

# ASA 7.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example

---

## Contents

### [Introduction](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Components Used](#)

#### [Conventions](#)

### [Configure](#)

#### [Step 1. Verify that the Date, Time, and Time Zone Values are Accurate](#)

#### [Step 2. Generate the RSA Key Pair](#)

#### [Step 3. Create the Trustpoint](#)

#### [Step 4. Generate the Certificate Enrollment](#)

#### [Step 5. Authenticate the Trustpoint](#)

#### [Step 6. Install the Certificate](#)

#### [Step 7. Configure WebVPN to Use the Newly Installed Certificate](#)

### [Verify](#)

### [Troubleshoot](#)

### [Related Information](#)

---

## Introduction

This configuration example describes how to manually install a 3rd party vendor digital certificate on the ASA for use with WebVPN. A Verisign Trial Certificate is used in this example. Each step contains the ASDM application procedure and a CLI example.

## Prerequisites

## Requirements

This document requires that you have access to a certificate authority (CA) for certificate enrollment. Supported 3rd party CA vendors are Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign.

## Components Used

This document uses an ASA 5510 that runs software version 7.2(1) and ASDM version 5.2(1). However, the procedures in

this document work on any ASA appliance that runs 7.x with any compatible ASDM version.

## Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

## Configure

In order to install a 3rd party vendor digital certificate on the PIX/ASA, complete these steps:

[Step 1. Verify that the Date, Time, and Time Zone Values are Accurate.](#)

[Step 2. Generate the RSA Key Pair.](#)

[Step 3. Create the Trustpoint.](#)

[Step 4. Generate the Certificate Enrollment.](#)

[Step 5. Authenticate the Trustpoint.](#)

[Step 6. Install the Certificate.](#)

[Step 7. Configure WebVPN to Use the Newly Installed Certificate.](#)

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

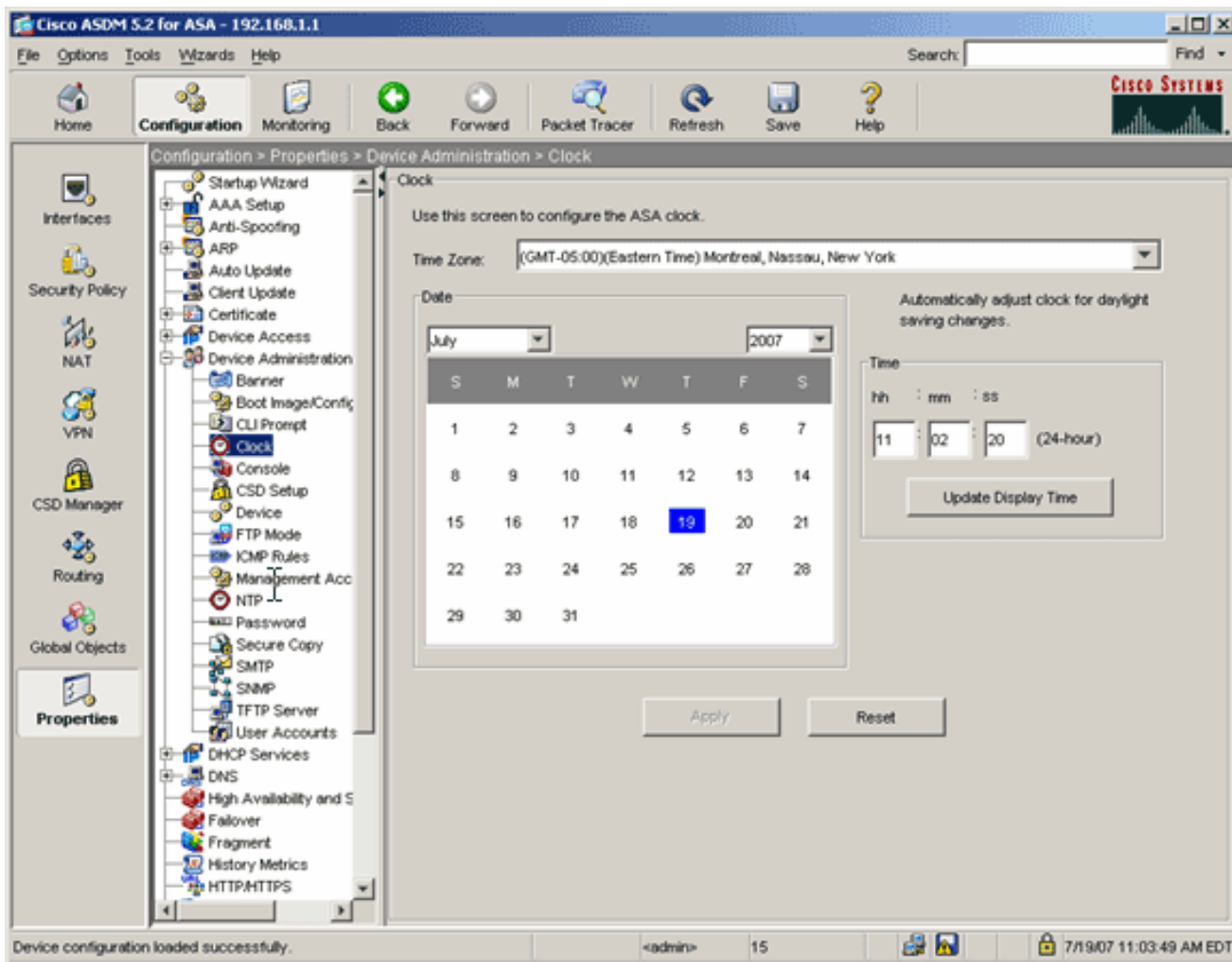
### Step 1. Verify that the Date, Time, and Time Zone Values are Accurate

#### ASDM Procedure

1. Click **Configuration**, and then click **Properties**.
2. Expand **Device Administration**, and choose **Clock**.
3. Verify that the information listed is accurate.

The values for Date, Time, and Time Zone must be accurate in order for proper certificate validation to occur.

