ASA에서 ASDM을 사용하여 Microsoft Windows CA에서 디지털 인증서를 얻는 방법

목차

소개

디지털 인증서를 사용하여 네트워크의 네트워크 디바이스 및 사용자를 인증할 수 있습니다.네트워크 노드 간 IPSec 세션을 협상하는 데 사용할 수 있습니다.

Cisco 디바이스는 다음 세 가지 주요 방법으로 네트워크에서 안전하게 자신을 식별합니다.

1. **사전 공유 키**.둘 이상의 장치에 동일한 공유 비밀 키가 있을 수 있습니다.피어는 사전 공유 키를 포함하는 키 해시를 컴퓨팅 및 전송하여 서로를 인증합니다.수신 피어가 사전 공유 키를 사용하여 동일한 해시를 독립적으로 만들 수 있는 경우 두 피어가 동일한 암호를 공유해야 하므로 다른 피어를 인증해야 합니다.이 방법은 수동적이며 확장성이 없습니다.
2. **자체 서명 인증서**.디바이스는 자체 인증서를 생성하고 유효한 것으로 서명합니다.이 유형의 인증서는 사용이 제한적이어야 합니다.컨피그레이션을 위해 SSH 및 HTTPS 액세스와 함께 이 인증서를 사용하는 것이 좋습니다.연결을 완료하려면 별도의 사용자 이름/암호 쌍이 필요합니다.**참고:** Persistent Self-Signed 인증서는 디바이스의 NVRAM(Nonvolatile Random-Access Memory)에 저장되므로 라우터가 다시 로드되는 경우에도 유지됩니다.자세한 내용은 영구 자체 서명 인증서를 참조하십시오.대표적인 사용 사례는 SSL VPN(WebVPN) 연결입니다.
3. **인증 기관 인증서**.서드파티는 통신을 시도하는 두 개 이상의 노드를 검증하고 인증합니다.각 노드에는 공개 키와 개인 키가 있습니다.공개 키는 데이터를 암호화하고 개인 키는 데이터를

해독합니다.동일한 출처에서 인증서를 취득했기 때문에 해당 ID를 확인할 수 있습니다.ASA 디바이스는 수동 등록 방법 또는 자동 등록 방법을 사용하여 서드파티로부터 디지털 인증서를 가져올 수 있습니다.**참고:** 선택한 디지털 인증서의 등록 방법 및 유형은 각 서드파티 제품의 기능 및 기능에 따라 달라집니다.자세한 내용은 인증서 서비스 공급업체에 문의하십시오.

Cisco ASA(Adaptive Security Appliance)는 사전 공유 키 또는 서드파티 CA(Certificate Authority)가 제공하는 디지털 인증서를 사용하여 IPSec 연결을 인증할 수 있습니다.또한 ASA는 자체 서명 디지털 인증서를 생성할 수 있습니다.이 옵션은 디바이스에 대한 SSH, HTTPS 및 Cisco ASDM(Adaptive Security Device Manager) 연결에 사용해야 합니다.

이 문서에서는 ASA용 Microsoft CA(Certificate Authority)에서 디지털 인증서를 자동으로 가져오는 데 필요한 절차를 설명합니다.수동 등록 방법은 포함되지 않습니다.이 문서에서는 컨피그레이션 단계에 ASDM을 사용하고 최종 CLI(Command Line Interface) 컨피그레이션을 제공합니다.

Cisco IOS® 플랫폼과 동일한 시나리오에 대한 자세한 내용은 Cisco IOS Certificate Enrollment Using Enhanced Enrollment Commands Configuration Example을 참조하십시오.

Cisco VPN 3000 Series Concentrator와 동일한 시나리오에 대해 자세히 알아보려면 Cisco VPN 3000 Concentrator 4.7.x 구성을 참조하여 디지털 인증서 및 SSL 인증서를 얻기를 참조하십시오.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

ASA 장치의 요구 사항

- Microsoft® Windows 2003 서버를 CA로 구성합니다.Microsoft 설명서 또는 Windows Server 2003용 공개 키 인프라 참조
- ASDM(Adaptive Security Device Manager)에서 Cisco ASA 또는 PIX 버전 7.x를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.
- 인증서 서비스용 추가 기능(mscep.dll)을 설치합니다.
- SCEP(Simple Certificate Enrollment Protocol) Add-on for Certificate Services 또는 Windows Server 2003 Resource Kit Tools에서 mscep.dll 파일에서 추가 기능에 대한 실행 파일(cepsetup.exe)을 가져옵니다 .**참고:** Microsoft Windows 시스템에서 올바른 날짜, 시간 및 시간대를 구성합니다.NTP(Network Time Protocol)를 사용하는 것은 권장되지만 필요하지는 않습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 5500 Series Adaptive Security Appliance, 소프트웨어 버전 7.x 이상
- Cisco Adaptive Security Device Manager 버전 5.x 이상
- Microsoft Windows 2003 Server 인증 기관

관련 제품

이 컨피그레이션은 Cisco PIX 500 Series Security Appliance 버전 7.x에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

Microsoft CA를 사용하여 인증서를 교환하도록 ASA 구성

작업

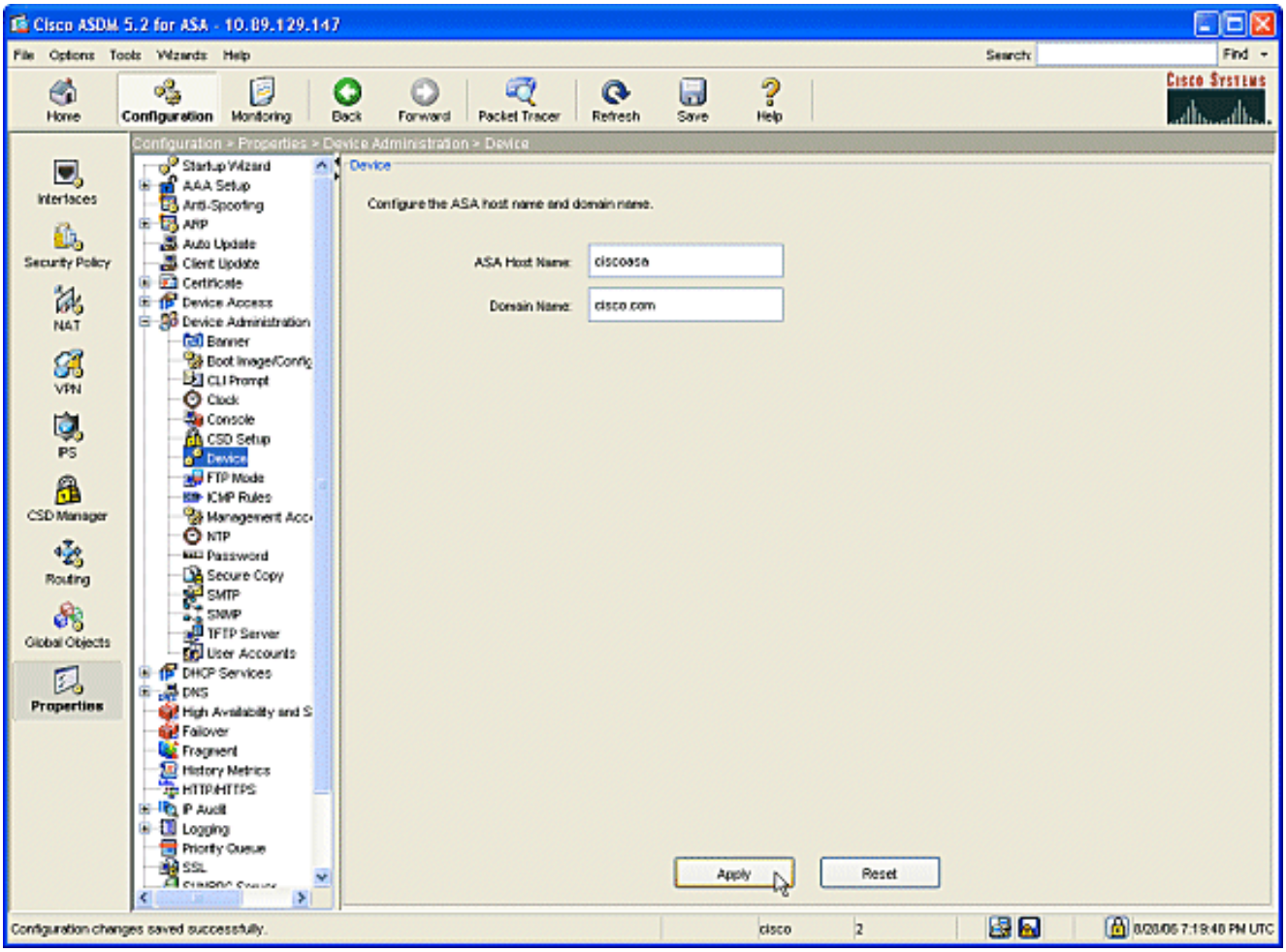
이 섹션에서는 Microsoft Certificate Authority에서 인증서를 받도록 ASA를 구성하는 방법을 보여줍니다.

