如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书

目录

简介

数字证书可以用于对网络上的网络设备和用户进行身份验证。可用于协商网络节点之间的 IPSec 会话。

Cisco 设备以三种主要方式在网络上安全地标识自身：

1. **预共享密钥**。两个或更多设备可以拥有相同的共享密钥。对等体通过计算和发送包括预共享密钥的数据监控哈希互相进行身份验证。如果接收方对等体可以独立地使用其预共享密钥创建相同的哈希，则它就会了解两个对等体必须共享同一个密钥，从而对另一个对等体进行身份验证。此方法要手动进行，因此扩展性不高。
2. **自签名证书**。设备生成其自己的证书，并将其签名为有效。此类型的证书应限制用途。将此证书与 SSH 和 HTTPS 访问配合用于配置目的是好例子。形成这种联系需要一个单独的用户名/口令对。**注：持**久自签名证书在路由器重新加载后仍然有效，因为它们保存在设备的非易失性随机访问存储器(NVRAM)中。有关详细信息，请参阅永久自签名证书。一个好的用法示例是 SSL VPN (WebVPN) 连接。
3. **证书颁发机构证书**。第三方对于尝试通信的两个或更多节点验证有效性和身份。每个节点都有公钥和私钥。公钥将数据加密，而私钥将数据解密。由于这些密钥从相同来源获得其证书，因此可以确保其各自的身份。ASA 设备可以通过手动注册方法或自动注册方法从第三方获得数字证书。**注：您**选择的数字证书的注册方法和类型取决于每个第三方产品的特性和功能。有关

详细信息，请与证书服务的供应商联系。

思科自适应安全设备(ASA)可以使用第三方证书颁发机构(CA)提供的预共享密钥或数字证书对IPSec连接进行身份验证。此外，ASA 可以生成自己的自签名数字证书。这应用于与设备的SSH、HTTPS和思科自适应安全设备管理器(ASDM)连接。

本文档演示了从ASA的Microsoft证书颁发机构(CA)自动获取数字证书所需的过程。其中不包括手动的注册方法。本文档使用ASDM执行配置步骤，并提供最终的命令行界面(CLI)配置。

要了解有关Cisco IOS®平台的相同方案的详细信息，请参阅Cisco IOS证书注册使用增强型注册命令的配置示例。

要详细了解与 Cisco VPN 3000 系列集中器相同的场景，请参阅配置 Cisco VPN 3000 集中器 4.7.x 以获得数字证书和 SSL 证书。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

ASA 设备的要求

- 将Microsoft® Windows 2003 Server配置为CA。请参阅 Microsoft 文档或 Windows Server 2003 的公钥基础架构
- 要允许自适应安全设备管理器(ASDM)配置Cisco ASA或PIX版本7.x，请参阅允许ASDM的HTTPS访问。
- 安装证书服务的附加项 (mscep.dll)。
- 从Simple Certificate Enrollment Protocol(SCEP)Add-on for Certificate Services 或从Windows Server 2003 Resource Kit Tools获取Add-on的可执行文件(cepsetup.exe) ，或mscep.dll文件。**注意：**在Microsoft Windows计算机上配置正确的日期、时间和时区。强烈建议使用网络时间协议(NTP)，但不必使用。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为 7.x 及更高版本的 Cisco ASA 5500 系列自适应安全设备
- Cisco 自适应安全设备管理器版本 5.x 及更高版本
- Microsoft Windows 2003 Server 证书颁发机构

相关产品

此配置也可用于Cisco PIX 500系列安全设备版本7.x。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置 ASA 与 Microsoft CA 交换证书

任务

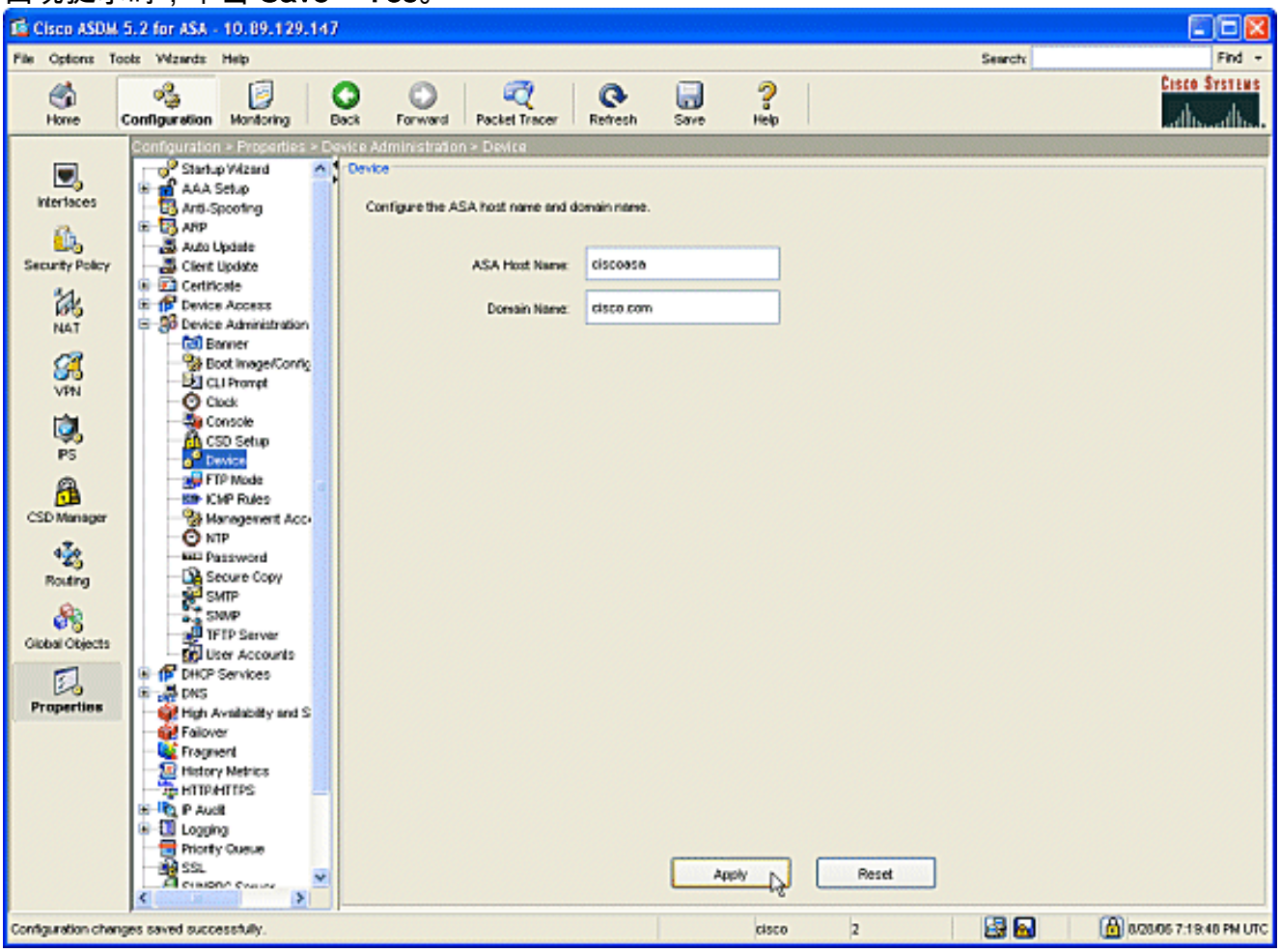
此部分中向您展示如何配置 ASA 从 Microsoft 证书颁发机构接收证书。