[+] Show Image [\[ASDM\]](#)



## Command Line Example

ciscoasa

```
ciscoasa#show clock
```

```
11:02:20.244 UTC Thu Jul 19 2007
```

```
ciscoasa#
```

## Step 2. Generate the RSA Key Pair

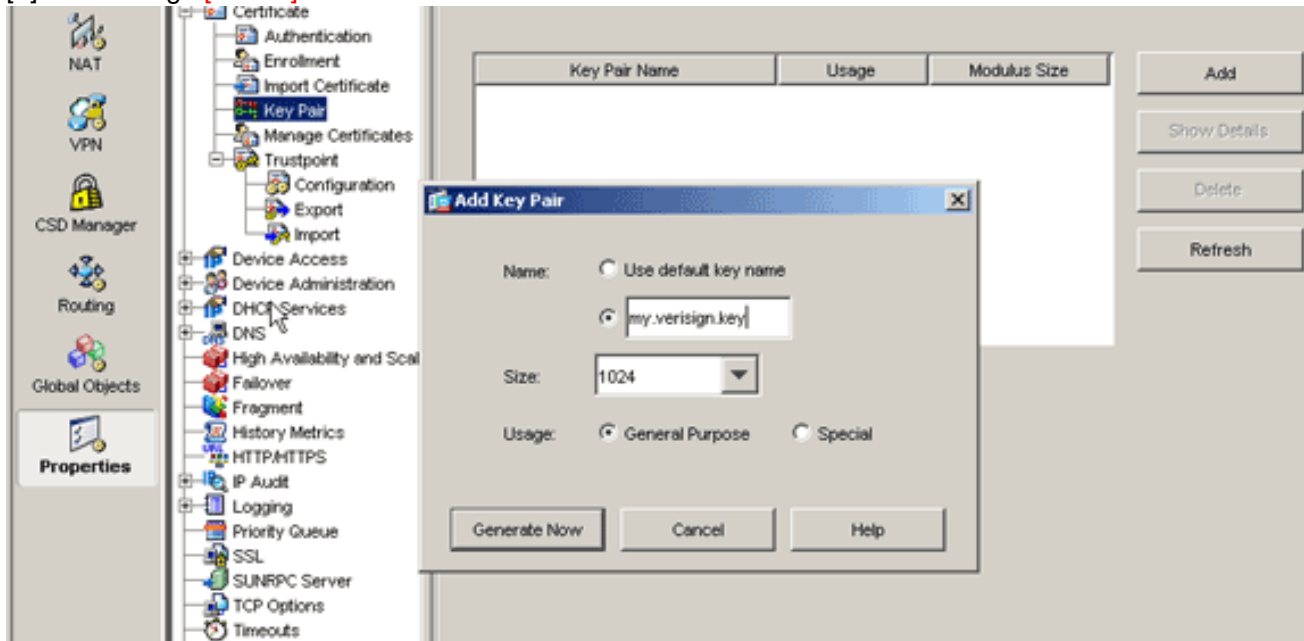
The generated RSA public key is combined with the ASA's identity information to form a PKCS#10 certificate request. You should distinctly identify the key name with the Trustpoint for which you create the key pair.

### ASDM Procedure

1. Click **Configuration**, and then click **Properties**.
2. Expand **Certificate**, and choose **Key Pair**.

3. Click **Add**.

[+] Show Image [ASDM]



4. Enter the key name, choose the modulus size, and select the usage type.

**Note:** The recommended key pair size is 1024.

5. Click **Generate**.

The key pair you created should be listed in the Key Pair Name column.

## Command Line Example

ciscoasa

```
ciscoasa#conf t
```

```
ciscoasa(config)#crypto key generate rsa label my.verisign.key modulus 1024
```

*! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.*

INFO: The name for the keys will be: my.verisign.key

Keypair generation process begin. Please wait...

```
ciscoasa(config)#
```

## Step 3. Create the Trustpoint

Trustpoints are required to declare the Certificate Authority (CA) that your ASA will use.

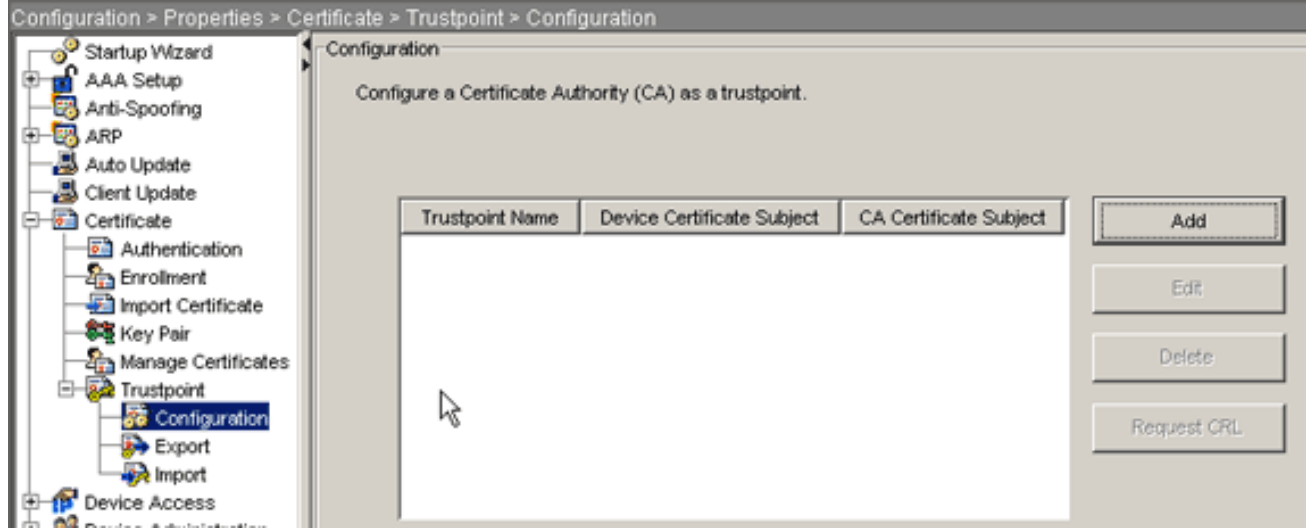
### ASDM Procedure

1. Click **Configuration**, and then click **Properties**.

2. Expand **Certificate**, and then expand **Trustpoint**.

3. Choose **Configuration**, and click **Add**.

[+] Show Image [ASDM]



