ASA で ASDM を使用して Microsoft Windows CA からデジタル証明書を取得する方法

内容

概要

デジタル証明書は、ネットワーク デバイスとネットワーク上のユーザの認証に使用できます。デジタル証明書は、ネットワーク ノード間の IPSec セッションのネゴシエーションに使用できます。

Cisco のデバイスでは、次の 3 つの主要な方法によりネットワーク上での自身のセキュアな識別が行われます。

1. **事前共有キー**：複数のデバイスが同じ共有秘密鍵を保持します。ピアでは、事前共有キーを含めたデータの鍵付きハッシュの計算と送信により相互認証を行います。受信側ピアでは自分の事前共有キーを使用して独自にハッシュを計算し、同じハッシュ値を得ることができた場合、両者が同じ秘密を共有していることになるので、相手側ピアが認証されます。この方法は手動的で、スケーラビリティに欠けています。
2. **自己署名証明書**：デバイスが自身の証明書を生成し、有効なものとして署名を行います。このタイプの証明書の用途は限られています。使用例としては、設定目的で SSH および HTTPS アクセスをするような場合です。接続を確立するには、ユーザ名とパスワードのペアが必要になります。**注：永続的な自己署名**証明書は、デバイスの不揮発性ランダムアクセスメモリ(NVRAM)に保存されるため、ルータのリロードに耐えることができます。詳細については、『永続的な自己署名証明書』を参照してください。この証明書の使用例としては

、SSL VPN（WebVPN）接続があります。

3. **認証局証明書**：通信を行う複数のノードの検証と認証をサードパーティが行います。各ノードが公開鍵と秘密鍵を保持します。公開鍵でデータを暗号化し、秘密鍵でデータを復号化します。両者が同じ発行元から証明書を取得しているため、互いの身元を確認できます。ASA デバイスでは、サードパーティから手動登録または自動登録の方法でデジタル証明書を取得できます。**注：選**択するデジタル証明書の登録方法と種類は、各サードパーティ製品の機能によって異なります。詳細については、証明書サービスのベンダーに問い合せてください。

Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）では、事前共有キーまたはサードパーティの Certificate Authority（CA; 認証局）から発行されたデジタル証明書を使用して、IPSec 接続を認証できます。また、自己署名デジタル証明書の作成も可能です。自己署名デジタル証明書は、SSH、HTTPS、および Cisco Adaptive Security Device Manager（ASDM）とデバイスの接続に使用します。

このドキュメントでは、ASA 用のデジタル証明書を Microsoft CA から自動的に取得するための手順を説明します。手動登録の方法については説明しません。このドキュメントでは ASDM を使用した設定手順を説明し、最終的な Command-Line Interface（CLI; コマンドライン インターフェイス）設定も示します。

Cisco IOS(R) プラットフォームを使用する場合の同様のシナリオについては、『拡張された登録コマンドを使用した Cisco IOS の証明書登録の設定例』を参照してください。

Cisco VPN 3000 シリーズ コンセントレータを使用する場合の同様のシナリオについては、『Cisco VPN 3000 Concentrator 4.7.x でデジタル証明書および SSL 証明書を取得するための設定』を参照してください。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

ASA デバイスの要件

- Microsoft(R) Windows 2003 Server を CA として設定する。Microsoft のドキュメントまたは『Public Key Infrastructure for Windows Server 2003』を参照してください。
- Cisco ASA または PIX バージョン 7.x を Adaptive Security Device Manager（ASDM）で設定できるようにする方法については、『ASDM 用の HTTPS アクセスの許可』を参照してください。
- 証明書サービス用のアドオン（mscep.dll）をインストールする。
- アドオンの実行可能ファイル（cepsetup.exe）を『Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services』から入手するか、mscep.dll ファイルを『Windows Server 2003 Resource Kit Tools』から入手する。**注：** Microsoft Windowsマシンで正しい日付、時刻、およびタイムゾーンを設定します。Network Time Protocol（NTP; ネットワーク タイム プロトコル）の使用を推奨します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Cisco Adaptive Security Device Manager バージョン 5.x 以降
- Microsoft Windows 2003 Server 認証局

関連製品

この設定は、Cisco PIX 500 シリーズ セキュリティ アプライアンス バージョン 7.x にも適用できます。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

Microsoft CA と証明書の交換を行うための ASA の設定

タスク

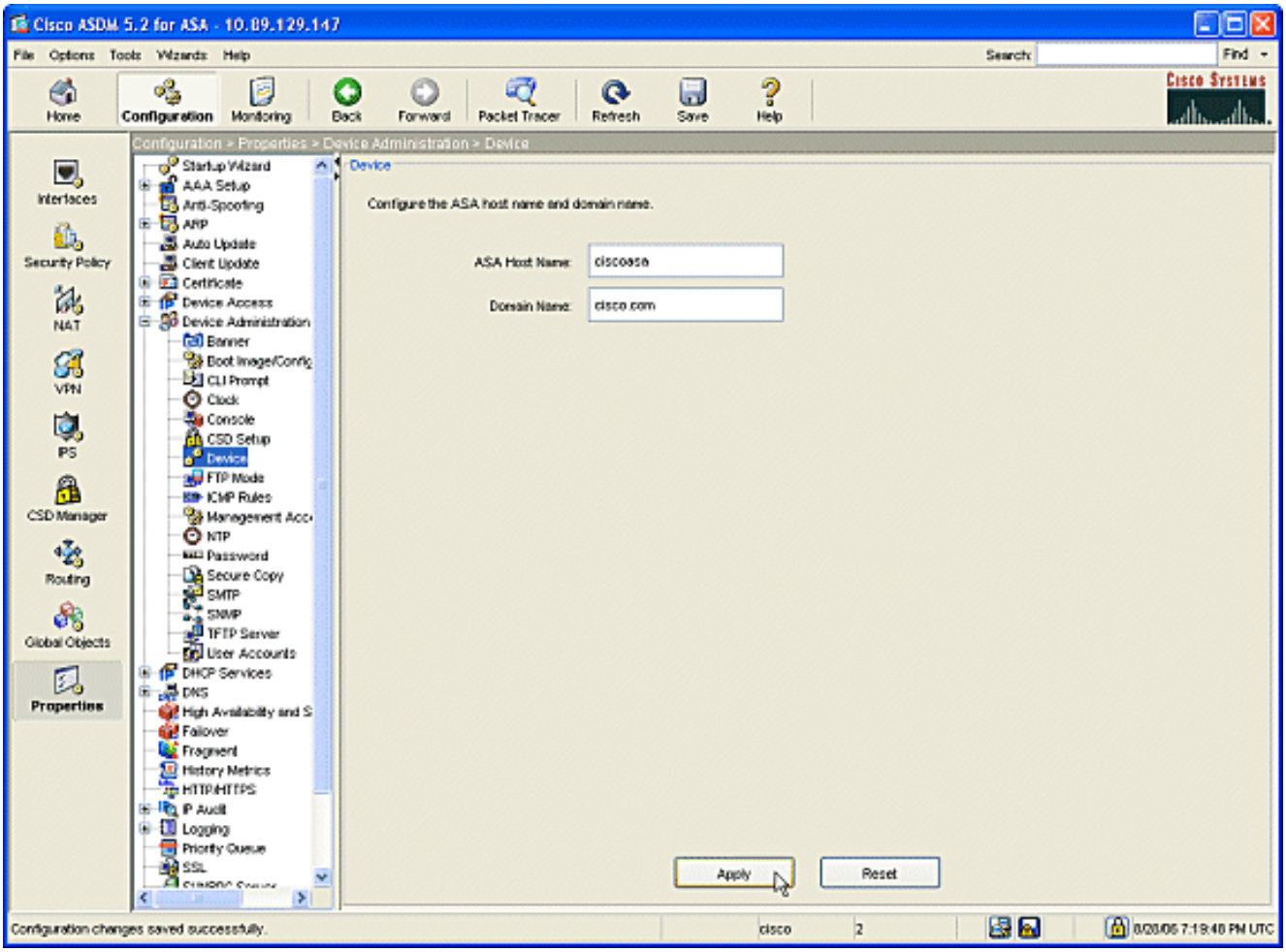
このセクションでは、Microsoft CA から証明書を受信するための ASA の設定方法について説明します。

