تكوين ASA كخادم CA محلي و AnyConnect وحدة الاستقبال والبث

المحتويات

المقدمة

يصف هذا المستند كيفية إعداد جهاز أمان مهايئ (ASA) من Cisco كخادم مرجع شهادات (CA) وكبوابة طبقة مآخذ التوصيل الآمنة (SSL) لعملاء Cisco AnyConnect Secure Mobility.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- أساسي ASA تشكيل أن يركض برمجية صيغة 9.1.x
- ASDM 7.3 أو أعلى

المكونات المستخدمة

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

- Cisco 5500 Series ASA أن ضكري برمجية صيغة 9.1(6)
- AnyConnect Secure Mobility Client الإصدار 4.x لـ Windows

- زاهج الكمبيوتر الذي يقوم بتشغيل ماظن ليغشت مدعوم لكل مخطط التوافق.

- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 7.3

ملاحظة: تنزيل حزمة عميل AnyConnect VPN (AnyConnect-win*.pkg) من برامج تنزيل Cisco (العملاء المسجلين فقط). انسخ عميل AnyConnect VPN إلى ذاكرة ASA flash، والتي يجب تنزيلها إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع قسم تثبيت عميل AnyConnect من دليل تكوين ASA للحصول على مزيد من المعلومات.

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

معلومات أساسية

وتوفر هيئة الشهادات في مكتب المحاسبة هذه الوظائف:

- جدمي عملية مرجع الشهادة الأساسية في ASA.
- يقوم بنشر الشهادات.
- يوفر الفحص الآمن للإبطال للشهادات الصادرة.
- يوفر مرجع ترخيص على ASA للاستخدام مع إتصالات VPN SSL المستندة إلى المستعرض (WebVPN) والاتصالات SSL المستندة إلى العميل (AnyConnect).
- يوفر شهادات رقمية موثوق بها للمستخدمين، بدون الحاجة إلى الاعتماد على ترخيص الشهادات الخارجي.
- يوفر سلطة داخلية آمنة لمصادقة الشهادة ويوفر تسجيل المستخدم المباشر عن طريق تسجيل الدخول إلى موقع الويب.

المبادئ التوجيهية والقيود

- مدعوم في وضع جدار الحماية الموجه والشفاف.
- يمكن إقامة خادم CA محلي واحد فقط في كل مرة على ASA.
- لا يتم دعم ميزة ASA كخادم CA محلي في إعداد تجاوز الفشل.
- لا يدعم ASA حاليا، والذي يعمل كخادم CA محلي، إلا إنشاء شهادات SHA1.
- يمكن إستخدام خادم CA المحلي لاتصالات SSL VPN المستندة إلى المستعرض والعميل. غير مدعوم حاليا لـ IPSec.
- لا يدعم موازنة حمل VPN لـ CA المحلي.
- لا يمكن أن يكون المرجع المصدق المحلي تابعا لمرجع مصدق آخر. ولا يمكن أن يعمل إلا بوصفه المرجع المصدق الجذري.
- يتعذر على ASA حاليا التسجيل إلى خادم CA المحلي لشهادة الهوية.
- عند اكتمال تسجيل الشهادة، يقوم ASA بتخزين ملف PKCS12 يحتوي على زوج المفاتيح الخاص بالمستخدم وسلسلة الشهادات، وهو ما يتطلب حوالي 2 كيلوبايت من ذاكرة الفلاش أو مساحة على القرص لكل تسجيل. يعتمد المقدار الفعلي لمساحة

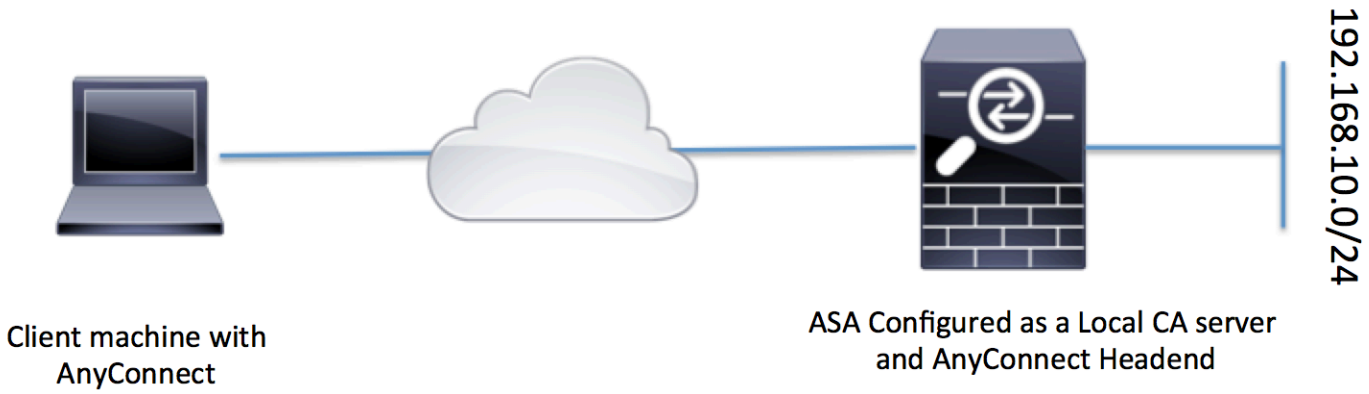
القرص على حجم مفتاح RSA الذي تم تكوينه وحقول الشهادة. ضع هذا المبدأ التوجيهي نصب عينيك عند إضافة عدد كبير من عمليات تسجيل الشهادة المعلقة على ASA مع مقدار محدود من ذاكرة Flash المتاحة، لأن ملفات PKCS12 هذه يتم تخزينها في ذاكرة الفلاش طوال مدة مهلة إستردار التسجيل التي تم تكوينها.

التكوين

يصف هذا القسم كيفية تكوين Cisco ASA كخادم CA محلي.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



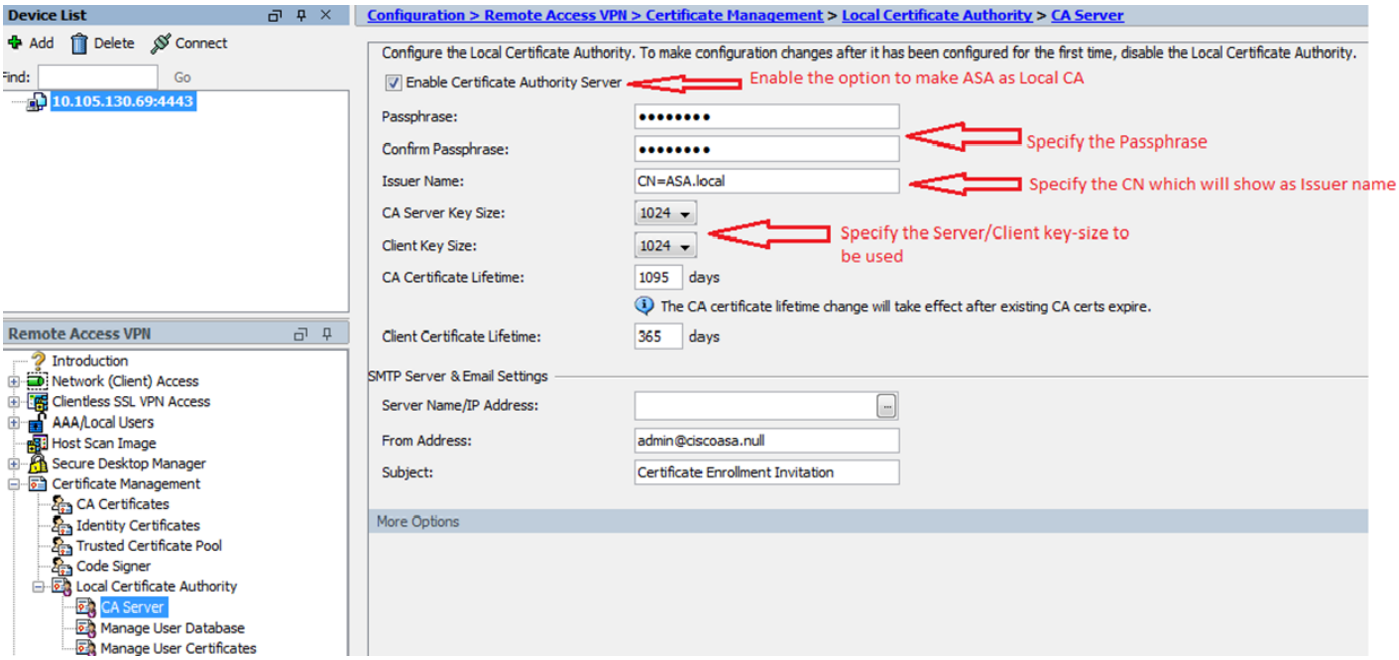
ASA كخادم CA محلي

الخطوة 1. تكوين خادم CA المحلي وتمكينه على ASA

- انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > إدارة الشهادات > المرجع المصدق المحلي للشهادات > خادم CA. تحقق من خيار تمكين خادم المرجع المصدق.
- قم بتكوين عبارة المرور. يجب أن تكون عبارة المرور حد أدنى، سبعة حروف تستخدم لترميز وحفظ ملف PKCS12 الذي يتضمن شهادة CA المحلية وزوج المفاتيح. تقوم عبارة المرور بإلغاء تأمين أرشيف PKCS12 في حالة فقد شهادة CA أو زوج المفاتيح.
- قم بتكوين اسم المصدر. سيظهر هذا الحقل ك CN لشهادة الجذر. ويمكن تحديد ذلك بالتنسيق التالي: CN (الاسم الشائع)، OU (الوحدة التنظيمية)، (س) المنظمة، L (المنطقة المحلية)، S (الولاية) و C (البلد).
- التكوين الاختياري: قم بتكوين إعدادات خادم SMTP وخادم البريد الإلكتروني لضمان إمكانية تلقي بروتوكول OTP للعملاء النهائيين عبر البريد لإكمال التسجيل.

يمكنك تكوين اسم المضيف أو عنوان IP لخادم البريد الإلكتروني/SMTP المحلي.
يمكنك أيضا تكوين حقل من العنوان والموضوع للبريد الإلكتروني الذي سيستلمه العملاء. بشكل افتراضي، يكون عنوان "من" هو admin@<ASA hostname>.null والموضوع هو دعوة تسجيل الشهادة.

- التكوين الاختياري: يمكنك تكوين المعلمات الاختيارية مثل حجم مفتاح العميل وحجم مفتاح خادم CA وعمر شهادة CA وعمر شهادة العميل أيضا.



مكافئ واجهة سطر الأوامر (CLI):

```
ASA(config)# crypto ca server
ASA(config-ca-server)# issuer-name CN=ASA.local
ASA(config-ca-server)# subject-name-default CN=ASA.local
ASA(config-ca-server)# lifetime certificate 365
ASA(config-ca-server)# lifetime ca-certificate 1095
ASA(config-ca-server)# passphrase cisco123
ASA(config-ca-server)# no shutdown
% Some server settings cannot be changed after CA certificate generation.
Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete
```

وهذه حقول إضافية يمكن تكوينها ضمن تكوين خادم CA المحلي.

عنوان URL لنقطة توزيع CRL	هذا هو موقع CRL على ASA. ولكن http://hostname.domain/+CSCOCA+/asa_ca.crl هو الموقع الافتراضي. يمكن تعديل عنوان URL.

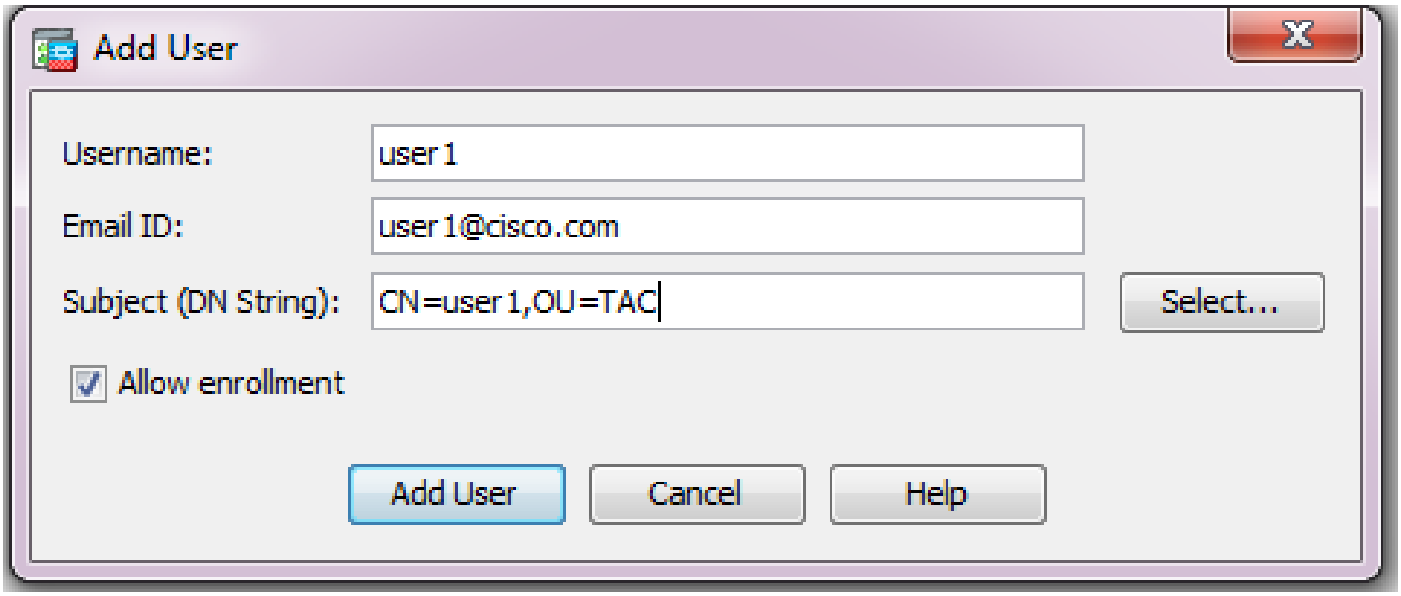
المنفذ والواجهة Publish-CRL	publish- واجهة ومنفذ معينين، أختر واجهة HTTP على لتوفير CRL لتنزيل أي يمكن أن يكون الذي والمنفذ، لرقم المنفذ أدخل ثم .المنسدلة القائمة من CRL رقم منفذ من 1-65535. التقصير ميناء رقم TCP ميناء 80.
عمر CRL	يقوم المرجع المصدق المحلي بتحديث CRL وإعادته في كل مرة يتم فيها إبطال شهادة المستخدم وأ إلغاء إبطالها، ولكن إذا لم تحدث تغييرات في الإبطال، تتم إعادة إصدار CRL تلقائيا مرة كل مدة بقاء CRL، وهي الفترة الزمنية التي تحددها باستخدام الأمر crl مدى الحياة أثناء تكوين CA المحلي. إذا لم تقم بتحديد مدة بقاء CRL، فإن الفترة الزمنية الافتراضية هي ست ساعات.
موقع تخزين قاعدة البيانات	يقوم ASA بالوصول إلى معلومات المستخدم والشهادات الصادرة وقوائم الإبطال وتنفيذها باستخدام قاعدة بيانات CA محلية. توجد قاعدة البيانات هذه في ذاكرة Flash المحلية بشكل افتراضي، أو يمكن تكوينها ليتم تحميله وإمكانية الوصول إليه من تثبيتها على نظام ملفات خارجي يتم تركيبه على ASA.
اسم الموضوع الافتراضي	أدخل موضوعا افتراضيا (سلسلة DN) للإلحاق اسم مستخدم في الشهادات الصادرة. يتم توفير سمات DN المسموح بها في هذه القائمة: ·CN (الاسم الشائع)SN (اسم العائلة) ·O (اسم المؤسسة) ·L (محلية) ·C (الدولة) ·OU (الوحدة التنظيمية) ·EA (عنوان البريد الإلكتروني) ·ST (الولاية/المقاطعة) ·T (العنوان)
فترة التسجيل	تعيين حد وقت التسجيل بالساعات التي يمكن للمستخدم خلالها إستيراد ملف PKCS12 من ASA. القيمة الافتراضية هي 24 ساعة. ملاحظة: إذا انتهت فترة التسجيل قبل أن يسترجع المستخدم ملف PKCS12 الذي يتضمن شهادة المستخدم، لا يسمح بالتسجيل.
انتهاء صلاحية رمز مرور لمرة واحدة	يحدد مقدار الوقت بالساعات الذي يكون فيه OTP صالحا لتسجيل المستخدم. تبدأ هذه الفترة الزمنية عندما يسمح للمستخدم بالتسجيل. القيمة التلقائية هي 72 ساعة.

تذكير انتهاء صلاحية الشهادة	تحديد عدد الأيام قبل انتهاء صلاحية الشهادة التي يتم فيها إرسال تذكير أولي لإعادة التسجيل إلى مالكي الشهادات.

الخطوة 2. إنشاء مستخدمين وإضافتهم إلى قاعدة بيانات ASA

- انتقل إلى Configuration (التكوين) > Remote Access VPN (الوصول عن بعد) > Certificate Management (إدارة الشهادات) > Local Certificate Authority (مرجع الشهادات المحلي) > Managed User Database.انقر فوق Add.

- حدد تفاصيل المستخدم مثل اسم المستخدم ومعرف البريد الإلكتروني واسم الموضوع، كما هو موضح في هذه الصورة.



