Comment obtenir un certificat numérique d'une autorité de certification Microsoft Windows à l'aide d'ASDM sur un dispositif ASA

Contenu

Introduction

Des certificats numériques peuvent être utilisés pour authentifier des périphériques et des utilisateurs de réseau sur le réseau. Ils peuvent être utilisés pour négocier des sessions IPSec entre les noeuds de réseau.

Les périphériques Cisco s'identifient en toute sécurité sur un réseau de trois manières principales :

1. **Clés pré-partagées**. Deux périphériques ou plus peuvent avoir la même clé secrète partagée. Les homologues s'authentifient mutuellement en calculant et en envoyant un hachage de données comportant la clé pré-partagée. Si l'homologue récepteur est capable de créer le même hachage indépendamment à l'aide de sa clé prépartagée, il sait que les deux homologues doivent partager le même secret, authentifiant ainsi l'autre homologue. Cette méthode est manuelle et pas très évolutive.
2. **Certificats auto-signés**. Un périphérique génère son propre certificat et le signe comme étant valide. Ce type de certificat doit avoir une utilisation limitée. L'utilisation de ce certificat avec accès SSH et HTTPS à des fins de configuration en sont de bons exemples. Une paire nom d'utilisateur/mot de passe distincte est nécessaire pour terminer la connexion.**Remarque :**

Les certificats auto-signés persistants survivent aux rechargements de routeur car ils sont enregistrés dans la mémoire vive non volatile (NVRAM) du périphérique. Référez-vous à Certificats auto-signés permanents pour plus d'informations. Un bon exemple d'utilisation est avec les connexions VPN SSL (WebVPN).

3. **Certificat d'autorité de certification**. Un tiers valide et authentifie les deux noeuds ou plus qui tentent de communiquer. Chaque noeud possède une clé publique et une clé privée. La clé publique chiffre les données et la clé privée les déchiffre. Comme ils ont obtenu leurs certificats de la même source, ils peuvent être assurés de leur identité respective. Le périphérique ASA peut obtenir un certificat numérique d'un tiers avec une méthode d'inscription manuelle ou une méthode d'inscription automatique.**Remarque :** La méthode d'inscription et le type de certificat numérique que vous choisissez dépendent des fonctionnalités et fonctions de chaque produit tiers. Pour plus d'informations, contactez le fournisseur du service de certificats.

L'appareil de sécurité adaptatif Cisco (ASA) peut utiliser des clés prépartagées ou des certificats numériques fournis par une autorité de certification tierce pour authentifier les connexions IPSec. En outre, l'ASA peut produire son propre certificat numérique autosigné. Il doit être utilisé pour les connexions SSH, HTTPS et Cisco Adaptive Security Device Manager (ASDM) au périphérique.

Ce document présente les procédures nécessaires pour obtenir automatiquement un certificat numérique auprès d'une autorité de certification Microsoft (AC) pour l'ASA. Il n'inclut pas la méthode manuelle d'inscription. Ce document utilise ASDM pour les étapes de configuration, ainsi que présente la configuration finale de l'interface de ligne de commande (CLI).

Référez-vous à Exemple de configuration de l'inscription des certificats Cisco IOS à l'aide des commandes d'inscription avancées afin d'en savoir plus sur le même scénario avec les plates-formes Cisco IOS®.

Référez-vous à Configuration du concentrateur Cisco VPN 3000 4.7.x pour obtenir un certificat numérique et un certificat SSL afin d'en savoir plus sur le même scénario avec le concentrateur Cisco VPN 3000.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

Exigences relatives au périphérique ASA

- Configurez Microsoft® Windows 2003 Server en tant qu'autorité de certification.Reportez-vous à votre documentation Microsoft ou à Infrastructure à clé publique pour Windows Server 2003
- Afin de permettre à Cisco ASA ou PIX Version 7.x d'être configuré par l'Adaptive Security Device Manager (ASDM), référez-vous à Autoriser l'accès HTTPS pour ASDM.
- Installez le module complémentaire pour les services de certificats (mscep.dll).
- Obtenez le fichier exécutable (cepsetup.exe) du module complémentaire à partir du module complémentaire SCEP (Simple Certificate Enrollment Protocol) pour les services de certificats ou du fichier mscep.dll à partir des outils du Kit de ressources Windows Server 2003.**Remarque :** configurez la date, l'heure et le fuseau horaire corrects sur l'ordinateur Microsoft Windows. L'utilisation du protocole NTP (Network Time Protocol) est fortement

recommandée, mais n'est pas nécessaire.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité adaptatif de la gamme Cisco ASA 5500, versions 7.x et ultérieures du logiciel
- Cisco Adaptive Security Device Manager version 5.x et ultérieure
- Autorité de certification Microsoft Windows 2003 Server

Produits connexes

Cette configuration peut également être utilisée avec l'Appliance de sécurité de la gamme Cisco PIX 500 version 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer l'ASA pour échanger des certificats avec l'autorité de certification Microsoft

Tâche

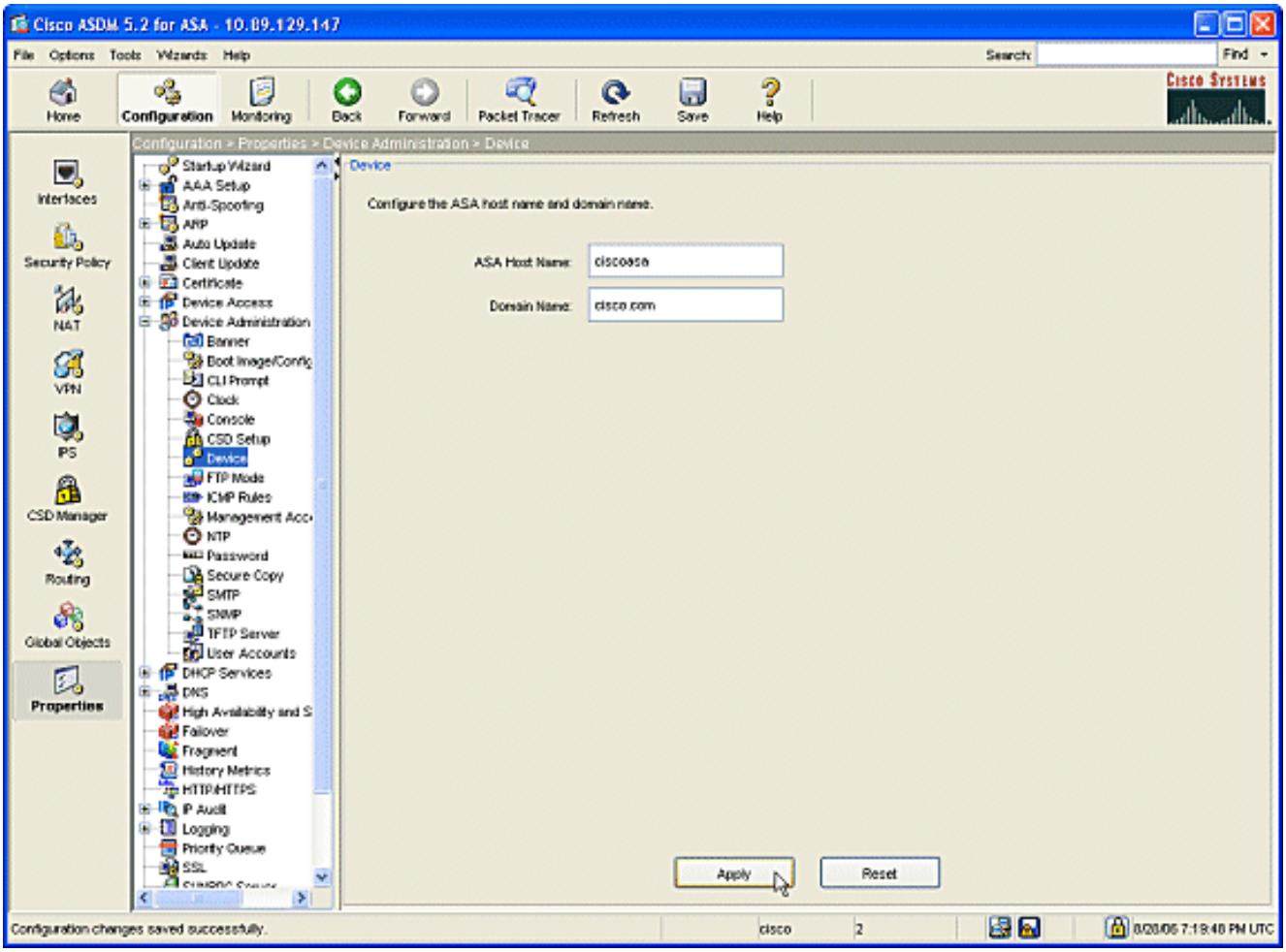
Dans cette section, vous voyez comment configurer l'ASA pour recevoir un certificat de l'autorité de certification Microsoft.

