Configurer SCEP pour le provisionnement de certificats localement significatif sur le WLC 9800

Contenu

Introduction

Ce document décrit comment configurer le contrôleur de réseau local sans fil (WLC) 9800 pour l'inscription LSC (Certificat significatif localement) pour les fins de jonction de point d'accès (AP) via les fonctionnalités NDES (Network Device Enrollment Service) de Microsoft et SCEP (Simple Certificate Enrollment Protocol) dans la norme Windows Server 2012 R2.

Conditions préalables

Pour exécuter SCEP avec succès avec Windows Server, le WLC 9800 doit répondre aux conditions suivantes :

- Il doit y avoir une accessibilité entre le contrôleur et le serveur.
- Le contrôleur et le serveur sont synchronisés avec le même serveur NTP, ou partagent la même date et le même fuseau horaire (si l'heure est différente entre le serveur AC et l'heure de l'AP, l'AP a des problèmes avec la validation et l'installation du certificat).

Les services IIS (Internet Information Services) de Windows Server doivent être activés précédemment.

Conditions requises

Cisco recommande que vous connaissiez ces technologies :

- Contrôleur LAN sans fil 9800 version 16.10.1 ou ultérieure.
- Microsoft Windows Server 2012 Standard.
- Infrastructure à clé privée (PKI) et certificats.

Components Used

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

- Logiciel WLC 9800-L version 17.2.1.
- Windows Server 2012 Standard R2.
- 3802 Points d'accès.

> **Note**: La configuration côté serveur de ce document est spécifiquement WLC SCEP, pour plus de consolidation, de sécurité et de configurations de serveurs de certificats, référez-vous à Microsoft TechNet.

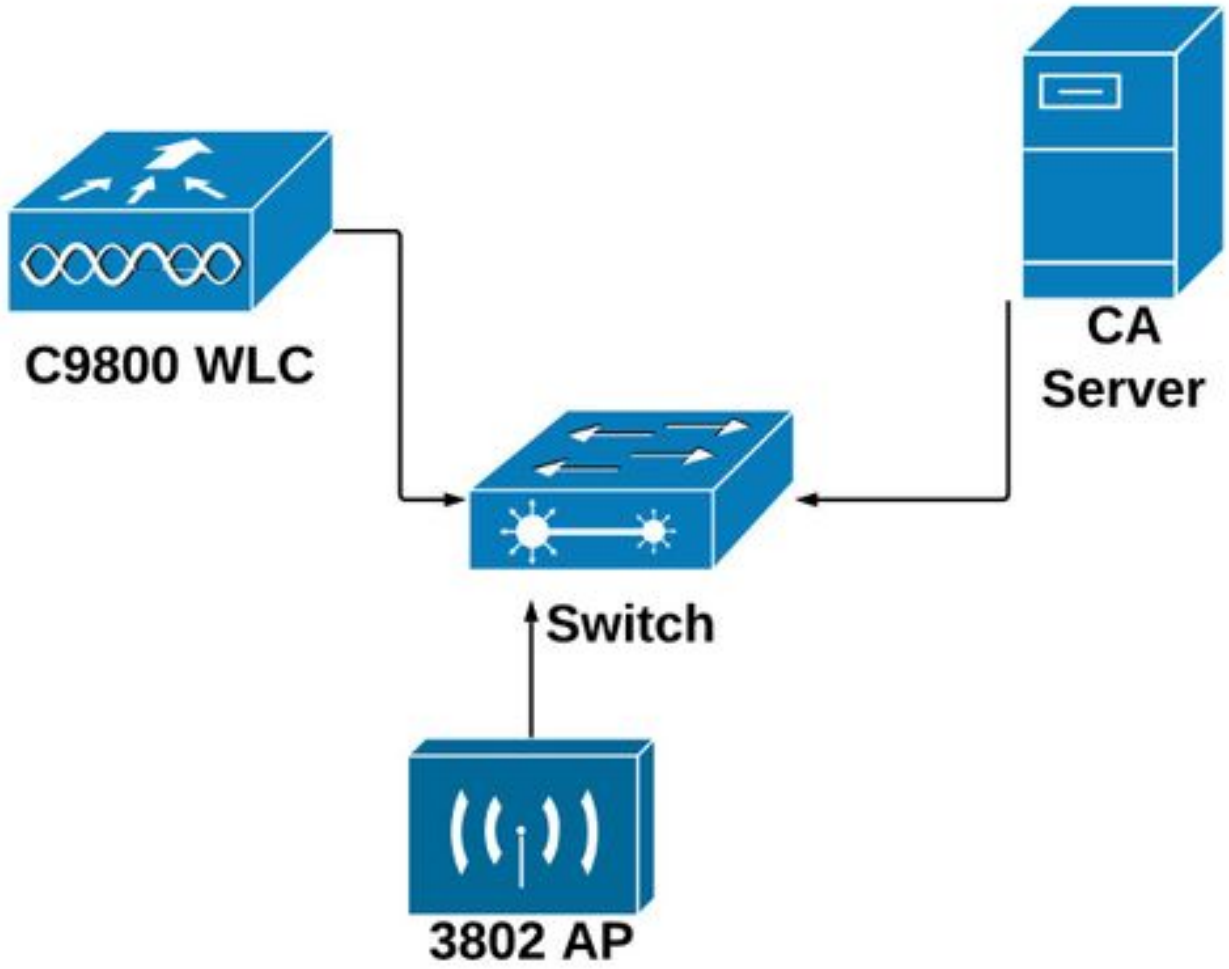
Informations générales

Les nouveaux certificats LSC, à la fois le certificat racine de l'autorité de certification (CA) et le certificat de périphérique, doivent être installés sur le contrôleur pour finalement le télécharger dans les points d'accès. Avec SCEP, l'autorité de certification et les certificats de périphérique sont reçus du serveur d'autorité de certification, puis installés automatiquement dans le contrôleur.

Le même processus de certification a lieu lorsque les points d'accès sont provisionnés avec des LSC ; pour ce faire, le contrôleur agit en tant que proxy CA et aide à obtenir la demande de certificat (auto-générée) signée par l'autorité de certification pour l'AP.

Configuration

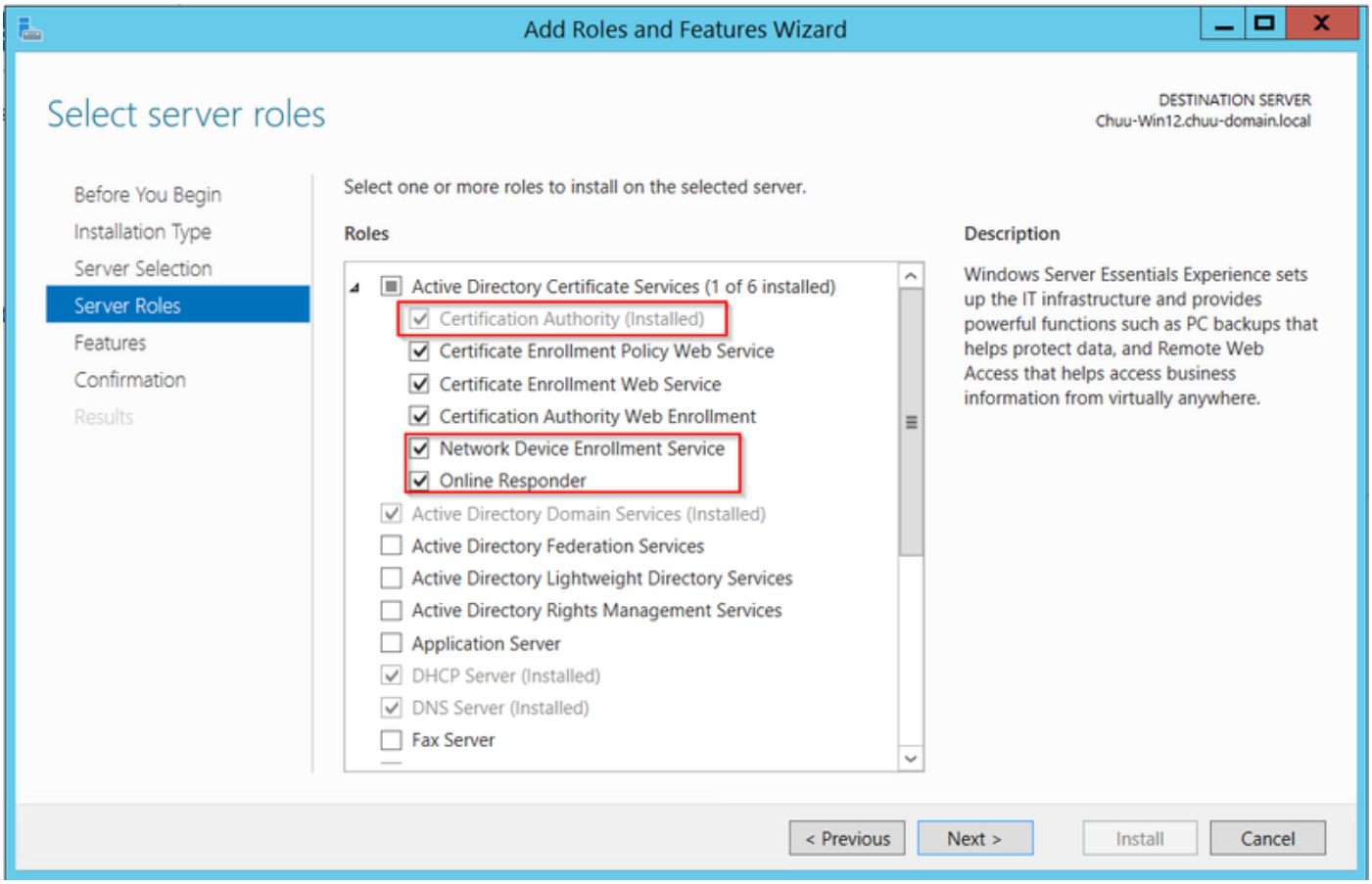
Diagramme du réseau



Activer les services SCEP dans Windows Server

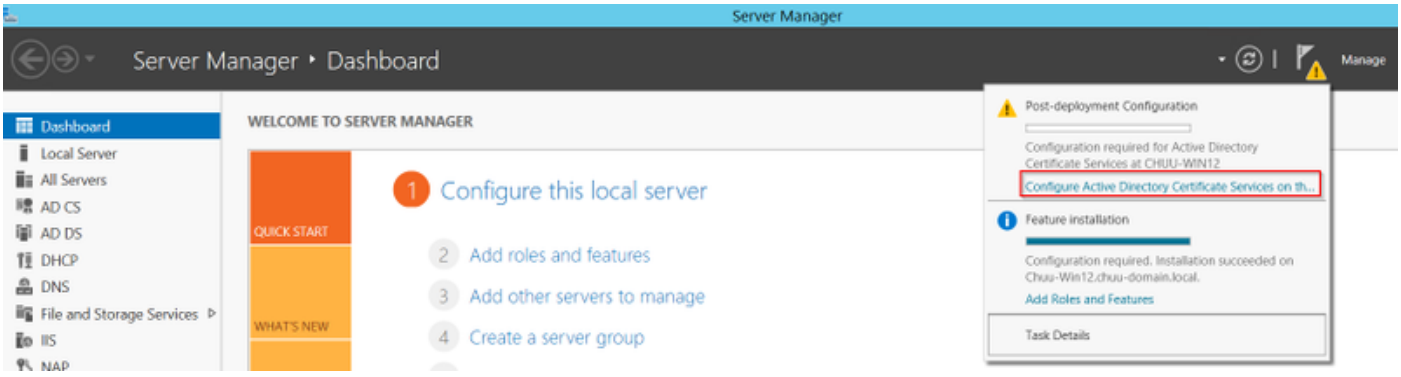
Étape 1. Dans l'application **Gestionnaire de serveur**, sélectionnez le menu **Gérer**, puis sélectionnez l'option **Ajouter des rôles et des fonctionnalités** pour ouvrir le rôle Assistant Ajout de rôles et de fonctionnalités. À partir de là, sélectionnez l'instance de serveur utilisée pour l'inscription au serveur SCEP.

