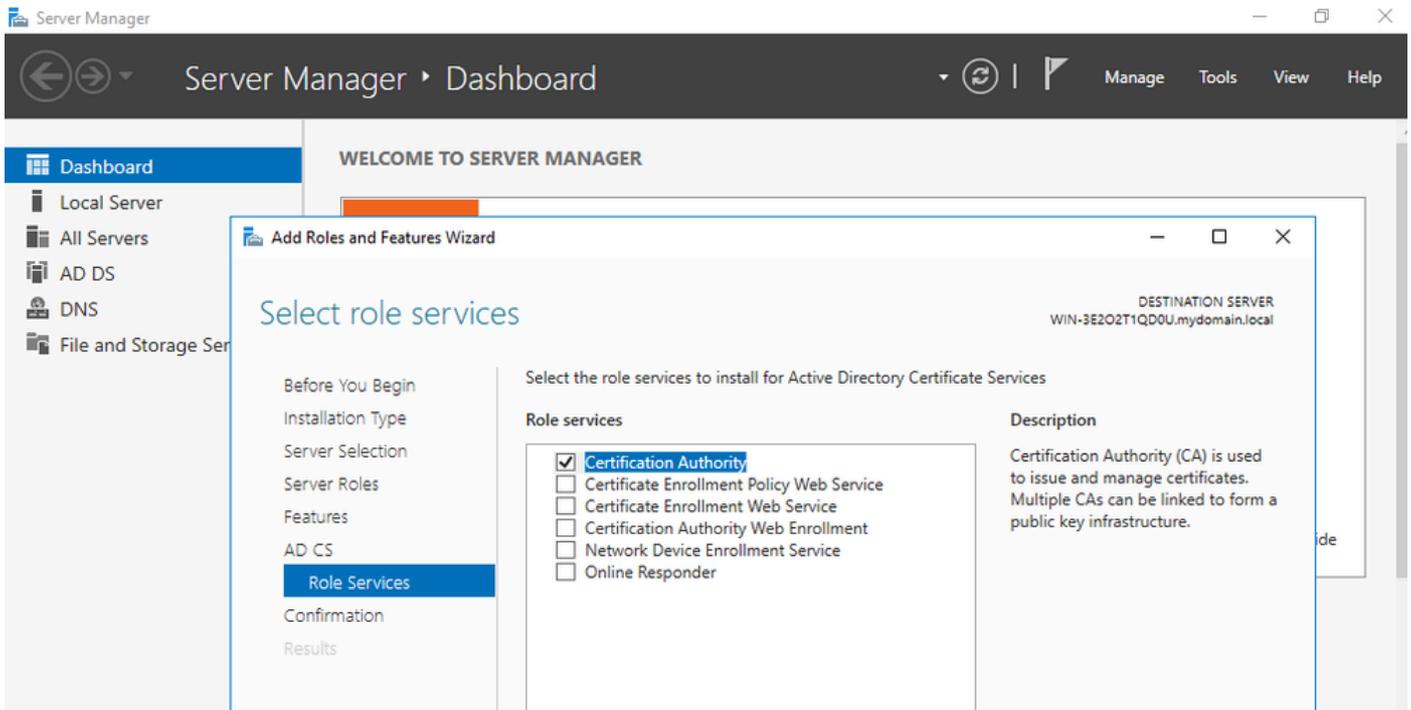


Scegliere un nome di foresta

Passaggio 6. Aggiungere il ruolo Servizi certificati al server:

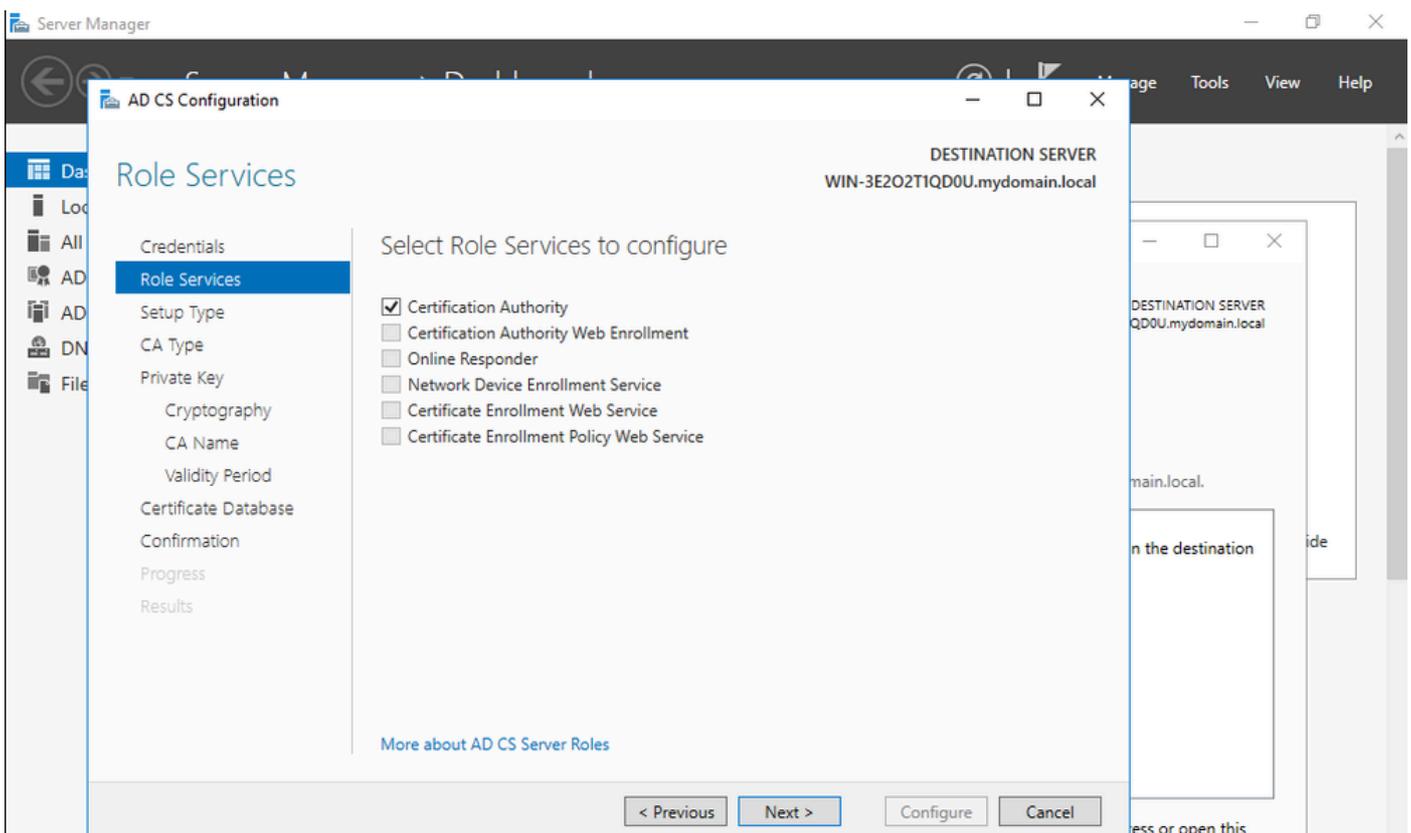


Aggiungi servizi certificati

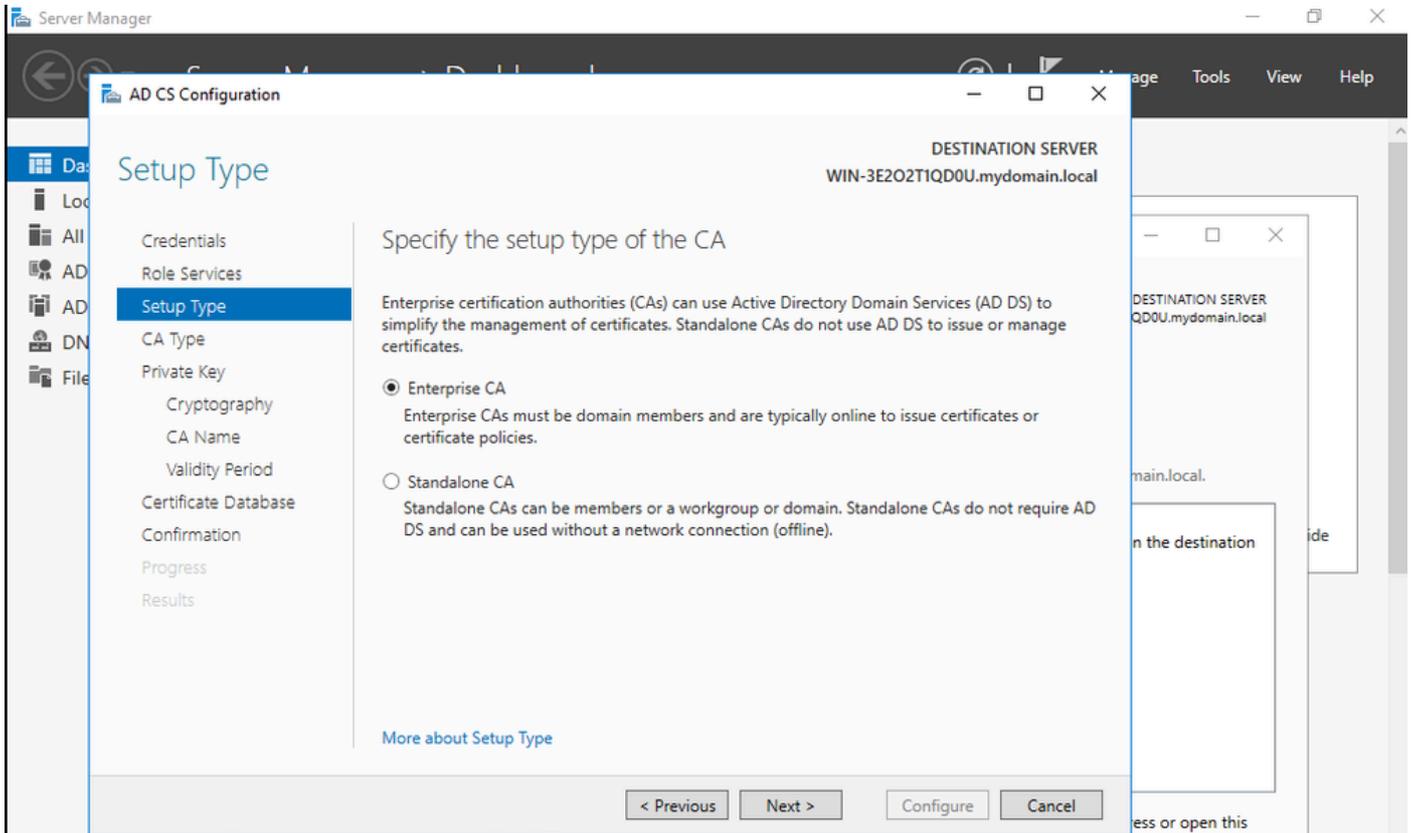


Aggiungi solo l'Autorità di certificazione

Passaggio 7. Al termine, configurare l'Autorità di certificazione.

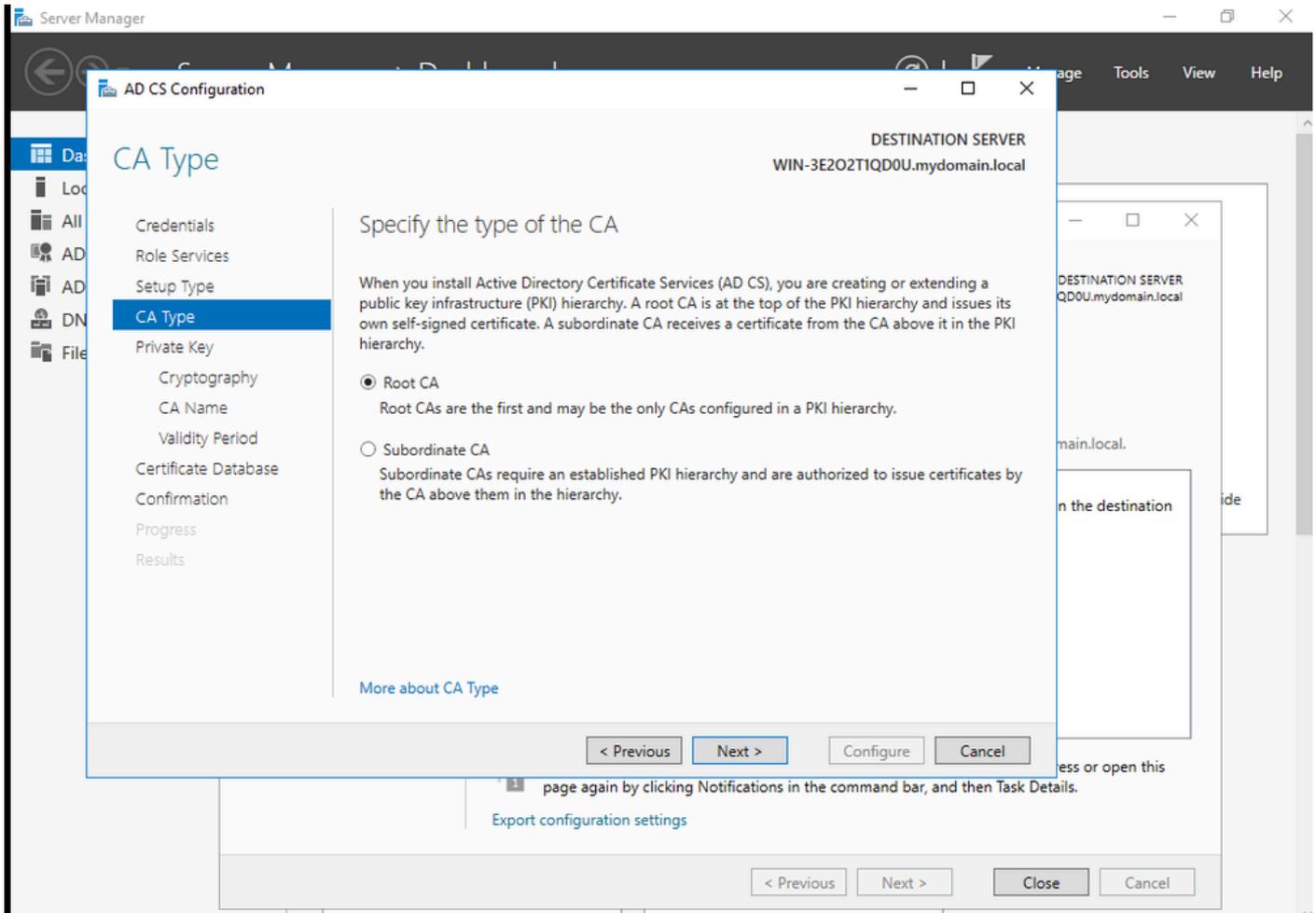


Passaggio 8. Selezionare Enterprise CA.