4. Configure these values:

- **Trustpoint Name:** The trustpoint name should be relevant to the intended usage. (This example uses *my.verisign.trustpoint*.)
- **Key pair:** Select the key pair generated in [Step 2](#). (*my.verisign.key*)

5. Ensure Manual Enrollment is selected.

6. Click **Certificate Parameters**.

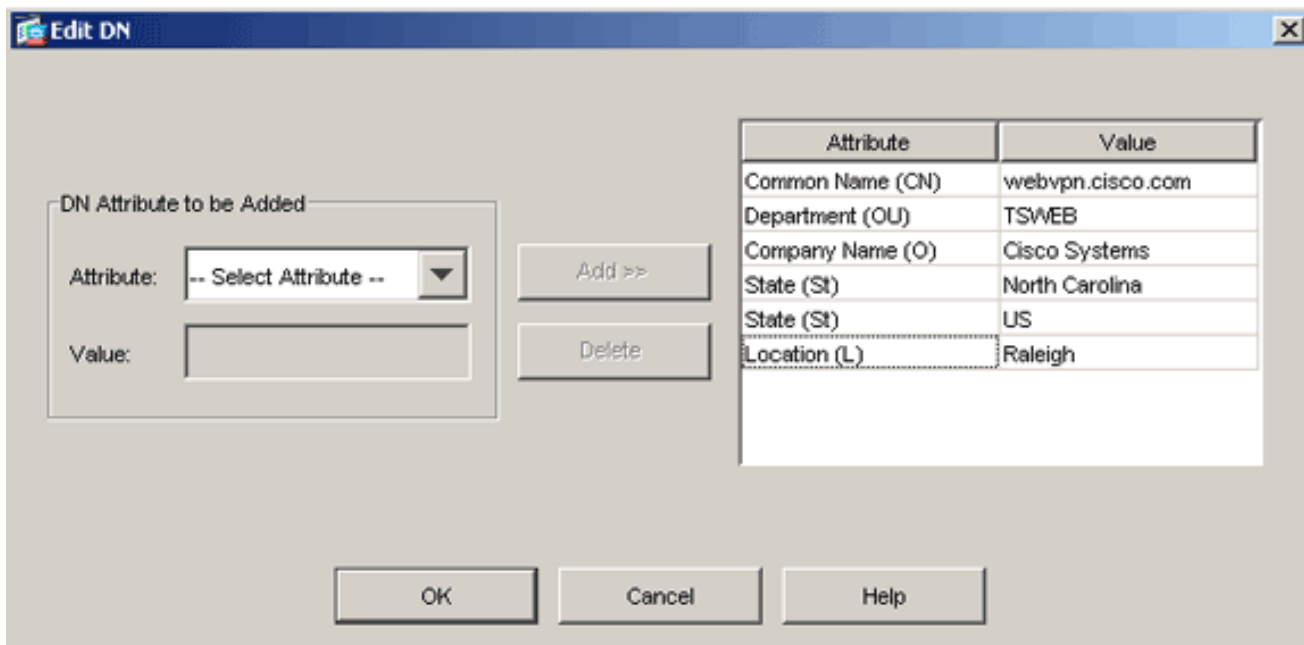
The Certificate Parameters dialog box appears.

7. Click **Edit**, and configure the attributes listed in this table:

Attribute	Description
CN	Fully qualified domain name (FQDN) that will be used for connections to your firewall (for example, webvpn.cisco.com)
OU	Department name
O	Company name (avoid special characters)
C	Country code (2 letter code without punctuation)
St	State (must be spelled out; for example, North Carolina)
L	City

In order to configure these values, choose a value from the Attribute drop-down list, enter the value, and click **Add**.

[+] Show Image [ASDM]