Étape 2. Vérifiez que les fonctionnalités **Certification Authority**, **Network Device Enrollment Service** et **Online Responder** sont sélectionnées, puis sélectionnez **Next** :



Étape 3. Sélectionnez **Suivant** deux fois, puis **Terminer** pour mettre fin à l'assistant de configuration. Attendez que le serveur termine le processus d'installation des fonctionnalités, puis sélectionnez **Fermer** pour fermer l'Assistant.

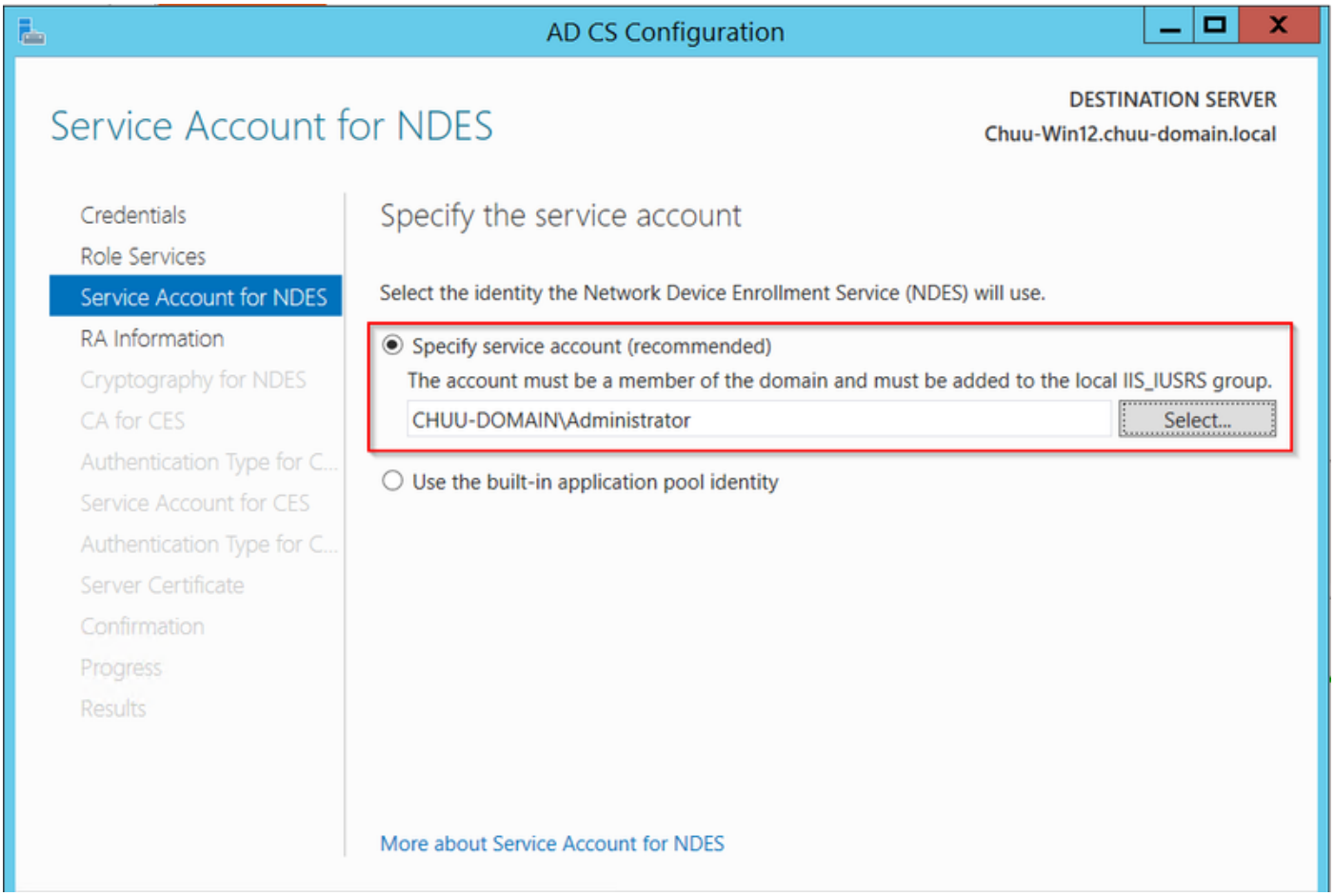
Étape 4. Une fois l'installation terminée, une icône d'avertissement apparaît dans l'icône de notification du Gestionnaire de serveur. Sélectionnez-le et sélectionnez le lien **Configurer les services Active Directory sur l'**option **du serveur de destination** pour lancer le menu de l'assistant **Configuration AD CS**.



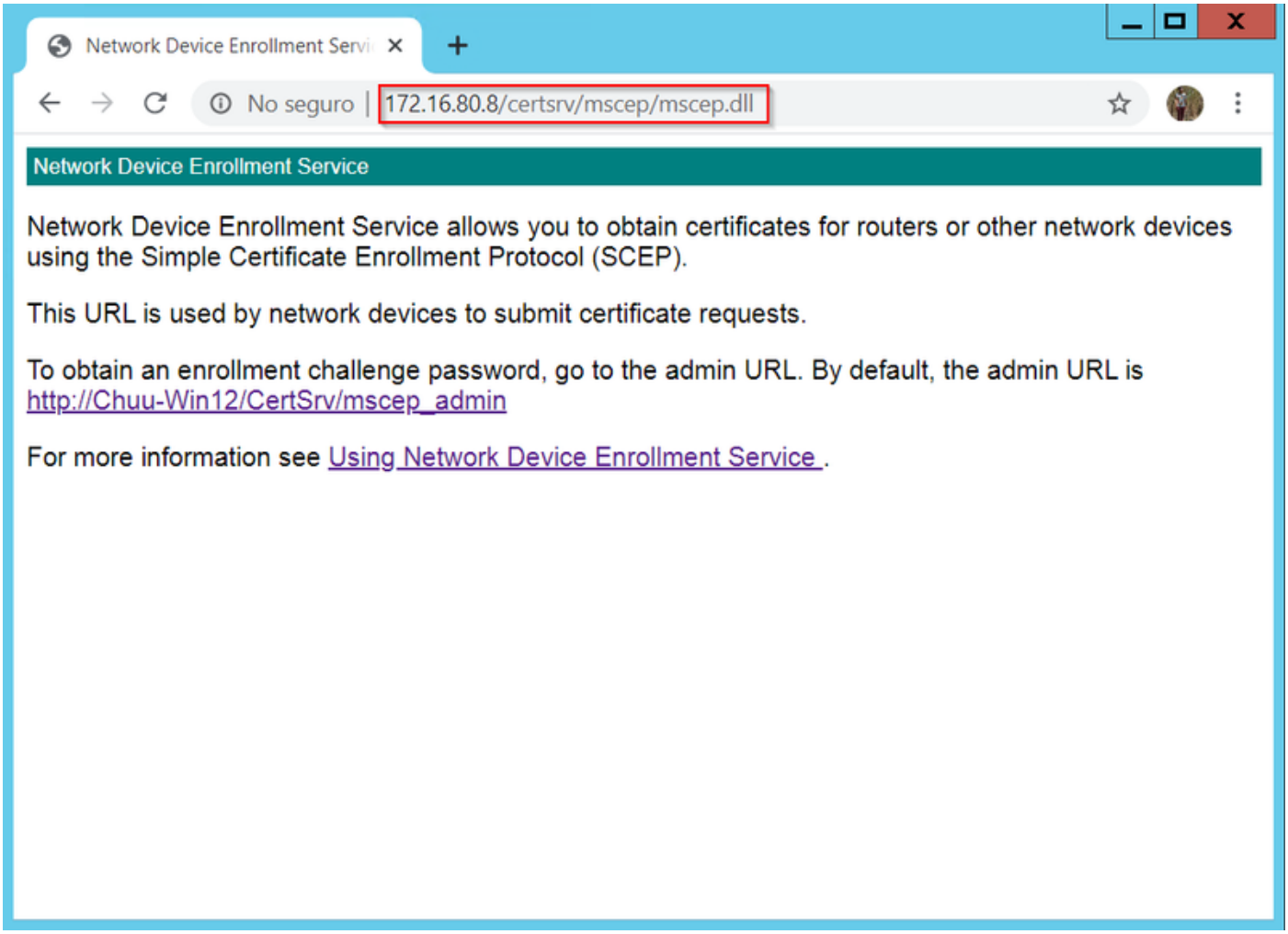
Étape 5. Sélectionnez les services de rôle **Network Device Enrollment Service** et **Online Responder** à configurer dans le menu, puis sélectionnez **Suivant**.

Étape 6. Dans le **compte de service pour NDES** sélectionnez l'une des options entre le pool d'applications intégré ou le compte de service, puis sélectionnez **Suivant**.

Note: Si le compte de service, assurez-vous que le compte fait partie du groupe **IIS_IUSRS**.



Étape 7. Sélectionnez **Suivant** pour les écrans suivants et laissez le processus d'installation terminer. Après l'installation, l'URL SCEP est disponible avec n'importe quel navigateur Web. Accédez à l'URL **http://<server ip>/certsrv/mscep/mscep.dll** pour vérifier que le service est disponible.