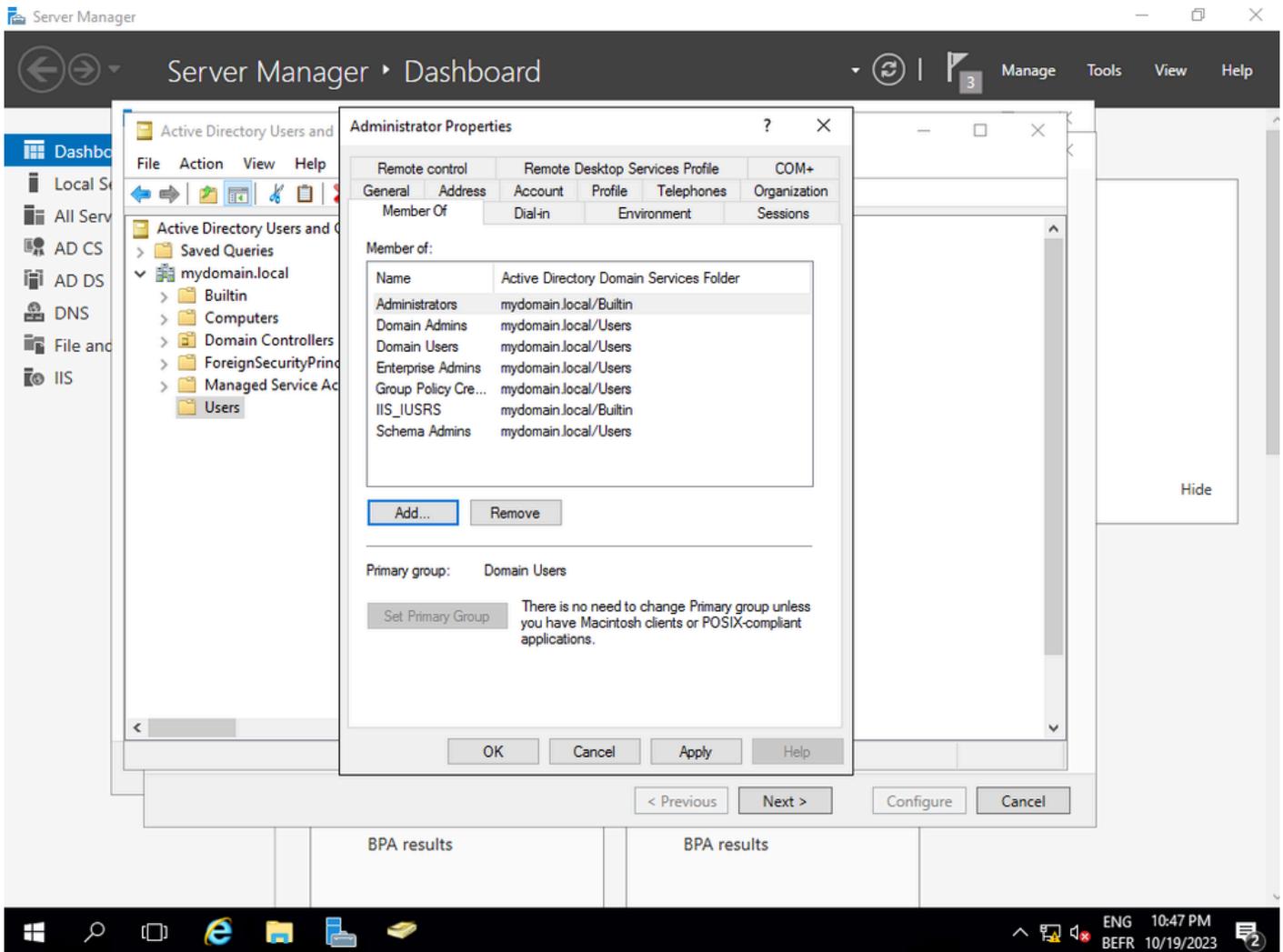
CA Enterprise

Passaggio 9. Rendere la CA radice. A partire da Cisco IOS XE 17.6, le CA subordinate sono supportate per LSC.



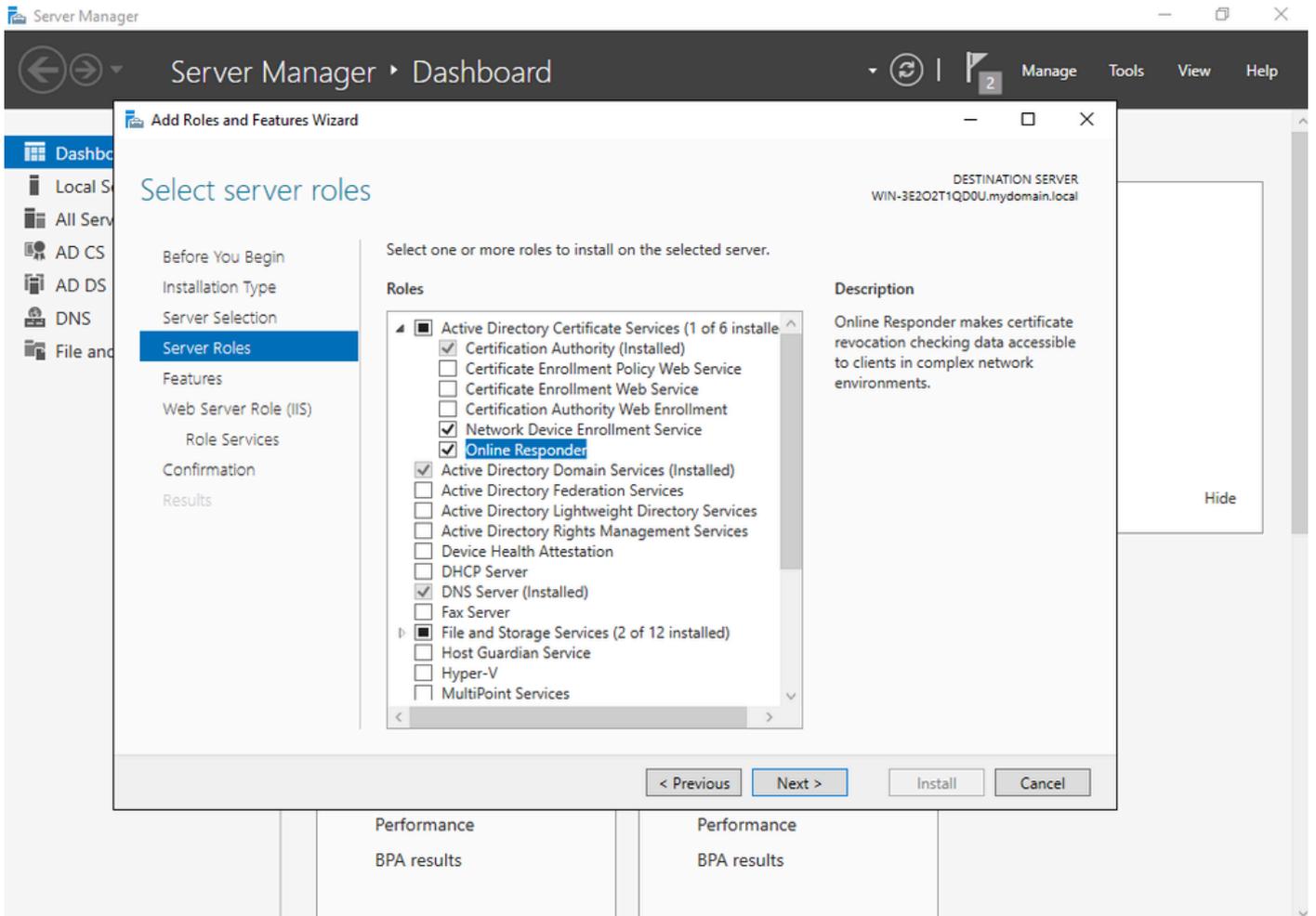
Scelta di una CA radice

È importante che l'account utilizzato per la CA faccia parte del gruppo IIS\_IUSRS. In questo esempio si utilizza l'account Administrator e si accede al menu Utenti e computer di Active Directory per aggiungere gli utenti Administrator al gruppo IIS\_IUSRS.



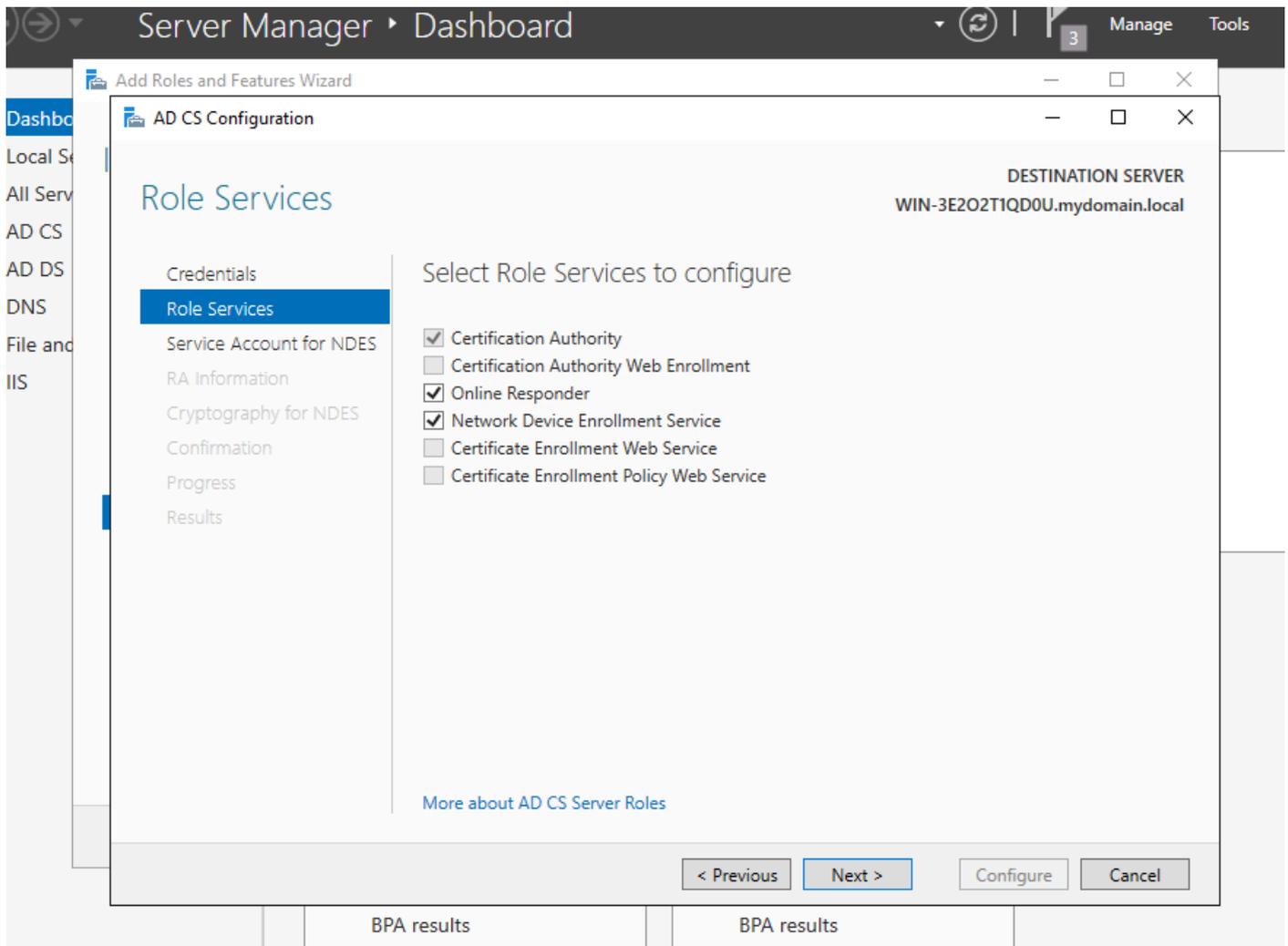
Aggiungere l'account amministratore al gruppo IIS\_USER

Passaggio 10. Dopo aver aggiunto un utente nel gruppo IIS appropriato, aggiungere ruoli e servizi. Aggiungere quindi i servizi Risponditore in linea e NDES all'Autorità di certificazione.



