الشهادات ذات الأهمية المحلية (LSC) مع WLC ومثال تكوين Windows Server 2012

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
تكوين Microsoft Windows Server
تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)
التحقق من الصحة
استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا وثيقة كيف أن يشكل شهادات هامة محليا (LSC) مع السلكي lan جهاز تحكم (WLC) و حديثا ركبت مايكروسوفت ويندوز لدل 2012 R2.

> **ملاحظة**: قد تختلف عمليات النشر الحقيقية في العديد من النقاط ويجب أن تتمتع بالتحكم الكامل ومعرفة الإعدادات الموجودة على Microsoft Windows Server 2012. يتم توفير مثال التكوين هذا فقط كقالب مرجع لعملاء Cisco لتنفيذ تكوين Microsoft Windows Server الخاص بهم وتكييفه من أجل تشغيل LSC.

المتطلبات الأساسية

المتطلبات

توصي Cisco بفهم كل تغييرات تم إجراؤه في Microsoft Windows Server والتحقق من وثائق Microsoft ذات الصلة إذا لزم الأمر.

> **ملاحظة**: ال يتم دعم LSC على WLC مع CA الوسيط، حيث أنه سيتم فقد CA الجذر من WLC بما أن وحدة التحكم تحصل على CA الوسيط فقط.

المكونات المستخدمة

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

- WLC، الإصدار 7.6
- نظام التشغيل Microsoft Windows Server 2012 R2

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

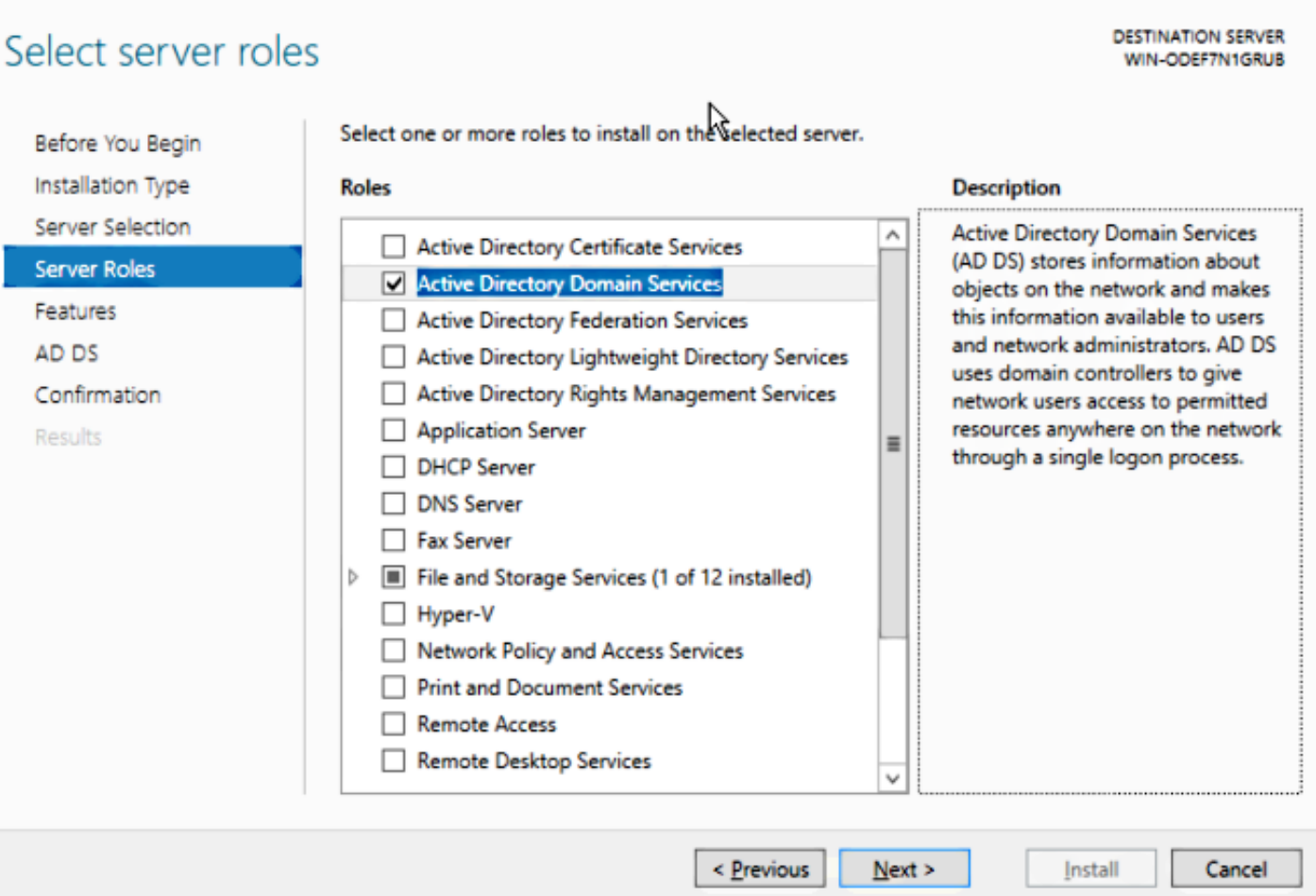
شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

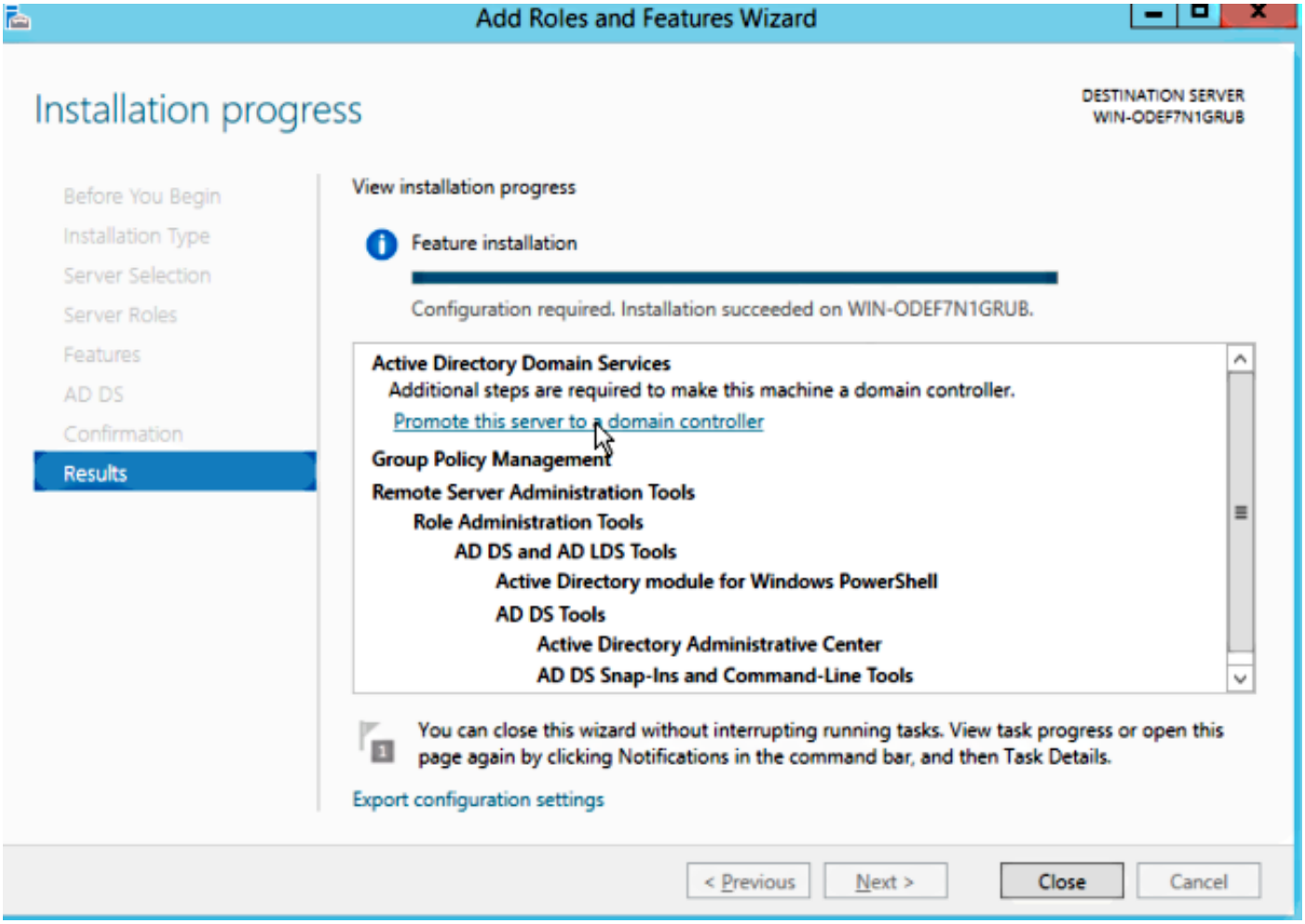
تكوين Microsoft Windows Server

يتم عرض هذا التكوين كما تم إجراؤه على Microsoft Windows Server 2012 المثبت حديثا. يجب تكييف الخطوات مع مجالك وتكوينك.

الخطوة 1. تثبيت خدمات مجال Active Directory لمعالج الأدوار والميزات.

