ةيوولا ةقاطب عم ASA 8.x AnyConnect ةقداصم البلجيكية

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد مصادقة ASA 8.x AnyConnect لاستخدام بطاقة الهوية البلجيكية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- ASA 5505 مع برنامج ASA 8.0 المناسب
- عميل AnyConnect
- ASDM 6.0

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

المعرف الإلكتروني عبارة عن بطاقة PKI (بنية أساسية للمفتاح العام) صادرة عن الحكومة البلجيكية يجب على المستخدمين إستخدامها للمصادقة على كمبيوتر Windows بعيد. يتم تثبيت عميل برنامج AnyConnect على الكمبيوتر المحلي ويأخذ بيانات اعتماد المصادقة من الكمبيوتر البعيد. بمجرد اكتمال المصادقة، يحصل المستخدم البعيد على حق الوصول إلى الموارد المركزية من خلال نفق SSL كامل. يتم تزويد المستخدم البعيد بعنوان IP تم الحصول عليه من تجمع تتم إدارته بواسطة ASA.

إعداد الكمبيوتر المحلي

نظام تشغيل

يجب أن يكون نظام التشغيل (Windows أو MacOS أو Unix أو Linux) الموجود على الكمبيوتر المحلي متداولا مع تثبيت جميع التصحيحات المطلوبة.

قارئ بطاقات

يجب تثبيت قارئ بطاقات إلكتروني على الكمبيوتر المحلي لاستخدام بطاقة eID. قارئ البطاقة الالكترونية عبارة عن جهاز ينشئ قناة اتصال بين البرامج الموجودة على الكمبيوتر والشريحة الموجودة على بطاقة الهوية.

للحصول على قائمة بقارئ البطاقات المعتمد، راجع عنوان URL هذا:
http://www.cardreaders.be/en/default.htm

ملاحظة: لاستخدام قارئ البطاقة، يجب تثبيت برامج التشغيل الموصى بها من قبل مورد الأجهزة.

برنامج وقت تشغيل eID

يجب تثبيت برنامج وقت تشغيل eID الذي توفره الحكومة البلجيكية. يتيح هذا البرنامج للمستخدم البعيد قراءة محتويات بطاقة eID والتحقق من صحتها وطباعتها. ويتوفر البرنامج بالفرنسية والهولندية لأنظمة تشغيل Windows و Mac OS X و Linux.

لمزيد من المعلومات، ارجع إلى عنوان URL هذا:

- http://www.belgium.be/zip/eid_datacapture_nl.html

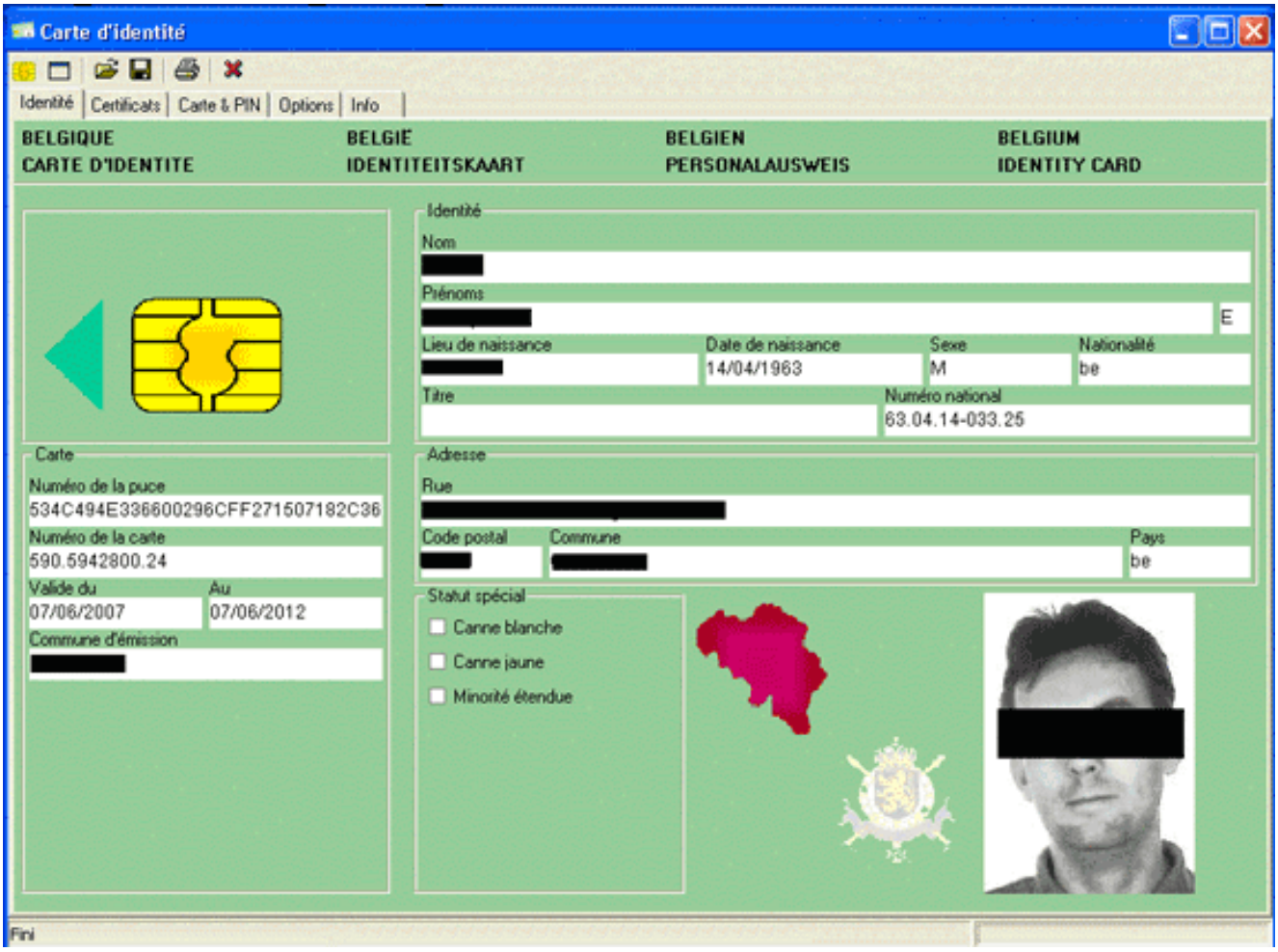
شهادة المصادقة

يجب إستيراد شهادة المصادقة إلى مخزن Microsoft Windows على الكمبيوتر المحلي. إذا فشل إستيراد الشهادة إلى المخزن، فلن يتمكن عميل AnyConnect من إنشاء اتصال SSL ب ASA.

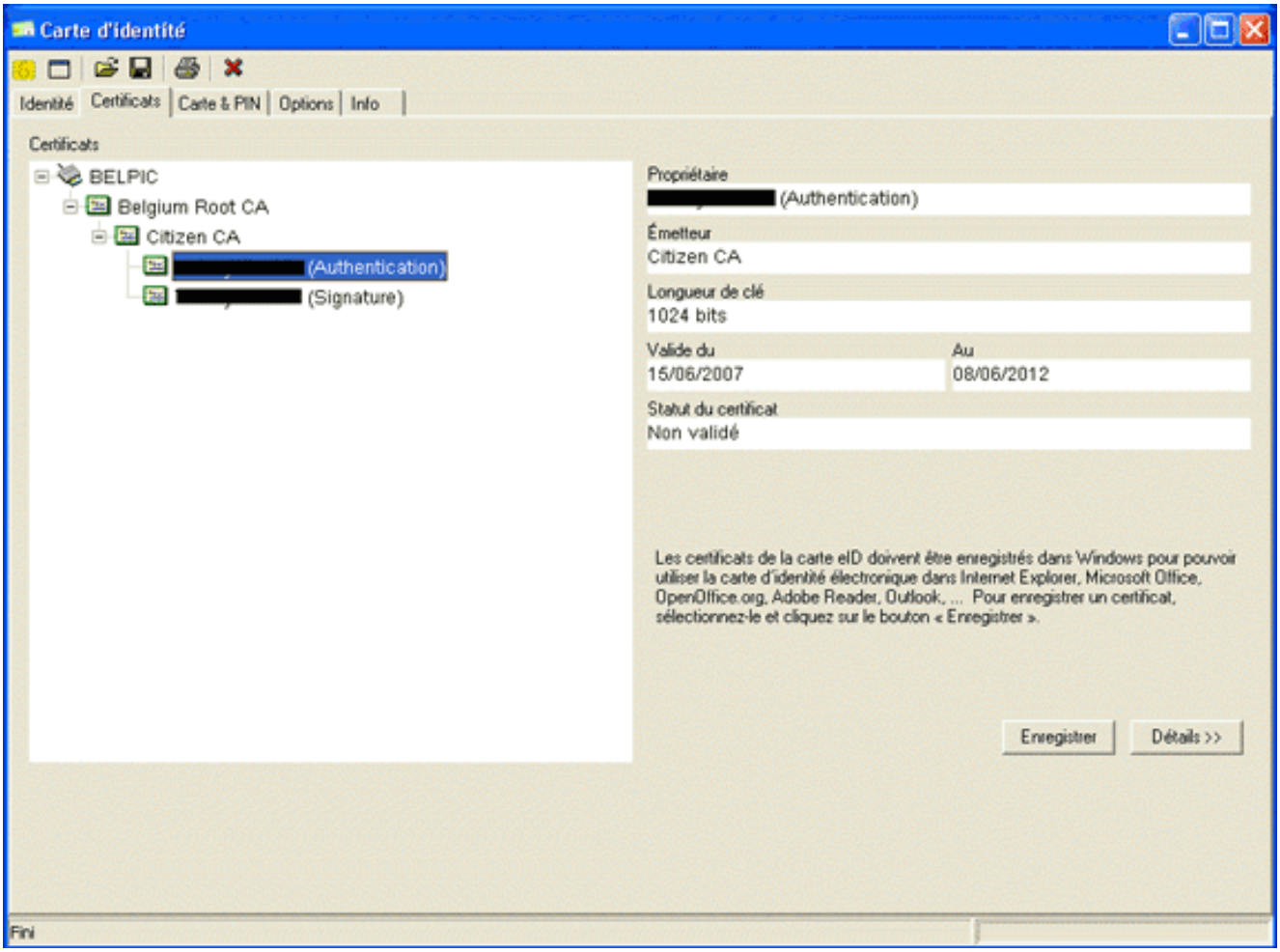
الإجراء

لاستيراد شهادة المصادقة إلى مخزن Windows، أكمل الخطوات التالية:

1. أدخل معرف eID الخاص بك في قارئ البطاقة، وقم بتشغيل البرامج الوسيطة للوصول إلى محتويات بطاقة eID.تظهر محتويات بطاقة eID.



2. انقر فوق علامة التبويب **شهادات** (FR).يتم عرض التدرج الهرمي للشهادات.