Instructions de configuration de l'ASA

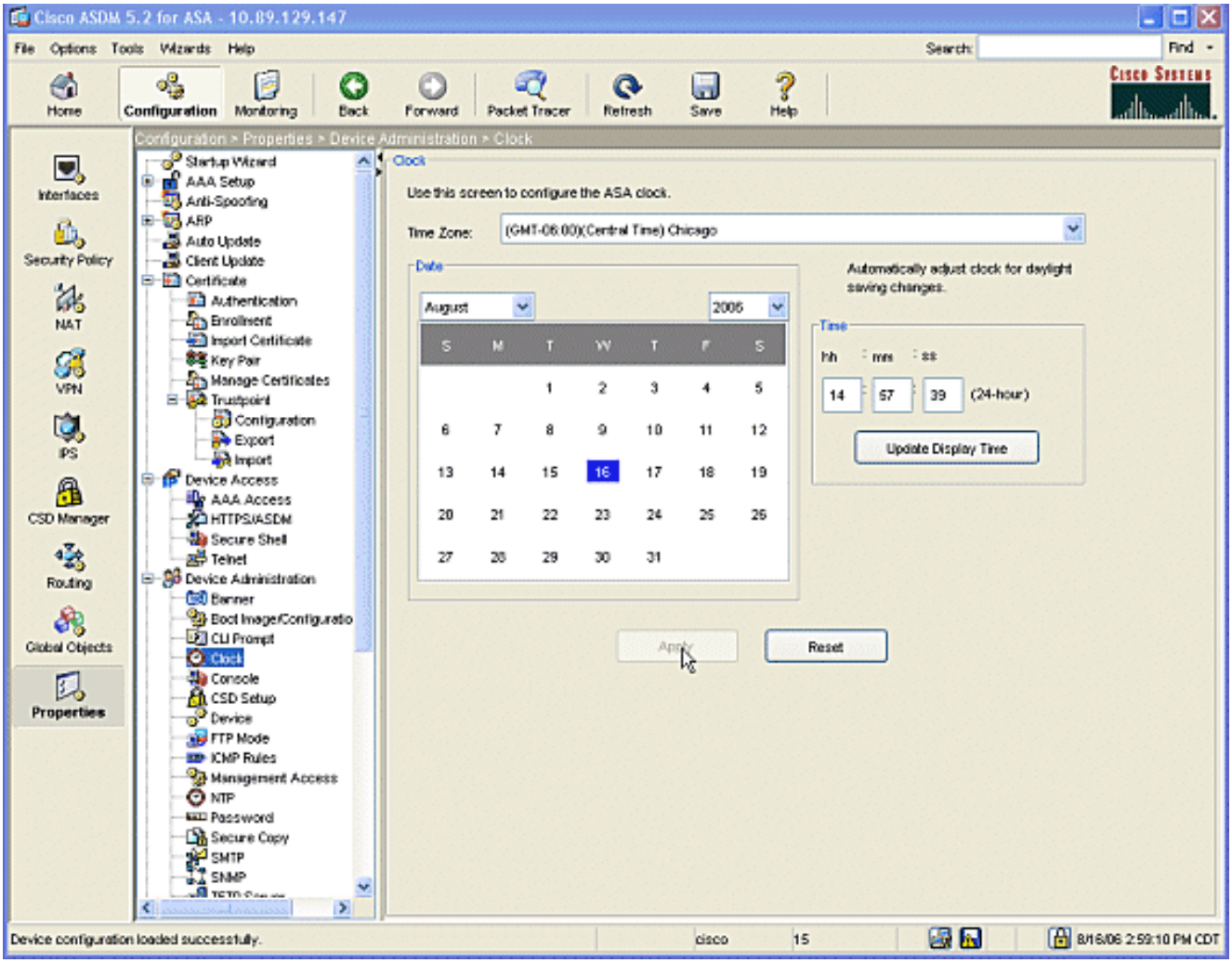
Les certificats numériques utilisent le composant date/heure/fuseau horaire comme un des contrôles de validité des certificats. Il est impératif de configurer l'autorité de certification Microsoft et tous vos périphériques avec la date et l'heure correctes. L'autorité de certification Microsoft utilise un module complémentaire (mscep.dll) à ses services de certificats afin de partager des certificats avec des périphériques Cisco.

Complétez ces étapes pour configurer ASA :