ASA の設定手順

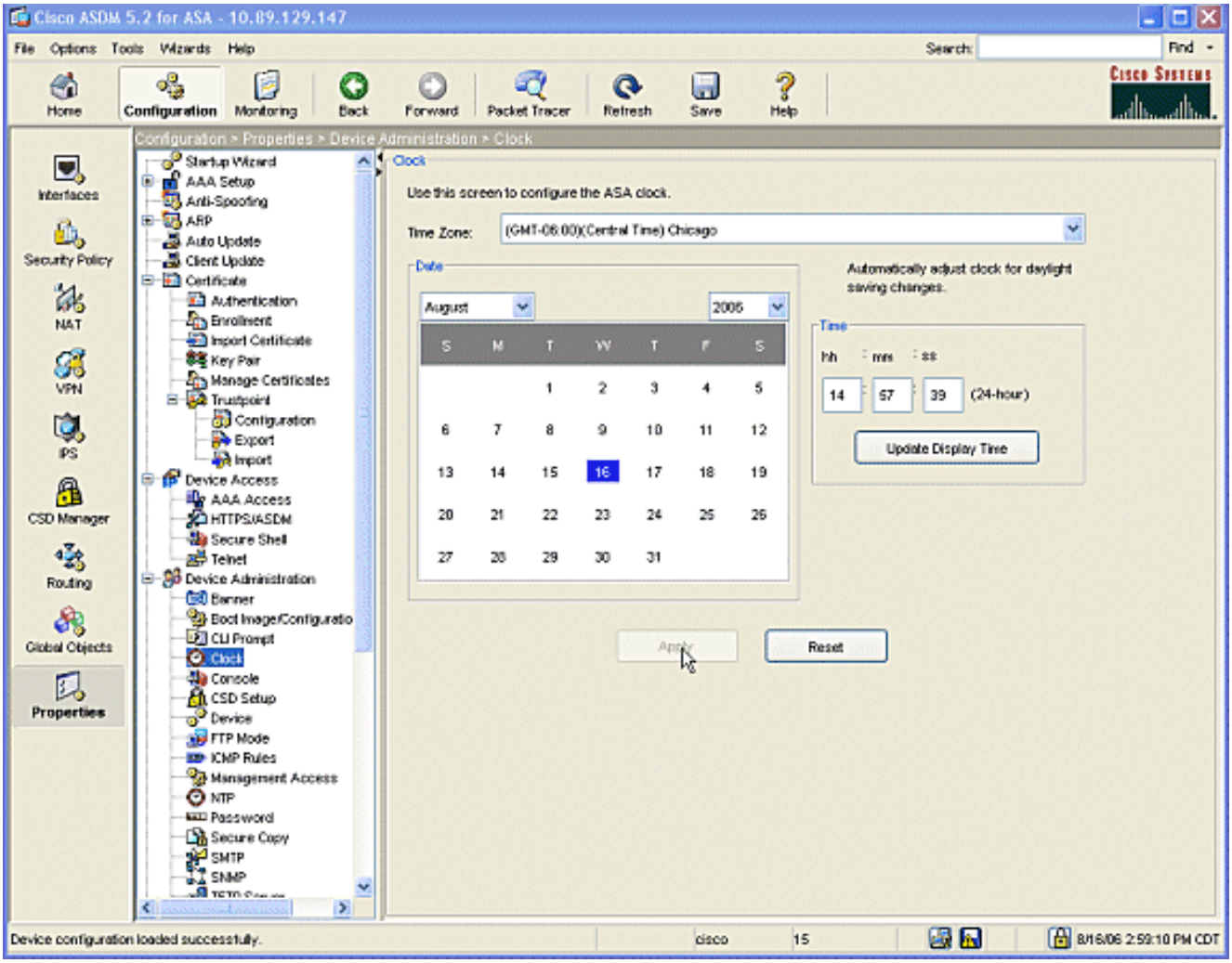
デジタル証明書では、証明書の有効性の確認項目の 1 つとして、日付、時刻、およびタイム ゾーン コンポーネントが使用されます。Microsoft CA およびすべてのデバイスに正しい日付と時刻を設定することが必要になります。Microsoft CA では証明書サービスへのアドオン（mscep.dll）を使用して、Cisco デバイスと証明書を共有します。

