كيفية الحصول على شهادة رقمية من Microsoft Windows CA باستخدام ASDM على ASA

المحتويات

المقدمة

يمكن إستخدام الشهادات الرقمية لمصادقة أجهزة الشبكة والمستخدمين على الشبكة. يمكن إستخدامها للتفاوض على جلسات عمل IPSec بين عقد الشبكة.

تعرف أجهزة Cisco على نفسها بأمان على الشبكة بثلاث طرق رئيسية:

1. **مفاتيح مشتركة مسبقا**. يمكن أن يحتوي جهازان أو أكثر على نفس المفتاح السري المشترك. يصادق النظراء بعضهم البعض عن طريق حساب حزمة مصقولة من البيانات تتضمن المفتاح المشترك مسبقا وإرسالها. وإذا كان النظير المتلقي قادرا على إنشاء التجزئة نفسها بشكل مستقل باستخدام مفتاحه المشفر مسبقا، فإنه يعرف انه يجب على كلا النظيرين الاشتراك في السر نفسه، مما يوثق النظير الآخر. هذه الطريقة يدوية وليست قابلة للتحجيم.
2. **شهادات موقعة ذاتيا**. يقوم الجهاز بإنشاء شهادته الخاصة ويوقع عليها على أنها صالحة. يجب أن يكون لهذا النوع من الشهادات إستخدام محدود. ومن الأمثلة الجيدة على ذلك إستخدام هذه الشهادة مع وصول SSH و HTTPS لأغراض التكوين. يلزم زوج اسم مستخدم/كلمة مرور منفصل لإكمال الاتصال.**ملاحظة:** تصمد الشهادات الموقعة ذاتيا المستمرة عند إعادة تحميل الموجه لأنها يتم حفظها في ذاكرة الوصول العشوائي غير المتطاير (NVRAM) للجهاز. راجع الشهادات الدائمة الموقعة ذاتيا للحصول على مزيد من المعلومات. أحد الأمثلة الجيدة على الاستخدام هو إتصالات WebVPN (SSL VPN).

3. **شهادة المرجع المصدق**. يقوم طرف ثالث بالتحقق من صحة العقد أو أكثر التي تحاول الاتصال والتحقق من صحتها. تحتوي كل عقدة على مفتاح عام وخاص. يقوم المفتاح العام بتشفير البيانات، ويقوم المفتاح الخاص بفك تشفير البيانات. ولأنهم حصلوا على شهاداتهم من نفس المصدر، يمكن التأكد من هوياتهم. يمكن لجهاز ASA الحصول على شهادة رقمية من جهة خارجية باستخدام طريقة التسجيل اليدوية أو طريقة التسجيل التلقائية.**ملاحظة:** تعتمد طريقة التسجيل ونوع الشهادة الرقمية التي تختارها على ميزات ووظائف كل منتج من إنتاج جهة خارجية. اتصل بمورد خدمة الشهادات للحصول على مزيد من المعلومات.

يمكن أن تستخدم أجهزة الأمان المعدلة (ASA) من Cisco مفاتيح مشتركة مسبقا أو شهادات رقمية توفرها مرجع مصدق من جهة خارجية (CA) لمصادقة إتصالات IPSec. بالإضافة إلى ذلك، يمكن لمكتب المحاسبة (ASA) إصدار شهادة رقمية ذاتية التوقيع. يجب إستخدام هذا الأمر لاتصالات SSH و HTTPS و Cisco Adaptive Security Device Manager (ASDM) بالجهاز.

يوضح هذا المستند الإجراءات اللازمة للحصول تلقائيا على شهادة رقمية من مرجع شهادات Microsoft (CA) خاص بالمرجع المصدق (ASA). ولا يتضمن الأسلوب اليدوي للتسجيل. يستخدم هذا المستند ASDM لخطوات التكوين، وكذلك يعرض تكوين واجهة سطر الأوامر النهائية (CLI).

ارجع إلى تسجيل شهادة Cisco IOS باستخدام مثال تكوين أوامر التسجيل المحسنة لمعرفة المزيد حول السيناريو نفسه مع الأنظمة الأساسية Cisco IOS®.

ارجع إلى تكوين مركز Cisco VPN 3000 4.7.x للحصول على شهادة رقمية وشهادة SSL لمعرفة المزيد حول نفس السيناريو مع مركز Cisco VPN 3000 Series Concentrator.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

متطلبات جهاز ASA

- قم بتكوين خادم Microsoft® Windows 2003 كمرجع مصدق.ارجع إلى وثائق Microsoft أو إلى البنية الأساسية للمفتاح العام ل Windows Server 2003
- للسماح بتكوين Cisco ASA أو PIX الإصدار x.7 بواسطة مدير أجهزة الأمان القابل للتكيف (ASDM)، ارجع إلى السماح بوصول HTTPS ل ASDM.
- قم بتثبيت الوظيفة الإضافية لخدمات الشهادات (mscep.dll).
- الحصول على الملف القابل للتنفيذ (cepsetup.exe) للوظيفة الإضافية من الوظيفة الإضافية لبروتوكول تسجيل الشهادات البسيط (SCEP) لخدمات الشهادات أو ملف mscep.dll من أدوات مجموعة موارد Windows Server 2003. **ملاحظة:** قم بتكوين التاريخ والوقت والمنطقة الزمنية الصحيحة على جهاز Microsoft Windows. يوصى بشدة باستخدام بروتوكول وقت الشبكة (NTP) ولكنه ليس ضروريا.

المكونات المستخدمة

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

- جهاز الأمان القابل للتكيف ASA 5500 Series، نسخة البرنامج x.7 والإصدارات الأحدث من Cisco
- Cisco Adaptive Security Device Manager، الإصدار x.5 والإصدارات الأحدث
- هيئة شهادة خادم Microsoft Windows 2003

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX 500 Series Security Appliance، الإصدار x.7.

الاصطلاحات

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

تكوين ASA لتبادل الشهادات باستخدام Microsoft CA

المهمة

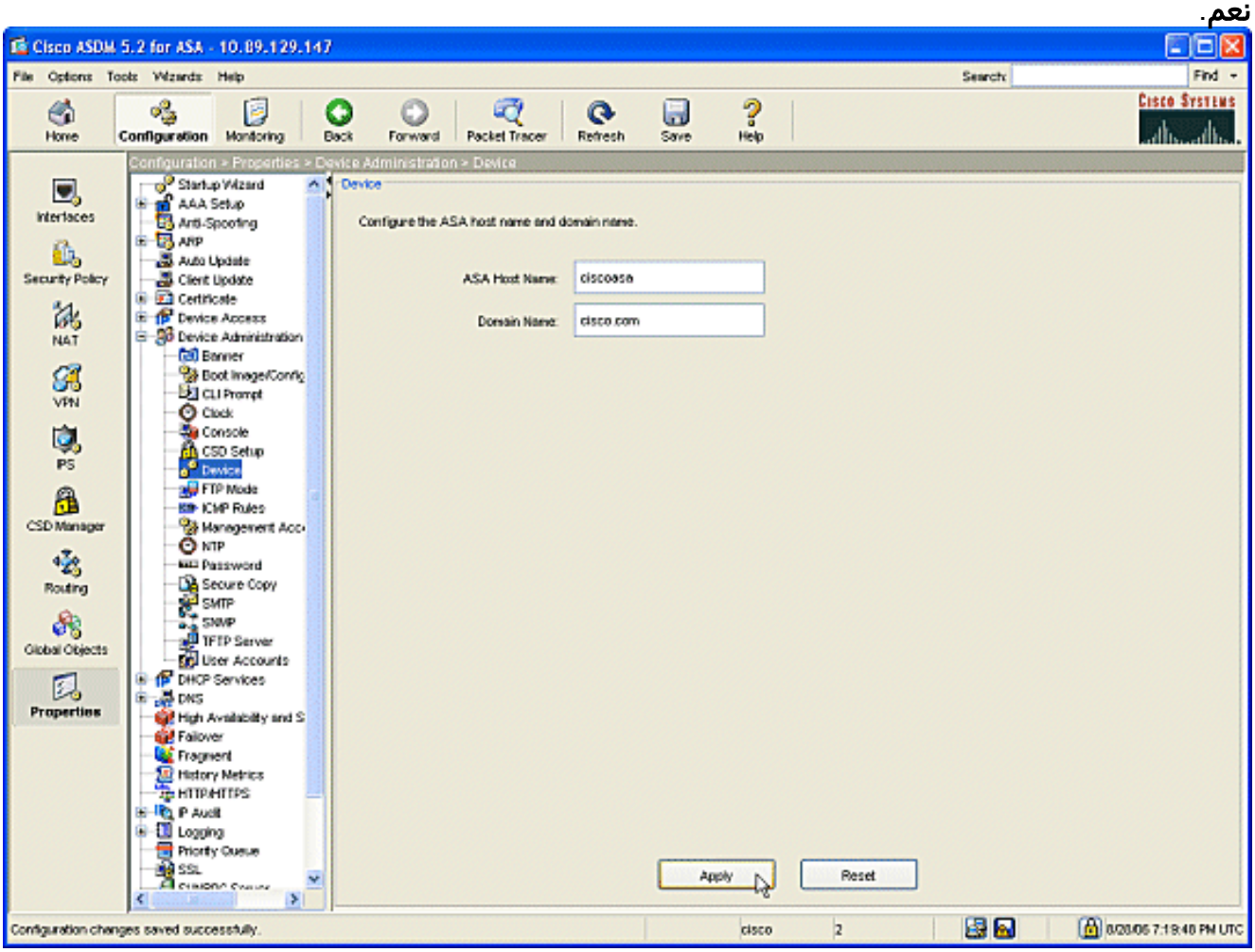
في هذا القسم، تظهر لك كيفية تكوين ASA لاستلام شهادة من مرجع شهادات Microsoft.

