

VeriSign SSL Certificate Installation to the Cisco ASA Using ASDM

Document ID: 81558

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Configuration

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

The security appliance uses the Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS) to achieve secure message transmission for both Adaptive Security Device Manager (ASDM) and WebVPN sessions. The SSL window allows you to configure SSL versions for clients and servers and encryption algorithms. It also lets you apply previously configured trustpoints to specific interfaces, and to configure a fallback trustpoint for interfaces that do not have an associated trustpoint.

This document guides you on how to use ASDM in order to install a VeriSign SSL certificate.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco ASA 5500 Series Security Appliance, version 7.2(1) and ASDM version 5.2(1).

The information in this document was created from the devices in a specific lab environment. This document describes the steps necessary to configure an ASA in order to obtain and install a trial SSL certificate obtained from VeriSign.

Conventions

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

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Configuration

Complete these steps in order to install the VeriSign SSL certificate on the Cisco ASA using ASDM:

1. Log in to the ASA via ASDM and configure a new trustpoint that identifies the certificate for SSL WebVPN authentication.
2. Go to **Configuration > Properties > Certificate > Authentication > New >**.
3. Enter a name for the trustpoint in the Trustpoint Name field.

This example is called **Test-ASA** (see Figure 2).

Note: The trustpoint name cannot contain any spaces.

4. Choose **New Key Pair...** in order to create a new key pair whose public key is to be certified for this trustpoint (see Figure 1).

Note: It is recommended to use a separate key pair so if the default key pair is regenerated, it will not invalidate the certificate. The Default-RSA-Key can be used.

5. Enter a name for this key.

This example is named **VerisignKey**.

6. Click **Generate Now**.

Figure 1

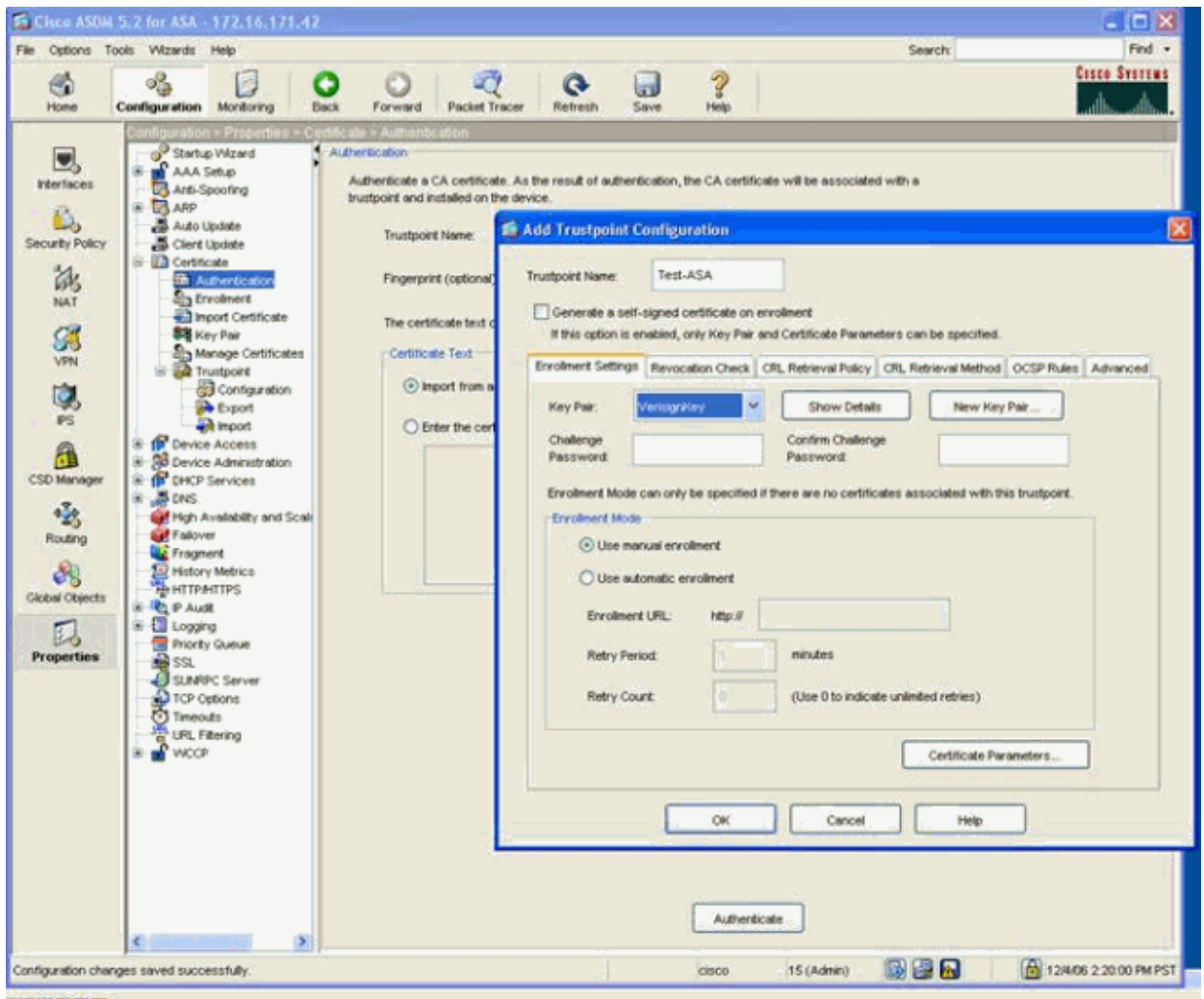


This is the command-line interface (CLI) command:

```
crypto key generate rsa label Verisign-Key noconfirm
```

7. Choose the newly created **Verisign-Key**, then click **Certificate Parameters**.

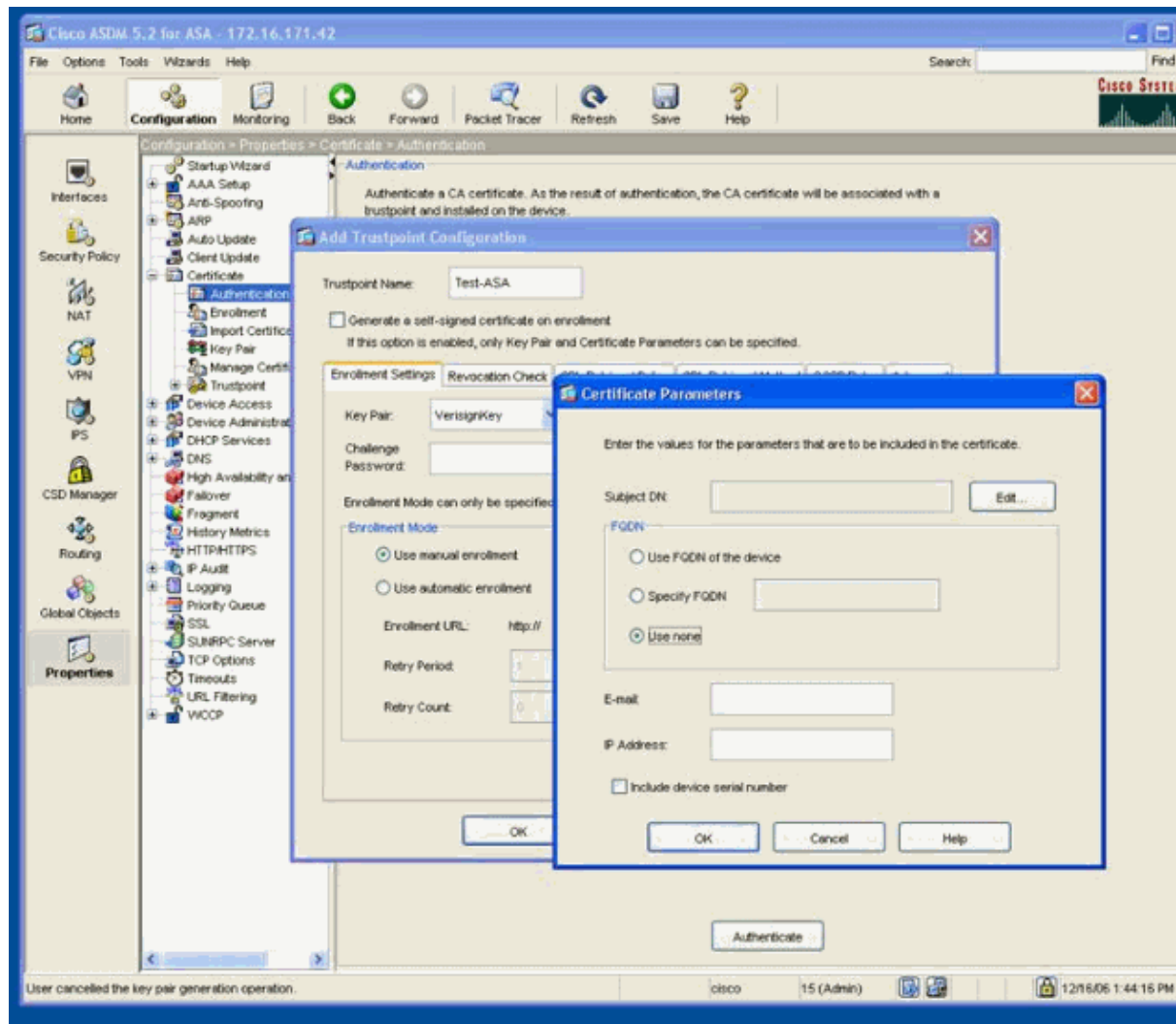
Figure 2



8. Complete the Certificate Parameters fields:

- a. Choose **Use none** under FQDN.
- b. Click **Edit**.

Figure 3



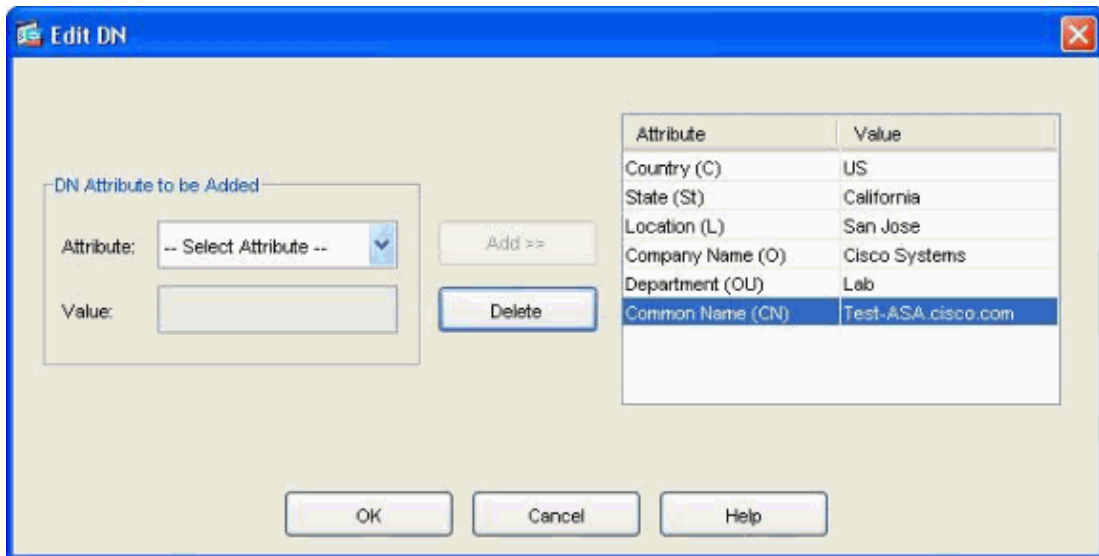
9. Enter the device certificate details.

Make sure you select these parameters when you enroll with VeriSign:

- ◆ Country
- ◆ State (fully spelled out, no abbreviations)
- ◆ Location (usually is the city)
- ◆ Company Name
- ◆ Department (Organizational Unit)
- ◆ Common Name (device name which must match the DNS entry, in this example Test-ASA.cisco.com – FQDN)

Note: If the Common Name entered does not match your DNS entry, you receive a Certificate error which states, The name of the security certificate is invalid or does not match the name of the site . Usually the name entered in the browser URL must match the Certificates CN field. The error is shown in Figure 33 in the Troubleshoot section of this document.

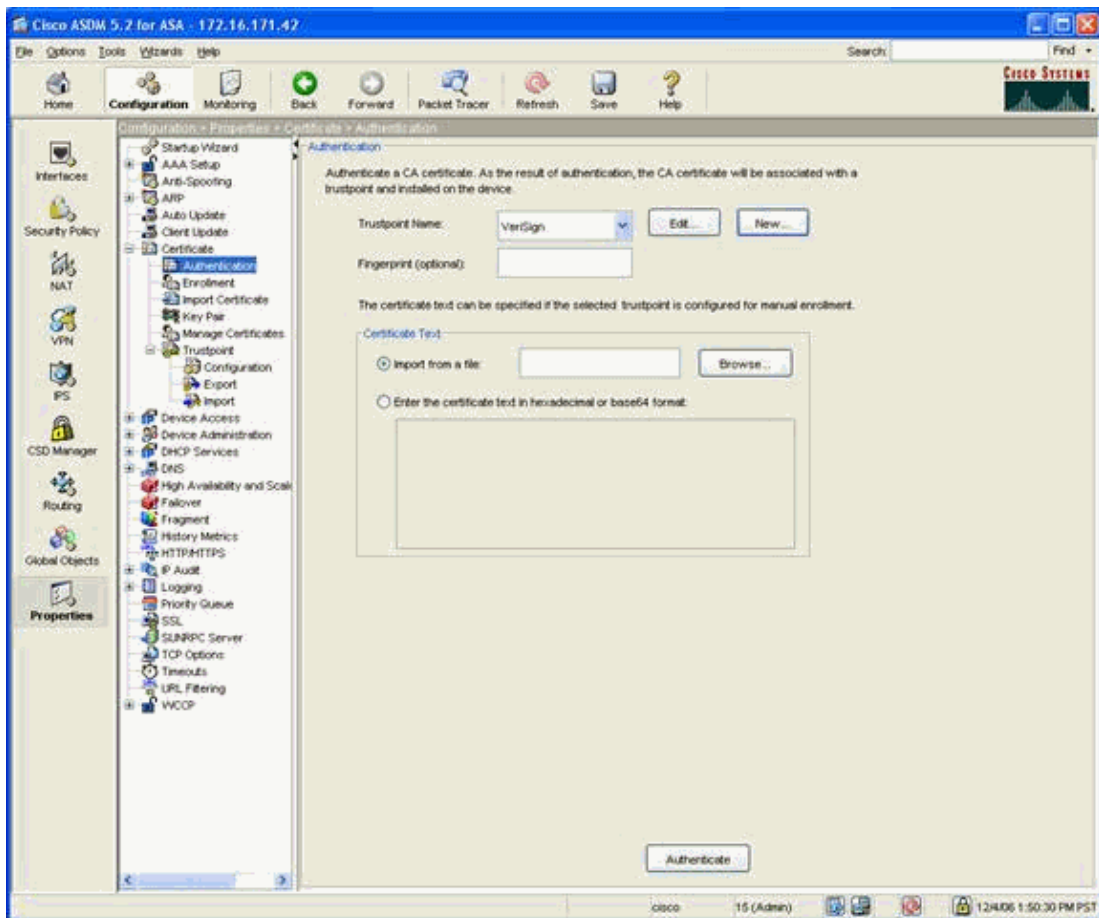
Figure 4



10. Choose **OK >OK >OK**.

This brings you to this window:

Figure 5

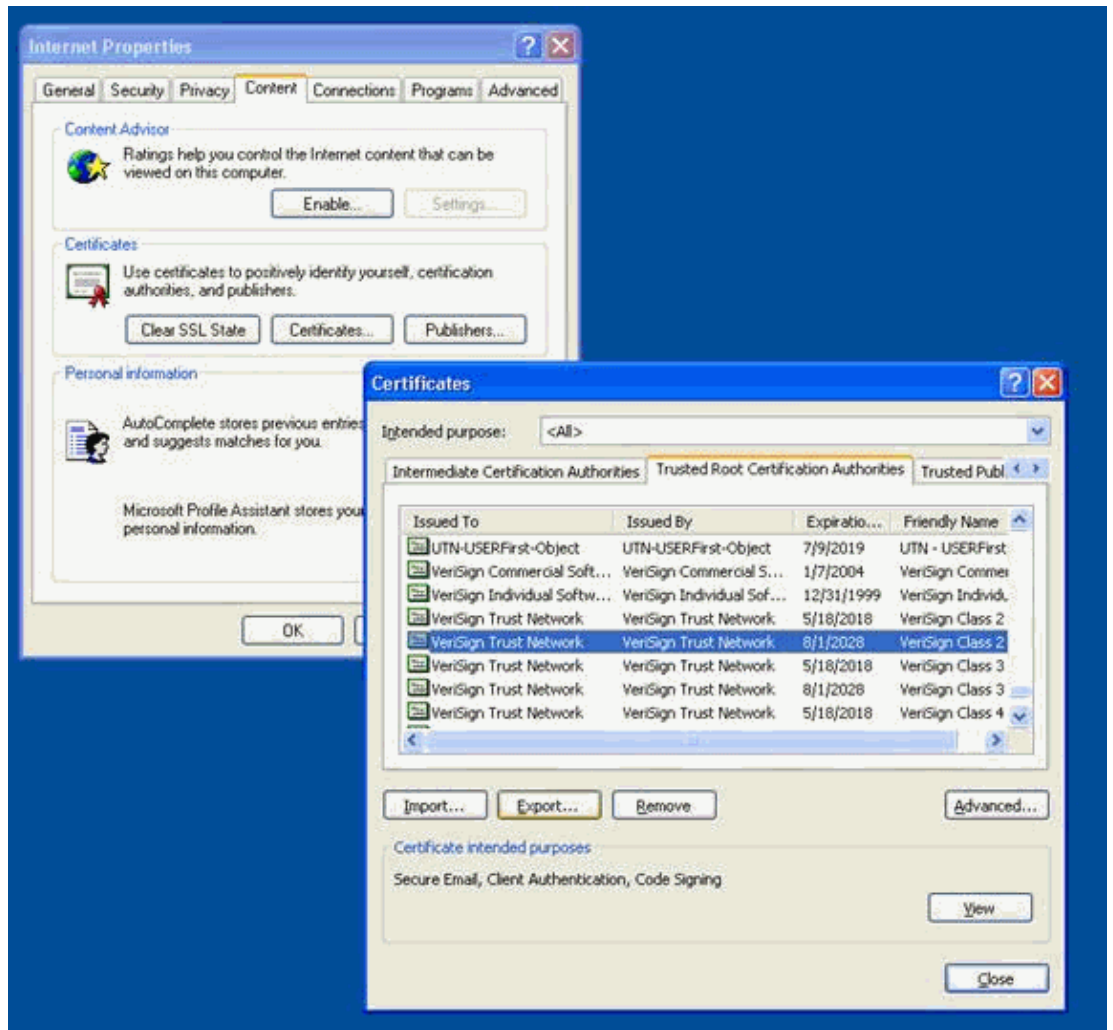


11. Get a VeriSign certificate from the PC certificates store:

- a. Right click on **IE (Internet Explorer)** icon on your desktop.
- b. Go to **Content > Certificates > Trusted Root Certification Authorities**.

