Come ottenere un certificato digitale da una CA di Microsoft Windows utilizzando ASDM su un'appliance ASA

Sommario

Introduzione

I certificati digitali possono essere utilizzati per autenticare i dispositivi e gli utenti della rete. Possono essere utilizzati per negoziare sessioni IPSec tra nodi di rete.

I dispositivi Cisco si identificano in modo sicuro su una rete in tre modi principali:

1. **Chiavi già condivise**. Due o più dispositivi possono avere la stessa chiave privata condivisa. I peer si autenticano a vicenda tramite il calcolo e l'invio di un hash di dati con chiave che include la chiave già condivisa. Se il peer ricevente è in grado di creare lo stesso hash in modo indipendente utilizzando la propria chiave già condivisa, sa che entrambi i peer devono condividere lo stesso segreto, autenticando così l'altro peer. Questo metodo è manuale e non molto scalabile.
2. **Certificati autofirmati**. Un dispositivo genera il proprio certificato e lo firma come valido. Questo tipo di certificato deve avere un utilizzo limitato. L'utilizzo di questo certificato con l'accesso SSH e HTTPS a scopo di configurazione è un buon esempio. Per completare la connessione è necessaria una coppia nome utente/password separata.**Nota:** i certificati autofirmati persistenti sono validi dopo i ricaricamenti del router perché sono stati salvati

nella memoria ad accesso casuale non volatile (NVRAM) del dispositivo. per ulteriori informazioni, fare riferimento a Certificati autofirmati persistenti. Un buon esempio di utilizzo è rappresentato dalle connessioni SSL VPN (WebVPN).

3. **Certificato dell'Autorità di certificazione**. Una terza parte convalida e autentica i due o più nodi che tentano di comunicare. Ogni nodo dispone di una chiave pubblica e privata. La chiave pubblica crittografa i dati, mentre la chiave privata li decrittografa. Poiché i certificati sono stati ottenuti dalla stessa fonte, è possibile garantire loro l'identità. Il dispositivo ASA può ottenere un certificato digitale da terze parti con un metodo di registrazione manuale o automatico.**Nota:** il metodo e il tipo di certificato digitale scelto dipende dalle caratteristiche e dalle funzioni di ogni prodotto di terze parti. Per ulteriori informazioni, contattare il fornitore del servizio certificati.

Per autenticare le connessioni IPSec, le appliance Cisco Adaptive Security (ASA) possono utilizzare chiavi già condivise o certificati digitali forniti da un'Autorità di certificazione (CA) di terze parti. Inoltre, l'ASA può produrre il proprio certificato digitale autofirmato. Da utilizzare per le connessioni SSH, HTTPS e Cisco Adaptive Security Device Manager (ASDM) al dispositivo.

In questo documento vengono illustrate le procedure necessarie per ottenere automaticamente un certificato digitale da un'autorità di certificazione (CA) Microsoft per l'appliance ASA. Non include il metodo di iscrizione manuale. In questo documento viene usato ASDM per la configurazione e viene presentata la configurazione finale dell'interfaccia della riga di comando (CLI).

Per ulteriori informazioni sullo stesso scenario delle piattaforme Cisco IOS®, fare riferimento agli esempi di configurazione della registrazione di certificati Cisco IOS con comandi di registrazione avanzata.

Per ulteriori informazioni sullo stesso scenario con Cisco VPN 3000 Concentrator 4.7.x, consultare il documento sulla configurazione di Cisco VPN 3000 Concentrator 4.7.x per ottenere un certificato digitale e un certificato SSL.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

Requisiti per il dispositivo ASA

- Configurare Microsoft® Windows 2003 Server come CA.Fare riferimento alla documentazione Microsoft o a Infrastruttura a chiave pubblica per Windows Server 2003
- Per consentire la configurazione di Cisco ASA o PIX versione 7.x con Adaptive Security Device Manager (ASDM), consultare il documento sulla concessione dell'accesso HTTPS per ASDM.
- Installare il componente aggiuntivo per Servizi certificati (mscep.dll).
- Ottenere il file eseguibile (cepsetup.exe) del componente aggiuntivo dal componente aggiuntivo SCEP (Simple Certificate Enrollment Protocol) per Servizi certificati o il file mscep.dll dagli strumenti del Resource Kit di Windows Server 2003 .**Nota:** configurare la data, l'ora e il fuso orario corretti nel computer con Microsoft Windows. L'utilizzo del protocollo NTP (Network Time Protocol) è fortemente consigliato ma non necessario.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Adaptive Security Appliance, versione software 7.x e successive
- Cisco Adaptive Security Device Manager versione 5.x e successive
- Autorità di certificazione di Microsoft Windows 2003 Server

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance versione 7.x.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione dell'appliance ASA per scambiare certificati con la CA Microsoft

Attività

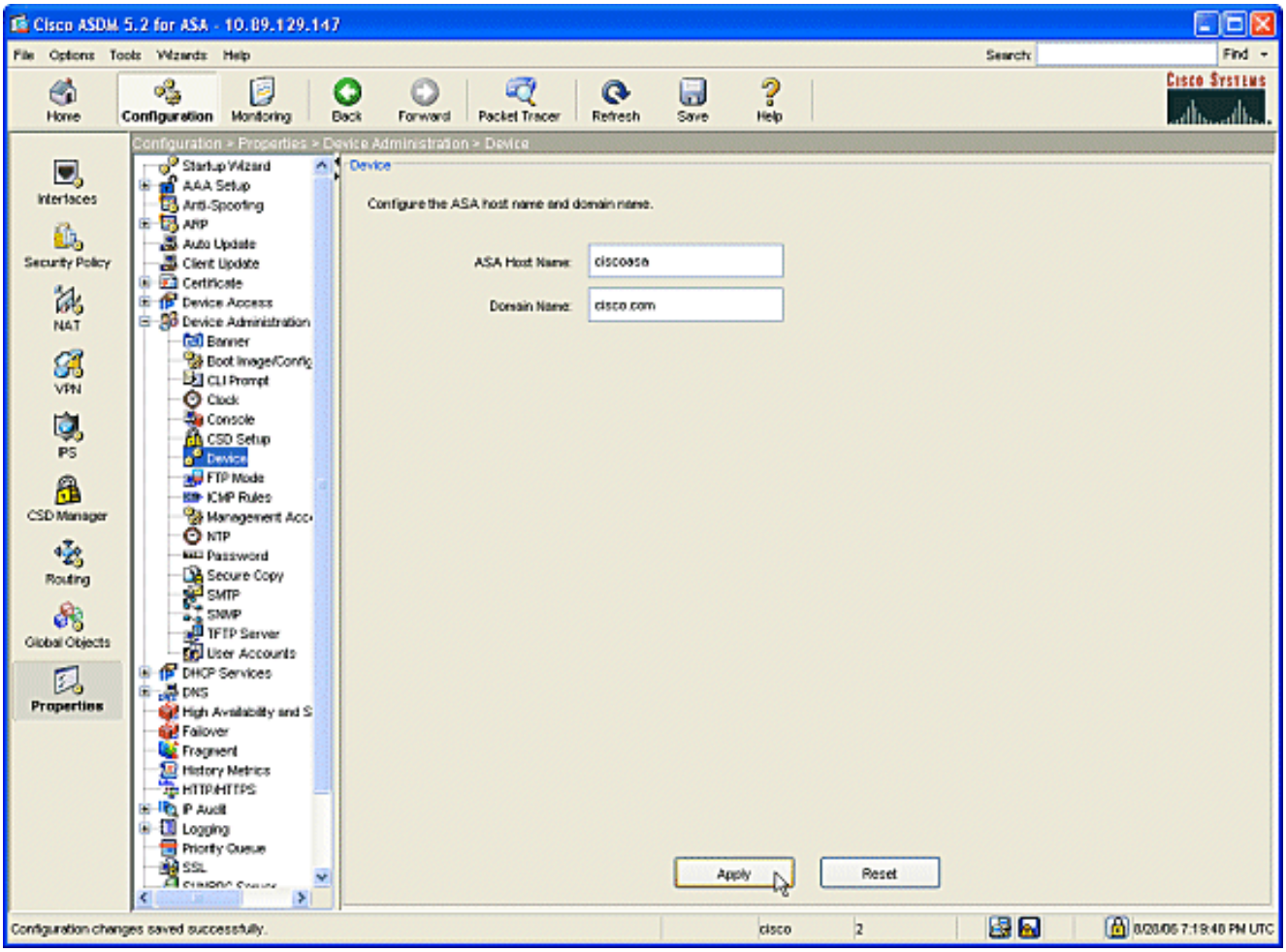
In questa sezione viene illustrato come configurare l'appliance ASA per ricevere un certificato da Microsoft Certificate Authority.