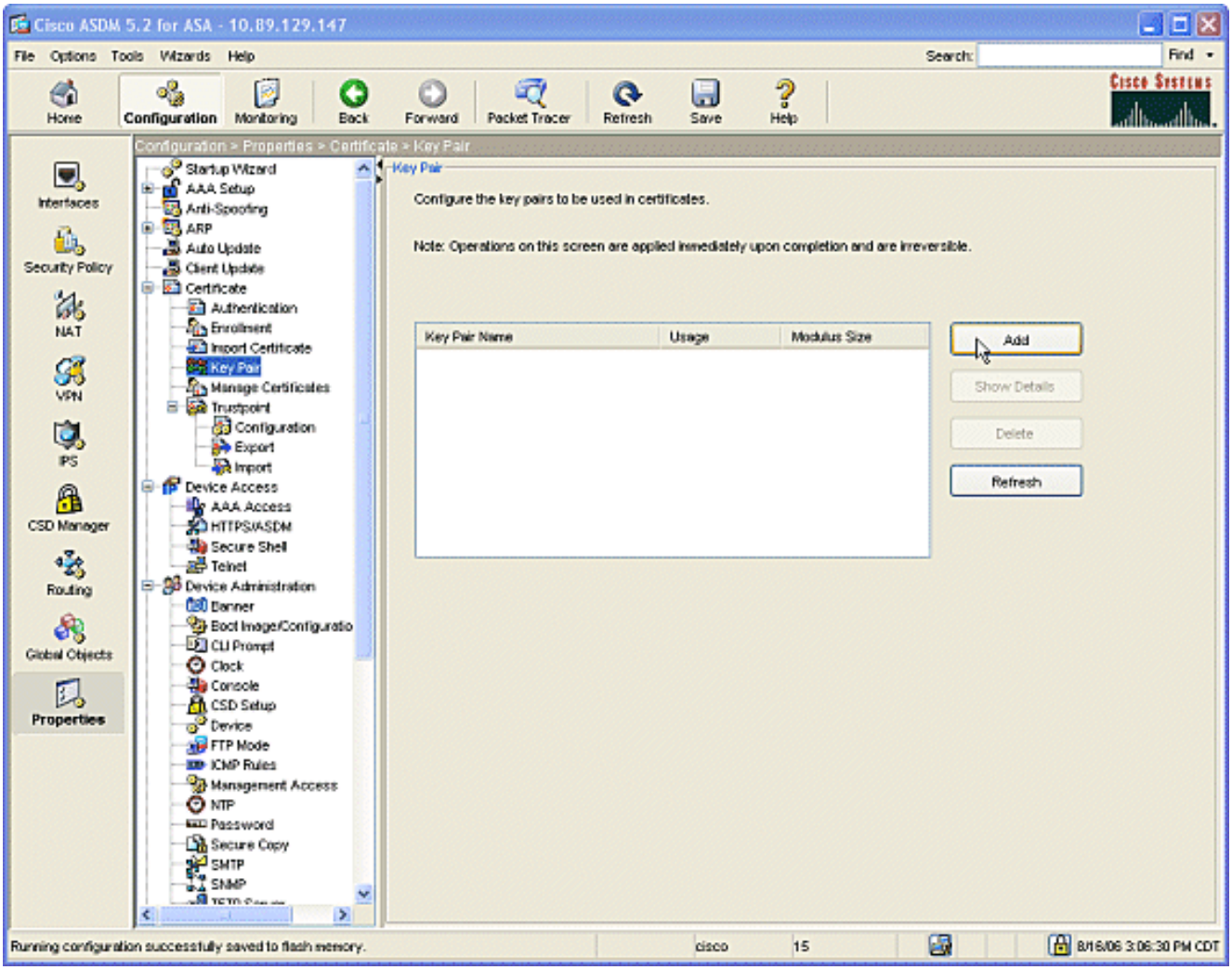
1. Ouvrez l'application ASDM et cliquez sur le bouton **Configuration**.Dans le menu de gauche, cliquez sur le bouton **Propriétés**.Dans le volet de navigation, cliquez sur **Device Administration > Device**.Saisissez un nom d'hôte et un nom de domaine pour l'ASA. Cliquez sur Apply.Lorsque vous y êtes invité, cliquez sur **Enregistrer > Oui**.



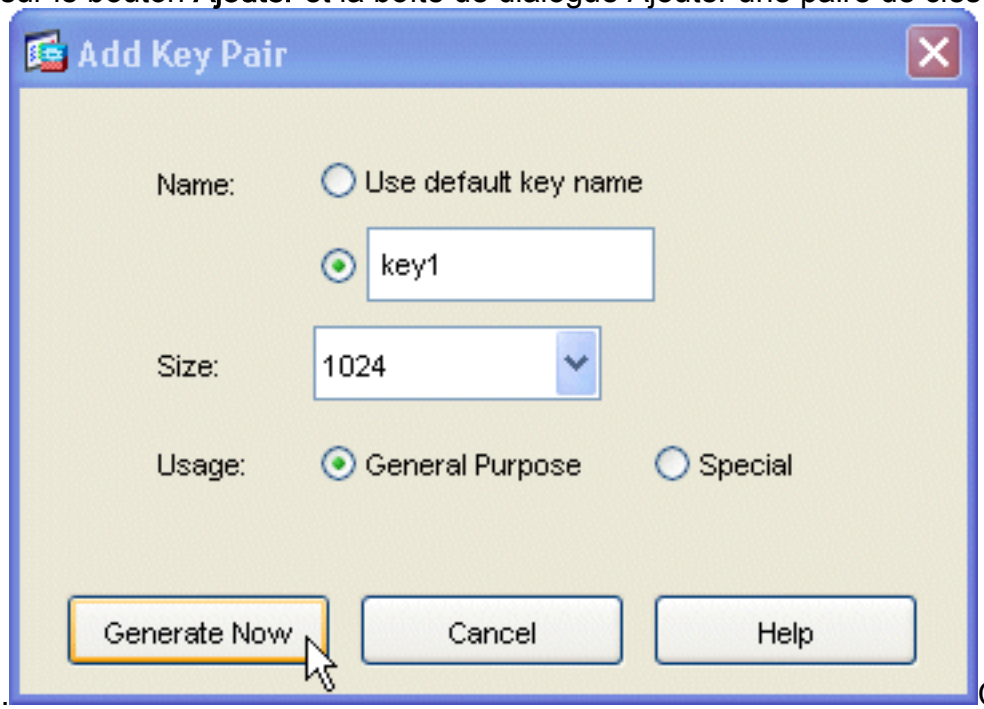
2. Configurez l'ASA avec la date, l'heure et le fuseau horaire corrects. Ceci est important pour la génération de certificats du périphérique. Utilisez un serveur NTP, si possible.Dans le volet de navigation, cliquez sur **Device Administration > Clock**.Dans la fenêtre Horloge, utilisez les champs et les flèches déroulantes pour définir la date, l'heure et le fuseau horaire corrects.



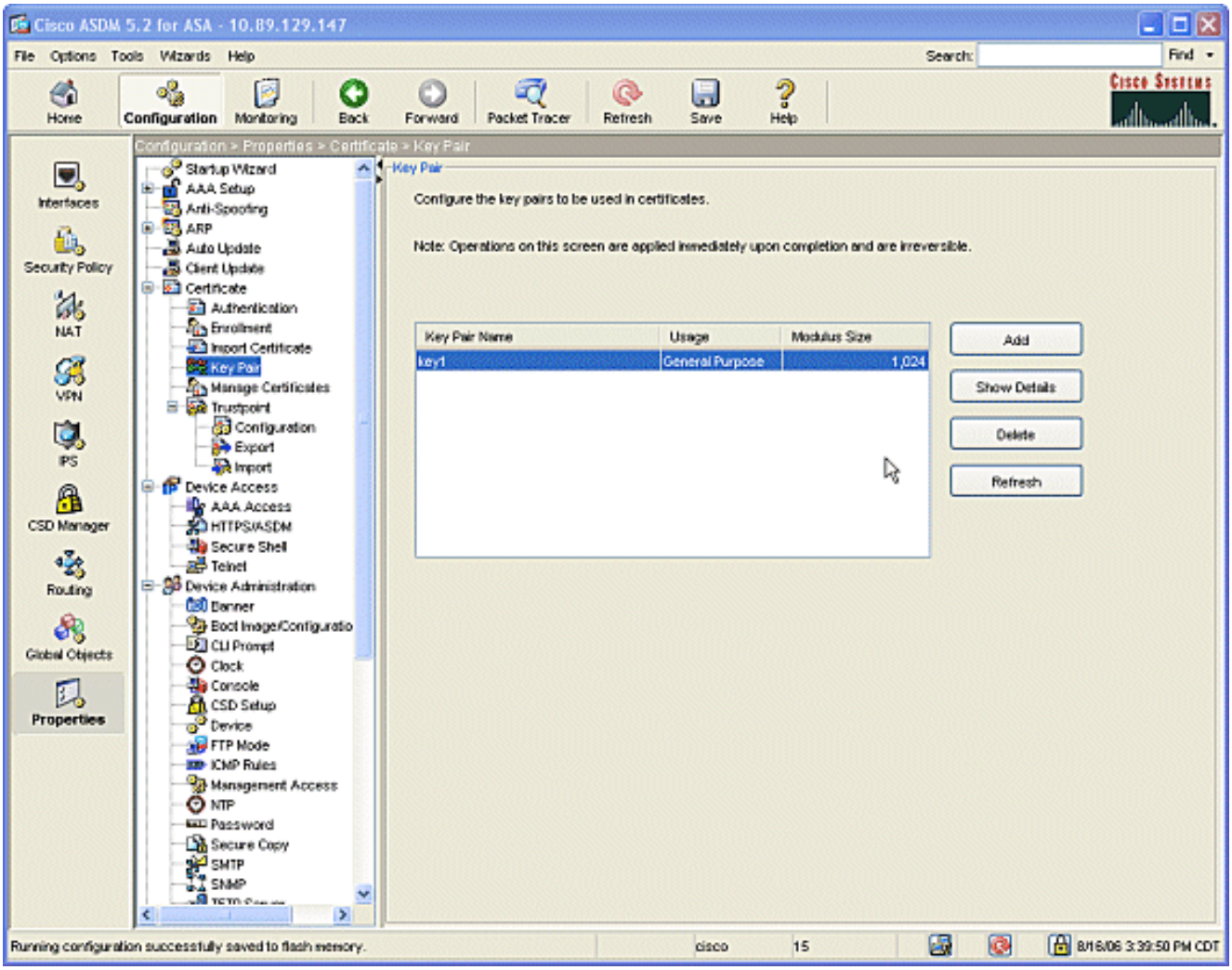
3. L'ASA doit avoir sa propre paire de clés (clés privées et publiques). La clé publique sera envoyée à l'autorité de certification Microsoft.Dans le volet de navigation, cliquez sur **Certificate > Key Pair**.



