Configurazione di SCEP per il provisioning di certificati importanti a livello locale su 9800 WLC

Sommario

Introduzione

In questo documento viene descritto come configurare il controller WLC 9800 per la registrazione di certificati LSC (Locally Significant Certificate) ai fini dell'aggiunta al punto di accesso tramite le funzionalità NDES (Network Device Enrollment Service) e SCEP (Simple Certificate Enrollment Protocol) di Windows Server 2012 R2 Standard.

Prerequisiti

Per eseguire correttamente SCEP con Windows Server, il WLC 9800 deve soddisfare i seguenti requisiti:

- Deve essere possibile raggiungere il controller e il server.
- Il controller e il server sono sincronizzati allo stesso server NTP o condividono la stessa data e lo stesso fuso orario (se l'ora tra il server CA e quella dell'access point è diversa, l'access point ha problemi con la convalida e l'installazione dei certificati).

Sul server di Windows deve essere attivato in precedenza Internet Information Services (IIS).

Requisiti

Cisco raccomanda la conoscenza delle seguenti tecnologie:

- Controller LAN wireless 9800 versione 16.10.1 o successiva.
- Microsoft Windows Server 2012 Standard.
- Infrastruttura a chiave privata (PKI) e certificati.

Componenti usati

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

- Software 9800-L WLC versione 17.2.1.
- Windows Server 2012 Standard R2.
- Access point 3802.

> **Nota:** La configurazione sul lato server di questo documento è specificamente SCEP WLC. Per ulteriori informazioni su configurazioni di server avanzate, di sicurezza e certificati, fare riferimento a Microsoft TechNet.

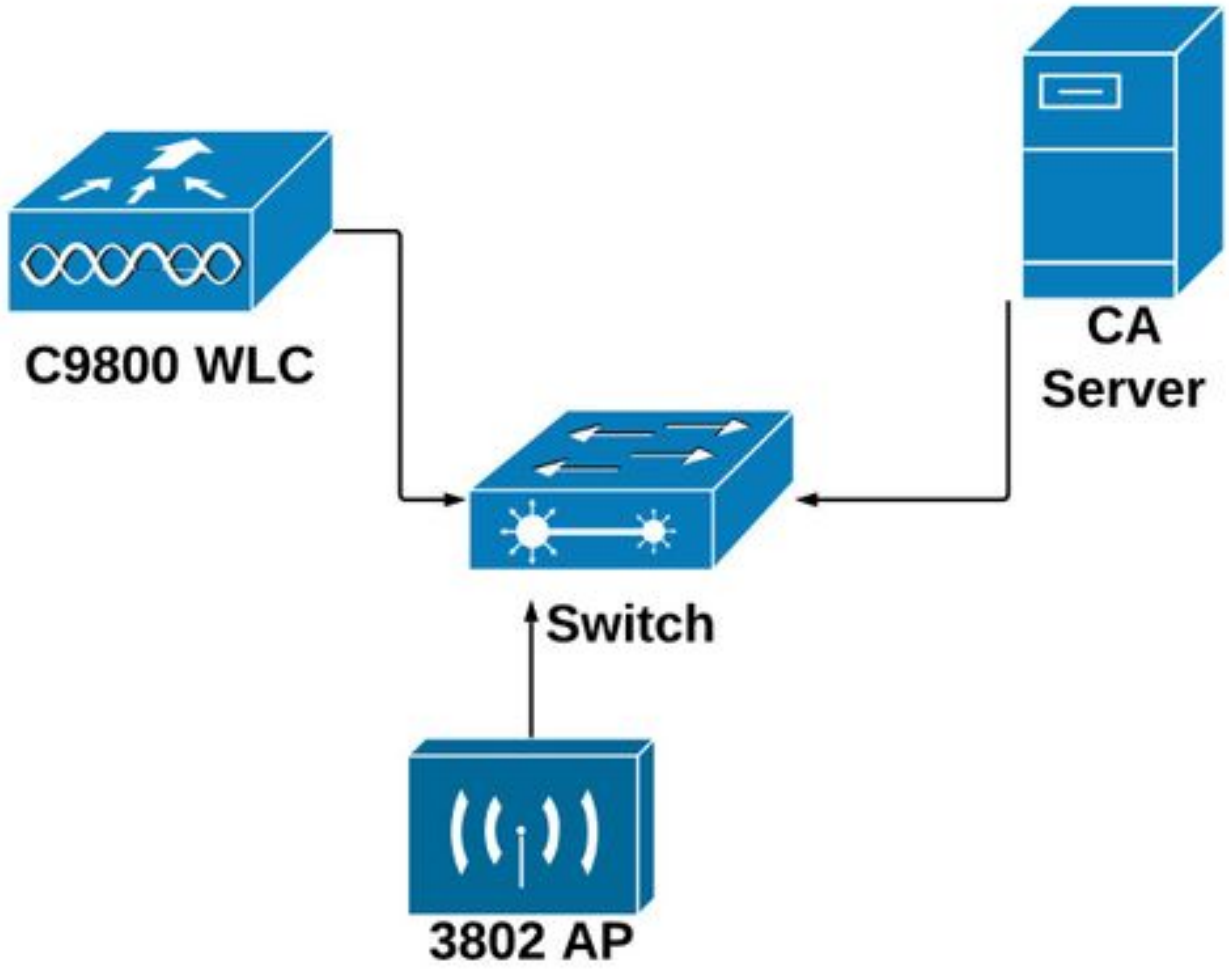
Premesse

I nuovi certificati LSC, sia il certificato radice CA (Certification Authority) che il certificato del dispositivo, devono essere installati nel controller per essere scaricati nei punti di accesso. Con SCEP, i certificati della CA e dei dispositivi vengono ricevuti dal server CA e successivamente installati automaticamente nel controller.

lo stesso processo di certificazione avviene quando i punti di accesso sono dotati di punti di accesso protetti; a tale scopo, il controller funge da proxy CA e contribuisce a ottenere la richiesta di certificato (generata automaticamente) firmata dalla CA per l'access point.

Configurazione

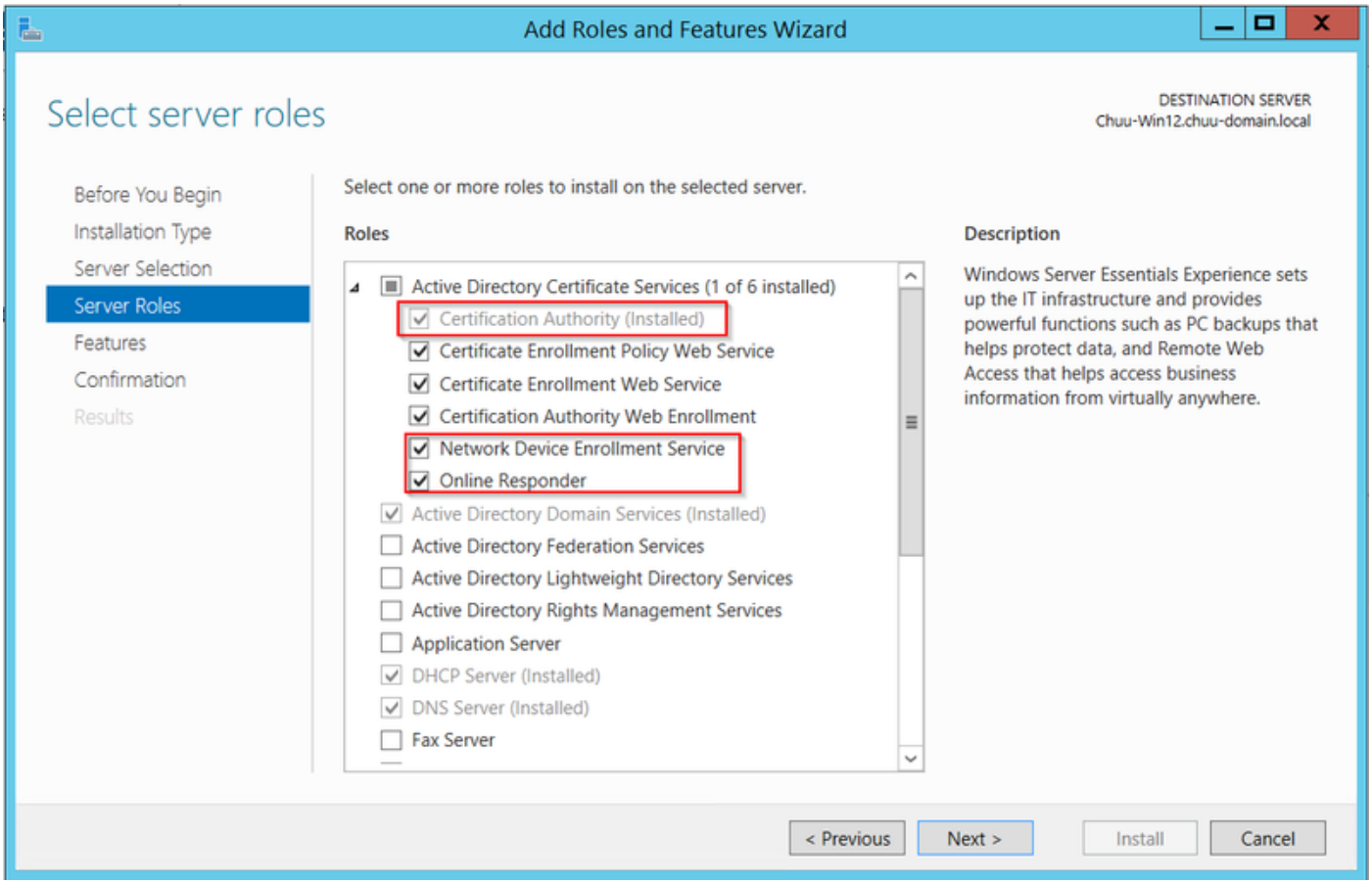
Esempio di rete



Abilitare i servizi SCEP in Windows Server

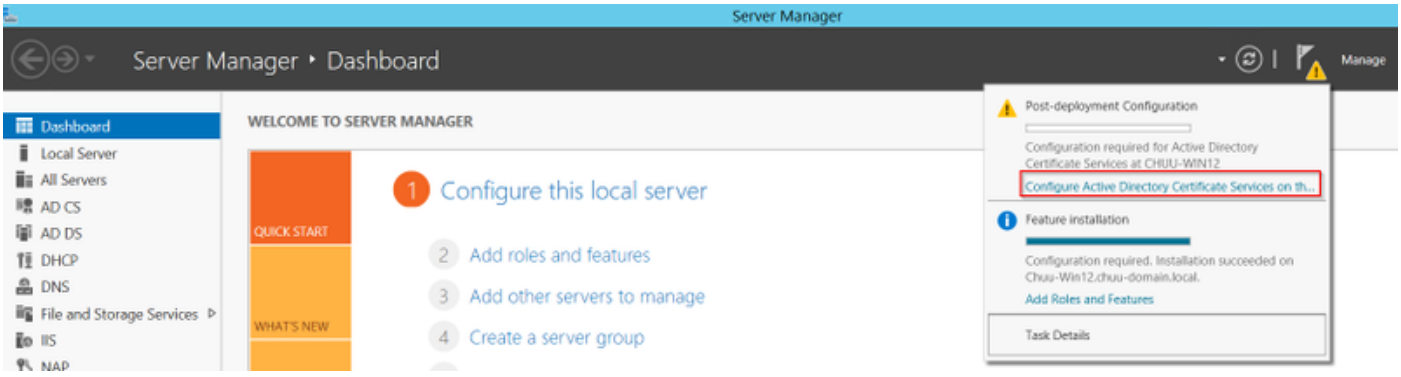
Passaggio 1. Nell'applicazione **Server Manager**, selezionare il menu **Gestisci**, quindi selezionare l'opzione **Aggiungi ruoli e funzionalità** per aprire la Configurazione guidata Aggiungi ruoli e funzionalità. Selezionare l'istanza del server utilizzata per la registrazione del server SCEP.