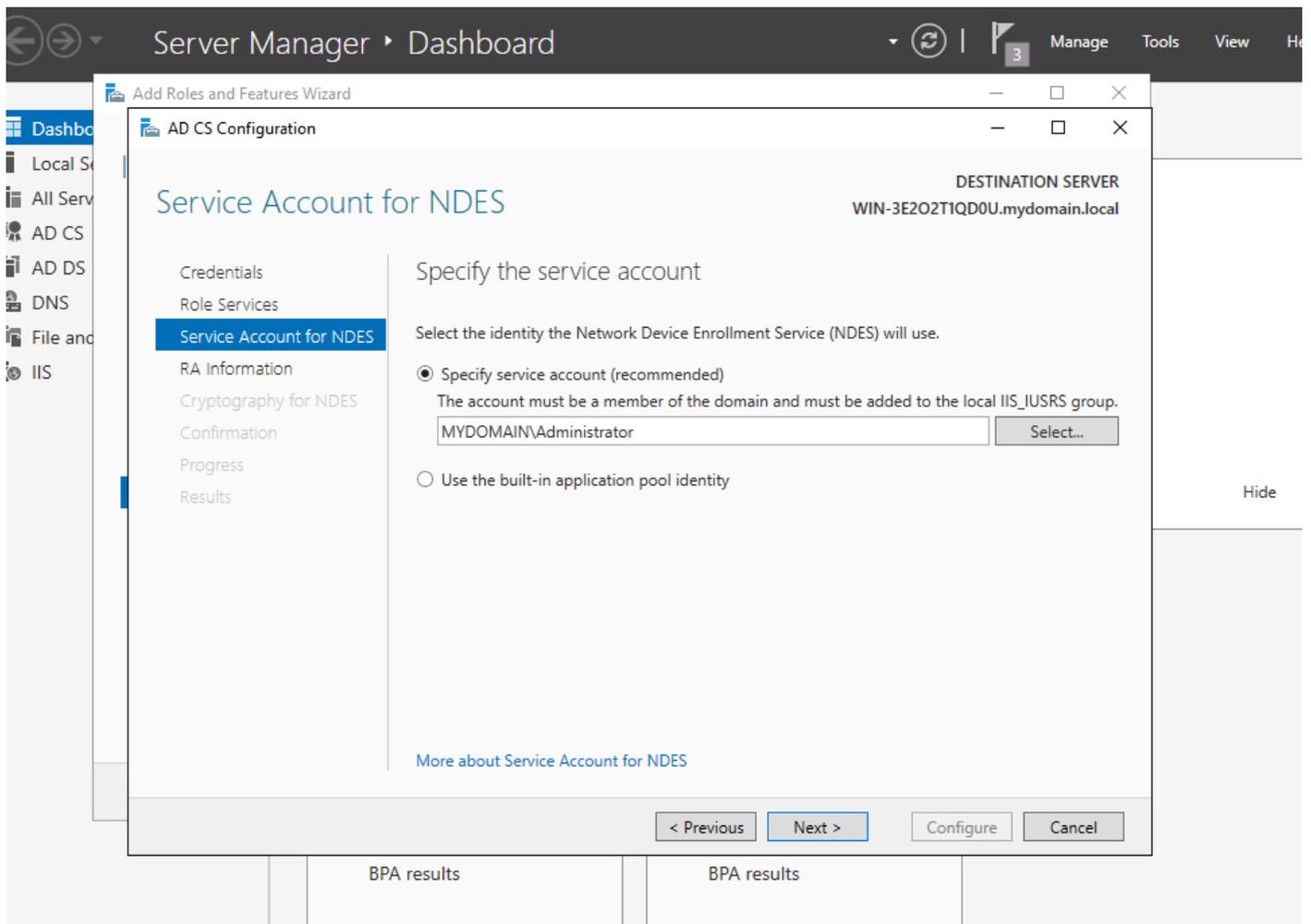
Installare i servizi NDES e Risponditore in linea

Passaggio 11. Una volta terminato, configurare i servizi.



Installa il risponditore online e il servizio NDES

Passaggio 12. Viene richiesto di scegliere un account del servizio. Questo è l'account aggiunto in precedenza al gruppo IIS\_IUSRS.



Selezionare l'utente aggiunto al gruppo IIS

Passaggio 13. Questa operazione è sufficiente per le operazioni SCEP, ma per ottenere l'autenticazione 802.1X è necessario installare anche un certificato sul server RADIUS. Per semplificare questa operazione, installare e configurare il servizio di registrazione Web in modo da poter copiare e incollare facilmente la richiesta di certificato ISE sul server Windows.

# Select server roles

DESTINATION SERVER  
WIN-3E202T1QD0U.mydomain.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- Confirmation
- Results

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

## Roles

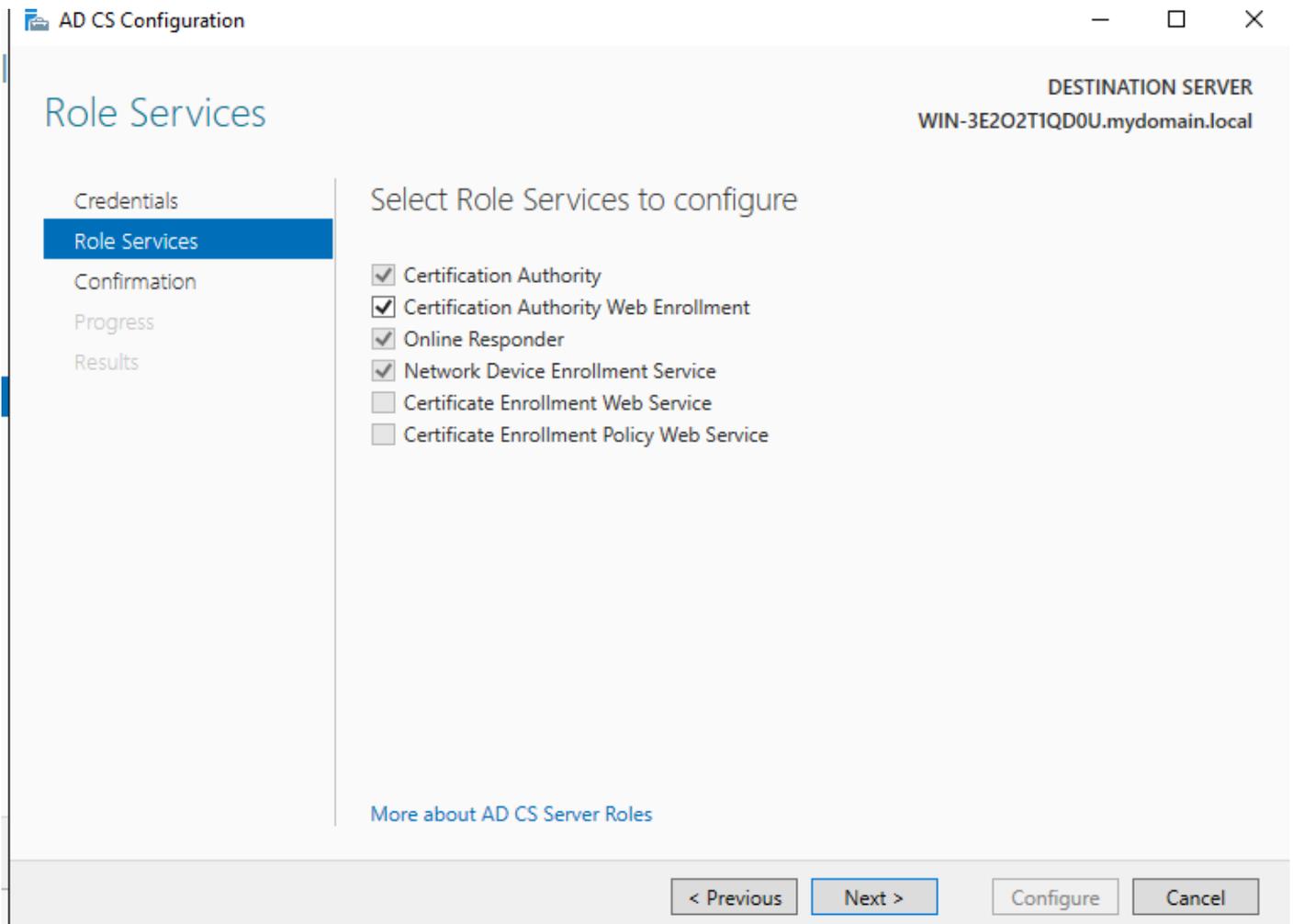
- Active Directory Certificate Services (3 of 6 installed)
  - Certification Authority (Installed)
  - Certificate Enrollment Policy Web Service
  - Certificate Enrollment Web Service
  - Certification Authority Web Enrollment**
  - Network Device Enrollment Service (Installed)
  - Online Responder (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
  - Host Guardian Service
  - Hyper-V
  - MultiPoint Services

## Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

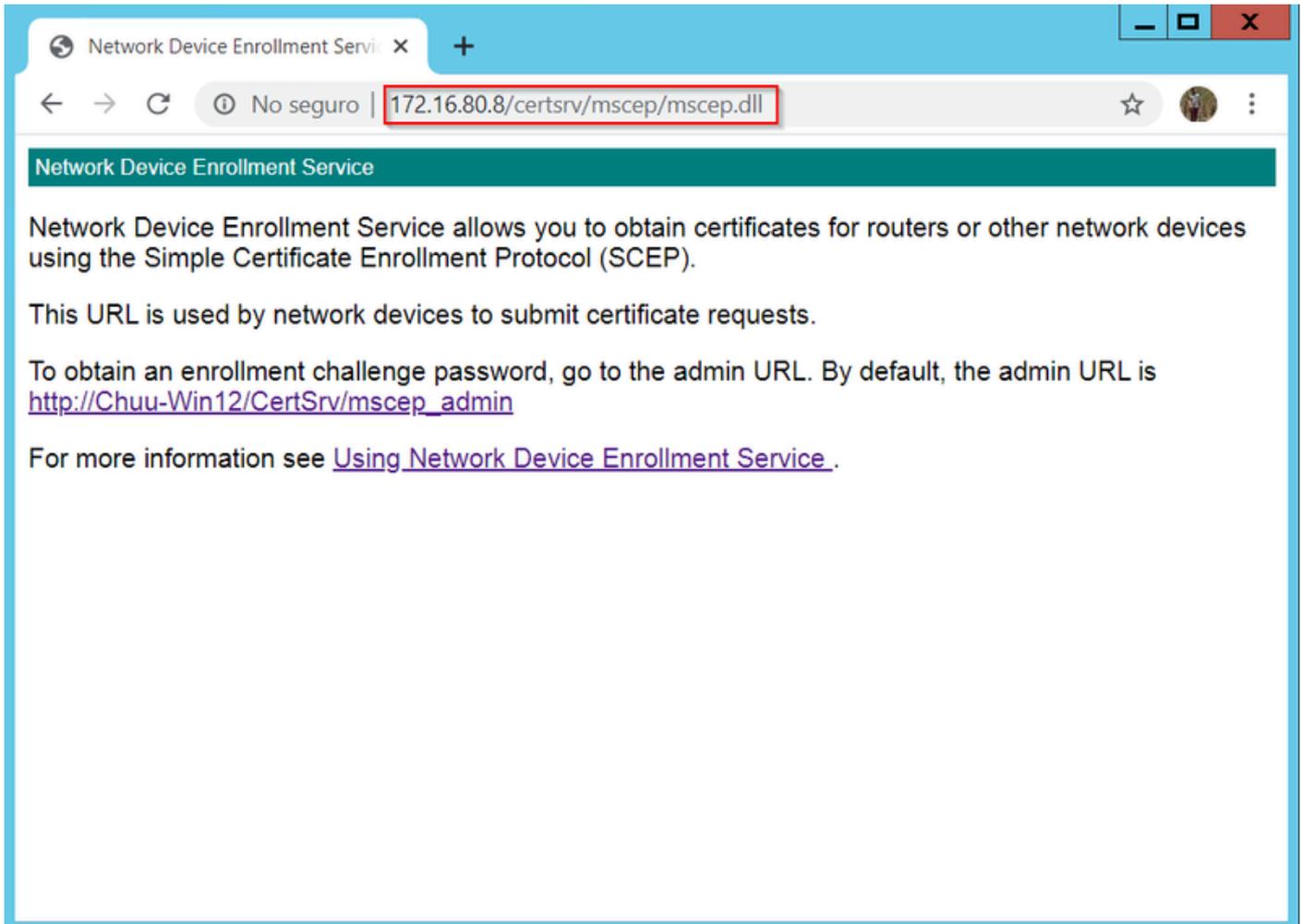
< Previous   Next >   Install   Cancel

Installa il servizio di registrazione Web



configurare il servizio di registrazione web

Passaggio 14. Per verificare il corretto funzionamento del servizio SCEP, visitare il sito <http://<serverip>/certsrv/mscep/mscep.dll> :