تعليمات لتكوين ASA

تستخدم الشهادات الرقمية مكون التاريخ/الوقت/المنطقة الزمنية كأحد عمليات التحقق من صلاحية الشهادة. يلزم تكوين Microsoft CA وجميع أجهزتك بالتاريخ والوقت الصحيحين. يستخدم المرجع المصدق ل Microsoft وظيفة إضافية (mscep.dll) إلى "خدمات الشهادات" الخاصة به لمشاركة الشهادات مع أجهزة Cisco.

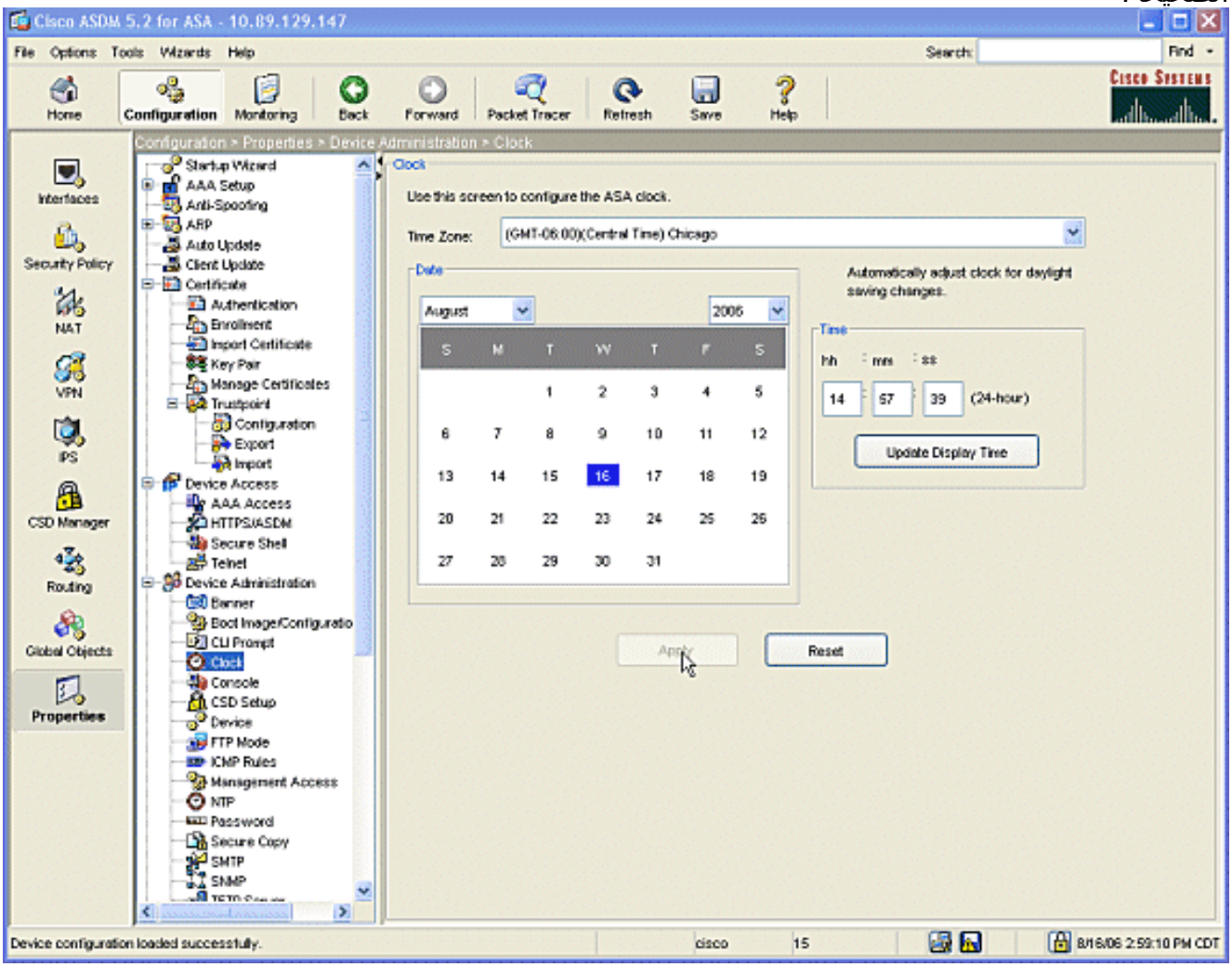
أتمت هذا steps أن يشكل ال ASA:

1. افتح تطبيق ASDM وانقر فوق زر **التكوين**.من القائمة اليسرى، انقر فوق الزر **خصائص**.من جزء التنقل، انقر فوق **إدارة الأجهزة > الجهاز**.دخلت مضيف إسم ومجال إسم ل ال ASA. طقطقة **يطبق**.عندما يطلب منك، انقر **حفظ > نعم**.

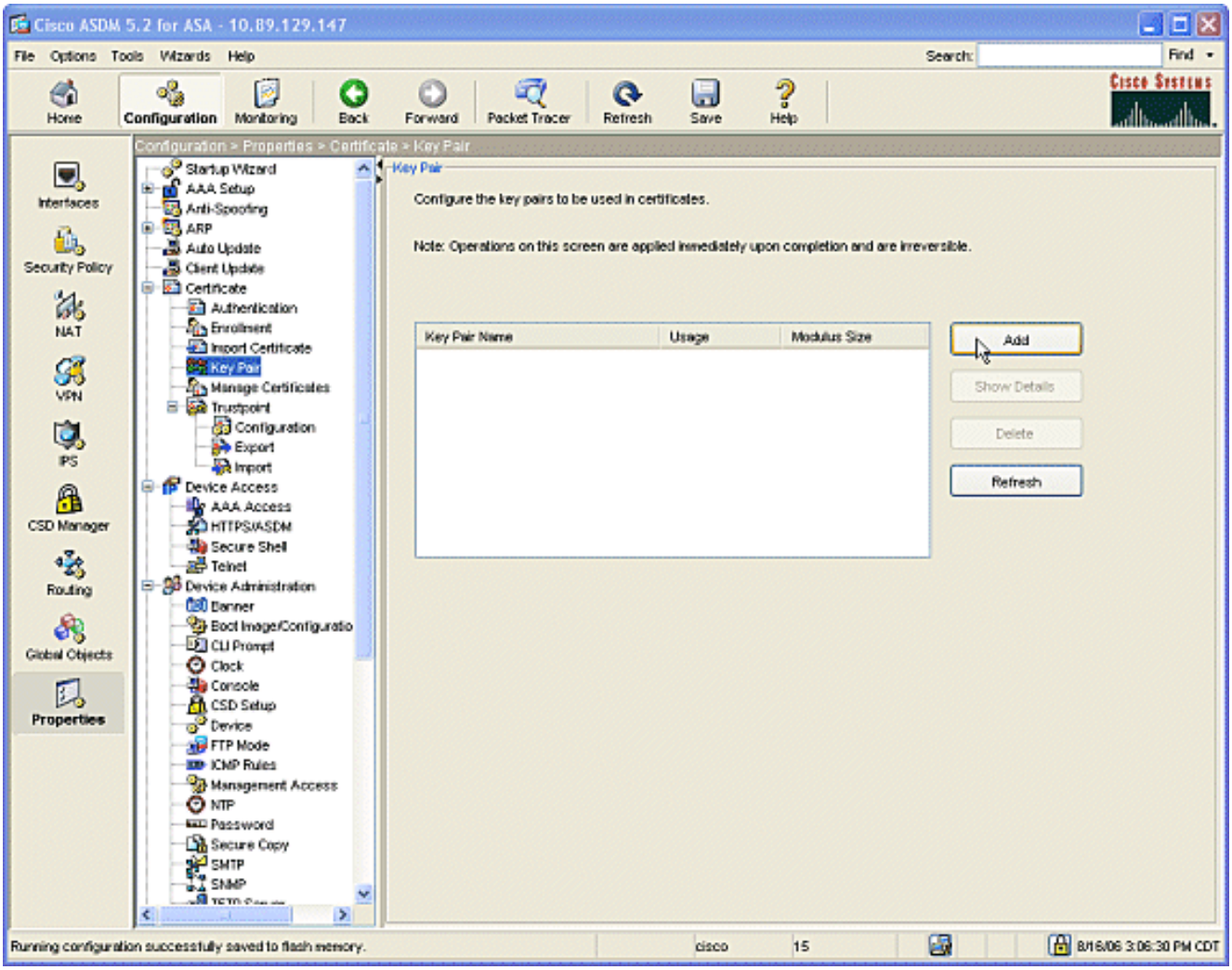


2. قم بتكوين ASA باستخدام التاريخ والوقت والمنطقة الزمنية الصحيحة. هذا مهم لإنشاء شهادة الجهاز. أستخدم