Passaggio 2. Verificare che le funzionalità **Certification Authority, Network Device Enrollment Service** e **Online Responder** siano selezionate, quindi selezionare **Avanti**:



Passaggio 3. Selezionare **Avanti** due volte, quindi **Fine** per terminare la configurazione guidata. **Attendere il completamento del processo di installazione delle funzionalità da parte del server, quindi selezionare Chiudi** per chiudere la procedura guidata.

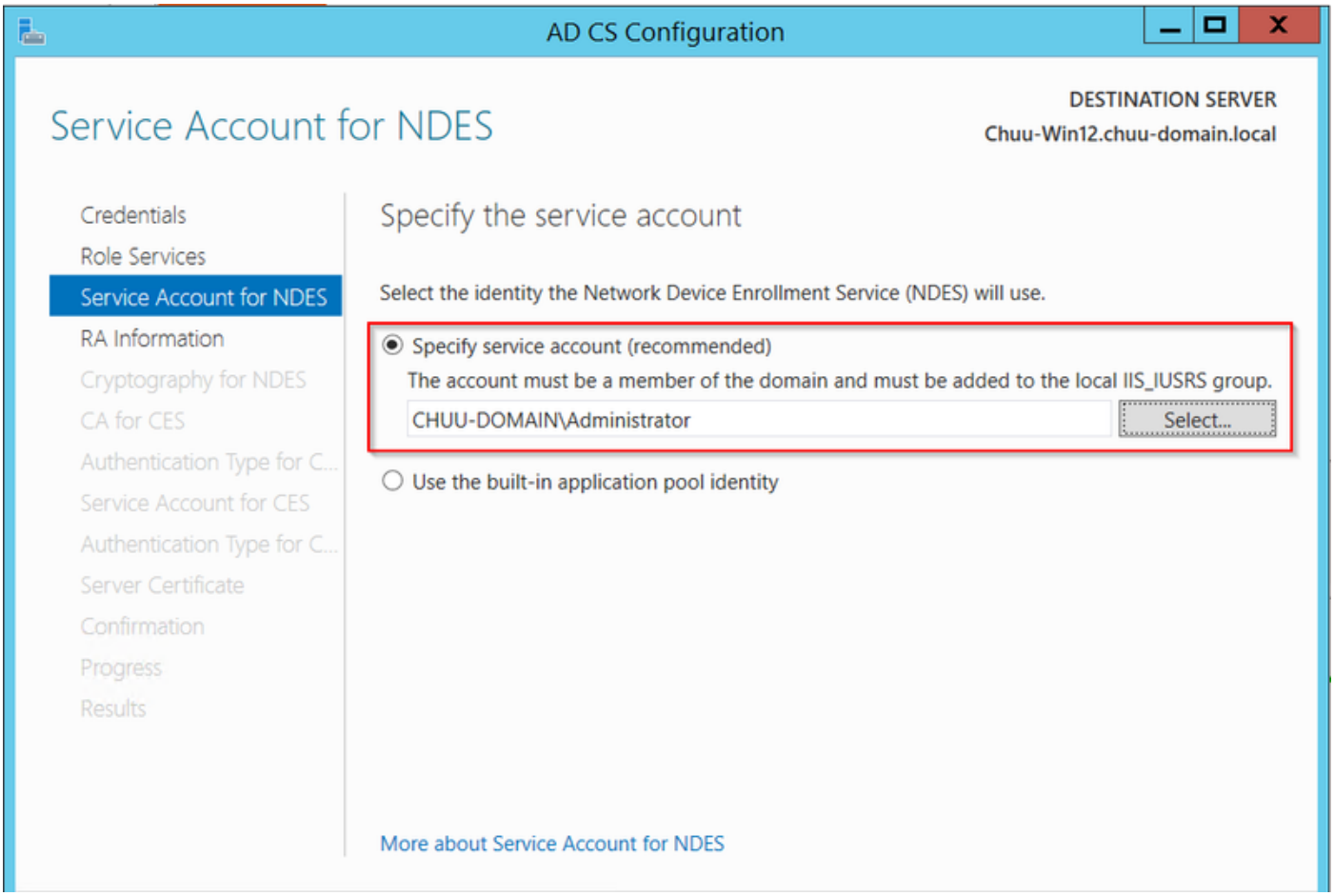
Passaggio 4. Al termine dell'installazione, viene visualizzata un'icona di avviso nell'icona di notifica di Server Manager. Selezionare l'opzione e fare clic sul collegamento **Configura servizi Active Directory nel server di destinazione** per avviare il menu **Configurazione** guidata Servizi certificati Active Directory.



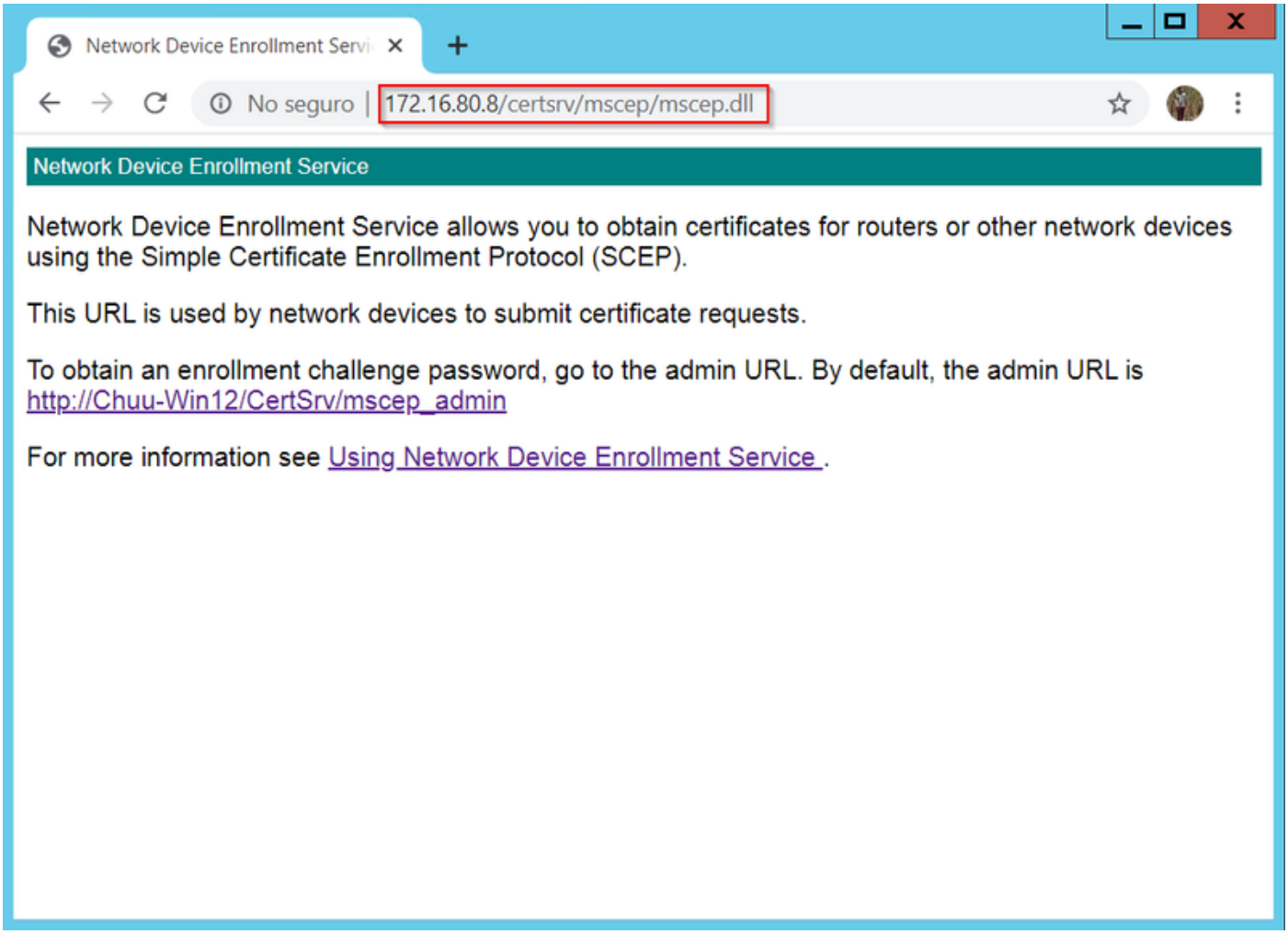
Passaggio 5. Selezionare il **servizio Registrazione dispositivi di rete** e i servizi ruolo **Risponditore in linea** da configurare nel menu, quindi scegliere **Avanti**.

Passaggio 6. In **Account di servizio per NDES** selezionare un'opzione tra il pool di applicazioni predefinito o l'account di servizio, quindi scegliere **Avanti**.

Nota: Se l'account del servizio fa parte del gruppo **IIS_IUSRS**.



Passaggio 7. Selezionare **Avanti** per le schermate successive e attendere il completamento del processo di installazione. Dopo l'installazione, l'URL SCEP sarà disponibile con qualsiasi browser Web. Passare all'URL **http://<server ip>/certsrv/mscep/mscep.dll** per verificare che il servizio sia disponibile.



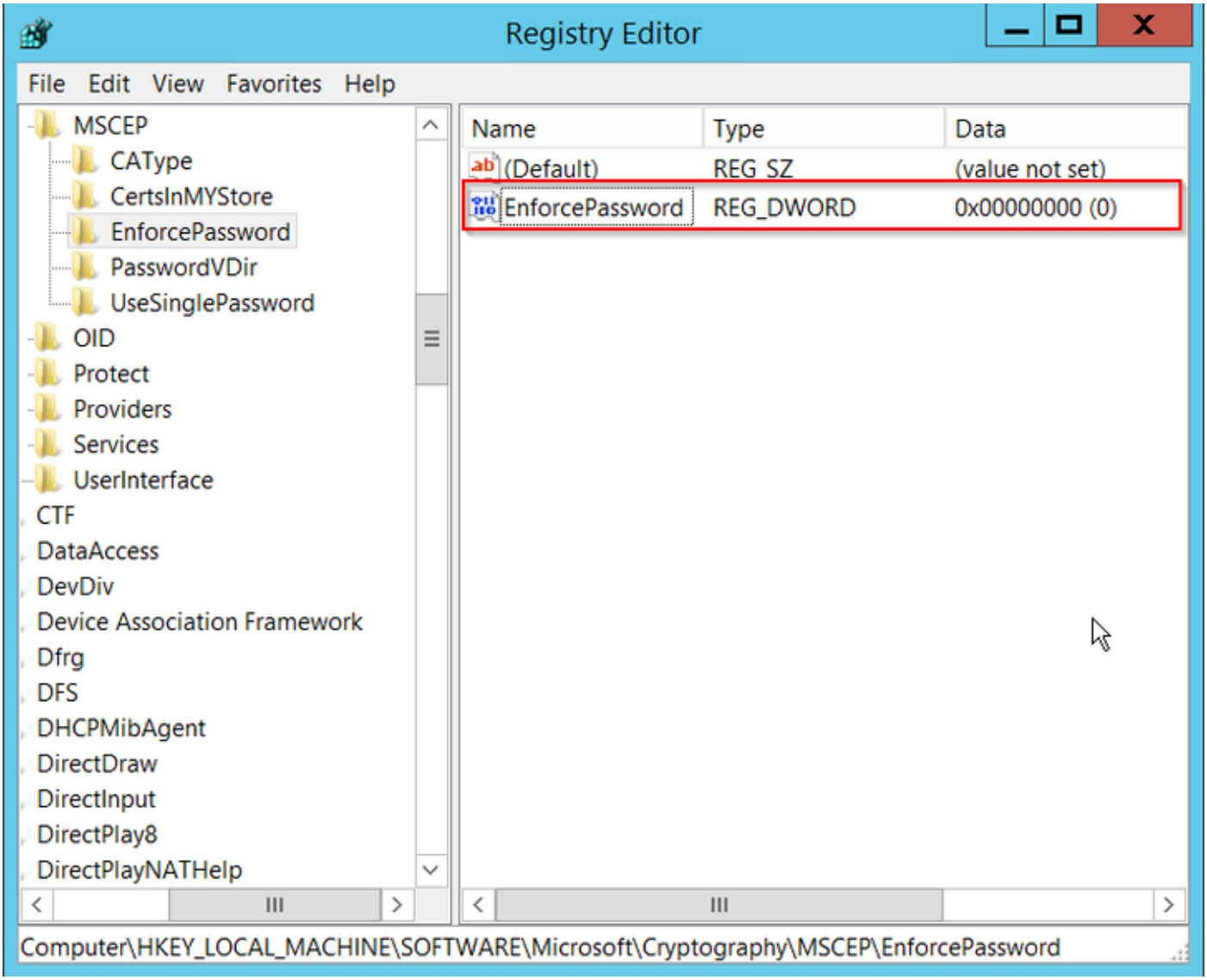
Disabilita requisito password di verifica registrazione SCEP

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:

Passaggio 1. Aprire l'Editor del Registro di sistema, cercare **Regedit** nel menu **Start**.

