

# Configurer 802.1X sur les points d'accès pour PEAP ou EAP-TLS avec LSC

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[AC SCEP Windows Server 2016](#)

[Configurer le modèle de certificat et le Registre](#)

[Configuration de LSC sur le 9800](#)

[Étapes de configuration de l'interface graphique LSC AP](#)

[Étapes de configuration LSC CLI AP](#)

[Vérification LSC AP](#)

[Dépannage du provisionnement LSC](#)

[Authentification 802.1X filaire AP utilisant LSC](#)

[Étapes de configuration de l'authentification 802.1x filaire AP](#)

[Configuration de l'interface graphique d'authentification 802.1x filaire AP](#)

[Configuration CLI d'authentification 802.1x filaire AP](#)

[Configuration du commutateur d'authentification 802.1x filaire AP](#)

[Installation du certificat du serveur RADIUS](#)

[Vérification de l'authentification 802.1x filaire AP](#)

[Dépannage de l'authentification 802.1X](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment authentifier les points d'accès Cisco sur leur port de commutation à l'aide des méthodes PEAP ou EAP-TLS 802.1X.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur sans fil

- Point d'accès
- Commutateur
- Serveur ISE
- Autorité de certification.

## Composants utilisés

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

- Contrôleur sans fil : C9800-40-K9 fonctionnant sous 17.09.02
- Point d'accès : C9117AXI-D
- Commutateur : C9200L-24P-4G fonctionnant sous 17.06.04
- Serveur AAA : ISE-VM-K9 exécutant 3.1.0.518
- Autorité de certification : Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Si vous voulez que vos points d'accès (AP) s'authentifient avec leur port de commutation en utilisant 802.1X, ils utilisent par défaut le protocole d'authentification EAP-FAST qui ne nécessite pas de certificats. Si vous voulez que les AP utilisent la méthode PEAP-mschapv2 (qui utilise des informations d'identification du côté AP mais un certificat du côté RADIUS) ou la méthode EAP-TLS (qui utilise des certificats des deux côtés), vous devez d'abord configurer LSC. C'est le seul moyen de provisionner un certificat de confiance/racine sur un point d'accès (et également un certificat de périphérique dans le cas d'EAP-TLS). Il n'est pas possible pour le point d'accès de faire PEAP et d'ignorer la validation côté serveur. Ce document traite d'abord de la configuration de LSC, puis du côté de la configuration 802.1X.

Utilisez un LSC si vous voulez que votre PKI offre une meilleure sécurité, que vous ayez le contrôle de votre autorité de certification (CA) et que vous définissiez des politiques, des restrictions et des utilisations sur les certificats générés.

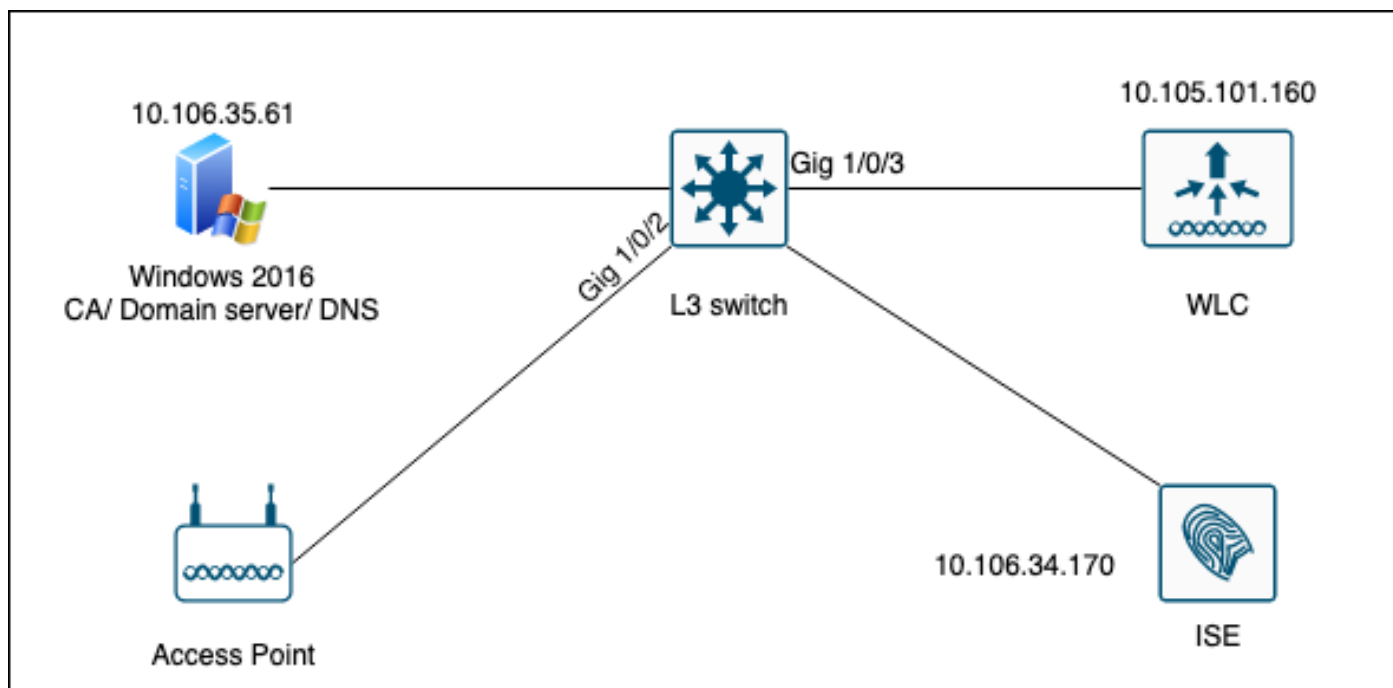
Avec LSC, le contrôleur obtient un certificat émis par l'autorité de certification. Un AP ne communique pas directement avec le serveur AC, mais le WLC demande des certificats au nom des AP qui se joignent. Les détails du serveur AC doivent être configurés sur le contrôleur et doivent être accessibles.

Le contrôleur utilise le protocole SCEP (Simple Certificate Enrollment Protocol) pour transférer les demandes de certificat générées sur les périphériques à l'autorité de certification et utilise à nouveau le protocole SCEP pour obtenir les certificats signés de l'autorité de certification.

Le SCEP est un protocole de gestion de certificats que les clients PKI et les serveurs CA utilisent pour prendre en charge l'inscription et la révocation de certificats. Il est largement utilisé dans

Cisco et pris en charge par de nombreux serveurs CA. Dans le protocole SCEP, HTTP est utilisé comme protocole de transport pour les messages PKI. L'objectif principal de SCEP est la livraison sécurisée des certificats aux périphériques réseau.

## Diagramme du réseau



## Configurer

Il y a deux choses à configurer principalement : la CA SCEP et le WLC 9800.

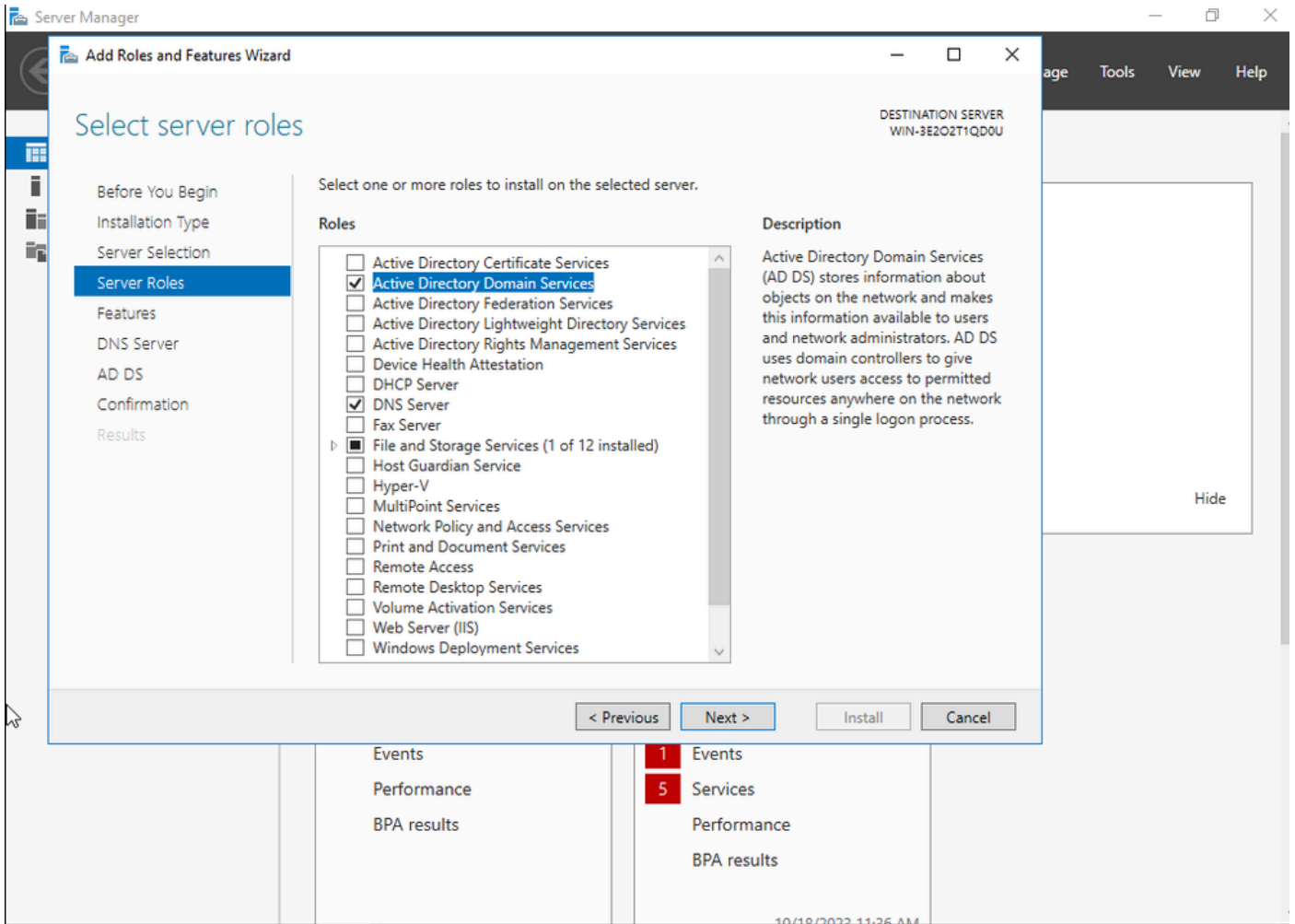
### AC SCEP Windows Server 2016

Ce document couvre une installation de base d'une autorité de certification SCEP Windows Server à des fins de travaux pratiques. Une autorité de certification Windows de production réelle doit être configurée de manière sécurisée et appropriée pour les opérations d'entreprise. Cette section a pour but de vous aider à le tester dans les travaux pratiques et de vous inspirer des paramètres requis pour que cette configuration fonctionne. Voici les étapes à suivre :

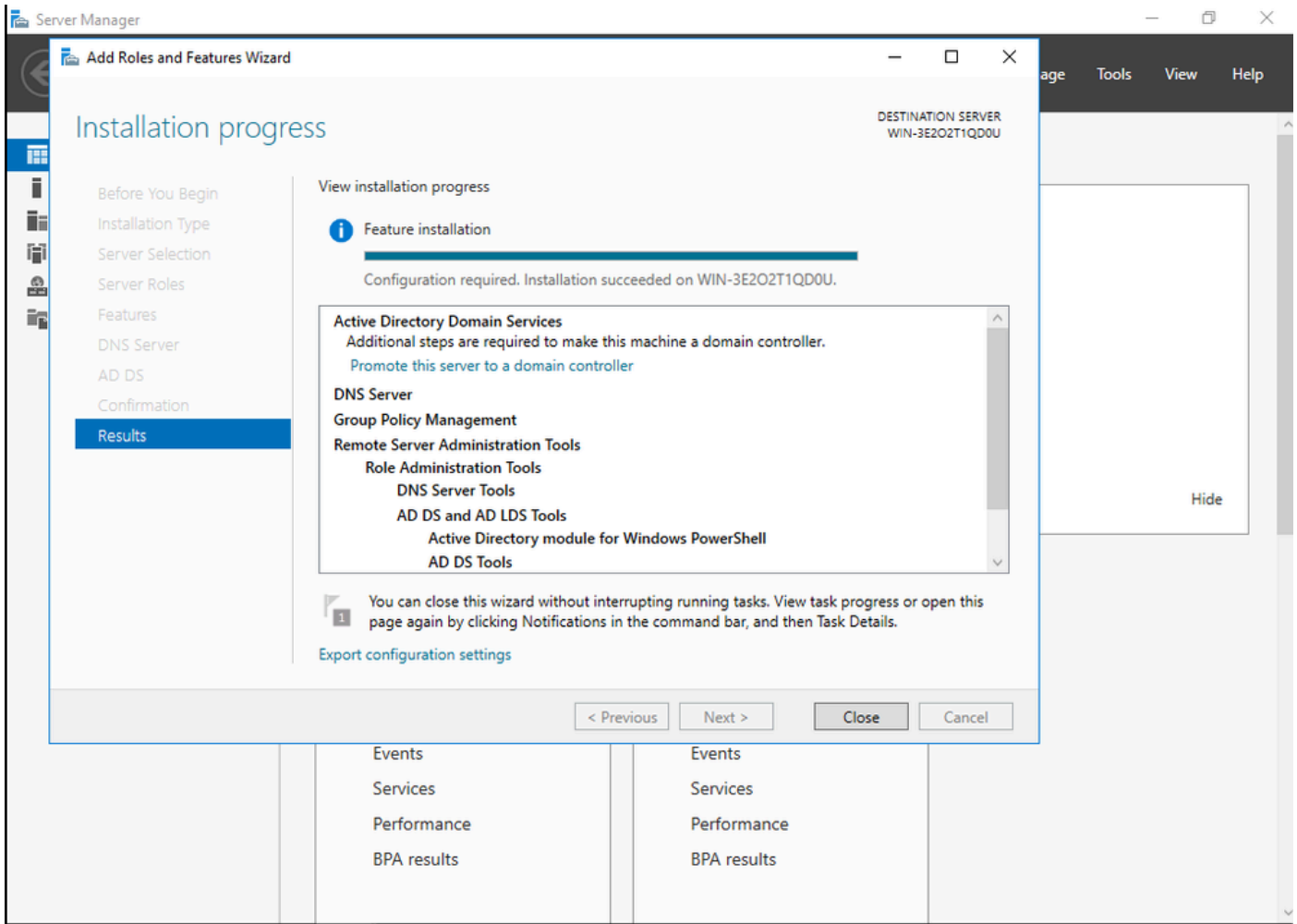
Étape 1. Installer une nouvelle version de Windows Server 2016 Desktop Experience.

Étape 2. Assurez-vous que votre serveur est configuré avec une adresse IP statique.

Étape 3. Installez un nouveau rôle et un nouveau service, en commençant par les services de domaine Active Directory et le serveur DNS.