Istruzioni per la configurazione dell'ASA

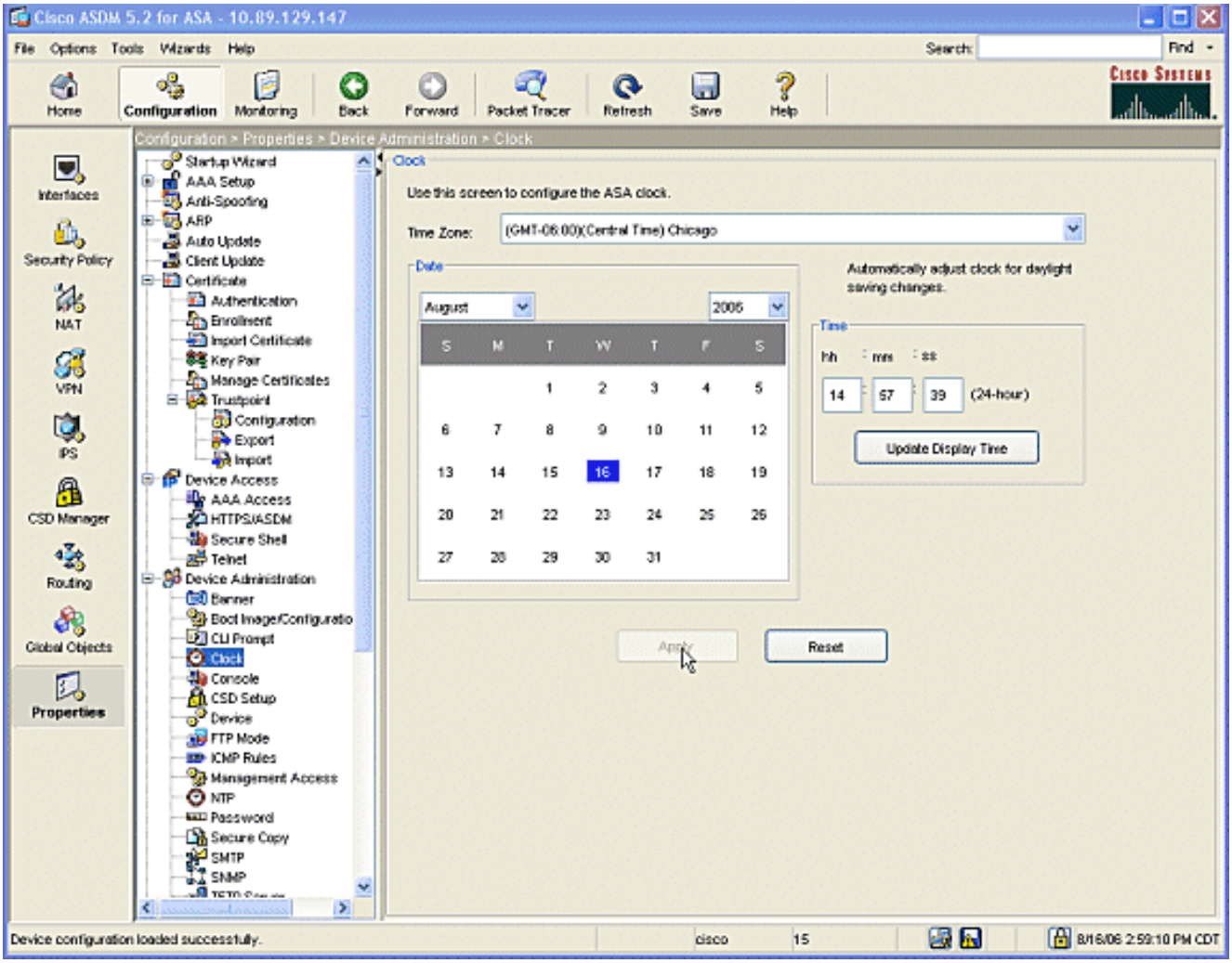
I certificati digitali utilizzano il componente data/ora/fuso orario come uno dei controlli per la validità dei certificati. È essenziale configurare la CA Microsoft e tutti i dispositivi con la data e l'ora corrette. L'autorità di certificazione Microsoft utilizza un componente aggiuntivo (mscep.dll) per i servizi certificati per condividere i certificati con i dispositivi Cisco.

Per configurare l'ASA, attenersi alla procedura seguente:

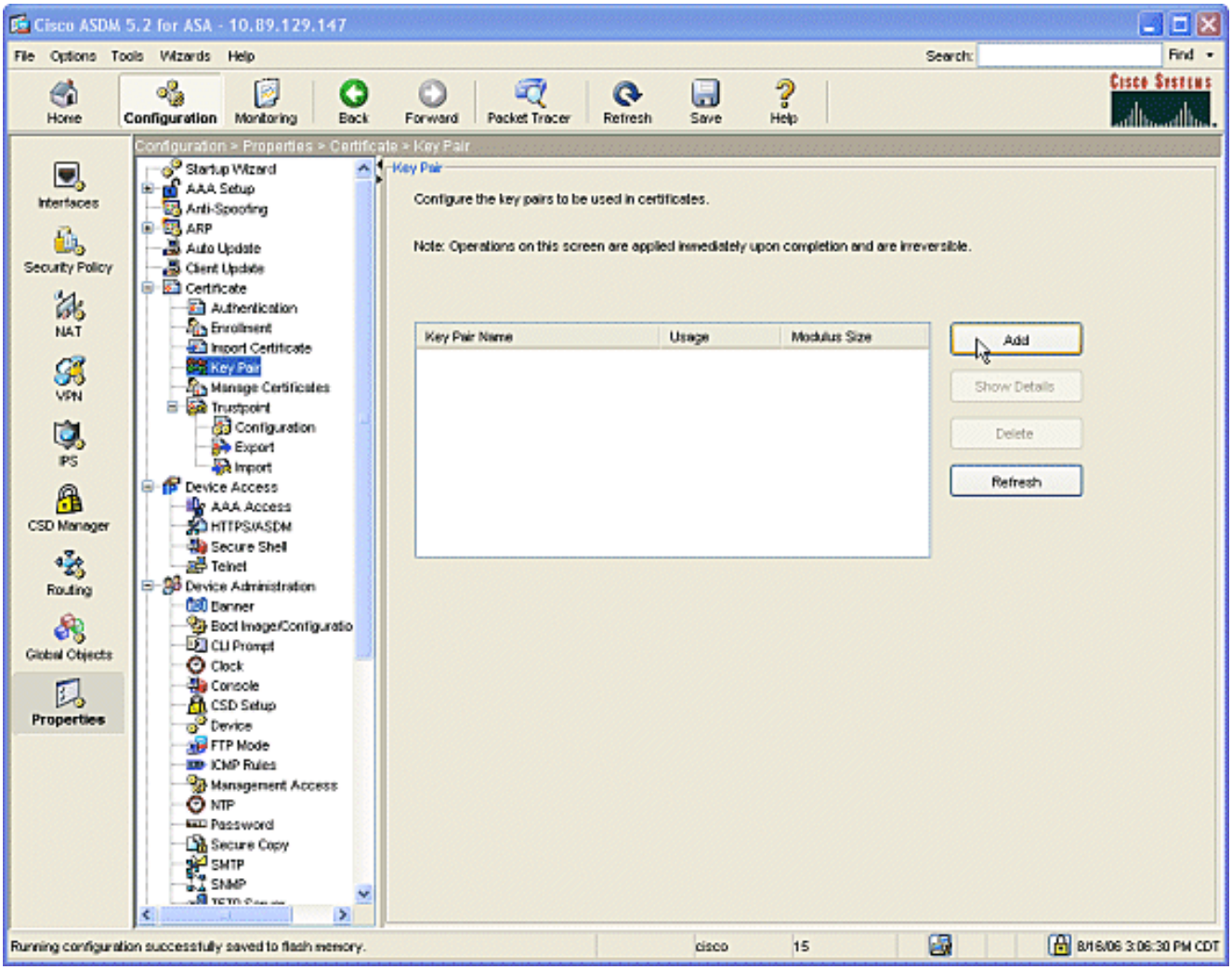
1. Aprire l'applicazione ASDM e fare clic sul pulsante **Configurazione**.Dal menu a sinistra, fare clic sul pulsante **Proprietà**.Nel riquadro di navigazione, fare clic su **Amministrazione periferica > Periferica**.Immettere il nome dell'host e il nome di dominio per l'appliance ASA. Fare clic su **Apply** (Applica).Quando richiesto, fate clic su **Salva (Save) > Sì (Yes)**.



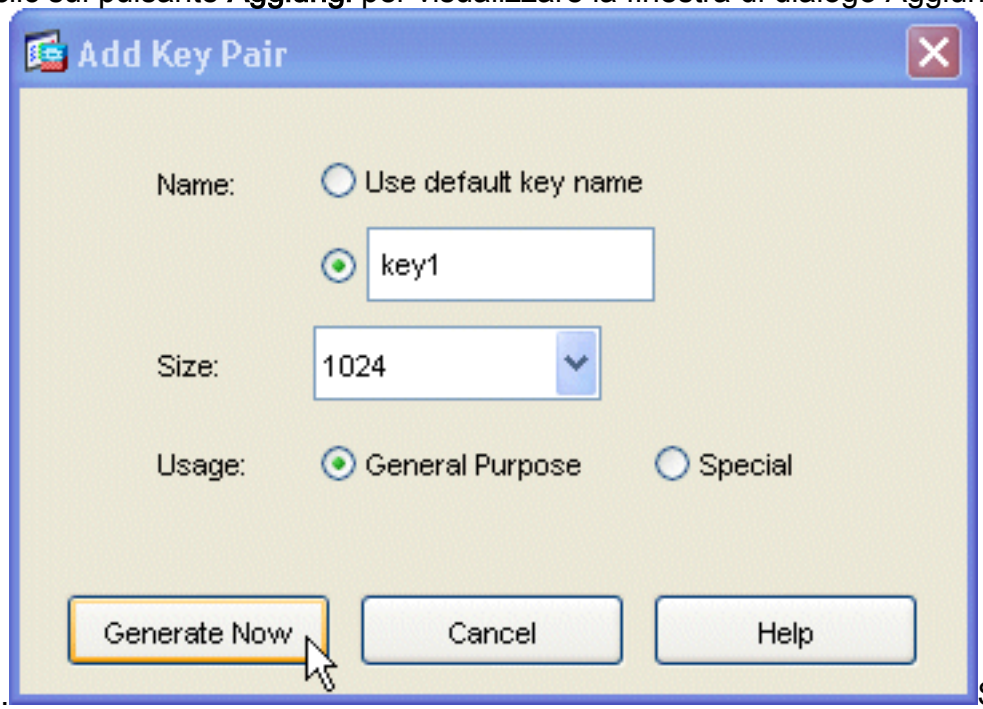
2. Configurare l'ASA con la data, l'ora e il fuso orario corretti. Questa operazione è importante per la generazione del certificato del dispositivo. Se possibile, utilizzare un server NTP.Nel riquadro di navigazione, fare clic su **Amministrazione periferica > Orologio**.Nella finestra Orologio, utilizzare i campi e le frecce a discesa per impostare la data, l'ora e il fuso orario corretti.



3. L'appliance ASA deve avere una propria coppia di chiavi (chiavi privata e pubblica). La chiave pubblica verrà inviata alla CA Microsoft.Nel riquadro di spostamento fare clic su **Certificato > Coppia di chiavi**.