Verifica portale SCEP

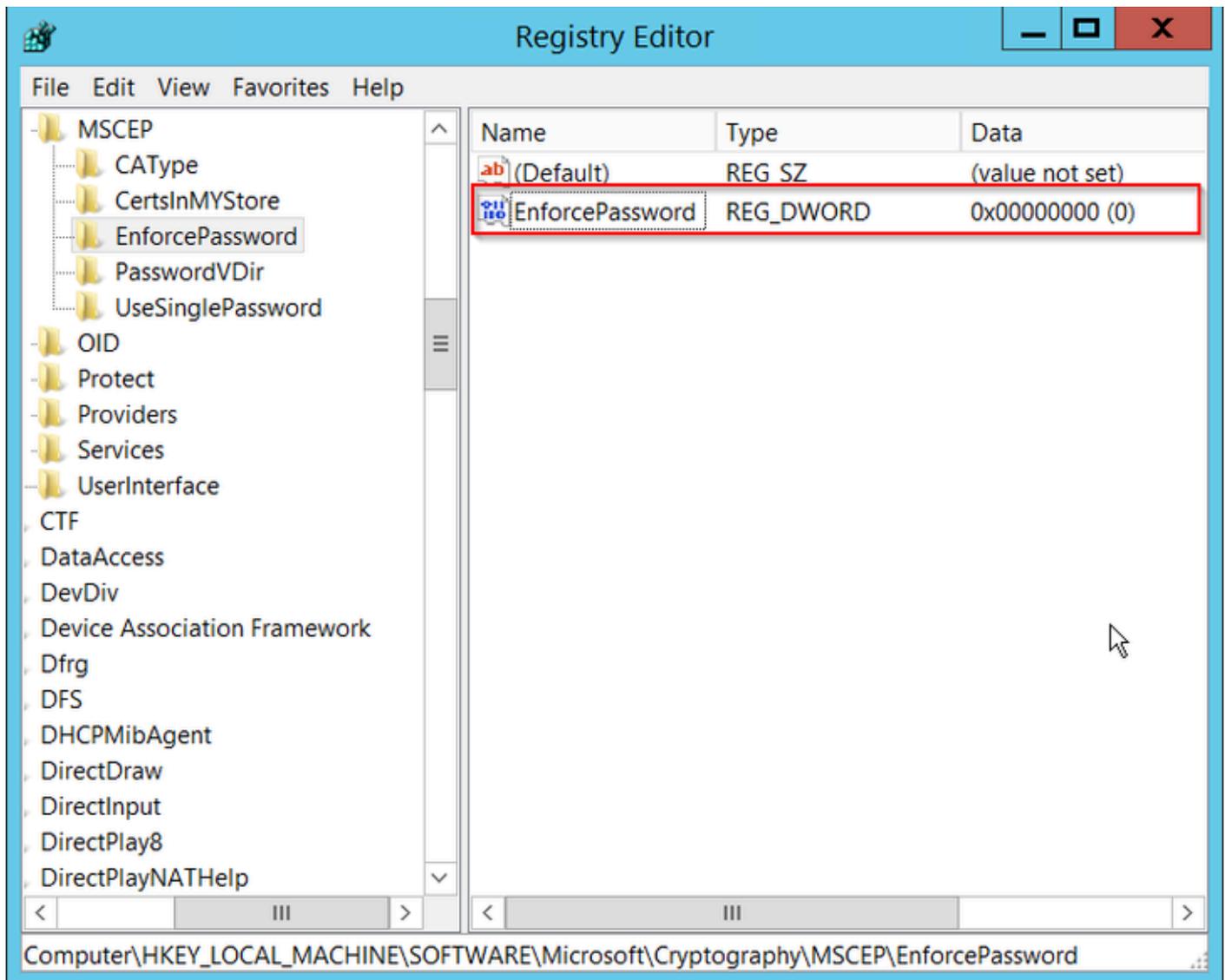
## Passaggio 15.

Per impostazione predefinita, Windows Server ha utilizzato una password di verifica dinamica per autenticare le richieste client ed endpoint prima della registrazione in Microsoft SCEP (MSCEP). È necessario un account amministratore per accedere alla GUI Web e generare una password su richiesta per ogni richiesta (la password deve essere inclusa nella richiesta). Il controller non è in grado di includere questa password nelle richieste che invia al server. Per rimuovere questa funzionalità, è necessario modificare la chiave del Registro di sistema nel server NDES:

Aprire l'Editor del Registro di sistema, cercare Regedit nel menu Start.

Selezionare Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP > EnforcePassword

Modificare il valore di EnforcePassword su 0. Se è già 0, lasciarlo invariato.



Impostare il valore di Enforcepassword

## Configurare il modello di certificato e il Registro di sistema

I certificati e le chiavi associate possono essere utilizzati in più scenari per scopi diversi definiti dai criteri di applicazione all'interno del server CA. I criteri di applicazione sono memorizzati nel campo Utilizzo chiave esteso (EKU) del certificato. Questo campo viene analizzato dall'autenticatore per verificare che venga utilizzato dal client per lo scopo previsto. Per assicurarsi che il criterio di applicazione appropriato sia integrato nei certificati WLC e AP, creare il modello di certificato appropriato e mapparlo al Registro di sistema NDES:

Passaggio 1. Selezionare Start > Strumenti di amministrazione > Autorità di certificazione.

Passaggio 2. Espandere la struttura di cartelle del server CA, fare clic con il pulsante destro del mouse sulle cartelle Modelli di certificato e selezionare Gestisci.

Passaggio 3. Fare clic con il pulsante destro del mouse sul modello di certificato Users, quindi scegliere Duplica modello dal menu di scelta rapida.

Passaggio 4. Passare alla scheda Generale, modificare il nome del modello e il periodo di validità

come desiderato, lasciare deselezionate tutte le altre opzioni.

---

 **Attenzione:** quando si modifica il periodo di validità, verificare che non sia superiore alla validità del certificato radice dell'Autorità di certificazione.

---

## Properties of New Template



Subject Name	Server	Issuance Requirements		
Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation

Template display name:

Template name:

Validity period:

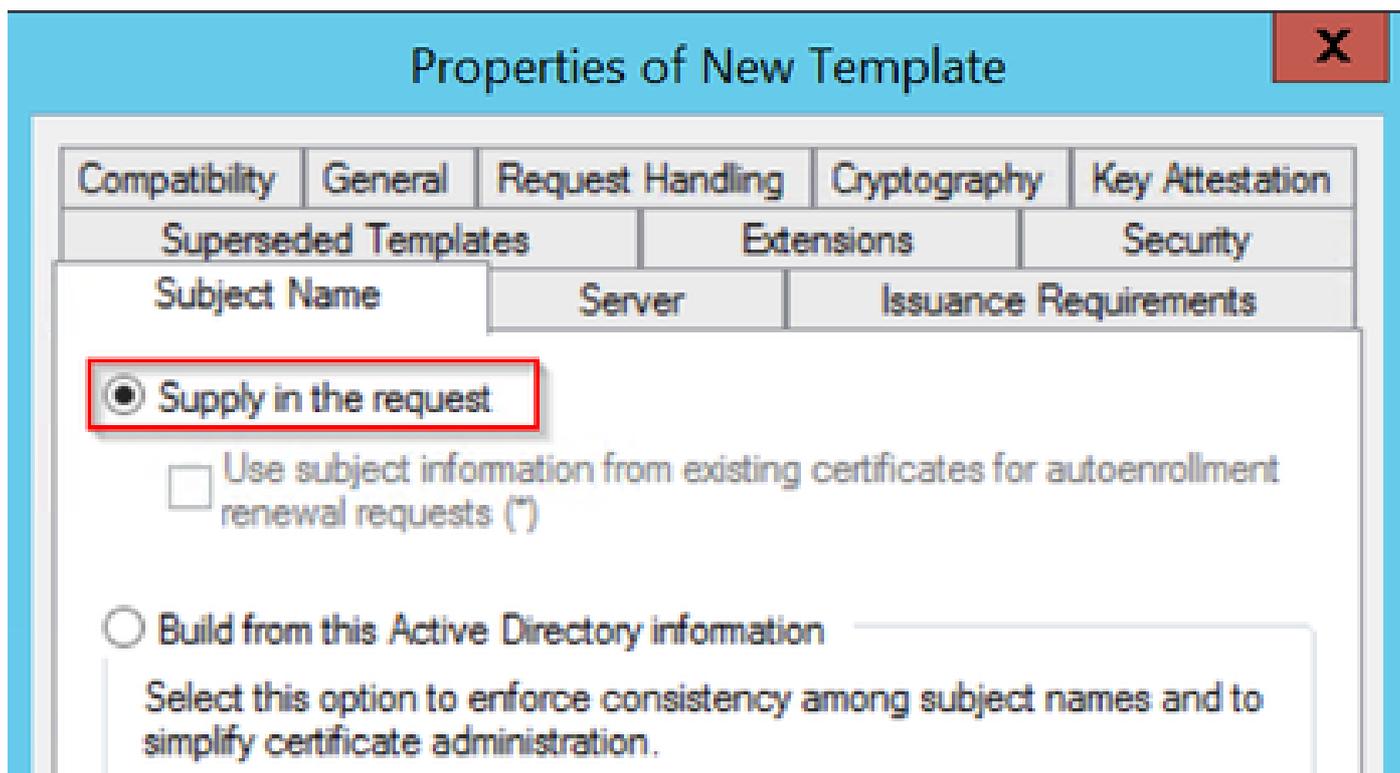
Renewal period:

Publish certificate in Active Directory

Do not automatically reenroll if a duplicate certificate exists in Active Directory

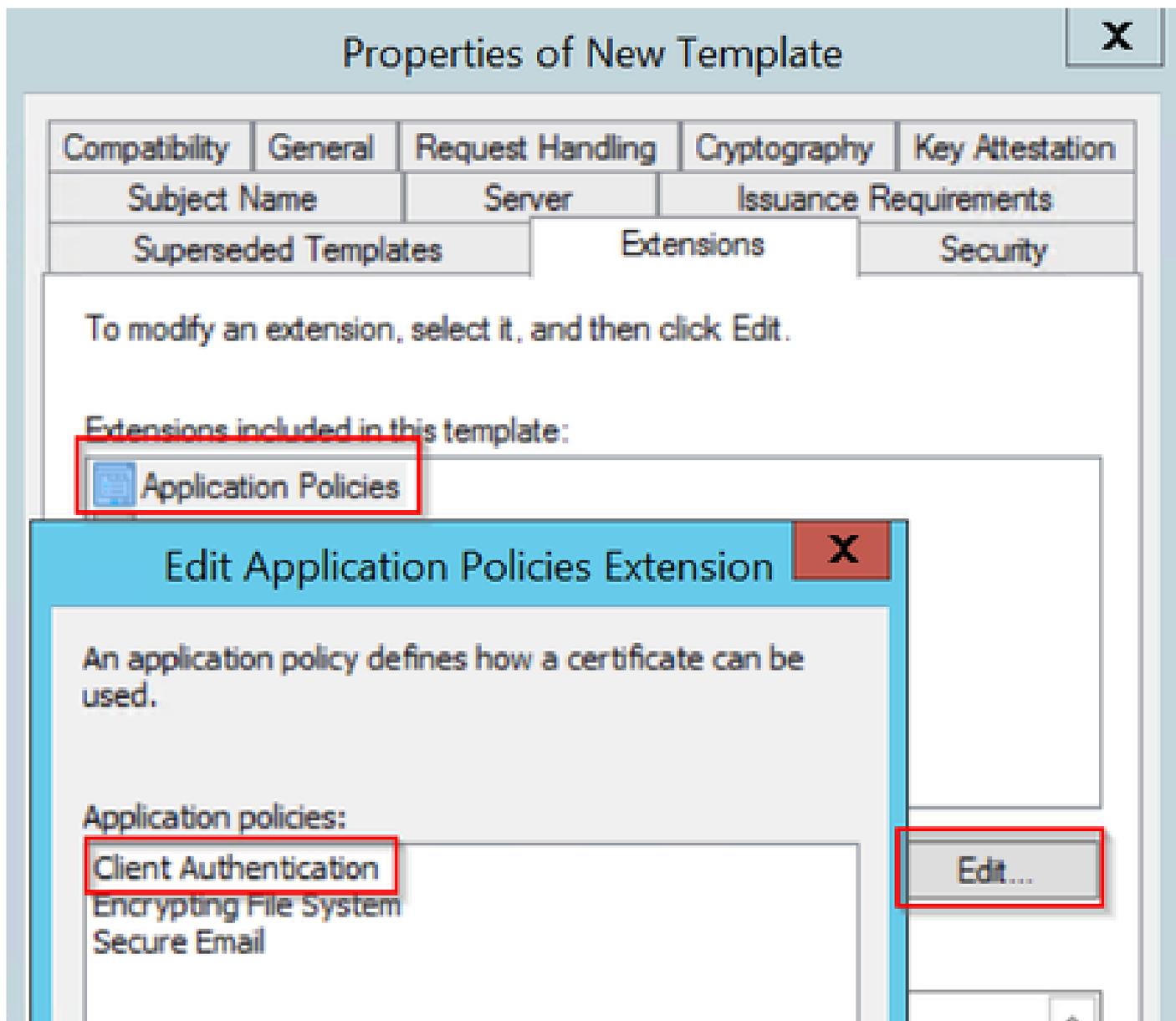
OK Cancel Apply Help

Passaggio 5. Passare alla scheda Nome soggetto e verificare che Fornitura nella richiesta sia selezionata. Viene visualizzata una schermata di popup che indica che gli utenti non hanno bisogno dell'approvazione dell'amministratore per ottenere la firma del certificato. Selezionare OK.