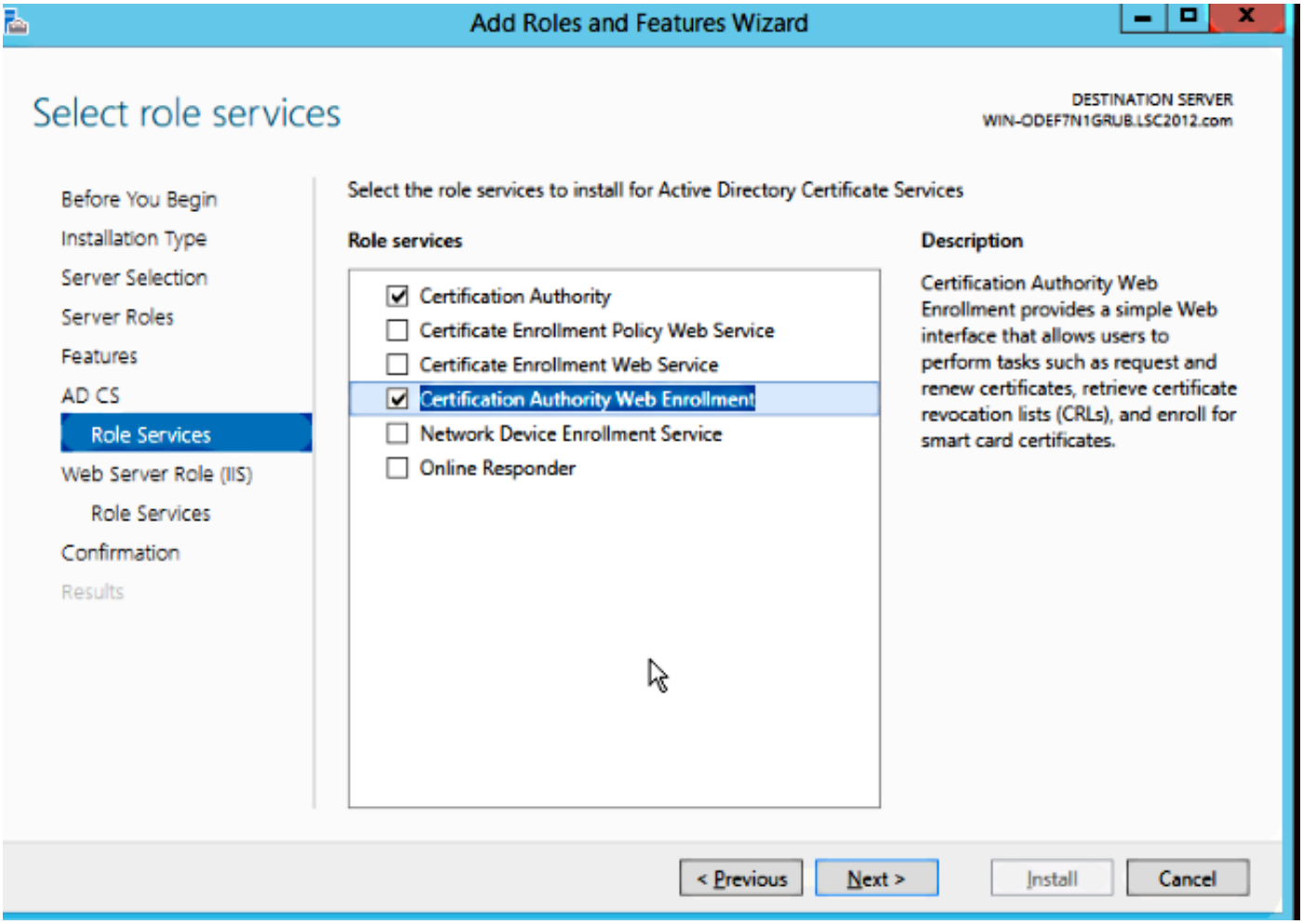


الخطوة 2. بعد التثبيت، يجب ترقية الخادم إلى وحدة التحكم بالمجال.

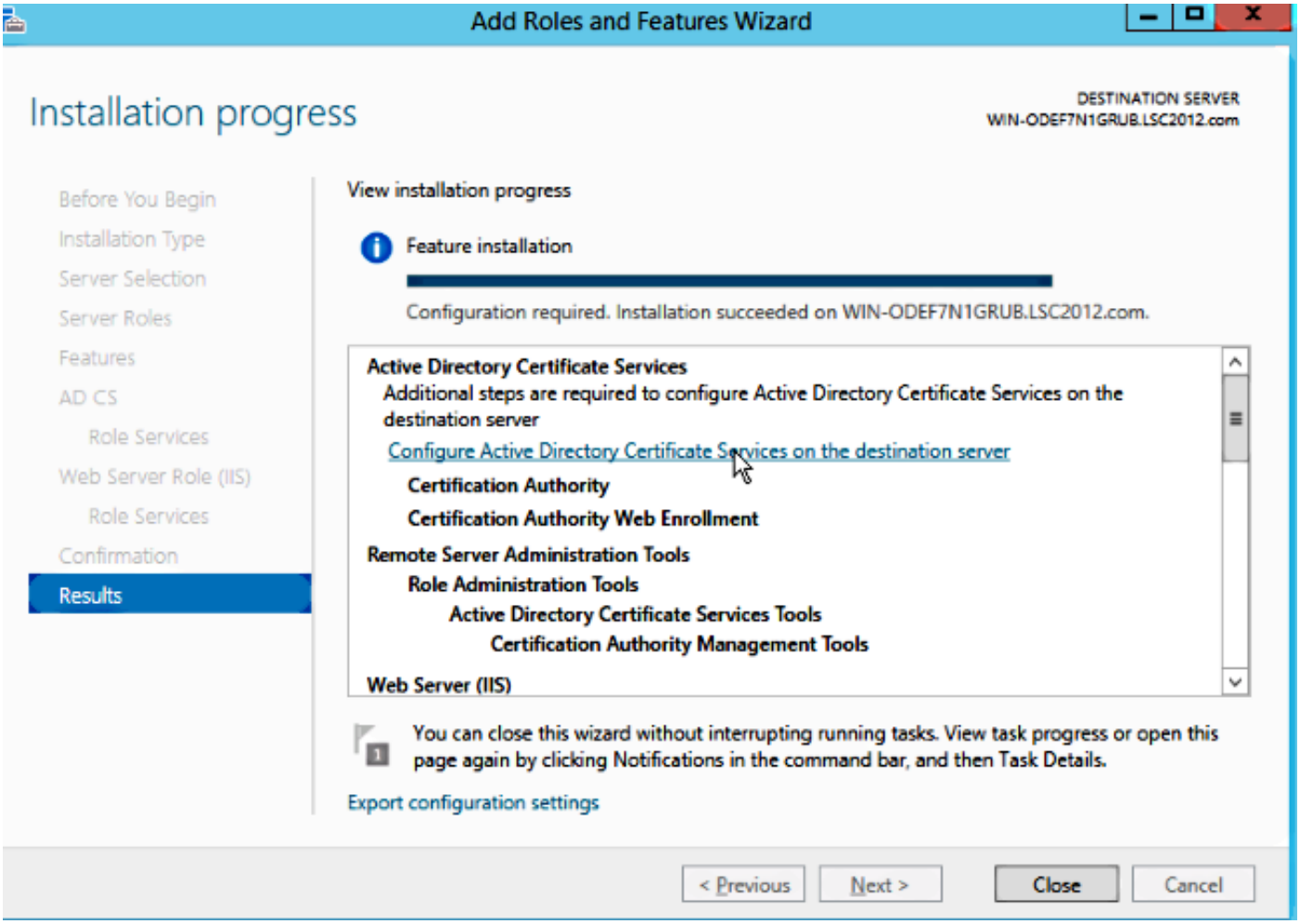


الخطوة 3. بما أن هذا إعداد جديد، فإنك تقوم بتكوين غابة جديدة، ولكن عادة في عمليات النشر الموجودة، قم بتكوين هذه النقاط بسلطة على وحدة التحكم بالمجال. هنا، أنت تختار ال **LSC2012.com** مجال. يؤدي هذا إلى تنشيط ميزة خادم اسم المجال (DNS) أيضا.