次の手順を実行して ASA を設定します。

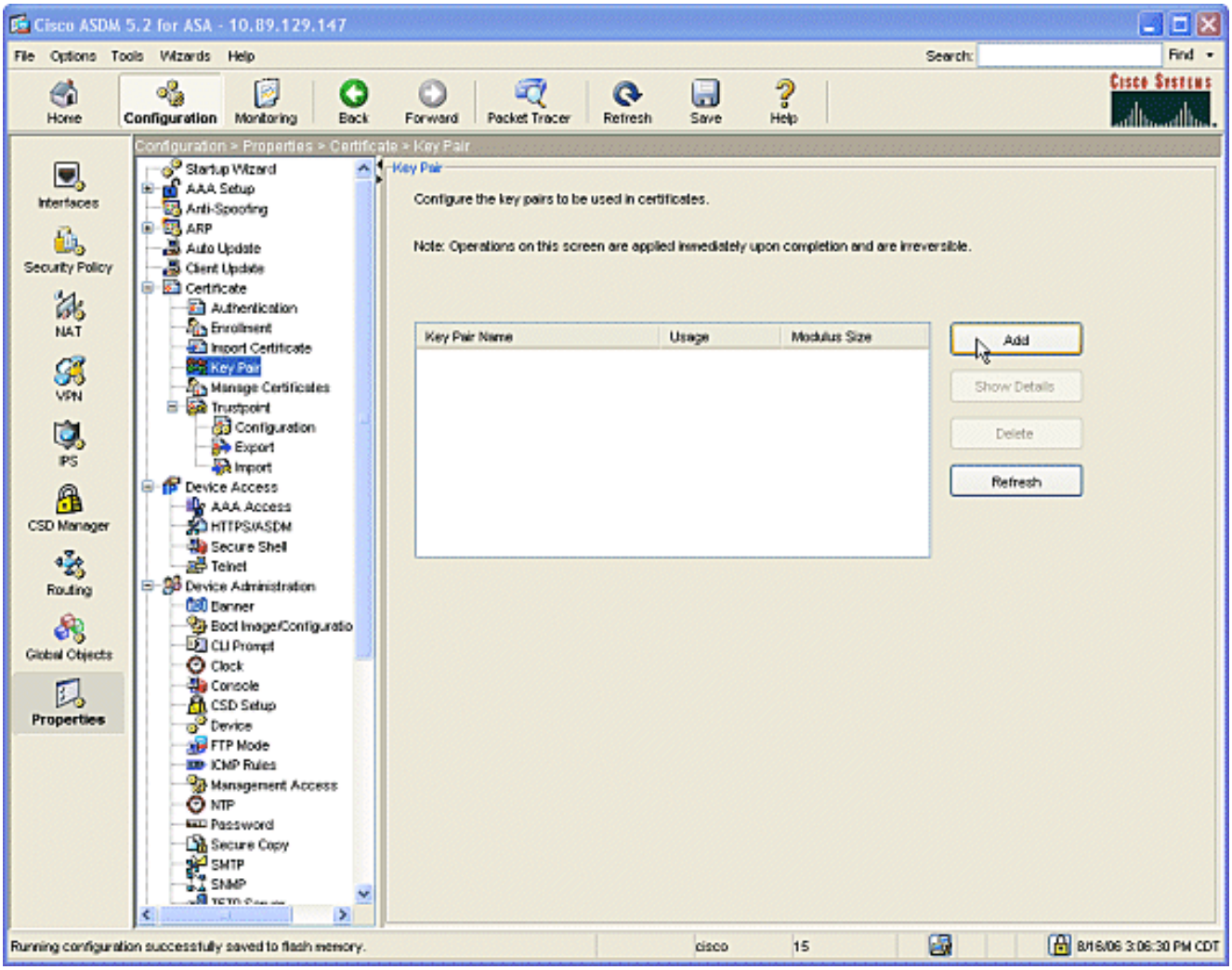
1. ASDM アプリケーションを開いて Configuration ボタンをクリックします。左側のメニューから Properties ボタンをクリックします。ナビゲーション ペインで、[Device Administration] > [Device] の順にクリックします。ASA のホスト名とドメイン名を入力します。[Apply] をクリックします。プロンプトが表示されたら、[Save] > [Yes] の順にクリックします。



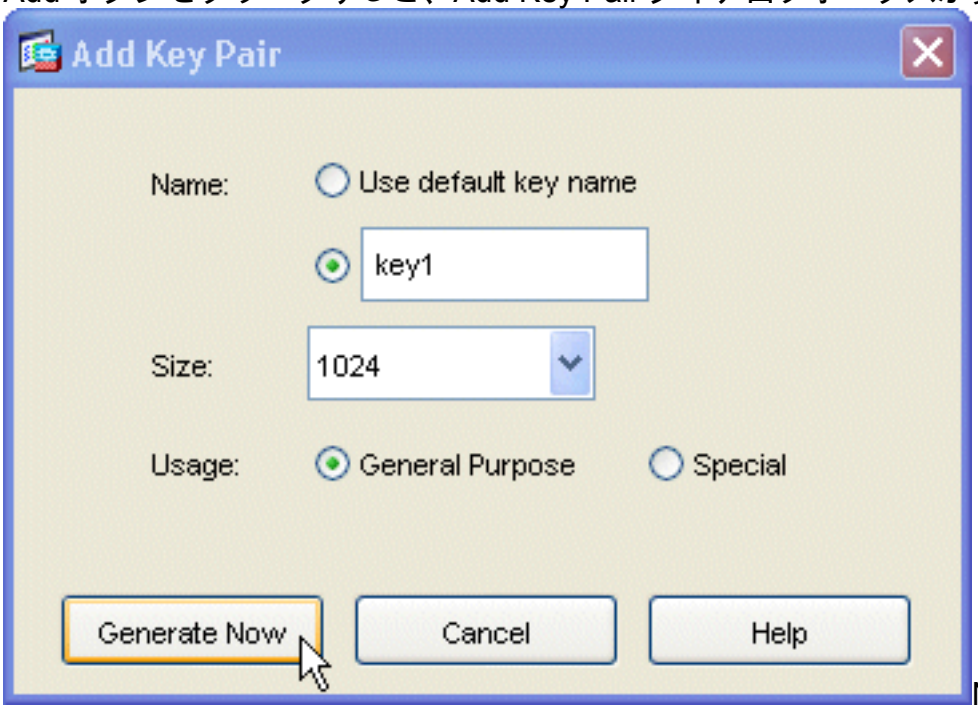
2. ASA を正しい日付、時刻、および時間帯で設定します。この作業は、デバイスの証明書を生成するための大切な手順です。可能な限り NTP サーバを使用します。ナビゲーション ペインで、[Device Administration] > [Clock] の順にクリックします。Clock ウィンドウでフィールドおよびドロップダウンの矢印を使用して、正しい日付、時刻、時間帯を設定します。



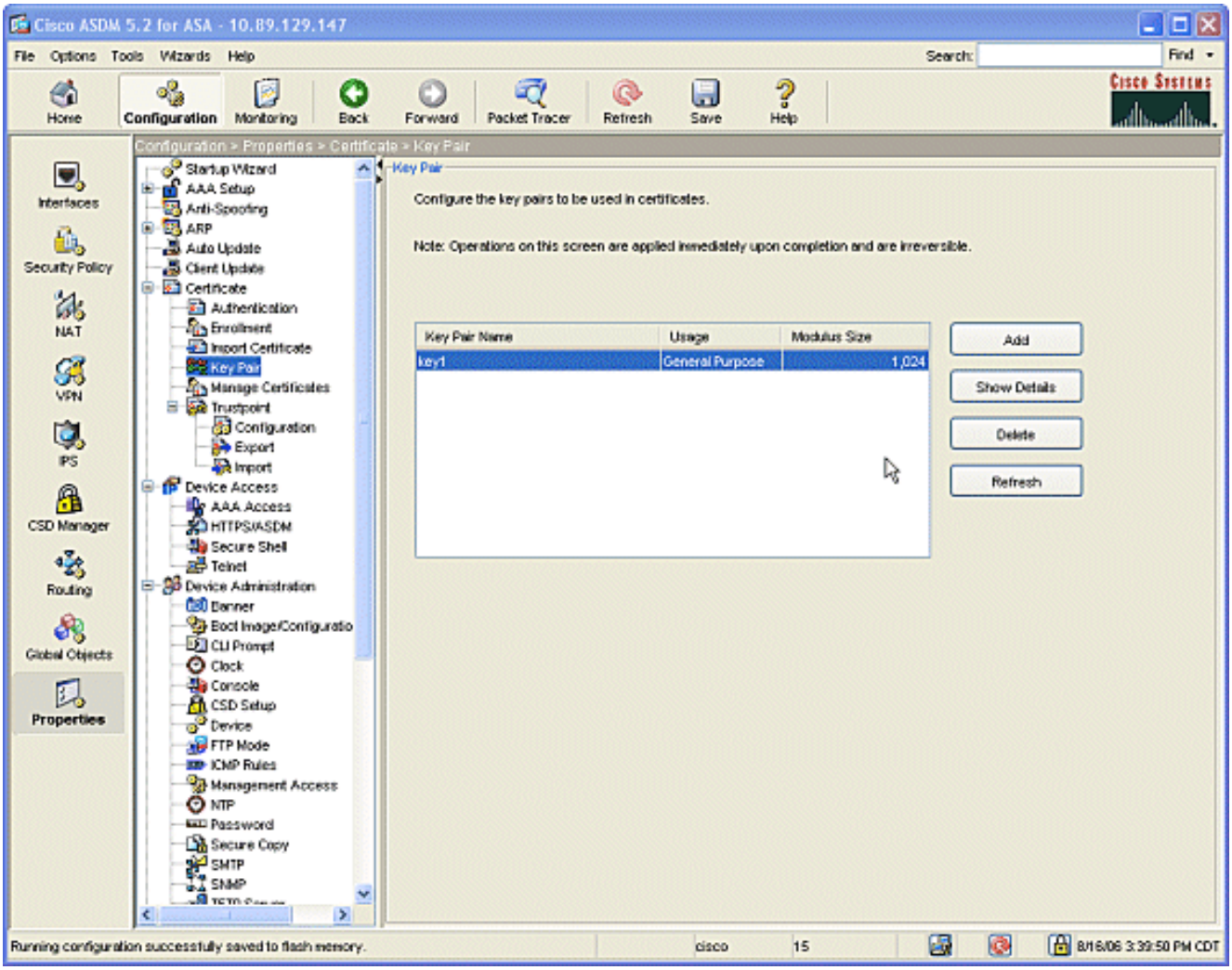
3. ASA は自身のキー ペア（秘密鍵と公開鍵）を保持する必要があります。 公開鍵は Microsoft CA に送信されます。ナビゲーション ペインで、[Certificate] > [Key Pair] の順にクリックします。