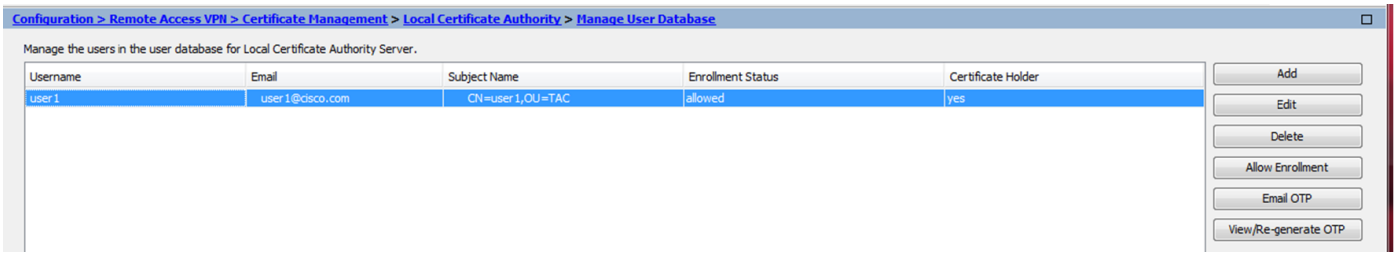
- تأكد من التحقق من السماح بالتسجيل بحيث يسمح لك بالتسجيل للشهادة.
- انقر فوق إضافة مستخدم لإكمال تكوين المستخدم.

مكافئ واجهة سطر الأوامر (CLI):

<#root>

```
ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com
```

- بعد إضافة المستخدم إلى "قاعدة بيانات المستخدم"، يتم عرض حالة التسجيل كمسموح به للتسجيل.



CLI للتحقق من حالة المستخدم:

<#root>

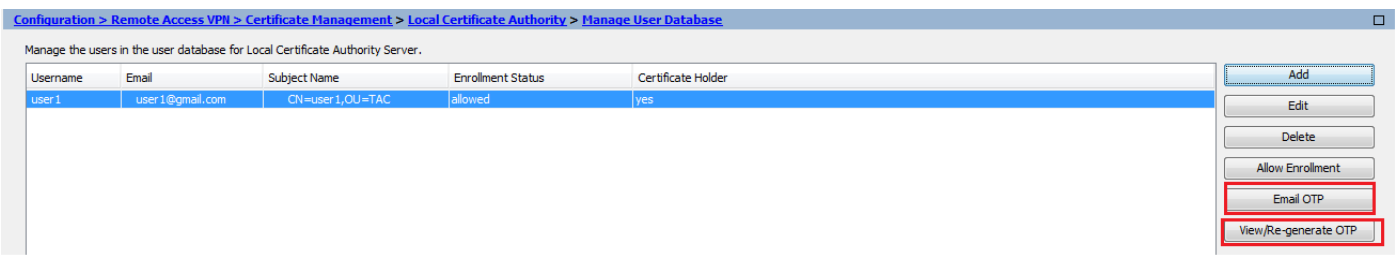
```
ASA# show crypto ca server user-db

                username: user1
                   email:    user1@cisco.com
                      dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
                notified: 1 times
                enrollment status:

Allowed to Enroll
```

- بعد إضافة المستخدم إلى قاعدة بيانات المستخدم، يمكن توفير كلمة مرور لمرة الواحدة (OTP) للمستخدم لإكمال التسجيل باستخدام أي من هذه الأمرين:

أرسل كلمة مرور لمرة الواحدة (يتطلب خادم SMTP وإعدادات البريد الإلكتروني ليتم تكوينها ضمن تكوين خادم CA).

أو

عرض/إعادة إنشاء عرض بروتوكول OTP مباشرة ومشاركته مع المستخدم بالنقر فوق بروتوكول الشجرة المتفرعة (OTP). يمكن إستخدام هذا أيضا لإعادة تكوين بروتوكول OTP.



مكافئ واجهة سطر الأوامر (CLI):

```
!! Email the OTP to the user
ASA# crypto ca server user-db allow user1 email-otp

!! Display the OTP on terminal
ASA# crypto ca server user-db allow user1 display-otp
Username: user1
OTP: 18D14F39C8F3DD84
Enrollment Allowed Until: 14:18:34 UTC Tue Jan 12 2016
```

الخطوة 3. تمكين WebVPN على واجهة WAN

- تمكين Web Access على ASA للعملاء لطلب التسجيل.

```
!! Enable web-access on the "Internet" interface of the ASA
ASA(config)# webvpn
ASA(config-webvpn)#enable Internet
```

الخطوة 4. إستيراد الشهادة على جهاز العميل

- على محطة العمل العميلة، افتح مستعرض وانتقل إلى الارتباط لإكمال التسجيل.
- يجب أن يكون IP/FQDN المستخدم في هذا الارتباط هو IP الخاص بالواجهة التي يتم تمكين webVPN عليها في تلك الخطوة، والتي هي واجهة الإنترنت.

<#root>

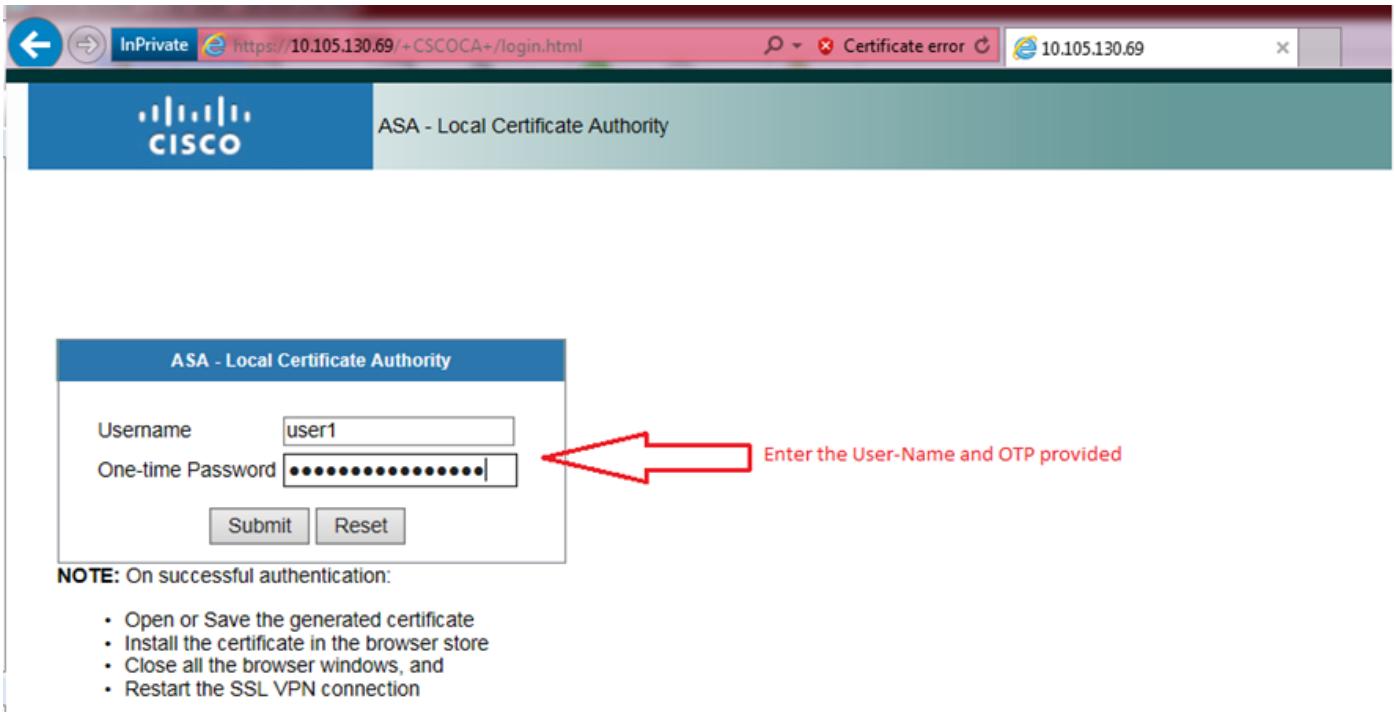
https://

<>

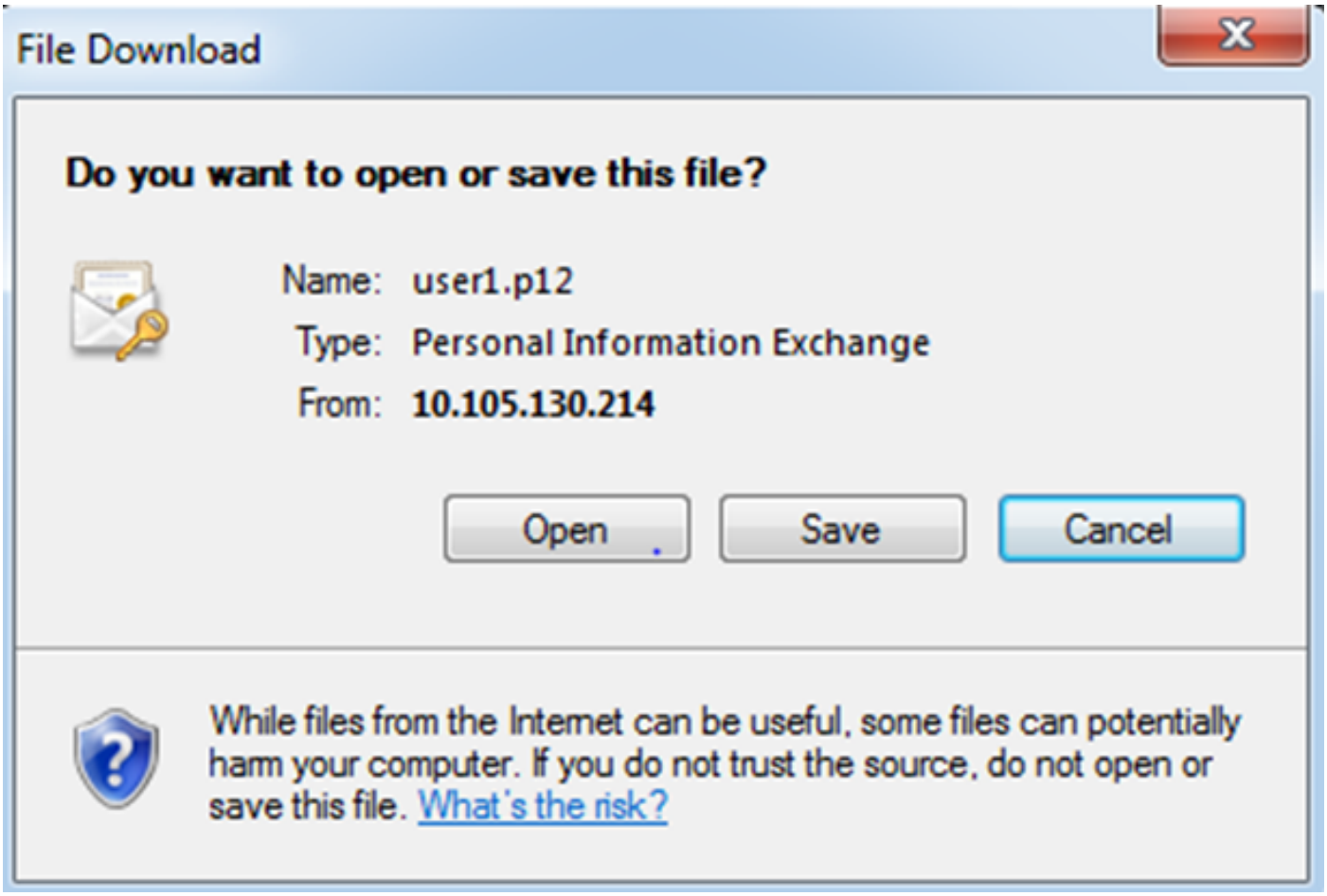
IP/FQDN>/+CSCOCA+/enroll.html

<>

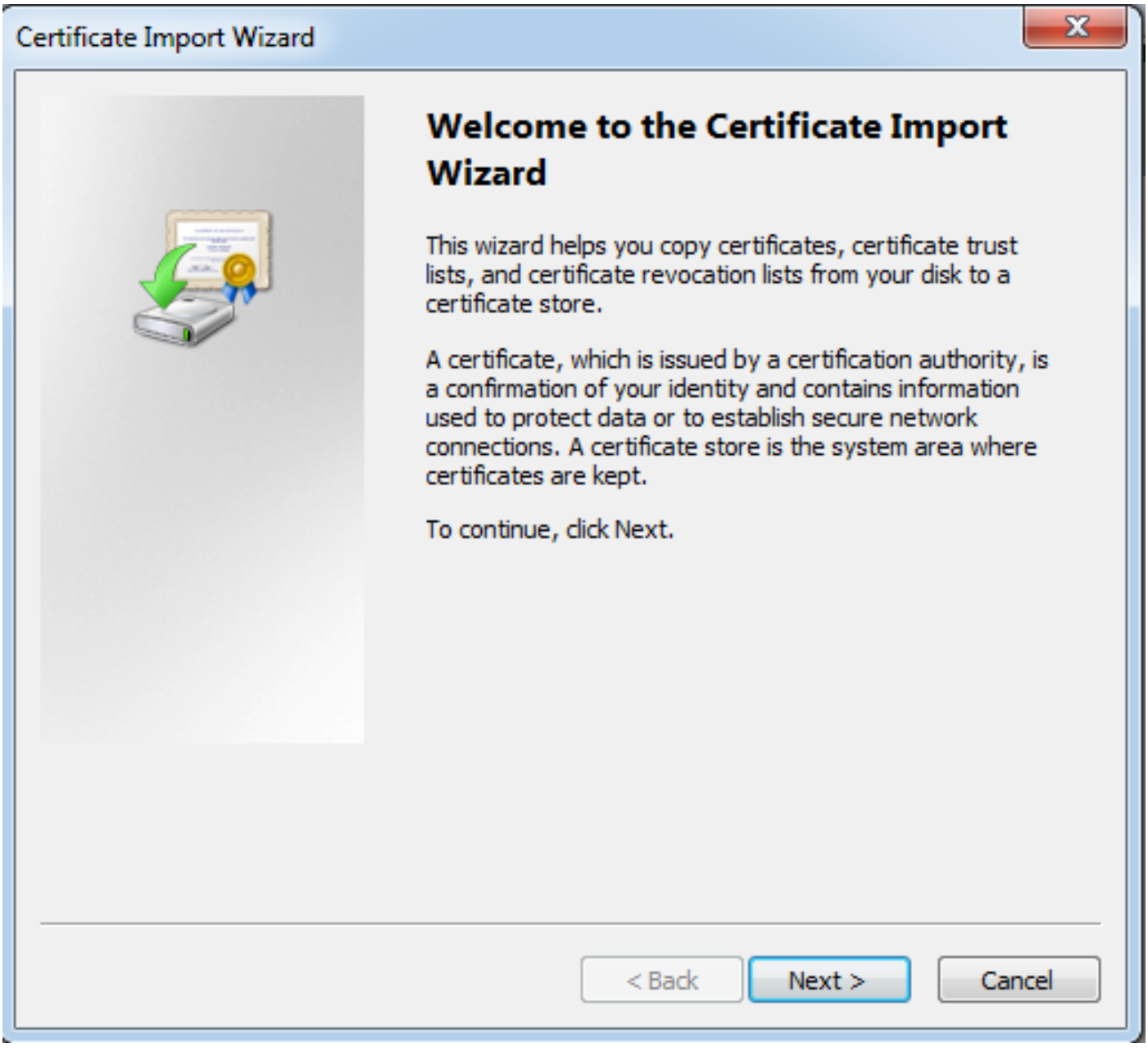
- أدخل ال username (يشكل على ال ASA تحت خطوة 2، خيار a) وال OTP، أي كان زودت عن طريق بريد إلكتروني أو يدويا.