Fornire nella richiesta

Passaggio 6. Passare alla scheda Estensioni, quindi selezionare l'opzione Criteri di applicazione e selezionare il pulsante Modifica.... Verificare che Autenticazione client sia nella finestra Criteri di applicazione; in caso contrario, selezionare Aggiungi e aggiungerlo.



Verifica estensioni

Passaggio 7. Passare alla scheda Protezione, verificare che l'account del servizio definito nel passaggio 6 di Abilita servizi SCEP in Windows Server disponga delle autorizzazioni Controllo completo del modello, quindi selezionare Applica e OK.

# Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security

Group or user names:

- Authenticated Users
- Administrator**
- Domain Admins (CHUU-DOMAIN\Domain Admins)
- Domain Users (CHUU-DOMAIN\Domain Users)
- Enterprise Admins (CHUU-DOMAIN\Enterprise Admins)

Add... Remove

Permissions for Administrator

	Allow	Deny
<b>Full Control</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

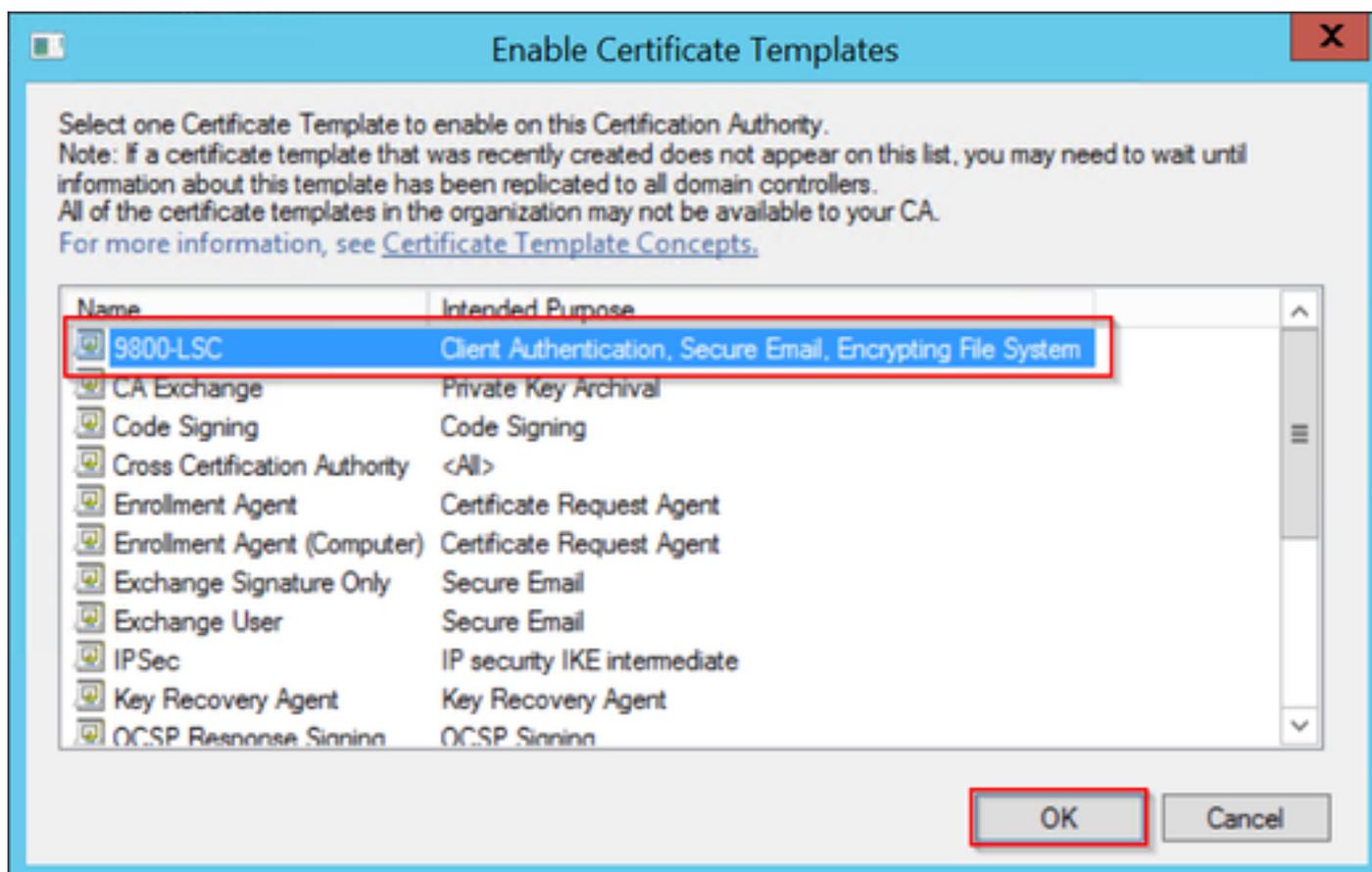
Advanced

OK Cancel **Apply** Help

Passaggio 8. Tornare alla finestra Autorità di certificazione, fare clic con il pulsante destro del mouse nella cartella Modelli di certificato e selezionare Nuovo > Modello di certificato da rilasciare.

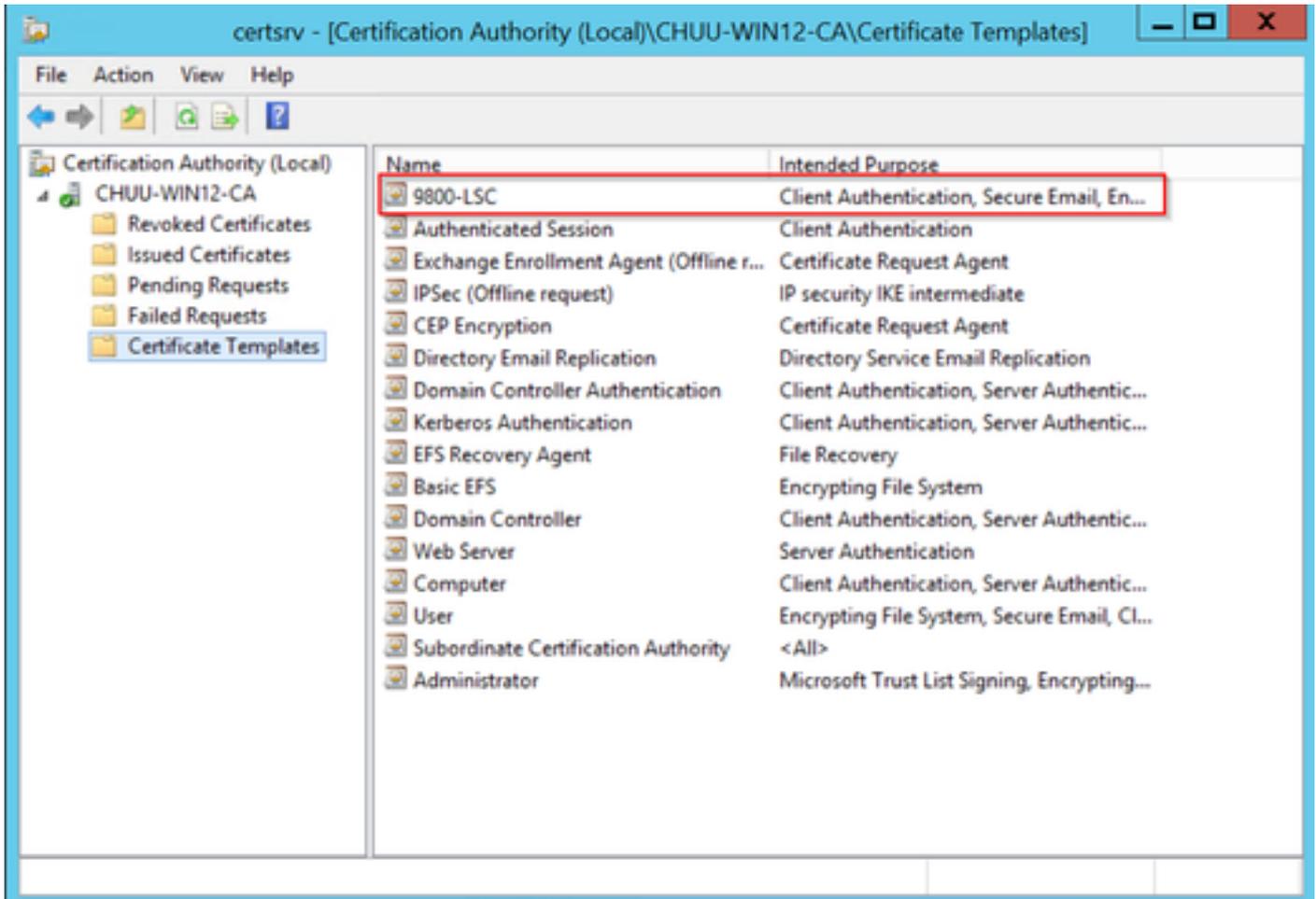
Passaggio 9. Selezionare il modello di certificato creato in precedenza, in questo esempio 9800-LSC, e selezionare OK.

 Nota: il modello di certificato appena creato può richiedere più tempo per essere elencato in più distribuzioni server in quanto deve essere replicato su tutti i server.



Scegliere il modello

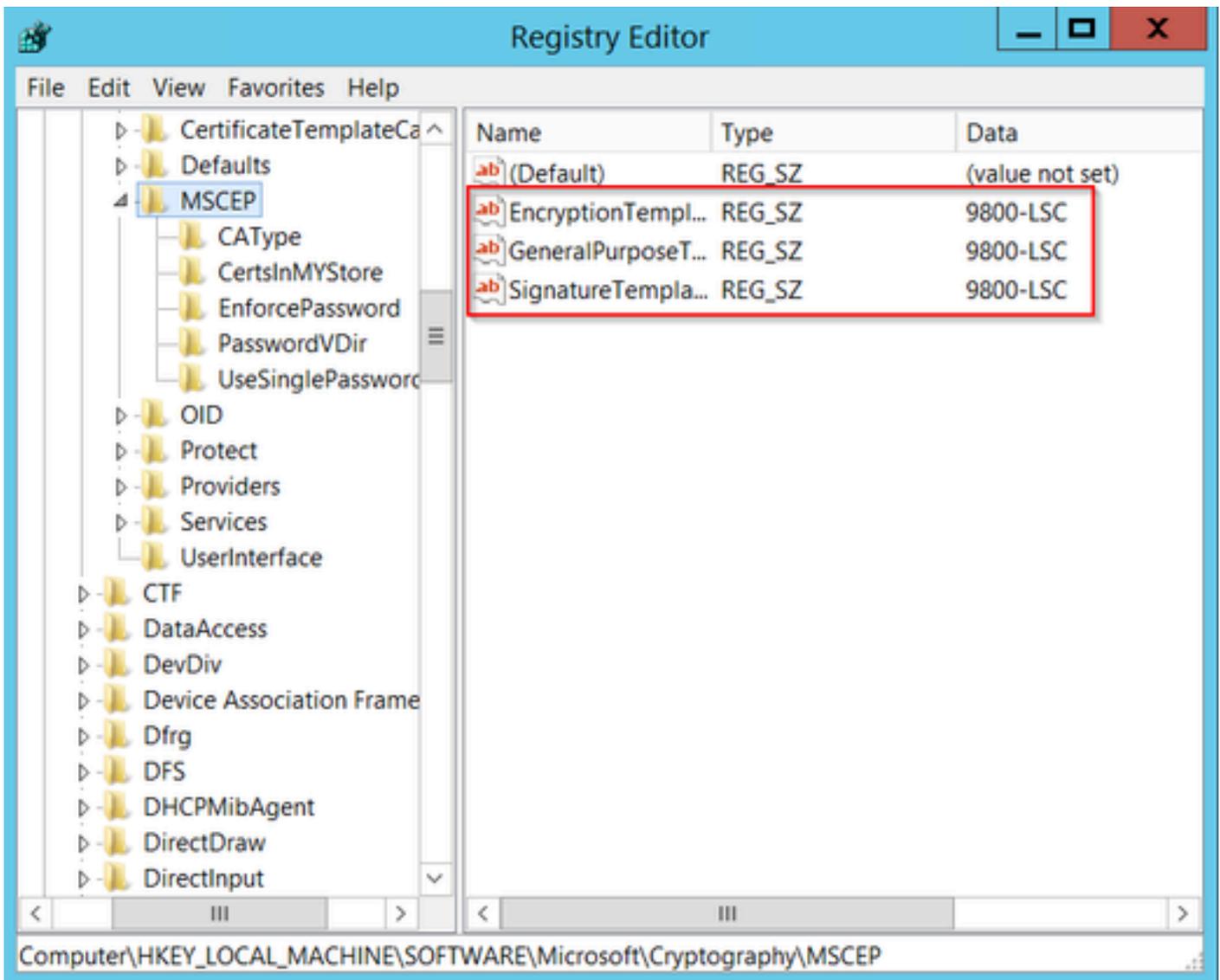
Il nuovo modello di certificato è ora elencato nel contenuto della cartella Modelli di certificato.



