ASA 8.X: مثال تكوين تسجيل SCEP ل AnyConnect

المحتويات

المقدمة

يتم إدخال وظيفة تسجيل SCEP في العميل المستقل AnyConnect 2.4. في هذه العملية، تقوم بتعديل ملف تعريف AnyConnect XML لتضمين تكوين مرتبط ب SCEP وإنشاء ملف تعريف اتصال ونهج مجموعة معين لتسجيل الشهادة. عندما يتصل مستخدم AnyConnect بهذه المجموعة المحددة، يرسل AnyConnect طلب تسجيل شهادة إلى خادم CA، ويقبل خادم CA الطلب أو يرفضه تلقائيا.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco التي تشغل الإصدار x.8 من البرنامج
- Cisco AnyConnect VPN، الإصدار 2.4

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يتمثل الهدف من تسجيل SCEP التلقائي ل AnyConnect في إصدار شهادة إلى العميل بطريقة آمنة وقابلة للتطوير. على سبيل المثال، لا يحتاج المستخدمون إلى طلب شهادة من خادم CA. يتم دمج هذه الوظيفة في عميل AnyConnect. تصدر الشهادات إلى العملاء بناء على معلمات الشهادة المذكورة في ملف تعريف XML.

نظرة عامة على التغييرات المطلوبة

تتطلب ميزة تسجيل SCEP ل AnyConnect تحديد معلمات شهادة معينة في ملف تعريف XML. يتم إنشاء ملف تعريف "نهج المجموعة" و"الاتصال" في ASA لتسجيل الشهادة، ويقترن ملف تعريف XML بهذا النهج. يتصل عميل AnyConnect بملف تعريف الاتصال الذي يستخدم هذا النهج المحدد ويرسل طلبا للحصول على شهادة مع المعلمات المحددة في ملف XML. تقبل جهة منح الشهادة (CA) الطلب أو ترفضه تلقائيا. يسترجع عميل AnyConnect الشهادات باستخدام بروتوكول SCEP إذا كان عنصر <CertificateSCEP> محددا في ملف تعريف العميل.

يجب أن تفشل مصادقة شهادة العميل قبل أن يحاول AnyConnect إسترداد الشهادات الجديدة تلقائيا، لذلك إذا كان لديك شهادة صالحة مثبتة بالفعل، فلن يحدث التسجيل.

عند تسجيل دخول المستخدمين إلى مجموعة معينة، يتم تسجيلهم تلقائيا. هناك أيضا طريقة يدوية متاحة لاسترجاع الشهادة حيث يتم تقديم المستخدمين مع زر **الحصول على شهادة**. وهذا لا يعمل إلا عندما يكون لدى العميل وصول مباشر إلى خادم CA، وليس من خلال النفق.

راجع دليل مسؤول عميل AnyConnect VPN، الإصدار 2.4 من Cisco للحصول على مزيد من المعلومات.

إعدادات XML لتمكين ميزة SCEP في AnyConnect

هذه هي العناصر المهمة التي يلزم تعريفها في ملف AnyConnect XML. راجع دليل مسؤول عميل AnyConnect VPN، الإصدار 2.4 من Cisco للحصول على مزيد من المعلومات.

- <AutoSCEPHost>—يحدد اسم مضيف ASA وملف تعريف الاتصال (مجموعة النفق) الذي تم تكوين إسترداد شهادة SCEP له. يجب أن تكون القيمة بتنسيق اسم المجال المؤهل بالكامل لاسم ملف تعريف ASA\Connection أو عنوان IP الخاص باسم ملف تعريف ASA\Connection.
- <CAURL>—يحدد خادم SCEP CA.
- <certificateSCEP>—يحدد كيفية طلب محتويات الشهادة.
- <DisplayGetCertButton>—يحدد ما إذا كانت واجهة المستخدم الرسومية (GUI) ل AnyConnect تعرض الزر الحصول على الشهادة. وهو يمكن المستخدمين من طلب تجديد الشهادة أو توفيرها يدويا.

هنا مثال لملف تخصيص:

```
<?"xml version="1.0" encoding="UTF-8?>
"/AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding>
"xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
<"xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
```

```
                                        <CertificateStore>All</CertificateStore>
                                    <CertificateStoreOverride>false</CertificateStoreOverride>
                                        <ProxySettings>Native</ProxySettings>
                  <AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
                    <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
                        <LocalLanAccess UserControllable="true">false</LocalLanAccess>
                                      AutoReconnect UserControllable="false">true>
                                  <"AutoReconnectBehavior UserControllable="false">
                                                ReconnectAfterResume
                                             <AutoReconnectBehavior/>
                                                    <AutoReconnect/>
                              <AutoUpdate UserControllable="false">true</AutoUpdate>
                                    <"RSASecurIDIntegration UserControllable="false">
                                                      Automatic
                                           <RSASecurIDIntegration/>
                    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
                    <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
                                    <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
                                  PPPExclusion UserControllable="false">Automatic>
  <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
                                                    <PPPExclusion/>
       <EnableScripting UserControllable="false">false</EnableScripting>
                                                <CertificateEnrollment>
        <AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
                                        <"CAURL PromptForChallengePW="false>
                                http://10.11.11.1/certsrv/mscep/mscep.dll
                                                       <CAURL/>
                                                <CertificateSCEP>
                                            <Name_CN>cisco</Name_CN>
                                        <Company_O>Cisco</Company_O>
                                <DisplayGetCertButton>true</DisplayGetCertButton>
                                                <CertificateSCEP/>
                                            <CertificateEnrollment/>
                                             <ClientInitialization/>
                                                      <ServerList>
                                                       <HostEntry>
                                    <HostName>asa2.cisco.com</HostName>
                                                      <HostEntry/>
                                                    <ServerList/>
                                                <AnyConnectProfile/>
```

تكوين ASA لدعم بروتوكول SCEP ل AnyConnect

من أجل توفير الوصول إلى سلطة تسجيل خاصة (RA)، يجب على مسؤول ASA إنشاء اسم مستعار يحتوي على قائمة التحكم في الوصول (ACL) التي تقيد اتصال الشبكة الجانبية الخاصة ب RA المرغوب. لاسترداد شهادة تلقائيا، يتصل المستخدمون بهذا الاسم المستعار ويصادقون عليه.

