

PIX/ASA : Obtain a Digital Certificate for the Security Appliance from a Microsoft Windows 2003 CA using ASDM

Document ID: 71050

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Configure the ASA to Exchange Certificates with the Microsoft CA

- Task
- Instructions to Configure the ASA
- Results

Verify

- Check and Manage Your Certificate
- Commands

Troubleshoot

- Commands

Related Information

Introduction

Digital certificates can be used to authenticate network devices and users on the network. They can be used to negotiate IPSec sessions between network nodes.

Cisco devices identify themselves securely on a network in three main ways:

1. **Pre-Shared Keys.** Two or more devices can have the same shared secret key. Peers authenticate each other by computing and sending a keyed hash of data that includes the preshared key. If the receiving peer is able to create the same hash independently using its preshared key, it knows that both peers must share the same secret, thus authenticating the other peer. This method is manual and not very scalable.
2. **Self-Signed Certificates.** A device generates its own certificate and signs it as being valid. This type of certificate should have limited usage. Using this certificate with SSH and HTTPS access for configuration purposes are good examples. A separate username/password pair is needed to complete the connection.

Note: Persistent Self-Signed Certificates survive router reloads because they are saved in the nonvolatile random-access memory (NVRAM) of the device. Refer to Persistent Self-Signed Certificates for more information. One good example of use is with SSL VPN (WebVPN) connections.

3. **Certificate Authority Certificate.** A third party validates and authenticates the two or more nodes that attempt to communicate. Each node has a public and private key. The public key encrypts data, and the private key decrypts data. Because they have obtained their certificates from the same source, they can be assured of their respective identities. The ASA device can obtain a digital certificate from a third-party with a manual enrollment method or an automatic enrollment method.

Note: The enrollment method and type of digital certificate you choose is dependent upon the features and functions of each third-party product. Contact the vendor of the certificate service for more information.

The Cisco Adaptive Security Appliance (ASA) can use pre-shared keys or digital certificates provided by a third-party Certificate Authority (CA) to authenticate IPSec connections. In addition, the ASA can produce its own self-signed digital certificate. This should be used for SSH, HTTPS, and Cisco Adaptive Security Device Manager (ASDM) connections to the device.

This document demonstrates the procedures necessary to automatically obtain a digital certificate from a Microsoft Certificate Authority (CA) for the ASA. It does not include the manual method of enrollment. This document uses ASDM for the configuration steps, as well as presents the final command-line interface (CLI) configuration.

Refer to Cisco IOS Certificate Enrollment Using Enhanced Enrollment Commands Configuration Example in order to learn more about the same scenario with Cisco IOS® platforms.

Refer to Configuring the Cisco VPN 3000 Concentrator 4.7.x to Get a Digital Certificate and a SSL Certificate in order to learn more about the same scenario with the Cisco VPN 3000 Series Concentrator.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

Requirements for the ASA device

- Configure the Microsoft® Windows 2003 Server as a CA.

Refer to your Microsoft documentation or to Public Key Infrastructure for Windows Server 2003

- In order to allow the Cisco ASA or PIX Version 7.x to be configured by the Adaptive Security Device Manager (ASDM), refer to Allowing HTTPS Access for ASDM.
- Install the Add-on for Certificate Services (mscep.dll).
- Obtain the executable file (cepsetup.exe) for the Add-on from the Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services or the mscep.dll file from the Windows Server 2003 Resource Kit Tools .

Note: Configure the correct date, time, and time zone on the Microsoft Windows machine. The use of the Network Time Protocol (NTP) is highly recommended but not necessary.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series Adaptive Security Appliance, Software Version 7.x and later
- Cisco Adaptive Security Device Manager Version 5.x and later
- Microsoft Windows 2003 Server Certificate Authority

Related Products

This configuration can also be used with Cisco PIX 500 Series Security Appliance Version 7.x.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure the ASA to Exchange Certificates with the Microsoft CA

Task

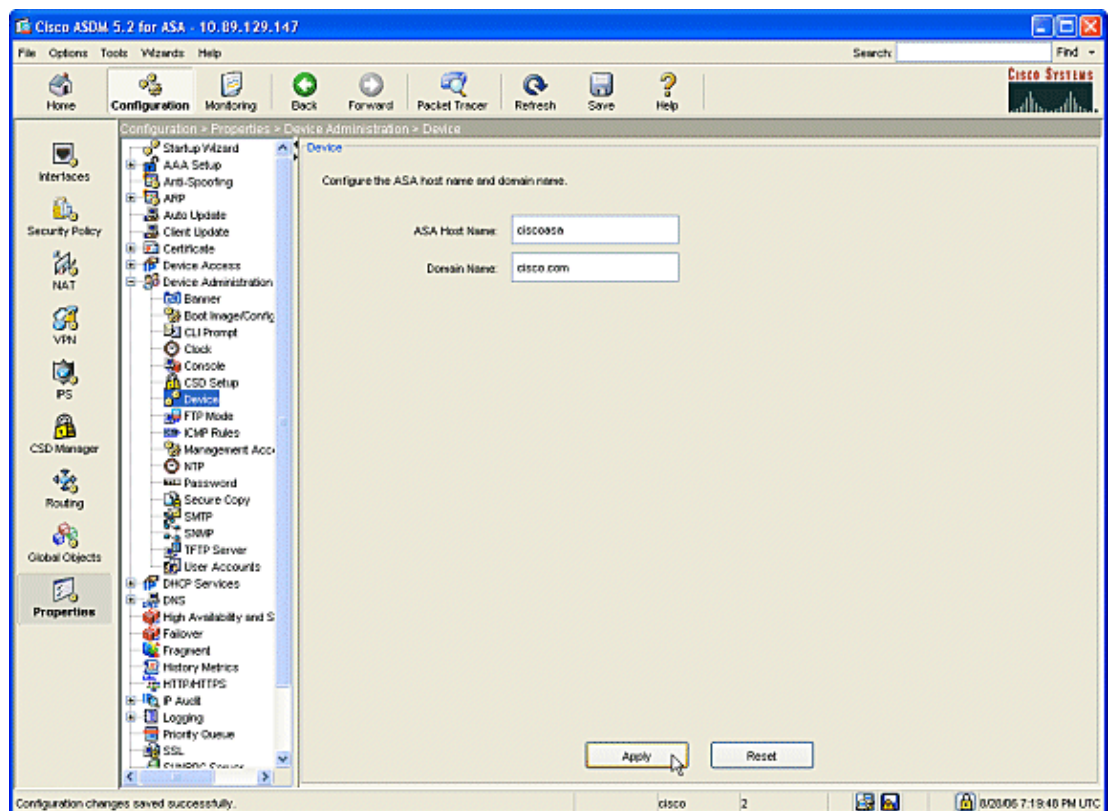
In this section, you are shown how to configure the ASA to receive a certificate from the Microsoft Certificate Authority.