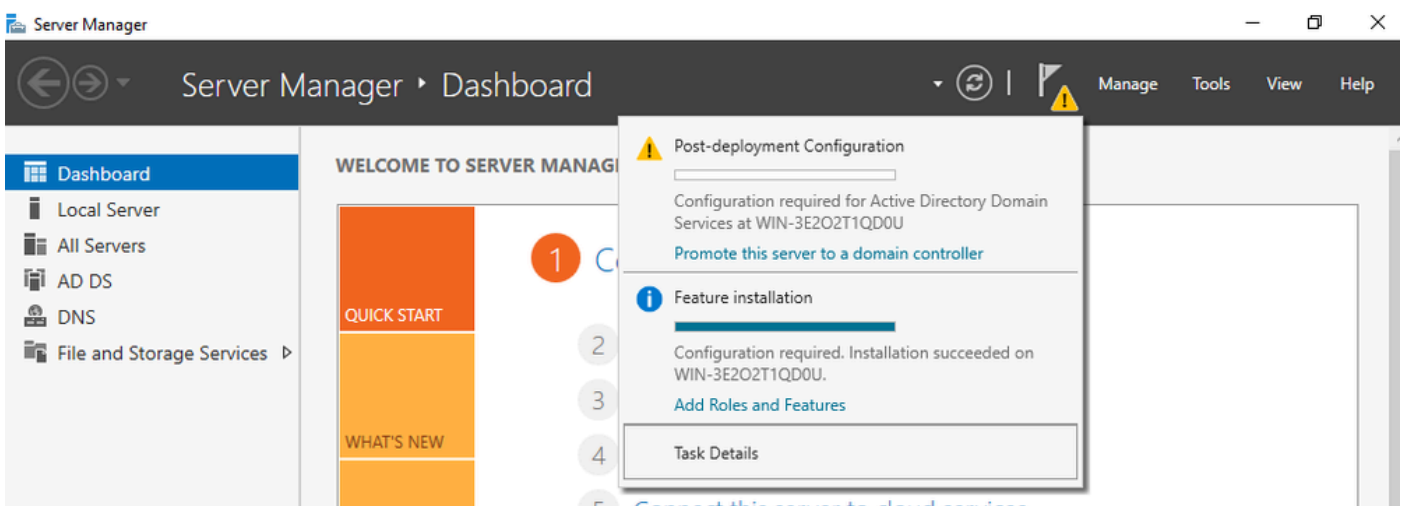


Installation Active Directory



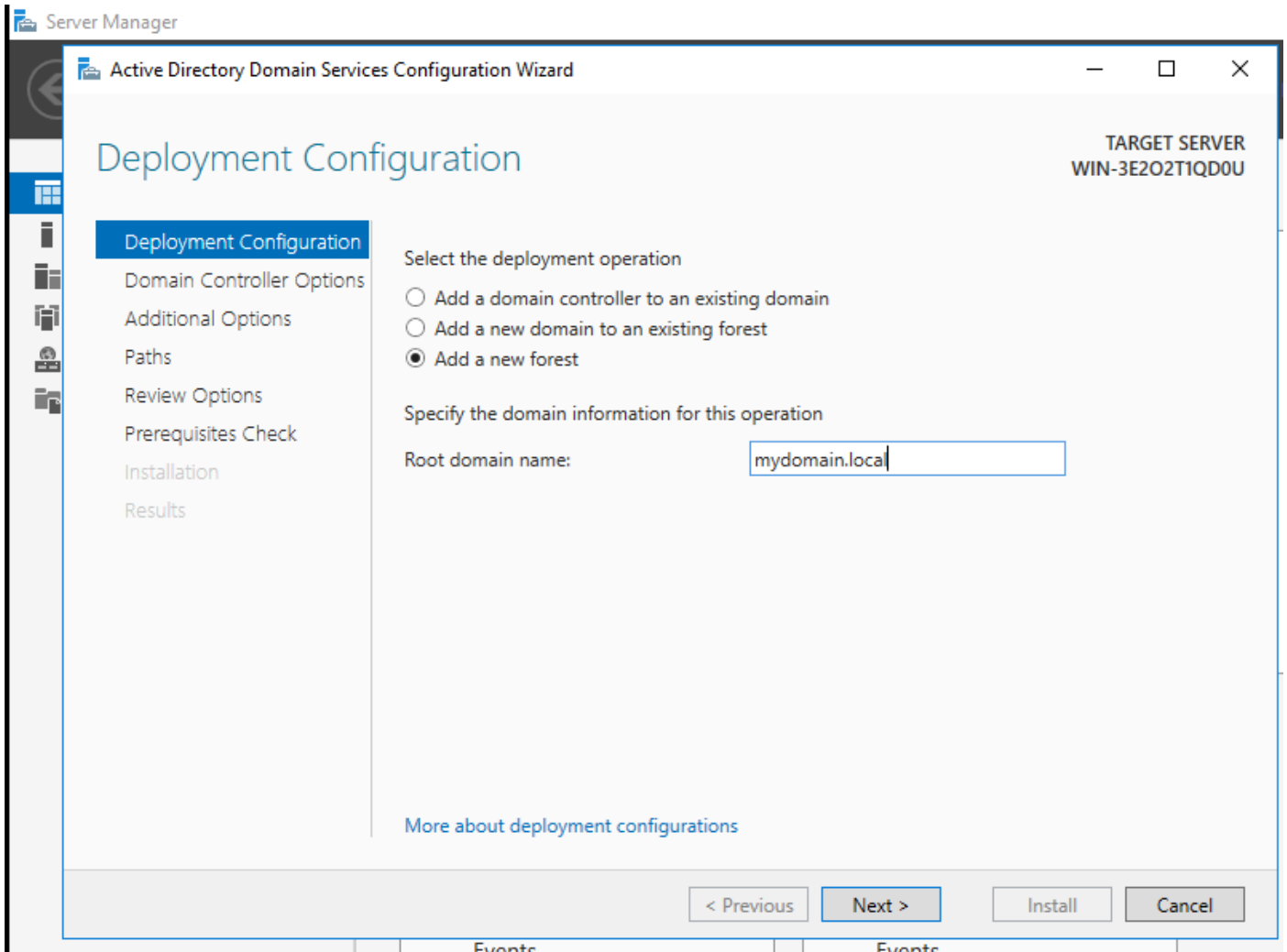
Fin de l'installation AD

Étape 4. Une fois terminé, cliquez sur dans le tableau de bord sur Promouvoir ce serveur en contrôleur de domaine.



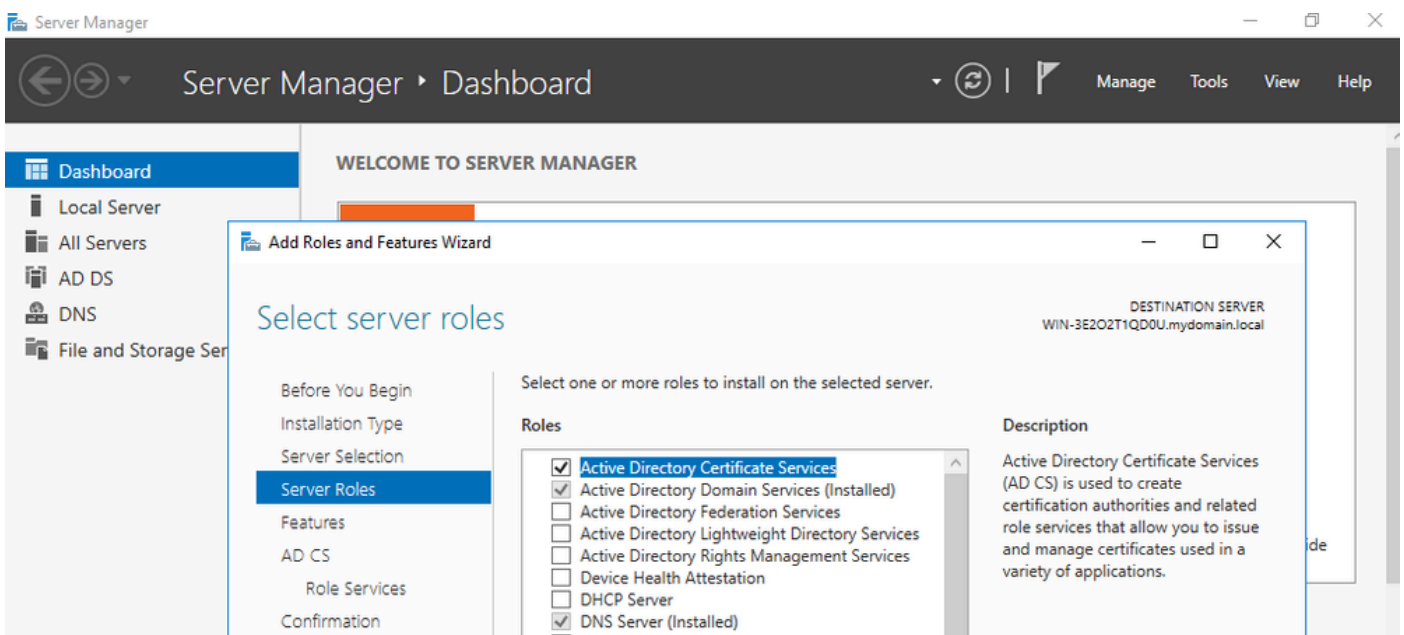
Configurer les services AD

Étape 5. Créez une nouvelle forêt et choisissez un nom de domaine.

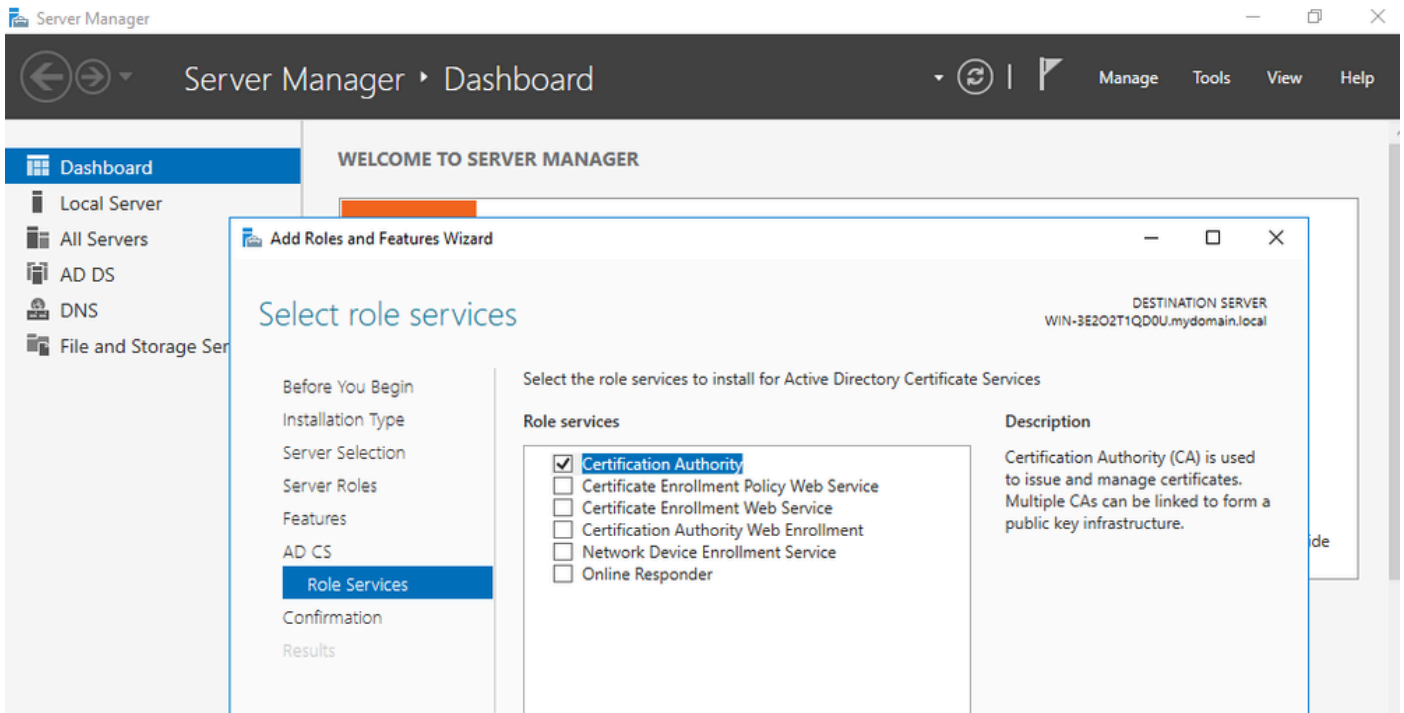


Choisir un nom de forêt

Étape 6. Ajoutez le rôle Services de certificats à votre serveur :