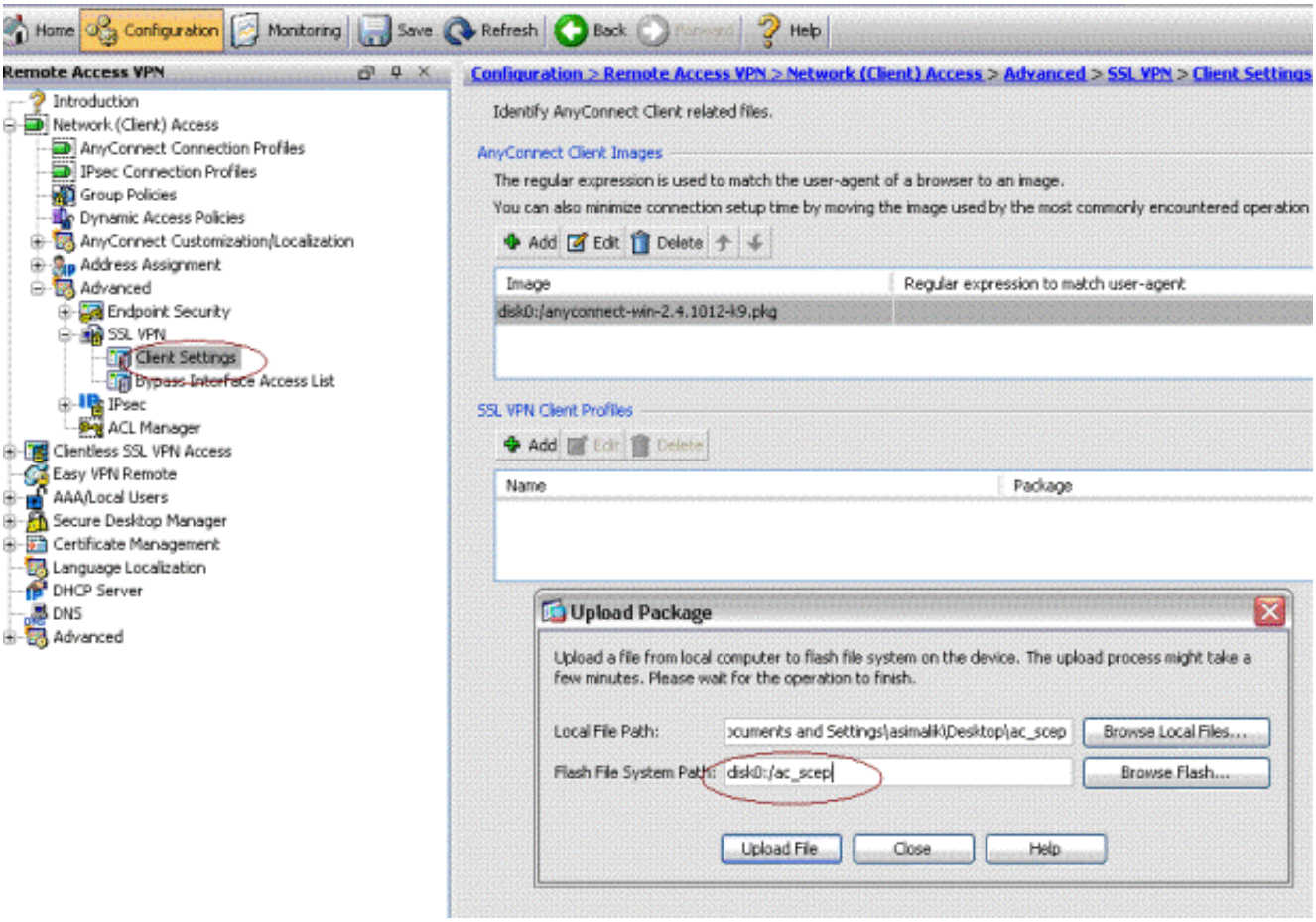
أكمل الخطوات التالية:

1. قم بإنشاء اسم مستعار على ASA للإشارة إلى المجموعة التي تم تكوينها بشكل محدد.
2. حدد الاسم المستعار في عنصر <AutomaticSCEPHost> في ملف تعريف العميل الخاص بالمستخدم.
3. قم بإرفاق ملف تعريف العميل الذي يحتوي على قسم <CertificateEnrollment> بالمجموعة المحددة التي تم تكوينها.
4. قم بتعيين قائمة تحكم في الوصول (ACL) للمجموعة التي تم تكوينها بشكل محدد لتقييد حركة المرور إلى RA الخاصة.

