如何使用ASA上的ASDM從Microsoft Windows CA獲取數位證書

目錄

簡介

數位證書可用於驗證網路上的網路裝置和使用者。它們可用於在網路節點之間協商IPSec會話。

思科裝置可通過三種主要方式在網路上安全地識別自己：

1. **預共用金鑰**。兩個或多個裝置可以具有相同的共用金鑰。對等體通過計算和傳送包含預共用金鑰的資料的金鑰雜湊來相互進行身份驗證。如果接收對等體能夠使用其預共用金鑰獨立建立相同的雜湊，則它知道兩個對等體必須共用相同的金鑰，從而驗證另一個對等體。此方法需要手動操作，擴展性不是很強。
2. **自簽名證書**。裝置會生成自己的證書並簽署為有效。此類證書的使用應該有限。例如，將此證書與SSH和HTTPS訪問配合使用以進行配置。需要單獨的使用者名稱/密碼對才能完成連線。**注意：持**續自簽名證書在路由器重新載入後仍然有效，因為它們儲存在裝置的非易失性隨機訪問儲存器(NVRAM)中。如需詳細資訊，請參閱持續自簽名的憑證。SSL VPN(WebVPN)連線就是一個很好的使用示例。
3. **證書頒發機構證書**。第三方驗證並驗證嘗試通訊的兩個或多個節點。每個節點都有一個公鑰和私鑰。公鑰加密資料，私鑰解密資料。由於他們是從同一來源獲得證書的，因此可以確保他們各自的身份。ASA裝置可以通過手動註冊方法或自動註冊方法從第三方獲取數位證書。**注意**：您選擇的數位證書的註冊方法和型別取決於每個第三方產品的特性和功能。有關詳細資訊，請與證書服務的供應商聯絡。

思科自適應安全裝置(ASA)可以使用由第三方證書頒發機構(CA)提供的預共用金鑰或數位證書來驗證IPSec連線。此外，ASA可以生成自己的自簽名數位證書。這應該用於裝置的SSH、HTTPS和思科自適應安全裝置管理器(ASDM)連線。

本文檔演示從Microsoft證書頒發機構(CA)自動獲取ASA的數位證書的必要步驟。它不包括手動註冊方法。本文檔使用ASDM執行配置步驟，並顯示最終的命令列介面(CLI)配置。

請參閱使用增強型註冊命令的Cisco IOS證書註冊配置示例，以瞭解更多有關Cisco IOS®平台相同方案的詳細資訊。

請參閱配置Cisco VPN 3000集中器4.7.x以獲得數位證書和SSL證書，以瞭解有關Cisco VPN 3000系列集中器的相同方案的詳細資訊。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

ASA裝置的要求

- 將Microsoft® Windows 2003 Server配置為CA。請參閱Microsoft文檔或Windows Server 2003公鑰基礎架構
- 要允許自適應安全裝置管理器(ASDM)配置Cisco ASA或PIX版本7.x，請參閱允許ASDM的HTTPS訪問。
- 安裝證書服務的載入項(mscep.dll)。
- 從證書服務的簡單證書註冊協定(SCEP)載入項獲取該載入項的執行檔(cepsetup.exe) ，或從Windows Server 2003資源工具包工具 獲取mscep.dll檔案。**注意：**在Microsoft Windows電腦上配置正確的日期、時間和時區。強烈建議但不必要使用網路時間協定(NTP)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA 5500系列自適應安全裝置軟體版本7.x及更高版本
- 思科自適應安全裝置管理器5.x版及更高版本
- Microsoft Windows 2003 Server證書頒發機構

相關產品

此配置還可以與Cisco PIX 500系列安全裝置版本7.x一起使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