ASA 구성 지침

디지털 인증서는 날짜/시간/표준 시간대 구성 요소를 인증서 유효성 검사 중 하나로 사용합니다 .Microsoft CA와 모든 장치를 올바른 날짜와 시간으로 구성해야 합니다.Microsoft CA는 Cisco 장치와 인증서를 공유하기 위해 인증서 서비스에 추가 기능(mscep.dll)을 사용합니다.

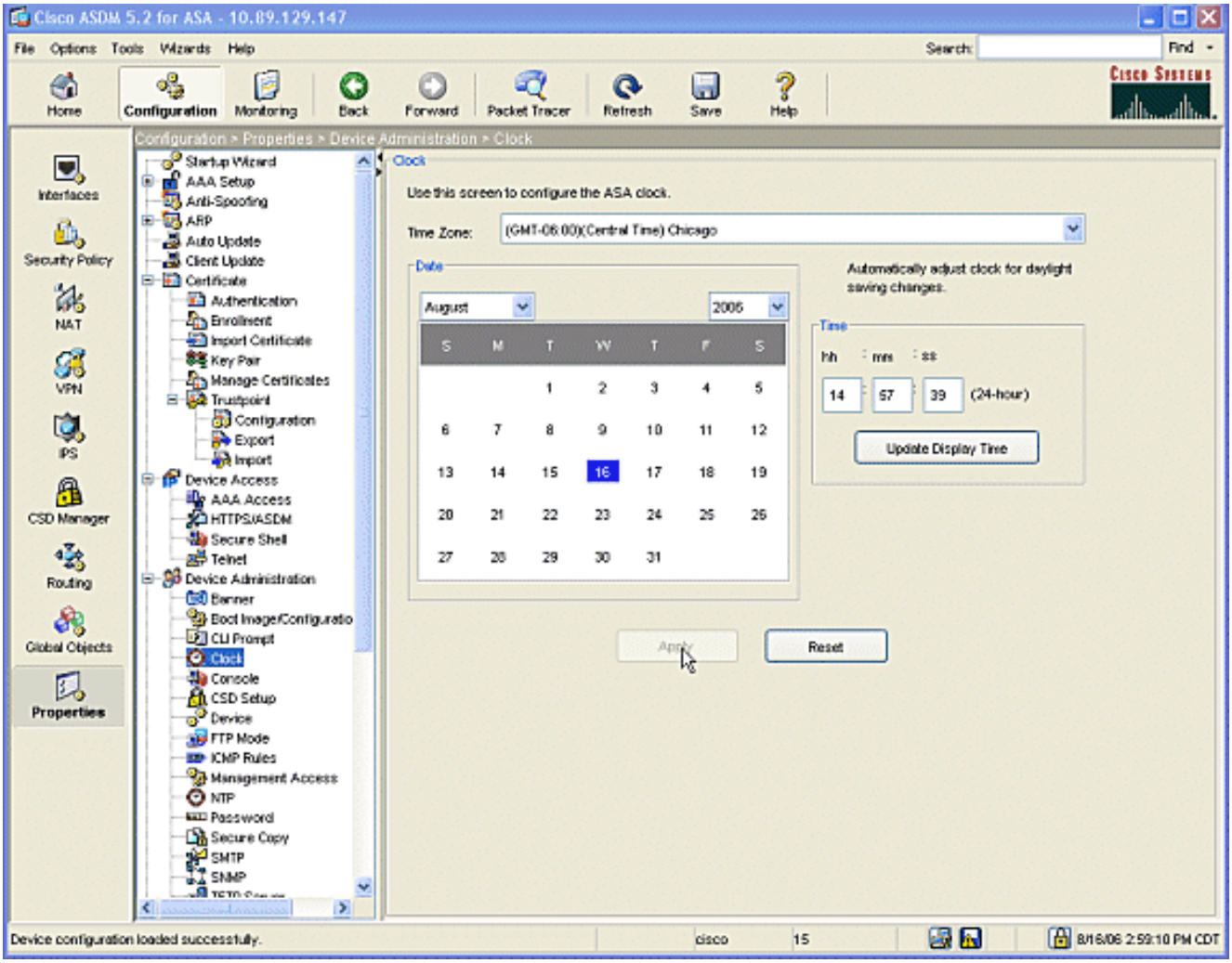
ASA를 구성하려면 다음 단계를 완료합니다.

1. ASDM 애플리케이션을 열고 Configuration(컨피그레이션) 버튼을 클릭합니다.왼쪽 메뉴에서 **속성** 단추를 클릭합니다.탐색 창에서 Device **Administration(디바이스 관리) > Device(디바이스)를 클릭합니다**.ASA의 호스트 이름 및 도메인 이름을 입력합니다.Apply를 **클릭합니다**.메시지가 표시되면 Save(저장) **> Yes(예)를** 클릭합니다
   .