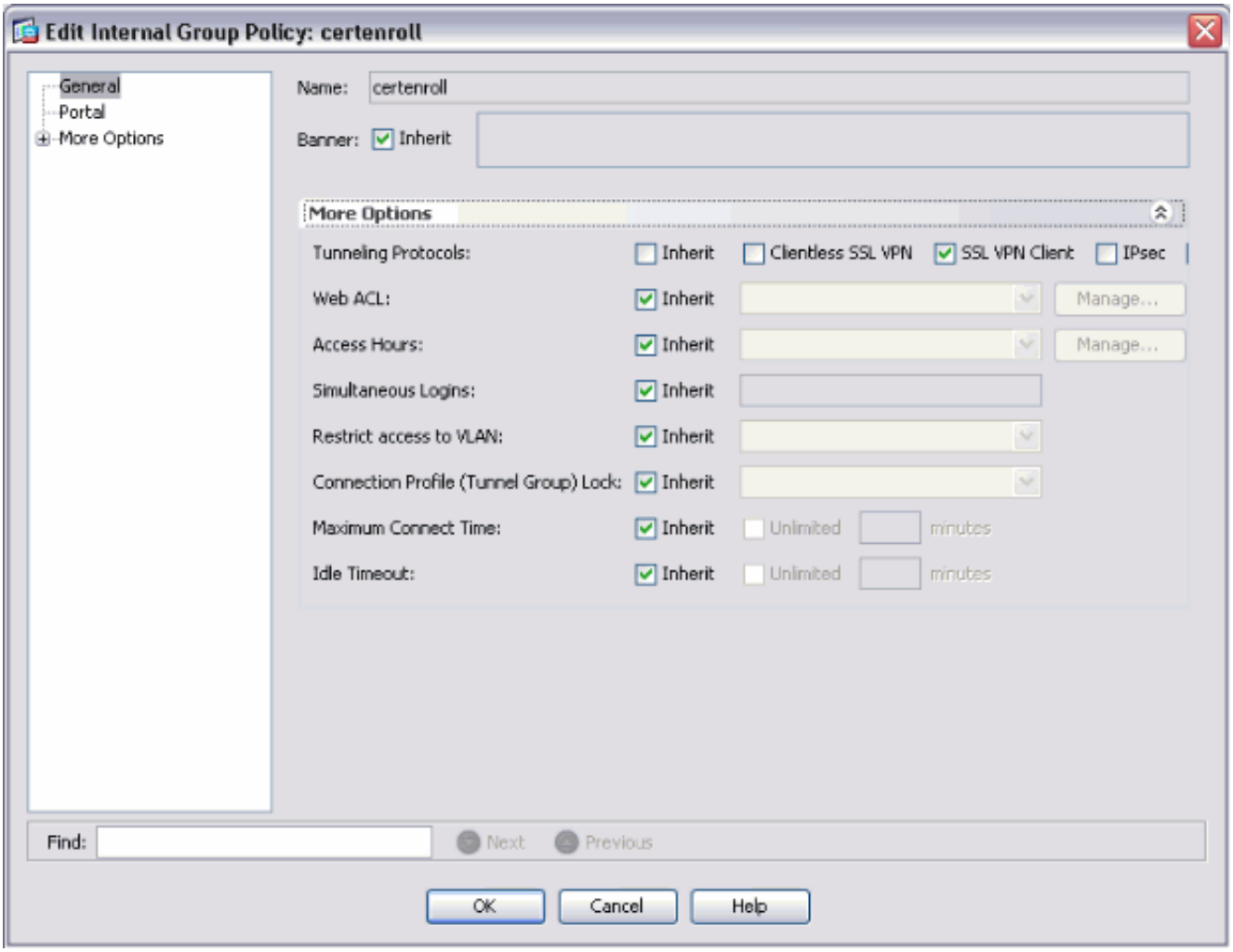
أكمل الخطوات التالية:

1. تحميل ملف تعريف XML إلى ASA.أخترت **Remote Access VPN > شبكة (زبون) منفذ > متقدم > SSL**

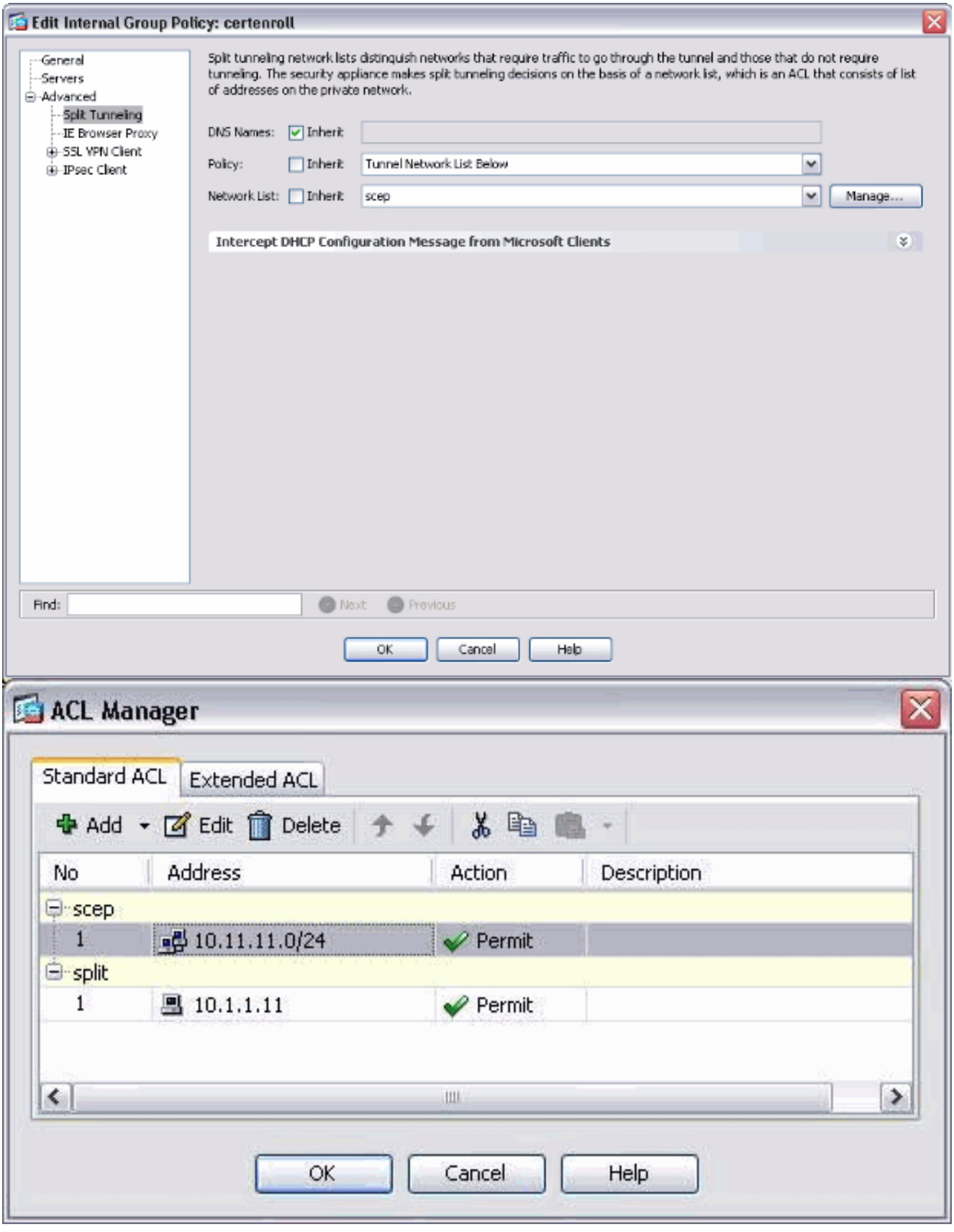
VPN>زبون عملية إعداد.تحت SSL VPN Client Profile، انقر فوق **إضافة**.انقر **تصفح الملفات المحلية** لتحديد ملف التخصيص، وانقر **تصفح Flash** لتحديد اسم ملف Flash.انقر فوق **تحميل الملف**.