Passaggio 2. Passare a **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP > EnforcePassword**

Passaggio 3. Modificare il valore di **EnforcePassword** su 0. Se è già 0, lasciarlo invariato.



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:

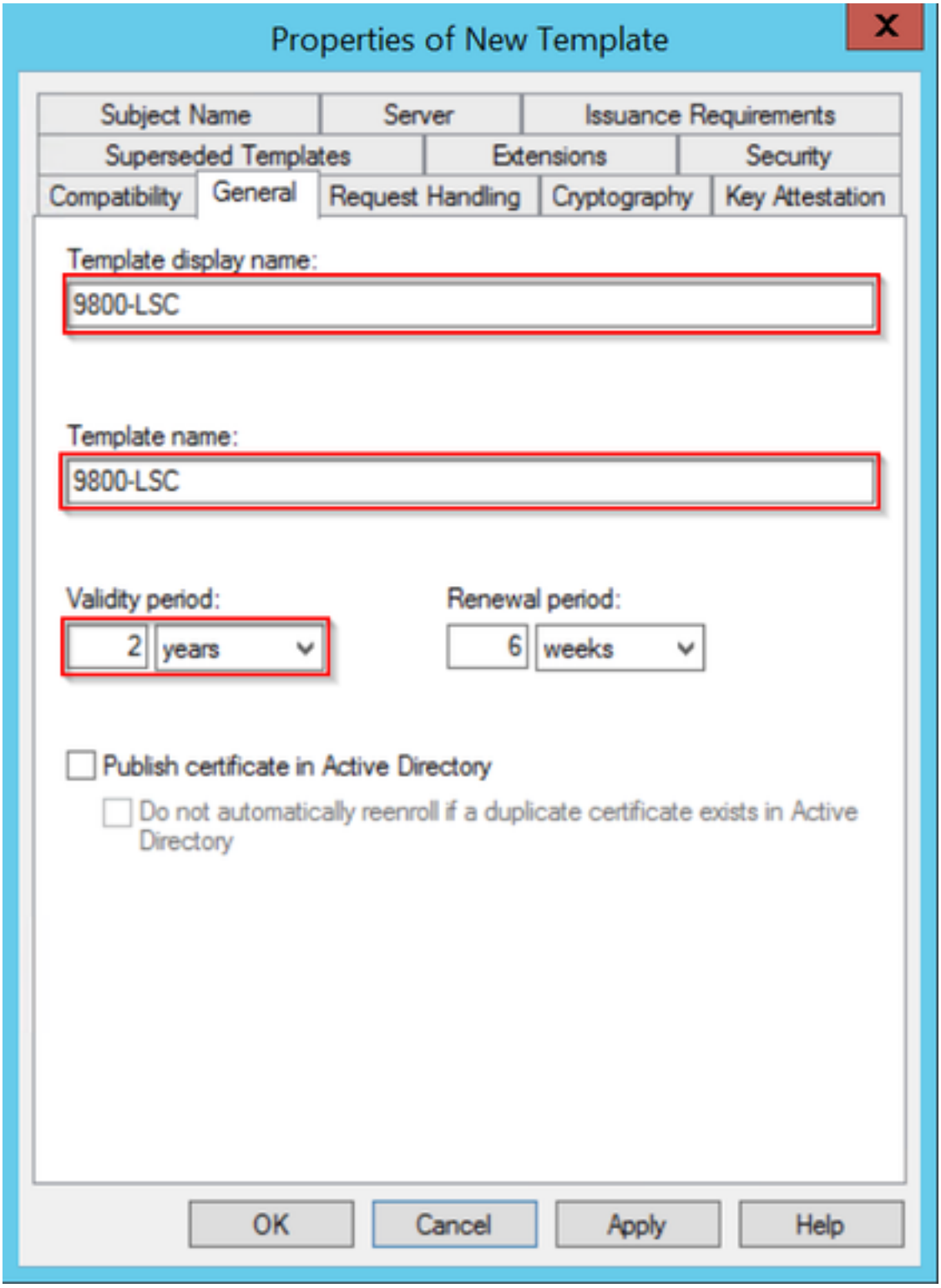
Passaggio 1. Passare a **Start > Strumenti di amministrazione > Autorità di certificazione**.

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**.

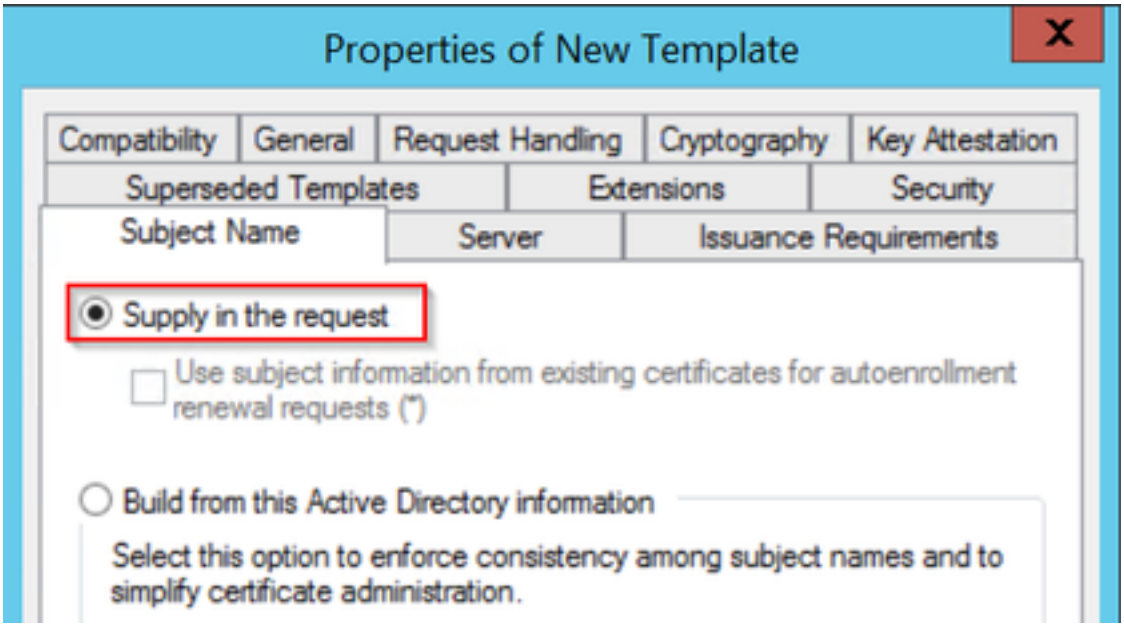
Passaggio 3. Fare clic con il pulsante destro del mouse sul modello di certificato **Users**, quindi selezionare **Duplica modello** nel menu di scelta rapida.

Passaggio 4. Passare alla scheda **Generale**, modificare il nome del modello e il periodo di validità come desiderato, lasciare deselezionate tutte le altre opzioni.

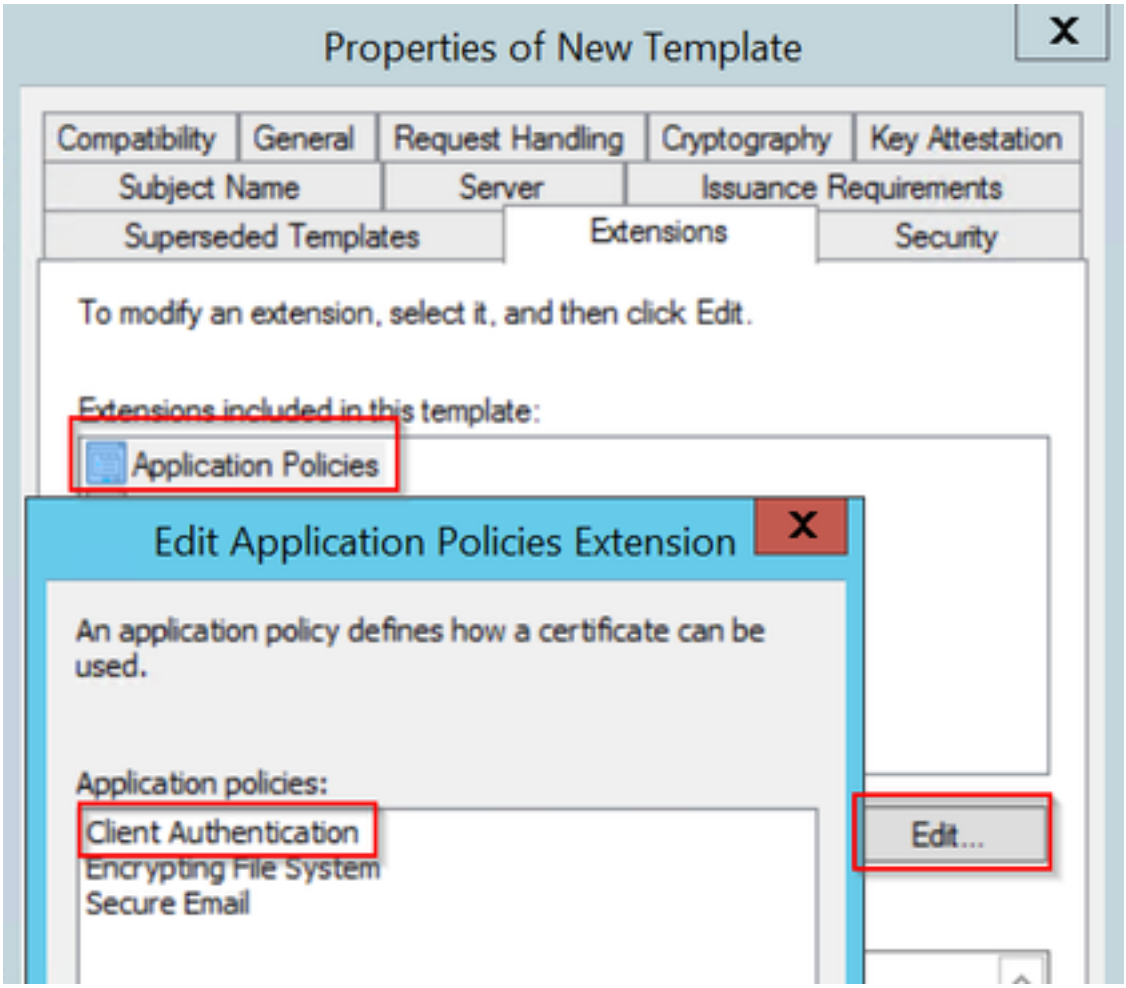
> **Attenzione:** Quando il periodo di validità viene modificato, verificare che non sia maggiore della validità del certificato radice dell'Autorità di certificazione.