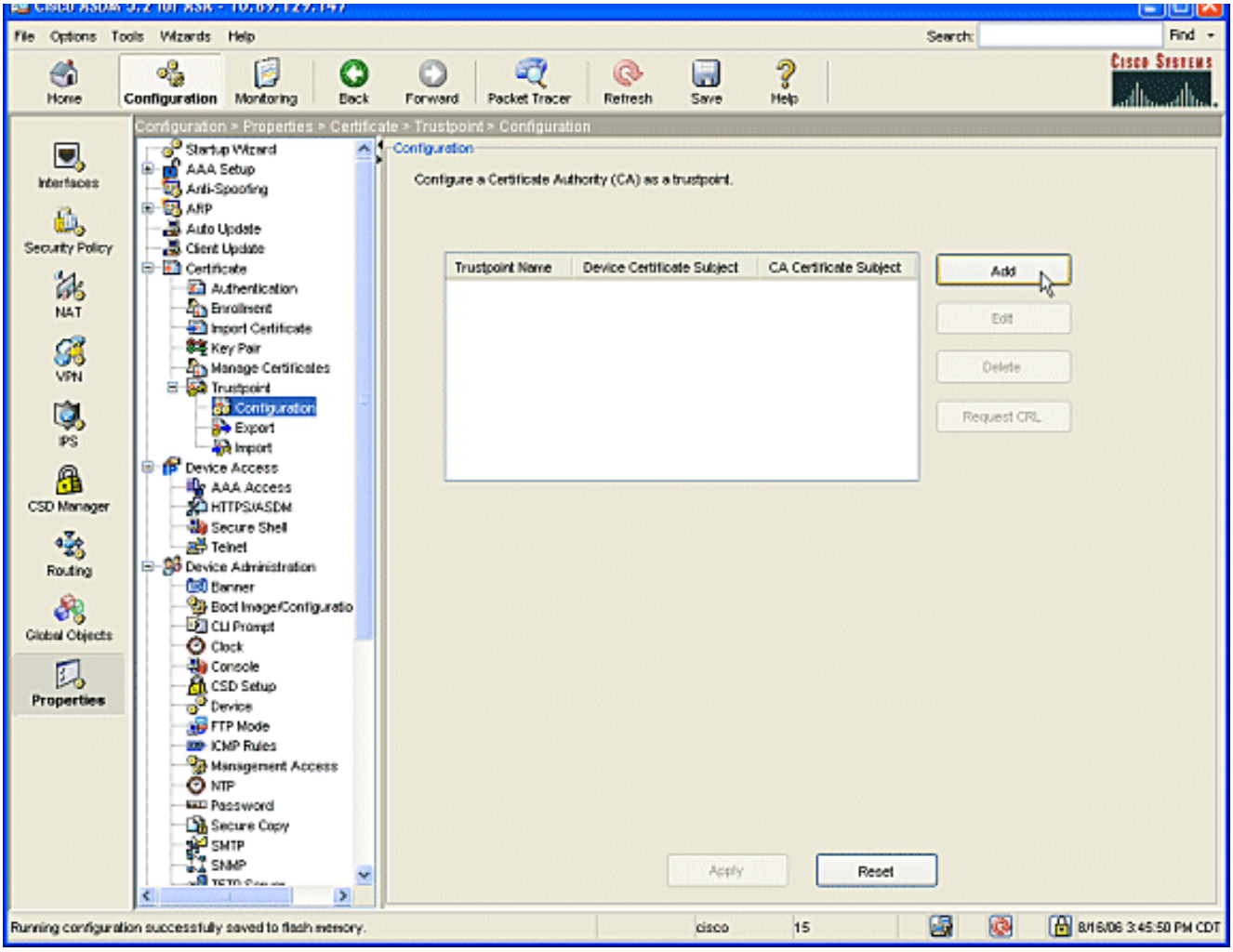
Cliquez sur le bouton **Ajouter** et la boîte de dialogue Ajouter une paire de clés