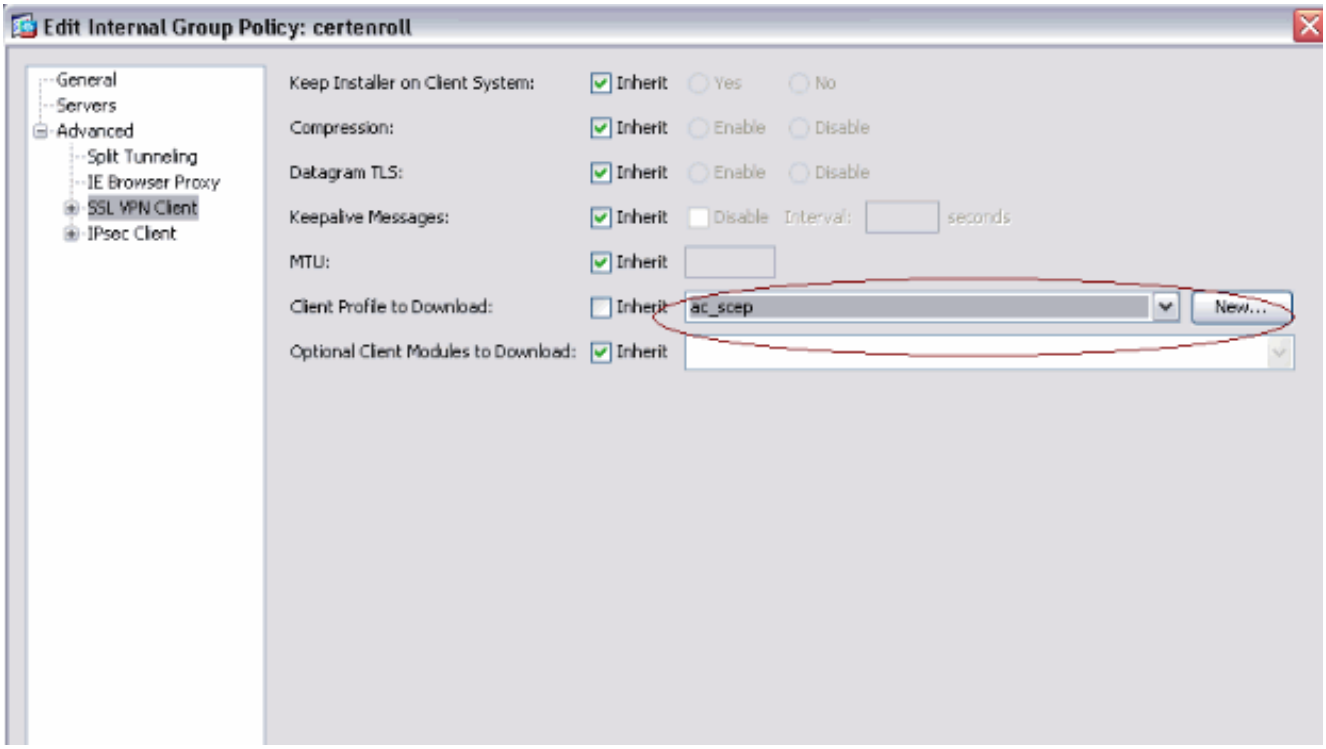
2. إعداد نهج مجموعة Certenroll لتسجيل الشهادة.أختر **Remote Access VPN (الوصول عن بعد) > Network Client Access (وصول عميل الشبكة) > Group Policy (نهج المجموعة)**، وانقر فوق **Add**.



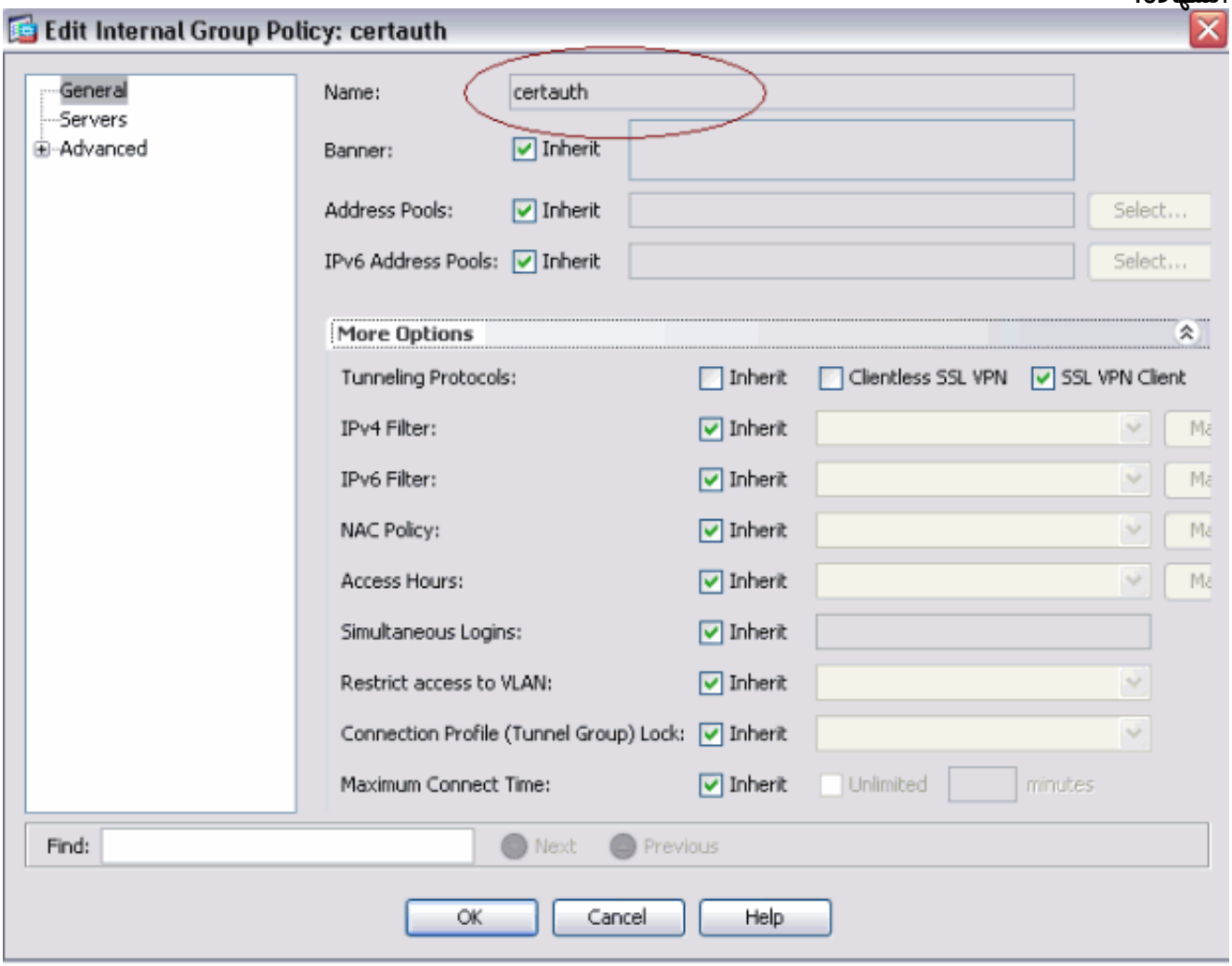
إضافة نفق انقسام لخادم CA.قم بالتوسيع **المتقدم**، ثم حدد **تقسيم الاتصال النفقي**.أختر **قائمة شبكات النفق أدناه** من قائمة النهج، وانقر فوق **إدارة** لإضافة قائمة التحكم في الوصول.