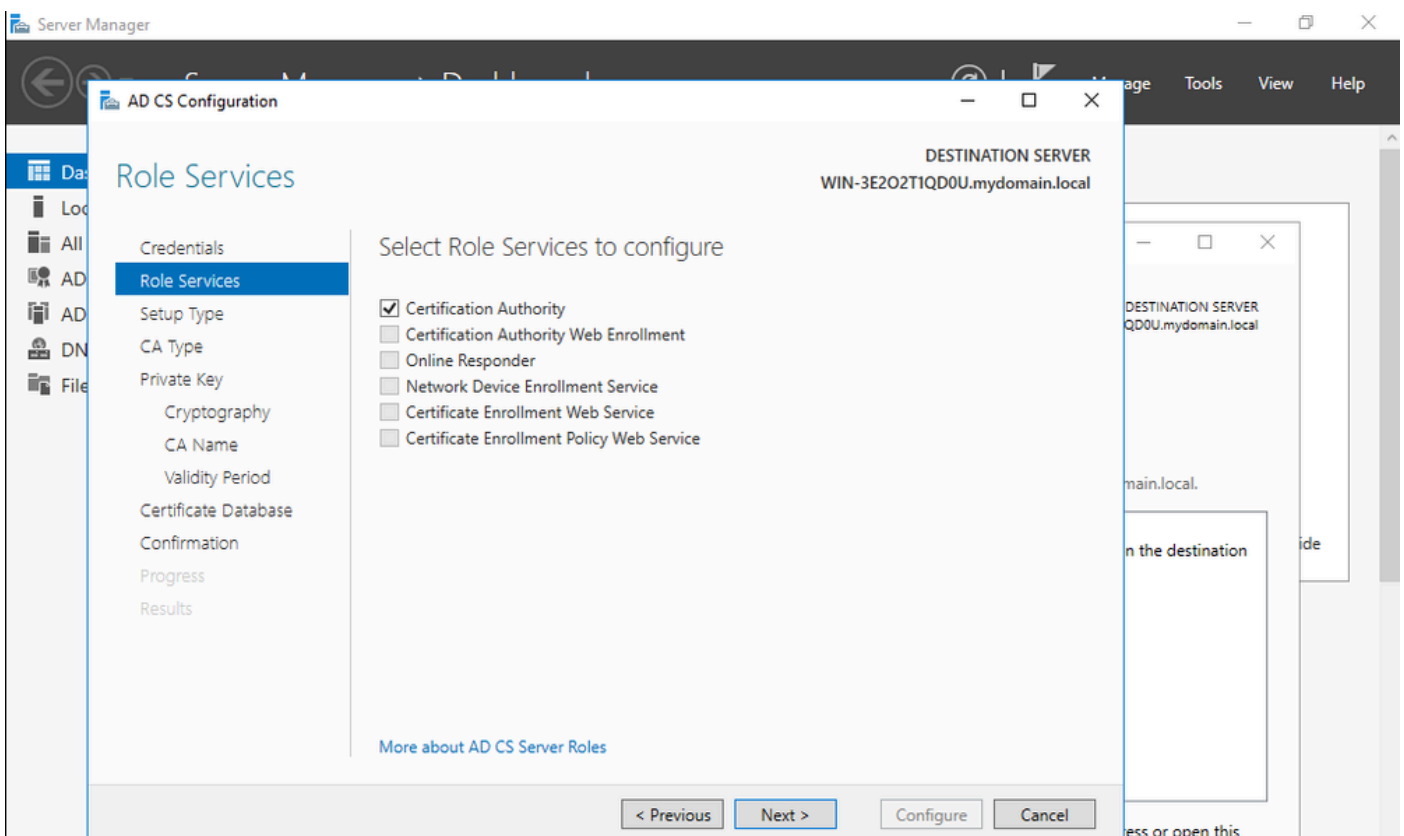


Ajouter des services de certificat

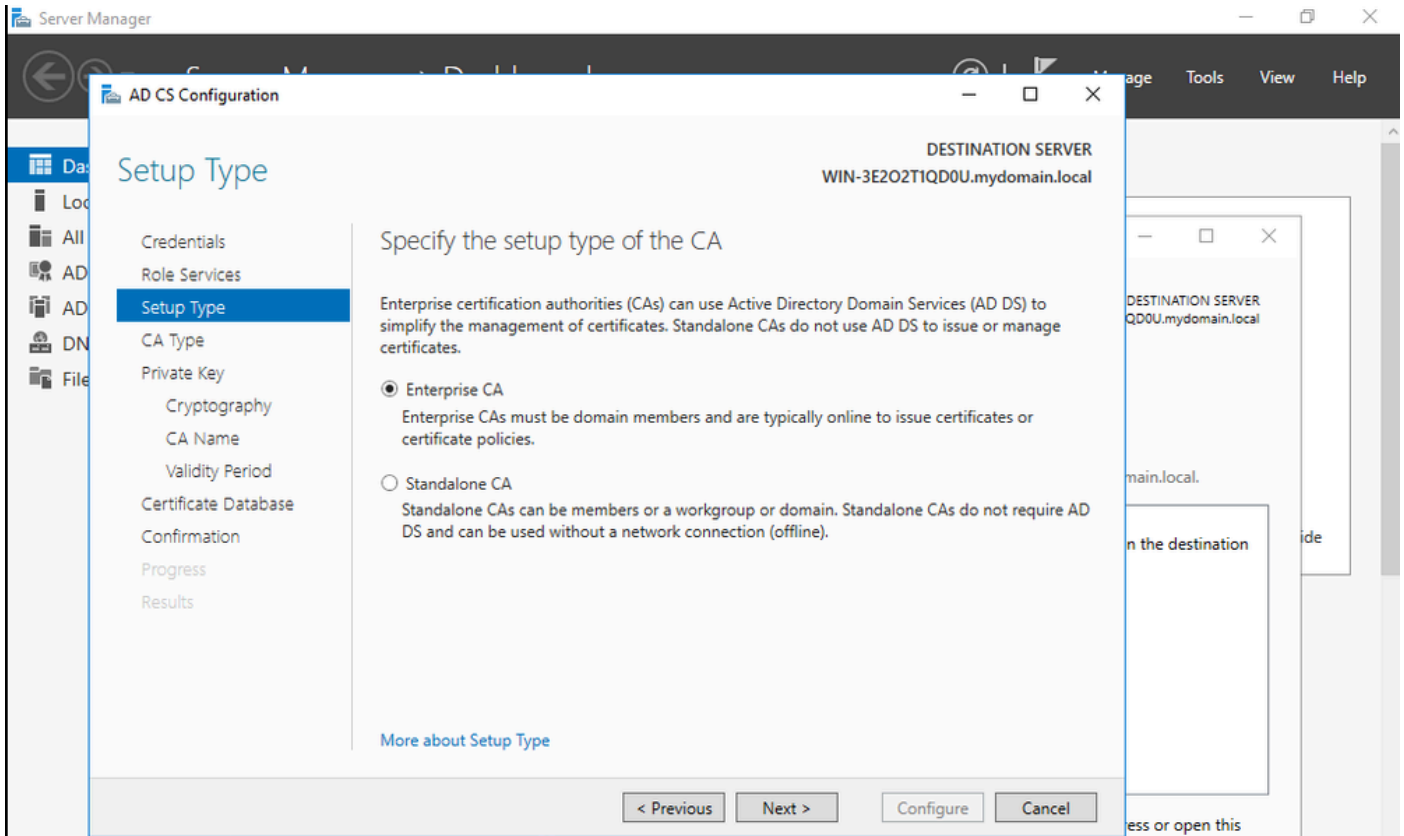


Ajouter uniquement l'autorité de certification

Étape 7. Une fois terminé, configurez votre autorité de certification.



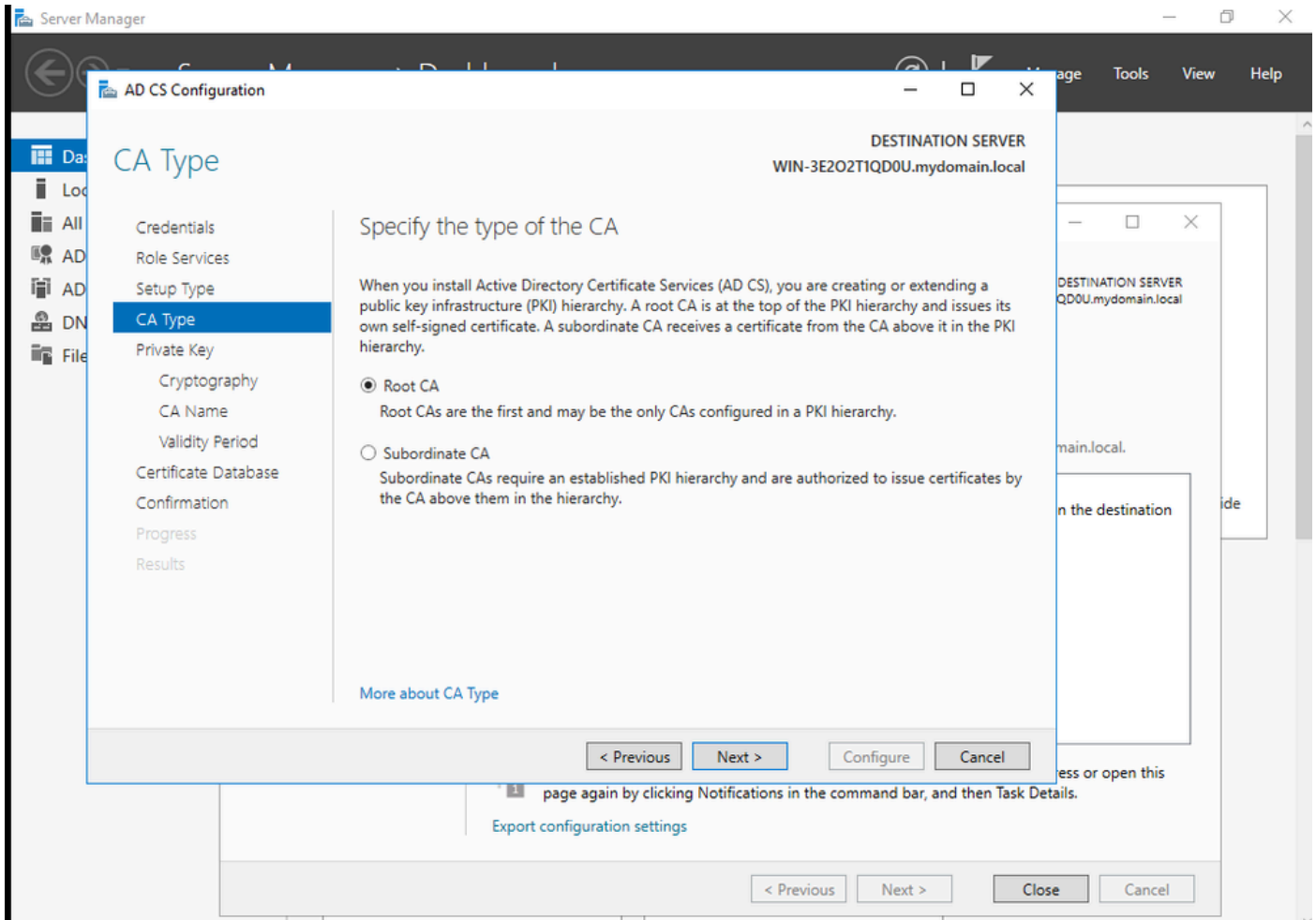
Étape 8. Sélectionnez Enterprise CA.



Autorité de certification Enterprise

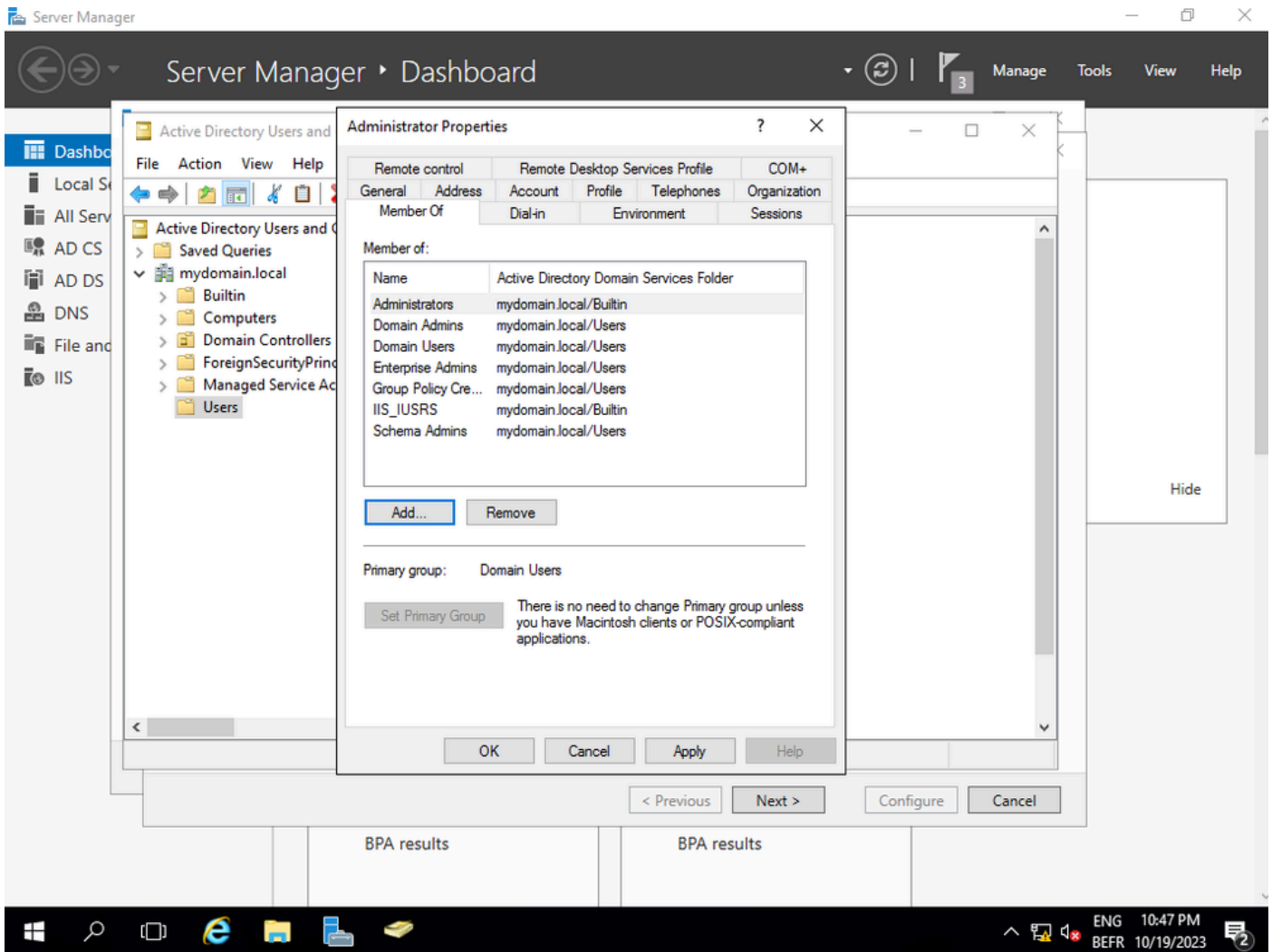
Étape 9. Faites-en une autorité de certification racine. Depuis Cisco IOS XE 17.6, les CA subordonnées sont prises en charge pour LSC.





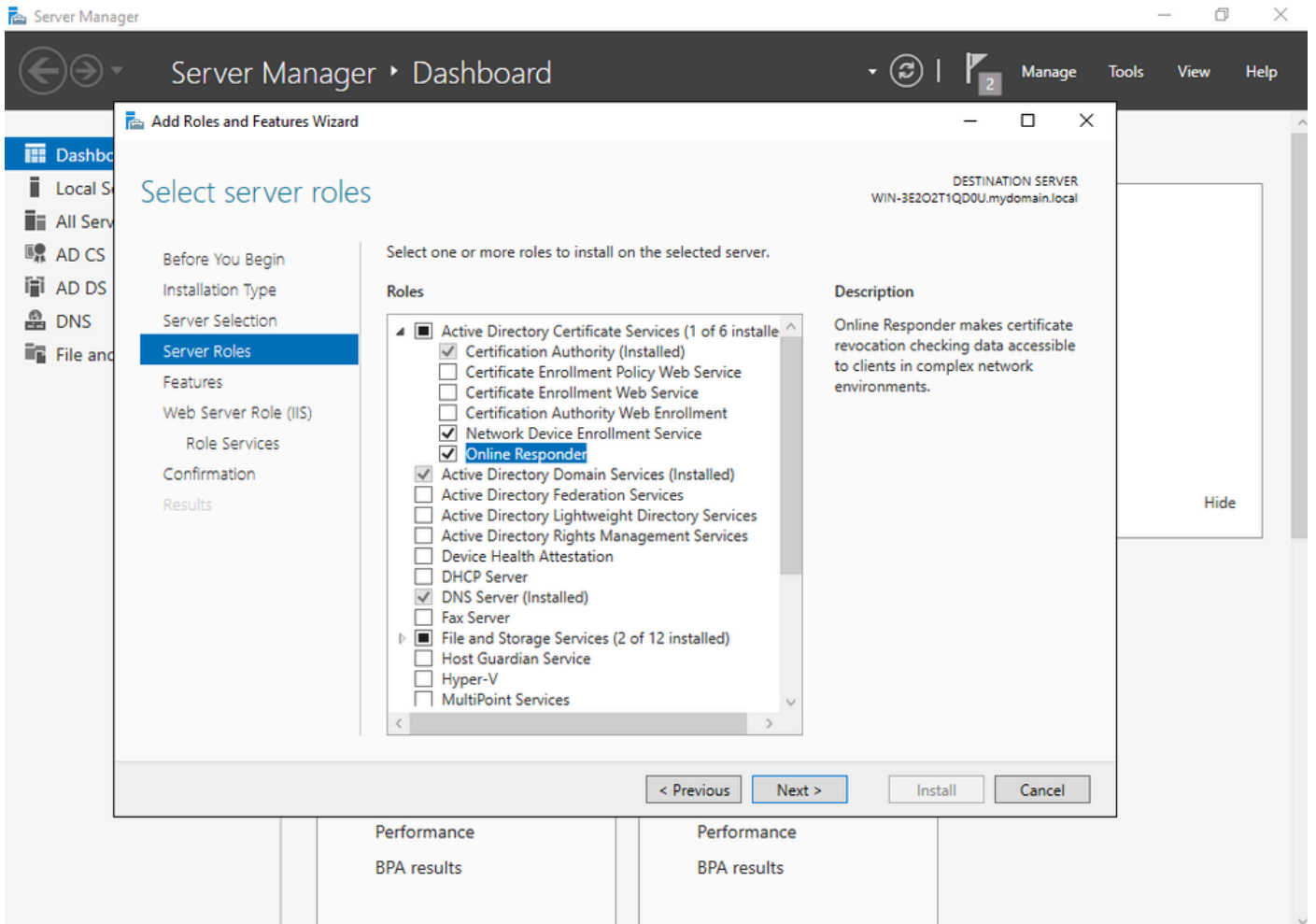
Choisir une autorité de certification racine

Il est important que le compte que vous utilisez pour votre autorité de certification fasse partie du groupe IIS\_IUSRS. Dans cet exemple, vous utilisez le compte Administrateur et accédez au menu Utilisateurs et ordinateurs Active Directory pour ajouter les utilisateurs Administrateur au groupe IIS\_IUSRS.