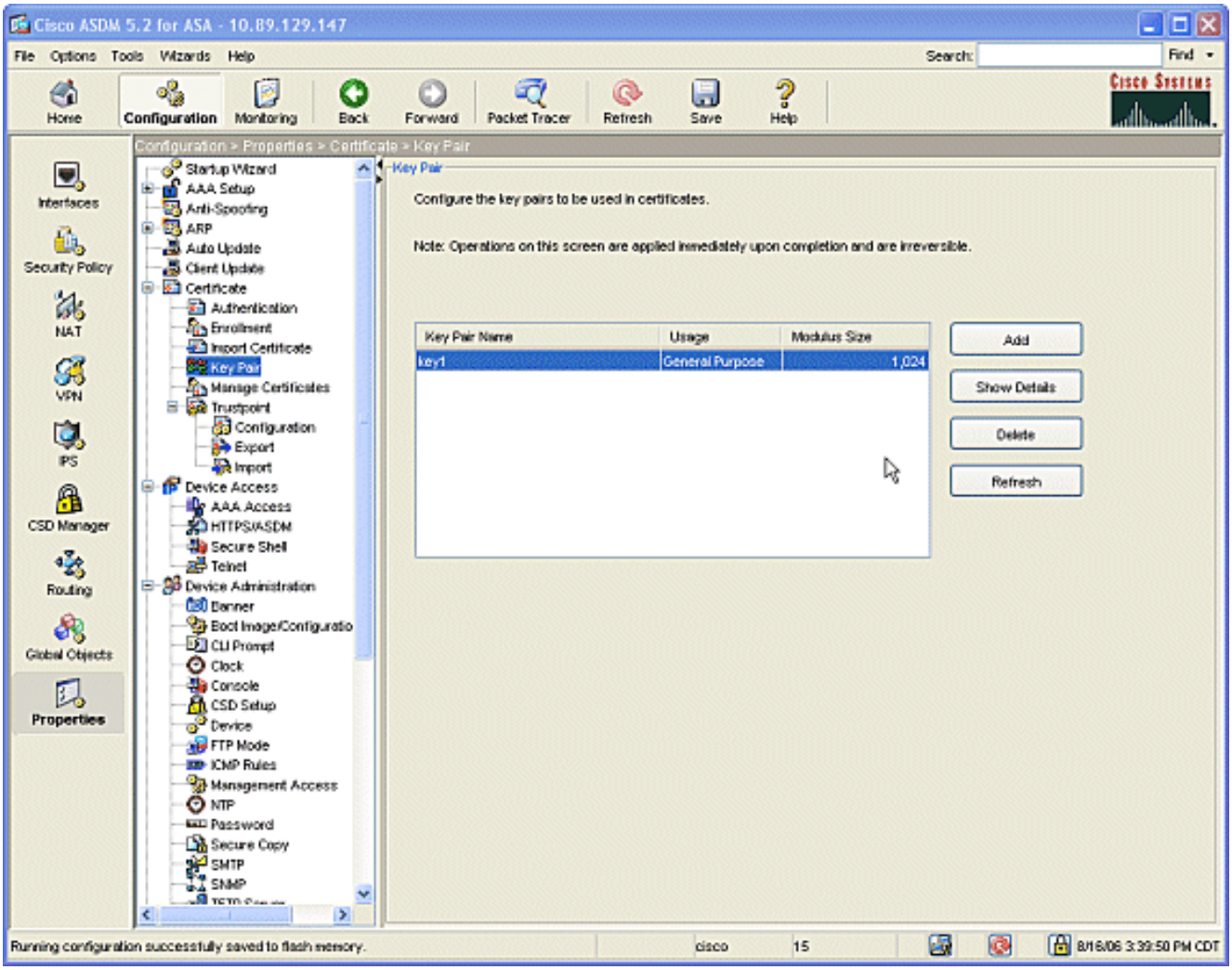


Fare clic sul pulsante **Aggiungi** per visualizzare la finestra di dialogo Aggiungi coppia di chiavi.

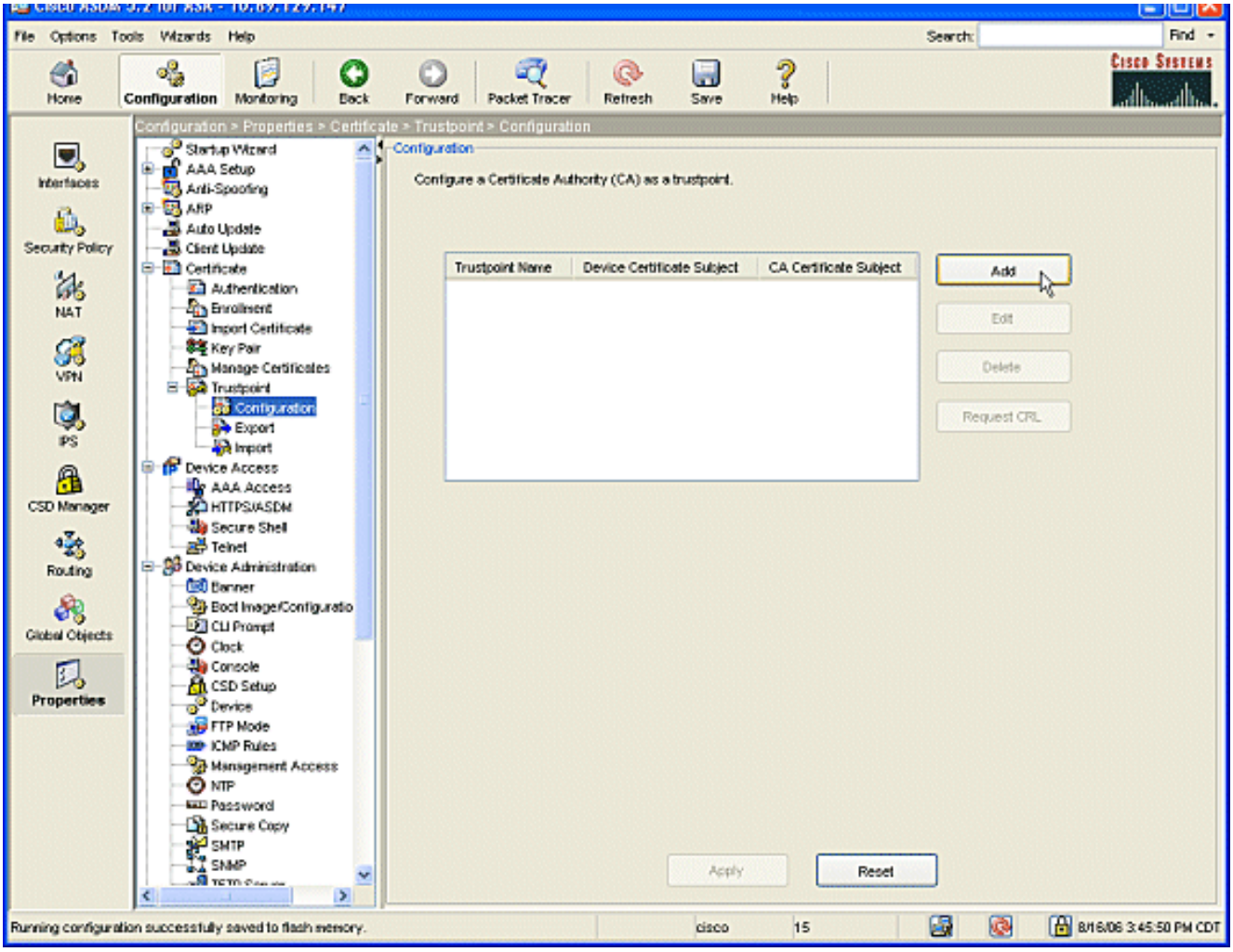


Selezionare il pulsante di opzione accanto al campo vuoto dell'area **Nome** e digitare il nome della chiave.Fare clic sul pulsante **Dimensioni:** nella casella di riepilogo a discesa per scegliere una dimensione per il tasto o accettare il valore predefinito.Selezionare il pulsante di opzione **Scopo generale** in Uso.Fare clic sul pulsante **Genera adesso** per rigenerare le chiavi e tornare alla finestra Coppia di chiavi, in cui è possibile visualizzare le informazioni relative alla coppia di

