Cómo obtener un certificado digital de Microsoft Windows CA usando el ASDM en un ASA

Contenido

Introducción

Los certificados digitales se pueden utilizar para autenticar dispositivos de red y usuarios en la red. Pueden ser utilizados para negociar sesiones IPSec entre los nodos de red.

Los dispositivos de Cisco se identifican con seguridad en una red en tres formas principales:

1. **Claves previamente compartidas**. Dos o más dispositivos pueden tener la misma clave secreta compartida. Los pares se autentican computando y enviando un hash cerrado de los datos que incluyen la clave del preshared. Si el par de recepción puede crear el mismo hash independientemente usando su clave del preshared, conoce que ambos pares deben compartir el mismo secreto, así la autenticidad del otro par. Este método es manual y no muy scalable.
2. **Certificados autofirmados**. Un dispositivo genera su propio certificado y lo firma como siendo válido. Este tipo de certificado debe haber limitado el uso. Usando este certificado con el acceso de SSH y HTTPS para los fines de la configuración son los buenos ejemplos. Un par de nombre de usuario/contraseña separado es necesario completar la conexión.**Nota:** Los certificados autofirmados persistentes sobreviven las recargas de router porque se guardan en memoria de acceso aleatorio no volátil (NVRAM) del dispositivo. Refiera a los certificados autofirmados persistentes para más información. Un buen ejemplo del uso está con las

conexiones SSL VPN (WebVPN).

3. **Certificado del Certificate Authority**. Otro vendedor valida y autentica dos o más Nodos que intentan comunicar. Cada nodo tiene una clave pública y privada. La clave pública cifra los datos, y la clave privada desencripta los datos. Porque han obtenido sus Certificados de la misma fuente, pueden ser confiados de sus identidades respectivas. El dispositivo ASA puede obtener un certificado digital de un de tercera persona con un método del Registro manual o un método del enlistamiento automático.**Nota:** El método de la inscripción y el tipo de certificado digital que usted elige es dependientes sobre las características y las funciones de cada producto de terceros. Entre en contacto al vendedor del servicio de certificados para más información.

El dispositivo de seguridad adaptante de Cisco (ASA) puede utilizar las claves previamente compartidas o los Certificados digitales proporcionados por un Certificate Authority (CA) de tercera persona para autenticar las conexiones del IPSec. Además, el ASA puede presentar su propio certificado digital uno mismo-firmado. Esto se debe utilizar para SSH, el HTTPS, y las conexiones del Cisco Adaptive Security Device Manager (ASDM) al dispositivo.

Este documento demuestra los procedimientos necesarios obtener automáticamente un certificado digital de un Microsoft Certificate Authority (CA) para el ASA. No incluye el método manual de inscripción. Este documento utiliza el ASDM para los pasos para la configuración, así como presenta la configuración final del comando line interface(cli).

Refiera a la inscripción del certificado del Cisco IOS usando el ejemplo aumentado de los comandos Configuration de la inscripción para aprender un escenario más casi igual con las Plataformas del ® del Cisco IOS.

Refiera a configurar el Cisco VPN 3000 Concentrator 4.7.x para conseguir un certificado digital y un certificado SSL para aprender un escenario más casi igual con el concentrador del Cisco VPN de la serie 3000.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

Requisitos para el dispositivo ASA

- Configure el servidor de Windows 2003 del Microsoft® como CA.Refiera a su documentación de Microsoft o al Public Key Infrastructure para el Servidor Windows 2003
- Para permitir Cisco ASA o versión de PIX 7.x que se configurarán por el Administrador de dispositivos de seguridad adaptante (ASDM), refiera a permitir el acceso HTTPS para el ASDM.
- Instale la agregación para los servicios de certificados (mscep.dll).
- Obtenga el archivo ejecutable (cepsetup.exe) para la agregación de la agregación del protocolo simple certificate enrollment (SCEP) para los servicios de certificados o el archivo mscep.dll del WindowsServer las herramientas de 2003 juegos de recursos.**Nota:** Configure la fecha, el tiempo, y el huso horario correctos en la máquina de Microsoft Windows. El uso del Network Time Protocol (NTP) se recomienda altamente pero no necesario.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 5500 Series dispositivo de seguridad adaptante de Cisco ASA, versión de software 7.x y posterior
- Versión 5.x y posterior del Cisco Adaptive Security Device Manager
- Certificate Authority del servidor de Microsoft Windows 2003

Productos Relacionados

Esta configuración se puede también utilizar con la versión 7.x del dispositivo de seguridad de la serie del Cisco PIX 500.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configure el ASA para intercambiar los Certificados por Microsoft CA

Tarea

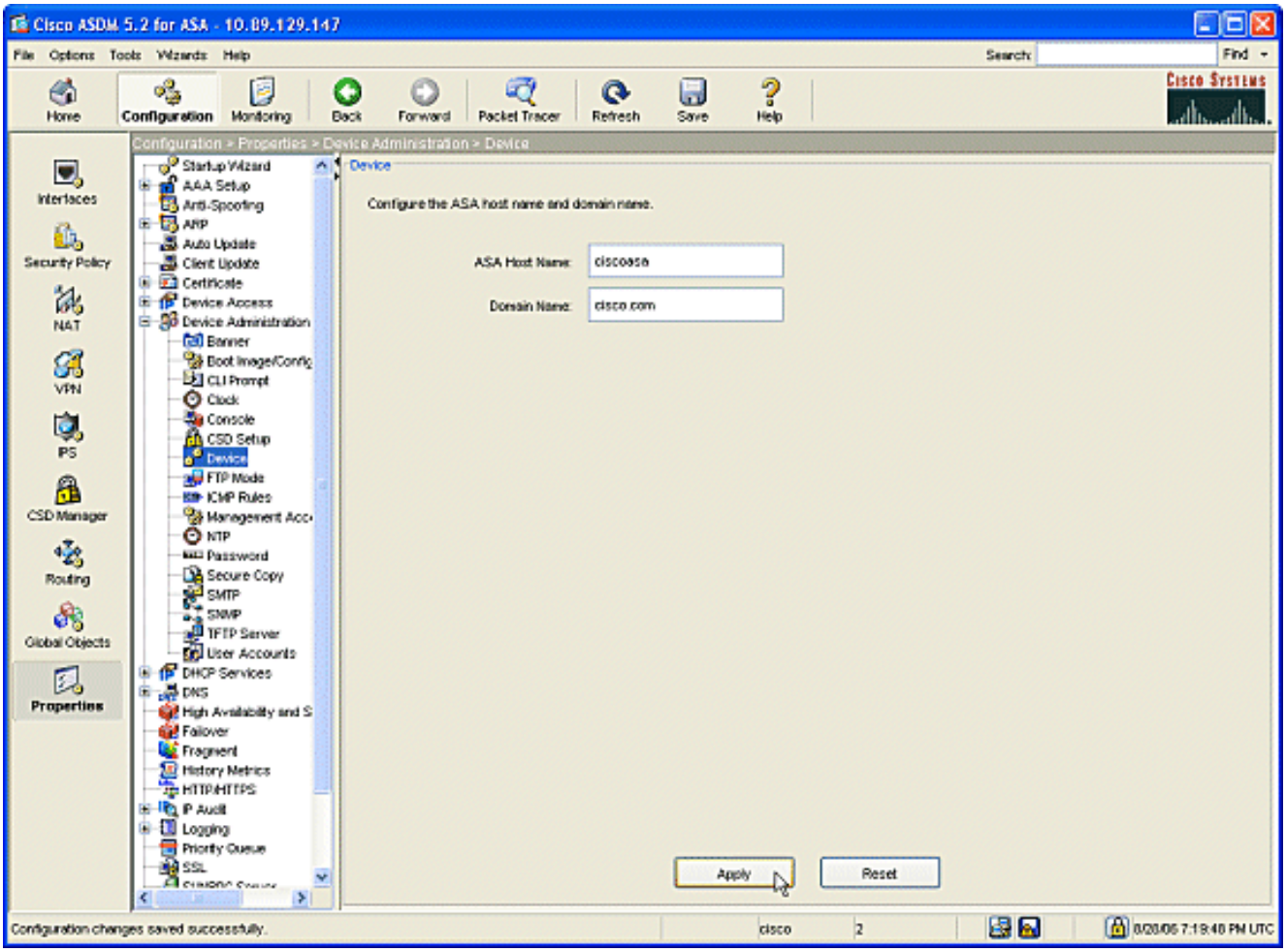
En esta sección, le muestran cómo configurar el ASA para recibir un certificado del Microsoft Certificate Authority.