配置ASA以與Microsoft CA交換證書

工作

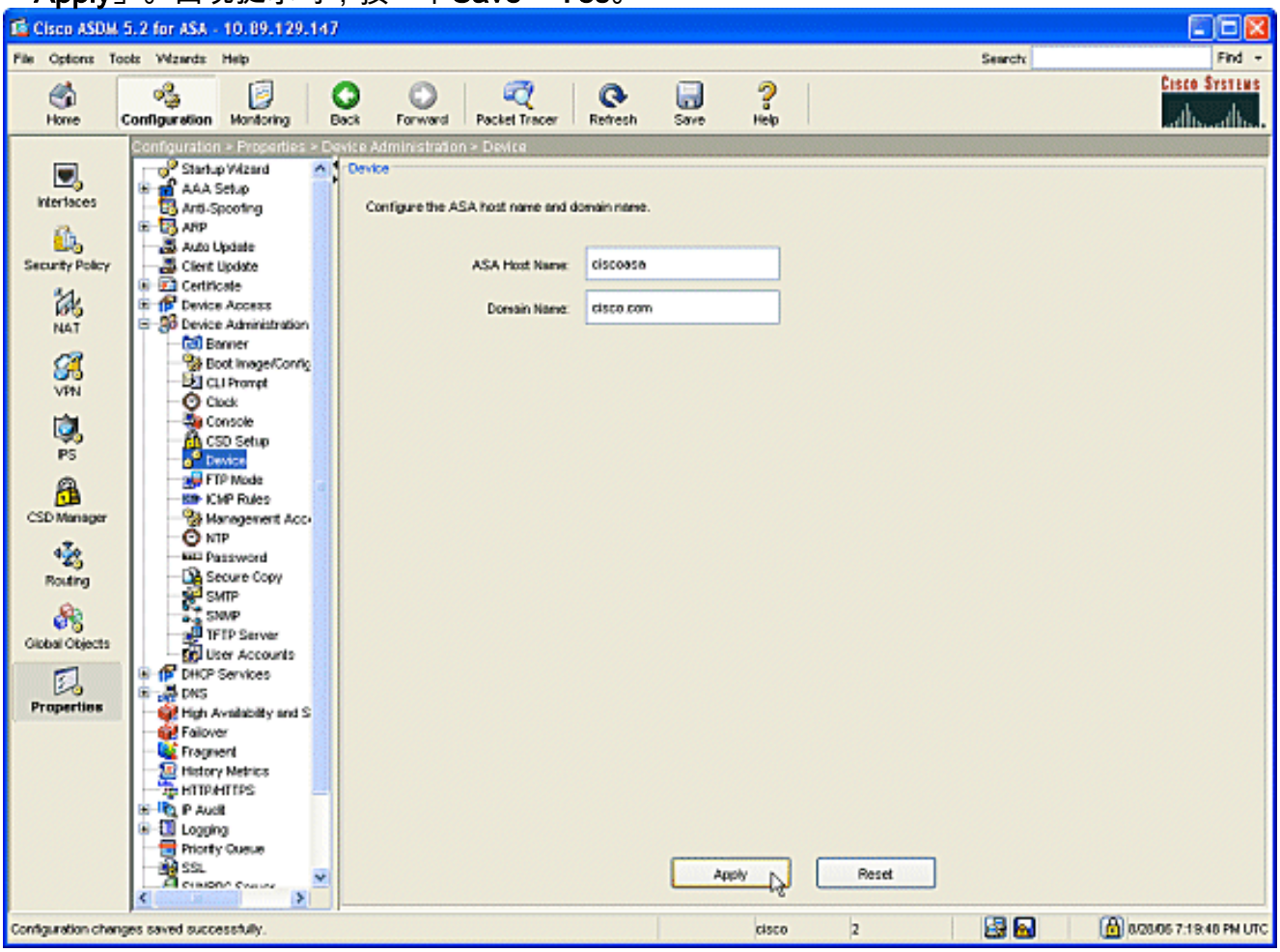
在此部分中，您將瞭解如何配置ASA以從Microsoft證書頒發機構接收證書。

配置ASA的說明

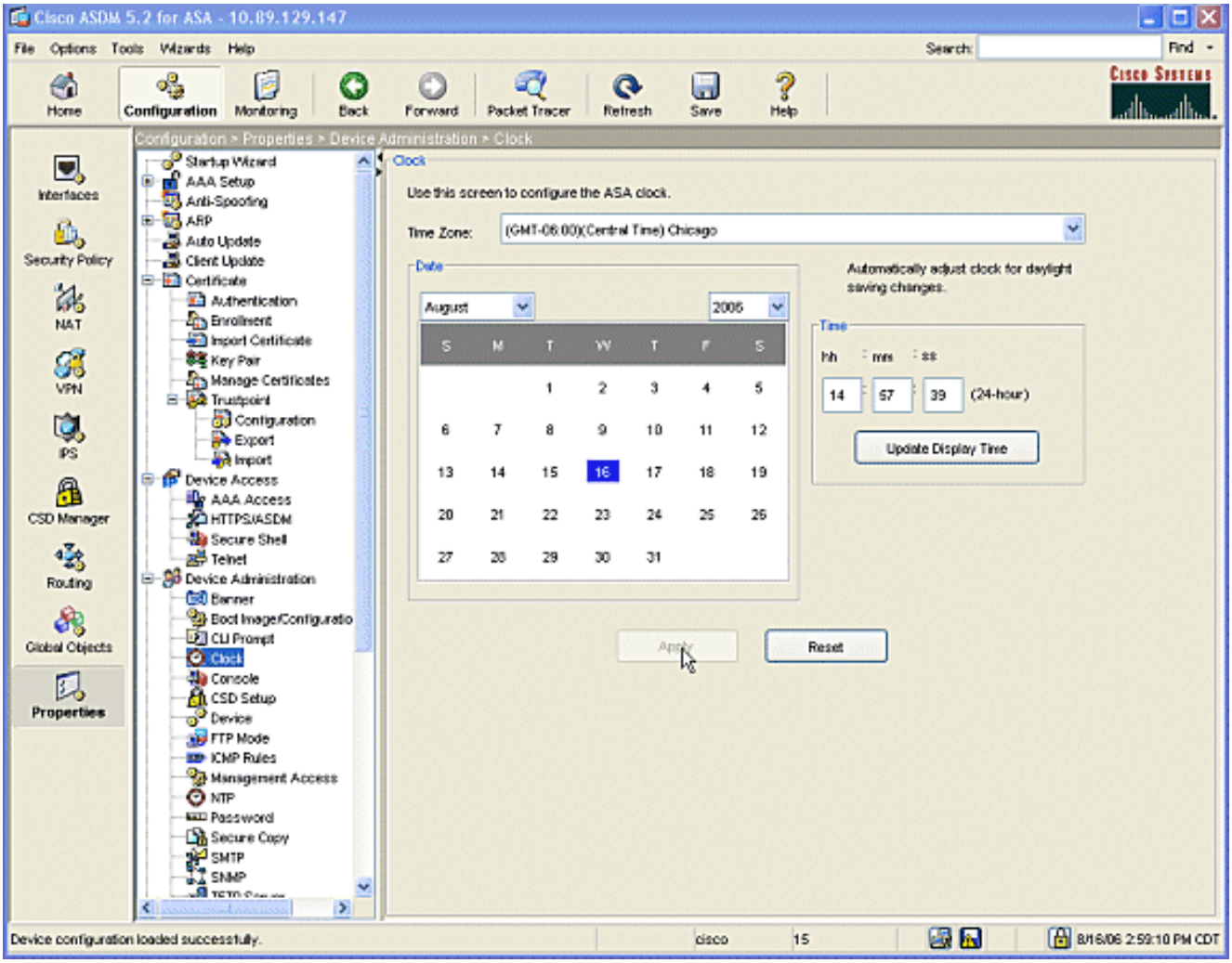
數位證書使用日期/時間/時區元件作為證書有效性的檢查之一。必須使用正確的日期和時間配置Microsoft CA和您的所有裝置。Microsoft CA在其Certificate Services中使用了一個外掛(mscep.dll)，以便與Cisco裝置共用證書。