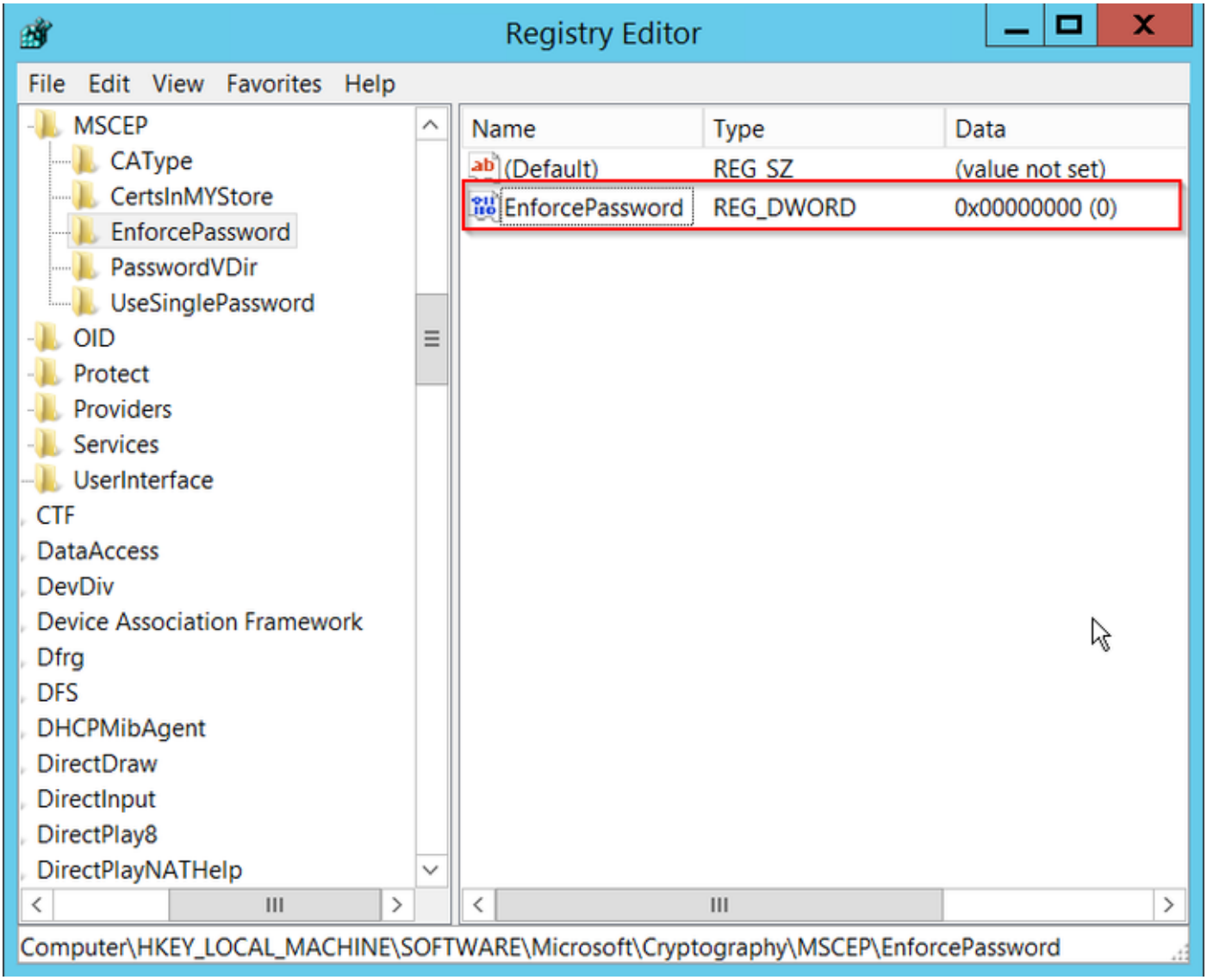
Désactiver la condition de mot de passe du défi d'inscription SCEP

Par défaut, Windows Server a utilisé un mot de passe de confirmation dynamique pour authentifier les demandes client et de point d'extrémité avant l'inscription dans Microsoft SCEP (MSCEP). Cela nécessite un compte d'administrateur pour accéder à l'interface utilisateur graphique Web afin de générer un mot de passe à la demande pour chaque demande (le mot de passe doit être inclus dans la demande).Le contrôleur ne peut pas inclure ce mot de passe dans les demandes qu'il envoie au serveur. Pour supprimer cette fonctionnalité, la clé de Registre sur le serveur NDES doit être modifiée :

Étape 1. Ouvrez l'Éditeur du Registre, recherchez **Regedit** dans le menu **Démarrer**.

Étape 2. Naviguez jusqu'à **Ordinateur > HKEY_LOCAL_MACHINE > LOGICIEL > Microsoft > Cryptographie > MSCEP > EnforcePassword**

Étape 3. Remplacez la valeur **EnforcePassword** par 0. S'il est déjà 0, laissez-le tel quel.



Configurer le modèle de certificat et le Registre

Les certificats et les clés associées peuvent être utilisés dans plusieurs scénarios à des fins différentes définies par les stratégies d'application au sein du serveur AC. La stratégie d'application est stockée dans le champ Utilisation de clé étendue (EKU) du certificat. Ce champ est analysé par l'authentificateur pour vérifier qu'il est utilisé par le client pour l'usage auquel il est destiné. Pour vous assurer que la stratégie d'application appropriée est intégrée aux certificats WLC et AP, créez le modèle de certificat approprié et mappez-le au Registre NDES :

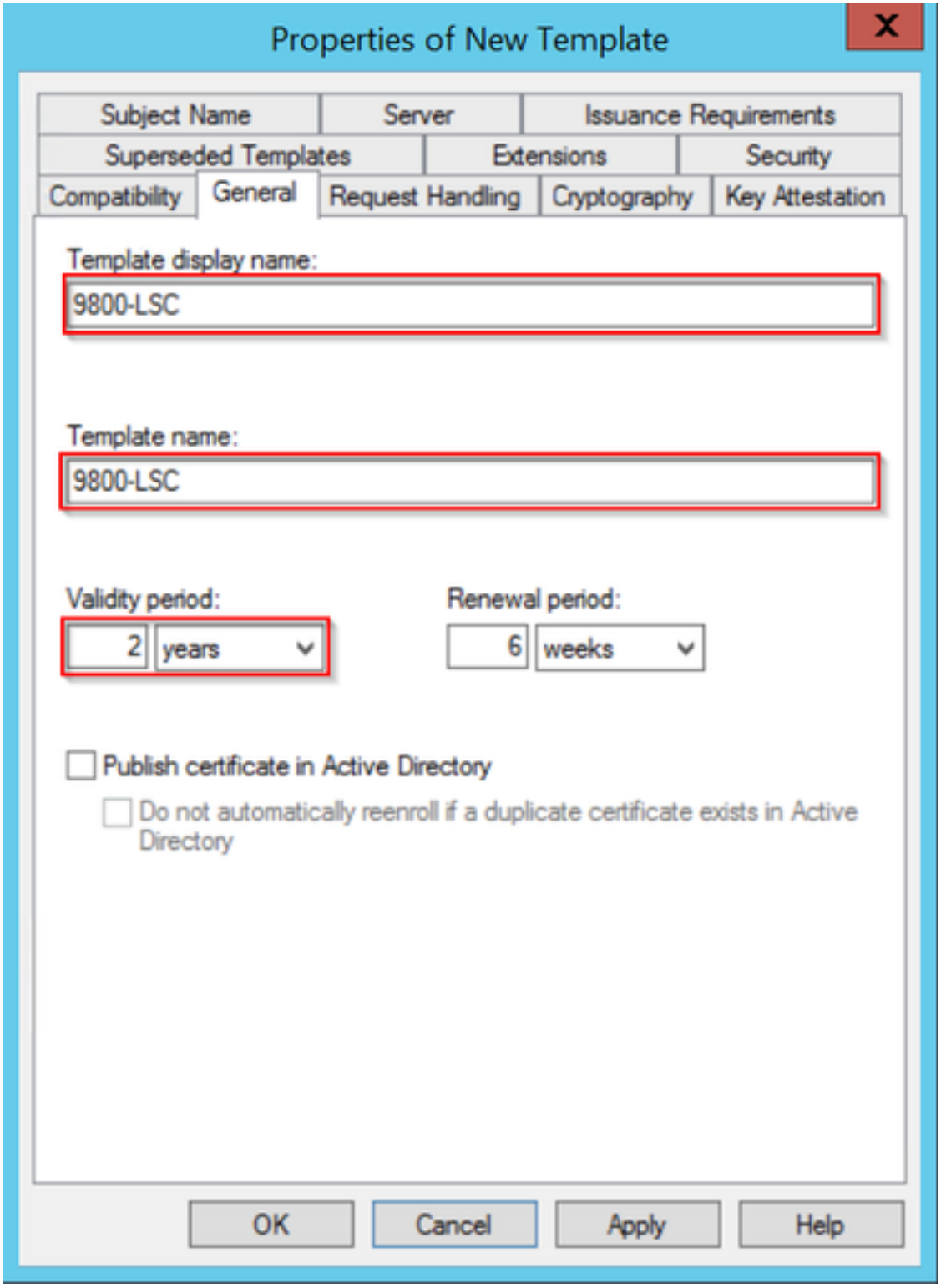
Étape 1. Accédez à **Démarrer > Outils d'administration > Autorité de certification**.

Étape 2. Développez l'arborescence des dossiers du serveur AC, cliquez avec le bouton droit sur les dossiers **Modèles de certificats** et sélectionnez **Gérer**.

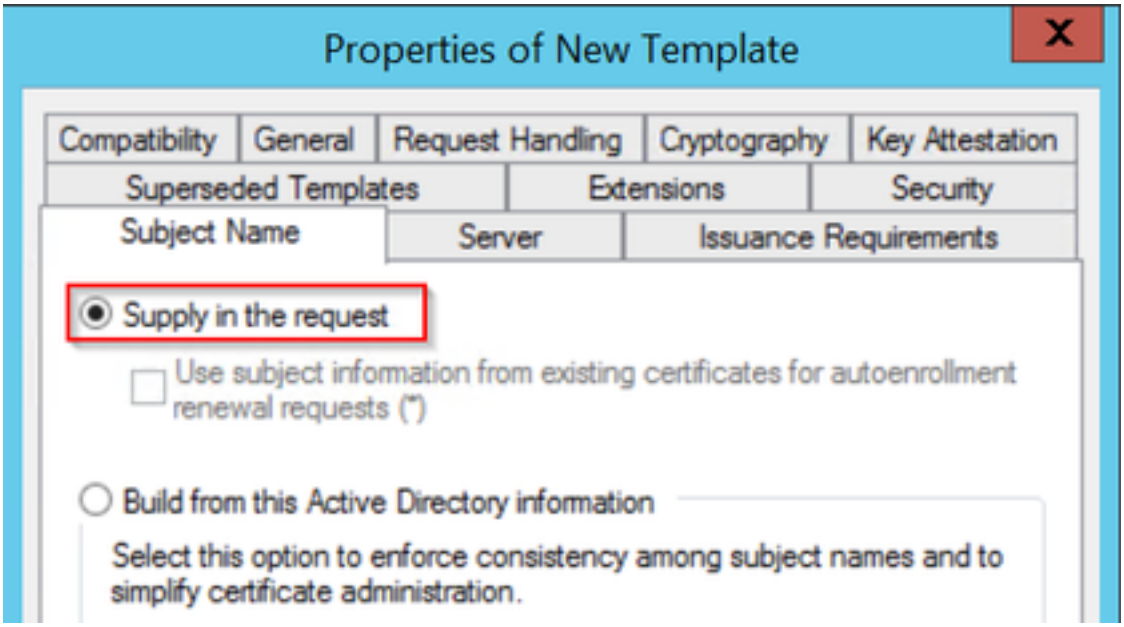
Étape 3. Cliquez avec le bouton droit sur le modèle de certificat **Utilisateurs**, puis sélectionnez **Modèle dupliqué** dans le menu contextuel.