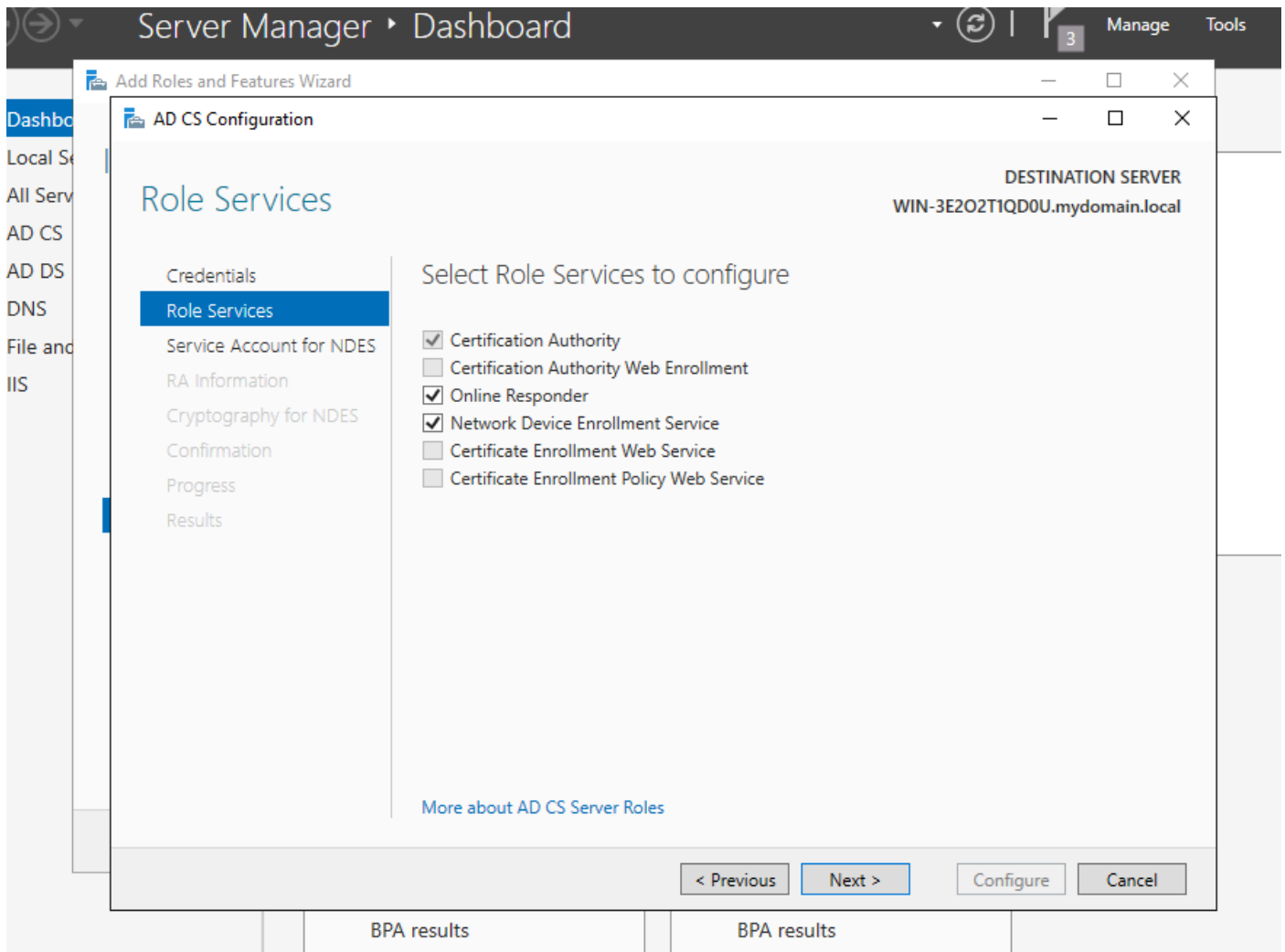
Ajoutez votre compte administrateur au groupe IIS\_USER

Étape 10. Une fois que vous avez un utilisateur dans le groupe IIS approprié, ajoutez des rôles et des services. Ajoutez ensuite le répondeur en ligne et les services NDES à votre autorité de certification.



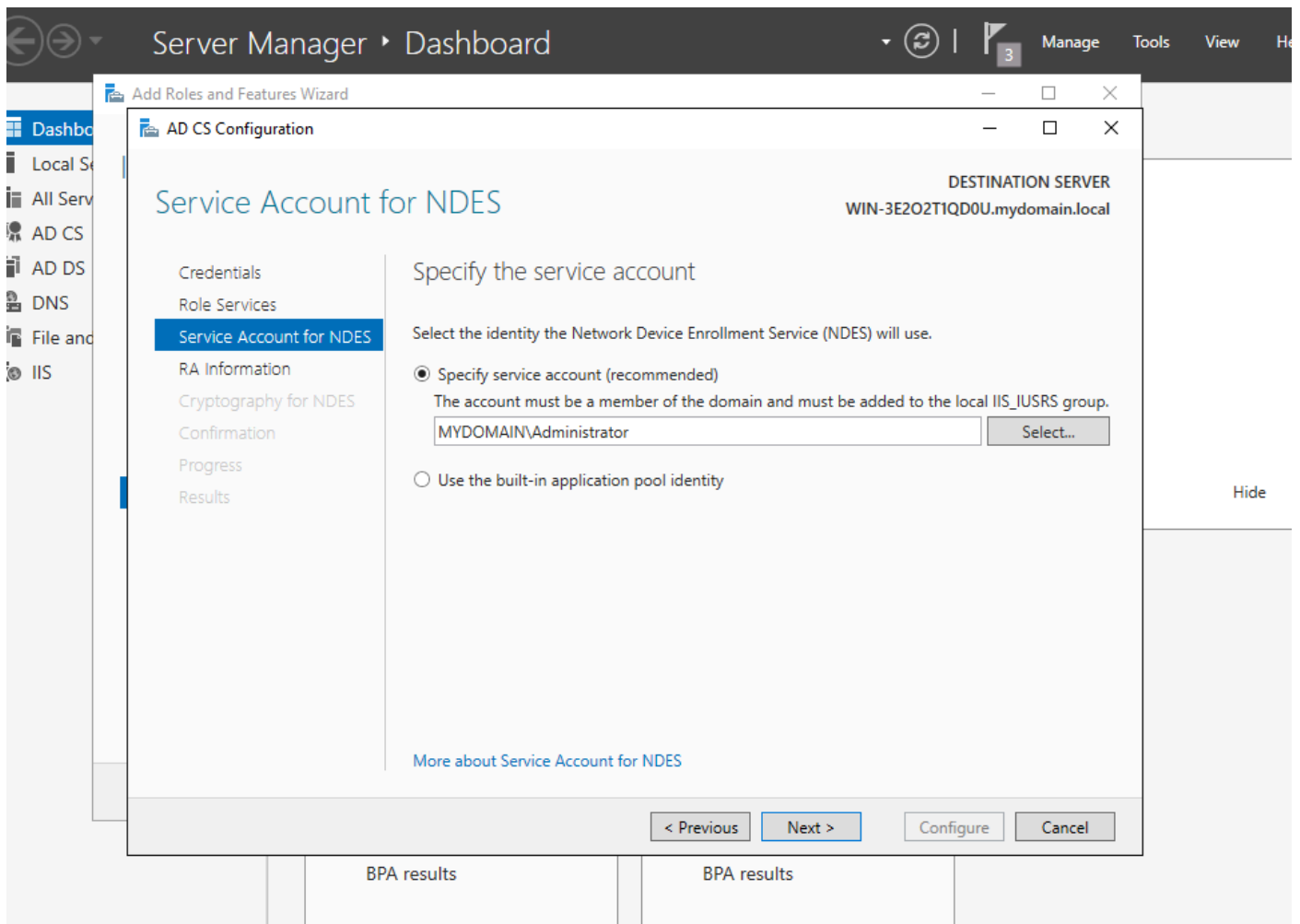
Installer le NDES et les services de répondeur en ligne

Étape 11. Une fois terminé, configurez ces services.



Installer le répondeur en ligne et le service NDES

Étape 12. Vous êtes invité à choisir un compte de service. Il s'agit du compte que vous avez précédemment ajouté au groupe IIS\_IUSRS.



Sélectionnez l'utilisateur que vous avez ajouté au groupe IIS

Étape 13. Ceci est suffisant pour les opérations SCEP, mais afin d'obtenir l'authentification 802.1X, vous devez également installer un certificat sur le serveur RADIUS. Par conséquent, pour simplifier, installez et configurez le service d'inscription Web afin de pouvoir copier et coller facilement la demande de certificat ISE sur votre serveur Windows.

# Select server roles

DESTINATION SERVER  
WIN-3E2O2T1QD0U.mydomain.local

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

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

## Roles

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

## Description

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

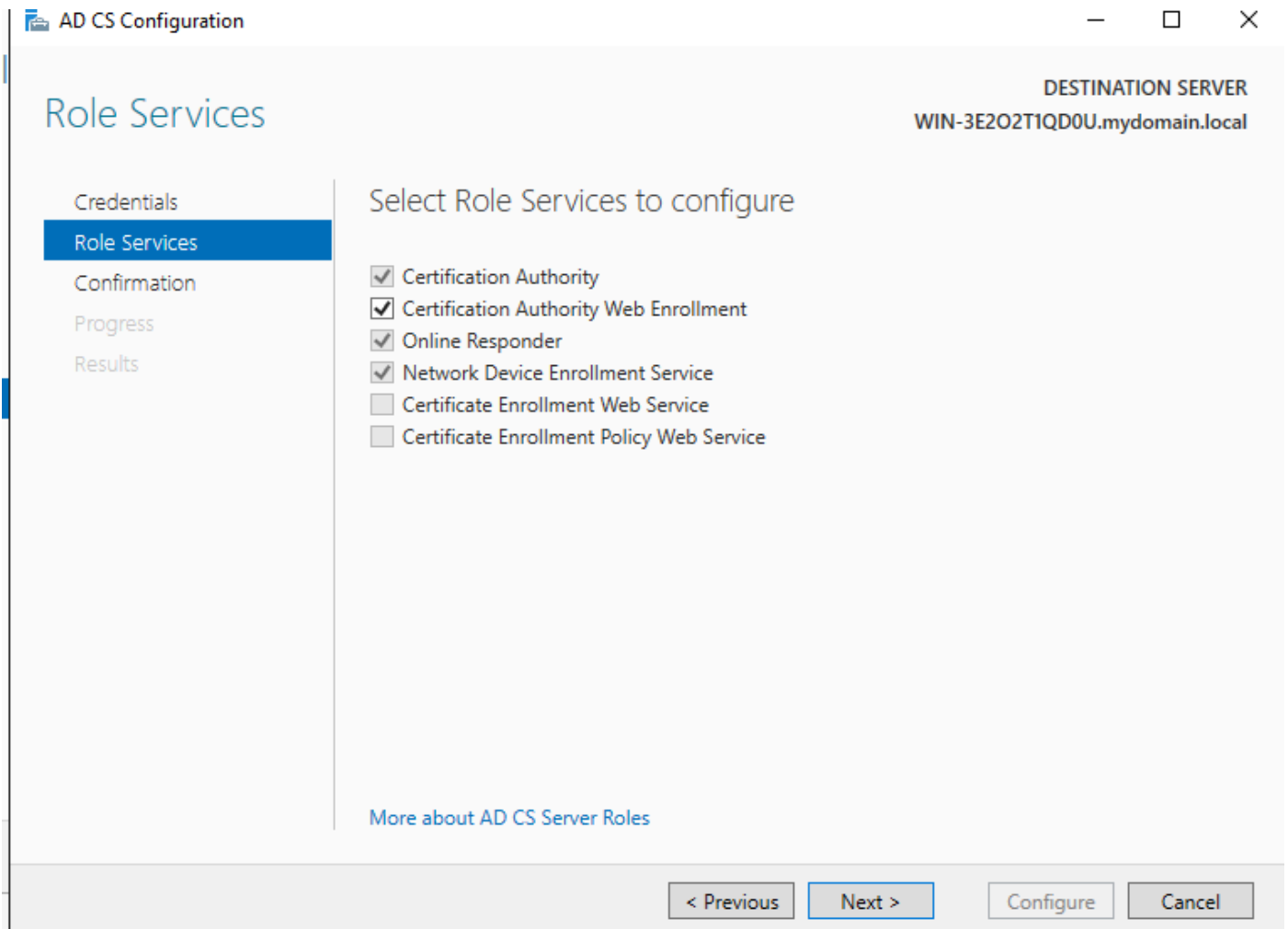
< Previous

Next >

Install

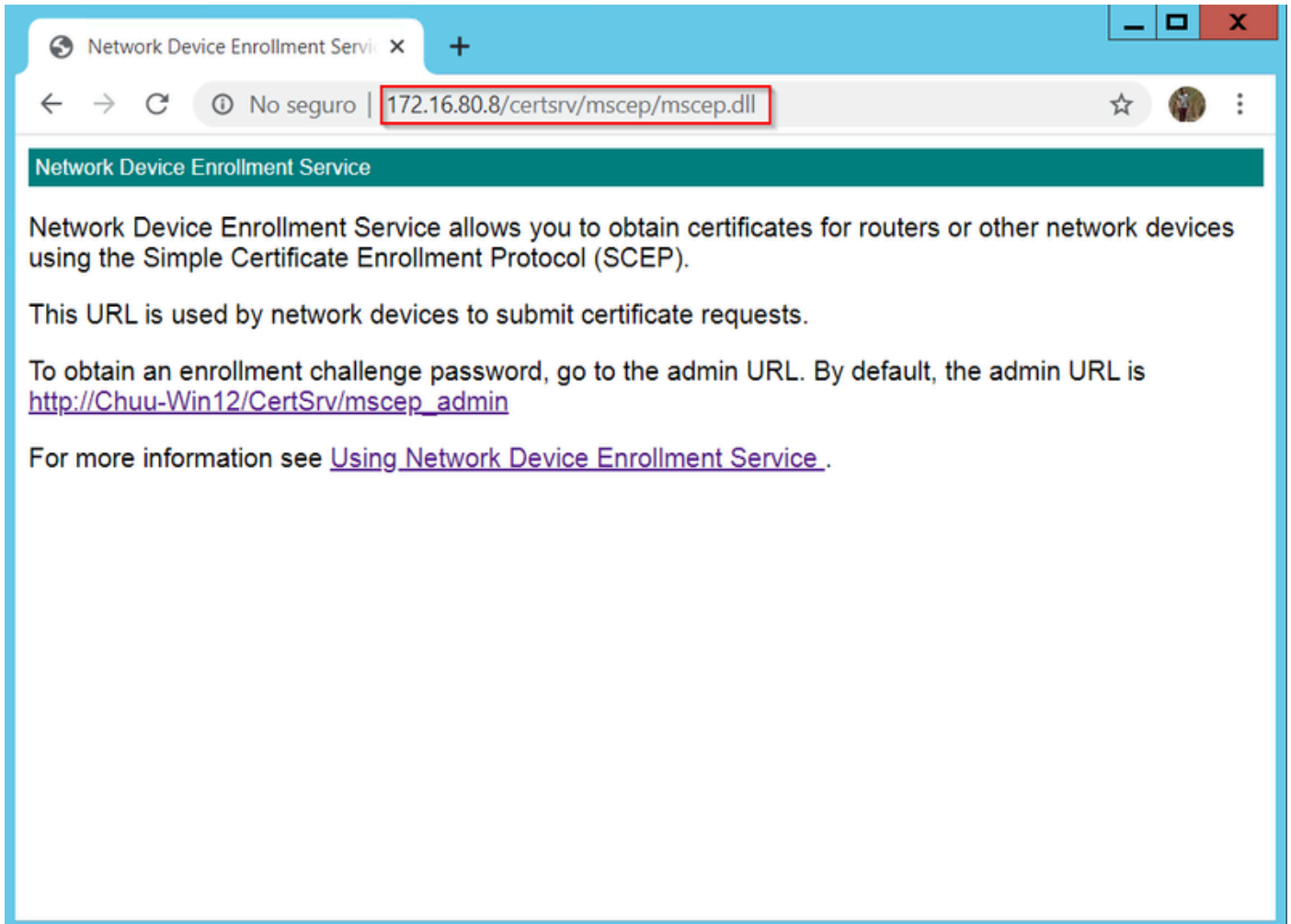
Cancel

Installer le service d'inscription Web



configurer le service d'inscription web

Étape 14. Vous pouvez vérifier que le service SCEP fonctionne correctement en visitant <http://<serverip>/certsrv/mscep/mscep.dll> :