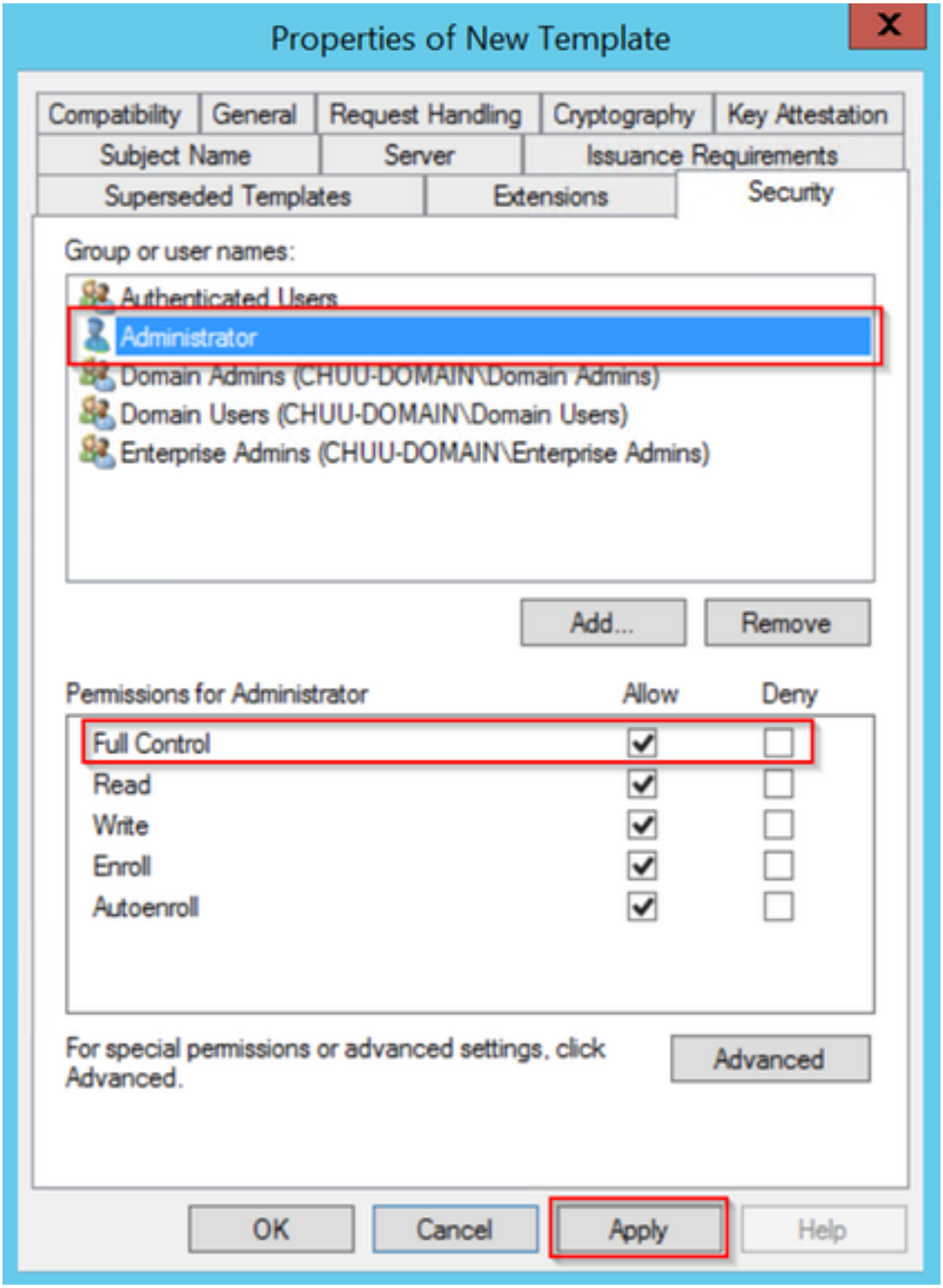
Passaggio 5. Passare alla scheda **Nome soggetto** e assicurarsi che **nella richiesta** sia selezionata **Fornitura**. Viene visualizzato un popup che indica che gli utenti non hanno bisogno dell'approvazione dell'amministratore per ottenere la firma del certificato. Selezionare **OK**.



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 applicazione**; in caso contrario, selezionare **Aggiungi** e aggiungerlo.



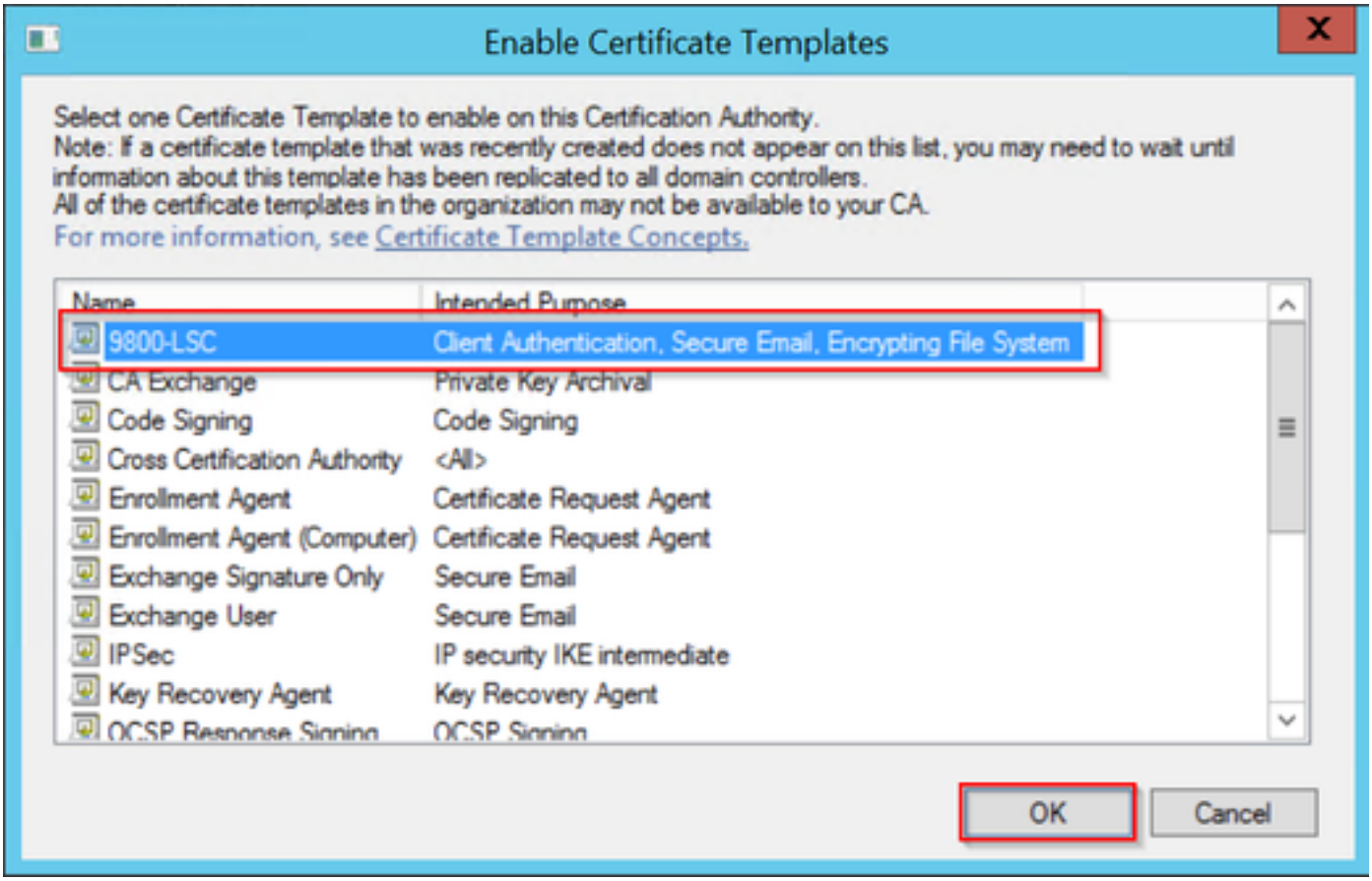
Passaggio 7. Passare alla scheda Protezione, verificare che l'account del servizio definito nel passaggio 6 di Abilita servizi SCEP in Windows Server disponga delle autorizzazioni **Controllo completo** del modello, quindi selezionare **Applica** e **OK**.



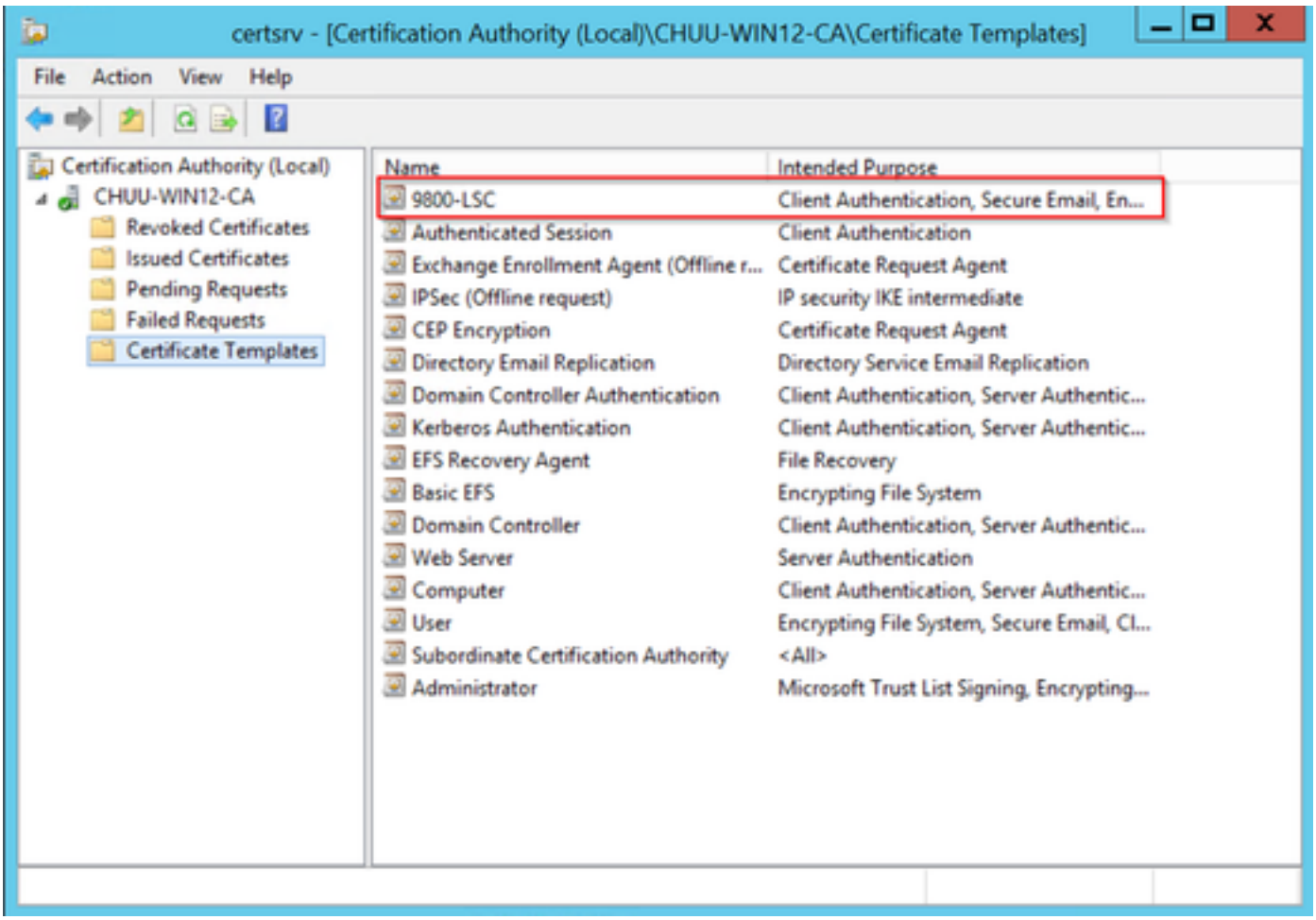
Passaggio 8. Tornare alla finestra **Autorità di certificazione**, fare clic con il pulsante destro del mouse nella cartella **Modelli di certificato** e selezionare **Nuovo > Modello di certificato da rilasciare**.

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 potrebbe richiedere più tempo per essere elencato in più distribuzioni server, in quanto deve essere replicato in tutti i server.