- c. Choose **VeriSign Trust Network** (any VeriSign root certificate should work from this window).
- d. Click **Export**.

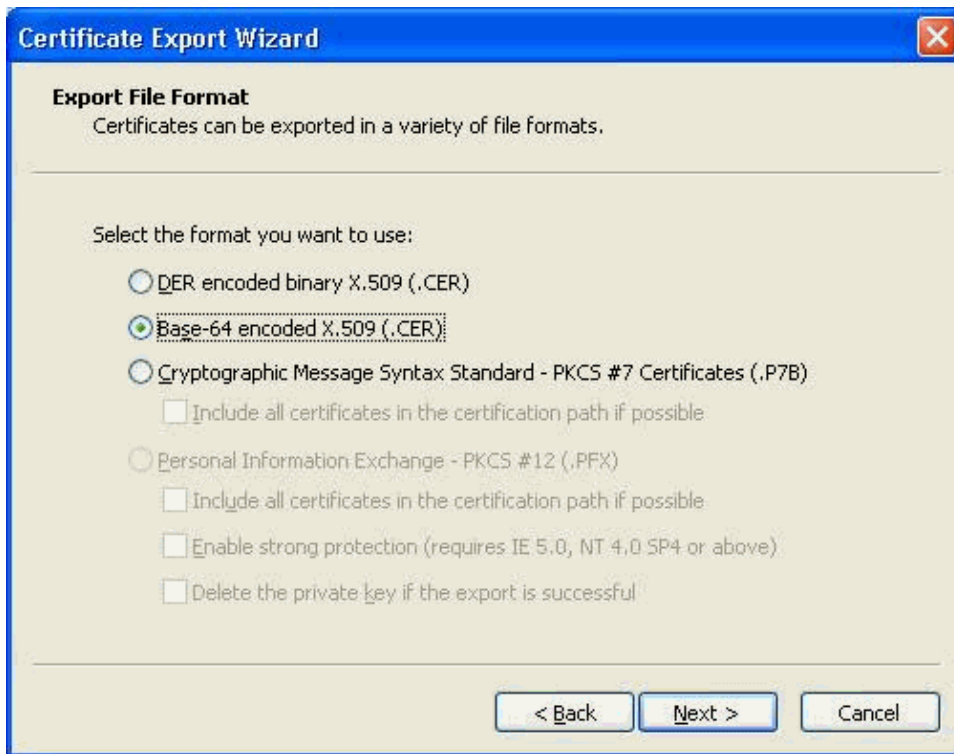
Figure 6



12. Export it as Base-64 encoded format.

Save this to a location on your PC and you will receive a message that the export is successful.

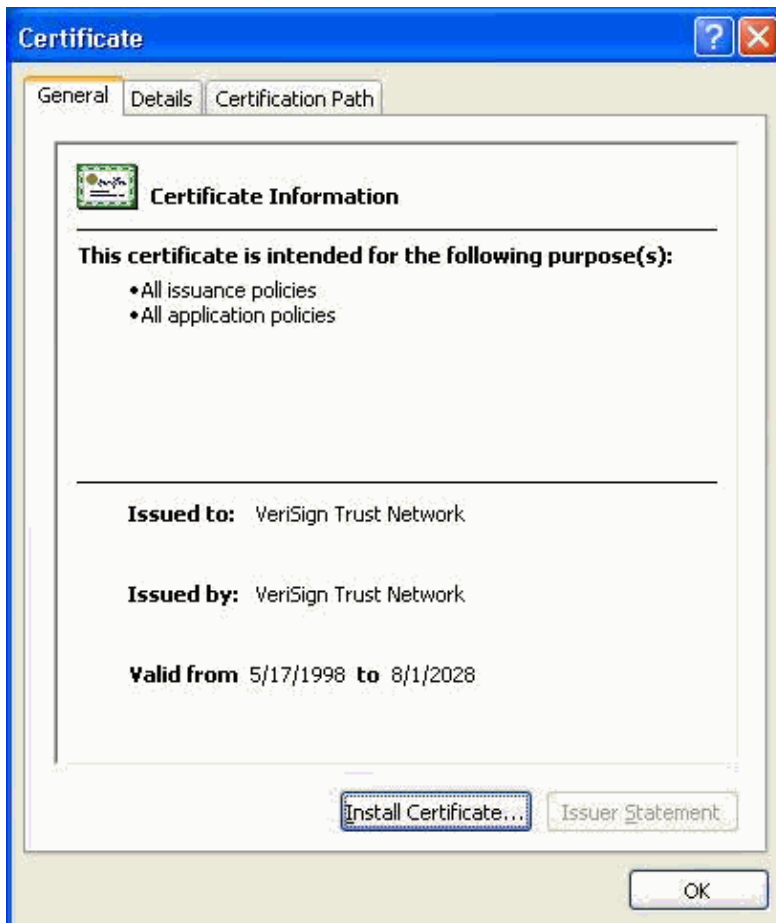
Figure 7



13. Verify the certificate that was downloaded to the PC.

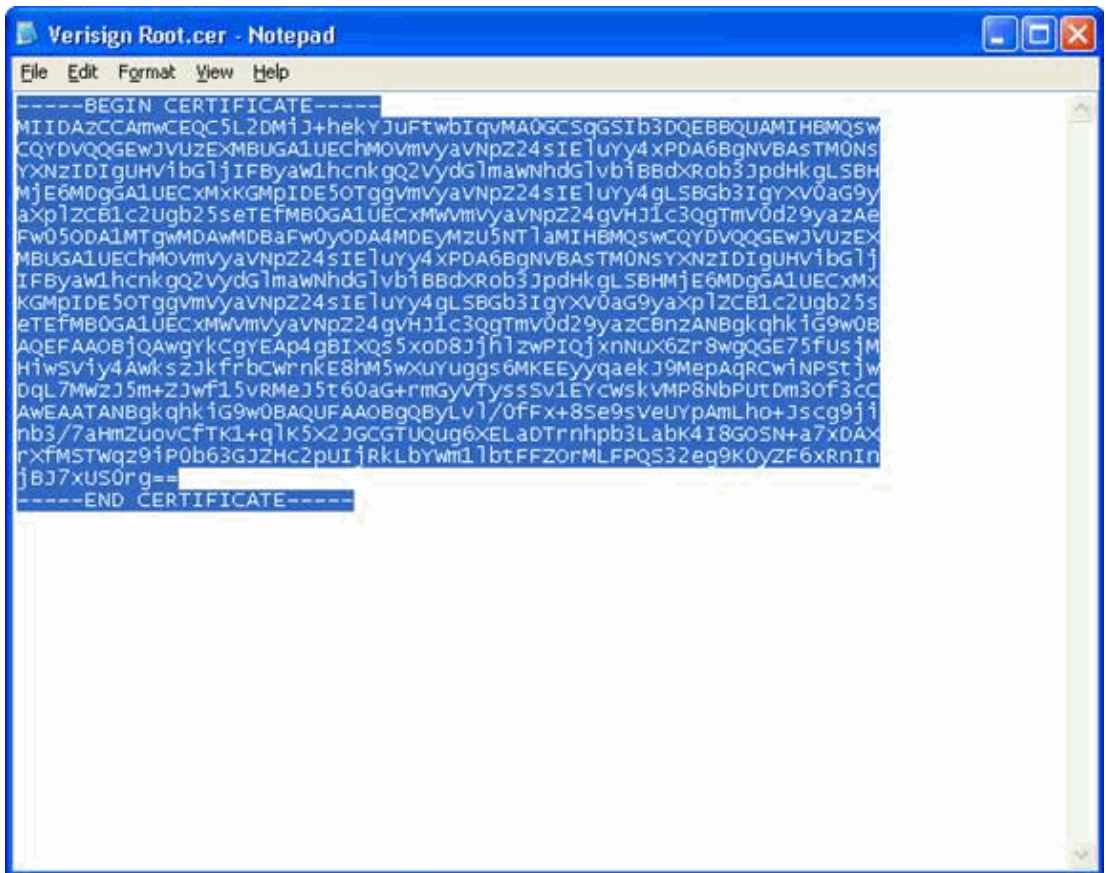
Check the certificate by double clicking it. If the Issued to: value is the same as the Issued by: (in this example VeriSign Trust Network), this indicates that this is a root certificate (see Figure 8). This shows you that this is a root certificate from VeriSign.

Figure 8



14. Open the certificate file in a text editor. Copy the entire selection and paste it to ASDM in the next window:

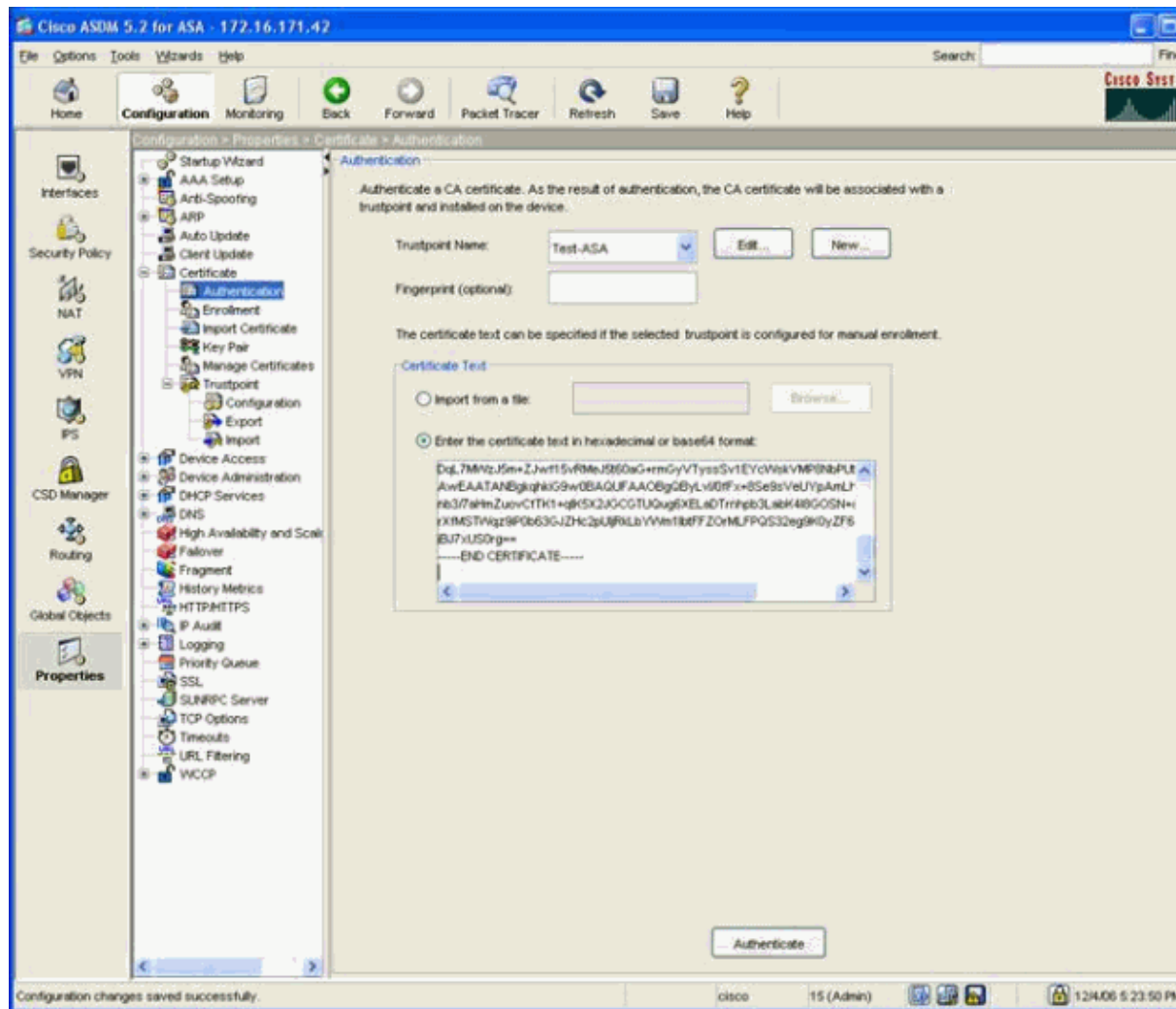
Figure 9



```
-----BEGIN CERTIFICATE-----
MIIDAzCCAmwCEQC5L2DMiJ+hekYJUftwbIqvMA0GCSqGSIb3DQEBBQUAMIHBMQSw
CQYDVQQGEwJVUzEXMBUGA1UEChMvMmVyaVNPZ224sIE1uyy4xPDA6BgNVBAsTM0Ns
YXNzIDIgUHViYy4xIFB5aw1hcnkqQ2vydG1mawNhdG1vb1BBdXR0b3JpdHkgLzBHM
MjE6MDgGA1UECxMxKGMPIDE5OTggvMmVyaVNPZ224sIE1uyy4gLSBGb3IgyXV0aG9y
aXp1ZCB1c2Ugb25seTEFMBOGA1UECXMwMmVyaVNPZ224gVHJ1c3QgTmV0d29yazAe
Fw05ODAlMTgwMDAwMDBaFw0yODA4MDEyMzU5NTlAMIHBMQSwCQYDVQQGEwJVUzEX
MBUGA1UEChMvMmVyaVNPZ224sIE1uyy4xPDA6BgNVBAsTM0NsYXNzIDIgUHViYy4x
IFB5aw1hcnkqQ2vydG1mawNhdG1vb1BBdXR0b3JpdHkgLzBHMjE6MDgGA1UECxMx
KGMPIDE5OTggvMmVyaVNPZ224sIE1uyy4gLSBGb3IgyXV0aG9yYXp1ZCB1c2Ugb25s
eTEFMBOGA1UECXMwMmVyaVNPZ224gVHJ1c3QgTmV0d29yazCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEAp4gBIxQs5x0d8JjflzwPIQjxnNux6Zr8wgQGE75fUsjM
H1wsviy4AwksszJkfrbcwrnKE8hM5wxUYuggs6MKEEyyqaekJ9MepAqRCw1NPstjw
DqL7MwzJ5m+ZJwf15VRMeJ5t60ag+rmgyvtyssSv1EYcswkVMP8NbPUTdm3of3CC
AWEAATANBgkqhkiG9w0BAQUFAAOBgQByLvl/0FFx+8Se9sveuypAmLho+Jscg9j1f
nb3/7aHmZUovcFTk1+q1k5x2JGCGTUQug6XELaDTrnhpb3LabK4I8G0SN+a7XDAX
rxFMSTwqz9iP0b63GJZHC2PUIjRkLbywm1lbtFFZorMLFPQS32eq9K0yZF6xRrIn
jBJ7xUS0rg==
-----END CERTIFICATE-----
```

15. Install the root certificate in ASDM, which is equivalent to Trusted Root Certification Authorities on your PC.
 - a. Go to **Configuration > Properties > Certificate > Authentication**.
 - b. Choose **Test-ASA**, then click **Authenticate**.
 - c. Choose **Enter the certificate text in hexadecimal or base64 format** and click **Authenticate**.

