Een digitaal certificaat verkrijgen van een Microsoft Windows-certificeringsinstantie met ASDM op een ASA

Inhoud

Inleiding

Digitale certificaten kunnen worden gebruikt om netwerkapparaten en -gebruikers op het netwerk te authentiseren. Ze kunnen worden gebruikt om IPSec sessies tussen netwerkknooppunten te onderhandelen.

Cisco-apparaten identificeren zich op drie belangrijke manieren veilig op een netwerk:

1. **Vooraf gedeelde sleutels**. Twee of meer apparaten kunnen dezelfde gedeelde geheime sleutel hebben. Peers authenticeren elkaar door data te berekenen en een kei aan data te verzenden die de vooraf gedeelde sleutel omvat. Als het ontvangende peer in staat is om het zelfde hash onafhankelijk te creëren met behulp van zijn preShared key, weet het dat beide peers hetzelfde geheim moeten delen, zodat het andere peer authentiek wordt. Deze methode is handmatig en niet erg schaalbaar.
2. **Zelfondertekende certificaten**. Een apparaat genereert zijn eigen certificaat en tekent het als geldig. Dit soort certificaat moet beperkt worden gebruikt. Het gebruik van dit certificaat met toegang tot SSH en HTTPS voor configuratiedoeleinden zijn goede voorbeelden. Er is een afzonderlijk gebruikersnaam/wachtwoord nodig om de verbinding te voltooien.**Opmerking:**

Persistente zelfgetekende certificaten overleven routerreloads omdat ze worden opgeslagen in het niet-vluchtige willekeurig toegankelijke geheugen (NVRAM) van het apparaat. Raadpleeg aanhoudende zelfondertekende certificaten voor meer informatie. Een goed voorbeeld van gebruik is met SSL VPN-verbindingen (WebVPN).

3. **Certificaatcertificaat van de autoriteit**. Een derde bevestigt en verklaart de twee of meer knopen die proberen te communiceren. Elk knooppunt heeft een openbare en particuliere sleutel. De openbare sleutel versleutelt gegevens en de privé-sleutel decrypteert gegevens. Omdat zij hun certificaten van dezelfde bron hebben verkregen, kunnen zij zich van hun respectieve identiteit verzekeren. Het ASA-apparaat kan een digitaal certificaat van een derde verkrijgen met een handmatige inschrijvingsmethode of een automatische inschrijvingsmethode.**Opmerking:** De inschrijvingsmethode en het type digitaal certificaat dat u kiest, zijn afhankelijk van de functies en functies van elk product van derden. Neem voor meer informatie contact op met de verkoper van de certificatiedienst.

De Cisco adaptieve security applicatie (ASA) kan gebruikmaken van pre-gedeelde sleutels of digitale certificaten die door een derde partij zijn opgegeven, om IPSec-verbindingen te authenticeren. Daarnaast kan de ASA zijn eigen, zelf getekende digitale certificaat produceren. Dit moet worden gebruikt voor SSH-, HTTPS- en Cisco Adaptieve Security apparaat Manager (ASDM)-verbindingen naar het apparaat.

Dit document toont de procedures aan die nodig zijn om automatisch een digitaal certificaat van een Microsoft certificaatinstantie (CA) voor de ASA te verkrijgen. Dit omvat niet de handmatige inschrijvingsmethode. Dit document gebruikt ASDM voor de configuratiestappen en presenteert de definitieve configuratie van de opdrachtregel in de interface (CLI).

Raadpleeg Cisco IOS certificaatinschrijving met uitgebreide inschrijving van Invoeropdrachten in Configuration Voorbeeld om meer te weten te komen over hetzelfde scenario met Cisco IOS®-platforms.

Raadpleeg de Cisco VPN 3000 Concentrator 4.7.x configureren om een digitaal certificaat en een SSL-certificaat te verkrijgen om meer te weten te komen over hetzelfde scenario met de Cisco VPN 3000 Series Concentrator.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

Eisen voor het ASA-apparaat

- Configureer de Microsoft® Windows 2003 Server als een CA.Raadpleeg uw Microsoft documentatie of openbare sleutelinfrastructuur voor Windows Server 2003
- Om de Cisco ASA of PIX versie 7.x te laten configureren door de Adaptieve Security Devices Manager (ASDM), raadpleeg HTTPS Access voor ASDM.
- Installeer de Add-on voor certificaatservices (mscep.dll).
- Verkrijg het uitvoerbare bestand (cepSetup.exe) voor het Add-on uit het Simple Certificate Enrollment Protocol (SCEP) Add-on voor certificaatservices of het mscep.dll-bestand van de Windows Server 2003 Resource Kit Tools .**Opmerking:** Configureer de juiste datum, tijd en tijdzone in de Microsoft Windows-machine. Het gebruik van het Network Time Protocol (NTP)

wordt ten zeerste aanbevolen, maar niet nodig.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 Series adaptieve security applicatie, software versie 7.x en hoger
- Cisco Adaptieve Security Office Manager versie 5.x en hoger
- Microsoft Windows 2003 Server-certificeringsinstantie

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco PIX 500 Series security applicatie, versie 7.x.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

ASA configureren om certificaten te ruilen met Microsoft CA

Taak

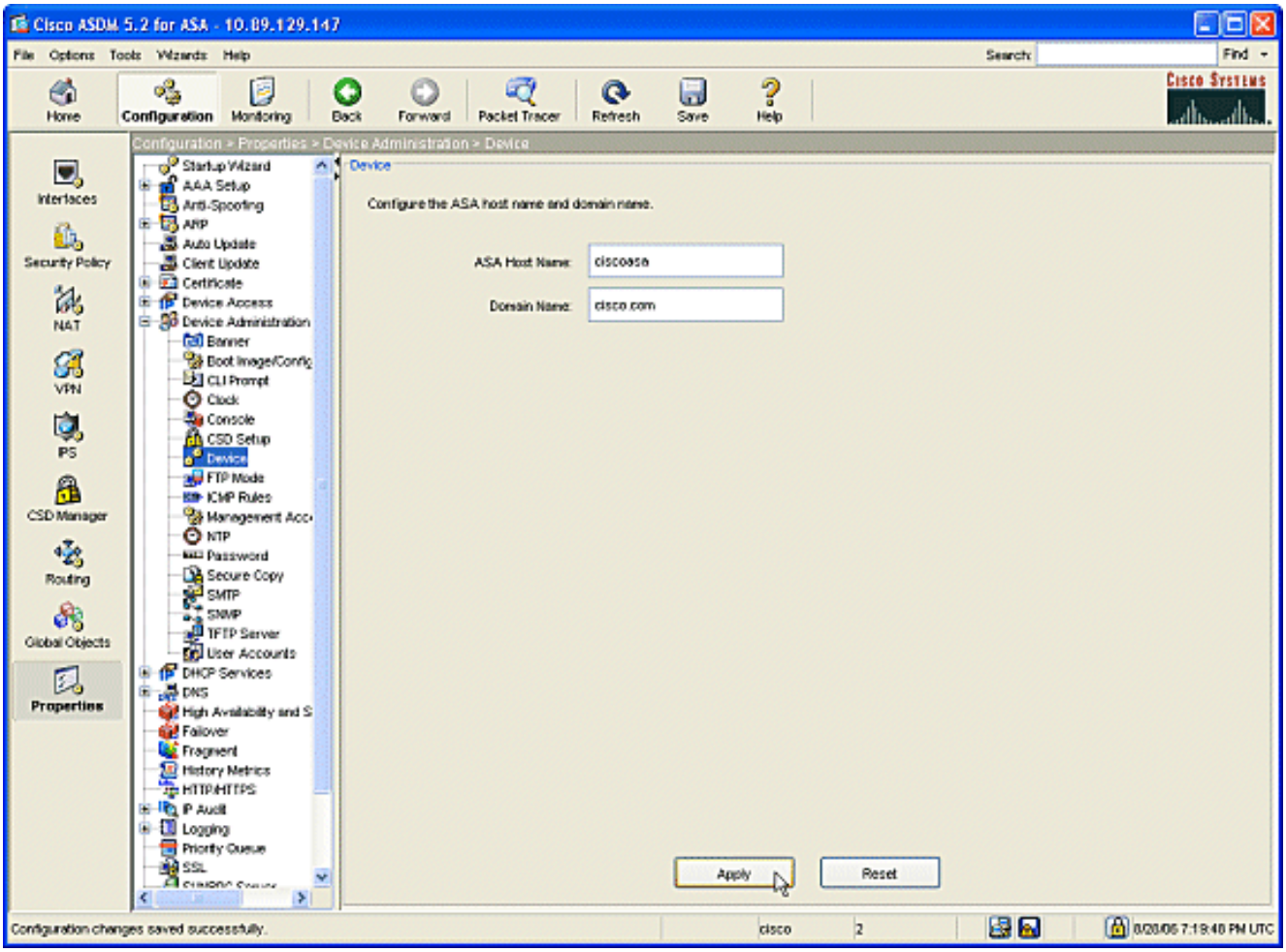
In deze sectie wordt u getoond hoe u de ASA kunt configureren om een certificaat te ontvangen van de Microsoft certificaatinstantie.