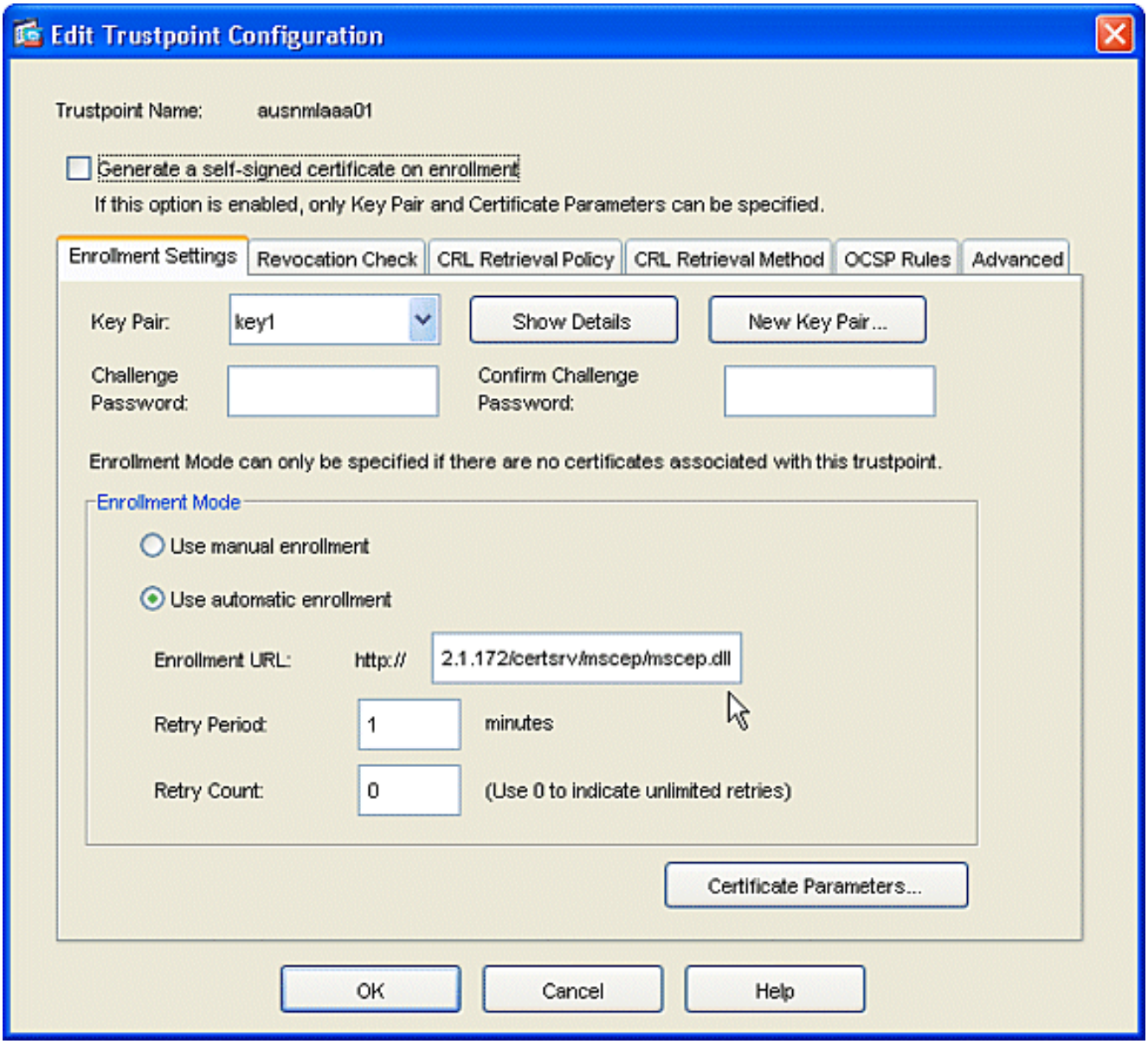
s'affiche. Cochez la case d'option en regard du champ vide de la zone **Nom** et saisissez le nom de la clé.Cliquez sur la **taille :** dans la zone de liste déroulante pour choisir une taille pour la clé ou accepter la valeur par défaut.Cochez la case d'option **Utilisation générale** sous Utilisation.Cliquez sur le bouton **Générer maintenant** pour régénérer les clés et revenir à la fenêtre Paire de clés, où vous pouvez afficher les informations de la paire de
clés.



4. Configurez l'autorité de certification Microsoft pour qu'elle soit considérée comme fiable. Dans le volet de navigation, cliquez sur **Trustpoint > Configuration**.Dans la fenêtre Configuration, cliquez sur le bouton **Ajouter**.

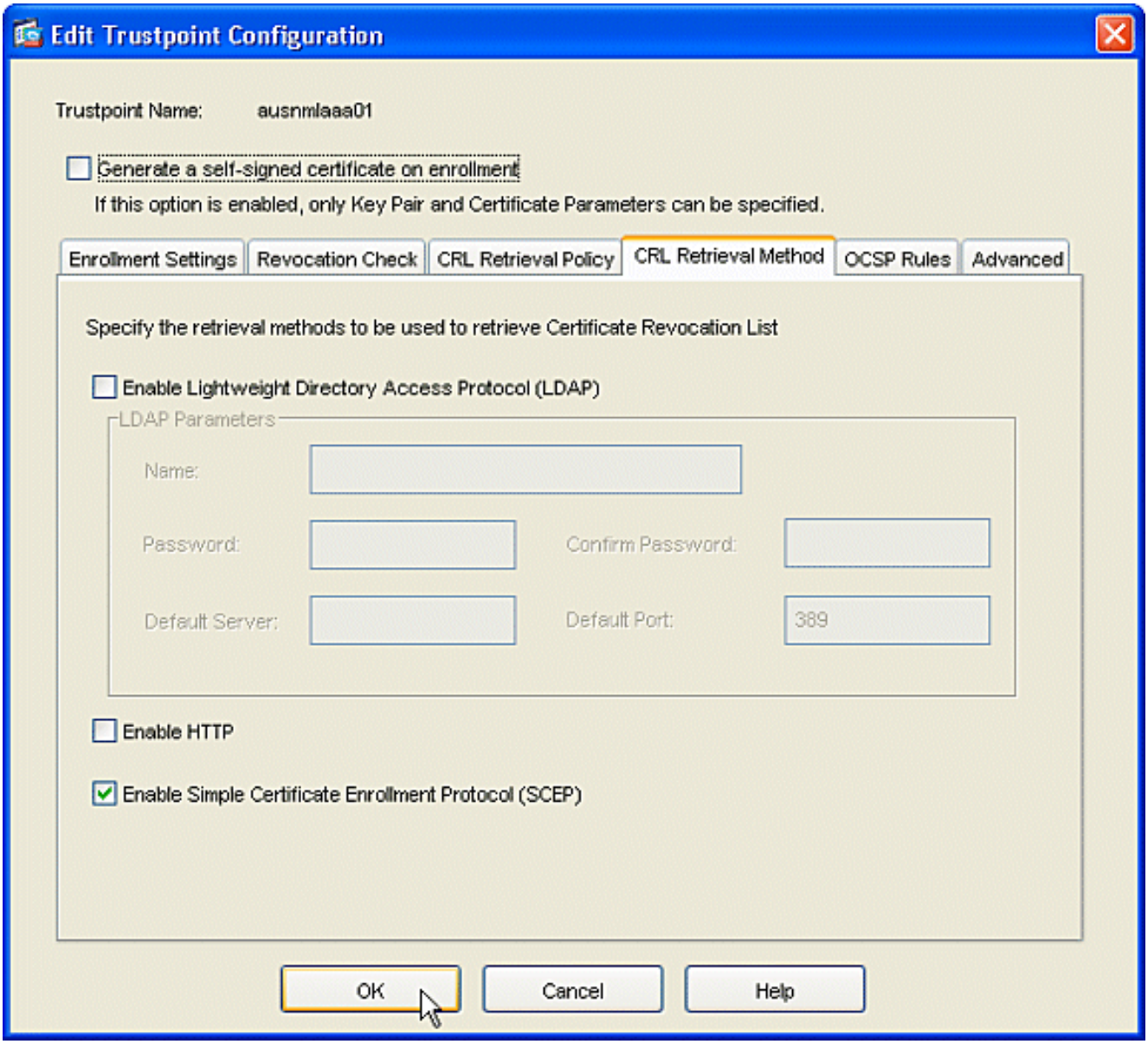


La fenêtre Edit Trustpoint Configuration s'affiche.