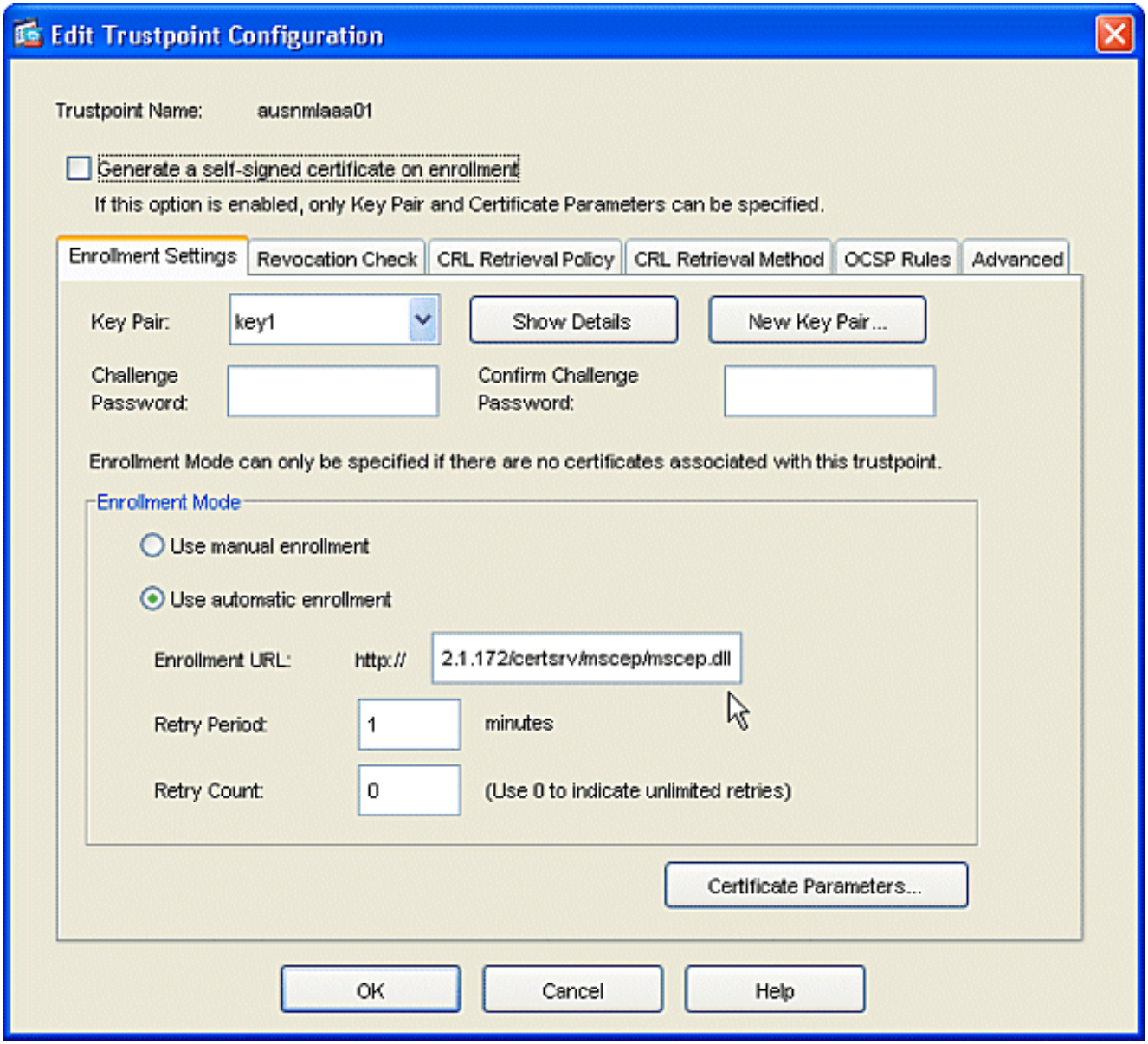
chiavi.



4. Configurare la CA Microsoft in modo che sia considerata attendibile. Nel riquadro di spostamento fare clic su **Punto di trust > Configurazione**.Dalla finestra Configuration, fare clic sul pulsante
Add.

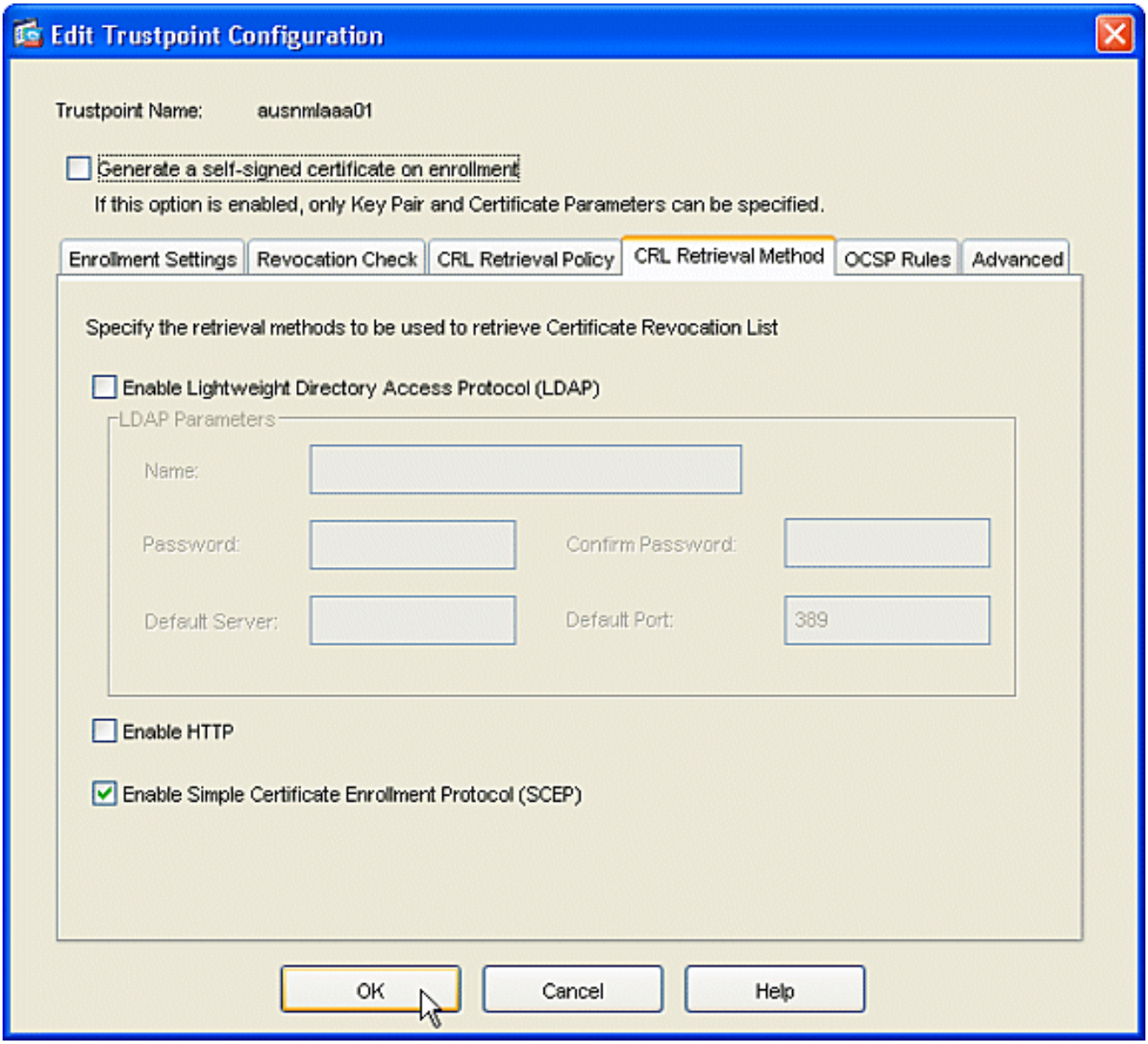


Verrà visualizzata la finestra Modifica configurazione trust point.