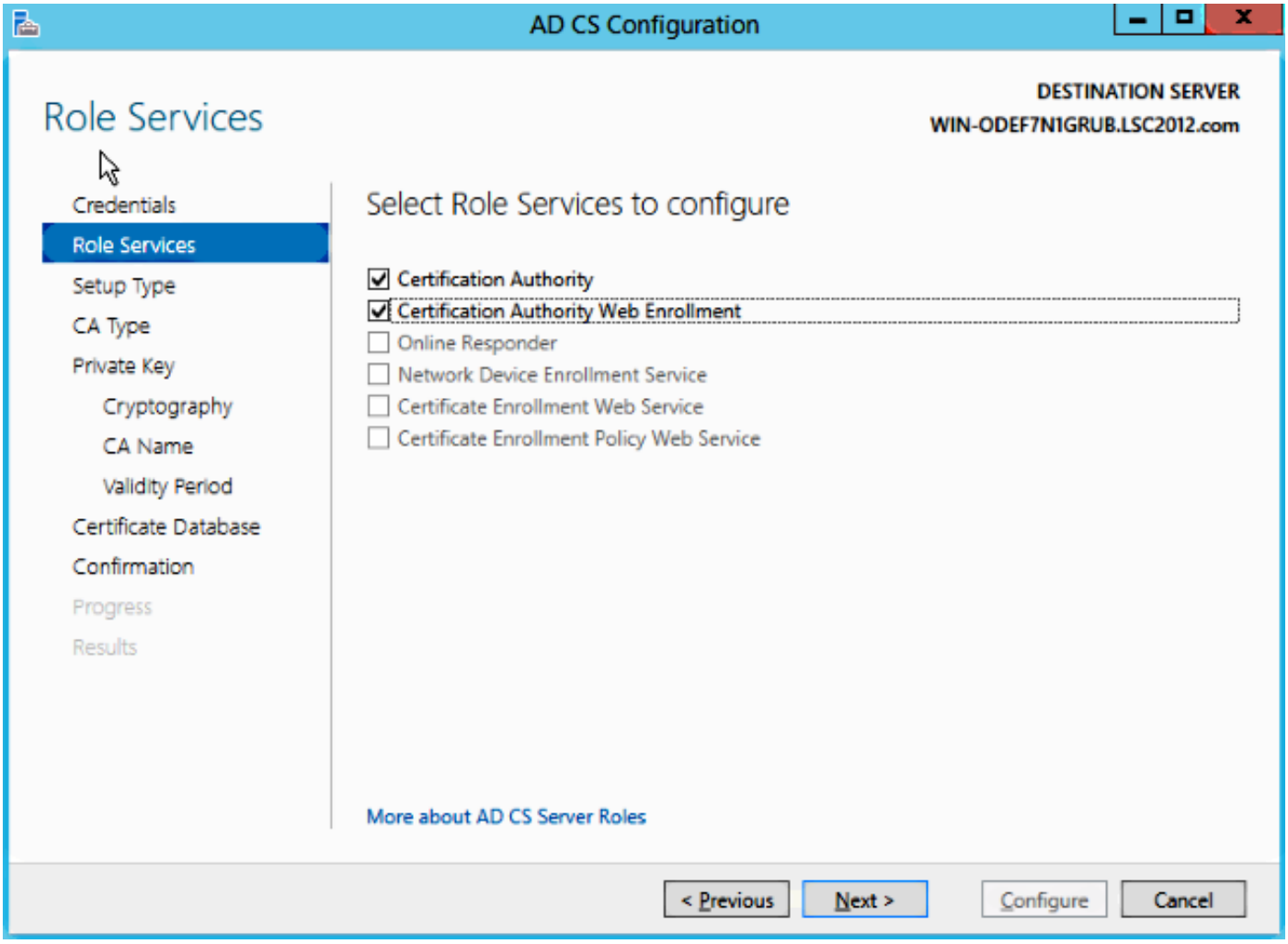
الخطوة 4. بعد إعادة التشغيل، قم بتثبيت خدمة المرجع المصدق (CA) بالإضافة إلى تسجيل الويب.



الخطوة 5.قم بتكوينها.



الخطوة 6. أختر المرجع المصدق للمؤسسة واترك كل شيء كافتراضي.

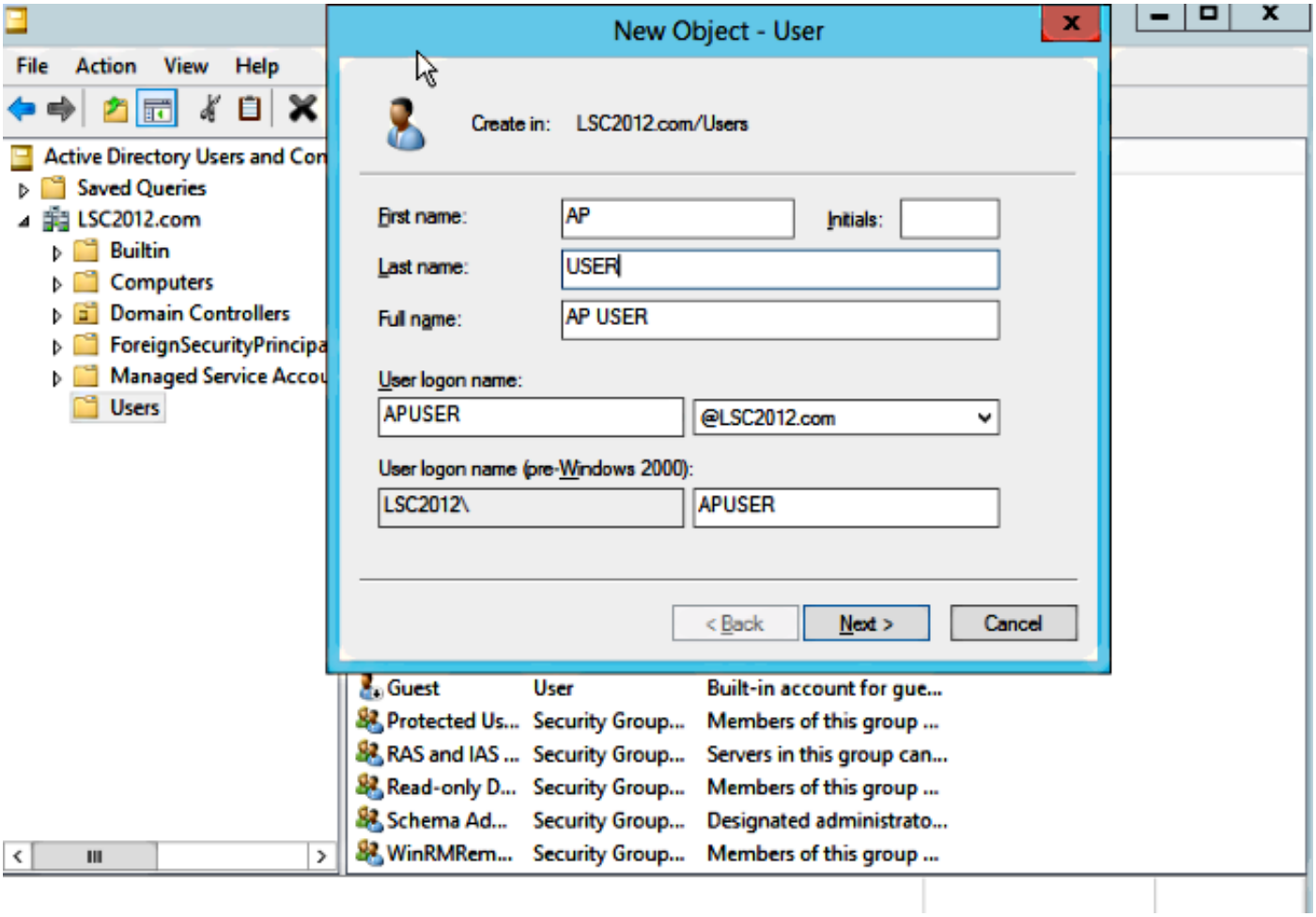


الخطوة 7. انقر على **قائمة Microsoft Windows/Start**.

الخطوة 8. **طقطقة أداة إداري**.

الخطوة 9. انقر فوق **مستخدمي Active Directory وأجهزة الكمبيوتر**.

الخطوة 10. قم بتوسيع المجال، وانقر بزر الماوس الأيمن فوق المجلد Users، واختر **كائن جديد > مستخدم**.



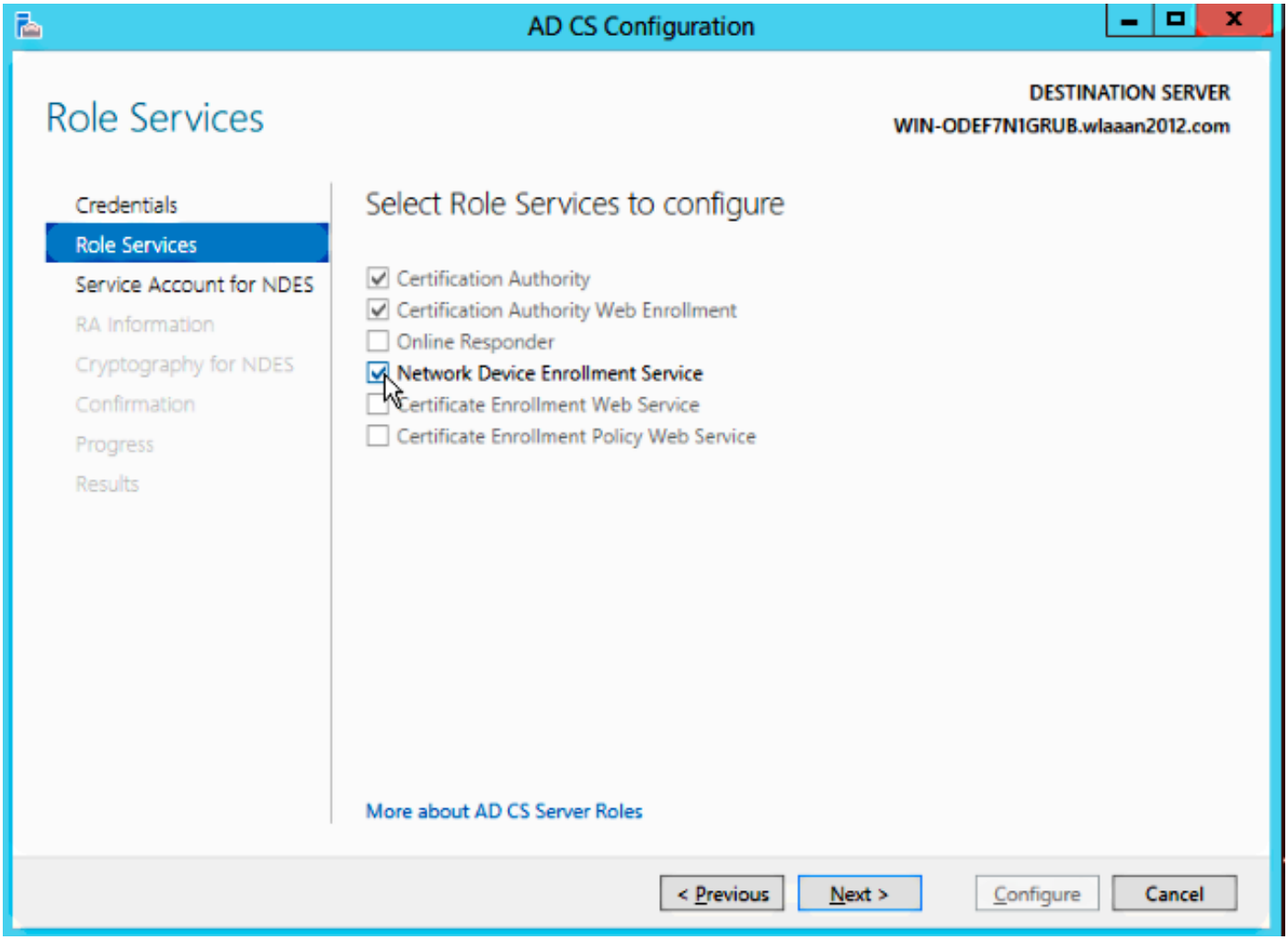
الخطوة 11. في هذا المثال، يسمى APUSER. ويجب عليك، بمجرد إنشائها، تحرير المستخدم وانقر فوق علامة التبويب **عضو في**"، وجعلها عضوا في مجموعة IIS_IUSRS