Étape 4. Accédez à l'onglet **Général**, modifiez le nom du modèle et la période de validité selon vos besoins, et ne cochez pas toutes les autres options.

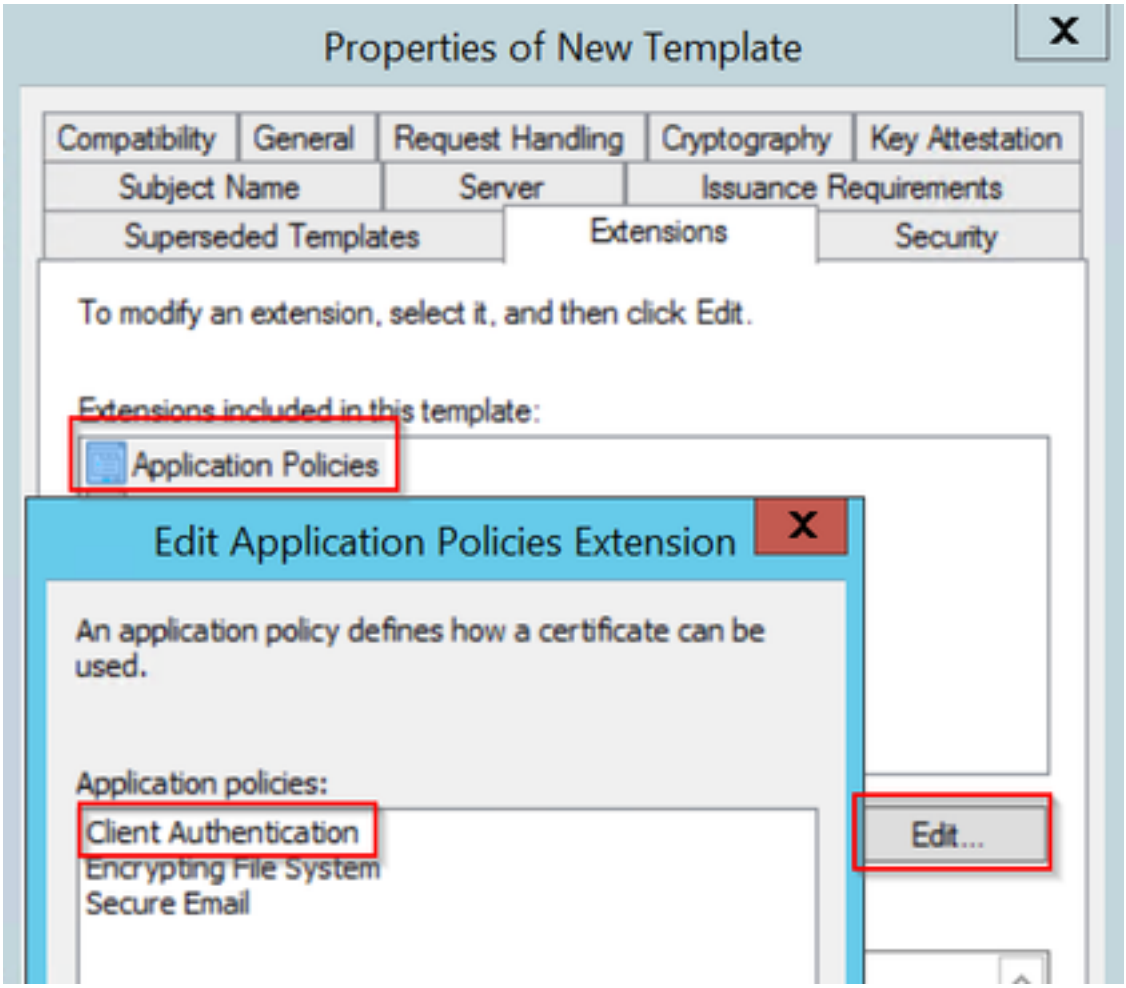
> **Attention** : Lorsque la période de validité est modifiée, assurez-vous qu'elle n'est pas supérieure à la validité du certificat racine de l'autorité de certification.



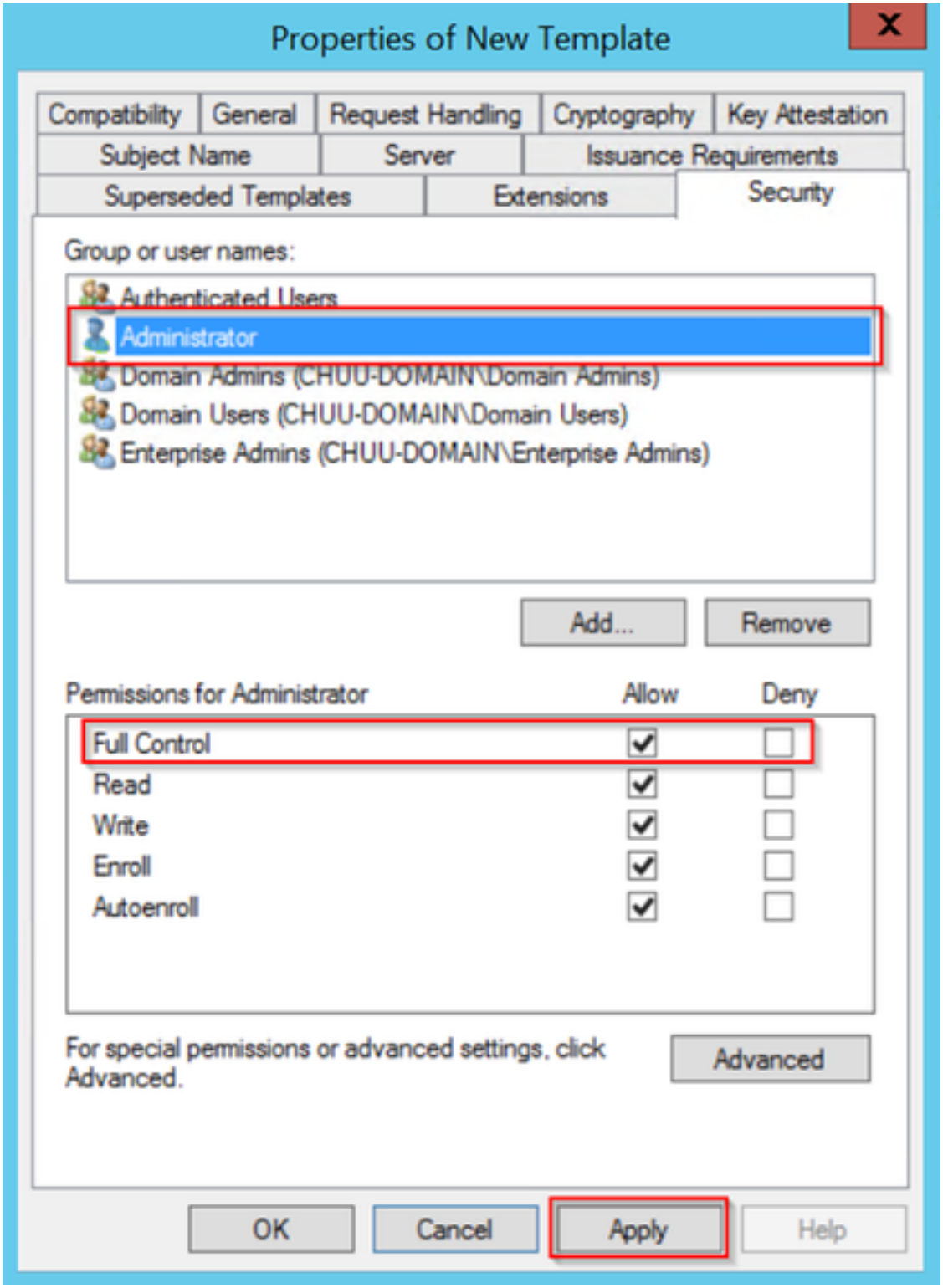
Étape 5. Accédez à l'onglet **Nom du sujet**, vérifiez que **Approvisionnement dans la demande** est sélectionné. Une fenêtre contextuelle apparaît pour indiquer que les utilisateurs n'ont pas besoin de l'approbation de l'administrateur pour obtenir la signature de leur certificat, sélectionnez **OK**.



Étape 6. Accédez à l'onglet **Extensions**, puis sélectionnez l'option **Stratégies d'application** et sélectionnez **Modifier...** bouton. Assurez-vous que **l'authentification du client** se trouve dans la fenêtre **Stratégies d'application** ; sinon, sélectionnez **Ajouter** et ajoutez-le.