Figure 10



This is the CLI command output:

```
ASA(config)#crypto ca trustpoint Test-ASA
ASA(config-ca-trustpoint)#revocation-check none
ASA(config-ca-trustpoint)#keypair VerisignKey
ASA(config-ca-trustpoint)#fqdn none
ASA(config-ca-trustpoint)#subject-name CN=Test-ASA,OU=Lab,O=Cisco Systems,C=US
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate Test-ASA nointeractive
Enter the certificate in hexadecimal or base64 representation....
```

End with the word "quit" on a line by itself.

```
ASA(config-pubkey)# -----BEGIN CERTIFICATE-----
ASA(config-pubkey)# MIIDAzCCAmwCEQC5L2DMiJ+hekYJuFtwbIqvMA0GCSqGSIb3DQEBBQUAM
ASA(config-pubkey)# CQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xPDA6BgNVB
ASA(config-pubkey)# YXNzIDIGUHVibGljIFByaW1hcnkgQ2VydGhmaWNhdGlvbiBBdXRob3Jpd
ASA(config-pubkey)# MjE6MDgGA1UECXMxKGMpIDE5OTggVmVyaVNpZ24sIEluYy4gLSBGb3Iy
ASA(config-pubkey)# aXplZCB1c2Ugb25seTEfMB0GA1UECXMWVmVyaVNpZ24gVHJ1c3QgTmV0d
ASA(config-pubkey)# Fw05ODAlMTgwMDAwMDBaFw0yODAlMDEyMzU5NTlamiHBMQswCQYDVQQGE
ASA(config-pubkey)# MBUGA1UEChMOVmVyaVNpZ24sIEluYy4xPDA6BgNVBAsTM0NsYXNzIDIGU
ASA(config-pubkey)# IFByaW1hcnkgQ2VydGhmaWNhdGlvbiBBdXRob3JpdHkgLSBHMjE6MDgGA
ASA(config-pubkey)# KGMpIDE5OTggVmVyaVNpZ24sIEluYy4gLSBGb3IyYXV0aG9yaXplZCB1c
ASA(config-pubkey)# eTEfMB0GA1UECXMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazCBnzANBjkgq
ASA(config-pubkey)# AQEFAAOBjQAwwYkCgYEAp4gBIXQs5xod8JjhlzwpIQjxnNuX6Zr8wQGE
ASA(config-pubkey)# HiwSViy4AWkszJkfrbcWrnkE8hm5wXuYuggs6MKEEyyqaekJ9MepAgRcW
```

```

ASA(config-pubkey)# DqL7MWzJ5m+ZJwf15vRMeJ5t60aG+rmGyVTySSv1EYcWskVMP8NbPUTD
ASA(config-pubkey)# AwEAATANBgkqhkiG9w0BAQUFAAOBgQByLv1/0fFx+8Se9sVeUYpAmLho+
ASA(config-pubkey)# nb3/7aHmZuovCfTK1+q1K5X2JGCGTUQug6XELaDTrnhpb3LabK4I8GOSN
ASA(config-pubkey)# rXfMSTWqz9iP0b63GJZHc2pUIjRkLbYWm1lbtFFZOrMLFPQS32eg9K0yZ
ASA(config-pubkey)# jBJ7xUS0rg==
ASA(config-pubkey)# -----END CERTIFICATE-----
ASA(config-pubkey)#quit

INFO: Certificate has the following attributes:

Fingerprint:      2dbbe525 d3d16582 3ab70efa e6ebe2e1

Trustpoint CA certificate accepted.

ASA(config)#

```

In ASDM, you see this verification of acceptance:

Figure 11

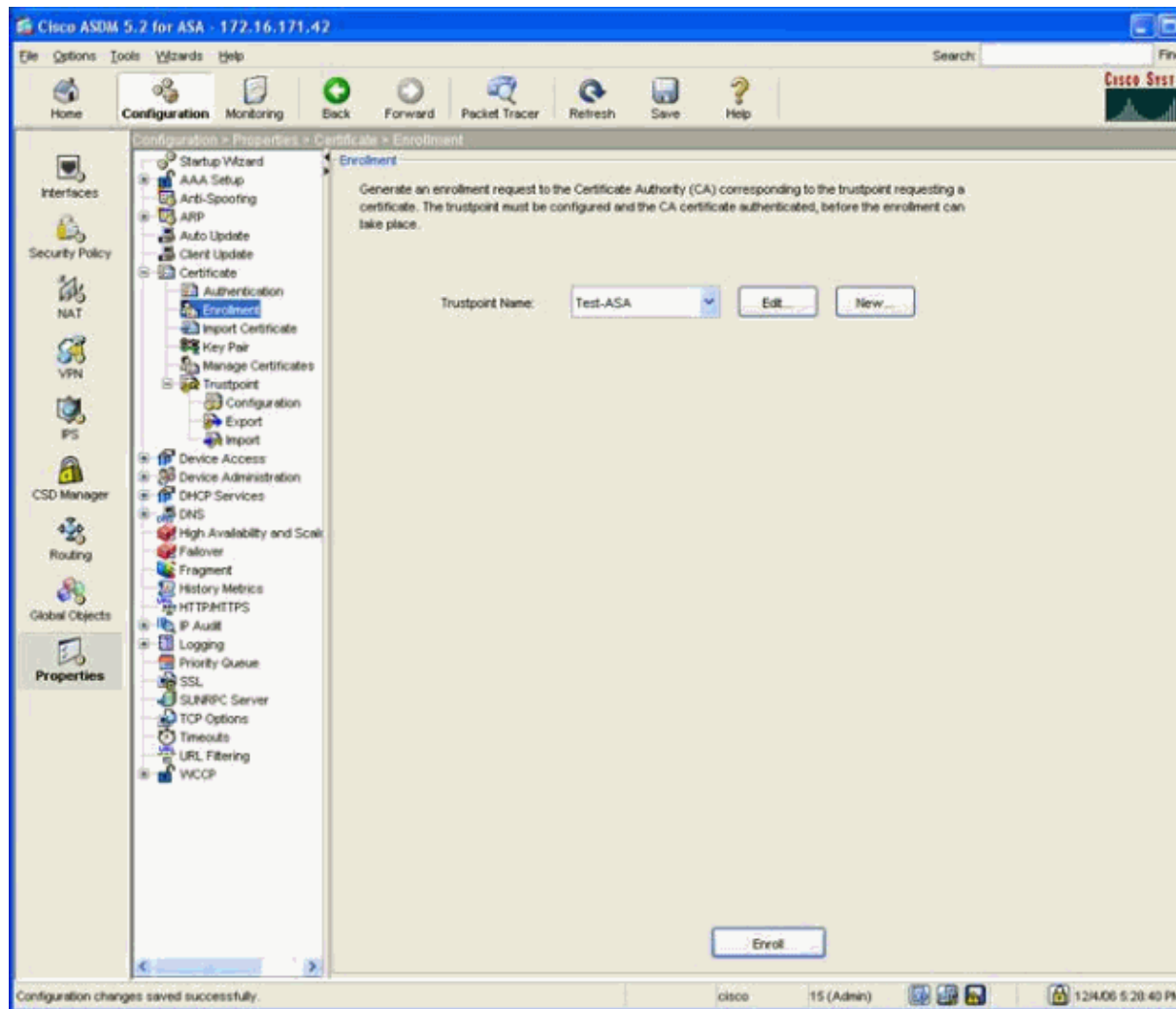


16. Issue the enrollment process in order to receive a SSL certificate from VeriSign.

- a. Go to **Configuration > Properties > Certificate > Enrollment >**.
- b. Choose your trustpoint: **Test-ASA**, then click **Enroll**.

Note: You will receive a warning that the FQDNs do not match. See Figure 13 and explanation after Figure 12.

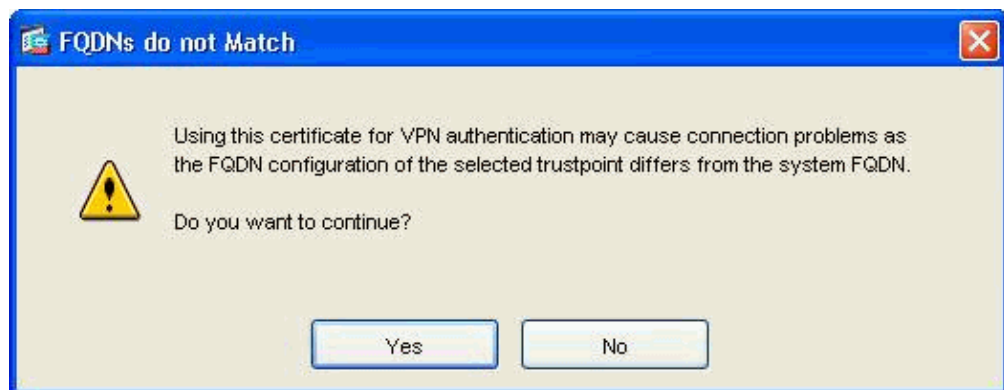
Figure 12



FQDN warning:

This error message is provided because **Use none** was selected in step 8 (see Figure 3). This is needed because VeriSign does not accept alternate subject names in certificate requests.

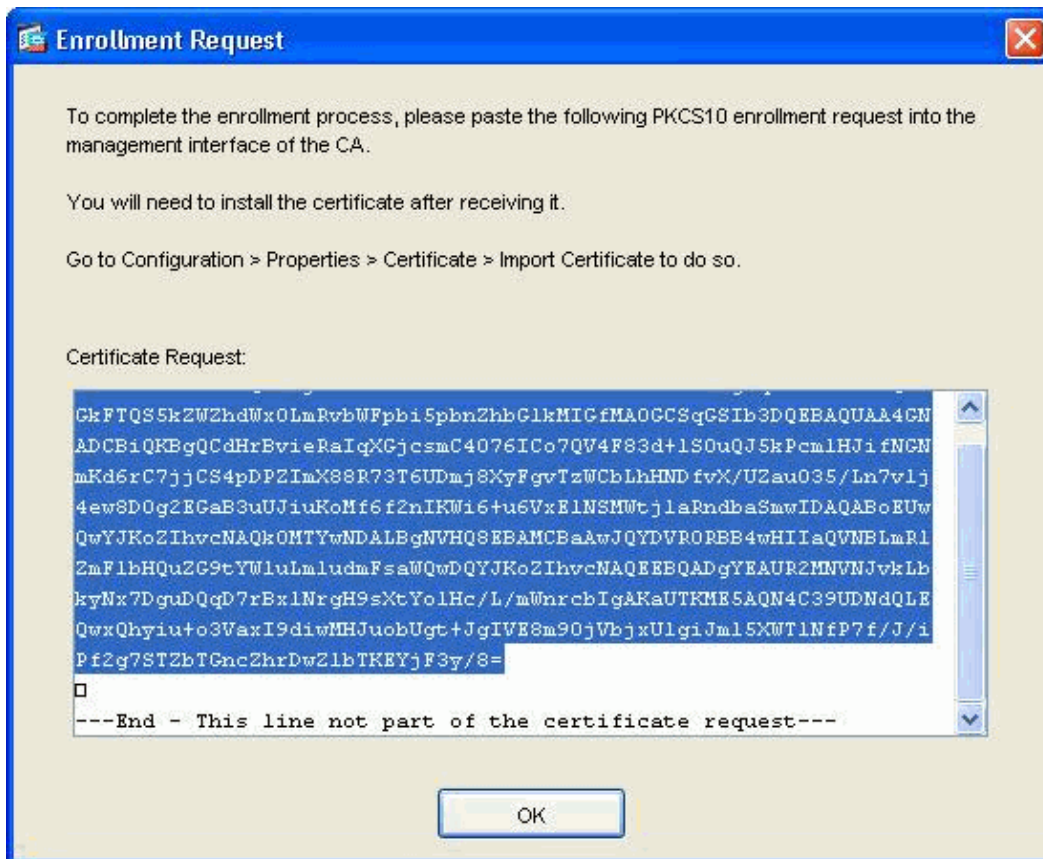
Figure 13



17. A popup appears which shows the Certificate Request hash. This needs to be copied to the VeriSign website. Select the text. You will need this text in the next step when you enroll with VeriSign.

Note: It is recommended to save the text to a text editor for backup purposes.

Figure 14



This is the CLI output:

Start the enrollment process with the CA.

```
ASA(config-ca-trustpoint)#crypto ca enroll Test-ASA noconfirm

Start certificate enrollment...

The subject name in the certificate will be: CN=Test-ASA,OU=Lab,O=Cisco Systems,C=U

The fully-qualified domain name will not be included in the certificate

Certificate Request follows:

MIIBzDCCATUCAQAwbjERMA8GA1UEBxMIU2FuIEpvc2UxEzARBgNVBAGTCkNhbgGlm
b3JuaWEwEzCzAJBgNVBAYTAlVTMRywFAyDVQOKEw1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLFwNMYWlxeTAPBgNVBAMTCFRlc3QtQVNBMIgfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCdHrBvieRaIqXGjcsM4076ICo7QV4F83d+1SOuQJ5kPcm1HJi fNGN
mKd6rC7jjCS4pDPZImX88R73T6UDmj8XyFgvTzWCbLhHNDfvX/Uzau035/Ln7v1j
4ew8D0g2EGaB3uUJiuKoMf6f2nIKWi6+u6VxE1NSMWtjlaRndbaSmwIDAQABoB4w
HAYJKoZIhvcNAQkOMQ8wDTALBgNVHQ8EBAMCBaAwDQYJKoZIhvcNAQEEBQADgYEA
a2MNQvd5HcRi / 3Sfg3zD1Xmc9pspA / FlocwRaWk6s / 4q+Juo26s8hy8d7YwoOxUL
XC1R47uhc4shbLwkz1HW124BjohxfFBV2UrMdUFGSu1HZsb9B+Np jln0EvJVj / / y
LR4EGppzqL9JdeR32cf7eFB02bpUVGKYDZqcM9WE1zE=

---End - This line not part of the certificate request---
```

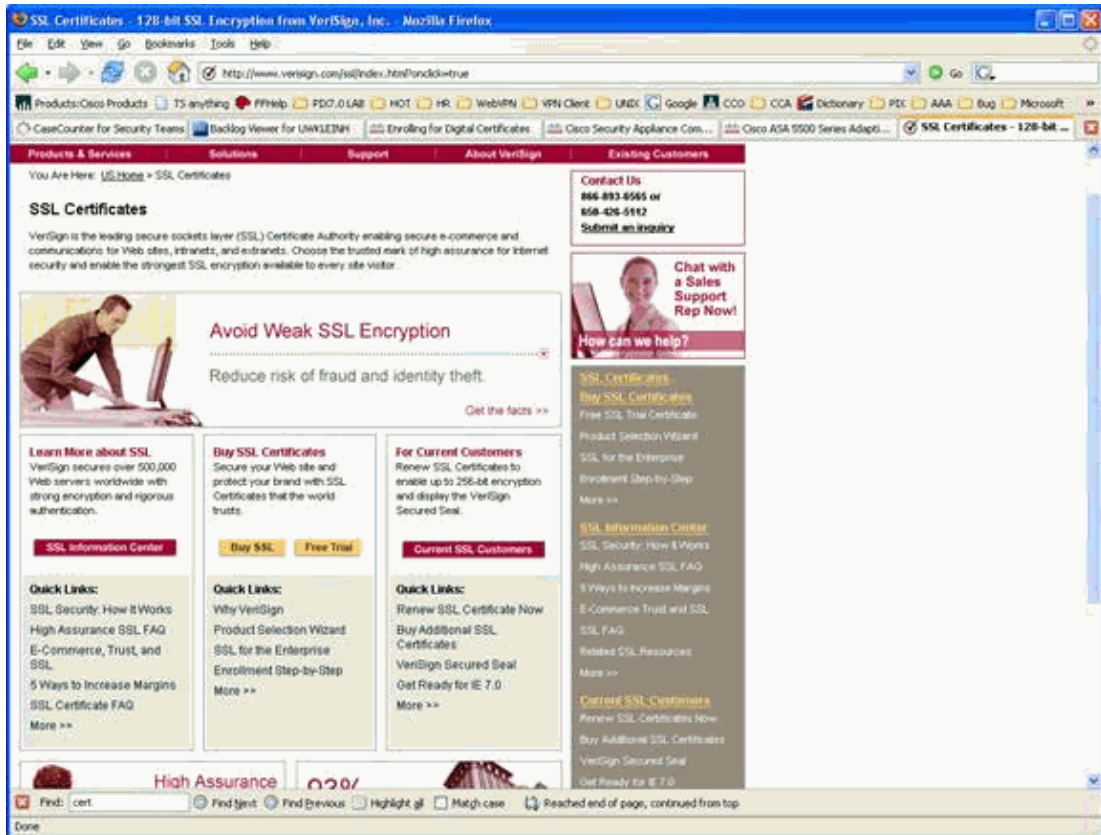
```
ASA(config)#
```

18. In order to receive the certificate from VeriSign, access the website at: <http://www.verisign.com/> and

choose **BUY SSL Certificates**.