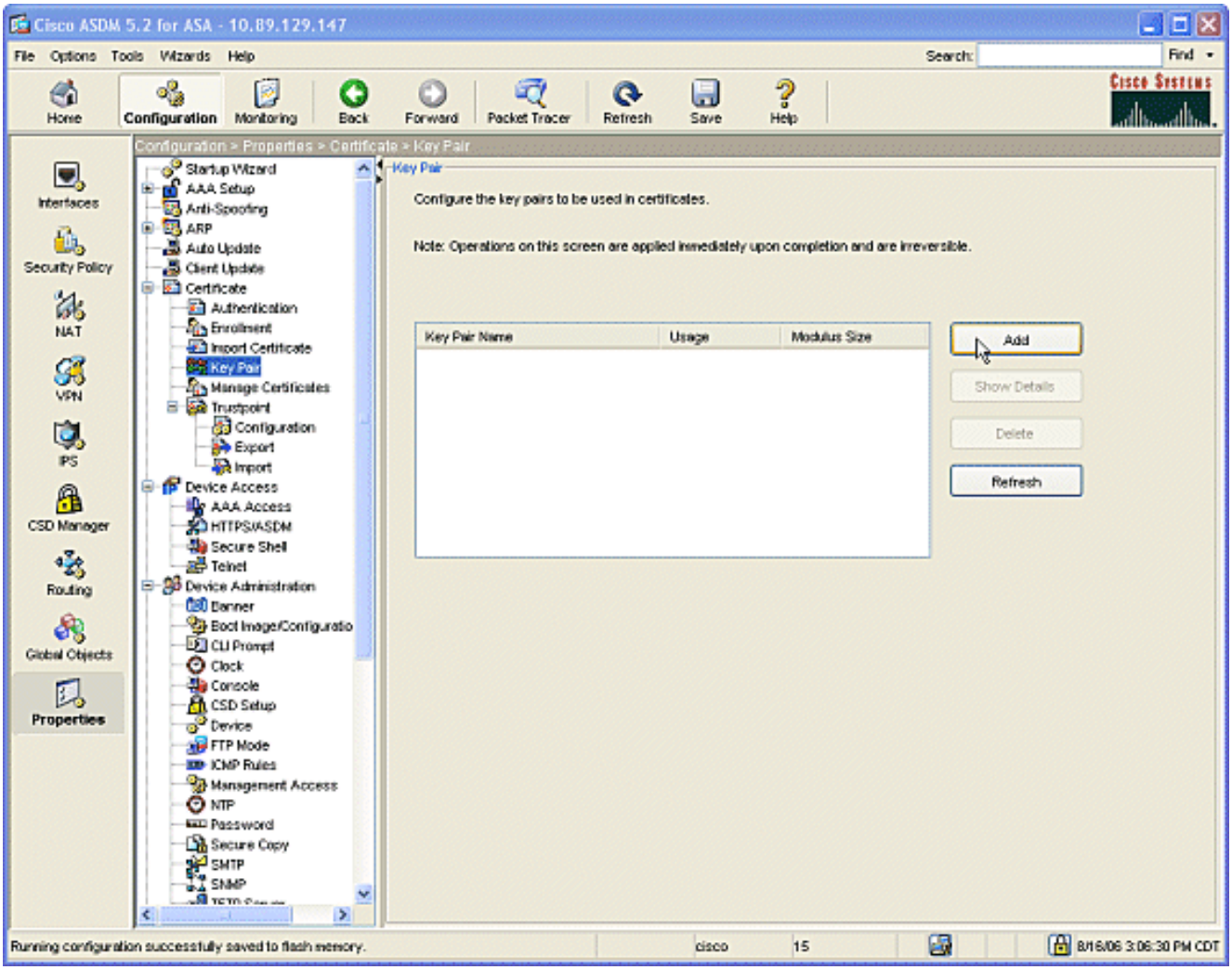
2. 올바른 날짜, 시간 및 시간대로 ASA를 구성합니다.이는 디바이스의 인증서 생성에 중요합니다.가능한 경우 NTP 서버를 사용합니다.탐색 창에서 Device **Administration(디바이스 관리) > Clock(시계)을 클릭합니다**.시계 창에서 필드와 드롭다운 화살표를 사용하여 올바른 날짜, 시간 및 시간대를 설정합니다

.

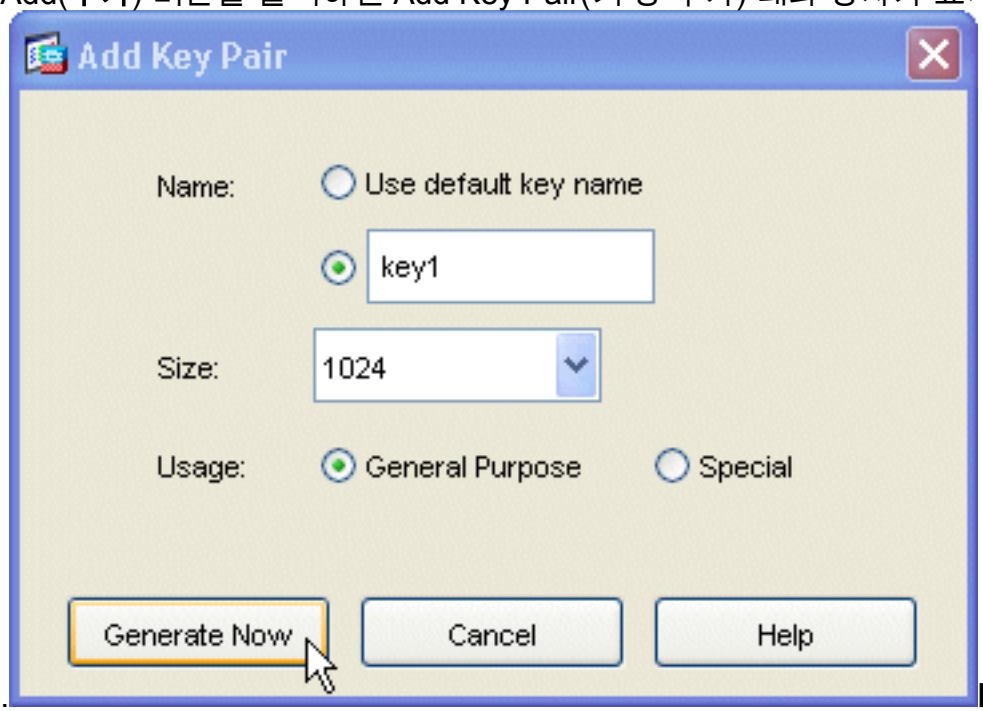


3. ASA에는 고유한 키 쌍(개인 및 공개 키)이 있어야 합니다. 공개 키가 Microsoft CA로 전송됩니다.탐색 창에서 Certificate(인증서) **> Key Pair(키 쌍)를** 클릭합니다

.