Instructions to Configure the ASA

Digital certificates use the date/time/time zone component as one of the checks for certificate validity. It is imperative to configure the Microsoft CA and all your devices with the correct date and time. The Microsoft CA uses an add-on (mscep.dll) to its Certificate Services in order to share certificates with Cisco devices.

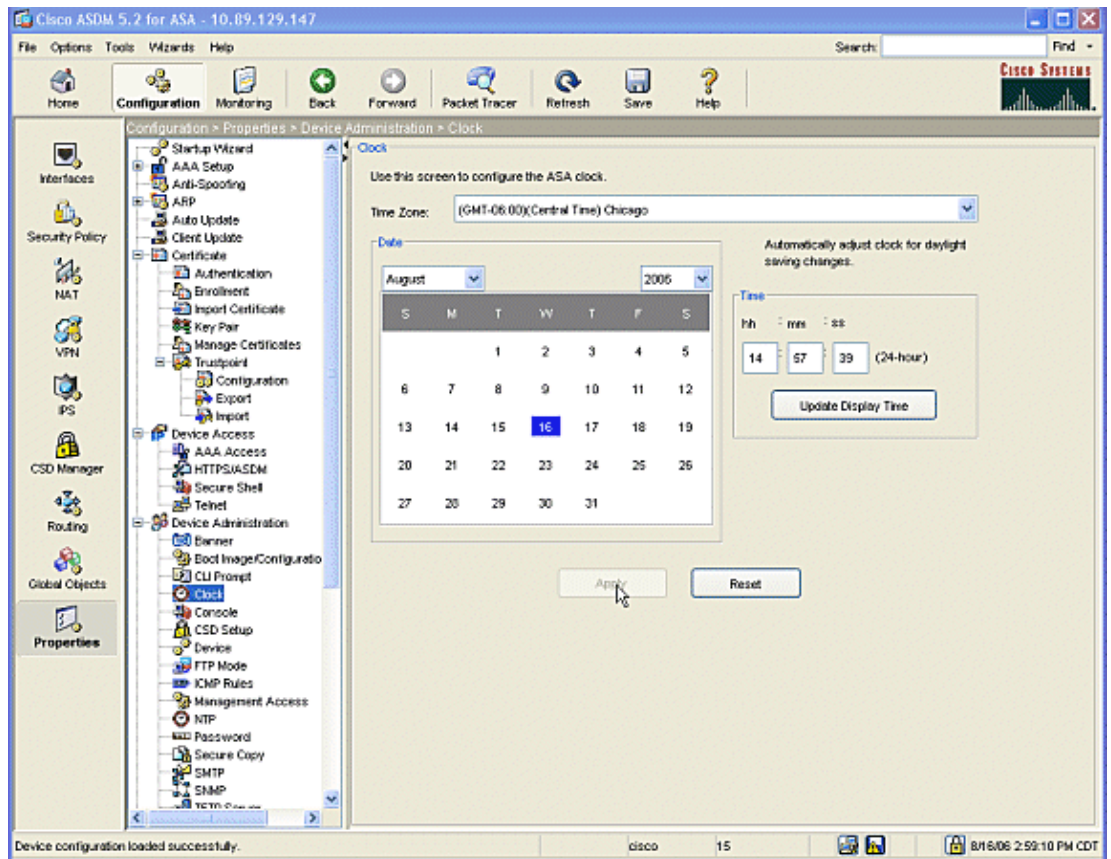
Complete these steps to configure the ASA:

1. Open the ASDM application and click the **Configuration** button.
 - a. From the left menu, click the **Properties** button.
 - b. From the navigation pane, click **Device Administration > Device**.
 - c. Enter a Host Name and Domain Name for the ASA. Click **Apply**.
 - d. When prompted, click **Save > Yes**.