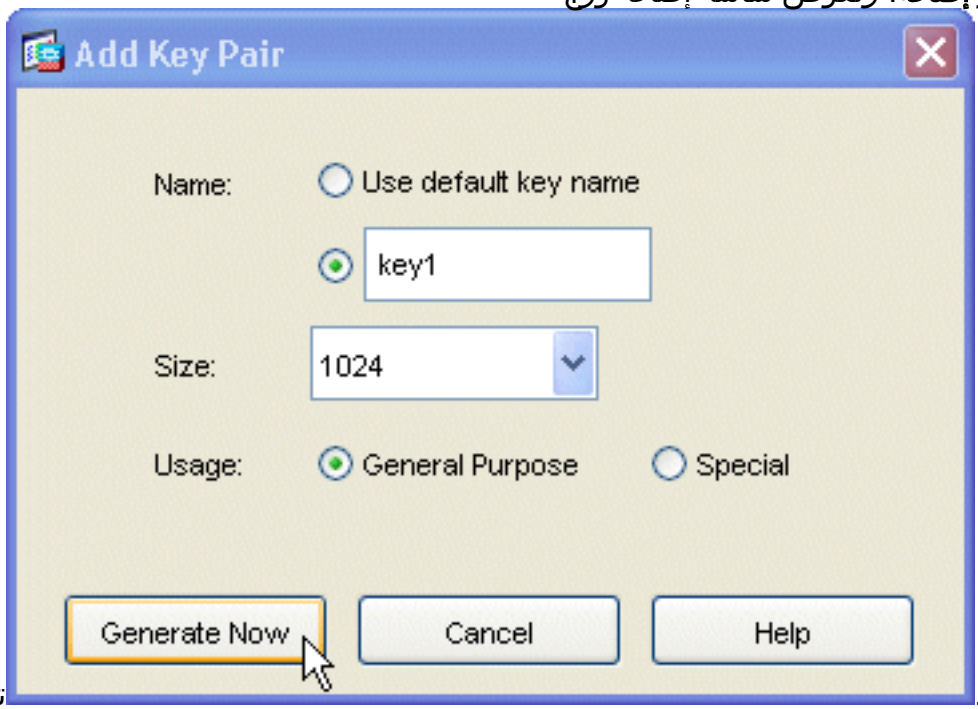
خادم NTP، إن أمكن.من جزء التنقل، انقر فوق **إدارة الأجهزة > الساعة**.في نافذة الساعة، أستخدم الحقول والسهم المنسدلة لتعيين التاريخ والوقت والمنطقة الزمنية الصحيحة.



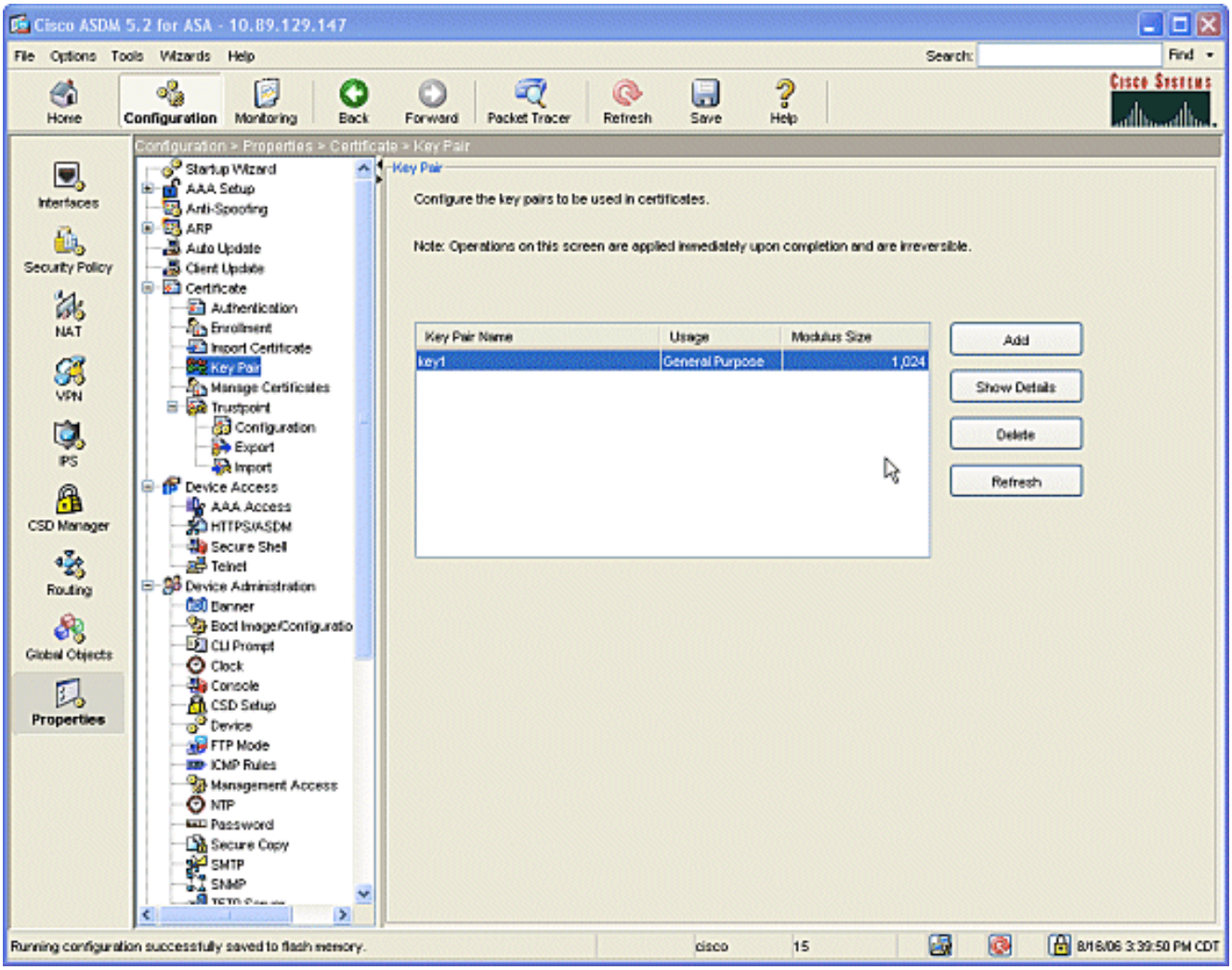
3. يجب أن يكون ل ASA زوج مفاتيح خاص به (المفاتيح الخاصة والعامة). سيتم إرسال المفتاح العام إلى Microsoft CA.من جزء التنقل، انقر فوق **شهادة > زوج المفاتيح**.