Instrucciones de configurar el ASA

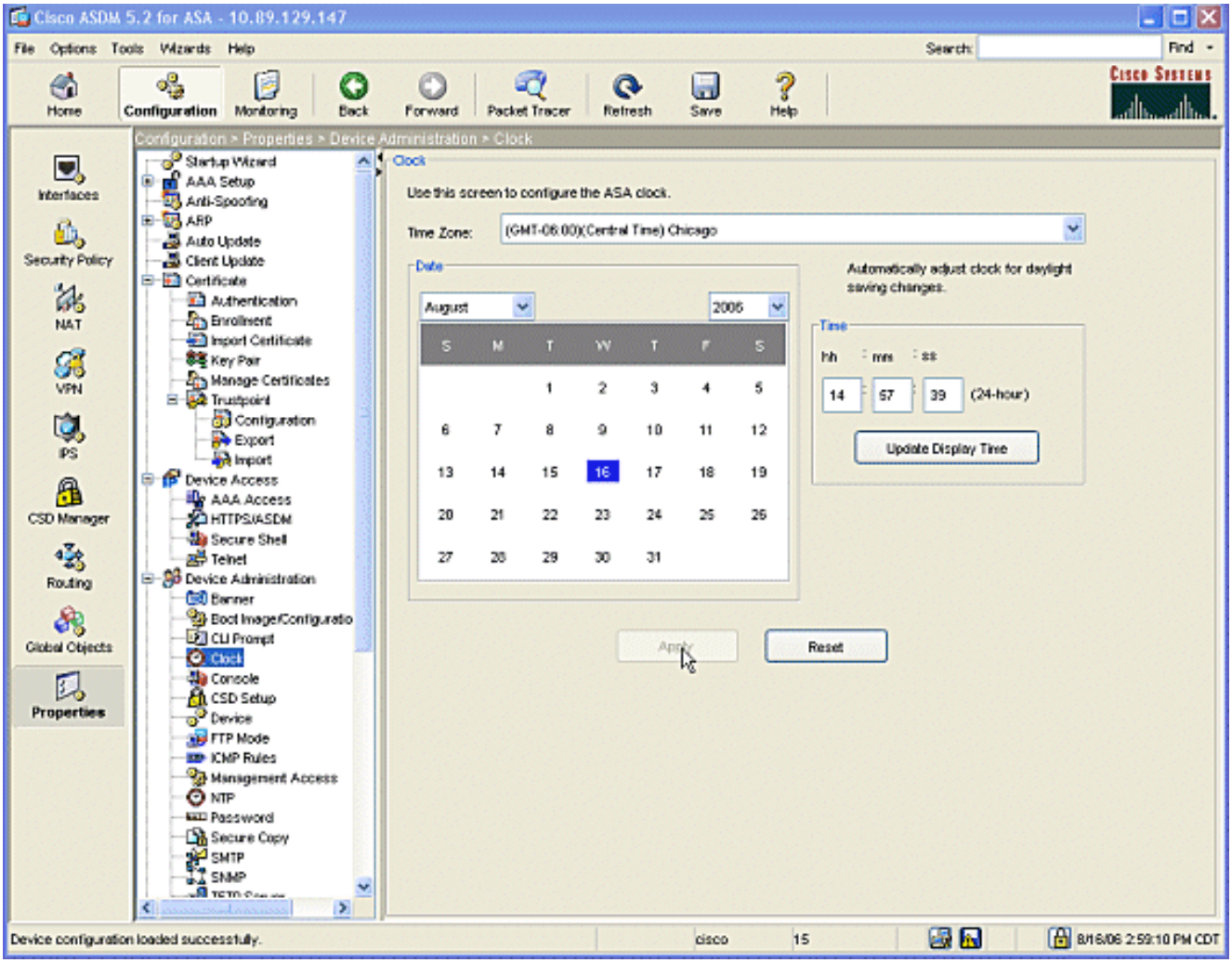
Los Certificados digitales utilizan el componente de la fecha/del tiempo/del huso horario como una de las comprobaciones para la validez del certificado. Es imprescindible configurar Microsoft CA y todos sus dispositivos con la fecha y hora correcta. Microsoft CA utiliza una agregación (mscep.dll) a sus Certificados de parte de los servicios de certificados para con los dispositivos de Cisco.

Complete estos pasos para configurar el ASA:

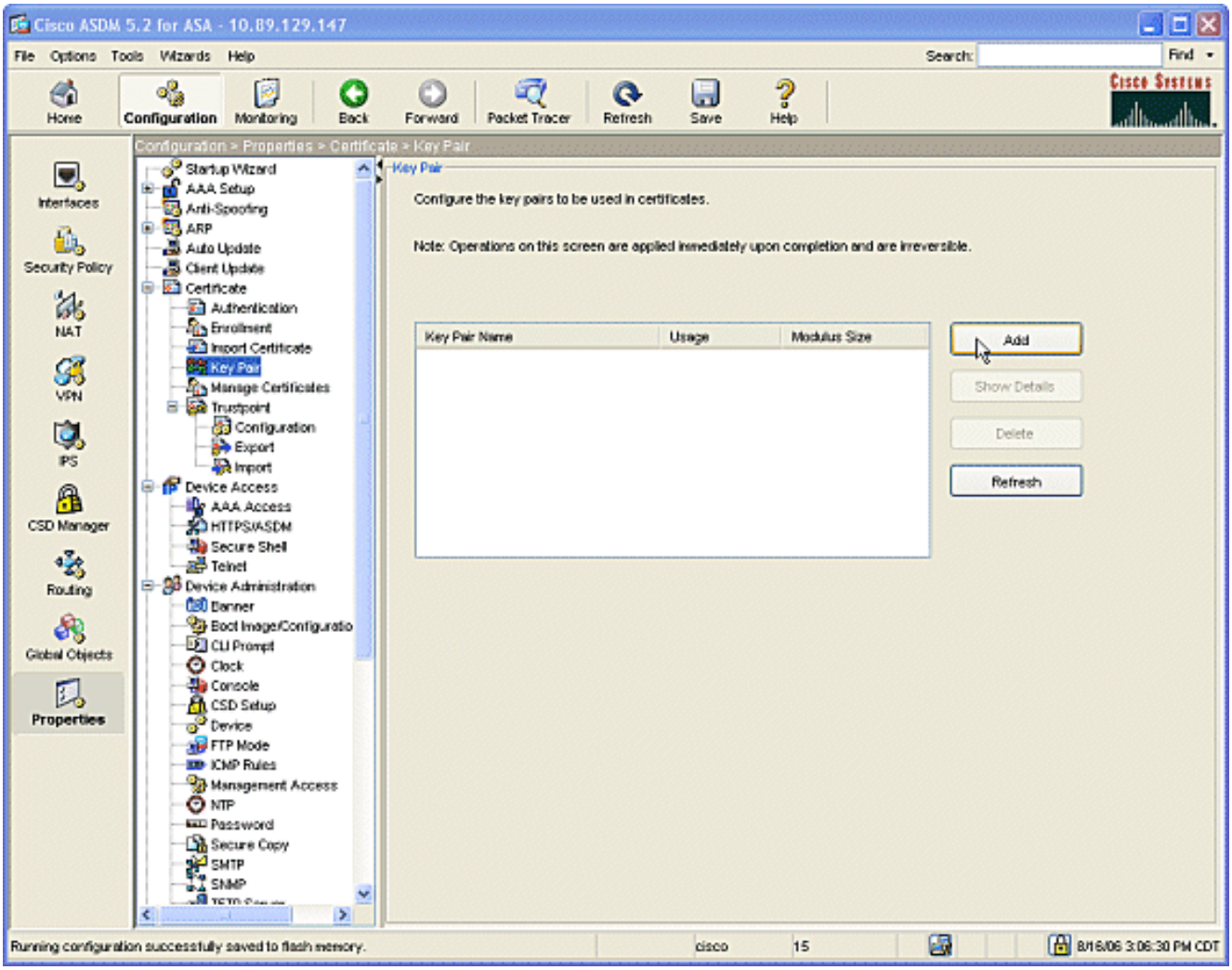
1. Abra la aplicación ASDM y haga clic el botón de la **configuración**.Del menú izquierdo, haga clic el **botón properties**.Del SCR_INVALID, haga clic **Device Administration (Administración del dispositivo) > dispositivo**.Ingrese un nombre del host y un Domain Name para el ASA. Haga clic en Apply (Aplicar).Cuando se le pregunte, **salvaguardia del** tecleo **> sí**.



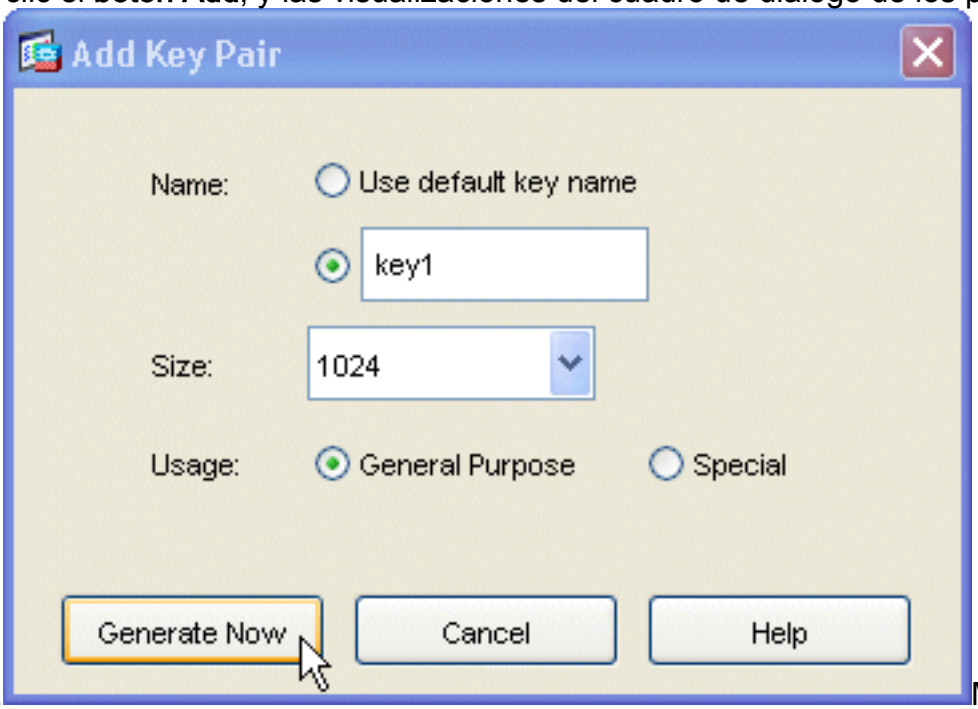
2. Configure el ASA con la fecha, el tiempo, y el huso horario correctos. Esto es importante para la generación del certificado del dispositivo. Utilice a un servidor NTP, si es posible.Del SCR_INVALID, haga clic **Device Administration (Administración del dispositivo) > reloj**.En la ventana del reloj, utilice los campos y las flechas desplegables para fijar la fecha, la hora, y el huso horario
correctos.



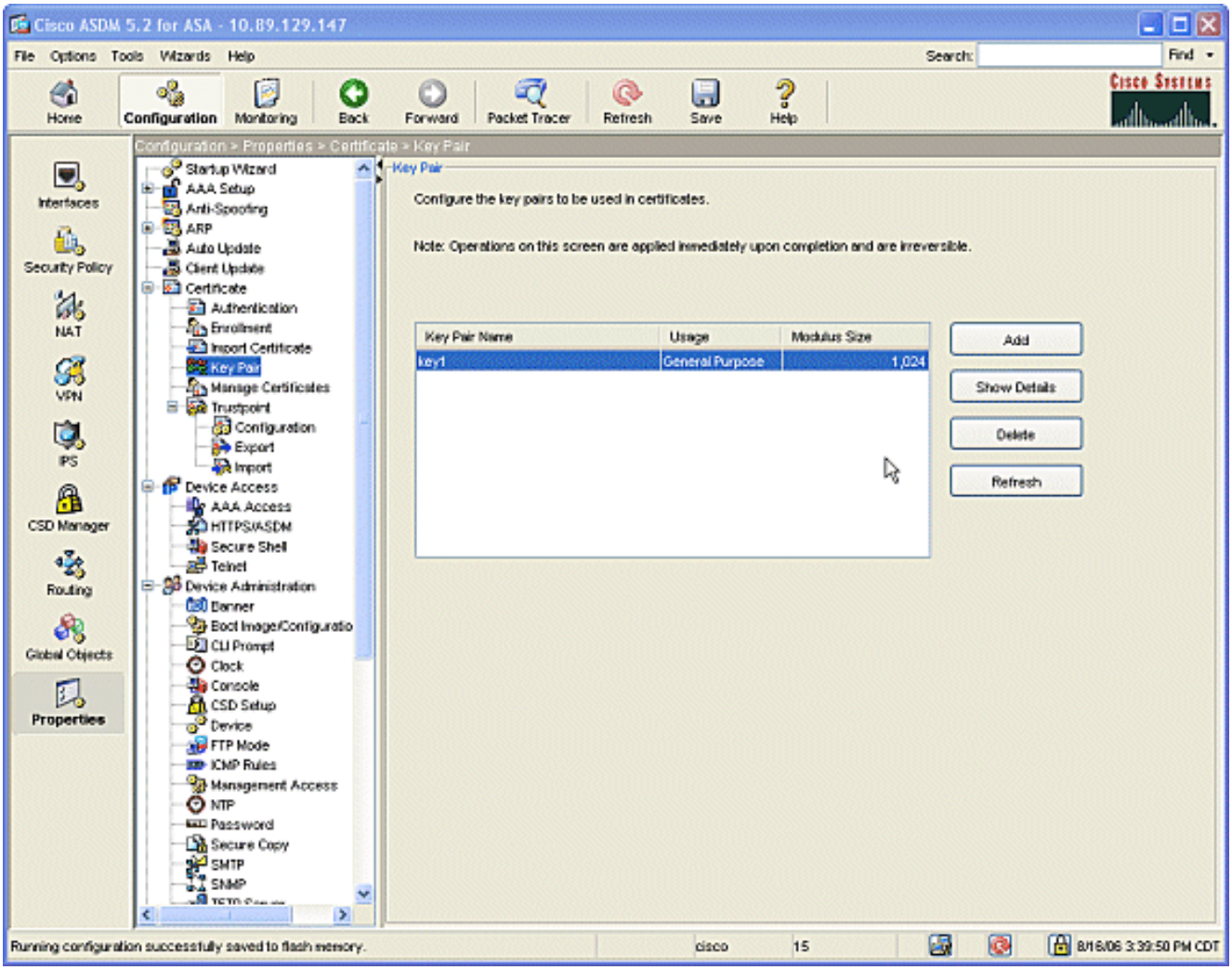
3. El ASA debe tener su propio par clave (soldado y las claves públicas). La clave pública será enviada a Microsoft CA.Del SCR_INVALID, **certificado > par clave del** tecleo.