حدد **SSL VPN Client**، واختر ملف التعريف ل certenroll من قائمة **ملف تعريف العميل للتنزيل**.

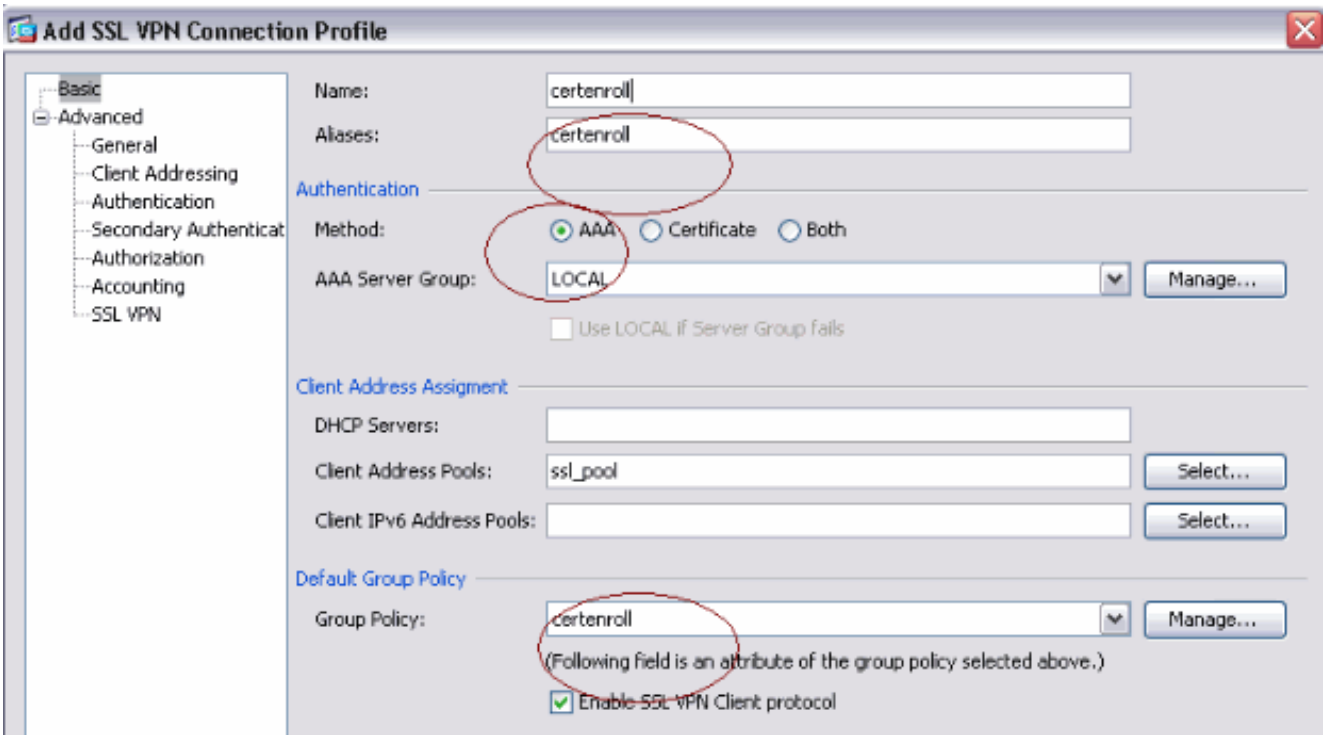


3. قم بإنشاء مجموعة أخرى تسمى **Certauth** لمصادقة الشهادة.