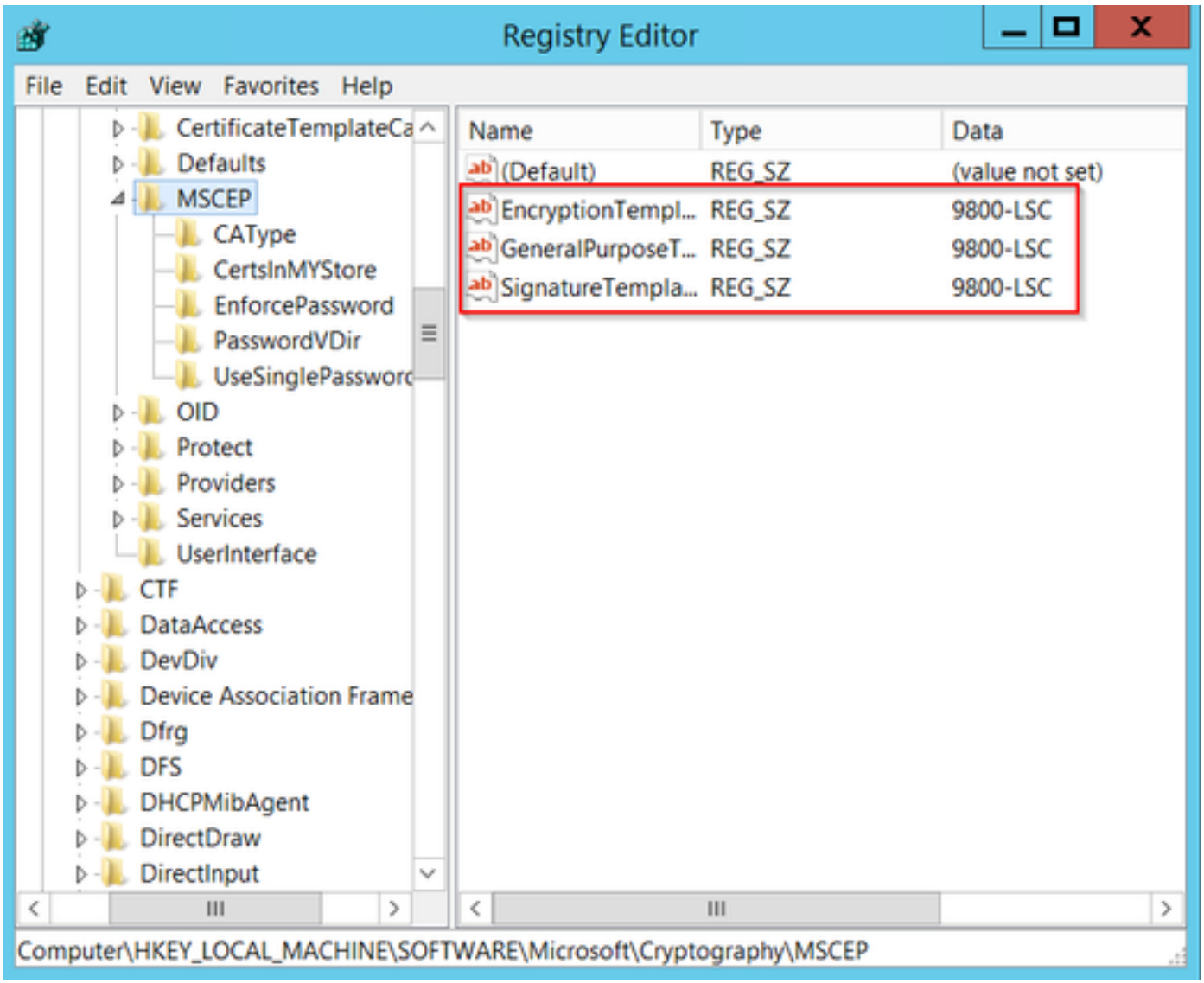
Il nuovo modello di certificato è ora elencato nel contenuto della cartella **Modelli di certificato**.



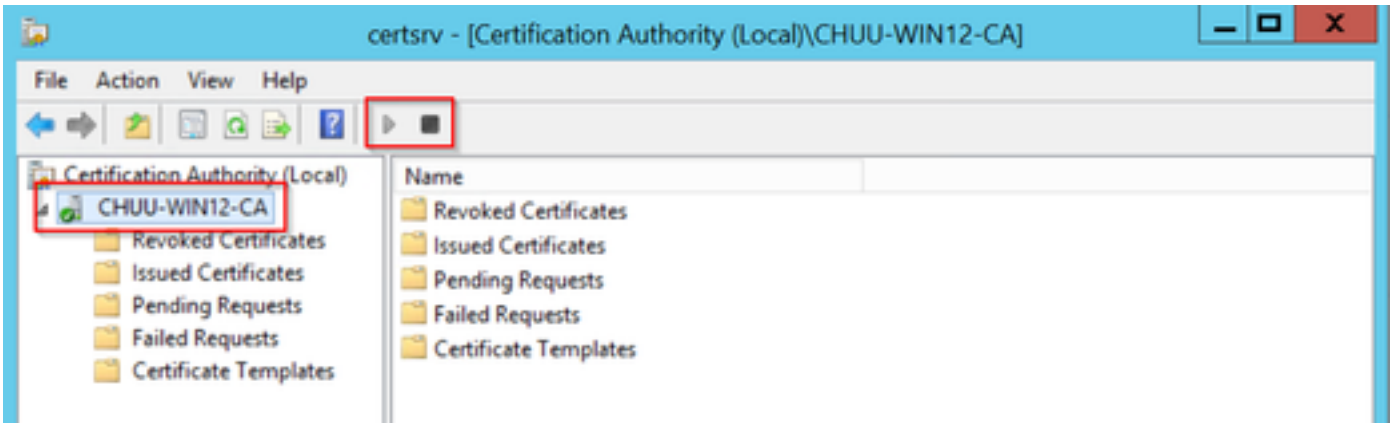
Passaggio 10. Tornare alla finestra **Editor del Registro di sistema** e selezionare **Computer >**

HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Crittografia > MSCEP.

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



Passaggio 12. Riavviare il server NDES, quindi tornare alla finestra **Autorità di certificazione**, selezionare il nome del server e scegliere il pulsante **Stope Play in seguito.**



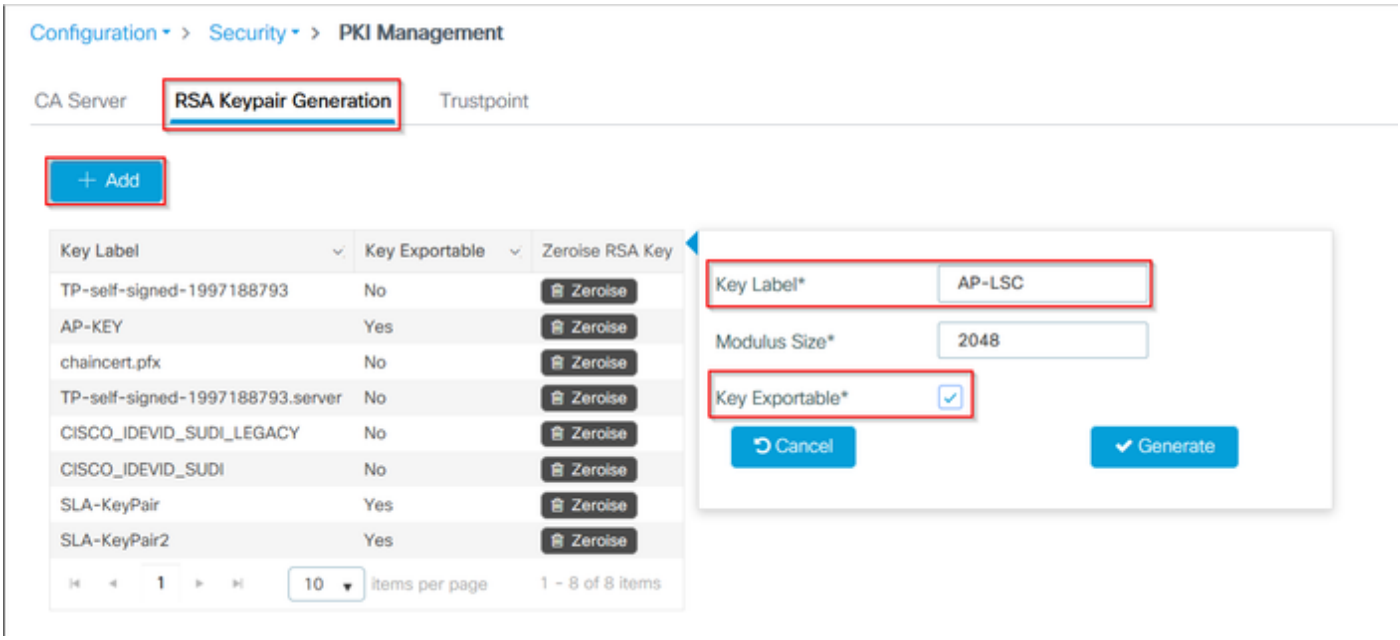
Configurazione del trust tra dispositivi 9800

Per autenticare gli access point dopo il provisioning, è necessario che nel controller sia stato

definito un trust point. Il trust point include il certificato del dispositivo 9800, insieme al certificato radice CA ottenuto dallo stesso server CA (in questo esempio Microsoft CA). Per poter essere installato nel trust point, un certificato deve contenere gli attributi del soggetto e una coppia di chiavi RSA associate. La configurazione viene eseguita tramite l'interfaccia Web o la riga di comando.

Passaggio 1. Passare a **Configurazione > Sicurezza > Gestione PKI** e selezionare la scheda **Generazione coppia di chiavi RSA**. Selezionare il pulsante **+ Aggiungi**.

Passaggio 2. Definire un'etichetta associata alla coppia di chiavi e assicurarsi che la casella di controllo **Esportabile** sia selezionata.



Configurazione CLI per i passaggi 1 e 2. In questo esempio di configurazione, la coppia di chiavi è generata con etichetta AP-LSC e dimensioni del modulo di 2048 bit:

```
9800-L(config)#crypto key generate rsa exportable general-keys modulus
```

```
The name for the keys will be: AP-LSC

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
```