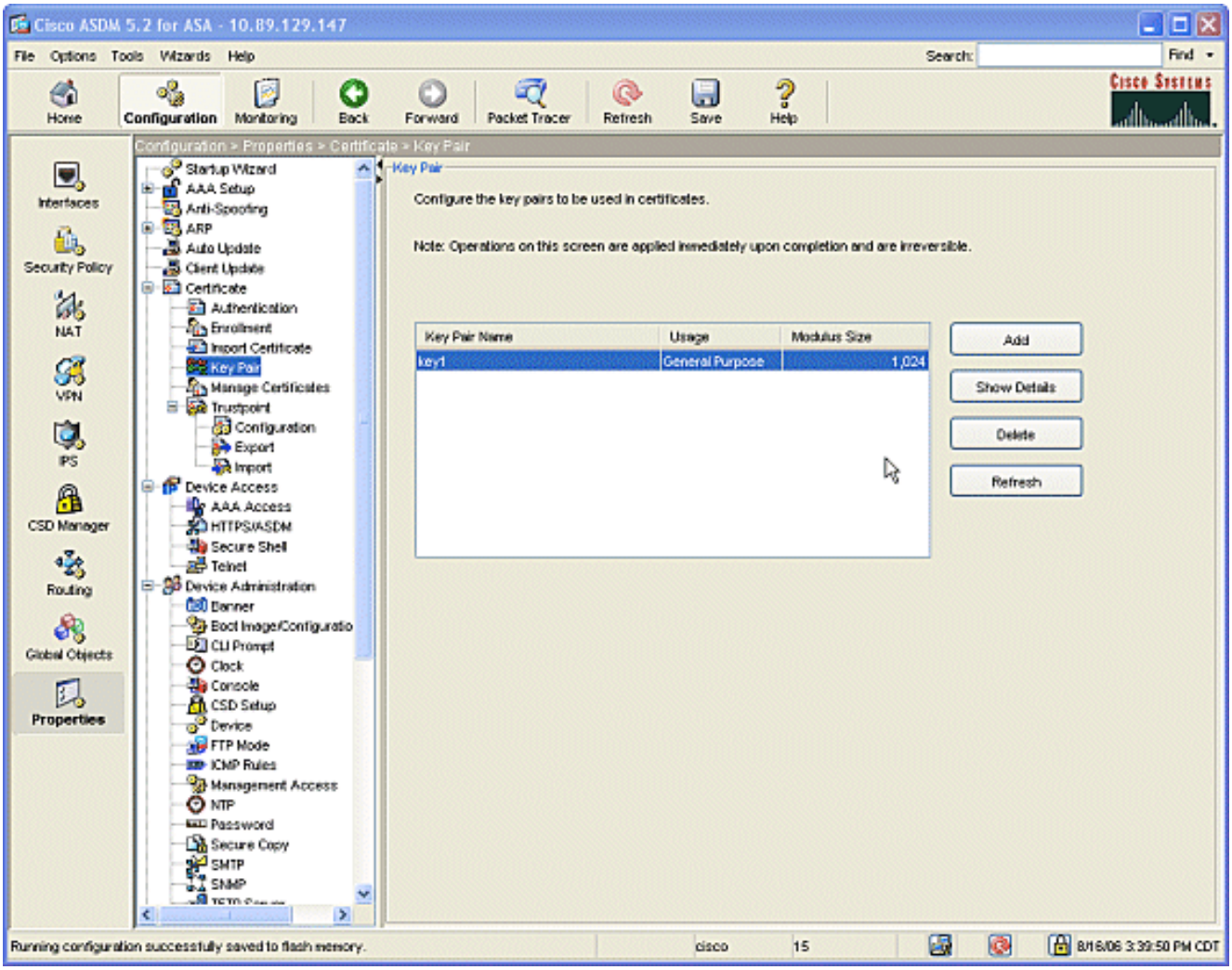


Add(**추가**) 버튼을 클릭하면 Add Key Pair(키 쌍 추가) 대화 상자가 표시됩니다

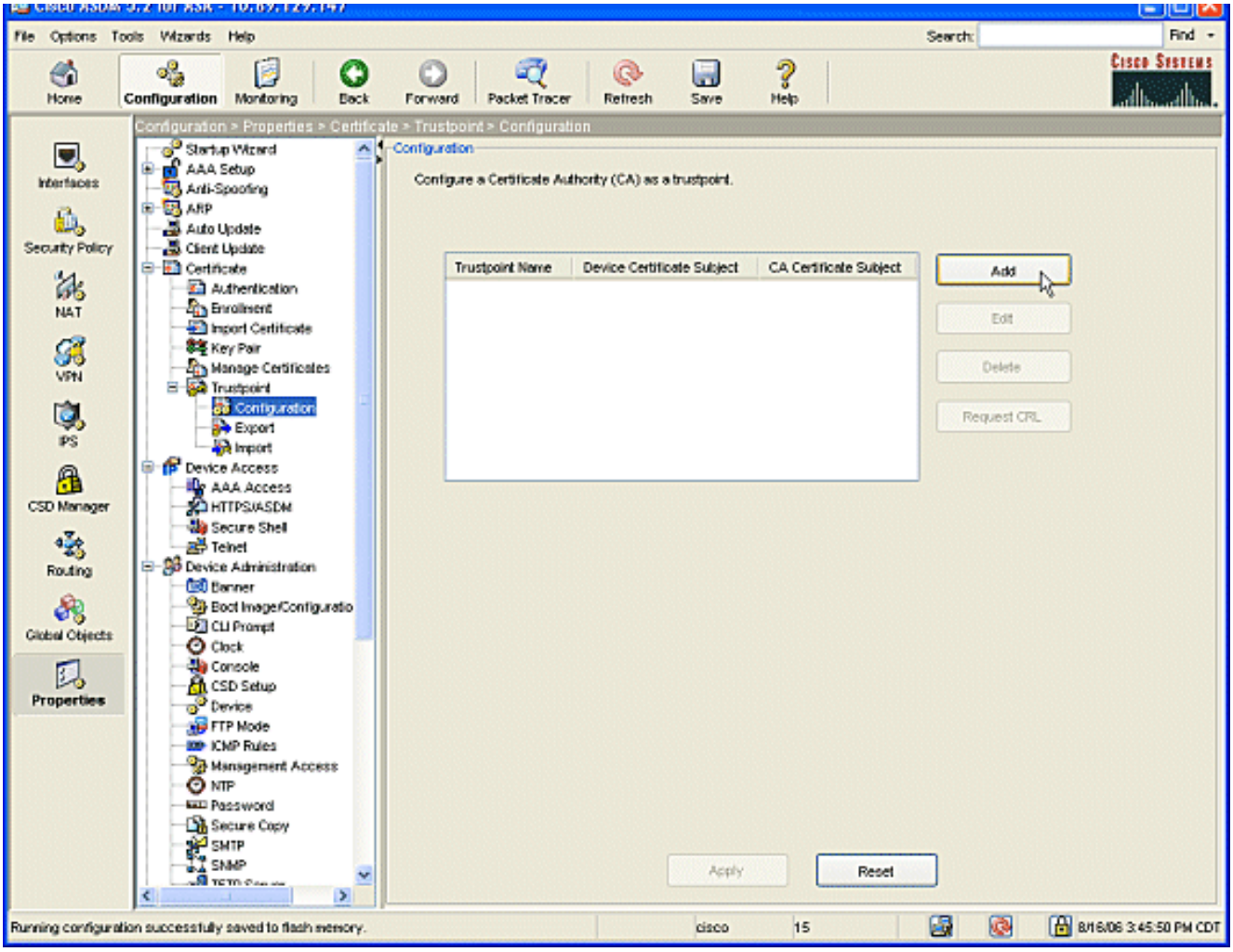


. **Name** 영역의 빈 필드 옆에 있는 라디오 버튼을 선택하고 키 이름을 입력합니다.**크기**를 클릭합니다.드롭다운 상자 옆의 화살표를 클릭하여 키의 크기를 선택하거나 기본값을 적용합니다.Usage(사용)에서 **General Purpose(범용)** 라디오 버튼을 선택합니다.Generate Now(**지금 생성**) 버튼을 클릭하여 키를 재생성하고 키 쌍의 정보를 볼 수 있는 Key Pair(키 쌍) 창으로 돌아갑니다

.

