تكوين دعم HTTPS لمكالمات ISE SCEP

المحتويات

المقدمة

يصف هذا المستند الخطوات المطلوبة لتكوين دعم بروتوكول نقل النص التشعبي الآمن (HTTPS) لتكامل بروتوكول تسجيل الشهادة الآمن (SCEP) مع محرك خدمات الهوية (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بخادم ويب لخدمات معلومات الإنترنت (IIS) من Microsoft
- الخبرة في تكوين SCEP والشهادات على ISE

المكونات المستخدمة

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

- ISE الإصدار x.1.1
- Windows Server 2008 R2 Enterprise مع تثبيت الإصلاحات العاجلة ل KB2483564 وKB2633200

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

يتم توفير المعلومات المتعلقة بخدمات شهادات Microsoft كدليل خاص ب Cisco Bring your your device (BYOD)). ارجع إلى TechNet من Microsoft كمصدر نهائي للحقيقة الخاصة بهيئة شهادة Microsoft وخدمة تسجيل أجهزة الشبكة (NDES) وتكوينات الخوادم ذات الصلة SCEP.

معلومات أساسية

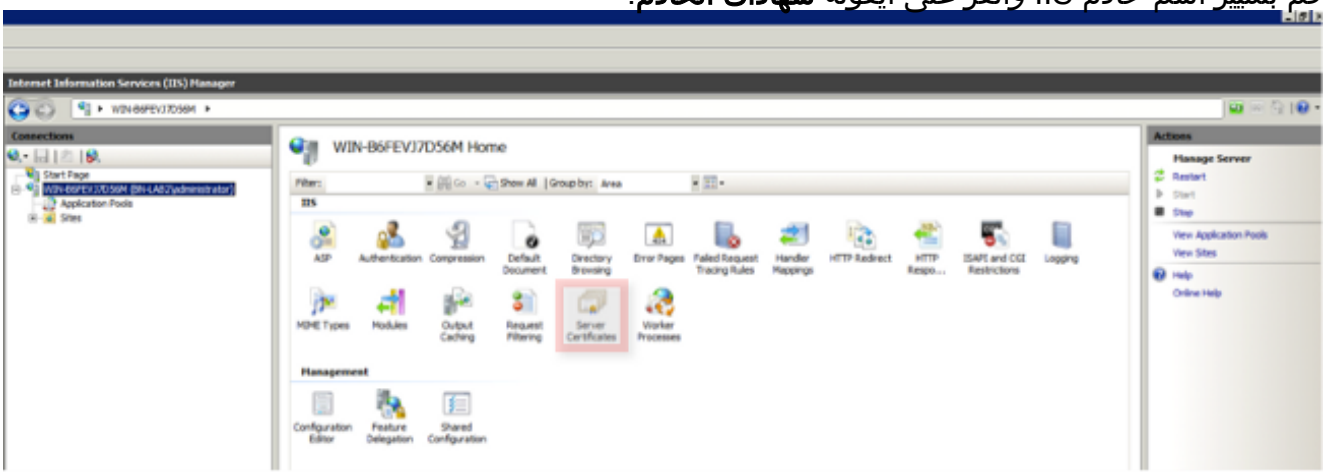
في نشر BYOD، يكون أحد المكونات الأساسية هو خادم Microsoft 2008 R2 Enterprise المثبت عليه دور NDES. هذا الخادم عضو في غابة Active Directory (AD). أثناء التثبيت الأولي ل NDES، يتم تثبيت خادم ويب IIS الخاص ب Microsoft وتكوينه تلقائيا لدعم إنهاء HTTP ل SCEP. في بعض عمليات نشر BYOD، قد يرغب العملاء في زيادة تأمين الاتصالات بين ISE و NDES باستخدام HTTPS. يوضح هذا الإجراء بالتفصيل الخطوات المطلوبة لطلب شهادة طبقة مأخذ التوصيل الآمنة (SSL) وتثبيتها لموقع SCEP على الويب.