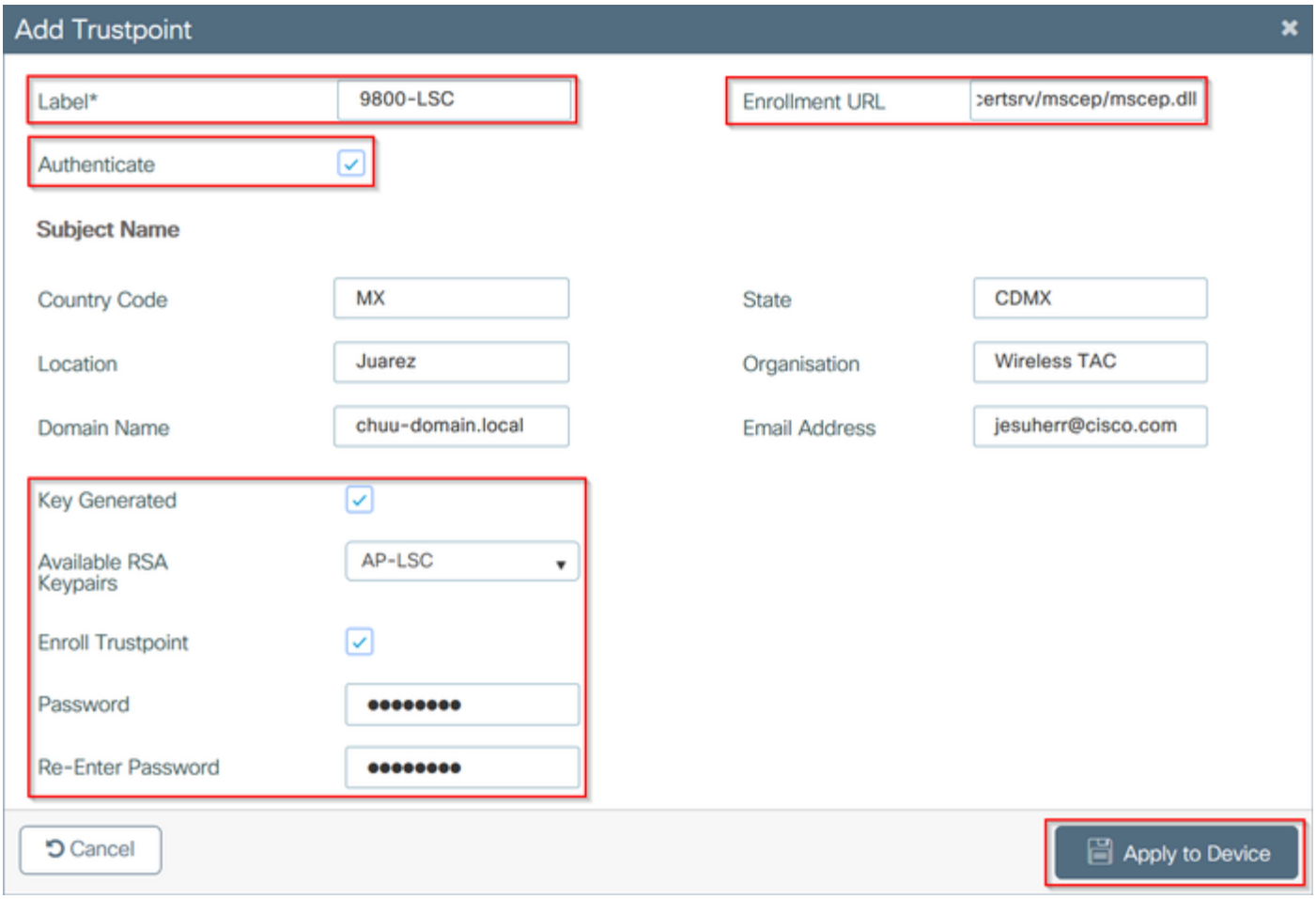
Passaggio 3. All'interno della stessa sezione, selezionare la scheda **Trustpoint** e scegliere il pulsante **+ Aggiungi**.

Passaggio 4. Inserire i dettagli del trust point con le informazioni sul dispositivo, quindi selezionare **Applica al dispositivo**:

- Il campo **Etichetta** è il nome associato al trust point
- Per l'**URL di registrazione,** utilizzare quello definito nel passaggio 7 della sezione **Abilitazione dei servizi SCEP in Windows Server**.
- Selezionare la casella di controllo **Autentica** per scaricare il certificato CA

- Il campo **Nome dominio** viene inserito come attributo nome comune della richiesta di certificato
- Selezionare la casella di controllo **Key Generated** (Generato da chiave), viene visualizzato un menu a discesa, selezionare la coppia di chiavi generata al punto 2
- Selezionare la casella di controllo **Registra trust point**, vengono visualizzati due campi password; digitare una password. Utilizzato per concatenare le chiavi del certificato con il certificato del dispositivo e il certificato della CA

Avviso: Il controller 9800 non supporta le catene di server multilivello per l'installazione di LSC, quindi la CA radice deve essere quella che firma le richieste di certificato dal controller e dagli access point.



Configurazione CLI per i passaggi tre e quattro:

Attenzione: La riga di configurazione del nome soggetto deve essere formattata con la sintassi LDAP. In caso contrario, non verrà accettata dal controller.

```
9800-L(config)#crypto pki trustpoint
```

```
9800-L(ca-trustpoint)#enrollment url http://
```

```
9800-L(ca-trustpoint)#subject-name C=




9800-L(ca-trustpoint)#rsakeypair




9800-L(ca-trustpoint)#revocation-check none
9800-L(ca-trustpoint)#exit
9800-L(config)#crypto pki authenticate




Certificate has the following attributes:
       Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
      Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-L(config)#crypto pki enroll <trustpoint name>
%
% 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:
Re-enter password:

% The subject name in the certificate will include: C=MX, ST=CDMX, L=Juarez, O=Wireless TAC,
CN=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
% The subject name in the certificate will include: 9800-L.alzavala.local
% Include the router serial number in the subject name? [yes/no]: no
% 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 AP-LSC' commandwill show the fingerprint.
```

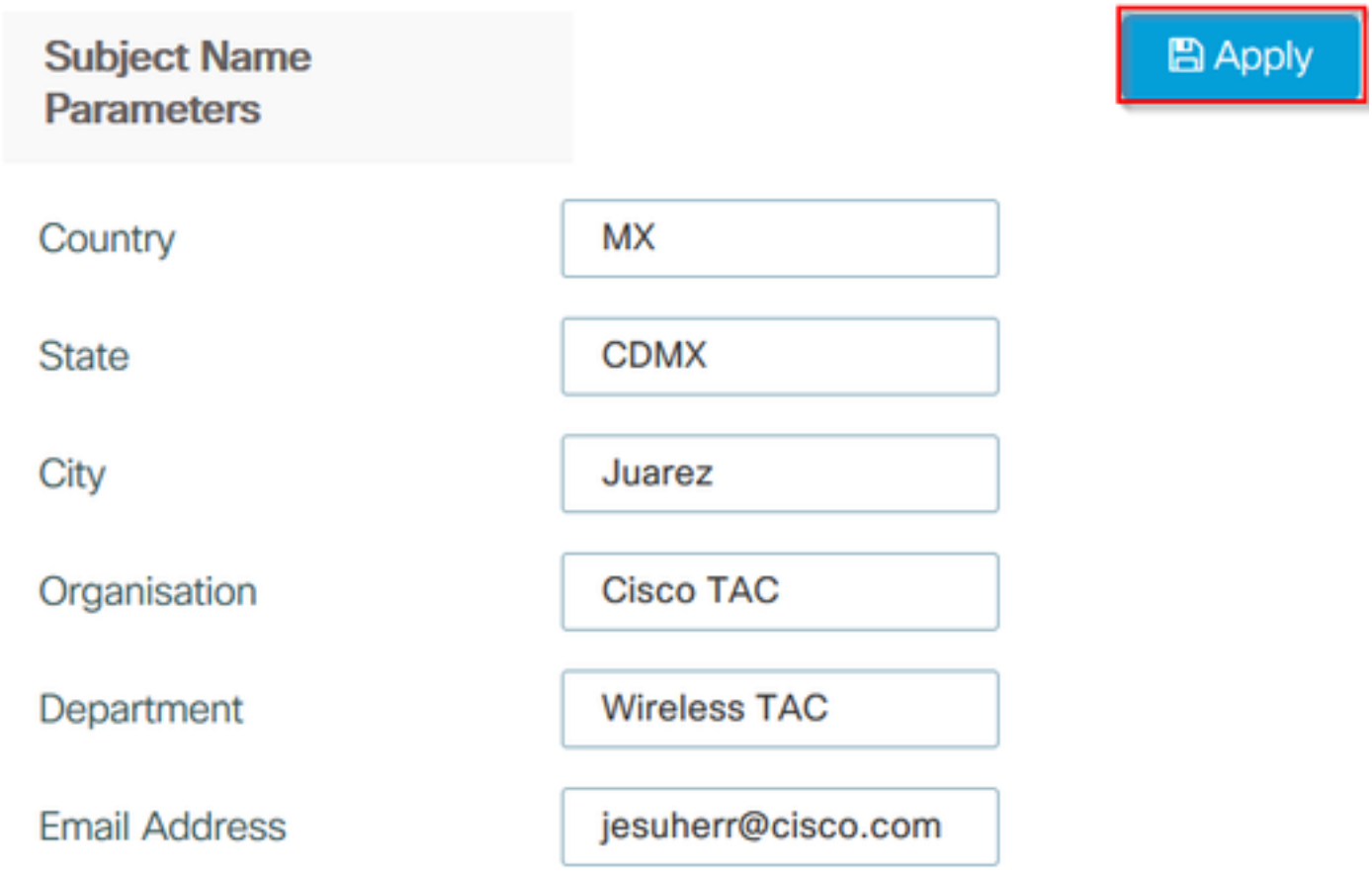
Definizione dei parametri di iscrizione AP e aggiornamento del trust di gestione

La registrazione AP utilizza i dettagli del trust point definiti in precedenza per determinare i dettagli del server a cui il controller inoltra la richiesta di certificato. Poiché il controller viene utilizzato come proxy per la registrazione dei certificati, è necessario conoscere i parametri del soggetto inclusi nella richiesta di certificato. La configurazione viene eseguita tramite l'interfaccia Web o la riga di comando.

Passaggio 1. Passare a **Configurazione > Wireless > Access Point** ed espandere il menu **LSC Provision**.

Passaggio 2. Inserire nei **Parametri nome soggetto** gli attributi specificati nelle richieste di

certificati AP, quindi selezionare **Applica**.

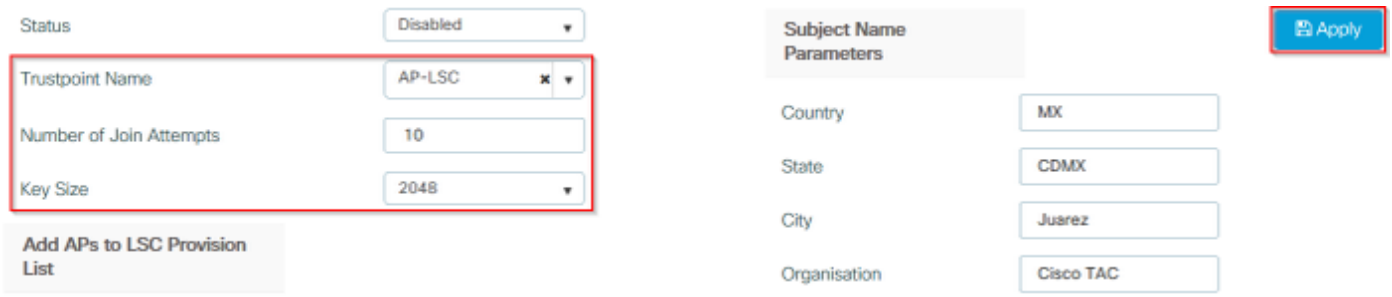


Configurazione CLI per i passaggi uno e due:

```
9800-L(config)#ap lsc-provision subject-name-parameter country
```

> **Nota**:i parametri Subject-name limitati a 2 caratteri come il codice del paese devono essere rigorosamente rispettati, poiché il WLC 9800 non convalida tali attributi.
> Per ulteriori informazioni consultare il documento CSCvo72999 difettoso come riferimento.

Passaggio 3. Nello stesso menu, selezionare il trustpoint definito in precedenza dall'elenco a discesa, specificare un numero di tentativi di join AP (questo definisce il numero di tentativi di join prima che utilizzi nuovamente il MIC) e impostare le dimensioni della chiave del certificato. Quindi fare clic su **Apply** (Applica).