配置 ASA 的说明

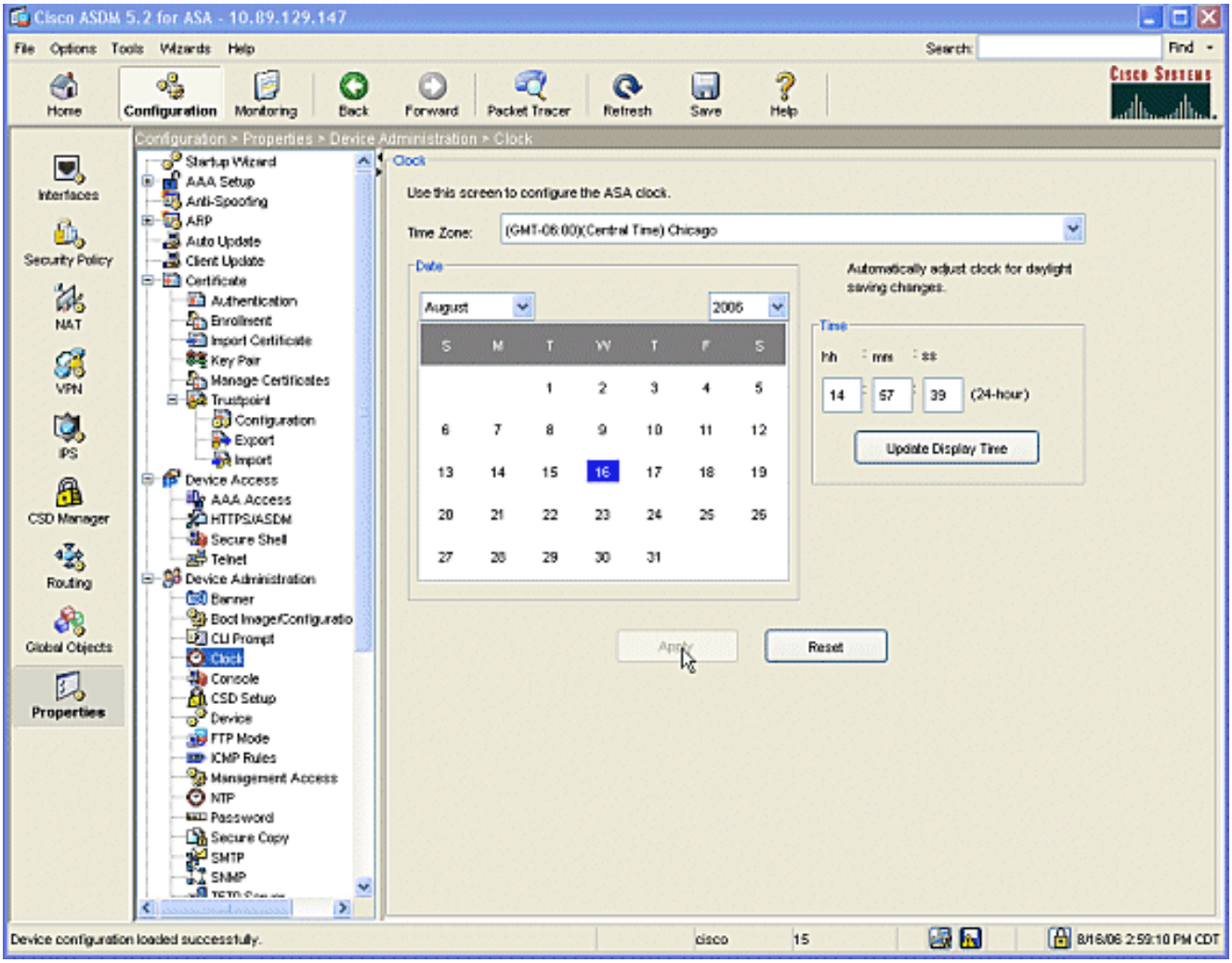
数字证书使用日期/时间/时区部分作为检查证书有效性的一种方法。必须用正确的日期和时间配置 Microsoft CA 和您的所有设备。Microsoft CA 使用其证书服务的附加项 (mscep.dll) 与 Cisco 设备共享证书。

完成下列步骤以配置 ASA：

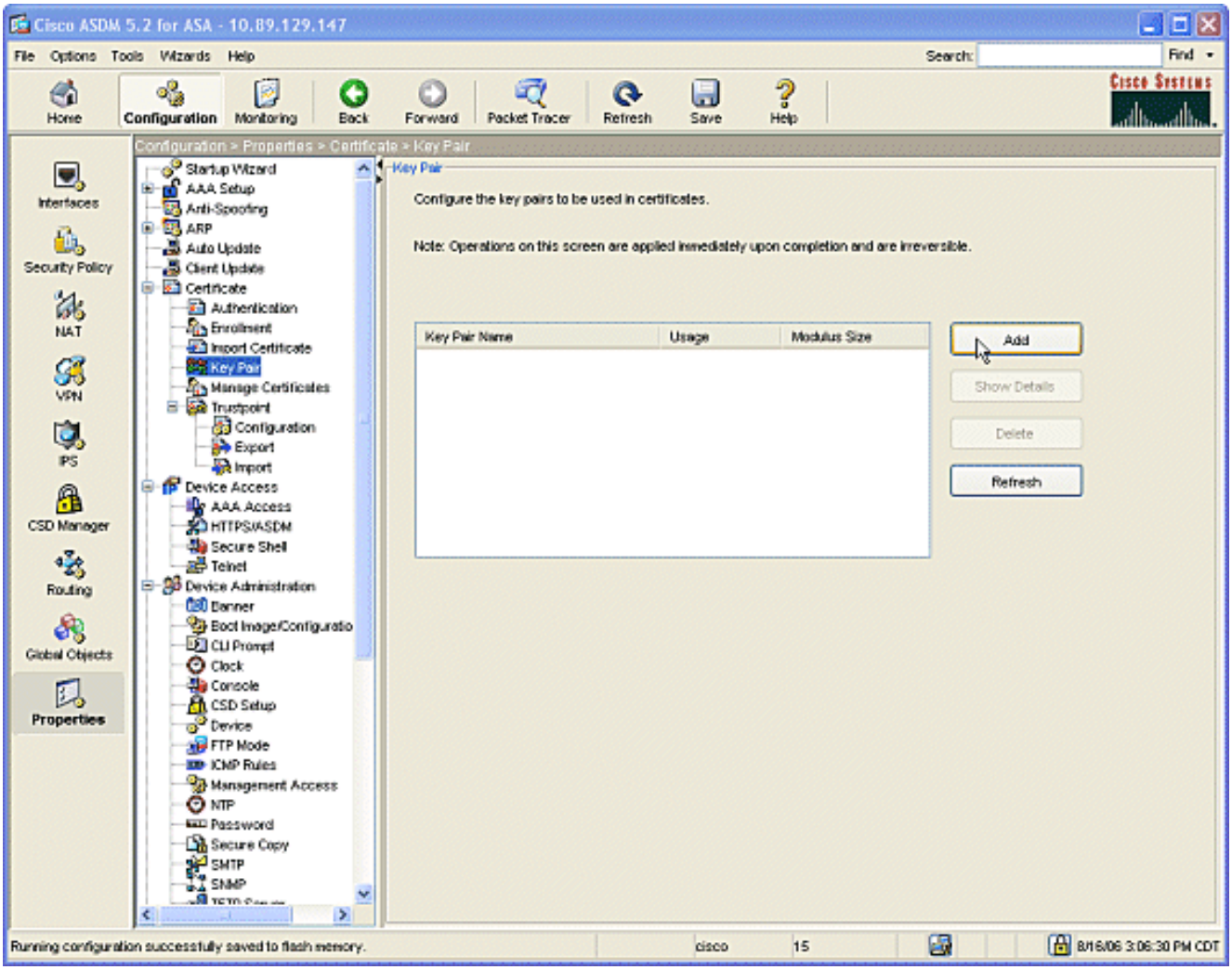
1. 打开 ASDM 应用程序，然后单击 **Configuration 按钮**。从左侧菜单中单击 **Properties 按钮**。从导航窗格中单击 **Device Administration > Device**。输入 ASA 的主机名和域名。单击 **Apply**。出现提示时，单击 **Save > Yes**。