التكوين

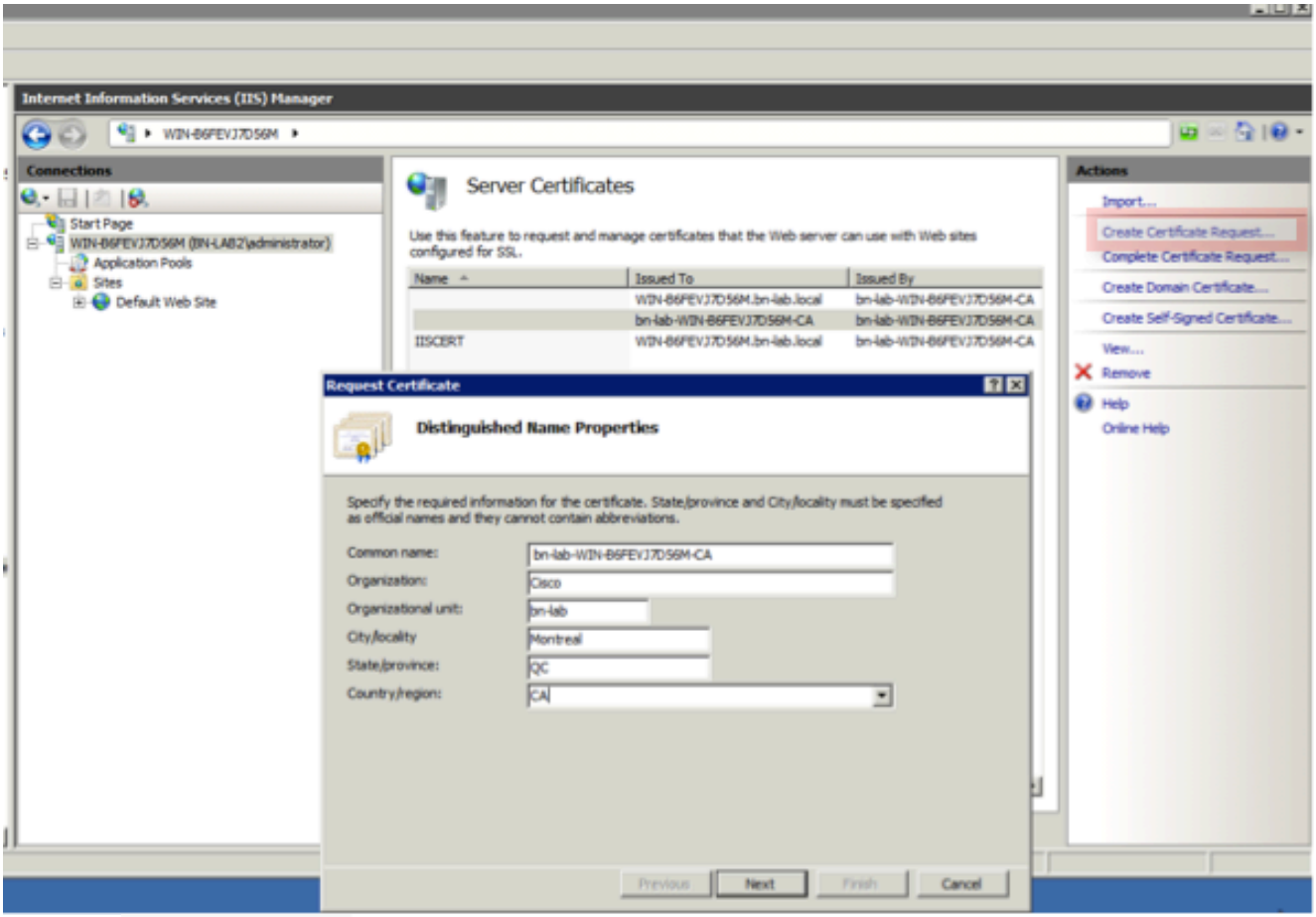
تكوين شهادة خادم NDES

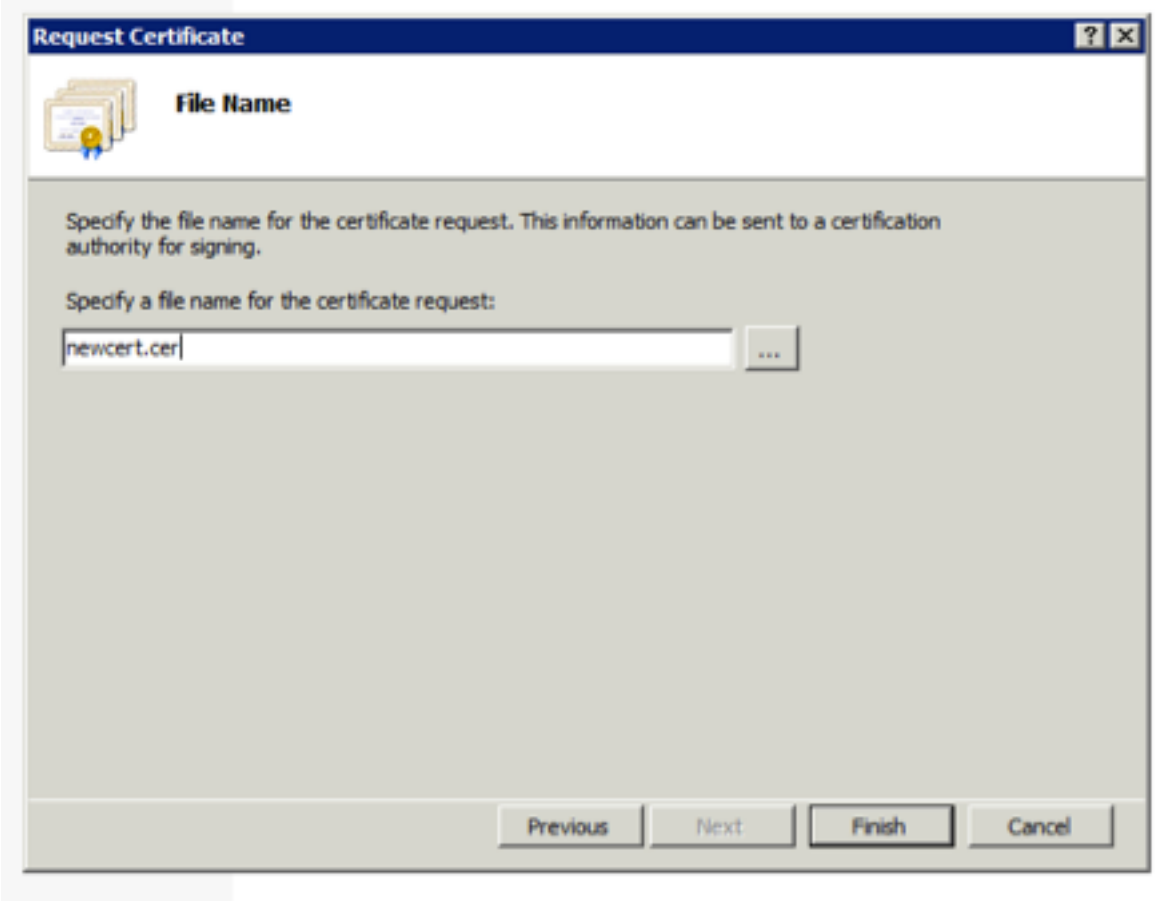
ملاحظة: يجب تكوين شهادة جديدة ل IIS (مطلوبة فقط عندما يتم دمج IIS مع PKI خاص بجهة خارجية مثل Verisign أو عندما يتم فصل أدوار خادم مرجع التصديق (CA) و NDES على خوادم منفصلة). في التثبيت، إذا كان دور NDES على خادم Microsoft CA حالي، يستخدم IIS شهادة هوية الخادم التي تم إنشاؤها أثناء إعداد CA. بالنسبة للتكوينات المستقلة مثل هذا، قم بالتخطي مباشرة إلى قسم **تكوين ربط NDES Server** في هذا المستند.

1. الاتصال بخادم NDES عبر وحدة التحكم أو RDP.
2. انقر على **بدء -> أدوات إدارية -> إدارة خدمات معلومات الإنترنت (IIS)**.
3. قم بتمييز اسم خادم IIS وانقر على أيقونة **شهادات الخادم**.