Configurazione CLI per il passaggio tre:

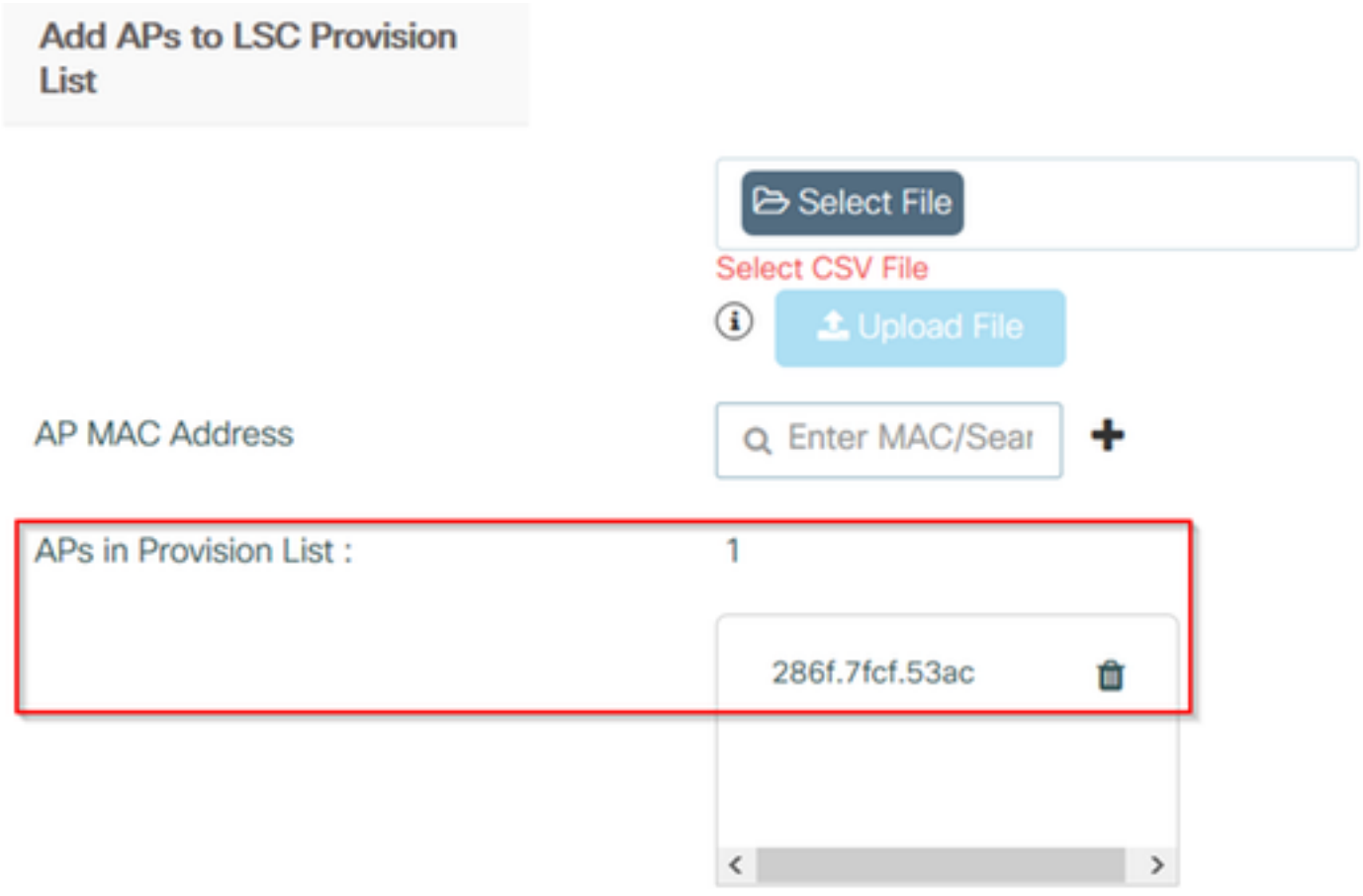
```
9800-L(config)#ap lsc-provision join-attempt
```

```
9800-L(config)#ap lsc-provision trustpoint
```

```
9800-L(config)#ap lsc-provision key-size
```

Passaggio 4. (Facoltativo) Il provisioning LSC AP può essere attivato per tutti gli AP aggiunti al controller o per specifici AP definiti in un elenco indirizzi MAC. Nello stesso menu, immettere l'indirizzo MAC Ethernet AP nel formato xxxx.xxxx.xxxx nel campo di testo e fare clic sul segno **+**. In alternativa, caricare un file csv che contiene gli indirizzi mac AP, selezionare il file e selezionare **Upload File** (Carica file).

> **Nota:** Il controller ignora qualsiasi indirizzo MAC nel file CSV che non riconosce dal proprio elenco di punti di accesso uniti.



Configurazione CLI per il passaggio 4:

```
9800-L(config)#ap lsc-provision mac-address
```

Passaggio 5. Selezionare **Abilitato** o **Elenco provisioning** dal menu a discesa accanto all'etichetta **Status**, quindi fare clic su **Apply** to Trigger AP LSC enrolllement.

> **Nota:** I punti di accesso iniziano la richiesta, il download e l'installazione del certificato. Una volta completata l'installazione del certificato, l'access point si riavvia e avvia il processo di unione con il nuovo certificato.

> **Suggerimento**: Se il provisioning LSC AP viene eseguito tramite un controller di pre-produzione utilizzato insieme all'elenco di provisioning, non rimuovere le voci AP dopo il provisioning del certificato. In questo caso, se gli access point eseguono il fallback su MIC e si uniscono allo stesso controller di pre-produzione, i relativi certificati LSC vengono cancellati.

Configurazione CLI per il passaggio cinque:

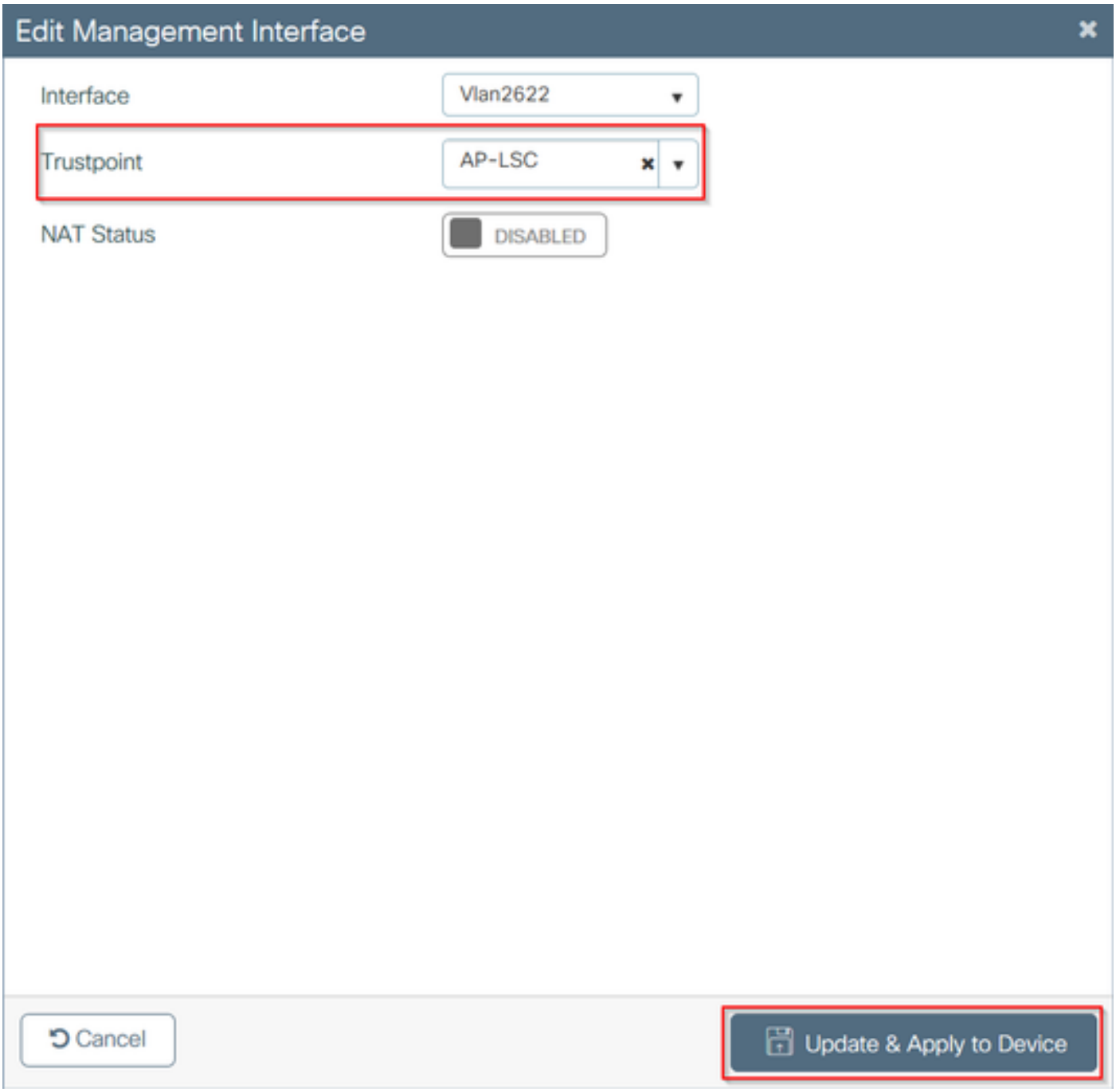
```
9800-L(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size
configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key
by-default or 256 bit key if configured.
Are you sure you want to continue? (y/n): y If specific AP list provisioning is preferred then
use: 9800-L(config)#ap lsc-provision provision-list
```

Passaggio 6. Passare a **Configurazione > Interfaccia > Wireless** e selezionare l'interfaccia di gestione. Nel campo **Trustpoint**, selezionare il nuovo trust point dal menu a discesa e fare clic su **Aggiorna e applica al dispositivo**.

> **Attenzione:** Se LSC è abilitato ma il trust point del WLC 9800 si riferisce al MIC o a un SSC, gli AP tentano di unirsi all'LSC per il numero configurato di tentativi di join. Una volta raggiunto il limite massimo di tentativi, i punti di accesso tornano al MIC e si uniscono nuovamente, ma poiché il provisioning LSC è abilitato, i punti di accesso richiedono un nuovo LSC. In questo modo si verifica un loop in cui il server CA firma costantemente i certificati per gli stessi access point e gli access point bloccati in un loop di richiesta di join e riavvio.

> **Nota:** Dopo l'aggiornamento del trust point di gestione per l'utilizzo del certificato LSC, i nuovi AP non potranno unirsi al controller con il MIC. Attualmente non è disponibile alcun supporto per aprire una finestra di accantonamento. Se è necessario installare nuovi access point, è necessario eseguire in precedenza il provisioning di tali access point con un LSC

firmato dalla stessa CA di quello presente nel trust point di gestione.



Configurazione CLI per la fase sei:

```
9800-L(config)#wireless management trustpoint
```

Verifica

Verifica installazione certificato controller

Per verificare che le informazioni LSC siano presenti nel trust point WLC 9800, eseguire il

comando **show crypto pki certificates verbose <nome trust point>**, due certificati sono associati al trust point creato per il provisioning e la registrazione LSC. In questo esempio il nome del trust point è "microsoft-ca" (viene visualizzato solo l'output rilevante):

```
9800-L#show crypto pki certificates verbose microsoft-ca
Certificate
  Status: Available
  Version: 3
  Certificate Usage: General Purpose
  Issuer:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
  Subject:
    Name: 9800-L.alzavala.local
    cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
    o=Wireless TAC
    l=Juarez
    st=CDMX
    c=MX
    hostname=9800-L.alzavala.local
  CRL Distribution Points:
    ldap:///CN=CHUU-WIN12-CA,CN=Chuu-
Win12,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Coint
Validity Date:
start date: 04:25:59 Central May 11 2020
end date: 04:25:59 Central May 11 2022 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption [...] Authority Info
Access: CA ISSUERS: ldap:///CN=CHUU-WIN12-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=chuu-
domain,DC=local?cACertificate?base?objectClass=certificationAuthority [...] CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 37268ED56080CB974EF3806CCACC77EC
  Certificate Usage: Signature
  Issuer:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
  Subject:
    cn=CHUU-WIN12-CA
    dc=chuu-domain
    dc=local
 Validity Date:
start date: 05:58:01 Central May 10 2019
end date: 06:08:01 Central May 10 2024 Subject Key Info: Public Key Algorithm: rsaEncryption RSA
Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption
```

Verifica della configurazione 9800 WLC LSC

Per verificare i dettagli relativi al trust di gestione wireless eseguire il comando **show wireless management trustpoint**, verificare che il trust point corretto, ovvero quello che contiene i dettagli LSC, in questo esempio AP-LSC, sia in uso e contrassegnato come Disponibile:

```
9800-L#show wireless management trustpoint

Trustpoint  Name : AP-LSC
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
```

```
Private key Info : Available
```

Per verificare i dettagli sulla configurazione del provisioning LSC dell'access point e l'elenco degli access point aggiunti all'elenco di provisioning, eseguire il comando **show ap lsc-provision summary**. Verificare che venga visualizzato lo stato di provisioning corretto:

```
9800-L#show ap lsc-provision summary
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : AP-LSC
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : MX
State : CDMX
City : Juarez
Orgn : Cisco TAC
Dept : Wireless TAC
Email : josuvill@cisco.com
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses :
--------------
xxxx.xxxx.xxxx
xxxx.xxxx.xxxx
```

Verifica installazione certificato punto di accesso

Per verificare i certificati installati nell'access point, eseguire il comando **show crypto** dalla CLI dell'access point, verificare che siano presenti sia il certificato radice CA che il certificato del dispositivo (l'output mostra solo i dati pertinenti):

```
AP3802#show crypto

[...]
------------------------------------------------------------------------------ LSC: Enabled
---------------------------- Device Certificate -----------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:00:0b
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Validity
            Not Before: May 13 01:22:13 2020 GMT
            Not After : May 13 01:22:13 2022 GMT
        Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC, CN=ap3g3-
286F7FCF53AC/emailAddress=josuvill@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)

---------------------------- Root Certificate ------------------------------
Certificate:
    Data:
```

```
        Version: 3 (0x2)
        Serial Number:
            32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Validity
            Not Before: May 10 05:58:01 2019 GMT
            Not After : May 10 05:58:01 2024 GMT
        Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Se si utilizza l'autenticazione LSC per la porta dello switch dot1x, dal punto di accesso è possibile verificare se l'autenticazione della porta è abilitata.