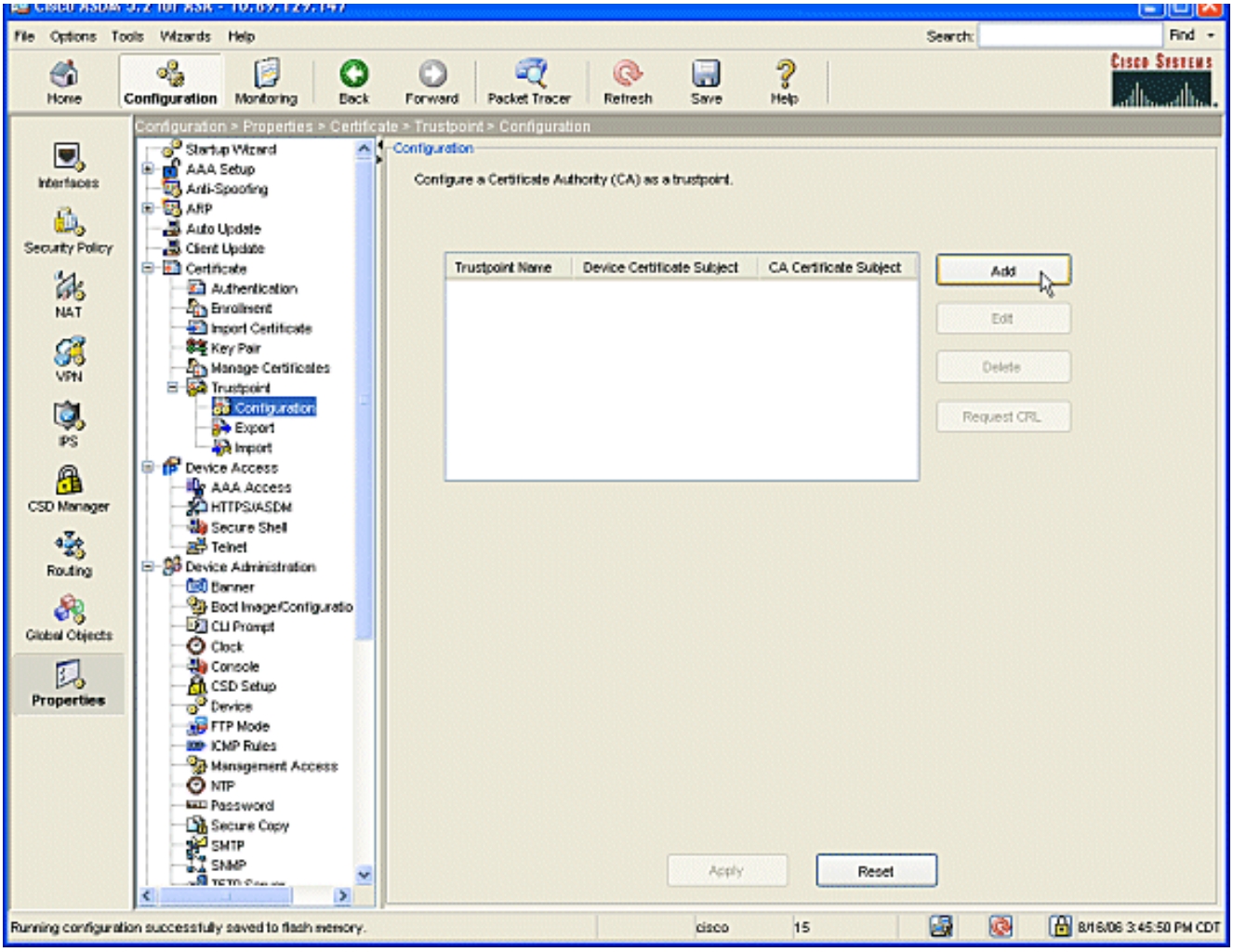
Haga clic el **botón Add**, y las visualizaciones del cuadro de diálogo de los pares de agregar