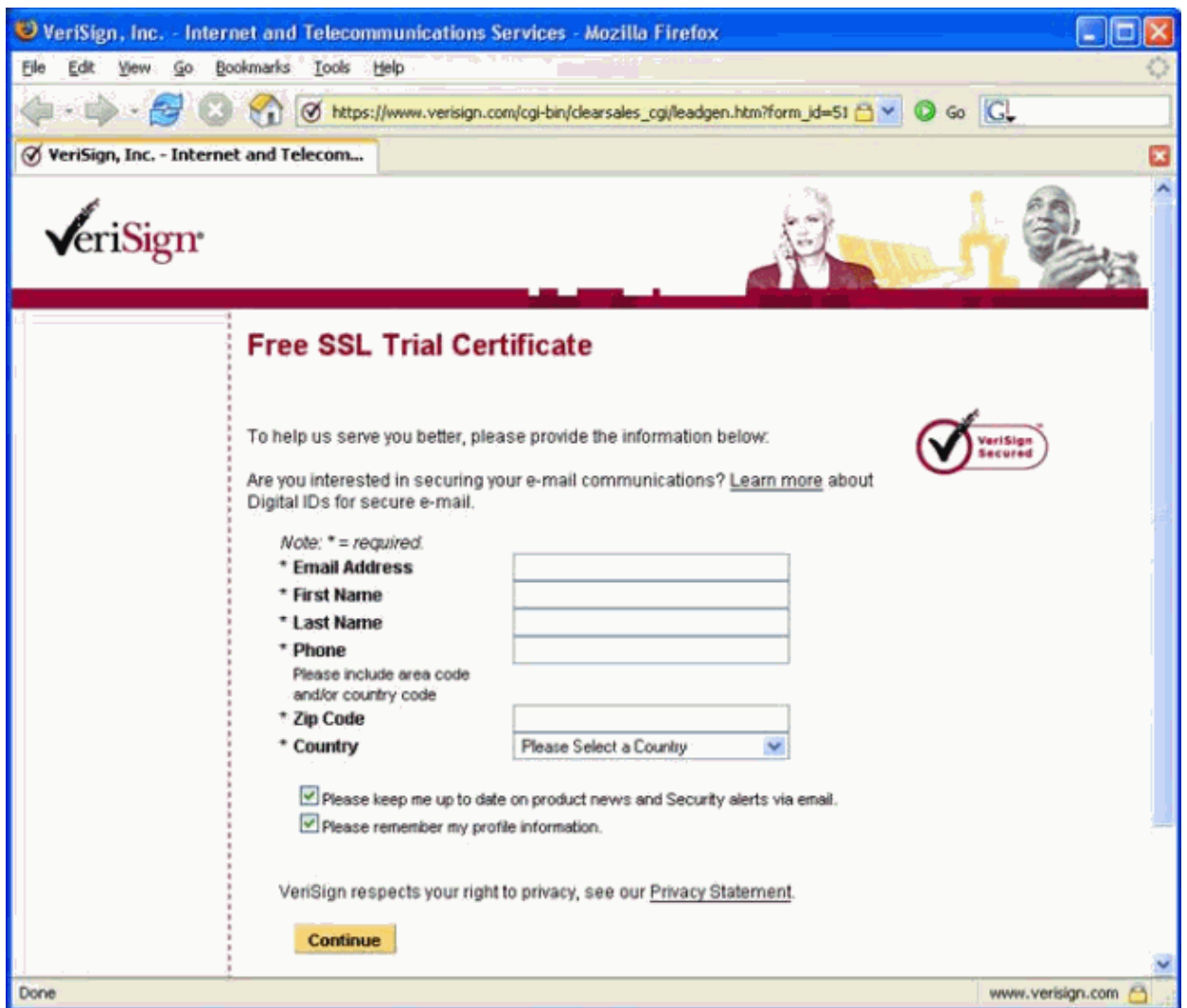
This brings you to this window:

Figure 15



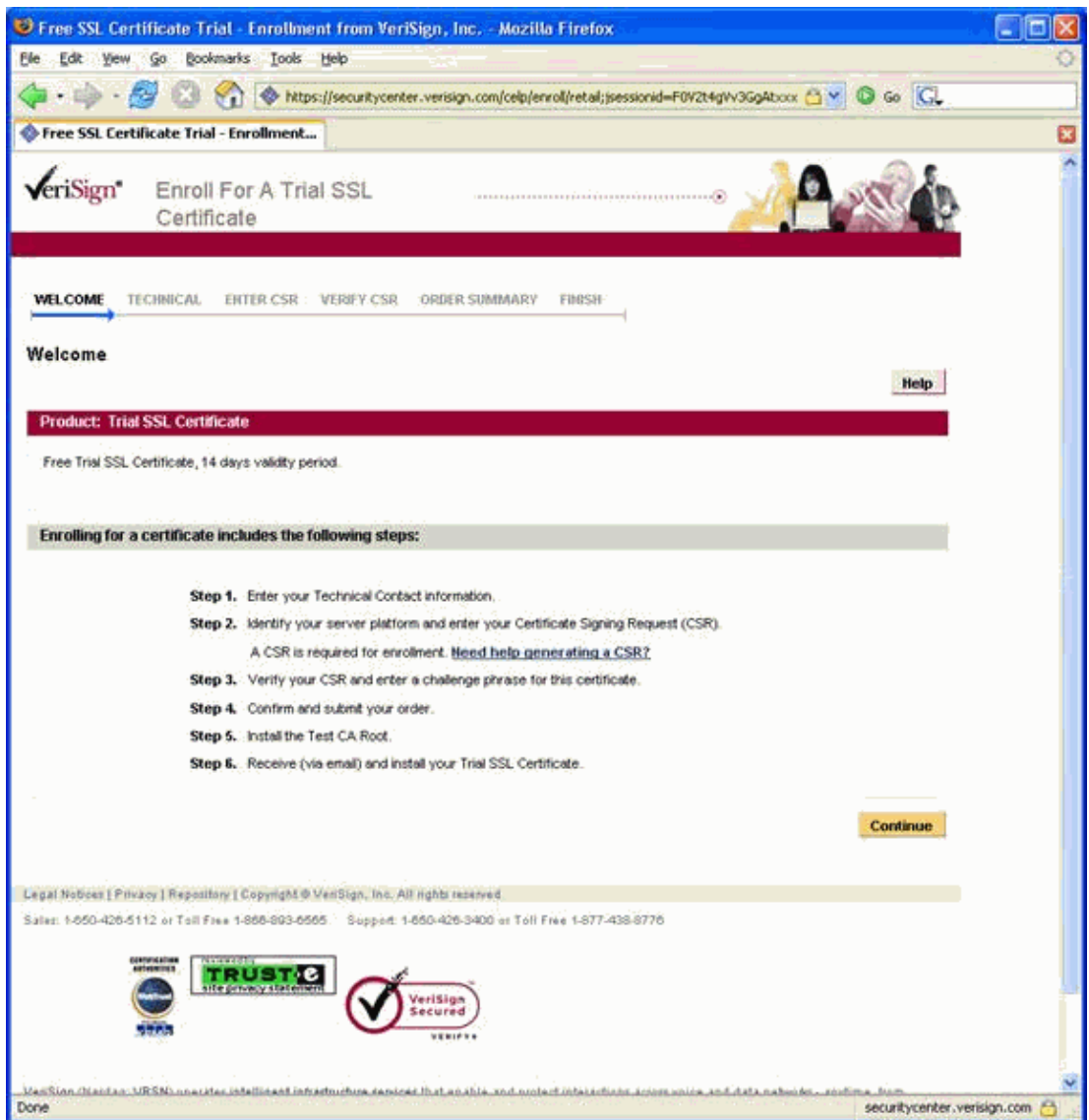
19. Click **Free Trial**, then complete the enrollment process, as shown in this window:

Figure 16



20. Enter the necessary information.

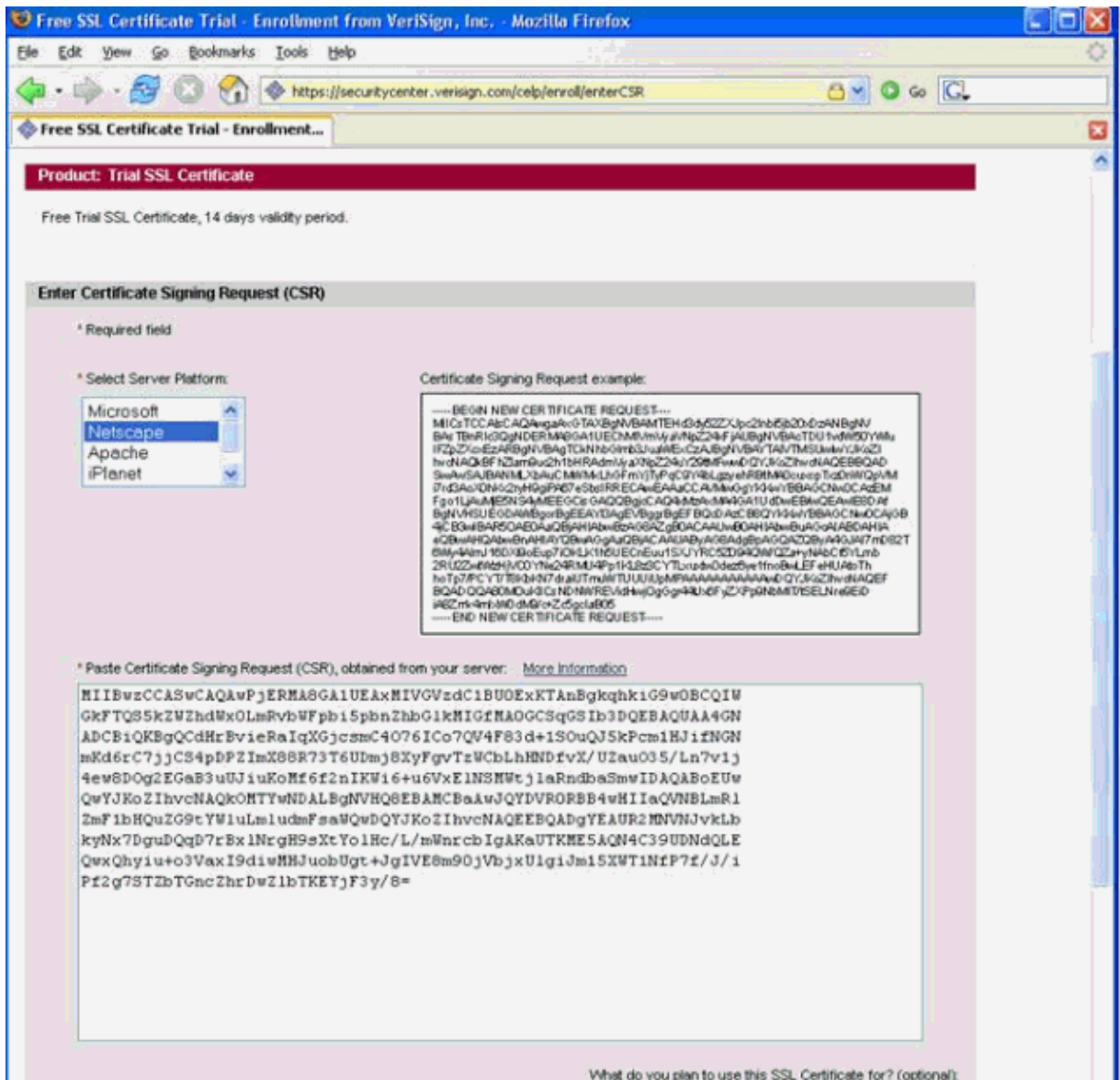
Figure 17



21. Copy the Certificate Request hash captured in step 17 (see Figure 14) and paste it to the VeriSign site.

Note: Make sure you choose **Netscape** from the Select Server Platform.

Figure 18



Note: The What do you plan to use the SSL Certificate for? (optional) option was left unselected at the default.

The device certificate is issued and emailed to you.

In the email, you receive the link to download the root and subsidiary root certificates, as well as an attachment of the device certificate itself.

22. Save the device certificate of the email from VeriSign to your PC by adding the Certificate hash to a text editor and save it as a .cer file.

This example is called **Test-ASA-Device cert.cer**.

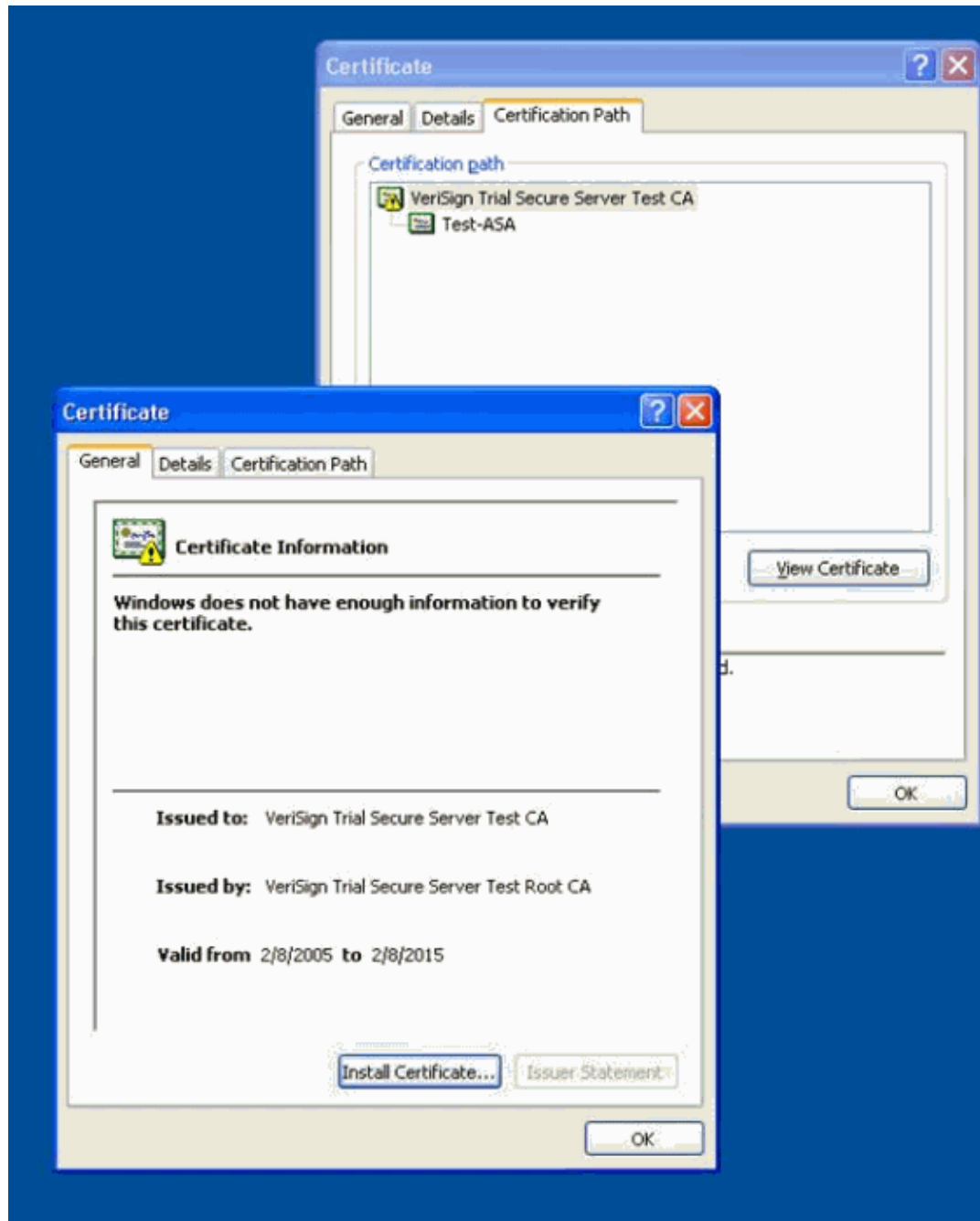
Figure 19



24. Save the Intermediate Root Certificate that is part of the chain.

- a. Choose **Details** of the Subordinate Root Certificate.
- b. Copy and save it as a Base-64 format file, **Trial-root.cer**.

