شكلت 802.1X على APs ل PEAP وأ EAP-TLS مع LSC

المحتويات

قمدقملا

يصف اذه وثيقة كيف أن يصاق cisco منفذ نقطة على هم switchport يستعمل 802.1X PEAP وأ EAP-TLS طريقة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم اللاسلكية

- نقطة الوصول
- تبديل
- خادم ISE
- جهة منح الشهادة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم اللاسلكية: C9800-40-K9 التي تشغل الإصدار 17.09.02
- نقطة الوصول: C9117AXI-D
- المحول: C9200L-24P-4G ضكري 17.06.04
- خادم AAA: ISE-VM-K9 الذي يشغل 3.1.0.518
- جهة منح الشهادة: Windows Server 2016

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

إذا أردت نقاط الوصول (APs) أن تصادق مع switchport الخاص بها باستخدام 802.1X، فإنها تستخدم افتراضيا بروتوكول مصادقة EAP-FAST الذي لا يتطلب شهادات. إن أردت أن لا APs أن يستعمل ال PEAP-MSCHAPV2 طريقة (أي يستعمل مسوغات على ال ap جانب غير شهادة على ال RADIUS جانب) أو ال EAP-TLS طريقة (أي يستعمل شهادة على كلا الجانب)، أنت يضطر أن يشكل LSC أولا. وهي الطريقة الوحيدة لتوفير شهادة موثوق بها/جذر على نقطة الوصول (وكذلك شهادة جهاز في حالة EAP-TLS). لا يمكن لنقطة الوصول إجراء PEAP وتجاهل التحقق من جانب الخادم. يغطي هذا المستند أولا تكوين LSC ثم جانب تكوين 802.1X.

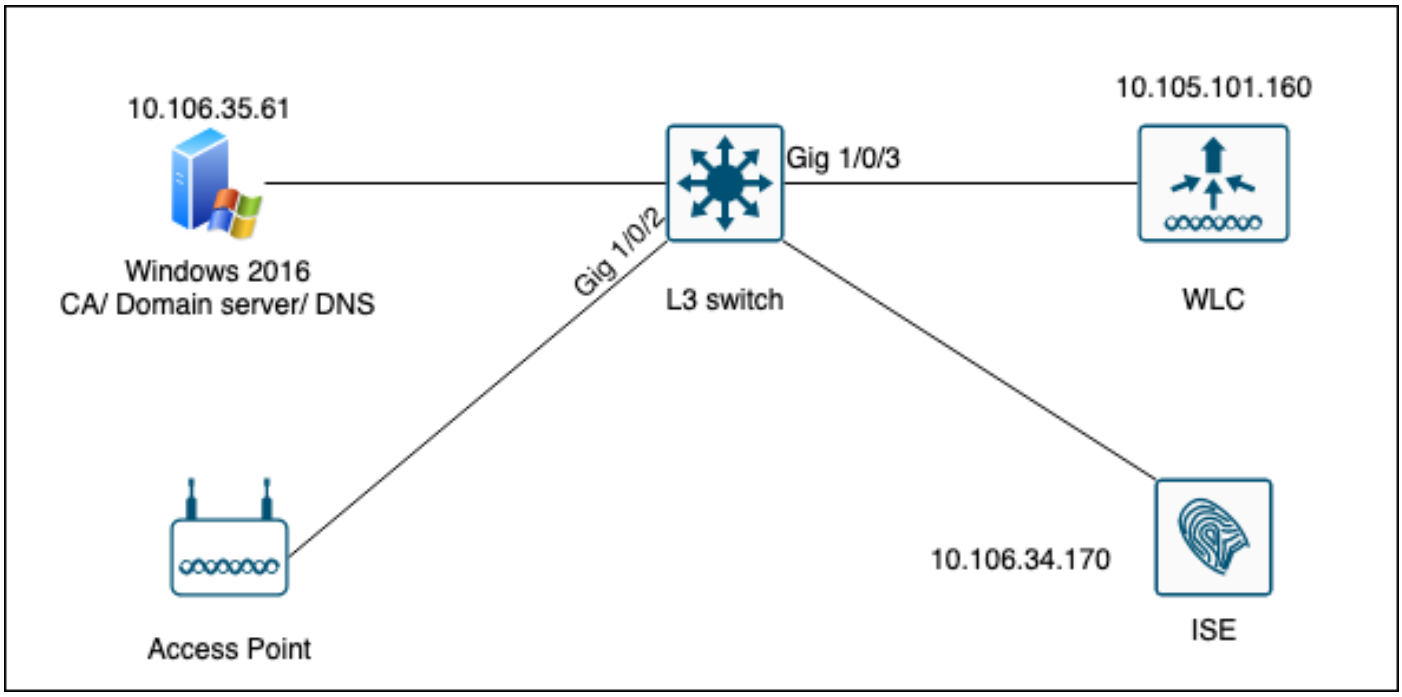
أستخدم LSC إذا كنت تريد أن توفر PKI تأمين أفضل، وتتحكم في مرجع الترخيص (CA)، وتحدد السياسات، والقيود، والاستخدامات على الشهادات التي تم إنشاؤها.

باستخدام LSC، يحصل جهاز التحكم على شهادة صادرة عن CA. لا تتصل نقطة الوصول مباشرة بخادم CA ولكن تتطلب وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) شهادات نيابة عن نقاط الوصول (APs) التي تنضم. يجب تكوين تفاصيل خادم CA على وحدة التحكم ويجب الوصول إليها.

تستخدم وحدة التحكم بروتوكول تسجيل الشهادة البسيط (SCEP) لإعادة توجيه الطلبات التي تم إنشاؤها على الأجهزة إلى CA وتستخدم SCEP مرة أخرى للحصول على الشهادات الموقعة من CA.

SCEP هو بروتوكول إدارة شهادات يستخدمه عملاء PKI وخوادم CA لدعم تسجيل الشهادة وإبطالها. وهو مستخدم على نطاق واسع في Cisco ومدعوم من قبل العديد من خوادم CA. في SCEP، يتم استخدام HTTP كبروتوكول نقل للرسائل PKI. الهدف الأساسي من بروتوكول SCEP هو الإصدار الآمن للشهادات إلى أجهزة الشبكة.

الرسم التخطيطي للشبكة



التكوين

هناك أمران للتكوين بشكل أساسي: SCEP CA و 9800 WLC.

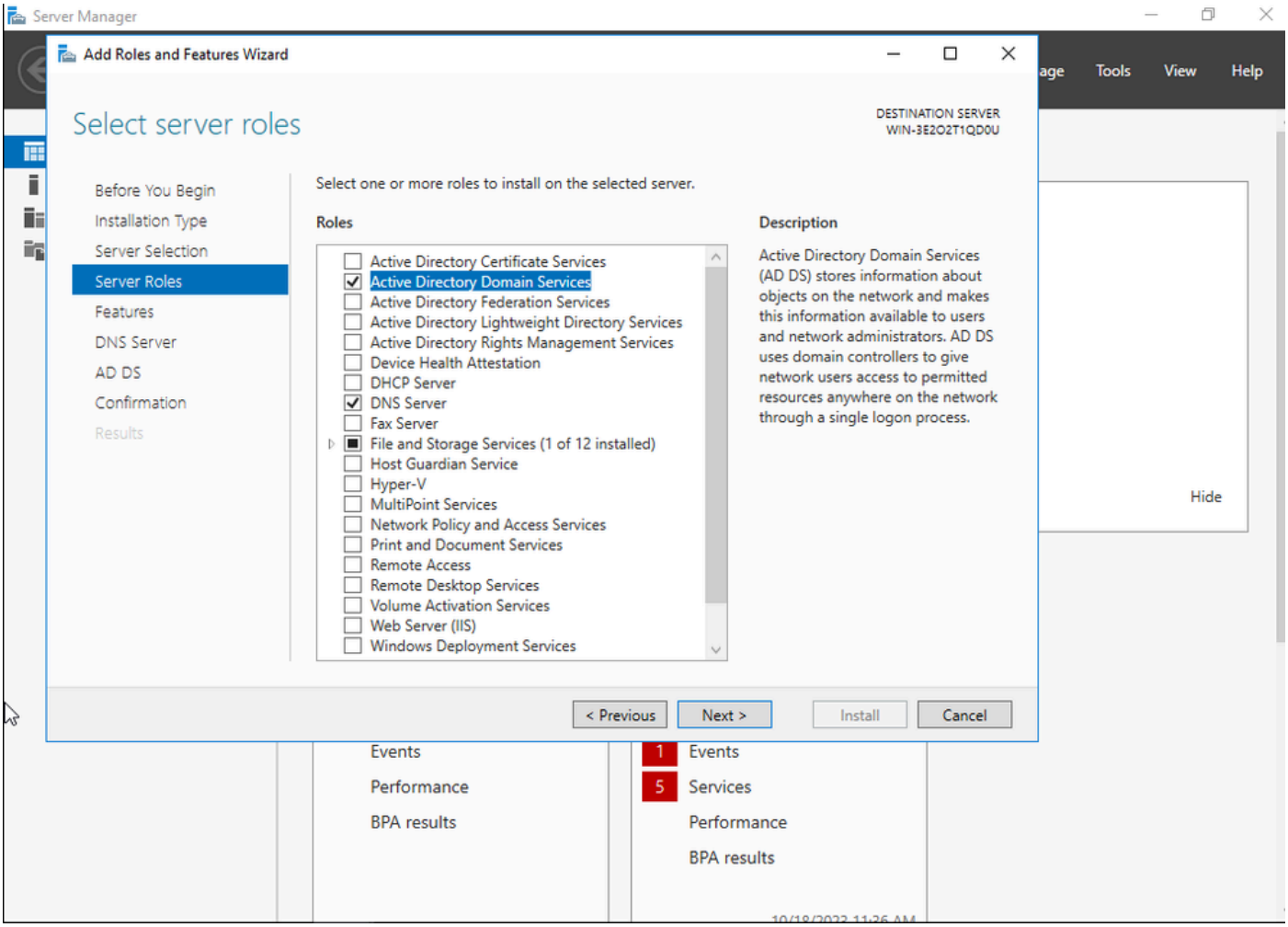
Windows Server 2016 SCEP CA

يغطي هذا المستند عملية تثبيت أساسية لنقطة الوصول SCEP ل Windows Server لأغراض معملية. يجب تكوين Windows CA الفعلي من فئة الإنتاج بشكل آمن ومناسب لعمليات التشغيل. يهدف هذا قسم أن يساعد أنت تختبر وه في المختبر فضلا عن أن يستلهم من الإعدادات المطلوبة أن يجعل هذا تشكيل يعمل. هذه هي الخطوات :

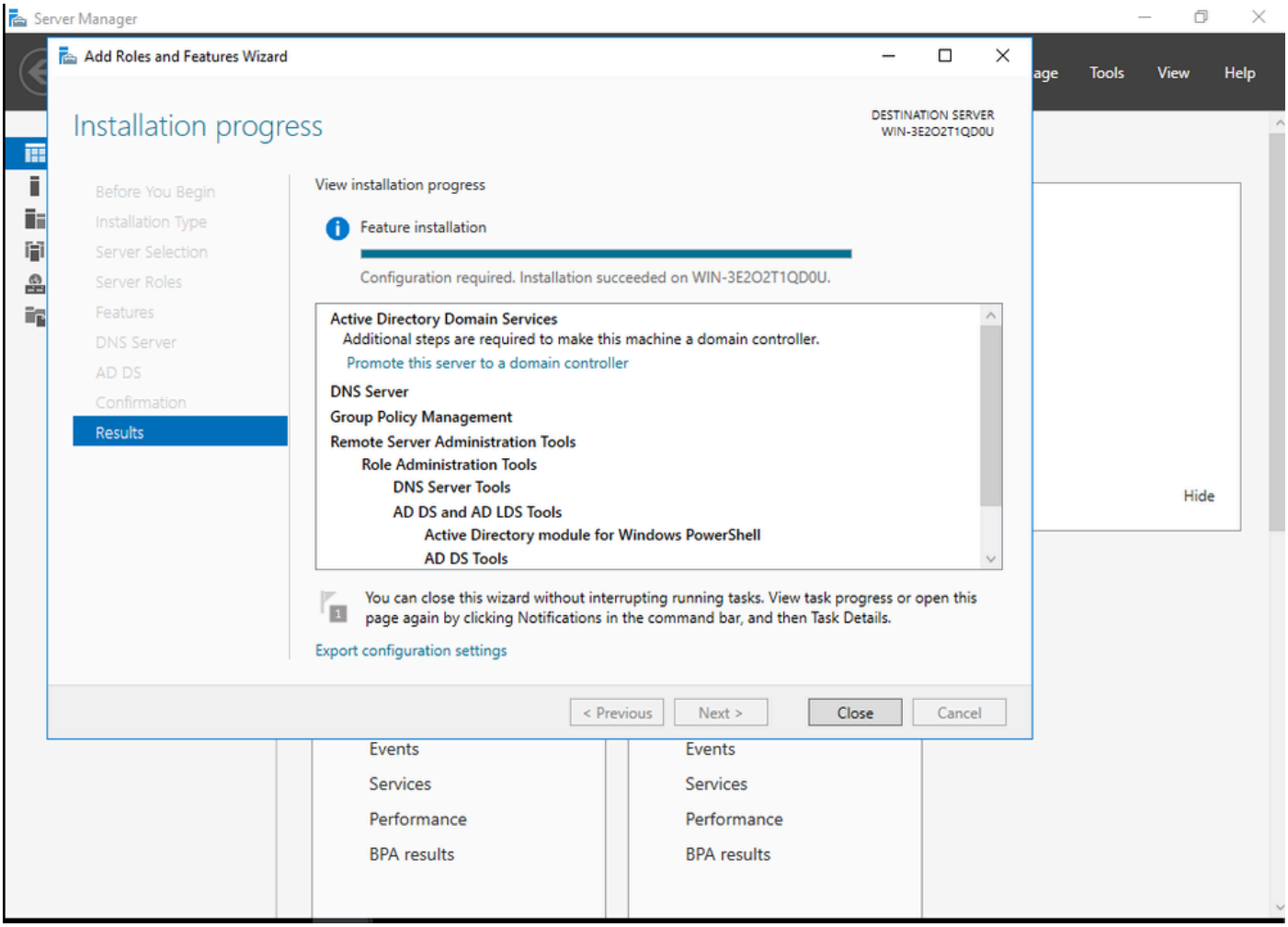
الخطوة 1.قم بتثبيت تجربة سطح مكتب Windows Server 2016 جديدة.

الخطوة 2. تأكد من تكوين الخادم باستخدام عنوان IP ثابت.

الخطوة 3. بدء تشغيل دور وخدمة جديدين، ابدأ بخدمات مجال خدمة Active Directory وخادم DNS.

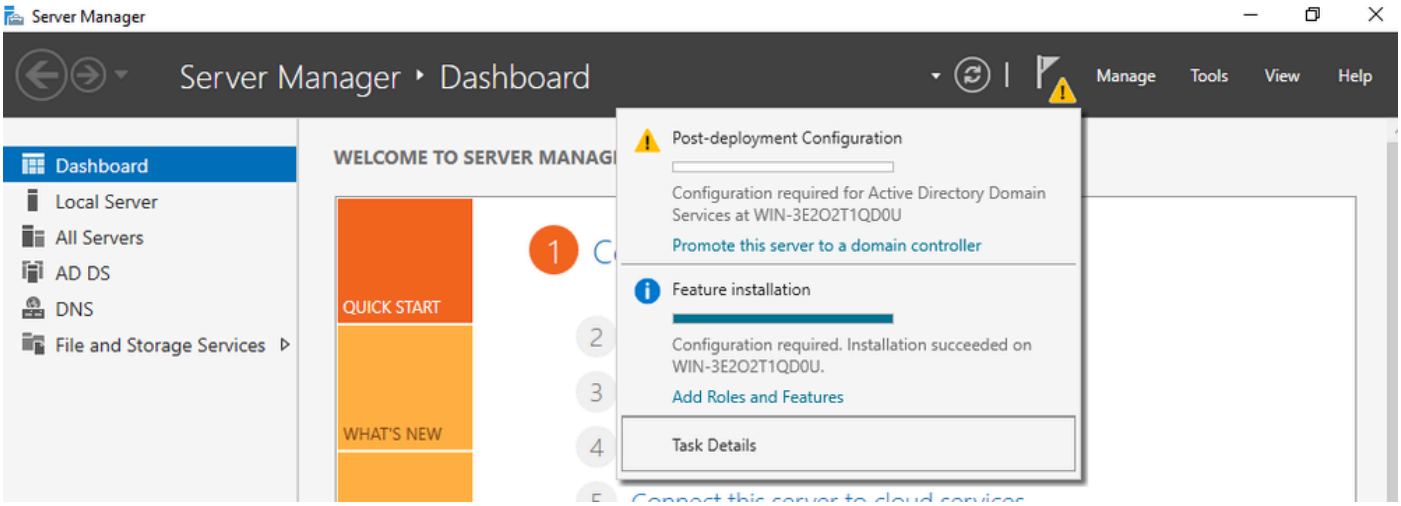


تثبيت Active Directory



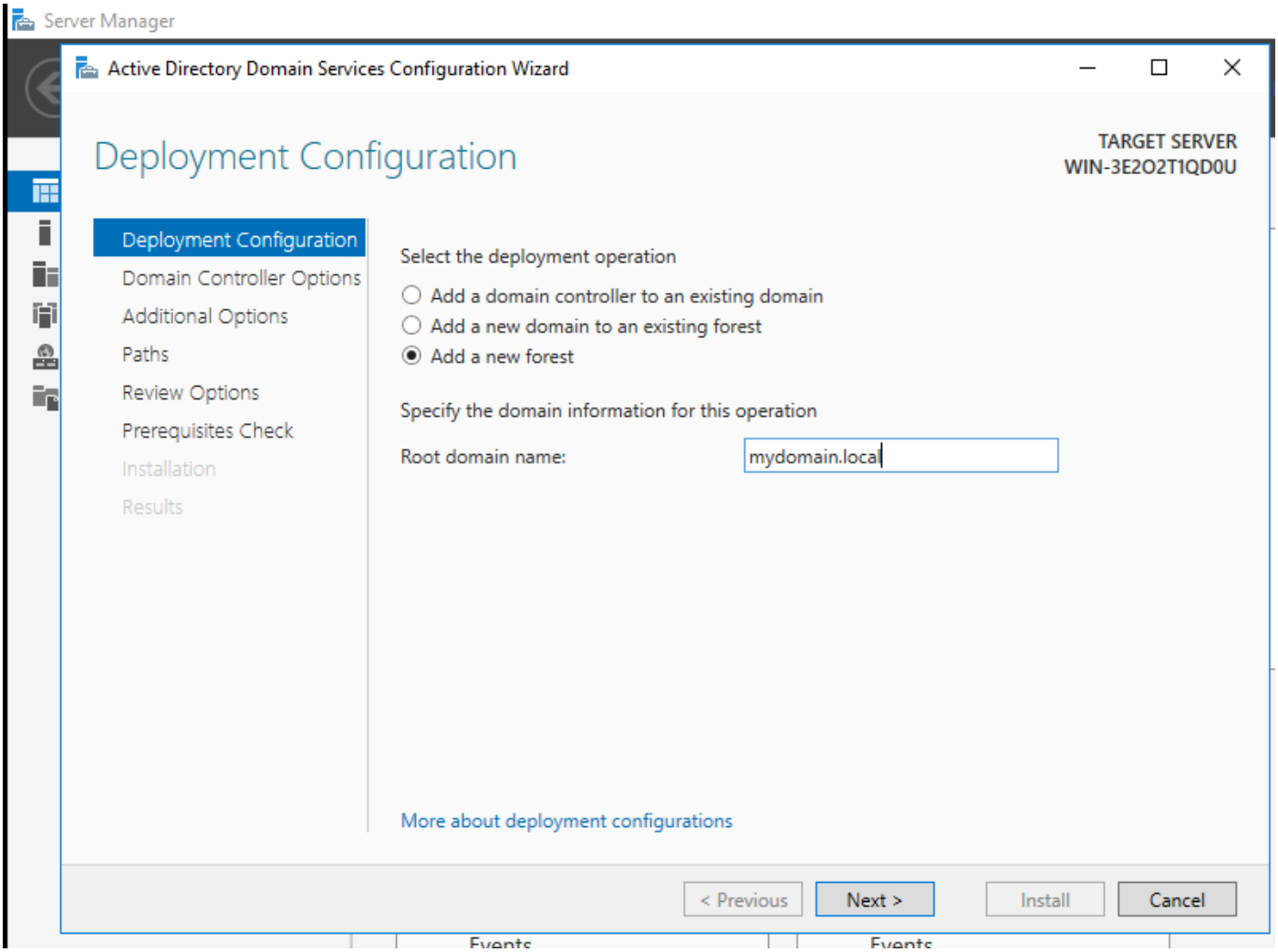
انتهاء تثبيت AD

الخطوة 4. بمجرد الانتهاء، انقر فوق لوحة المعلومات الخاصة بترقية هذا الخادم إلى وحدة تحكم بالمجال.