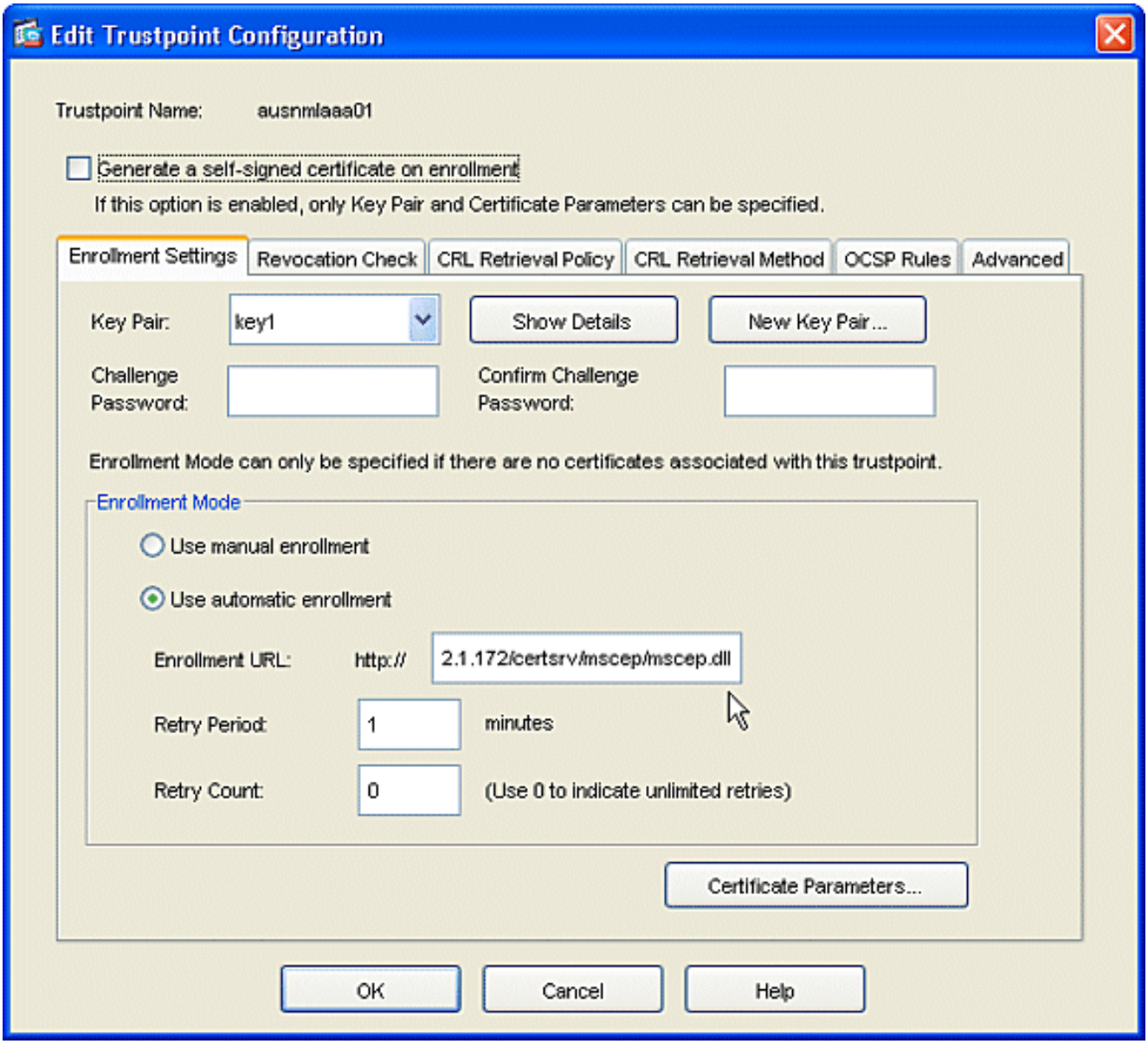
clave.Marque el botón de radio al lado del campo vacío del área del **nombre**, y teclee adentro el nombre para la clave.Haga clic el **tamaño:** flecha por la casilla desplegable para elegir un tamaño para la clave, o para validar el valor por defecto.Marque el botón de radio **de fines generales** bajo uso.Haga clic la **generación ahora** abotonan para regenerar las claves y para volver a la ventana del par clave, donde usted puede ver la información para el par clave.



4. Configure Microsoft CA que se considerará digno de confianza. Del SCR_INVALID, haga clic el **trustpoint > la configuración**.De la ventana de configuración, haga clic el **botón Add**.

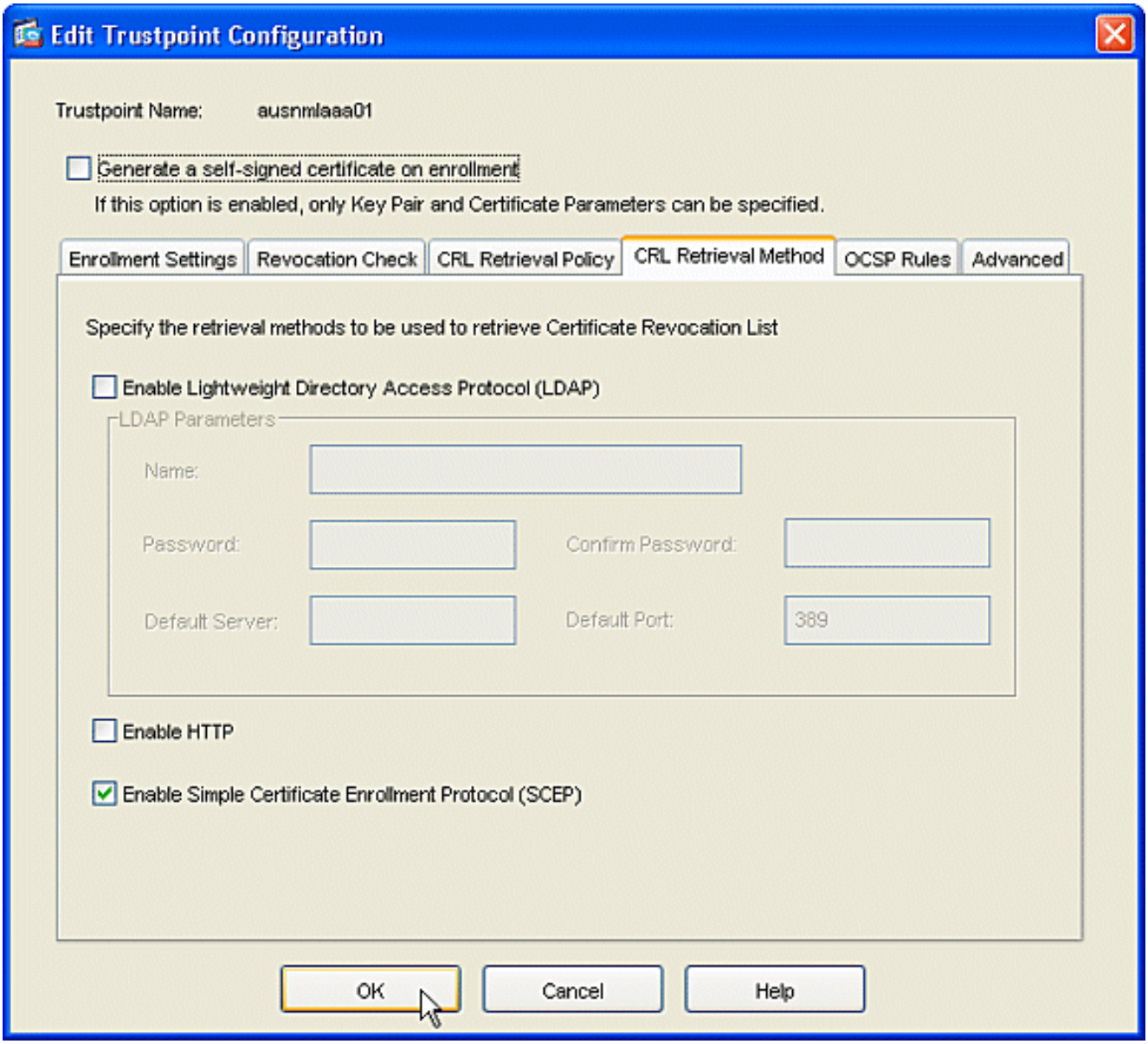


Las visualizaciones de la ventana de configuración del trustpoint del editar.