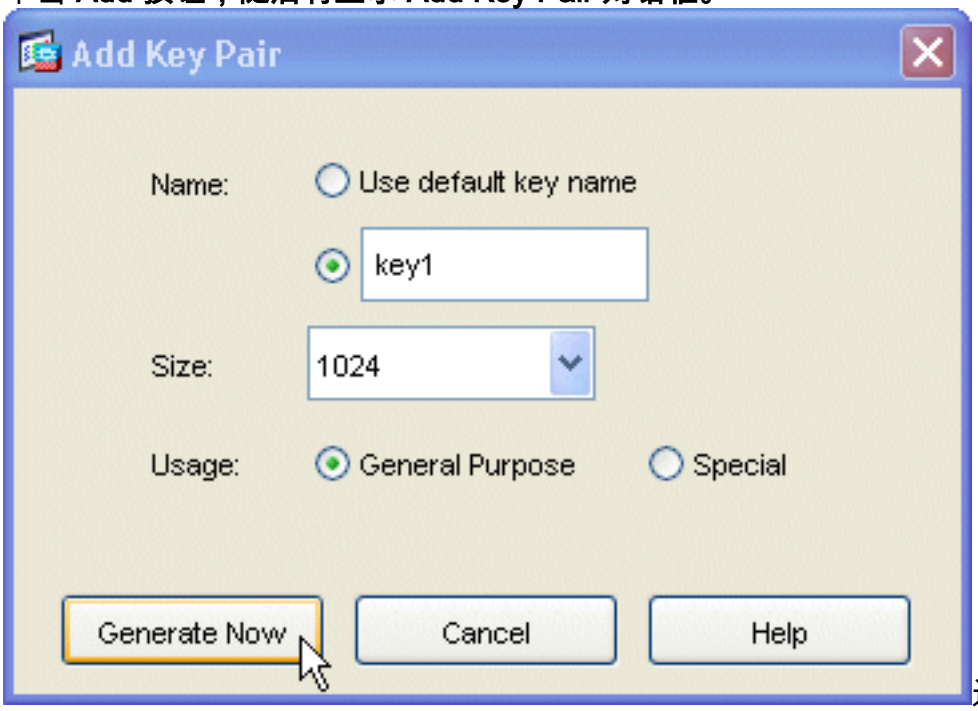
2. 用正确的日期、时间和时区配置 ASA。这对设备的证书生成过程很重要。如有可能，使用 NTP 服务器。从导航窗格中单击 **Device Administration > Clock**。在 Clock 窗口中，使用各个字段和下拉箭头设置正确的日期、时间和时区。



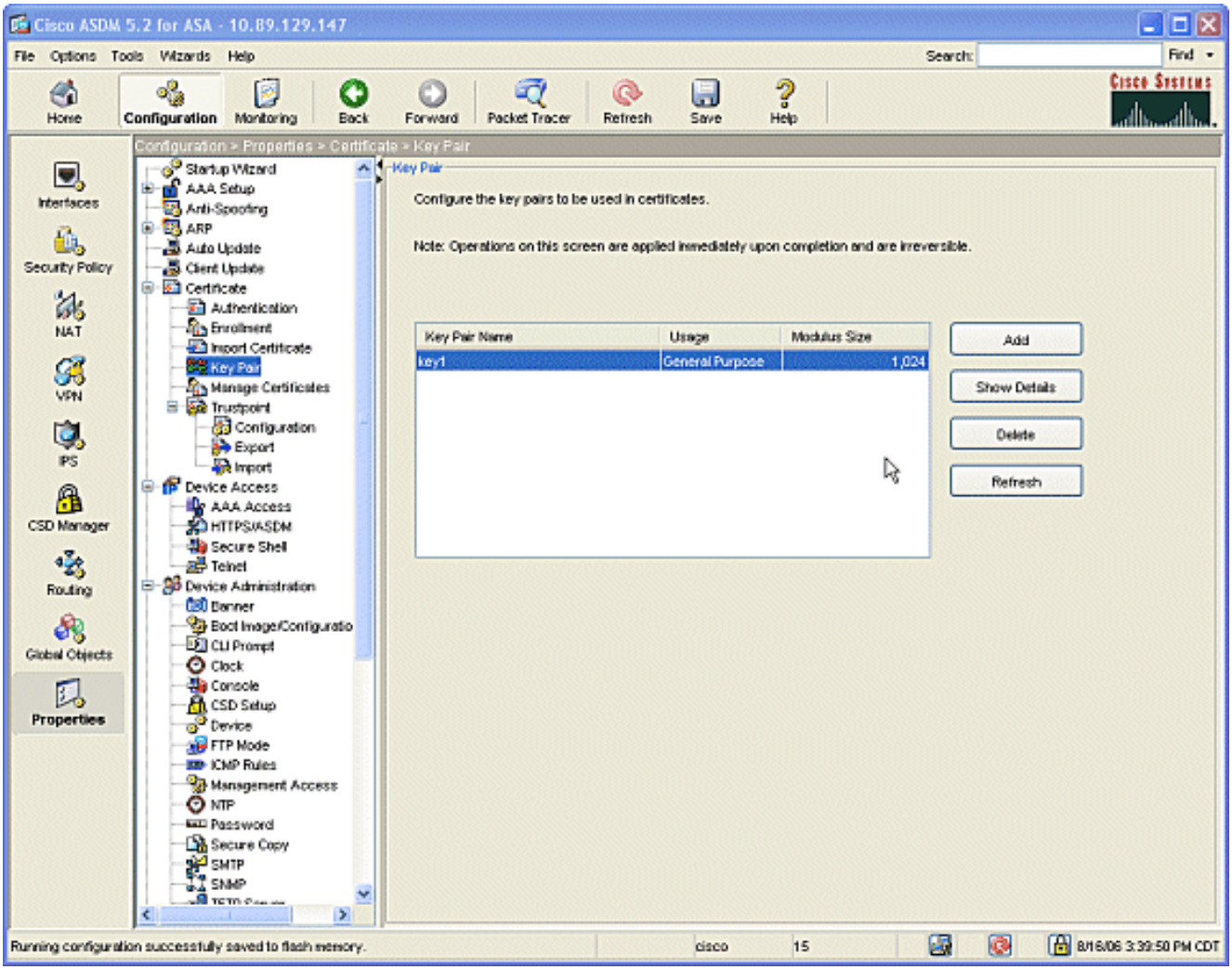
3. ASA 必须有自己的密钥对（私钥和公钥）。 公钥将发送到 Microsoft CA。从导航窗格中单击 **Certificate > Key Pair**。