Instructies voor het configureren van de ASA

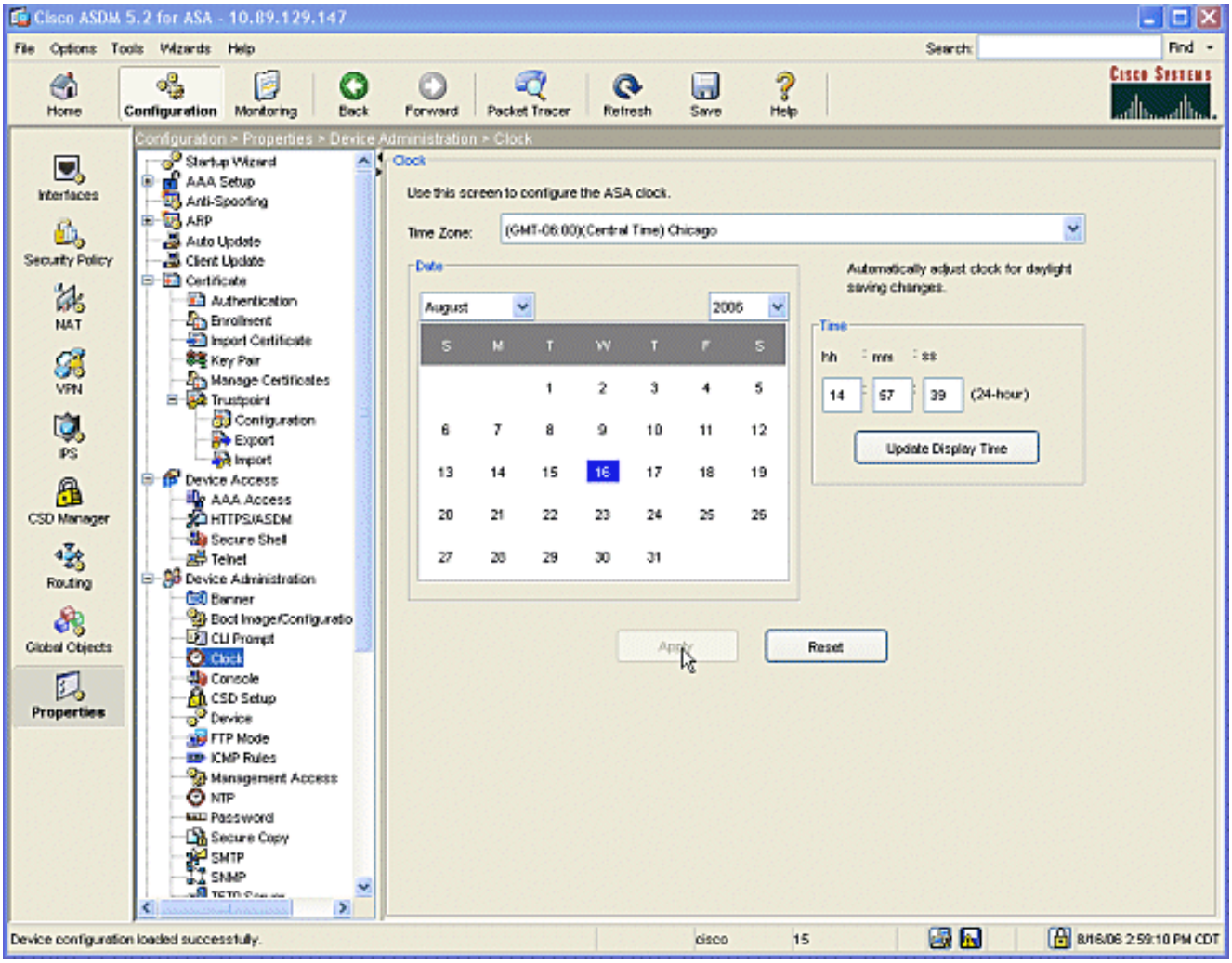
In digitale certificaten wordt de datum/tijd/tijdzone-component gebruikt als een van de controles op de geldigheid van het certificaat. Het is noodzakelijk om de Microsoft CA en al uw apparaten met de juiste datum en tijd te configureren. Microsoft CA gebruikt een add-on (mscep.dll) aan zijn certificaatservices om certificaten met Cisco-apparaten te delen.

Voltooi deze stappen om de ASA te configureren:

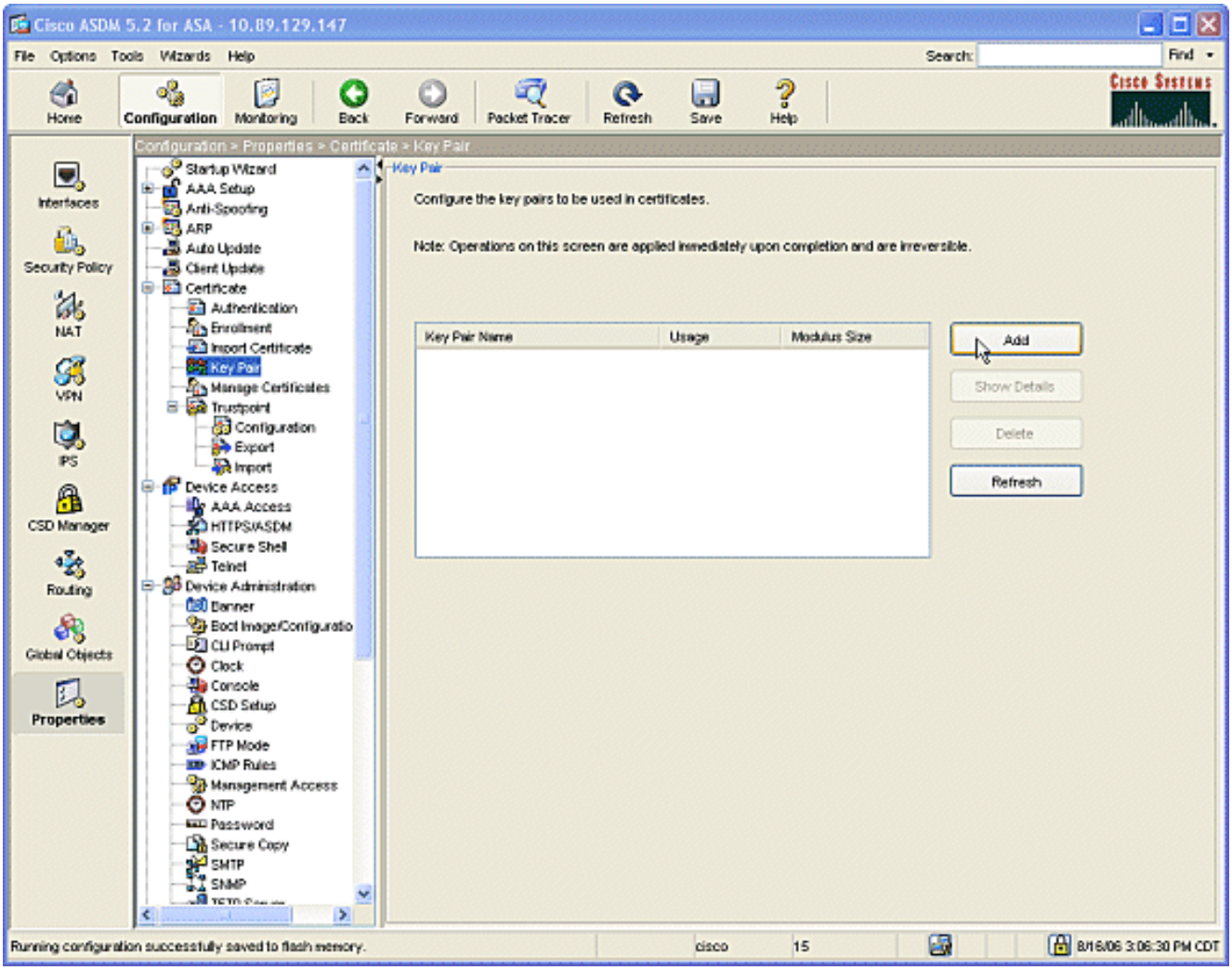
1. Open de ASDM-toepassing en klik op de knop **Configuration**.Klik in het linkermenu op de knop **Eigenschappen**.Klik vanuit het navigatiedeelvenster op **Apparaatbeheer > Apparaat**.Voer een Host Name en Domain Name in voor de ASA. Klik op **Apply** (Toepassen).Klik desgevraagd op **Opslaan > Ja**.



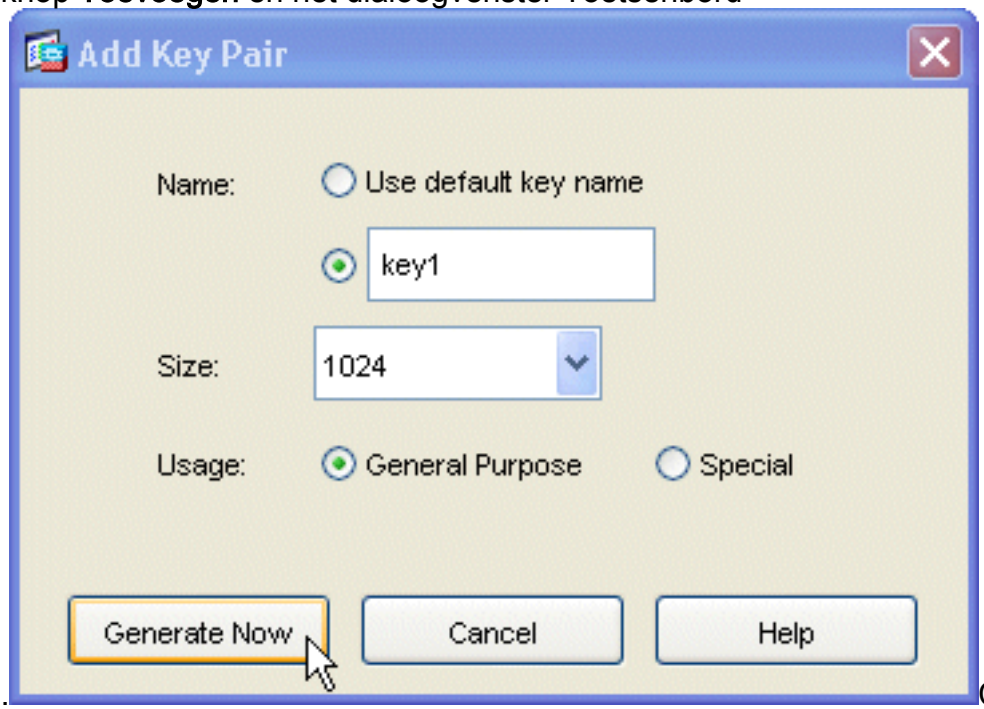
2. Configureer de ASA met de juiste datum, tijd en tijdzone. Dit is belangrijk voor het genereren van het certificaat van het apparaat. Gebruik indien mogelijk een NTP-server.Klik vanuit het navigatiedeelvenster op **Apparaatbeheer > Kloktijd**.Gebruik in het venster Clock de velden en de vervolgkeuzelijsten om de juiste datum, tijd en tijdzone in te stellen.