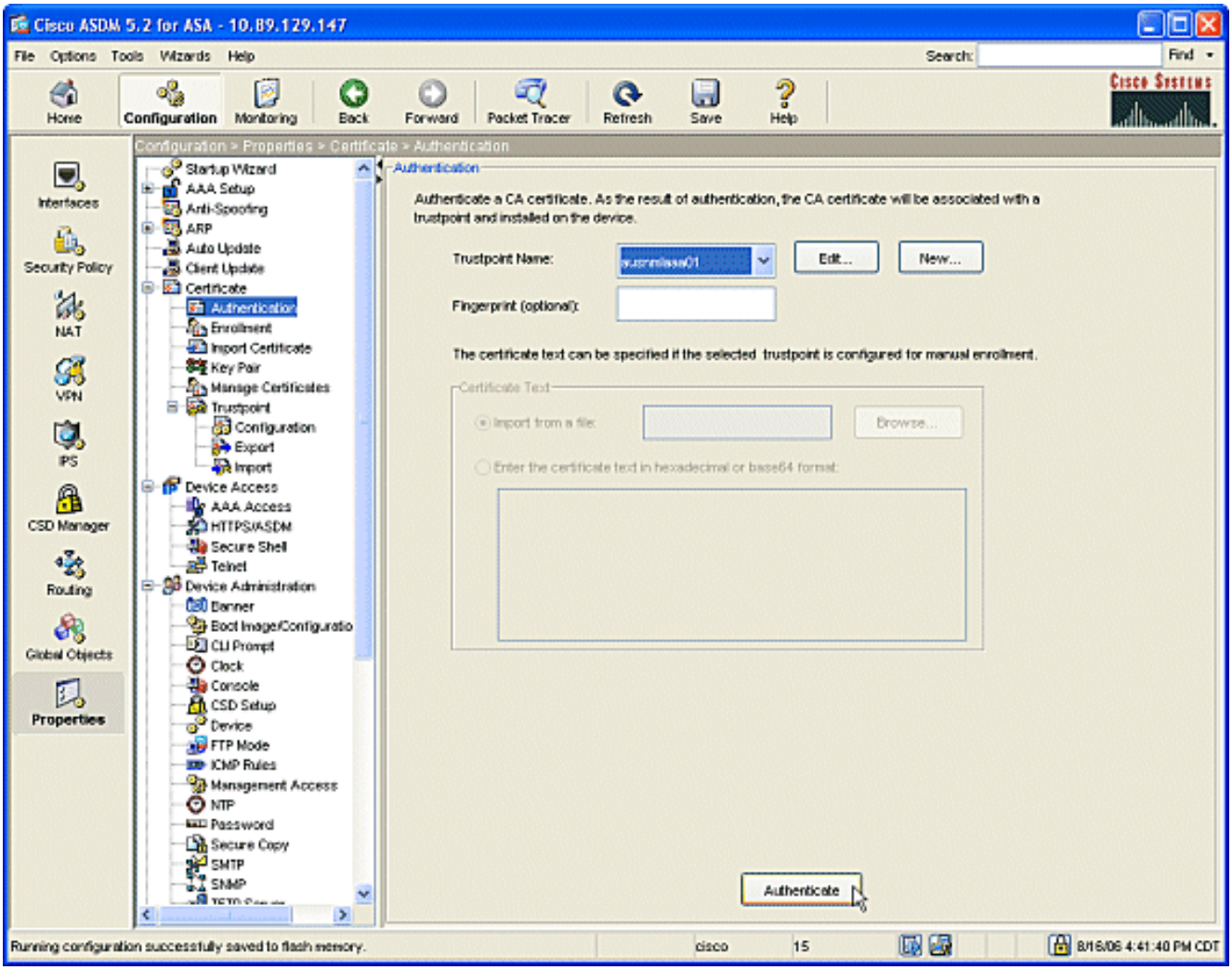


Complétez un nom pour le point de confiance avec le nom de l'autorité de certification.Cliquez sur la **paire de clés :** dans la liste déroulante, puis sélectionnez le nom de la paire de clés que vous avez créée.Cochez la case d'option **Utiliser l'inscription automatique**, puis saisissez l'URL de l'Autorité de certification Microsoft : **http://CA_IP_Address/certsrv/mscep/mscep.dll**.

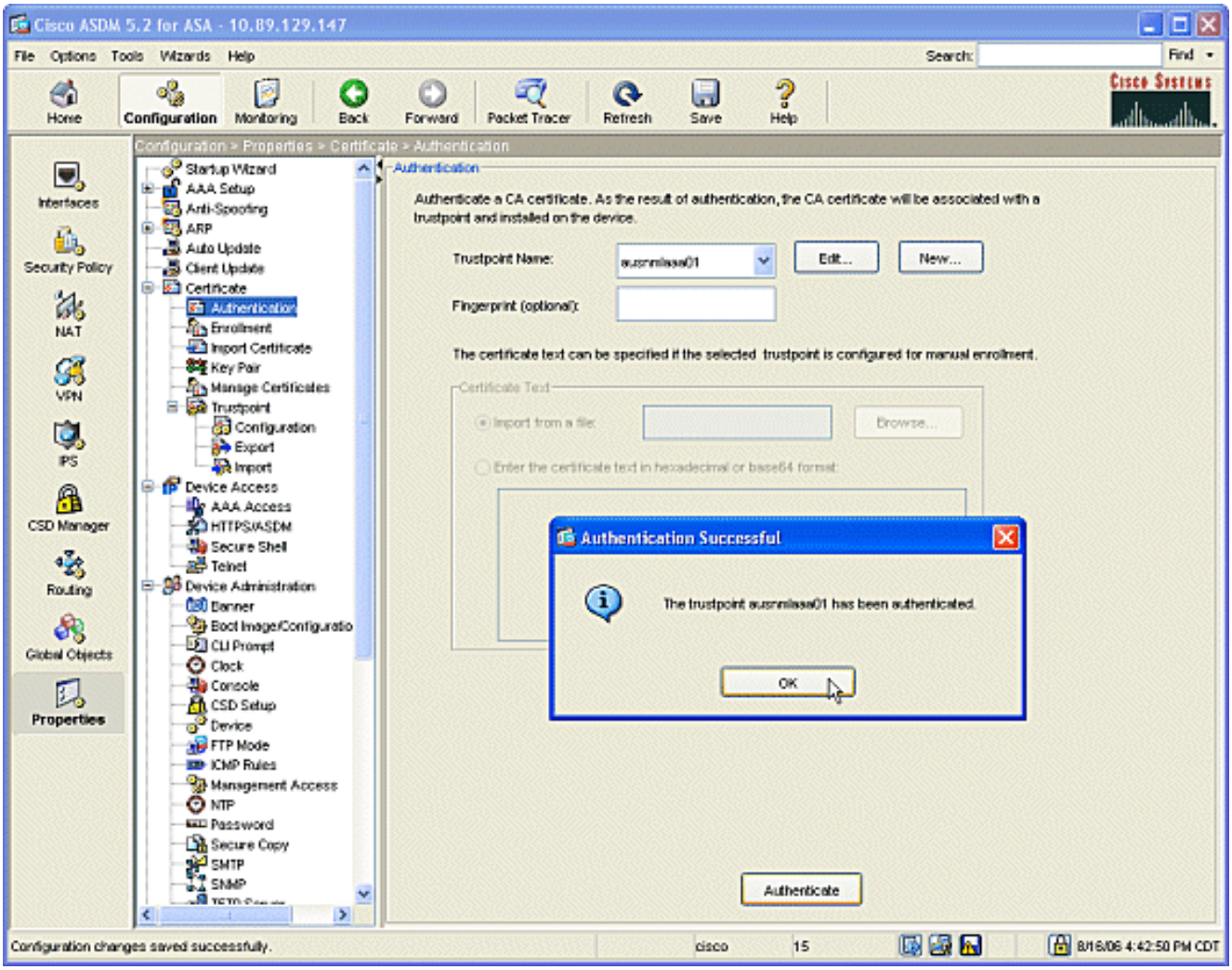
5. Cliquez sur l'onglet **Méthode d'extraction de l'appel**.Décochez les cases Enable HTTP et Enable Lightweight Directory Access Protocol (LDAP).Cochez la case Activer le protocole SCEP (Simple Certificate Enrollment Protocol). Conservez tous les autres paramètres d'onglet à leurs paramètres par défaut.Cliquez sur le bouton **OK**.