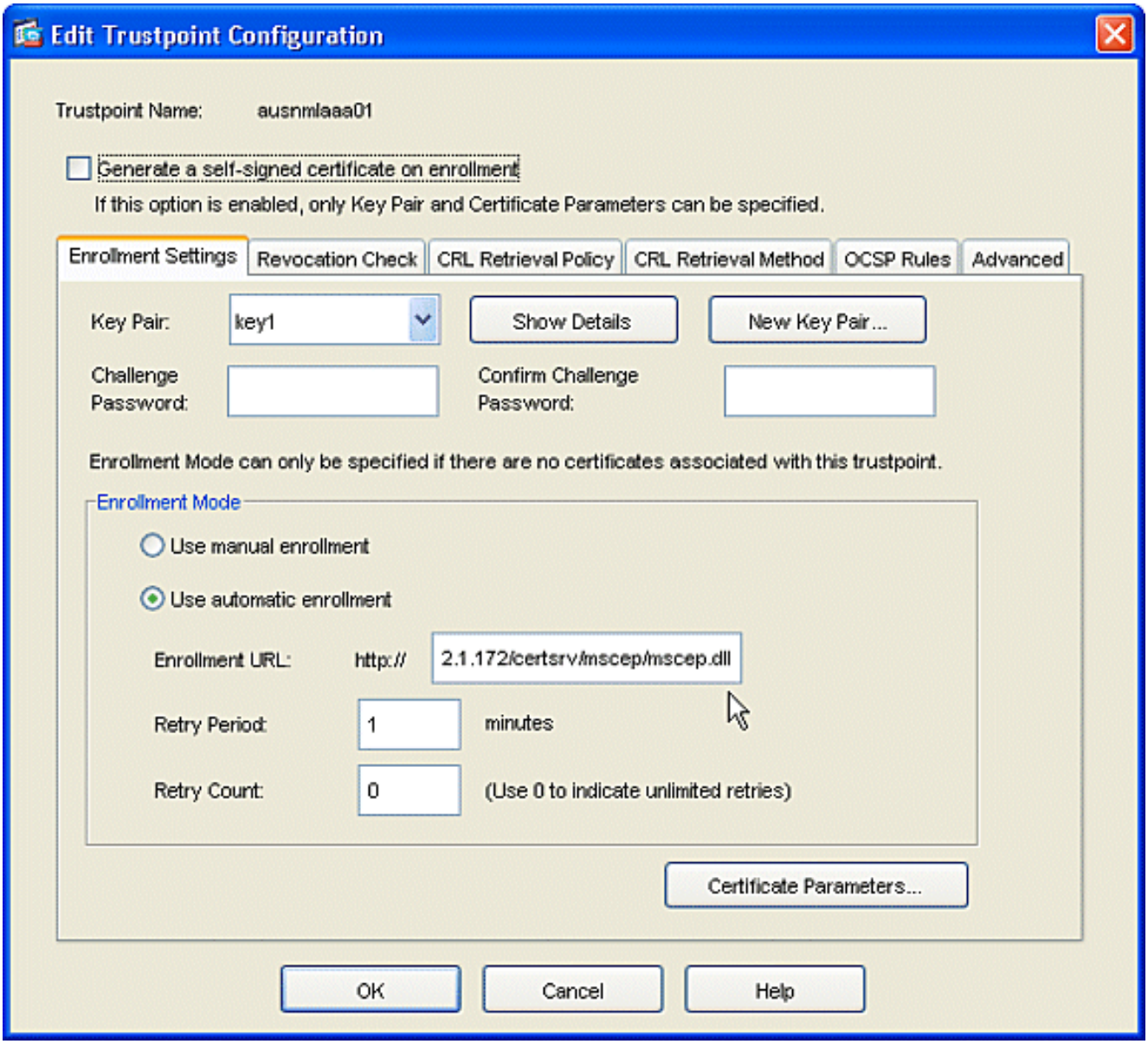


4. Microsoft CA를 신뢰할 수 있도록 구성합니다.탐색 창에서 Trustpoint(신뢰 지점) **> Configuration(컨피그레이션)을 클릭합니다**.구성 창에서 **추가** 버튼을 클릭합니다
.



신뢰 지점 구성 편집 창이 표시됩니다

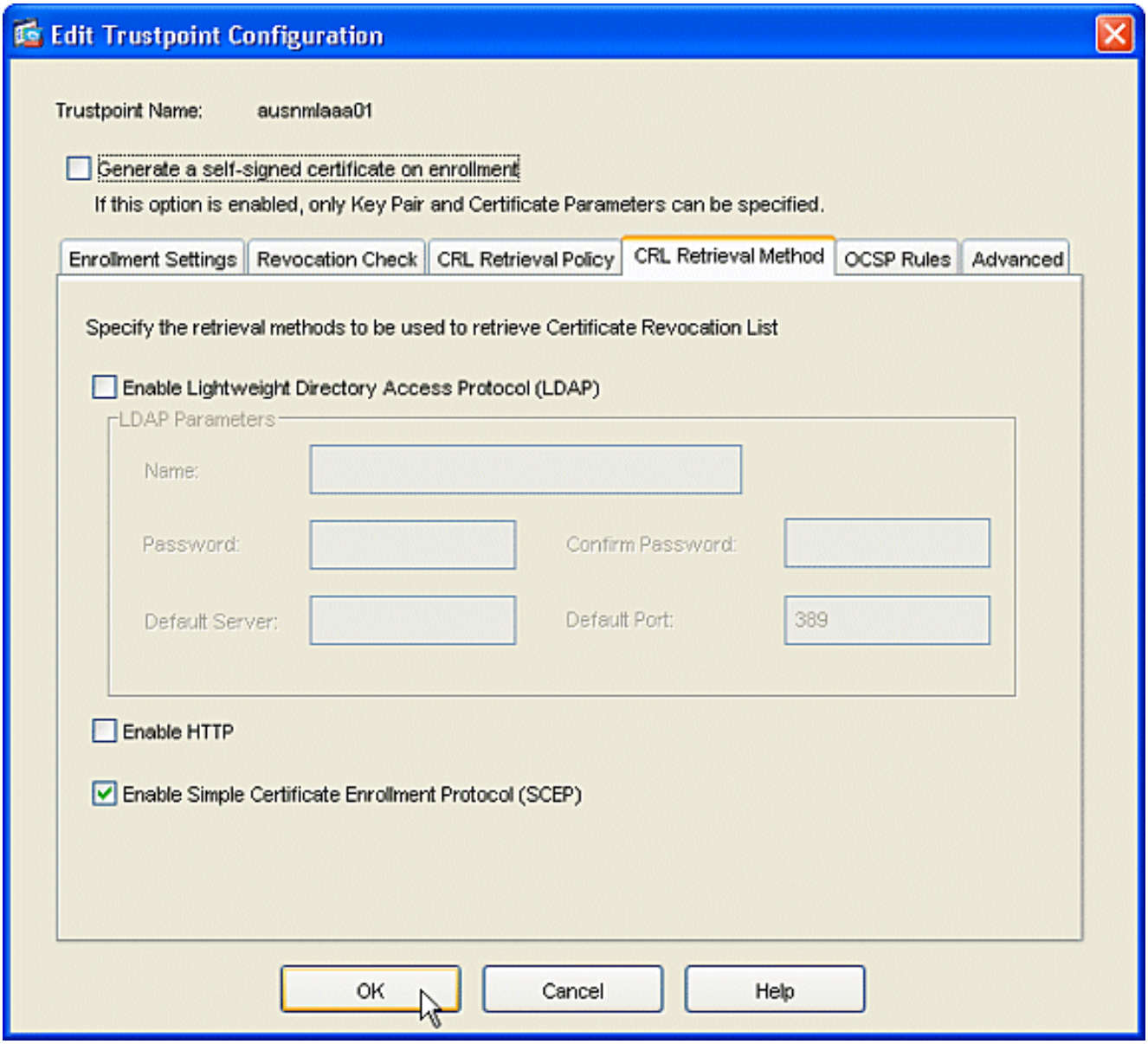
.