تعيينات حقوق المستخدم المطلوبة هي:

- السماح بتسجيل الدخول محليا

- تسجيل الدخول كخدمة

الخطوة 12. قم بتثبيت خدمة تسجيل جهاز الشبكة (NDES).



- أختر عضو الحساب الخاص بمجموعة IIS_USRS، **APUSER** في هذا المثال، كحساب خدمة ل NDES.

الخطوة 13. انتقل إلى الأدوات الإدارية.

الخطوة 14. انقر فوق خدمات معلومات الإنترنت (IIS).

الخطوة 15. قم بتوسيع **الخادم > المواقع > موقع الويب الافتراضي > CERT SRV.**

الخطوة 16. لكل من mscep وmscep_admin، انقر فوق **المصادقة**. تأكد من تمكين المصادقة المجهولة.

الخطوة 17. انقر بزر الماوس الأيمن فوق **مصادقة Windows** واختر **الموفرين**. تأكد من أن مدير NT LAN (NTLM) هو الأول في القائمة.

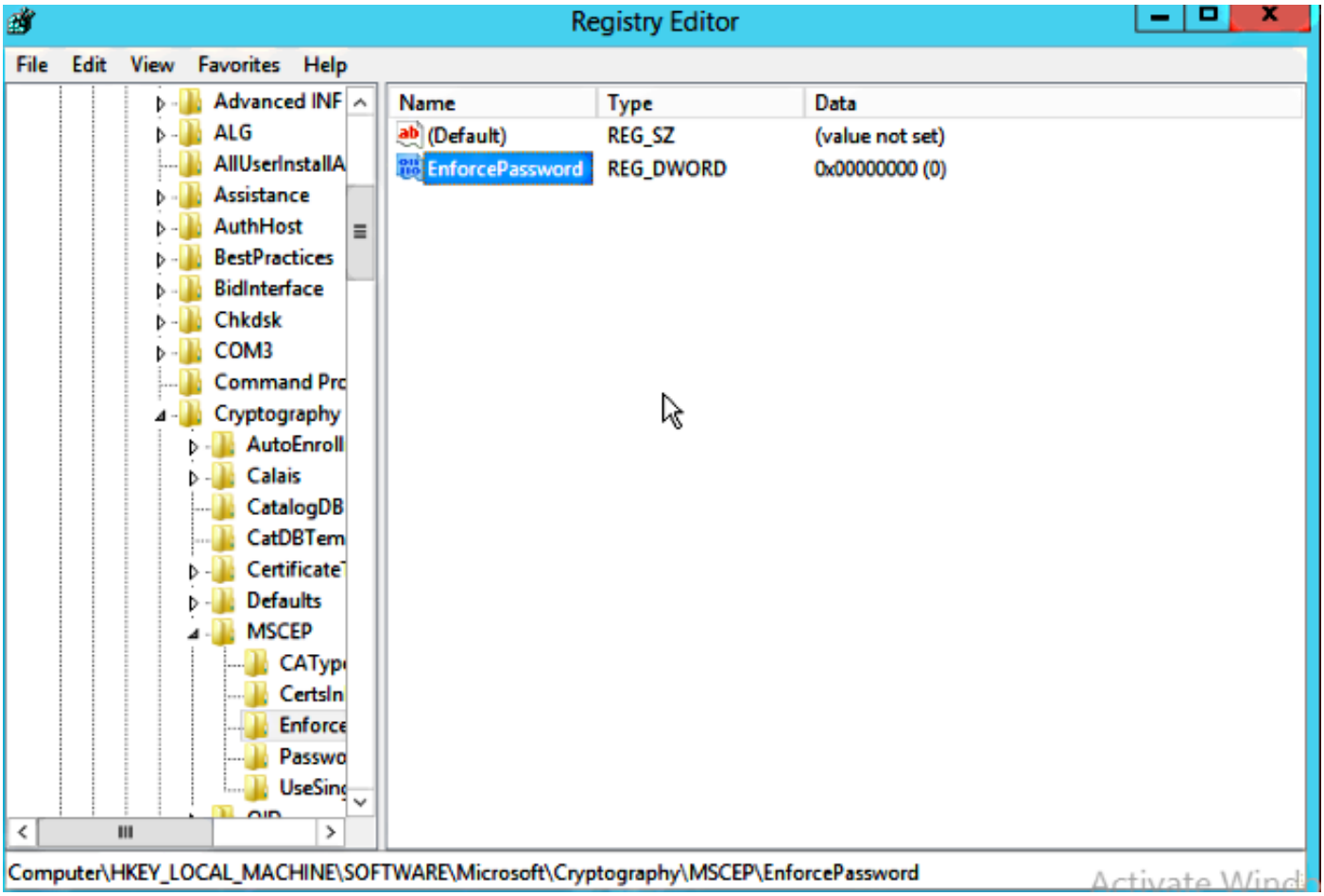
الخطوة 18. قم بتعطيل تحدي المصادقة في إعدادات السجل، وإلا يتوقع بروتوكول تسجيل الشهادة البسيط (SCEP) مصادقة كلمة مرور التحدي، والتي لا تدعمها عنصر التحكم في

الشبكة المحلية اللاسلكية (WLC).

الخطوة 19. افتح تطبيق regedit.

الخطوة 20. انتقل إلى HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\.

الخطوة 21. تعيين EnforcementPassword على 0.



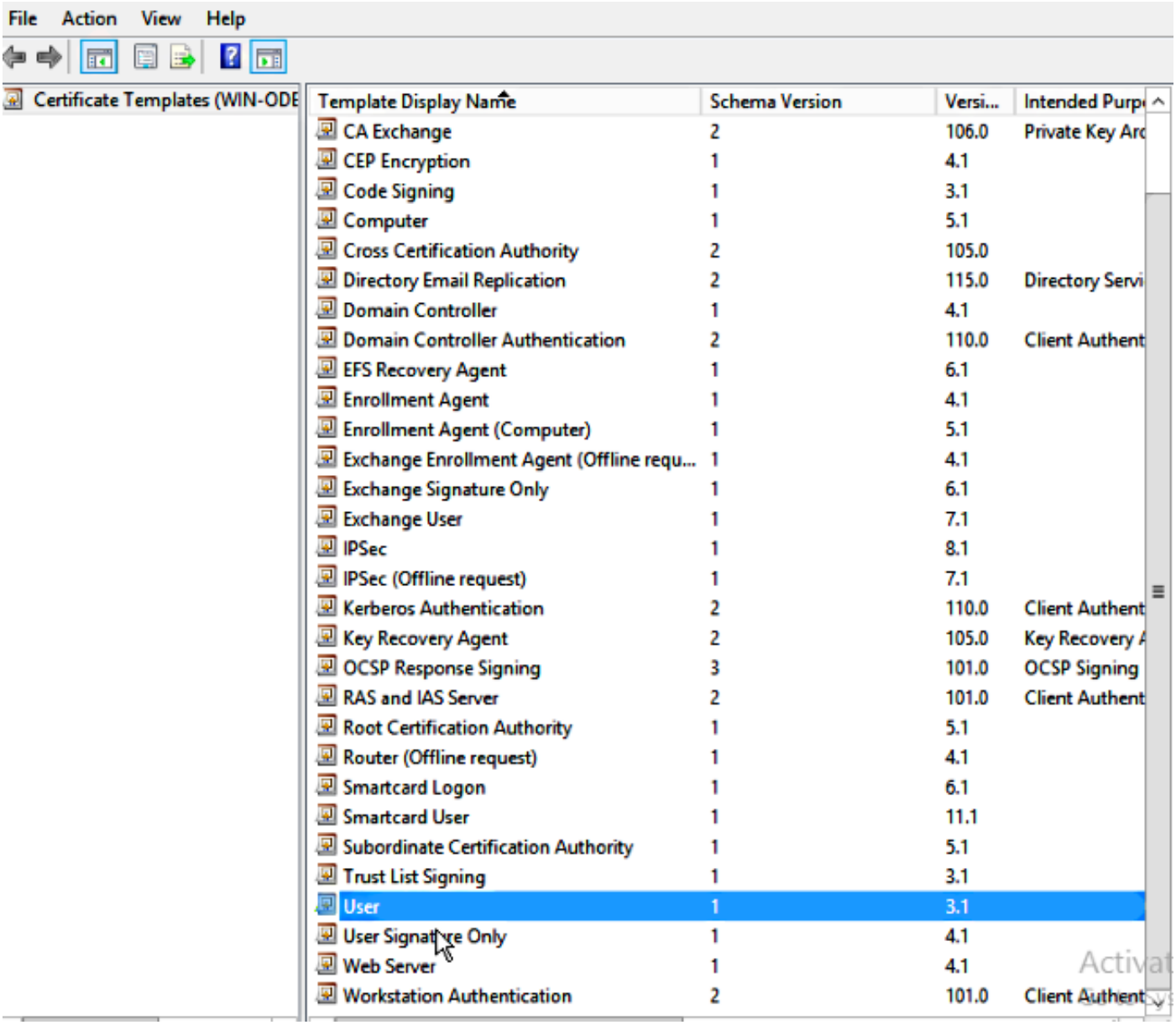
الخطوة 22. انقر على قائمة Microsoft Windows/Start.