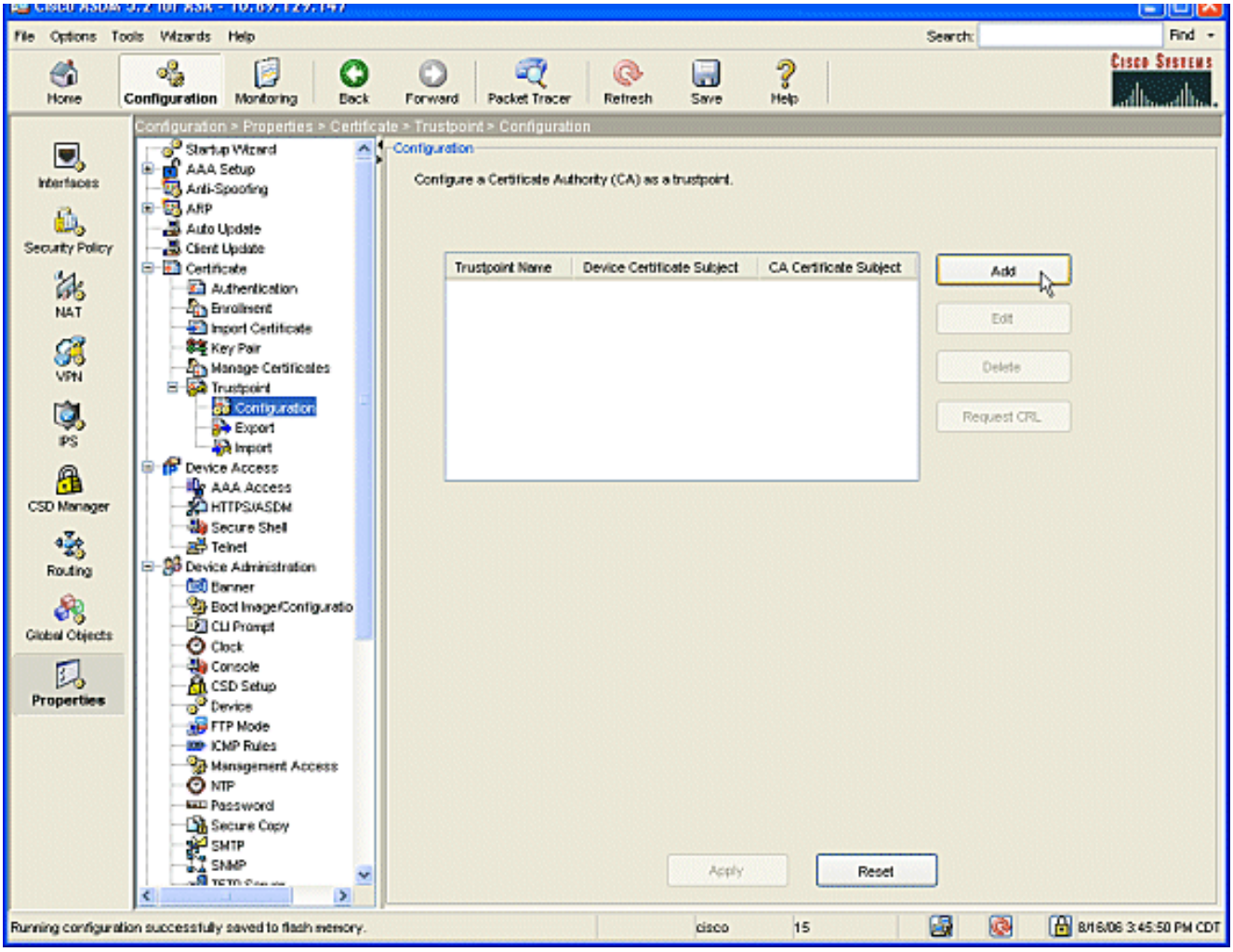
انقر زر **إضافة**، وتعرض شاشة إضافة زوج



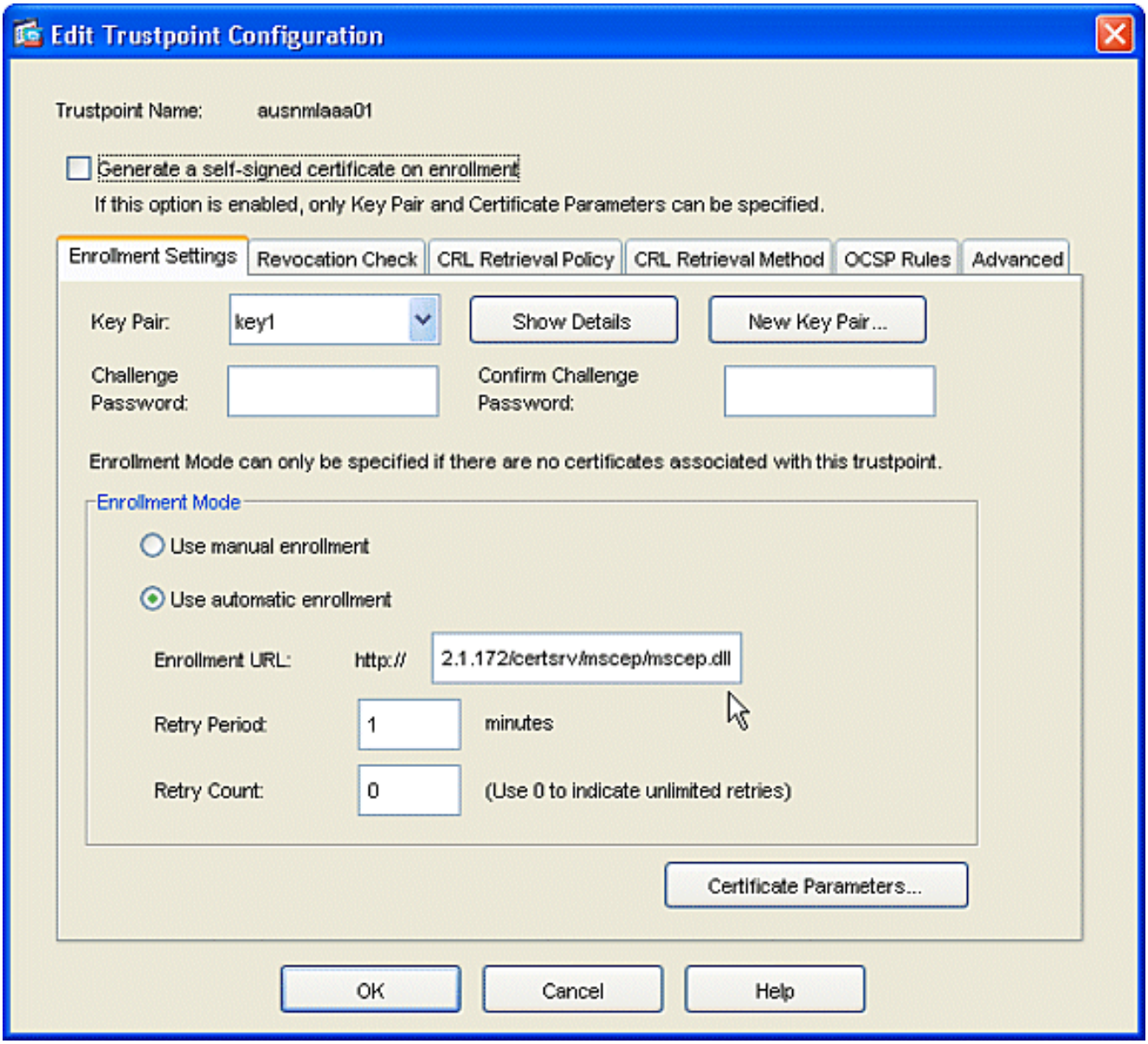
مفاتيح.تحقق من زر الخيار الموجود بجانب الحقل الفارغ من منطقة **الاسم**، واكتب اسم المفتاح.انقر فوق **الحجم:** السهم بجوار المربع المنسدل لاختيار حجم للمفتاح، أو قبول الافتراضي.افحص زر الخيار **العام الغرض** تحت الاستخدام.انقر فوق الزر **إنشاء الآن** لإعادة إنشاء المفاتيح والعودة إلى نافذة زوج المفاتيح، حيث يمكنك عرض المعلومات الخاصة بزوج
المفاتيح.



4. قم بتكوين المرجع المصدق ل Microsoft لاعتباره جديرا بالثقة. من جزء التنقل، انقر فوق **TrustPoint > التكوين**.من نافذة "التكوين"، انقر فوق الزر **إضافة**.