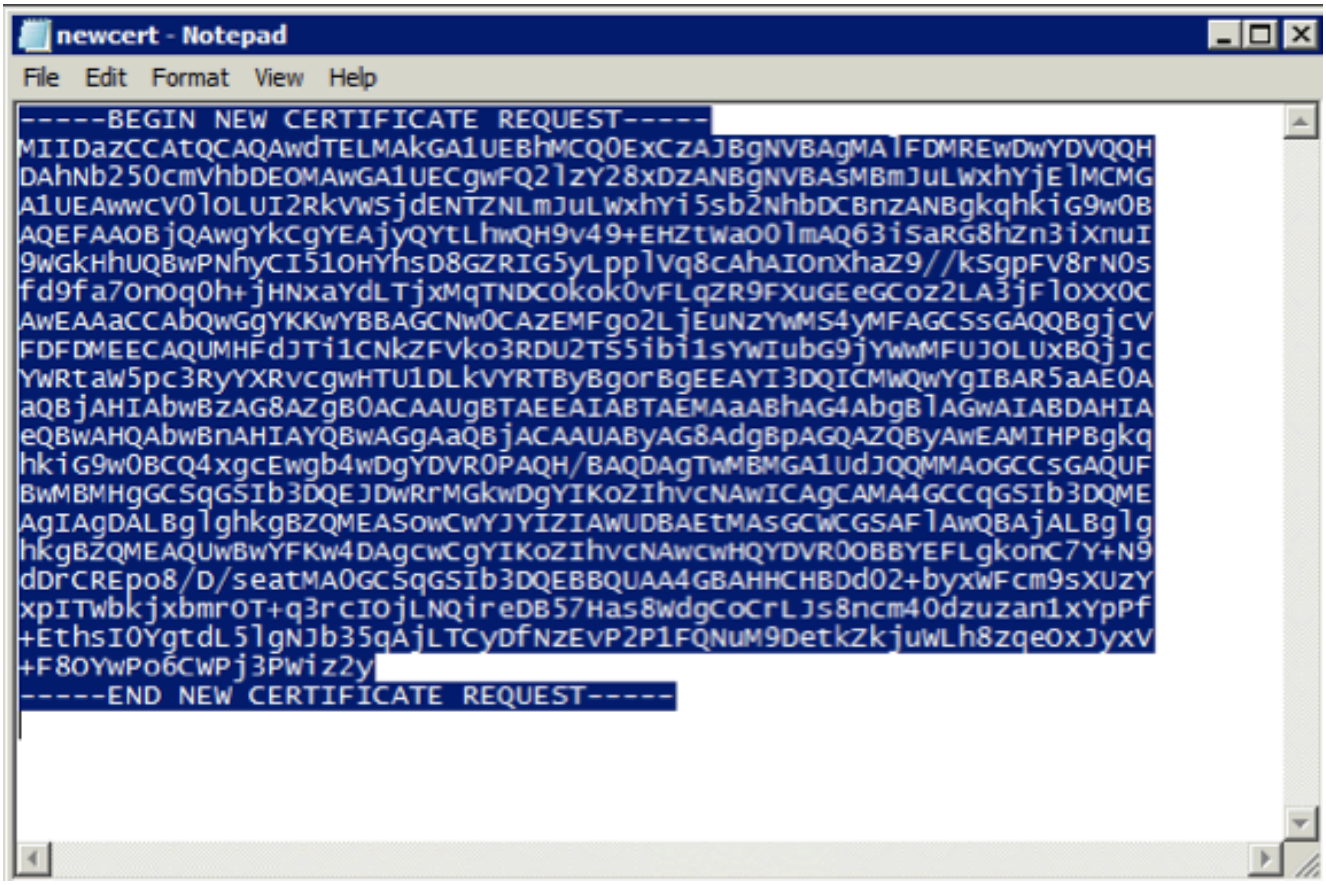


4. انقر على **إنشاء طلب شهادة**، وأكمل الحقول.

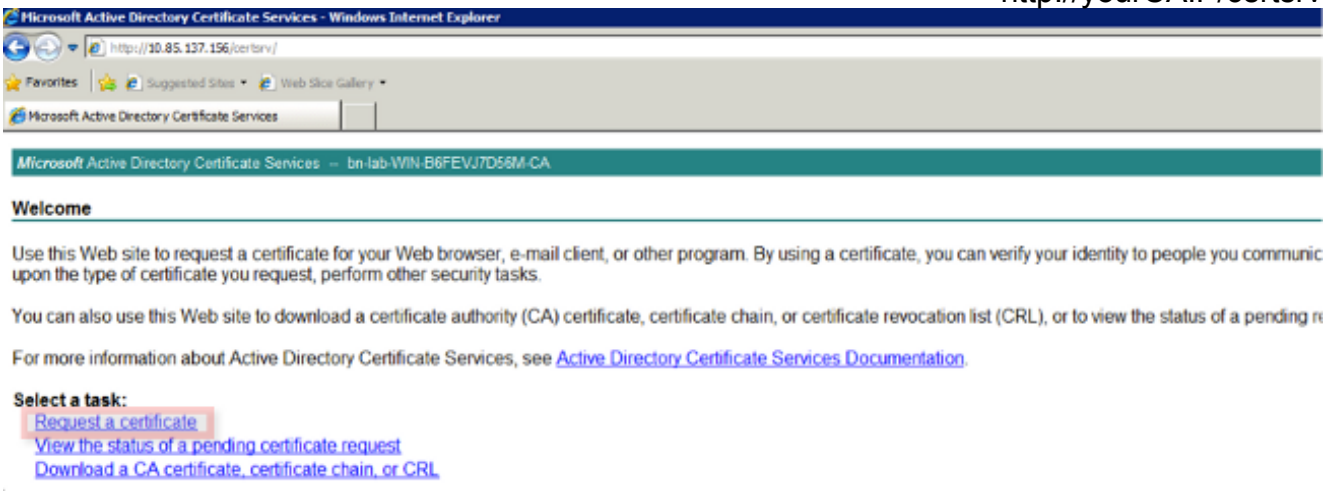




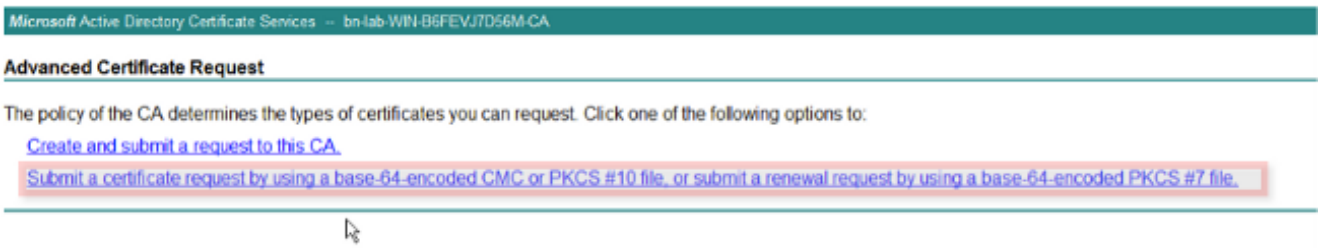
5. افتح ملف .cer الذي تم إنشاؤه في الخطوة السابقة باستخدام محرر نصي وانسخ المحتوى إلى الحافظة.