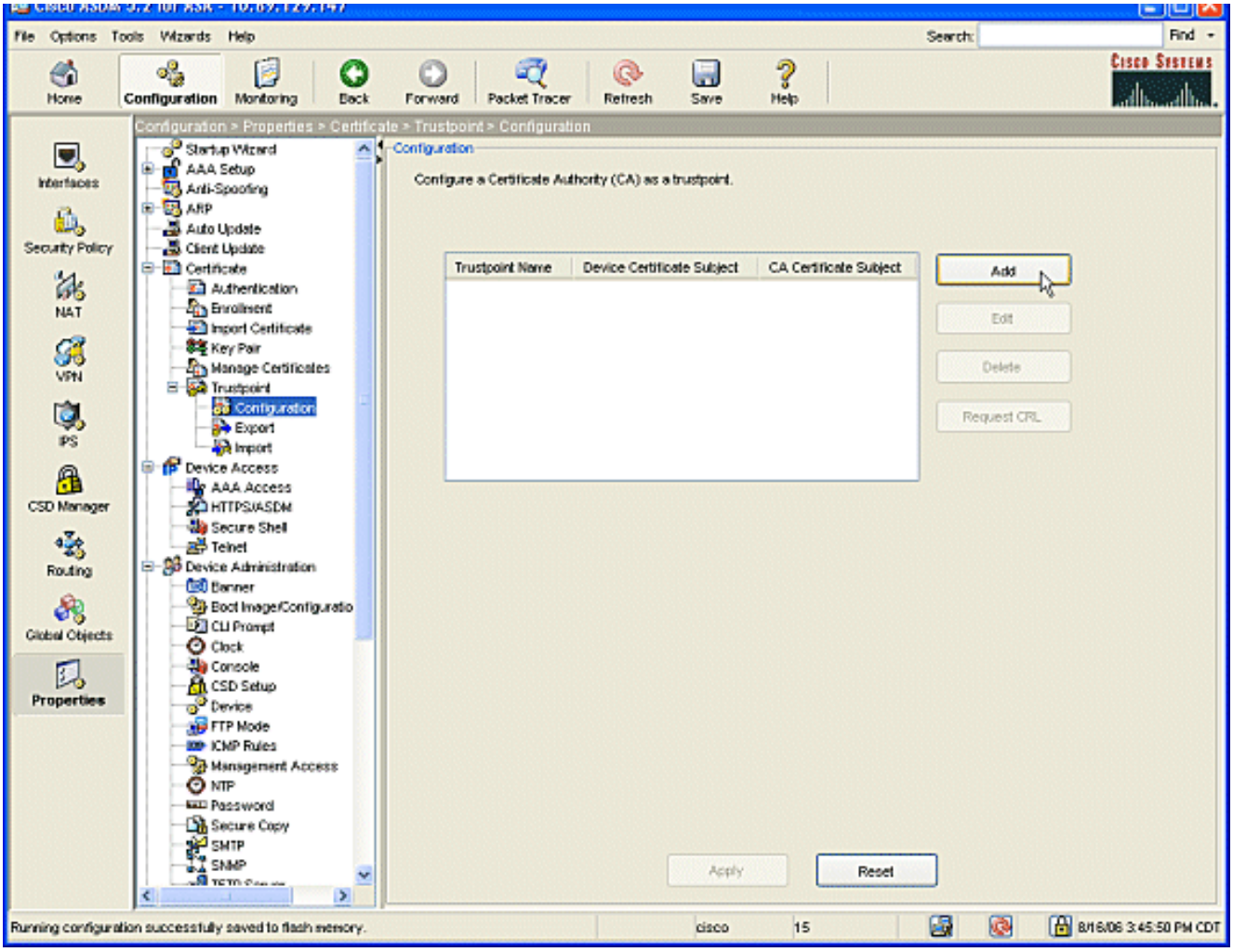
Add ボタンをクリックすると、Add Key Pair ダイアログボックスが表示されます。