Vérification du portail SCEP

## Étape 15.

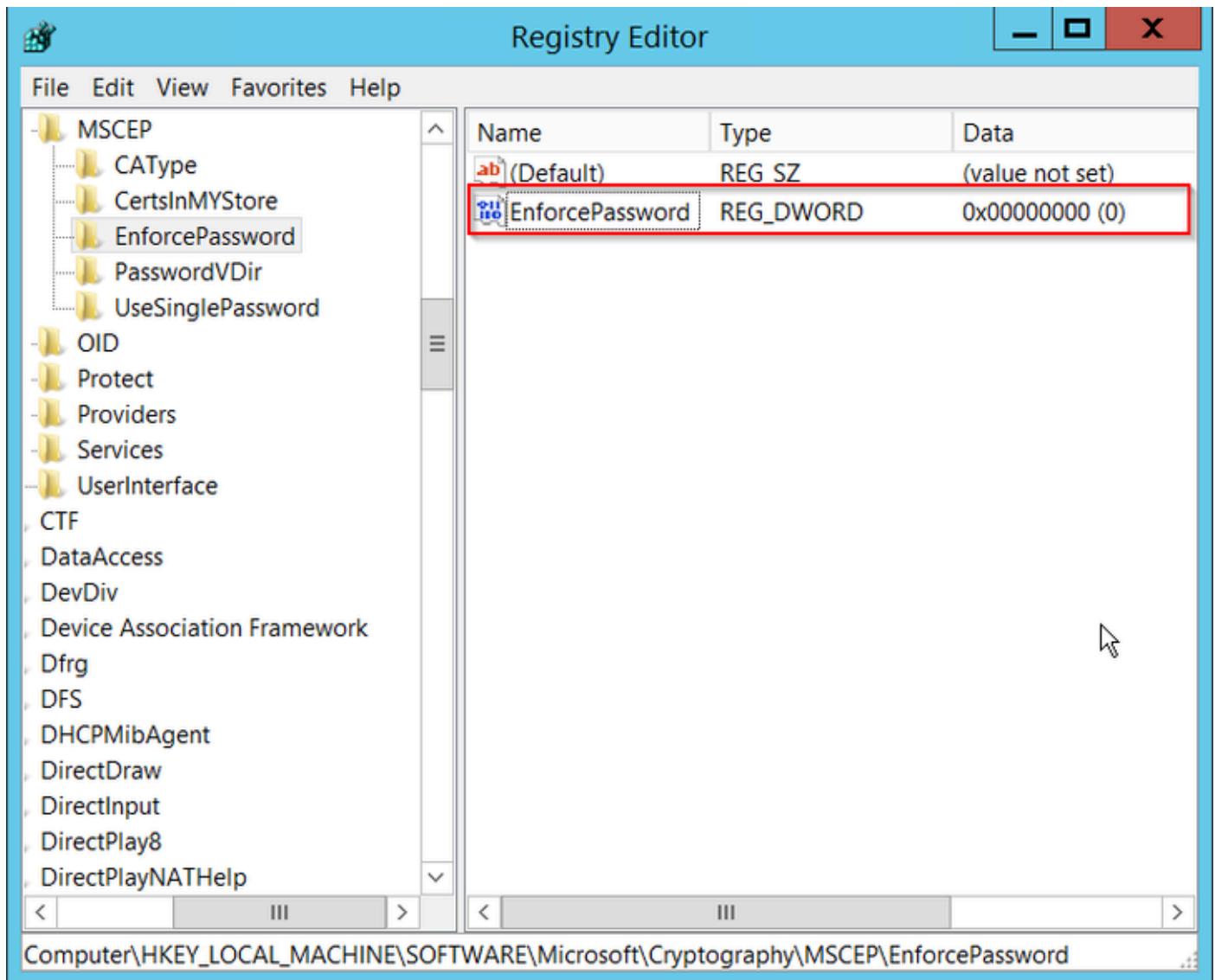
Par défaut, Windows Server a utilisé un mot de passe de demande de confirmation dynamique pour authentifier les demandes des clients et des terminaux avant l'inscription dans Microsoft SCEP (MSCEP). Cela nécessite un compte d'administrateur pour accéder à l'interface utilisateur graphique Web afin de générer un mot de passe à la demande pour chaque demande (le mot de passe doit être inclus dans la demande). Le contrôleur n'est pas en mesure d'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 :

Ouvrez l'Éditeur du Registre et recherchez Regedit dans le menu Démarrer.

Accédez à Computer > HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword

Modifiez la valeur EnforcePassword sur 0. S'il est déjà 0, laissez-le tel quel.





Définition de la valeur Enforcepassword

## Configurer le modèle de certificat et le Registre

Les certificats et les clés associées peuvent être utilisés dans plusieurs scénarios à différentes fins définies par les stratégies d'application au sein du serveur AC. La stratégie d'application est stockée dans le champ Extended Key Usage (EKU) du certificat. Ce champ est analysé par l'authentificateur pour vérifier qu'il est utilisé par le client pour l'usage prévu. 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 Users, puis sélectionnez Duplicate Template dans le menu contextuel.

Étape 4. Accédez à l'onglet Général, modifiez le nom du modèle et la période de validité comme

vous le souhaitez, laissez toutes les autres options décochées.

---

 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.

---

## Properties of New Template



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

Template display name:

Template name:

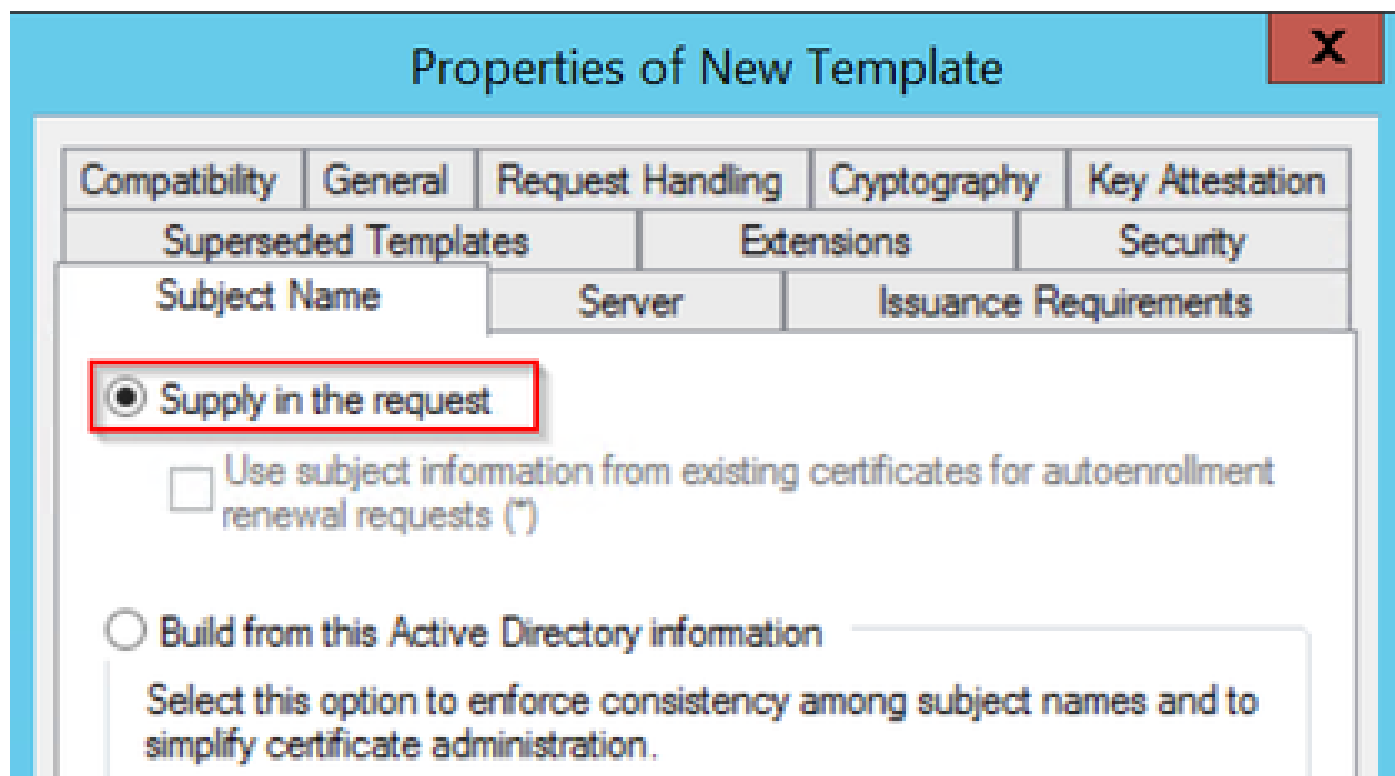
Validity period:  years

Renewal period:  weeks

Publish certificate in Active Directory

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

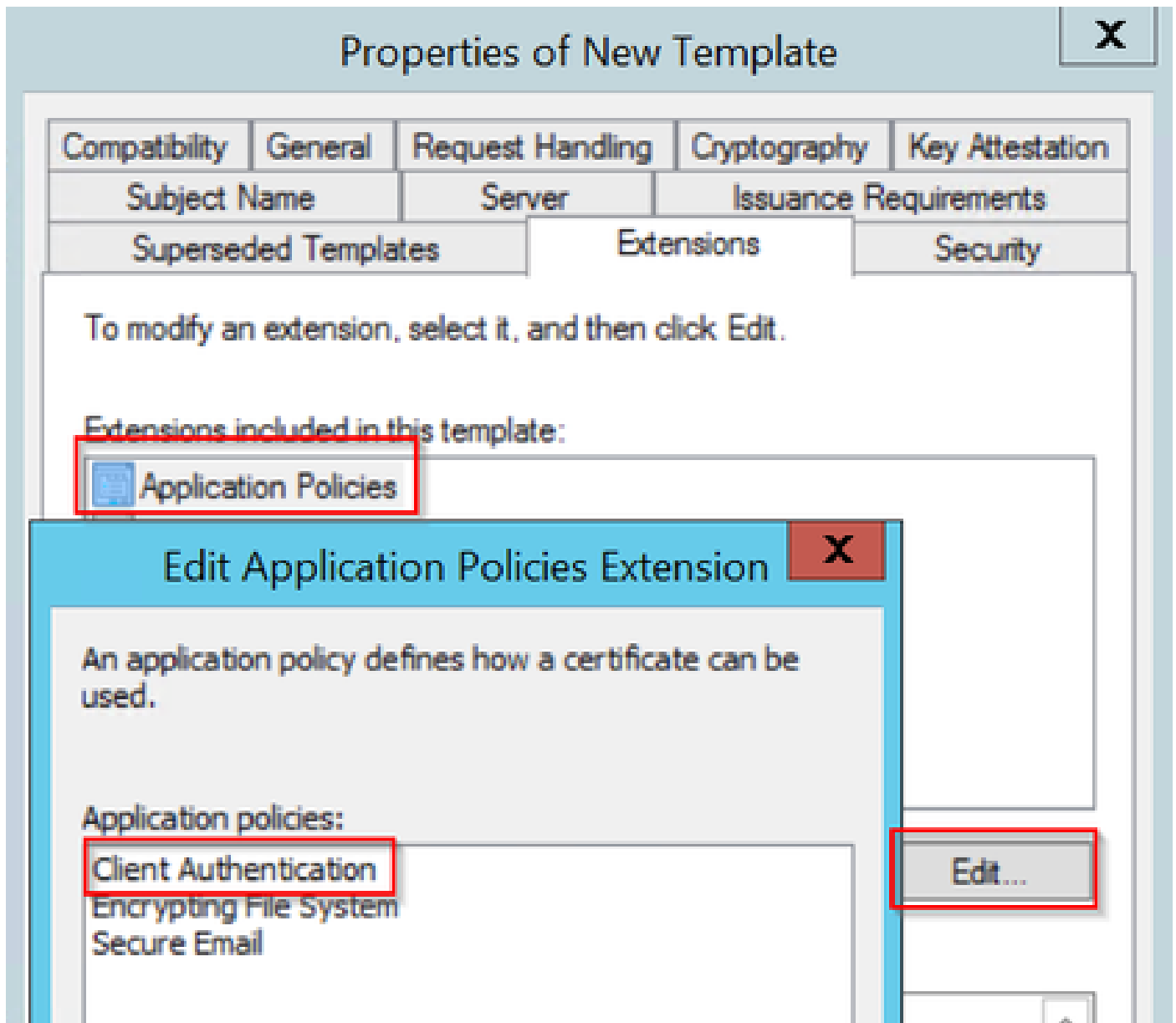
Étape 5. Accédez à l'onglet Nom de l'objet, vérifiez que Approvisionnement dans la demande est sélectionné. Une fenêtre contextuelle apparaît pour indiquer que les utilisateurs n'ont pas besoin de l'approbation de l'administrateur pour obtenir leur certificat signé, sélectionnez OK.



The screenshot shows the 'Properties of New Template' dialog box with the 'Subject Name' tab selected. The 'Supply in the request' radio button is selected and highlighted with a red box. Below it is an unchecked checkbox for 'Use subject information from existing certificates for autoenrollment renewal requests (?)'. The 'Build from this Active Directory information' radio button is unselected. The dialog has a blue title bar with a close button (X) in the top right corner. The tabs at the top are Compatibility, General, Request Handling, Cryptography, and Key Attestation. Below the tabs are sections for Superseded Templates, Extensions, and Security. The 'Subject Name' section includes a 'Server' field and 'Issuance Requirements'.

Fourniture dans la demande

Étape 6. Accédez à l'onglet Extensions, puis sélectionnez l'option Stratégies d'application et cliquez sur le bouton Modifier.... Assurez-vous que Client Authentication est dans la fenêtre Application Policies ; sinon, sélectionnez Add et ajoutez-le.



Vérifier les postes

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 le serveur Windows dispose des autorisations Contrôle total du modèle, puis sélectionnez Appliquer et OK.

# Properties of New Template



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

Group or user names:

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

Add... Remove

Permissions for Administrator

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

For special permissions or advanced settings, click Advanced.