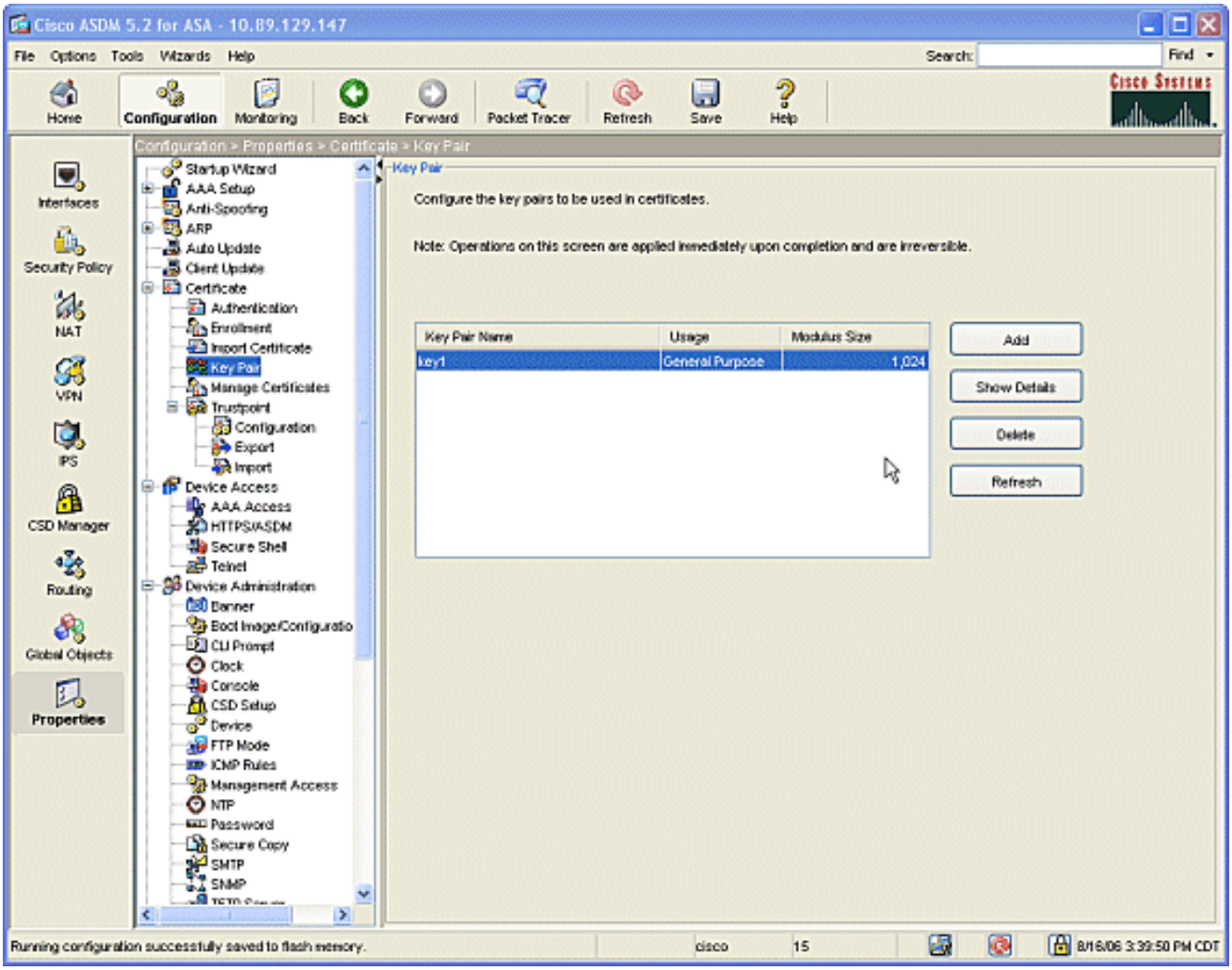
3. ASA moet zijn eigen toetsenbord hebben (particuliere en openbare sleutels). De openbare sleutel wordt naar Microsoft CA verzonden.Klik vanuit het navigatiedeelvenster op **Certificaat > Toetsenbord**.



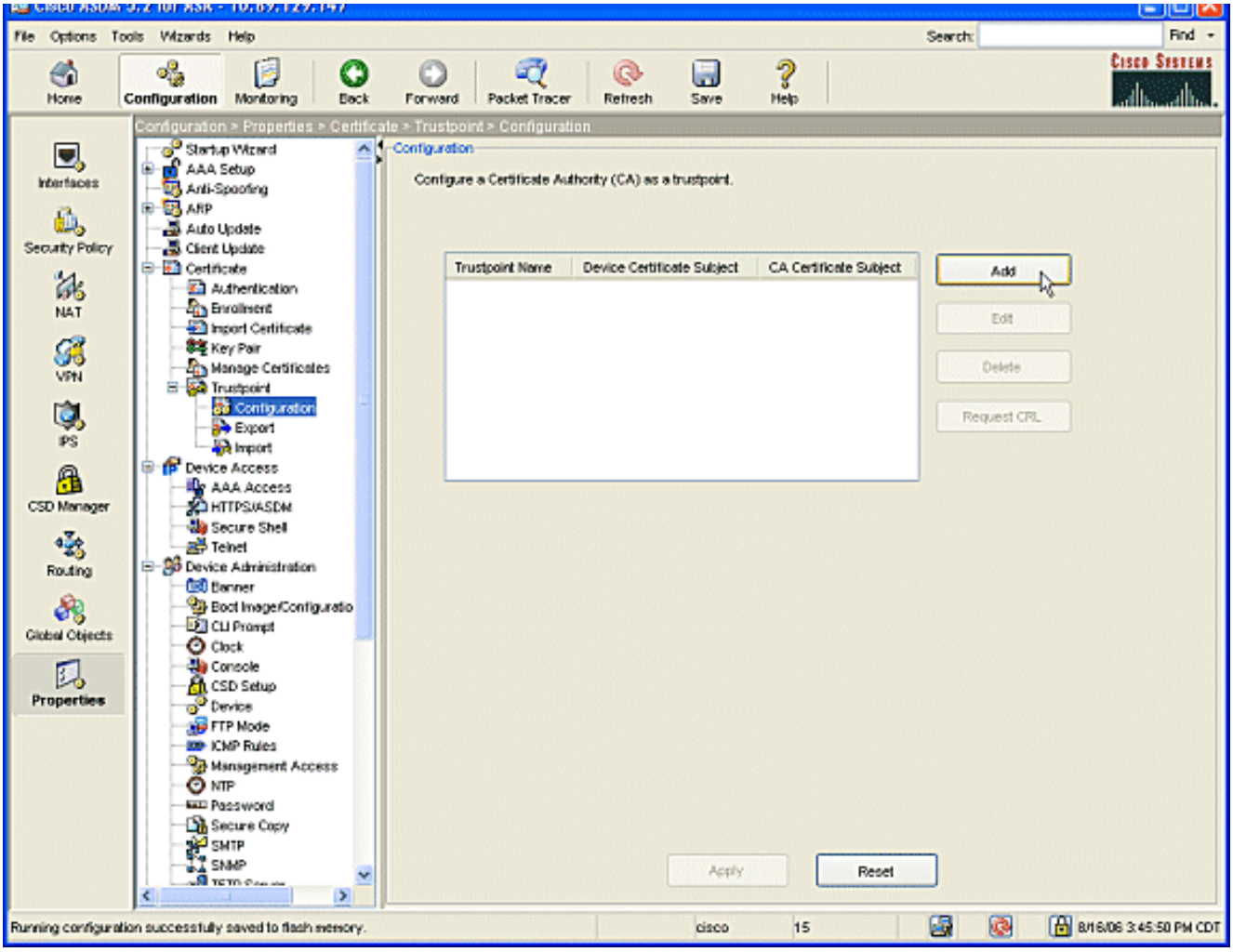
Klik op de knop **Toevoegen** en het dialoogvenster Toetsenbord