Figure 21

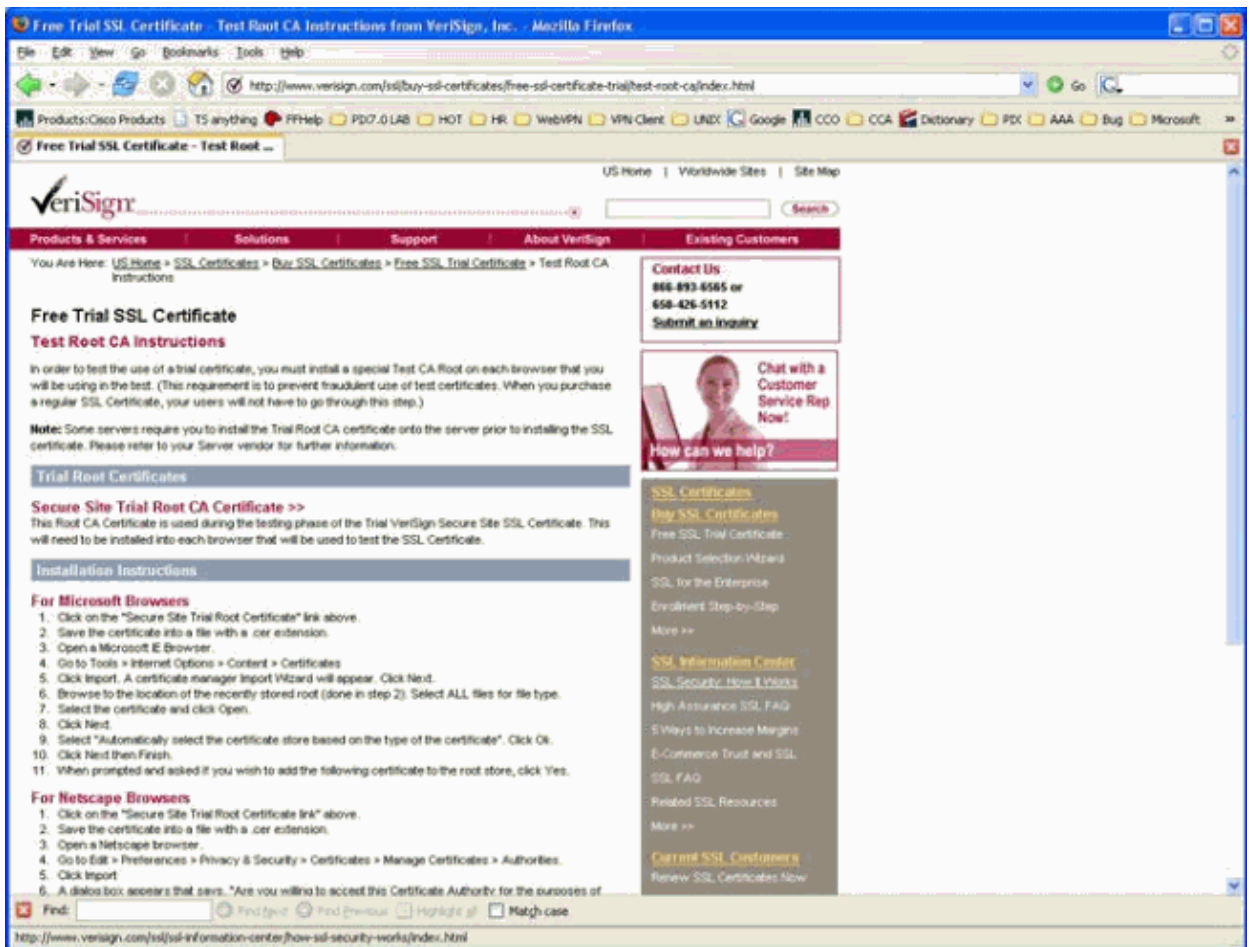


25. Get the root certificate for the subsidiary root.

You still do not have the issuer for the VeriSign Trial Secure Server Test CA.

This can be downloaded from the link which VeriSign sent in the email.

Figure 22



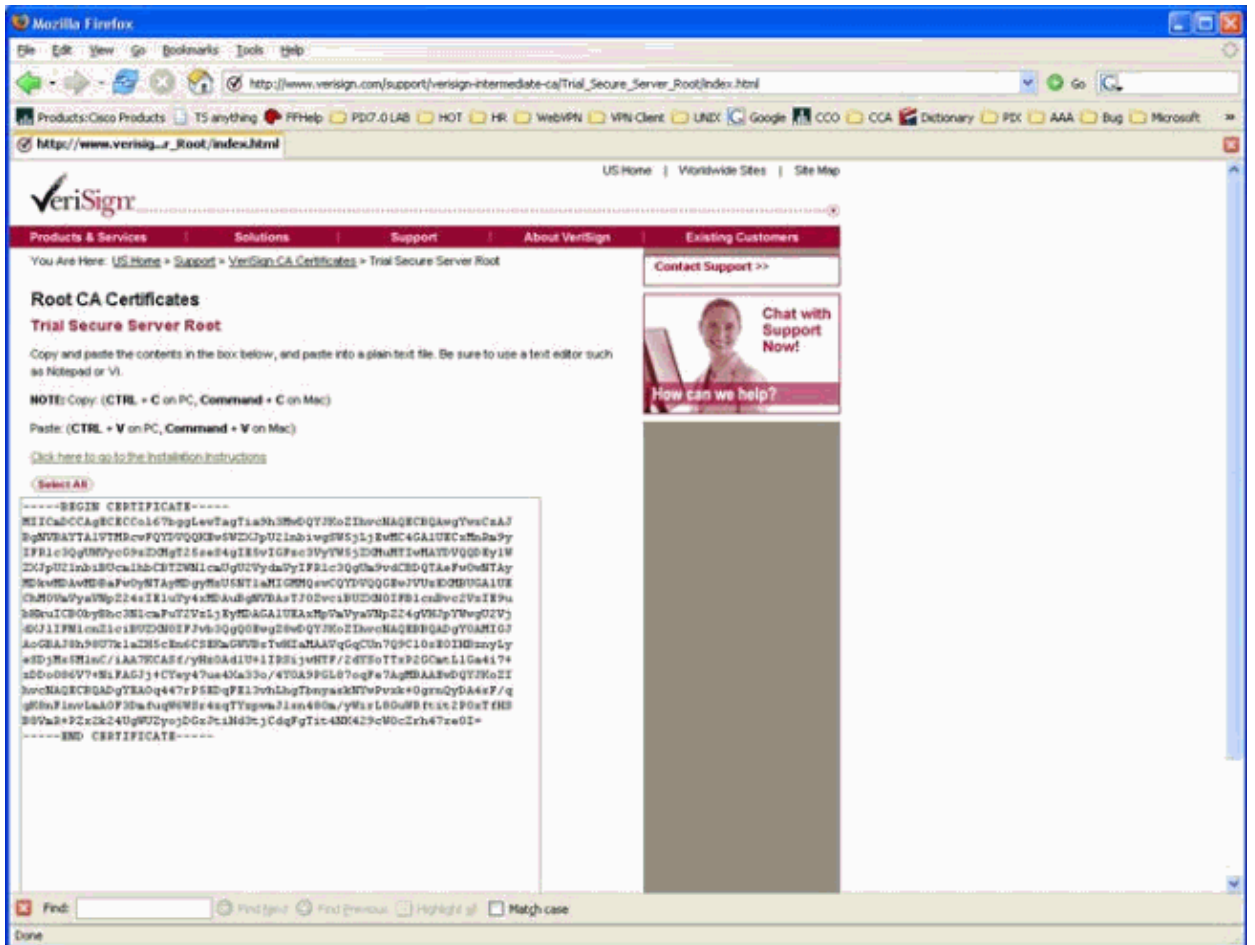
26. Save the root certificate again to your PC.

Choose the certificate hash and save it with a text editor.

This example is called **VeriSign-Root-CA.cer**.

Note: VeriSign might send you a certificate from a root which is different then the one you selected during previous enrollment.

Figure 23



27. Verify the root certificate.

You can see that the Issued by: and Issued to: are the same. This indicates it is the root.

Figure 24



28. Compare the subsidiary and device certificate in order to make sure you have this entire chain:

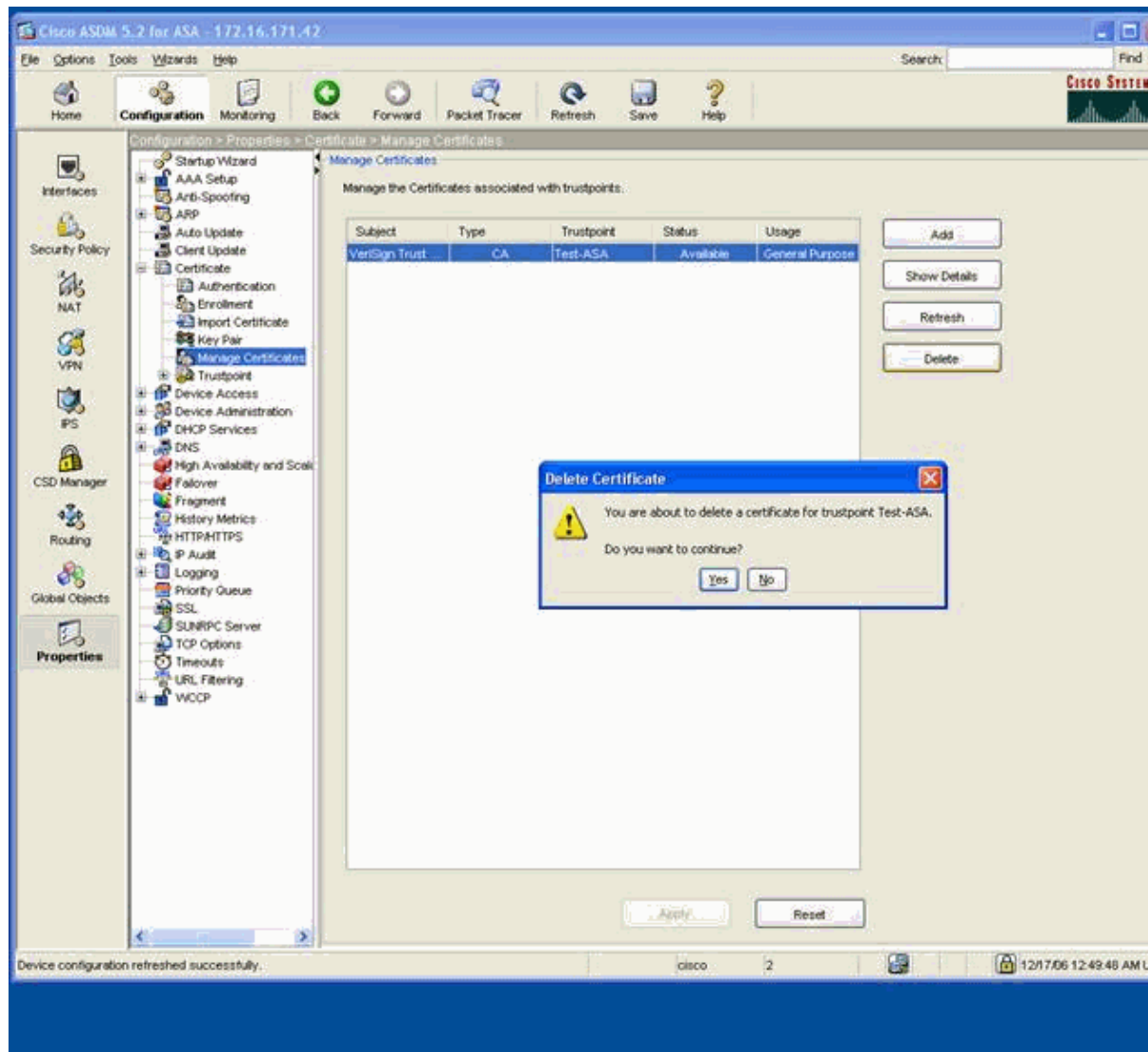
- ◆ VeriSign–Root–CA.cer
- ◆ Sub–Root–Trial.cer
- ◆ Test–ASA–Device cert.cer

29. Install the certificate chain in ASAM to your ASA .

Note: If the certificate issued by VeriSign is issued by a different root than the one you used in step 4, then you need to delete the certificate for the Test–ASA trustpoint before you continue.

- a. Go to **Configuration > Properties > Certificate > Manage Certificates**.
- b. Choose your certificate associated with the Test–ASA Certificate request, then click **Delete**.
- c. Confirm the Delete Certificate warning.
- d. Click **Apply**.

Figure 25



This only deletes the certificate used with the enrollment process, not the trustpoint.
 30. Complete these steps in order to enter the entire chain:

a. Find the certificate to delete.

```
ASA(config)#show running-config crypto ca
crypto ca trustpoint Test-ASA
enrollment terminal
fqdn none
subject-name CN=Test-ASA,OU=Lab,O=Cisco Systems,C=US,St=California,L=San Jose
keypair VerisignKey
crl configure
crypto ca certificate chain Test-ASA
certificate ca 00b92f60cc889fa17a4609b85b706c8aaf
!--- This is the name of the certificate to delete.
```

```
30820303 3082026c 021100b9 2f60cc88 9fa17a46 09b85b70 6c8aaf30 0d06092a
864886f7 0d010105 05003081 c1310b30 09060355 04061302 55533117 30150603

55040a13 0e566572 69536967 6e2c2049 6e632e31 3c303a06 0355040b 1333436c
61737320 32205075 626c6963 20507269 6d617279 20436572 74696669 63617469
6f6e2041 7574686f 72697479 202d2047 32313a30 38060355 040b1331 28632920
31393938 20566572 69536967 6e2c2049 6e632e20 2d20466f 72206175 74686f72
697a6564 20757365 206f6e6c 79311f30 1d060355 040b1316 56657269 5369676e
20547275 7374204e 6574776f 726b301e 170d3938 30353138 30303030 30305a17
0d323830 38303132 33353935 395a3081 c1310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 3c303a06 0355040b
1333436c 61737320 32205075 626c6963 20507269 6d617279 20436572 74696669
63617469 6f6e2041 7574686f 72697479 202d2047 32313a30 38060355 040b1331
28632920 31393938 20566572 69536967 6e2c2049 6e632e20 2d20466f 72206175
74686f72 697a6564 20757365 206f6e6c 79311f30 1d060355 040b1316 56657269
5369676e 20547275 7374204e 6574776f 726b3081 9f300d06 092a8648 86f70d01
01010500 03818d00 30818902 818100a7 88012174 2ce71a03 f098e197 3c0f2108
f19cdb97 e99afcc2 040613be 5f52c8cc 1e2c1256 2cb80169 2ccc991f adb096ae
7904f213 39c17b98 ba082ce8 c284132c aa69e909 f4c7a902 a442c223 4f4ad8f0
0ea2fb31 6cc9e66f 992707f5 e6f44c78 9e6deb46 86fab986 c954f2b2 c4afd446
1c5ac915 30ff0d6c f52d0e6d ce7f7702 03010001 300d0609 2a864886 f70d0101
05050003 81810072 2ef97fd1 f171fbc4 9ef6c55e 518a4098 b868f89b 1c83d8e2
9dbdffed ale666ea 2f09f4ca d7eaa52b 95f62460 864d442e 83a5c42d a0d3ae78
696f72da 6cae08f0 639237e6 bbc43017 ad77cc49 35aacfd8 8fd1beb7 18964773
6a542234 642db616 9b595bb4 51593ab3 0b14f412 df67a0f4 ad32645e b1467227
8c127bc5 44b4ae
```

```
quit
```

```
ASA(config)#
```

b. Delete the old root certificate.

```
ASA(config)#crypto ca certificate chain Test-ASA
```

```
ASA(config-cert-chain)#no certificate ca 00b92f60cc889fa17a4609b85b706c8aaf
```

```
WARNING: The CA certificate will be disassociated from this trustpoint and
```

will be removed if it is not associated with any other trustpoint. Any other certificates issued by this CA and associated with this trustpoint will also be removed.

Are you sure you want to remove the certificate? [yes/no]: **yes**

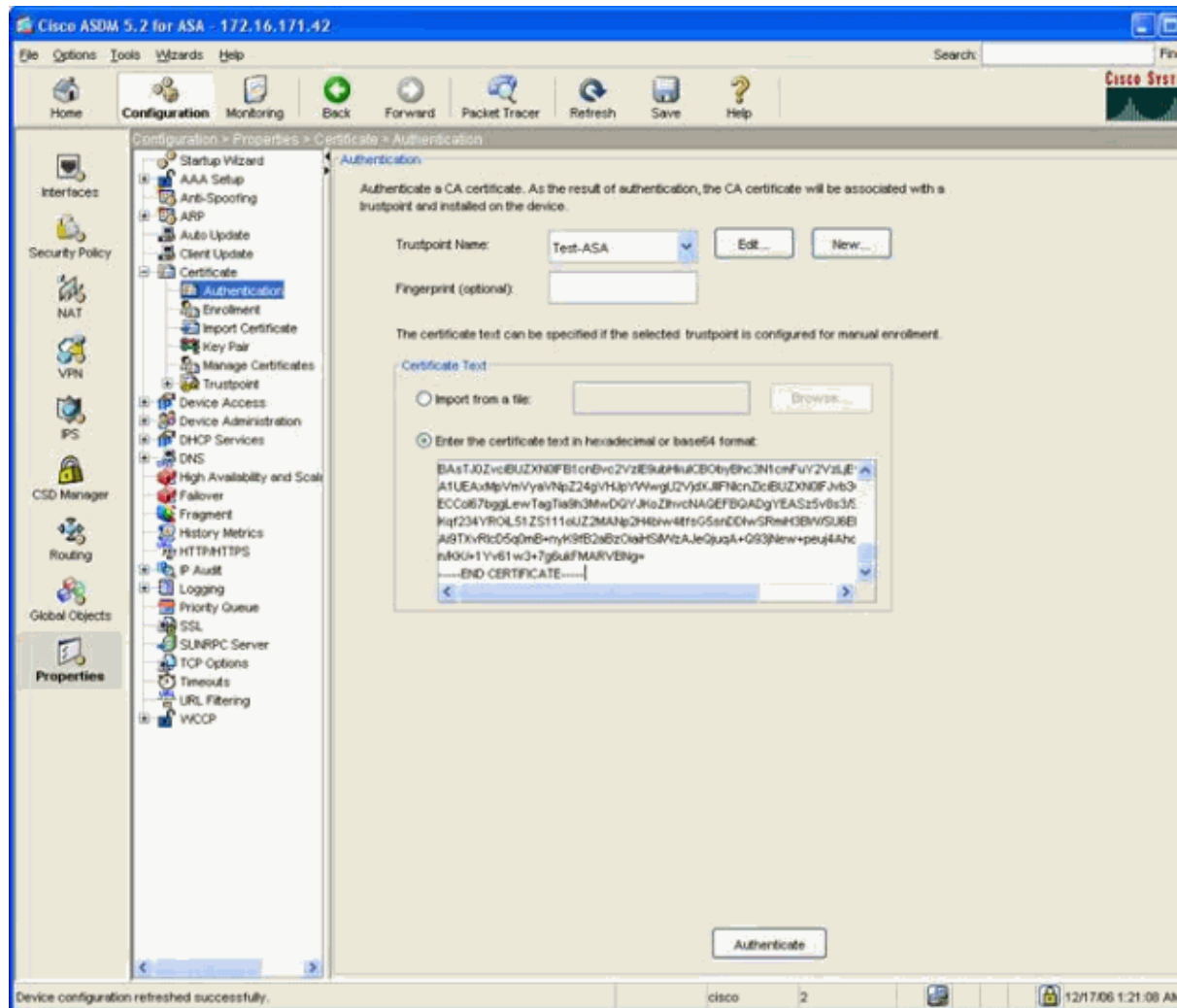
ASA(config-cert-chain)#

31. Authenticate the subordinate root with the original authentication request.

- a. Go to **Configuration > Properties > Certificate > Authentication** and choose **Test-ASA**.
- b. Choose **Enter the certificate text in hexadecimal or base64 format**.
- c. Paste the certificate hash of the Sub-Root-Trial.cer file.
- d. Click **Authenticate**.