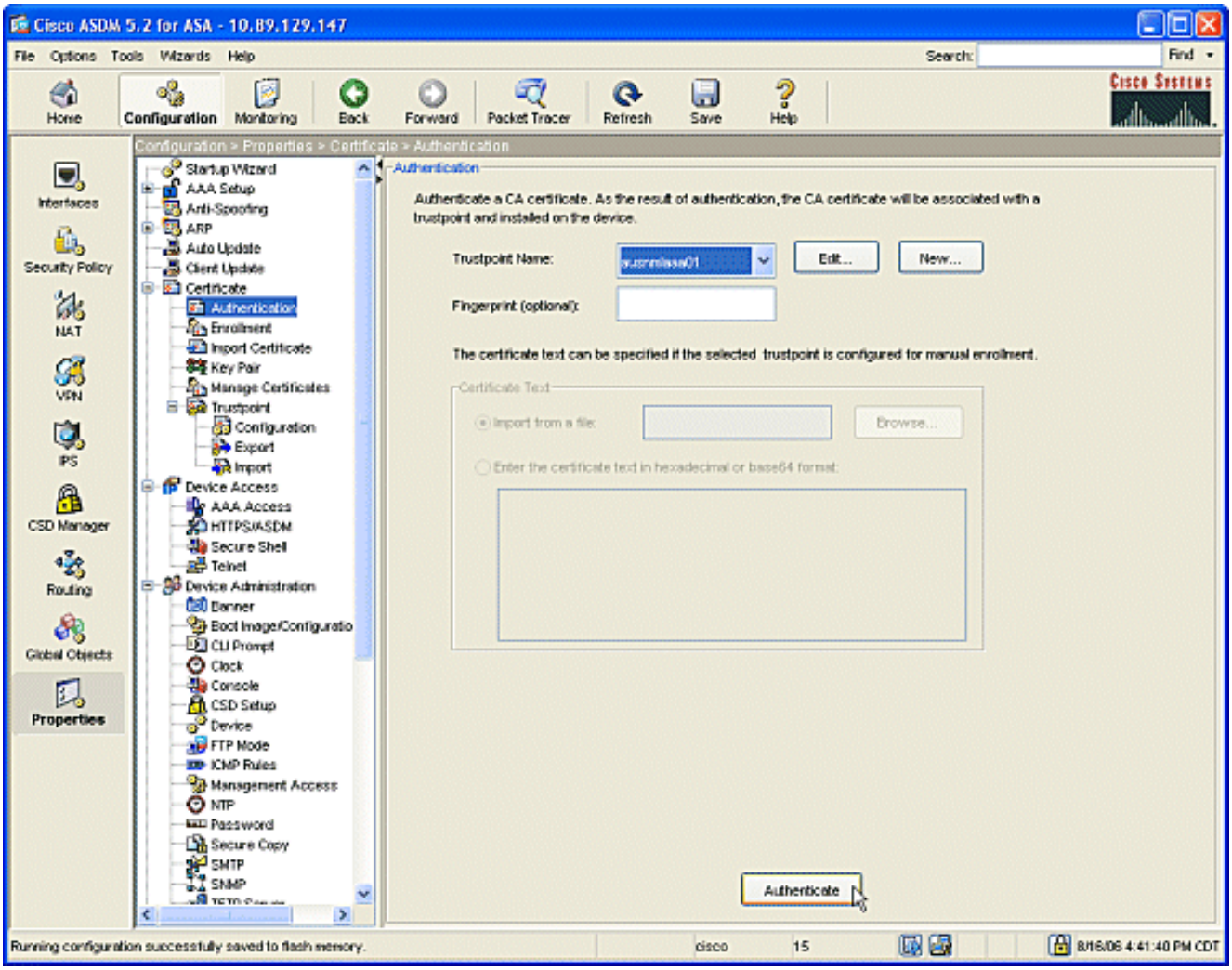


Complete un nombre para el trustpoint del nombre de CA.Haga clic el **par clave:** la flecha por la casilla desplegable, y elige el nombre del par clave que usted creó.Marque el botón de radio del **enlistamiento automático del uso**, y ingrese el URL para el Microsoft CA: **http://CA_IP_Address/certsrv/mscep/mscep.dll**.

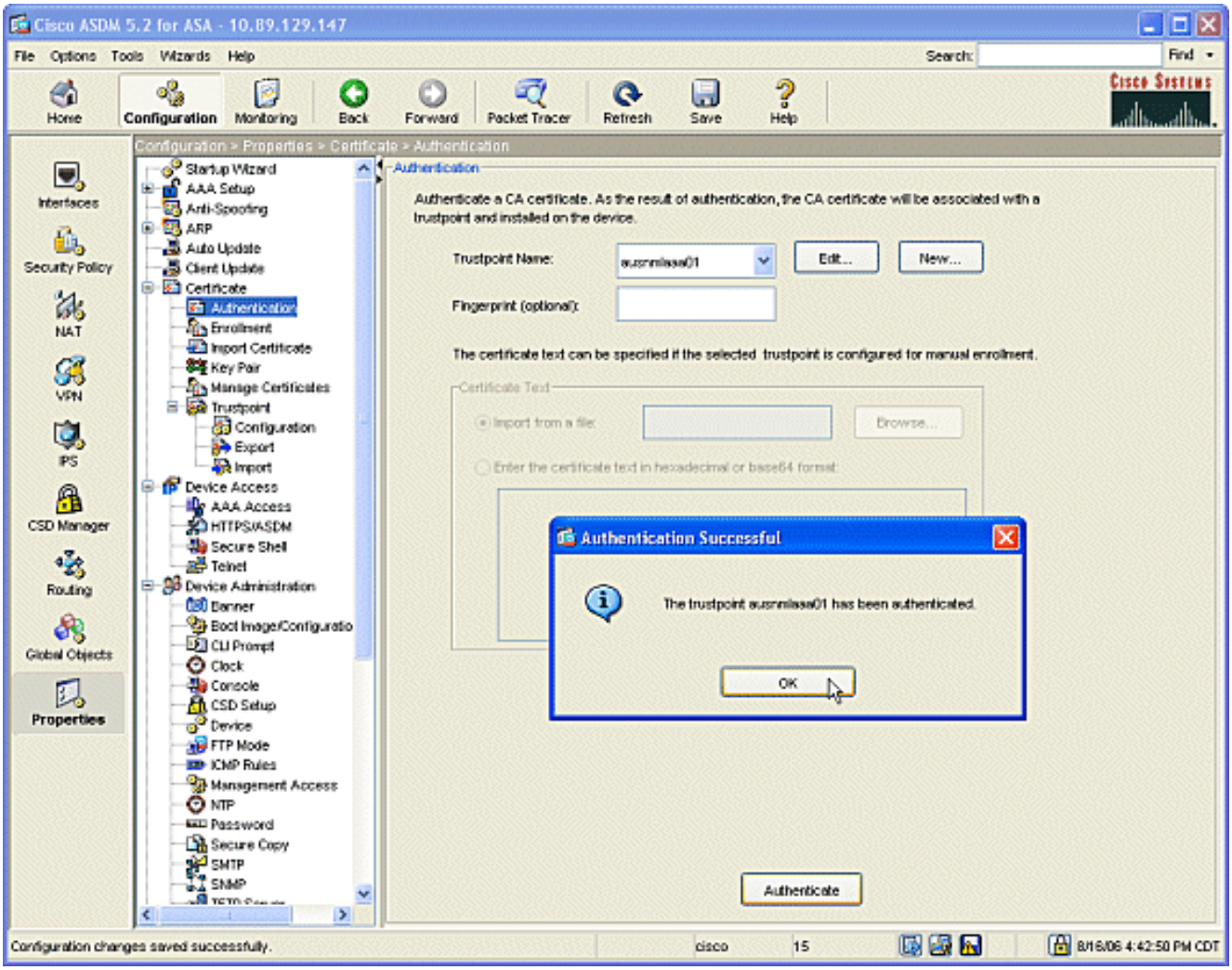
5. Haga clic la lengueta del **método de la extracción del crl**.Desmarque el permiso HTTP y habilite las casillas de verificación del Lightweight Directory Access Protocol (LDAP).Marque la casilla de verificación del protocolo simple certificate enrollment del permiso (SCEP). Deje el resto de las fijaciones del tabulador en sus configuraciones predeterminadas.Haga clic en el botón OK
(Aceptar)