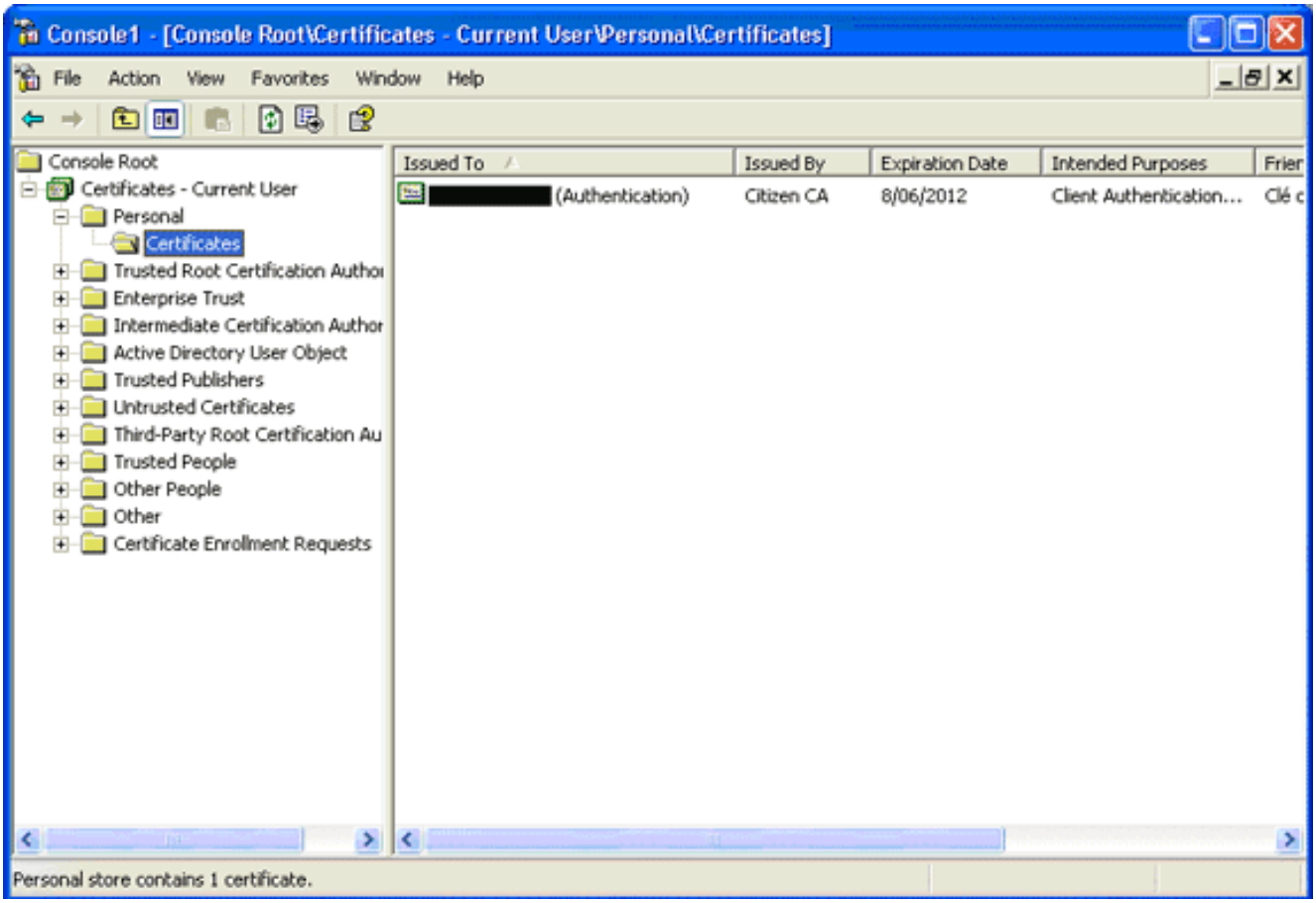
3. قم بتوسيع **جذر المرجع المصدق** في بلجيكا، ثم قم بتوسيع **Citizen CA**.
4. أختر إصدار **المصادقة** للشهادة المسماة.
5. انقر فوق زر **التسجيل** (FR).يتم نسخ الشهادة إلى مخزن Windows.

ملاحظة: عندما تنقر على زر **التفاصيل**، يظهر إطار يعرض تفاصيل عن الترخيص. في علامة التبويب تفاصيل، حدد حقل **الموضوع** لعرض حقل الرقم التسلسلي. يحتوي حقل الرقم التسلسلي على قيمة فريدة يتم إستخدامها لتفويض المستخدم. على سبيل المثال، الرقم التسلسلي "56100307215" يمثل مستخدم تاريخ ميلاده هو 3 أكتوبر 1956 برقم تسلسلي 072 ورقم شيك 15. *يجب إرسال طلب موافقة من السلطات الفيدرالية لتخزين هذه الأرقام. وتقع على عاتقكم مسؤولية إصدار الإقرارات الرسمية المناسبة فيما يتعلق بالاحتفاظ بقاعدة بيانات للمواطنين البلجيكيين في بلدكم.*

التحقق من الصحة

للتحقق من أن الشهادة تم إستيرادها بنجاح، أكمل الخطوات التالية:

1. على جهاز Windows XP، افتح نافذة DOS، واكتب الأمر **mmc**.يظهر تطبيق وحدة التحكم.
2. أختر **ملف > إضافة/إزالة الأداة الإضافية** (أو اضغط Ctrl+M).تظهر شاشة إضافة/إزالة أداة إضافية.
3. انقر فوق الزر **إضافة**.تظهر شاشة إضافة أداة إضافية مستقلة.
4. في قائمة الأدوات الإضافية المستقلة المتاحة، أختر **شهادات**، وانقر **إضافة**.
5. طقطقت **My user account** لاسلكي زر، وطقطقة **إنجاز**.تظهر الأداة الإضافية للشهادة في شاشة إضافة/إزالة أداة إضافية.
6. انقر فوق **إغلاق** لإغلاق شاشة إضافة أداة إضافية مستقلة، ثم انقر فوق **موافق** في شاشة إضافة/إزالة الأداة الإضافية لحفظ التغييرات والعودة إلى تطبيق وحدة التحكم.
7. ضمن المجلد الجذر لوحدة التحكم، قم بتوسيع **الشهادات - المستخدم الحالي**.
8. قم بتوسيع **التراخيص الشخصية**، ثم قم بتوسيع **التراخيص**.يجب أن تظهر الشهادة المستوردة في مخزن Windows كما هو موضح في هذه
الصورة:



تثبيت AnyConnect

يجب تثبيت "عميل AnyConnect" على الكمبيوتر البعيد. يستخدم برنامج AnyConnect ملف تكوين XML يمكن تحريره لإعداد قائمة بالعبارات المتاحة مسبقا. يتم تخزين ملف XML في هذا المسار على الكمبيوتر البعيد:

C:\Documents و Settings*٪username٪*\Application Data\Cisco\Cisco AnyConnect VPN Client

حيث *٪USERNAME٪* هو اسم المستخدم على الكمبيوتر البعيد.

اسم ملف XML هو *preferences.xml*. هنا مثال من محتويات الملف:

```
<?"xml version="1.0" encoding="UTF-8?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

حيث *192.168.0.1* هو عنوان IP الخاص ببوابة ASA.

متطلبات ASA

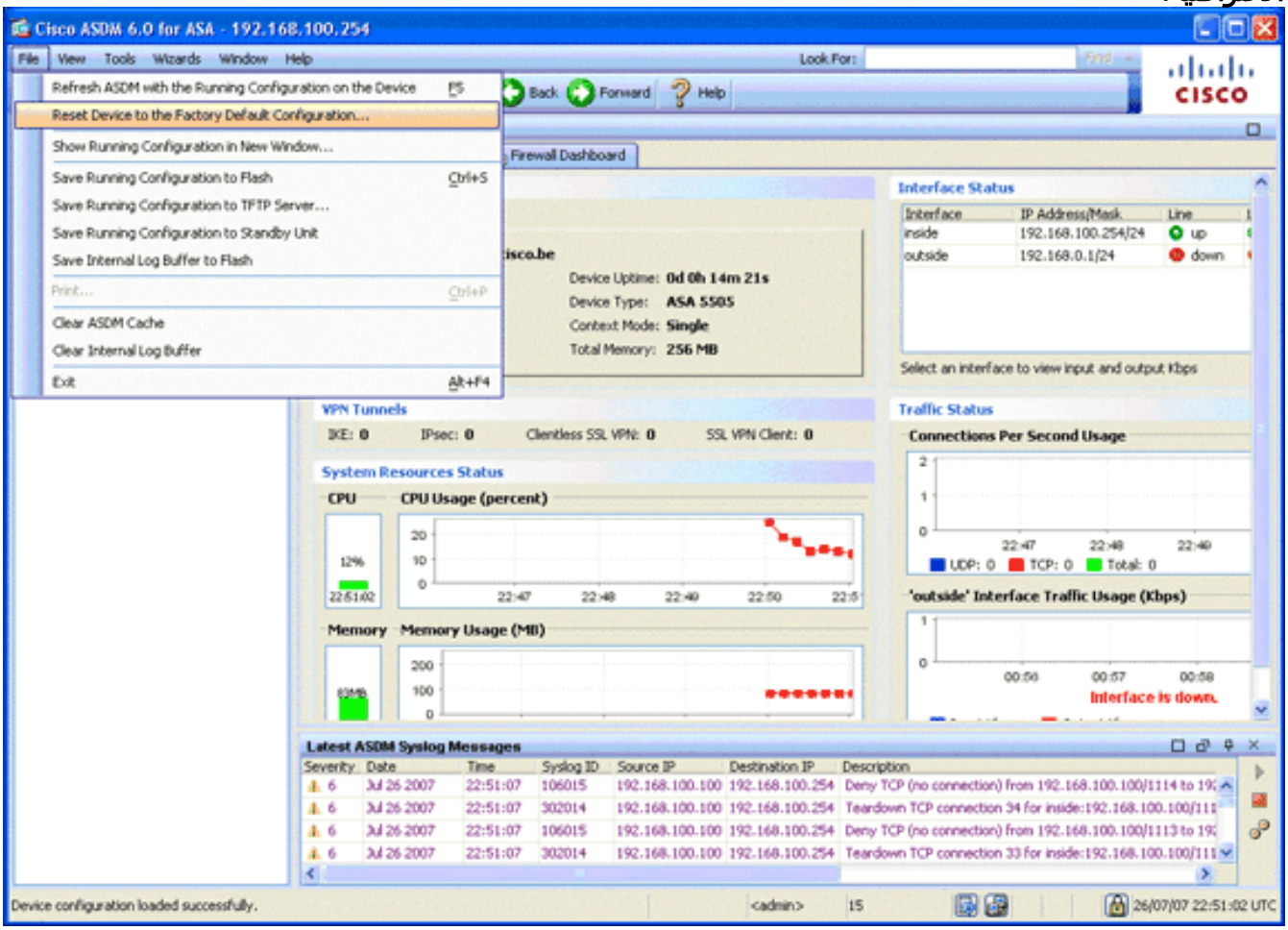
تأكد من استيفاء ASA لهذه المتطلبات:

- يجب تشغيل AnyConnect و ASDM في الذاكرة المؤقتة (flash).استعملت in order to أتمت الإجراء في هذا وثيقة، ASA 5505 مع المناسب ASA 8.0 برمجية ركبت. يجب تحميل تطبيقات AnyConnect و ASDM مسبقا في ذاكرة الفلاش. أستخدم الأمر **show flash** لعرض محتويات flash:

```
:ciscoasa#show flash
length--  -----date/time------  path--  --#--
Jun 26 2007 10:24:02  asa802-k8.bin    14524416  66
```

```
                    Jun 26 2007 10:25:28  asdm-602.bin      6889764  67
                    Jul 09 2007 07:37:06  anyconnect-win-2.0.0343-k9.pkg      2635734  68
```

- يجب أن يعمل ASA مع إعدادات المصنع الافتراضية.يمكنك تخطي هذا المتطلب إذا كنت تستخدم هيكل ASA جديد لإكمال الإجراءات في هذا المستند. وإلا، أكمل الخطوات التالية لإعادة ضبط ASA إلى إعدادات المصنع الافتراضية:في تطبيق ASDM، اتصل بهيكل ASA، واختر **ملف > إعادة ضبط الجهاز إلى تكوين إعدادات المصنع الافتراضية**.



أترك القيم الافتراضية في القالب.قم بتوصيل الكمبيوتر الشخصي لديك على الإيثرنت 1/0 داخل الواجهة، ثم جدد عنوان IP الخاص بك الذي سيتم توفيره بواسطة خادم DHCP الخاص ب ASA.**ملاحظة:** لإعادة ضبط ASA إلى إعدادات المصنع الافتراضية من سطر الأوامر، أستخدم الأوامر التالية :