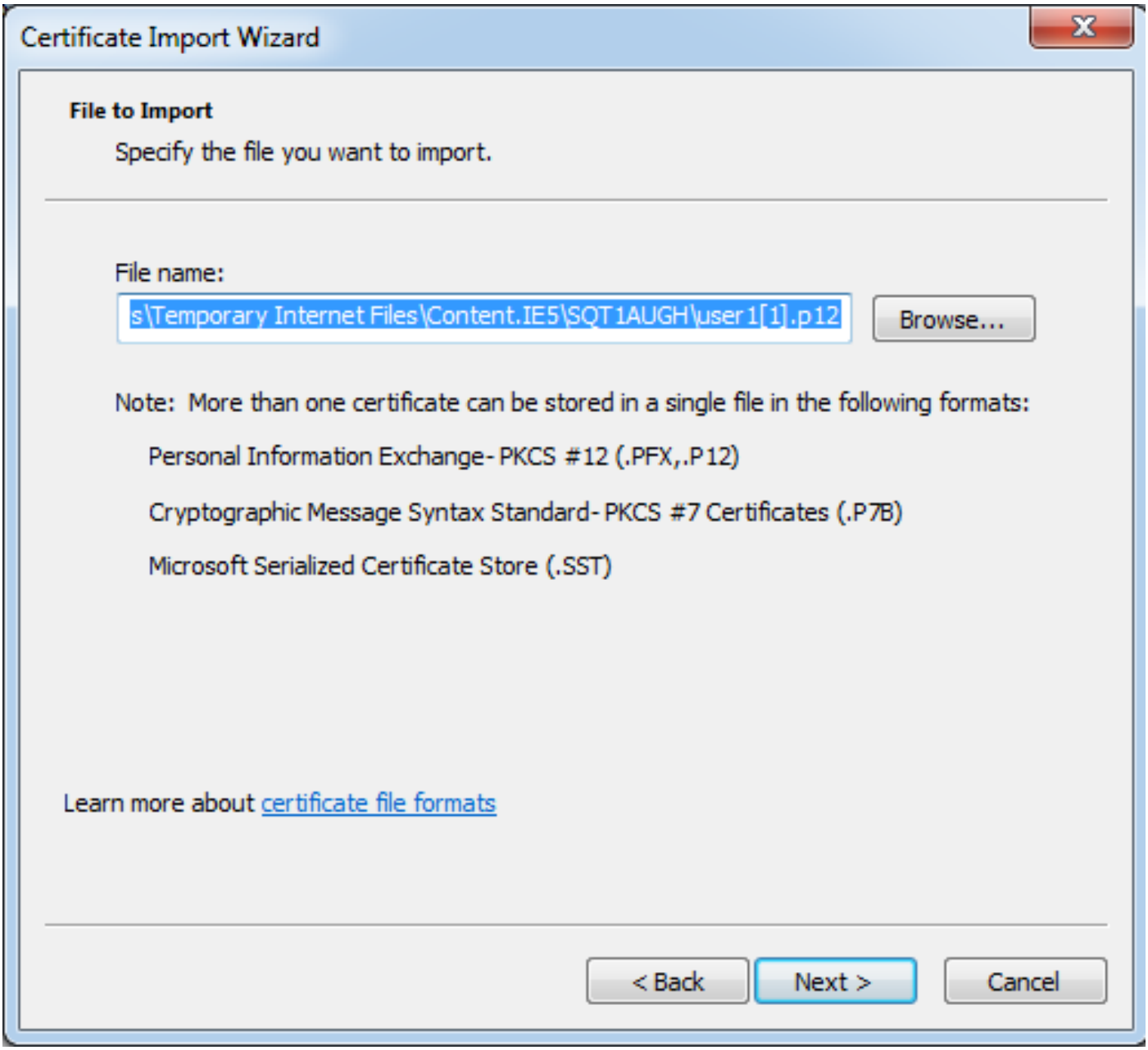
- انقر على فتح لتثبيت شهادة العميل المتلقاة من ASA مباشرة.
- عبارة المرور لتثبيت شهادة العميل هي نفسها عبارة OTP التي تم تلقيها سابقا.



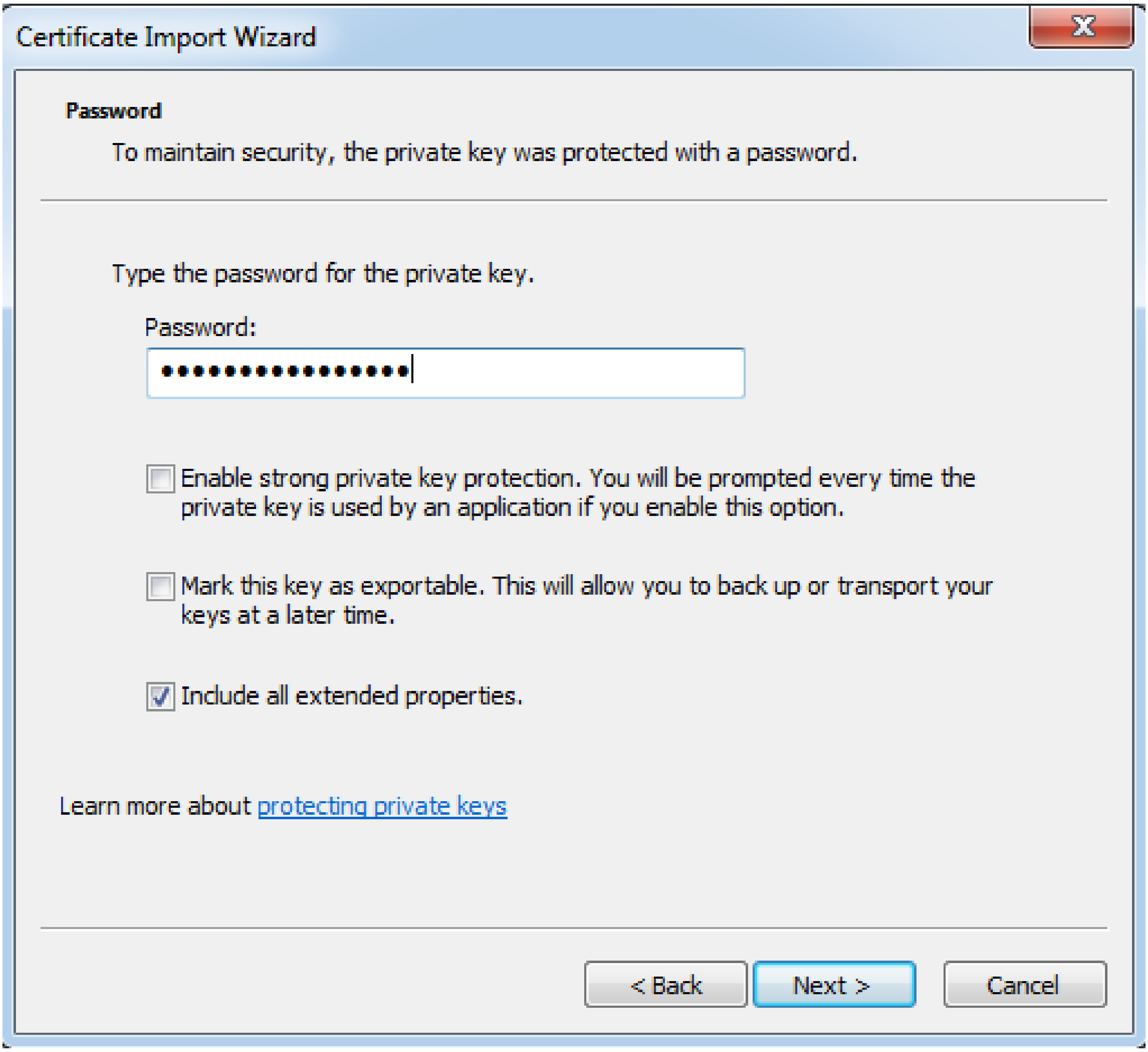
- انقر فوق Next (التالي).



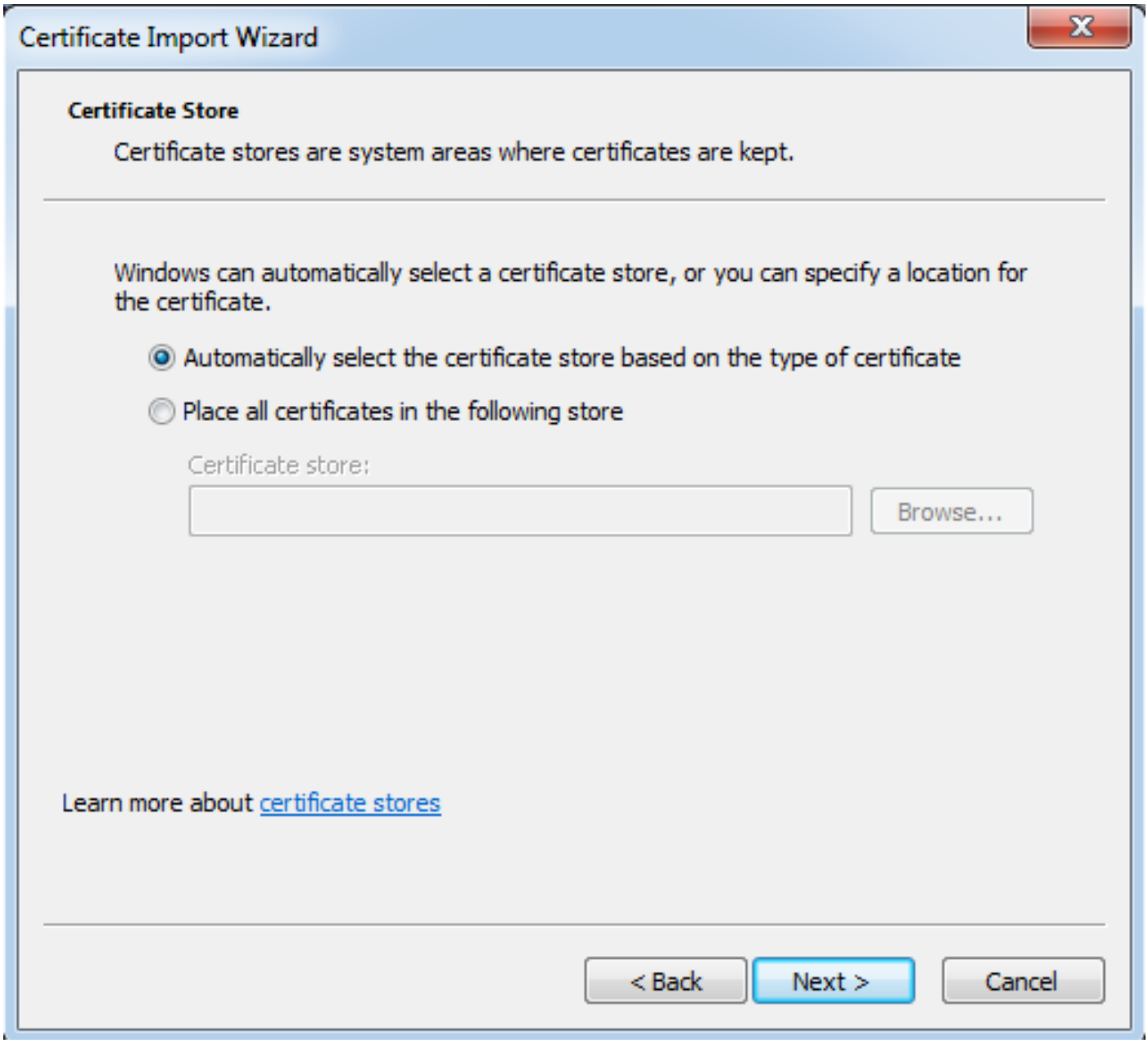
- أترك المسار كافتراضي وانقر التالي.



- دخلت ال OTP في الكلمة مجال.
- يمكنك تحديد الخيار لوضع علامة قابل للتصدير على هذه المفتاح حتى يمكن تصدير المفتاح من محطة العمل في المستقبل اذا تطلب الأمر.
- انقر فوق التالي



- يمكنك تثبيت الشهادة يدويا في مخزن شهادات معين أو تركها لتختار المتجر تلقائيا.
- انقر فوق Next (التالي).



- طقطقة إنجاز in order to أتمت التثبيت.

Certificate Import Wizard

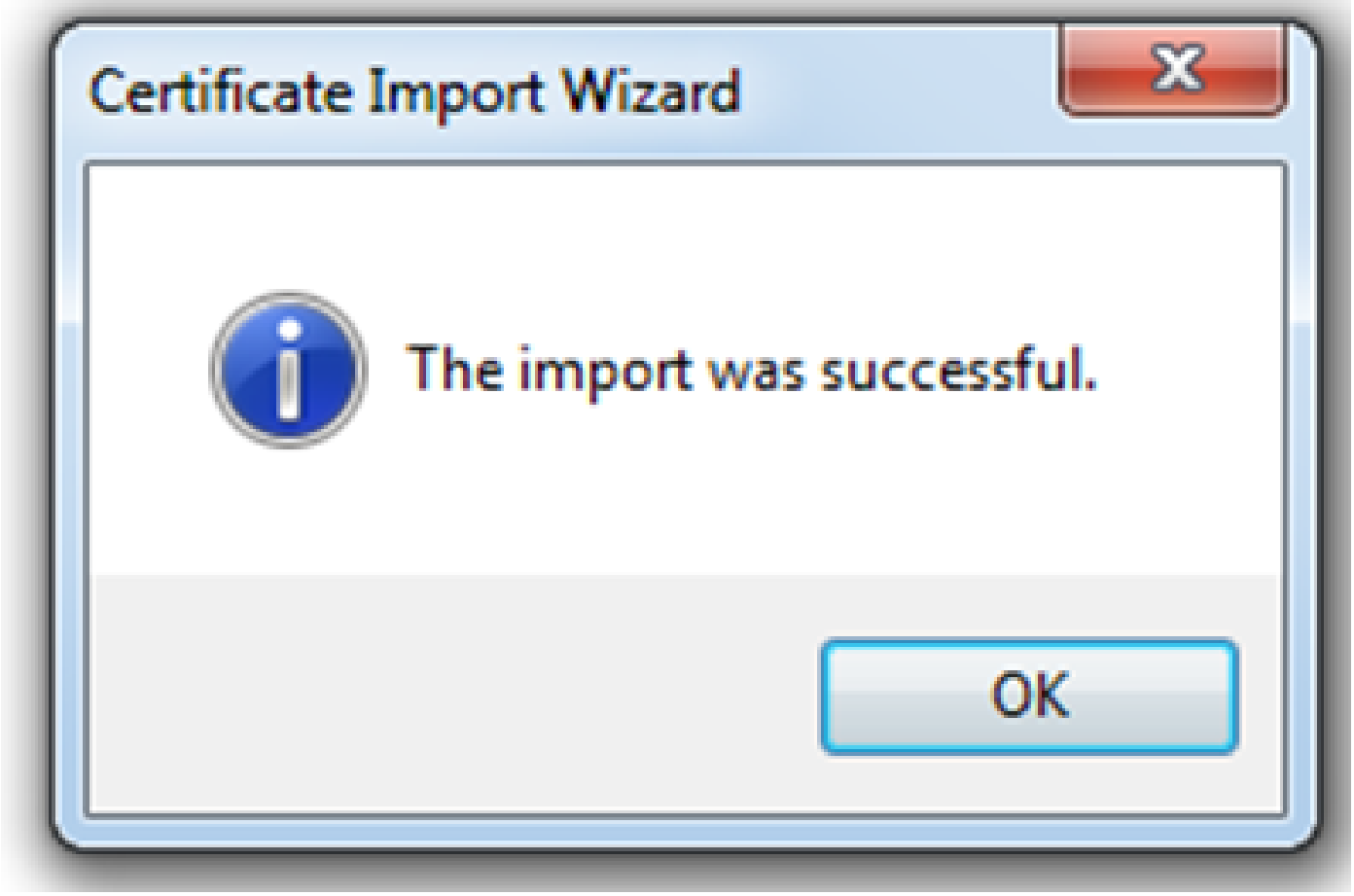
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

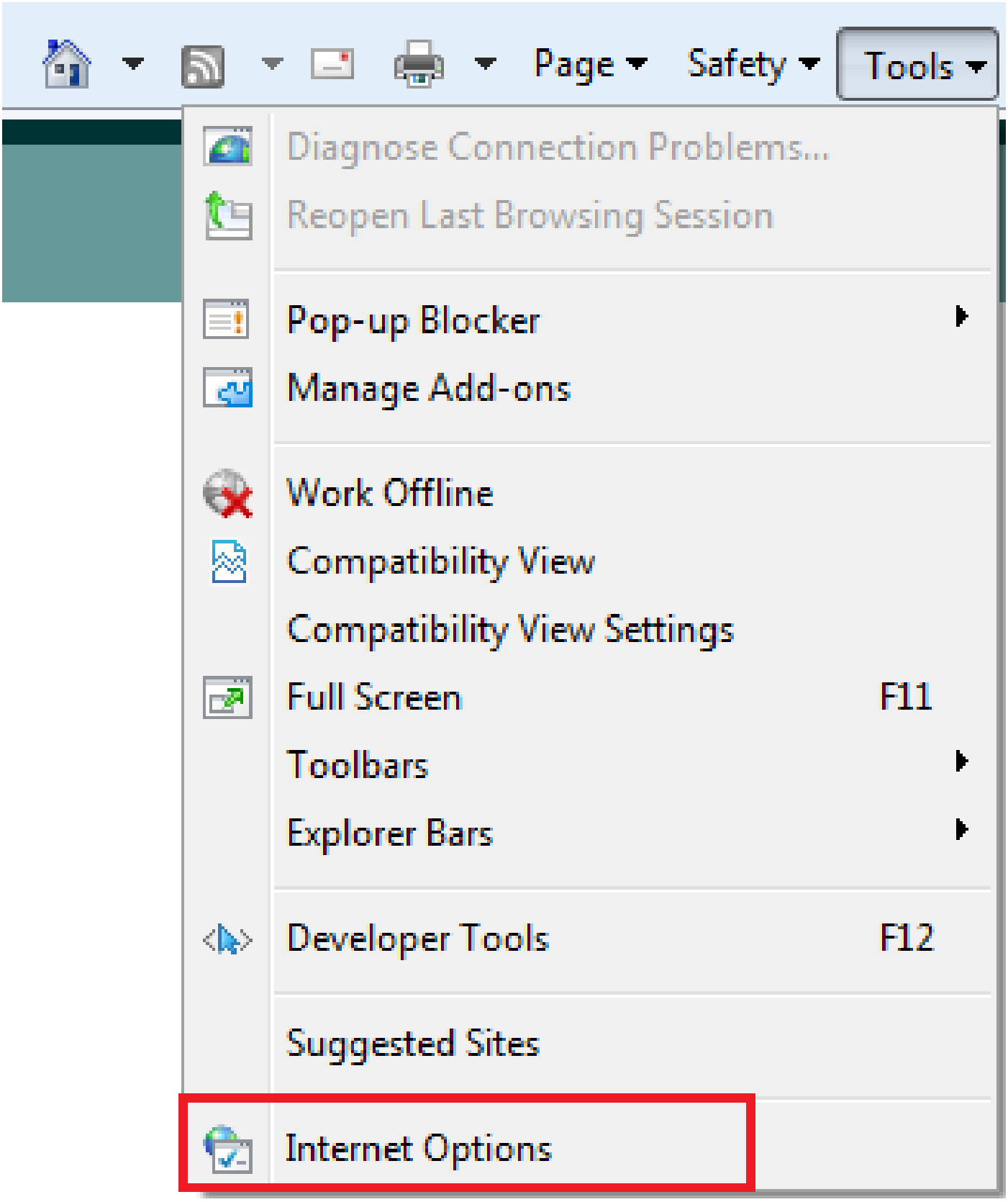
You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Users\mrsethi\AppData\Lo