完成以下步驟以配置ASA:

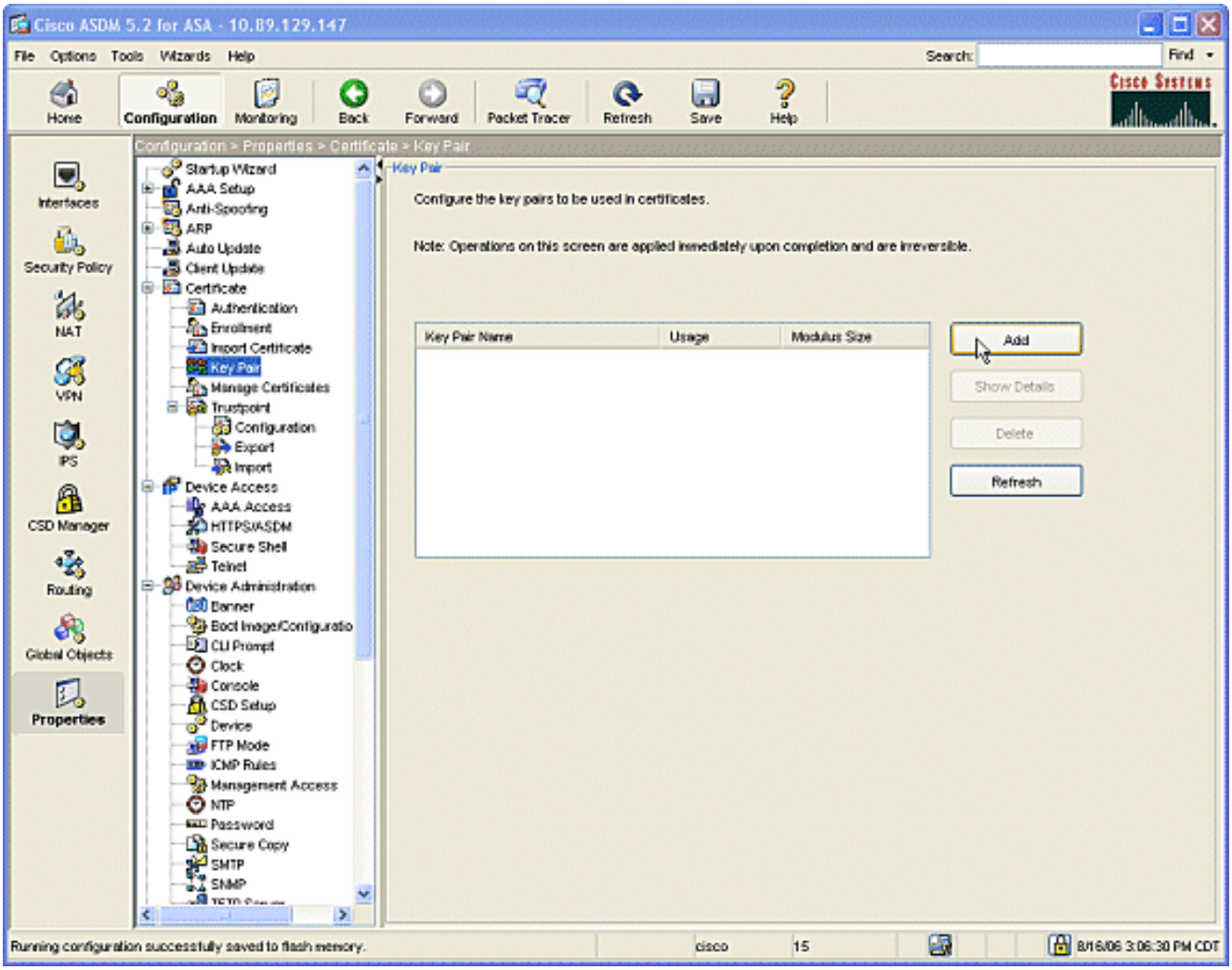
1. 開啟ASDM應用程式，然後按一下**Configuration**按鈕。在左側選單中，按一下**Properties**按鈕。在導航窗格中，按一下**Device Administration > Device**。輸入ASA的主機名和域名。按一下「**Apply**」。出現提示時，按一下**Save > Yes**。