```
ciscoasa#conf t
ciscoasa#config factory-default 192.168.0.1 255.255.255.0
```

تكوين ASA

بمجرد إعادة ضبط إعدادات المصنع الافتراضية ل ASA، يمكنك بدء تشغيل ASDM إلى 192.168.0.1 للاتصال ب ASA على واجهة إيثرنت 1/0 الداخلية.

ملاحظة: يتم الاحتفاظ بكلمة المرور السابقة (أو يمكن أن تكون فارغة بشكل افتراضي).

بشكل افتراضي، يقبل ASA جلسة إدارة واردة بعنوان IP للمصدر في الشبكة الفرعية 24/192.168.0.0. يوفر خادم DHCP الافتراضي الذي يتم تمكينه على الواجهة الداخلية ل ASA عناوين IP في النطاق 24/129-192.168.0.2، صالحة للاتصال بالواجهة الداخلية باستخدام ASDM.

أتمت هذا steps in order to شكلت ال ASA:

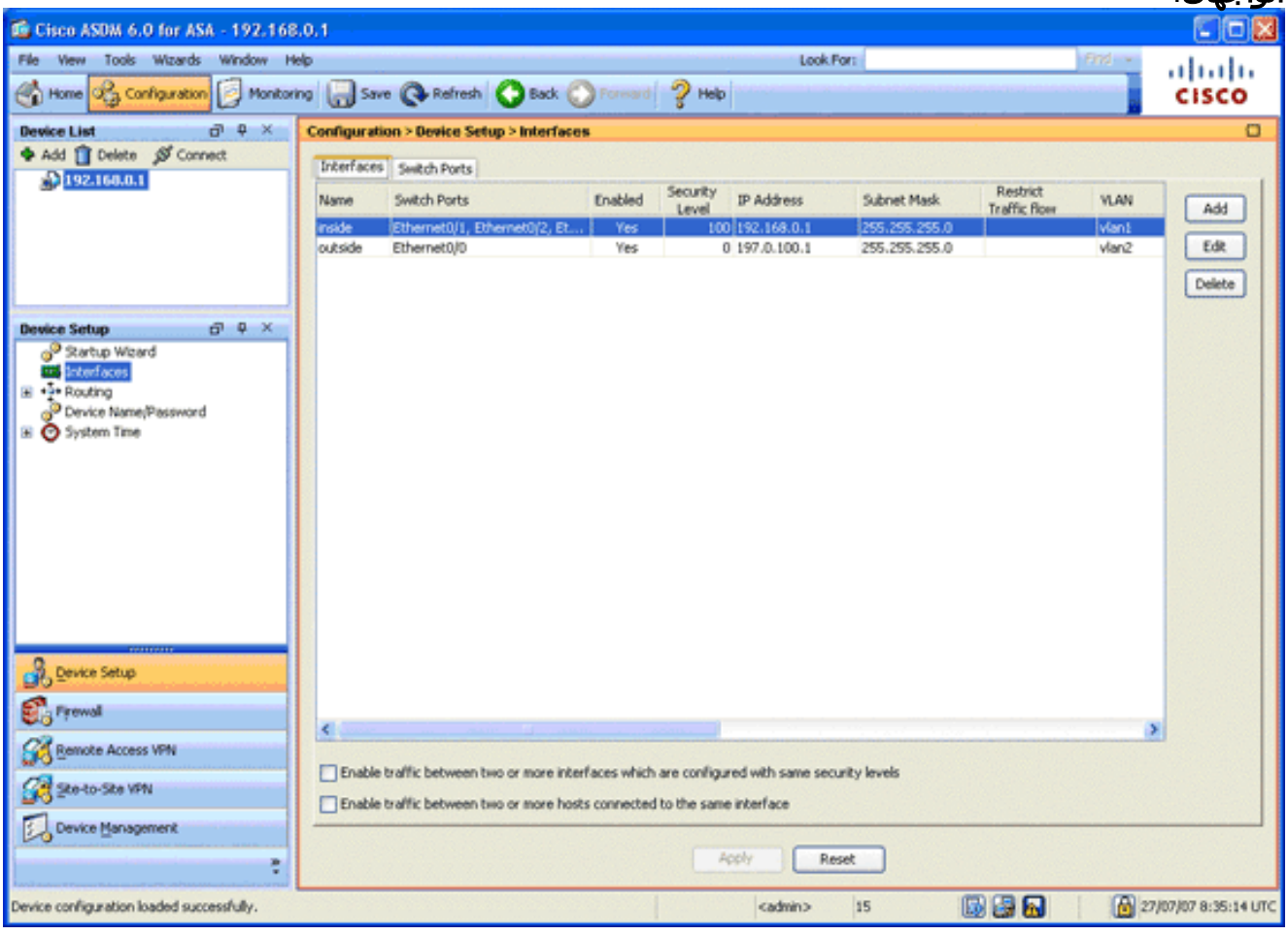
1. تمكين الواجهة الخارجية
2. تكوين اسم المجال وكلمة المرور ووقت النظام

3. تمكين خادم DHCP على الواجهة الخارجية
4. شكلت ال eID VPN عنوان بركة
5. إستيراد شهادة المرجع المصدق الجذر البلجيكي
6. تكوين طبقة مآخذ التوصيل الآمنة
7. تحديد نهج المجموعة الافتراضي
8. تعريف تعيين الشهادة
9. إضافة مستخدم محلي
10. إعادة تشغيل ASA

الخطوة 1. تمكين الواجهة الخارجية

تصف هذه الخطوة كيفية تمكين الواجهة الخارجية.

1. في تطبيق ASDM، انقر على **تكوين**، ثم انقر على **إعداد الجهاز**.
2. في منطقة إعداد الجهاز، أختر **الواجهات**، ثم انقر فوق علامة التبويب **الواجهات**.

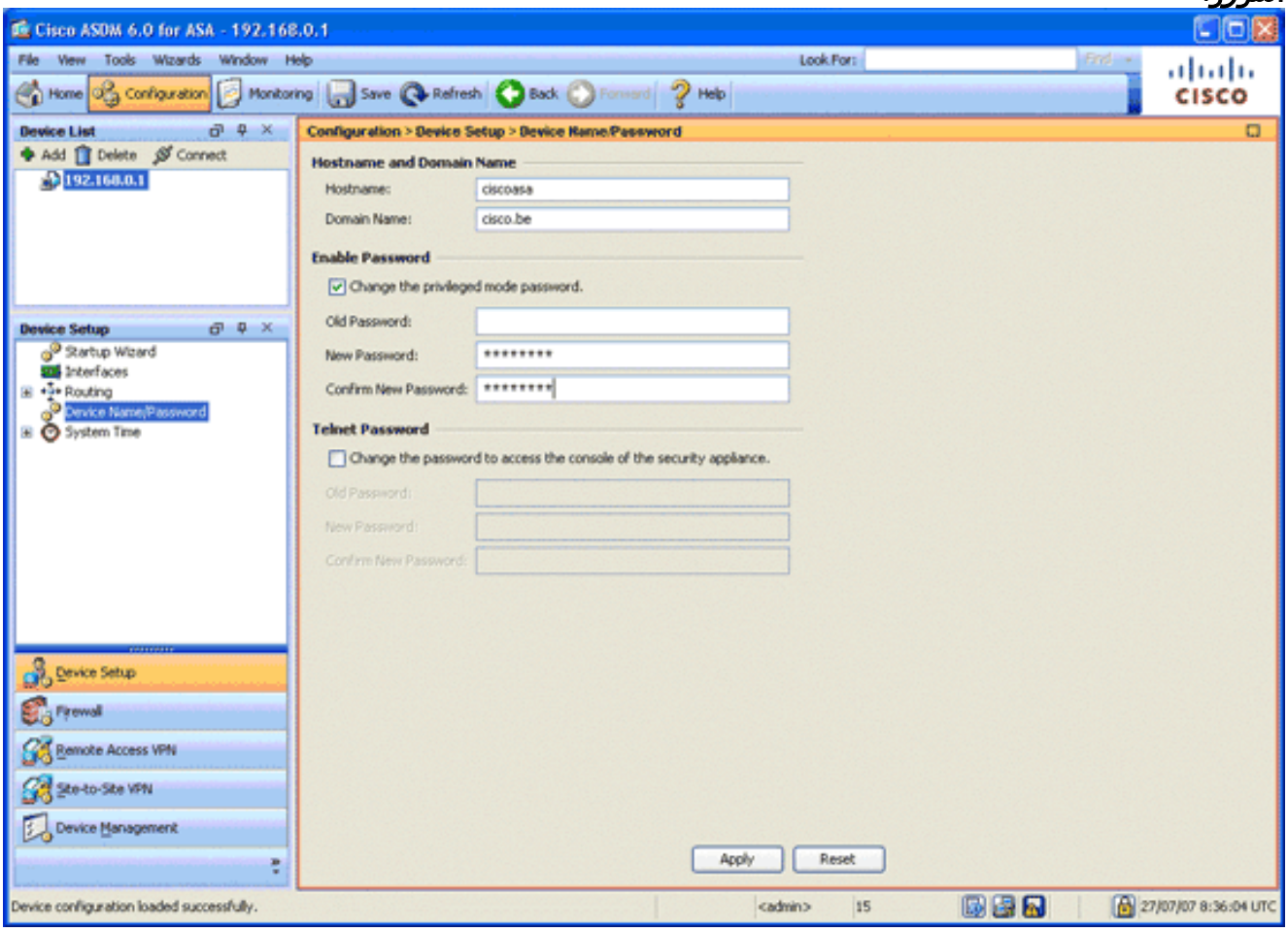


3. حدد الواجهة الخارجية، وانقر **تحرير**.
4. في قسم عنوان من علامة التبويب عام، أختر **إستخدام عنوان IP ثابت** خيار.
5. أدخل **197.0.100.1** لعنوان IP و**255.255.255.0** لقناع الشبكة الفرعية.
6. طقطقة **يطبق**.

الخطوة 2. تكوين اسم المجال وكلمة المرور ووقت النظام

تصف هذه الخطوة كيفية تكوين اسم المجال وكلمة المرور ووقت النظام.

1. في منطقة "إعداد الجهاز"، أختر **اسم الجهاز/كلمة المرور**.

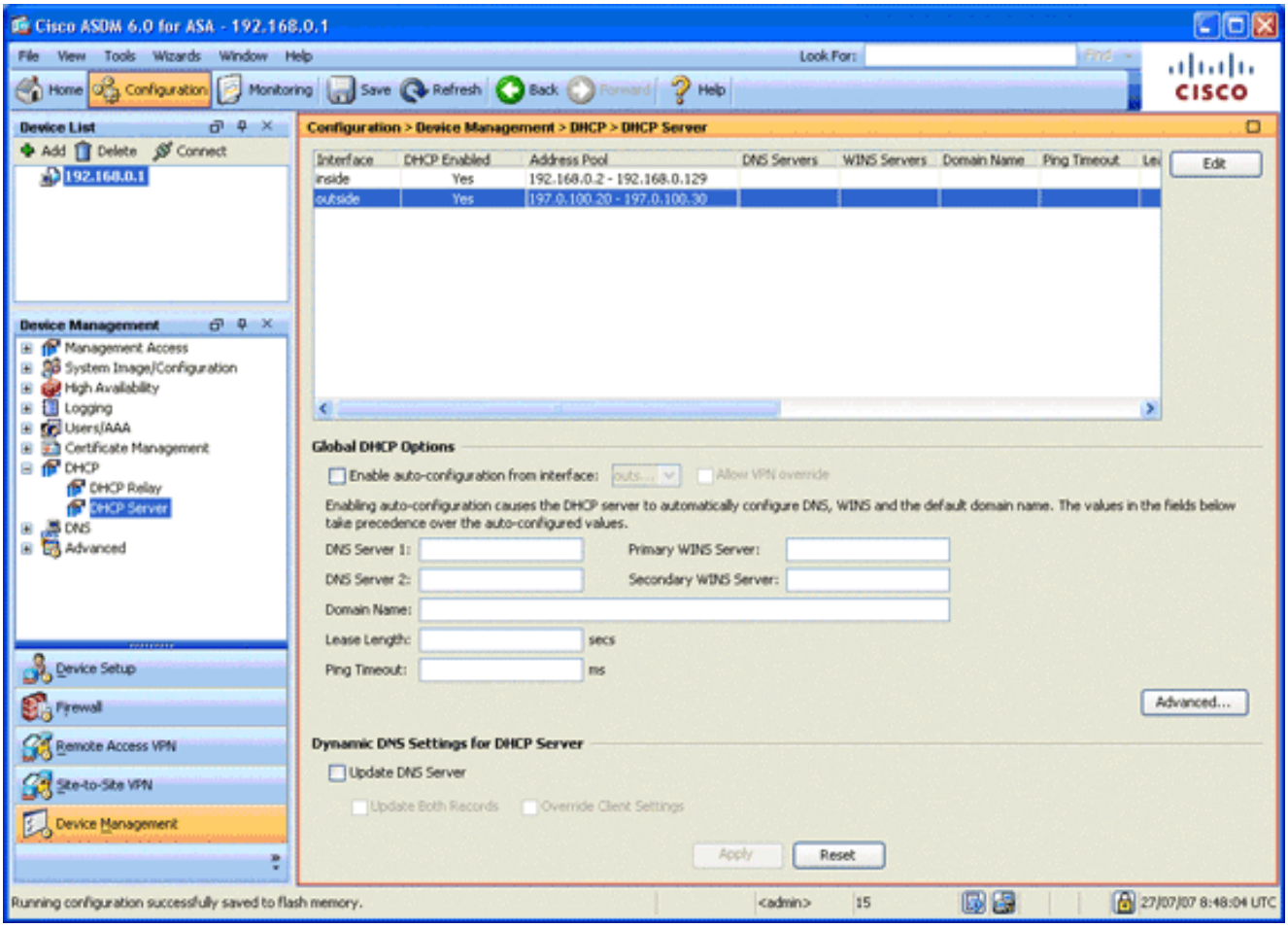


2. دخلت **cisco.be** ل ال domain name، ودخلت **cisco123** ل ال enable كلمة قيمة.**ملاحظة:** بشكل افتراضي، تكون كلمة المرور فارغة.
3. طقطقة **يطبق**.
4. في منطقة "إعداد الجهاز"، أختر **وقت النظام**، وقم بتغيير قيمة الساعة (إذا لزم الأمر).
5. طقطقة **يطبق**.

الخطوة 3. قم بتمكين خادم DHCP على الواجهة الخارجية.

تصف هذه الخطوة كيفية تمكين خادم DHCP على الواجهة الخارجية لتسهيل الاختبار.

1. انقر فوق **تكوين**، ثم انقر فوق **إدارة الأجهزة**.
2. في منطقة إدارة الجهاز، قم بتوسيع **DHCP**، واختر **خادم DHCP**.

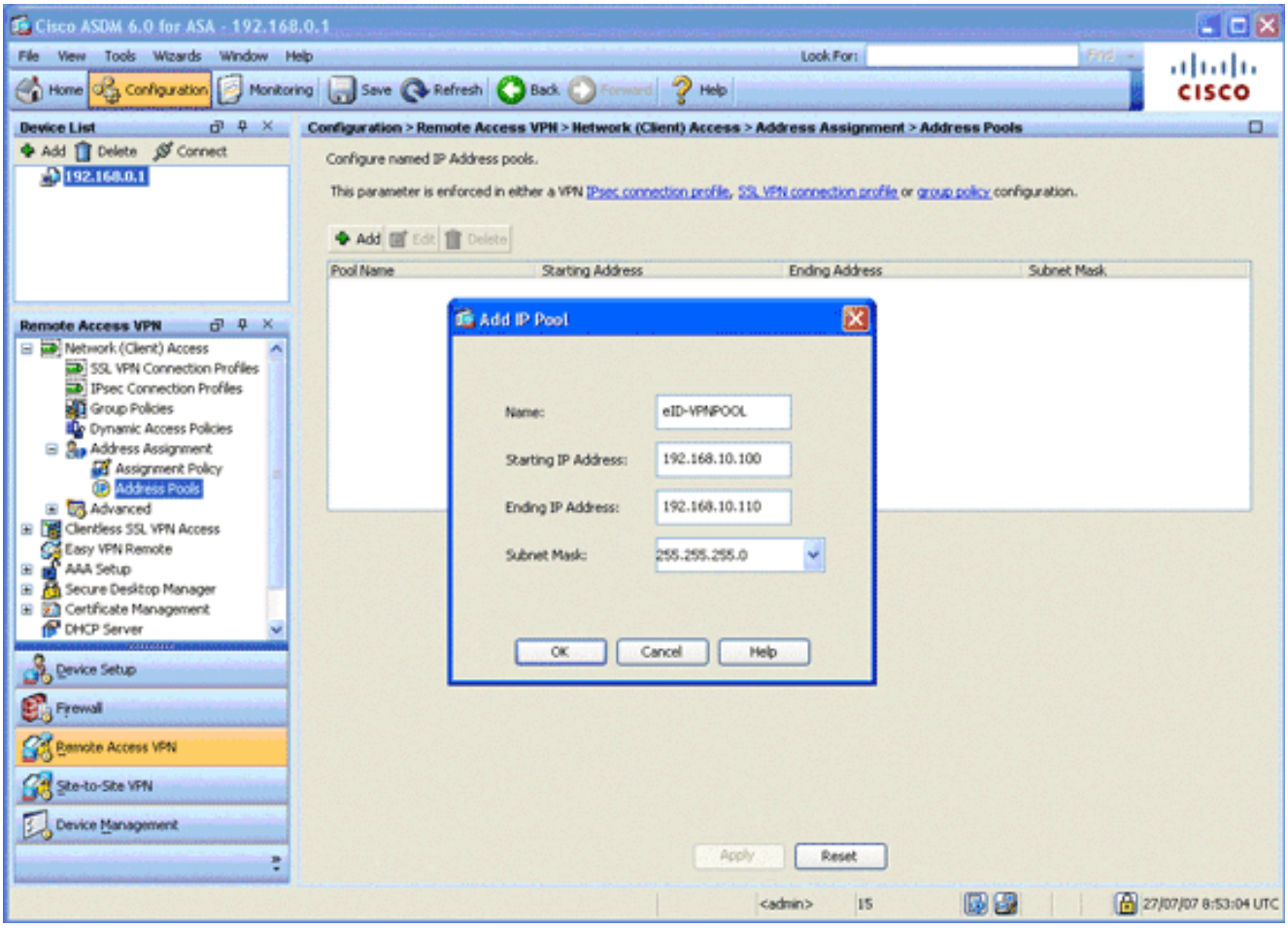