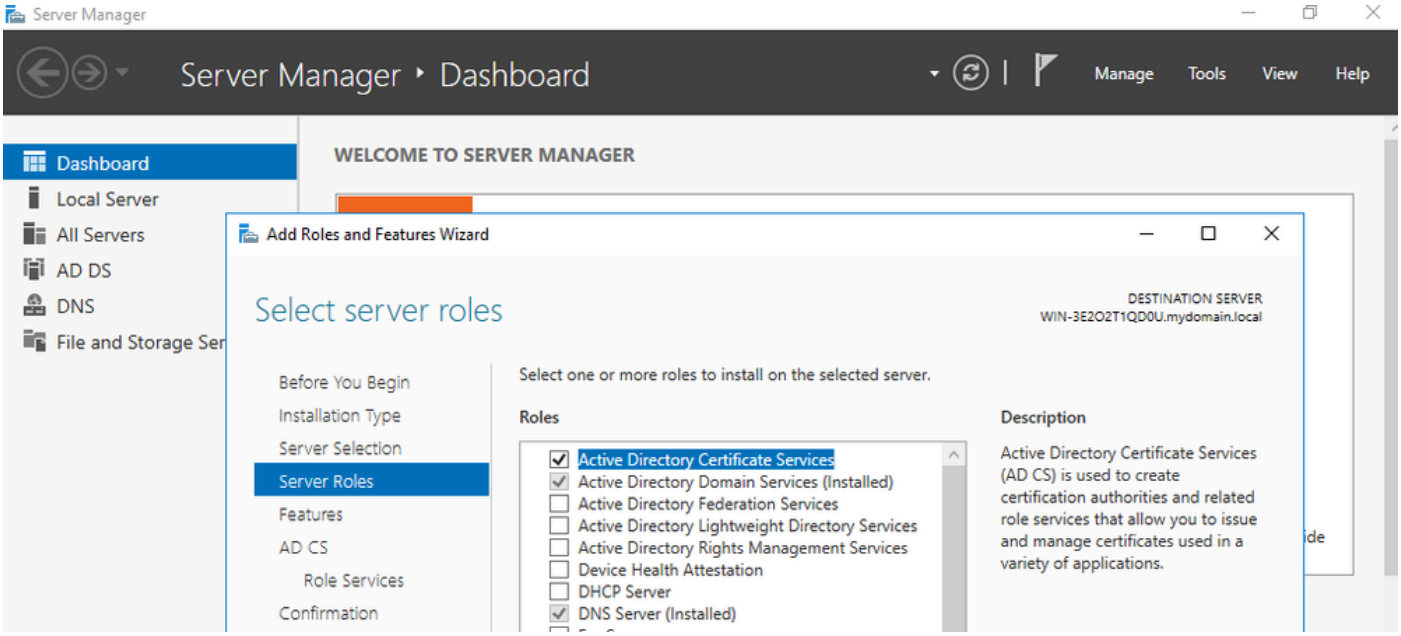
تكوين خدمات AD

الخطوة 5. قم بإنشاء غابة جديدة واختر اسم مجال.

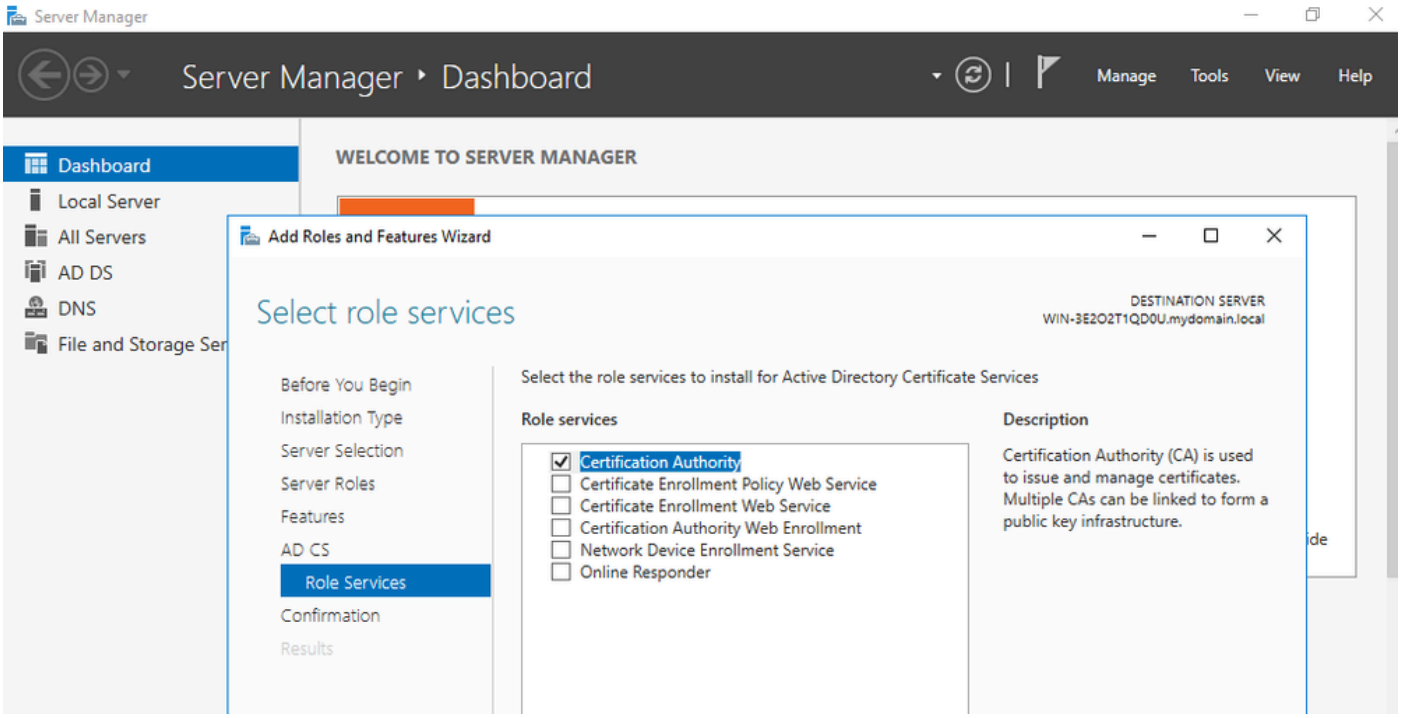


اختيار اسم غابة

الخطوة 6. أضف دور خدمات الشهادات إلى الخادم:

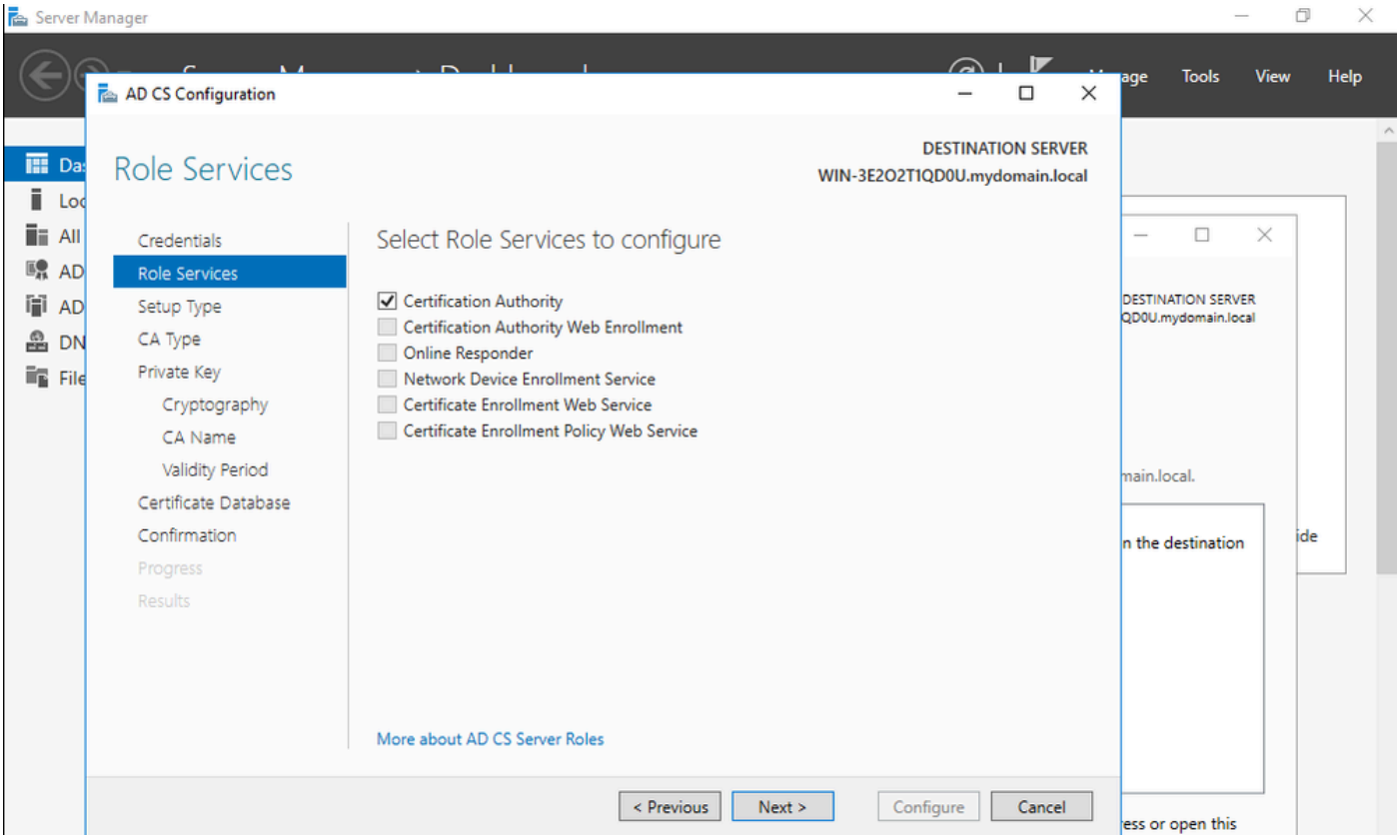


إضافة خدمات شهادات

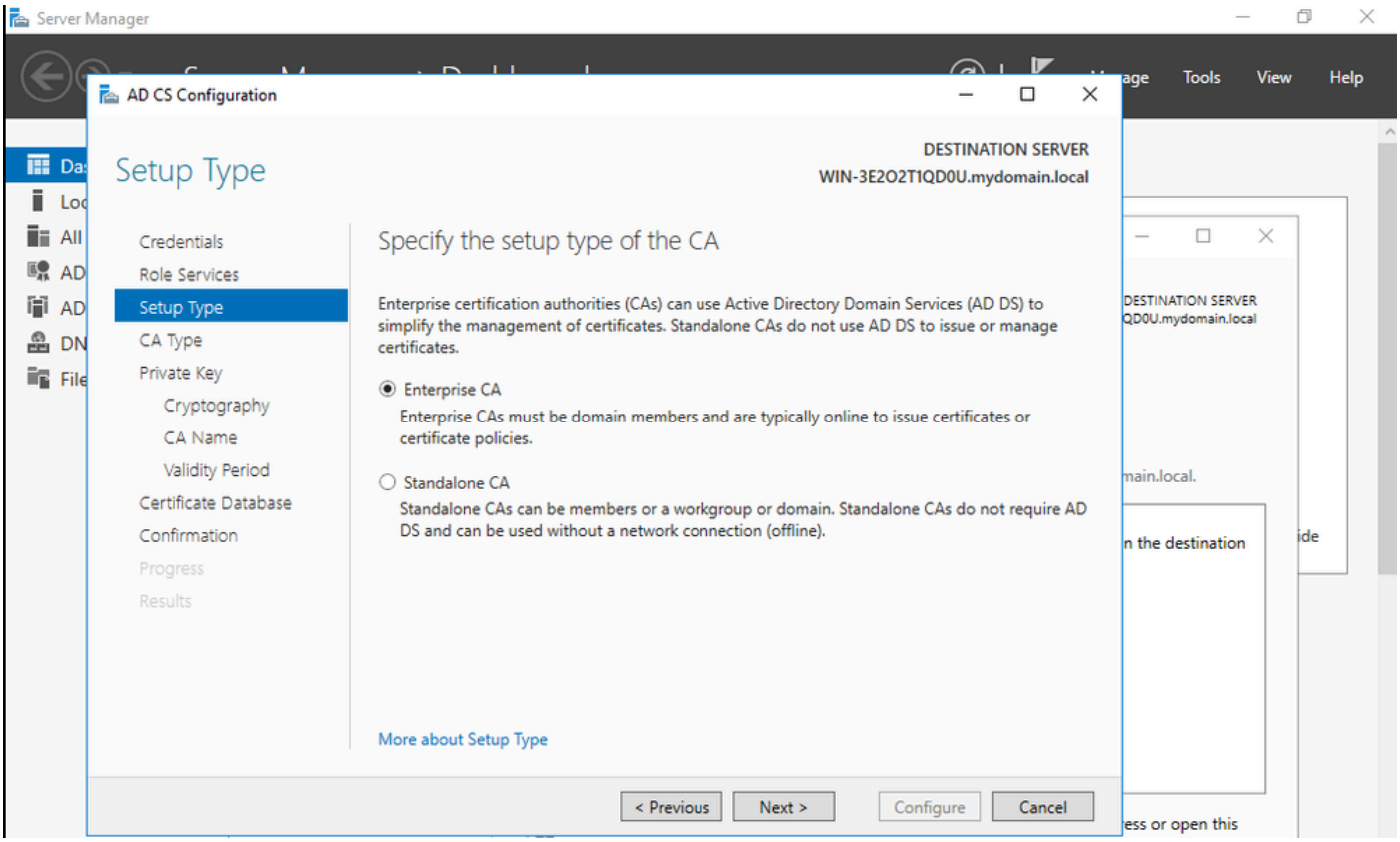


إضافة المرجع المصدق فقط

الخطوة 7. بمجرد الانتهاء، قم بتكوين المرجع المصدق الخاص بك.

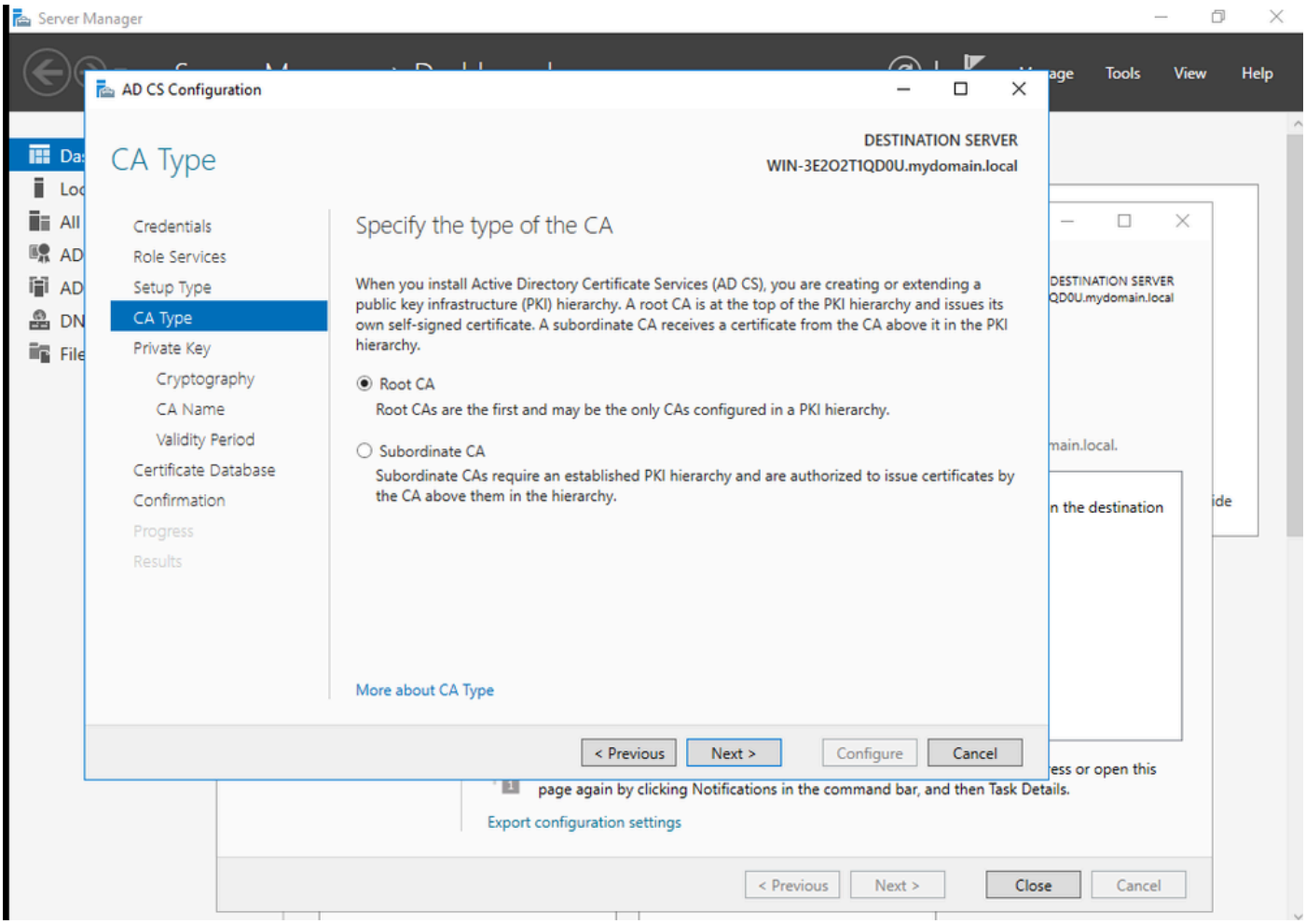


الخطوة 8. أختر Enterprise CA.