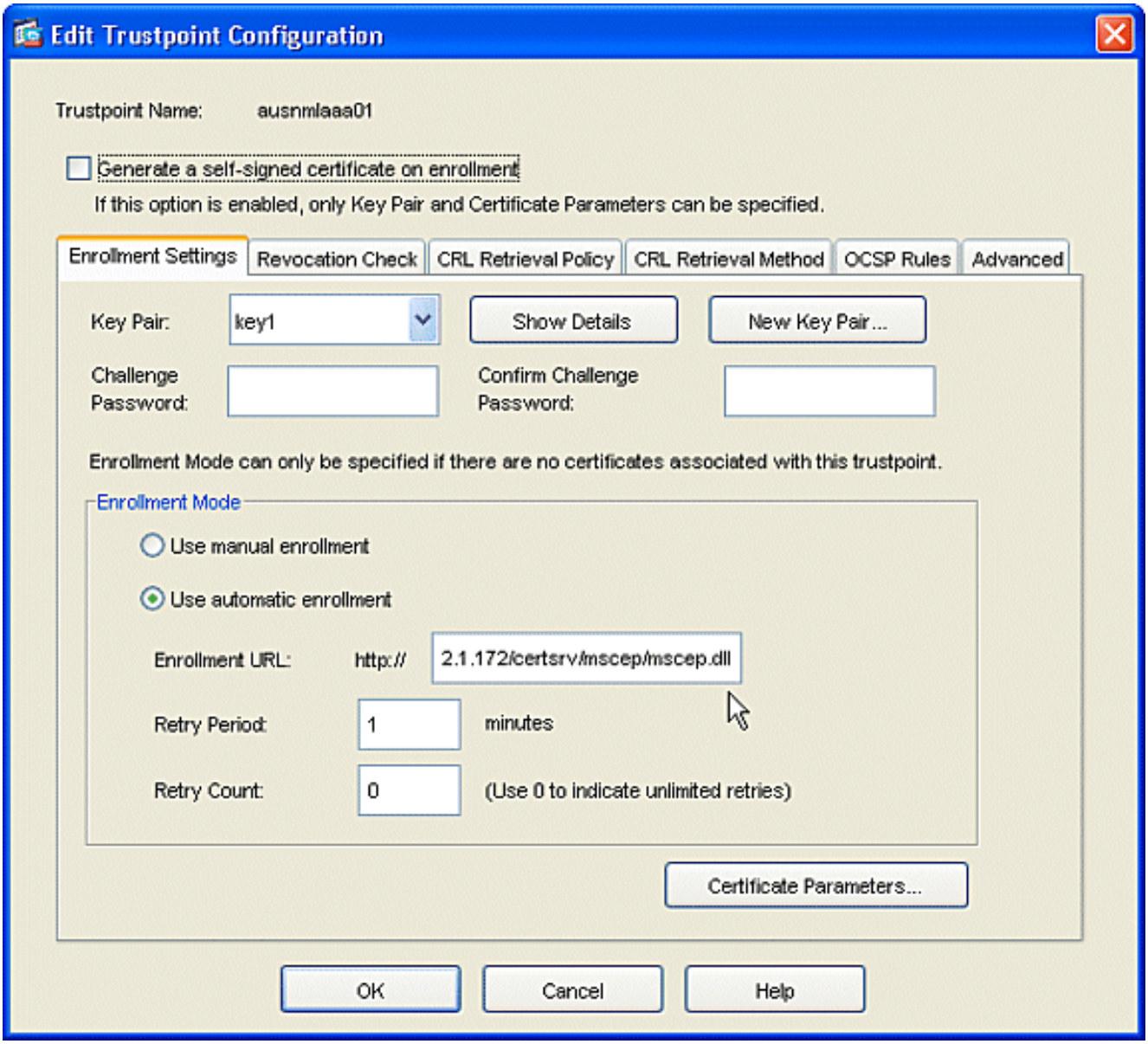
Name 領域の空白のフィールドの横にあるオプション ボタンにチェックマークを入れ、鍵の名前を入力します。[Size:]矢印（ドロップダウン ボックスの横）をクリックして鍵のサイズを選択するか、デフォルトを受け入れます。Usage で General Purpose オプション ボタンにチェックマークを入れます。Generate Now ボタンをクリックして鍵を再作成し、Key Pair ウィンドウに戻ります。このウィンドウでキー ペアの情報を確認できます。



4. Microsoft CA を信頼するための設定を行います。ナビゲーション ペインで、[Trustpoint] > [Configuration] の順にクリックします。Configuration ウィンドウで Add ボタンをクリックします。