3. انتقيت القارن خارجي من القارن قائمة، وطقطقة **يحرر**.يظهر مربع الحوار تحرير خادم DHCP.
4. حدد خانة الاختيار **تمكين خادم DHCP**.
5. دخلت في ال DHCP عنوان بركة، عنوان من 197.0.100.20 إلى 197.0.100.30.
6. في منطقة "خيارات DHCP العمومية"، قم بإلغاء تحديد خانة الاختيار **تمكين التكوين التلقائي من الواجهة**.
7. طقطقة **يطبق**.

الخطوة 4. شكلت ال eID VPN عنوان بركة

تصف هذه الخطوة كيفية تحديد تجمع لعناوين IP التي يتم إستخدامها لتوفير عملاء AnyConnect عن بعد.

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. في منطقة إزالة شبكة VPN الخاصة بالوصول، قم بتوسيع **الوصول إلى الشبكة (العميل)**، ثم قم بتوسيع **تعيين العنوان**.
3. أخترت **عنوان بركة**، وبعد ذلك طقطقت **ال add**زر يتواجد في التشكيل يعين عنوان بركة منطقة.يظهر مربع الحوار إضافة تجمع IP.



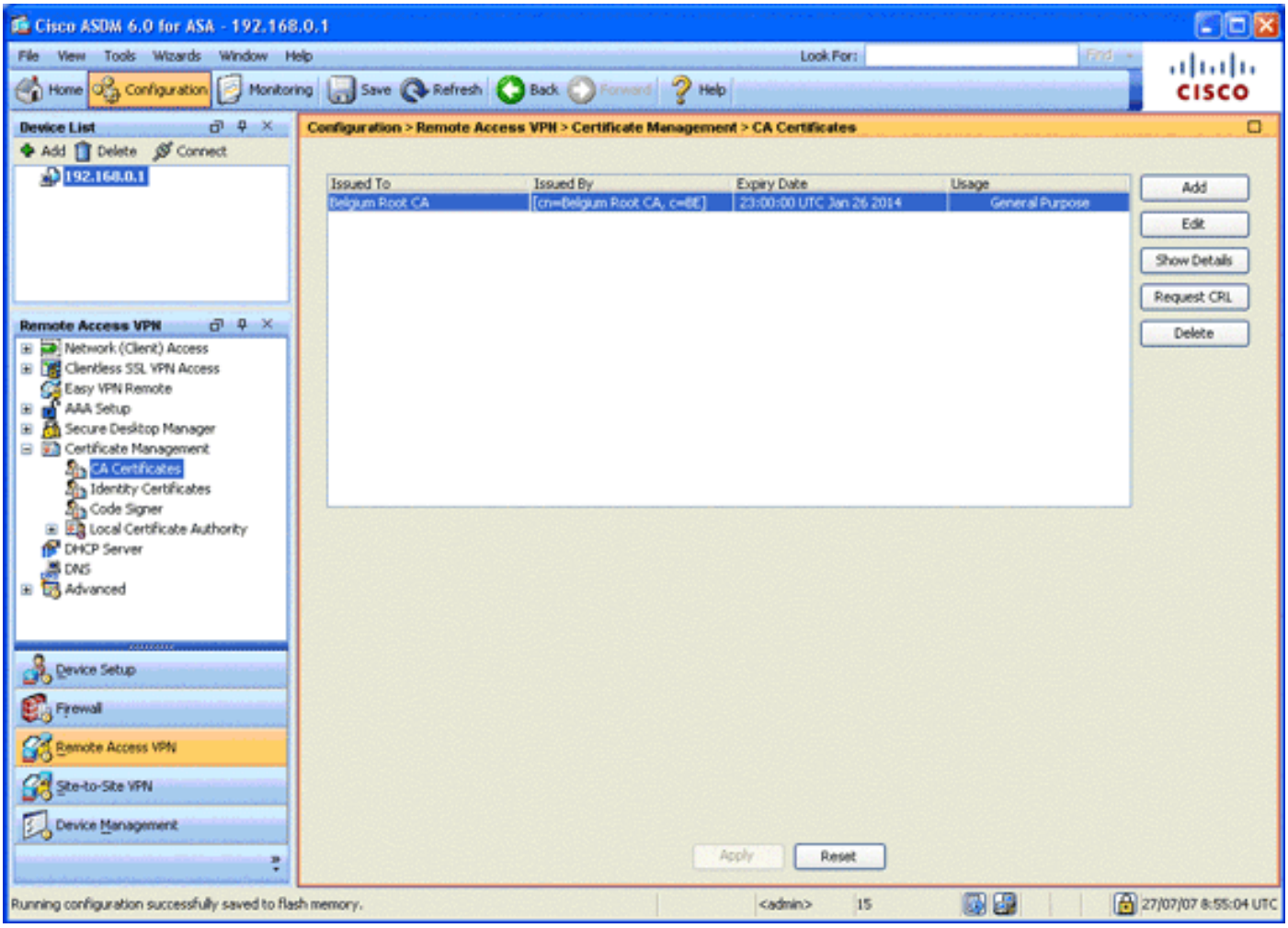
4. دخلت في الإسم مجال، **eID-VPNPOOL**.
5. في حقلي عنوان IP الأولي والنهاية لعنوان IP، أدخل نطاق من عنوان IP من 192.168.10.100 إلى 192.168.10.110.
6. أختر **255.255.255.0** من قائمة قناع الشبكة الفرعية المنسدلة، انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

الخطوة 5. إستيراد شهادة المرجع المصدق الجذر البلجيكي

تصف هذه الخطوة كيفية إستيراد شهادة المرجع المصدق (CA) الجذر البلجيكي إلى ASA.

1. قم بتنزيل وتثبيت شهادات المرجع المصدق (CA) البلجيكي (belgiumMRCA.crt و belgiumUMRCA2.crt) من موقع الحكومة على الويب، وقم بتخزينها على جهاز الكمبيوتر المحلي لديك.موقع الحكومة البلجيكية على الإنترنت يوجد على العنوان: http://certs.eid.belgium.be/
2. في منطقة شبكة VPN للوصول عن بعد، قم بتوسيع **إدارة الشهادات**، واختر **شهادات CA**.
3. انقر فوق **إضافة**، ثم انقر فوق **تثبيت من الملف**.
4. استعرض الموقع الذي قمت فيه بحفظ ملف شهادة المرجع المصدق (CA) الجذر البلجيكي (belgiumMRCA.crt)، وانقر فوق **تثبيت الشهادة**.
5. انقر فوق **تطبيق** لحفظ التغييرات التي قمت بها.

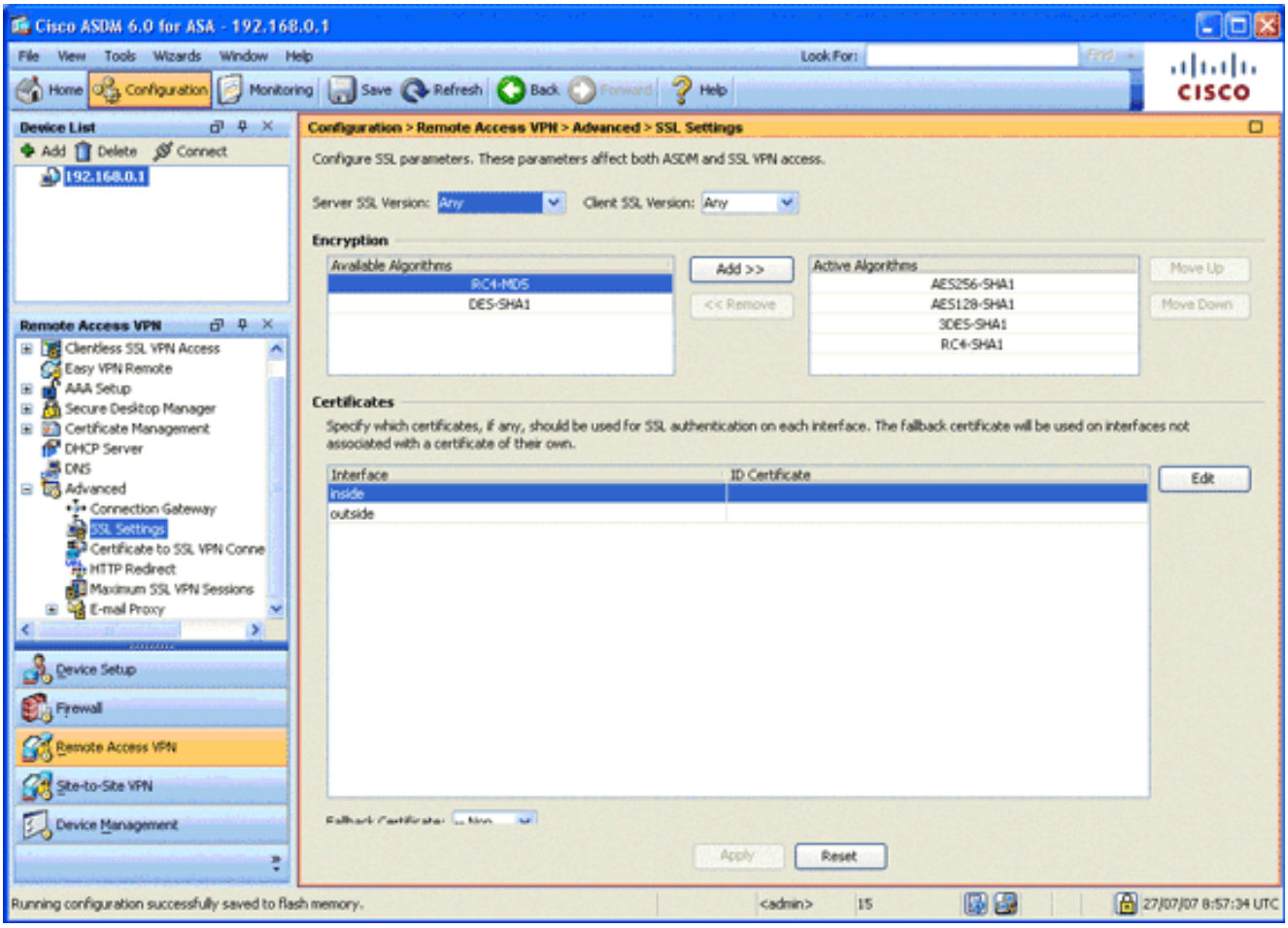
تظهر هذه الصورة الشهادة المثبتة على ASA:



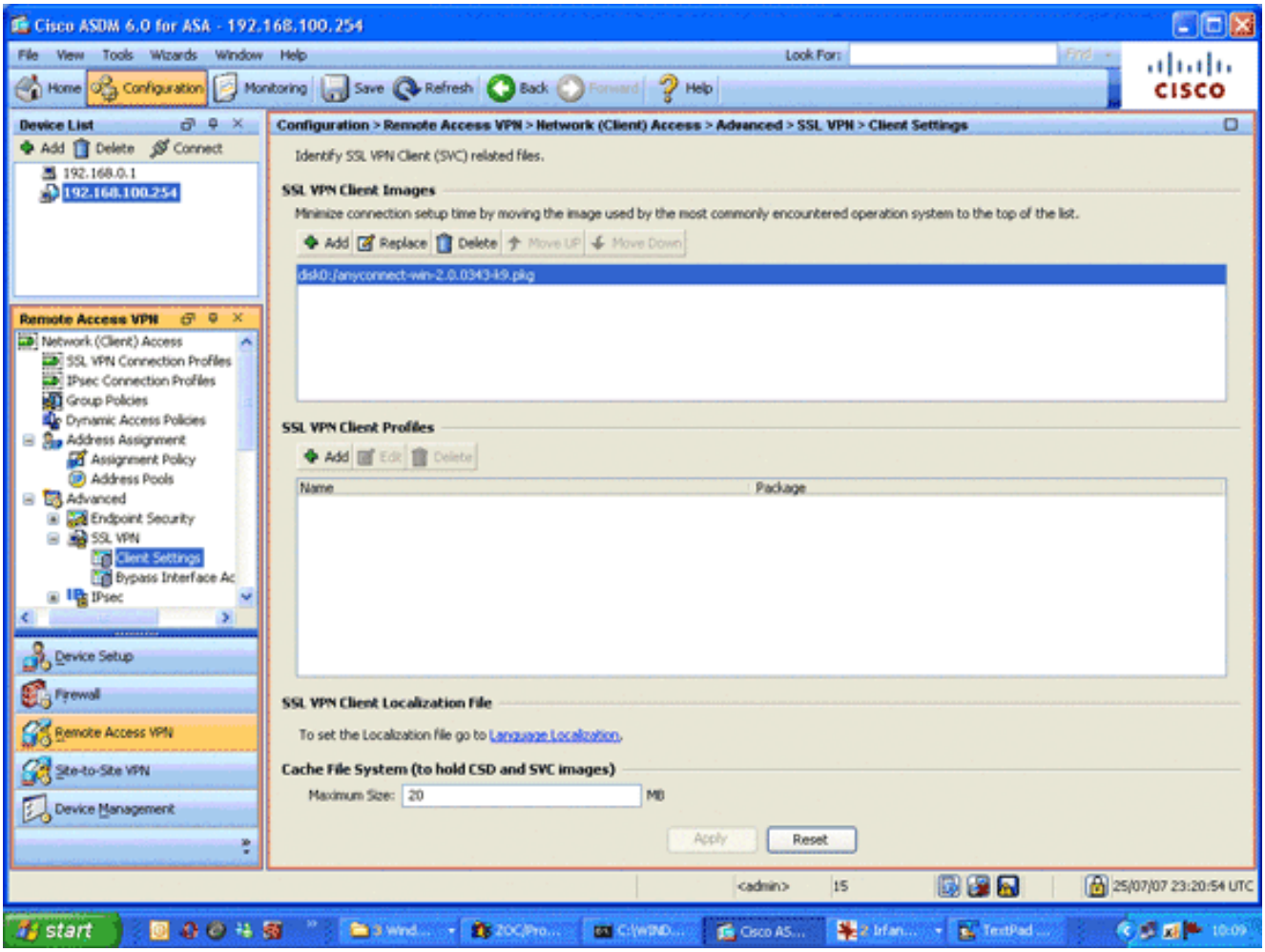
الخطوة 6. تكوين طبقة مآخذ التوصيل الآمنة

تصف هذه الخطوة كيفية ترتيب أولويات خيارات التشفير الآمن، وتعريف صورة عميل SSL VPN، وتحديد ملف تعريف الاتصال.

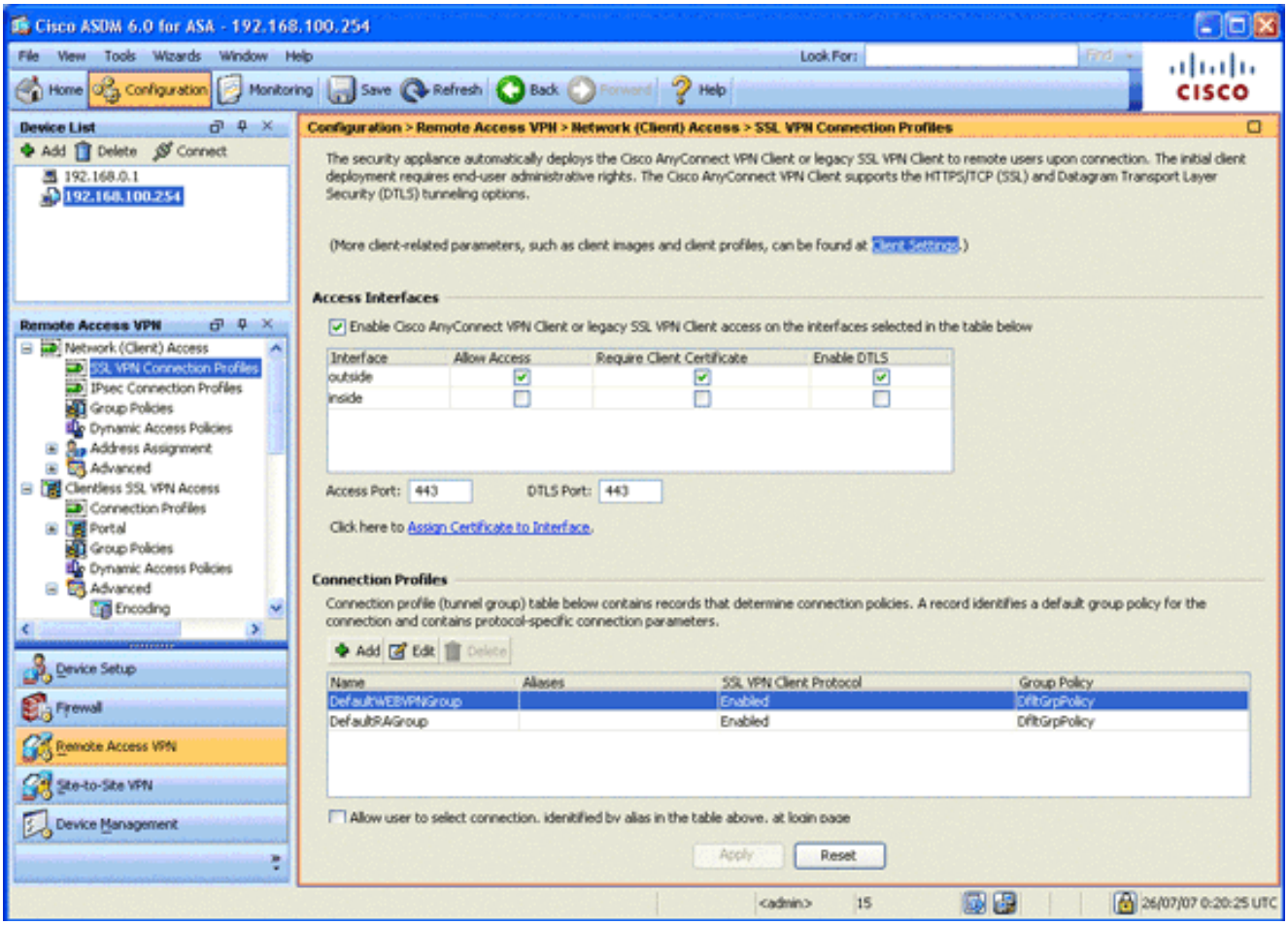