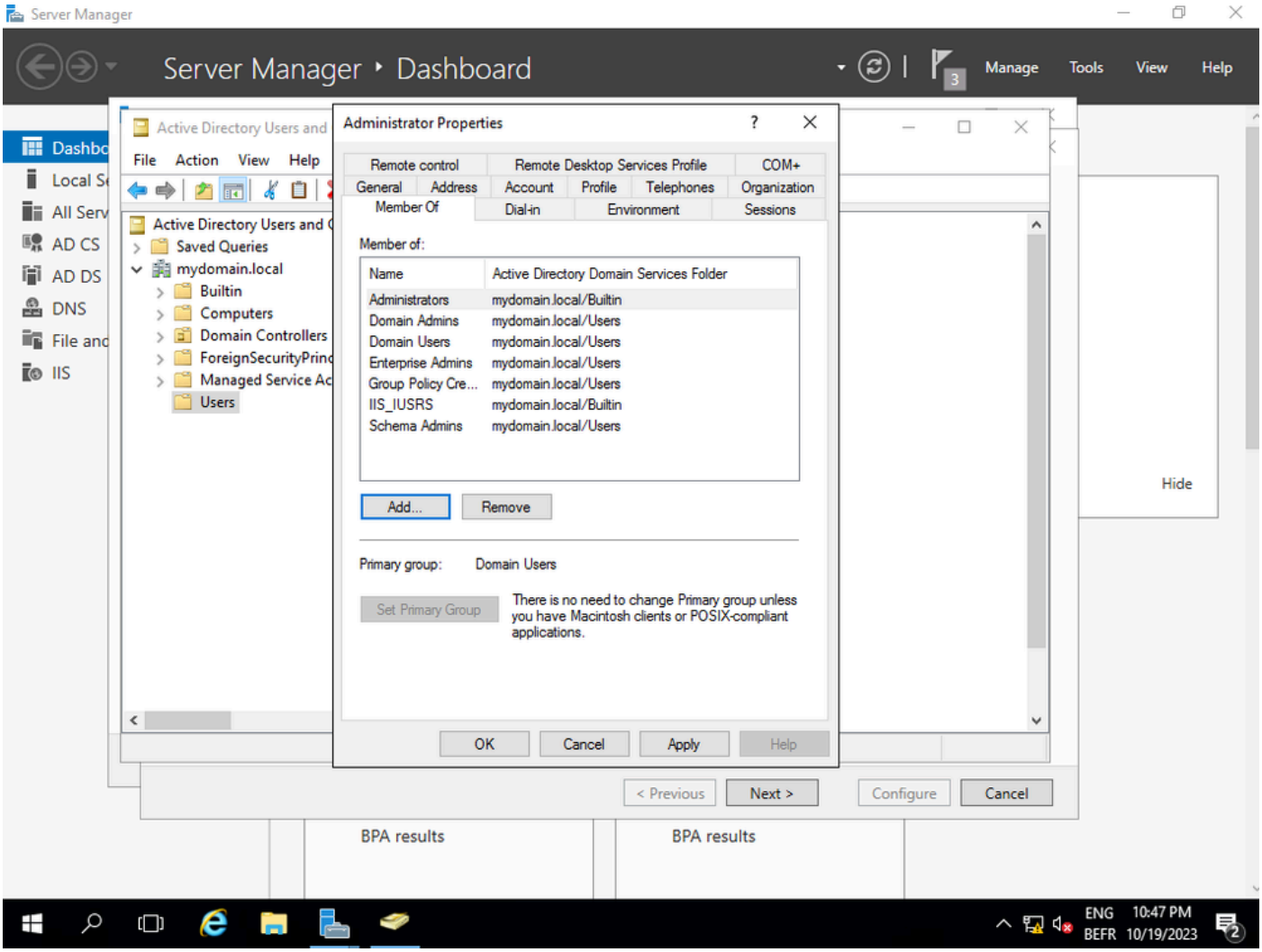
مرجع مصدق للمؤسسة

الخطوة 9. أجعلِ المرجع المصدق الجذر. منذ Cisco IOS XE 17.6، يتم دعم CAs التابعة لـ LSC.



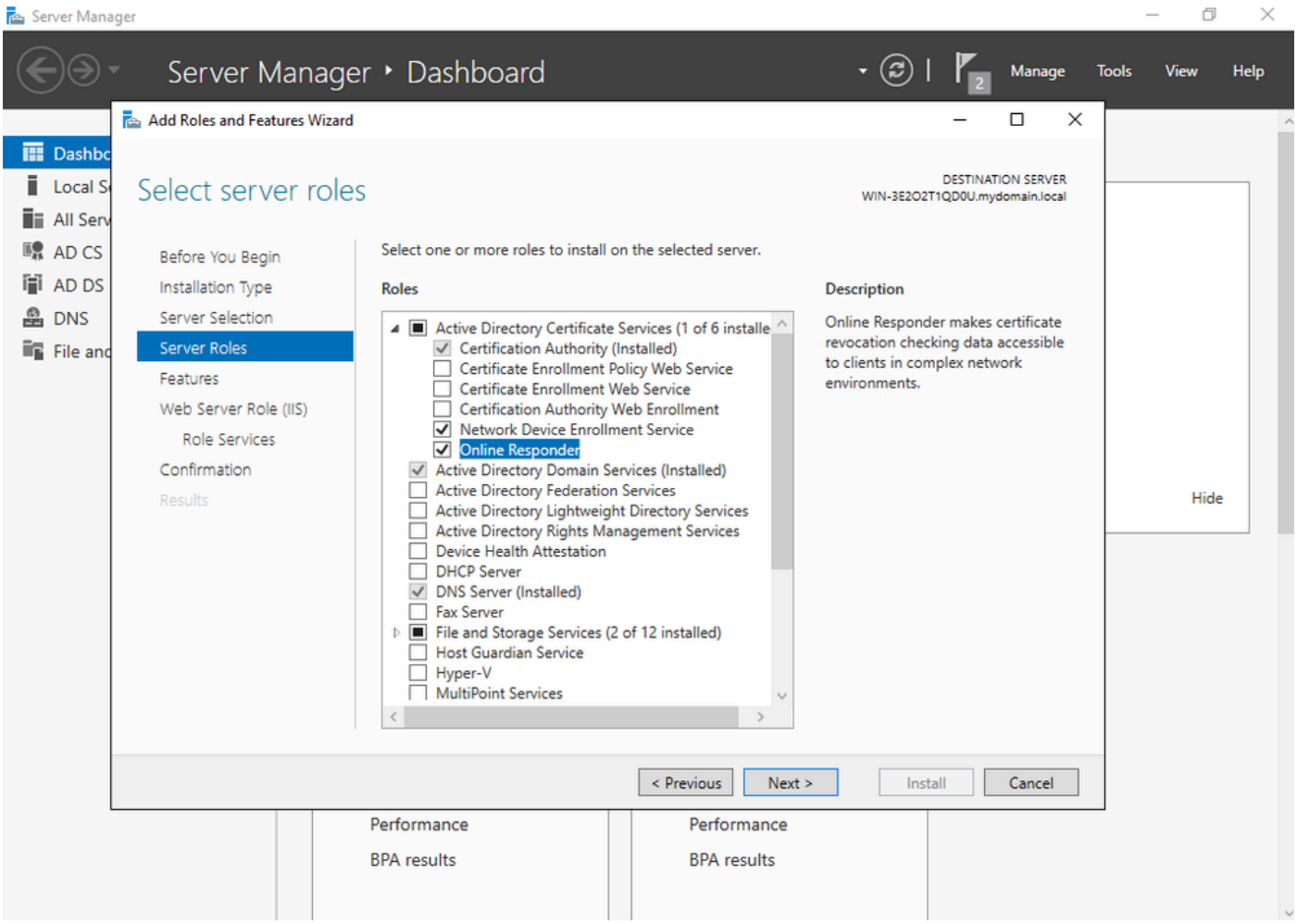
اختيار مرجع مصدق جذري

من المهم أن يكون لديك الحساب الذي تستخدمه لكي يكون المرجع المصدق جزءا من مجموعة IIS_IUSRS. في هذا المثال، يمكنك إستخدام حساب Administrator والانتقال إلى القائمة Active Directory Users and Computers لإضافة المستخدمين المسؤولين إلى مجموعة IIS_IUSRS.



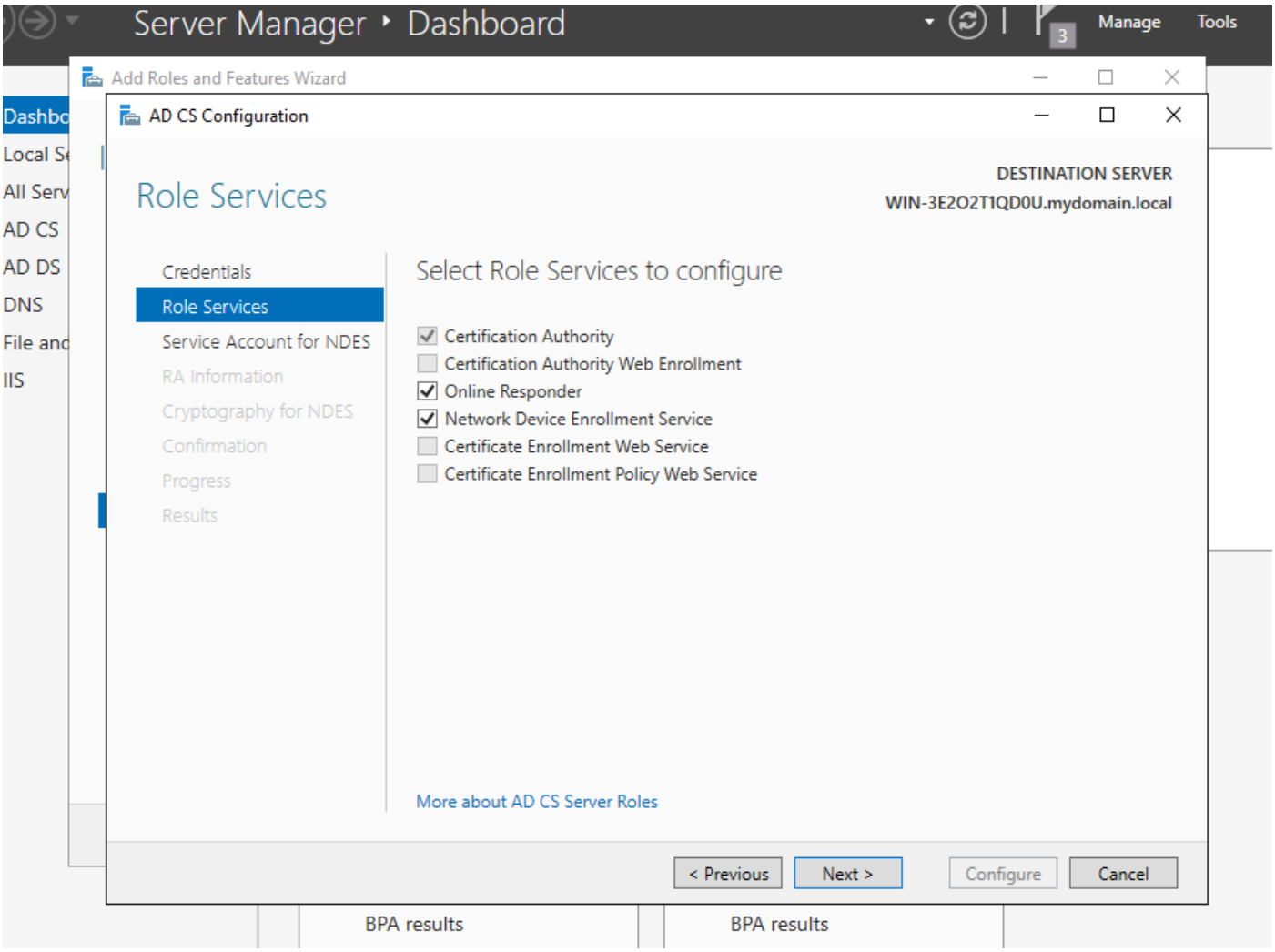
إضافة حساب المستخدم الخاص بك إلى مجموعة IIS_USER

الخطوة 10. بمجرد أن يكون لديك مستخدم في مجموعة IIS الصحيحة، قم بإضافة الأدوار والخدمات. ثم أضف خدمات Online Responder و NDES إلى مرجع التصديق الخاص بك.



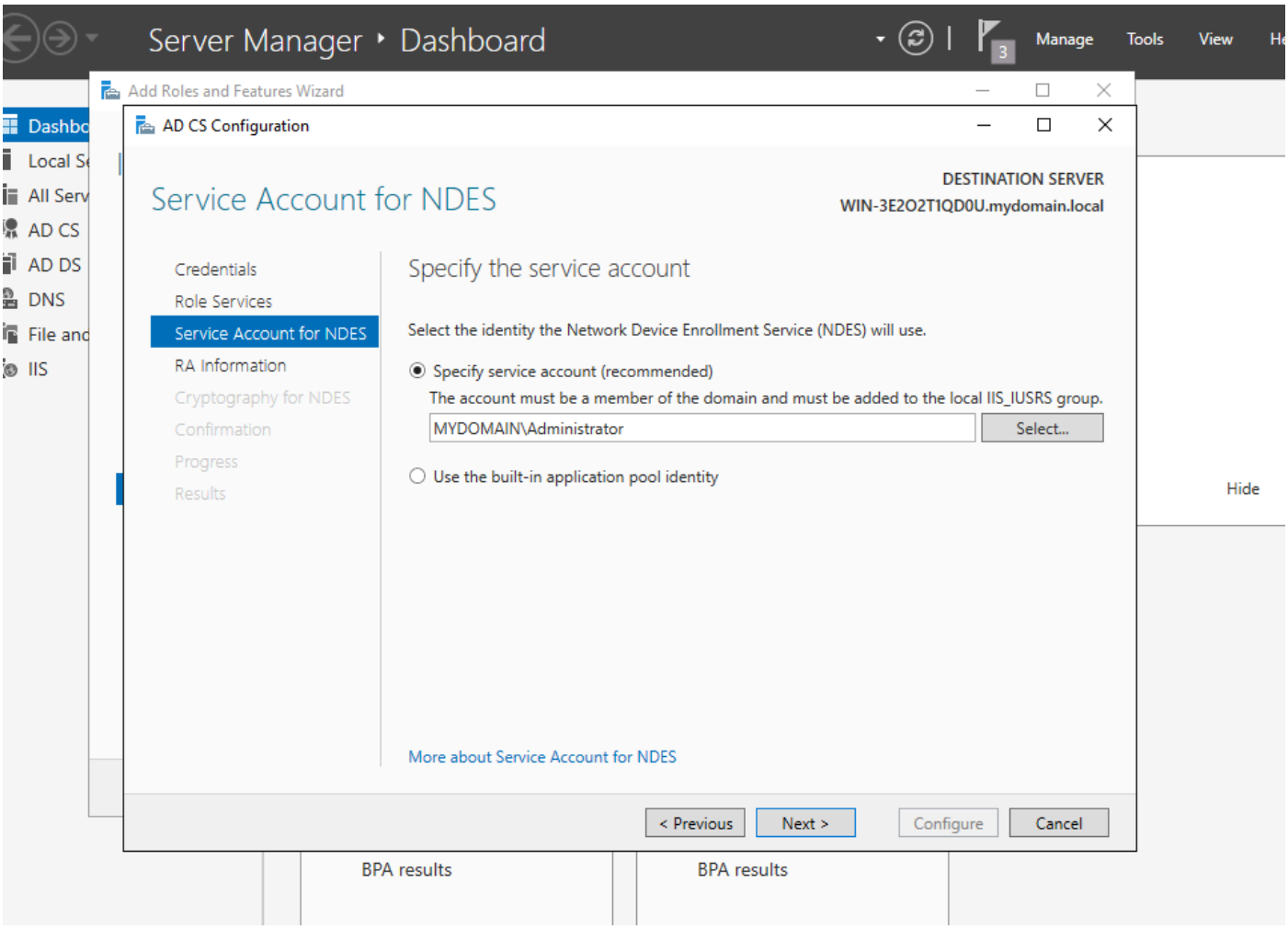
تثبيت NDES وخدمات المستجيب عبر الإنترنت

الخطوة 11. بمجرد القيام بذلك، قم بتكوين هذه الخدمات.



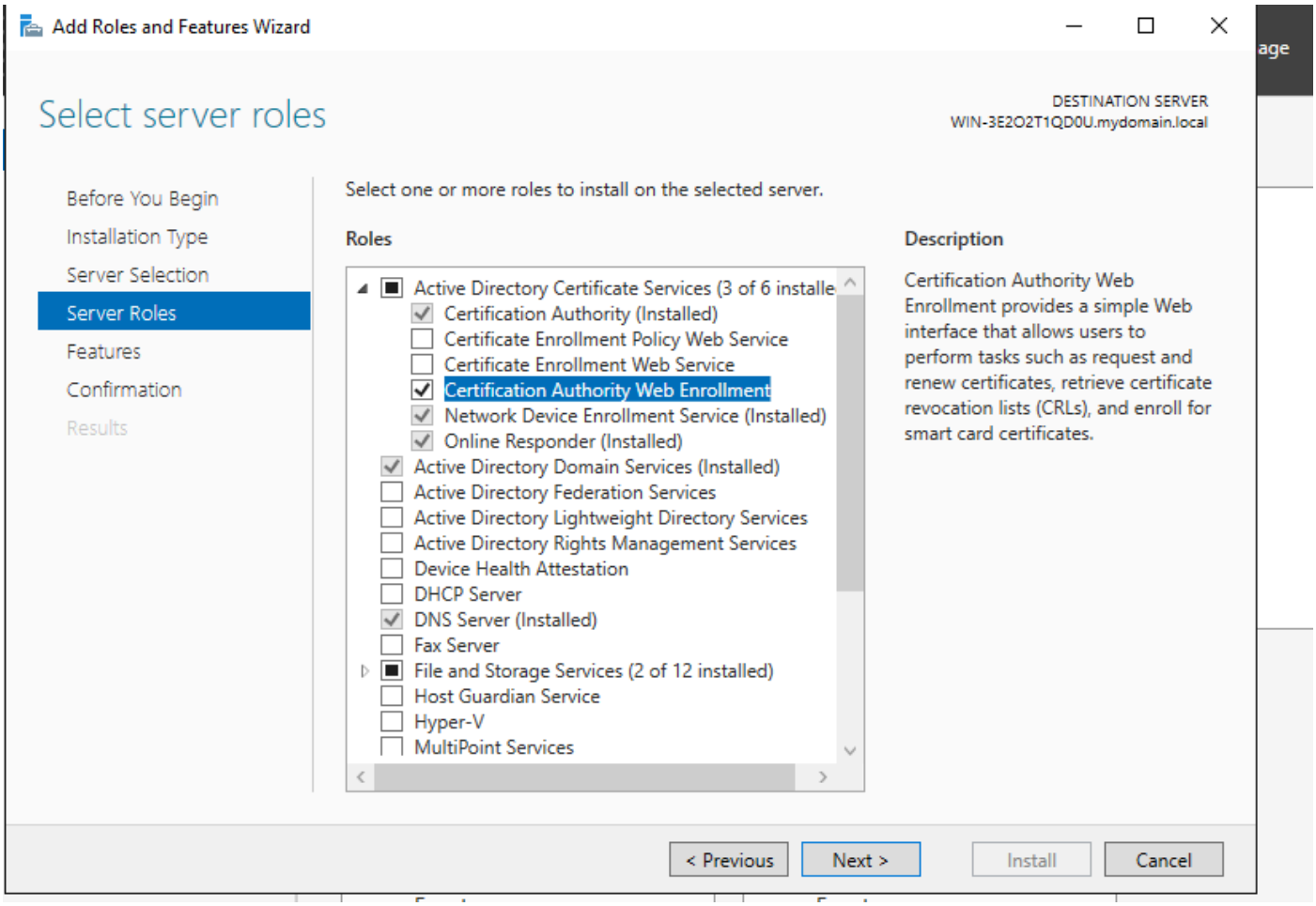
تثبيت خدمة Online Responsder و NDES

الخطوة 12. تتم مطالبتك باختيار حساب خدمة. هذا هو الحساب الذي أضفته من قبل إلى مجموعة IIS_IUSRS.