Selezionare LSC

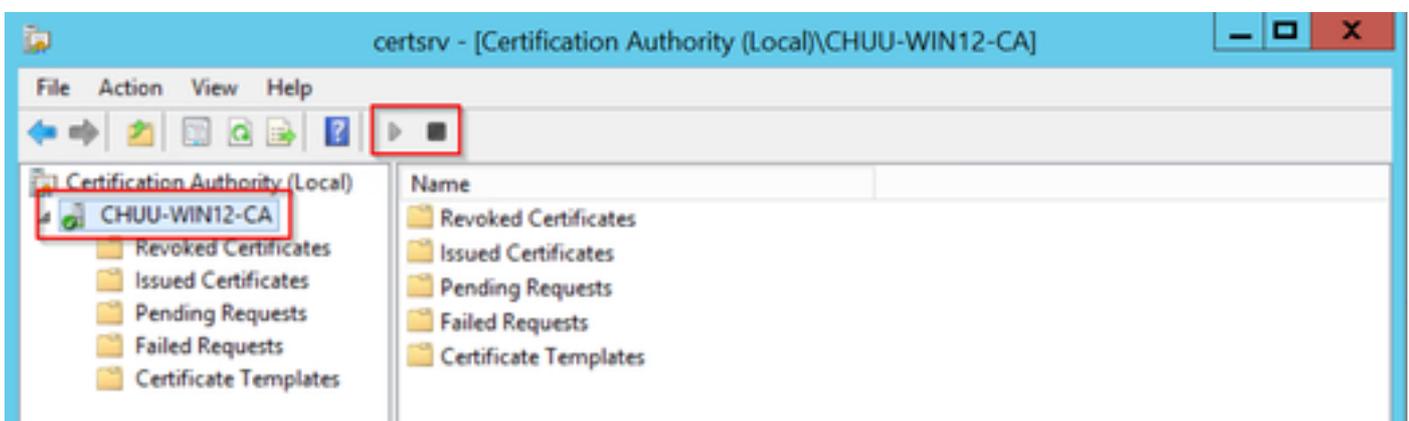
Passaggio 10. Tornare alla finestra Editor del Registro di sistema e selezionare Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.

Passaggio 11. Modificare i registri EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate in modo che puntino al nuovo modello di certificato creato.



Modificare il modello nel Registro di sistema

Passaggio 12. Riavviare il server NDES, quindi tornare alla finestra Certification Authority, selezionare il nome del server e scegliere il pulsante Stop and Play.



## Configurazione di LSC su 9800

Di seguito vengono riportati i passaggi in sequenza per configurare LSC per AP in WLC.

1. Creare la chiave RSA. Questa chiave viene utilizzata in seguito per il trust point PKI.
2. Creare un trust point e mappare la chiave RSA creata.
3. Abilitare il provisioning LSC per i punti di accesso e mappare il trust point.
  1. Abilitare LSC per tutti gli access point collegati.
  2. Abilitare LSC per i punti di accesso selezionati tramite l'elenco di provisioning.
4. Modificare il trust point di gestione wireless e puntare al trust point LSC.

## Procedura di configurazione GUI di AP LSC

Passaggio 1. Passare a Configurazione > Sicurezza > Gestione PKI > Generazione coppia di chiavi.

1. Fare clic su Add (Aggiungi) e assegnare un nome appropriato.
2. Aggiungere le dimensioni della chiave RSA.
3. L'opzione chiave esportabile è facoltativa. Questa operazione è necessaria solo se si desidera esportare la chiave dalla casella.
4. Selezionare Genera

The screenshot shows the 'Key Pair Generation' configuration dialog in the Cisco ISE GUI. The dialog is overlaid on a table of existing key pairs. The configuration fields are:

- Key Name\*:** AP-SCEP
- Key Type\*:** RSA Key (selected), EC Key
- Modulus Size\*:** 2048
- Key Exportable\*:**

The 'Generate' button is highlighted with a red box. The table in the background has the following data:

Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	<input type="checkbox"/>
9800-40.cisco.com	RSA	No	<input type="checkbox"/>
TP-self-signed-2147029136.server	RSA	No	<input type="checkbox"/>
CISCO_IDEVID_SUDI	RSA	No	<input type="checkbox"/>
CISCO_IDEVID_SUDI_LEGACY	RSA	No	<input type="checkbox"/>

Passaggio 2. Passare a Configurazione > Sicurezza > Gestione PKI > Trustpoint

1. Fare clic su Add (Aggiungi) e assegnare un nome appropriato.
2. Immettere l'URL di registrazione (qui l'URL è <http://10.106.35.61:80/certsrv/mscep/mscep.dll>) e gli altri dettagli.
3. Selezionare le coppie di chiavi RSA create nel passaggio 1.
4. Fare clic su Authenticate.
5. Fare clic su Enroll trustpoint e immettere una password.
6. Fare clic su Applica a dispositivo.

Configuration > Security > PKI Management

### Add Trustpoint

Label\*  Enrollment Type  SCEP  Terminal

**Subject Name**

Country Code  State

Location  Domain Name

Organization  Email Address

Enrollment URL  Authenticate

Key Generated  Available RSA Keypairs

Enroll Trustpoint

Password\*

Re-Enter Password\*

3. Passare a Configurazione > Wireless > Access Point. Scorrere verso il basso e selezionare LSC Provision.

1. Selezionare lo stato come abilitato. Ciò abilita LSC per tutti gli access point connessi a questo WLC.
2. Selezionare il nome del trust point creato nel passaggio 2.

Compilate il resto dei dettagli in base alle vostre esigenze.

Configuration > Wireless > Access Points

All Access Points

Total APs: 1

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP0CDD-F89A-46ED	C9117AXI-D	2	<span style="color: green;">●</span>	0 days 0 hrs 26 mins 42 secs	10.105.101.158	80ec.3579.0300	0cd0.f99a.46e0	Local	Yes	Registered	Healthy

1 - 1 of 1 access points

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

**LSC Provision**

Status

Trustpoint Name

Number of Join Attempts

Key Size

Certificate chain status

Subject Name Parameters

Country

State

City

Organization

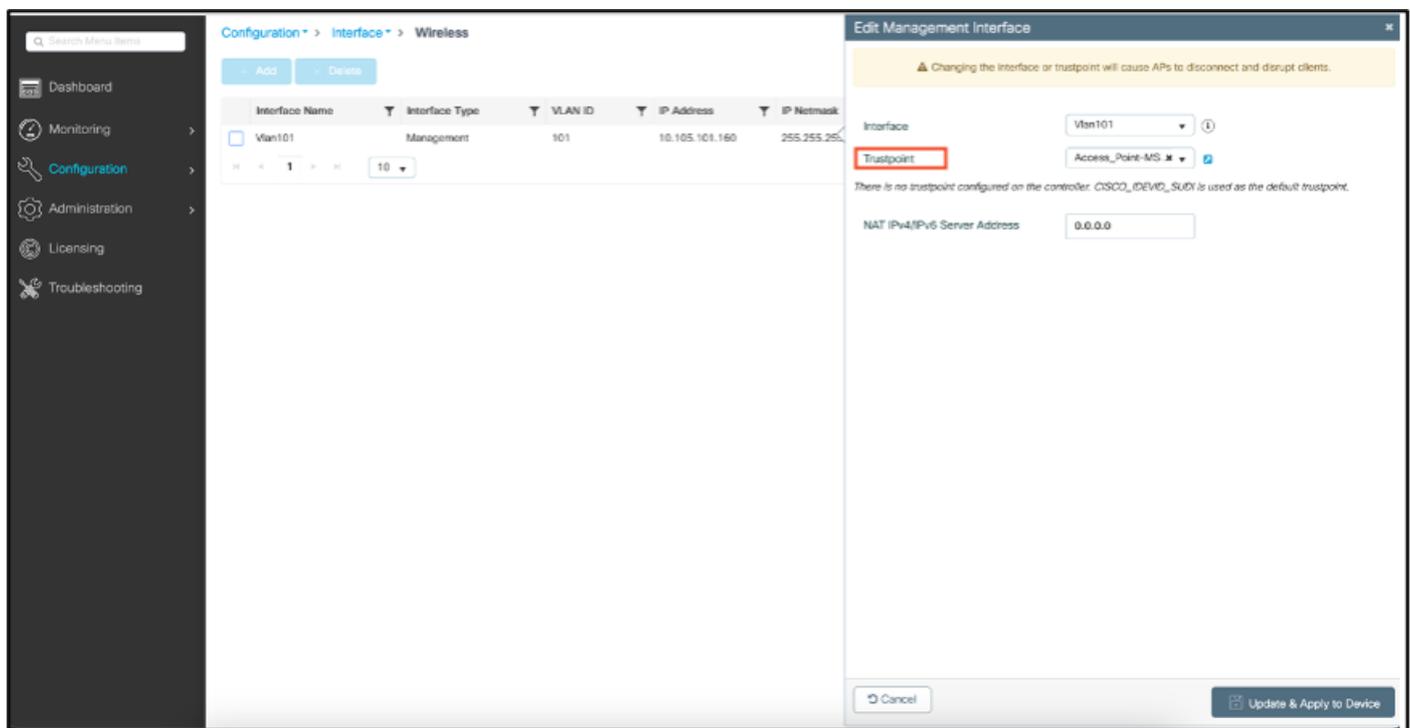
Dopo aver abilitato LSC, i punti di accesso scaricano il certificato tramite WLC e lo riavviano. Nella sessione della console dell'access point verrà quindi visualizzato un frammento di codice simile a questo.

```
[*09/25/2023 10:03:28.0993] .....
[*09/25/2023 10:03:28.7016] .....+++++
[*09/25/2023 10:03:28.7663] writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:03:28.7666] -----
[*09/25/2023 10:03:28.9212] LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:03:28.9212]
[*09/25/2023 10:03:28.9293] LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:03:28.9293]
[*09/25/2023 10:03:28.9635] LSC certs and private key verified
[*09/25/2023 10:03:28.9635]
[*09/25/2023 10:03:29.4997] LSC private key written to hardware TAM
[*09/25/2023 10:03:29.4997]
[*09/25/2023 10:03:29.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed
```

Passaggio 4. Dopo aver abilitato LSC, è possibile modificare il certificato di gestione wireless in modo che corrisponda al trust point LSC. In questo modo, gli access point si uniscono ai relativi certificati LSC e il WLC utilizza il proprio certificato LSC per l'aggiunta all'access point. Questa operazione è facoltativa se l'unica operazione che si desidera eseguire è l'autenticazione 802.1X dei punti di accesso.

1. Selezionare Configurazione > Interfaccia > Wireless, quindi fare clic su Interfaccia di gestione.
2. Modificare il trust point in modo che corrisponda al trust point creato nel passaggio 2.

La parte di configurazione dell'interfaccia utente grafica di LSC è terminata. Gli access point devono essere in grado di collegarsi al WLC utilizzando il certificato LSC.