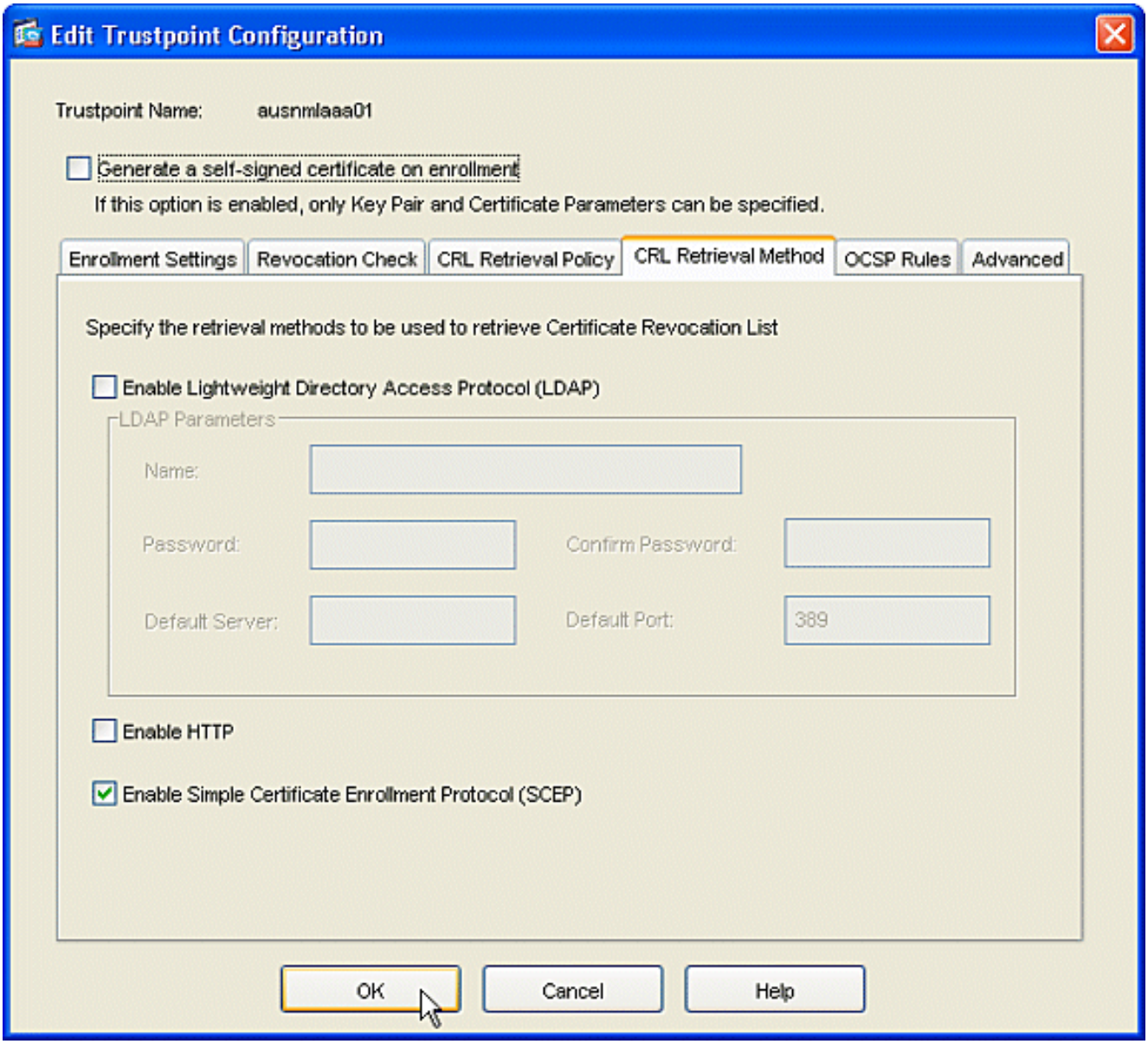


تظهر نافذة تحرير تكوين
.TrustPoint

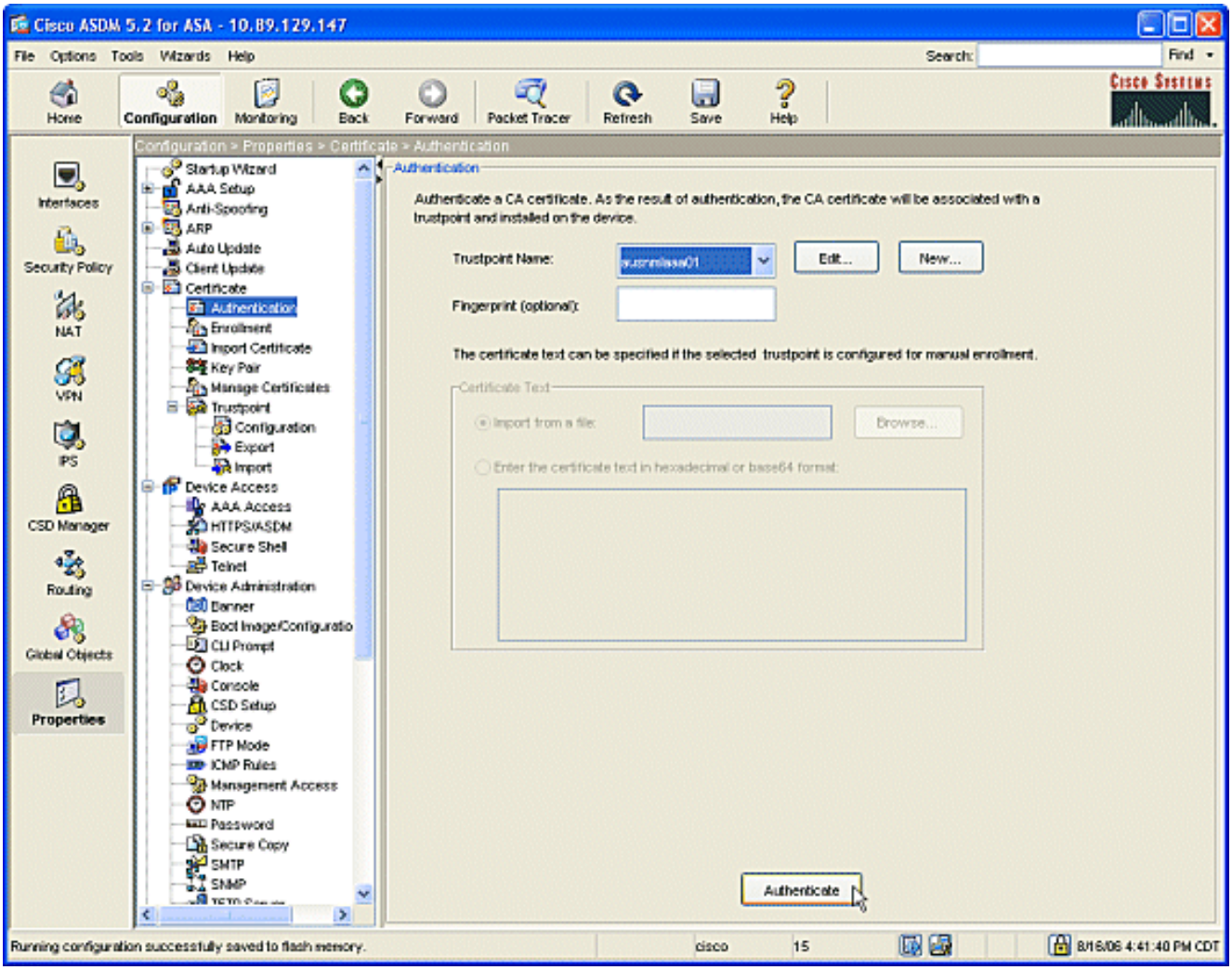


قم بتعبئة اسم ل TrustPoint باسم المرجع المصدق.انقر فوق **زوج المفاتيح:** السهم بجوار المربع المنسدل، واختر اسم زوج المفاتيح الذي قمت بإنشائه.تحقق من الزر **إستخدام** راديو **التسجيل التلقائي**، وأدخل عنوان URL ل **http://CA_IP_Address/certsrv/mscep/mscep.dll** Microsoft CA:.

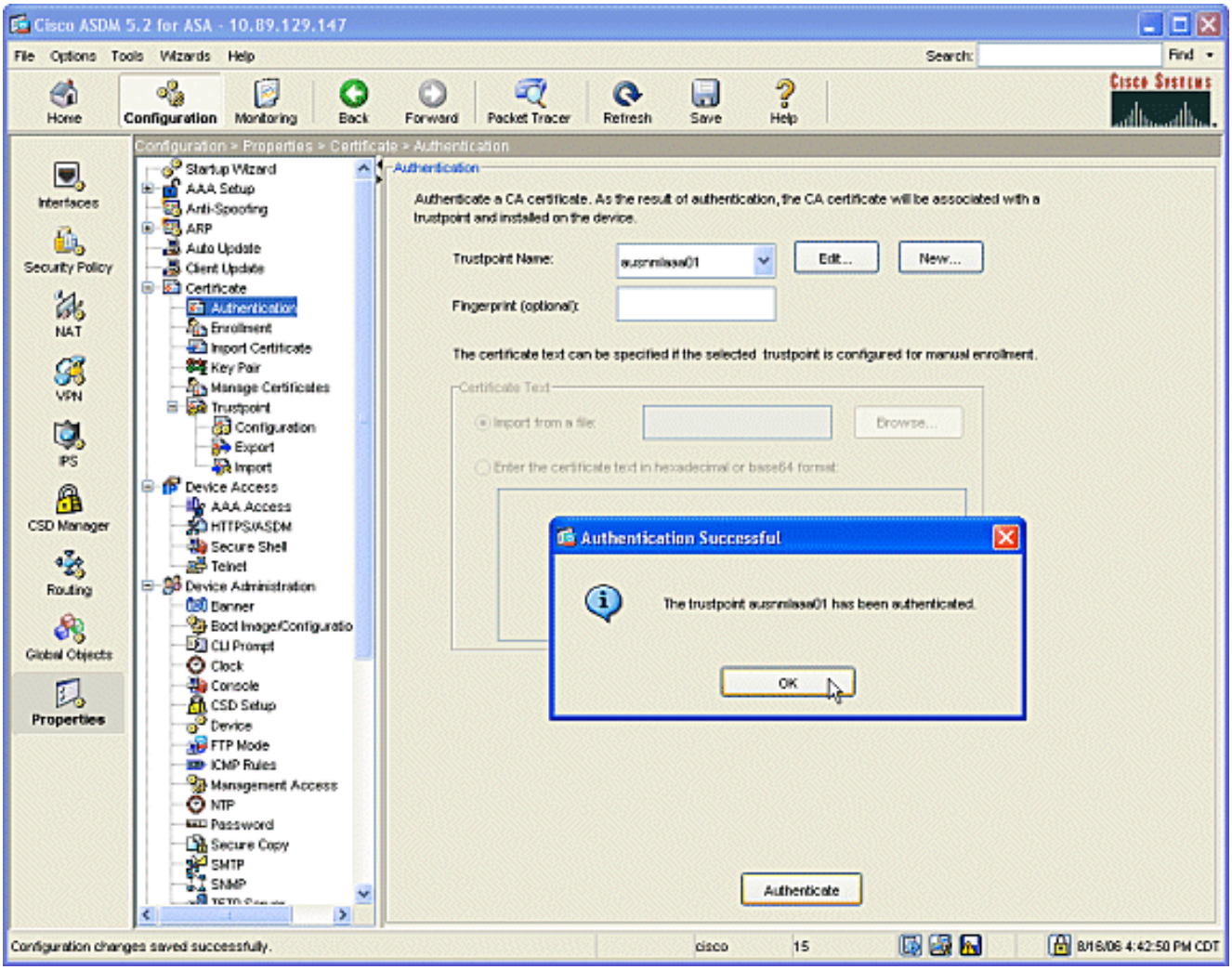
5. انقر فوق علامة التبويب **أسلوب إسترداد CRL**.قم بإلغاء تحديد خانة الاختيار تمكين http وتمكين البروتوكول الخفيف للوصول إلى الدليل (LDAP).حدد خانة الاختيار تمكين بروتوكول تسجيل الشهادة البسيط (SCEP). أترك كل إعدادات الجدولة الأخرى في إعداداتها الافتراضية.انقر فوق الزر **موافق**.