신뢰 지점의 이름을 CA의 이름으로 채웁니다.**키 쌍**을 클릭합니다.드롭다운 상자 옆의 화살표를 클릭하고 생성한 키 쌍의 이름을 선택합니다.Use automatic enrollment(**자동 등록 사용**) 라디오 버튼을 선택하고 Microsoft CA의 URL을 입력합니다 .http://CA_IP_Address/certsrv/mscep/mscep.dll

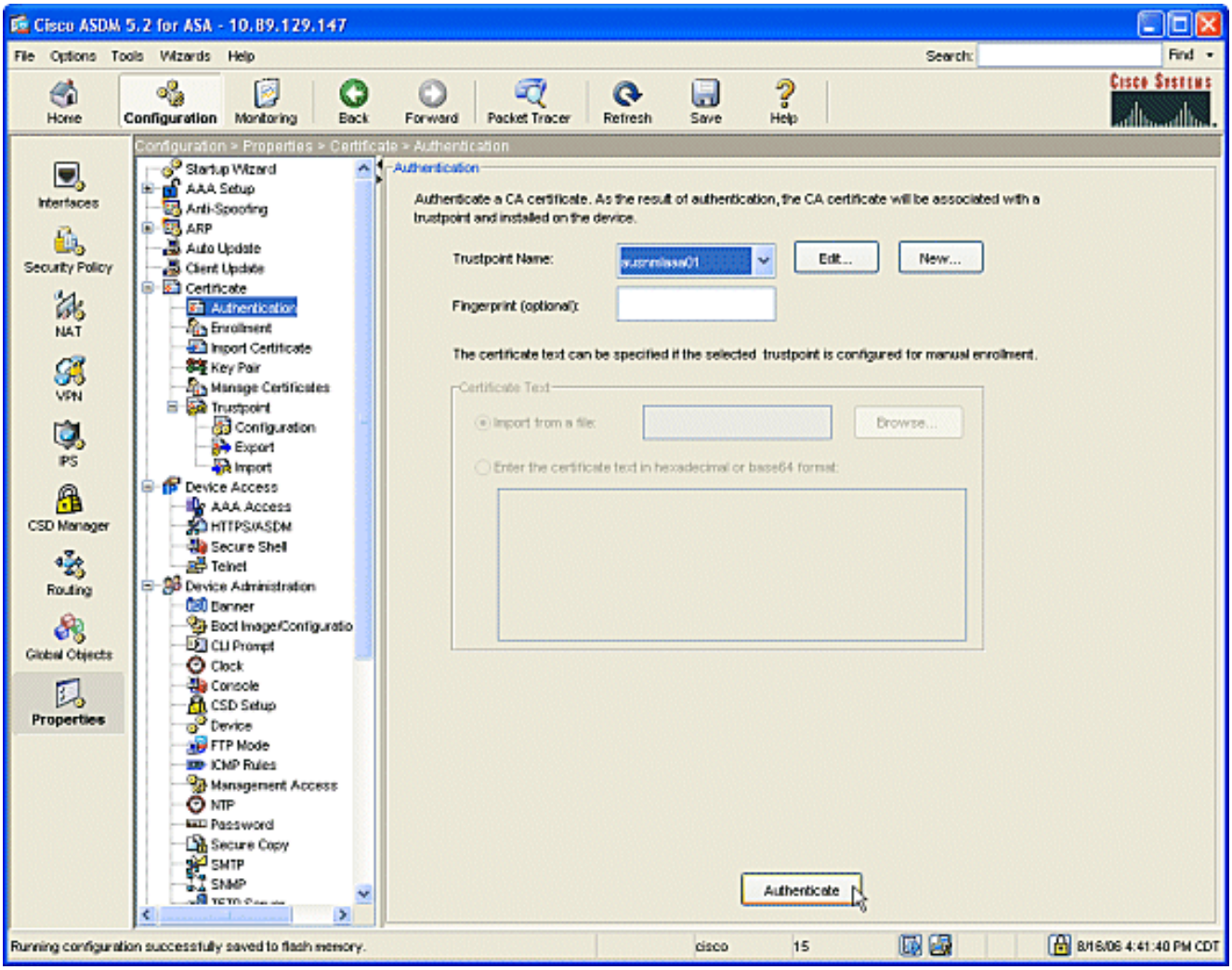
5. Crl Retrieval **Method** 탭**을** 클릭합니다.Enable HTTP and Enable Lightweight Directory Access Protocol (LDAP) 확인란을 선택 취소합니다.Enable Simple Certificate Enrollment Protocol (SCEP) 확인란을 선택합니다.다른 모든 탭 설정을 기본 설정으로 유지합니다.**확인** 버튼을 클릭합니다

.

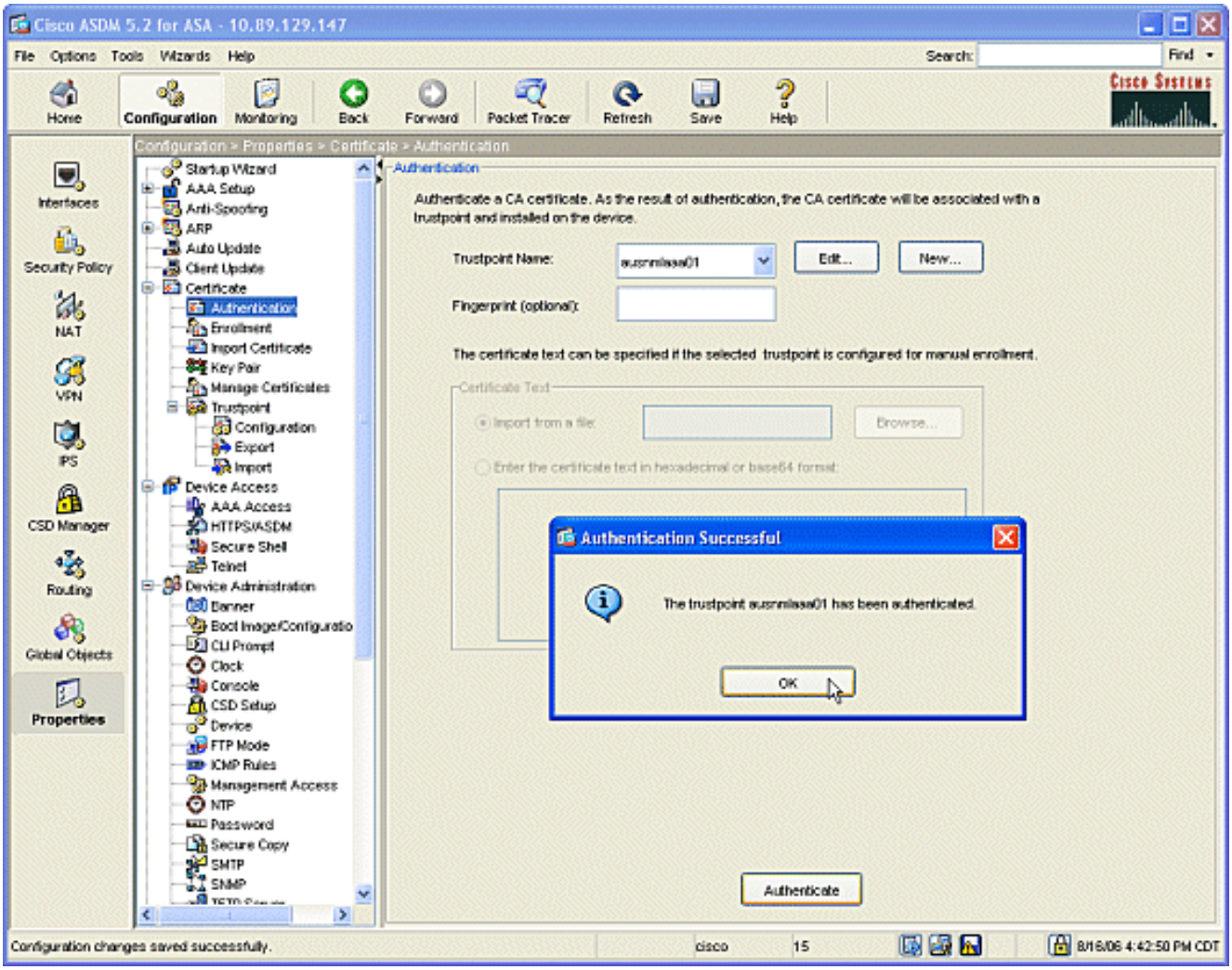


6. Microsoft CA를 인증하고 등록합니다.탐색 창에서 Certificate(인증서) **> Authentication(인증)을** 클릭합니다.새로 생성된 신뢰 지점이 신뢰 지점 이름에 표시되는지 **확인합니다.**필드 .Authenticate(인증) 버튼**을** 클릭합니다

.