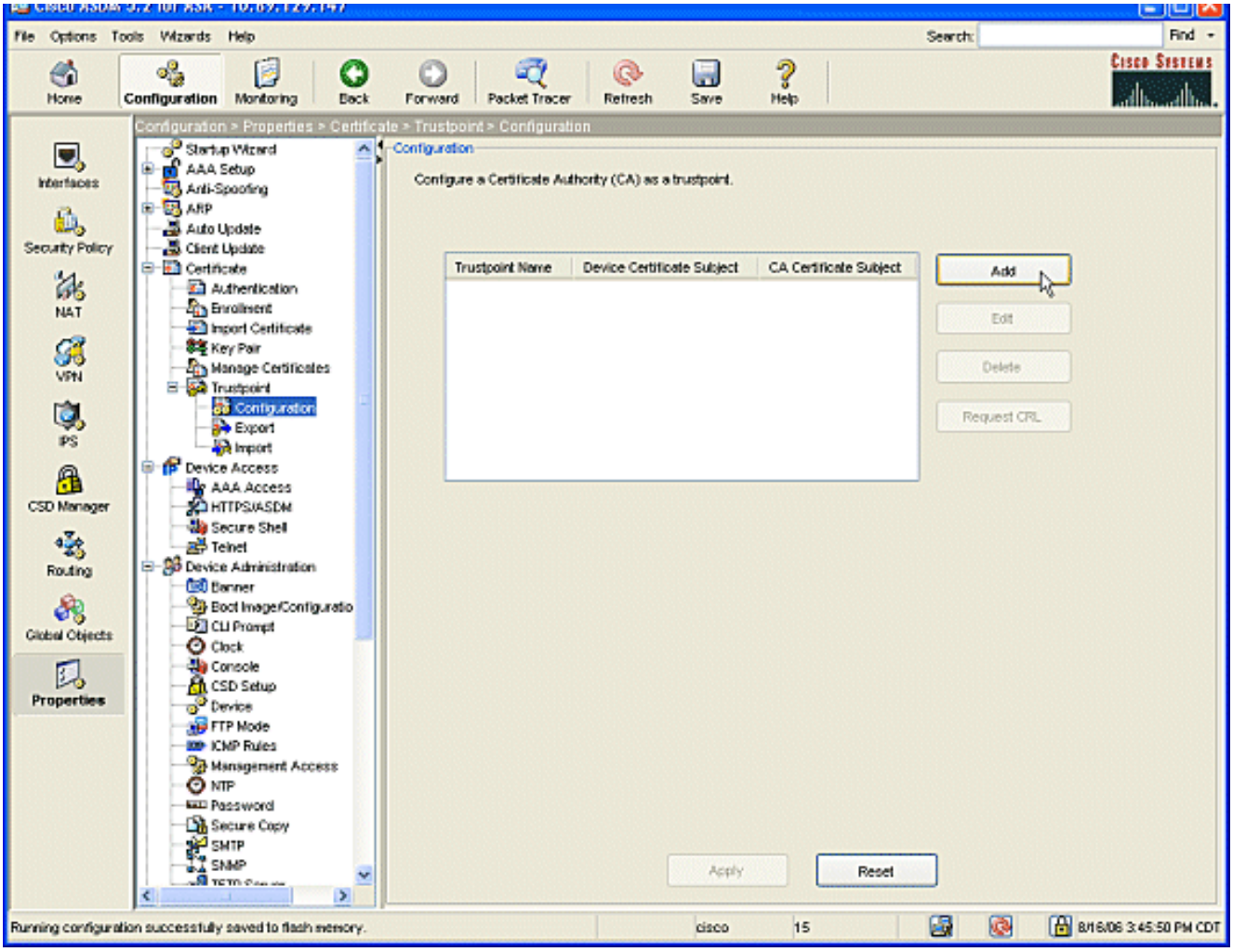
单击 **Add 按钮，随后将显示 Add Key Pair 对话框。**



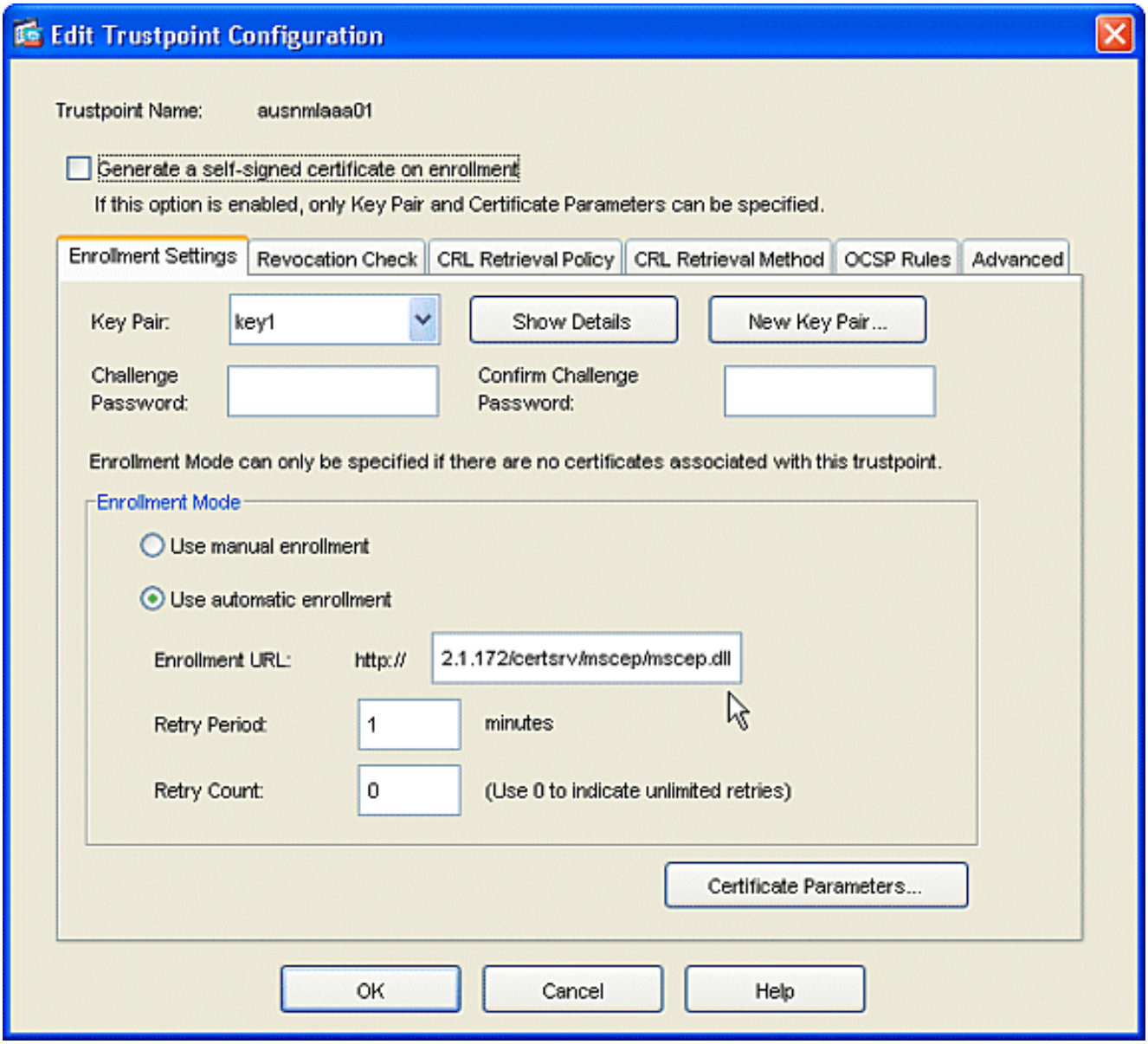
选中 **Name 区域的空白字段旁的单选按钮，然后键入密钥的名称。**单击下拉框旁的 **Size:**箭头以选择密钥的大小或接受默认值。选中 Usage 下的 **General Purpose 单选按钮。**单击 **Generate Now 按钮以重新生成密钥并返回 Key Pair 窗口，从中可以查看密钥对的信息。**



4. 配置 Microsoft CA 以将其视为可信。从导航窗格中单击 **Trustpoint > Configuration**。从 Configuration 窗口中单击 **Add 按钮。**