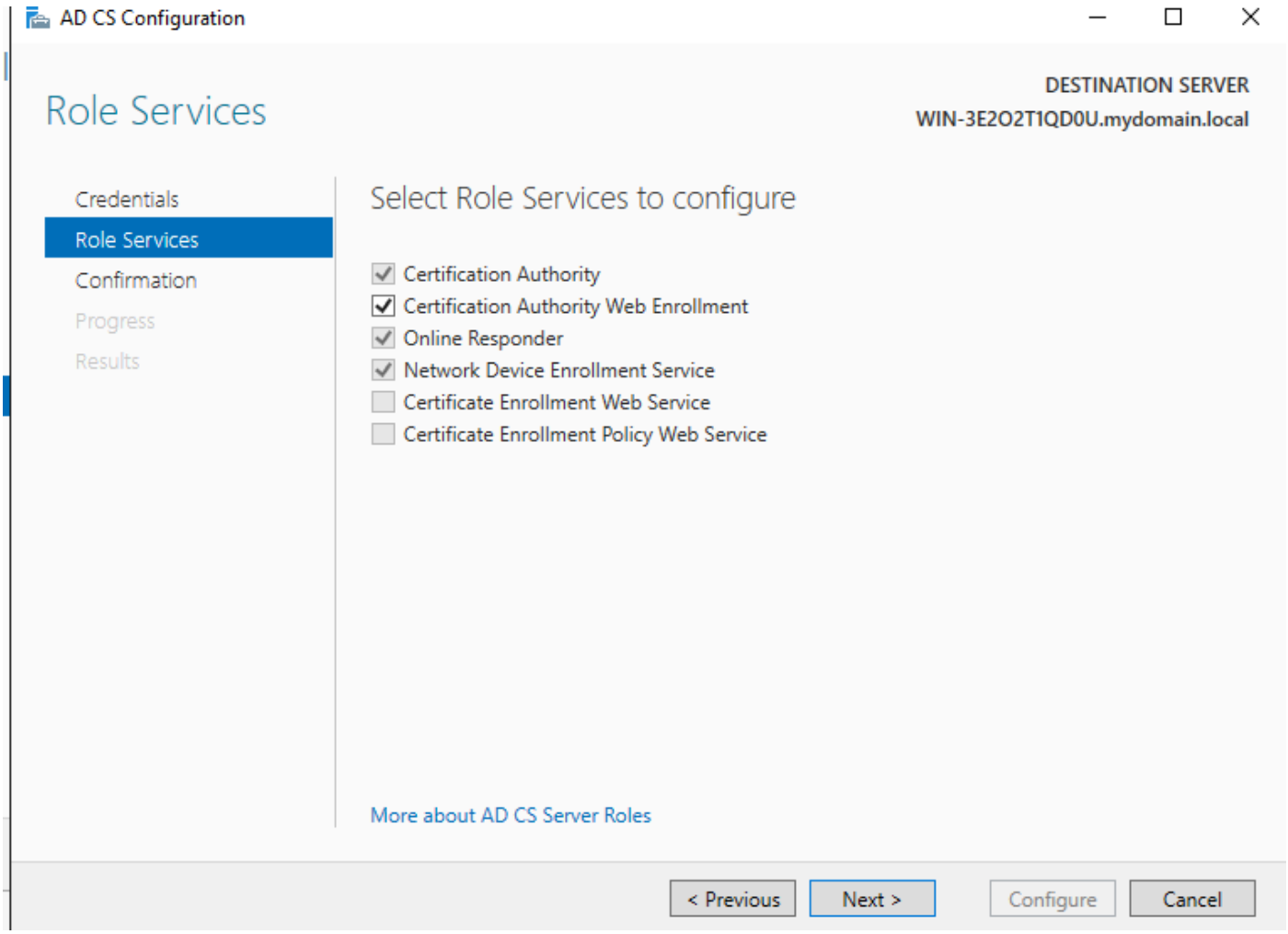


انتقاء المستخدم الذي أضفته إلى مجموعة IIS

الخطوة 13.اذه يكفي لعمليات SCEP، ولكن لتحقيق مصادقة 802.1X، يلزمك أيضا تثبيت شهادة على خادم RADIUS. لذلك، قم بتثبيت خدمة تسجيل الويب وتكوينها بسهولة حتى تتمكن من نسخ ولصق طلب شهادة ISE على خادم Windows.

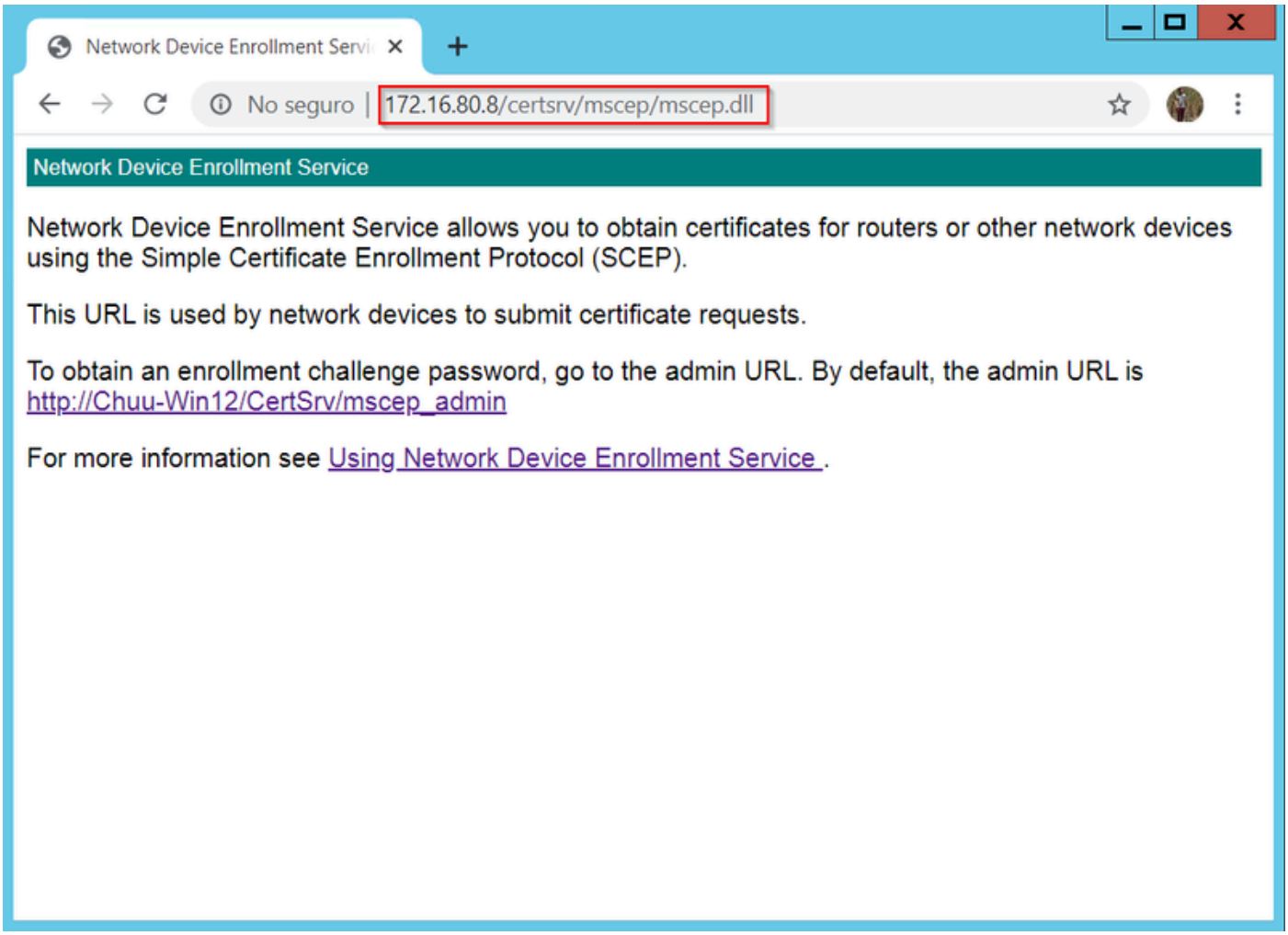


تثبيت خدمة تسجيل الويب



تكوين خدمة تسجيل الويب

الخطوة 14. يمكنك التحقق من تشغيل خدمة SCEP بشكل صحيح من خلال زيارة http://<serverify>/certsrv/mscep/mscep.dll :



التحقق من مدخل SCEP

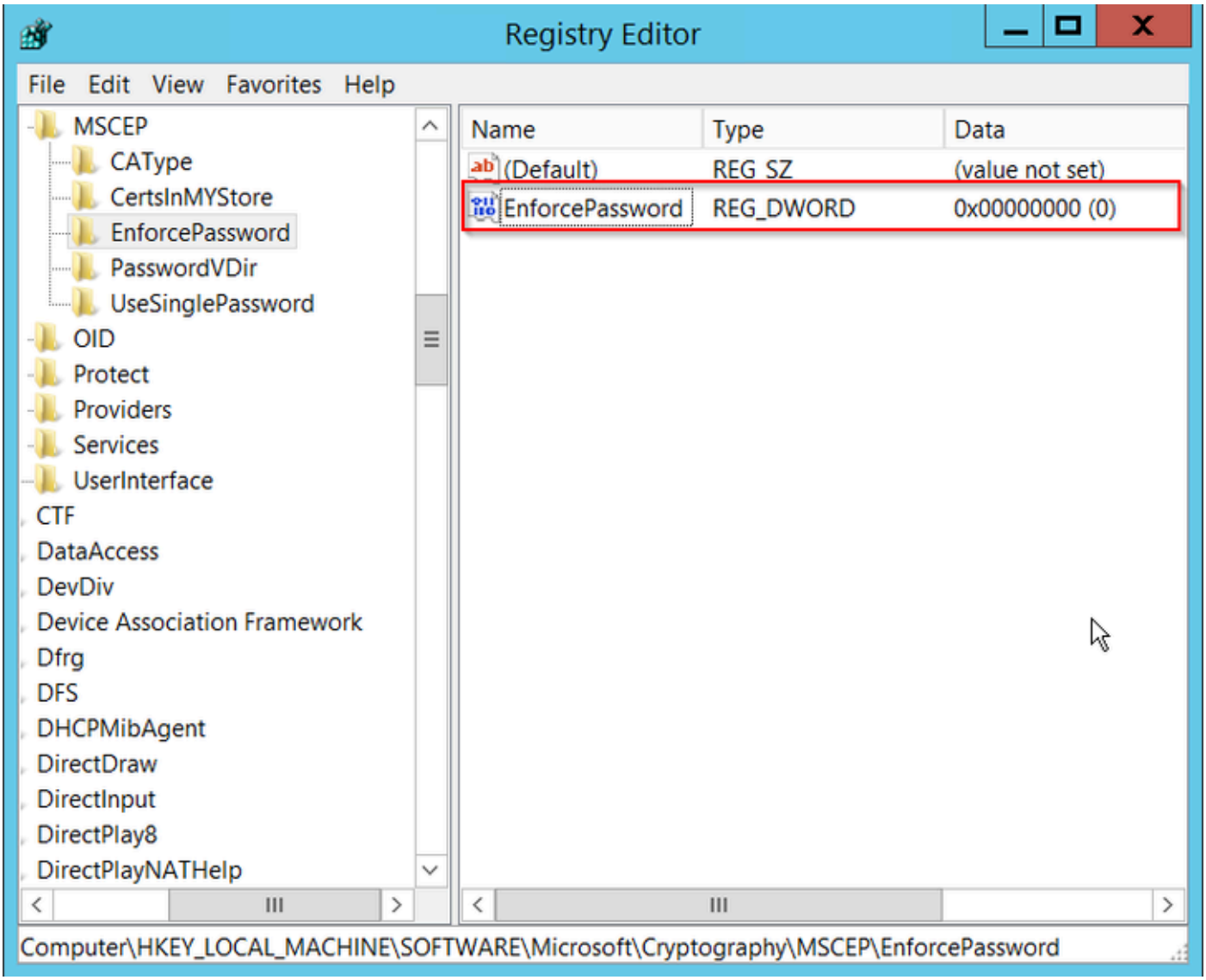
الخطوة 15.

وبشكل افتراضي، أستخدم خادم Windows كلمة مرور "تحدي ديناميكي" لمصادقة طلبات العميل ونقطة النهاية قبل التسجيل داخل Microsoft SCEP (MSCEP). يتطلب هذا حساب مسؤول للتصفح إلى واجهة المستخدم الرسومية (GUI) للويب لإنشاء كلمة مرور حسب الطلب لكل طلب (يجب تضمين كلمة المرور ضمن الطلب).يتعذر على وحدة التحكم تضمين كلمة المرور هذه ضمن الطلبات التي ترسلها إلى الخادم. لإزالة هذه الميزة، يلزم تعديل مفتاح التسجيل الموجود على خادم NDES:

افتح "محرر التسجيل"، ابحث عن Regedit ضمن القائمة Start.

انتقل إلى الكمبيوتر > HKEY_LOCAL_MACHINE > برنامج > Microsoft > تشفير > MSCEP > EnforcementPassword

قم بتغيير قيمة EnforcementPassword إلى 0. إذا كانت 0 بالفعل، فاتركها كما هي.



تعيين قيمة كلمة فرض التحدي

تكوين قالب الشهادة وتسجيلها

يمكن إستخدام الشهادات والمفاتيح المقترنة بها في سيناريوهات متعددة لأغراض مختلفة تم تحديدها بواسطة نهج التطبيق داخل خادم المرجع المصدق. يتم تخزين نهج التطبيق في حقل "إستخدام المفاتح الموسع (EKU)" للشهادة. يتم تحليل هذا الحقل بواسطة المصدق للتحقق من إستخدامه من قبل العميل للغرض المقصود منه. للتأكد من دمج سياسة التطبيق المناسبة لشهادات WLC و AP، قم بإنشاء قالب الشهادة المناسب وقم بتعيينه إلى سجل NDES:

الخطوة 1. انتقل إلى ابدأ > أدوات إدارية > المرجع المصدق.

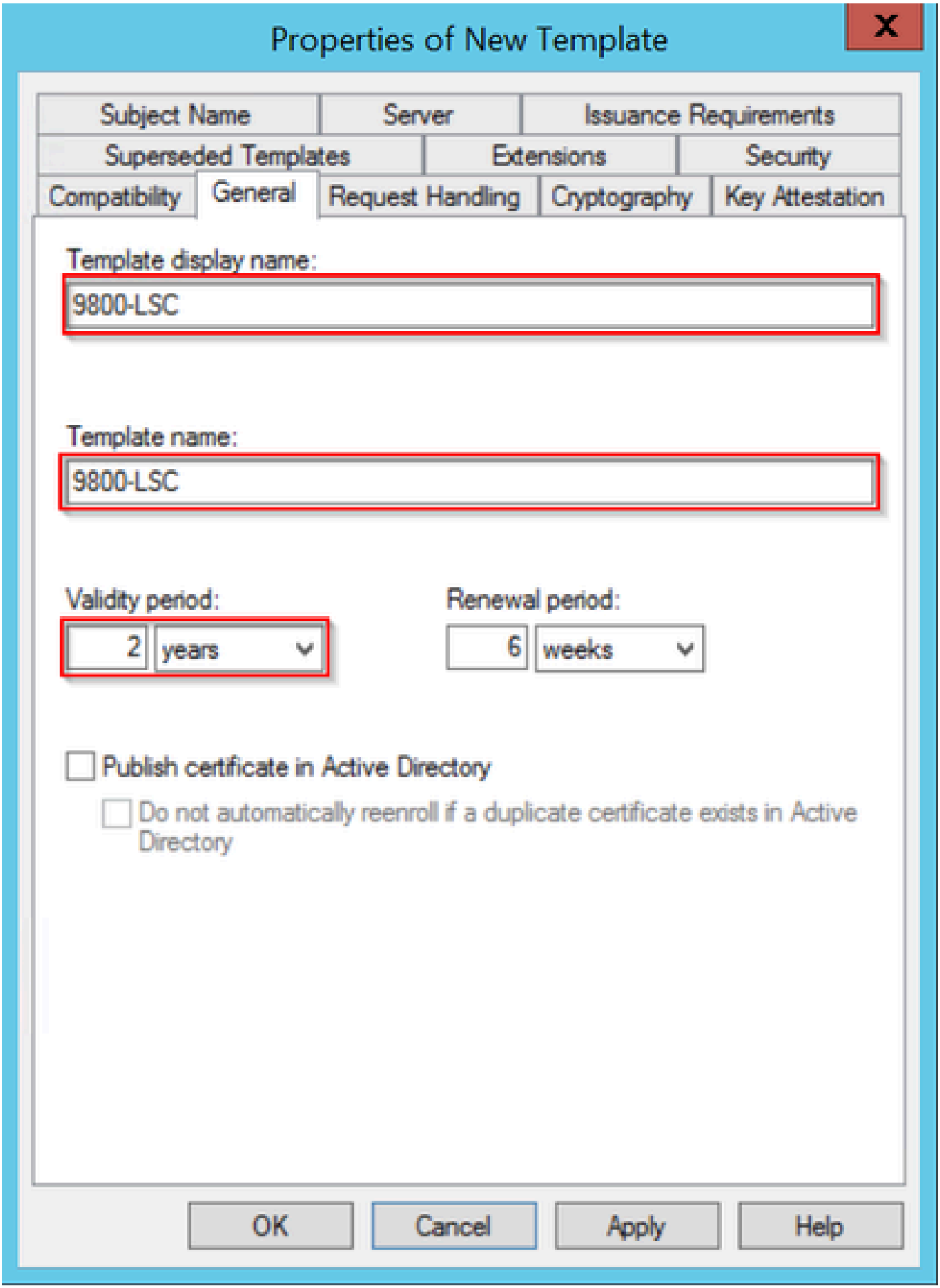
الخطوة 2. قم بتوسيع شجرة مجلد خادم المرجع المصدق، انقر بزر الماوس الأيمن فوق مجلدات قوالب الترخيص وحدد إدارة.