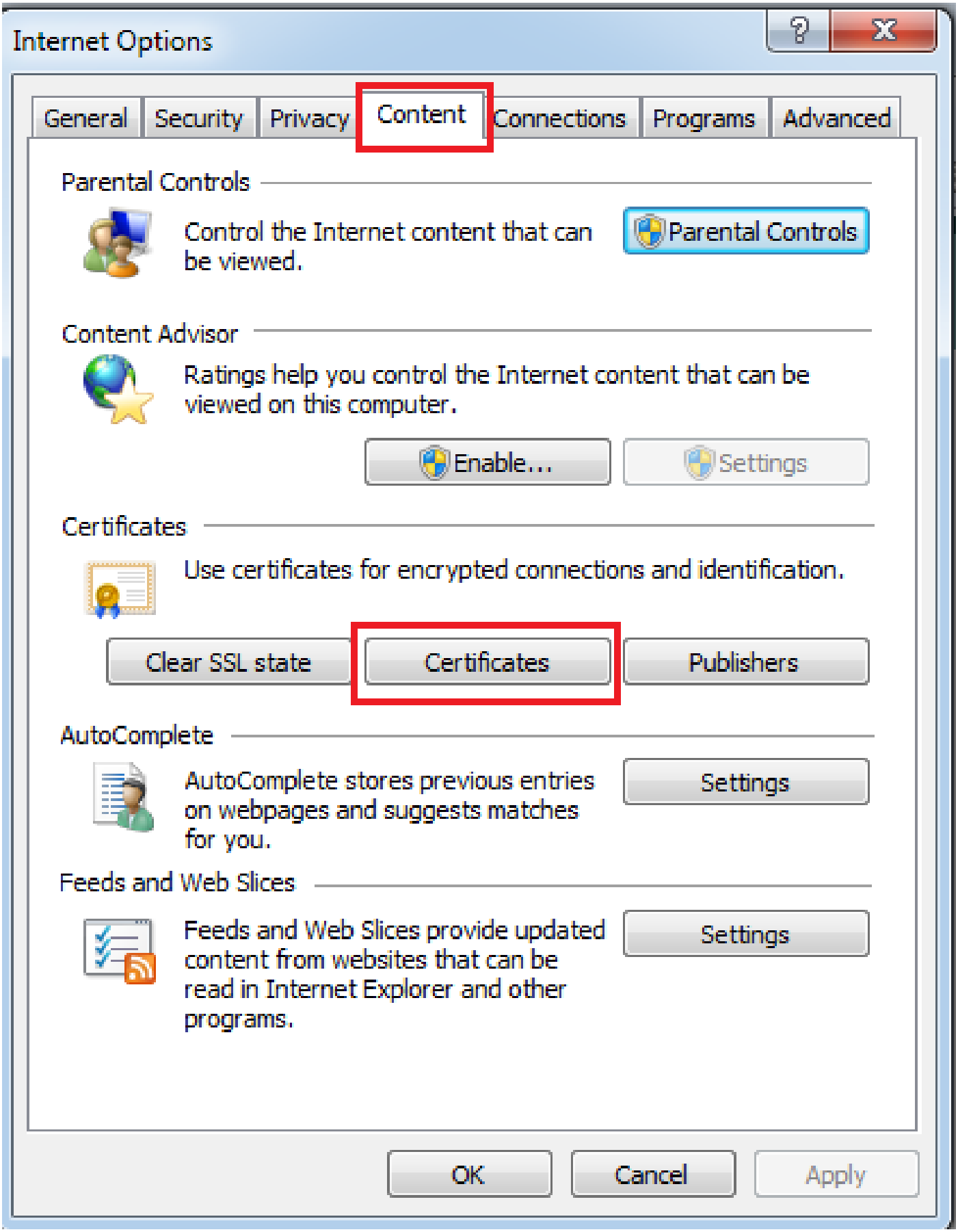
< Back | Finish | Cancel



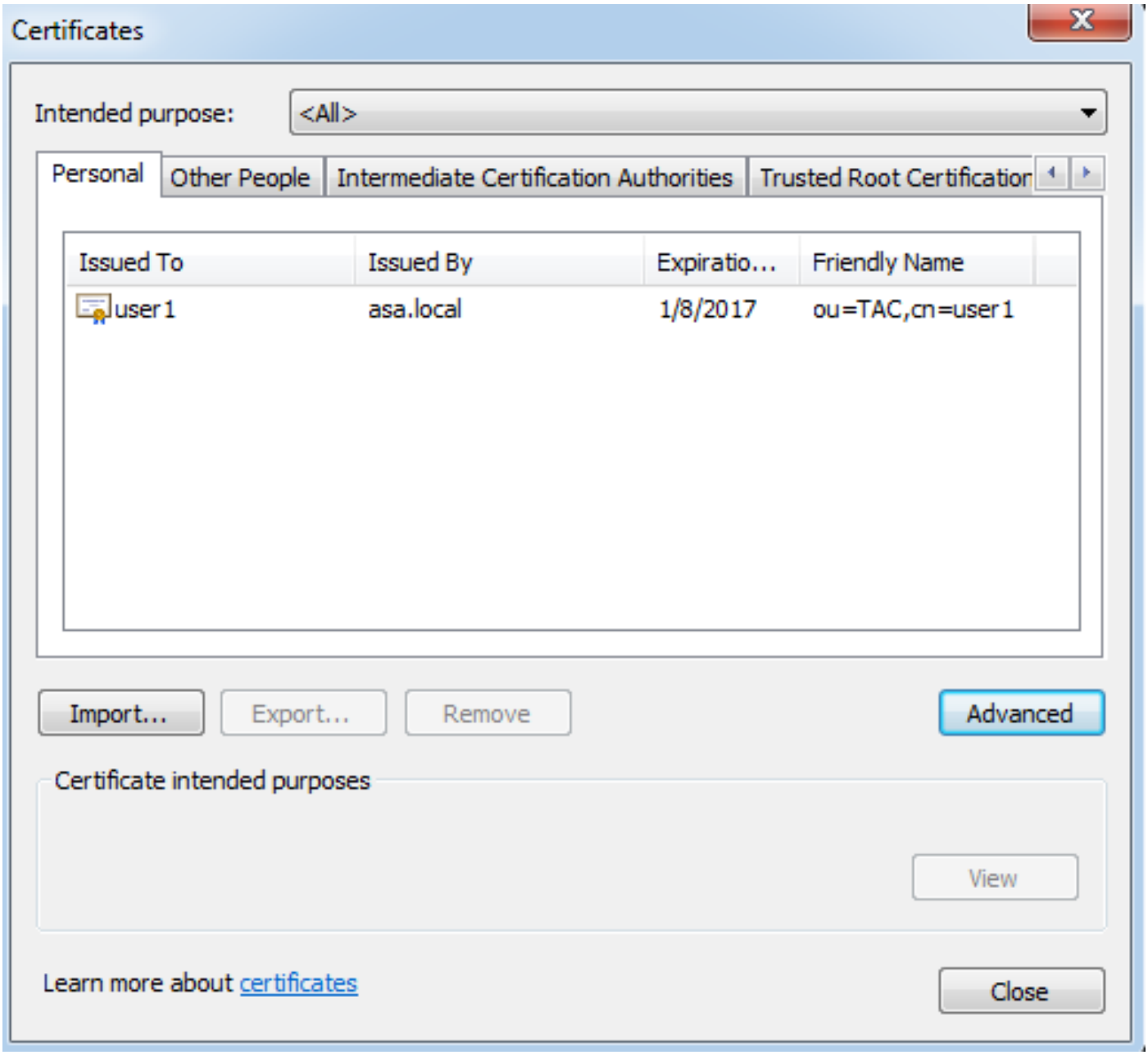
- بمجرد تثبيت الشهادة بنجاح، يمكنك التحقق من صحتها.
- افتح IE وانتقل إلى أدوات > خيارات الإنترنت.



- انتقل إلى علامة التبويب محتوى وانقر فوق الشهادات، كما هو موضح في هذه الصورة.



- تحت المتجر الشخصي، يمكنك أن ترى الشهادة تم استلامها من ال ASA.



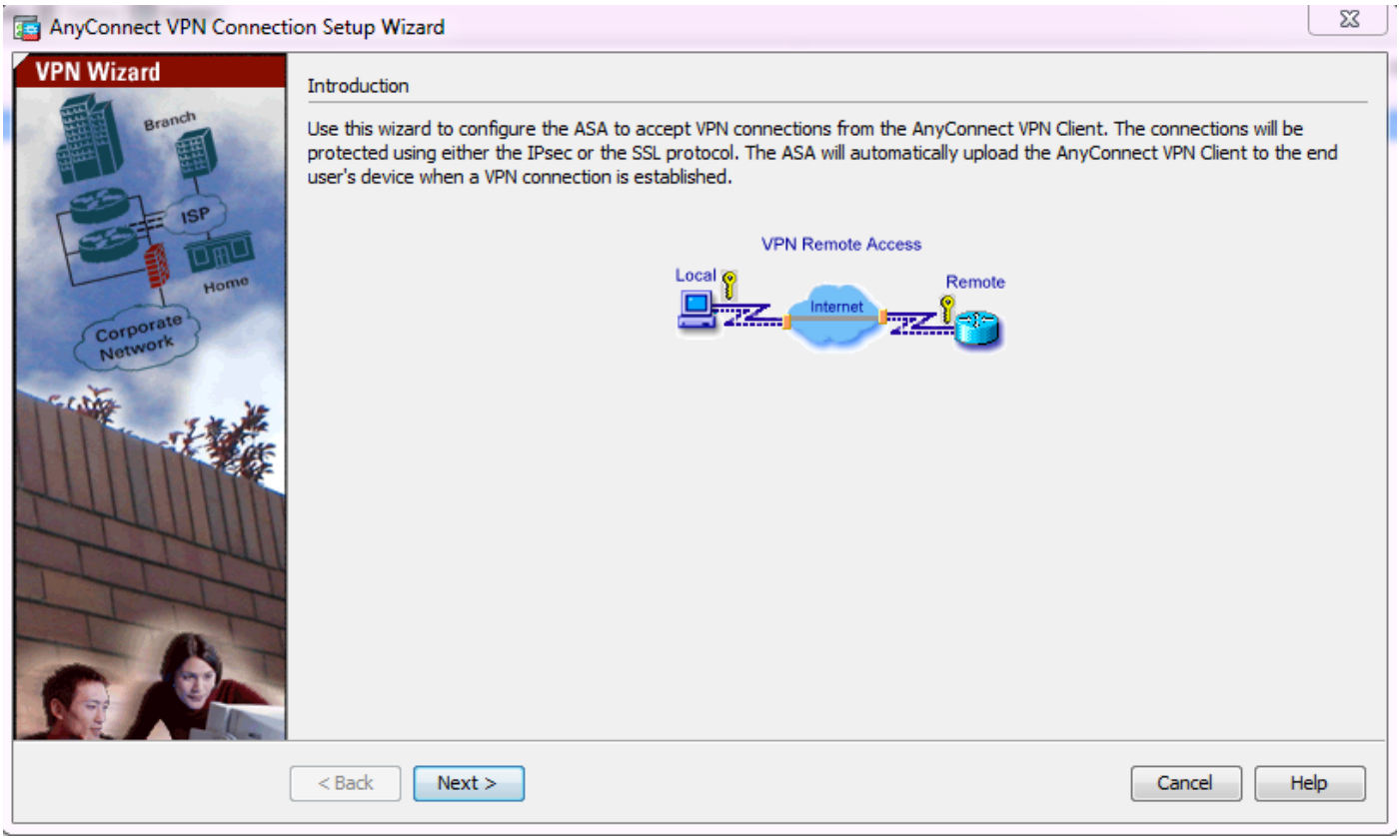
AnyConnect لعملاء SSL كبوابة ASA

معالج تكوين ASDM AnyConnect

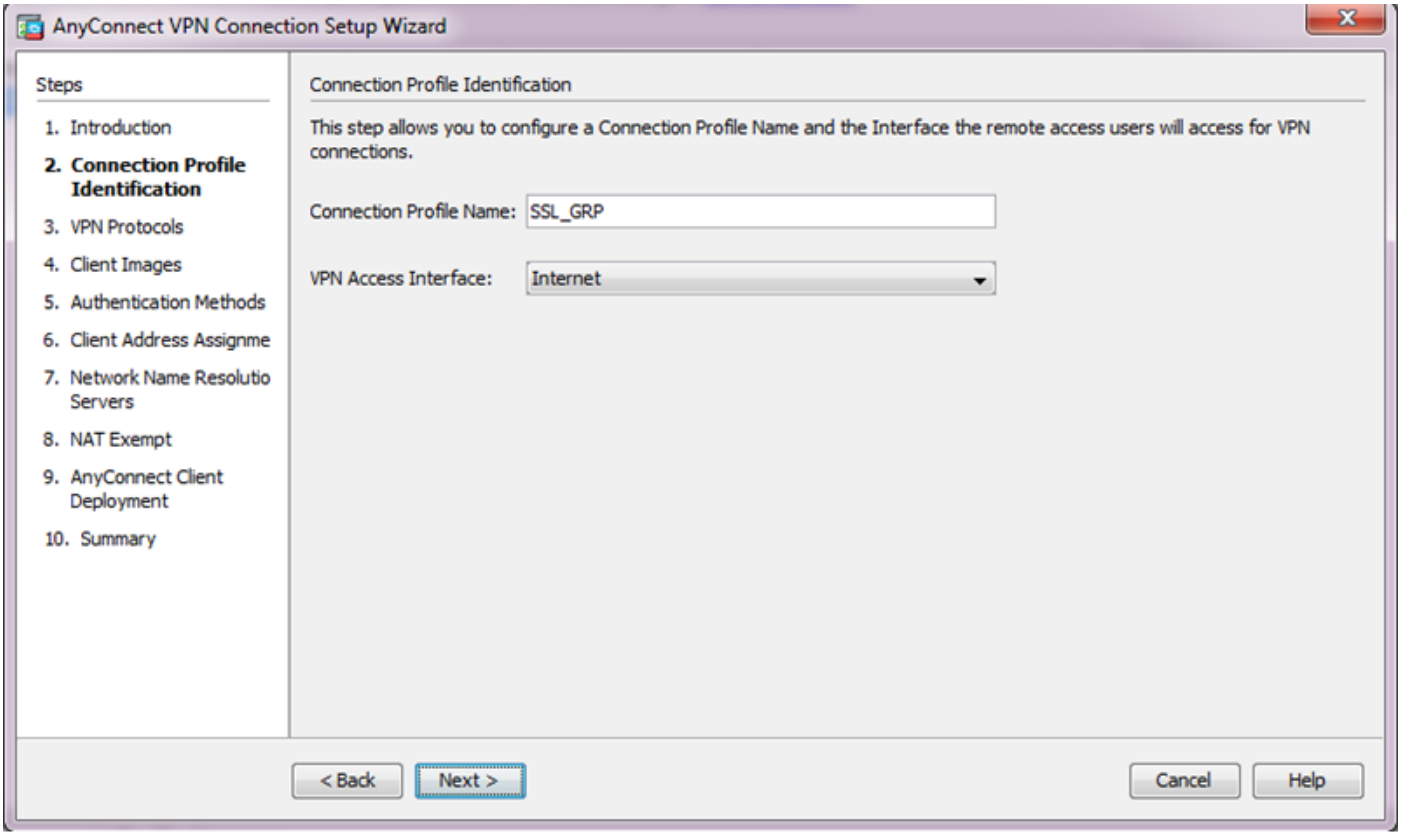
يمكن إستخدام معالج تكوين AnyConnect/CLI لتكوين AnyConnect Secure Mobility Client. قبل ASA حماية جدار صرق/قرص المؤقتة الذاكرة إلى AnyConnect لعميل حزمة عميل تحميل من تأكد المتابعة.

أكمل هذه الخطوات لتكوين AnyConnect Secure Mobility Client عبر معالج التكوين:

1. قم بتسجيل الدخول إلى ASDM وانتقل إلى معالجات> VPN > معالج AnyConnect VPN.
لبدء معالج التكوين وانقر فوق التالي.



2. أدخل اسم ملف تعريف الاتصال، واختر الواجهة التي سيتم إنهاء VPN عليها من القائمة المنسدلة لواجهة الوصول إلى شبكة VPN، وانقر فوق التالي.