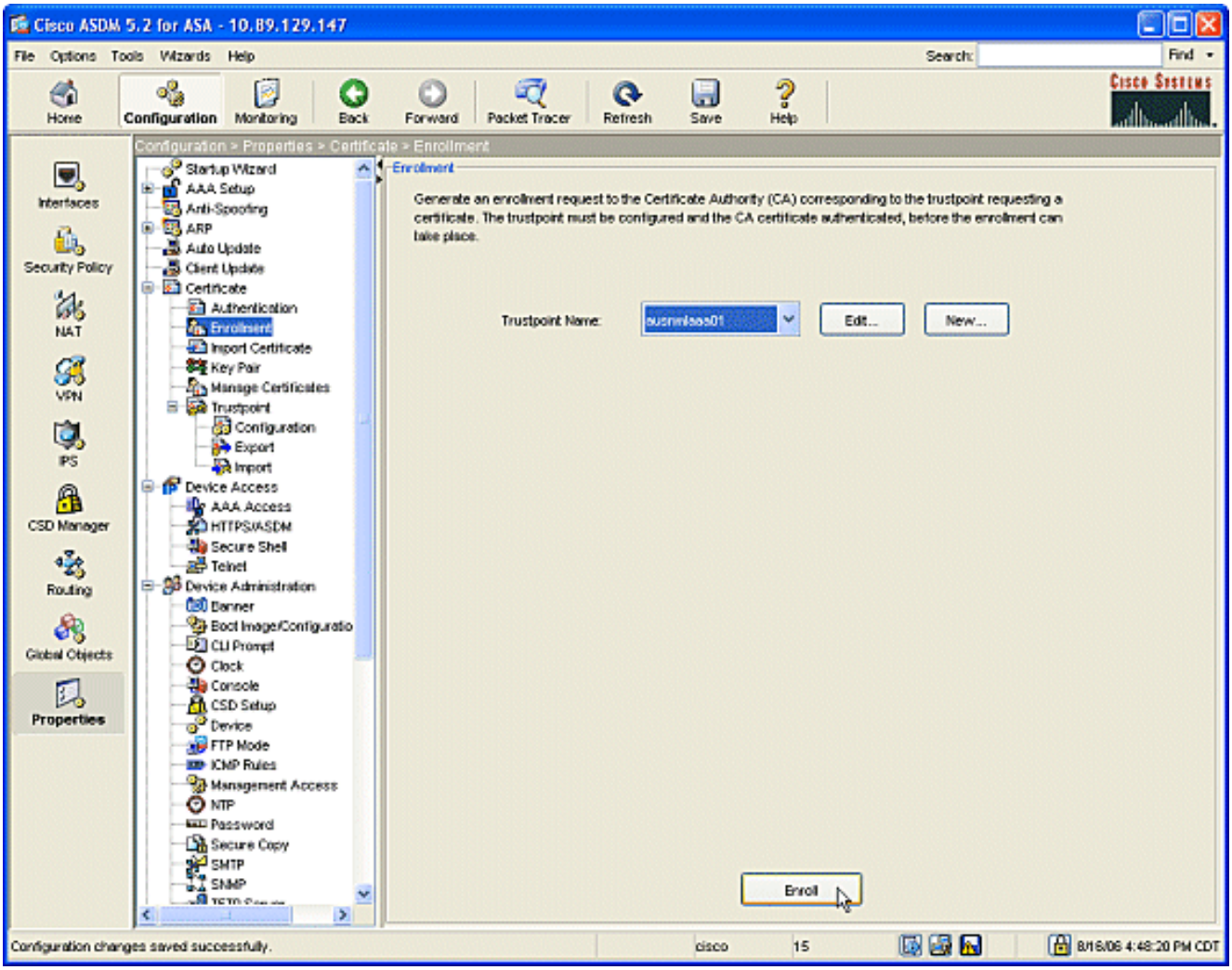


7. 신뢰 지점이 인증되었음을 알리는 대화 상자가 표시됩니다.**확인** 버튼을 클릭합니다
.