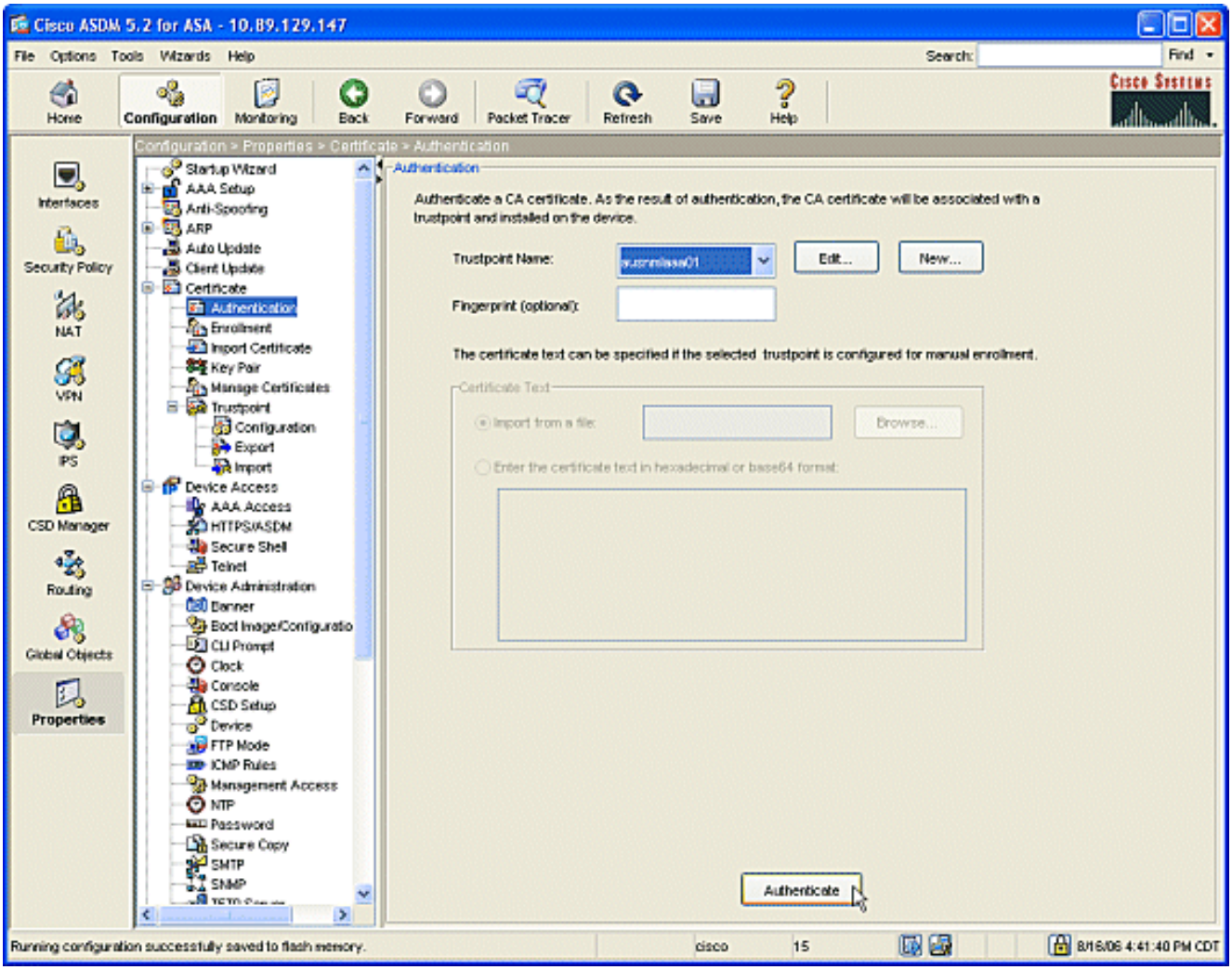


Specificare il nome del trust point con il nome della CA.Fare clic sulla **coppia di chiavi:** nella casella di riepilogo a discesa e scegliere il nome della coppia di chiavi creata.Selezionare il pulsante di opzione **Usa registrazione automatica** e immettere l'URL per la CA Microsoft: **http://CA_IP_Address/certsrv/mscep/mscep.dll**.

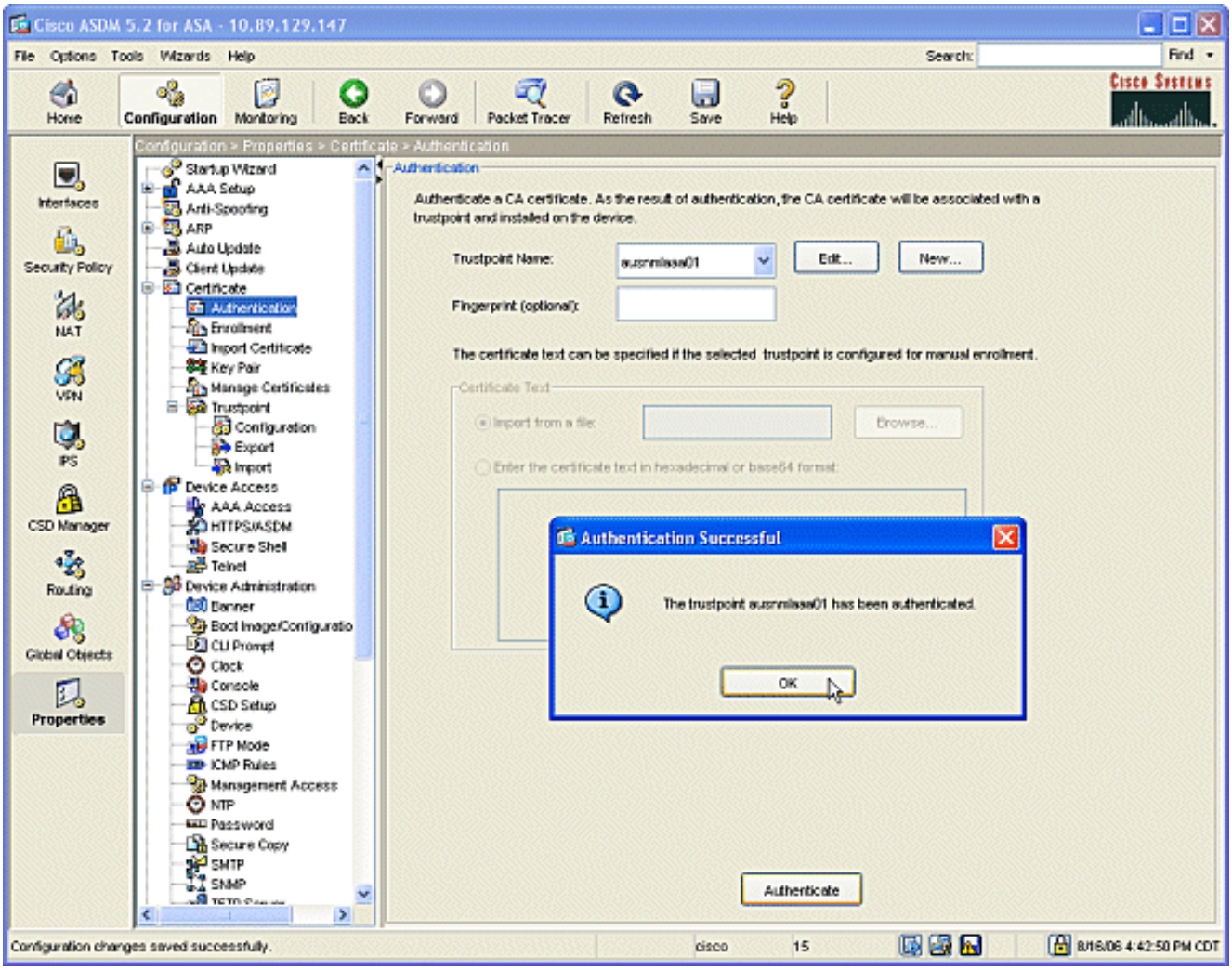
5. Fare clic sulla scheda **Crl Retrieval Method (Metodo di recupero crl)**.Deselezionare le caselle di controllo Abilita HTTP e Abilita LDAP (Lightweight Directory Access Protocol).Selezionare la casella di controllo Abilita SCEP (Simple Certificate Enrollment Protocol). Mantenere le altre impostazioni di tabulazione predefinite.Fare clic sul pulsante **OK**.