Advanced

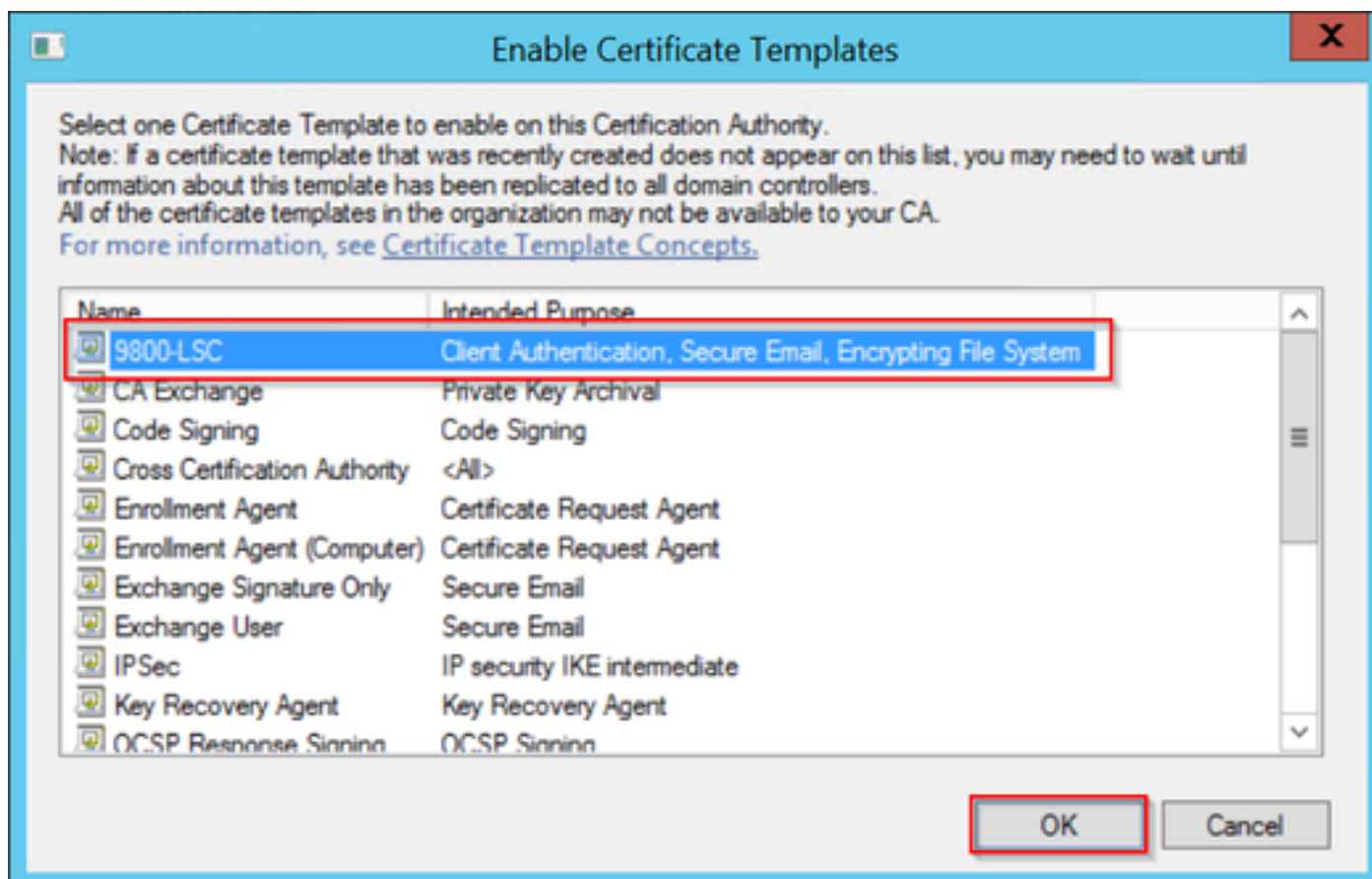
OK Cancel **Apply** Help

Donner un contrôle total

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

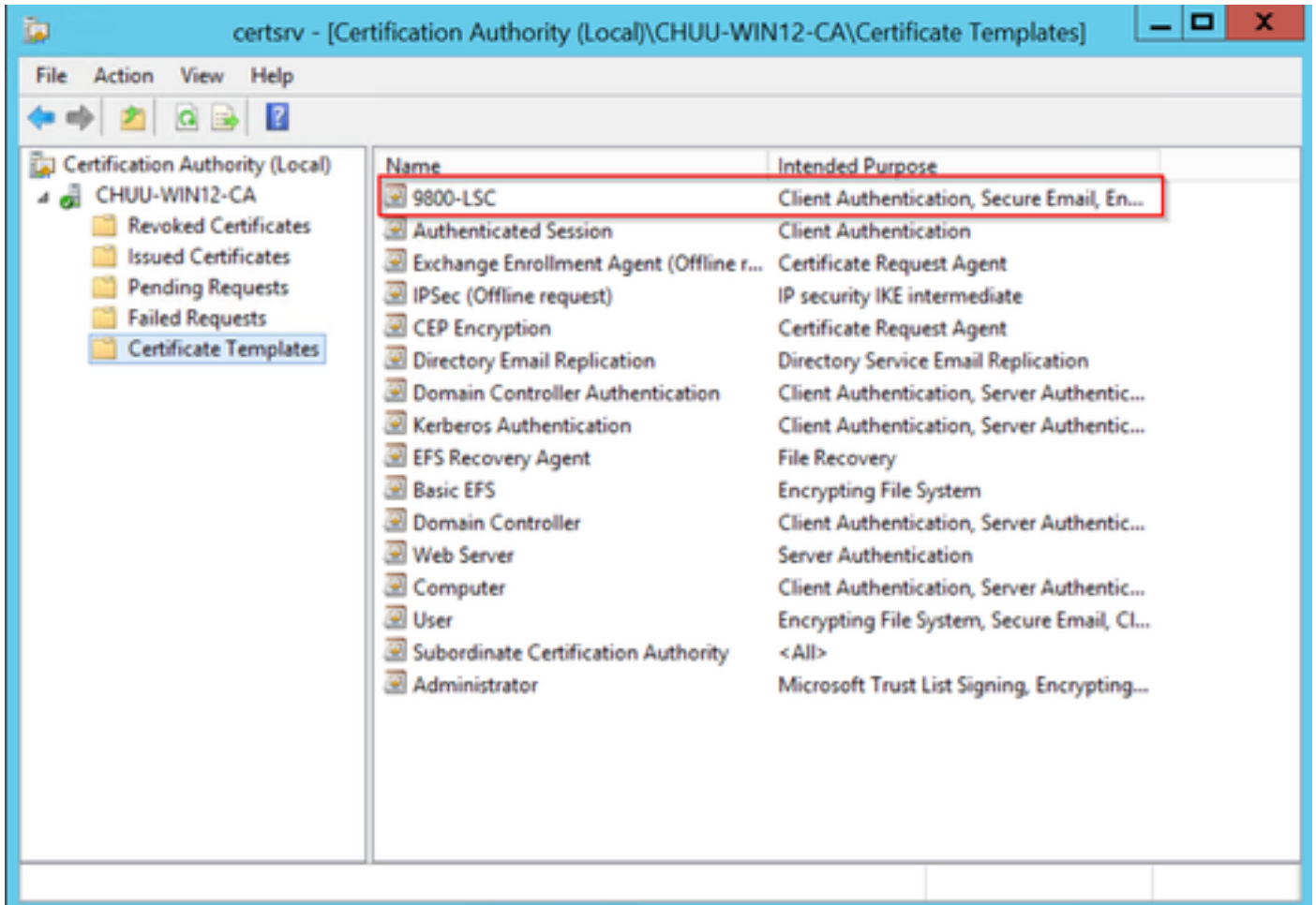
Étape 9. Sélectionnez le modèle de certificat précédemment créé, dans cet exemple est 9800-LSC, et sélectionnez OK.

 Remarque : 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.



Sélectionnez le modèle

Le nouveau modèle de certificat est maintenant répertorié dans le contenu du dossier Modèles de certificat.

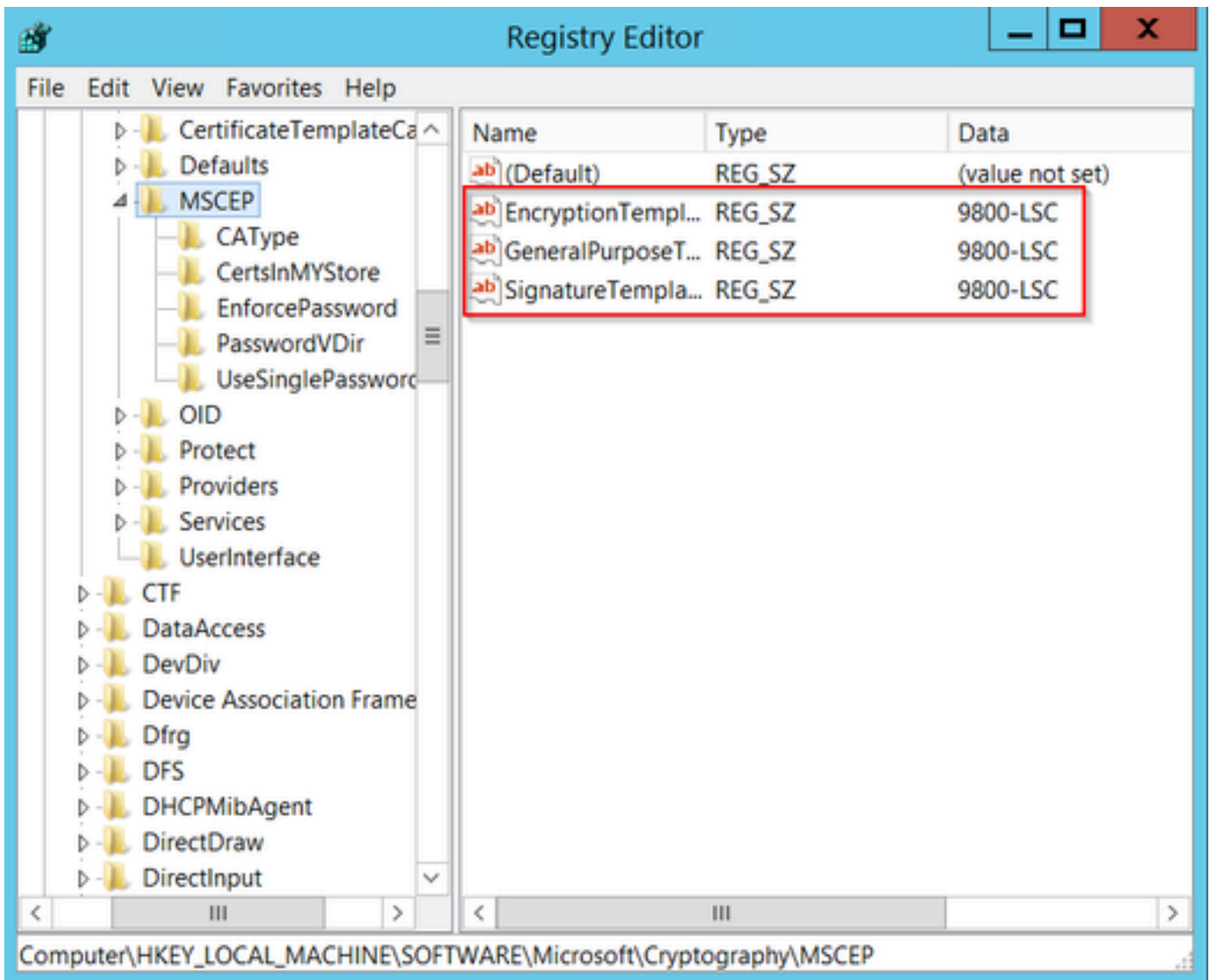


Sélectionnez le LSC

Étape 10. Revenez à la fenêtre Éditeur du Registre et naviguez jusqu'à Ordinateur > HKEY\_LOCAL\_MACHINE > LOGICIEL > Microsoft > Cryptographie > MSCEP.

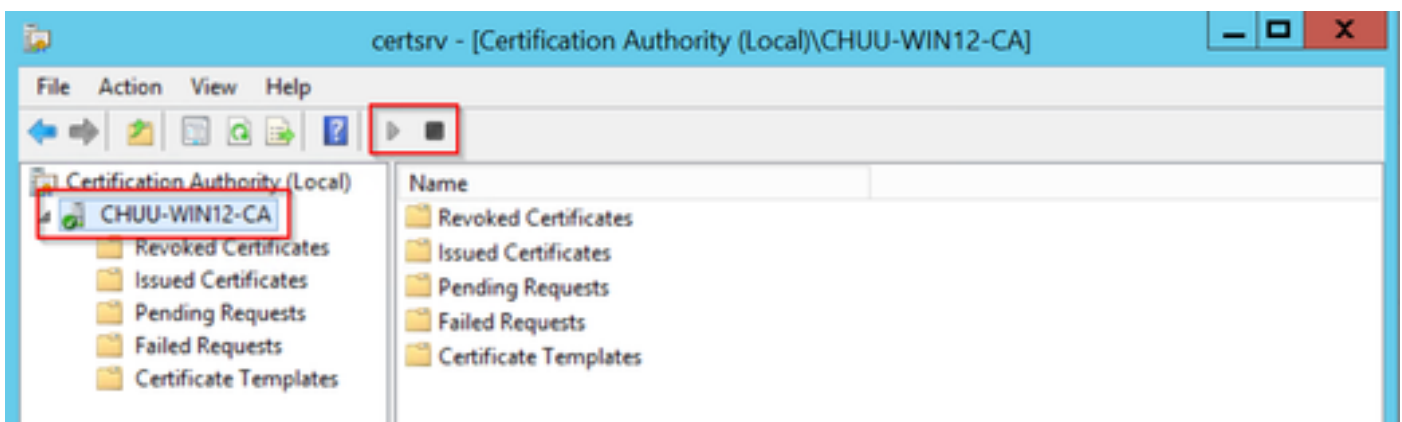
Étape 11. Modifiez les registres EncryptionTemplate, GeneralPurposeTemplate et SignatureTemplate afin qu'ils pointent vers le modèle de certificat nouvellement créé.





Modifier le modèle dans le Registre

Étape 12. Redémarrez le serveur NDES, revenez à la fenêtre Certification Authority, sélectionnez le nom du serveur, puis cliquez sur le bouton Stop and Play.



## Configuration de LSC sur le 9800

Voici les étapes dans l'ordre pour configurer LSC pour AP dans WLC.

1. Créez une clé RSA. Cette clé est utilisée ultérieurement pour le point de confiance PKI.
2. Créez un point de confiance et mappez la clé RSA créée.
3. Activez le provisionnement LSC pour les points d'accès et mappez le point de confiance.
  1. Activez LSC pour tous les points d'accès joints.
  2. Activez LSC pour les points d'accès sélectionnés via la liste de provisionnement.
4. Modifiez le point de confiance de gestion sans fil et pointez sur le point de confiance LSC.

## Étapes de configuration de l'interface graphique LSC AP

Étape 1. Accédez à Configuration > Security > PKI Management > Key Pair Generation.

1. Cliquez sur Ajouter et donnez-lui un nom approprié.
2. Ajoutez la taille de la clé RSA.
3. L'option exportable key est facultative. Cela n'est nécessaire que si vous souhaitez exporter la clé hors de la boîte.
4. Sélectionnez Générer

Configuration > Security > PKI Management

Trustpoints CA Server **Key Pair Generation** Add Certificate Trustpool

+ Add

Key Name	Key Type	Key Exportable	Zeroize
TP-self-signed-2147029136	RSA	No	Zeroize
9800-40.cisco.com	RSA	No	Zeroize
TP-self-signed-2147029136.server	RSA	No	Zeroize
CISCO_IDEVID_SUDI	RSA	No	Zeroize
CISCO_IDEVID_SUDI_LEGACY	RSA	No	Zeroize

Key Name\* AP-SCEP

Key Type\*  RSA Key  EC Key

Modulus Size\* 2048

Key Exportable\*

Cancel Generate

Étape 2. Accédez à Configuration > Security > PKI Management > Trustpoints

1. Cliquez sur Ajouter et donnez-lui un nom approprié.
2. Saisissez l'URL d'inscription (ici, l'URL est <http://10.106.35.61:80/certsrv/mscep/mscep.dll>) et le reste des détails.
3. Sélectionnez les paires de clés RSA créées à l'étape 1.
4. Cliquez sur Authentifier.
5. Cliquez sur enroll trustpoint et saisissez un mot de passe.
6. Cliquez sur Apply to Device.