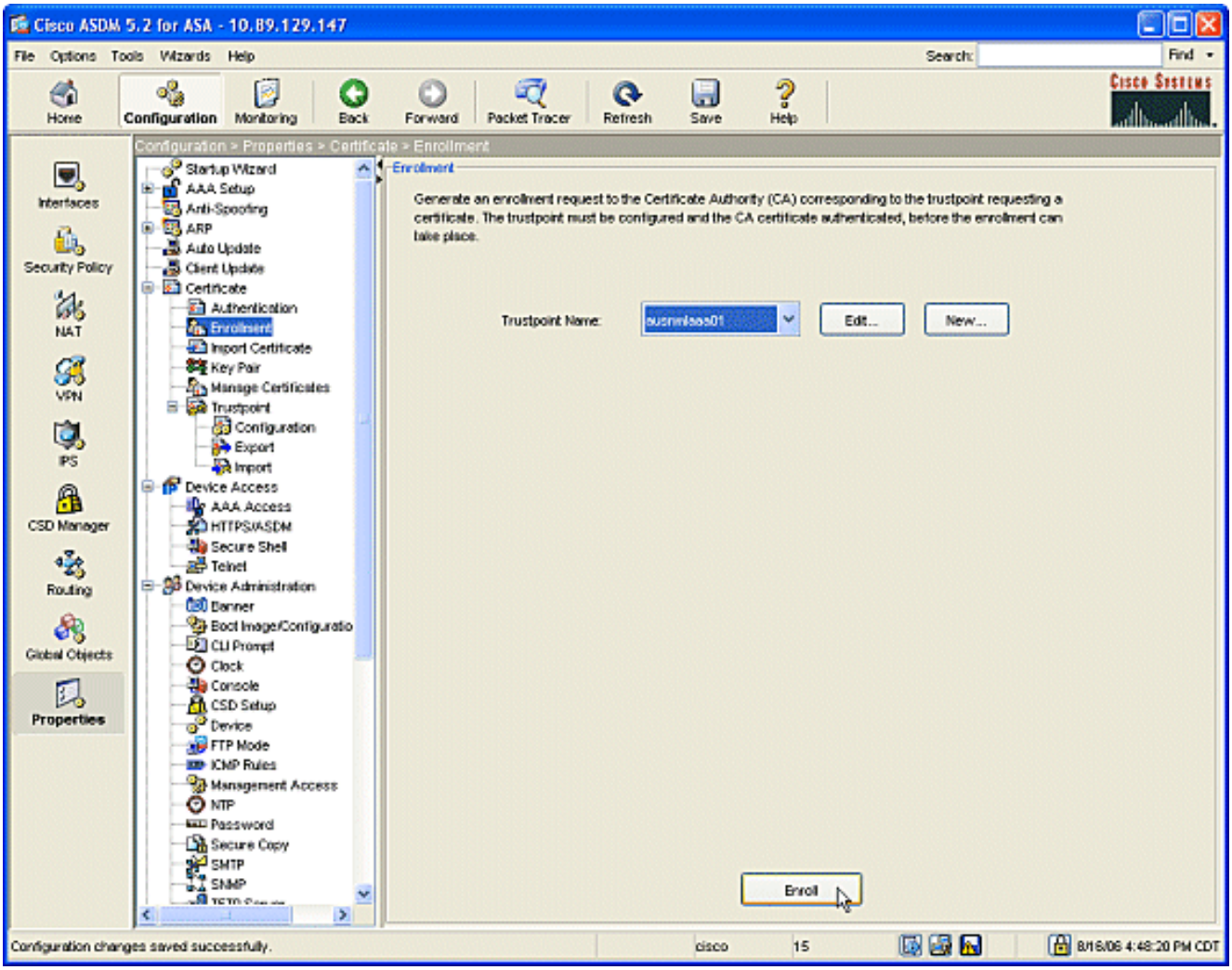
6. Autentique y aliste con Microsoft CA. Del SCR_INVALID, haga clic el **certificado > la autenticación**. Aseegurese el demostraciones creadas recientemente del trustpoint en el **nombre del trustpoint:** campo. Haga clic el botón de la **autenticidad**.



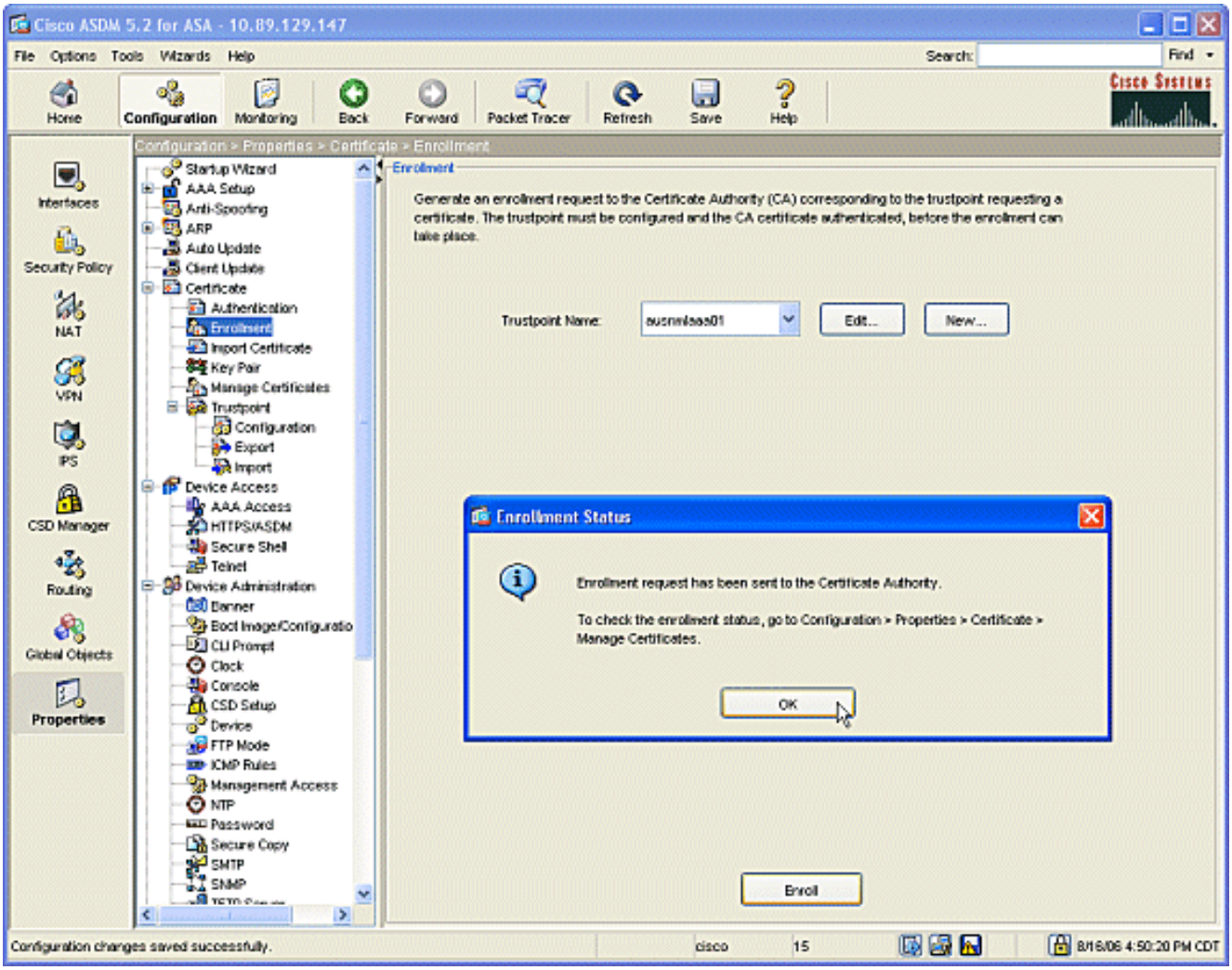
7. Visualizaciones de un cuadro de diálogo para informarle que se ha autenticado el trustpoint. Haga clic en el botón OK
(Aceptar)