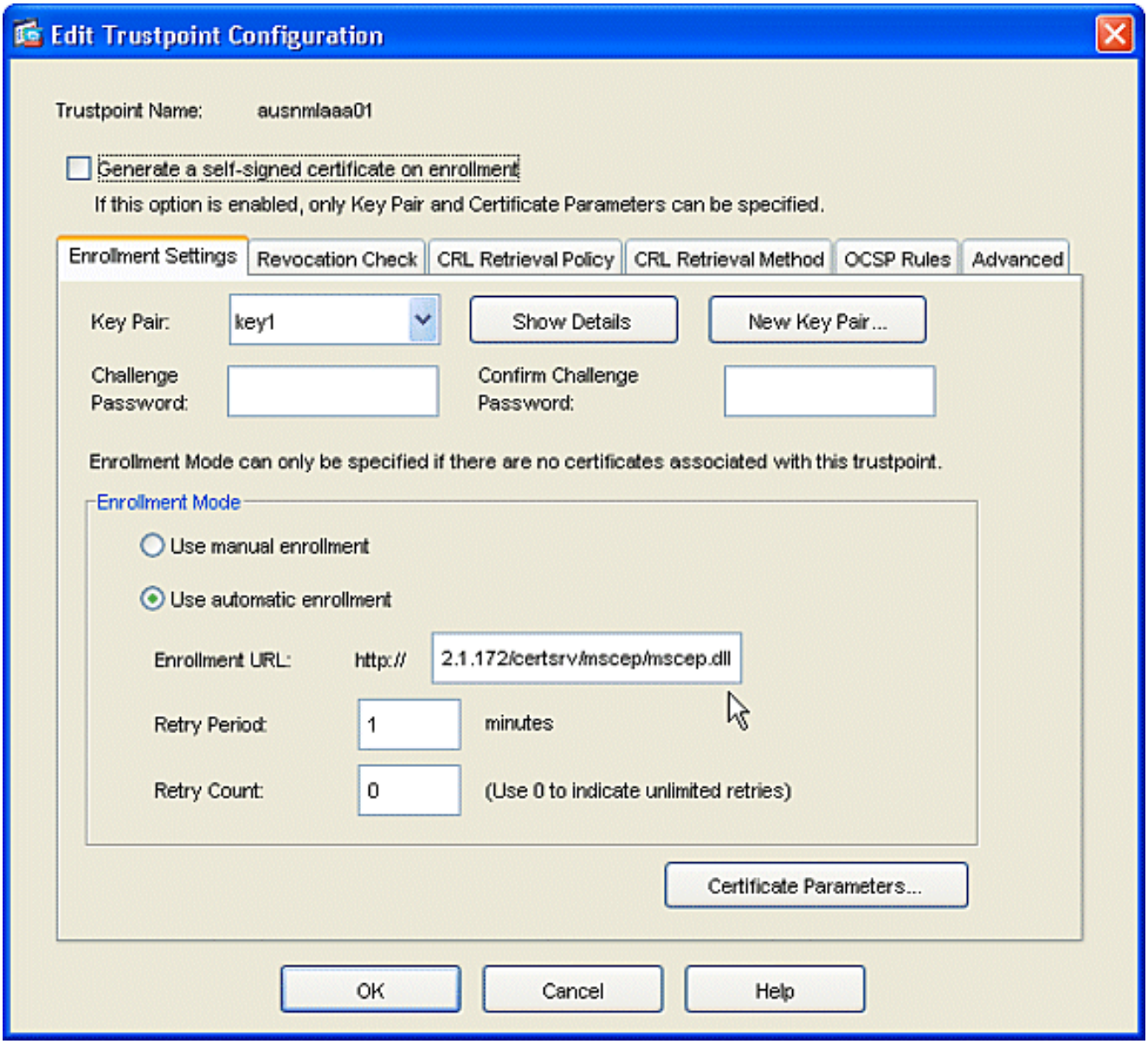
toevoegen.Controleer de radioknop naast het blancoveld van het naamgebied en type in de naam voor de toets.Klik op de **grootte:** Als u in het uitrolvak een grootte voor de toets wilt kiezen, accepteert u de standaardinstelling.Controleer de selectieknop **voor algemene doeleinden** onder gebruik.Klik op de knop **Generate Now** om de toetsen te regenereren en terug te keren naar het hoofdvenster, waar u de informatie voor het sleutelpaar kunt bekijken.



4. Configureer de Microsoft CA als betrouwbaar. Klik vanuit het navigatiedeelvenster op **Trustpunt > Configuration**.Klik vanuit het venster Configuration op de knop **Add**.

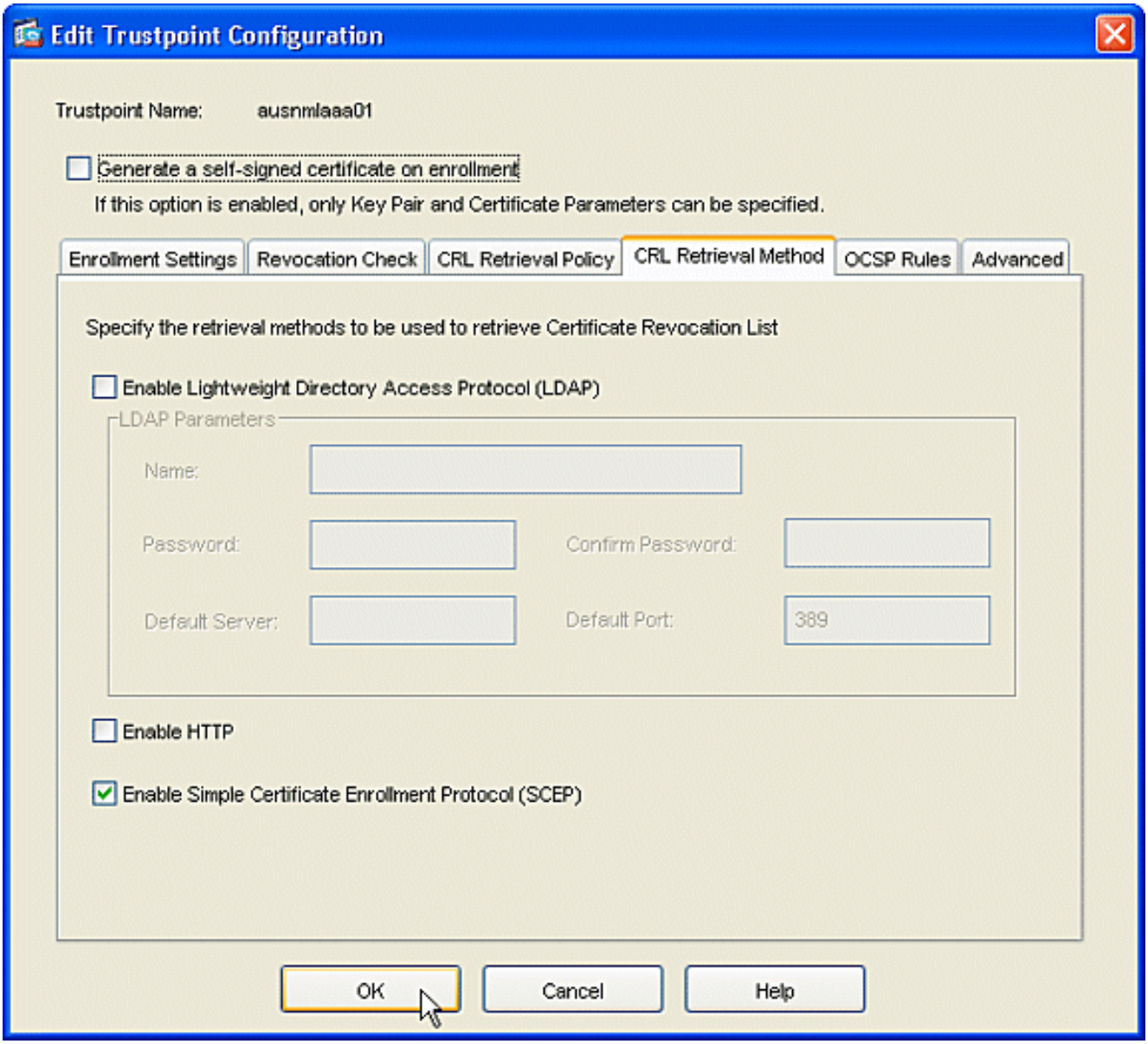


Het venster Configuration voor Trustpoint bewerken toont.