الخطوة 23. اكتب MMC.

الخطوة 24. في قائمة ملف، أختر إضافة/إزالة إضافة. أختر مرجع مصدق.

الخطوة 25. انقر بزر الماوس الأيمن فوق مجلد قالب الشهادة وانقر فوق إدارة.

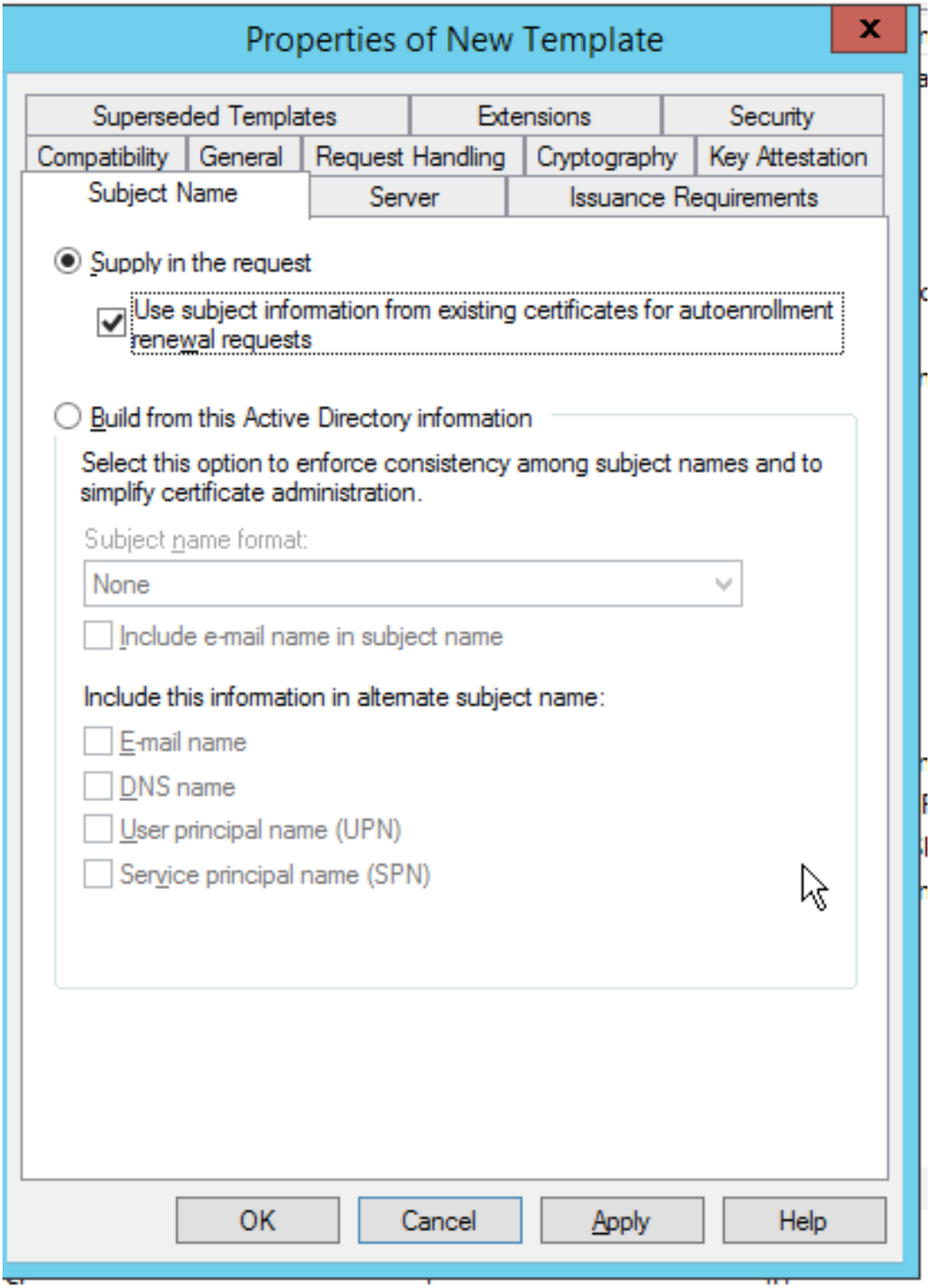
الخطوة 26. انقر بزر الماوس الأيمن فوق قالب موجود، مثل المستخدم، واختر مضاعفة قالب.



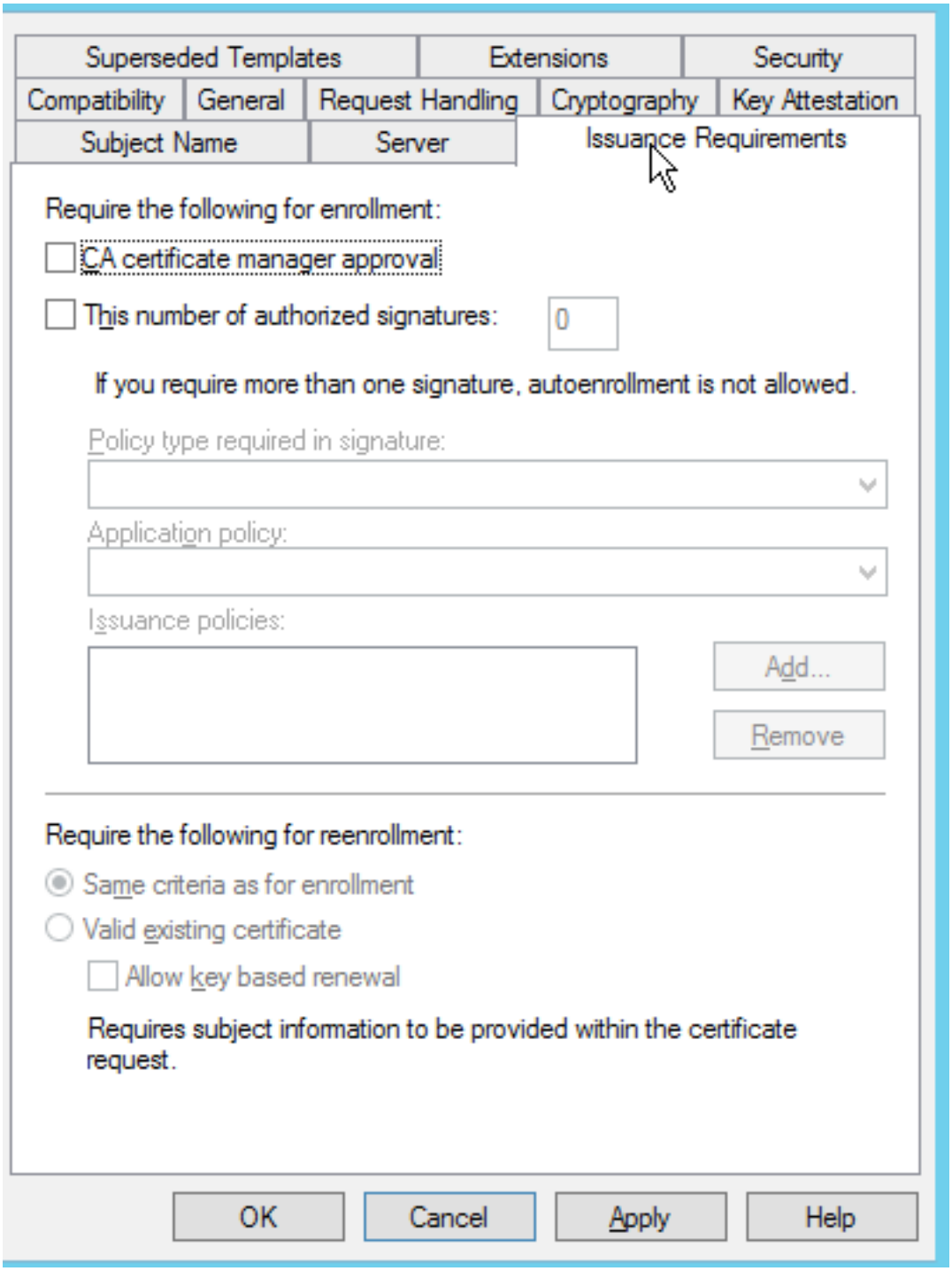
الخطوة 27. أختر المرجع المصدق ليكون Microsoft Windows 2012 R2.

الخطوة 28. في علامة التبويب "عام"، أضف اسم عرض مثل WLC وفترة صلاحية.