1. ترتيب خيارات التشفير الأكثر أمانا حسب الأولوية.في منطقة "الوصول عن بعد إلى VPN"، قم بتوسيع **إعدادات متقدمة**، واختر **إعدادات SSL**. في قسم التشفير، يتم تكديس الخوارزميات النشطة، من أعلى لأسفل، كما يلي:AES256-SHA1AES128-SHA13DES-SHA1التعاون التقني 4-SHA1



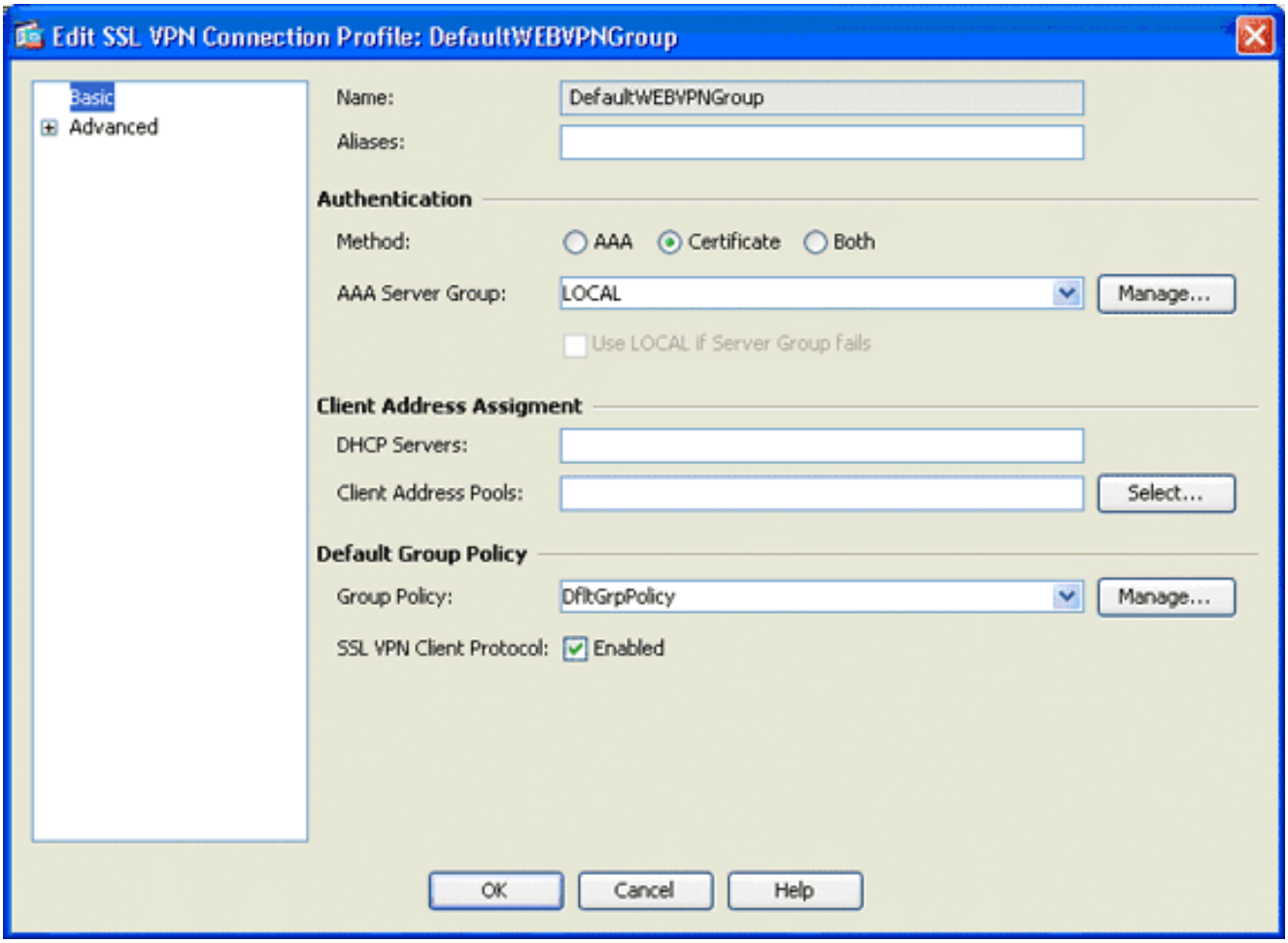
2. قم بتعريف صورة عميل SSL VPN لعميل AnyConnect.في منطقة Remote Access VPN للوصول عن بعد، قم بتوسيع **Advanced**، وتوسيع **SSL VPN**، واختر **إعدادات العميل**.في منطقة صور عميل SSL VPN، انقر فوق **إضافة**.أختر حزمة AnyConnect المخزنة في الذاكرة المؤقتة (flash).تظهر حزمة AnyConnect في قائمة صور عملاء SSL VPN كما هو موضح في هذه الصورة:



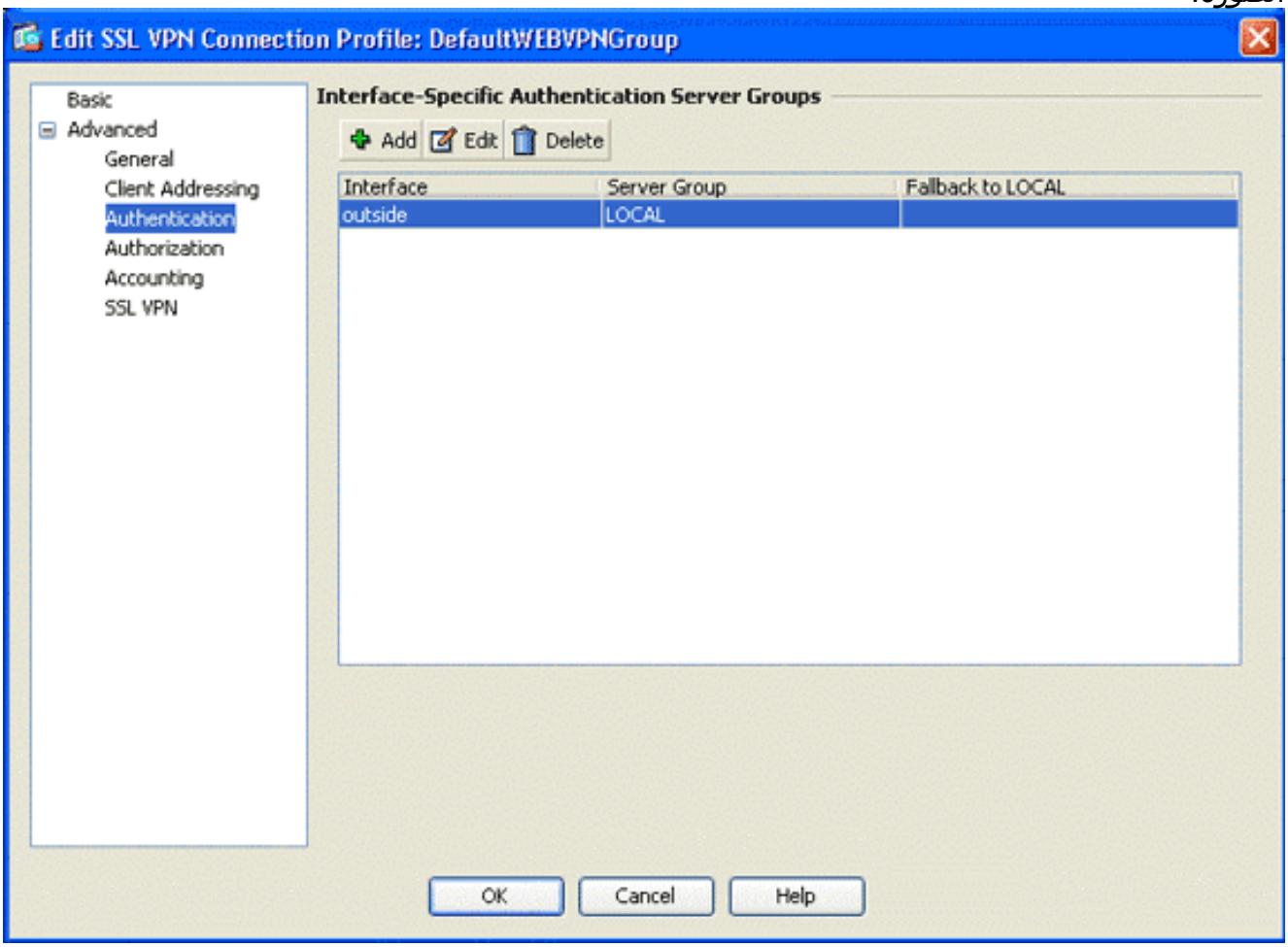
3. تعريف ملف تعريف اتصال DefaultWEBVPNGgroup.في منطقة "الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد"، قم بتوسيع **الوصول إلى الشبكة (العميل)**، واختر **ملفات تعريف اتصال VPN ل SSL**.في منطقة واجهات الوصول، حدد خانة الاختيار **تمكين عميل AnyConnect VPN من Cisco**.بالنسبة للواجهة الخارجية، حدد خانات الاختيار **السماح بالوصول** و**طلب شهادة العميل** و**تمكين DTLS** كما هو موضح في هذه الصورة:



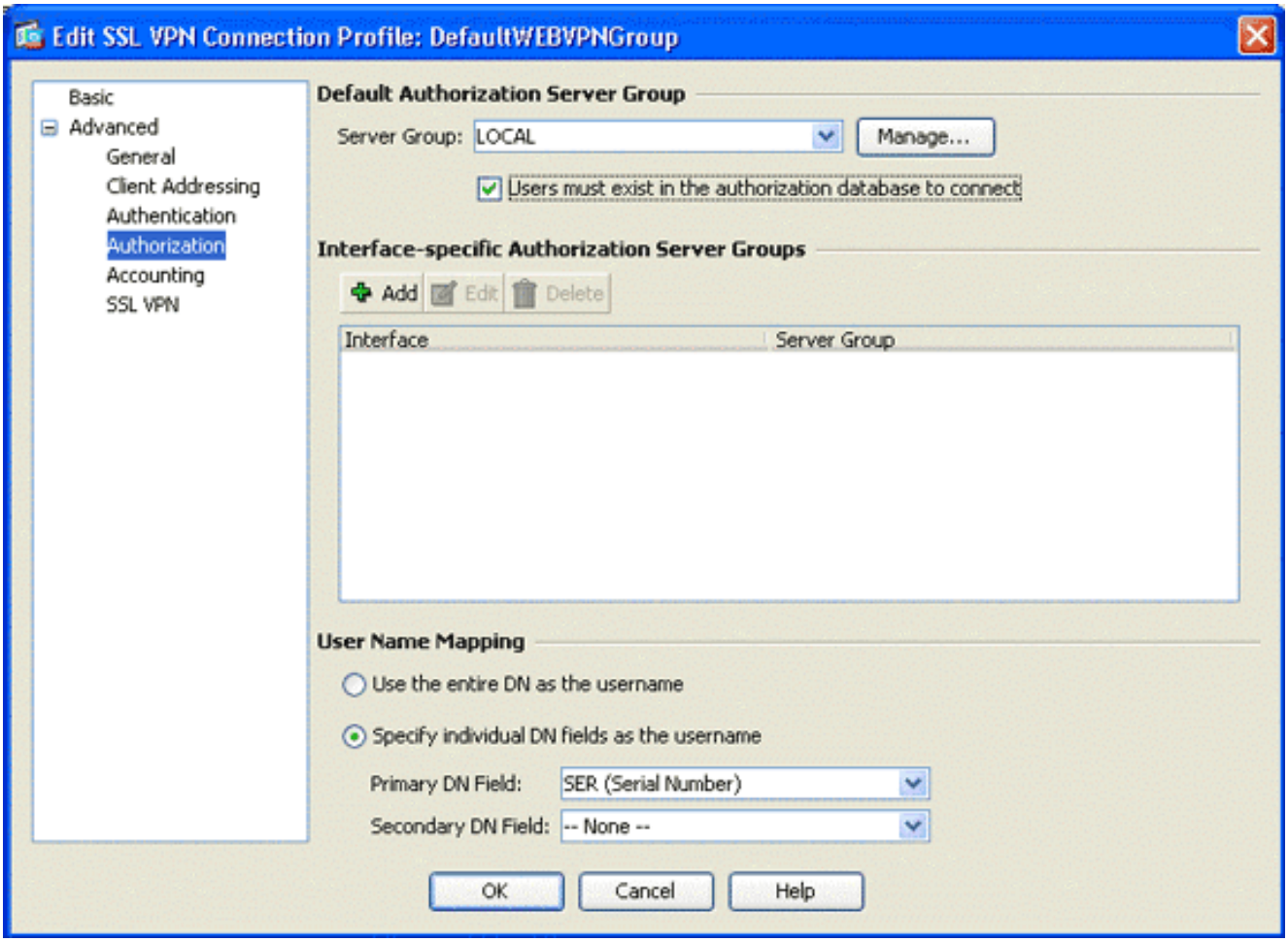
في منطقة "توصيفات التوصيل"، أختر **DefaultWEBvpngGroup**، ثم انقر على **تحرير**.يظهر مربع الحوار تحرير ملف تعريف اتصال SSL VPN.



في منطقة التنقل، أختر **أساسي**.في منطقة المصادقة، انقر على زر **ترخيص** الراديو.في منطقة "نهج المجموعة" الافتراضية، حدد خانة الاختيار **SSL VPN Client Protocol**.قم بتوسيع **المتقدم**، واختر **المصادقة**.انقر فوق **إضافة**، وأضف الواجهة الخارجية مع مجموعة خوادم محلية كما هو موضح في هذه الصورة:



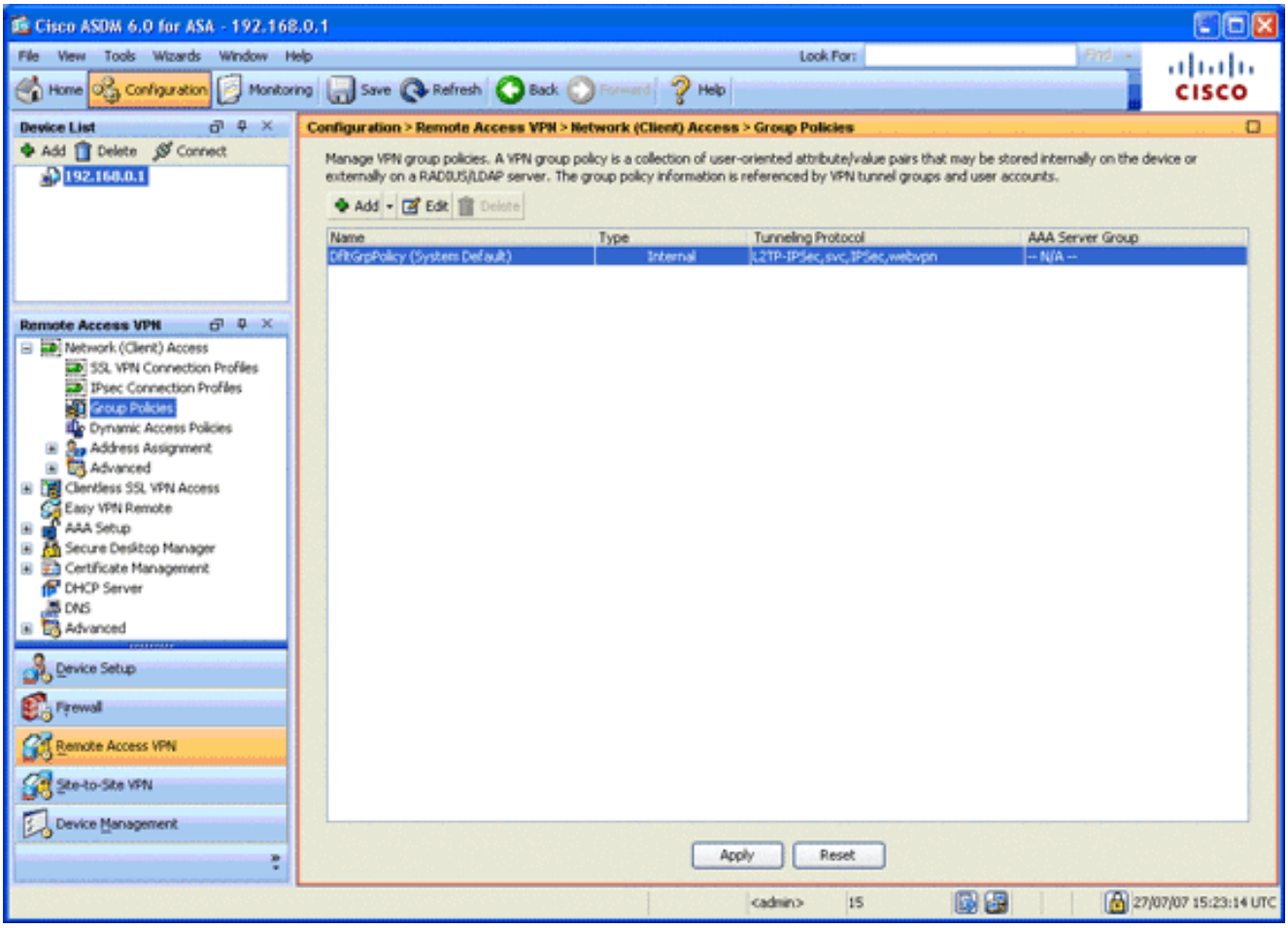
في منطقة التنقل، أختر **التفويض**.في منطقة "مجموعة خوادم التخويل" الافتراضية، أختر **LOCAL** من القائمة المنسدلة "مجموعة الخوادم"، وحدد **أنه يجب وجود المستخدمين في قاعدة بيانات التخويل للاتصال** بمربع الاختيار.في منطقة تعيين اسم المستخدم، أختر **SER (الرقم التسلسلي)** من القائمة المنسدلة لحقل DN الأساسي، واختر **None** من حقل DN الثانوي، وانقر فوق **موافق**.



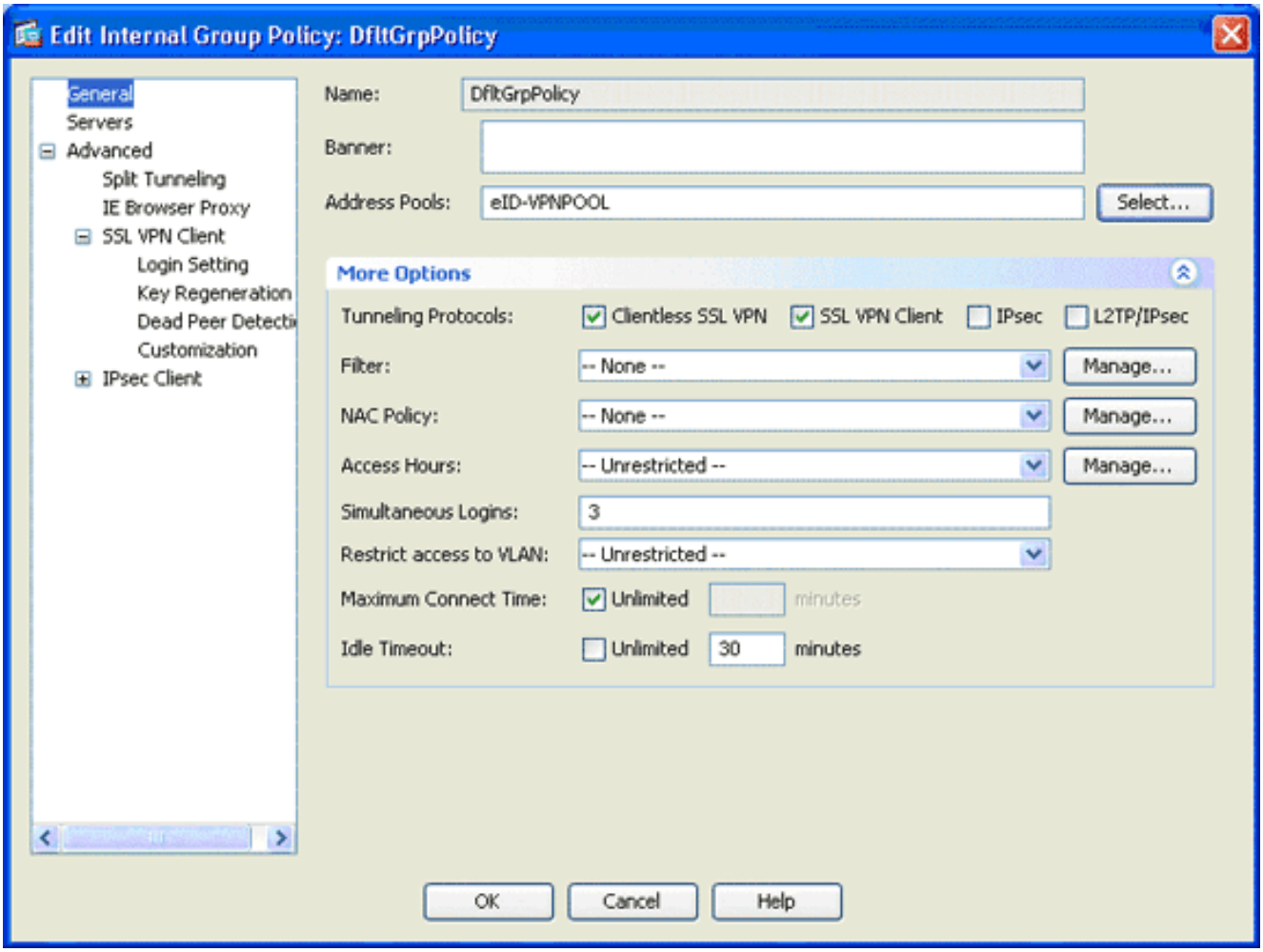
الخطوة 7. تحديد نهج المجموعة الافتراضي

تصف هذه الخطوة كيفية تحديد نهج المجموعة الافتراضي.

1. في منطقة "الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد"، قم بتوسيع **الوصول إلى الشبكة (العميل)**، واختر **نهج المجموعة**.



2. أختر **DfltGrpPolicy** من قائمة نهج المجموعة، وانقر فوق **تحرير**.
3. يظهر مربع الحوار تحرير نهج المجموعة الداخلي.