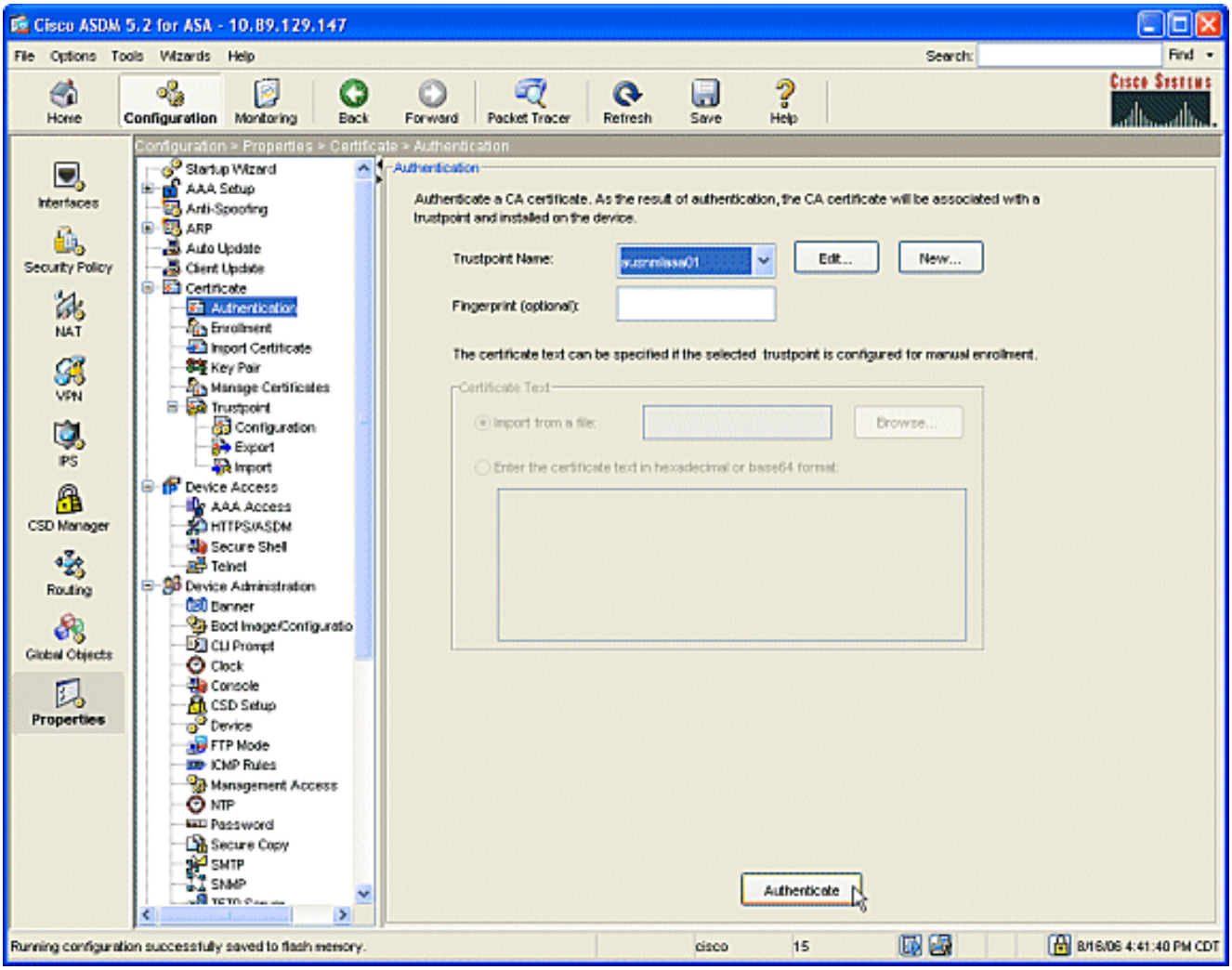


Vul een naam in voor het Trustpoint met de naam van de CA.Klik op het **sleutelvenster:** pijl door het uitrolvak en kies de naam van het sleutelpaar dat u hebt gemaakt.Controleer de radioknop **Automatische inschrijving** en voer de URL voor Microsoft CA in: **http://CA_IP_Address/certsrv/mscep/mscep.dll**.

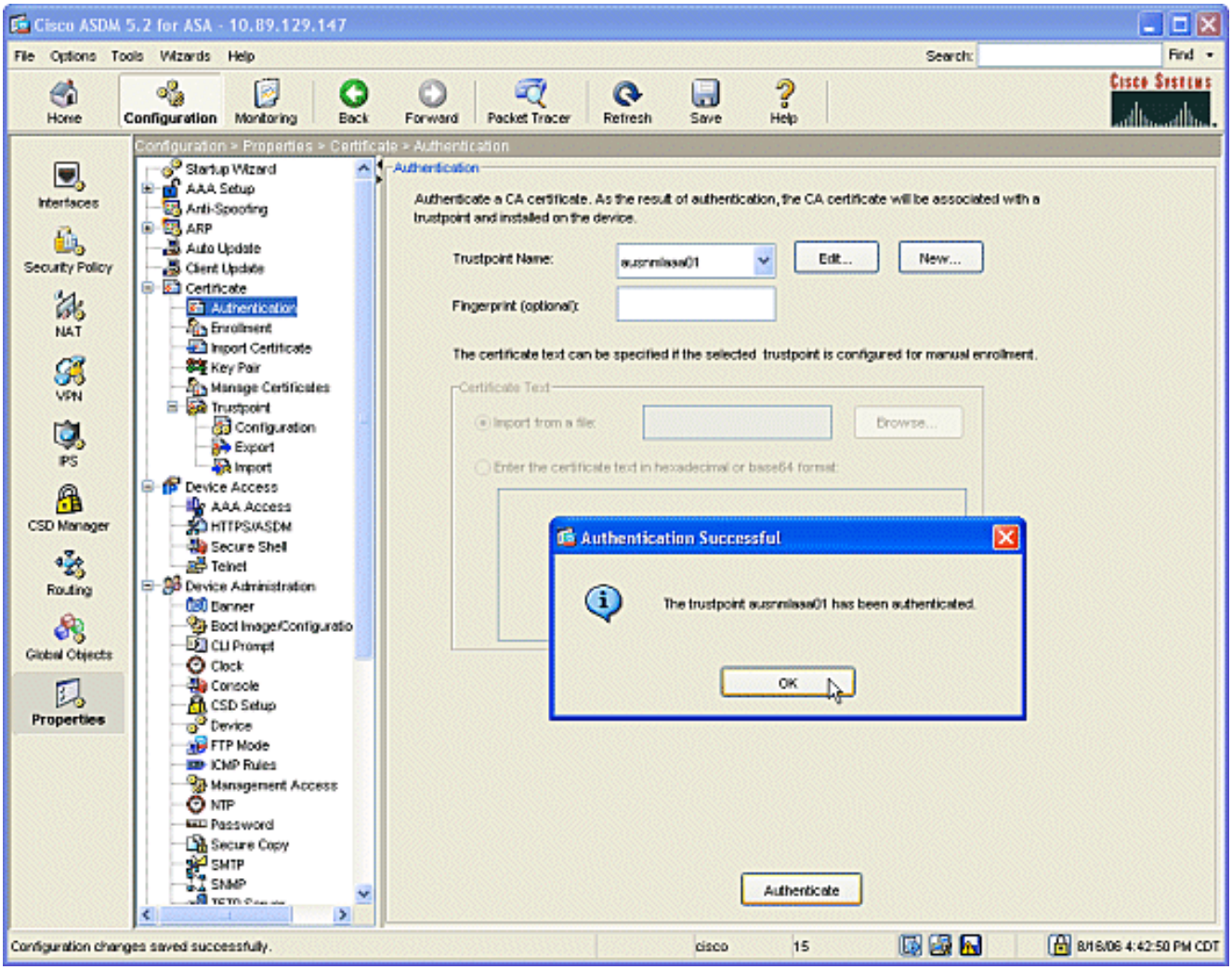
5. Klik op het tabblad **Retourenmethode**.Schakel de aanvinkvakje Enable HTTP en Enable Light Directory Access Protocol (LDAP) uit.Controleer het aanvinkvakje Enable Simple certificaatinschrijving Protocol (SCEP). Laat alle andere tabinstellingen achter bij hun standaardinstellingen.Klik op de knop **OK**.