Configuration > Security > PKI Management

### Add Trustpoint

Label\*  Enrollment Type  SCEP  Terminal

**Subject Name**

Country Code  State

Location  Domain Name

Organization  Email Address

Enrollment URL  Authenticate

Key Generated  Available RSA Keypairs

Enroll Trustpoint

Password\*

Re-Enter Password\*

Étape 3. Accédez à Configuration > Wireless > Access Points. Faites défiler vers le bas et sélectionnez LSC Provision.

1. Sélectionnez l'état Activé. Cela active LSC pour tous les AP qui sont connectés à ce WLC.
2. Sélectionnez le nom du point de confiance que nous avons créé à l'étape 2.

Remplissez le reste des détails en fonction de vos besoins.

Configuration > Wireless > Access Points

All Access Points

Total APs: 1

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP000-F89A-6E0	C9117AX-D	2	<span style="color: green;">●</span>	0 days 0 hrs 26 mins 42 secs	10.105.101.198	d0ec.3579.0300	0cd0.f89a.45a0	Local	Yes	Registered	Health

Misconfigured APs: Tag: 0, Country Code: 0, LSC Fallback: 0

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

**LSC Provision**

Status

Trustpoint Name

Number of Join Attempts

Key Size

Certificate chain status: Not Available

Subject Name Parameters

Country

State

City

Organization

Une fois que vous activez LSC, les AP téléchargent le certificat via WLC et redémarrent. Dans la

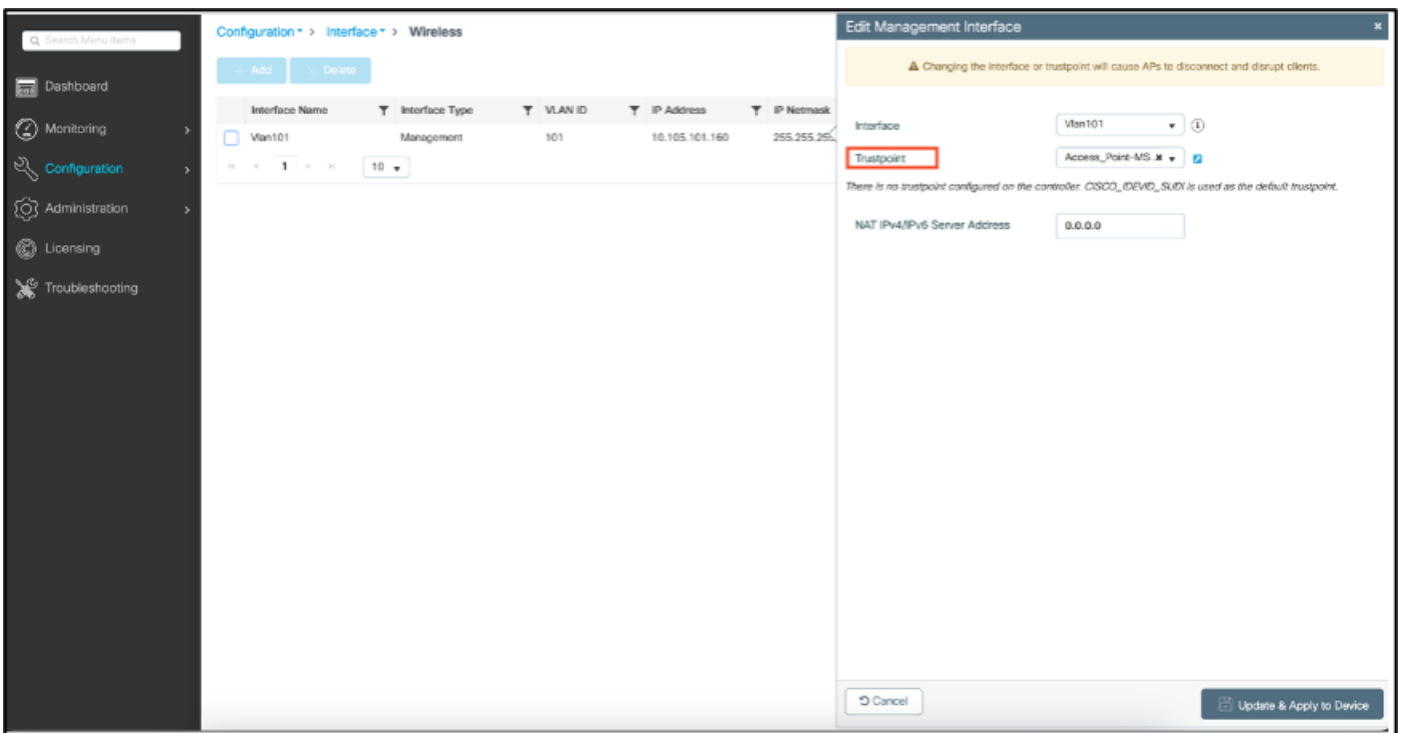
session de console AP, vous voyez alors quelque chose comme cet extrait.

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

Étape 4. Une fois LSC activé, vous pouvez modifier le certificat de gestion sans fil pour qu'il corresponde au point de confiance LSC. Cela fait que les AP se joignent avec leurs certificats LSC et le WLC utilise son certificat LSC pour la jonction d'AP. Il s'agit d'une étape facultative si votre seul intérêt est d'effectuer l'authentification 802.1X de vos AP.

1. Accédez à Configuration > Interface > Wireless et cliquez sur Management Interface.
2. Modifiez le point de confiance pour qu'il corresponde au point de confiance que nous avons créé à l'étape 2.

Nous voici à la fin de la partie de configuration LSC GUI. Les AP doivent pouvoir joindre le WLC en utilisant le certificat LSC maintenant.



## Étapes de configuration LSC CLI AP

1. Créez une clé RSA à l'aide de cette commande.

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

```
% You already have RSA keys defined named AP-SCEP.
% They will be replaced
```

```
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storage
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. Créez un point de confiance PKI et mappez la paire de clés RSA. Saisissez l'URL d'inscription et les autres détails.

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. Authentifiez et inscrivez le point de confiance PKI auprès du serveur AC à l'aide de la commande `crypto pki authenticate <trustpoint>`. Entrez un mot de passe à l'invite.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' command will show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
```

```
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

#### 4. Configurez la jonction AP avec le certificat LSC.

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

#### 5. Modifiez le point de confiance de gestion sans fil pour qu'il corresponde au point de confiance créé ci-dessus.

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

### Vérification LSC AP

Exécutez ces commandes sur le WLC pour vérifier le LSC.

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

```

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

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

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
-----

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

9800-40#

```

```

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

```

Une fois les AP rechargés, connectez-vous à l'interface de ligne de commande des AP et exécutez ces commandes pour vérifier la configuration LSC.

```

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

```

```

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

```

```

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

```

```

AP0CD0.F89A.46E0#sho dtls connections

Number of DTLS connection = 1

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

Current connection certificate issuer name: sumans-lab-ca

```

## Dépannage du provisionnement LSC

Vous pouvez effectuer une capture EPC à partir du port de commutation de liaison ascendante WLC ou AP pour vérifier le certificat utilisé par AP pour former le tunnel CAPWAP. Vérifiez à partir du PCAP si le tunnel DTLS est correctement construit.

```

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

```

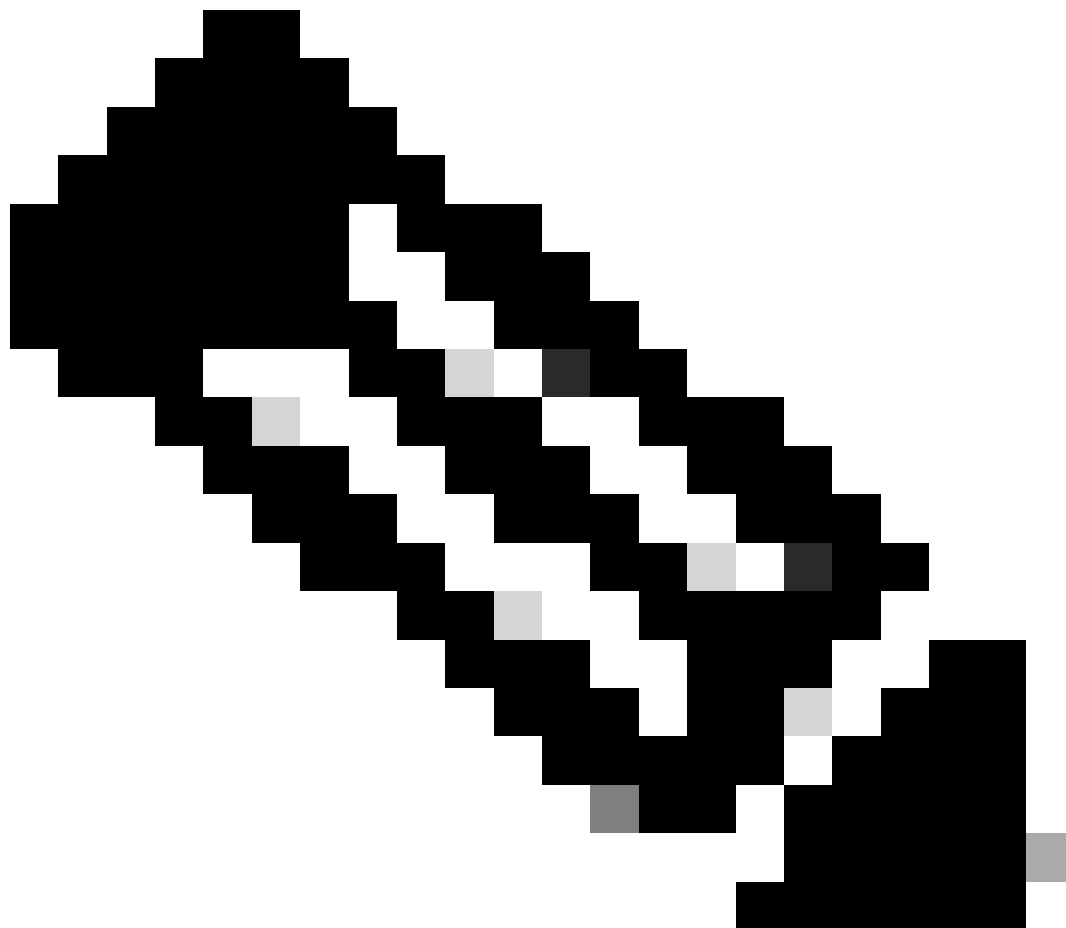
Les débogages DTLS peuvent être exécutés sur AP et WLC pour comprendre le problème du certificat.



## Authentification 802.1X filaire AP utilisant LSC

Le point d'accès est configuré pour utiliser le même certificat LSC pour s'authentifier. Le point d'accès agit comme demandeur 802.1X et est authentifié par le commutateur sur le serveur ISE. Le serveur ISE communique avec le service AD dans le back-end.

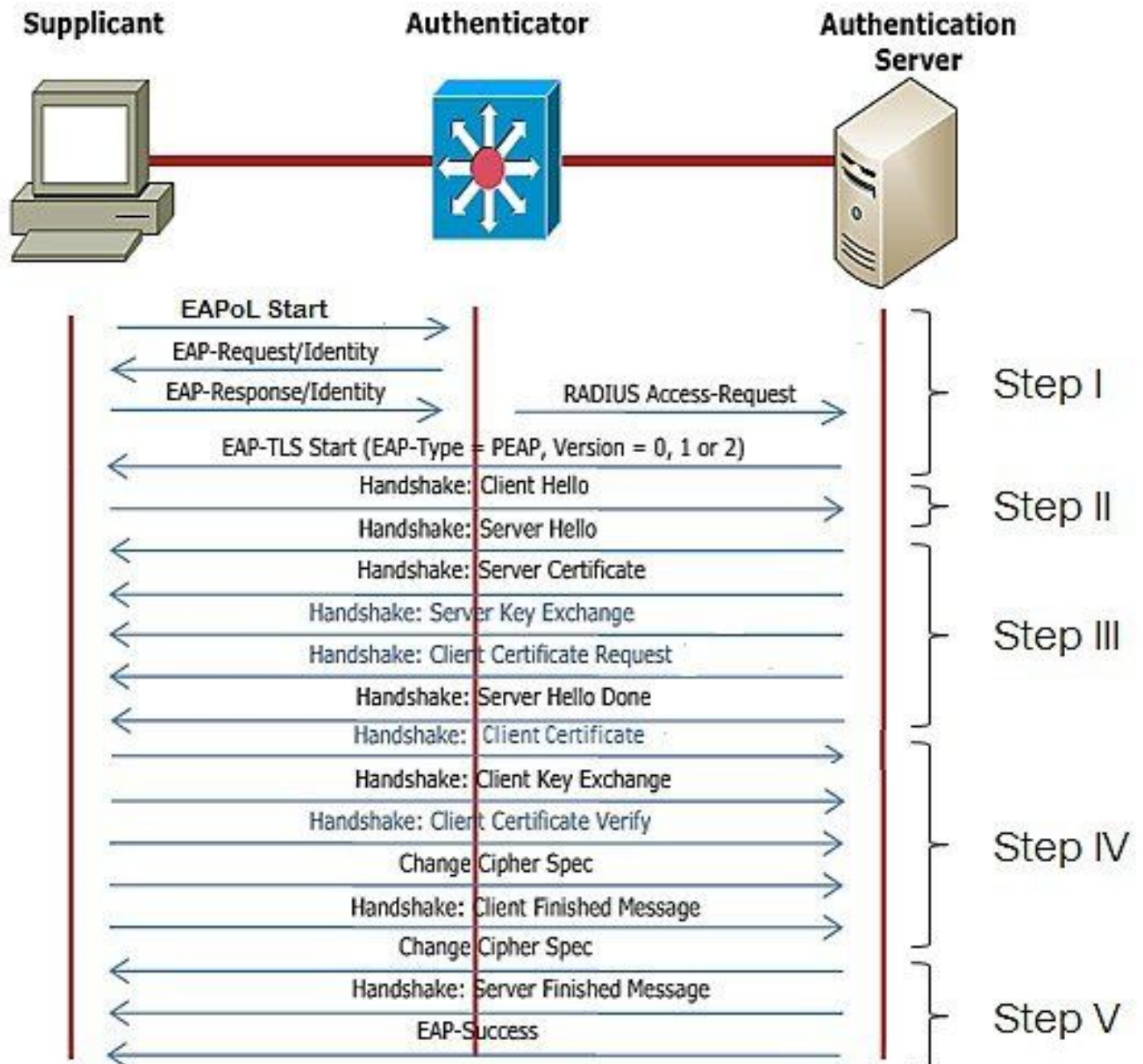
---



Remarque : une fois l'authentification dot1x activée sur le port de commutation de liaison ascendante AP, les AP ne peuvent pas transférer ou recevoir de trafic tant que l'authentification n'est pas passée. Pour récupérer les points d'accès dont l'authentification a échoué et obtenir l'accès au point d'accès, désactivez l'authentification dot1x sur le port de commutation filaire du point d'accès.

---

Workflow d'authentification EAP-TLS et échange de messages

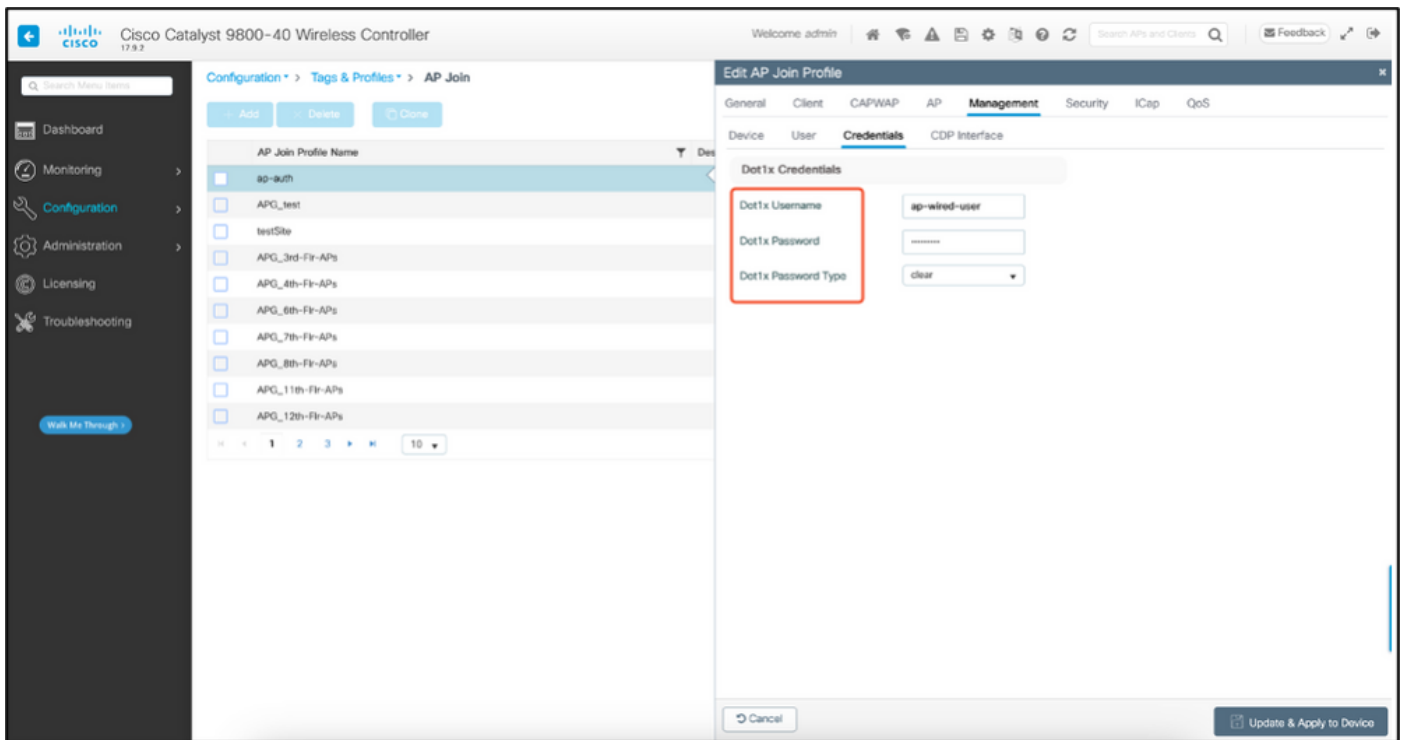
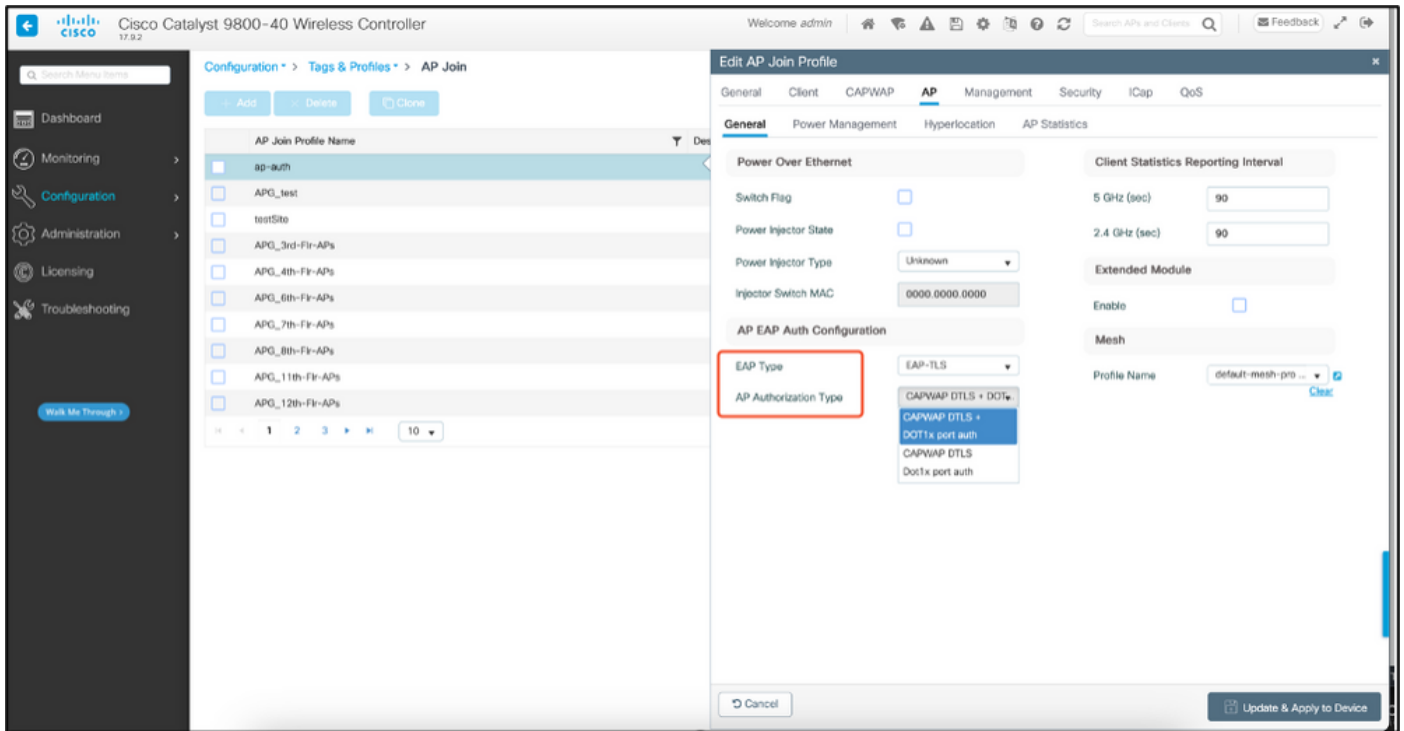


## Étapes de configuration de l'authentification 802.1x filaire AP

1. Activez l'authentification de port dot1x avec CAPWAP DTLS et sélectionnez le type EAP.
2. Créez des identifiants dot1x pour les points d'accès.
3. Activez dot1x sur le port du commutateur.
4. Installez un certificat sécurisé sur le serveur RADIUS.

## Configuration de l'interface graphique d'authentification 802.1x filaire AP

1. Accédez au profil de jointure AP et cliquez sur le profil.
  1. Cliquez sur AP > General. Sélectionnez le type EAP et le type d'autorisation AP « CAPWAP DTLS + dot1x port auth ».
  2. Accédez à Management > Credentials et créez un nom d'utilisateur et un mot de passe pour AP dot1x auth.



## Configuration CLI d'authentification 802.1x filaire AP

Utilisez ces commandes pour activer dot1x pour les AP à partir de l'interface de ligne de commande. Cela active uniquement l'authentification filaire pour les AP qui utilisent le profil de jointure spécifique.

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