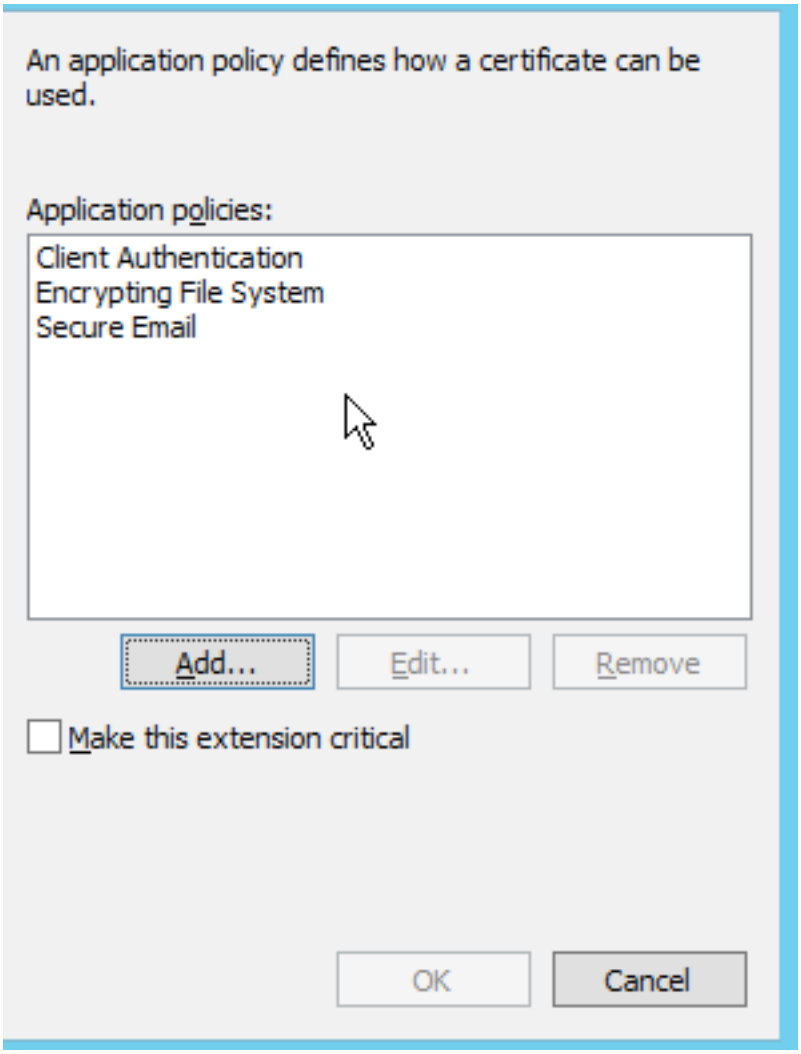
الخطوة 29. في علامة التبويب اسم الموضوع، تأكد من تحديد **التوريد في الطلب**.



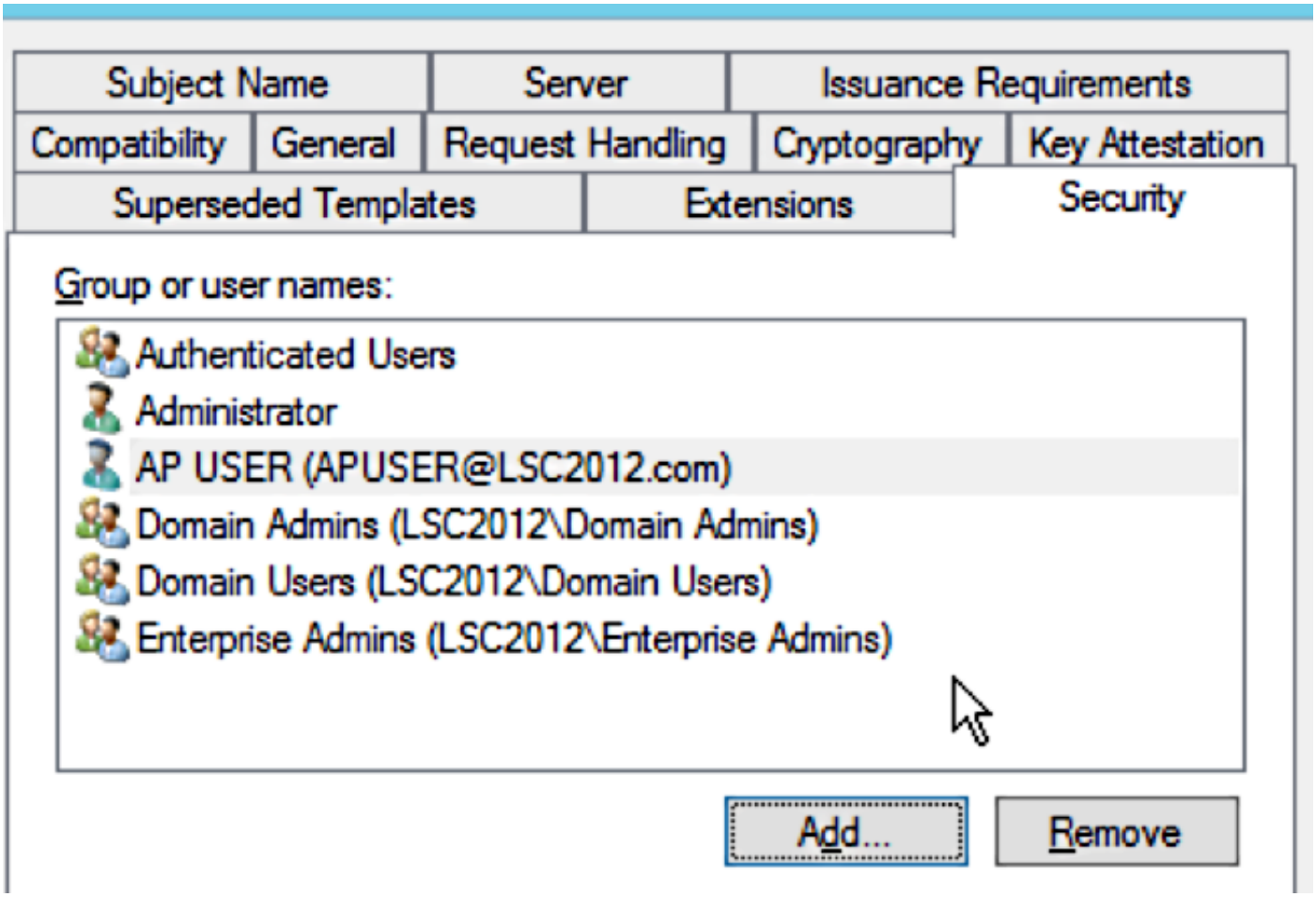
الخطوة 30. انقر فوق علامة التبويب متطلبات الإصدار. توصي Cisco بترك سياسات الإصدار فارغة في بيئة CA هرمية نموذجية:



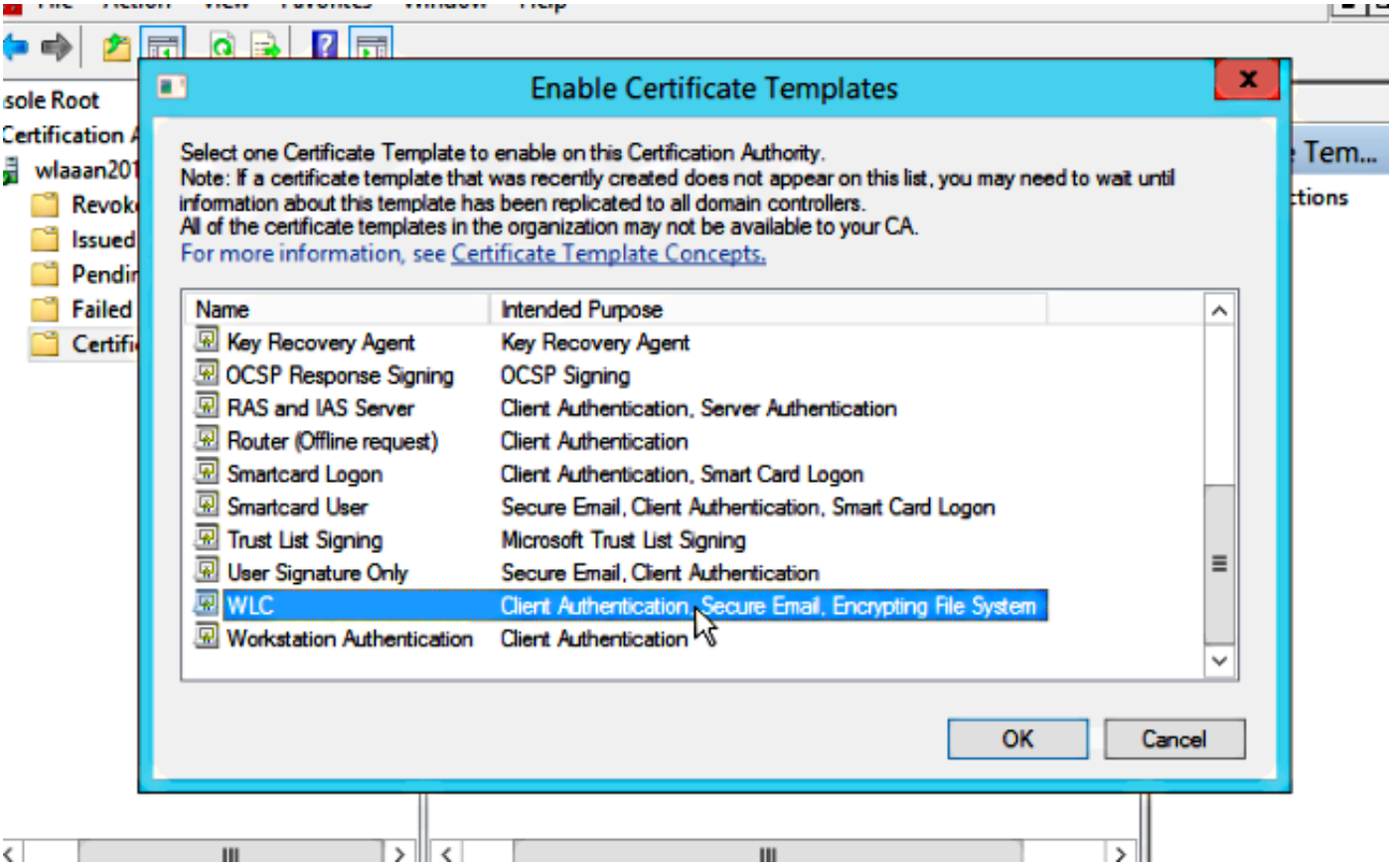
الخطوة 31. انقر فوق علامة التبويب الملحقات ونهج التطبيق، ثم **تحرير**. انقر فوق **إضافة**، وتأكد من إضافة مصادقة العميل كنهج تطبيق. وانقر فوق **OK**.