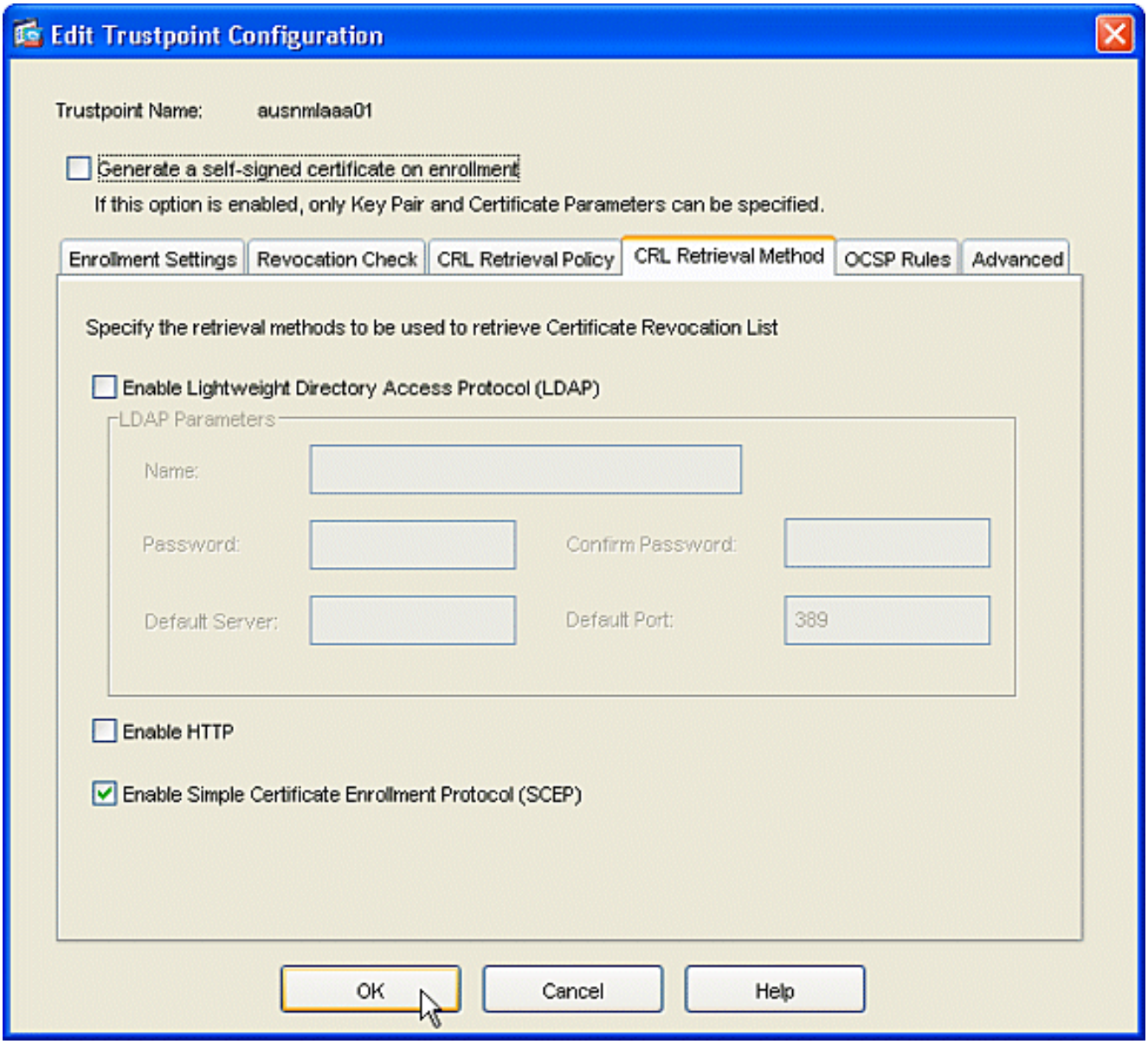


[Edit Trustpoint Configuration] ウィンドウが表示されます。

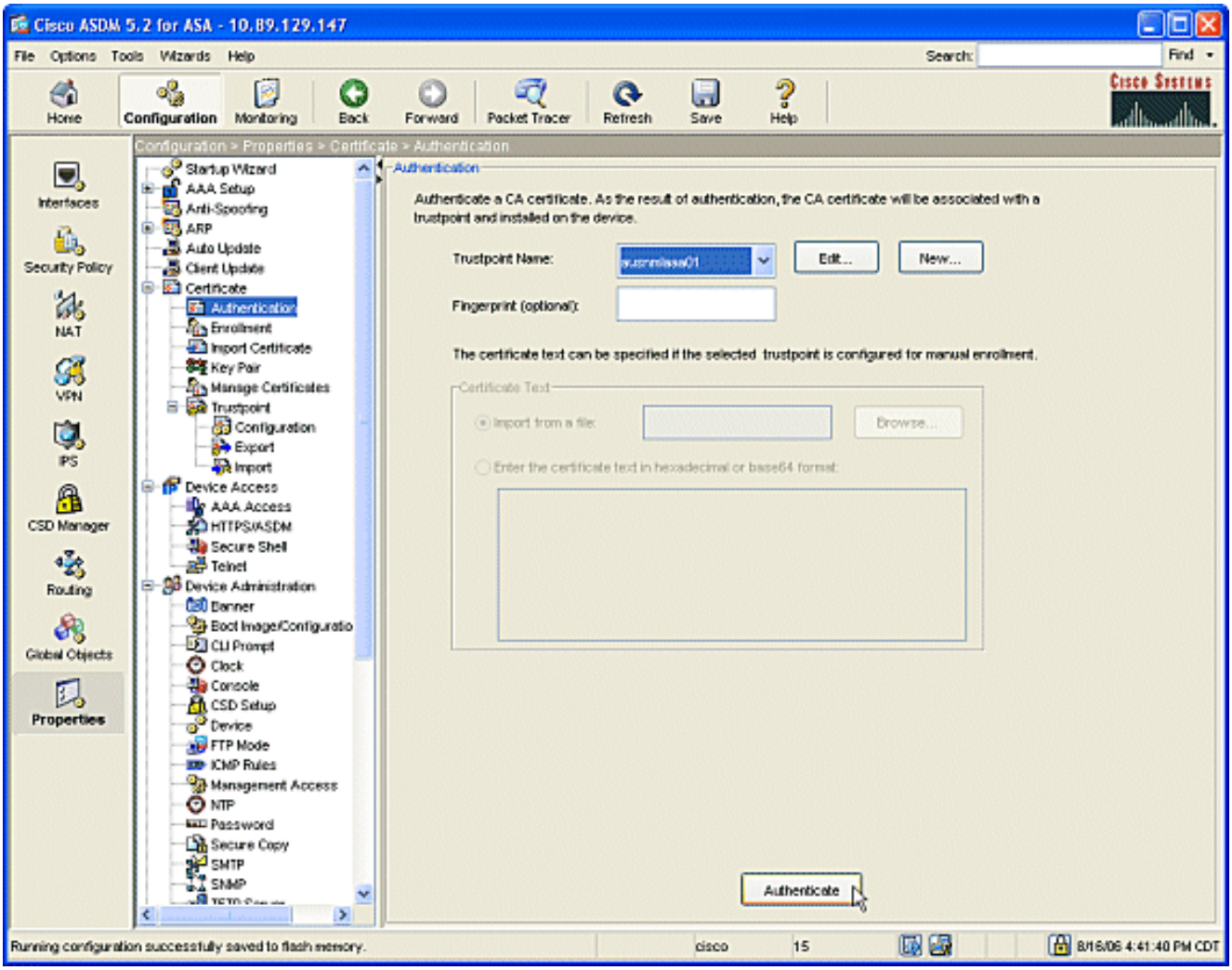


CA の名前を使ってトラストポイントの名前を入力します。[Key Pair:]矢印（ドロップダウン ボックスの横）をクリックして、作成したキー ペアの名前を選択します。[Use automatic enrollment] **オプション ボタンをオンにして、次の Microsoft CA の URL を入力します。http://CA_IP_Address/certsrv/mscep/mscep.dll**。

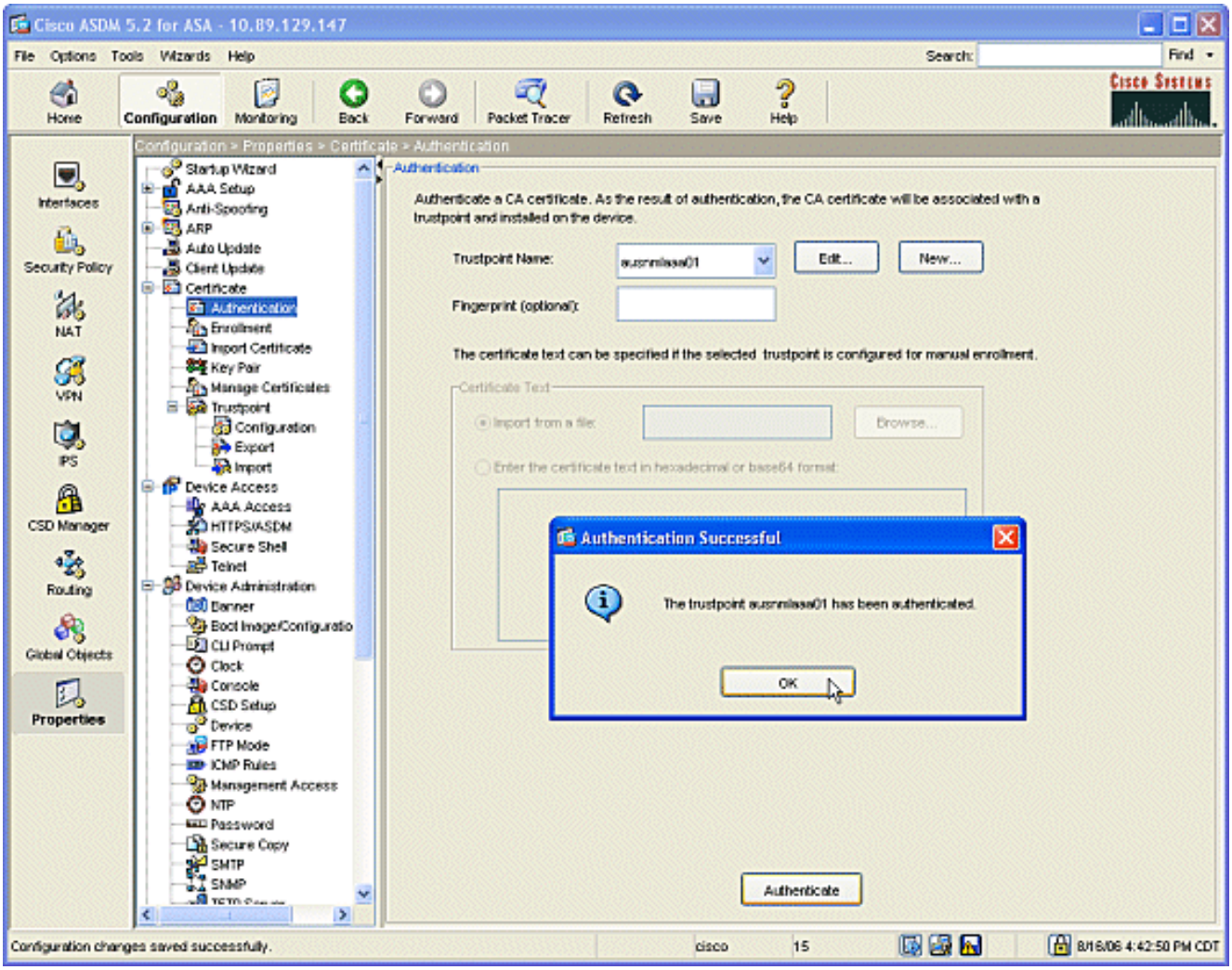
5. Crl Retrieval Method タブをクリックします。Enable HTTP と Enable Lightweight Directory Access Protocol (LDAP) のチェックボックスのチェックマークを外します。Enable Simple Certificate Enrollment Protocol (SCEP) チェックボックスにチェックマークを入れます。その他すべてのタブの設定は、デフォルト設定のままにしておきます。OK ボタンをクリックします。