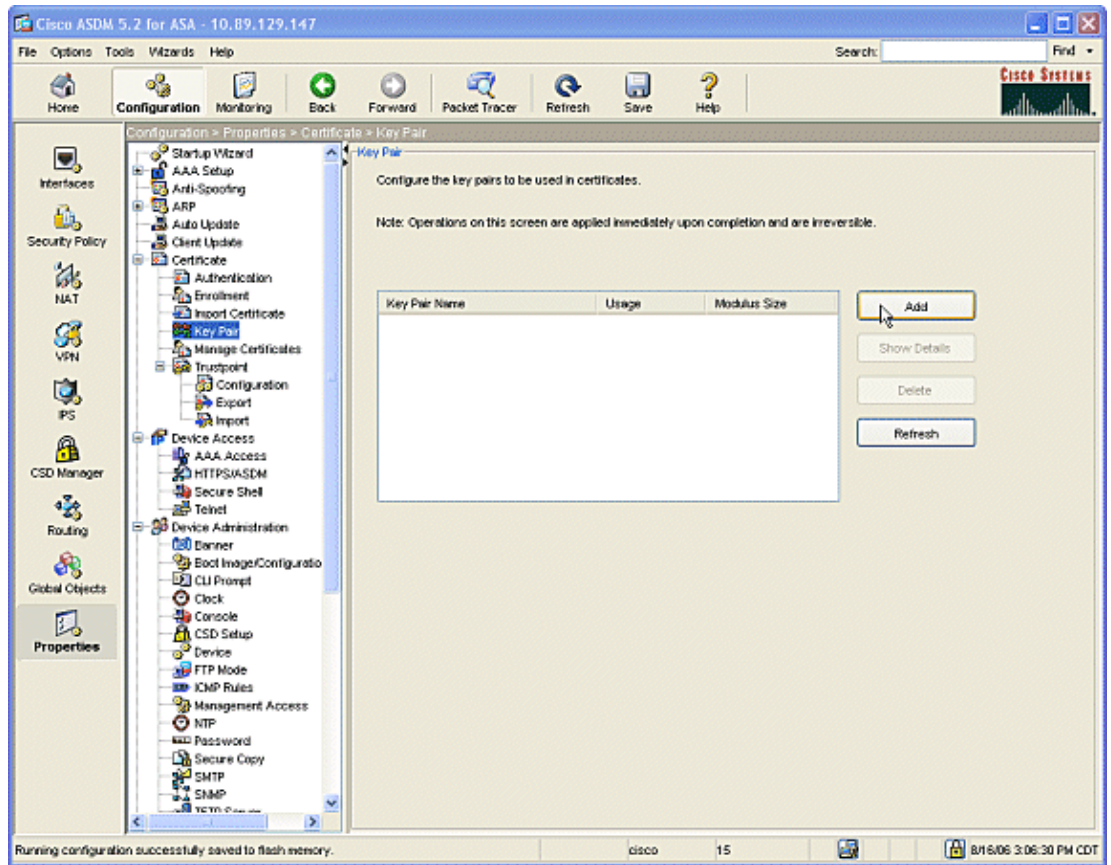
2. Configure the ASA with the correct date, time, and time zone. This is important for certificate generation of the device. Use an NTP server, if possible.

- a. From the navigation pane, click **Device Administration > Clock**.
- b. In the Clock window, use the fields and drop-down arrows to set the correct date, time, and time zone.

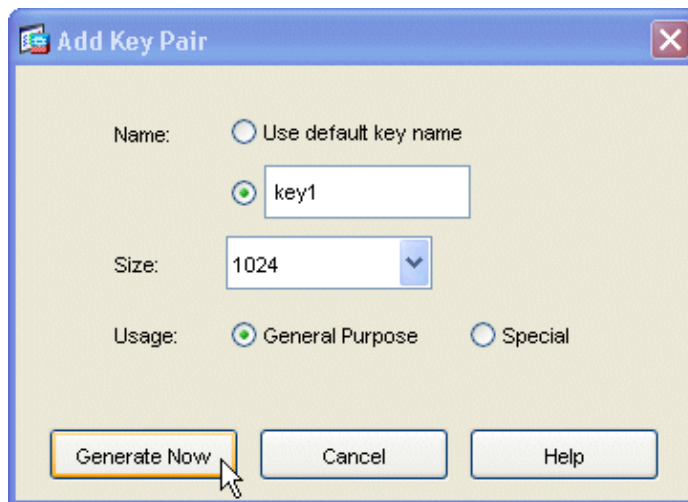


3. The ASA must have its own key pair (private and public keys). The public key will be sent to the Microsoft CA.

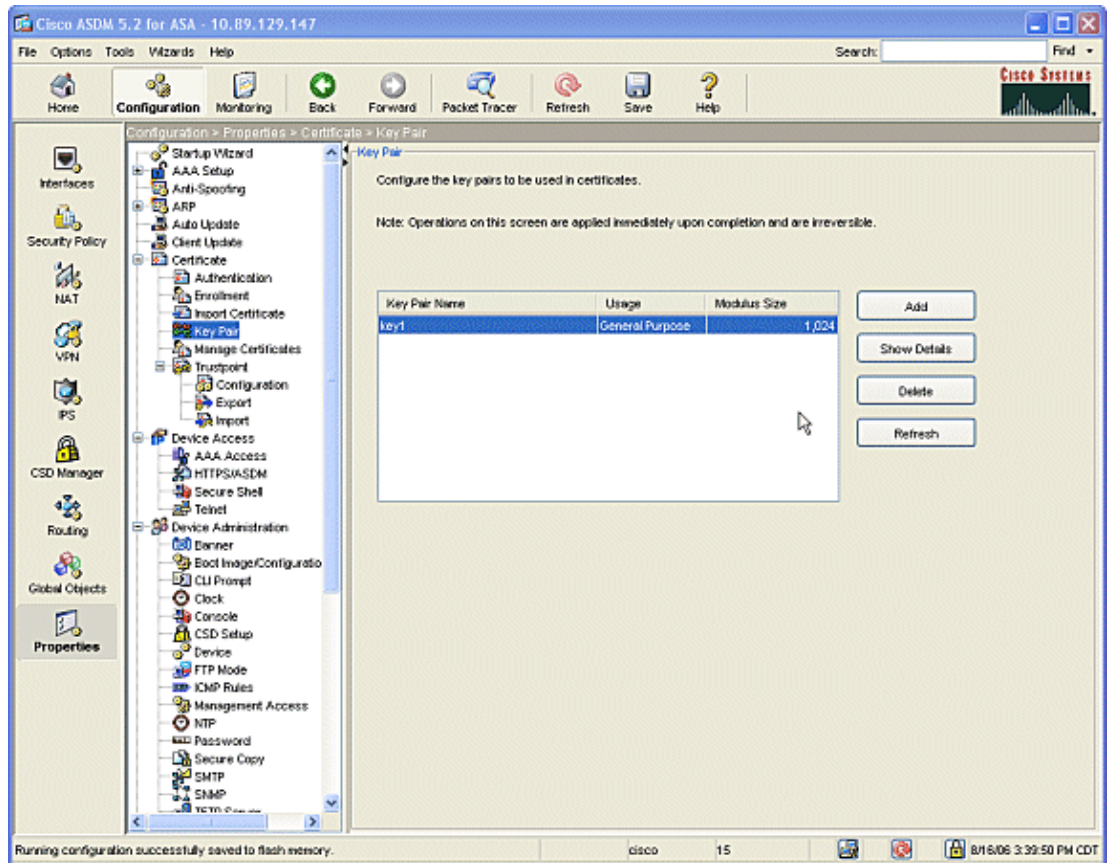
- a. From the navigation pane, click **Certificate > Key Pair**.



b. Click the **Add** button, and the Add Key Pair dialogue box displays.