8. Del SCR_INVALID, haga clic la **inscripción**. Aseegurese las visualizaciones del nombre del trustpoint en el campo de nombre del trustpoint, y haga clic el botón del **alistar**.



9. Visualizaciones de un cuadro de diálogo para informarle que la petición fue enviada al tecleo CA el **botón OK**.



Nota: En una máquina independiente de Microsoft Windows usted debe publicar los Certificados para cualquier petición que se haya sometido a CA. El certificado estará en un estado pendiente hasta que usted haga clic con el botón derecho del ratón el certificado y haga clic el problema en el servidor de Microsoft.

Resultados

Ésta es la configuración CLI esa los resultados de los pasos del ASDM:

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
```

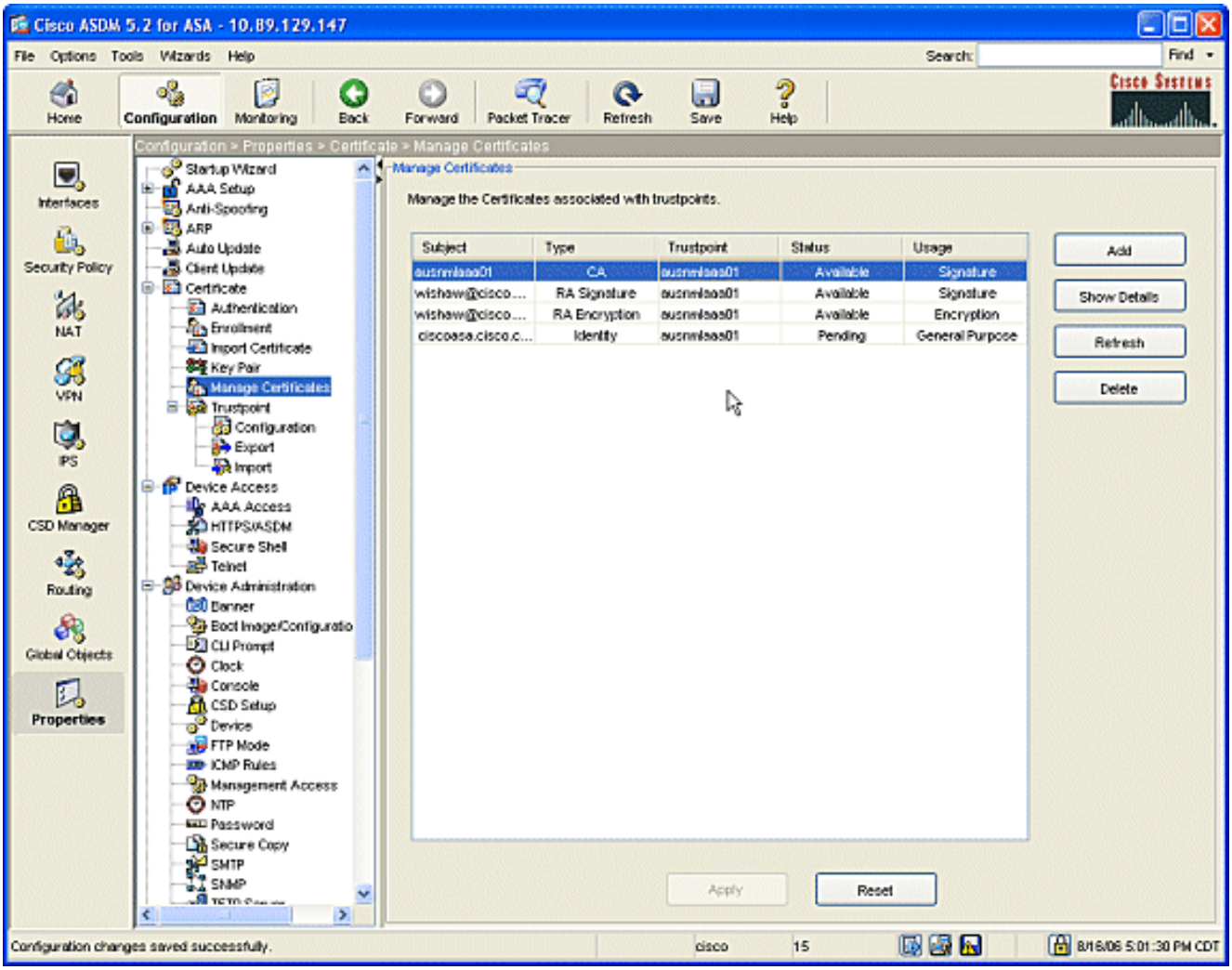
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Marque y maneje su certificado

Revise y maneje su certificado.

1. Abra la aplicación ASDM y haga clic el botón de la **configuración**.
2. Del menú izquierdo, haga clic el **botón properties**.Haga clic el **certificado**.El tecleo **maneja el certificado**.



Comandos

En el ASA usted puede utilizar varios **comandos show** en la línea de comando de verificar el estatus de un certificado.

- Utilizan al comando show crypto ca certificates de ver la información sobre su certificado, el certificado de CA, y cualquier Certificados del registration authority (RA).
- **El trustpoints del** comando show crypto **Ca** se utiliza para verificar la configuración del trustpoint.
- Utilizan al comando show crypto key mypubkey rsa de visualizar las claves públicas RSA de su ASA.
- Utilizan al comando show crypto ca crls de visualizar todos los CRL ocultados.

Nota: La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

Use esta sección para resolver problemas de configuración.

Refiera al Public Key Infrastructure para el Servidor Windows 2003 para más información sobre cómo resolver problemas Microsoft Windows 2003 CA.

Comandos

Nota: El uso de los **comandos debug** puede afectar negativamente su dispositivo de Cisco. Antes de que utilice los **comandos debug**, consulte Información Importante sobre los Comandos Debug.

Información Relacionada

- Configurar el Cisco VPN 3000 Concentrator 4.0.x para conseguir un certificado digital