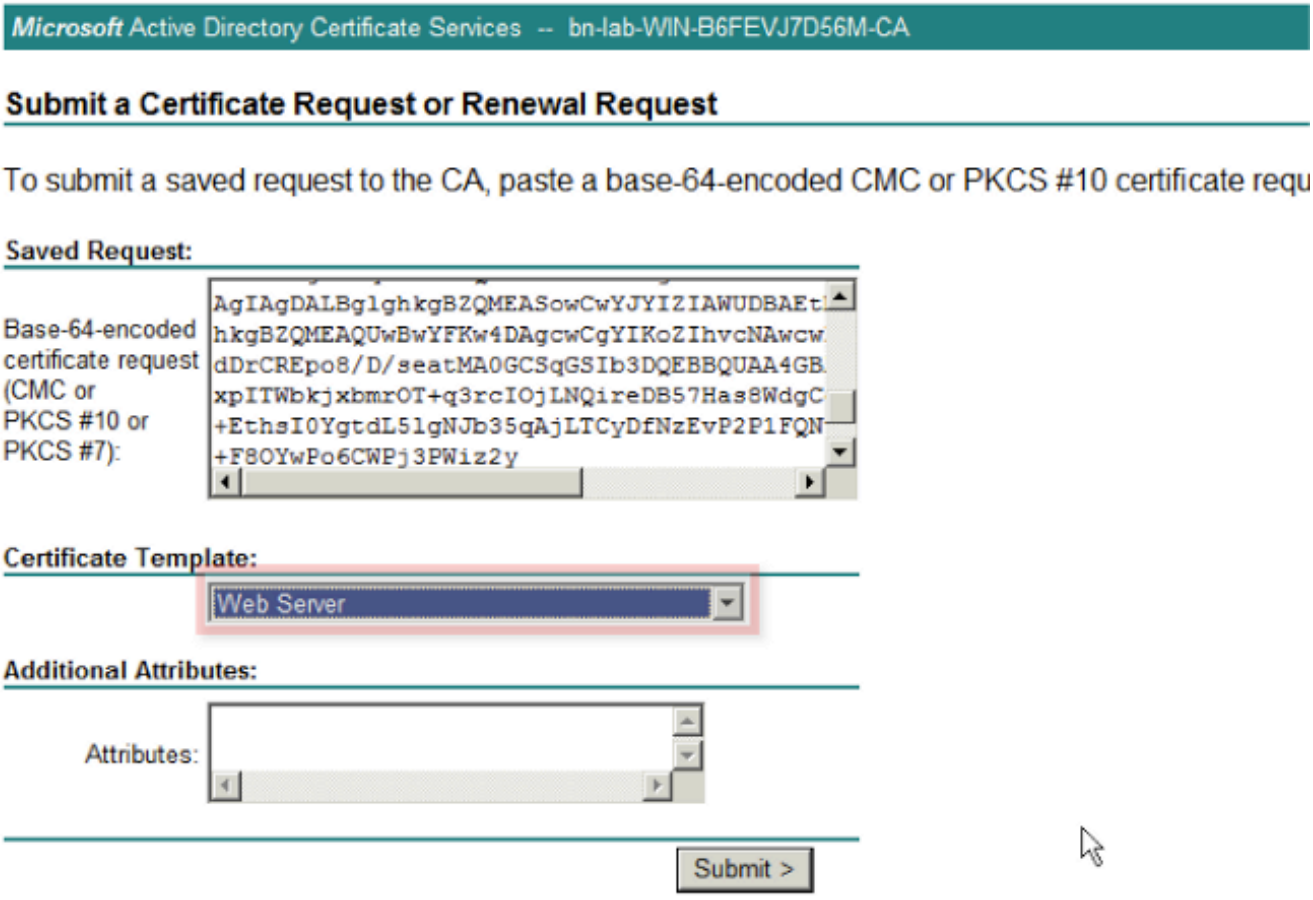
6. قم بالوصول إلى موقع ويب تسجيل Microsoft CA على الويب وانقر فوق **طلب شهادة**.مثال على URL: http://yourCAIP/certsrv