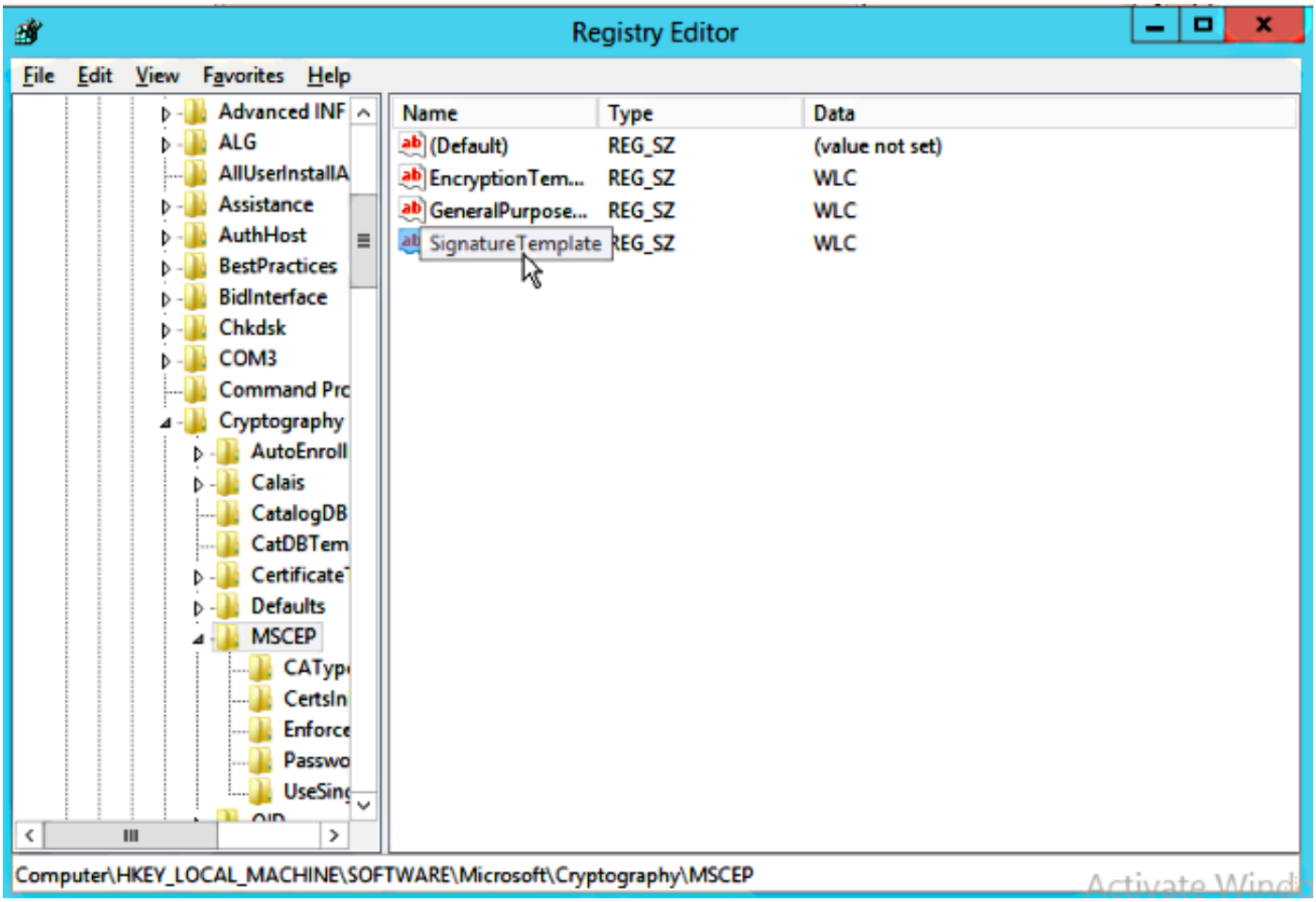
الخطوة 32. انقر فوق عالمة التبويب أمان، ثم انقر فوق **إضافة...** تأكد من أن حساب خدمة SCEP المحدد في تثبيت خدمة NDES له تحكم كامل بالقالب، وانقر فوق **موافق**.



الخطوة 33. العودة إلى واجهة واجهة المستخدم الرسومية (GUI) الخاصة بمرجع التصديق. انقر بزر الماوس الأيمن فوق **دليل قوالب الشهادات**. انتقل إلى **جديد > قالب الشهادة المراد إصداره**. حدد قالب WLC الذي تم تكوينه مسبقا، وانقر فوق **موافق**.



الخطوة 34. قم بتغيير قالب SCEP الافتراضي في إعدادات السجل تحت الكمبيوتر > HKEY_LOCAL_MACHINE > برنامج > Microsoft > تشفير > MSCEP. قم بتغيير مفاتيح EncryptionTemplate و GeneralPurposeTemplate و SignatureTemplate من IPsec (طلب دون اتصال) إلى قالب WLC الذي تم إنشاؤه مسبقًا.



الخطوة 35. أعد تمهيد النظام.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

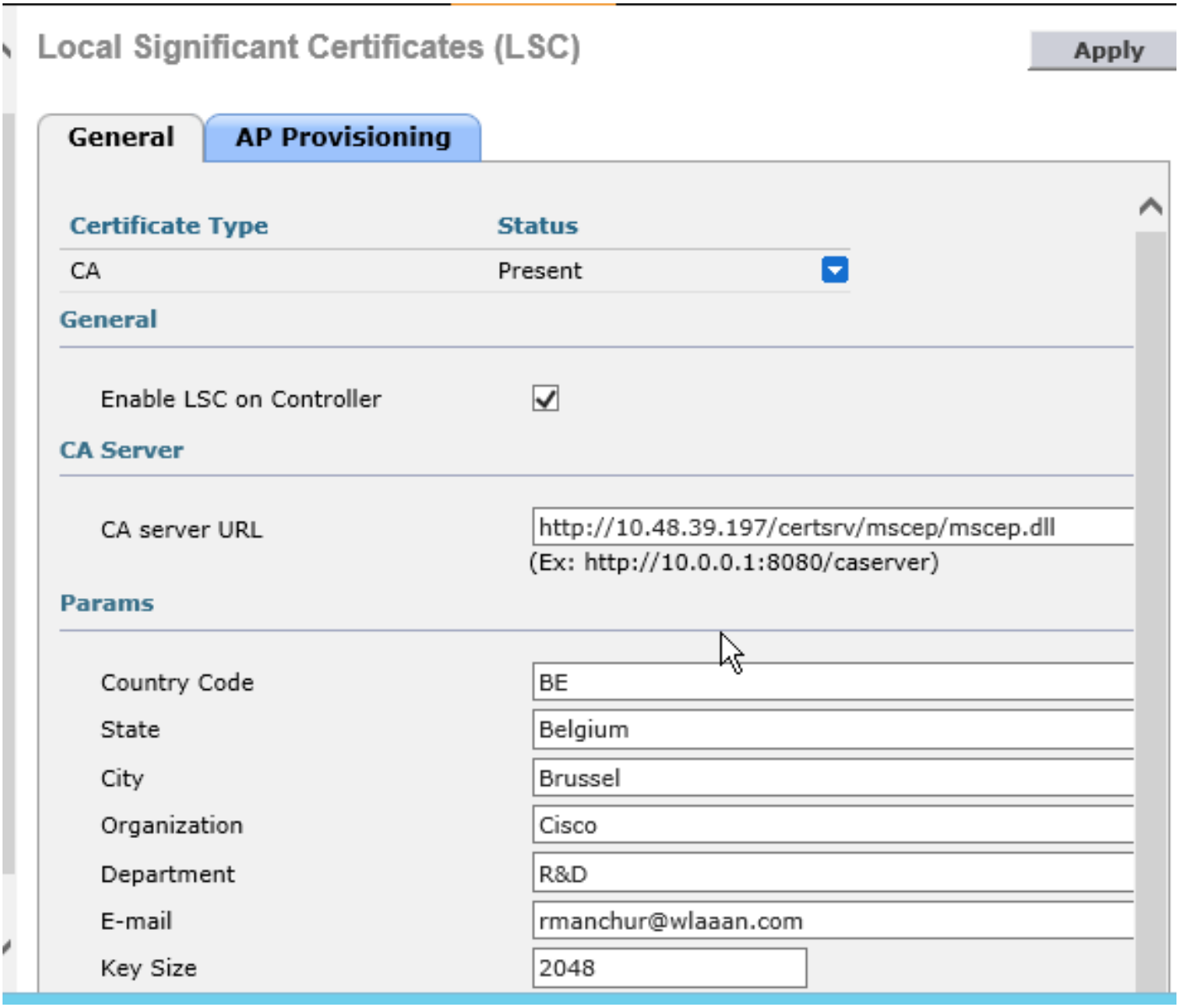
الخطوة 1. على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى قائمة الأمان. انقر على **شهادات > LSC**.