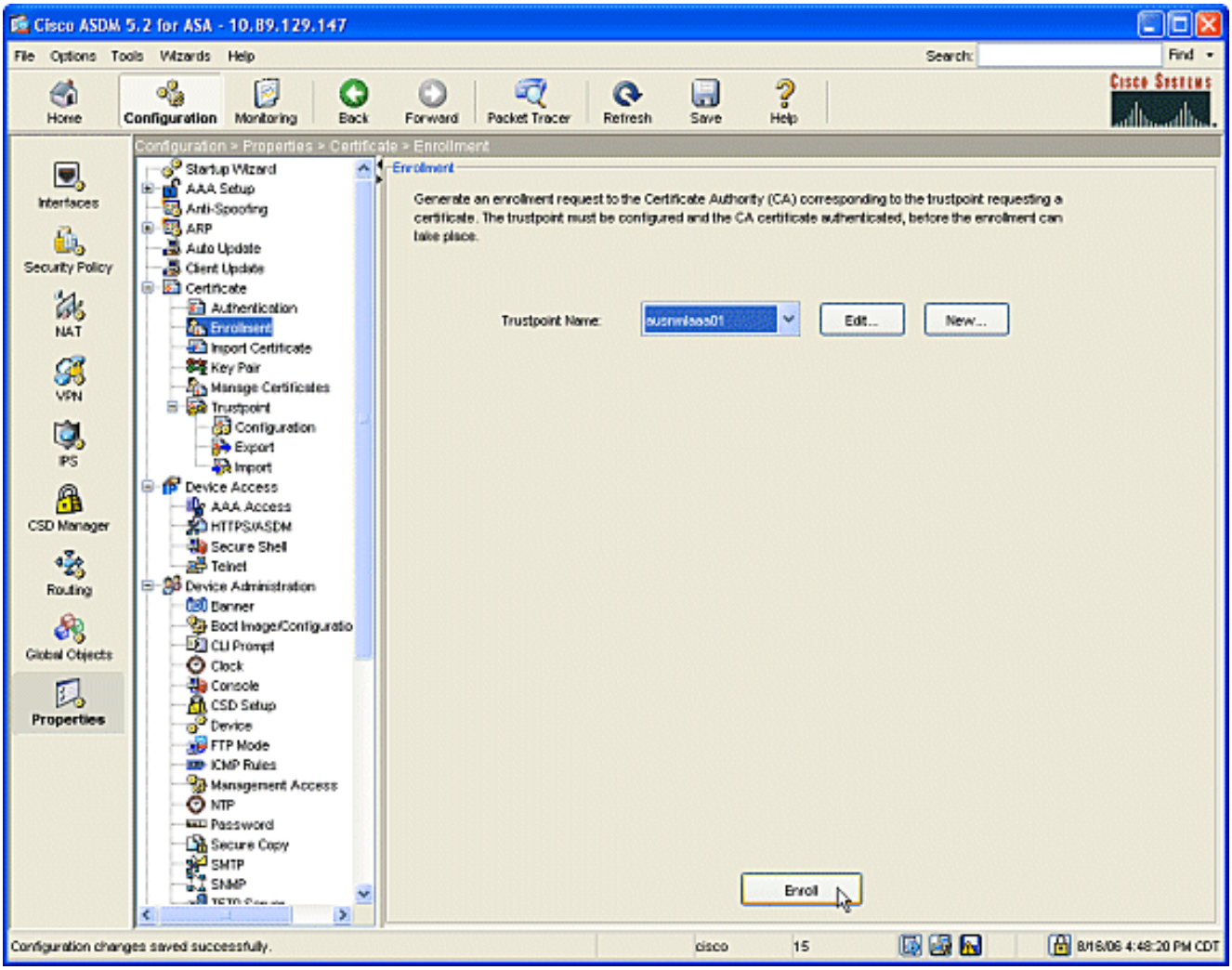
6. Autenticazione e registrazione con la CA Microsoft. Nel riquadro di spostamento fare clic su **Certificato > Autenticazione**. Verificare che il nuovo punto di trust venga visualizzato in **Nome punto di trust:** campo. Fare clic sul pulsante **Autentica**.



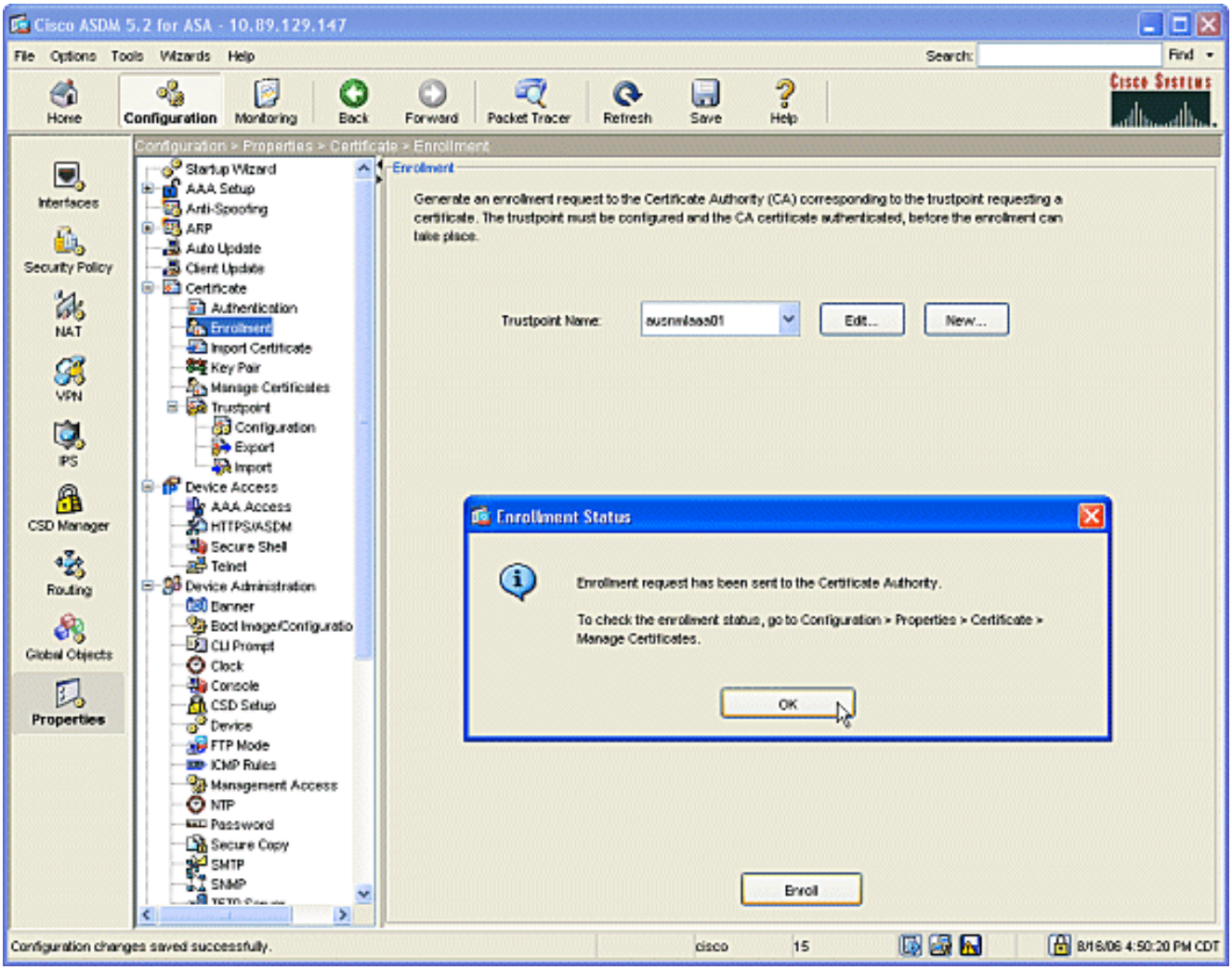
7. Verrà visualizzata una finestra di dialogo per informare che il trust point è stato autenticato. Fare clic sul pulsante
OK.