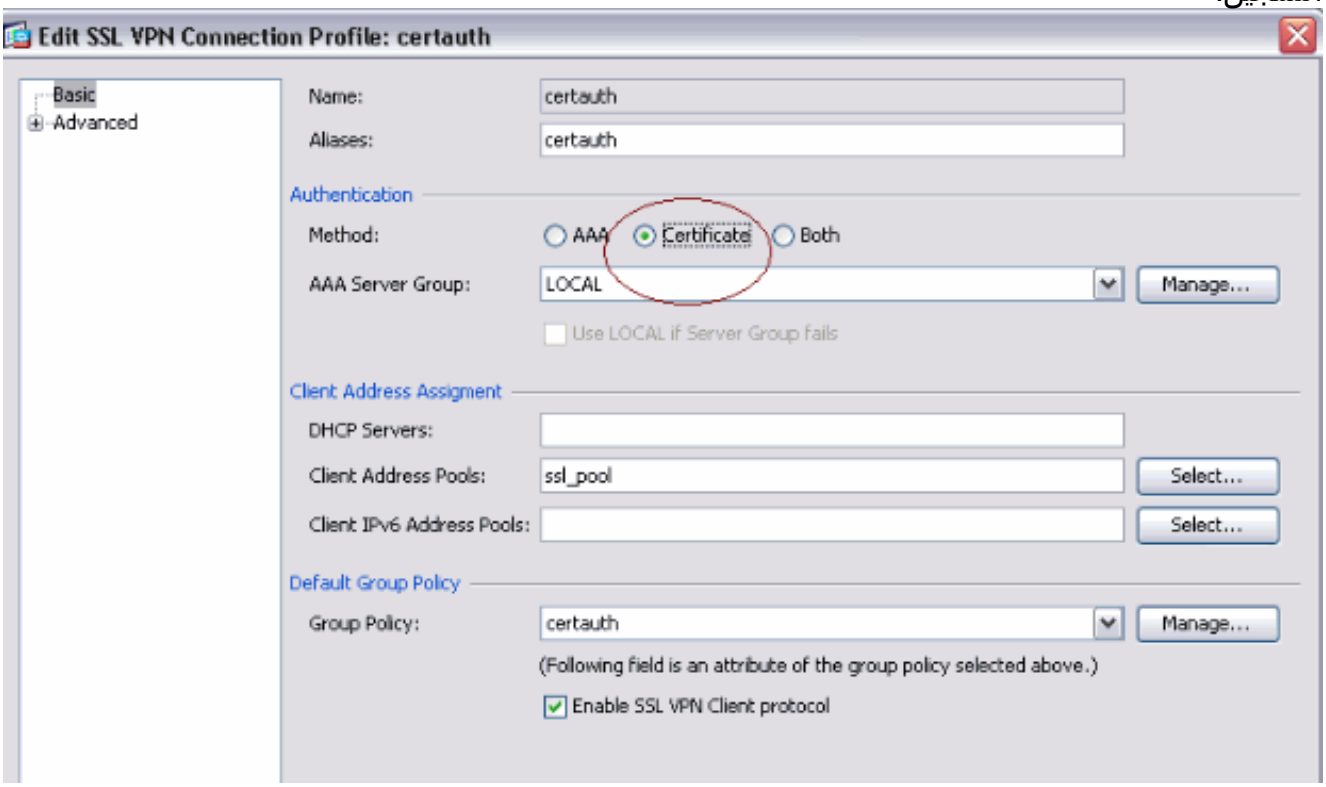


4. إنشاء ملف تعريف اتصال Certenroll.أختر **Remote Access VPN (الوصول عن بعد) > Network Client Access (وصول عميل الشبكة) > توصيفات توصيل AnyConnect**، ثم انقر فوق **إضافة**.أدخل مجموعة **certenroll** في حقل الأسماء المستعارة.**ملاحظة:** يجب أن يتطابق اسم الاسم المستعار مع القيمة المستخدمة في ملف تعريف AnyConnect ضمن

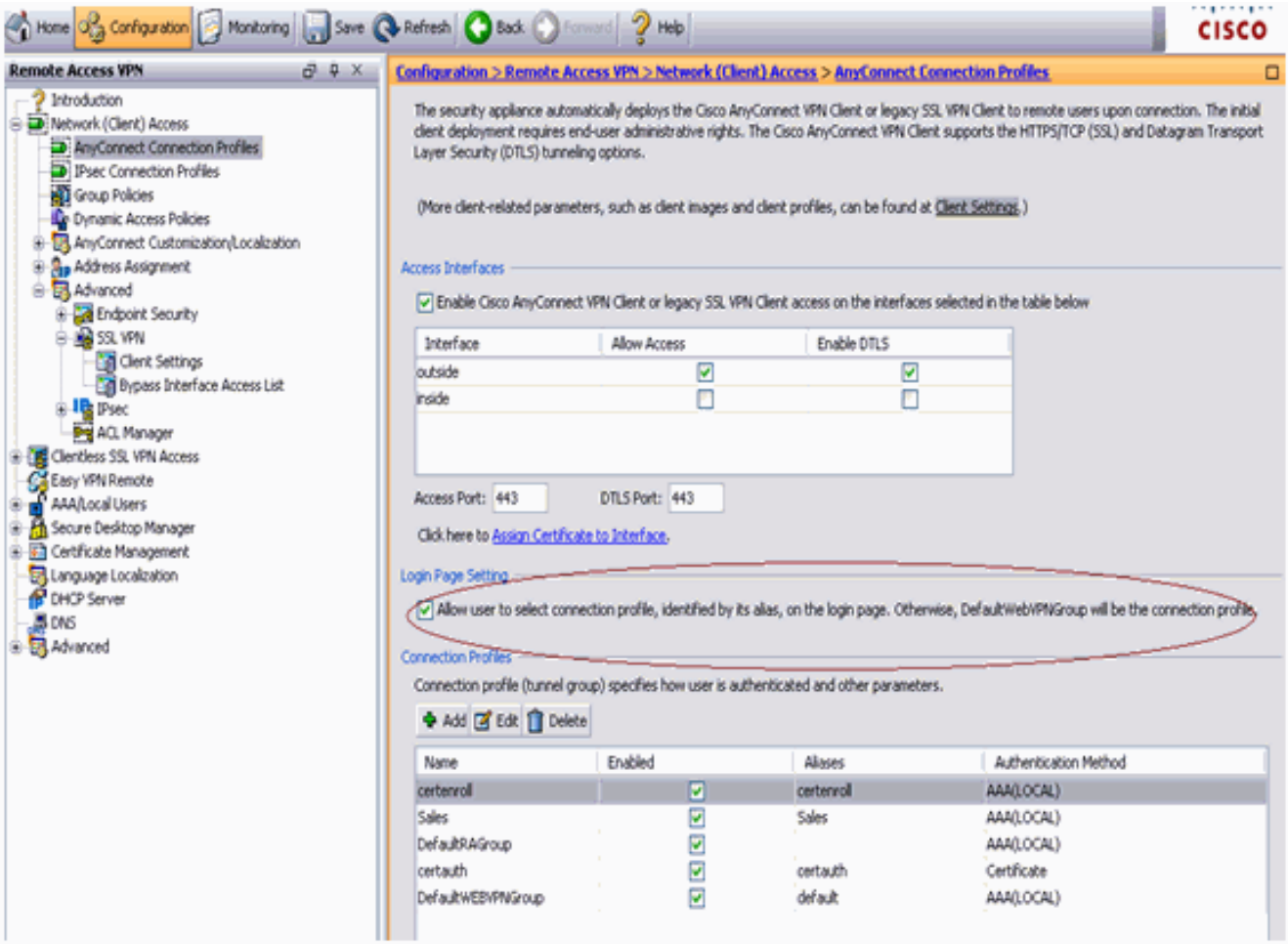
.AutoSCEPHost



5. إنشاء توصيف توصيل آخر يسمى **التحقق** بمصادقة الشهادة. هذا هو ملف تعريف الاتصال الفعلي الذي يتم إستخدامه بعد
التسجيل.