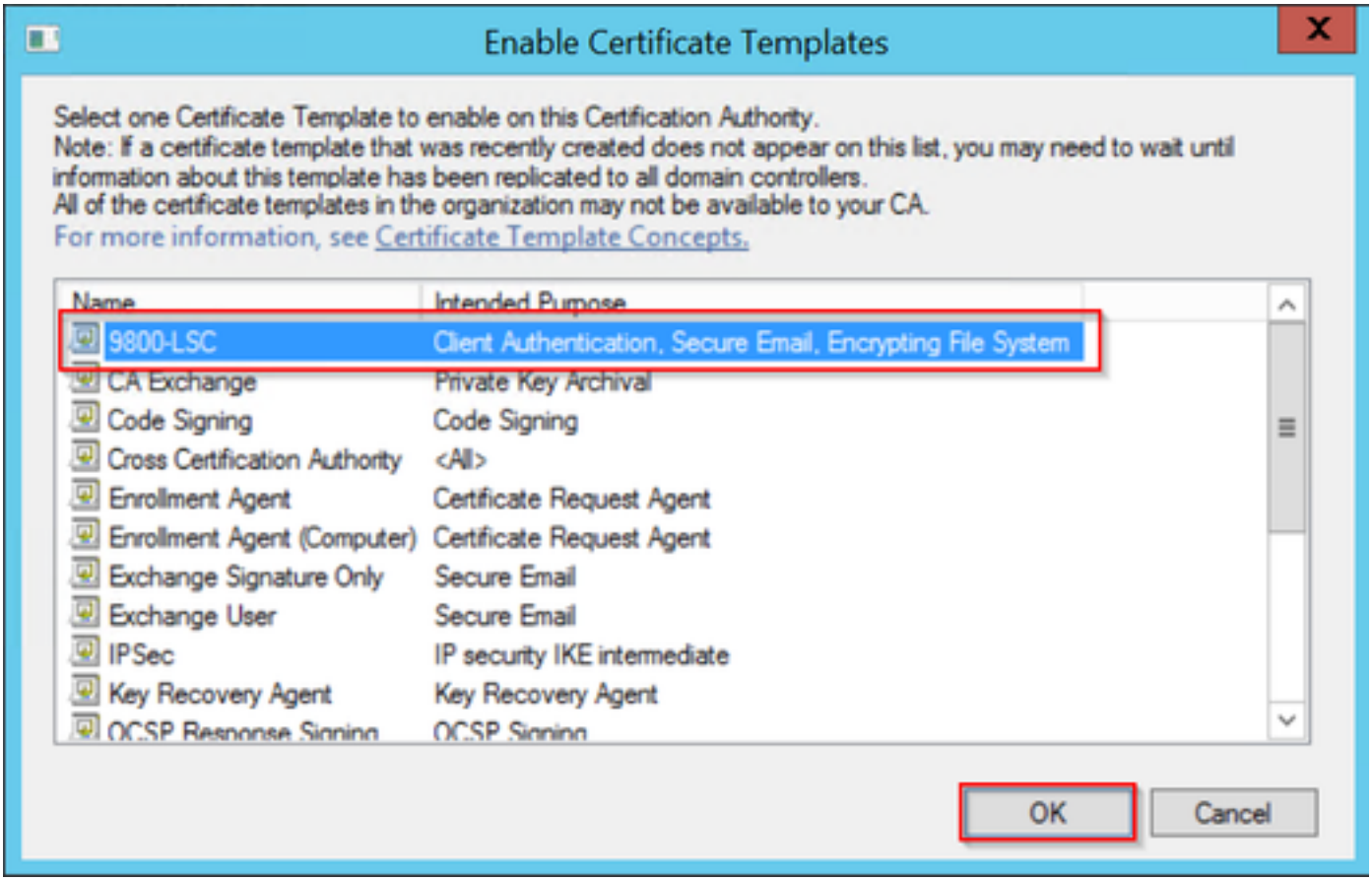
Étape 7. Accédez à l'onglet Sécurité, vérifiez que le compte de service défini à l'étape 6 de l'option Activer les services SCEP dans Windows **Server** dispose des autorisations **Contrôle total** du modèle, puis sélectionnez **Appliquer** et **OK**.



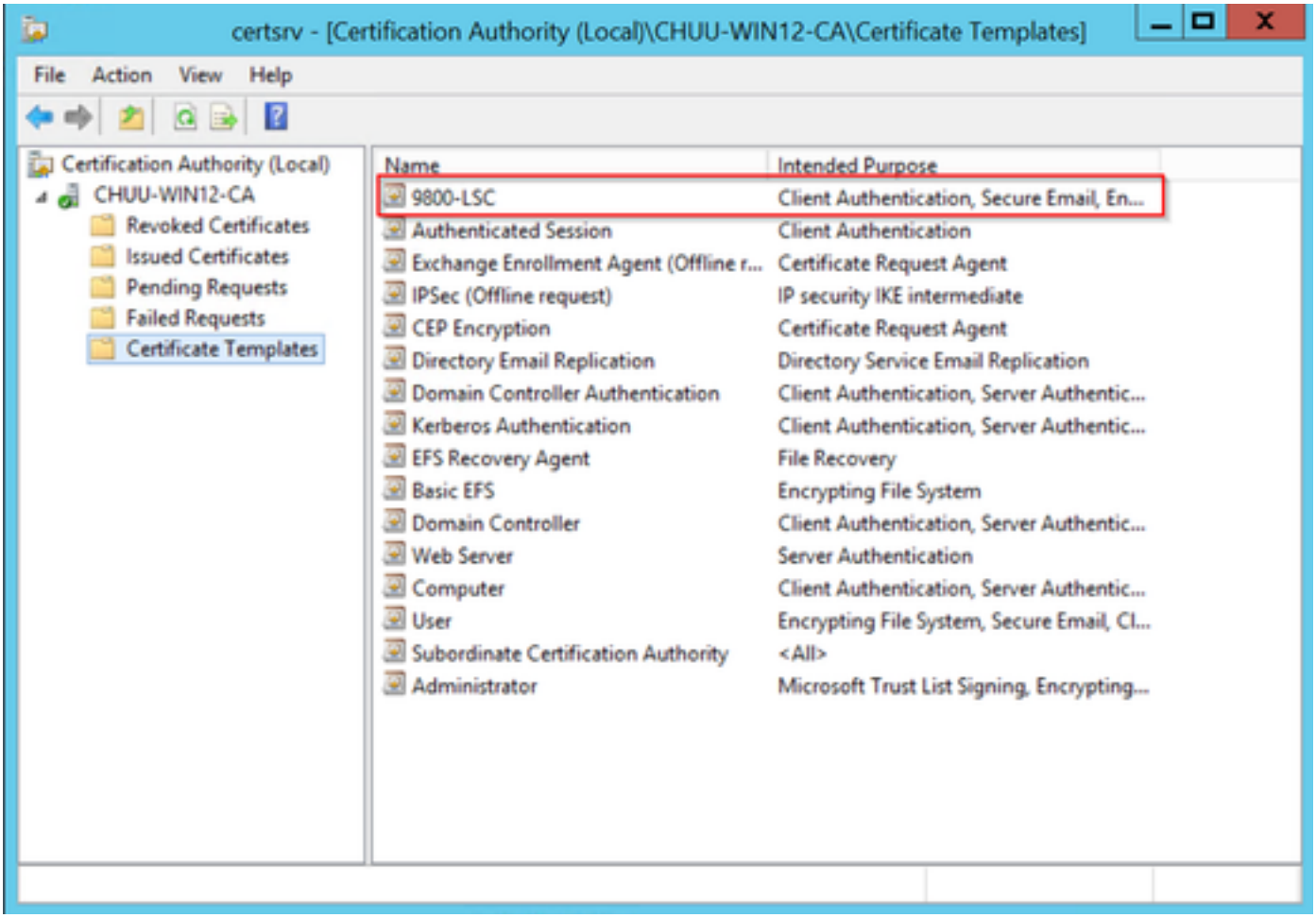
Étape 8. Revenez à la fenêtre **Autorité de certification**, cliquez avec le bouton droit dans le dossier **Modèles de certificat** et sélectionnez **Nouveau > Modèle de certificat à émettre**.

Étape 9. Sélectionnez le modèle de certificat précédemment créé, dans cet exemple, 9800-LSC, puis sélectionnez **OK**.

> **Note**: Le modèle de certificat nouvellement créé peut prendre plus de temps pour être répertorié dans plusieurs déploiements de serveurs car il doit être répliqué sur tous les serveurs.

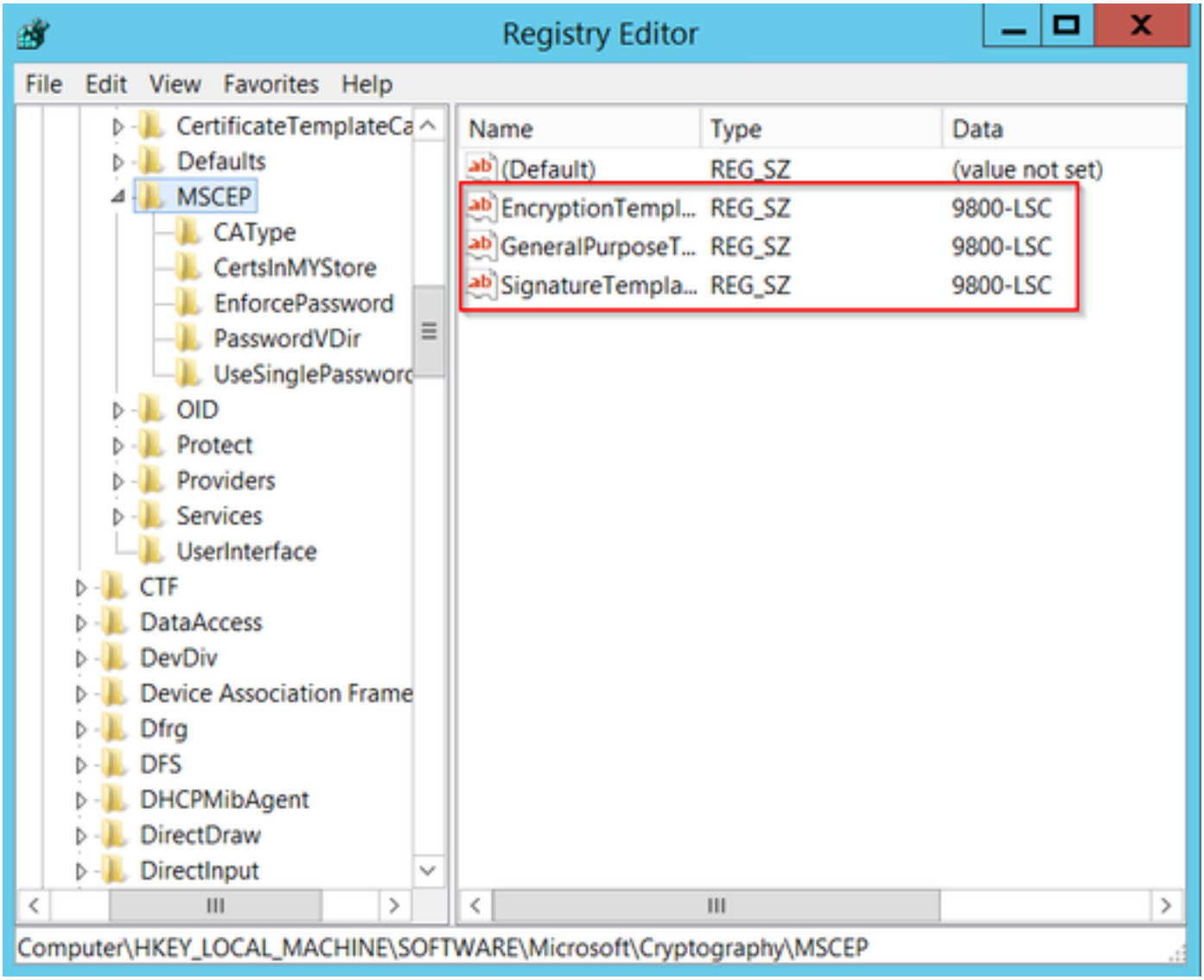


Le nouveau modèle de certificat figure maintenant dans le contenu du dossier **Modèles de certificat**.