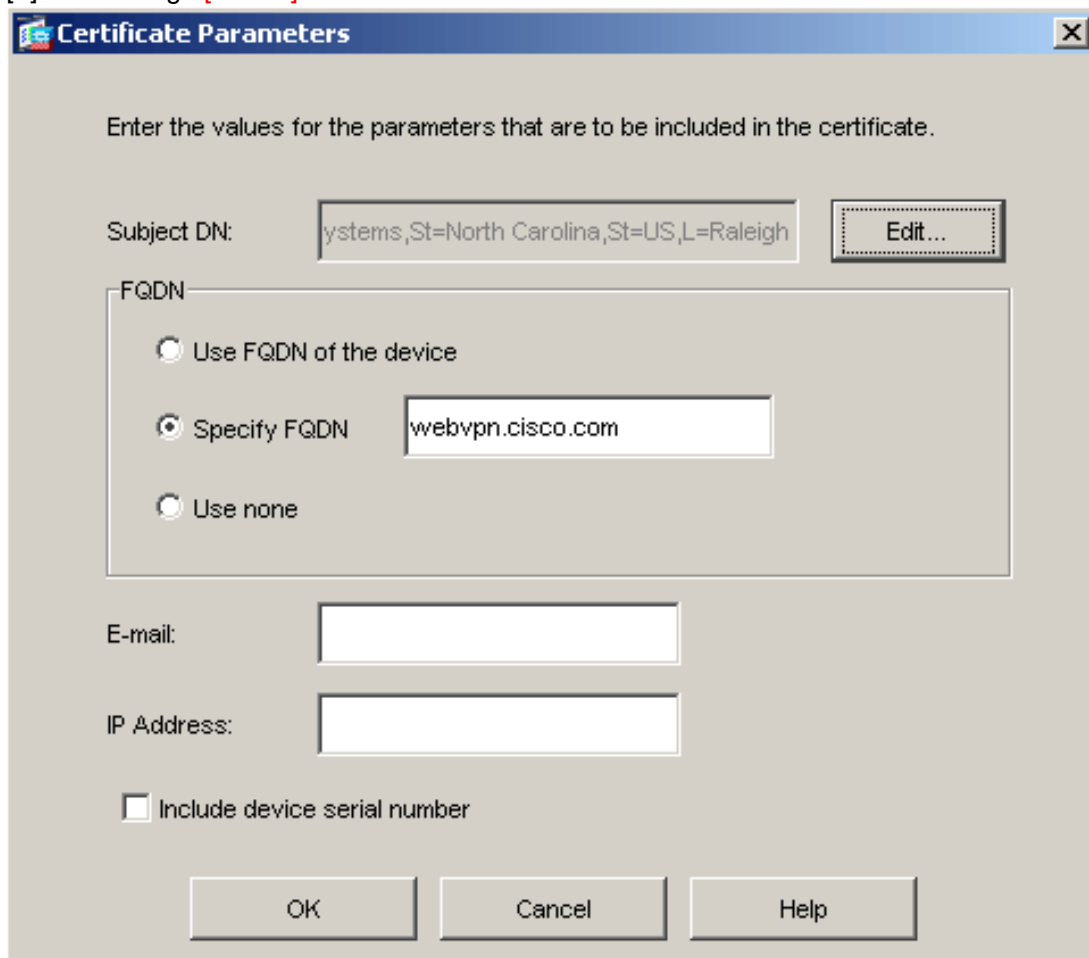


8. Once the appropriate values are added, click **OK**.

9. In the Certificate Parameters dialog box, enter the FQDN in the Specify FQDN field.

This value should be same FQDN you used for the Common Name (CN).

[+] Show Image [\[ASDM\]](#)



10. Click **OK**.

11. Verify the correct key pair is selected, and click the **Use manual enrollment** radio button.

12. Click **OK**, and then click **Apply**.

[+] Show Image [ASDM]

**Add Trustpoint Configuration**

Trustpoint Name:

Generate a self-signed certificate on enrollment  
If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Enrollment Settings | Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

Key Pair:  Show Details New Key Pair...

Challenge Password:  Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.

Enrollment Mode

Use manual enrollment  
 Use automatic enrollment

Enrollment URL:

Retry Period:  minutes

Retry Count:  (Use 0 to indicate unlimited retries)

Certificate Parameters...

OK Cancel Help

## Command Line Example

```
ciscoasa
```

```
ciscoasa(config)#crypto ca trustpoint my.verisign.trustpoint

! Creates the trustpoint.

ciscoasa(config-ca-trustpoint)#enrollment terminal

! Specifies cut and paste enrollment with this trustpoint.

ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,
      O=Cisco Systems,C=US,St=North Carolina,L=Raleigh

! Defines x.500 distinguished name.

ciscoasa(config-ca-trustpoint)#keypair my.verisign.key

! Specifies key pair generated in Step 3.

ciscoasa(config-ca-trustpoint)#fqdn wevpn.cisco.com

! Specifies subject alternative name (DNS:).

ciscoasa(config-ca-trustpoint)#exit
```

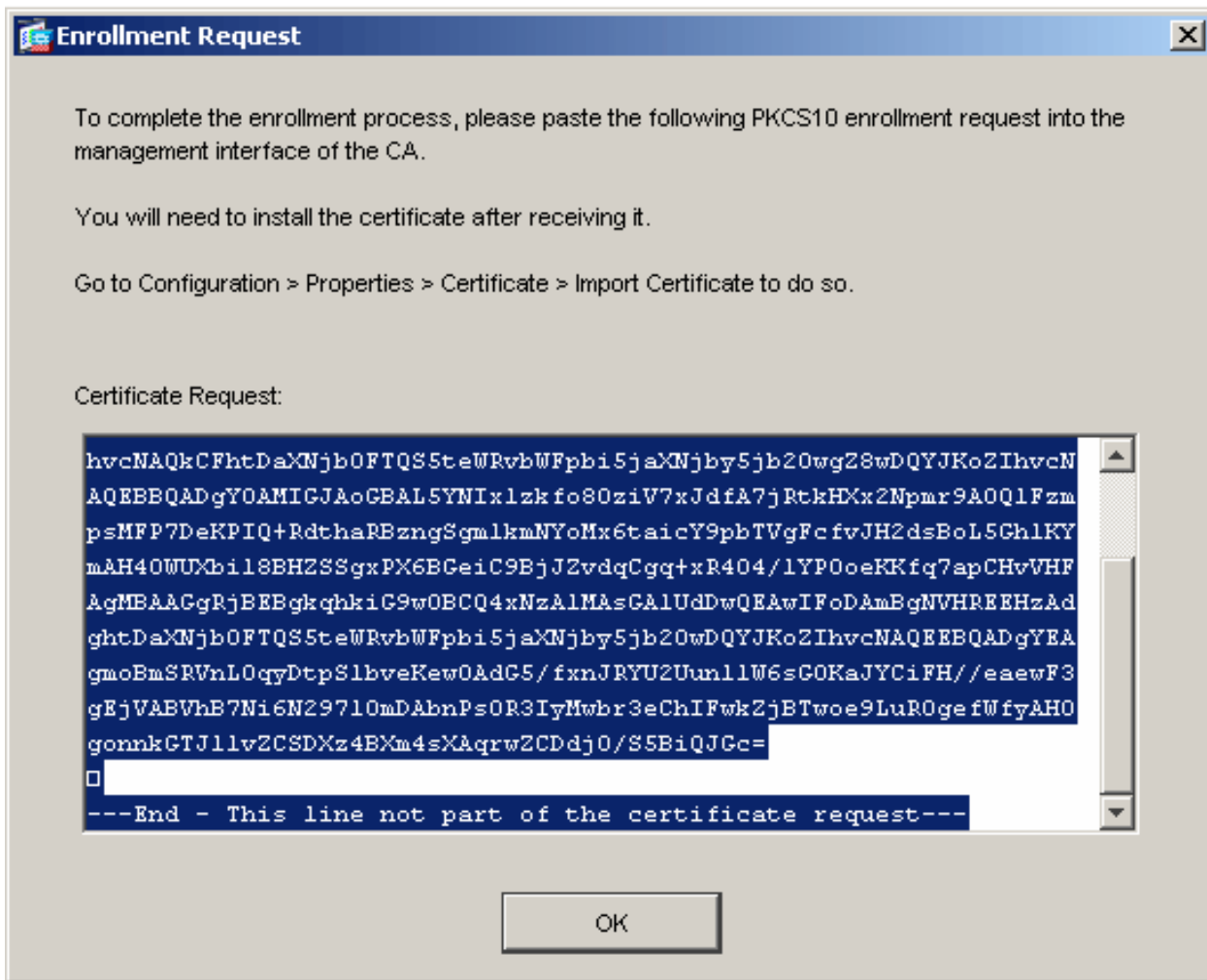
## Step 4. Generate the Certificate Enrollment