6. للتأكد من تمكين إستخدام الاسم المستعار، راجع **السماح للمستخدم بتحديد ملف تعريف الاتصال، المعرف بواسطة الاسم المستعار، في صفحة تسجيل الدخول. وإلا، فإن DefaultWebVPNGgroup هو ملف تعريف الاتصال.**



إختبار بروتوكول SCEP ل AnyConnect

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. بدء تشغيل عميل AnyConnect، والاتصال بملف تعريف

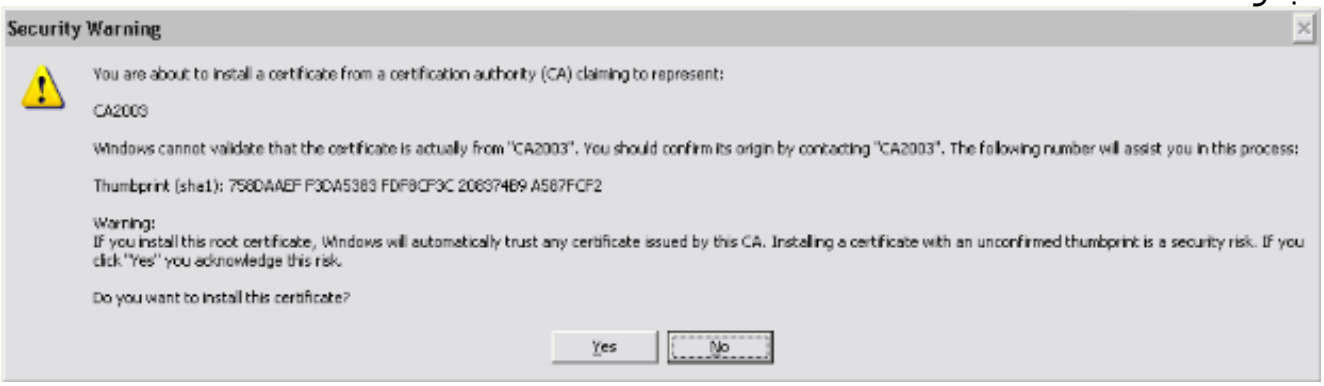
يقوم AnyConnect بتمرير طلب التسجيل إلى خادم CA من خلال Certenroll.

يمرر AnyConnect طلب SCEP.

التسجيل مباشرة ولا يمر عبر النفق، إذا تم إستخدام زر **الحصول على**

شهادة.

2. يظهر هذا التحذير. انقر على **نعم** لتثبيت شهادة المستخدم والشهادة الجذر



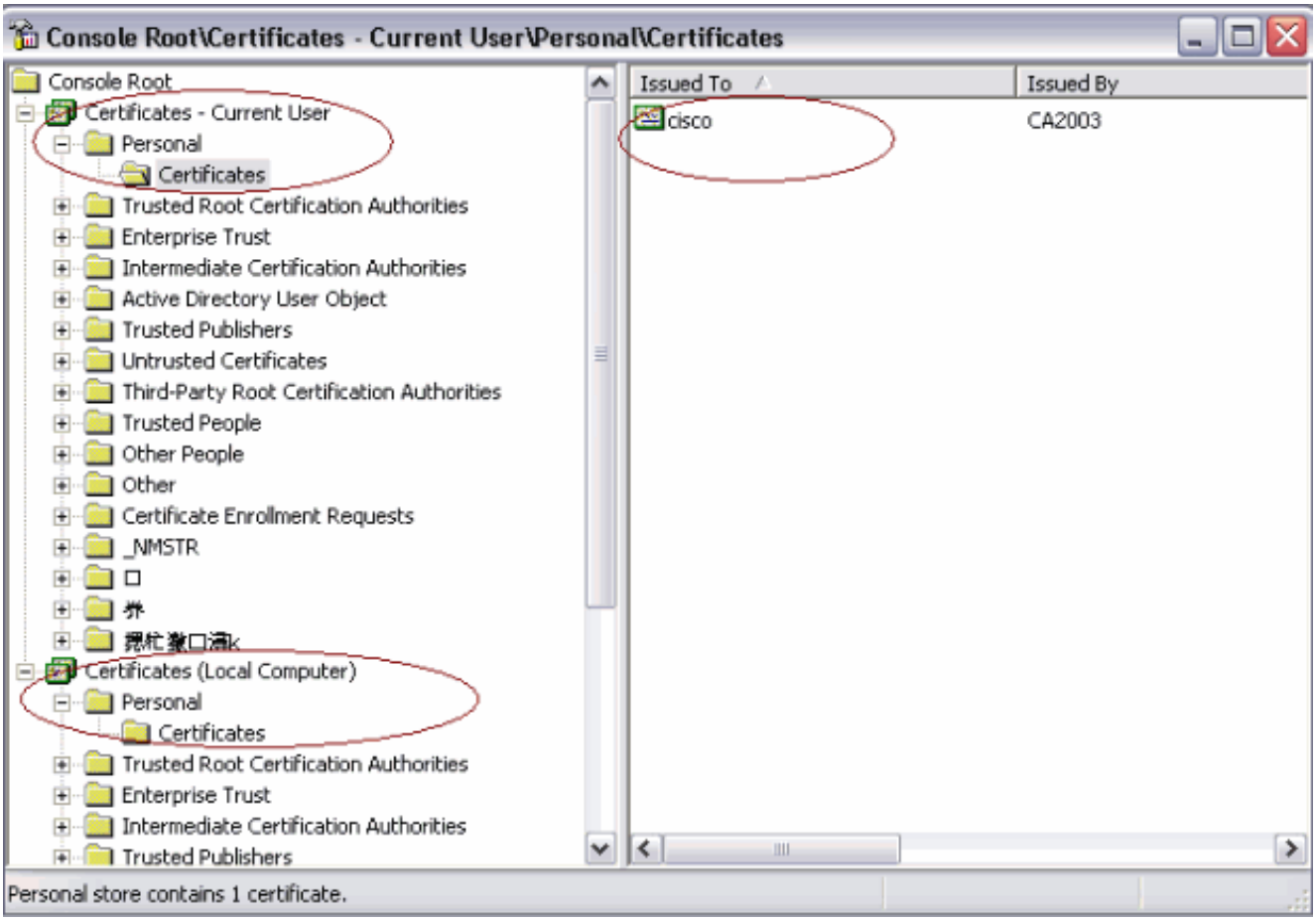
3. بمجرد تسجيل الشهادة، اتصل بملف تعريف **الشهادة**.