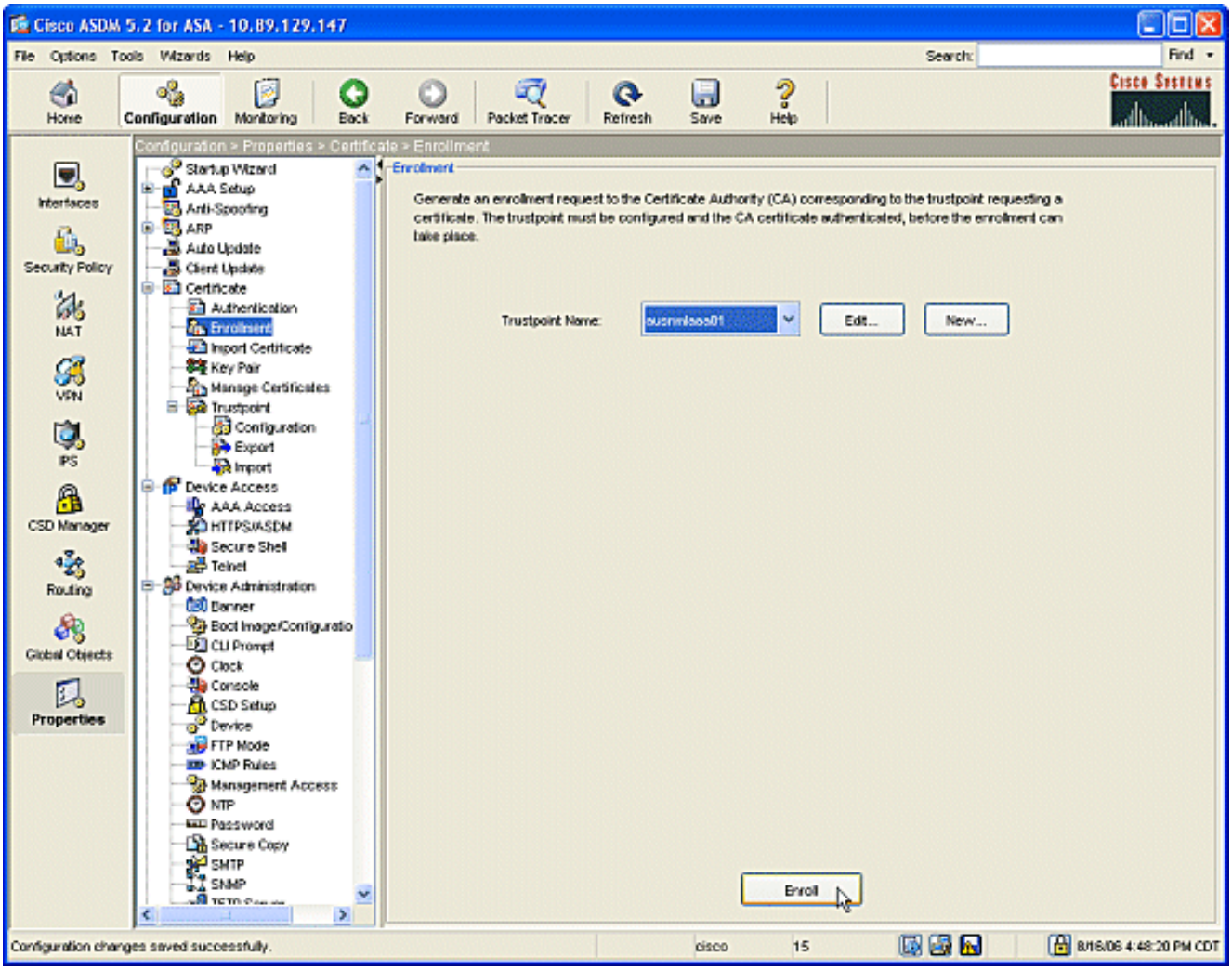
6. Verifieer en registreer met Microsoft CA. Klik vanuit het navigatiedeelvenster op **Certificaat > Verificatie**. Zorg ervoor dat het nieuwe trustpoint in de **Trustpoint Name** verschijnt: veld. Klik op de knop
Verificeren.



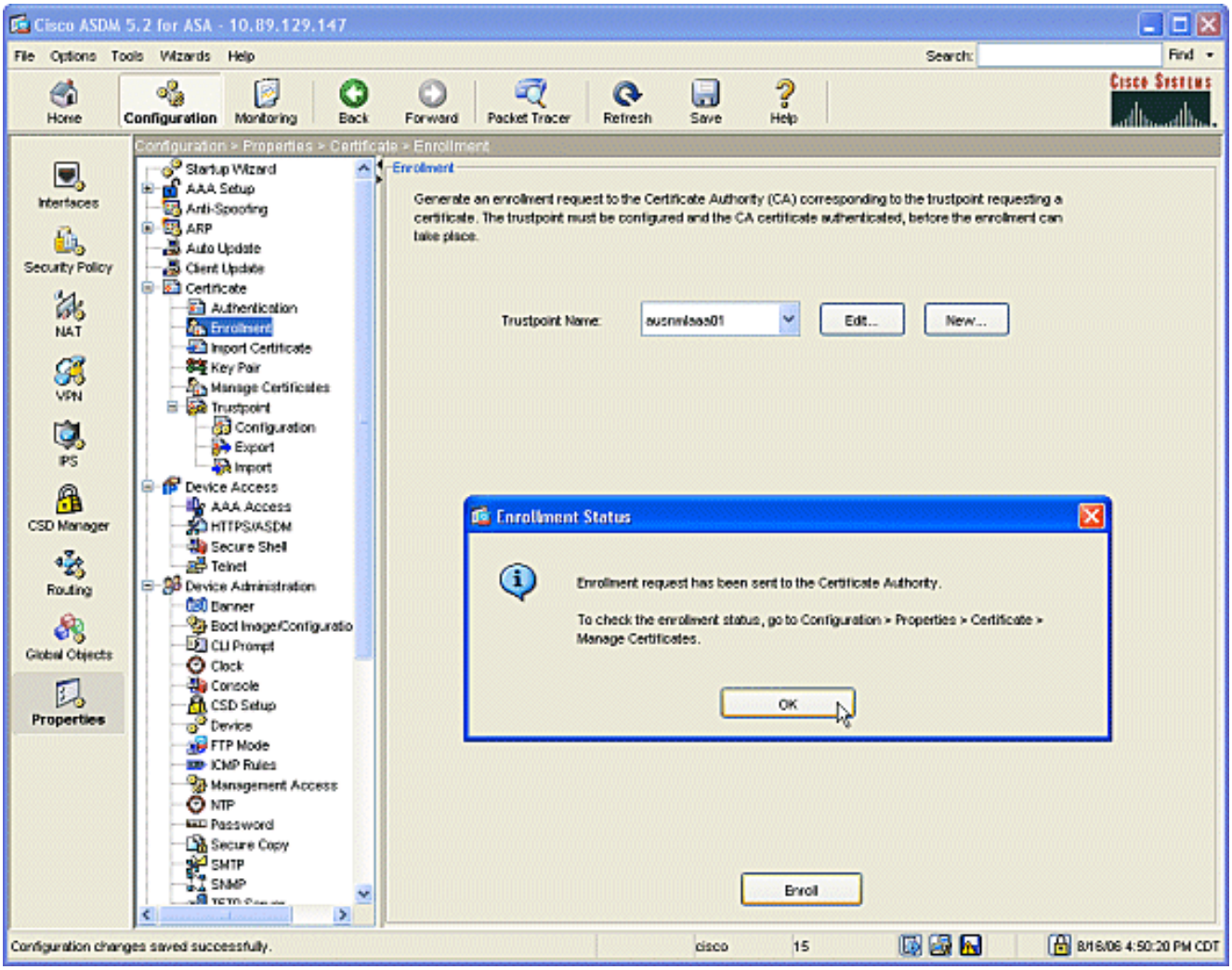
7. Een dialoogvenster toont aan dat u wilt laten weten dat het vertrouwde punt is geauthentiseerd. Klik op de knop **OK**.