This is the trustpoint that was used in the enrollment request in step 4. This binds the subordinate root certificate with the trustpoint.

Figure 26



This is the CLI output:

```

ASA(config-cert-chain)#crypto ca authenticate Test-ASA nointeractive

Enter the certificate in hexadecimal or base64 representation....

End with the word "quit" on a line by itself.

ASA(config-pubkey)# -----BEGIN CERTIFICATE-----

ASA(config-pubkey)# MIIEdCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0BA

ASA(config-pubkey)# jDELMakGAlUEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBjb2MwMTAwL

ASA(config-pubkey)# EydGb3IgVGVzdCBQdXJwb3NlcyBPbmh5LiAgTm8gYXNzdXJhbmNlcy4xM

ASA(config-pubkey)# BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIzIGVGVzdCBSb290I

ASA(config-pubkey)# DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYTA

ASA(config-pubkey)# FQYDVQKKEw5WZXXJpU2lnbiwgSW5jLjEwMC4GA1UECzMnRm9yIFRlc3QgU

ASA(config-pubkey)# ZXMGt25seS4gIE5vIGFzc3VyYW5jZXMumUIWQAYDVQQLEz1UZXXJtcyBvZ

ASA(config-pubkey)# YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpM

ASA(config-pubkey)# BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIzIGVGVzdCBQd

ASA(config-pubkey)# DQYJKoZIhvcNAQEBBQADgGEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAuw

ASA(config-pubkey)# DV8zgpvxuwaMv6fNQBHSF4eKkFDcJLjVnP53ZiGcLAAwTC5ivGpGqE61

ASA(config-pubkey)# d851Pl/6XxK0EdmrN7qVMmvBMGRsmOjjelop5f0nKPqVoNK2qNUB6n451

ASA(config-pubkey)# E0bdru16quZ+II2cGFAGl0SyRy4wvY/dpVHuZOZqYcIkk08yGotR2xA1D

ASA(config-pubkey)# 5RmNqLLKSvYHhJ25EskFhgR2qCxx2EQJdnDXuTw0+4t1qj97ydk5iDox

ASA(config-pubkey)# tnp3TIY6S07bTb9gxJck4pGbcf8DOPvOfGRulwPfuUzC8v+WKC20+sK6Q

ASA(config-pubkey)# AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBABA

ASA(config-pubkey)# hvhFAQcVMDIwMAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3LnZlcmlzaWduL

ASA(config-pubkey)# cHMvdGVzdGNhLzAObGNVHQ8BAf8EBAMCAQYwEQYJYIZIAyb4QgEBBAQDA

ASA(config-pubkey)# AlUdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGNo

ASA(config-pubkey)# MIGMMQswCQYDVQQGEwJVUzEXMBUGAlUEChMOVmVyaVNPZ24sIEluYy4xM

ASA(config-pubkey)# BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3NlcmFuY2VzL

ASA(config-pubkey)# AlUEAxMpVmVyaVNPZ24gVHJpYWwgU2VjdXJlIFNlcnZlcmlBUZXN0IFJvb

ASA(config-pubkey)# ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/S

ASA(config-pubkey)# Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU6

ASA(config-pubkey)# Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaihSiIWzAJeQjuqA+Q93jNew+peuj

ASA(config-pubkey)# n/KK/+1Yv61w3+7g6ukFMARVBNg=

ASA(config-pubkey)# -----END CERTIFICATE-----

ASA(config-pubkey)# quit

```

INFO: Certificate has the following attributes:

Fingerprint: 8de989db 7fcc5e3b fdde2c42 0813ef43

Trustpoint 'Test-ASA' is a subordinate CA and holds a non self-signed certificate

Trustpoint CA certificate accepted.

ASA(config)#

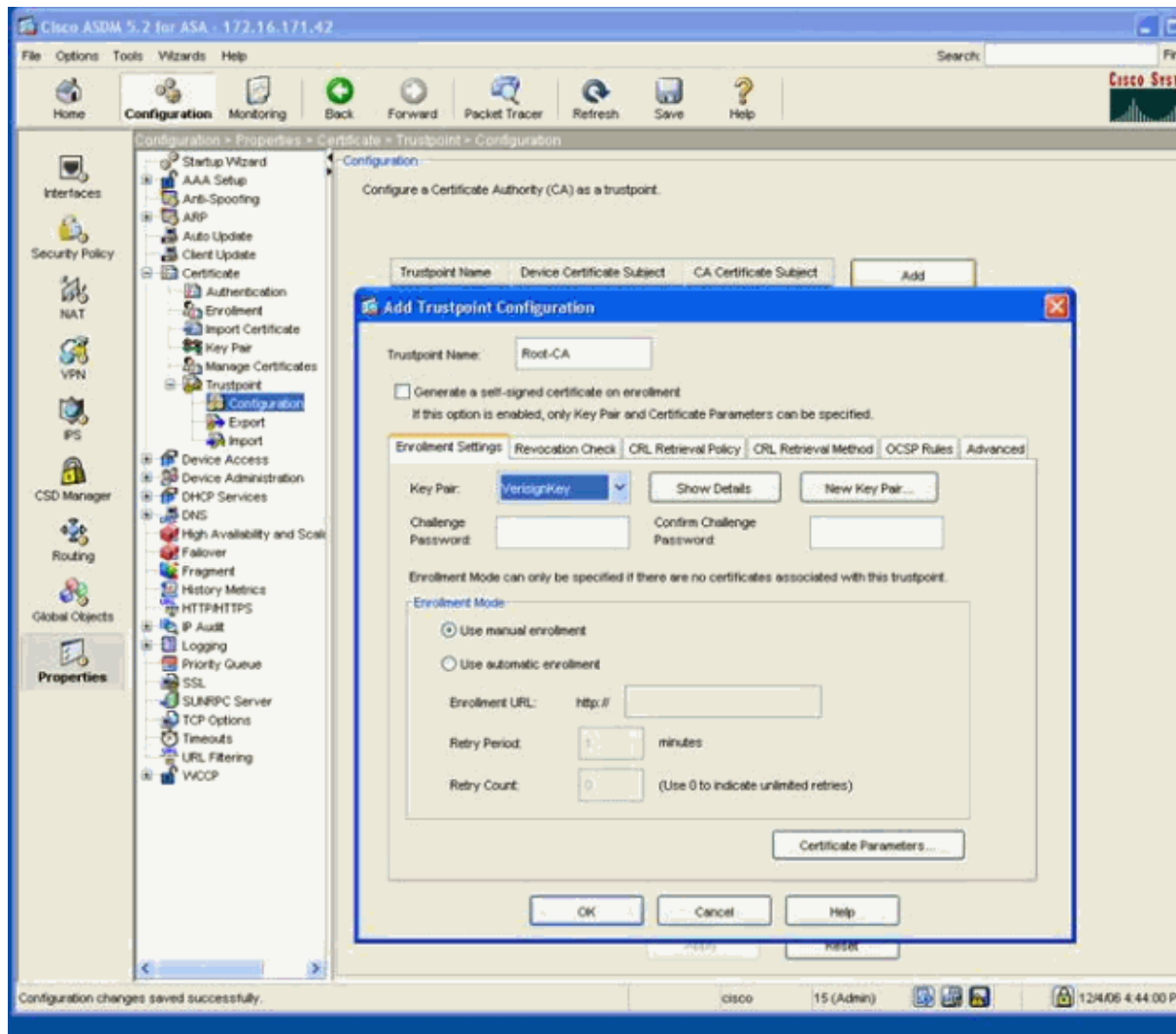
32. Create a new trustpoint for the new root.

- a. Go to **Configuration > Properties > Certificate > Trustpoint > Configuration > Add.**
- b. Enter a Trustpoint Name.

This example is named **Root-CA**

- c. Choose **VeriSignKey** as the Key Pair.
- d. Click **OK**, then click **Apply**.

Figure 27



This is the CLI output:

```
ASA(config)#crypto ca trustpoint Root-CA

ASA(config-ca-trustpoint)#revocation-check none

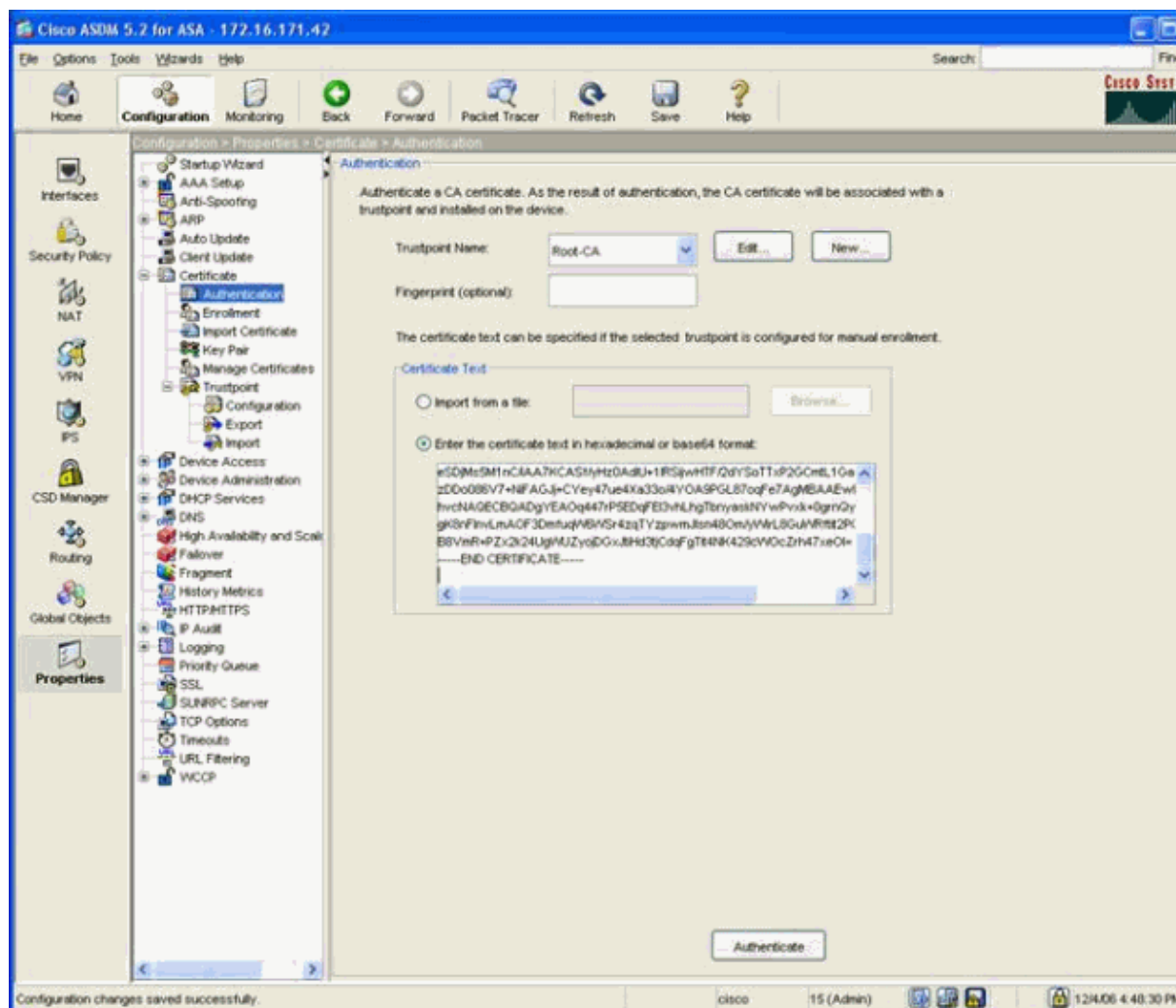
ASA(config-ca-trustpoint)#keypair VerisignKey

ASA(config-ca-trustpoint)#enrollment terminal
```

33. Authenticate the Root CA.

- Go to **Configuration > Properties > Certificate > Authentication**.
- Choose **Root CA** under Trustpoint Name.
- Choose **Enter the certificate text in hexadecimal or base64 format**.
- Paste the certificate hash of the VeriSign-Root-CA.cer file.
- Click **Authenticate**.

Figure 28



This is the CLI output:

```
ASA(config-ca-trustpoint)#crypto ca authenticate Root-CA noninteractive

Enter the certificate in hexadecimal or base64 representation....
```

End with the word "quit" on a line by itself.

```
ASA(config-pubkey)# -----BEGIN CERTIFICATE-----
```

```
ASA(config-pubkey)# MIICmDCCAgECECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQECBQAw
```

```
ASA(config-pubkey)# BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UEC
```

```
ASA(config-pubkey)# IFRlc3QgUHVycG9zZXMGt25seS4gIE5vIGFzc3VyYW5jZXMumTIwMAYDV
```

```
ASA(config-pubkey)# ZXJpU2lnbiBUcm1hbCBTZWN1cmUgU2VydmVYIFRlc3QgUm9vdCBDQTAeF
```

```
ASA(config-pubkey)# MDkwMDAwMDBaFw0yNTAyMDgyMzU5NTlaMIGMMQswCQYDVQQGEwJVVzEXM
```

```
ASA(config-pubkey)# ChMOVmVyaVNPz24sIEluYy4xMDAuBgNVBAsTJ0ZvcjBUZXN0IFB1cnBvc
```

```
ASA(config-pubkey)# bHkuICBObyBhc3N1cmFuY2VzLjEyMDAGA1UEAxMpVmVyaVNPz24gVHJpY
```

```
ASA(config-pubkey)# dXJlIFN1cnZlcjBUZXN0IFJvb3QgQ0EwgZ8wDQYJKoZIhvcNAQEBBQAg
```

```
ASA(config-pubkey)# AoGBAJ8h98U7klaZH5cEn6CSEKmgWVBsTwhIaMAAVqGqCUn7Q9C10sEOI
```

```
ASA(config-pubkey)# eSDjMs5M1nC/iAA7KCASF/yHz0AdlU+1IRSi jwHTF/2dYSOTTxP2GCmtL
```

```
ASA(config-pubkey)# zDDo086V7+NifAGJj+CYey47ue4Xa33o/4YOA9PGL87oqFe7AgMBAAEwD
```

```
ASA(config-pubkey)# hvcNAQECBQADgYEAQq447rP5EDqFE13vhLhgTbnyaskNYwPvXk+0grnQY
```

```
ASA(config-pubkey)# gK8nFlnvLmAOF3DmfuqW6WSr4zqTYzpwmlsn480m/yWirL8GuWRftit2
```

```
ASA(config-pubkey)# B8VmR+PZx2k24UgWUZYojDGxJtiHd3tjCdqFgTit4NK429cWocZrh47xe
```

```
ASA(config-pubkey)# -----END CERTIFICATE-----
```

```
ASA(config-pubkey)# quit
```

```
INFO: Certificate has the following attributes:
```

```
Fingerprint:      b69da440 5202500d d59ce1b8 4b66c4ac
```