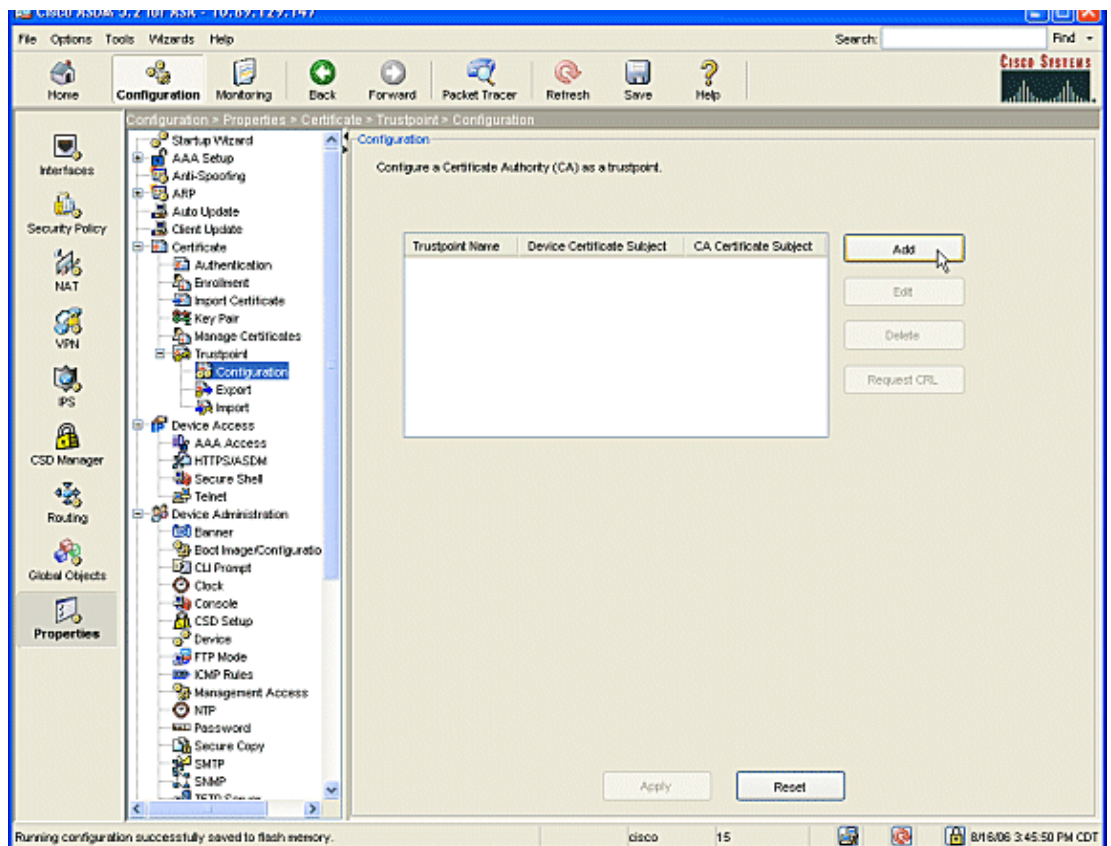


- c. Check the radio button beside the blank field of the **Name** area, and type in the name for the key.
- d. Click the **Size:** arrow by the drop-down box to choose a size for the key, or accept the default.
- e. Check the **General Purpose** radio button under Usage.
- f. Click the **Generate Now** button to regenerate the keys and return to the Key Pair window, where you can view the information for the key pair.