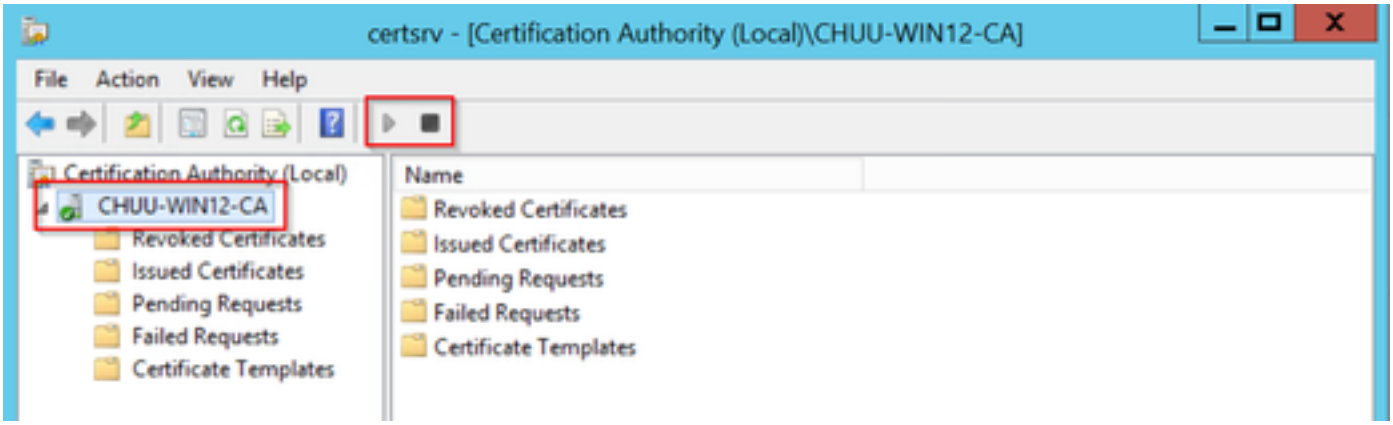


Étape 10. Revenez à la fenêtre **Éditeur du Registre** et accédez à **Ordinateur > HKEY_LOCAL_MACHINE > LOGICIEL > Microsoft > Cryptographie > MSCEP**.

Étape 11. Modifiez les registres **EncryptionTemplate**, **GeneralPurposeTemplate** et **SignatureTemplate** afin qu'ils pointent vers le nouveau modèle de certificat créé.



Étape 12. Redémarrez le serveur NDES. Revenez donc à la fenêtre **Certification Authority**, sélectionnez le nom du serveur et sélectionnez le bouton **Stop** and **Play**.

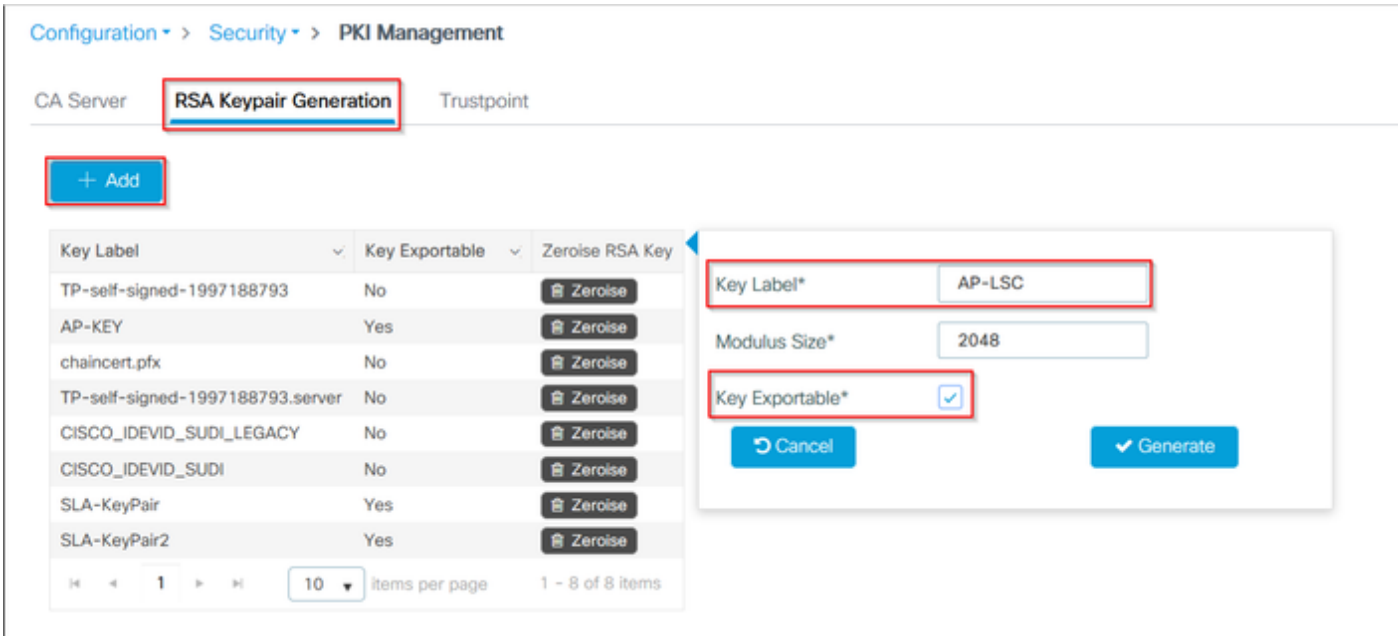


Configurer le point de confiance du périphérique 9800

Le contrôleur doit avoir un point de confiance défini pour authentifier les AP une fois qu'ils ont été provisionnés. Le point de confiance inclut le certificat de périphérique 9800, ainsi que le certificat racine de l'autorité de certification obtenu tous deux à partir du même serveur d'autorité de certification (Microsoft CA dans cet exemple). Pour qu'un certificat soit installé dans le point de confiance, il doit contenir les attributs d'objet ainsi qu'une paire de clés RSA qui lui sont associées. La configuration est effectuée via l'interface Web ou la ligne de commande.

Étape 1. Accédez à **Configuration > Security > PKI Management** et sélectionnez l'onglet **RSA Keypair Generation**. Sélectionnez le bouton **+ Ajouter**.

Étape 2. Définissez une étiquette associée à la paire de clés et assurez-vous que la case **Exportable** est cochée.



Configuration CLI pour les étapes 1 et 2, dans cet exemple de configuration, la paire de clés est générée avec l'étiquette AP-LSC et la taille de module de 2 048 bits :

```
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)
```

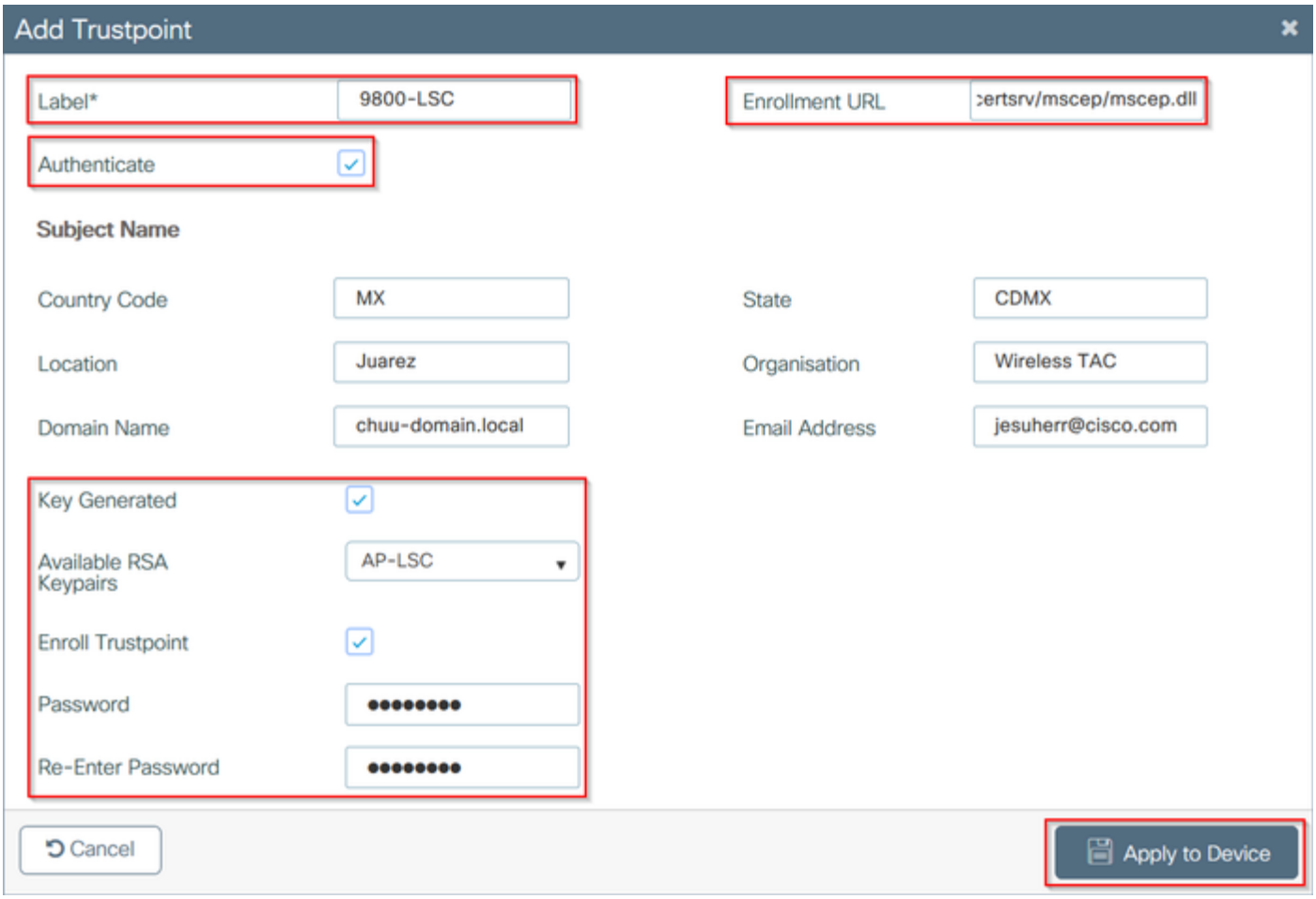
Étape 3. Dans la même section, sélectionnez l'onglet **Trustpoint**, puis cliquez sur le bouton **+ Ajouter**.

Étape 4. Complétez les détails du point de confiance avec les informations du périphérique, puis sélectionnez **Appliquer au périphérique** :

- Le champ **Étiquette** est le nom associé au point de confiance
- Pour **l'URL d'inscription** utilisez celle définie à l'étape 7 de la section **Activer les services SCEP dans Windows Server**

- Cochez la case **Authentifier** pour que le certificat d'Autorité de certification soit téléchargé
- Le champ **Nom de domaine** est placé comme attribut de nom commun de la demande de certificat
- Cochez la case **Clé générée**, un menu déroulant s'affiche, sélectionnez la paire de clés générée à l'étape 2
- Cochez la case **Enroll Trustpoint**, deux champs de mot de passe s'affichent ; saisissez un mot de passe. Ceci est utilisé pour chaîner les clés de certificat avec le certificat de périphérique et le certificat d'autorité de certification

> **Avertissement :** Le contrôleur 9800 ne prend pas en charge les chaînes de serveurs à plusieurs niveaux pour l'installation LSC, de sorte que l'autorité de certification racine doit être celle qui signe les demandes de certificat du contrôleur et des points d'accès.