الخطوة 3. انقر بزر الماوس الأيمن فوق قالب شهادة المستخدمين، ثم حدد تكرار القالب في قائمة السياق.

الخطوة 4. انتقل إلى علامة التبويب عام، وقم بتغيير اسم القالب وفترة الصلاحية حسب

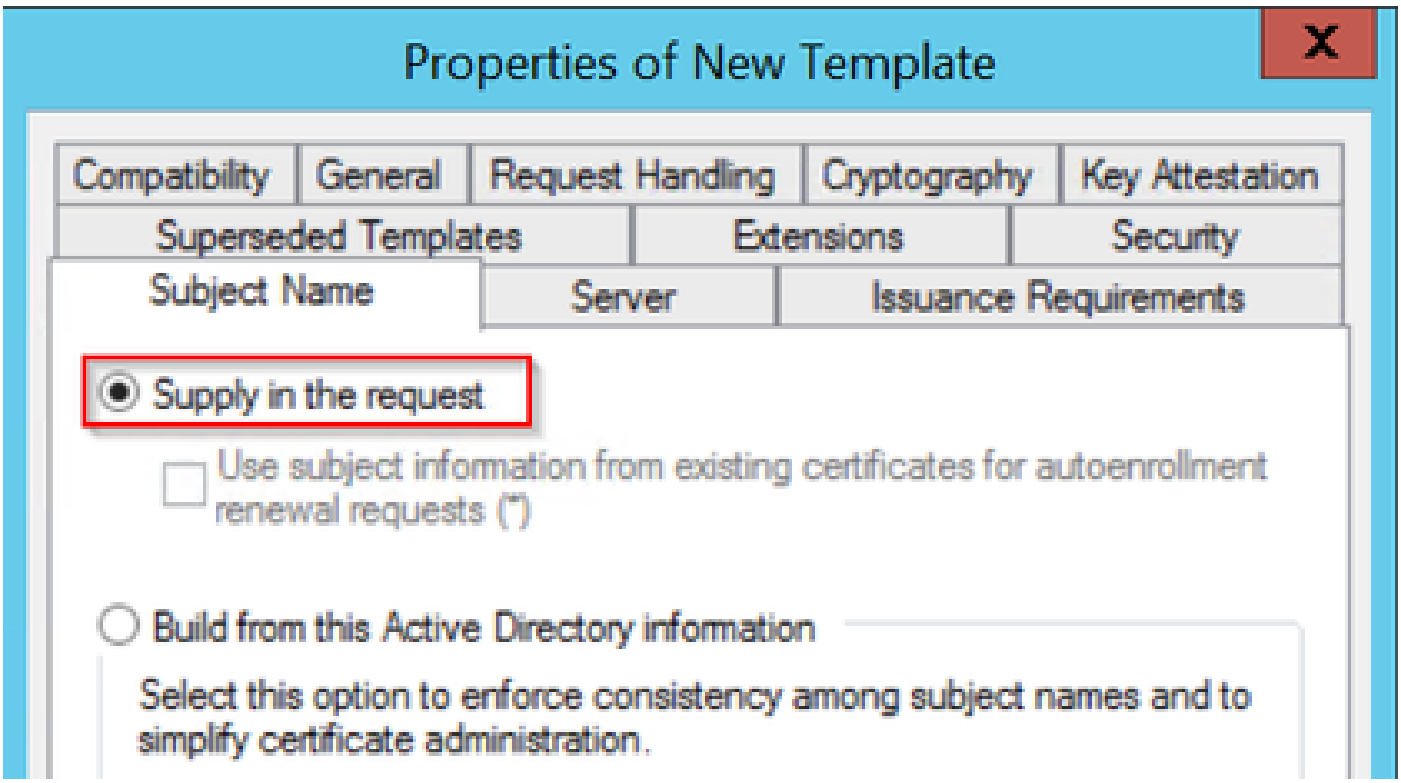
الرغبة، أترك كل الخيارات الأخرى بدون تحديد.

⚠ تحذير: عند تعديل فترة الصلاحية، تأكد من أنها ليست أكبر من صلاحية شهادة جذر المرجع المصدق.



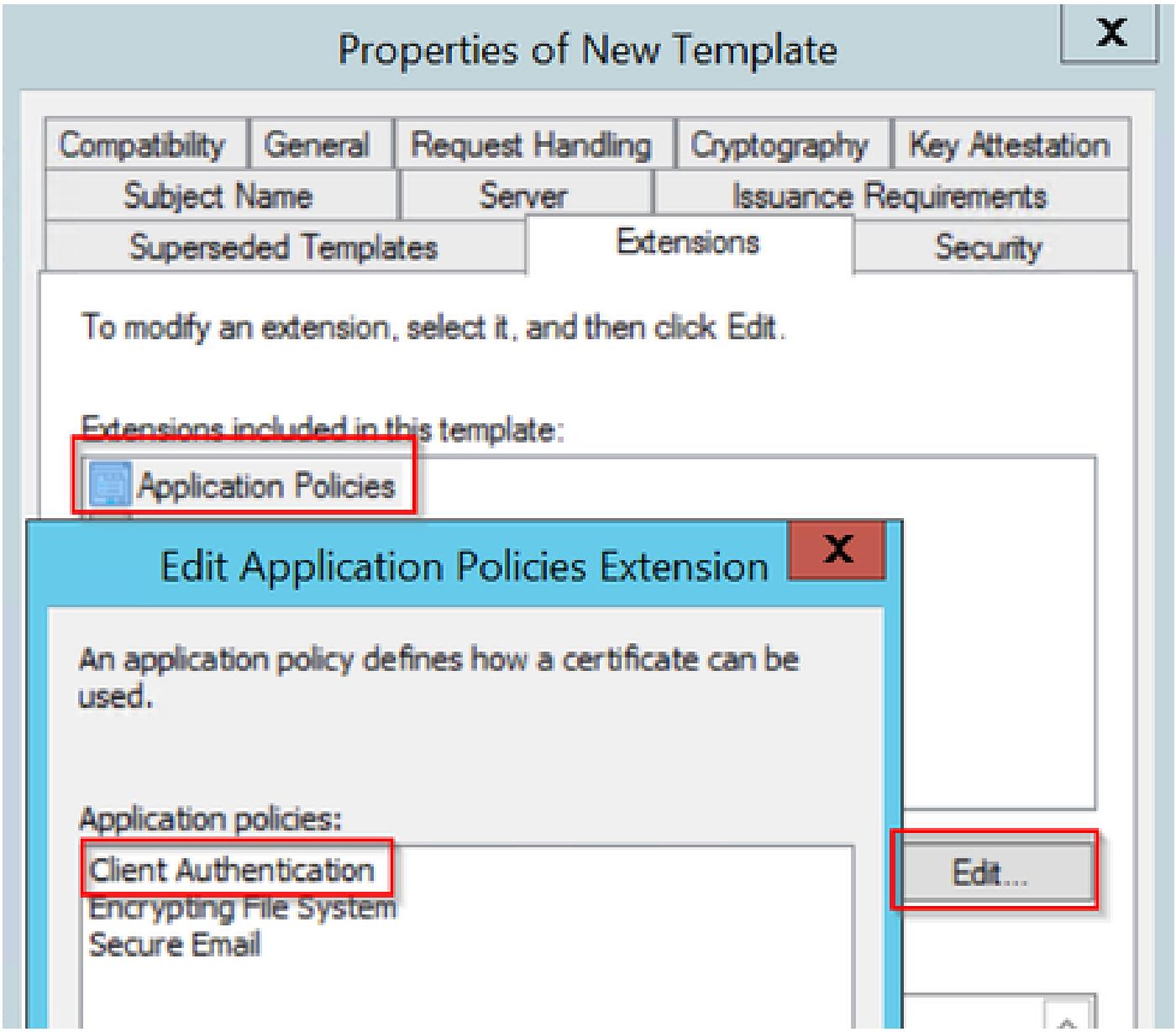
تكوين قالب الشهادة

الخطوة 5. انتقل إلى علامة التبويب اسم الموضوع، وتأكد من تحديد التوريد في الطلب. يبدو أن منبثق يشير إلى أن المستخدمين لا يحتاجون لموافقة المسؤول للحصول على توقيعهم على الشهادة، حدد موافق.



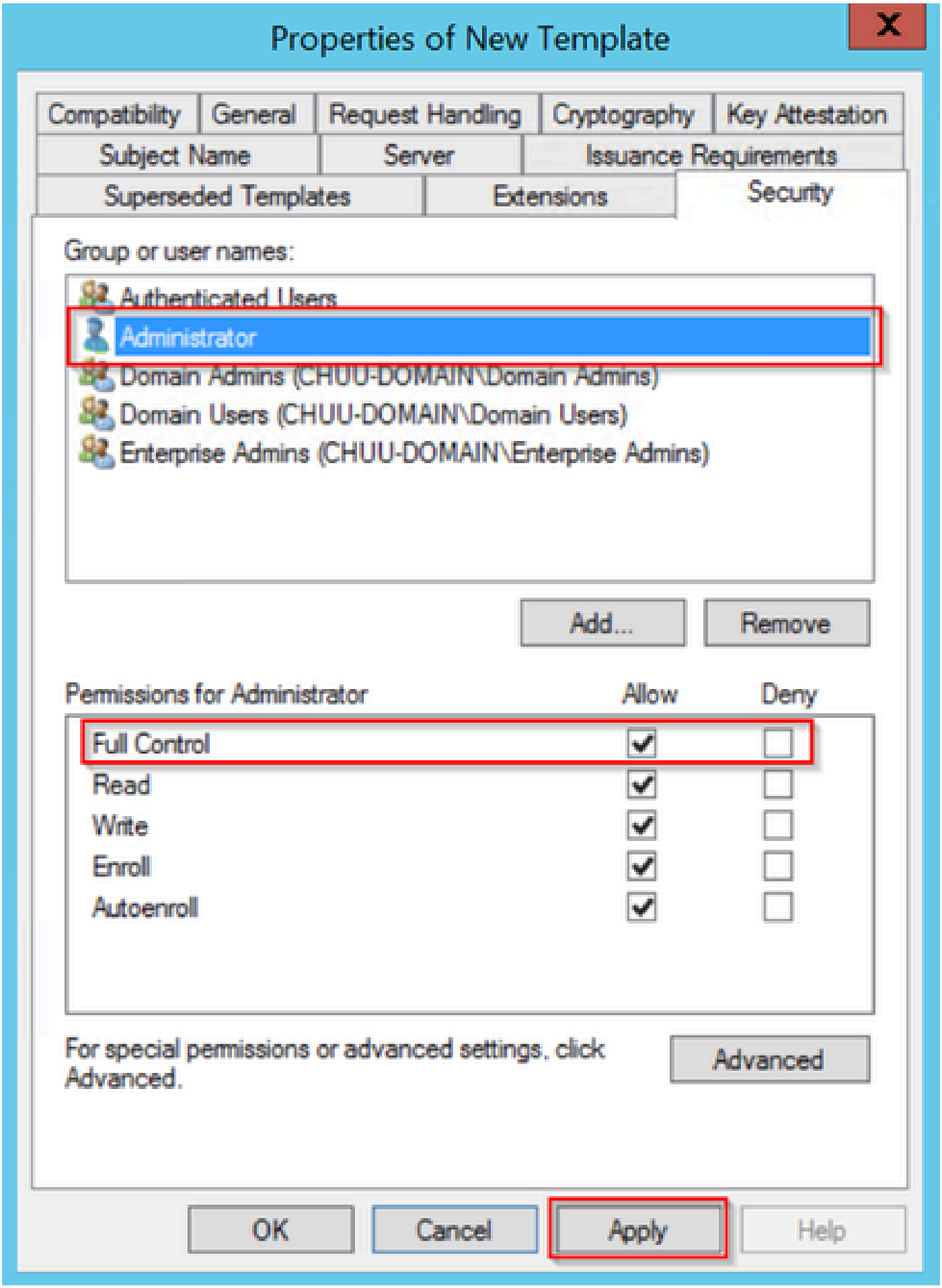
التوريد في الطلب

الخطوة 6. انتقل إلى علامة التبويب الملحقات، ثم حدد خيار نهج التطبيقات وحدد الزر تحرير.... تأكد من أن مصادقة العميل موجودة في نافذة سياسات التطبيق، وإلا، حدد إضافة وأضفه.



التحقق من الملحقات

الخطوة 7. انتقل إلى عالمة التبويب أمان، وتأكد من أن حساب الخدمة المحدد في الخطوة 6 من تمكين خدمات SCEP في Windows Server لديه أذونات التحكم الكامل الخاصة بالقالب، ثم حدد تطبيق وموافق.

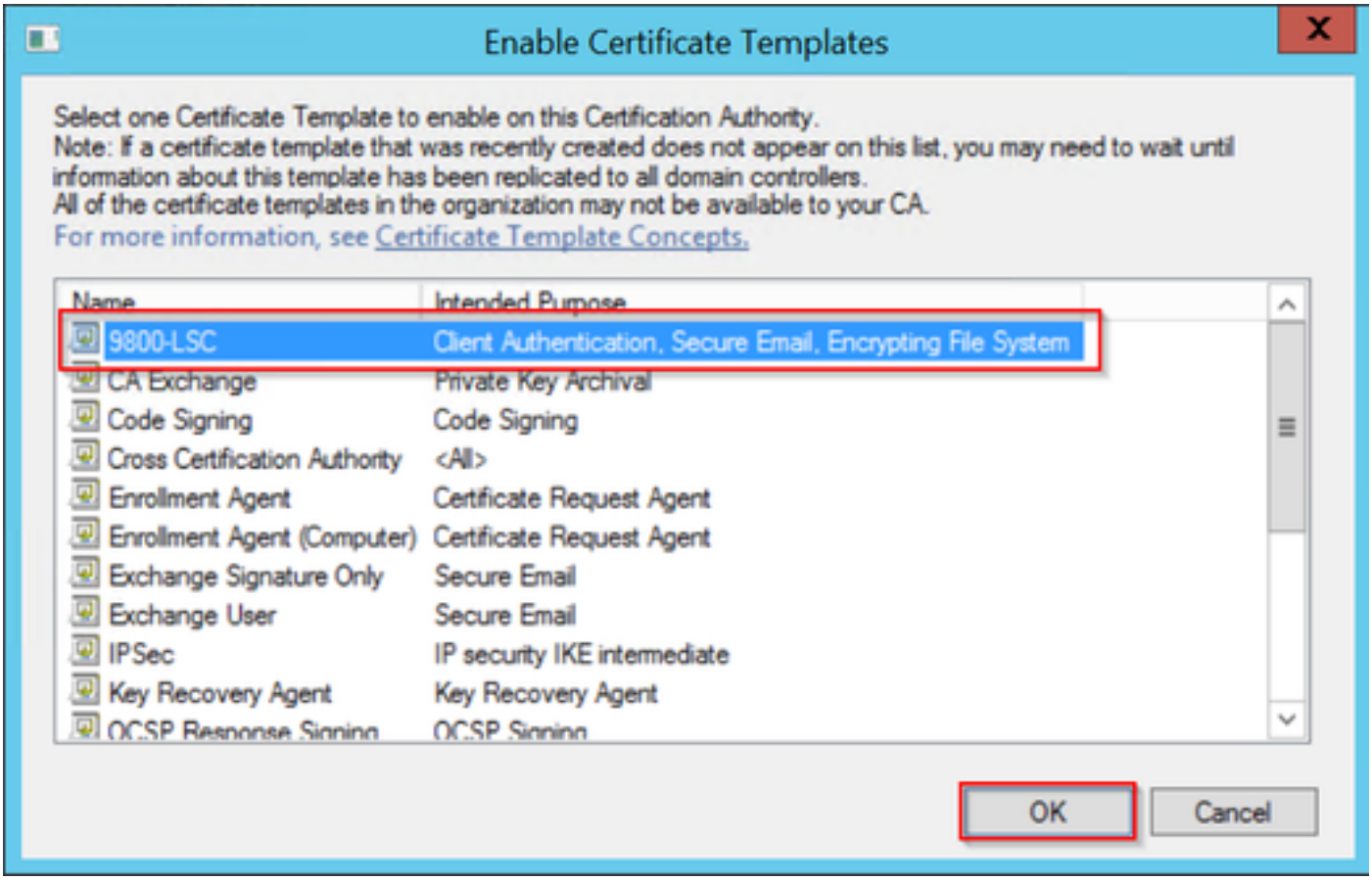


منح التحكم الكامل

الخطوة 8. ارجع إلى نافذة المرجع المصدق، وانقر بزر الماوس الأيمن في المجلد قوالب الشهادة وحدد جديد > قالب الشهادة المراد إصداره.

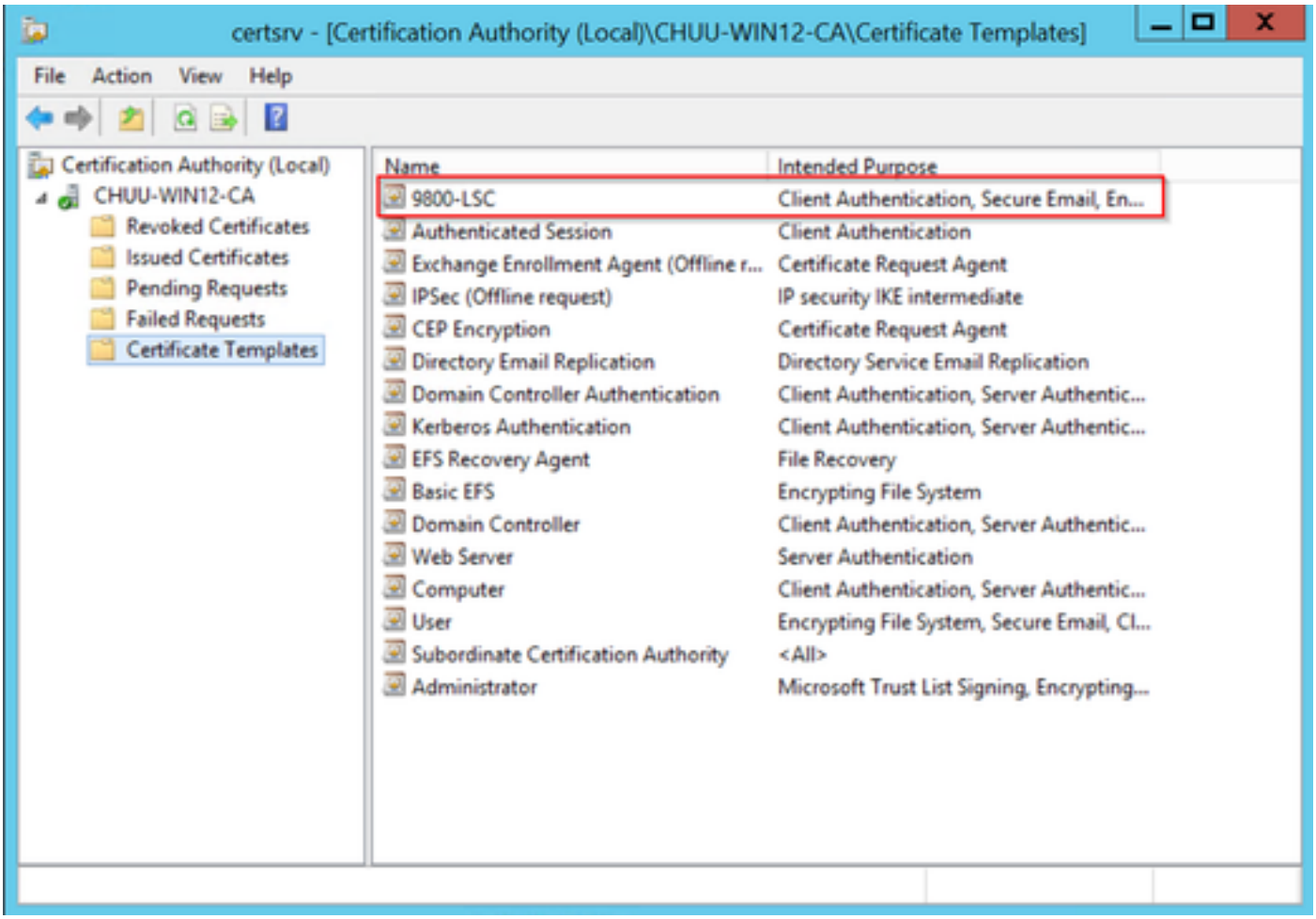
الخطوة 9. حدد قالب الشهادة الذي تم إنشاؤه مسبقا، في هذا المثال 9800-LSC، وحدد موافق.