### ASDM Procedure

1. Click **Configuration**, and then click **Properties**.
2. Expand **Certificate**, and choose **Enrollment**.
3. Verify the Trustpoint created in [Step 3](#) is selected, and click **Enroll**.

A dialog box appears that lists the certificate enrollment request (also referred to as a certificate signing request).

[+] Show Image [\[ASDM\]](#)



4. Copy the PKCS#10 enrollment request to a text file, and then submit the CSR to the appropriate 3rd party vendor.

After the 3rd party vendor receives the CSR, they should issue an identity certificate for installation.

## Command Line Example

ciscoasa

```
ciscoasa(config)#crypto ca enroll my.verisign.trustpoint
```

```
! Initiates CSR. This is the request to be
! submitted via web or email to the 3rd party vendor.
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will be: CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh
```

```
% The fully-qualified domain name in the certificate will be: webvpn.cisco.com
```

```
% Include the device serial number in the subject name? [yes/no]: no
```

```
! Do not include the device's serial number in the subject.
```

Display Certificate Request to terminal? [yes/no]: **yes**

*! Displays the PKCS#10 enrollment request to the terminal.  
! You will need to copy this from the terminal to a text  
! file or web text field to submit to the 3rd party CA.*

Certificate Request follows:

```
MIICHjCCAYcCAQAwgaAxEDAObgNVBAcTB1JhbGVpZ2gxZzAVBgNVBAgTDk5vcnRo
IENhcm9saW5hMQswCQYDVOQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31zdGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNvbTEhMB8G
CSqGSIB3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIB3DQEBAQUA
A4GNADCBIQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB9M4yTx5b
Fm886s8F73WsfQPynBdfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt3oMXSNPO
mldZ0xJVnRip9cyQp/983pm5PfDD6/ho0nTktxi+1cEX0luBMh7oKargwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBywFIIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIB3DQEBBAUAA4GBABrxpY0q7SeOHZf3yEJq
po6wG+oZpsvpYI/HemKULaRc783w4BMO5lulIEHgRqAxrTbQn0B7JPIbkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/Uo13yWce
0Bzg59cYXq/vkoqZV/tBuACr
```

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

Redisplay enrollment request? [yes/no]: **no**

ciscoasa(config)#

## Step 5. Authenticate the Trustpoint

Once you receive the identity certificate from the 3rd party vendor, you can proceed with this step.

### ASDM Procedure

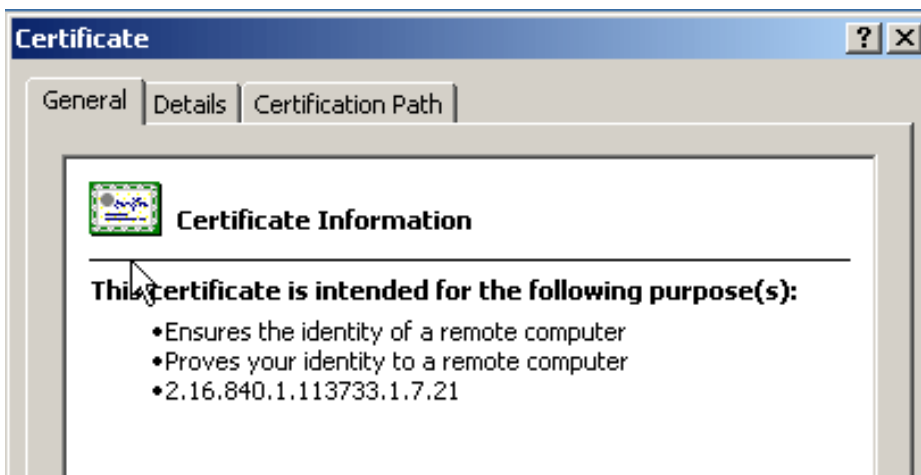
1. Save the identity certificate to your local computer.
2. If you were provided a base64-encoded certificate that did not come as a file, you must copy the base64 message, and paste it into a text file.
3. Rename the file with a .cer extension.

**Note:** Once the file is renamed with the .cer extension, the file icon should display as a certificate.

4. Double-click the certificate file.

The Certificate dialog box appears.