Configuration CLI pour les étapes 3 et 4 :

> **Attention** : La ligne de configuration du nom de sujet doit être formatée dans la syntaxe LDAP, sinon elle n'est pas acceptée par le contrôleur.

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

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

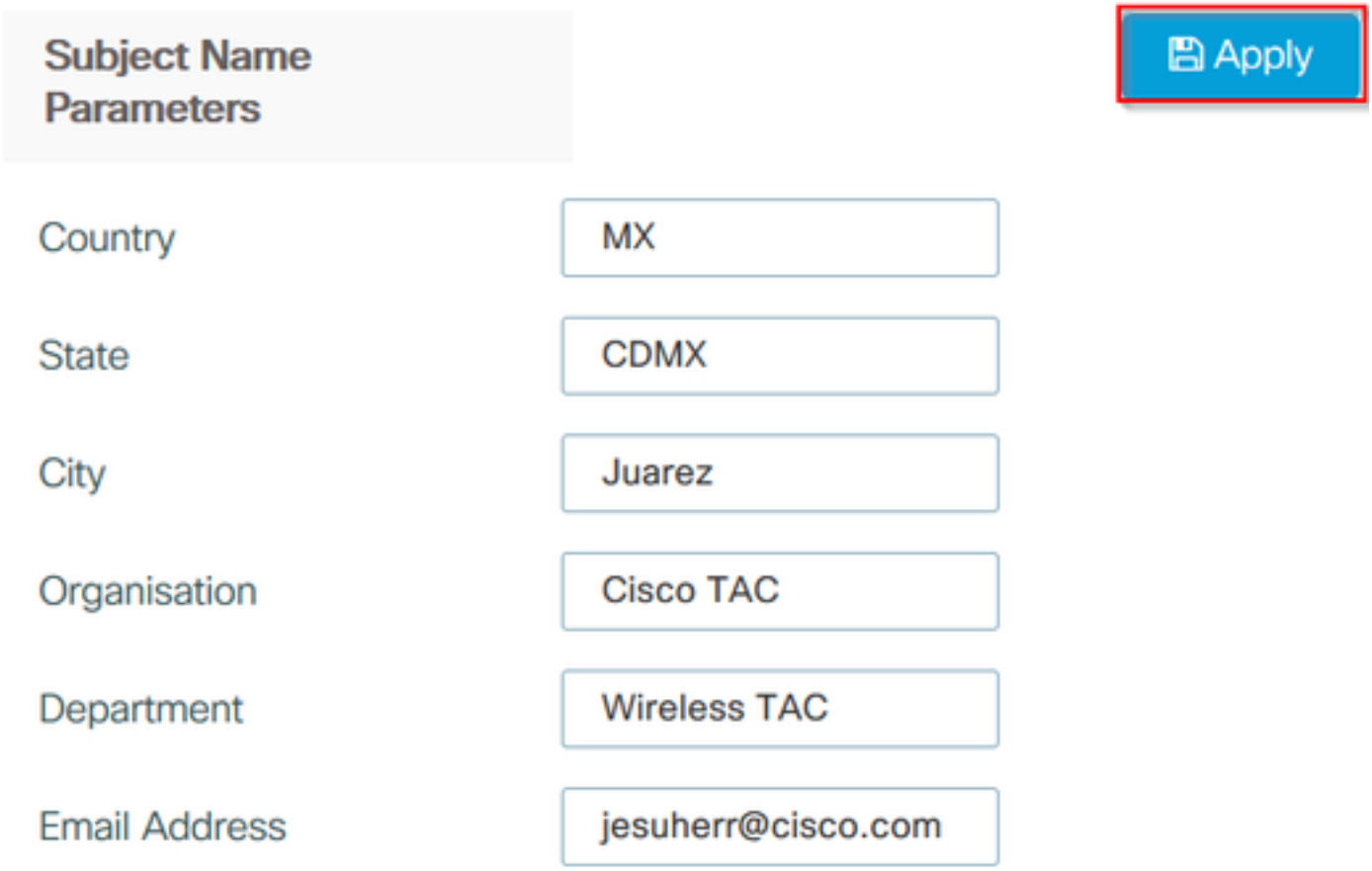
```
9800-L(ca-trustpoint)#subject-name C=



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.
```

Définir les paramètres d'inscription AP et le point de confiance de gestion des mises à jour

L'inscription de point d'accès utilise les détails de point de confiance précédemment définis pour déterminer les détails du serveur auquel le contrôleur transfère la demande de certificat. Puisque le contrôleur est utilisé comme proxy pour l'inscription de certificat, il doit être conscient des paramètres de sujet inclus dans la demande de certificat. La configuration est effectuée via l’interface Web ou la ligne de commande.

Étape 1. Accédez à **Configuration > Wireless > Access Points** et développez le menu **LSC Provisioning**.

Étape 2. Remplissez les **paramètres de nom de sujet** avec les attributs qui sont remplis dans les demandes de certificat AP, puis sélectionnez **Appliquer**.

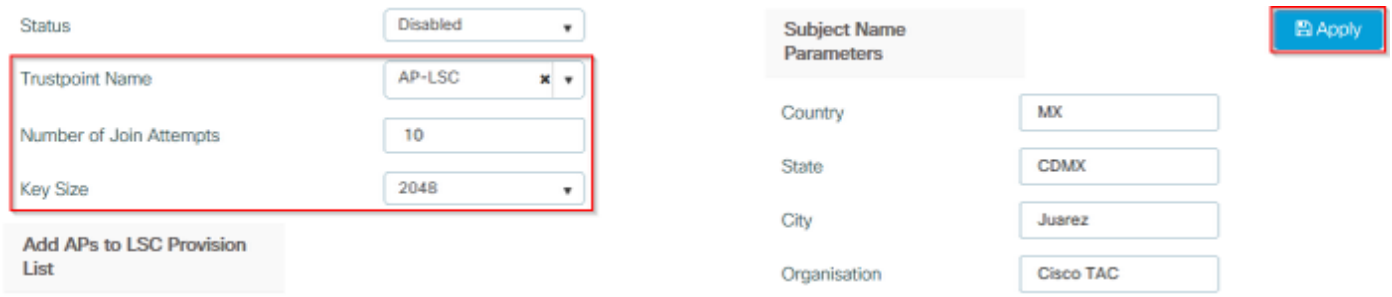


Configuration CLI pour les étapes 1 et 2 :

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

> **Remarque** : les paramètres Subject-name limités à 2 caractères comme le code de pays doivent être strictement respectés, car le WLC 9800 ne valide pas ces attributs.
> Pour plus d'informations consultez le défaut CSCvo72999 comme référence.

Étape 3. Dans le même menu, sélectionnez le point de confiance précédemment défini dans la liste déroulante, spécifiez un certain nombre de tentatives de jointure AP (cela définit le nombre de tentatives de jointure avant qu'il n'utilise à nouveau le MIC), et définissez la taille de la clé de certificat. Cliquez ensuite sur **Apply**.



Configuration CLI pour l'étape 3 :

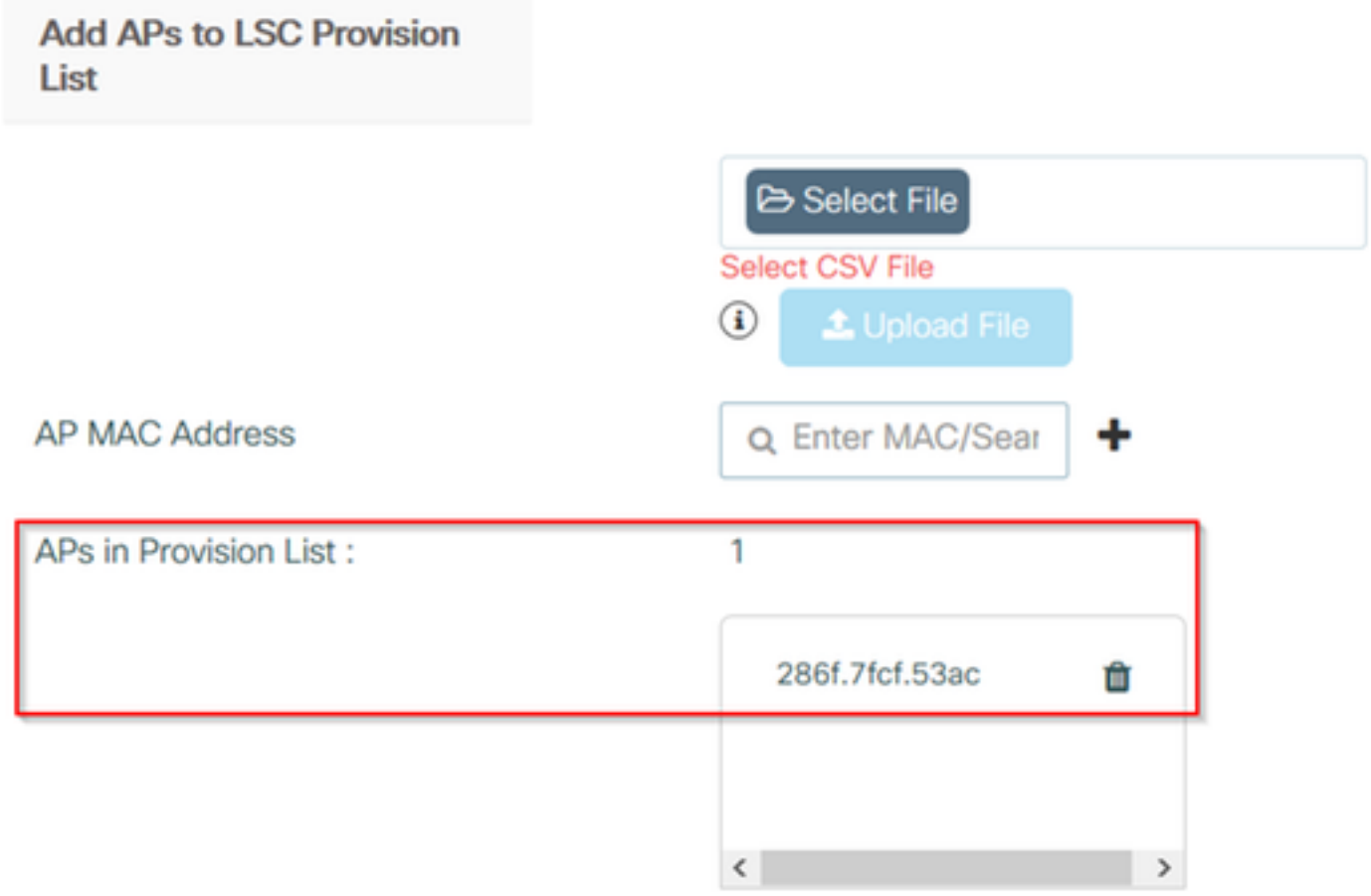
```
9800-L(config)#ap lsc-provision join-attempt
```

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

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

Étape 4. (Facultatif) Le provisionnement LSC des points d'accès peut être déclenché pour tous les points d'accès joints au contrôleur, ou pour des points d'accès spécifiques définis dans une liste d'adresses MAC. Dans le même menu, entrez l'adresse MAC Ethernet AP au format xxxx.xxxx.xxxx dans le champ de texte et cliquez sur le signe **+**. Vous pouvez également télécharger un fichier csv contenant les adresses MAC AP, sélectionner le fichier, puis sélectionner **Télécharger le fichier**.