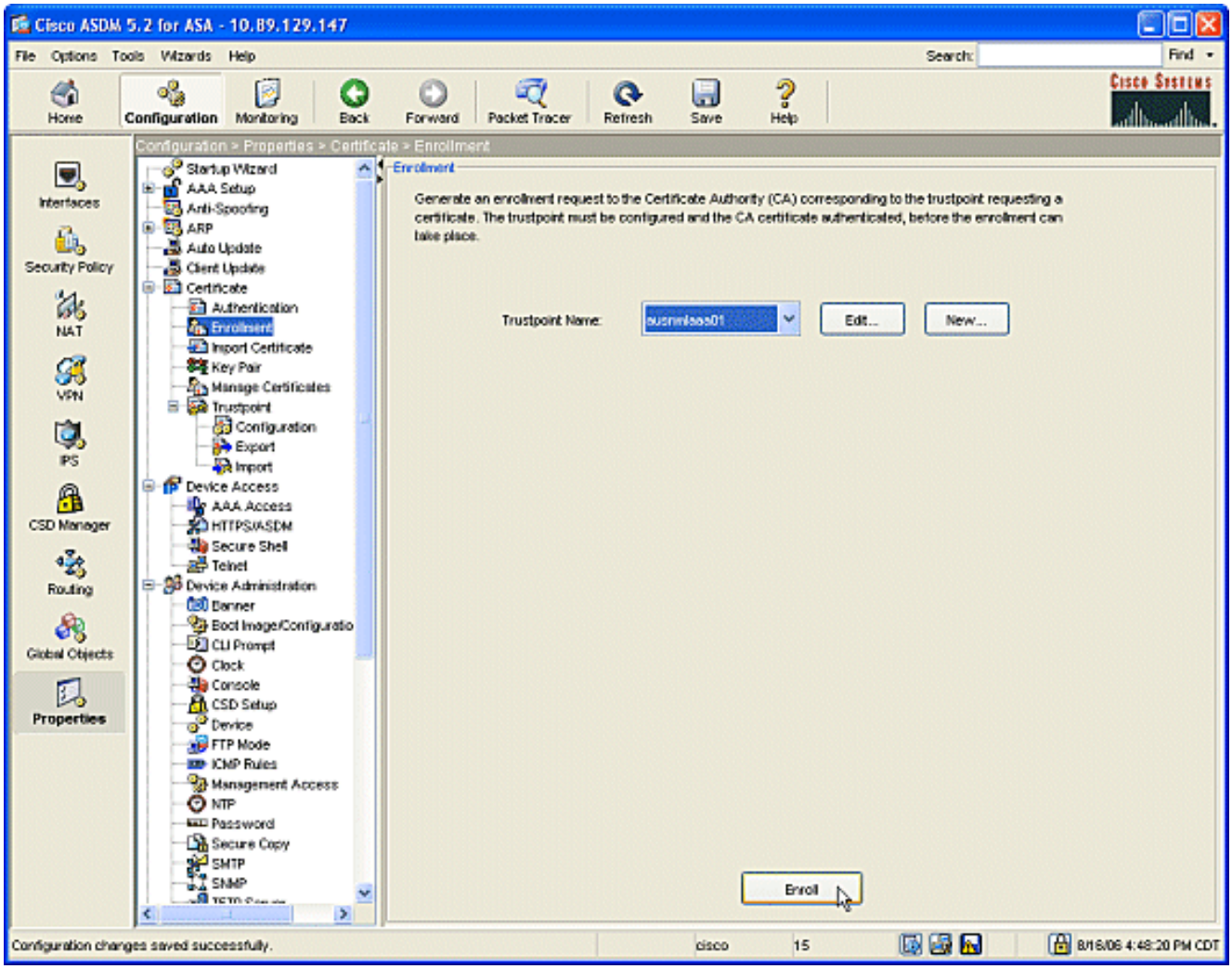
6. مصادقة Microsoft CA والتسجيل به. من جزء التنقل، انقر على **شهادة > مصادقة**. تأكد من إظهار TrustPoint الذي تم إنشاؤه حديثا في الحقل **TrustPoint Name**:. انقر فوق زر **المصادقة**.



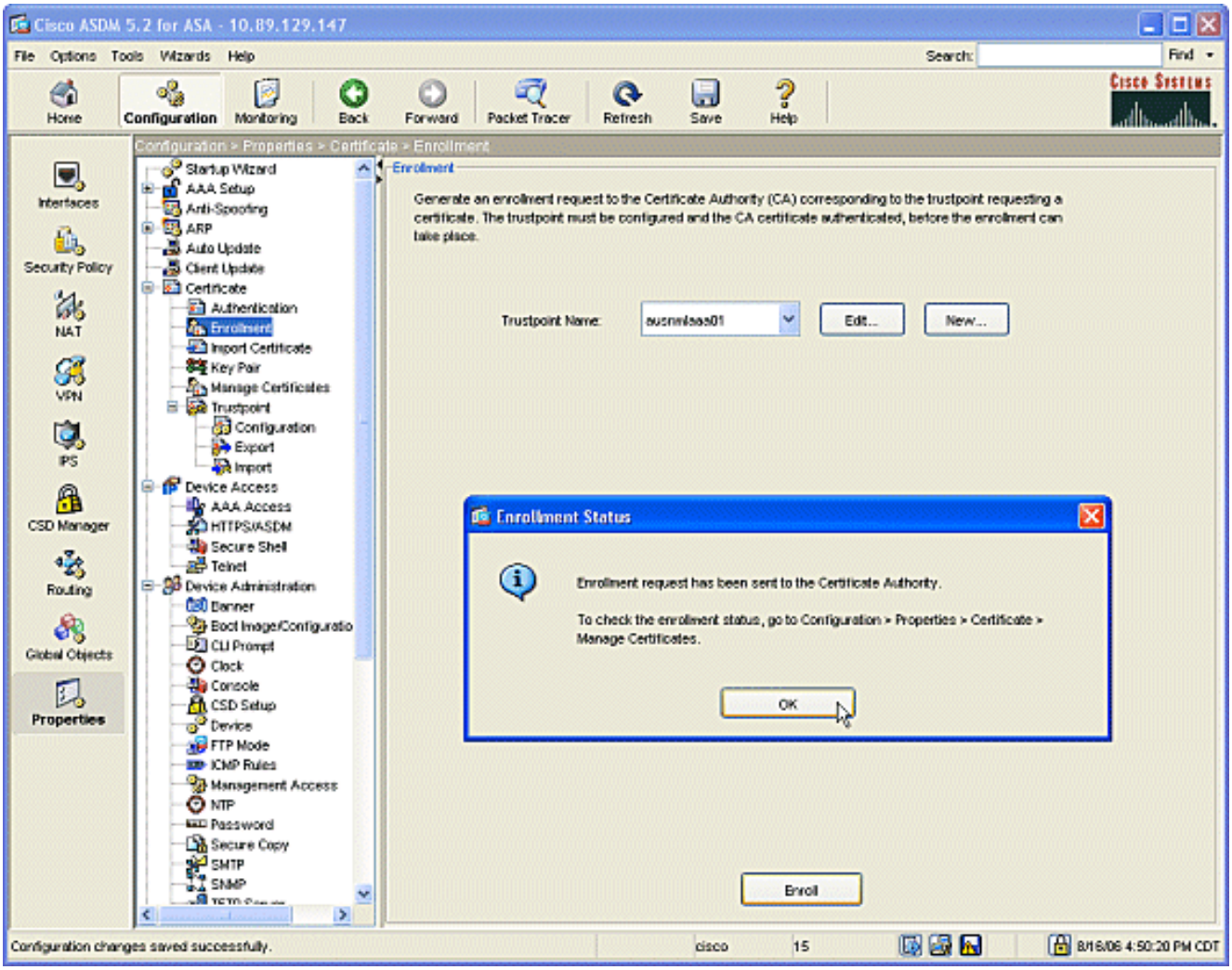
7. يعرض مربع حوار لإعلامك بأنه قد تم مصادقة TrustPoint. انقر فوق الزر **موافق**.