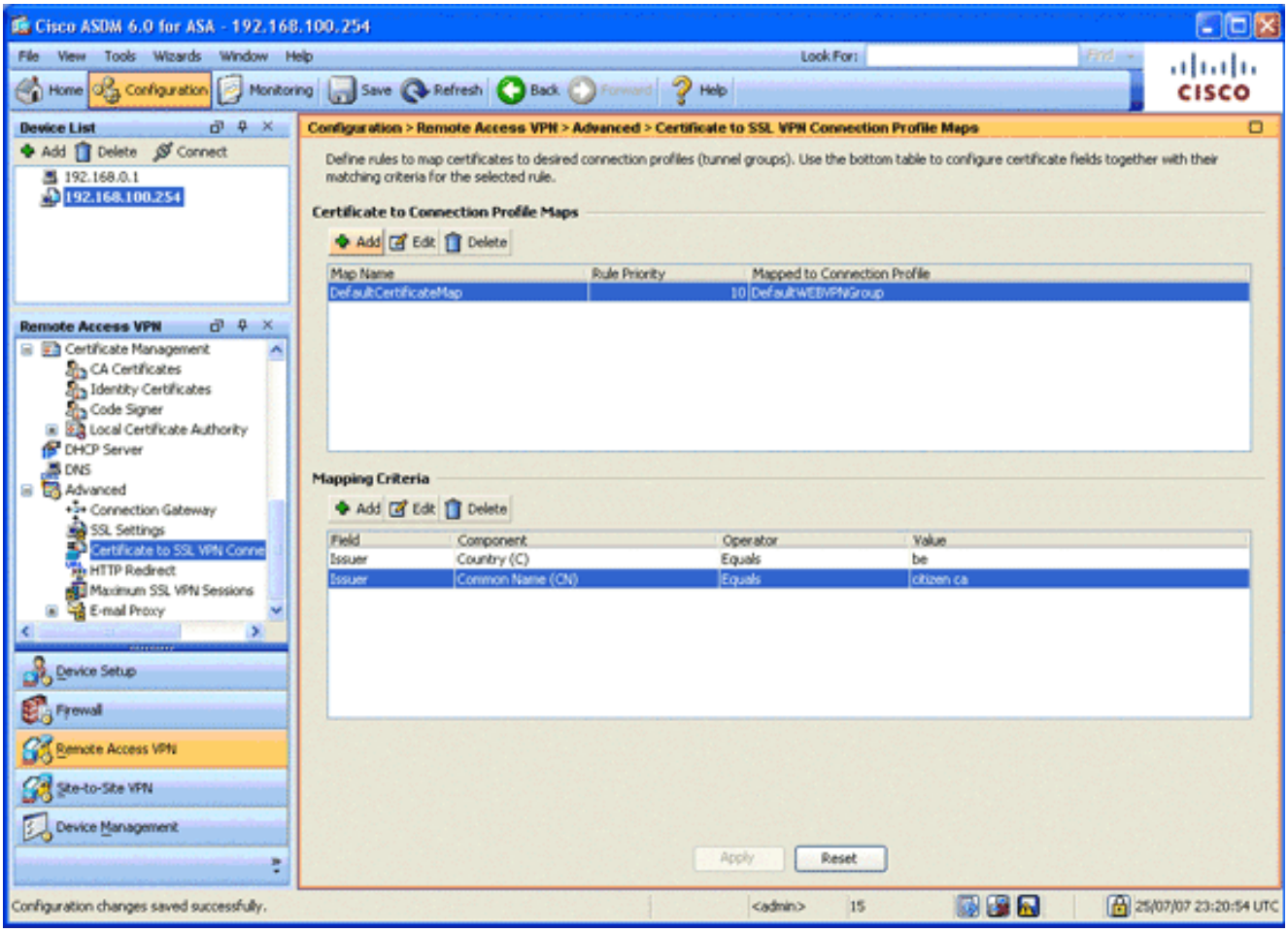


4. من منطقه الملاحه أختر **عام**.
5. لتجمعات العناوين، انقر فوق **تحديد** لاختيار تجمع عناوين، واختر **eID-VPNpool**.
6. في منطقة "المزيد من الخيارات"، قم بإلغاء تحديد خانات الاختيار **IPsec** و**L2TP/IPsec**، وانقر فوق **موافق**.

الخطوة 8. تعريف تعيين الشهادة

تصف هذه الخطوة كيفية تعريف معايير تعيين الشهادة.

1. في منطقة "شبكة VPN للوصول عن بعد"، انقر على **خيارات متقدمة**، واختر **شهادة إلى خرائط ملفات تعريف اتصال SSL VPN**.
2. في منطقة "شهادة إلى خرائط ملف تعريف الاتصال"، انقر على **إضافة**، واختر **DefaultCertificateMap** من قائمة الخريطة.يجب أن تتطابق هذه الخريطة مع *DefaultWEBVPNProfile* في حقل ملف تعريف الاتصال المعين.
3. في منطقة فئة الترجمة، انقر **إضافة**، وقم بإضافة القيم التالية:الحقل: المصدر، البلد (ج)، يساوي، "كن"الحقل: المصدر، الاسم الشائع (CN)، يساوي، "Citizen ca"يجب أن تظهر معايير التعيين كما هو موضح في هذه الصورة:

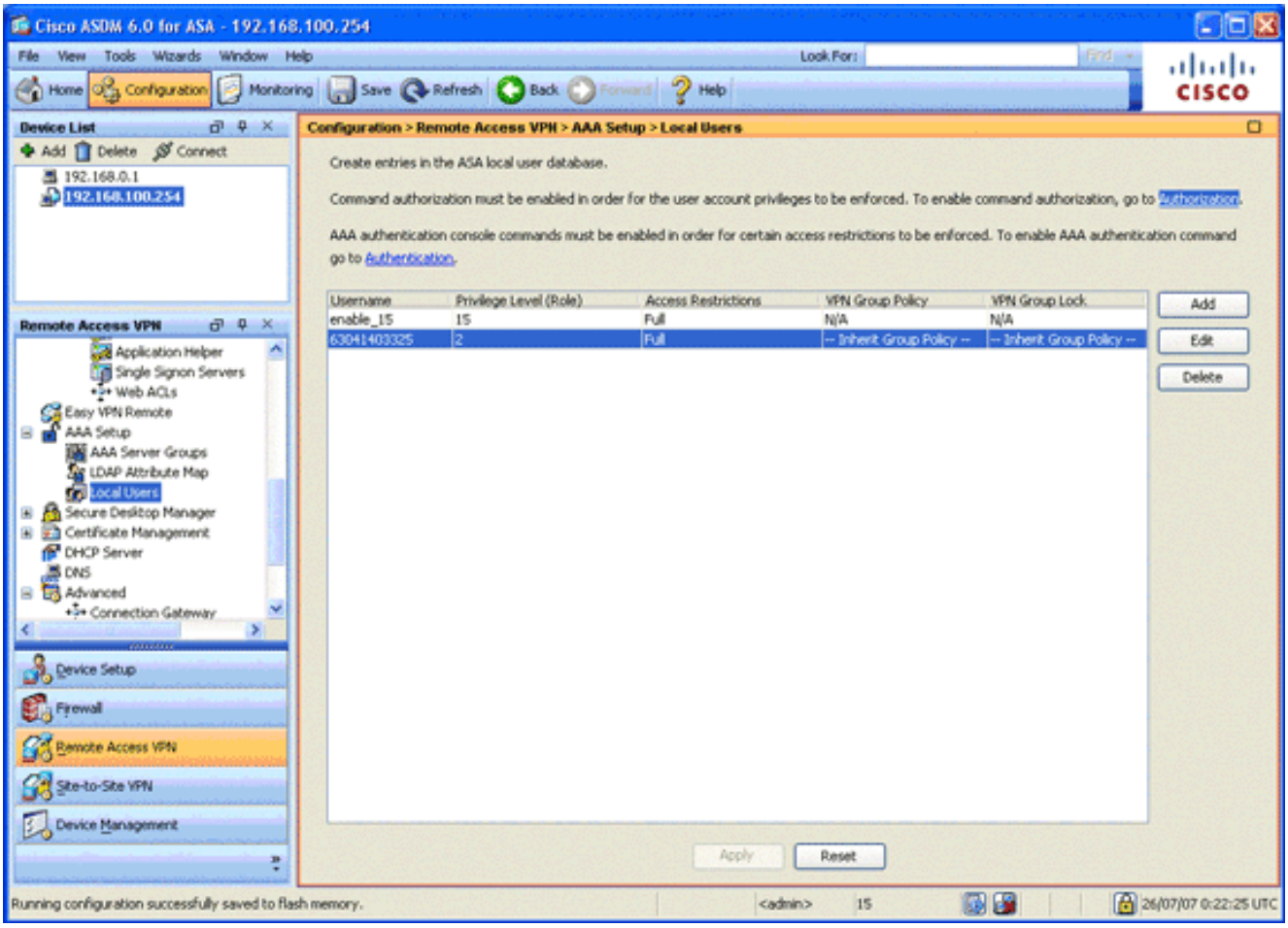


4. طقطقة **يطبق**.

الخطوة 9. إضافة مستخدم محلي

تصف هذه الخطوة كيفية إضافة مستخدم محلي.

1. في منطقة "الوصول عن بعد إلى شبكة VPN"، قم بتوسيع **إعداد AAA**، واختر **المستخدمين المحليين**.
2. في منطقة "المستخدمين المحليين"، انقر فوق **إضافة**.
3. في حقل اسم المستخدم، أدخل الرقم التسلسلي لشهادة المستخدم. على سبيل المثال، 56100307215 (كما هو موضح في قسم شهادة المصادقة في هذا المستند).



4. طقطقة **يطبق**.

الخطوة 10. إعادة تشغيل ASA

أعد تمهيد ASA لضمان تطبيق جميع التغييرات على خدمات النظام.

توليف دقيق

أثناء الاختبار، قد لا يتم إغلاق بعض أنفاق SSL بشكل صحيح. بما أن ASA يفترض أن عميل AnyConnect قد يفصل الاتصال ويعيد الاتصال، فلا يتم إسقاط النفق، مما يوفر له فرصة العودة. ومع ذلك، أثناء الاختبارات التي يتم إجراؤها في المختبرات باستخدام ترخيص أساسي (نفقين من نوع SSL بشكل افتراضي)، قد تستنفد الترخيص عندما لا يتم إغلاق أنفاق SSL بشكل صحيح. إذا حدثت هذه المشكلة، فاستخدم الأمر **vpn-sessiondb logoff b** ***option***>>لتسجيل الخروج من جميع جلسات SSL النشطة.

تهيئة لمدة دقيقة واحدة

لإنشاء تكوين عامل بسرعة، قم بإعادة ضبط ASA الخاص بك إلى إعدادات المصنع الافتراضية، وألصق هذا التكوين في وضع التكوين:

سيسكوسا
ciscoasa#**conf t** ciscoasa#**clear configure all** ciscoasa#**domain-name cisco.be** ciscoasa#**enable password 9jNfZuG3TC5tCVH0 encrypted** !