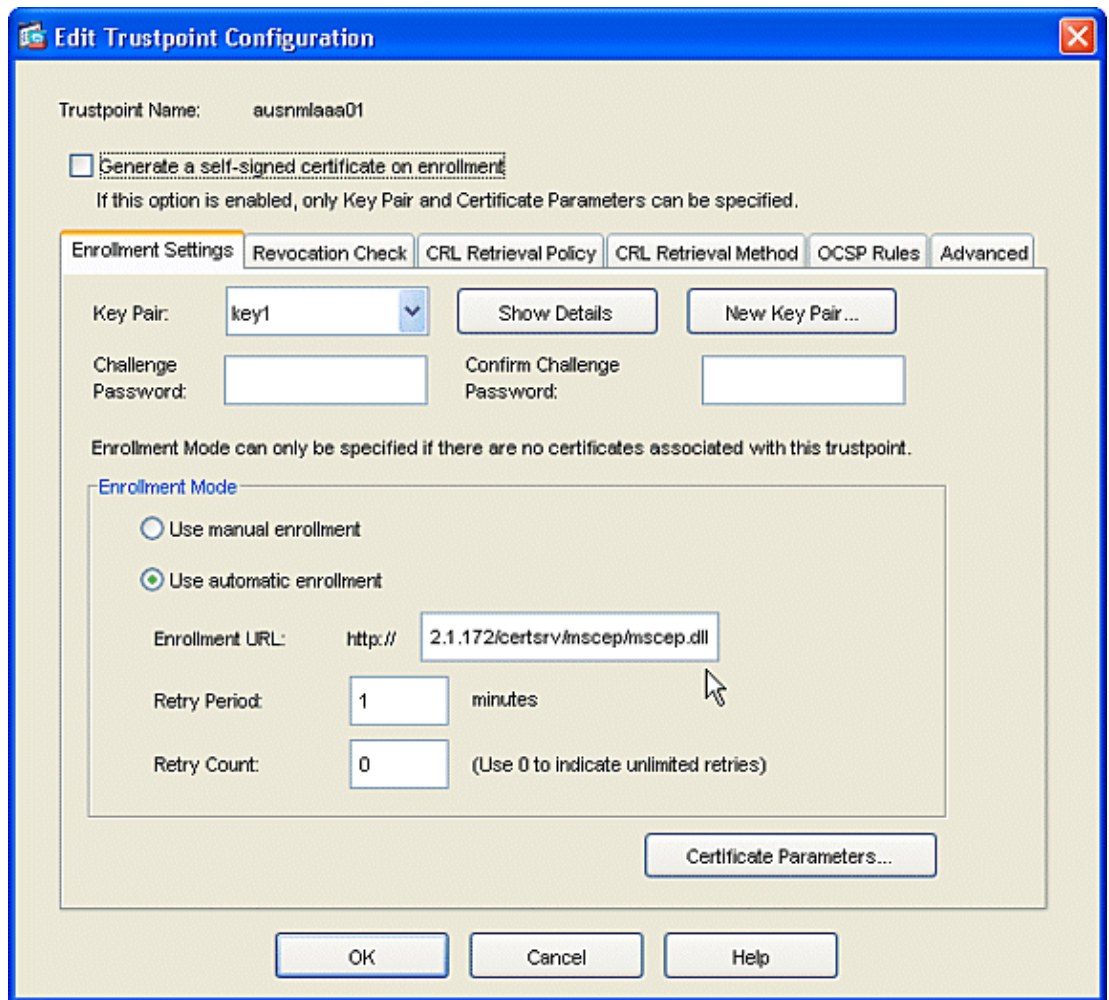


4. Configure the Microsoft CA to be considered trustworthy. From the navigation pane, click **Trustpoint > Configuration**.

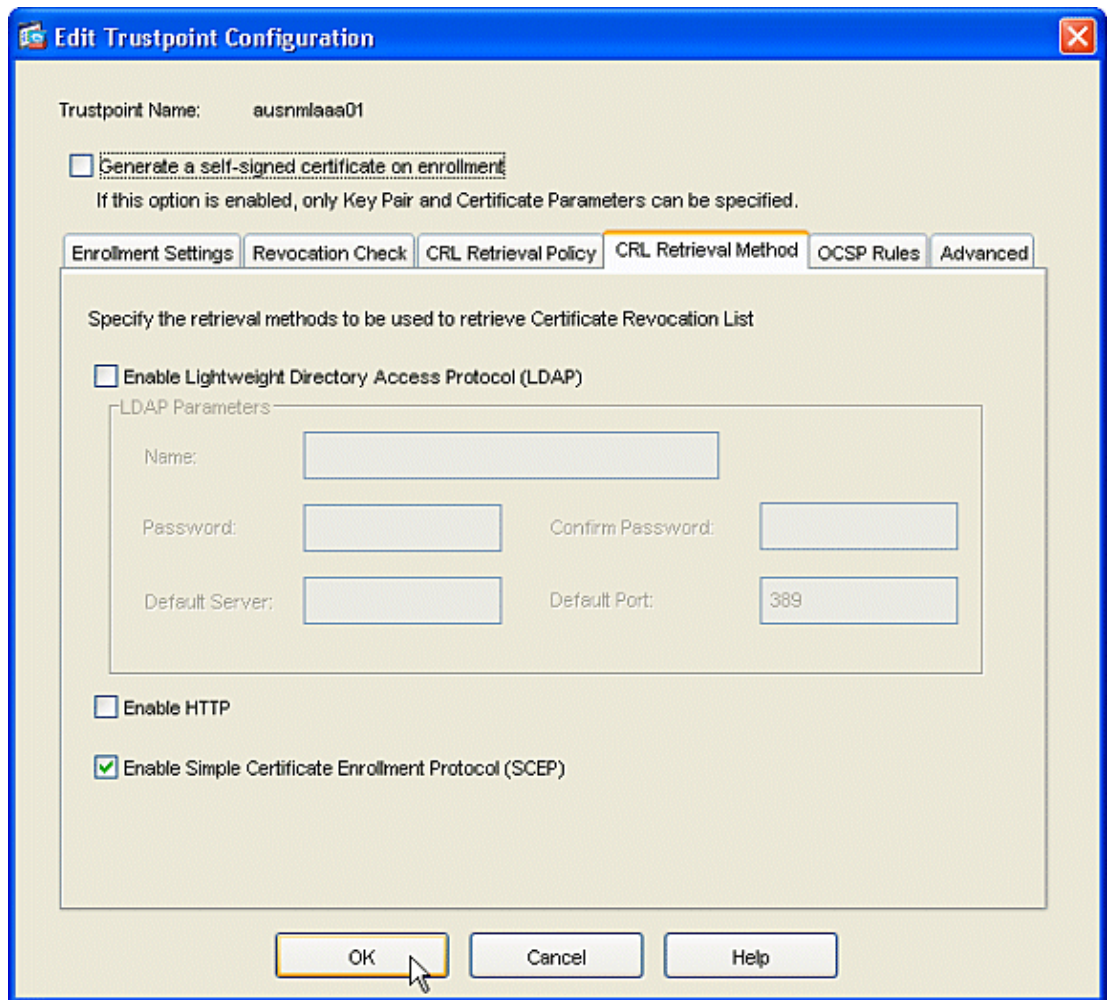
a. From the Configuration window, click the **Add** button.