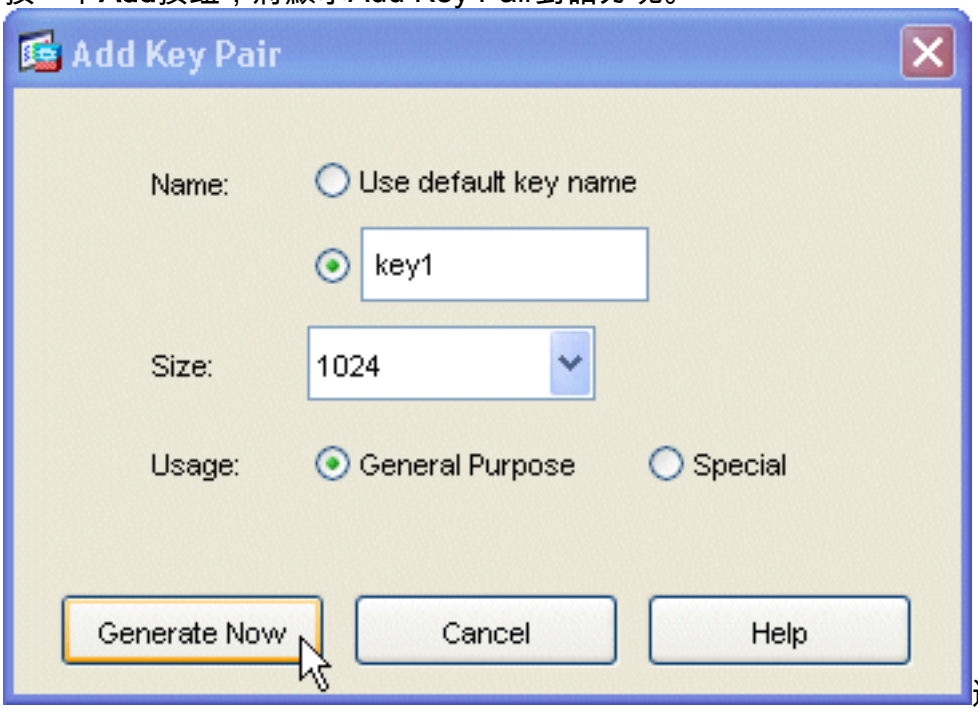
2. 使用正確的日期、時間和時區配置ASA。這對於裝置的證書生成非常重要。如果可能，使用NTP伺服器。在導航窗格中，按一下**裝置管理>時鐘**。在「時鐘」視窗中，使用欄位和下拉箭頭設定正確的日期、時間和時區。



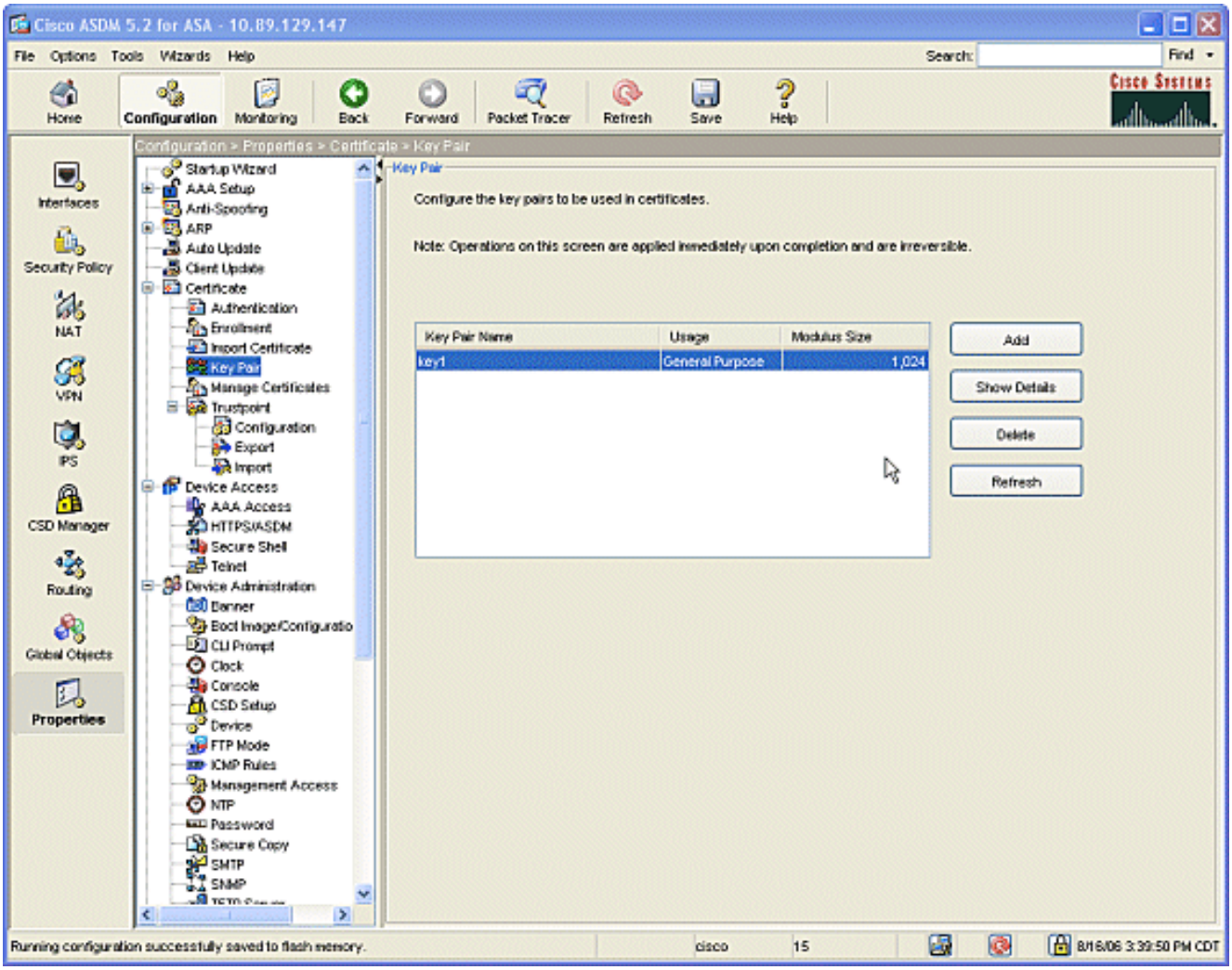
3. ASA必須擁有自己的金鑰對（私鑰和公鑰）。 公鑰將被傳送到Microsoft CA。在導航窗格中，按一下**證書>金鑰對**。