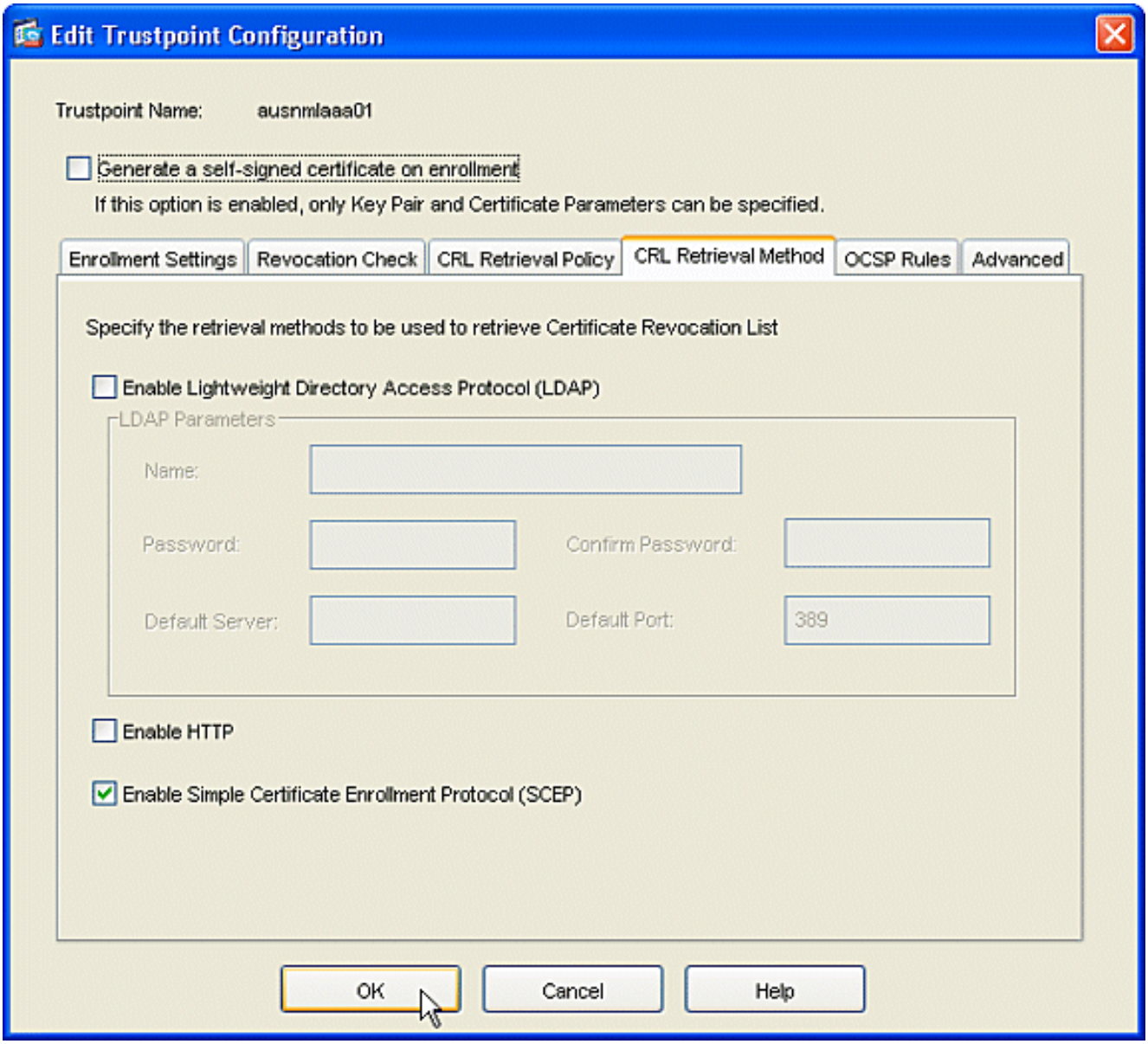


此时显示 Edit Trustpoint Configuration 窗口。

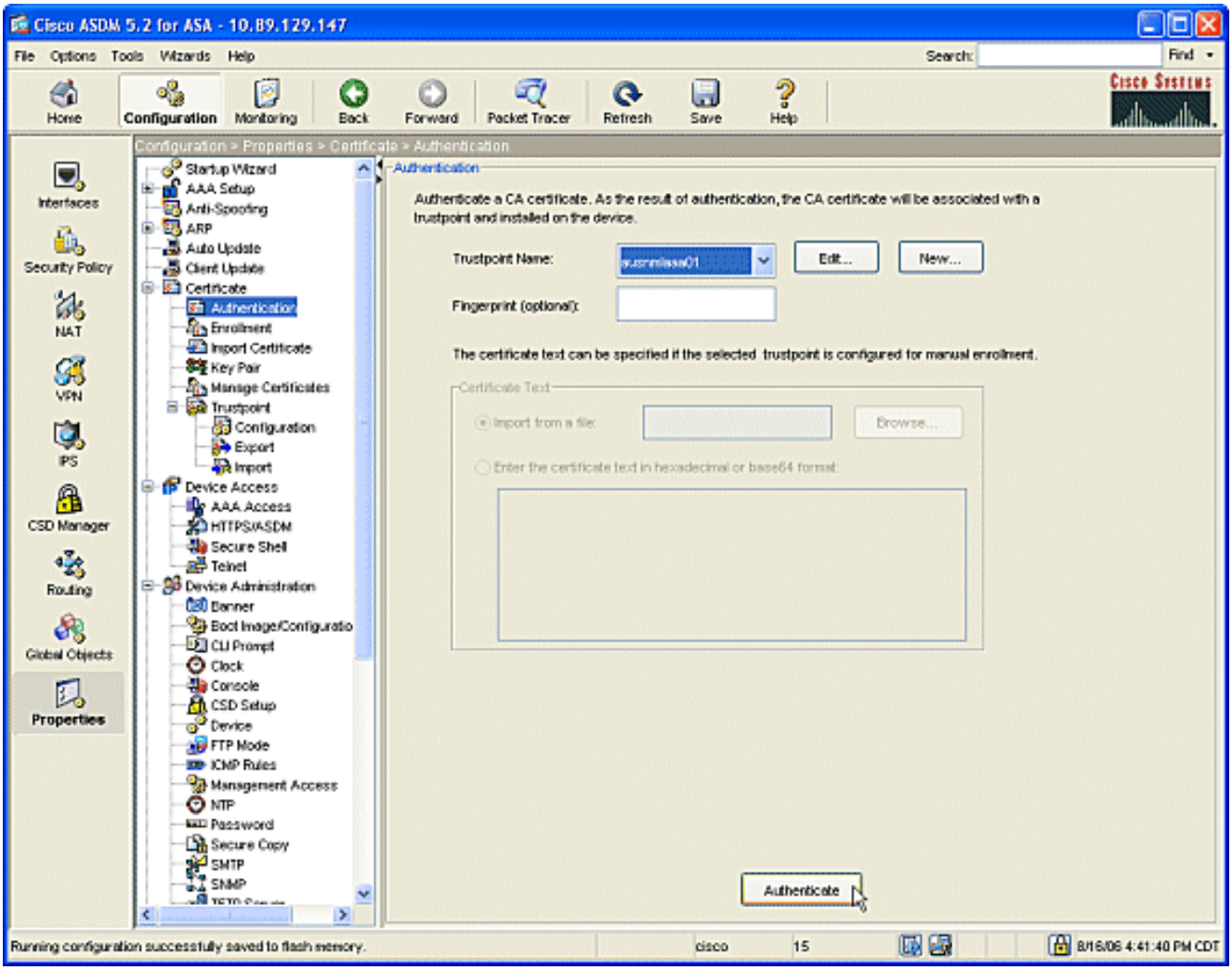


用 CA 的名称填写信任点的名称。单击下拉框旁的 **Key Pair:**箭头，然后选择您所创建的密钥对的名称。选中 **Use automatic enrollment 单选按钮，然后输入 Microsoft CA 的 