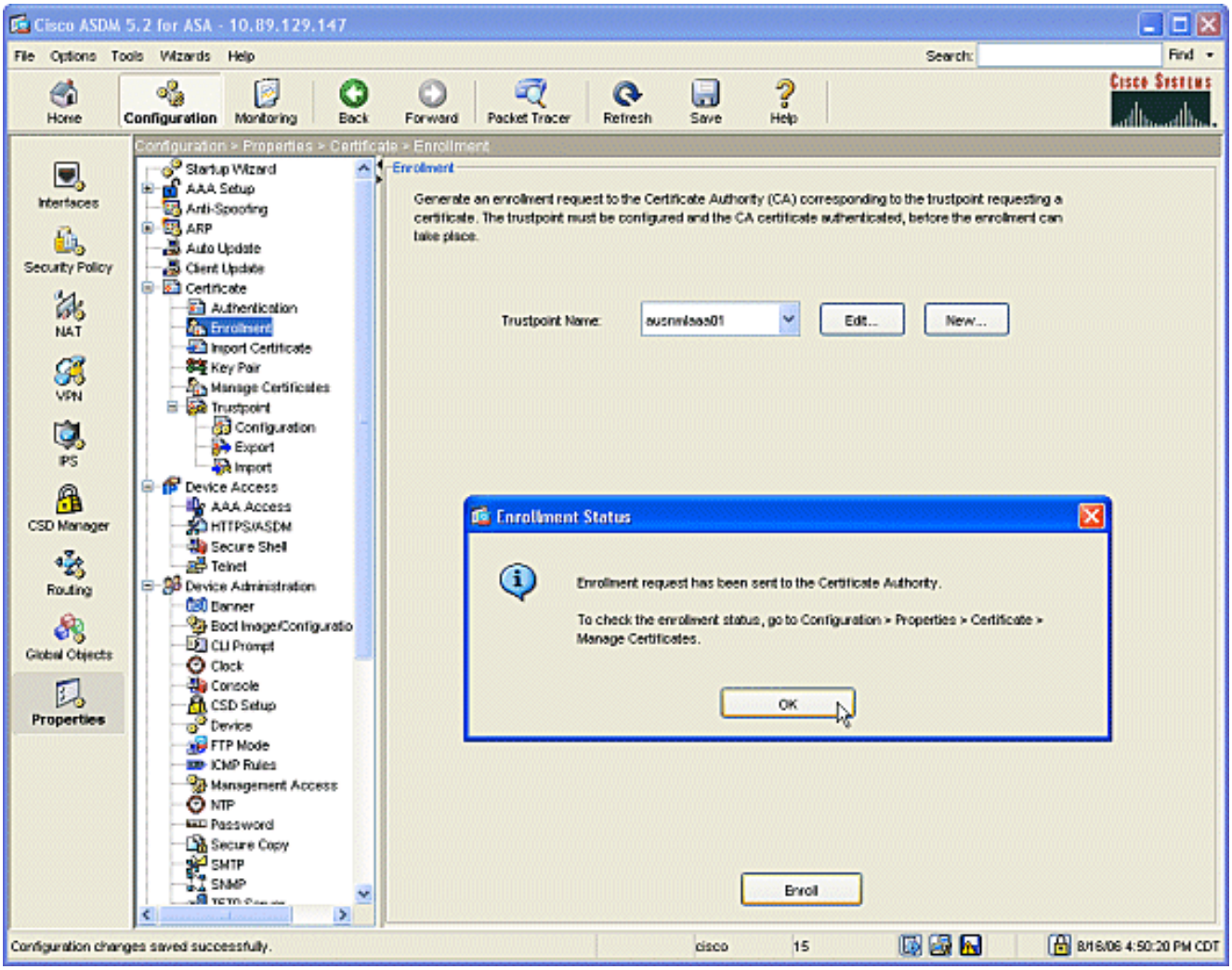


8. 탐색 창에서 Enrollment(등록)를 **클릭합니다**.신뢰 지점 이름이 Trustpoint Name(신뢰 지점 이름) 필드에 표시되는지 확인하고 Enroll(등록) 버튼을 클릭합니다

.



9. 요청이 CA로 전송되었음을 알리는 대화 상자가 표시됩니다.**확인** 버튼을 클릭합니다
.



참고: Microsoft Windows 독립 실행형 컴퓨터에서 CA에 제출된 모든 요청에 대해 인증서를 발급해야 합니다.인증서를 마우스 오른쪽 단추로 클릭하고 Microsoft Server에서 문제를 클릭할 때까지 인증서는 보류 상태입니다.

결과

다음은 ASDM 단계에서 발생하는 CLI 컨피그레이션입니다.

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
```

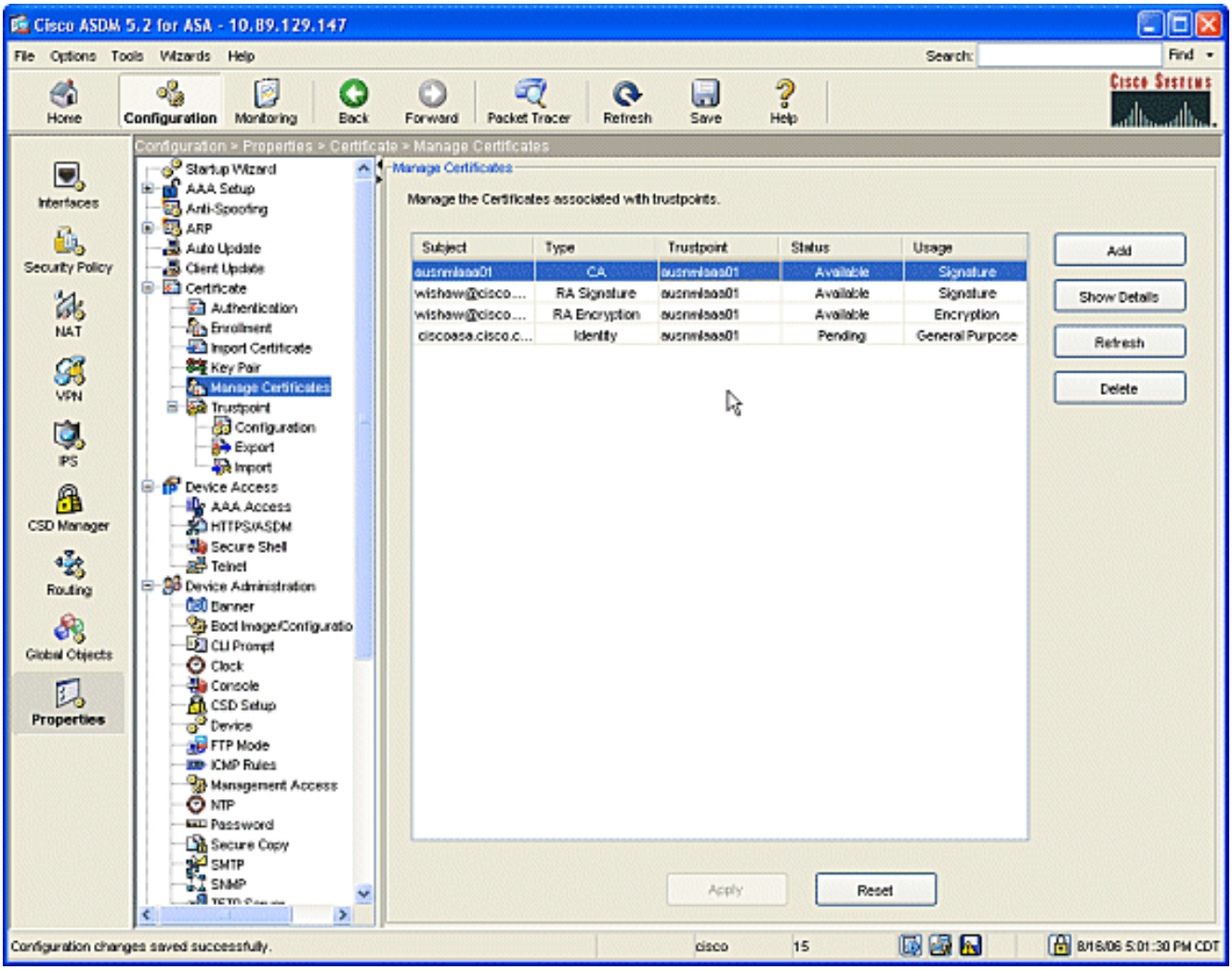
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

인증서 확인 및 관리

인증서를 검토하고 관리합니다.

1. ASDM 애플리케이션을 열고 Configuration(컨피그레이션) 버튼을 클릭합니다.
2. 왼쪽 메뉴에서 **속성** 단추를 클릭합니다.Certificate(**인증서)를 클릭합니다**.Manage **Certificate를 클릭합니다**
   .



명령

ASA에서 명령줄에 여러 **show** 명령을 사용하여 인증서의 상태를 확인할 수 있습니다.

- show crypto **ca certificates** 명령은 인증서, CA 인증서 및 RA(모든 등록 기관) 인증서에 대한 정보를 보는 데 사용됩니다.
- show crypto **ca trustpoints** 명령은 신뢰 지점 컨피그레이션을 확인하는 데 사용됩니다.
- show crypto **key mypubkey rsa** 명령은 ASA의 RSA 공개 키를 표시하는 데 사용됩니다.
- show crypto ca crls 명령**은** 캐시된 모든 CRL을 표시하는 데 사용됩니다.

참고: Output Interpreter Tool(등록된 고객만 해당)(OIT)은 특정 **show** 명령을 **지원합니다**.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

Microsoft Windows 2003 CA 문제 해결 방법에 대한 자세한 내용은 Windows Server 2003 용 공개 키 인프라를 참조하십시오.

명령

참고: debug 명령을 사용하면 Cisco 디바이스에 부정적인 영향을 미칠 수 있습니다.debug 명령을

사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- 디지털 인증서를 얻기 위해 Cisco VPN 3000 Concentrator 4.0.x 구성