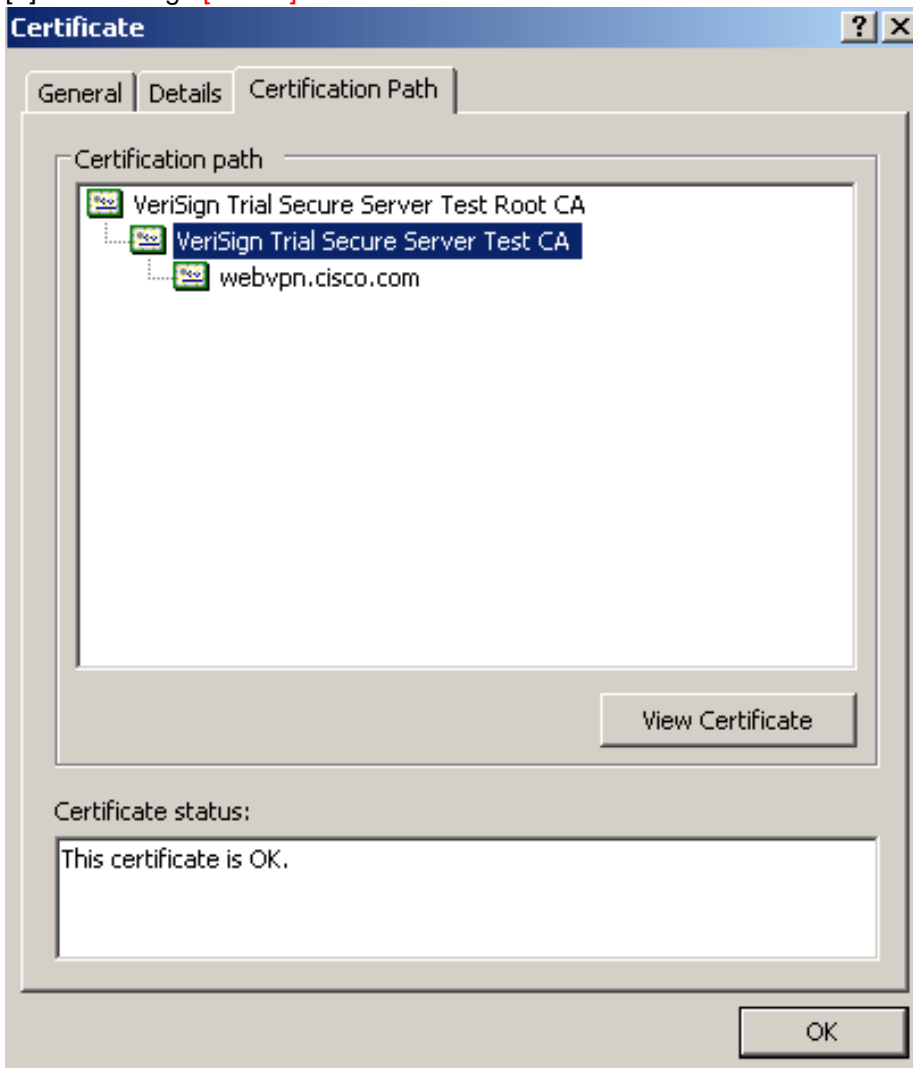
[+] Show Image **[ASDM]**



**Note:** If the "Windows does not have enough information to verify this certificate" message appears in the General tab, you must obtain the 3rd party vendor root CA or intermediate CA certificate before you continue with this procedure. Contact your 3rd party vendor or CA administrator in order to obtain the issuing root CA or intermediate CA certificate.

5. Click the **Certificate Path** tab.
6. Click the CA certificate located above your issued identity certificate, and click **View Certificate**.

[+] Show Image [ASDM]



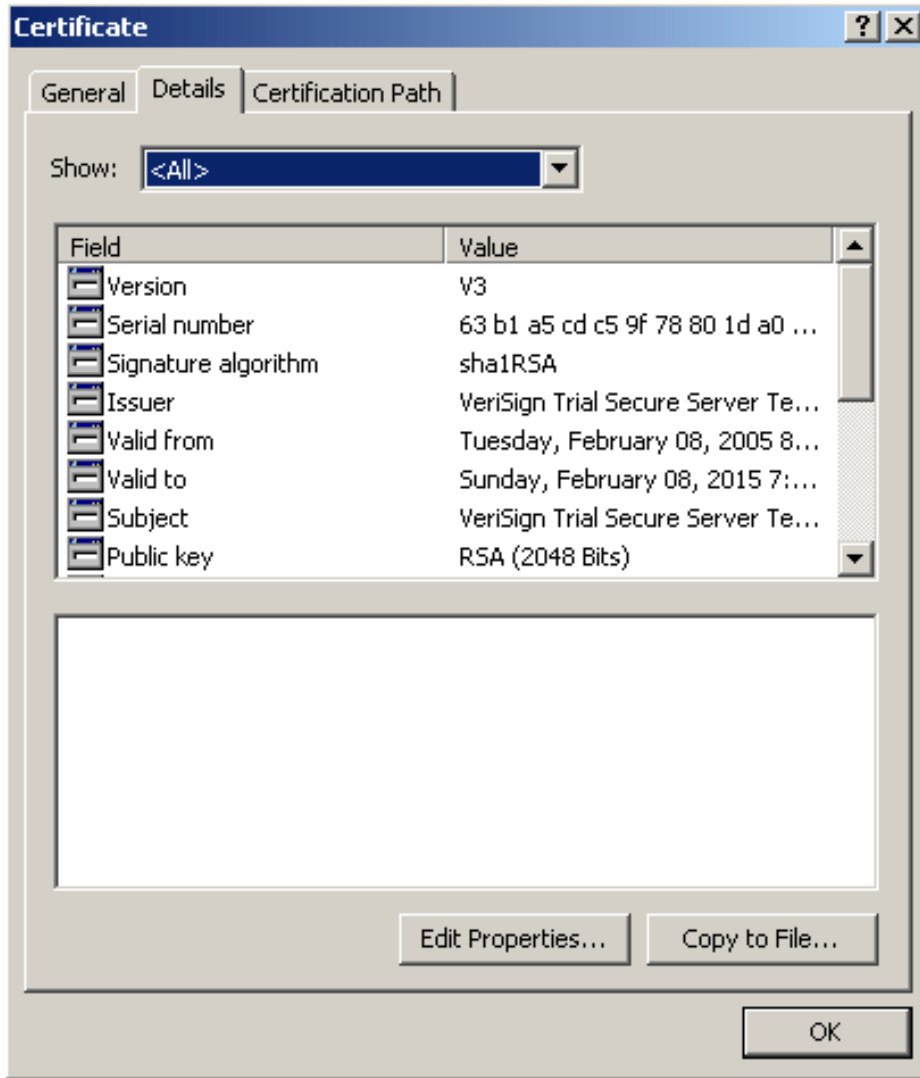
Detailed information about the intermediate CA certificate appears.