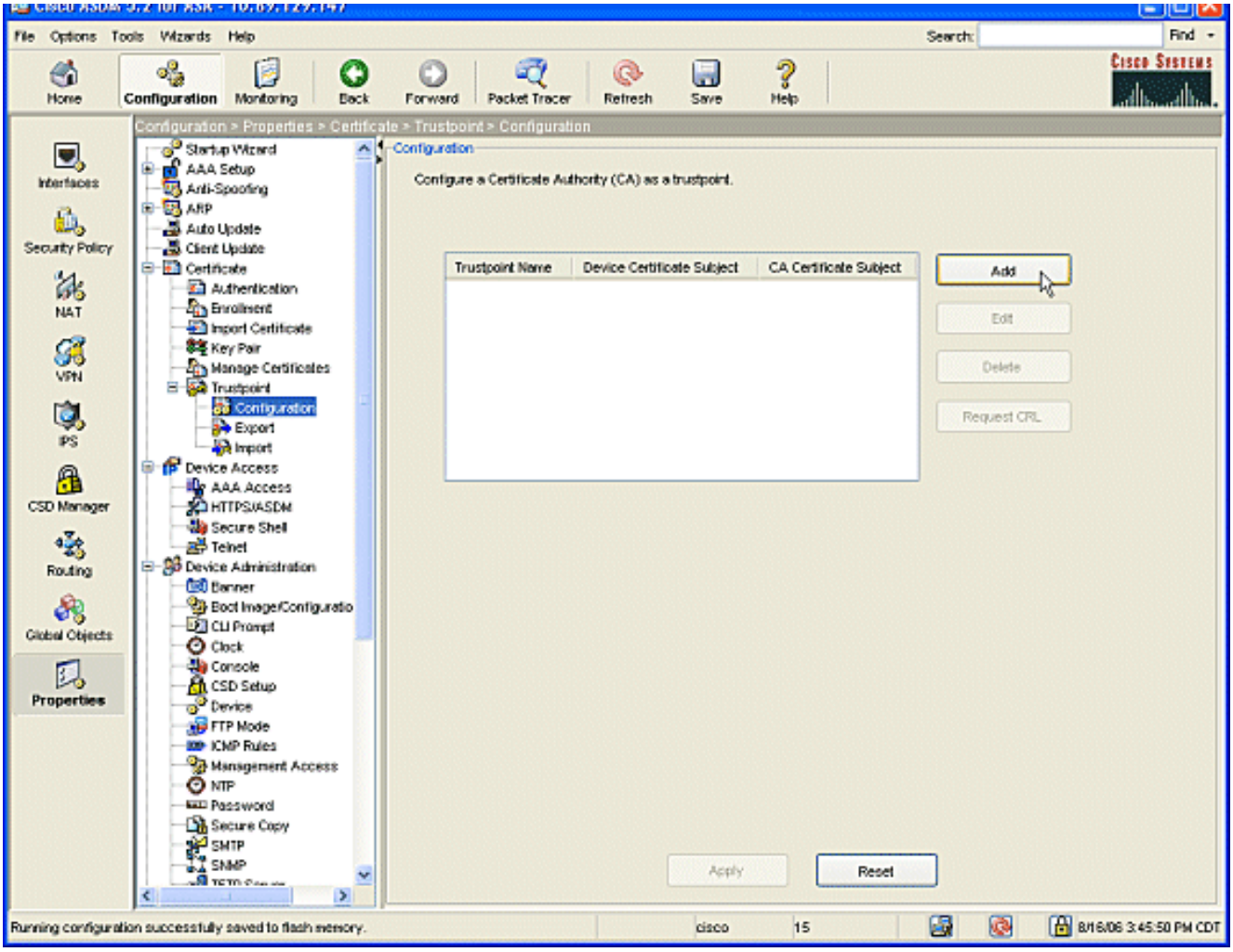
按一下**Add**按鈕，將顯示Add Key Pair對話方塊。



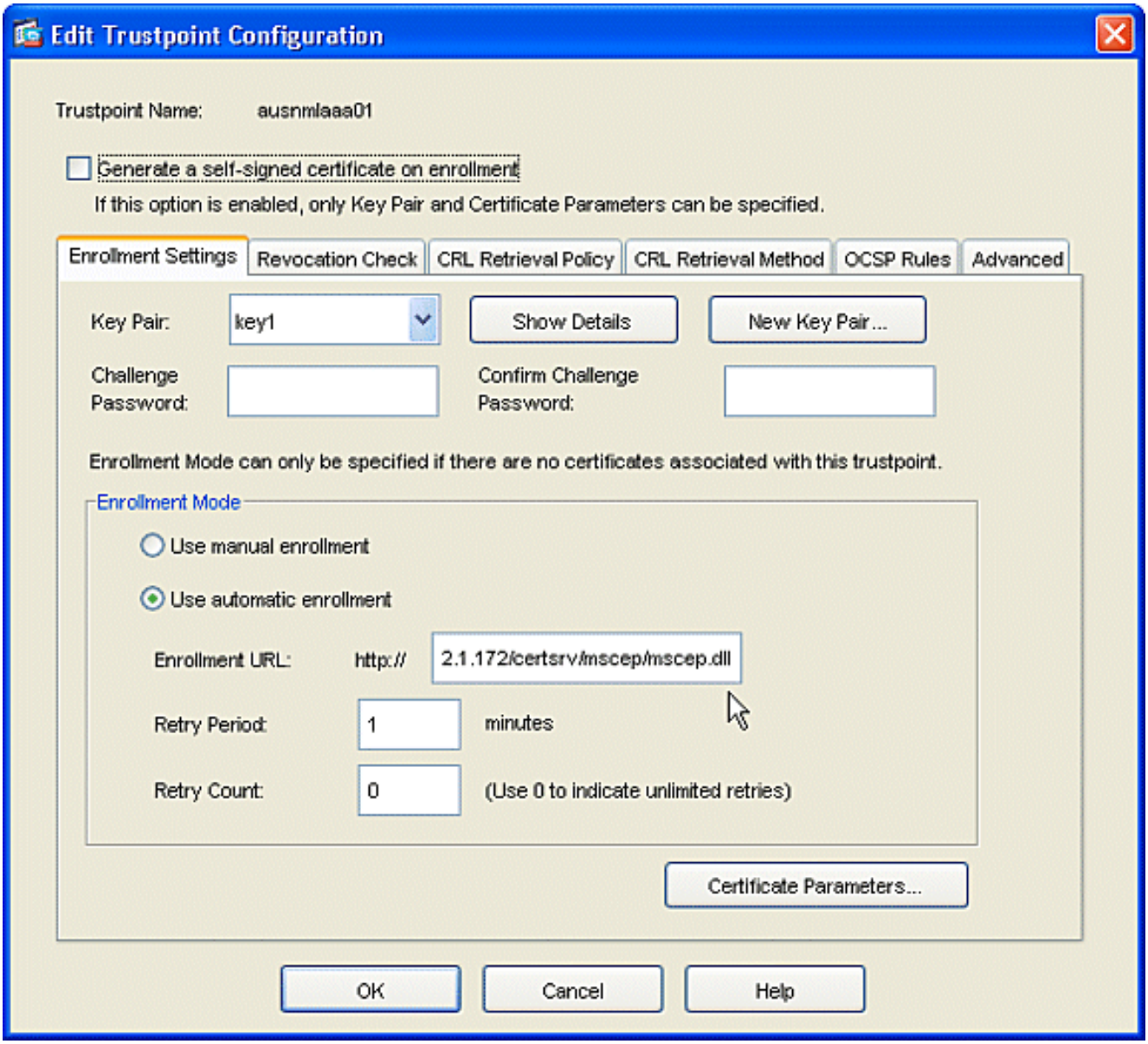
選中**名稱**區域的空白欄位旁的單選按鈕，然後鍵入金鑰的名稱。按一下「**Size:**箭頭鍵選擇鍵的大小，或接受預設值。選中Usage下的**General Purpose**單選按鈕。按一下**Generate Now**按鈕以重新生成金鑰並返回到「金鑰對」視窗，在此視窗中可以檢視金鑰對的資訊。