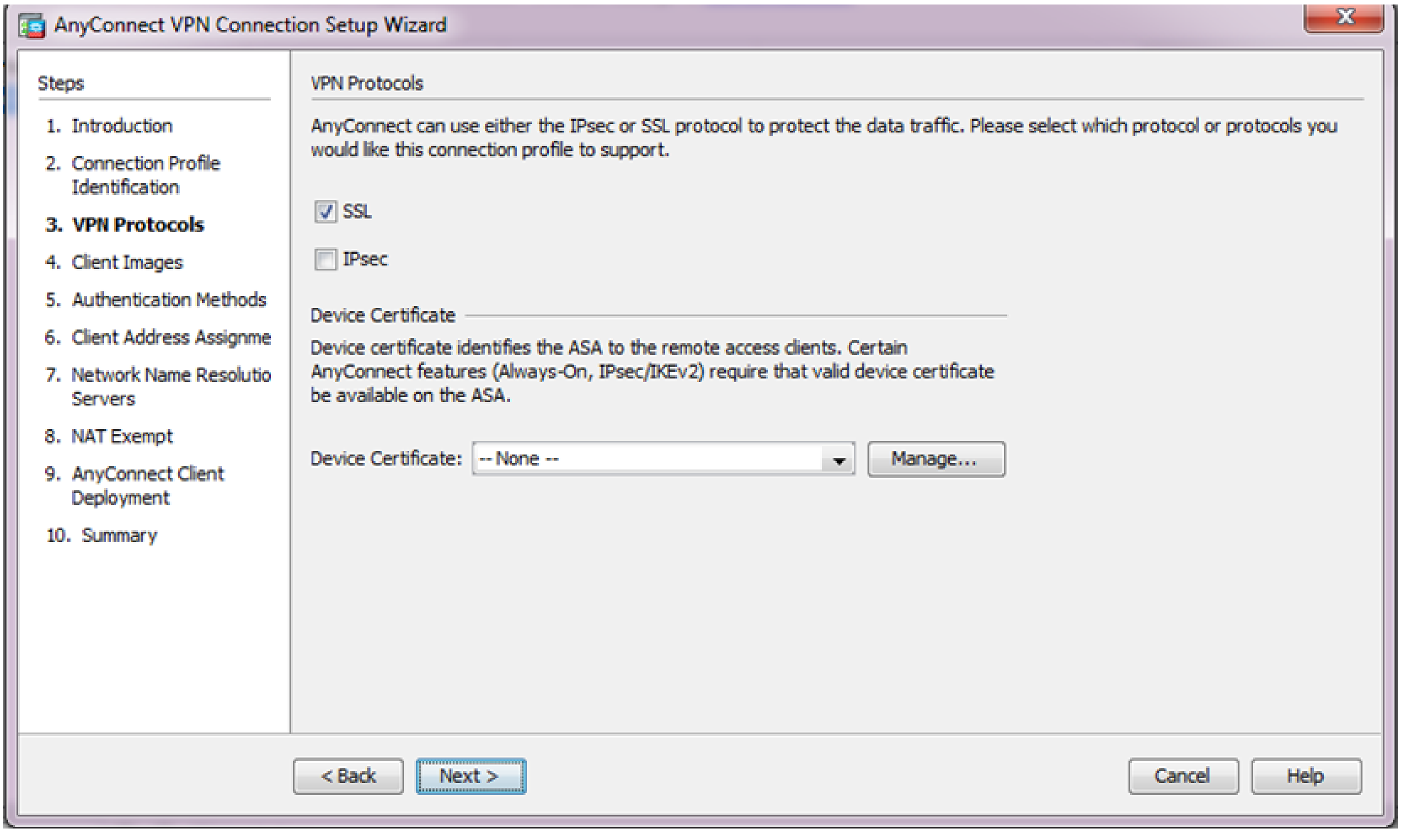
3. حدد خانة الاختيار SSL لتمكين طبقة مآخذ التوصيل الآمنة (SSL). يمكن أن تكون شهادة الجهاز عبارة عن شهادة صادرة عن جهة خارجية موثوق بها (مثل Verisign أو Entrust)، أو شهادة موقعة ذاتيًا. إذا كانت الشهادة مثبتة بالفعل على ASA، فيمكن اختيارها من خلال القائمة

المنسدلة.

1. ملاحظة: هذه الشهادة هي الشهادة من جانب الخادم التي سيتم تقديمها من قبل ASA إلى عملاء SSL. إذا لم تكن هناك شهادات خادم مثبتة حاليا على ASA مما يجب إنشاء شهادة موقعة ذاتيا، فانقر بعد ذلك على إدارة.

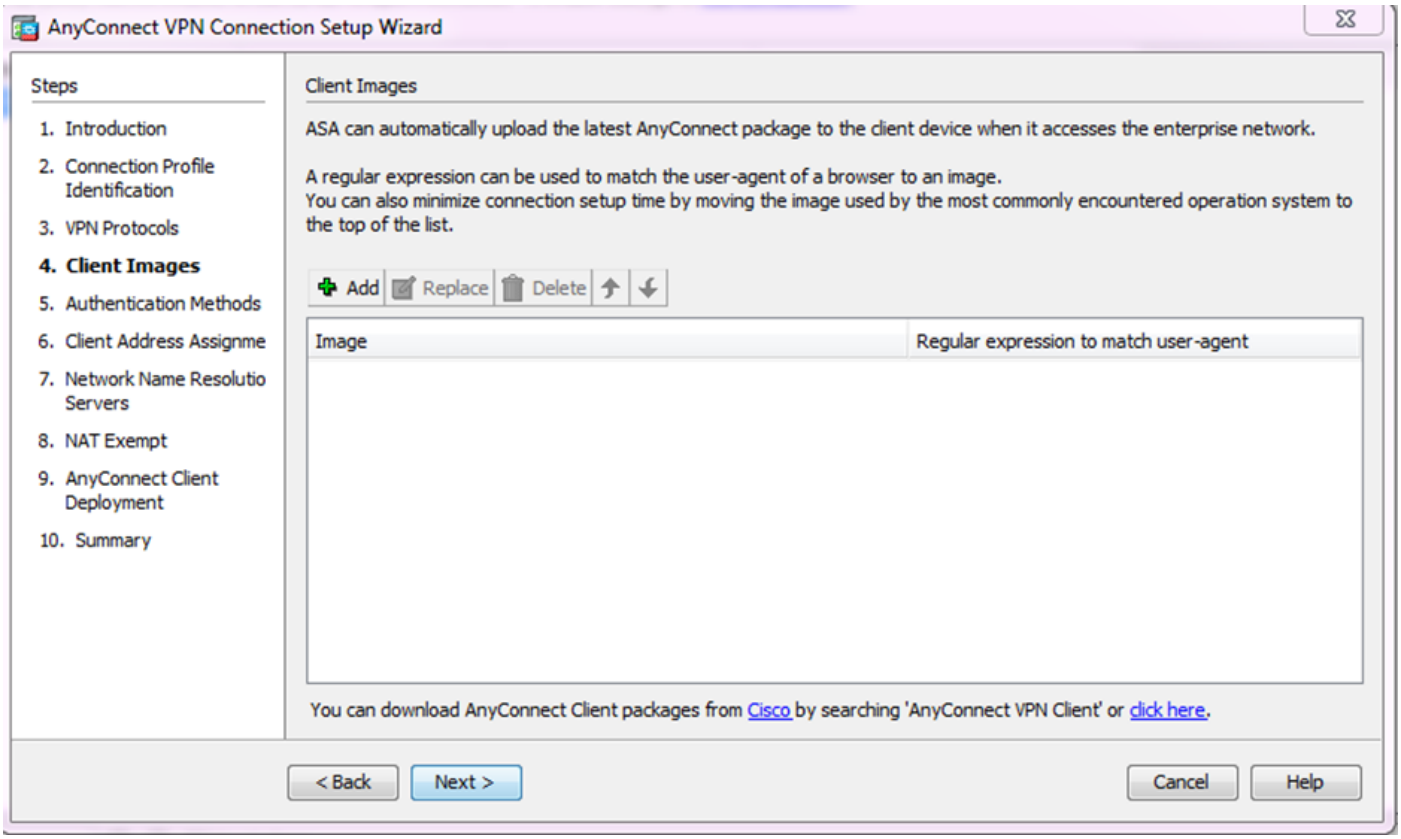
لتثبيت شهادة جهة خارجية، أكمل الخطوات الموضحة في مستند Cisco [ASA 8.x تثبيت شهادات بائعين من جهة خارجية يدوياً للاستخدام مع نموذج تكوين WebVPN.]

- قم بتمكين بروتوكولات VPN وشهادة الجهاز.
- انقر فوق Next (التالي).

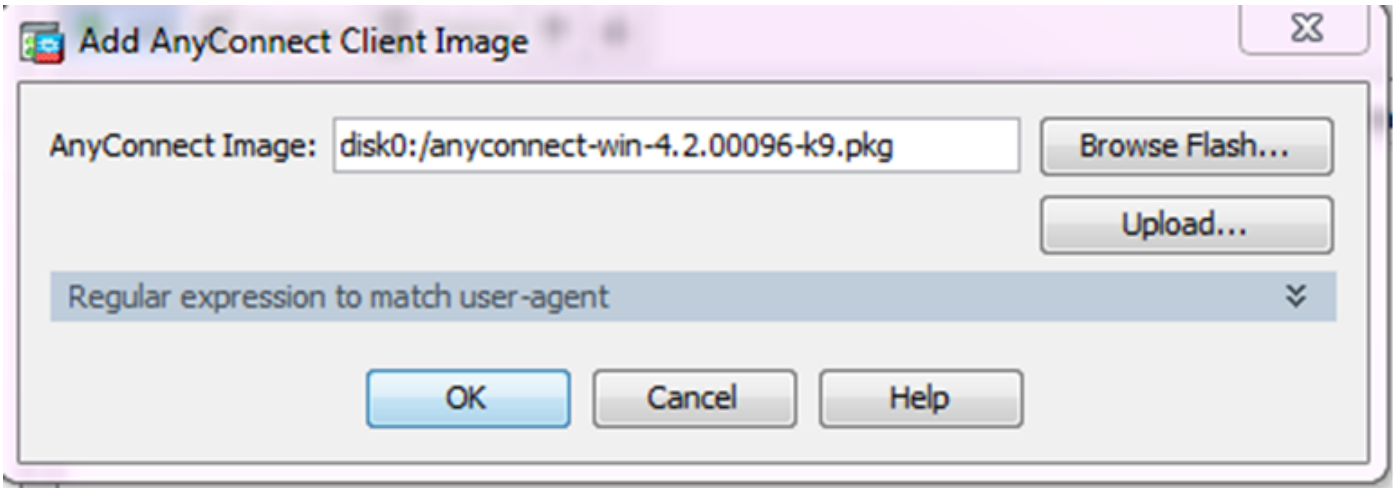


4. انقر فوق إضافة لإضافة حزمة عميل AnyConnect (.pkg file) من محرك الأقراص المحلي أو من ذاكرة Flash/disk الخاصة ب ASA.

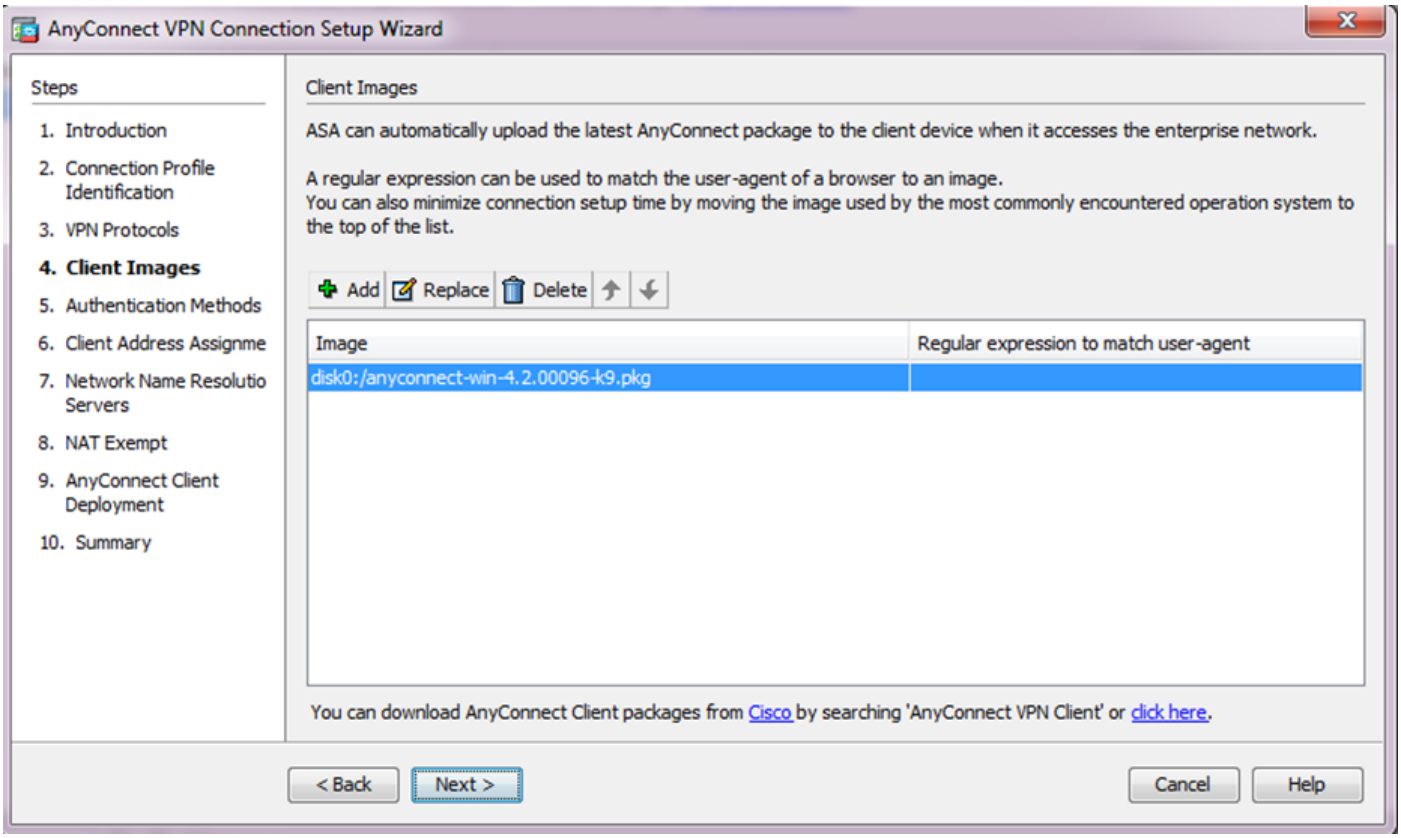
انقر فوق إستعراض ذاكرة Flash (الذاكرة المؤقتة) لإضافة الصورة من محرك أقراص Flash (الذاكرة المؤقتة)، أو انقر فوق تحميل لإضافة الصورة من محرك الأقراص المحلي للجهاز المضيف.



- يمكنك تحميل ملف AnyConnect.pkg إما من ذاكرة ASA Flash/Disk(إذا كانت الحزمة موجودة بالفعل) أو من محرك الأقراص المحلي.
- إستعراض الذاكرة المؤقتة - لتحديد حزمة AnyConnect من ذاكرة ASA المؤقتة/الأقراص.
- التحميل - لتحديد حزمة AnyConnect من المحرك المحلي للجهاز المضيف.
- وانقر فوق OK.

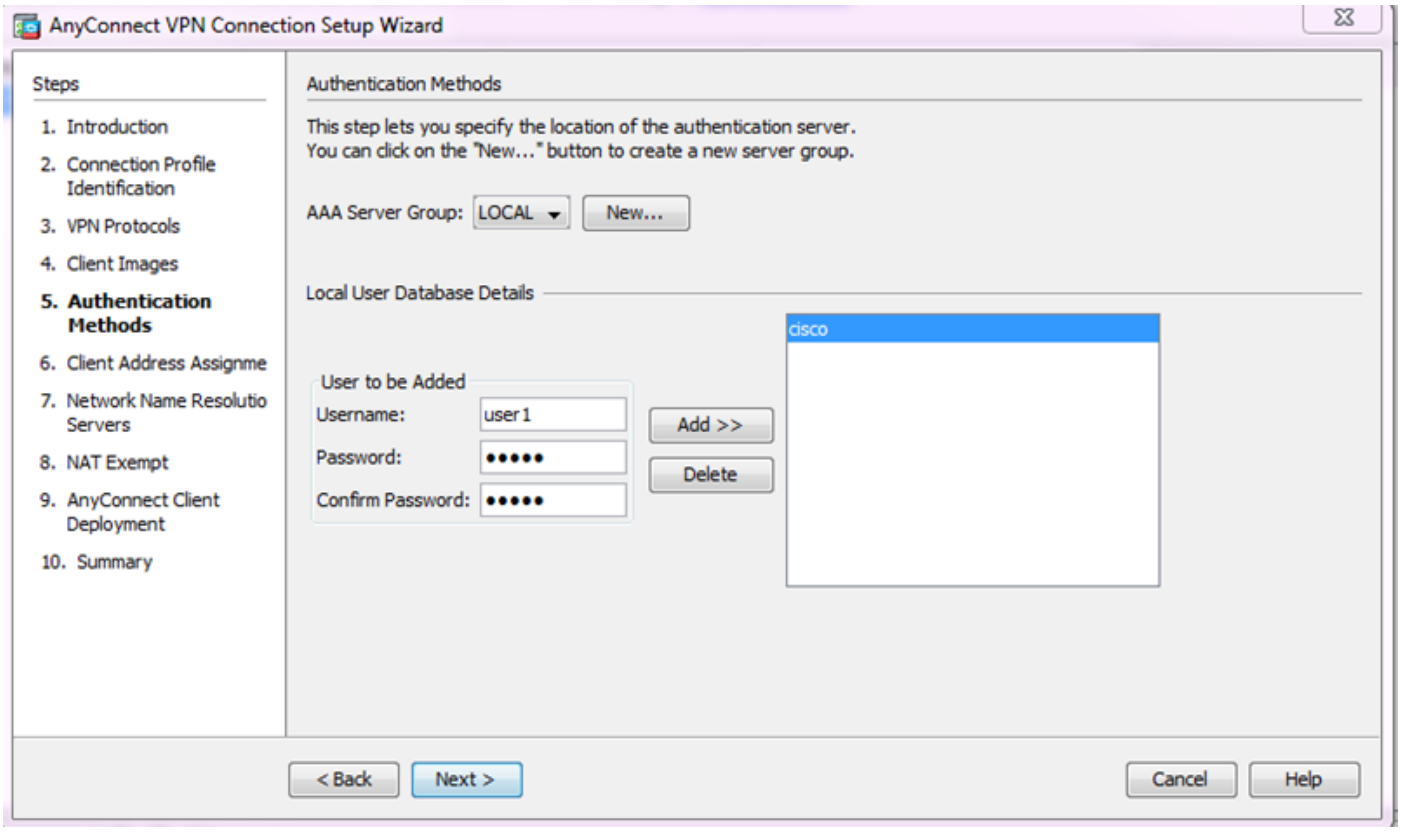


- انقر فوق Next (التالي).