**Warning:** Do not install the identity (device) certificate in this step. Only the root, subordinate root, or CA certificate are added in this step. The identity (device) certificates are installed in [Step 6](#).

7. Click **Details**.

[+] Show Image [\[ASDM\]](#)

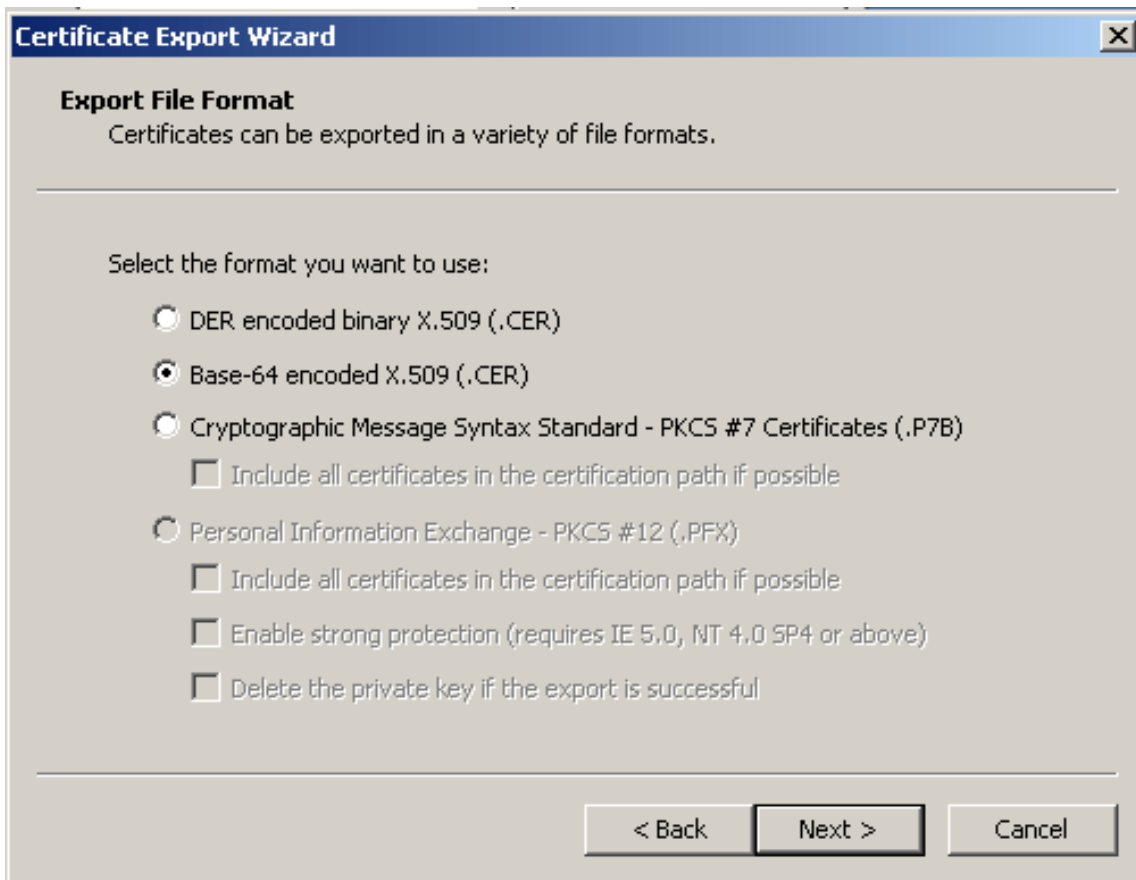


8. Click **Copy to File**.

9. Within the Certificate Export Wizard, click **Next**.

10. In the Export File Format dialog box, click the **Base-64 encoded X.509 (.CER)** radio button, and click **Next**.

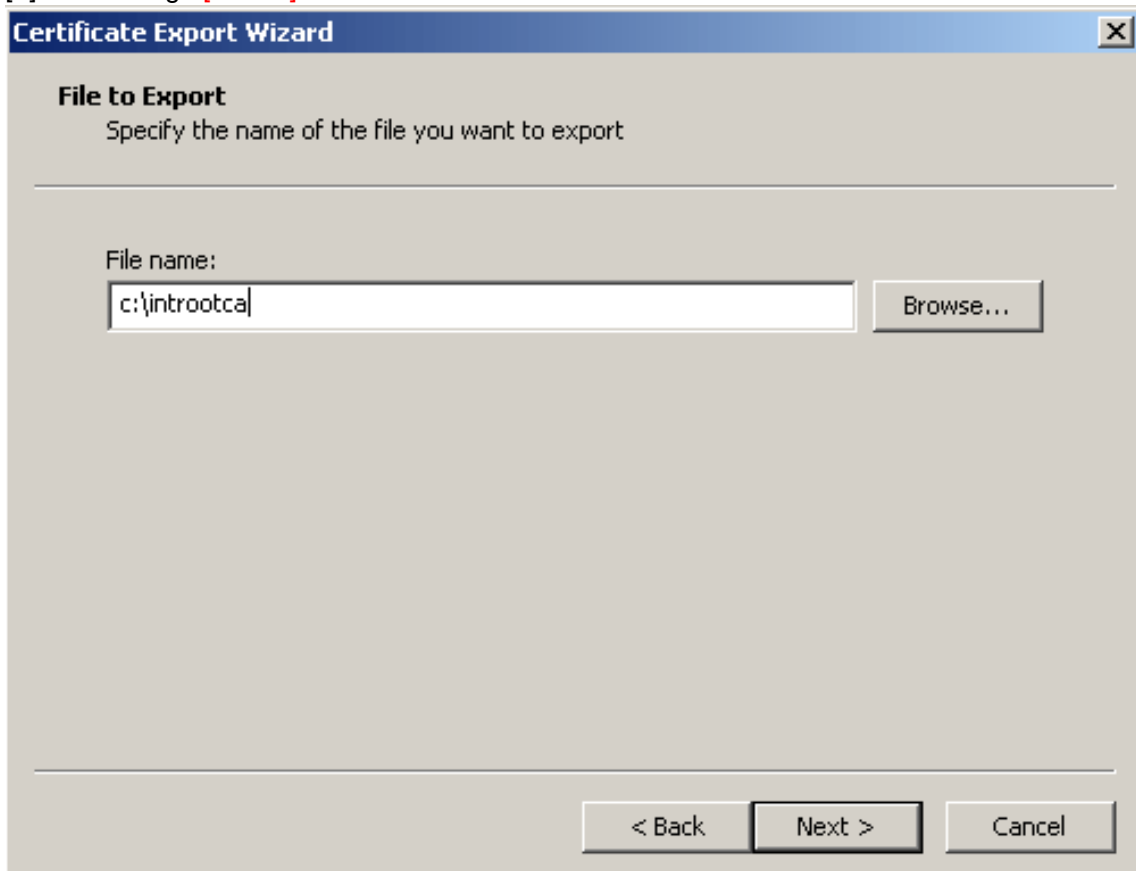
[+] Show Image [\[ASDM\]](#)