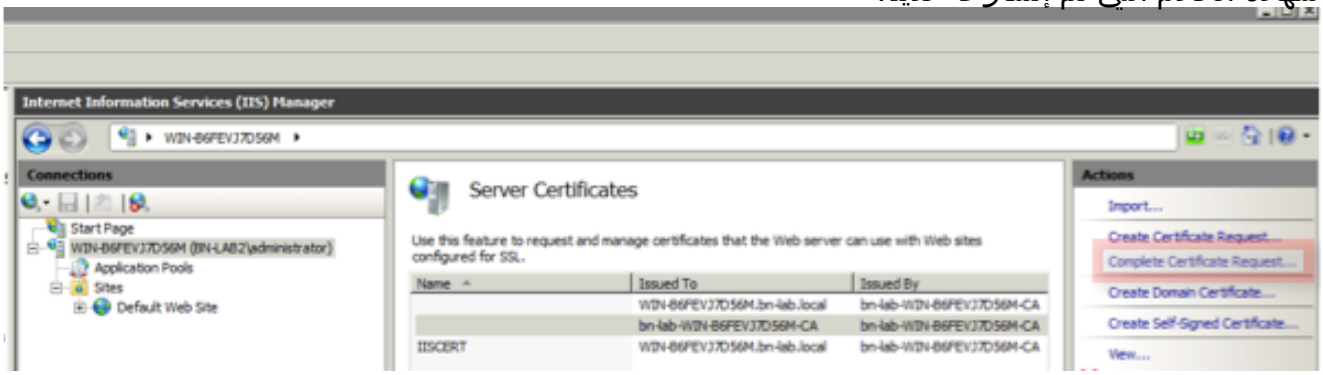
7. انقر على **إرسال طلب شهادة باستخدام...** الصق في محتوى الشهادة من الحافظة، واختر قالب **خادم الويب**.



8. انقر على **إرسال** ثم احفظ ملف الشهادة على سطح المكتب.

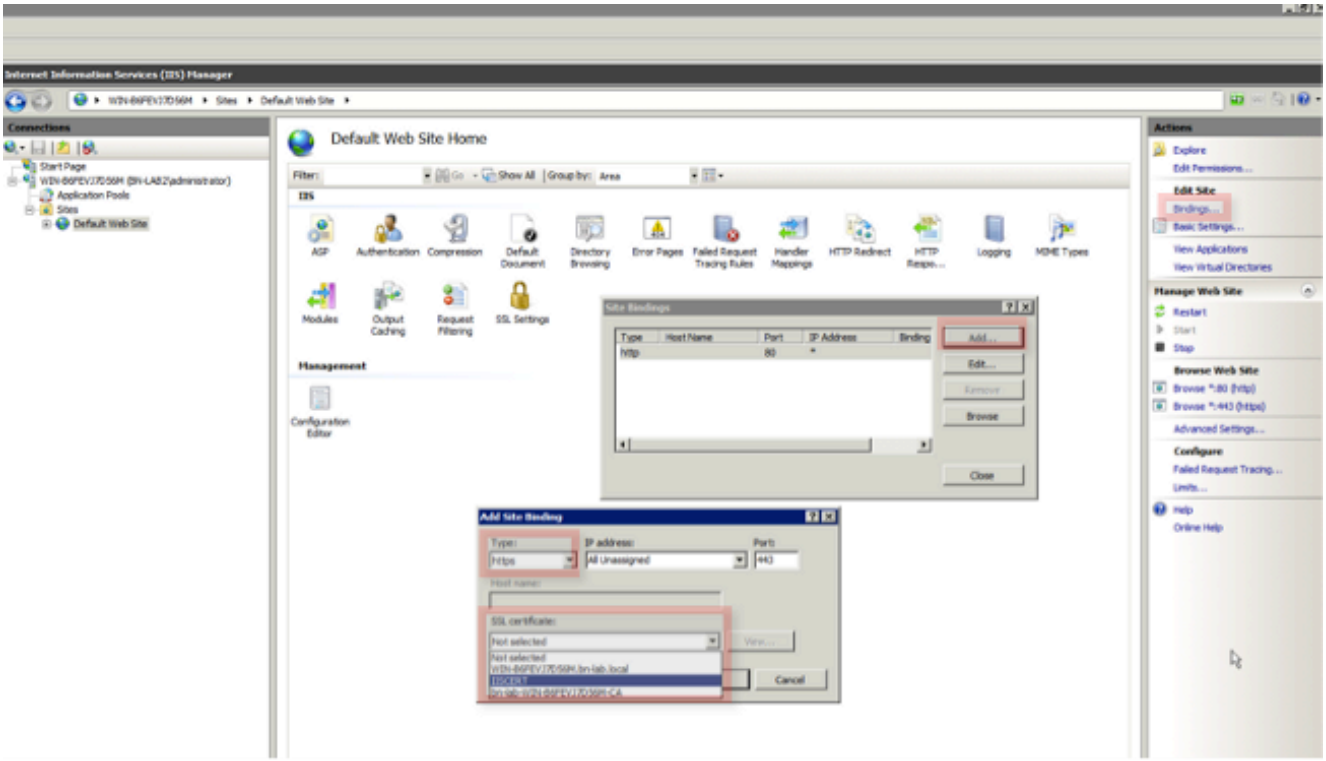


9. ارجع إلى خادم NDES وافتح وحدة إدارة IIS. انقر على اسم الخادم ثم انقر على **إكمال طلب الشهادة** لاستيراد شهادة الخادم التي تم إنشاؤها حديثا.