## Passi di configurazione CLI di AP LSC

1. Creare una chiave RSA utilizzando questo comando.

```
9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP
```

```
% You already have RSA keys defined named AP-SCEP.
```

```
% They will be replaced
```

```
% The key modulus size is 2048 bits
```

```
% Generating 2048 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 0 seconds)
```

```
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storage
```

```
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Creare un trust point PKI ed eseguire il mapping della coppia di chiavi RSA. Immettere l'URL di registrazione e il resto dei dettagli.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
```

```
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
```

```
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
```

```
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
```

```
9800-40(ca-trustpoint)#revocation none
```

```
9800-40(ca-trustpoint)#exit
```

3. Autenticare e registrare il trust point PKI con il server CA utilizzando il comando `crypto pki authentication <trustpoint>`. Immettere una password nel prompt della password.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
```

```
Certificate has the following attributes:
```

```
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
```

```
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
9800-40(config)#crypto pki enroll Access_Point-MS-CA
```

```
%
```

```
% Start certificate enrollment ..
```

```
% Create a challenge password. You will need to verbally provide this
```

```
password to the CA Administrator in order to revoke your certificate.
```

```
For security reasons your password will not be saved in the configuration.
```

```
Please make a note of it.
```

```
Password:
```

```
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
```

```
Re-enter password:
```

```
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
```

```
% The subject name in the certificate will include: 9800-40.cisco.com
```

```
% Include the router serial number in the subject name? [yes/no]: yes
```

```
% The serial number in the certificate will be: TTM244909MX
```

```
% Include an IP address in the subject name? [no]: no
```

```
Request certificate from CA? [yes/no]: yes
```

```
% Certificate request sent to Certificate Authority
```

```
% The 'show crypto pki certificate verbose Access_Point-MS-CA' command will show the fingerprint.
```

```
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
```

```
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
```

```
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
```

```
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
```

```
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
```

```
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=email@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

#### 4. Configurare il join AP con il certificato LSC.

```
9800-40(config)#ap lsc-provision join-attempt 10
9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L
9800-40(config)#ap lsc-provision key-size 2048
9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA
9800-40(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration
Are you sure you want to continue? (y/n): y
```

#### 5. Modificare il trust di gestione wireless in modo che corrisponda al trust point creato in precedenza.

```
9800-40(config)#wireless management trustpoint Access_Point-MS-CA
```

### Verifica LSC AP

Eseguire questi comandi sul WLC per verificare il LSC.

```
#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate
```

```

9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash      : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
-----

9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable

9800-40#

```

```

9800-40#sho ap name AP@CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-OTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP @02.lx LSC Status
Certificate status : Not Available
AP LSC authentication state : CAPWAP-OTLS

```

Una volta ricaricati gli access point, accedere alla CLI dell'access point ed eseguire questi comandi per verificare la configurazione di LSC.

```

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```

```

AP@CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
----- Device Certificate -----
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:18
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
  Validity
    Not Before: Sep 28 04:15:28 2023 GMT
    Not After : Sep 27 04:15:28 2024 GMT
  Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0 emailAddress = mail@tac-lab.local
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:

```

```

AP0CD0.F89A.46E0#sho crypto | in LSC
LSC: Enabled
AP0CD0.F89A.46E0#sho capwap cli config | in lsc
AP lsc enable : 1
AP lsc reboot cnt : 0
AP lsc max num of retry : 10
AP lsc mode : 0x1
AP lsc dtls fallback state : 0
AP0CD0.F89A.46E0#
Read timed out

```

```

AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
-----
[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

Current connection certificate issuer name: sumans-lab-ca

```

## Risoluzione dei problemi di provisioning LSC

È possibile eseguire un'acquisizione EPC dalla porta dello switch di uplink WLC o AP per verificare il certificato utilizzato dal punto di accesso per formare il tunnel CAPWAP. Verificare dal PCAP se la creazione del tunnel DTLS è riuscita.

```

▼ Datagram Transport Layer Security
  ▼ DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
    Content Type: Handshake (22)
    Version: DTLS 1.2 (0xfefd)
    Epoch: 0
    Sequence Number: 5
    Length: 82
  ▼ Handshake Protocol: Certificate (Reassembled)
    Handshake Type: Certificate (11)
    Length: 1627
    Message Sequence: 2
    Fragment Offset: 1557
    Fragment Length: 70
    Certificates Length: 1624
  ▼ Certificates (1624 bytes)
    Certificate Length: 1621
  ▼ Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d. (pkcs-9-at-emailAddress@mail@tac-lab.local,id-at-commonName=
  ▼ signedCertificate
    version: v3 (2)
    serialNumber: 0x5c000000181814edda85f9bfd1000000000018
  ▼ signature (sha256WithRSAEncryption)
    Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
  ▼ issuer: rdnSequence (0)
  ▼ rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
  ▼ RDNSquence item: 1 item (dc=com)
  ▼ RelativeDistinguishedName item (dc=com)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: com
  ▼ RDNSquence item: 1 item (dc=tac-lab)
  ▼ RelativeDistinguishedName item (dc=tac-lab)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: tac-lab
  ▼ RDNSquence item: 1 item (dc=sumans)
  ▼ RelativeDistinguishedName item (dc=sumans)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: sumans
  ▼ RDNSquence item: 1 item (id-at-commonName=sumans-lab-ca)
  ▼ RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
    Object Id: 2.5.4.3 (id-at-commonName)
  ▼ DirectoryString: printableString (1)
    printableString: sumans-lab-ca
  ▼ validity
  ▼ notBefore: utcTime (0)
    utcTime: 2023-09-28 04:15:28 (UTC)
  ▼ notAfter: utcTime (0)
    utcTime: 2024-09-27 04:15:28 (UTC)
  ▼ subject: rdnSequence (0)

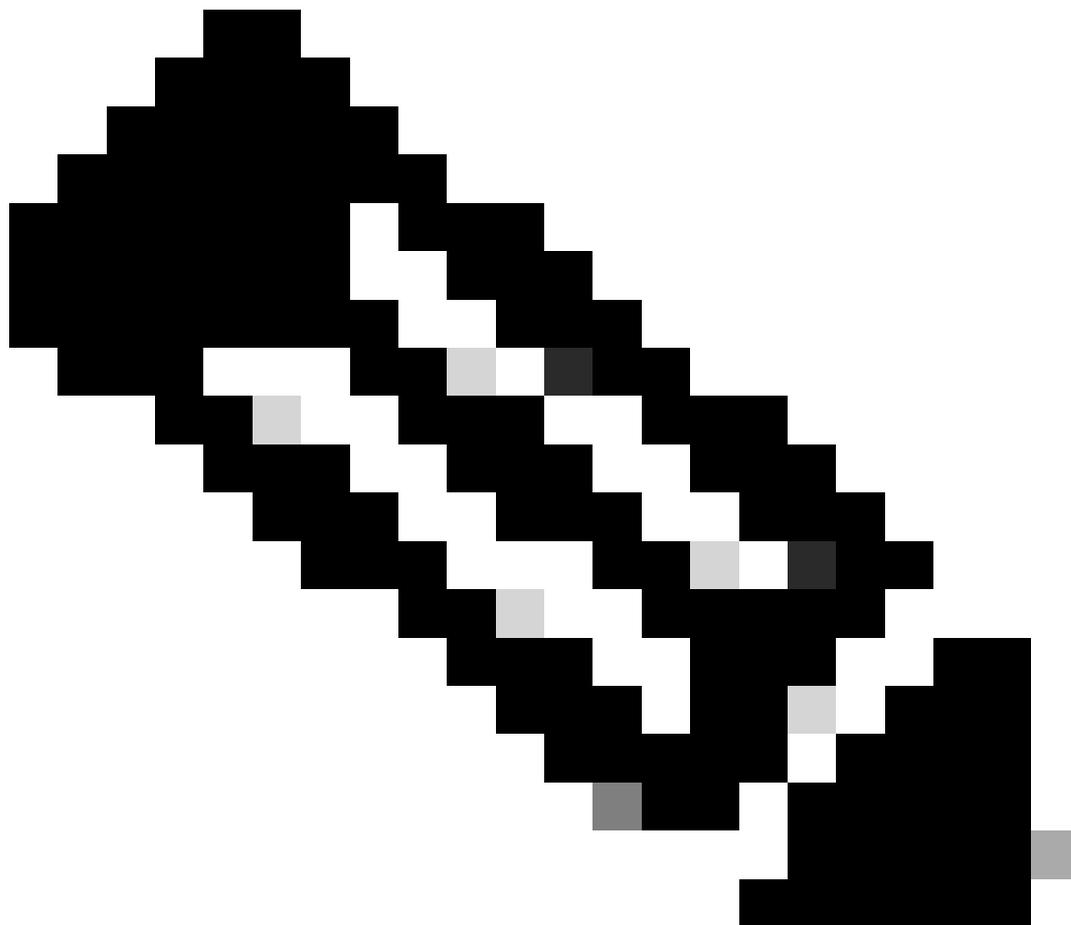
```

I debug DTLS possono essere eseguiti su AP e WLC per comprendere il problema del certificato.

## Autenticazione 802.1X cablata AP tramite LSC

Il punto di accesso è configurato per utilizzare lo stesso certificato LSC per autenticarsi. AP agisce come supplicant 802.1X ed è autenticato dallo switch sul server ISE. Il server ISE comunica con AD nel back-end.

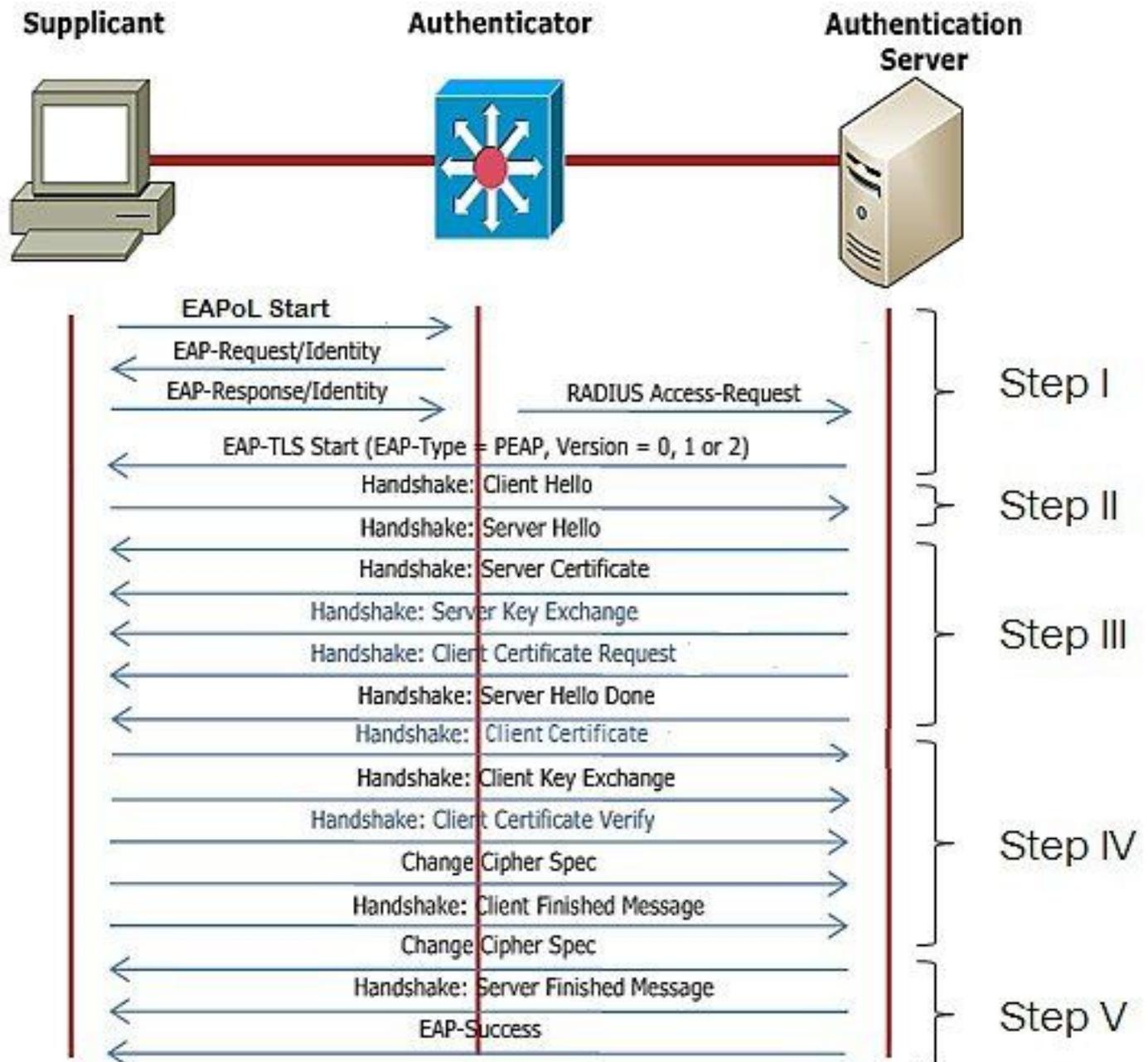
---



Nota: se l'autenticazione dot1x è abilitata sulla porta dello switch di uplink AP, i punti di accesso non possono inoltrare né ricevere traffico finché non viene passata l'autenticazione. Per ripristinare i punti di accesso con autenticazione non riuscita e ottenere l'accesso al punto di accesso, disabilitare l'autenticazione dot1x sulla porta dello switch cablato del punto di accesso.

---

Flusso di lavoro autenticazione EAP-TLS e scambio messaggi

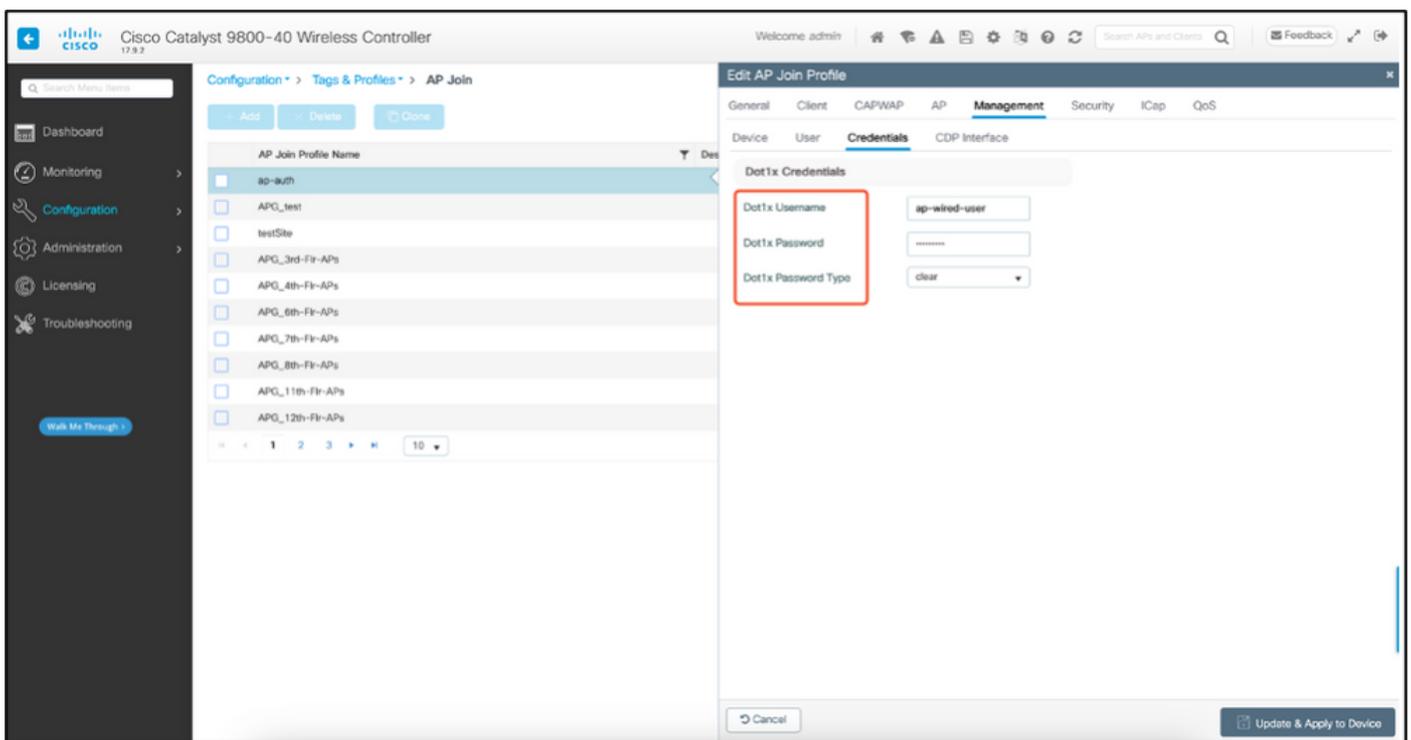
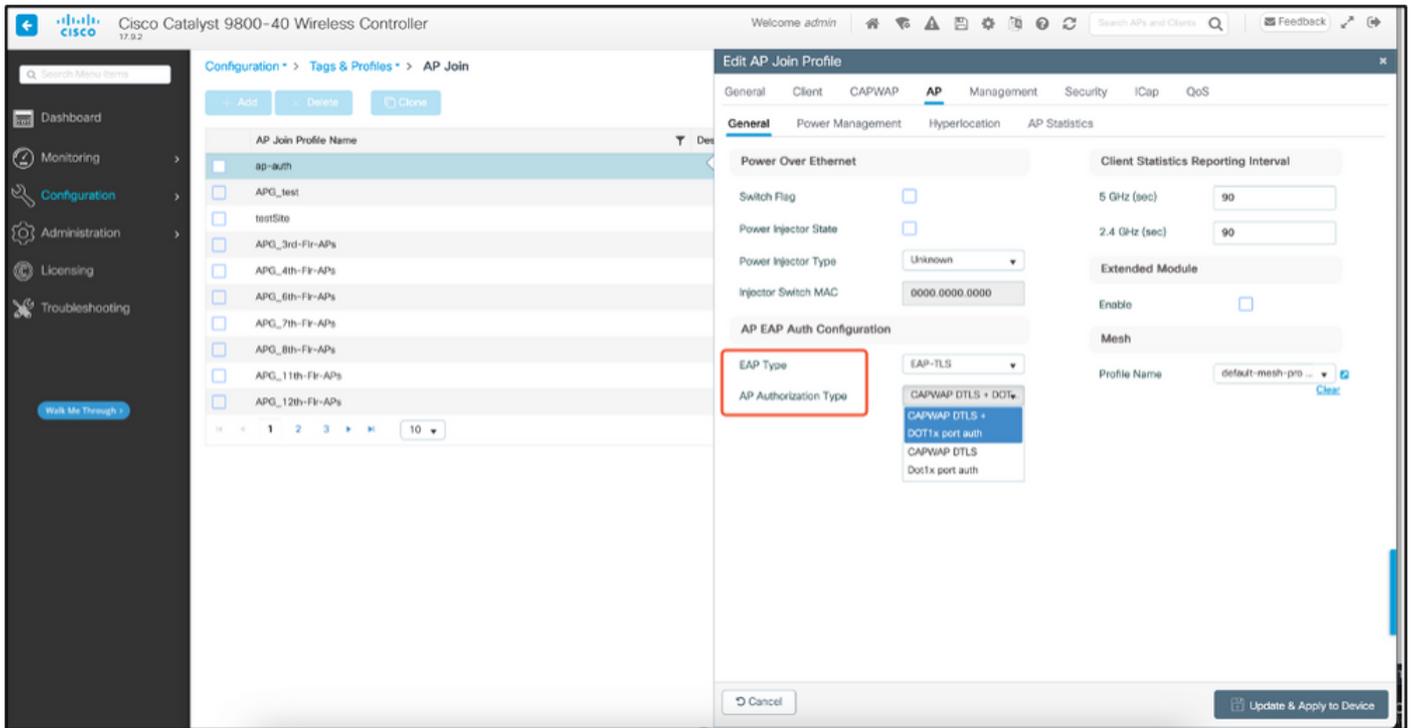


## Passi di configurazione dell'autenticazione 802.1x per dispositivi cablati AP

1. Abilitare dot1x port auth insieme a CAPWAP DTLS e selezionare il tipo EAP.
2. Creare credenziali dot1x per i punti di accesso.
3. Abilitare dot1x sulla porta dello switch.
4. Installare un certificato attendibile nel server RADIUS.

## Configurazione GUI autenticazione 802.1x cablata AP

1. Passare al profilo di join AP e fare clic sul profilo.
  1. Fare clic su AP > Generale. Selezionare il tipo EAP e il tipo di autorizzazione AP come "CAPWAP DTLS + dot1x port auth".
  2. Selezionare Gestione > Credenziali e creare un nome utente e una password per l'autenticazione AP dot1x.



## Configurazione CLI autenticazione 802.1x cablata AP

Usare questi comandi per abilitare il dot1x per gli access point dalla CLI. In questo modo viene abilitata solo l'autenticazione cablata per i punti di accesso che utilizzano il profilo di join specifico.