4. 將Microsoft CA配置為可信。在導航窗格中，按一下**信任點>配置**。在「配置」視窗中，按一下**Add**按鈕。

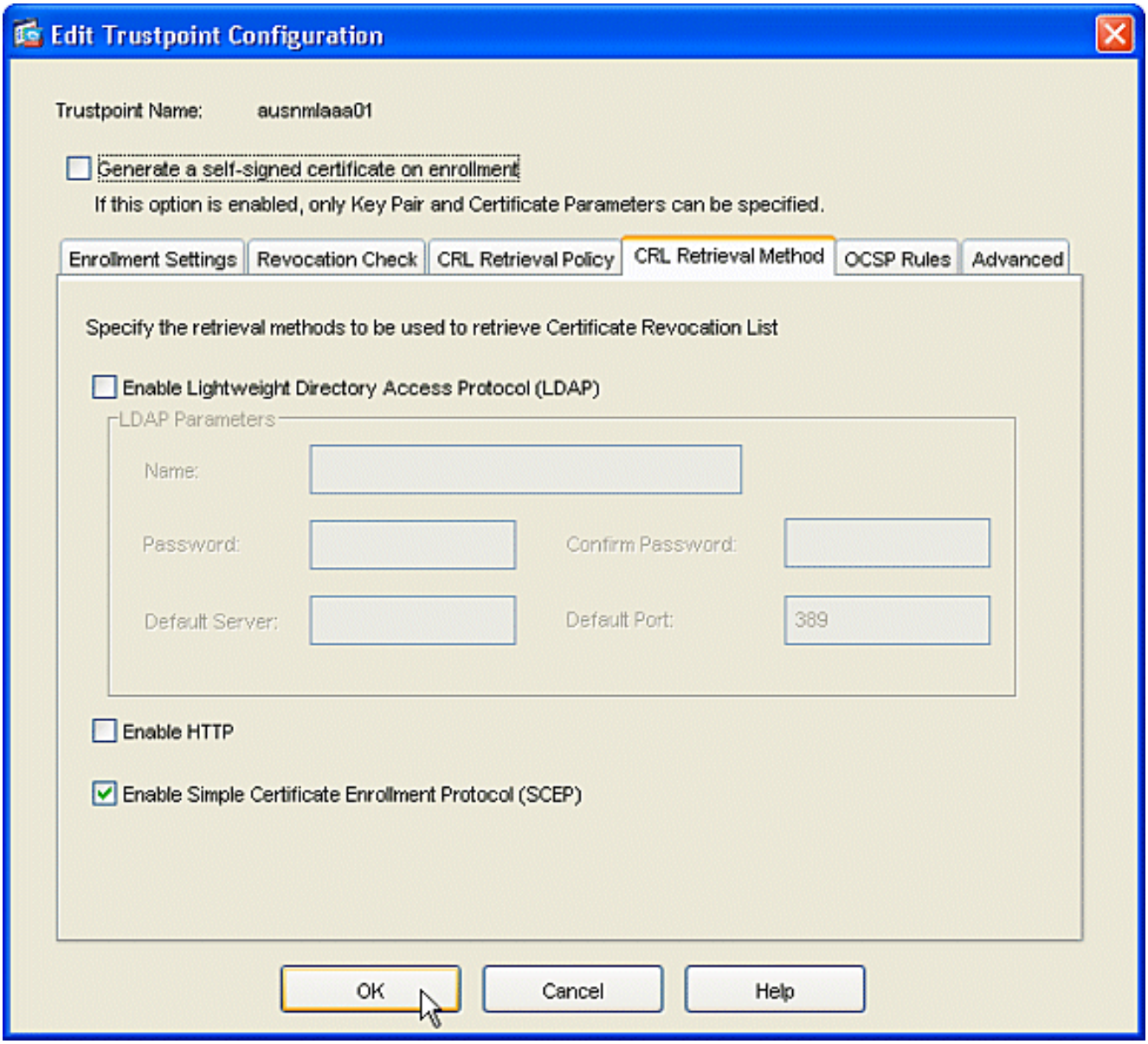


將顯示「編輯信任點配置」視窗。

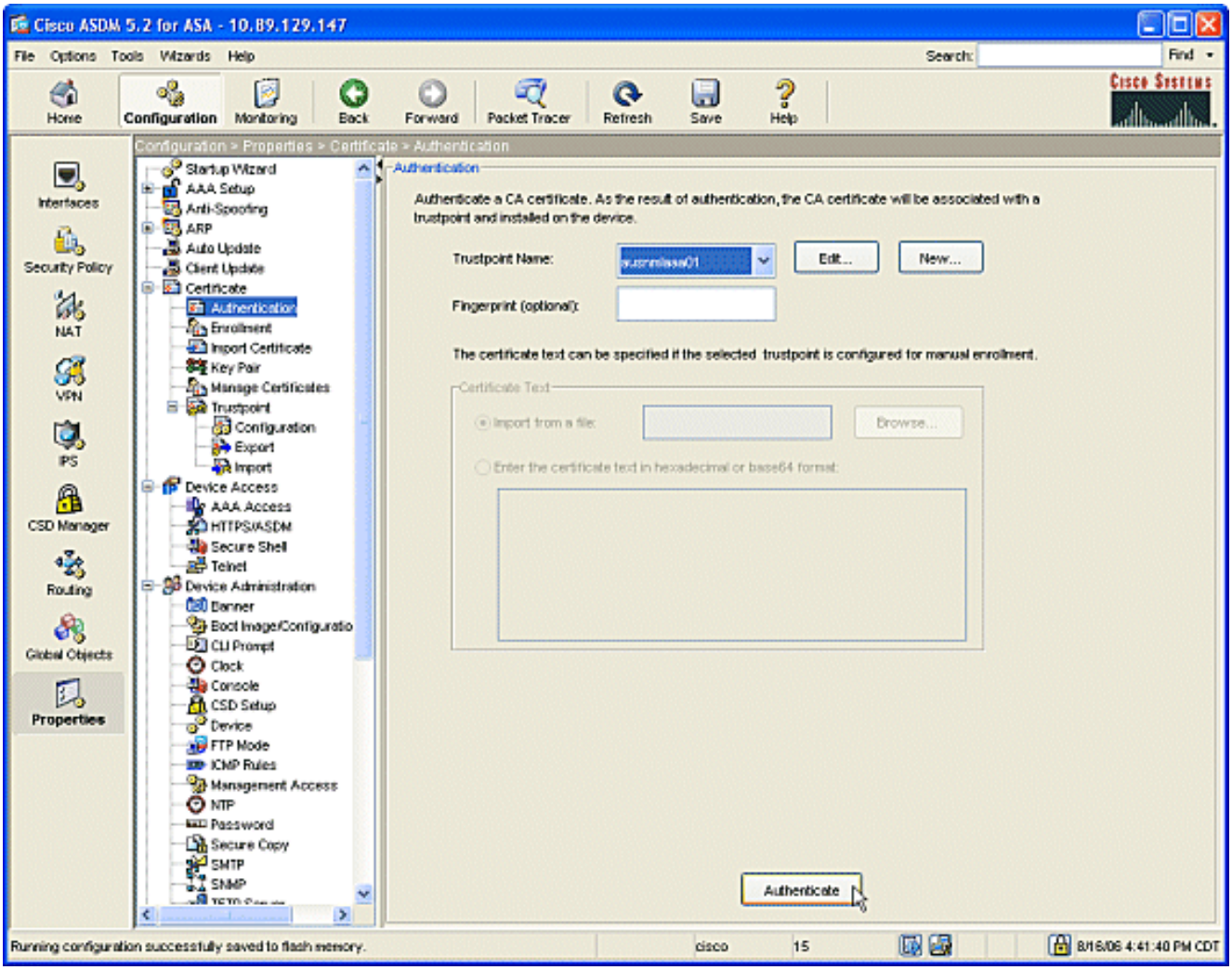


使用CA的名稱填充信任點的名稱。按一下「**Key Pair:**鍵對的名稱。選中**Use automatic enrollment**單選按鈕，並輸入Microsoft CA的URL:**http://CA_IP_Address/certsrv/mscep/mscep.dll**。

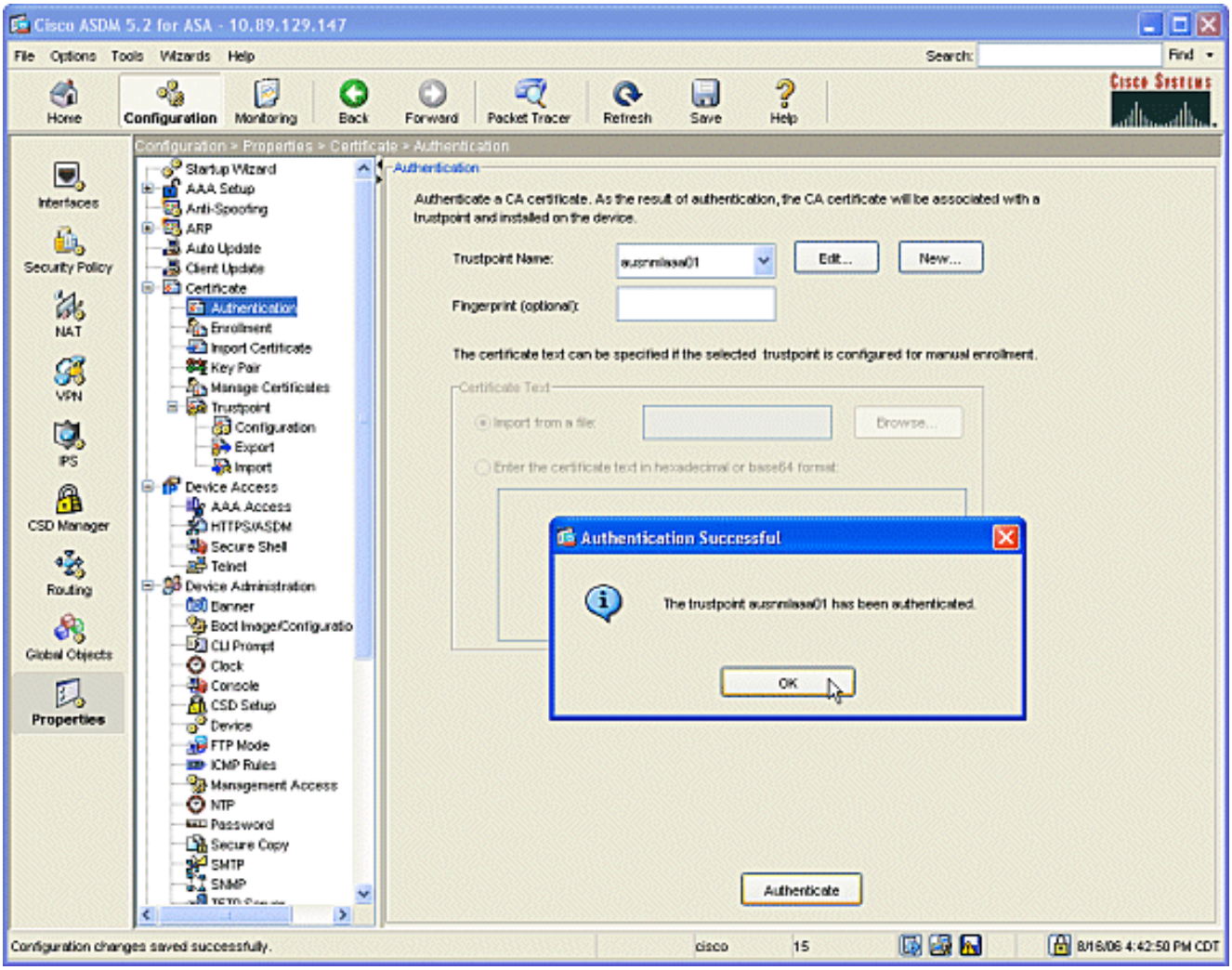
5. 按一下**Crl檢索方法**頁籤。取消選中Enable HTTP和Enable Lightweight Directory Access Protocol(LDAP)覈取方塊。選中Enable Simple Certificate Enrollment Protocol(SCEP)覈取方塊。將所有其他頁籤設定保留為預設設定。按一下**OK**按鈕。