8. من جزء التنقل، انقر فوق **التسجيل**. تأكد من عرض اسم TrustPoint في حقل اسم TrustPoint، وانقر فوق زر
التسجيل.



9. يظهر مربع حوار لإعلامك بأن الطلب تم إرساله إلى CA. انقر فوق الزر **موافق**.



ملاحظة: على جهاز Microsoft Windows المستقل، يجب إصدار الشهادات لأي طلبات تم إرسالها إلى المرجع المصدق. ستكون الشهادة في حالة معلقة حتى تنقر بزر الماوس الأيمن فوق الشهادة ثم انقر فوق إصدار على خادم Microsoft.

النتائج

هذا هو تكوين واجهة سطر الأوامر (CLI) الذي ينتج من خطوات ASDM:

سيسكوسا

```
ciscoasa# sh run
(ASA Version 7.2(1
!
hostname ciscoasa
domain-name cisco.com
enable password t/G/EqWCJSp/Q6R4 encrypted
names
name 172.22.1.172 AUSNMLAAA01
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
```

```
                    ip address 10.4.4.1 255.255.255.0
                                                     !
                                        interface Ethernet0/2
                                                 shutdown
                                               no nameif
                                          no security-level
                                              no ip address
                                                     !
                                       interface Management0/0
                                                 shutdown
                                               no nameif
                                          no security-level
                                              no ip address
                                                     !
                                passwd 2KFQnbNIdI.2KYOU encrypted
                                             ftp mode passive
       Set your correct date/time/time zone ! clock ---!
     timezone CST -6 clock summer-time CDT recurring dns
     server-group DefaultDNS domain-name cisco.com pager
  lines 20 logging enable logging asdm informational mtu
                inside 1500 mtu outside 1500 asdm image
   disk0:/asdm521.bin no asdm history enable arp timeout
      14400 nat (inside) 0 0.0.0.0 0.0.0.0 route outside
      0.0.0.0 0.0.0.0 172.22.1.1 1 timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
   icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
       1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
       0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
       disconnect 0:02:00 timeout uauth 0:05:00 absolute
      username cisco password VjcVTJy0i9Ys9P45 encrypted
        privilege 15 http server enable http AUSNMLAAA01
   255.255.255.255 outside http 172.22.1.0 255.255.255.0
    outside http 64.101.0.0 255.255.0.0 outside no snmp-
      server location no snmp-server contact snmp-server
        enable traps snmp authentication linkup linkdown
    coldstart ! !--- identify the trustpoint ! crypto ca
                    trustpoint ausnmlaaa01 enrollment url
  http://172.22.1.172:80/certsrv/mscep/mscep.dll keypair
key1 crl configure no protocol http no protocol ldap !--
  - the certificate chain generated automatically crypto
            ca certificate chain ausnmlaaa01 certificate
61c79bea000100000008 30820438 30820320 a0030201 02020a61
   c79bea00 01000000 08300d06 092a8648 86f70d01 01050500
   30423113 3011060a 09922689 93f22c64 01191603 636f6d31
   15301306 0a099226 8993f22c 64011916 05636973 636f3114
   30120603 55040313 0b617573 6e6d6c61 61613031 301e170d
   30363038 31363231 34393230 5a170d30 37303831 36323135
   3932305a 30233121 301f0609 2a864886 f70d0109 02131263
   6973636f 6173612e 63697363 6f2e636f 6d30819f 300d0609
   2a864886 f70d0101 01050003 818d0030 81890281 8100c2c7
   fefc4b18 74e7972e daee53a2 b0de432c 4d34ec76 48ba37e6
   e7294f9b 1f969088 d3b2aaef d6c44cfa bdbe740b f5a89131
   b177fd52 e2bfb91c d665f54e 7eee0916 badc4601 79b4f7b3
   8102645a 01fedb62 e8db2a60 188d13fc 296803a5 68739bb6
   940cd33a d746516f 01d52935 8b6302b6 3c3e1087 6c5e91a9
   c5e2f92b d3cb0203 010001a3 8201d130 8201cd30 0b060355
   1d0f0404 030205a0 301d0603 551d1104 16301482 12636973
   636f6173 612e6369 73636f2e 636f6d30 1d060355 1d0e0416
   0414080d fe9b7756 51b5e63b fa6dcfa5 076030db 08c5301f
   0603551d 23041830 16801458 026754ae 32e081b7 8522027e
   33bffe79 c6abb730 75060355 1d1f046e 306c306a a068a066
   86306874 74703a2f 2f617573 6e6d6c61 61613031 2f436572
   74456e72 6f6c6c2f 6175736e 6d6c6161 61303128 31292e63
   726c8632 66696c65 3a2f2f5c 5c415553 4e4d4c41 41413031
```

```
    5c436572 74456e72 6f6c6c5c 6175736e 6d6c6161 61303128
    31292e63 726c3081 a606082b 06010505 07010104 81993081
    96304806 082b0601 05050730 02863c68 7474703a 2f2f6175
    736e6d6c 61616130 312f4365 7274456e 726f6c6c 2f415553
    4e4d4c41 41413031 5f617573 6e6d6c61 61613031 2831292e
    63727430 4a06082b 06010505 07300286 3e66696c 653a2f2f
    5c5c4155 534e4d4c 41414130 315c4365 7274456e 726f6c6c
    5c415553 4e4d4c41 41413031 5f617573 6e6d6c61 61613031
    2831292e 63727430 3f06092b 06010401 82371402 04321e30
    00490050 00530045 00430049 006e0074 00650072 006d0065
    00640069 00610074 0065004f 00660066 006c0069 006e0065
    300d0609 2a864886 f70d0101 05050003 82010100 0247af67
    30ae031c cbd9a2fb 63f96d50 a49ddff6 16dd377d d6760968
    8ad6c9a8 c0371d65 b5cd6a62 7a0746ed 184b9845 84a42512
    67af6284 e64a078b 9e9d1b7a 028ffdd7 d262f6ba f28af7cf
    57a48ad4 761dcfda 3420c506 e8c4854c e4178304 a1ae6e38
    a1310b5b 2928012b 40aaad56 1a22d4ce 7d62a0e5 931f74f5
    5510574f 27a6ea21 3f3d2118 2a087aad 0177cc56 1f8c024c
    42f9fb9a ef180bc1 4fca1504 59c3b850 acad01a9 c2fbb46b
    2be53a9f 10ad50a4 1f557b8d 1f25f7ae b2e2eeca 7800053c
     3afd436 73863d76 53bd58c9 803fe5e9 708f00fd 85e84220
    0c713c3f 4ccb0c0b 84bb265d fd40c9d0 a68efb3e d6faeef0
           b9958ca7 d1eb25f8 51f38a50 quit certificate ca
       62829194409db5b94487d34f44c9387b 308203ff 308202e7
    a0030201 02021062 82919440 9db5b944 87d34f44 c9387b30
    0d06092a 864886f7 0d010105 05003042 31133011 060a0992
    268993f2 2c640119 1603636f 6d311530 13060a09 92268993
    f22c6401 19160563 6973636f 31143012 06035504 03130b61
    75736e6d 6c616161 3031301e 170d3036 30383136 31383135
    31325a17 0d313130 38313631 38323430 325a3042 31133011
    060a0992 268993f2 2c640119 1603636f 6d311530 13060a09
    92268993 f22c6401 19160563 6973636f 31143012 06035504
    03130b61 75736e6d 6c616161 30313082 0122300d 06092a86
    4886f70d 01010105 00038201 0f003082 010a0282 01010096
    1abddec6 ce3768e6 4e04b42f ec28d6f9 330cd9a2 9ec3eb9e
    8a091cf8 b4969158 3dc6d6ba 332bc3b4 32fc1495 9ac85322
    1c842df1 7a110be2 7f2fc5e2 3a475da8 711e4ff7 0dd06c21
    6f6e3517 621c89f9 a01779b8 3a5fce63 3ed66c58 2982dbf2
    21f9c139 5cd6cf17 7bde4c0a 22033312 d1b98435 e3a05003
    888da568 6223243f 834316f0 4874168d c291f098 24177ade
    a71d5128 120e1848 6f8a5a33 6f4efa1c 27bb7c4d f49fb0f7
    57736f7d 320cf834 1ef28649 b719ae7c e58de17f 1259f121
    df90668d aee59f71 dd1110a2 de8a2a8b db6de0c7 b5540e21
    4ff1a0c5 7cb0290e bfd5a7bb 21bd7ad3 bce7b986 e0f77b30
    c8b719d9 37c355f6 ec103188 7d5d3702 03010001 a381f030
    81ed300b 0603551d 0f040403 02018630 0f060355 1d130101
    ff040530 030101ff 301d0603 551d0e04 16041458 026754ae
    32e081b7 8522027e 33bffe79 c6abb730 75060355 1d1f046e
    306c306a a068a066 86306874 74703a2f 2f617573 6e6d6c61
    61613031 2f436572 74456e72 6f6c6c2f 6175736e 6d6c6161
    61303128 31292e63 726c8632 66696c65 3a2f2f5c 5c415553
    4e4d4c41 41413031 5c436572 74456e72 6f6c6c5c 6175736e
    6d6c6161 61303128 31292e63 726c3012 06092b06 01040182
    37150104 05020301 00013023 06092b06 01040182 37150204
    16041490 48bcef49 d228efee 7ba90b35 879a5a61 6a276230
    0d06092a 864886f7 0d010105 05000382 01010042 f59e2675
    0defc49d abe504b8 eb2b2161 b76842d3 ab102d7c 37c021d4
    a18b62d7 d5f1337e 22b560ae acbd9fc5 4b230da4 01f99495
    09fb930d 5ff0d869 e4c0bf07 004b1deb e3d75bb6 ef859b13
    6b6e0697 403a4a58 4f6dd1bc 3452f329 a73b572a b41327f7
    5af61809 c9fb86a4 b8d4aca6 f5ebc97f 2c3e306b ea58ed49
    c245be2a 03f40878 273ae747 02b22219 5e3450a9 6fd72f1d
    40e0931a 7b5cc3b0 d6558ec7 514ef928 b1dfa9ab 732ecea0
    40a458c3 e824fd6f b7c6b306 122da64d b3ab23b1 adacf609
```

```
    1d1132fb 15aa6786 06fbf713 b25a4a5c 07de565f 6364289c
    324aacff abd6842e b24d4116 5c0934b3 794545df 47da8f8d
         2b0e8461 b2405ce4 6528 99 quit telnet 64.101.0.0
       255.255.0.0 outside telnet timeout 5 ssh timeout 5
  console timeout 0 ! class-map inspection_default match
  default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
       policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
    inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
     policy global_policy global prompt hostname context
   Cryptochecksum:fa0c88a5c687743ab26554d54f6cb40d : end
```