```
                                        interface Vlan1
                                         nameif inside
                                    security-level 100
                    ip address 192.168.0.1 255.255.255.0
                                        interface Vlan2
                                         nameif outside
                                     security-level 0
                    ip address 197.0.100.1 255.255.255.0
                                    interface Ethernet0/0
                                switchport access vlan 2
                                          no shutdown
                                    interface Ethernet0/1
                                          no shutdown
                                                   !
                         passwd 2KFQnbNIdI.2KYOU encrypted
                                dns server-group DefaultDNS
                                    domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
                                       mask 255.255.255.0
                             asdm image disk0:/asdm-602.bin
                                     no asdm history enable
                               global (outside) 1 interface
                             nat (inside) 1 0.0.0.0 0.0.0.0
          dynamic-access-policy-record DfltAccessPolicy
                                       http server enable
                    http 192.168.0.0 255.255.255.0 inside
                    crypto ca trustpoint ASDM_TrustPoint0
                                     enrollment terminal
                                          crl configure
     crypto ca certificate map DefaultCertificateMap 10
                                   issuer-name attr c eq be
                        issuer-name attr cn eq citizen ca
            crypto ca certificate chain ASDM_TrustPoint0
        certificate ca 580b056c5324dbb25057185ff9e5a650
        3082027c a0030201 02021058 0b056c53 30820394
                                   24dbb250 57185ff9 e5a65030
        0d06092a 864886f7 0d010105 05003027 310b3009
                                   06035504 06130242 45311830
        0403130f 42656c67 69756d20 526f6f74 16060355
                                   20434130 1e170d30 33303132
        3030305a 170d3134 30313236 32333030 36323330
                                   30305a30 27310b30 09060355
        0f42656c 55040313 30160603 42453118 04061302
                                   6769756d 20526f6f 74204341
        300d0609 2a864886 f70d0101 01050003 30820122
                                   82010f00 3082010a 02820101
        00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
                                   c720eb30 915a75f5 e2d2cfc8
        4c149842 58adc711 c540406a 5af97412 2787e99c
                                   e5714e22 2cd11218 aa305ea2
        21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
                                   a8014fad 226670fa 4b1d95c1
        3058eabc d965d89a b488eb49 4652dfd2 531576cb
                                   145d1949 b16f6ad3 d3fdbcc2
        2dec453f 093f58be fcd4ef00 8c813572 bff718ea
                                   96627d2b 287f156c 63d2caca
        7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
                                   30e8efc4 ab935e07 de328f12
        74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf
                                   6ce3841d de872e33 0b3c74e2
        2e5ce0e5 c631f9db 40fa6aa1 a48a939b 21503895
                                   a7210687 1d27d3c4 a1c94cb0
        6f020301 0001a381 bb3081b8 300e0603 551d0f01
                                   01ff0404 03020106 300f0603
```