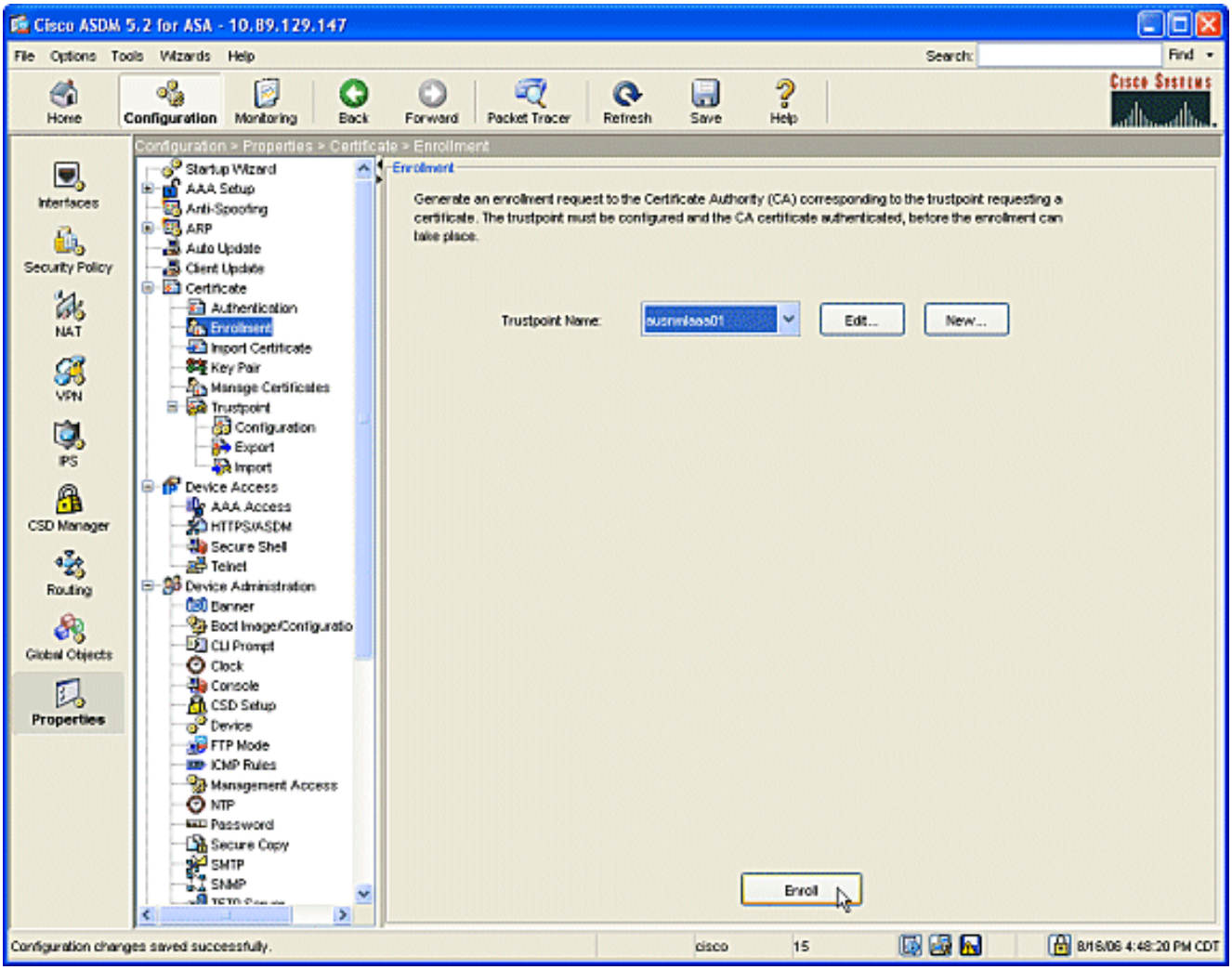
6. Authentifiez et inscrivez-vous avec l'Autorité de certification Microsoft. Dans le volet de navigation, cliquez sur **Certificate > Authentication**. Assurez-vous que le nouveau point de confiance apparaît dans le **nom du point de confiance :** champ. Cliquez sur le bouton **Authentifier**.



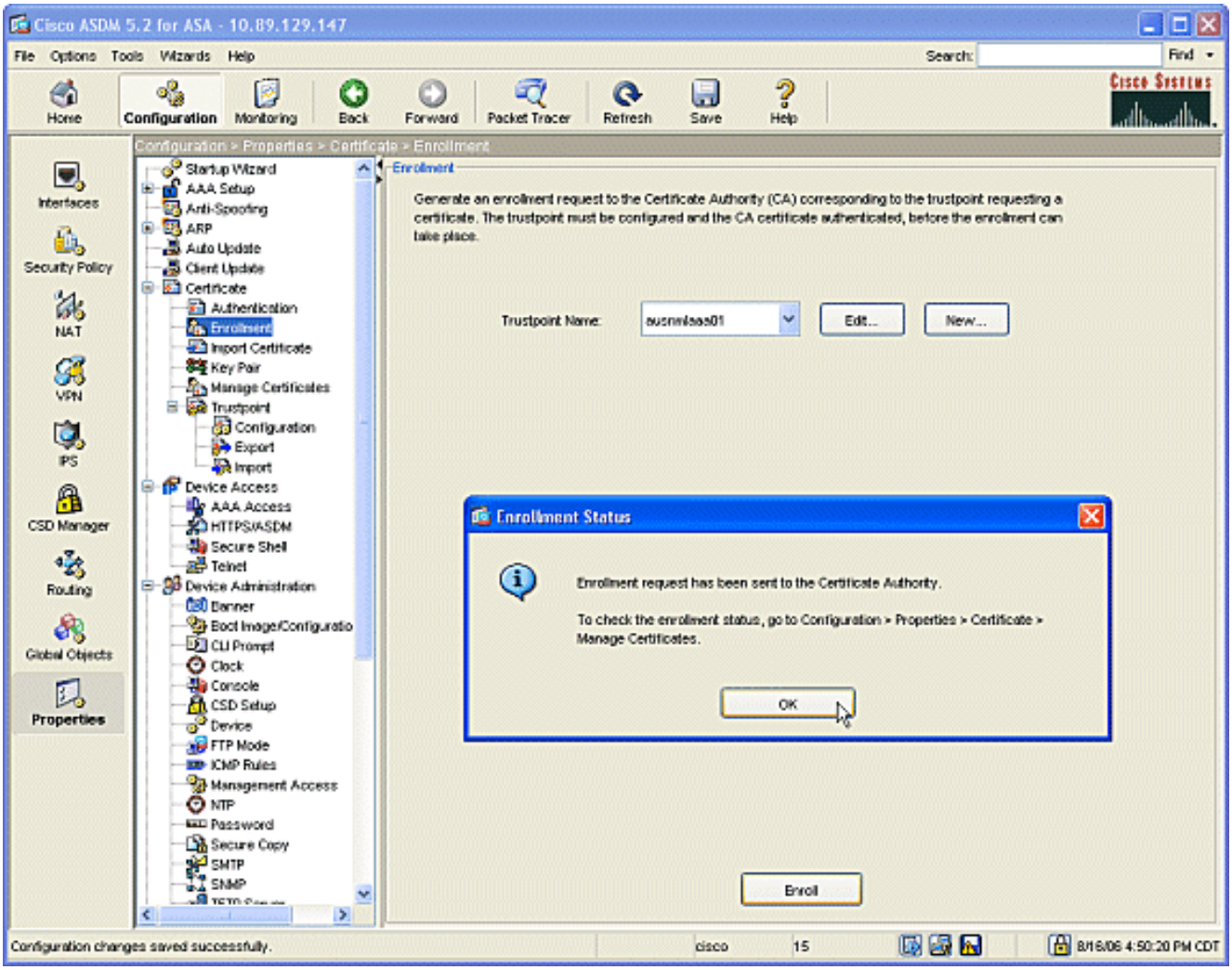
7. Une boîte de dialogue s'affiche pour vous informer que le point de confiance a été authentifié. Cliquez sur le bouton **OK**.