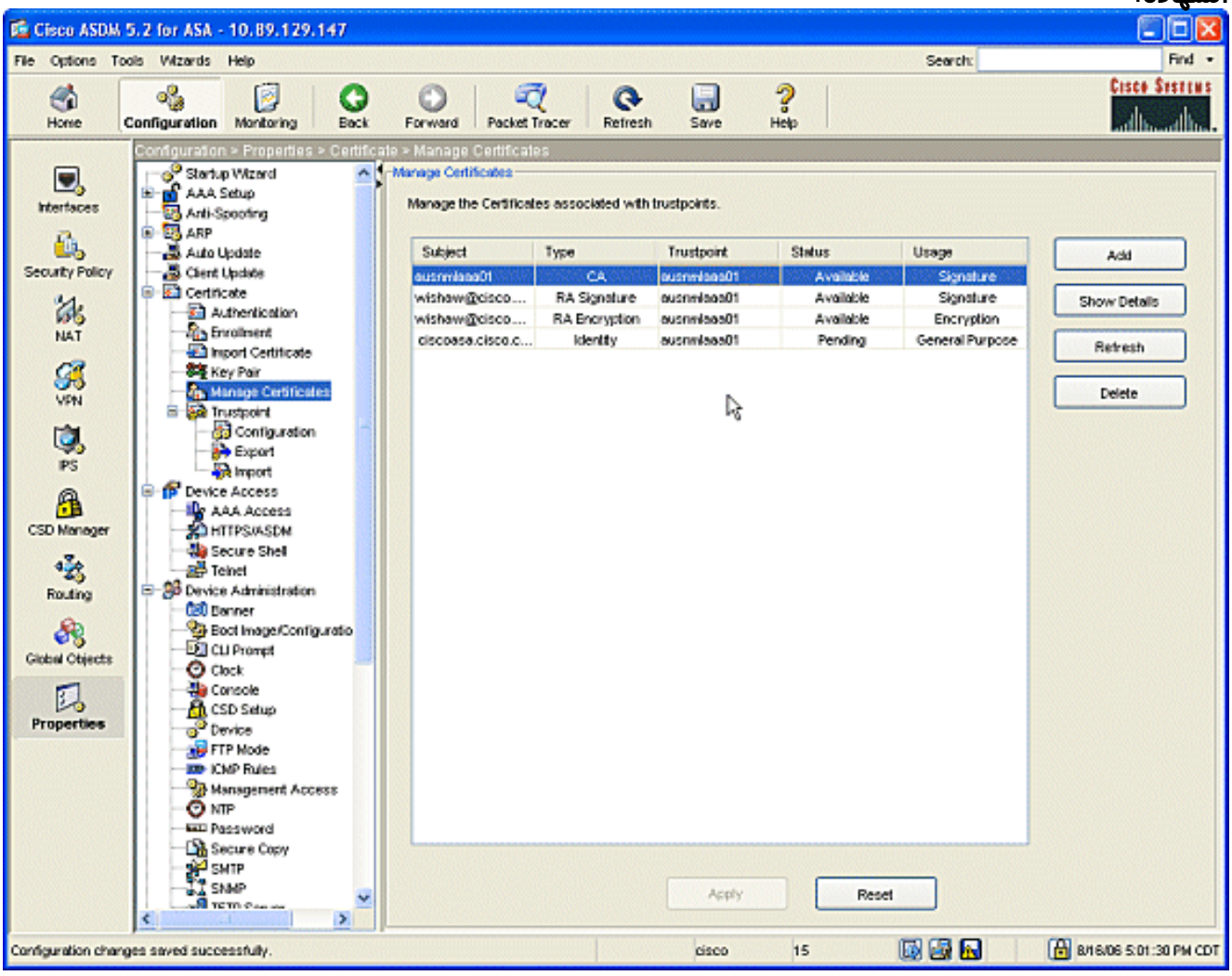
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

التحقق من الشهادة وإدارتها

مراجعة الشهادة وإدارتها.

1. افتح تطبيق ASDM وانقر فوق زر **التكوين**.
2. من القائمة اليسرى، انقر فوق الزر **خصائص**.انقر على **شهادة**.انقر على **إدارة الشهادة**.



الأوامر

على ال ASA أنت يستطيع استعملت عدة **عرض** أمر في الأمر خط أن يدقق الحالة من شهادة.

- يستخدم الأمر **show crypto ca certificates** لعرض معلومات حول شهادتك، وشهادة CA، وأي شهادات مرجع تسجيل (RA).
- يتم إستخدام الأمر **show crypto ca trustPoints** للتحقق من تكوين TrustPoint.
- يتم إستخدام الأمر **show crypto key mypubkey rsa** لعرض مفاتيح RSA العامة من ASA لديك.
- يتم إستخدام الأمر **show crypto ca crl** لعرض جميع قوائم التحكم في الوصول إلى البنية الأساسية (CRL) المخزنة مؤقتا .

ملاحظة: الإنتاج مترجم بساند أداة (بسجل زبون فقط) (OIT) مؤكد **عرض** أمر. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

ارجع إلى البنية الأساسية للمفتاح العام ل Windows Server 2003 للحصول على مزيد من المعلومات حول كيفية أستكشاف أخطاء Microsoft Windows 2003 CA وإصلاحها.

الأوامر

ملاحظة: يمكن أن يؤثر إستخدام أوامر **تصحيح الأخطاء سلبا** على جهاز Cisco الخاص بك. قبل إستخدام أوامر **debug**، ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء.

معلومات ذات صلة

- تكوين مركز Cisco VPN 3000 Concentrator 4.0.x للحصول على شهادة رقمية

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).