ملاحظة: يمكن أن يستغرق قالب الشهادة الذي تم إنشاؤه حديثا وقتا أطول للإدراج في عمليات نشر خوادم متعددة لأنه يحتاج إلى النسخ المتماثل على كافة الخوادم.



إختيار القالب

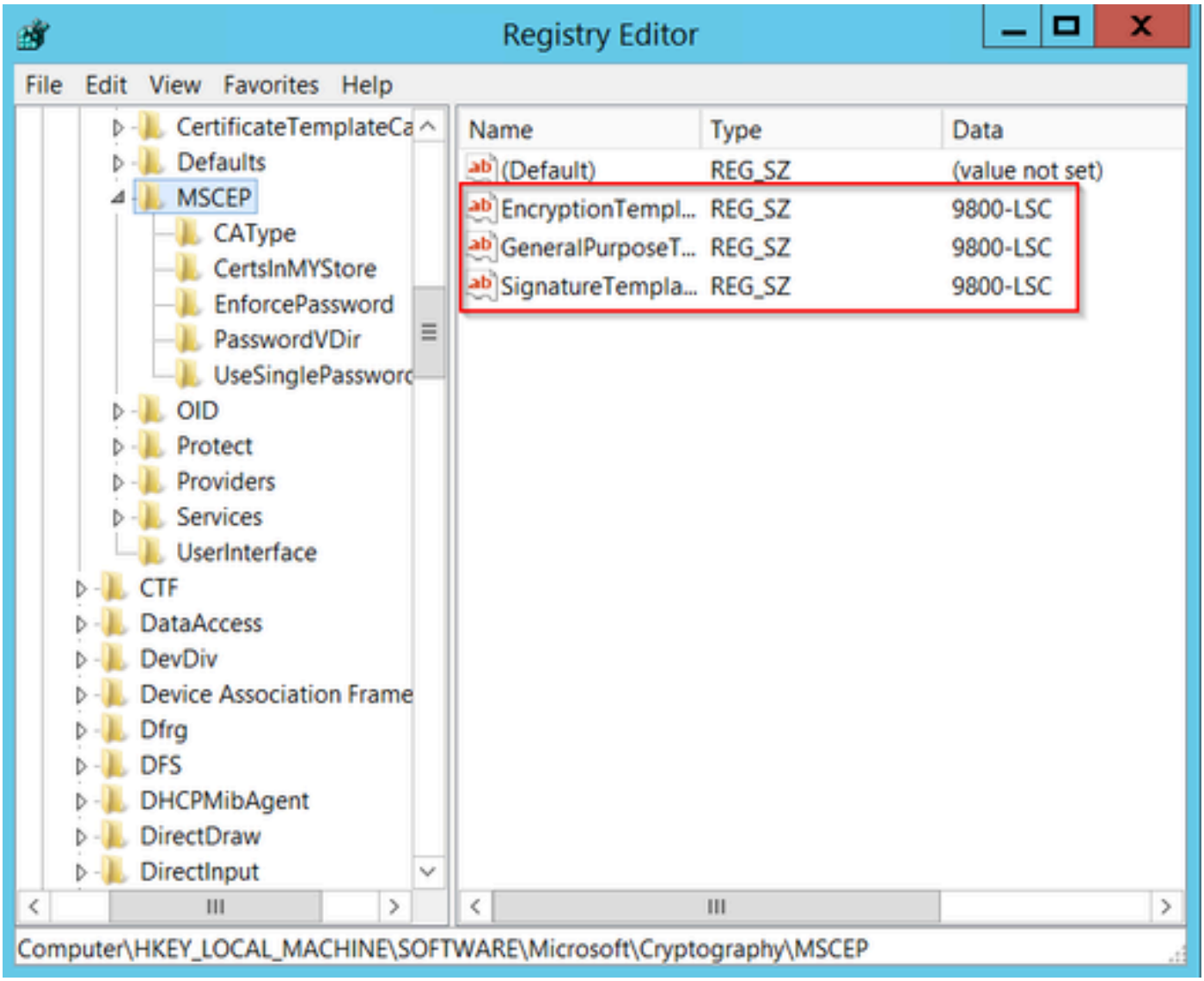
يتم سرد قالب الشهادة الجديد الآن ضمن محتوى مجلد قوالب الشهادات.



ددح LSC

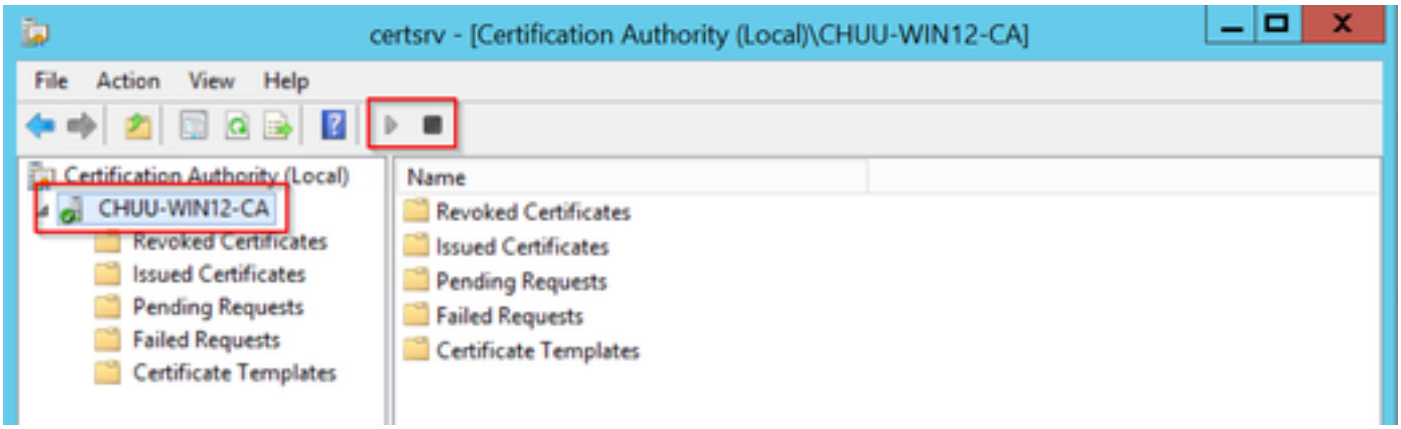
الخطوة 10. ارجع إلى نافذة محرر السجل وانتقل إلى Computer > HKEY_LOCAL_MACHINE > Software > Microsoft > Cryptography > MSCEP.

الخطوة 11. قم بتحرير سجلات EncryptionTemplate وGeneralPurposeTemplate وSignatureTemplate بحيث تشير إلى قالب الشهادة الذي تم إنشاؤه حديثا.



تغيير القالب في السجل

الخطوة 12. أعد تشغيل خادم NDES، لذلك ارجع إلى نافذة المرجع المصدق، وحدد اسم الخادم، وحدد زر إيقاف وتشغيل بنجاح.



تكوين LSC على 9800

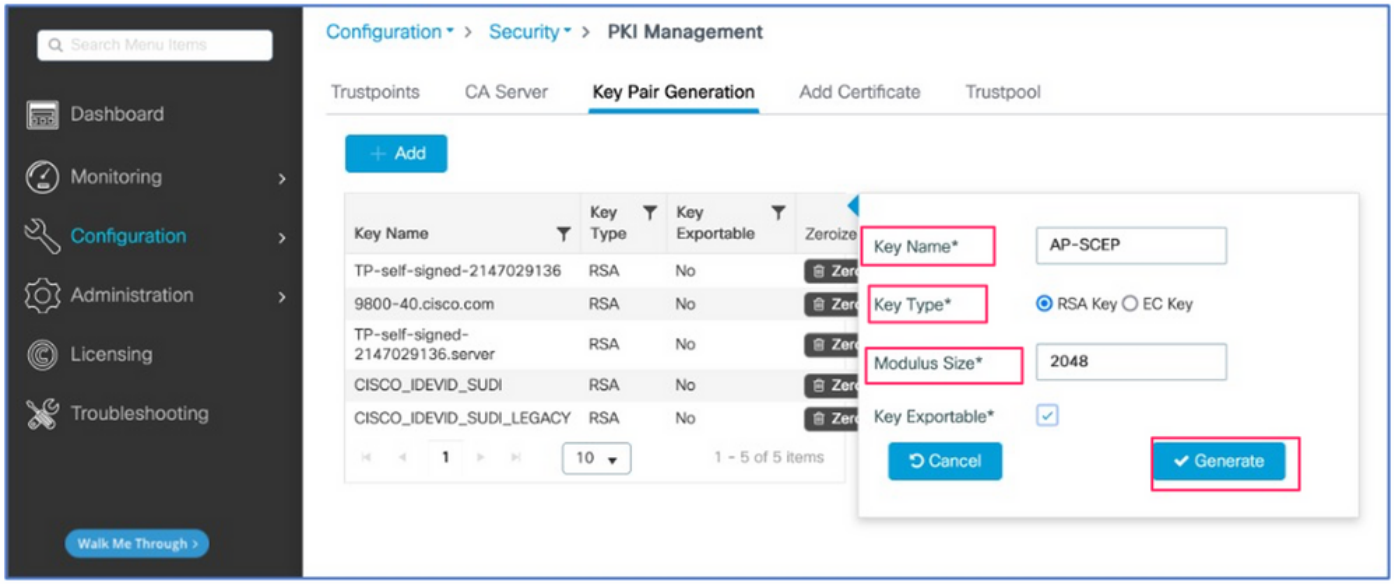
هنا الـ steps في تسلسل لـ يشكل LSC لـ ap في WLC.

1. قم بإنشاء مفتاح RSA. يتم إستخدام هذا المفتاح لاحقا ل PKI TrustPoint.
2. قم بإنشاء نقطة ثقة وتعيين مفتاح RSA الذي تم إنشاؤه.
3. قم بتمكين إعداد LSC لنقاط الوصول وتعيين TrustPoint.
    1. قم بتمكين LSC لجميع نقاط الوصول المنضمة.
    2. تمكين LSC لنقاط الوصول المحددة عبر قائمة التوفير.
4. قم بتغيير نقطة ثقة الإدارة اللاسلكية وأشر إلى نقطة ثقة LSC.

خطوات تكوين واجهة المستخدم الرسومية (GUI) ل AP LSC

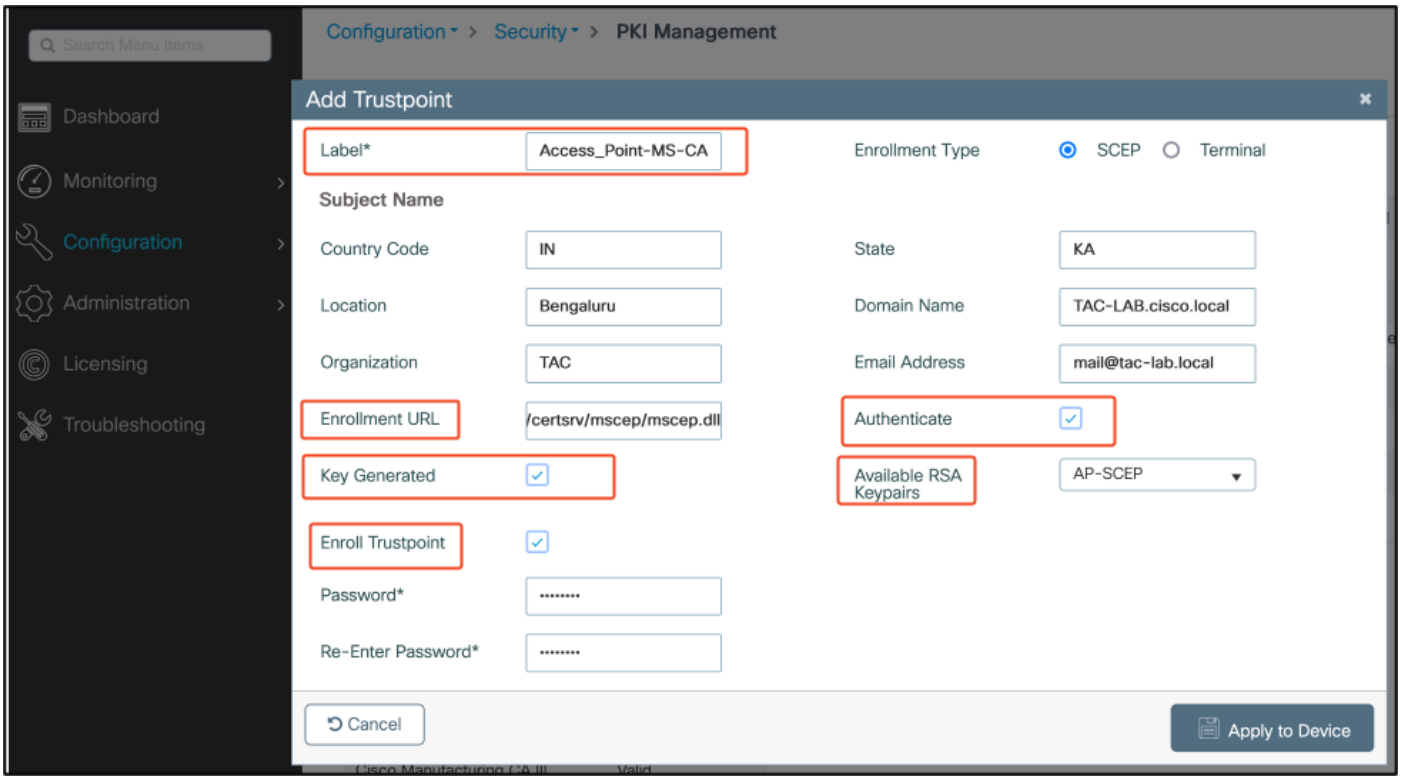
الخطوة 1. انتقل إلى التكوين > الأمان > إدارة PKI > إنشاء زوج المفاتيح.

1. طقطقة يضيف ويعطيه اسم مناسب.
2. قم بإضافة حجم مفتاح RSA.
3. إن خيار المفتاح القابل للتصدير إختياري. هذا مطلوب فقط إذا كنت تريد تصدير المفتاح خارج المربع.
4. حدد إنشاء



الخطوة 2. انتقل إلى التكوين > الأمان > إدارة PKI > نقاط الثقة

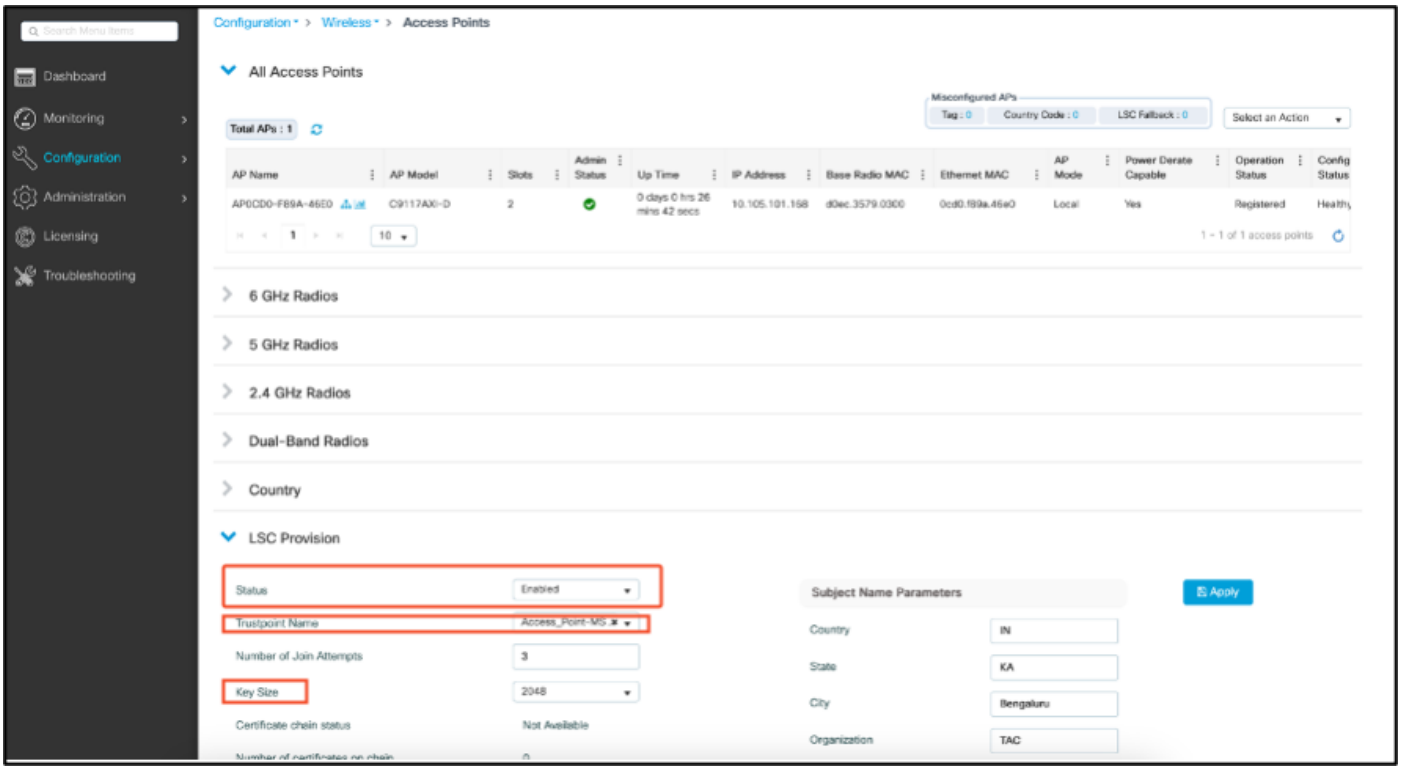
1. طقطقة يضيف ويعطيه اسم مناسب.
2. أدخل عنوان URL للتسجيل (عنوان URL هنا هو http://10.106.35.61:80/certsrv/mscep/mscep.dll) وباقي التفاصيل.
3. حدد أزواج مفاتيح RSA التي تم إنشاؤها في الخطوة 1.
4. انقر على المصادقة.
5. انقر فوق تسجيل TrustPoint وأدخل كلمة مرور.
6. انقر فوق تطبيق على الجهاز.