```
        551d1301 01ff0405 30030101 ff304206 03551d20
                                 043b3039 30370605 60380101
        01302e30 2c06082b 06010505 07020116 20687474
                                 703a2f2f 7265706f 7369746f
        72792e65 69642e62 656c6769 756d2e62 65301d06
                                 03551d0e 04160414 10f00c56
        9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
                                 60864801 86f84201 01040403
        1f060355 1d230418 30168014 10f00c56 02000730
                                 9b61ea57 3ab63597 6d9fddb9
        148edbe6 300d0609 2a864886 f70d0101 05050003
                                 82010100 c86d2251 8a61f80f
        966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
                                 48a74c49 37d773a1 6a01655e
        32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
                                 5d0f37ba 76d240bd cc2d3fd3
        4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
                                 45f4dae7 b5634544 110d2a7f
        337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
                                 60f2d787 f6572e7a 7e6a1380
        1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
                                 755481f3 1bad779c e8b28fdb
        83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
                                 ba218c97 1a21d4ea 2d3bacba
        eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
                                 fff26e87 7d46c974 d6efeb3d
        7de6596e 069404e4 a2558738 286a225e e2be7412
                                                 b004432a
                                                   quit
                             no crypto isakmp nat-traversal
                                                        !
          dhcpd address 192.168.0.2-192.168.0.129 inside
                                          dhcpd enable inside
         dhcpd address 197.0.100.20-197.0.100.30 outside
                                         dhcpd enable outside
                                                        !
                         service-policy global_policy global
    ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
                                                       sha1
    ssl certificate-authentication interface outside port
                                                       443
                                                    webvpn
                                             enable outside
       svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
                                                svc enable
           certificate-group-map DefaultCertificateMap 10
                                         DefaultWEBVPNGroup
                    group-policy DfltGrpPolicy attributes
                          vpn-tunnel-protocol svc webvpn
                         address-pools value eID-VPNPOOL
                          username 63041403325 nopassword
       tunnel-group DefaultWEBVPNGroup general-attributes
             authentication-server-group (outside) LOCAL
                         authorization-server-group LOCAL
                                   authorization-required
                         authorization-dn-attributes SER
        tunnel-group DefaultWEBVPNGroup webvpn-attributes
                               authentication certificate
                                                       exit
                                             copy run start
```

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- 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).