الخطوة 2. حدد خانة الاختيار **تمكين LSC في وحدة التحكم**.

الخطوة 3. أدخل عنوان URL الخاص بـ Microsoft Windows Server 2012. وبشكل افتراضي، يتم إلحاقه بـ **/certsrv/mscep/mscep.dll**.

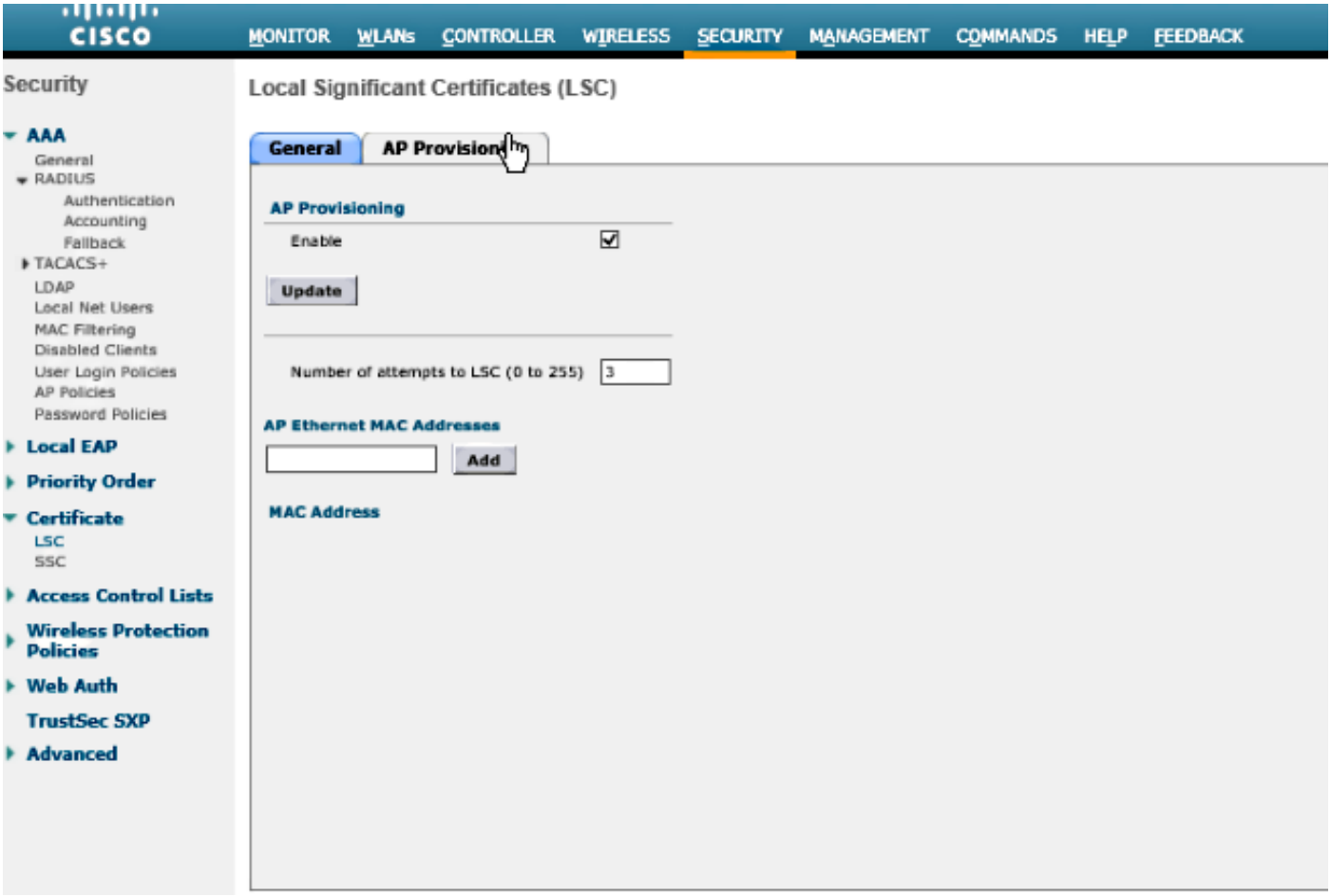
الخطوة 4. أدخل التفاصيل الخاصة بك في قسم **Params**.

الخطوة 5. تطبيق التغيير.



الخطوة 6. انقر فوق السهم الأزرق الموجود على سطر CA العلوي واختر **إضافة**. يجب أن تغير الحالة من **غير موجود** إلى **موجود**.

الخطوة 7. انقر فوق علامة التبويب توفير نقطة الوصول".



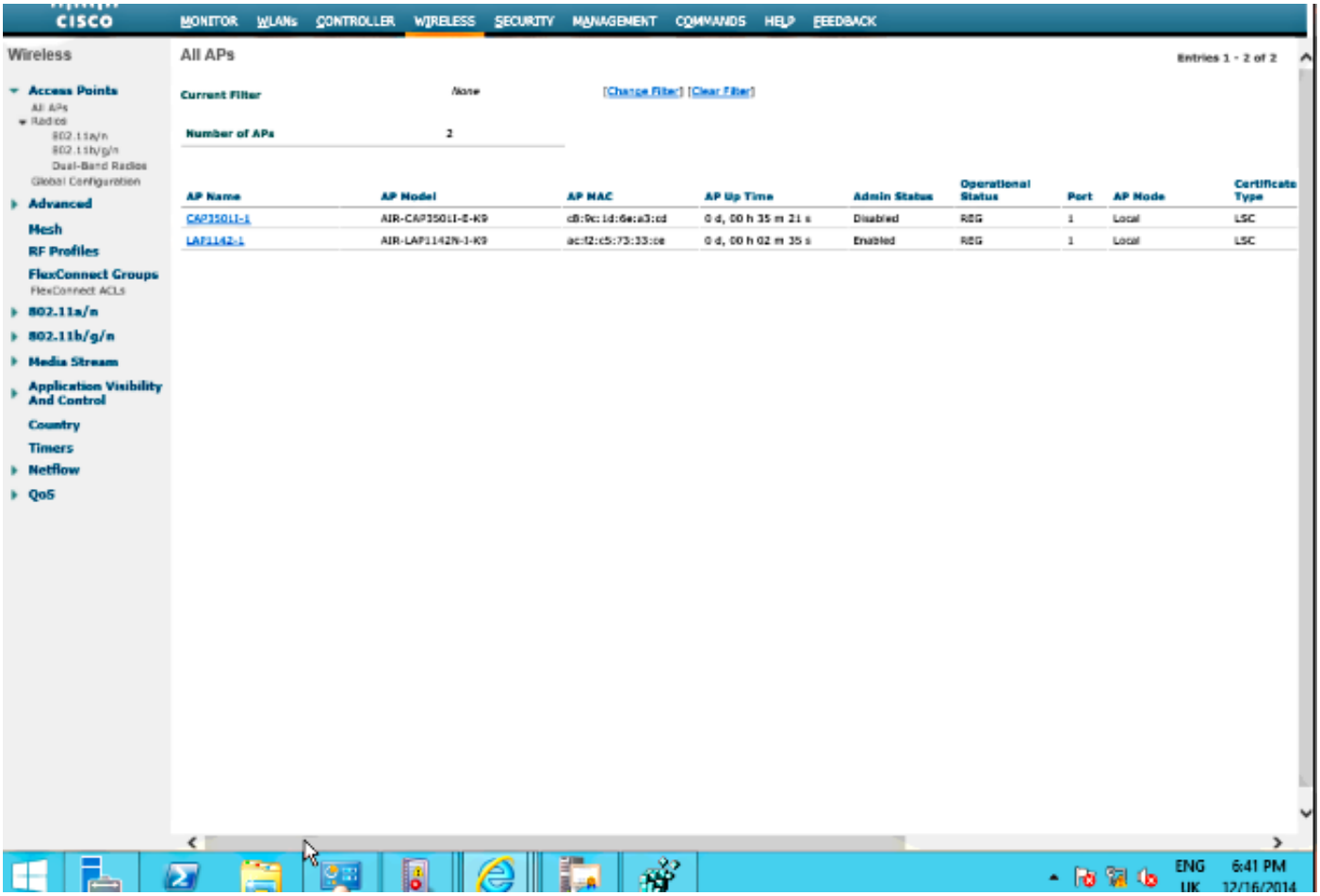
الخطوة 8. حدد خانة الاختيار **enable** ضمن توزيد AP وانقر **تحديث**.

الخطوة 9. قم بإعادة تشغيل نقاط الوصول إذا لم تكن قد قامت بإعادة تشغيل نفسها.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تتضمن نقطة الوصول، بعد إعادة التشغيل، إلى الخلف وتعرض مع LSC كنوع الشهادة في القائمة اللاسلكية.



ملاحظة: بعد 8.3.112، لا يمكن لنقاط الوصول إلى MIC الانضمام على الإطلاق بمجرد تمكين LSC. لذلك تصبح ميزة التعداد "محاولات الوصول إلى LSC" ذات إستخدام محدود.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).