الخطوة 3.انتقل إلى التكوين > السلكي > نقاط الوصول. قم بالتمرير لأسفل وحدد توفير LSC.

1. تحديد الحالة كممكنة. هذا يمكن LSC ل all the APs أن يكون ربطت إلى هذا WLC.
2. حدد اسم TrustPoint الذي أنشأناه في الخطوة 2.

المأ بقية التفاصيل وفقا لاحتياجاتك.



ما إن يمكن أنت LSC، APs جلبت الشهادة عن طريق WLC وأعد تمهيد. في جلسة عمل وحدة

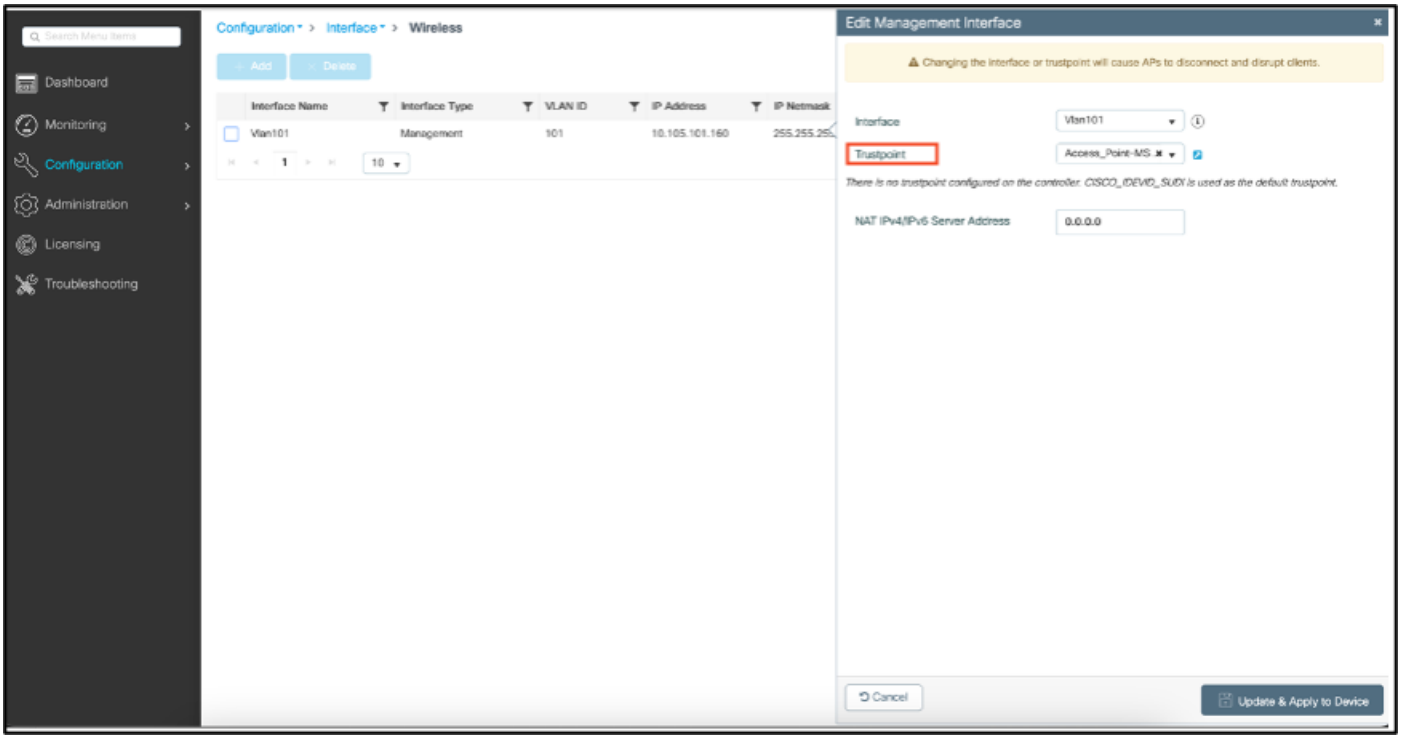
التحكم بنقطة الوصول، سترى شيئا مثل هذه القصاصة.

```
[*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
```

الخطوة 4. بمجرد تمكين LSC، يمكنك تغيير شهادة الإدارة اللاسلكية لتطابق TrustPoint ل LSC. هذا يجعل APs يتقارن مع LSC شهادة واL WLC يستعمل وه LSC شهادة ل AP يتقارن. هذه خطوة إختيارية إذا كنت مهتما فقط بعمل مصادقة 802.1X لنقاط الوصول الخاصة بك.

1. انتقل إلى Configuration (التكوين) > Interface (الواجهة) > Wireless وانقر فوق واجهة الإدارة.
2. قم بتغيير TrustPoint لتطابق TrustPoint الذي أنشأناه في الخطوة 2.

وهذا يختتم جزء تكوين واجهة المستخدم الرسومية (GUI) ل LSC. يجب أن تكون نقاط الوصول قادرة على الانضمام إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام شهادة LSC الآن.



خطوات تكوين واجهة سطر الأوامر (CLI) ل AP LSC

1. قم بإنشاء مفتاح RSA باستخدام هذا الأمر.

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

2. إنشاء نقطة ثقة PKI وتعيين زوج مفاتيح RSA. أدخل عنوان URL الخاص بالتسجيل وباقي التفاصيل.

```
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. مصادقة نقطة ثقة PKI وتسجيلها مع خادم CA باستخدام الأمر crypto pki authenticate <trustPoint>. أدخل كلمة مرور في مطالبة كلمة المرور.

```
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' commandwill 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. قم بتكوين انضمام نقطة الوصول باستخدام شهادة 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-LA
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. قم بتغيير TrustPoint الخاصة بالإدارة اللاسلكية لتطابق TrustPoint التي تم إنشاؤها أعلاه.

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

التحقق من AP LSC

تأكد من أن WLC يدفع الشهادة 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 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       : Not Available
AP LSC authentication state                  : CAPWAP-DTLS
```

بمجرد إعادة تحميل نقاط الوصول، قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) لنقطة الوصول ثم قم بتشغيل هذه الأوامر للتحقق من تكوين LSC.

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

```
AP0CD0.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
```

أستكشاف أخطاء إعداد LSC وإصلاحها

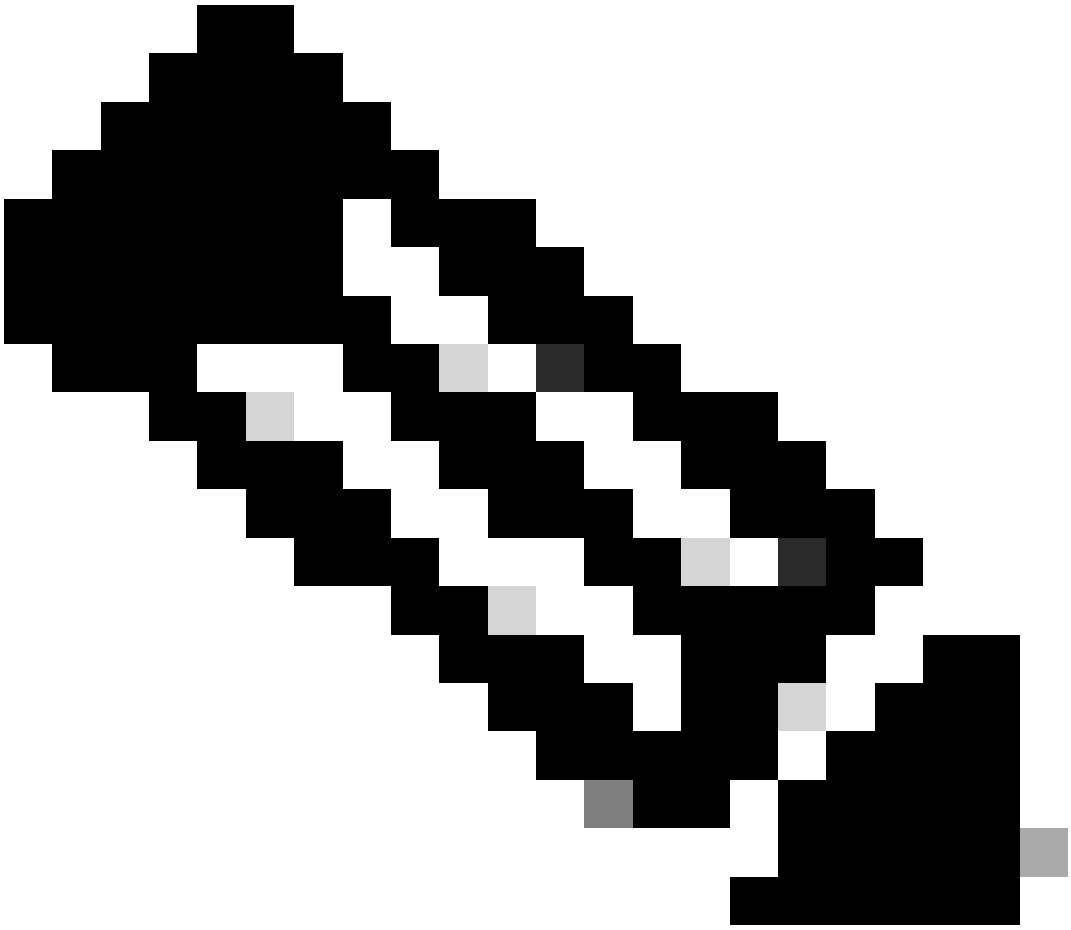
يمكنك أخذ التقاط EPC من منفذ مدول توصيل WLC أو AP للتحقق من الشهادة التي تستخدمها نقطة الوصول لتكوين نفق CAPWAP. تحقق من PCAP إذا تم إنشاء نفق DTLS بنجاح.