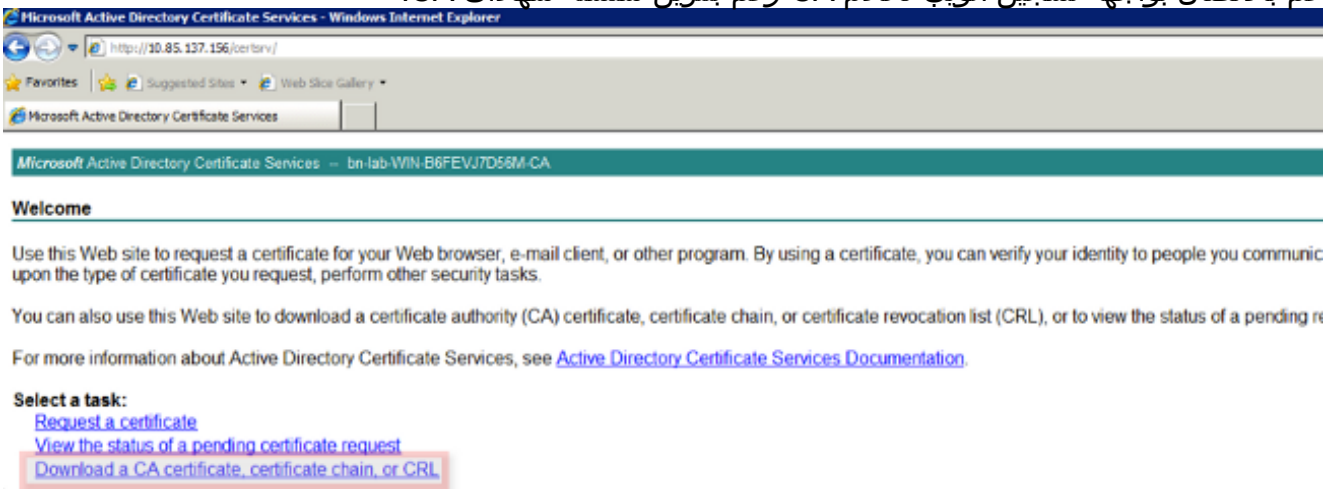
تكوين ربط NDES Server IIS

1. قم بتوسيع **اسم الخادم**، وتوسيع **المواقع**، وانقر فوق **موقع ويب الافتراضي**.
2. انقر فوق **روابط** في الزاوية العلوية اليمنى.
3. انقر فوق **إضافة**، وقم بتغيير TypeTo HTTPS، واختر الشهادة من القائمة المنسدلة.
4. وانقر فوق **OK**.