```
AP3802#show ap authentication status
AP dot1x feature is disabled.
```

> **Nota:** Per abilitare la porta dot1x per i punti di accesso, è necessario definire le credenziali dot1x per i punti di accesso nel profilo del punto di accesso o nella configurazione del punto di accesso stessa con valori fittizi.

Risoluzione dei problemi

Problemi comuni

1. Se i modelli non sono mappati correttamente nel Registro di sistema del server o se il server richiede una richiesta di verifica della password, la richiesta di certificato per il WLC 9800 o gli access point viene rifiutata.
2. Se i siti predefiniti di IIS sono disabilitati, anche il servizio SCEP viene disabilitato, pertanto l'URL definito nel trust point non è raggiungibile e il WLC 9800 non invia alcuna richiesta di certificato.
3. Se l'ora non è sincronizzata tra il server e il WLC 9800, i certificati non vengono installati poiché il controllo della validità dell'ora ha esito negativo.

Comandi debug e log

Utilizzare questi comandi per risolvere i problemi relativi alla registrazione dei certificati dei controller 9800:

```
9800-L#debug crypto pki transactions
9800-L#debug crypto pki validation
9800-L#debug crypto pki scep
```

Per risolvere i problemi e monitorare la registrazione dei punti di accesso, utilizzare questi comandi:

```
AP3802#debug capwap client payload
AP3802#debug capwap client events
```

Dalla riga di comando dell'access point, il comando **show log** indica se l'access point ha avuto problemi con l'installazione del certificato e fornisce dettagli sul motivo per cui il certificato non è

stato installato:

```
[...]
Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.3429] AP has joined controller 9800-L Mar 19
19:39:13 kernel: 03/19/2020 19:39:13.3500] SELinux: initialized (dev mtd_inodefs, type
mtd_inodefs), not configured for labeling Mar 19 19:39:13 kernel: *03/19/2020 19:39:13.5982]
Generating a RSA private key Mar 19 19:39:14 kernel: *03/19/2020 19:39:13.5989]
..................... Mar 19 19:39:15 kernel: *03/19/2020 19:39:14.4179] .. Mar 19 19:39:15
kernel: *03/19/2020 19:39:15.2952] writing new private key to '/tmp/lsc/priv_key' Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.2955] ----- Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5421] cen_validate_lsc: Verification failed for certificate: Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] countryName = MX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421]
stateOrProvinceName = CDMX Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] localityName =
Juarez Mar 19 19:39:15 kernel: *03/19/2020 19:39:15.5421] organizationName = cisco-tac Mar 19
19:39:15 kernel: *03/19/2020 19:39:15.5421] commonName = ap3g3- Mar 19 19:39:15 kernel:
*03/19/2020 19:39:15.5421] emailAddress = jesuherr@cisco.com Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427] LSC certificates/key failed validation! Mar 19 19:39:15 kernel: *03/19/2020
19:39:15.5427]
```

Esempio di tentativo di registrazione riuscito

Di seguito viene riportato l'output dei debug citati per la corretta registrazione sia del controller che dei relativi access point associati.

Importazione certificato radice CA in 9800 WLC:

```
[...]
Certificate has the following attributes: Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B % Do you accept this certificate?
[yes/no]: yes CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA
Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-
LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8
CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened
CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0
(compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC,
refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length
received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length :
(3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0
CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert
Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:47:34 GMT Connection:
close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates.
CRYPTO_PKI_SCEP: Client received CA and RA certificate
CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3
certificates. CRYPTO_PKI:crypto_pkcs7_extract_ca_cert found cert CRYPTO_PKI: Bypassing SCEP
capabilities request 0 CRYPTO_PKI: transaction CRYPTO_REQ_CA_CERT completed CRYPTO_PKI: CA
certificate received. CRYPTO_PKI: CA certificate received. CRYPTO_PKI:
crypto_pki_get_cert_record_by_cert() CRYPTO_PKI: crypto_pki_authenticate_tp_cert() CRYPTO_PKI:
trustpoint AP-LSC authentication status = 0 Trustpoint CA certificate accepted.
```

9800 WLC device enrollment:

```
[...]
CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI_SCEP: Client sending GetCACert
request CRYPTO_PKI: Sending CA Certificate Request: GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent:
Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint
AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message
CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco
PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked
```

```
trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI_SCEP: Client Sending GetCACaps request with msg = GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACaps&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Header length received: 171 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (34) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: text/plain Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 34 CRYPTO_PKI: HTTP header content length is 34 bytes CRYPTO_PKI_SCEP: Server returned capabilities: 92 CA_CAP_RENEWAL CA_CAP_S alz_9800(config)#HA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: %PKI-6-CSR_FINGERPRINT: CSR Fingerprint MD5 : 9BFBA438303487562E888087168F05D4 CSR Fingerprint SHA1: 58DC7DB84C632A7307631A97A6ABCF65A3DEFEEF CRYPTO_PKI: Certificate Request Fingerprint MD5: 9BFBA438 30348756 2E888087 168F05D4 CRYPTO_PKI: Certificate Request Fingerprint SHA1: 58DC7DB8 4C632A73 07631A97 A6ABCF65 A3DEFEEF PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E 00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 65 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 66 CRYPTO_PKI: Expiring peer's cached key with key id 66 PKI: Trustpoint AP-LSC has no router cert PKI: Signing pkcs7 with AP-LSC trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2807) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: received msg of 2995 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 2807 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 66 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 67 CRYPTO_PKI: Expiring peer's cached key with key id 67 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (AF58BA9313638026C5DC151AF474723F) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Newly-issued Router Cert: issuer=cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial=1800043245DC93E1D943CA70000043 start date: 21:38:34 Central May 19 2020 end date: 21:38:34 Central May 19 2022 Router date: 21:48:35 Central May 19 2020 %PKI-6-CERT_INSTALL: An ID certificate has been installed under Trustpoint : AP-LSC Issuer-name : cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local Subject-name : cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com,o=Wireless TAC,l=Juarez,st=CDMX,c=MX,hostname=alz_9800.alzavala.local Serial-number: 1800000043245DC93E1D943CA7000000000043 End-date : 2022-05-19T21:38:34Z Received router cert from CA CRYPTO_PKI: Not adding alz_9800.alzavala.local to subject-alt-name field because : Character allowed in the domain name. Calling pkiSendCertInstallTrap to send alert CRYPTO_PKI: All enrollment requests completed for trustpoint AP-LSC
```

Output di debug della registrazione AP dal lato controller, questo output viene ripetuto più volte per ciascun AP collegato al WLC 9800:

```
[...]
CRYPTO_PKI: (A6964) Session started - identity selected (AP-LSC) CRYPTO_PKI: Doing re-auth to
```

fetch RA certificate. CRYPTO_PKI_SCEP: Client sending GetCACert request CRYPTO_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO_PKI: Header length received: 192 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO_PKI_SCEP: Client received CA and RA certificate CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI:crypto_pkcs7_insert_ra_certs found RA certs CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 PKCS10 request is compulsory CRYPTO_PKI: byte 2 in key usage in PKCS#10 is 0x5 May 19 21: alz_9800(config)#51:04.985: CRYPTO_PKI: all usage CRYPTO_PKI: key_usage is 4 CRYPTO_PKI: creating trustpoint clone Proxy-AP-LSC8 CRYPTO_PKI: Creating proxy trustpoint Proxy-AP-LSC8 CRYPTO_PKI: Proxy enrollment request trans id = 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: Proxy forwading an enrollment request CRYPTO_PKI: using private key AP-LSC for enrollment CRYPTO_PKI: Proxy send CA enrollment request with trans id: 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO_PKI: No need to re-auth as we have RA in place CRYPTO_PKI: Capabilites already obtained CA_CAP_RENEWAL CA_CAP_SHA_1 CA_CAP_SHA_256 CA_CAP_SHA_512 CRYPTO_PKI: transaction CRYPTO_REQ_CERT completed CRYPTO_PKI: status: PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 0F 0E 00 00 00 00 00 38 CRYPTO_PKI: Deleting cached key having key id 67 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 68 CRYPTO_PKI: Expiring peer's cached key with key id 68 PKI: Trustpoint Proxy-AP-LSC8 has no router cert and loaded PKI: Signing pkcs7 with Proxy-AP-LSC8 trustpoint temp self-signed cert CRYPTO_PKI_SCEP: Client sending PKCSReq CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: http connection opened CRYPTO_PKI: Sending HTTP message CRYPTO_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 3 CRYPTO_PKI: Header length received: 188 CRYPTO_PKI: parse content-length header. return code: (0) and content-length : (2727) CRYPTO_PKI: Complete data arrived CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO_PKI: received msg of 2915 bytes CRYPTO_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 2727 CRYPTO_PKI: Prepare global revocation service providers CRYPTO_PKI: Deleting cached key having key id 68 CRYPTO_PKI: Attempting to insert the peer's public key into cache CRYPTO_PKI:Peer's public inserted successfully with key id 69 CRYPTO_PKI: Expiring peer's cached key with key id 69 CRYPTO_PKI: Remove global revocation service providers The PKCS #7 message has 1 alz_9800(config)# verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO_PKI_SCEP: Client received CertRep - GRANTED (7CBB299A2D9BC77DBB1A8716E6474C0C) CRYPTO_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Received router cert from CA CRYPTO_PKI: Enrollment poroxy callback status: CERT_REQ_GRANTED CRYPTO_PKI: Proxy received router cert from CA CRYPTO_PKI: Rcvd request to end PKI session A6964. CRYPTO_PKI: PKI session A6964 has ended. Freeing all resources. CRYPTO_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO_PKI: Cleaning RA certificate for TP : AP-LSC CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO_CS: removing trustpoint clone Proxy-AP-LSC8

Output di debug registrazione AP dal lato AP:

```
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 40 len 407
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: CERTIFICATE_PARAMETER_PAYLOAD(63) vendId 409600
LSC set retry number from WLC: 1
```

```
Generating a RSA private key
...
..............................
writing new private key to '/tmp/lsc/priv_key'
-----
[ENC] CAPWAP_WTP_EVENT_REQUEST(9)
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) Len 1135 Total 1135
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 41 len 20
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_CERT_ENROLL_PENDING from WLC

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
Received Capwap watchdog update msg.
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 42 len 1277
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving ROOT_CERT

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 43 len 2233
..Vendor Type: SPAM_VENDOR_ID_PAYLOAD(104) vendId 409600
...Vendor SubType: LSC_CERTIFICATE_PAYLOAD(64) vendId 409600
LSC_ENABLE: saving DEVICE_CERT

SC private key written to hardware TAM

root: 2:  LSC enabled
AP Rebooting: Reset Reason - LSC enabled
```

In questo modo si conclude l'esempio di configurazione per la registrazione LSC tramite SCEP.