URL：http://CA_IP_Address/certsrv/mscep/mscep.dll。**

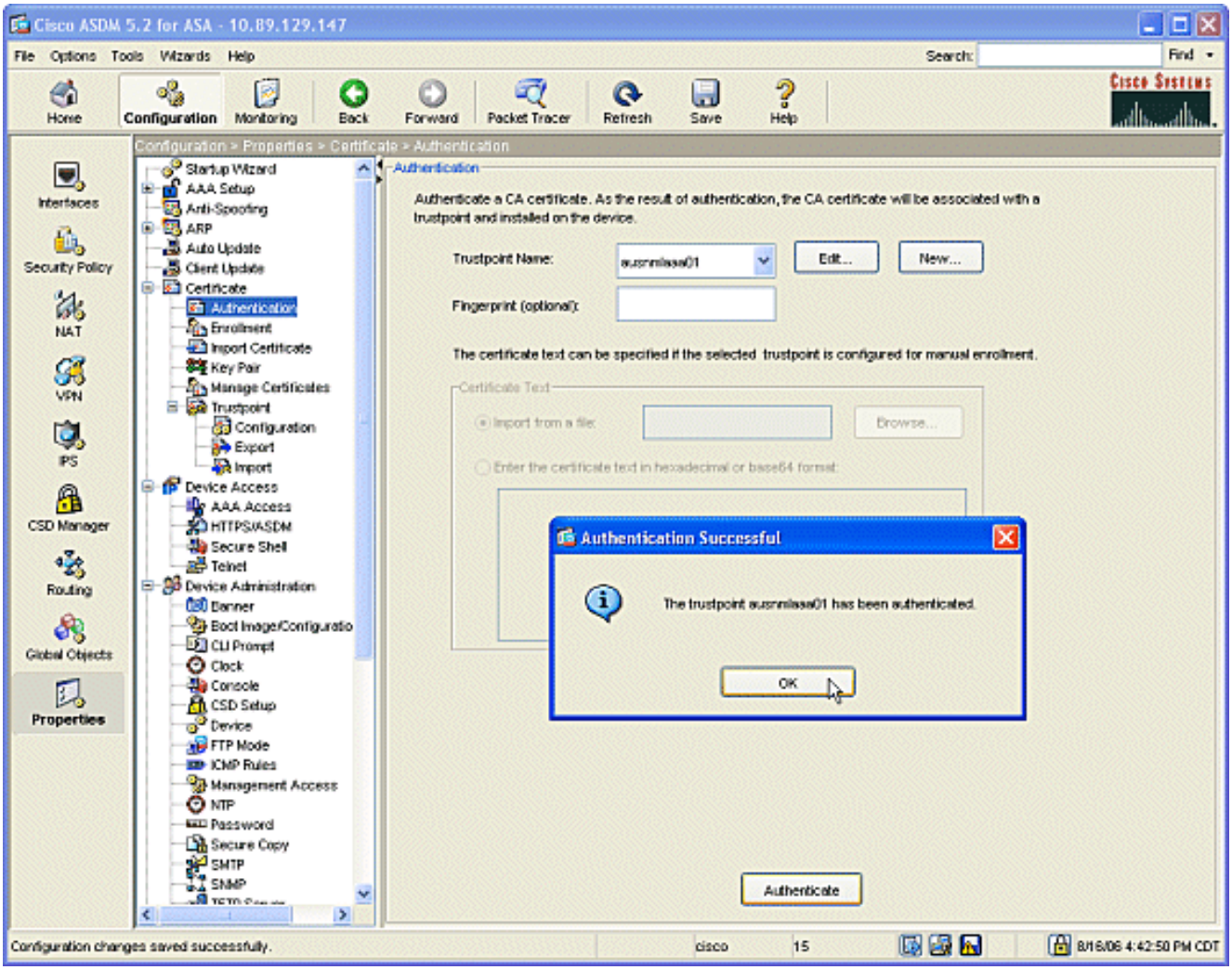
5. 单击 **Crl Retrieval Method** 选项卡。取消选中Enable HTTP和Enable Lightweight Directory Access Protocol(LDAP)复选框。选中启用简单证书注册协议(SCEP)复选框。将所有其他选项卡设置保留其默认设置。单击 **OK 按钮。**