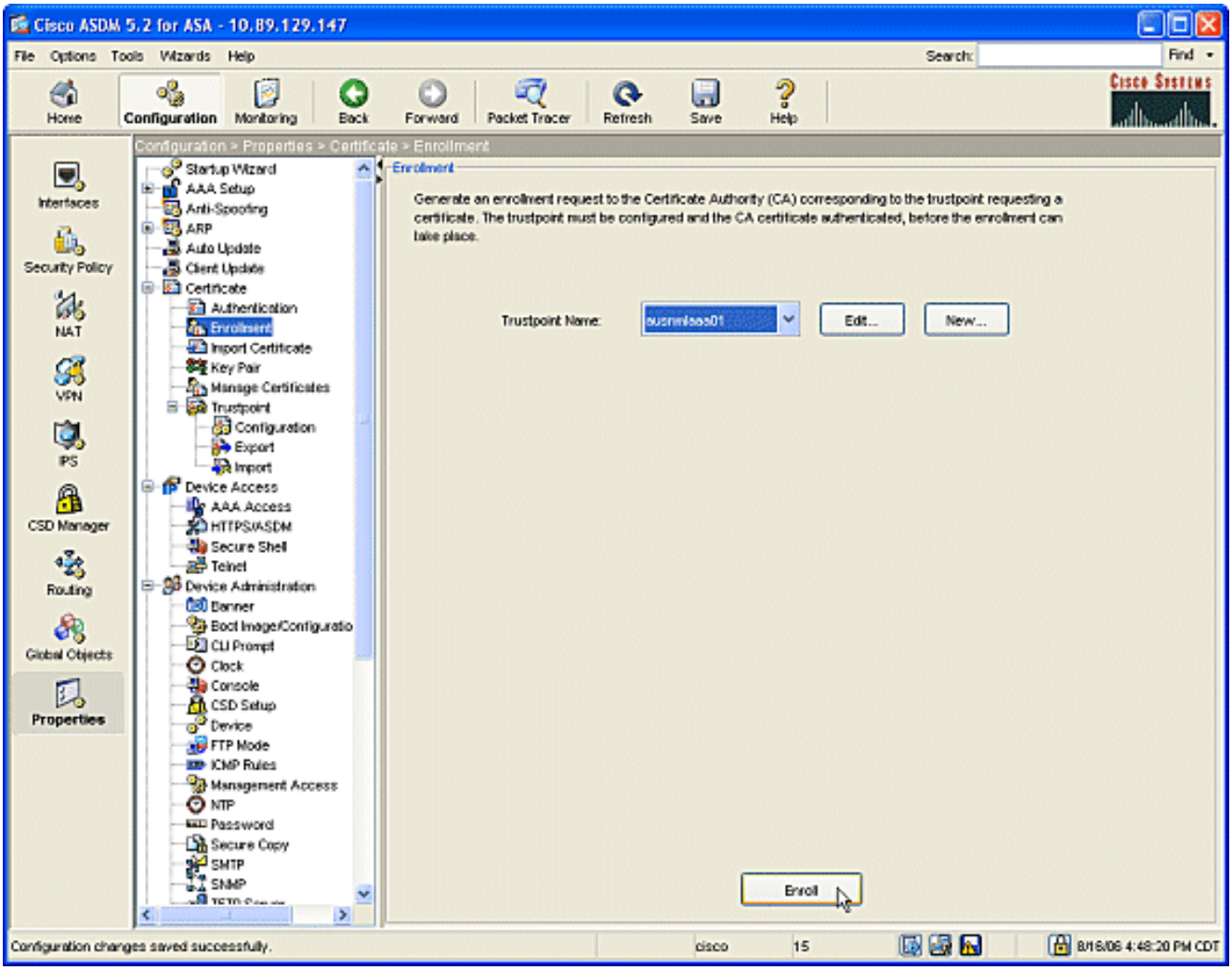
6. 通過Microsoft CA進行身份驗證和註冊。在導航窗格中，按一下**Certificate > Authentication**。確保新建立的信任點顯示在**信任點名稱**：欄位.按一下**Authenticate**按鈕。



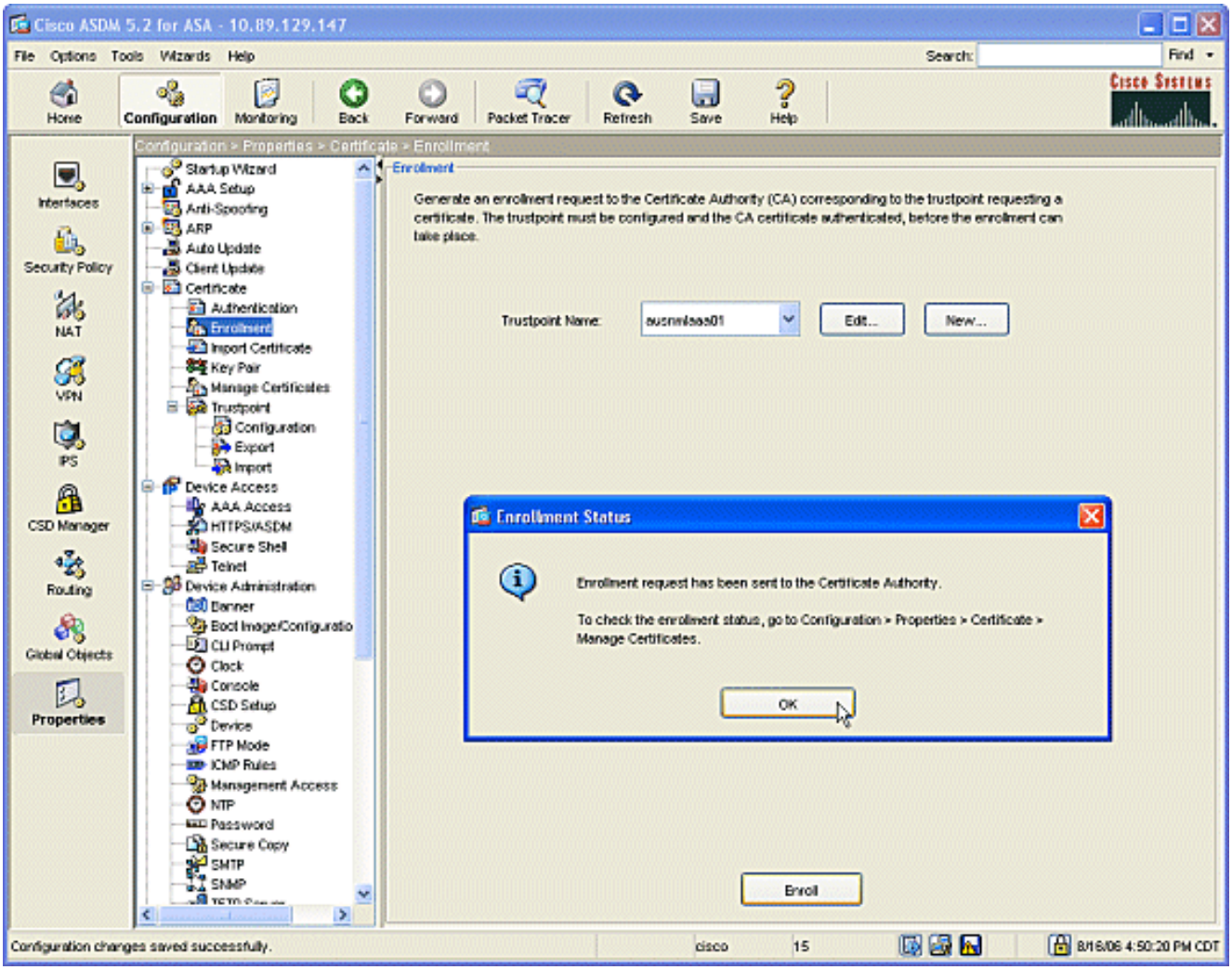
7. 系統將顯示一個對話方塊，通知您信任點已經過身份驗證。按一下**OK**按鈕。