```
#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123
```

```
9808-48(config)#ap profile ap-auth
9808-48(config-ap-profile)#dot1x cap-type cap-tls
9808-48(config-ap-profile)#dot1x lsc-ap-auth-state both
9808-48(config-ap-profile)#
```

## Configurazione switch di autenticazione 802.1x cablato AP

Queste configurazioni dello switch vengono usate in LAB per abilitare l'autenticazione tramite cavo AP. È possibile avere configurazioni diverse in base al progetto.

```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

## Installazione certificato server RADIUS

L'autenticazione viene eseguita tra il punto di accesso (che agisce come supplicant) e il server RADIUS. Entrambi devono considerare attendibile l'altro certificato. L'unico modo per fare in modo che l'access point consideri attendibile il certificato del server RADIUS è che il server RADIUS utilizzi un certificato rilasciato dalla CA SCEP che ha rilasciato anche il certificato dell'access point.

In ISE, andare a Amministrazione > Certificati > Genera richieste di firma del certificato

Generare un CSR e compilare i campi con le informazioni del nodo ISE.

### Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

**ISE Identity Certificates:**

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.
- Data Connect Certificate - Connect to Oracle Database

**ISE Certificate Authority Certificates:**

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

**Usage**

Certificate(s) will be used for **EAP Authentication**

Allow Wildcard Certificates

**Node(s)**

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ISE99	ISE99#EAP Authentication

**Subject**

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Una volta generato, potete esportarlo e copiarlo e incollarlo come testo.

Passare all'indirizzo IP della CA di Windows e aggiungere /certsrv/ all'URL

Fare clic su Richiedi certificato

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Fare clic su Invia una richiesta di certificato utilizzando una base 64 ....

← ↻ Non sécurisé | 192.168.1.98/certsrv/certrqad.asp

Microsoft Active Directory Certificate Services – mydomain-WIN-3E2021QD0U-CA

### Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- [Create and submit a request to this CA.](#)
- [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

Incollare il testo CSR nella casella di testo. Scegliere il modello di certificato del server Web.

← ↻ Non sécurisé | 192.168.1.98/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – mydomain-WIN-3E2021QD0U-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

**Certificate Template:**

(No templates found) ▾

**Additional Attributes:**

Attributes:

È quindi possibile installare il certificato in ISE tornando al menu Richiesta di firma del certificato e facendo clic su Binding del certificato. È quindi possibile caricare il certificato ottenuto dall'unità C di Windows.

☰ Cisco ISE Administration - System

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority >

## Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click this list.

🔍 View 📄 Export 🗑️ Delete 🔗 Bind Certificate

<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
<input checked="" type="checkbox"/>	ISE99#EAP Authentication	CN=ISE99.mydomain.local	4096		Mon, 30 Oct 2023	ISE99

## Verifica autenticazione 802.1x cablata AP

Accedere alla console al punto di accesso ed eseguire il comando:

```
#show ap authentication status
```

Autenticazione app non abilitata:

```
AP0CD0.F89A.46E0#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E0#
```

Registri console da AP dopo l'abilitazione dell'autenticazione AP:

```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

Autenticazione del punto di accesso completata:

```
AP0CD0.F89A.46E0#sho ap authentication status
dot1x mgmt IEEE 802.1X (no WPA)
dot1x state=COMPLETED
address=0c:d0:f8:9a:46:e0
supplicant PAK state=AUTHENTICATED
supplicantStatus=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
dot1x_tls_version=TLSv1.2
EAP TLS cipher=ECDSA-RSA-AES256-GCM-SHA384
tls_session_reused=0
dot1x_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ca2bdd11f40494a4325dc98d1919af48b9f33ce526f18eda11effcb2ea0238cf95244aaf5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

Verifica WLC:

```
9800-40#sho ap name AP0CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate Expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-DTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 802.1x LSC Status
Certificate status : Available
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP LSC authentication state : CAPWAP-DTLS and 802.1x authentication
```

Stato interfaccia Switchport dopo autenticazione riuscita:

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
-----
Gi1/0/2 0cd0.f89a.46e0 dot1x DATA Auth 9765690A0000005CCEED0FBF
```

Di seguito è riportato un esempio di log della console del punto di accesso che indica la riuscita dell'autenticazione:

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
```

```
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 comp1
```

## Risoluzione dei problemi di autenticazione 802.1X

Prendere PCAP sul collegamento uplink AP e verificare l'autenticazione radius. Di seguito è riportato un frammento di autenticazione riuscita.

479.	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, Identity[Packet size limited during capture]
479.	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2	Encrypted Handshake Message
479.	07:47:17.256975	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.267976	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.270982	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.274979	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.277983	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.311988	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.324988	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2	Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, (Change Cipher Spec, Encrypted Handshake M...
479.	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)[Packet size limited during capture]
479.	07:47:17.376978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Accept id=251

TCPdump collect da ISE, acquisire l'autenticazione.

80	07:47:17.192983	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
80	07:47:17.205983	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
80	07:47:17.256975	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
79	07:47:17.267976	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
79	07:47:17.270982	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
79	07:47:17.274979	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
79	07:47:17.277983	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
78	07:47:17.311988	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
78	07:47:17.318968	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
78	07:47:17.324988	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
78	07:47:17.342969	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=250
80	07:47:17.376978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Challenge id=250
80	07:47:17.384978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Request id=251
82	07:47:01.945978	10.186.34.178	10.185.101.151	RADIUS	1812 55431 Access-Accept id=251

In caso di problemi durante l'autenticazione, sarà necessaria l'acquisizione simultanea di pacchetti da un uplink cablato AP e dal lato ISE.

Comando debug per AP:

```
#debug ap authentication packet
```

## Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- [Configurazione di 802.1X sull'access point con AireOS](#)
- [Guida alla configurazione di 9800 per LSC](#)
- [Esempio di configurazione LSC per 9800](#)
- [Configurazione di 802.1X per i punti di accesso su 9800](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).