8. Klik in het navigatiedeelvenster op **inschrijving**. Zorg dat de naam van het vertrouwenspunt in het veld Naam van het Trustpoint wordt weergegeven en klik vervolgens op de knop **Invoegen**.



9. Er verschijnt een dialoogvenster om u te laten weten dat het verzoek naar de CA is verzonden. Klik op de knop **OK**.



Opmerking: Op een standaard-Alone machine van Microsoft Windows moet u de certificaten voor om het even welke verzoeken uitgeven die aan CA zijn voorgelegd. Het certificaat wordt in behandeling totdat u met de rechtermuisknop op het certificaat klikt en op de Microsoft Server klikt op afgifte.

Resultaten

Dit is de CLI-configuratie die het resultaat is van de ASDM-stappen:

ciscoa

```
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
```

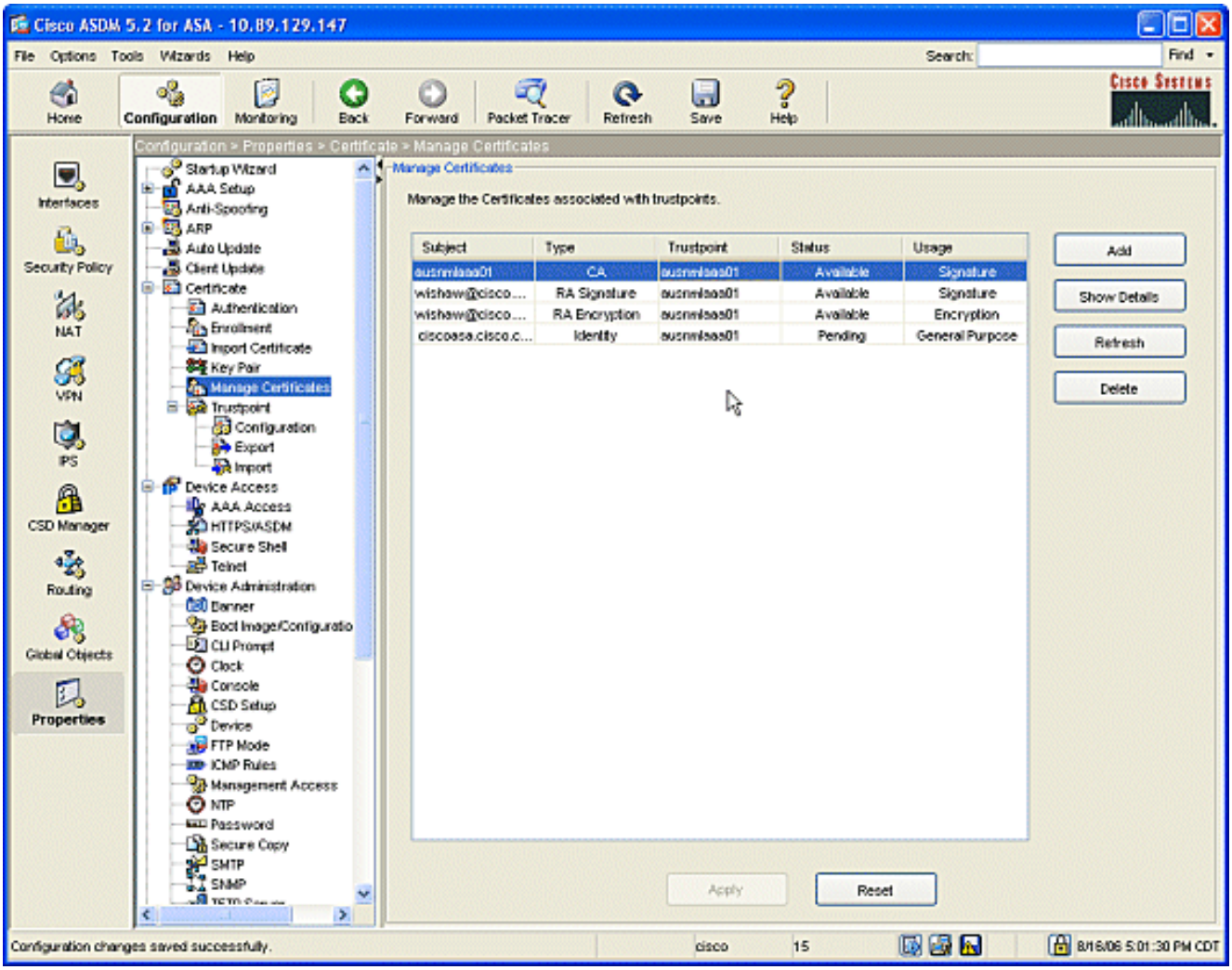
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer en beheer uw certificaat

Controleer en beheer uw certificaat.

1. Open de ASDM-toepassing en klik op de knop **Configuration**.
2. Klik in het linkermenu op de knop **Eigenschappen**.Klik op **Certificaat**.Klik op **Certificaat beheren**.



Opdrachten

In ASA kunt u meerdere **show** opdrachten in de opdrachtregel gebruiken om de status van een certificaat te controleren.

- De opdracht **toont crypto ca certificaten** die worden gebruikt om informatie te bekijken over uw certificaat, het CA certificaat en alle registrerende autoriteit (RA) certificaten.
- De commando **show crypto ca trustpoints** wordt gebruikt om de configuratie van de trustpunten te verifiëren.
- De opdracht **toont crypto-toets mypubkey rsa** wordt gebruikt om de RSA openbare toetsen van uw ASA weer te geven.
- De opdracht **toont crypto ca crls** die wordt gebruikt om alle gecachgeerde CRLs weer te geven.

Opmerking: Uitvoer Tolk (alleen geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Raadpleeg de openbare sleutelinfrastructuur voor Windows Server 2003 voor meer informatie over hoe u Microsoft Windows 2003 CA kunt oplossen.

Opdrachten

Opmerking: het gebruik van **debug-**opdrachten kan een negatieve invloed hebben op uw Cisco-apparaat. Voordat u **debug**-opdrachten gebruikt, raadpleegt u Belangrijke informatie over Debug Commands.

Gerelateerde informatie

- De Cisco VPN 3000 Concentrator 4.0.x configureren om een digitaal certificaat te verkrijgen