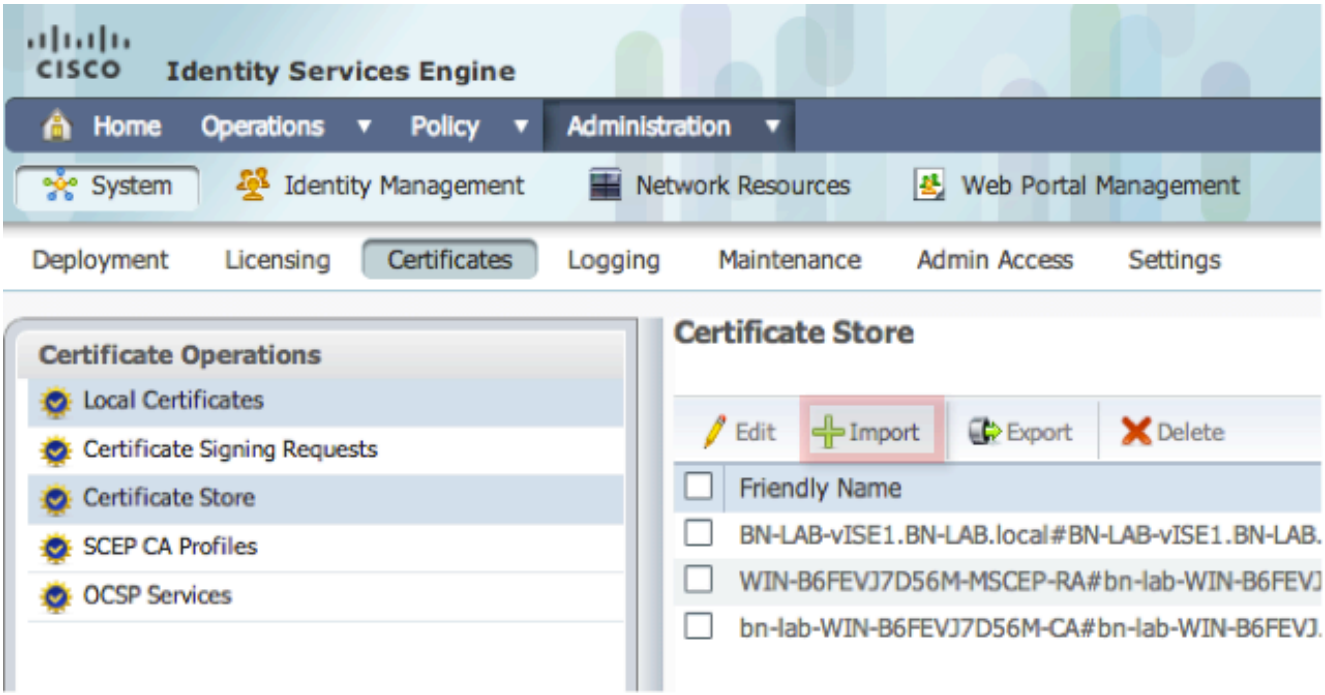


تكوين خادم ISE

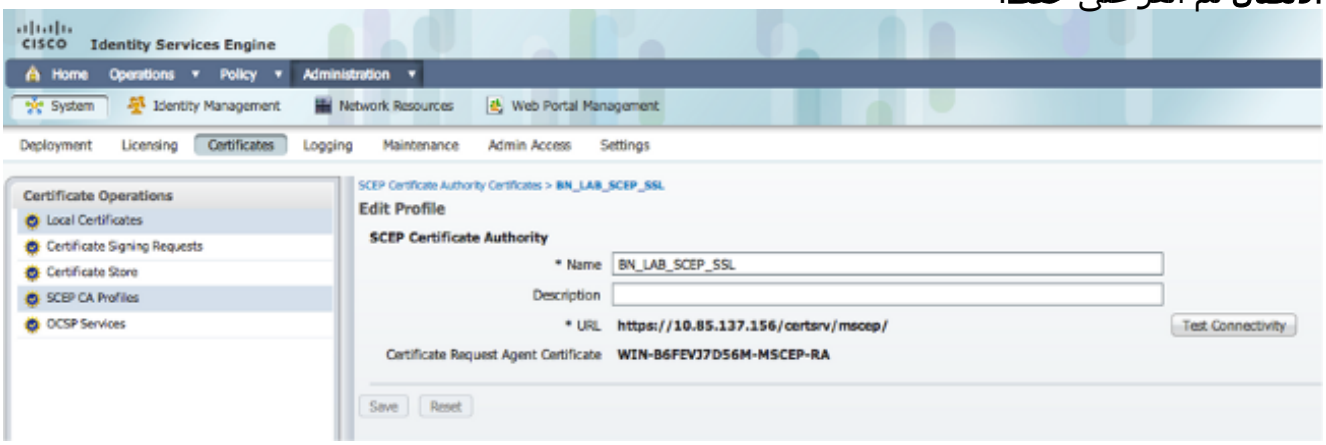
1. قم بالاتصال بواجهة تسجيل الويب لخادم CA وقم بتنزيل سلسلة شهادات CA.



2. من واجهة المستخدم الرسومية ISE، انتقل إلى **الإدارة -> الشهادات -> مخزن الشهادات** واستورد سلسلة شهادات CA إلى مخزن ISE.



3. انتقل إلى **الإدارة -> الشهادات -> توصيفات SCEP CA** وقم بتكوين عنوان URL ل HTTPS. انقر على **إختبار الاتصال** ثم انقر على **حفظ**.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

- انتقل إلى **الإدارة -> الشهادات -> مخزن الشهادات** وتحقق من وجود سلسلة شهادات CA وشهادة هيئة تسجيل خوادم (RA) NDES.
- أستخدم Wireshark أو تفريغ TCP لمراقبة تبادل SSL الأولي بين عقدة مسؤول ISE وخادم NDES.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- قم بتقسيم مخطط شبكة BYOD إلى نقاط طريق منطقية للمساعدة في تحديد نقاط تصحيح الأخطاء والامساك على طول المسار بين نقاط النهاية هذه - ISE و NDES و CA.
- تأكد من السماح ل TCP 443 بشكل ثنائي الإتجاه بين ISE وخادم NDES.

- راقب سجلات تطبيقات خادم CA و NDES لأخطاء التسجيل واستخدم Google أو TechNet للبحث عن تلك الأخطاء.
- أستخدم الأداة المساعدة لتفريغ TCP على ISE PSN وأداة مراقبة حركة مرور البيانات من وإلى خادم NDES. ويوجد هذا ضمن **العمليات > أدوات التشخيص > الأدوات العامة**.
- ركبت Wireshark على ال NDES نادل أو استعملت فسحة بين دعامتين على وسيط مفتاح in order to على قبض SCEP حركة مرور إلى ومن ال ISE PSN.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

معلومات ذات صلة

- تكوين دعم SCEP ل BYOD
- الدعم التقني والمستندات - Cisco Systems

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).