8. Nel riquadro di spostamento fare clic su **Registrazione**. Assicurarsi che il nome del trust point venga visualizzato nel campo Nome trust point e fare clic sul pulsante **Registra**.



9. Verrà visualizzata una finestra di dialogo per informare che la richiesta è stata inviata alla CA. Fare clic sul pulsante
OK.



Nota: Su un computer autonomo Microsoft Windows è necessario rilasciare i certificati per tutte le richieste inviate alla CA. Il certificato sarà in sospeso finché non si fa clic con il pulsante destro del mouse sul certificato e si sceglie Problema in Microsoft Server.

Risultati

Questa è la configurazione CLI risultante dai passi 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
```

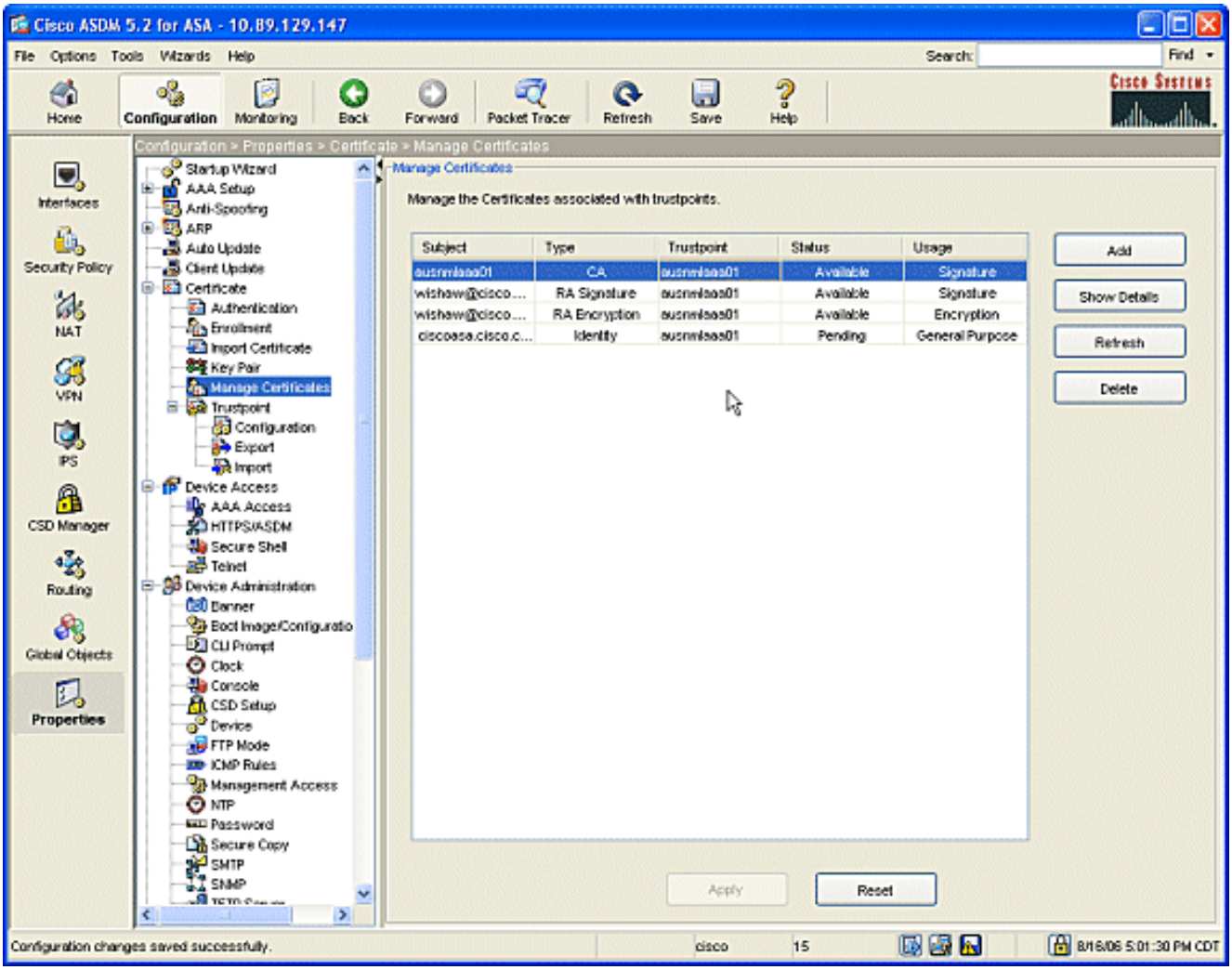
Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica e gestisci il certificato

Controllare e gestire il certificato.

1. Aprire l'applicazione ASDM e fare clic sul pulsante **Configurazione**.
2. Dal menu a sinistra, fare clic sul pulsante **Proprietà**.Fare clic su **Certificato**.Fare clic su **Gestisci certificato**.



Comandi

Sull'appliance ASA è possibile utilizzare diversi comandi **show** nella riga di comando per verificare lo stato di un certificato.

- Il comando **show crypto ca certificates** viene utilizzato per visualizzare le informazioni sul certificato, sul certificato CA e su qualsiasi certificato dell'Autorità di registrazione (RA).
- Il comando **show crypto ca trustpoints** viene utilizzato per verificare la configurazione del trust point.
- Il comando **show crypto key mypubkey rsa** viene usato per visualizzare le chiavi pubbliche RSA dell'appliance ASA.
- Il comando **show crypto ca crls** viene usato per visualizzare tutti i CRL memorizzati nella cache.

Nota: lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Per ulteriori informazioni su come risolvere i problemi relativi alla CA di Microsoft Windows 2003, fare riferimento a Infrastruttura a chiave pubblica per Windows Server 2003 .

Comandi

Nota: l'uso dei comandi di **debug** può avere un impatto negativo sul dispositivo Cisco. Prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Informazioni correlate

- Configurazione di Cisco VPN 3000 Concentrator 4.0.x per ottenere un certificato digitale