> **Note**: Le contrôleur ignore toute adresse mac dans le fichier csv qu'il ne reconnaît pas dans sa liste d'AP jointe.



Configuration CLI pour l'étape 4 :

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

Étape 5. Sélectionnez **Enabled** ou **Provisioning List** dans le menu déroulant en regard de l'étiquette **Status**, puis cliquez sur **Apply** to Trigger AP LSC enrollement.

> **Note**: Les points d'accès commencent la demande de certificat, le téléchargement et l'installation. Une fois le certificat entièrement installé, le point d'accès redémarre et lance le processus de jointure avec le nouveau certificat.

> **Astuce** : Si le provisionnement LSC AP est effectué via un contrôleur de pré-production est utilisé avec la liste de provisionnement, ne supprimez pas les entrées AP une fois le certificat provisionné. Si cela est fait, et que les AP reviennent à MIC et rejoignent le même contrôleur de pré-production, leurs certificats LSC sont effacés.

Configuration CLI pour l'étape 5 :

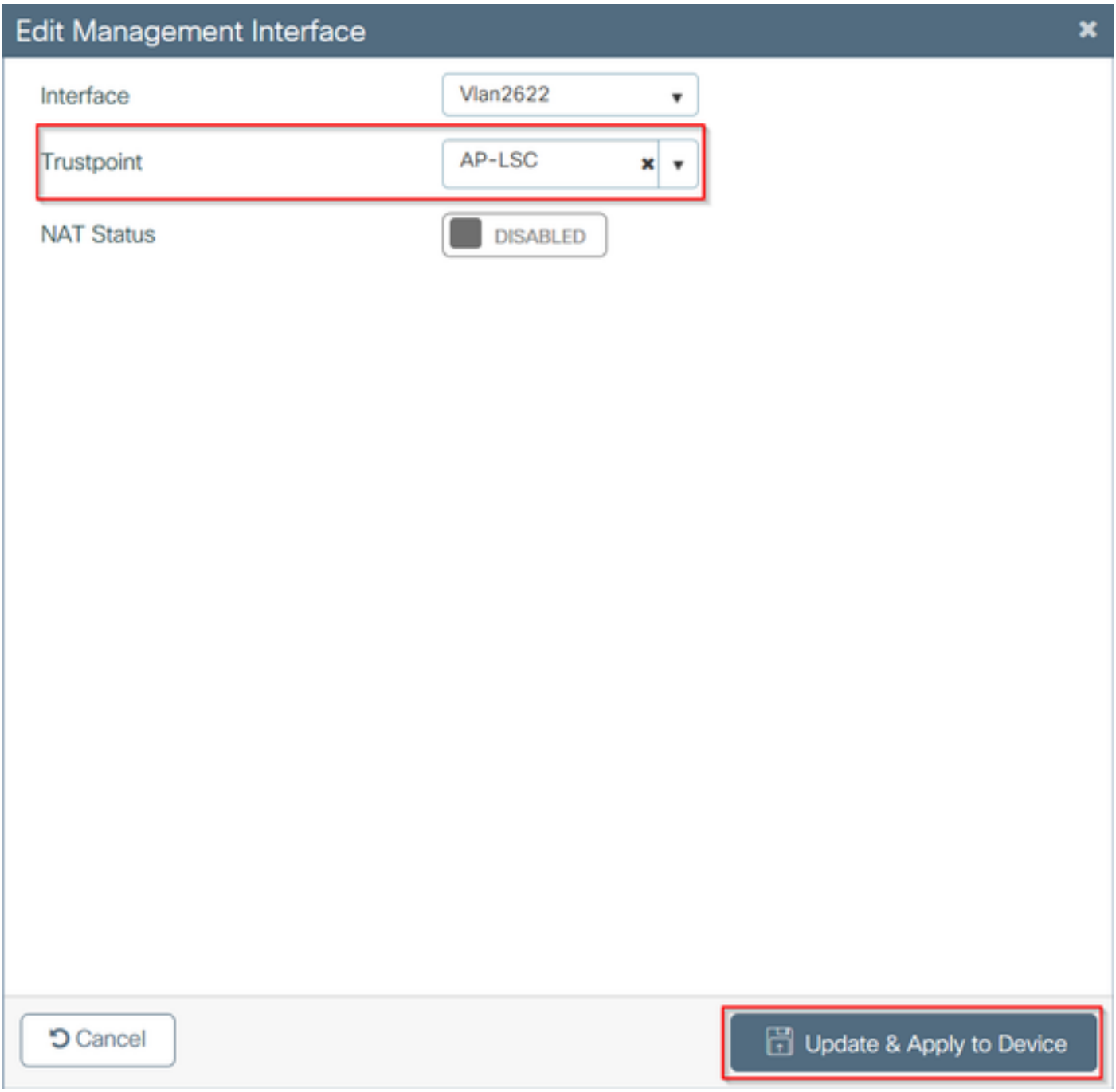
```
9800-L(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size
configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key
by-default or 256 bit key if configured.
Are you sure you want to continue? (y/n):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

Étape 6. Accédez à **Configuration > Interface > Wireless** et sélectionnez l'interface de gestion. Dans le champ **Trustpoint**, sélectionnez le nouveau point de confiance dans le menu déroulant et cliquez sur **Mettre à jour et appliquer au périphérique**.

> **Attention** : Si LSC est activé mais que le point de confiance du WLC 9800 fait référence au MIC ou à un SSC, les AP tentent de se joindre au LSC pour le nombre configuré de tentatives de jointure. Une fois la limite de tentatives maximale atteinte, les points d'accès reviennent à MIC et se joignent à nouveau, mais comme la mise en service LSC est activée, les points d'accès demandent un nouveau LSC. Cela mène à une boucle où le serveur AC signe des certificats en permanence pour les mêmes AP et les AP coincés dans une boucle de demande de jointure-redémarrage.

> **Note**: Une fois que le point de confiance de gestion est mis à jour pour utiliser le certificat LSC, les nouveaux points d'accès ne peuvent pas joindre le contrôleur avec le MIC. Actuellement, il n'y a aucune prise en charge pour ouvrir une fenêtre de provisionnement. Si vous devez installer de nouveaux points d'accès, ils doivent être préalablement provisionnés avec un LSC signé par la même autorité de certification que celle du point de confiance de

gestion.



Configuration CLI pour l'étape 6 :

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

Vérification

Vérifier l'installation du certificat du contrôleur

Pour vérifier que les informations LSC sont présentes dans le point de confiance du WLC 9800,

exécutez la commande **show crypto pki certificate verbose <trustpoint name>**, deux certificats sont associés au point de confiance créé pour le provisionnement et l'inscription LSC. Dans cet exemple, le nom du point de confiance est « microsoft-ca » (seul le résultat pertinent est affiché) :

```
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
```

Vérifier la configuration LSC du WLC 9800

Afin de vérifier les détails sur le point de confiance de gestion sans fil exécutez la commande **show wireless management trustpoint**, assurez-vous que le point de confiance correct (celui qui contient les détails LSC, AP-LSC dans cet exemple) est en cours d'utilisation et est marqué comme Disponible :

```
9800-L#show wireless management trustpoint

Trustpoint  Name : AP-LSC
Certificate Info : Available
```

```
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
Private key Info : Available
```

Afin de vérifier les détails de la configuration de l'approvisionnement LSC de l'AP, ainsi que la liste des AP ajoutés à la liste de fourniture, exécutez la commande **show ap lsc-provision summary**. Assurez-vous que l'état de disposition correct est affiché :

```
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
```

Vérifier l'installation du certificat de point d'accès

Afin de vérifier les certificats installés dans l'AP exécuter la commande **show crypto** à partir de l'interface de ligne de commande de l'AP, assurez-vous que le certificat racine de l'autorité de certification et le certificat de périphérique sont tous deux présents (le résultat affiche uniquement les données pertinentes) :

```
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)
```

Si LSC pour l'authentification dot1x du port de commutateur est utilisé, à partir du point d'accès, vous pouvez vérifier si l'authentification du port est activée.

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

> **Note**: Pour activer le port dot1x pour les AP, il est nécessaire de définir les informations d'identification dot1x pour les AP dans le profil AP ou la configuration AP elle-même avec des valeurs factices.

Dépannage

Problèmes courants

1. Si les modèles ne sont pas correctement mappés dans le Registre du serveur ou si le serveur nécessite une vérification par mot de passe, la demande de certificat pour le WLC 9800 ou les AP est rejetée.
2. Si les sites par défaut IIS sont désactivés, le service SCEP est également désactivé, par conséquent l'URL définie dans le point de confiance n'est pas accessible et le WLC 9800 n'envoie aucune demande de certificat.
3. Si l'heure n'est pas synchronisée entre le serveur et le WLC 9800, les certificats ne sont pas installés car la vérification de validité de l'heure échoue.

Commandes Debug et Log

Utilisez ces commandes pour dépanner l'inscription de certificat de contrôleur 9800 :

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

Afin de dépanner et de surveiller l'inscription des points d'accès, utilisez ces commandes :

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

Àpartir de la ligne de commande AP, **show logging** indique si le point d'accès a rencontré des

problèmes avec l'installation du certificat, et fournit des détails sur la raison pour laquelle le certificat n'a pas été installé :

```
[...]
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]
```

Exemple de tentative d'inscription réussie

Il s'agit de la sortie des débogages précédemment mentionnés pour une inscription réussie à la fois pour le contrôleur et ses AP associés.

Importation de certificat racine CA vers le WLC 9800 :

```
[...]
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.
```

Inscription des périphériques WLC 9800 :

```
[...]
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
```

Sortie de débogage d'inscription AP côté contrôleur, cette sortie est répétée plusieurs fois pour chaque AP qui est joint au 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

Sortie de débogage d'inscription AP côté 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
```

Ceci conclut l'exemple de configuration pour l'inscription LSC via SCEP.