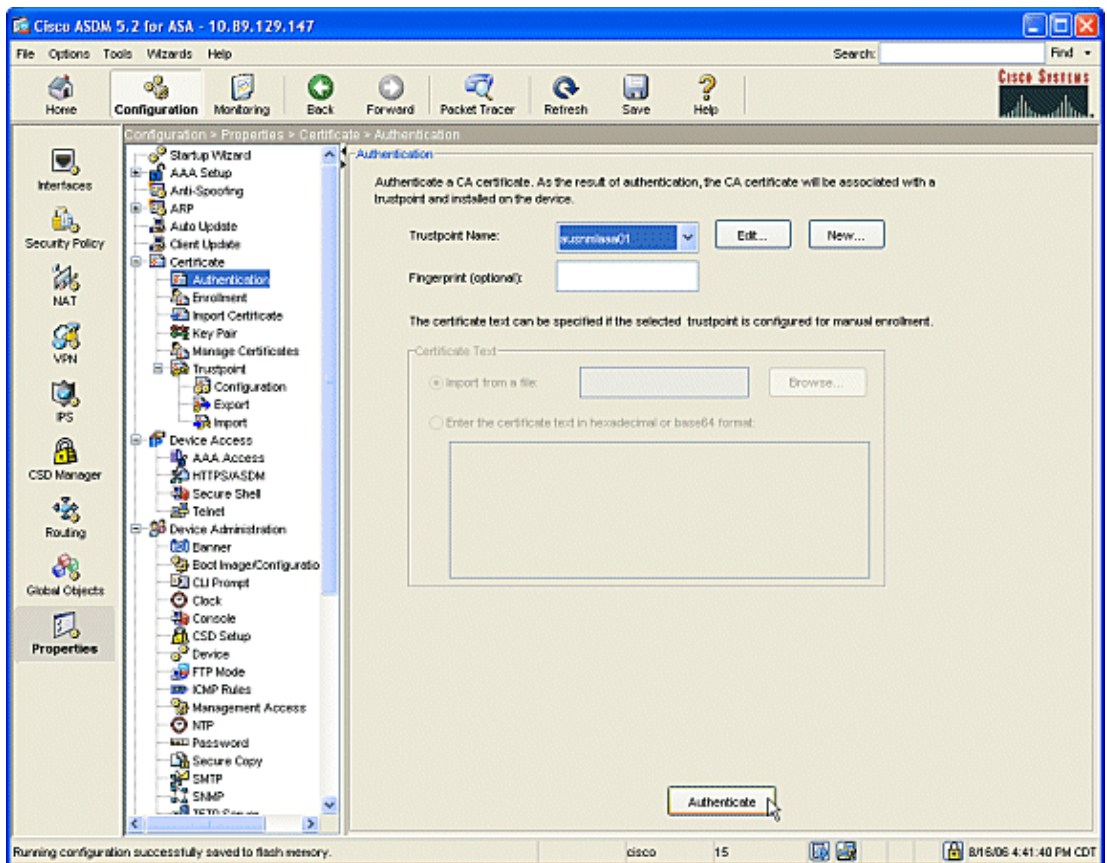
b. The Edit Trustpoint Configuration window displays.



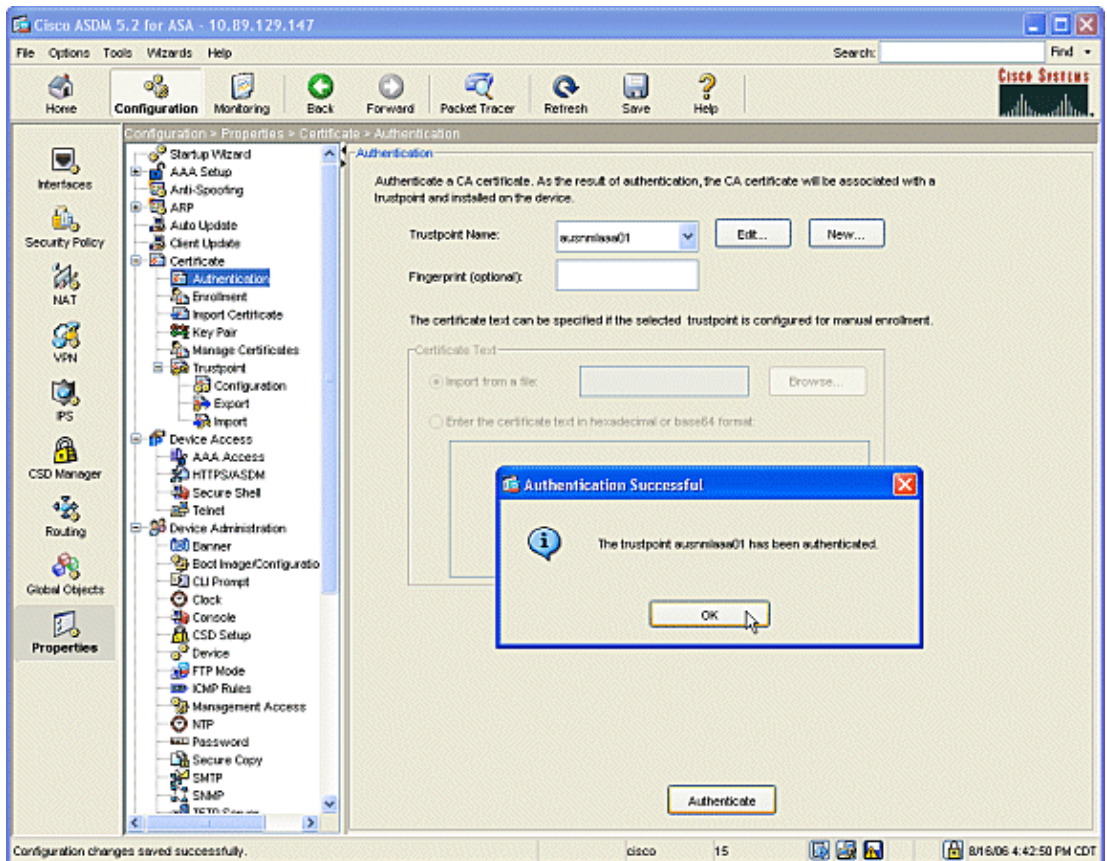
- c. Fill in a name for the Trustpoint with the name of the CA.
 - d. Click the **Key Pair**: arrow by the drop-down box, and choose the name of the key pair that you created.
 - e. Check the **Use automatic enrollment** radio button, and enter the URL for the Microsoft CA: **http://CA_IP_Address/certsrv/mscep/mscep.dll**.
5. Click the **Crl Retrieval Method** tab.
- a. Uncheck the Enable HTTP and Enable Lightweight Directory Access Protocol (LDAP) check boxes.
 - b. Check the Enable Simple Certificate Enrollment Protocol (SCEP) check box. Leave all other tab settings at their default settings.
 - c. Click the **OK** button.