8. Dans le volet de navigation, cliquez sur **Inscription**. Assurez-vous que le nom du point de confiance s'affiche dans le champ Nom du point de confiance, puis cliquez sur le bouton **Inscription**.



9. Une boîte de dialogue s'affiche pour vous informer que la demande a été envoyée à l'Autorité de certification. Cliquez sur le bouton **OK**.



Note: Sur un ordinateur autonome Microsoft Windows, vous devez émettre les certificats pour toutes les demandes qui ont été soumises à l'autorité de certification. Le certificat sera en attente jusqu'à ce que vous cliquiez avec le bouton droit sur le certificat et que vous cliquiez sur question sur Microsoft Server.

Résultats

Il s'agit de la configuration CLI qui résulte des étapes ASDM :

ciscosa

```
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
```

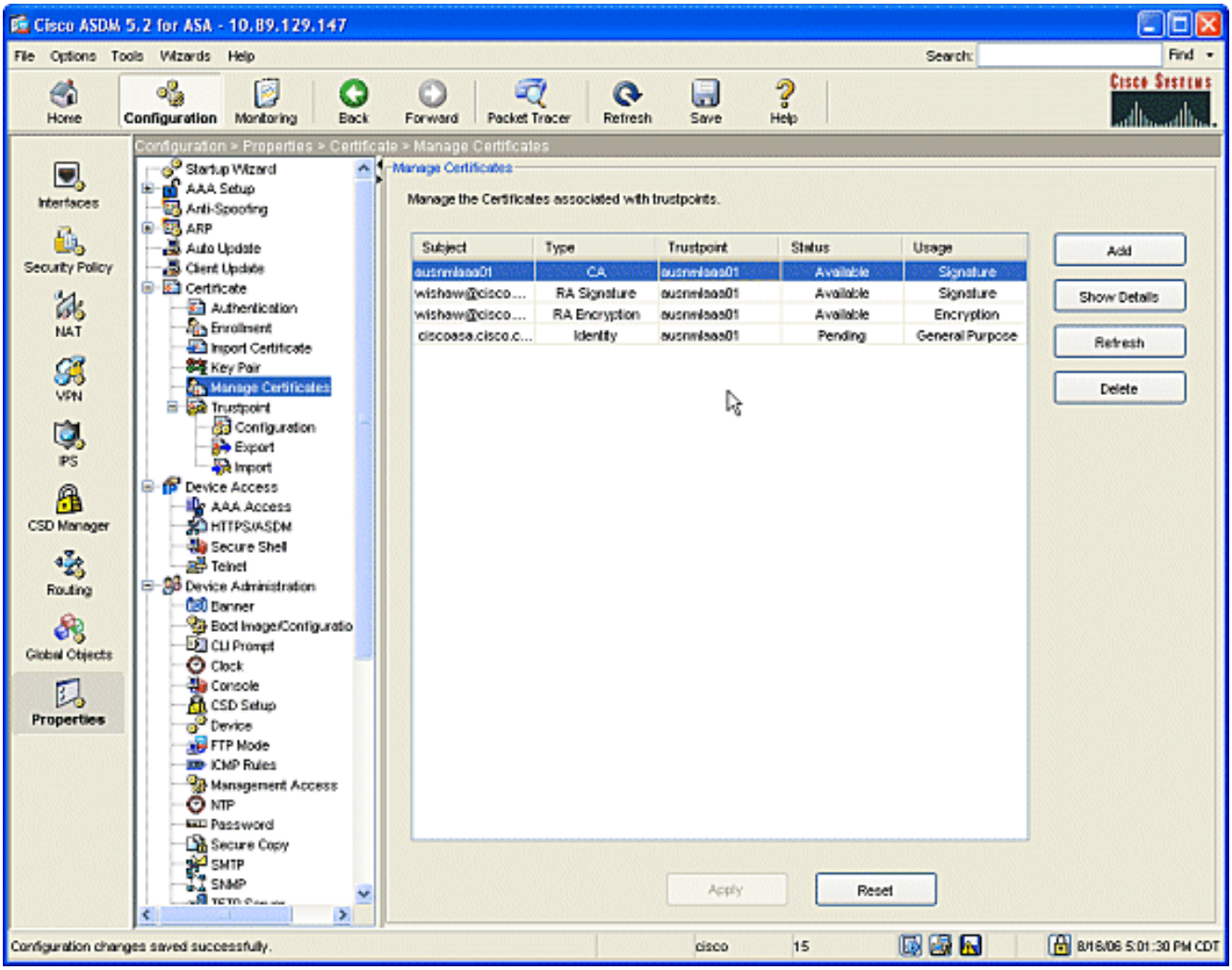
Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérifier et gérer votre certificat

Vérifiez et gérez votre certificat.

1. Ouvrez l'application ASDM et cliquez sur le bouton **Configuration**.
2. Dans le menu de gauche, cliquez sur le bouton **Propriétés**.Cliquez sur **Certificat**.Cliquez sur **Gérer le certificat**.



Commandes

Sur l'ASA, vous pouvez utiliser plusieurs commandes **show** sur la ligne de commande pour vérifier l'état d'un certificat.

- La commande **show crypto ca certificate** permet d'afficher des informations sur votre certificat, le certificat de l'autorité de certification et tous les certificats de l'autorité de certification.
- La commande **show crypto ca trustpoints** est utilisée pour vérifier la configuration de trustpoint.
- La commande **show crypto key mypubkey rsa** est utilisée pour afficher les clés publiques RSA de votre ASA.
- La commande **show crypto ca crls** est utilisée pour afficher toutes les listes de révocation de certificats mises en cache .

Note : L'outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Dépannage

Utilisez cette section pour dépanner votre configuration.

Référez-vous à Infrastructure à clé publique pour Windows Server 2003 pour plus d'informations sur la façon de dépanner Microsoft Windows 2003 CA.

Commandes

Remarque : l'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug , référez-vous à la section** Informations importantes sur les commandes Debug.

Informations connexes

- Configuration du concentrateur Cisco VPN 3000 4.0.x pour obtenir un certificat numérique