8. 在導航窗格中，按一下**註冊**。確保信任點名稱顯示在Trustpoint Name欄位中，然後按一下**Enroll**按鈕。



9. 系統將顯示一個對話方塊，通知您已將該請求傳送到CA。按一下**OK**按鈕。



附註： 在Microsoft Windows獨立電腦上，您必須為提交到CA的任何請求頒發證書。證書將處於掛起狀態，直到按一下右鍵證書並在Microsoft伺服器上按一下issue。

結果

以下是ASDM步驟產生的CLI配置：

ciscoasa

```
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
```

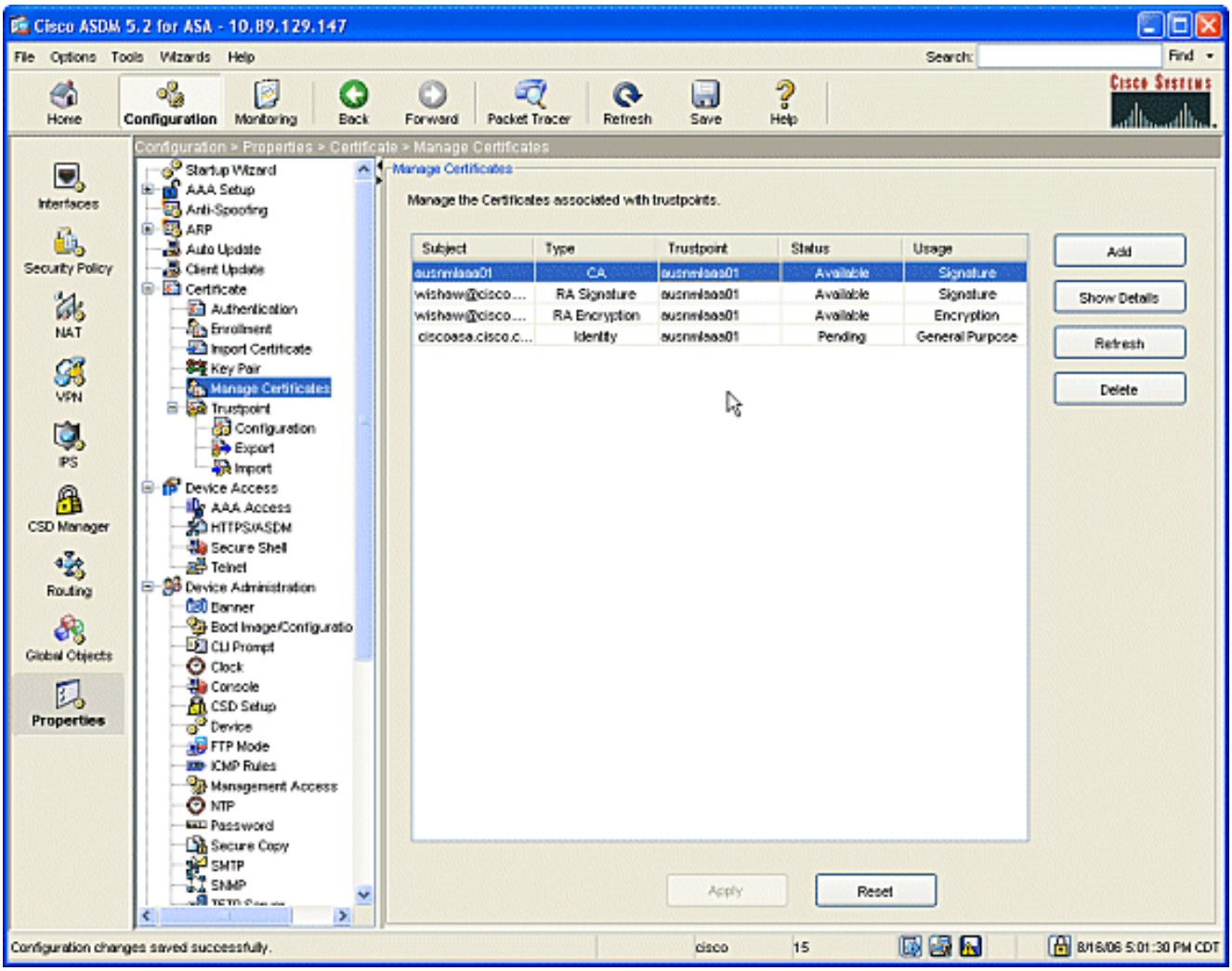
驗證

使用本節內容，確認您的組態是否正常運作。

檢查和管理證書

檢查和管理您的證書。

1. 開啟ASDM應用程式，然後按一下**Configuration**按鈕。
2. 在左側選單中，按一下**Properties**按鈕。按一下「**Certificate**」。按一下「**Manage Certificate**」。



指令

在ASA上，您可以在命令列中使用多個**show**命令來驗證證書的狀態。

- **show crypto ca certificates**命令用於檢視有關您的證書、CA證書和任何註冊機構(RA)證書的資訊。
- **show crypto ca trustpoints**命令用於驗證信任點配置。
- **show crypto key mypubkey rsa**命令用於顯示ASA的RSA公鑰。
- **show crypto ca crls**命令用於顯示所有快取的CRL。

註：Output Interpreter Tool(僅限註冊客戶)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

使用本節內容，對組態進行疑難排解。

有關如何對Microsoft Windows 2003 CA進行故障排除的詳細資訊，請參閱Windows Server 2003的公鑰基礎架構 。

指令

注意：使用**debug**指令可能會對思科裝置造成負面影響。使用**debug**指令之前，請先參閱有關Debug指令的重要資訊。

相關資訊

- **配置Cisco VPN 3000 Concentrator 4.0.x以獲取數位證書**