```
9800-40(config)#ap profile ap-auth
9800-40(config-ap-profile)#dot1x eap-type eap-tls
9800-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9800-40(config-ap-profile)#
```

## Configuration du commutateur d'authentification 802.1x filaire AP

Cette configuration de commutateur est utilisée dans les travaux pratiques pour activer l'authentification filaire AP. Vous pouvez avoir une configuration différente en fonction de la conception.

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

## Installation du certificat du serveur RADIUS

L'authentification se produit entre le point d'accès (qui agit en tant que demandeur) et le serveur RADIUS. Les deux doivent se faire confiance. Le seul moyen pour que le point d'accès approuve le certificat du serveur RADIUS est de faire en sorte que le serveur RADIUS utilise un certificat émis par l'autorité de certification SCEP qui a également émis le certificat AP.

Dans ISE, accédez à Administration > Certificates > Generate Certificate Signing Requests

Générez un CSR et remplissez les champs avec les informations de votre noeud ISE.

### Certificate Signing Request

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

**ISE Identity Certificates:**

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

**ISE Certificate Authority Certificates:**

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

**Usage**

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

Allow Wildcard Certificates

**Node(s)**

Generate CSR's for these Nodes:

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

**Subject**

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Une fois généré, vous pouvez l'exporter et le copier-coller en tant que texte.

Accédez à votre adresse IP AC Windows et ajoutez /certsrv/ à l'URL

Cliquez sur Demander un certificat

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

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

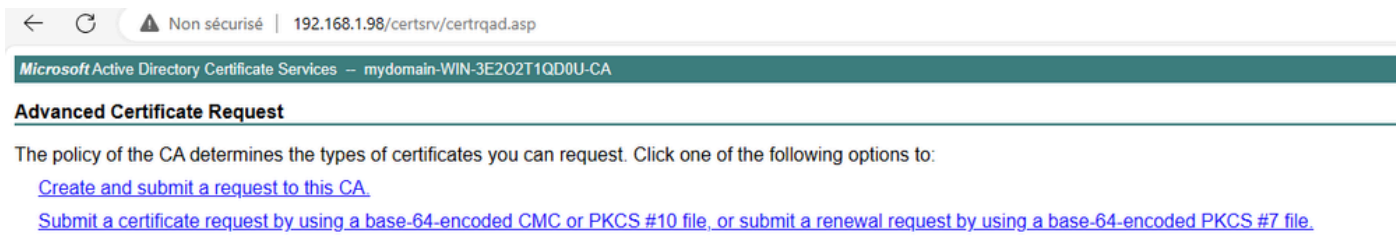
### Welcome

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

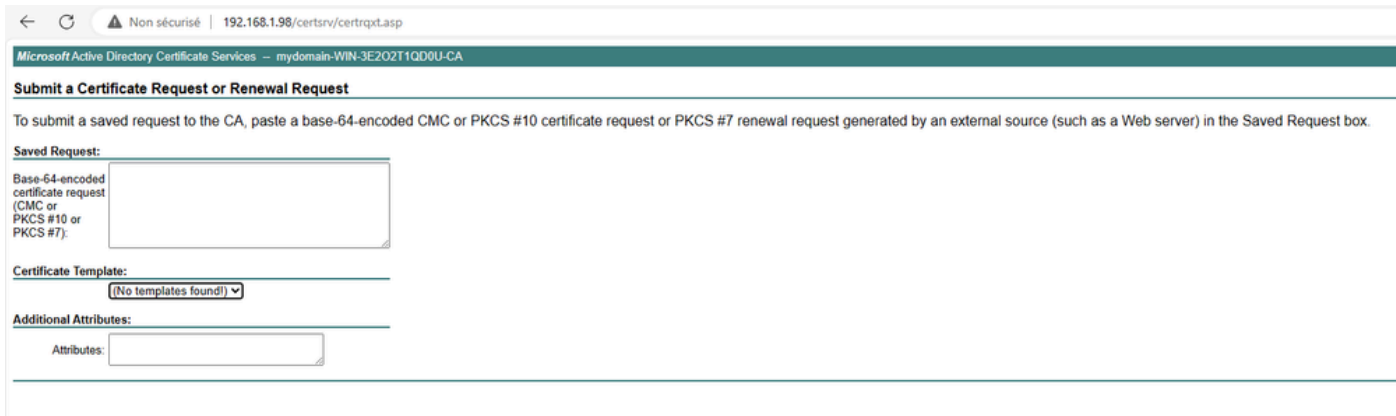
**Select a task:**

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

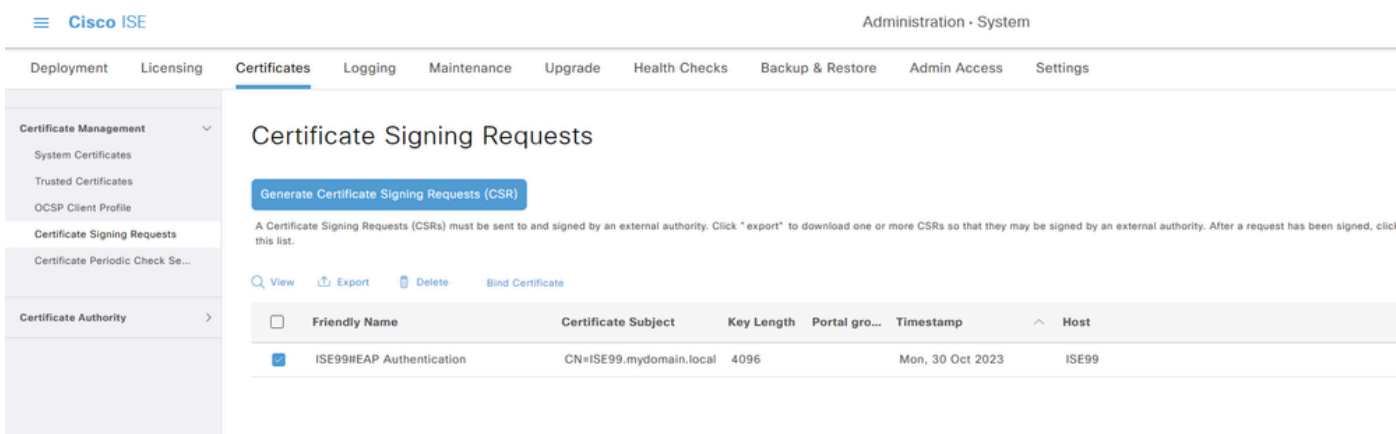
Cliquez sur Submit a certificate request by using a base-64 ....



Collez le texte CSR dans la zone de texte. Sélectionnez le modèle de certificat du serveur Web.



Vous pouvez ensuite installer ce certificat sur ISE en revenant au menu Certificate Signing Request et en cliquant sur Bind certificate. Vous pouvez ensuite télécharger le certificat obtenu à partir de votre ordinateur Windows C.



## Vérification de l'authentification 802.1x filaire AP

Accédez au point d'accès via la console et exécutez la commande :

```
#show ap authentication status
```

L'authentification AP n'est pas activée :

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

Journaux de console à partir du point d'accès après activation de l'authentification ap :

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

AP authentifié avec succès :

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

Vérification WLC :

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

État de l'interface du port de commutation après authentification réussie :

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

Voici un exemple de journaux de console AP indiquant une authentification réussie :

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```

# Dépannage de l'authentification 802.1X

Prenez PCAP sur la liaison ascendante AP et vérifiez l'authentification RADIUS. Voici un extrait d'authentification réussie.

479.	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, Identity(Packet size limited during capture)
479.	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2	Access-Challenge 1a234
479.	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2	Encrypted Handshake Message
479.	07:47:17.256975	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.267976	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.270962	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2	Access-Challenge 1a234
479.	07:47:17.274979	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.277963	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge 1a234
479.	07:47:17.311968	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)
479.	07:47:17.324988	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2	Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
479.	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP...	EAP	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.376979	10.186.34.178	10.185.101.151	RADIUS	Access-Accept id=251

TCPdump collecte de l'ISE capturant l'authentification.

80	07:47:18.177803	10.186.34.178	10.185.101.151	RADIUS	Access-Request 1a234
80	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge 1a234
80	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Request 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Request 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Request 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Request 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Challenge 1a234
79	07:47:18.182983	10.186.34.178	10.185.101.151	RADIUS	Access-Request 1a234
82	07:47:01.945978	10.186.34.178	10.185.101.151	RADIUS	Access-Accept id=251

Si un problème est observé pendant l'authentification, une capture de paquets simultanée à partir de la liaison ascendante filaire AP et du côté ISE serait nécessaire.

Commande de débogage pour AP :

```
#debug ap authentication packet
```

## Informations connexes

- [Assistance technique et téléchargements Cisco](#)
- [Configuration de 802.1X sur AP avec AireOS](#)
- [Guide de configuration du 9800 pour LSC](#)
- [Exemple de configuration LSC pour 9800](#)
- [Configuration de 802.1X pour les points d'accès sur 9800](#)



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.