تخزين الشهادة في Microsoft Windows بعد طلب SCEP

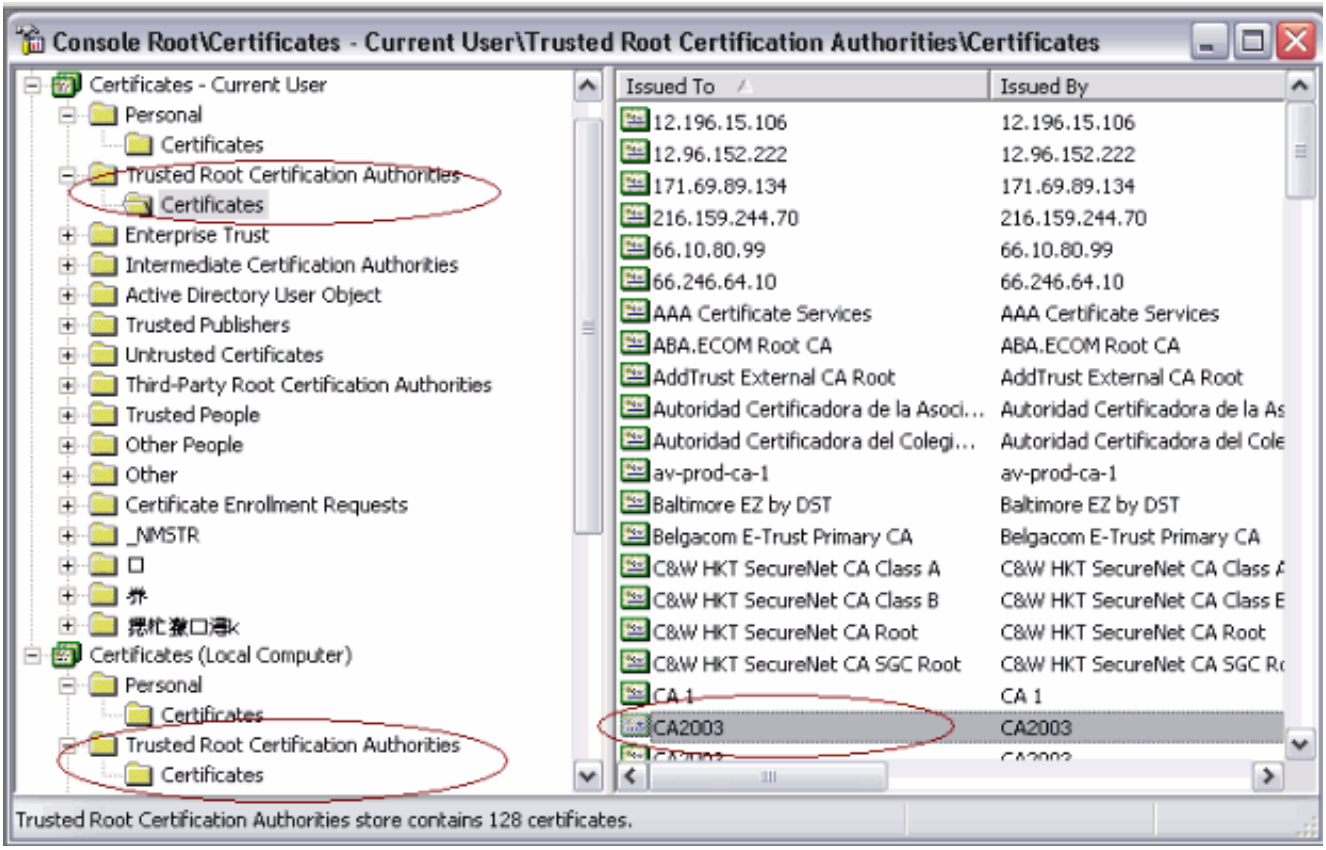
أكمل الخطوات التالية:

1. انقر على **ابدأ > تشغيل > mmc**.
2. انقر فوق **إضافة/إزالة انجذاب**.

3. انقر **إضافة**، واختر **شهادات**.
4. إضافة شهادات **حساب المستخدم** وحساب **الكمبيوتر**.تظهر هذه الصورة شهادة المستخدم المثبتة في مخزن شهادات
:Windows



تظهر هذه الصورة شهادة المرجع المصدق المثبتة في مخزن شهادات
:Windows



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- يعمل تسجيل بروتوكول SCEP ل AnyConnect فقط عند فشل مصادقة الشهادة. إذا لم يتم التسجيل، تحقق من مخزن الشهادات. إذا كانت الشهادات مثبتة بالفعل، قم بحذفها ثم أعد إختبارها.
- لا يعمل تسجيل SCEP ما لم يتم إستخدام الأمر **ssl certificate-authentication interface خارج المنفذ 443**.راجع معرفات أخطاء Cisco هذه للحصول على مزيد من المعلومات:معرف تصحيح الأخطاء من Cisco CSCtf06778 (العملاء المسجلون فقط) — لا يعمل تسجيل SCEP ل AnyConnect مع مصادقة الوحدة النمطية 2 لكل مجموعةمعرف تصحيح الأخطاء من Cisco CSCtf06844 (العملاء المسجلون فقط) —تسجيل SCEP ل AnyConnect لا يعمل مع ASA لكل مجموعة مصادقة
- إذا كان خادم CA على الجزء الخارجي من ASA، فتأكد من السماح بدوران الشعر باستخدام الأمر **نفسه-security-traffic allowed intra-interface**. أضفت أيضا ال nat خارج و access-list أمر كما هو موضح في هذا المثال:

```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
```

حيث يمثل 172.16.1.0 تجمع AnyConnect، ويمثل 171.69.89.87 عنوان IP لخادم CA.

- إذا كان خادم CA موجودا بالداخل، فتأكد من تضمينه في قائمة الوصول إلى النفق المقسم لنهج مجموعة **certenroll**. في هذا المستند، يفترض أن خادم CA موجود بالداخل.

```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

معلومات ذات صلة

- دليل مسؤول عميل AnyConnect VPN من Cisco، الإصدار 2.4
- 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).