```
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: 3082065130820539a00302010202135c000000181814edda85f9bfd1000000000018300d… (pkcs-9-at-emailAddress=mail@tac-lab.local,id-at-commonNa
          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)
                RDNSequence item: 1 item (dc=com)
                  RelativeDistinguishedName item (dc=com)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: com
                RDNSequence item: 1 item (dc=tac-lab)
                  RelativeDistinguishedName item (dc=tac-lab)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: tac-lab
                RDNSequence item: 1 item (dc=sumans)
                  RelativeDistinguishedName item (dc=sumans)
                      Object Id: 0.9.2342.19200300.100.1.25 (dc)
                      IA5String: sumans
                RDNSequence 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)
```

يمكن تشغيل تصحيح أخطاء DTLS على AP و WLC لفهم مشكلة الشهادة.

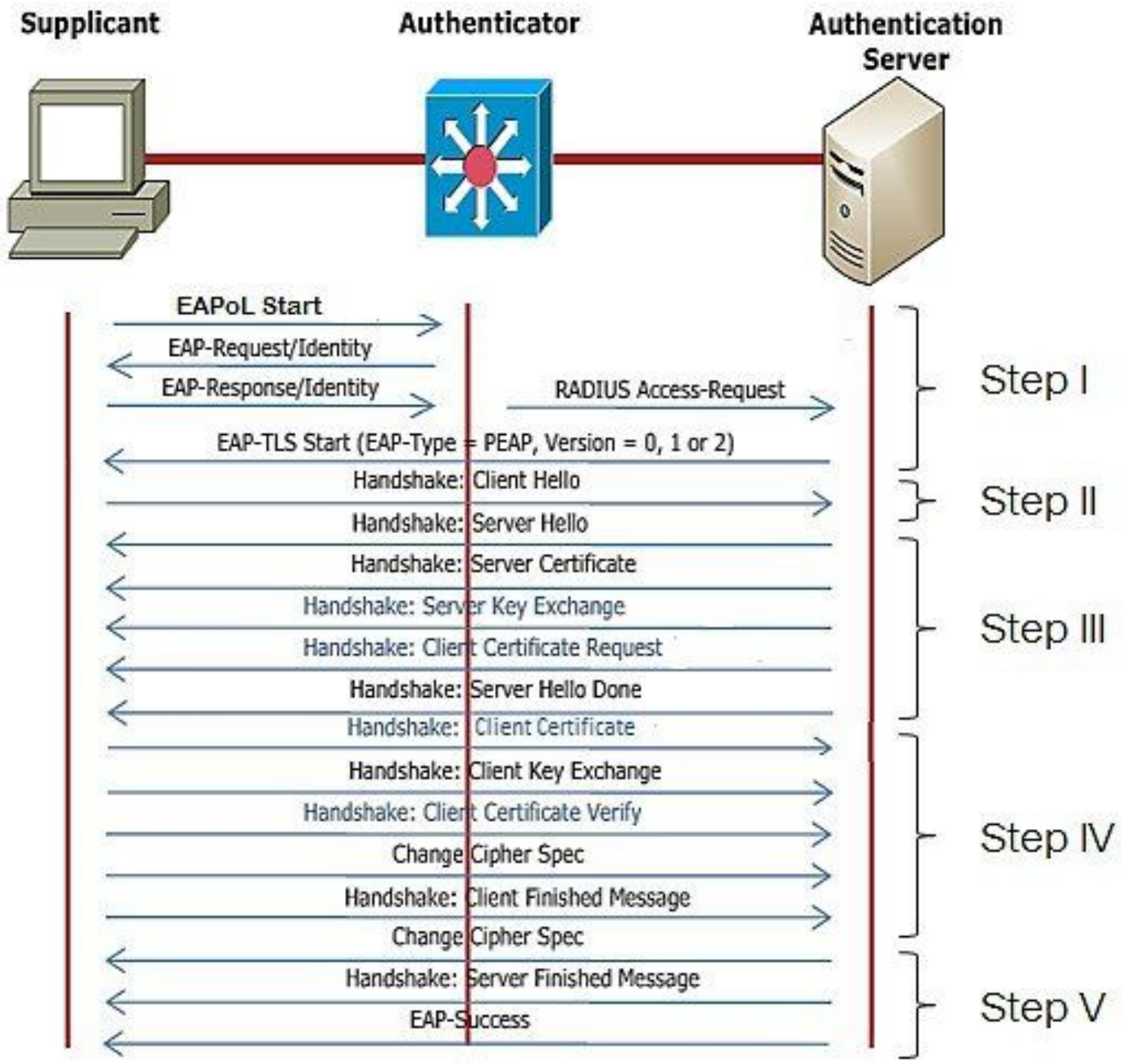
نقطة الوصول السلكية مصادقة 802.1X باستخدام LSC

تم تكوين نقطة الوصول باستخدام نفس شهادة LSC للمصادقة على نفسها. تعمل نقطة الوصول كموجه 802.1X وتتم مصادقتها بواسطة المحول مقابل خادم ISE. يتحدث خادم ISE إلى الإعلان في مؤخرة الشاشة.



ملاحظة: بمجرد تمكين مصادقة dot1x على منفذ محول توصيل AP، لا يمكن لنقاط الوصول إعادة توجيه أو إستقبال أي حركة مرور حتى يتم تمرير المصادقة. باستخدام مصادقة غير ناجحة والوصول إلى AP، قم بتعطيل مصادقة نقاط الوصول (AP) على منفذ المحول السلكي لنقطة الوصول.

سير عمل مصادقة EAP-TLS وتبادل الرسائل

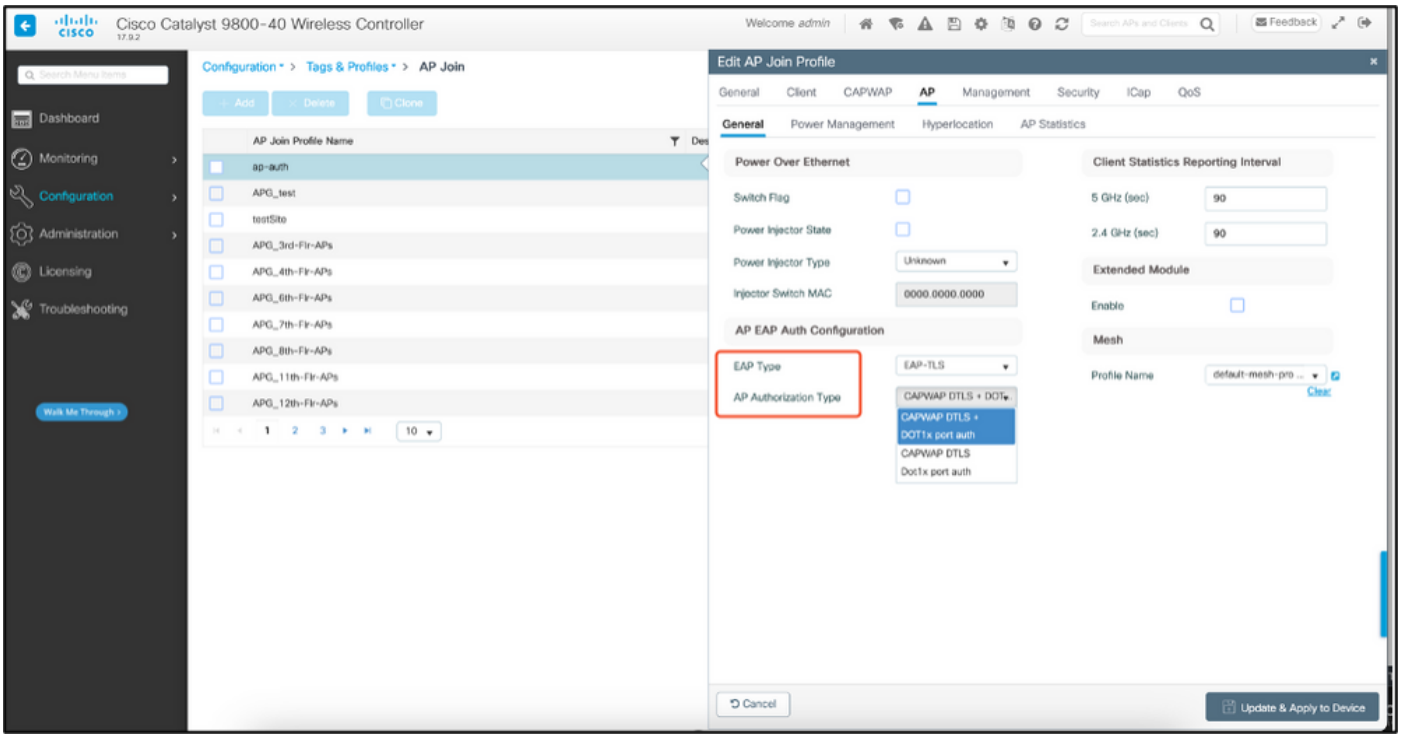


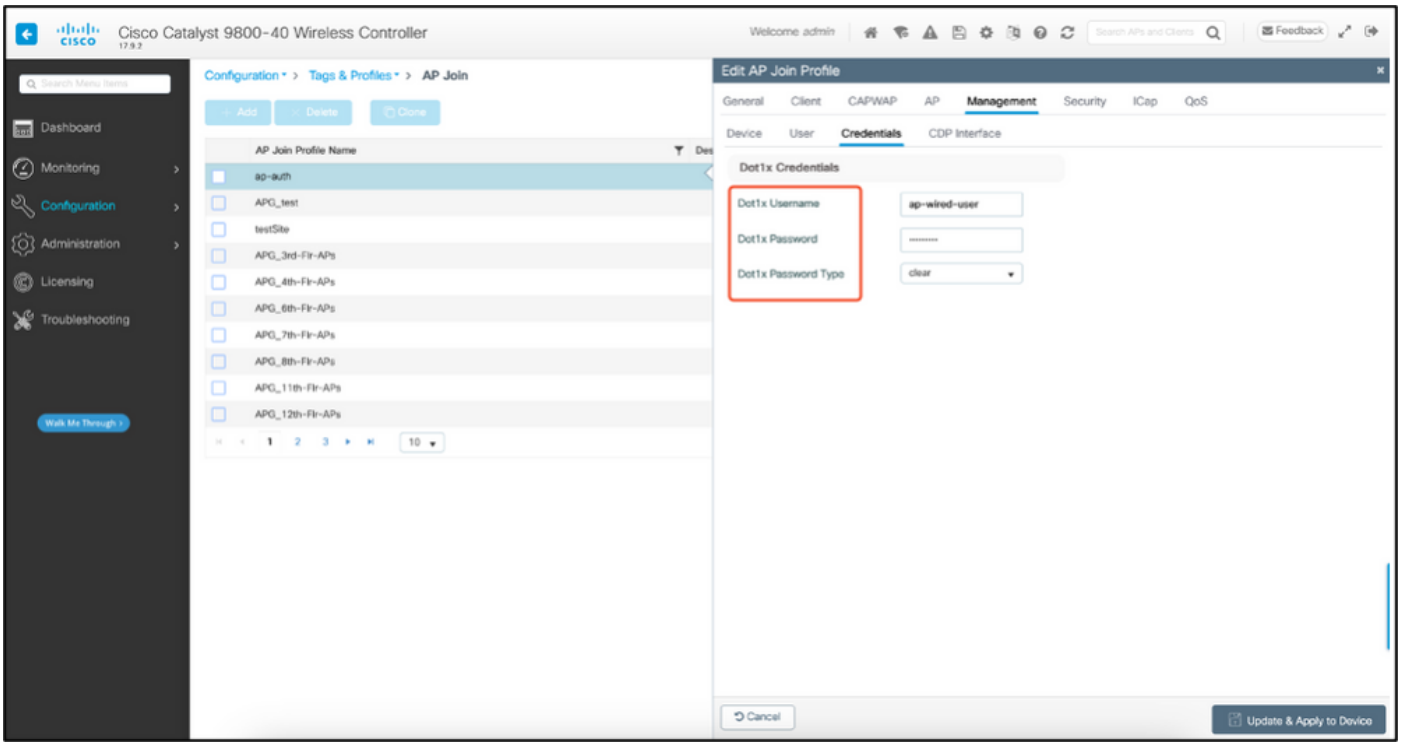
خطوات تكوين مصادقة 802.1x السلكية لنقطة الوصول

1. قم بتمكين مصادقة المنفذ dot1x مع DTLS ل CAPWAP وحدد نوع EAP.
2. قم بإنشاء بيانات اعتماد dot1x لنقاط الوصول.
3. مكنت dot1x على المفتاح ميناء.
4. تثبيت شهادة موثوق بها على خادم RADIUS.

نقطة الوصول السلكية تكوين واجهة المستخدم الرسومية (GUI) لمصادقة 802.1x

1. انتقل إلى ملف تعريف ربط نقطة الوصول وانقر على ملف التعريف.
    1. انقر على نقطة الوصول > عام. حدد نوع EAP ونوع تخويل AP ك "CAPWAP DTLS + dot1x Port auth".
    2. انتقل إلى إدارة > بيانات اعتماد وقم بإنشاء اسم مستخدم وكلمة مرور لنقطة الوصول dot1x auth.





AP Wired 802.1x صحة هوية CLI تشكيل

استعملت هذه أمر أن يمكن dot1x ل APs من ال CLI. ال يؤدي هذه إلا إلى تمكين المصادقة السلكية لنقاط الوصول التي تستخدم توصيف الربط المعين.

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

لي ap سلكي 802.1x صحة وهية مفتاح تشكيل

يتم إستخدام تكوينات المحول هذه في LAB لتمكين مصادقة AP السلكية. يمكنك الحصول على تهيئة مختلفة استنادا إلى التصميم.

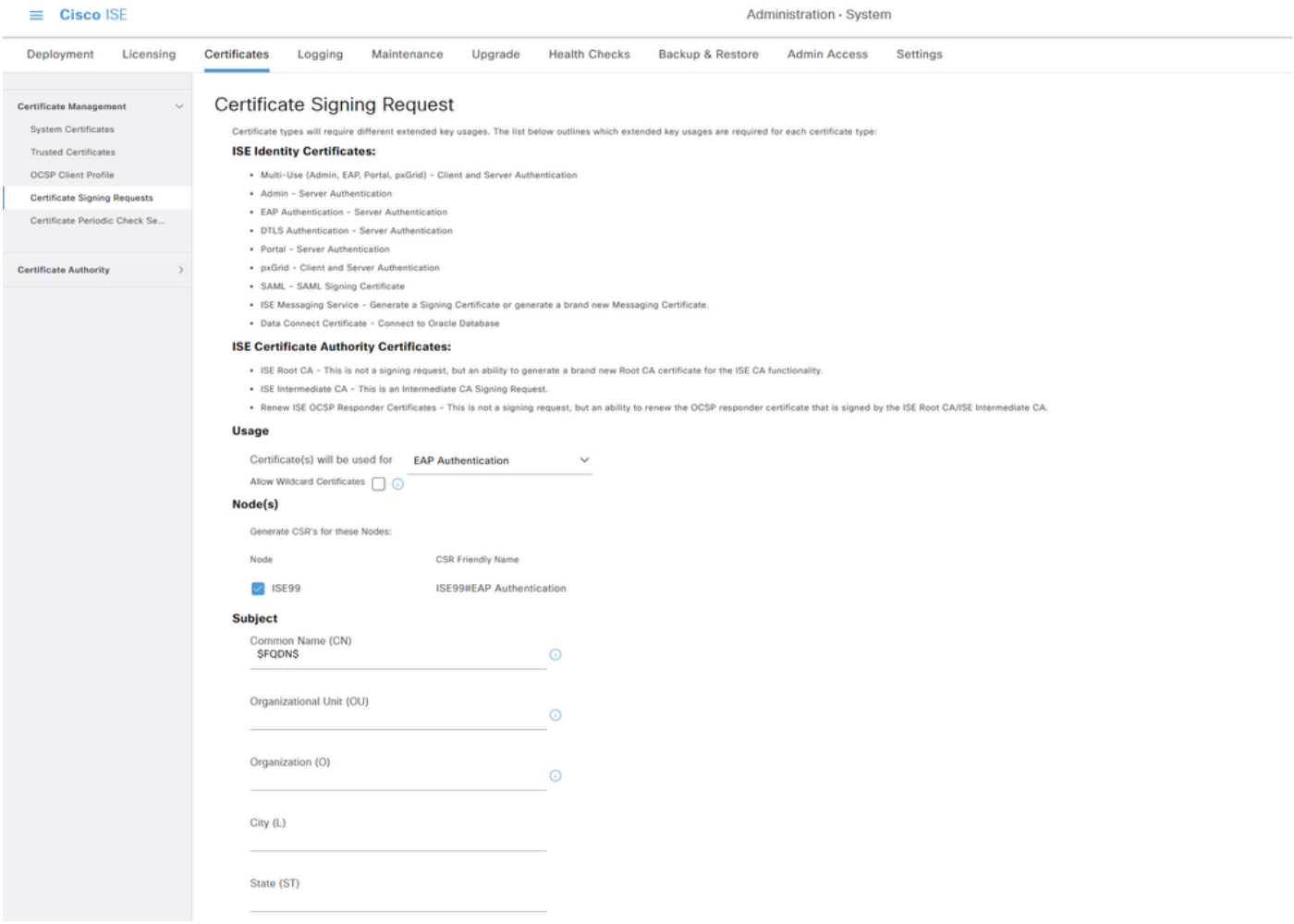
```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
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
```

تثبيت شهادة خادم RADIUS

تحدث المصادقة بين نقطة الوصول (التي تعمل كمتمس) وخادم RADIUS. يجب أن يثق كل منهما في شهادة الآخر. الطريقة الوحيدة التي تثق بها نقطة الوصول في شهادة خادم RADIUS هي أن يستخدم خادم RADIUS شهادة صادرة من مرجع SCEP CA الذي أصدر شهادة AP أيضا.

في ISE، انتقل إلى الإدارة > شهادات > إنشاء طلبات توقيع شهادات

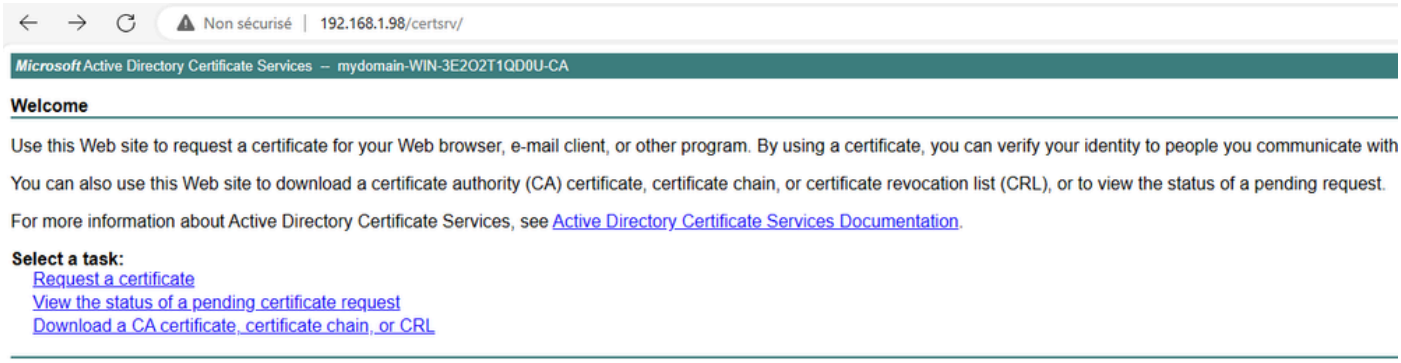
قم بإنشاء CSR وتعبئة الحقول بمعلومات عقدة ISE الخاصة بك.



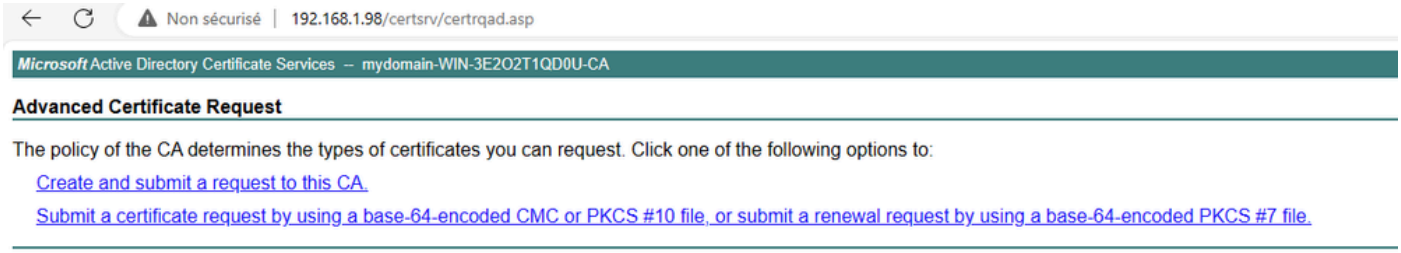
بمجرد أن يتم توليدها، يمكنك تصديرها ونسخ لصقها كنص أيضا.

انتقل إلى عنوان IP الخاص ب Windows CA وأضف /certsrv/ إلى عنوان URL

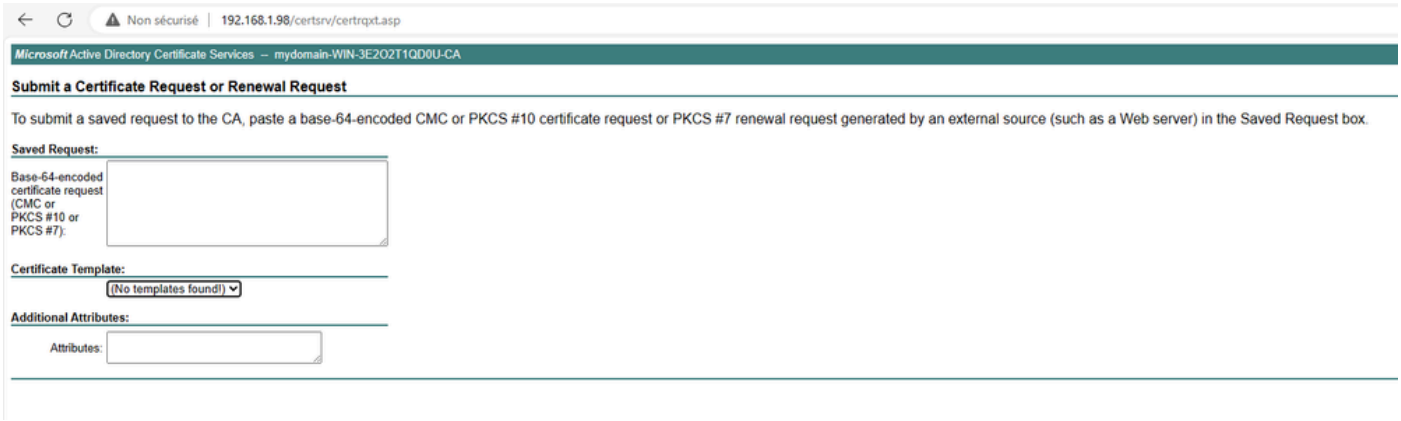
انقر على طلب شهادة



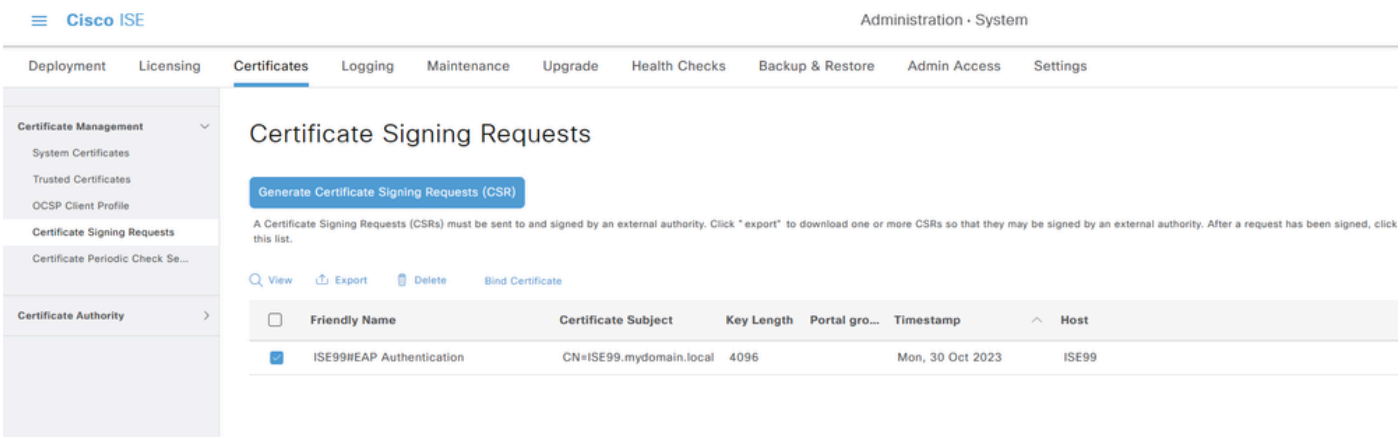
انقر على إرسال طلب شهادة باستخدام base-64 ...



الصق نص CSR في مربع النص. أختر قالب شهادة خادم الويب.



يمكنك بعد ذلك تثبيت هذه الشهادة على ISE بالرجوع إلى قائمة طلب توقيع الشهادة والنقر فوق ربط الشهادة. يمكنك بعد ذلك تحميل الشهادة التي حصلت عليها من Windows C.



نقطة الوصول: التحقق من مصادقة 802.1x السلكية

احصل على وصول وحدة التحكم إلى نقطة الوصول وقم بتشغيل الأمر:

```
#show ap authentication status
```

لم يتم تمكين مصادقة نقطة الوصول:

```
AP0CD0.F89A.46E8#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E8#
```

سجلات وحدة التحكم من AP بعد تمكين مصادقة 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
```

تمت مصادقة AP بنجاح:

```
AP0CD0.F89A.46E0#sho ap authentication status
key_mgmt=IEEE 802.1X (no WPA)
wpa_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=0d7b91a744885a6e8e460d49fee7d2d5604ea2bdd11f40494a4325dc98d1919af48b9fb33ee526f18eda11effcb2ea0238cf95244aafb5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

التحقق من WLC:

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

حالة واجهة Switchport بعد المصادقة الناجحة:

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

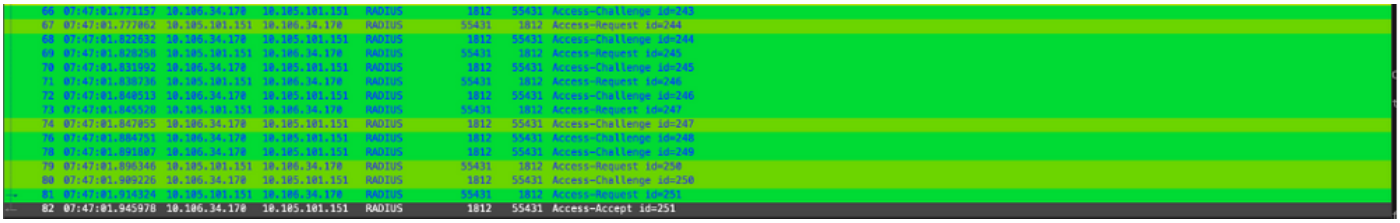
هذه عينة من سجلات وحدة تحكم نقطة الوصول تشير إلى مصادقة ناجحة:

```
[*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
```

أستكشاف أخطاء مصادقة 802.1X وإصلاحها

خذ PCAP على وصلة AP وتحقق من مصادقة RADIUS. فيما يلي جزء من المصادقة الناجحة.

يجمع TCPdump من ISE لالتقاط المصادقة.



إذا كانت هناك مشكلة تالحظ أثناء المصادقة، فسيلزم التقاط الحزم بشكل متزامن من وصلة AP السلكية وجانب ISE.

أمر تصحيح الأخطاء ل AP:

```
#debug ap authentication packet
```

معلومات ذات صلة

- الدعم التقني والتنزيلات من Cisco
- تكوين 802.1X على AP باستخدام AireOS
- دليل التكوين 9800 ل LSC
- LSC تشكيل مثال ل 9800
- تكوين 802.1X لنقاط الوصول على 9800

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).