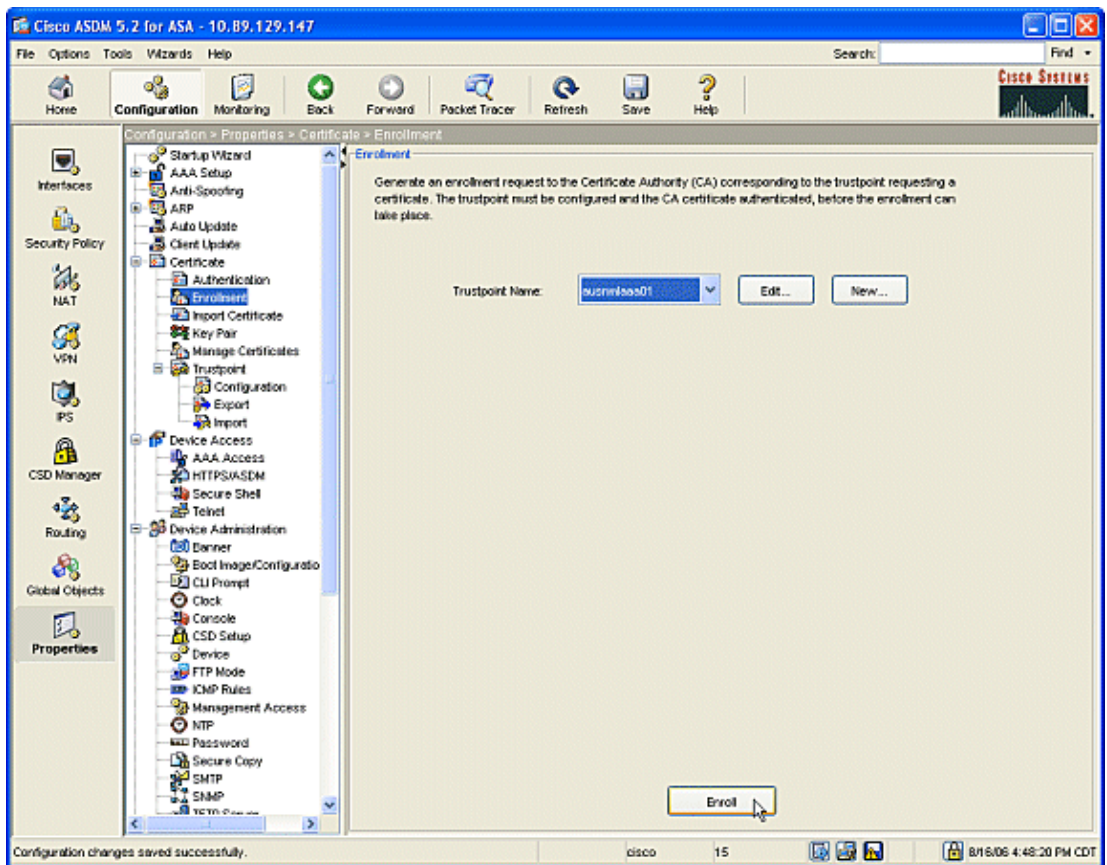
6. Authenticate and enroll with the Microsoft CA. From the navigation pane, click **Certificate > Authentication**. Make sure the the newly created trustpoint shows in the **Trustpoint Name:** field. Click the **Authenticate** button.



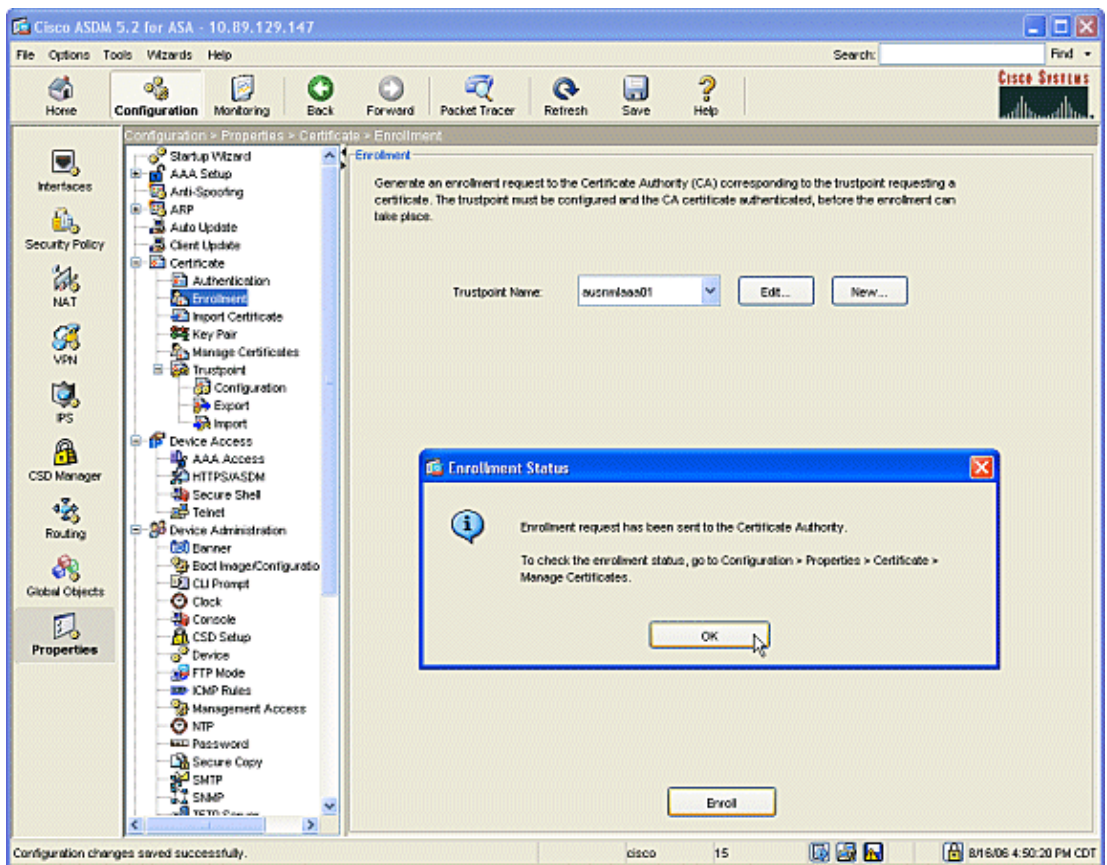
7. A dialogue box displays to inform you that the trustpoint has been authenticated. Click the **OK** button.