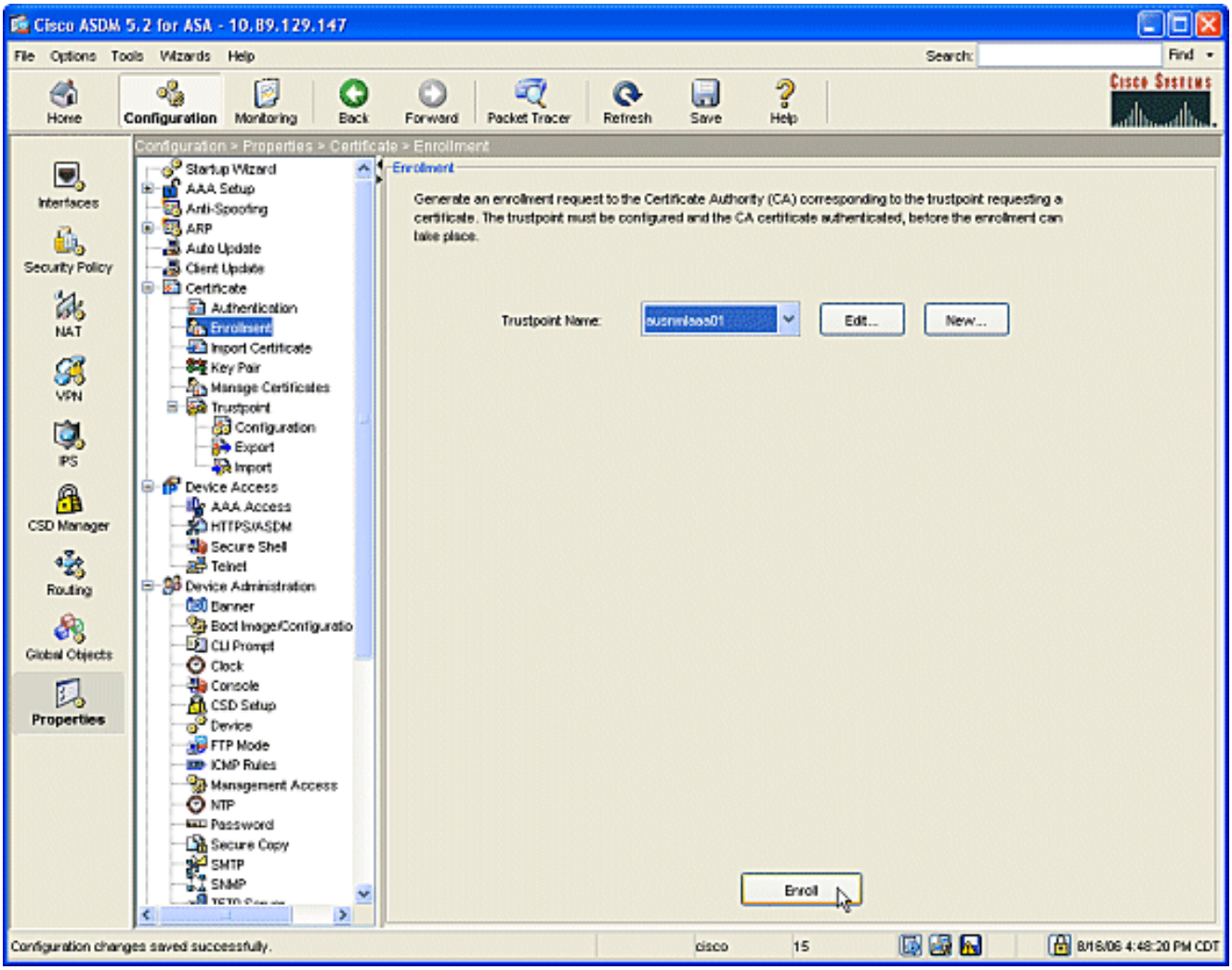
6. Microsoft CA で認証と登録を行います。ナビゲーション ペインで、[Certificate] > [Authentication] の順にクリックします。新しく作成されたトラストポイントが [Trustpoint Name:]フィールドにプローブ間隔値を入力します。Authenticate ボタンをクリックします。



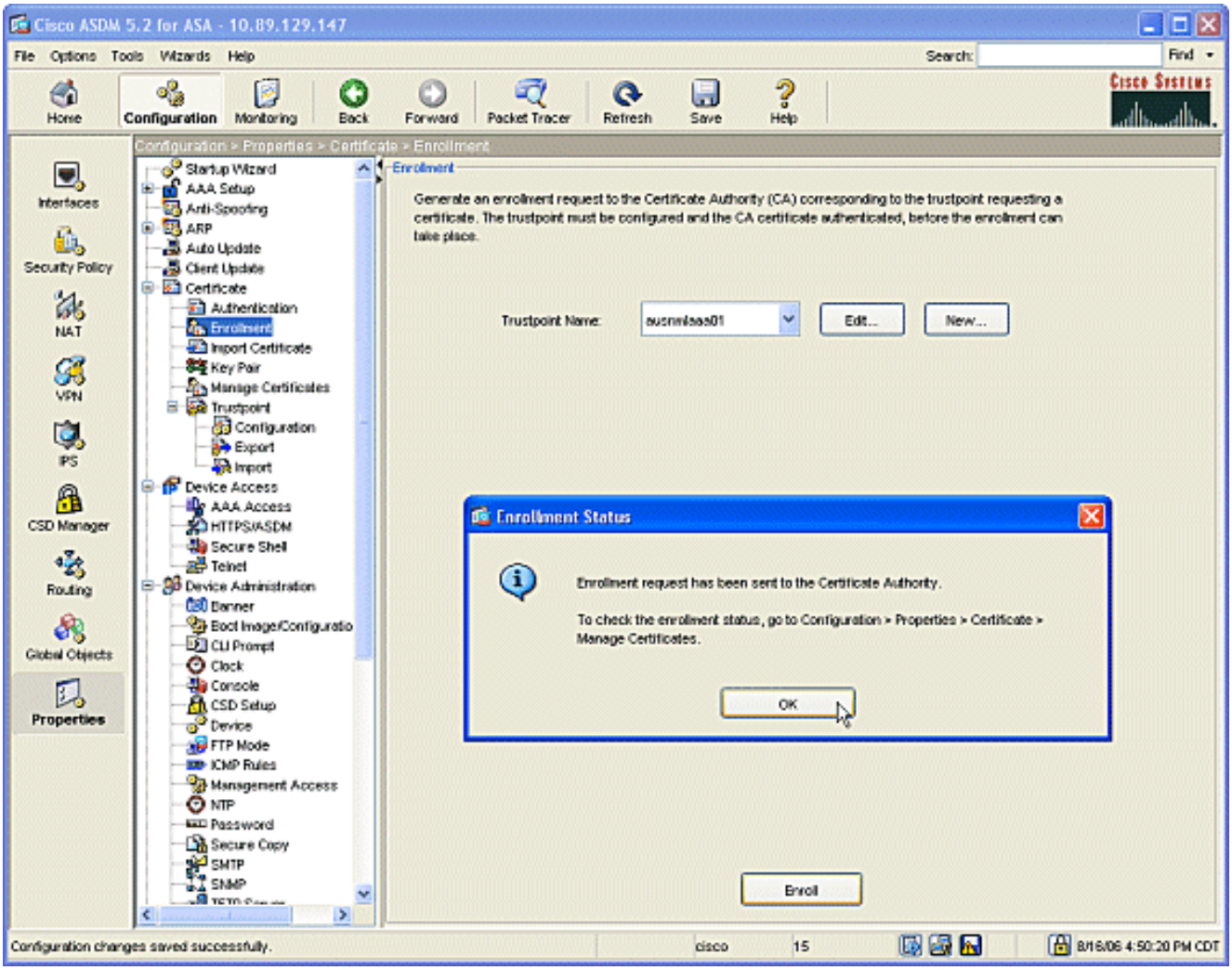
7. トラストポイントが認証されたことを通知するダイアログボックスが表示されます。OK ボタンをクリックします。