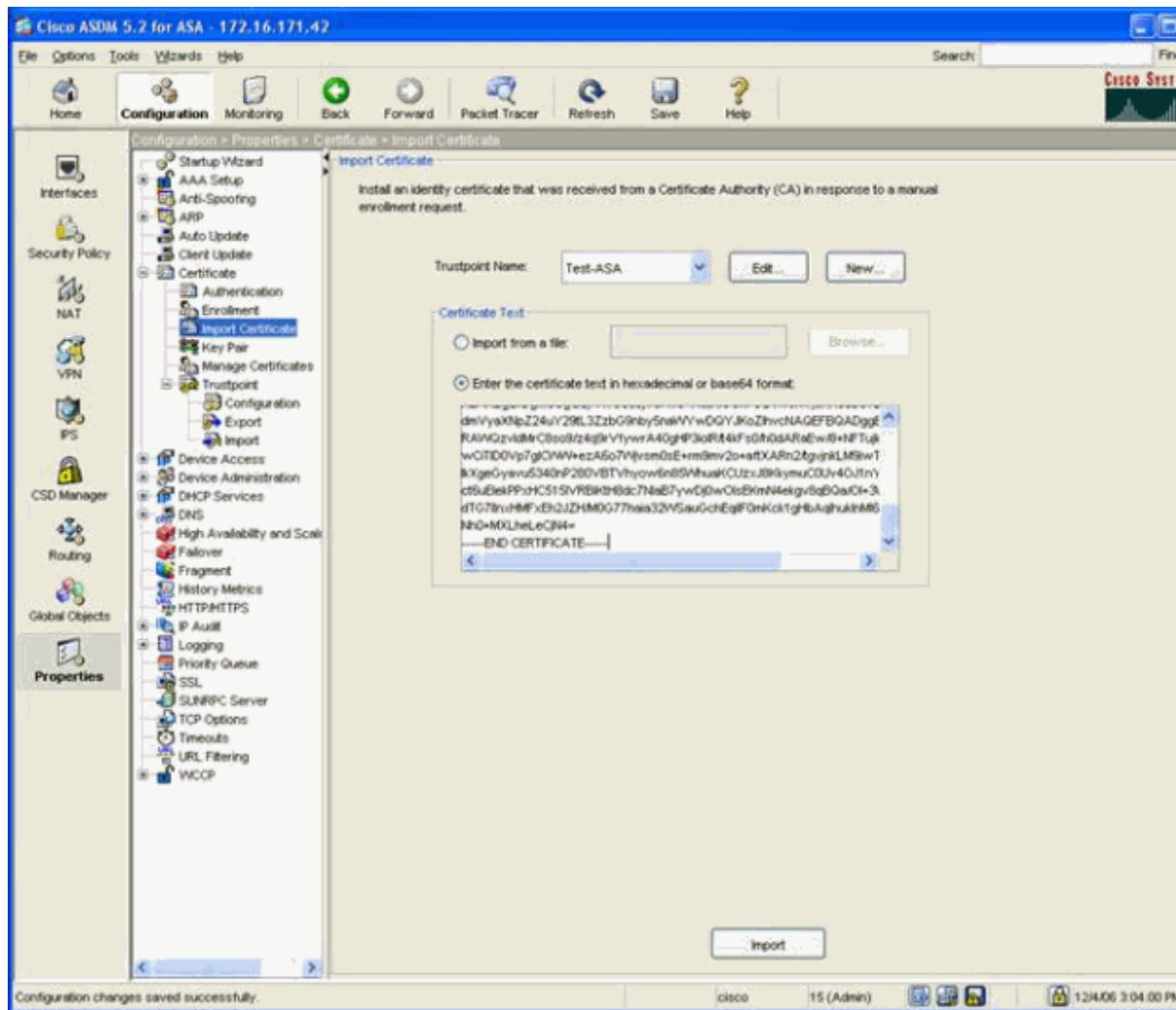
```
Trustpoint CA certificate accepted.
```

```
ASA(config)#
```

34. Import the device certificate which was sent to you in the email from VeriSign.

- Go to **Configuration > Properties > Certificate > Import Certificate**.
- Choose **Test-ASA** under Trustpoint Name.
- Choose **Enter the certificate text in hexadecimal or base64 format**.
- Paste the certificate hash of the Test-ASA-Device cert.cer file.
- Click **Import**.

Figure 29



This is the CLI output:

```

ASA(config)#
ASA(config)#crypto ca import Test-ASA certificate nointeractive
Enter the certificate in hexadecimal or base64 representation....
ASA(config-pubkey)# -----BEGIN CERTIFICATE-----
ASA(config-pubkey)# MIIFVjCCBD6gAwIBAgIQYSGLk7K0KNOQxQte58FYeTANBqkqhkiG9w0BA
ASA(config-pubkey)# yzELMAkGA1UEBhMCVVMxZjZAVBgnVBAoTD1Zlcm1TaWduLCBjbmuMTAwL
ASA(config-pubkey)# EydG3IgvGVzdBQdXJwb3NlcYBPbm5LiAgTm8gYXNzdXJhbmNlcY4xO
ASA(config-pubkey)# BAsTOVr1cm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb
ASA(config-pubkey)# L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNPZ224gVHJpYWwgU2Vjd
ASA(config-pubkey)# cnZlciBUZXN0IENBMB4XDTA2MTIxNzAwMDAwMfoXDTA2MTIzMTIzNTk1O
ASA(config-pubkey)# CzAJBgNVBAYTAlVTMRMwEQYDVQQIEWpDYWxpZm9yYm1hMREwDwYDVQQH
ASA(config-pubkey)# Sm9zZTEwMjZlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb
ASA(config-pubkey)# VQQLFDZlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb

```

```

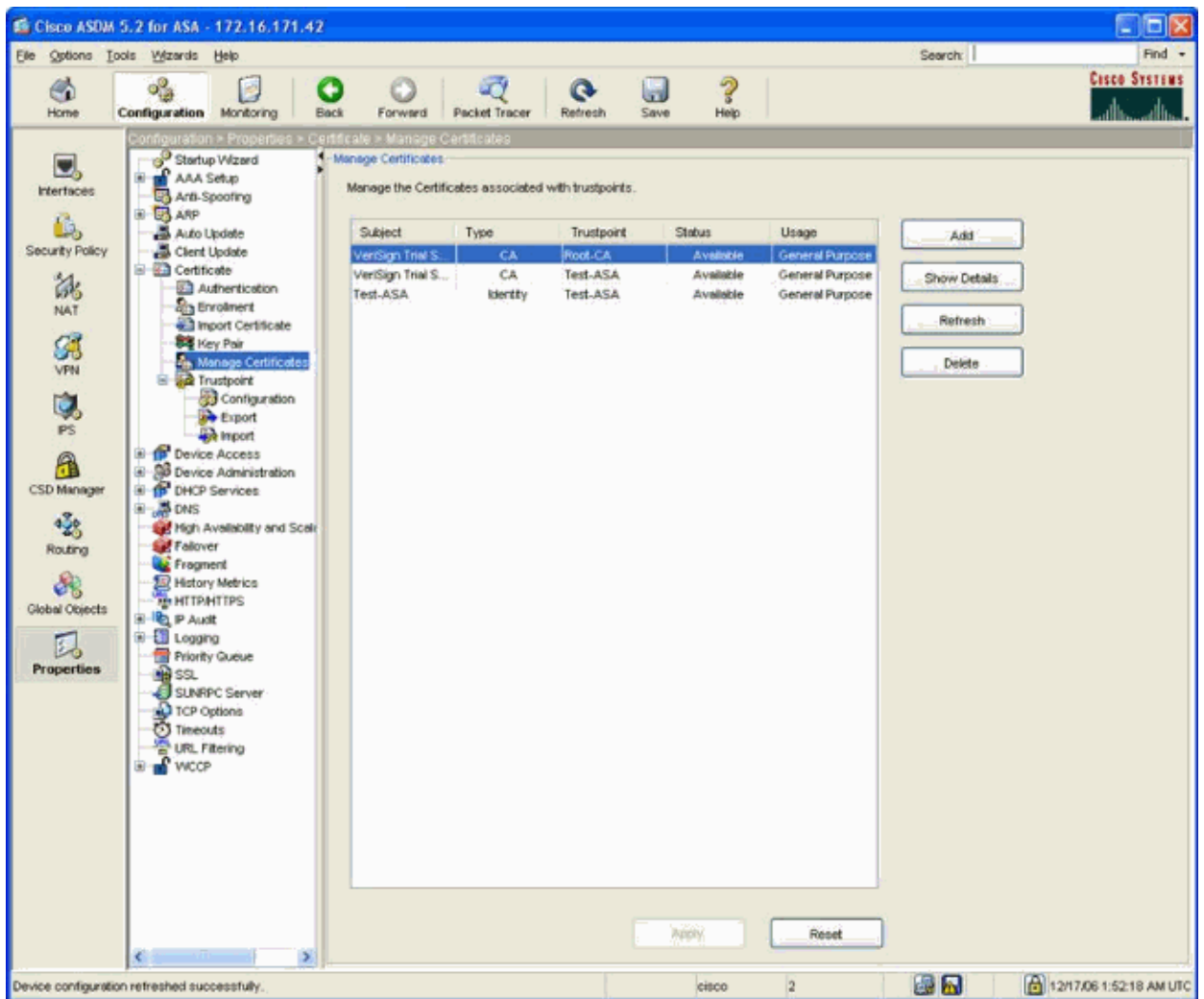
ASA(config-pubkey)# IChjKTA1MREwDwYDVQQDFAhUZXXN0LUFTQTCBnzANBgkqhkiG9w0BAQEFA
ASA(config-pubkey)# gYkCgYEAnR6wb4nkWiKlxo3LJguDu+iAqO0FeBfN3ftUjrkCeZD3JtRyY
ASA(config-pubkey)# eqwu44wkuKQz2SJl/PEe90+lA5o/F8hYL081gmy4RzQ371/1GWrjt+fy5
ASA(config-pubkey)# PAzoNhBmgd7lCYriqDH+n9pyClouvruclcRJTUjFrY5WkZ3W2kpsCAwEAA
ASA(config-pubkey)# ggHTMAkGAlUdEwQCMAAwCwYDVR0PBQAQDAgWgMEMGAlUdHwQ8MDowOKA2o
ASA(config-pubkey)# dHA6Ly9TVlJlJTZW1cmUtY3JsLnZlcm1zaWduLmNvbS9TVlJlUcmlhbDIwM
ASA(config-pubkey)# MEOGA1UdIARDMEewPwYKYIZIAYb4RQEHEFTaxMC8GCCsGAQUFBwIBFiNod
ASA(config-pubkey)# L3d3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrB
ASA(config-pubkey)# AQYIKwYBBQUHAWIwHwYDVR0jBBGwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh
ASA(config-pubkey)# KwYBBQUHAQEebDBqMCQGCCsGAQUFBzABhhhodHRwOi8vb2Nzc52ZXJpc
ASA(config-pubkey)# b20wQgYIKwYBBQUHMAKGNmh0dHA6Ly9TVlJlJTZW1cmUtYWlhLnZlcm1za
ASA(config-pubkey)# bs9TVlJlUcmlhbDIwMDUtYWlhLmNlcjBuBgggrBgEFBQcBDARiMGChXqBcM
ASA(config-pubkey)# FglpbWFnZS9naWYwITAFMacGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHi
ASA(config-pubkey)# FiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJK
ASA(config-pubkey)# AQEFBQADggEBACE8/b+pm1Z000xE+UVBANME6Ct/Qvja9FZkUcMVmCjpd
ASA(config-pubkey)# GmEDug54Usn+2lCpBwhoqeFN3a00B0ngtRpc00mQXx0fkeb0OP+fEa4fD
ASA(config-pubkey)# xhZVQ7Htx/WHq1fNsOfRNdy2lWQ2Mn0qyR1c4UhwSbn2XbJkb0SriZb3p
ASA(config-pubkey)# kkeE/y1ML6afW1gf0fSManVTB/nvw2lEFgUJm8pEWei2g1Lk09w3hkHkC
ASA(config-pubkey)# Auy0AHqvRNfuIC7YE/BuaPD5ZtH19NRAPddYhLvqy4DJQlTfnG+lZ6VGH
ASA(config-pubkey)# rKBw/hJznHvBl42TxRV5006suDEesbtsJoc=
ASA(config-pubkey)# -----END CERTIFICATE-----
ASA(config-pubkey)# quit
INFO: Certificate successfully imported
ASA(config)#

```

35. Verify that the certificates have been installed correctly.

Go to **Configuration > Properties > Certificate > Manage Certificates**.

Figure 30



This is the CLI output:

```

ASA(config)#show crypto ca certificates

Certificate

Status: Available

Certificate Serial Number: 61218b93b2b428dd10c50b5ee7c15879

Certificate Usage: General Purpose

Public Key Type: RSA (1024 bits)

Issuer Name:

    cn=VeriSign Trial Secure Server Test CA
    ou=Terms of use at https://www.verisign.com/cps/testca (c)05
    ou=For Test Purposes Only. No assurances.
    o=VeriSign\, Inc.
    c=US

Subject Name:

```

cn=Test-ASA

!--- This is the device certificate.

ou=Terms of use at www.verisign.com/cps/testca (c)05

ou=Lab

o=Cisco Systems

l=San Jose

st=California

c=US

OCSP AIA:

URL: <http://ocsp.verisign.com>

CRL Distribution Points:

[1] <http://SVRSecure-crl.verisign.com/SVRTrial2005.crl>

Validity Date:

start date: 00:00:00 UTC Dec 17 2006

end date: 23:59:59 UTC Dec 31 2006

Associated Trustpoints: Test-ASA

CA Certificate

Status: Available

Certificate Serial Number: 20a897aedb8202dec136a04e26bd8773

Certificate Usage: General Purpose

Public Key Type: RSA (1024 bits)

Issuer Name:

cn=VeriSign Trial Secure Server Test Root CA

ou=For Test Purposes Only. No assurances.

o=VeriSign\, Inc.

c=US

Subject Name:

cn=VeriSign Trial Secure Server Test Root CA

!--- This is the subordinate root.

ou=For Test Purposes Only. No assurances.

```
o=VeriSign\, Inc.  
c=US  
Validity Date:  
start date: 00:00:00 UTC Feb 9 2005  
end date: 23:59:59 UTC Feb 8 2025  
Associated Trustpoints: Root-CA
```

CA Certificate

```
Status: Available  
Certificate Serial Number: 63b1a5cdc59f78801da0636cf975467b  
Certificate Usage: General Purpose  
Public Key Type: RSA (2048 bits)  
Issuer Name:  
cn=VeriSign Trial Secure Server Test Root CA  
!-- This is the root certificate.  
ou=For Test Purposes Only. No assurances.  
o=VeriSign\, Inc.  
c=US  
Subject Name:  
cn=VeriSign Trial Secure Server Test CA  
ou=Terms of use at https://www.verisign.com/cps/testca (c)05  
ou=For Test Purposes Only. No assurances.  
o=VeriSign\, Inc.  
c=US  
Validity Date:  
start date: 00:00:00 UTC Feb 9 2005  
end date: 23:59:59 UTC Feb 8 2015  
Associated Trustpoints: Test-ASA
```

```
ASA(config)#
```

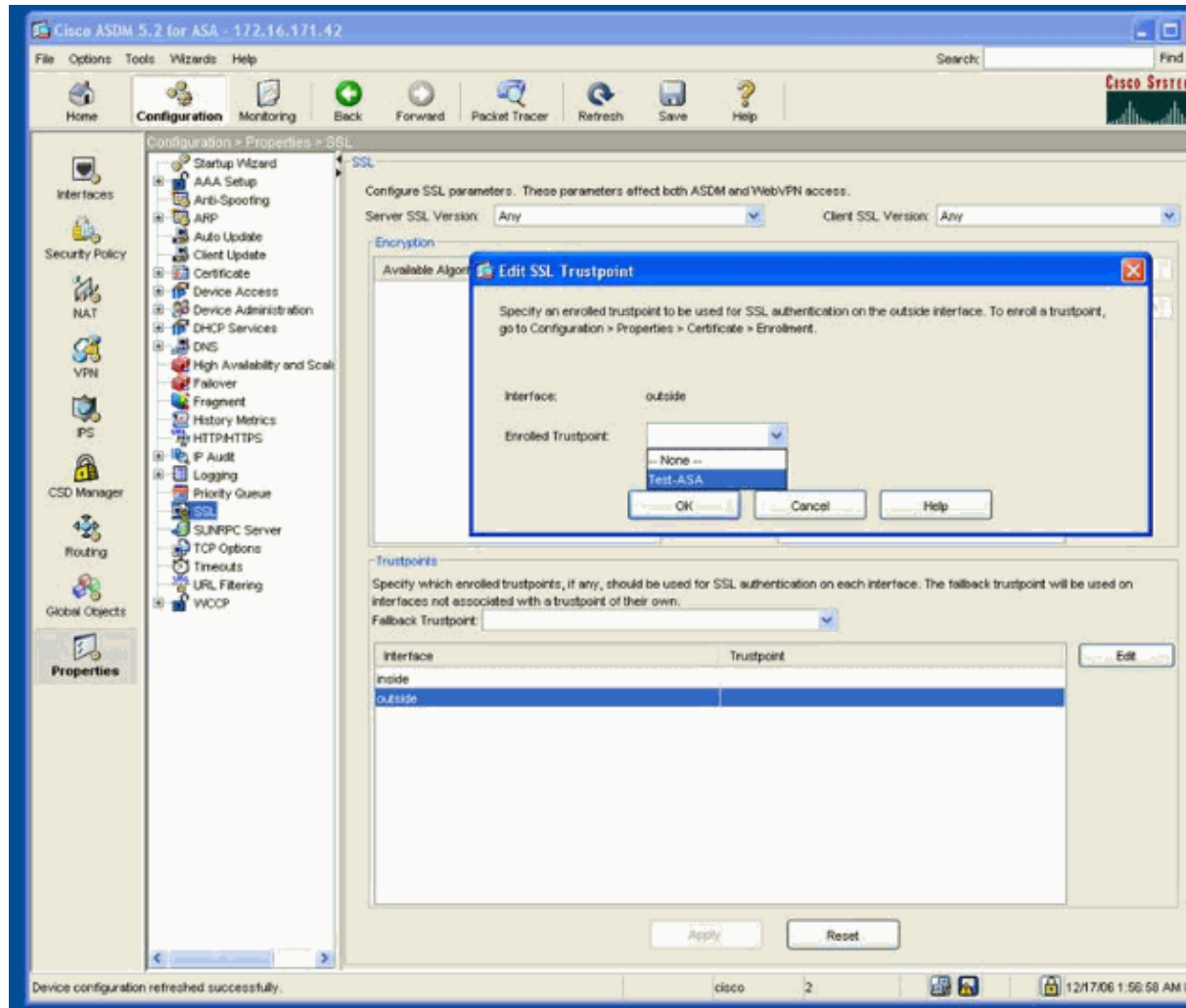
36. Apply the new trustpoint to the outside interface for SSL VPN.

a. Go to **Configuration > Properties > SSL**.