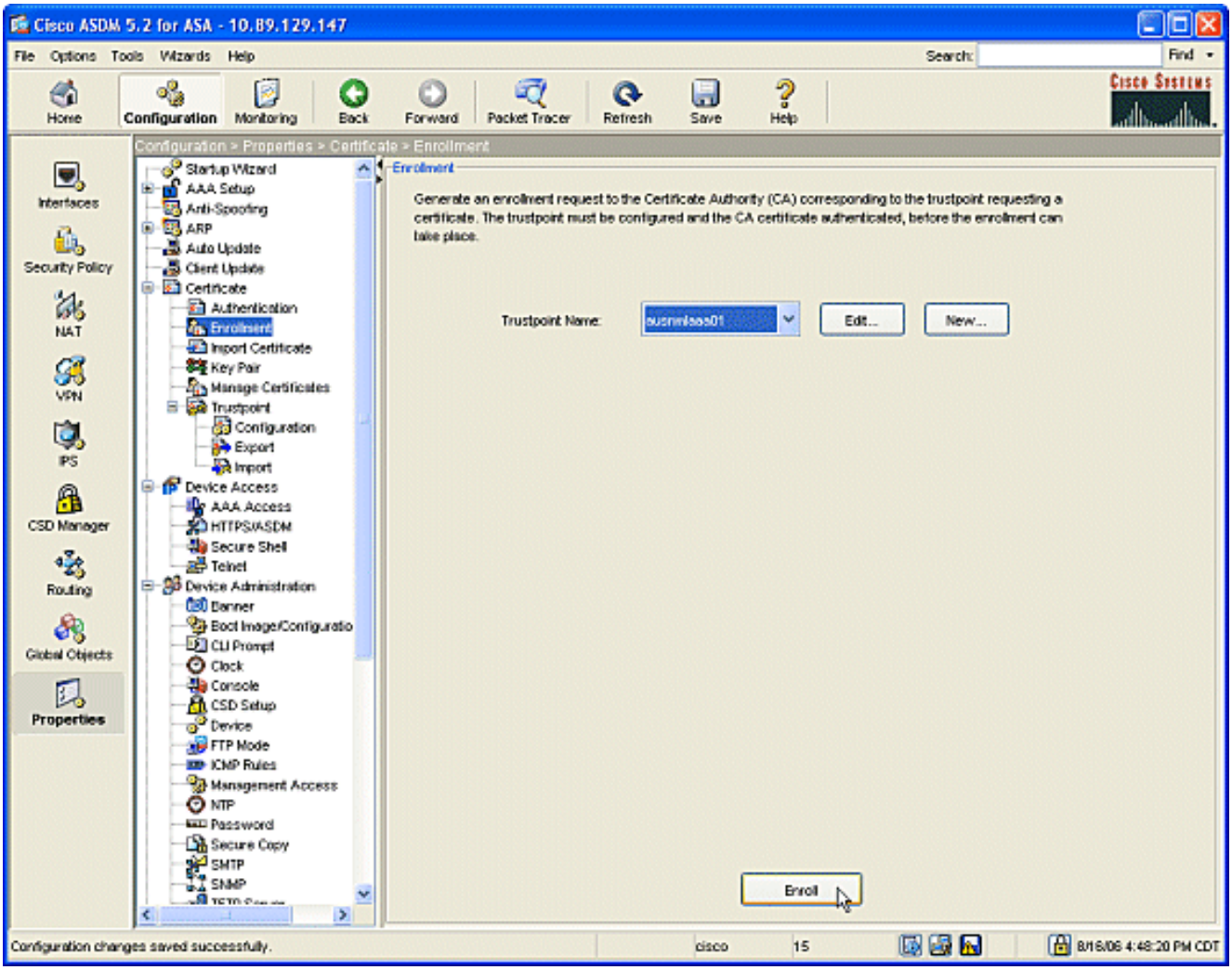
6. 对 Microsoft CA 进行身份验证并注册到它。从导航窗格中单击 **Certificate > Authentication**。确定新创建的信任点显示在 **Trustpoint Name:**字段。单击 **Authenticate 按钮。**



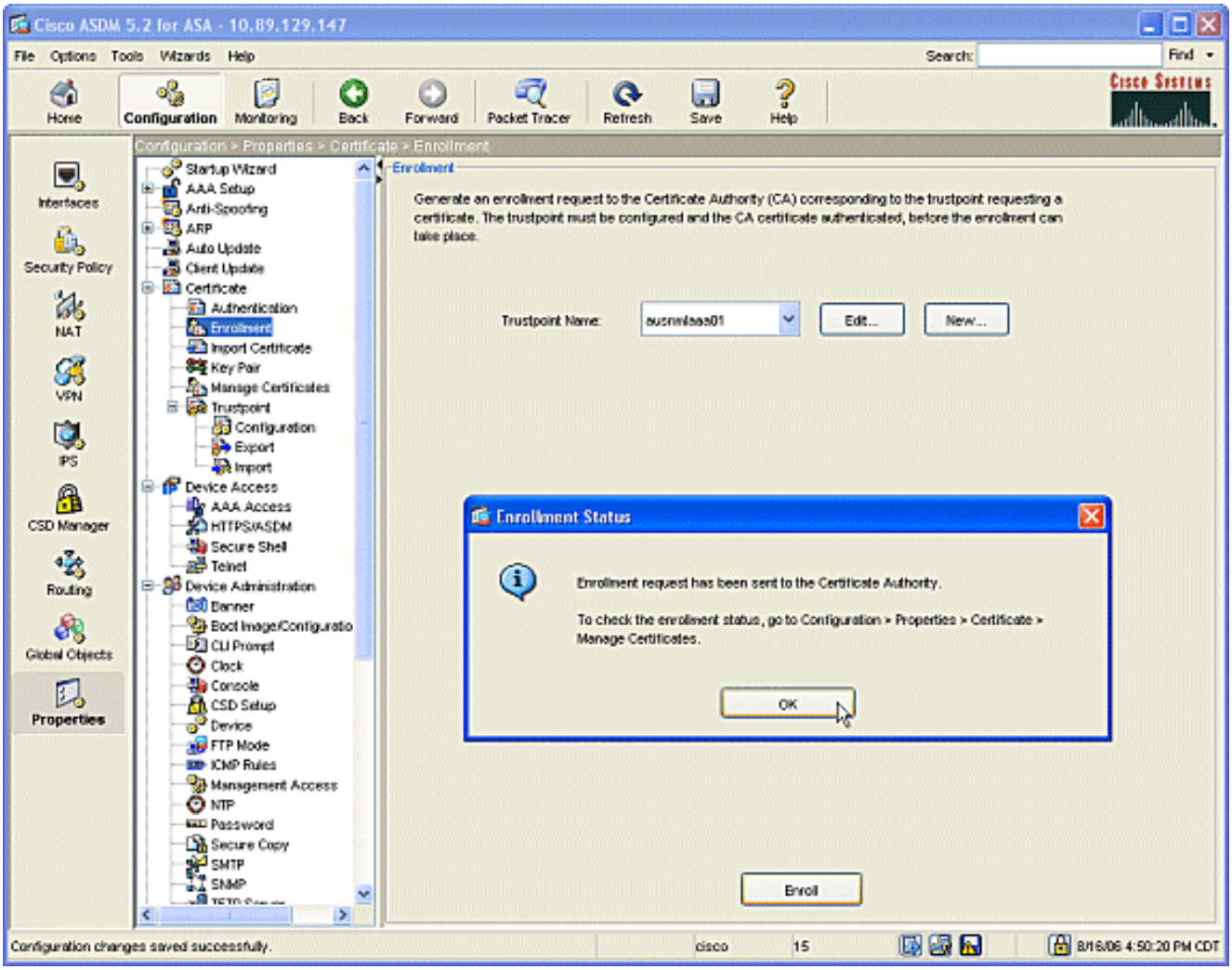
7. 此时将显示一个对话框，通知您已对该信任点进行过身份验证。单击 **OK 按钮。**