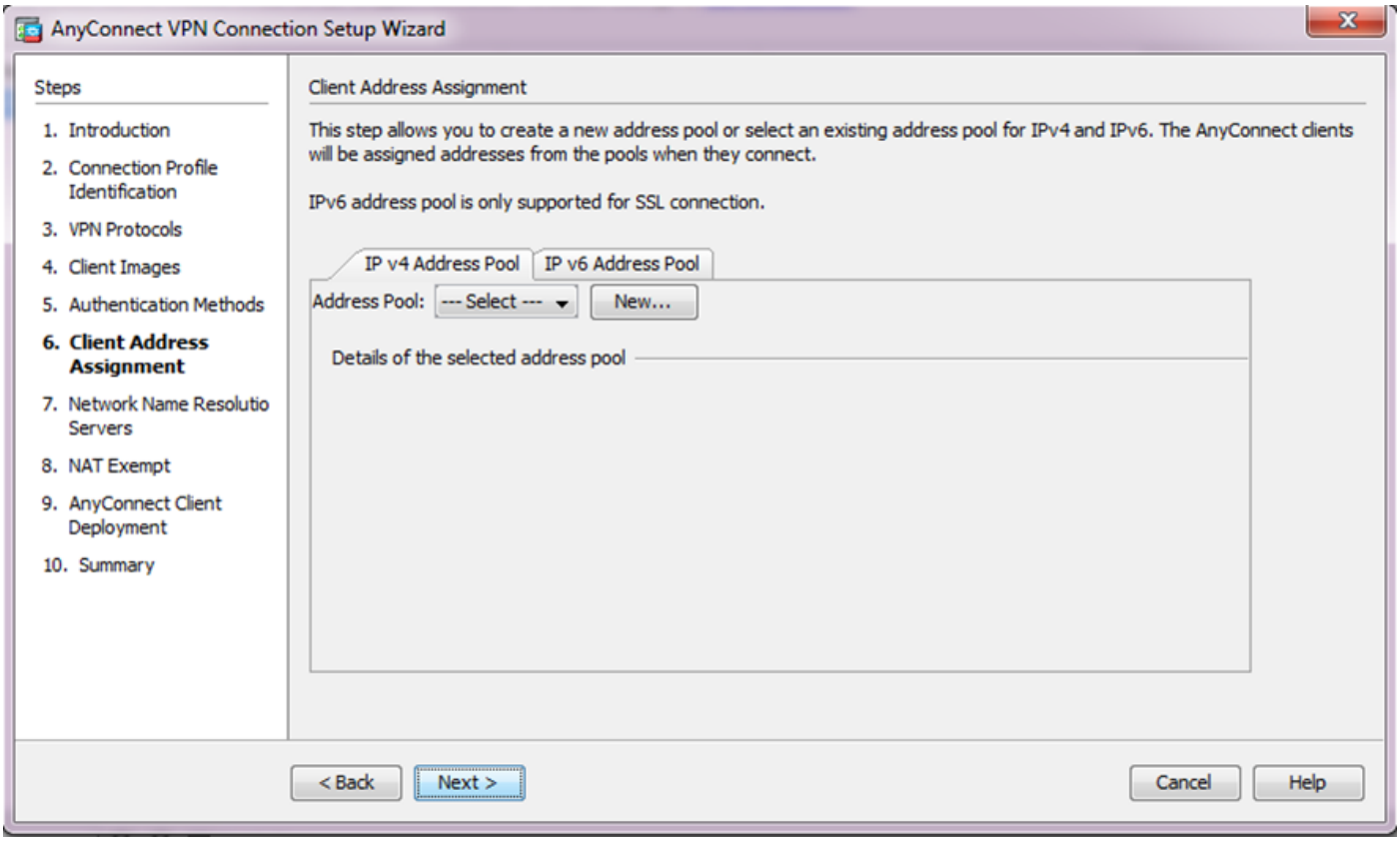


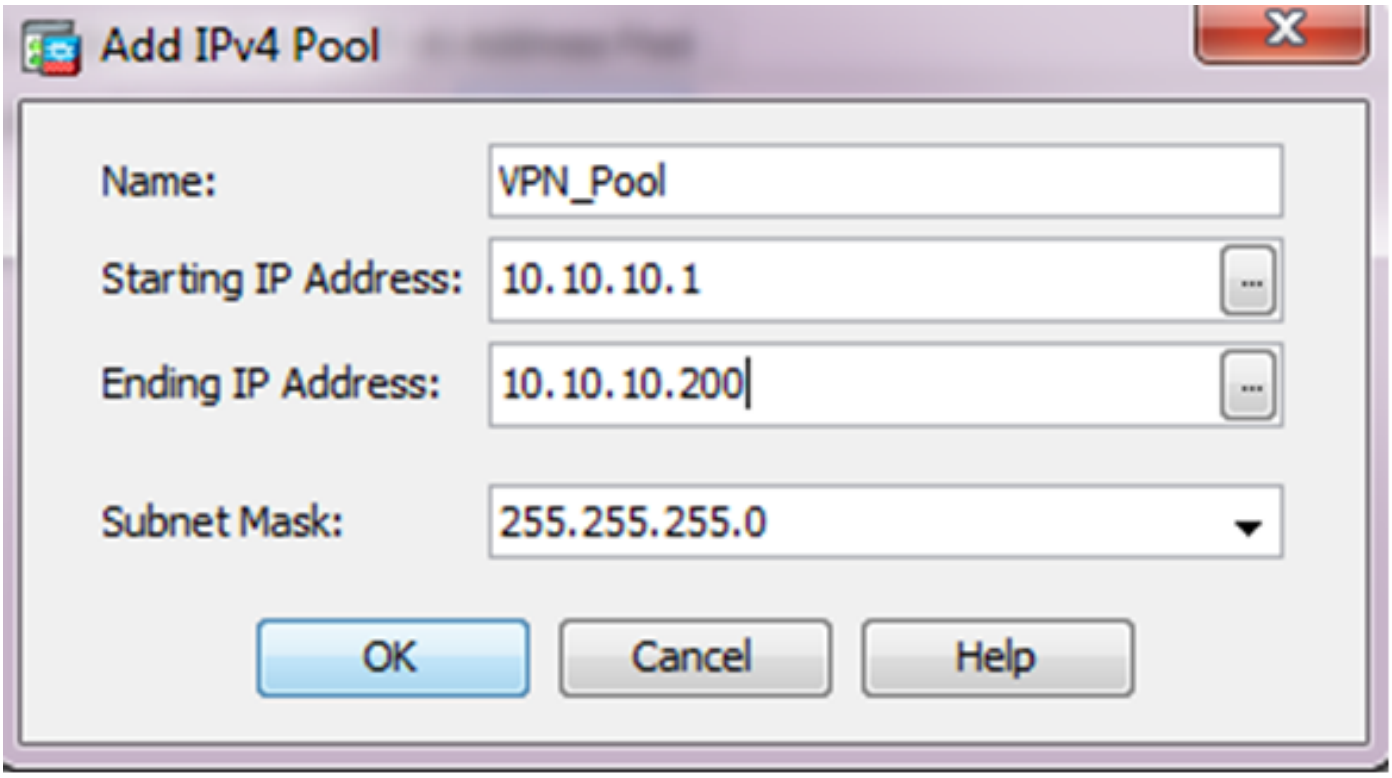
5. يمكن إكمال مصادقة المستخدم عبر مجموعات خوادم المصادقة والتفويض والمحاسبة (AAA). إذا تم تكوين المستخدمين بالفعل، فأختر محلي وانقر فوق التالي. وإلا قم بإضافة مستخدم إلى قاعدة بيانات المستخدم المحلية وانقر فوق التالي.

ملاحظة: في هذا المثال، يتم تكوين المصادقة المحلية، مما يعني أنه سيتم استخدام قاعدة بيانات المستخدم المحلي على ASA للمصادقة.

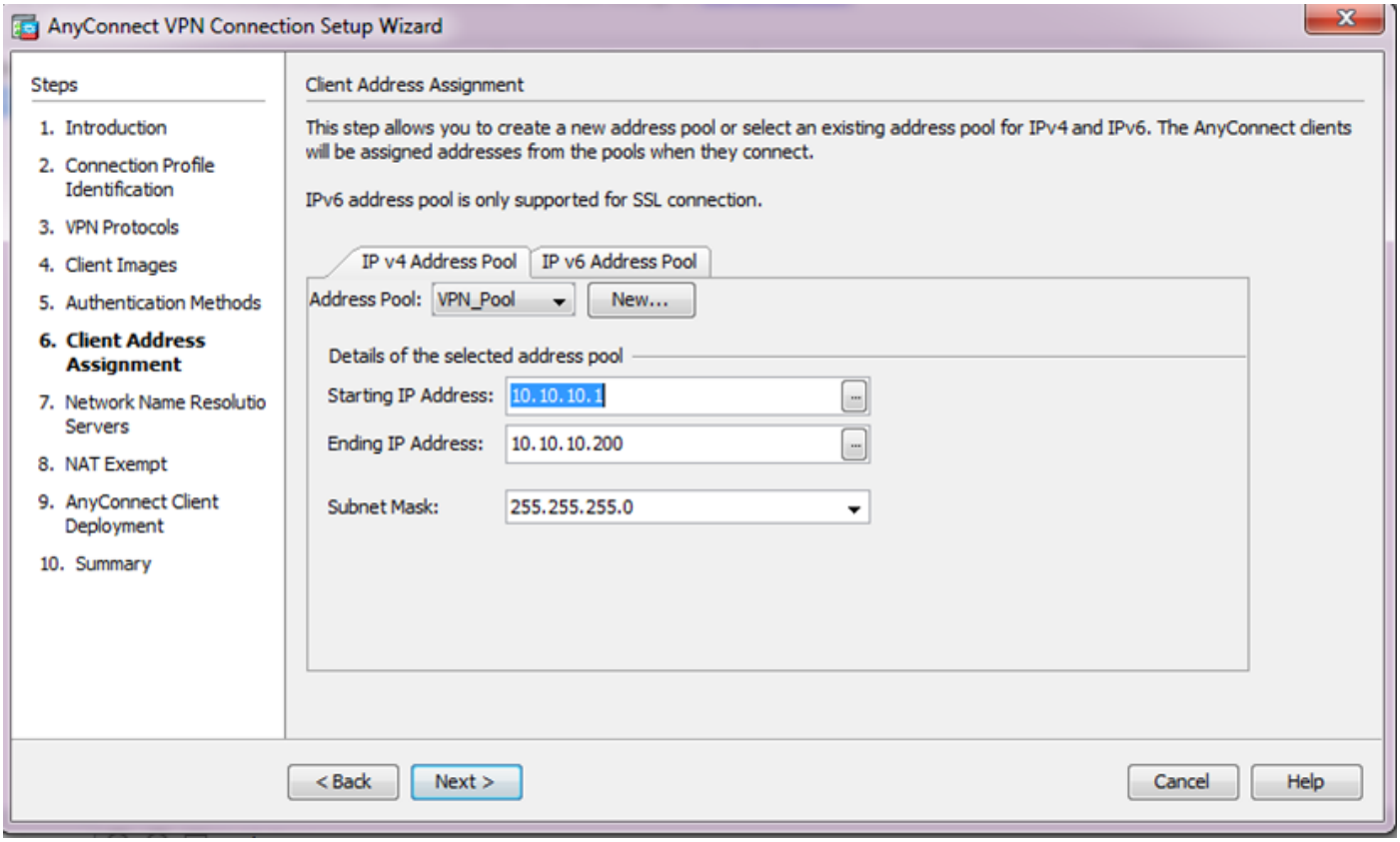


6. تأكد من تكوين تجمع العناوين لعملاء VPN. إذا تم تكوين تجمع IP بالفعل، فقم بتحديده من القائمة المنسدلة. وإذا لم تكن هناك مساحة، فانقر فوق جديد للتكوين. طقطقت ما إن يتم، بعد ذلك.