- b. Choose **outside**.
- c. Choose **Test-ASA** under Enrolled Trustpoint.
- d. Click **OK**, then click **Apply**.

If your entire certificate chain is successfully installed, you see the respective trustpoint that you can bind to the interface.

Figure 31



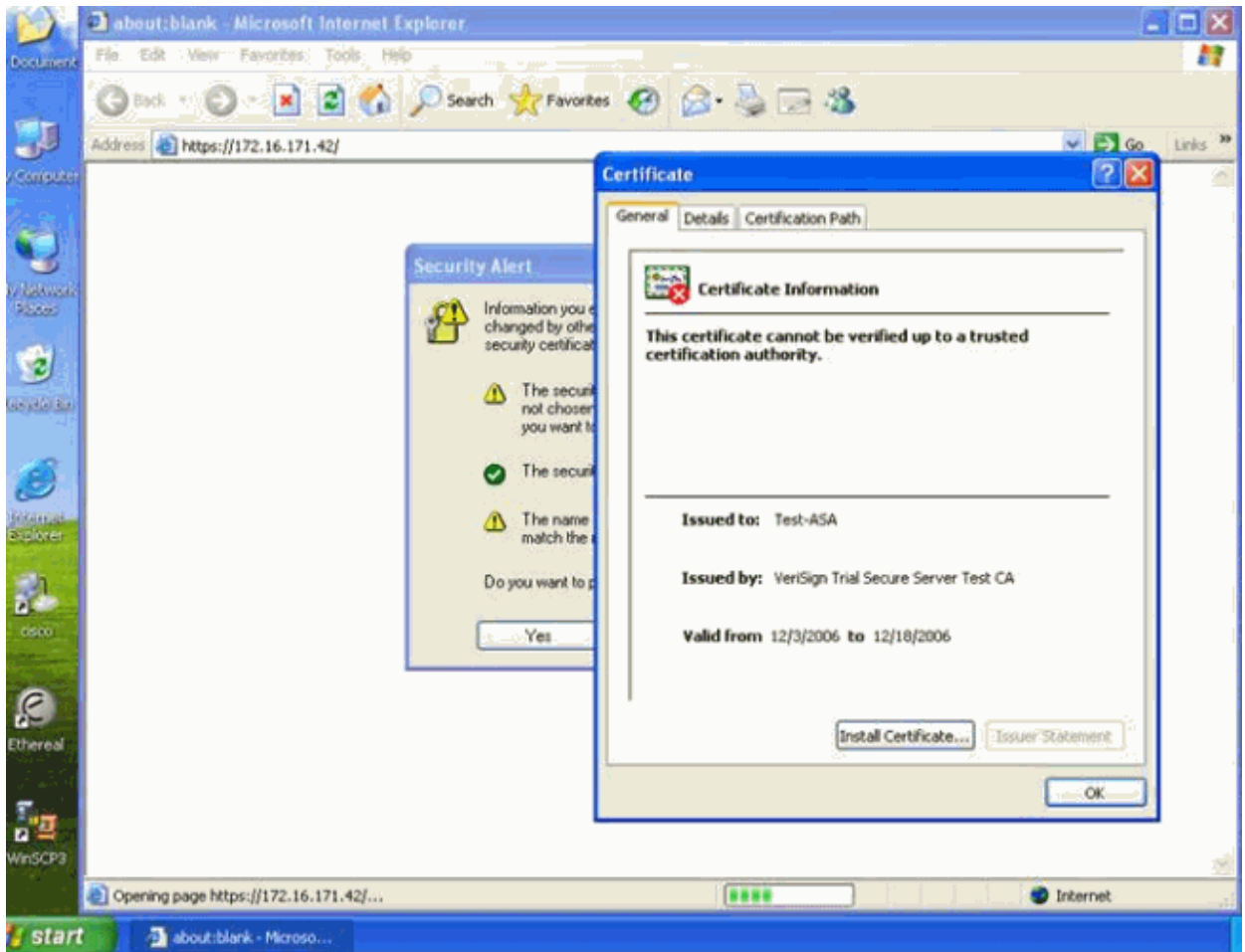
This is the CLI output:

```
ASA(config)#ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 rc4-md5
```

```
ASA(config)#ssl trust-point Test-ASA outside
```

37. With your browser, connect to the ASA outside to test and see if you received the correct SSL certificate.

Figure 32



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

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

These are possible Certificate errors you might see:

- The FQDN in the certificate does not match the URL entered in the browser.
- The root of this certificate is not trusted or has not been imported to the local Certificate store.

Figure 33



This is the configuration:

```
ASA#show running-config

: Saved

:

ASA Version 7.2(1)

!

terminal width 200

hostname ASA

domain-name default.domain.invalid

enable password 2KFQnbNIdI.2KYOU encrypted

names

!

interface Ethernet0/0

 nameif outside

 security-level 0

 ip address 172.16.171.42 255.255.255.0

!

interface Ethernet0/1

 nameif inside

 security-level 100

 ip address 192.168.100.50 255.255.255.0
```

```
!  
interface Ethernet0/2  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Ethernet0/3  
  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  
dns server-group DefaultDNS  
  domain-name default.domain.invalid  
pager lines 24  
mtu outside 1500  
mtu inside 1500  
no failover  
asdm image disk0:/asdm521.bin  
no asdm history enable  
arp timeout 14400  
route outside 0.0.0.0 0.0.0.0 172.16.171.1 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 3USUcOPFUiMCO4Jk encrypted
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
http server enable 8080
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ca trustpoint Test-ASA
  enrollment terminal
  fqdn none
  subject-name CN=Test-ASA,OU=Lab,O=Cisco Systems,C=US,St=California,L=San Jose
  keypair VerisignKey
  crl configure
crypto ca trustpoint Root-CA
  enrollment terminal
  keypair VerisignKey
  crl configure
crypto ca certificate chain Test-ASA
  certificate 61218b93b2b428dd10c50b5ee7c15879
    30820556 3082043e a0030201 02021061 218b93b2 b428dd10 c50b5ee7 c1587930
    0d06092a 864886f7 0d010105 05003081 cb310b30 09060355 04061302 55533117
    30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 30302e06 0355040b
    1327466f 72205465 73742050 7572706f 73657320 4f6e6c79 2e20204e 6f206173
    73757261 6e636573 2e314230 40060355 040b1339 5465726d 73206f66 20757365
    20617420 68747470 733a2f2f 7777772e 76657269 7369676e 2e636f6d 2f637073
    2f746573 74636120 28632930 35312d30 2b060355 04031324 56657269 5369676e
    20547269 616c2053 65637572 65205365 72766572 20546573 74204341 301e170d
```

30363132 31373030 30303030 5a170d30 36313233 31323335 3935395a 3081aa31
0b300906 03550406 13025553 31133011 06035504 08130a43 616c6966 6f726e69
61311130 0f060355 04071408 53616e20 4a6f7365 31163014 06035504 0a140d43
6973636f 20537973 74656d73 310c300a 06035504 0b14034c 6162313a 30380603
55040b14 31546572 6d73206f 66207573 65206174 20777777 2e766572 69736967
6e2e636f 6d2f6370 732f7465 73746361 20286329 30353111 300f0603 55040314
08546573 742d4153 4130819f 300d0609 2a864886 f70d0101 01050003 818d0030
81890281 81009d1e b06f89e4 5a22a5c6 8dcb260b 83bbe880 a8ed0578 17cdddfb
548eb902 7990f726 d472627c d18d98a7 7aac2ee3 8c24b8a4 33d92265 fcf11ef7
4fa5039a 3f17c858 2f4f3582 6cb84734 37ef5ff5 196ae3b7 e7f2e7ee fd63e1ec
3c0ce836 106681de e5098ae2 a831fe9f da720a5a 2ebebba5 71125352 316b6395
a46775b6 929b0203 010001a3 8201d730 8201d330 09060355 1d130402 3000300b
0603551d 0f040403 0205a030 43060355 1d1f043c 303a3038 a036a034 86326874
74703a2f 2f535652 53656375 72652d63 726c2e76 65726973 69676e2e 636f6d2f
53565254 7269616c 32303035 2e63726c 304a0603 551d2004 43304130 3f060a60
86480186 f8450107 15303130 2f06082b 06010505 07020116 23687474 70733a2f
2f777777 2e766572 69736967 6e2e636f 6d2f6370 732f7465 73746361 301d0603
551d2504 16301406 082b0601 05050703 0106082b 06010505 07030230 1f060355
1d230418 30168014 66228e81 e03159dd 2a7fab46 c5360206 7027875a 30780608
2b060105 05070101 046c306a 30240608 2b060105 05073001 86186874 74703a2f
2f6f6373 702e7665 72697369 676e2e63 6f6d3042 06082b06 01050507 30028636
68747470 3a2f2f53 56525365 63757265 2d616961 2e766572 69736967 6e2e636f
6d2f5356 52547269 616c3230 30352d61 69612e63 6572306e 06082b06 01050507
010c0462 3060a15e a05c305a 30583056 1609696d 6167652f 67696630 21301f30
0706052b 0e03021a 04144b6b b9289606 0cbbd052 389b29ac 4b078b21 05183026
16246874 74703a2f 2f6c6f67 6f2e7665 72697369 676e2e63 6f6d2f76 736c6f67
6f312e67 6966300d 06092a86 4886f70d 01010505 00038201 0100213c fdbfa99b
564e38ec 44f94541 027304e8 2b7f42f8 c0f45664 51c31598 28e90e69 63fce6bc
1a6103ba 0e7852c9 feda50a9 070868a9 e14dda3 b40749e0 b51a5c38 e9905f1d
1f91e6f4 38ff9f11 ae1f0d25 9b37d647 c6165543 b1edc7f5 87ab57cd b0e7d135
dcb69564 36327d2a c91d5ce1 487049b9 f65db264 6f44ab89 96f7a6f8 e1f71e5a
924784ff 294c2fa6 9f5b581f d1f48c6a 755307f9 efc36d44 1605099b ca4459e8

b68352e4 d3dc3786 41e40a80 fb0a0524 02ecb400 7aaf44d7 ee202ed8 13f06e68
f0f966d1 f5f4d440 3dd75884 bbeacb80 c94254df 9c6fa567 a5461ed8 c27c078b
aca070fe 12739c7b c1978d93 c515793b 4eacb831 1eb1bb6c 2687

quit

certificate ca 63b1a5cdc59f78801da0636cf975467b

308204c0 30820429 a0030201 02021063 b1a5cdc5 9f78801d a0636cf9 75467b30
0d06092a 864886f7 0d010105 05003081 8c310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 30302e06 0355040b
1327466f 72205465 73742050 7572706f 73657320 4f6e6c79 2e20204e 6f206173
73757261 6e636573 2e313230 30060355 04031329 56657269 5369676e 20547269
616c2053 65637572 65205365 72766572 20546573 7420526f 6f742043 41301e17
0d303530 32303930 30303030 305a170d 31353032 30383233 35393539 5a3081cb
310b3009 06035504 06130255 53311730 15060355 040a130e 56657269 5369676e
2c20496e 632e3130 302e0603 55040b13 27466f72 20546573 74205075 72706f73
6573204f 6e6c792e 20204e6f 20617373 7572616e 6365732e 31423040 06035504
0b133954 65726d73 206f6620 75736520 61742068 74747073 3a2f2f77 77772e76
65726973 69676e2e 636f6d2f 6370732f 74657374 63612028 63293035 312d302b
06035504 03132456 65726953 69676e20 54726961 6c205365 63757265 20536572
76657220 54657374 20434130 82012230 0d06092a 864886f7 0d010101 05000382
010f0030 82010a02 82010100 bb171add 4ce07ca3 5f003efc d02ec049 6fe8827f
0d5f3382 9bfl1bb07 5a32fe9f 35004748 5e1e2a41 437092c9 5673f9dd 988670b0
00c130b9 8afla91a a13ad410 43e99aa4 77ce653e 5ffa5f12 b411d9ab 37ba9532
6bc13064 6c98e8e3 7b5a29e5 fd2728fa 95a0d2b6 a8d501ea 7e39d4fe 2aa32a92
1346ddae ed7aaae6 7e208d9c 185006d6 84b2472e 30bd8fdd a551ee64 e66a61c2
242b4f32 1a8b51db 10350ff3 820a664e e5198da8 b2ca495c 181e1276 e44b2416
1811daa0 b15f6110 25d9c35e e4f0d3ee 2d96a8fd ef2764e6 20e8c632 9f57ab1b
b67a774c 863a4b4e db4dbf60 c490a4e2 919b71ff 0338fbce 7c646ed7 0a5f5146
42f2ff96 282db4fa c2ba40c1 02030100 01a38201 5c308201 58301206 03551d13
0101ff04 08300601 01ff0201 00304b06 03551d20 04443042 3040060a 60864801
86f84501 07153032 30300608 2b060105 05070201 16246874 7470733a 2f2f7777
772e7665 72697369 676e2e63 6f6d2f63 70732f74 65737463 612f300e 0603551d
0f0101ff 04040302 01063011 06096086 480186f8 42010104 04030201 06301d06

```
03551d0e 04160414 66228e81 e03159dd 2a7fab46 c5360206 7027875a 3081b206
03551d23 0481aa30 81a7a181 92a4818f 30818c31 0b300906 03550406 13025553
31173015 06035504 0a130e56 65726953 69676e2c 20496e63 2e313030 2e060355
040b1327 466f7220 54657374 20507572 706f7365 73204f6e 6c792e20 204e6f20
61737375 72616e63 65732e31 32303006 03550403 13295665 72695369 676e2054
7269616c 20536563 75726520 53657276 65722054 65737420 526f6f74 20434182
1020a897 aedb8202 dec136a0 4e26bd87 73300d06 092a8648 86f70d01 01050500
03818100 4b3e6ff2 cdff4a3c d1bd8da5 2aa7f6df 86113a22 f9d594b5 d75a1467
6300369d 87e1b8b0 e22b5fb0 6e6c9c30 e5c12466 887dc15b f494e841 330fda22
022f535e f448703e 6ad2607e 9f22bd7c 1d9a0733 a26a21d2 8885b300 97908eea
80f90f77 8cd7b0fa 97ae8f80 2176f18d 9ff28aff ed58bfad 70dfeee0 eae90530 045504d8
```

quit

crypto ca certificate chain Root-CA

certificate ca 20a897aedb8202dec136a04e26bd8773

```
30820298 30820201 021020a8 97aedb82 02dec136 a04e26bd 8773300d 06092a86
4886f70d 01010205 0030818c 310b3009 06035504 06130255 53311730 15060355
040a130e 56657269 5369676e 2c20496e 632e3130 302e0603 55040b13 27466f72
20546573 74205075 72706f73 6573204f 6e6c792e 20204e6f 20617373 7572616e
6365732e 31323030 06035504 03132956 65726953 69676e20 54726961 6c205365
63757265 20536572 76657220 54657374 20526f6f 74204341 301e170d 30353032
30393030 30303030 5a170d32 35303230 38323335 3935395a 30818c31 0b300906
03550406 13025553 31173015 06035504 0a130e56 65726953 69676e2c 20496e63
2e313030 2e060355 040b1327 466f7220 54657374 20507572 706f7365 73204f6e
6c792e20 204e6f20 61737375 72616e63 65732e31 32303006 03550403 13295665
72695369 676e2054 7269616c 20536563 75726520 53657276 65722054 65737420
526f6f74 20434130 819f300d 06092a86 4886f70d 01010105 0003818d 00308189
02818100 9f21f7c5 3b925699 1f97049f a09210a9 8659506c 4f01c868 c00056a1
aa0949fb 43d0b5d2 c10e2070 739f22f2 7920e332 ce4cd670 bf88003b 2820127f
fc87cf40 1d954fb5 2114a28f 01d317fd 9d612a13 4f13f618 29ad2f51 9ae22efe
cc30e8d3 ce95efe3 62140189 8fe0987b 2e3bb9ee 176b7de8 ff860e03 d3c62fce
e8a857bb 02030100 01300d06 092a8648 86f70d01 01020500 03818100 3aae38ee
b3f9103a 85125def 84b8604d b9f26ac9 0d6303ef c64fb482 b9d0c830 38b05fea
```

```
80af2716 59ef2e60 0e1770e6 7eea96e9 64abe33a 93633a70 98996c9f 8f0e9bfc
968ab2fc 1ae5917e d8add8f3 b14df1d2 07c56647 e3d9c769 36e14816 519ca88c
31b126d8 87777b63 09da8581 38ade0d2 b8dbd716 39c66b87 8ef178e2

quit

telnet timeout 5

ssh 0.0.0.0 0.0.0.0 outside

ssh timeout 60

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  
  
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 rc4-md5  
  
ssl trust-point Test-ASA outside  
  
prompt hostname context  
  
Cryptochecksum:6afb9dec2c5e353e3ec4bd0d6971af0  
  
: end  
  
ASA#
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [Request for Comments \(RFCs\)](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jan 15, 2007

Document ID: 81558