8. From the navigation pane, click **Enrollment**. Make sure the trustpoint name displays in the Trustpoint Name field, and click the **Enroll** button.



9. A dialogue box displays to inform you that the request was sent to the CA. Click the **OK** button.



Note: On a Microsoft Windows Stand-Alone machine you must issue the certificates for any requests that have been submitted to the CA. The certificate will be in a pending status until

you right click the certificate and click issue on the Microsoft Server.

Results

This is the CLI configuration that results from the ASDM steps:

```

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 bdb740b 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 a49dfff6 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 1abdddec6 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 4f6ddlbc 3452f329
a73b572a b41327f7 5af61809 c9fb86a4 b8d4aca6 f5ebc97f 2c3e306b ea58ed49
c245be2a 03f40878 273ae747 02b22219 5e3450a9 6fd72f1d 40e0931a 7b5cc3b0
d6558ec7 514ef928 bldfa9ab 732ecea0 40a458c3 e824fd6f b7c6b306 122da64d
b3ab23b1 adacf609 ld1132fb 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
```

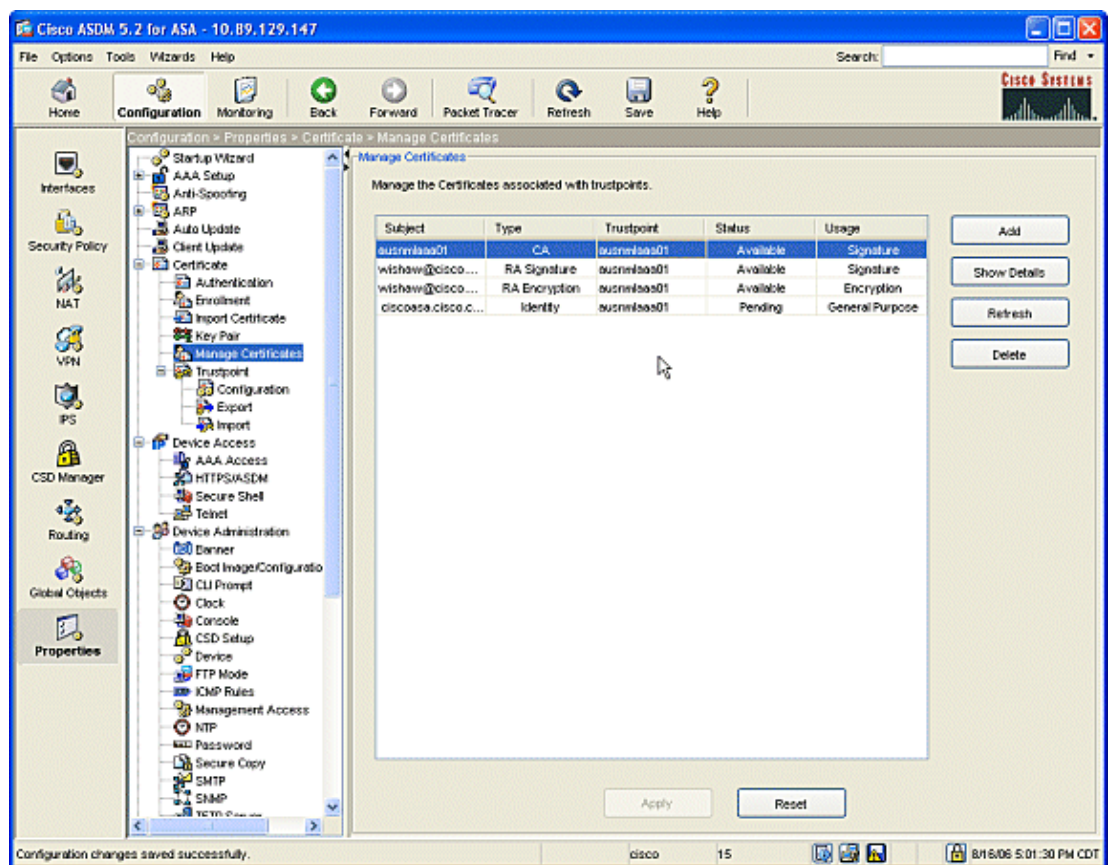
Verify

Use this section to confirm that your configuration works properly.

Check and Manage Your Certificate

Review and manage your certificate.

1. Open the ASDM application and click the **Configuration** button.
2. From the left menu, click the **Properties** button.
 - a. Click **Certificate**.
 - b. Click **Manage Certificate**.



Commands

On the ASA you can use several **show** commands at the command line to verify the status of a certificate.

- The command **show crypto ca certificates** is used to view information about your certificate, the CA certificate, and any registration authority (RA) certificates.
- The command **show crypto ca trustpoints** is used to verify the trustpoint configuration.
- The command **show crypto key mypubkey rsa** is used to display the RSA public keys of your ASA.
- The command **show crypto ca crls** is used to display all cached CRLs .

Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Use this section to troubleshoot your configuration.

Refer to Public Key Infrastructure for Windows Server 2003 for more information on how to troubleshoot Microsoft Windows 2003 CA.

Commands

Note: The use of **debug** commands can adversely impact your Cisco device. Before you use **debug** commands, refer to Important Information on Debug Commands.

Related Information

- [Configuring Microsoft Certificate services](#)
 - [Configuring the Cisco VPN 3000 Concentrator 4.0.x to Get a Digital Certificate](#)
 - [Cisco PIX Security Appliance Software Version 7.1](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 19, 2006

Document ID: 71050