8. ナビゲーション ペインで Enrollment をクリックします。Trustpoint Name フィールドにトラストポイント名が表示されていることを確認し、Enroll ボタンをクリックします。



9. 要求が CA に送信されたことを通知するダイアログボックスが表示されます。OK ボタンをクリックします。



注： Microsoft Windows のスタンドアロン マシンで、CA に送信されたすべての要求に対して証明書を発行する必要があります。Microsoft Server で証明書を右クリックして issue をクリックするまで、証明書は保留状態になります。

成果

ASDM での設定の結果、次のような CLI 設定が得られます。

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
```

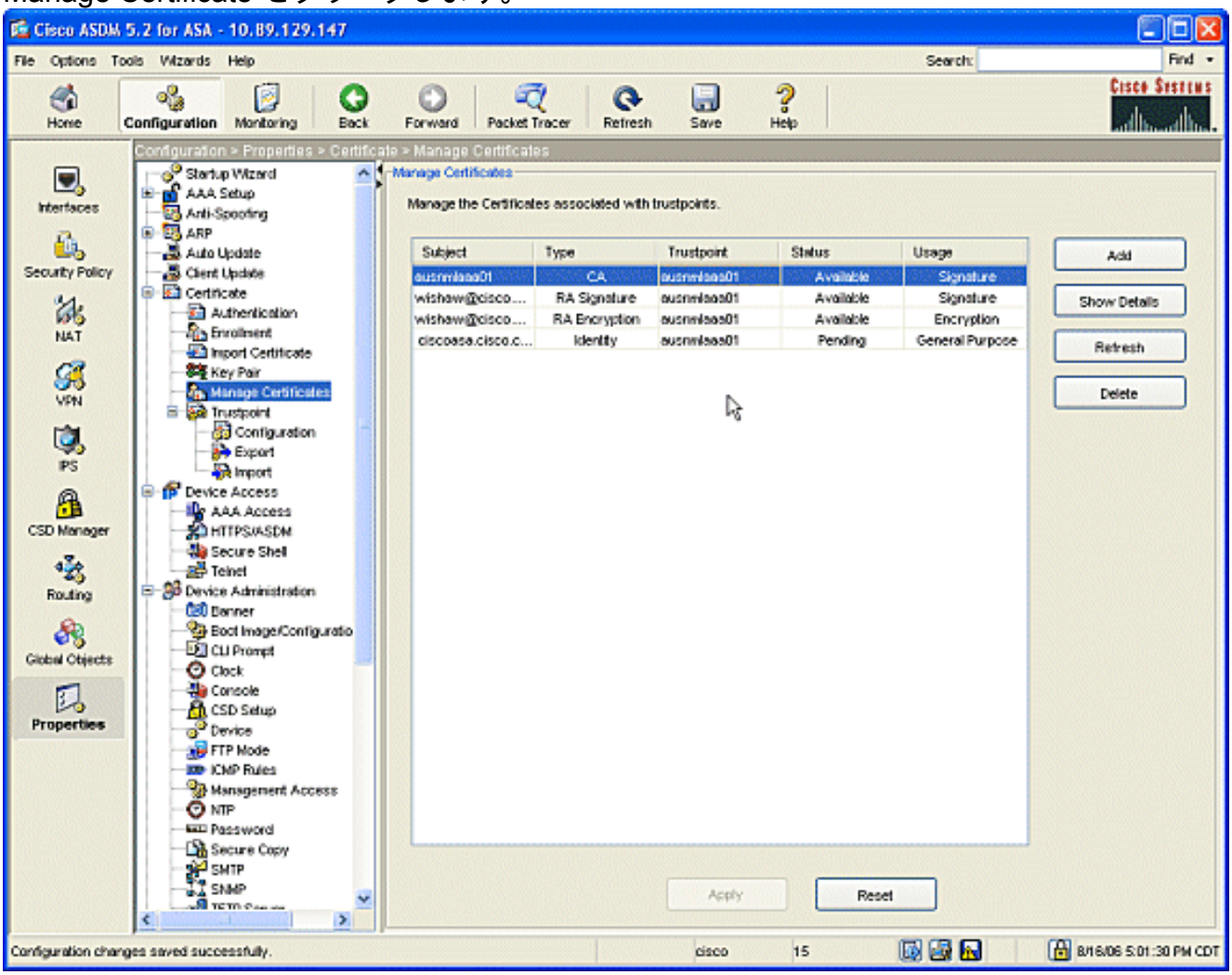
確認

ここでは、設定が正常に機能しているかどうかを確認します。

証明書の確認と管理

証明書の確認と管理を行います。

1. ASDM アプリケーションを開いて Configuration ボタンをクリックします。
2. 左側のメニューから Properties ボタンをクリックします。Certificate をクリックします。Manage Certificate をクリックします。



コマンド

ASA では、コマンドラインで各種の show コマンドを使用し、証明書の状況を確認できます。

- show crypto ca certificates コマンドを使用すると、自身の証明書、CA 証明書、および Registration Authority（RA; 登録局）証明書に関する情報が表示されます。
- show crypto ca trustpoints コマンドを使用すると、トラストポイントの設定を確認できます。
- show crypto key mypubkey rsa コマンドを使用すると、ASA の RSA 公開鍵が表示されます。
- show crypto ca crls コマンドを使用すると、キャッシュされているすべての CRL が表示されます。

注：アウトプットインタープリタツール(登録ユーザ専用)(OIT)は、特定のshowコマンドをサポートしています。OIT を使用して、show コマンドの出力の分析を表示します。

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

Microsoft Windows 2003 CAのトラブルシューティング方法の詳細は、『Public Key Infrastructure for Windows Server 2003』を参照してください。

コマンド

注：debugコマンドを使用すると、シスコデバイスに悪影響が及ぶ可能性があります。debug コマンドを使用する前に、「debug コマンドの重要な情報」を参照してください。

関連情報

- **Cisco VPN 3000 コンセントレータ 4.0.x でデジタル証明書を取得するための設定**