8. 从导航窗格中单击 **Enrollment**。确保信任点名称显示在 Trustpoint Name 字段中，然后单击 **Enroll 按钮**。



9. 此时将显示一个对话框，通知您已向 CA 发送了该请求。单击 **OK 按钮。**



注意： 在 Microsoft Windows 独立计算机上，必须对已提交给 CA 的任何请求都颁发证书。证书将处于挂起状态，直到在 Microsoft 服务器上右键单击该证书然后单击 issue 为止。

结果

以下是从 ASDM 步骤得到的 CLI 配置：

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
```

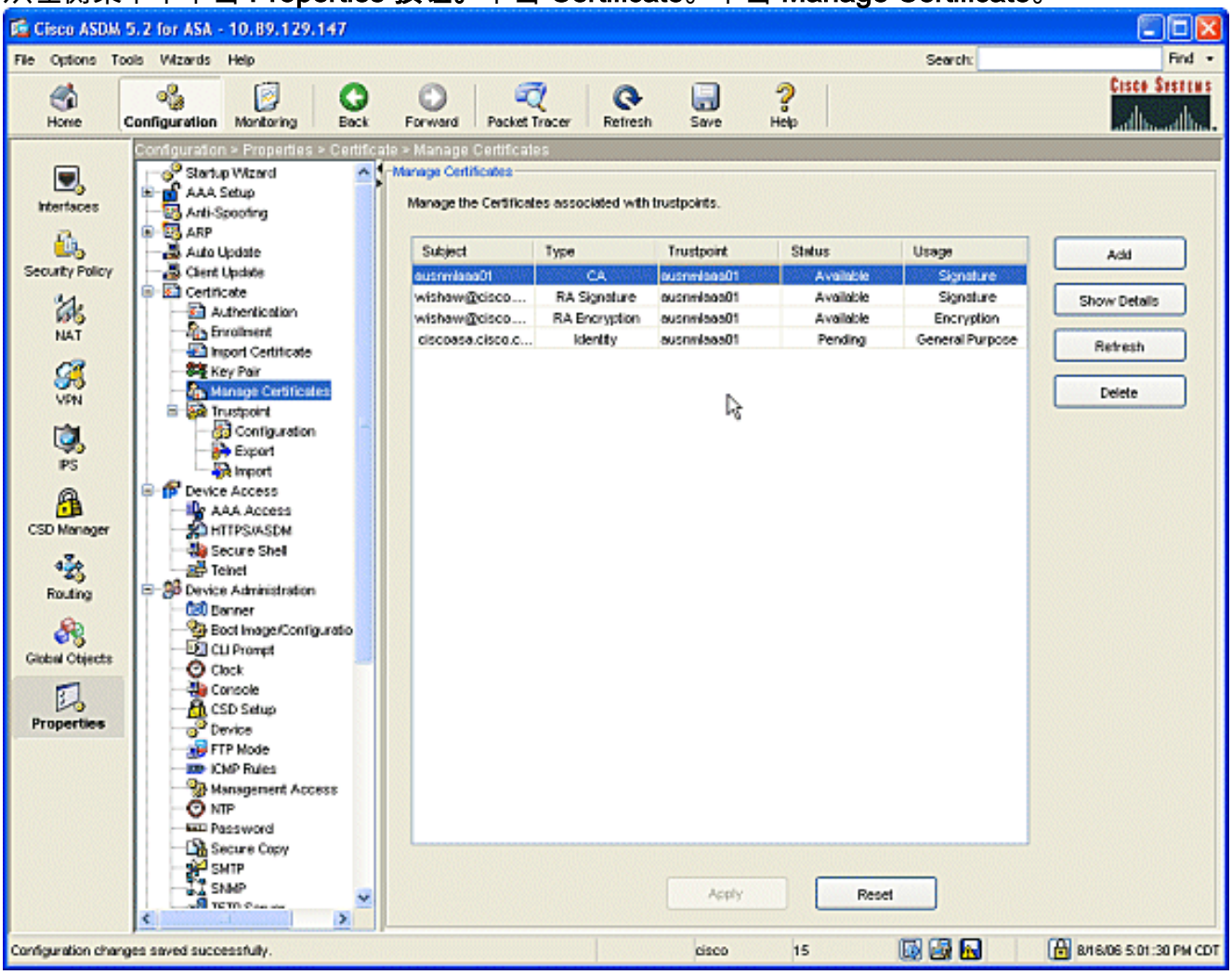
验证

使用本部分可确认配置能否正常运行。

检查和管理证书

检查和管理证书。

1. 打开 ASDM 应用程序，然后单击 **Configuration 按钮。**
2. 从左侧菜单中单击 **Properties 按钮。**单击 **Certificate。**单击 **Manage Certificate。**



命令

在 ASA 上，可以在命令行中使用若干 **show 命令以验证证书的状态。**

- 命令**show crypto ca certificates**用于查看有关证书、CA证书和任何注册机构(RA)证书的信息。
- 命令 **show crypto ca trustpoints 用于验证信任点配置。**
- 命令 **show crypto key mypubkey rsa 用于显示 ASA 的 RSA 公钥。**
- 命令 **show crypto ca crls 用于显示所有缓存的 CRL。**

注意：输出解释器工具(仅注册客户)(OIT)支持某些**show**命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

使用本部分可排除配置故障。

有关如何排除Microsoft Windows 2003 CA故障的详细信息 ，请参阅Windows Server 2003的公钥基础设施。

命令

注意：使用debug命令可能会对Cisco设备造成负面影响。使用 debug 命令之前，请参阅**有关 Debug 命令的重要信息。**

相关信息

- **配置 Cisco VPN 3000 集中器 4.0.x 以获得数字证书**