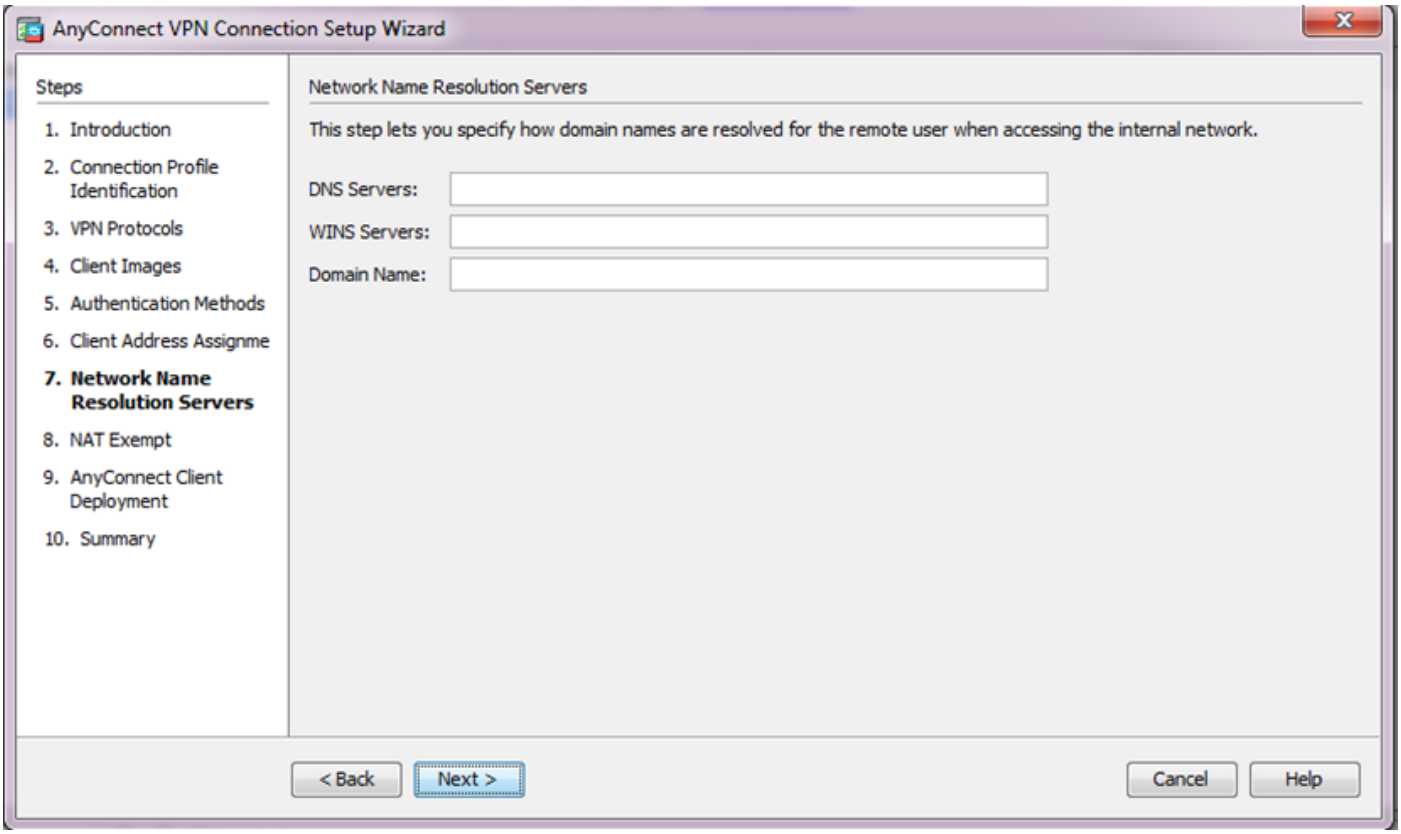




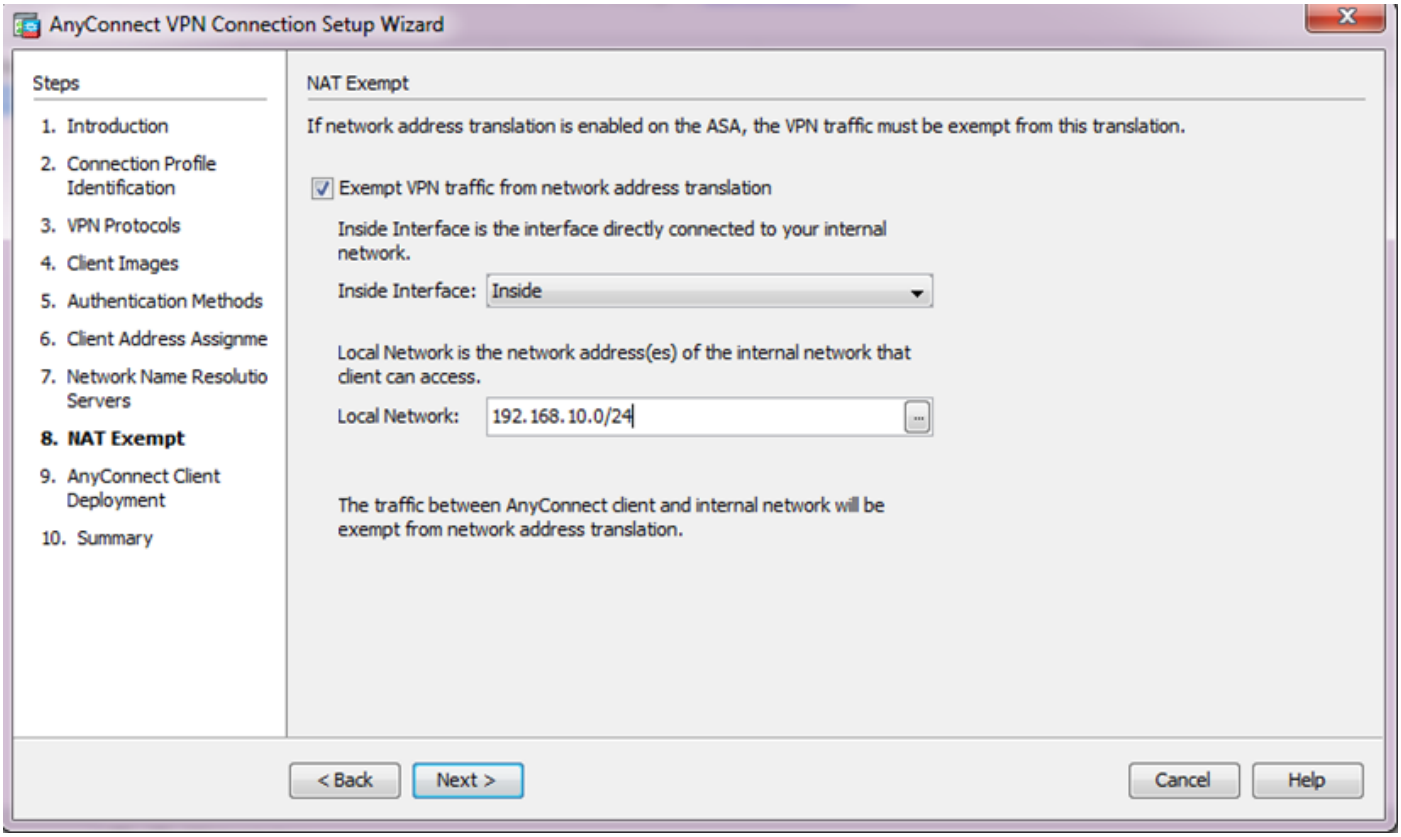
- انقر فوق Next (التالي).



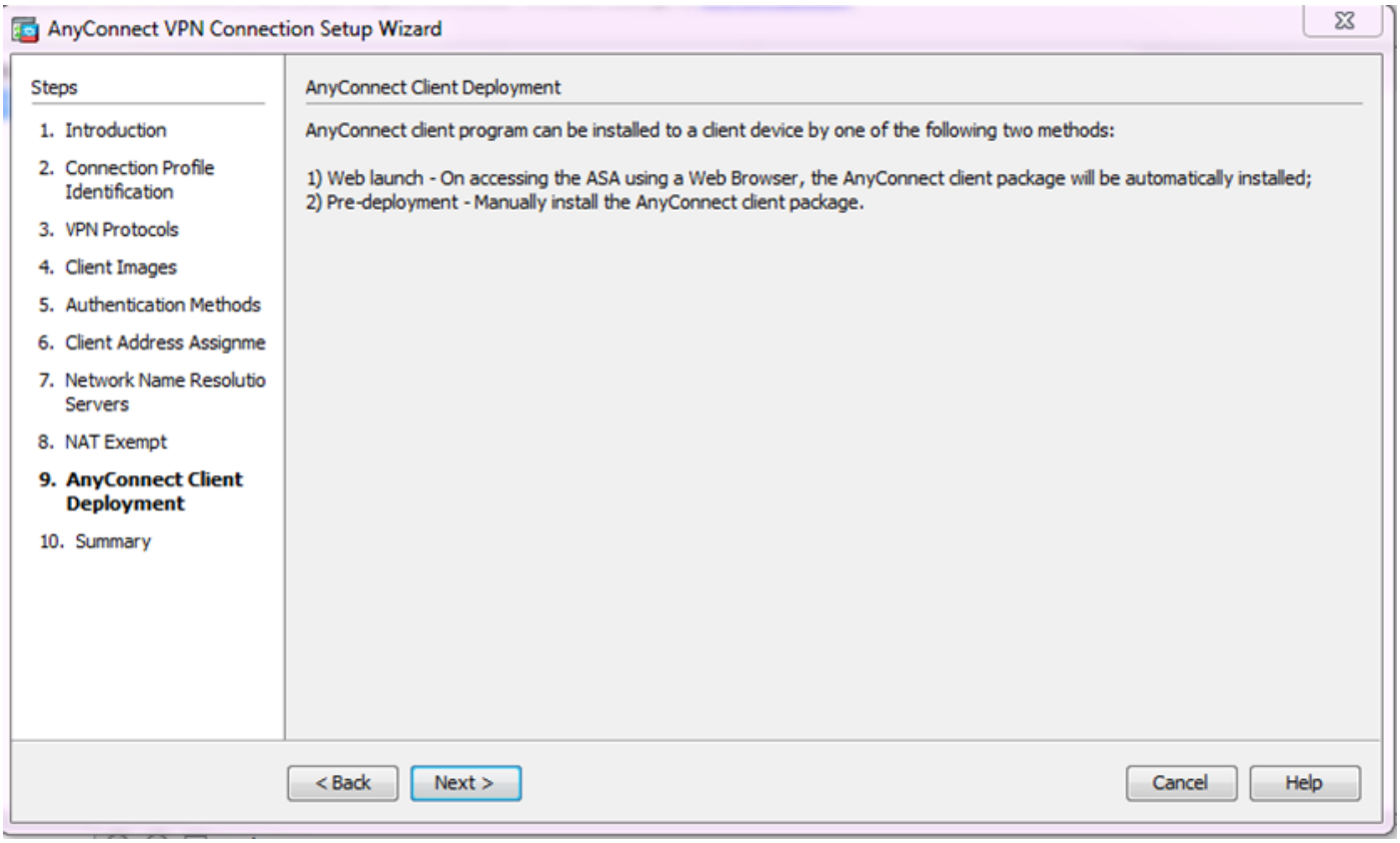
7. بشكل إختياري، قم بتكوين خوادم نظام اسم المجال (DNS) وشبكات DN في حقلي DNS واسم المجال، ثم انقر فوق التالي.



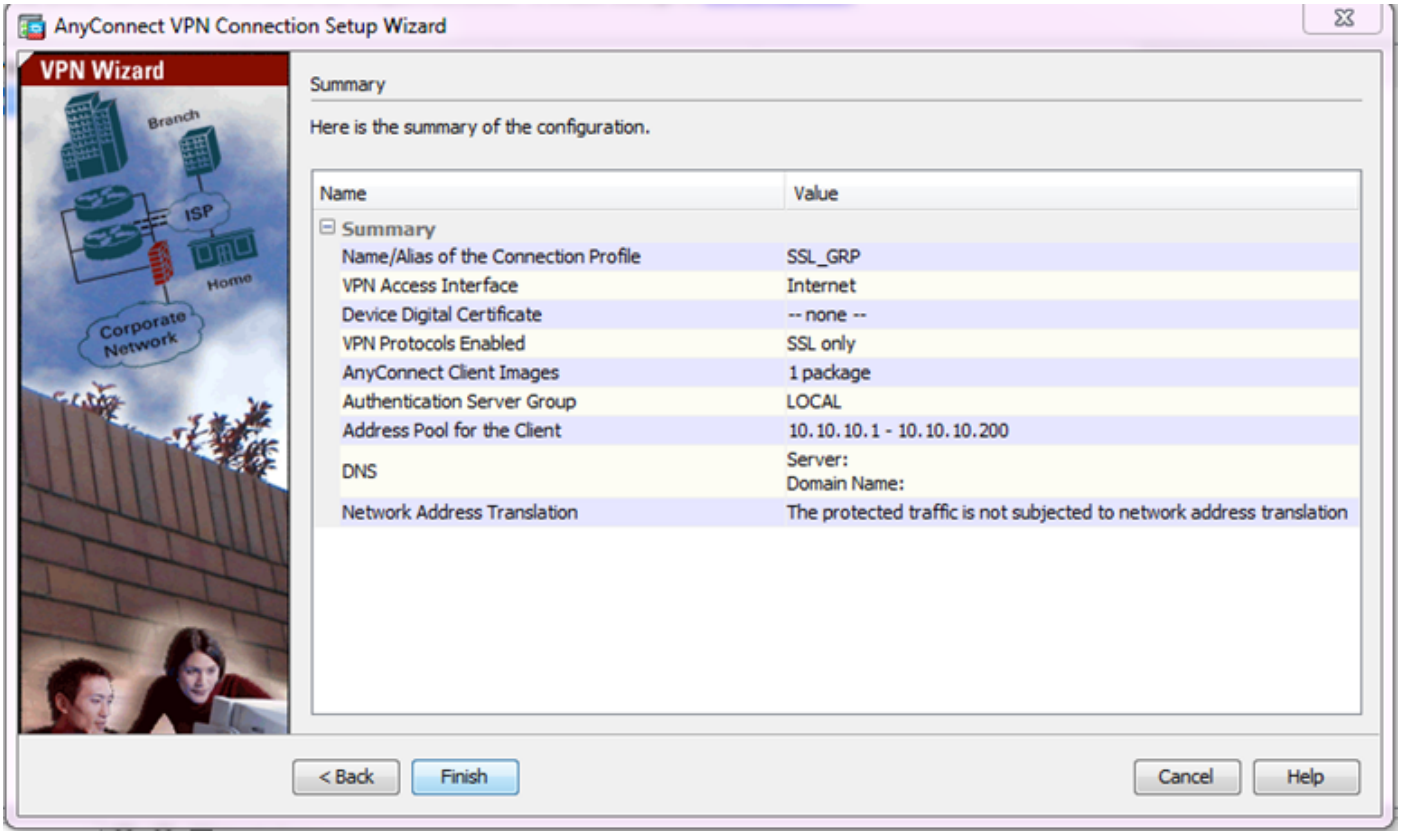
8. تأكد من أنه يجب إستثناء حركة مرور البيانات بين العميل والشبكة الفرعية الداخلية من أي ترجمة عنوان شبكة (NAT) ديناميكية. مكنت ال VPN معفي حركة مرور من شبكة عنوان ترجمة تدقيق ويشكل ال LAN قارن أن يكون استعملت للإعفاء. أيضا، حدد الشبكة المحلية التي يجب إعفاؤها وانقر فوق التالي.



9. انقر فوق التالي.

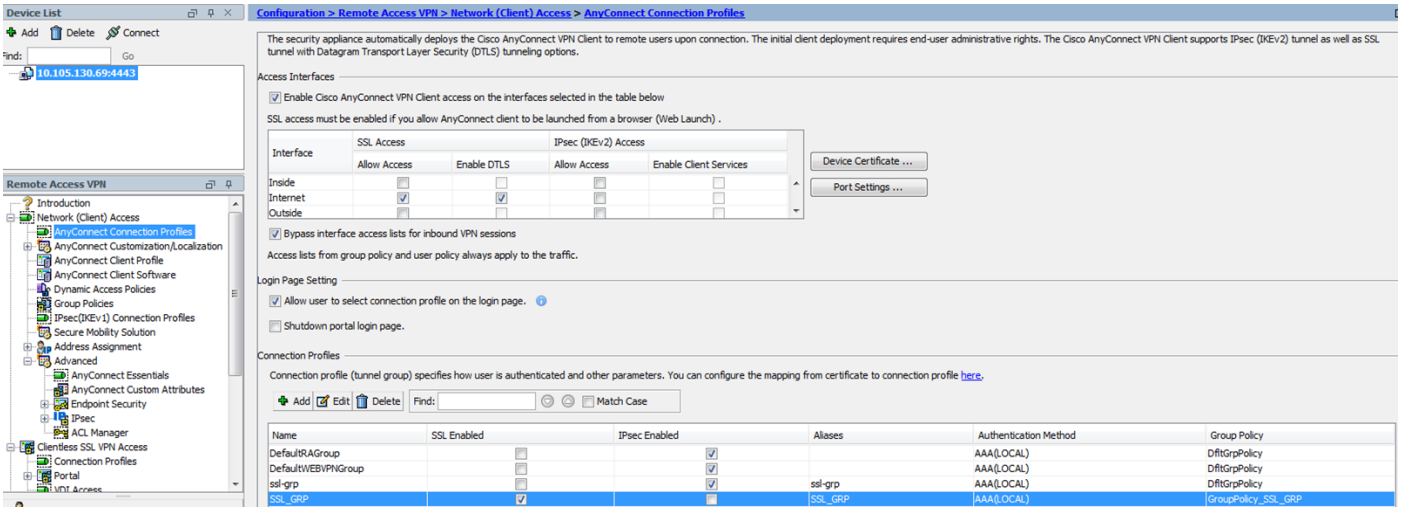


10. تعرض الخطوة الأخيرة الملخص، انقر فوق إنهاء لإكمال الإعداد.

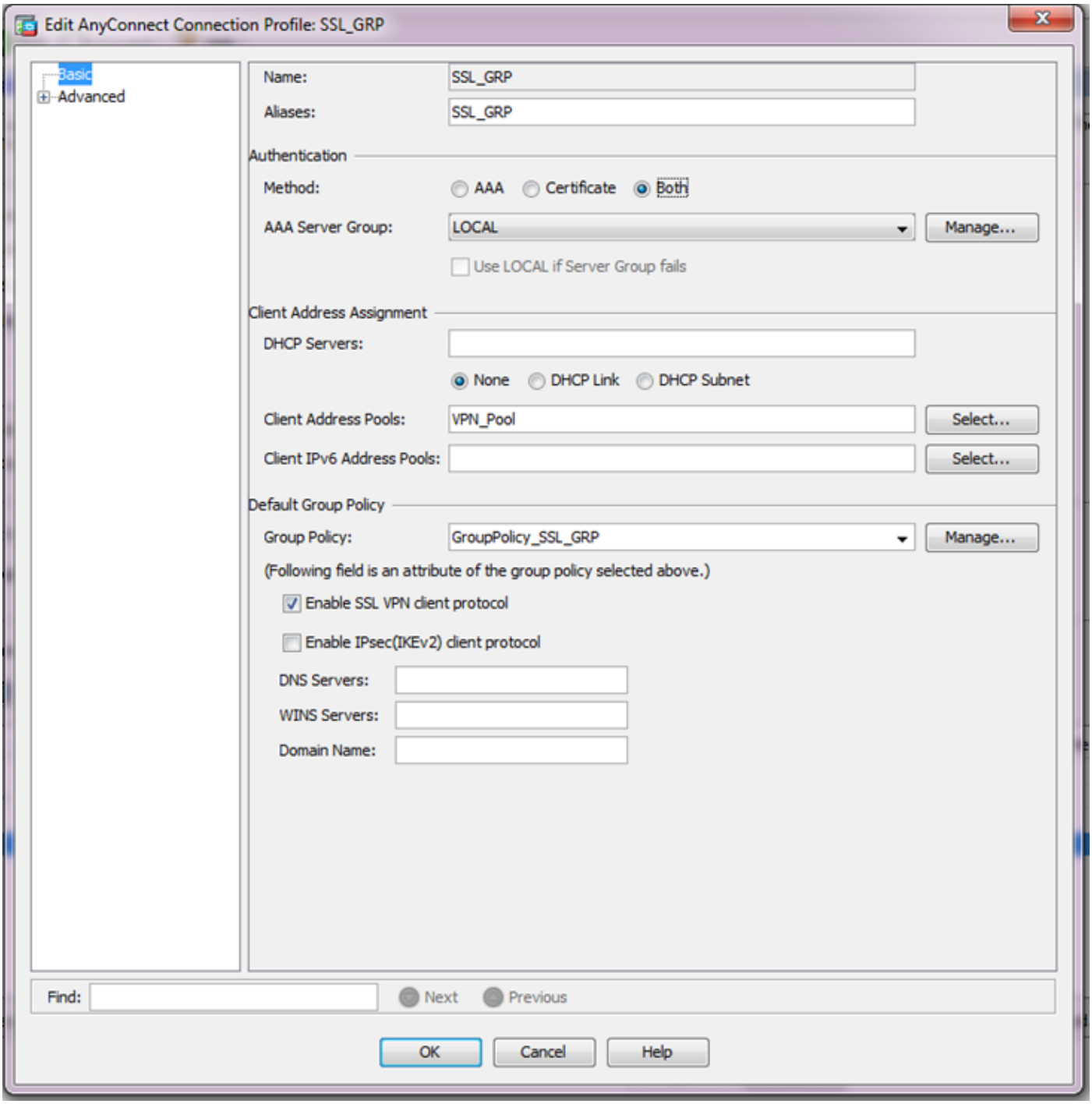


اكتمل تكوين عميل AnyConnect الآن. ومع ذلك، عند تكوين AnyConnect عبر معالج التكوين، فإنه يقوم بتكوين أسلوب المصادقة كالمصادقة والتفويض والمحاسبة (AAA) بشكل افتراضي. لمصادقة العملاء عبر الشهادات واسم المستخدم/كلمة المرور، يجب تكوين مجموعة النفق (ملف تعريف الاتصال) لاستخدام الشهادات و AAA كطريقة للمصادقة.

- انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > الوصول إلى الشبكة (العميل) > توصيفات توصيل AnyConnect.
- يجب أن ترى ملف تعريف الاتصال المضاف الجديد SSL_GRP المدرج.



- لتحديد AAA ومصادقة الشهادة، حدد ملف تعريف الاتصال SSL_GRP وانقر فوق تحرير.
- تحت أسلوب المصادقة، حدد الكل.



تكوين CLI ل AnyConnect

```
<#root>

!! *****Configure the VPN Pool*****

ip local pool VPN_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0

!! *****Configure Address Objects for VPN Pool and Local Network*****

object network NETWORK_OBJ_10.10.10.0_24
 subnet 10.10.10.0 255.255.255.0
```

```
object network NETWORK_OBJ_192.168.10.0_24
 subnet 192.168.10.0 255.255.255.0
 exit


!! *****Configure WebVPN*****


webvpn
 enable Internet
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 exit

!! *****Configure User*****

username user1 password mbO2jYs13AXlIAGa encrypted privilege 2

!! *****Configure Group-Policy*****


group-policy GroupPolicy_SSL_GRP internal
group-policy GroupPolicy_SSL_GRP attributes
 vpn-tunnel-protocol ssl-client
 dns-server none
 wins-server none
 default-domain none
 exit

!! *****Configure Tunnel-Group*****

tunnel-group SSL_GRP type remote-access
tunnel-group SSL_GRP general-attributes
 authentication-server-group LOCAL
default-group-policy GroupPolicy_SSL_GRP
 address-pool  VPN_Pool
tunnel-group SSL_GRP webvpn-attributes
 authentication aaa certificate
 group-alias SSL_GRP enable
 exit

!! *****Configure NAT-Exempt Policy*****

nat (Inside,Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24 destinati
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ملاحظة: تدعم أداة مترجم الإخراج (المعالج المسجلون فقط) بعض أوامر show. استخدم أمر show. مُخرَج الأمر "عرض تحليل لمترجم الإخراج لأداة

تأكد من تمكين خادم CA.

show crypto ca server

<#root>

```
ASA(config)# show crypto ca server
Certificate Server LOCAL-CA-SERVER:

Status: enabled

State: enabled
Server's configuration is locked  (enter "shutdown" to unlock it)

Issuer name: CN=ASA.local

CA certificate fingerprint/thumbprint: (MD5)
        32e868b9 351a1b07 4b59cce5 704d6615
CA certificate fingerprint/thumbprint: (SHA1)
        6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d
  Last certificate issued serial number: 0x1
CA certificate expiration timer: 19:25:42 UTC Jan 8 2019
          CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016
    Current primary storage dir: flash:/LOCAL-CA-SERVER/

    Auto-Rollover configured, overlap period 30 days
         Autorollover timer: 19:25:42 UTC Dec 9 2018

WARNING: Configuration has been modified and needs to be saved!!
```

تأكد من السماح للمستخدم بالتسجيل بعد إضافة:

<#root>

```
*****Before Enrollment*****

ASA#

show crypto ca server user-db

                username: user1
            email:    user1@cisco.com
            dn:       CN=user1,OU=TAC
        allowed:  19:03:11 UTC Thu Jan 14 2016
                        notified: 1 times
        enrollment status: Allowed to Enroll

>>> Shows the status "Allowed to Enroll"
```

```
*****After Enrollment*****


                                                username: user1
                                              email:    user1@cisco.com
                                              dn:       CN=user1,OU=TAC
                                    allowed:  19:05:14 UTC Thu Jan 14 2016
                                                notified: 1 times

                                          enrollment status: Enrolled

                                , Certificate valid until 19:18:30 UTC Tue Jan 10 2017,
                                                Renewal: Allowed
```

يمكنك التحقق من تفاصيل اتصال AnyConnect إما عبر CLI أو ASDM.

Via CLI

show vpn-sessionDB detail AnyConnect

<#root>

```
                                        ASA# show vpn-sessiondb detail anyconnect


                                                Session Type: AnyConnect Detailed

                                Username     : user1                  Index        : 1
                            Assigned IP  : 10.10.10.1            Public IP    : 10.142.189.181
                                        Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
                                                          License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
 Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
                                    Bytes Tx     : 13822                  Bytes Rx     : 13299
                                      Pkts Tx      : 10                     Pkts Rx      : 137
                                        Pkts Tx Drop : 0                      Pkts Rx Drop : 0
                                  Group Policy : GroupPolicy_SSL_GRP    Tunnel Group : SSL_GRP
                                                       Login Time   : 19:19:10 UTC Mon Jan 11 2016
                                                          Duration     : 0h:00m:47s
                                                          Inactivity   : 0h:00m:00s
                                                             NAC Result   : Unknown
                                     VLAN Mapping : N/A                    VLAN         : none

                                                       AnyConnect-Parent Tunnels: 1
                                                              SSL-Tunnel Tunnels: 1
                                                             DTLS-Tunnel Tunnels: 1

                                                                 AnyConnect-Parent:
                                                                 Tunnel ID    : 1.1
                                                           Public IP    : 10.142.189.181
                                 Encryption   : none                  Hashing      : none
                                  TCP Src Port : 52442                 TCP Dst Port : 443
                                                       Auth Mode    : Certificate and userPassword
                              Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
                                                             Client OS    : Windows
                                                          Client Type  : AnyConnect
                             Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
                                    Bytes Tx     : 6911                   Bytes Rx     : 768
                                      Pkts Tx      : 5                      Pkts Rx      : 1
```

```
                                Pkts Tx Drop : 0                       Pkts Rx Drop : 0

                                                                          SSL-Tunnel:
                                                                      Tunnel ID    : 1.2
                    Assigned IP  : 10.10.10.1            Public IP    : 10.142.189.181
                             Encryption   : RC4                    Hashing      : SHA1
                           Encapsulation: TLSv1.0                TCP Src Port : 52443
TCP Dst Port : 443                        Auth Mode    : Certificate and userPassword
                    Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
                                                             Client OS    : Windows
                                                        Client Type  : SSL VPN Client
                    Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
                           Bytes Tx     : 6911                    Bytes Rx     : 152
                             Pkts Tx      : 5                       Pkts Rx      : 2
                             Pkts Tx Drop : 0                       Pkts Rx Drop : 0

                                                                         DTLS-Tunnel:
                                                                      Tunnel ID    : 1.3
                    Assigned IP  : 10.10.10.1            Public IP    : 10.142.189.181
                             Encryption   : AES128                 Hashing      : SHA1
                           Encapsulation: DTLSv1.0               UDP Src Port : 59167
UDP Dst Port : 443                        Auth Mode    : Certificate and userPassword
                    Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
                                                             Client OS    : Windows
                                                       Client Type  : DTLS VPN Client
                    Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.2.00096
                         Bytes Tx     : 0                       Bytes Rx     : 12907
                           Pkts Tx      : 0                       Pkts Rx      : 142
                             Pkts Tx Drop : 0                       Pkts Rx Drop : 0

                                                                             NAC:
                     Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
                    SQ Int (T)   : 0 Seconds             EoU Age(T)   : 51 Seconds
                               Hold Left (T): 0 Seconds                Posture Token:
                                                                       Redirect URL :
```

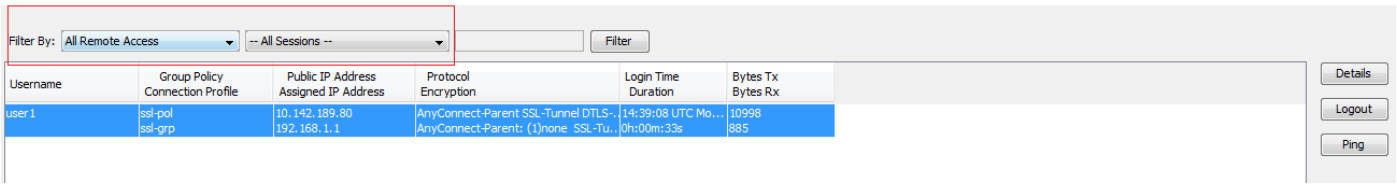
عبر ASDM

- انتقل إلى مراقبة > VPN > إحصائيات VPN > جلسات العمل.
- أختر عامل التصفية بواسطة الوصول عن بعد بالكامل.
- يمكنك تنفيذ أي من الإجراءات لعميل AnyConnect المحدد.

التفاصيل- توفير مزيد من المعلومات حول جلسة العمل

تسجيل الخروج- لتسجيل خروج المستخدم يدويا من وحدة الاستقبال والبث

إختبار الاتصال - لاختبار اتصال عميل AnyConnect من وحدة الاستقبال والبث



استكشاف الأخطاء وإصلاحها

يوفر هذه القسم معلومات يمكن إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

تنبيه: على ASA، يمكنك تعيين مستويات تصحيح أخطاء مختلفة؛ يتم استخدام المستوى الأول افتراضيًا. إذا قمت بتغيير مستوى تصحيح الأخطاء، فقد تتزايد درجة توسع تصحيح الأخطاء. قم بذلك بحذر، وخاصةً في بيئات الإنتاج.

- debug crypto ca
- debug crypto ca خادم
- debug crypto ca messages
- تصحيح أخطاء حركات crypto ca
- debug webVPN AnyConnect

يظهر إخراج تصحيح الأخطاء هذا عندما يتم تمكين خادم CA باستخدام الأمر no shutdown.

<#root>

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: input signal enqueued: no shut   >>>>> Command issued to Enable the CA server
                                                  Crypto CS thread wakes up!

                        CRYPTO_CS: enter FSM: input state disabled, input signal no shut
                                                CRYPTO_CS: starting enabling checks
                                              CRYPTO_CS: found existing serial file.
CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019
    CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate
            CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
                                                  CRYPTO_CS: DB version 1
                                      CRYPTO_CS: last issued serial number is 0x4
                                                CRYPTO_CS: closed ser file
            CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl
                                    CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists.
                                          CRYPTO_CS: Read 220 bytes from crl file.
                                                CRYPTO_CS: closed crl file
                CRYPTO_PKI: Storage context locked by thread Crypto CA Server

                                                CRYPTO_PKI: inserting CRL
                                    CRYPTO_PKI: set CRL update timer with delay: 20250
                CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016

                CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016
                CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016
                                    CRYPTO_PKI: CRL cache delay being set to: 20250000
            CRYPTO_PKI: Storage context released by thread Crypto CA Server
```

```
CRYPTO_CS: Inserted Local CA CRL into cache!

CRYPTO_CS: shadow not configured; look for shadow cert
CRYPTO_CS: failed to find shadow cert in the db
CRYPTO_CS: set shadow generation timer
CRYPTO_CS: shadow generation timer has been set
CRYPTO_CS: Enabled CS.
CRYPTO_CS: exit FSM: new state enabled
CRYPTO_CS: cs config has been locked.

Crypto CS thread sleeps!
```

يظهر إخراج تصحيح الأخطاء هذا تسجيل العميل

<#root>

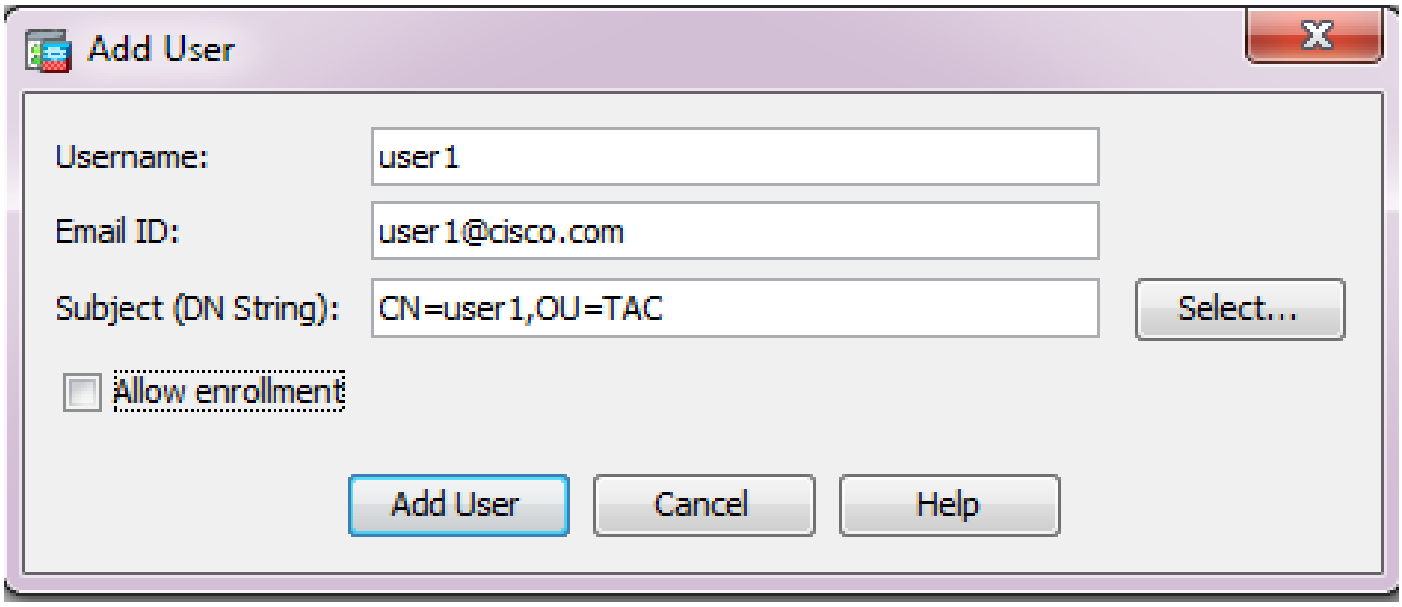
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

قد يفشل تسجيل العميل بموجب هذه الشروط:

السيناريو الأول.

- يتم إنشاء المستخدم في قاعدة بيانات خادم CA بدون إذن التسجيل.



مكافئ واجهة سطر الأوامر (CLI):

<#root>

```
ASA(config)# show crypto ca server user-db

                username: user1
            email:    user1@cisco.com
            dn:       CN=user1,OU=TAC
              allowed:  <not allowed>
                    notified: 0 times

enrollment status: Not Allowed to Enroll
```

- في الحالة التي يكون فيها المستخدم غير مسموح له بالتسجيل، تقوم محاولة إنشاء/إرسال بريد إلكتروني إلى OTP للمستخدم بإنشاء رسالة الخطأ هذه.

2. السيناريو

- تحقق من المنفذ والواجهة التي يتوفر عليها مدخل التسجيل باستخدام الأمر show run webVPN. المنفذ الافتراضي هو 443 ولكن يمكن تعديله.
- تأكد من أن العميل لديه إمكانية الوصول إلى الشبكة إلى عنوان IP الخاص بالواجهة التي يتم تمكين webVPN عليها على المنفذ المستخدم للوصول بنجاح إلى مدخل التسجيل.

قد يفشل العميل في الوصول إلى مدخل تسجيل ASA في هذه الحالات:

1. إذا قام أي جهاز وسيط بحظر الاتصالات الواردة من العميل إلى IP webVPN الخاص بـ ASA على المنفذ المحدد.
2. تم إيقاف حالة الواجهة التي يتم تمكين WebVPN عليها.

- يوضح هذا الإخراج أن مدخل التسجيل متاح على عنوان IP الخاص بواجهة الإنترنت على المنفذ المخصص 4433.

<#root>

```
ASA(config)# show run webvpn

webvpn
```

```
port 4433


enable Internet

no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

3. السيناريو

- ل (الذاكرة المؤقتة) Flash ذاكرة وه CA Server Database Storage ل الافتراضي الموضع ASA.
- عانة أثناء مستخدم لل حفظه و PKCS12 ملف لإنشاء حرة مساحة Flash ذاكرة أن من تأكد التسجيل.
- في الحالة التي ال تتوفر فيها مساحة حرة كافية لذاكرة Flash (الذاكرة المؤقتة)، في حالة فشل ASA في إكمال عملية تسجيل العميل ويقوم بإنشاء سجلات تصحيح الأخطاء هذه:

<#root>

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255

CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12

CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.

CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1
```

معلومات ذات صلة

- Cisco ASA 5500 Series Adaptive Security Appliances أجهزة الأمان
- دليل استكشاف أخطاء عميل AnyConnect VPN Client والحلول - المشكلات الشائعة
- إدارة جلسات عميل AnyConnect ومراقبتها واستكشاف أخطائها وإصلاحها
- Cisco Systems - المستندات والدعم التقني

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).