11. Enter the file name and location to which you want to save the CA certificate.

12. Click **Next**, and then click **Finish**.

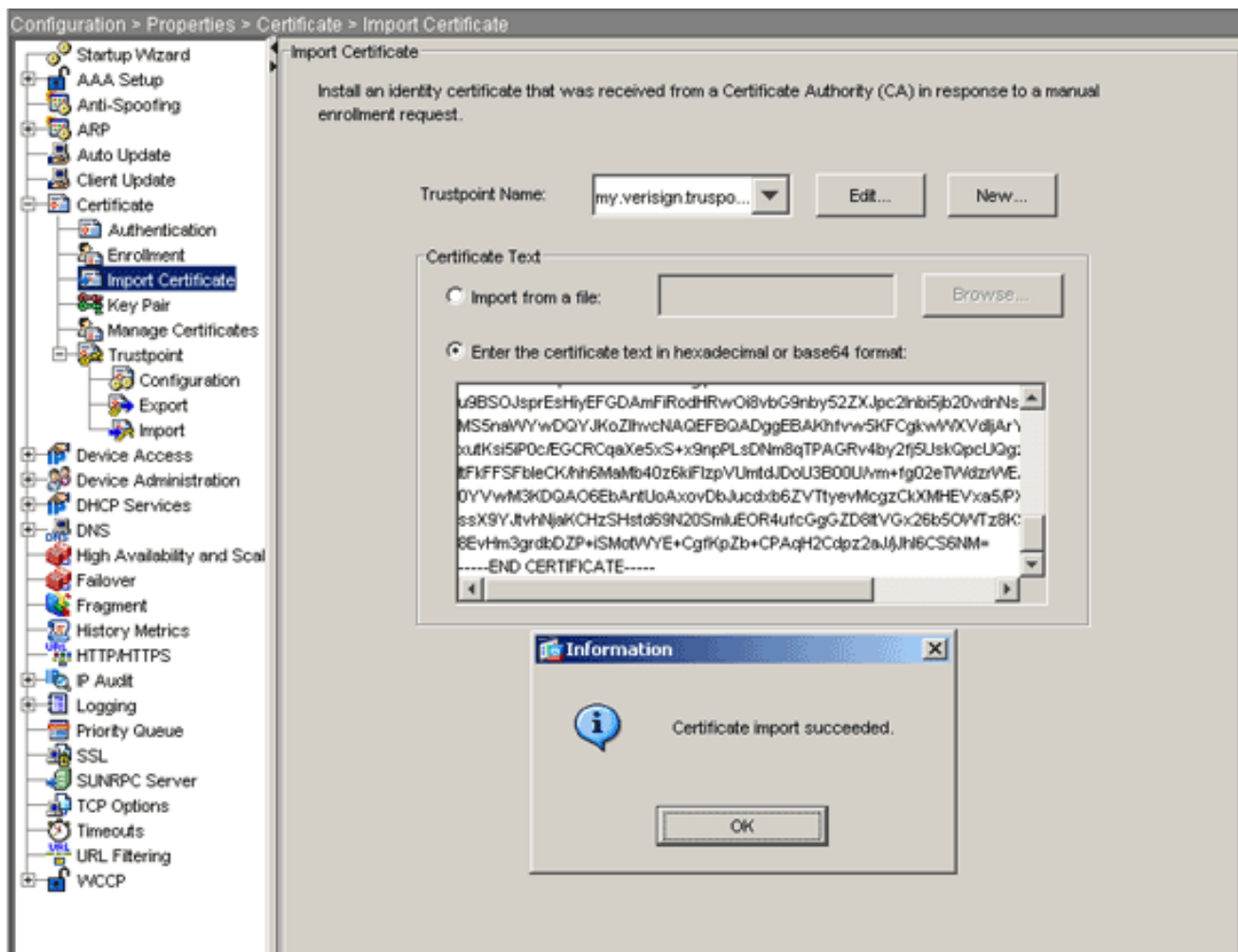
[+] Show Image [\[ASDM\]](#)











4. Click **Import**, and then click **OK**.

## Command Line Example

ciscoasa

```
ciscoasa(config)#crypto ca import my.verisign.trustpoint certificate
```

*! Initiates prompt to paste the base64 identity certificate provided by the 3rd party vendor.*

% The fully-qualified domain name in the certificate will be: webvpn.cisco.com

Enter the base 64 encoded certificate.

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

```
-----BEGIN CERTIFICATE-----
```

```
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjftANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxZAVBbnVBAoTDlZlcm1TaWduLCBjb20vY3Bz
EydGb3IgdGVzZCBQdXJwb3NlcyBpbm5LiAgTm8gYXNzdXJhbmNlcy4xQjBAbG9y
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwcovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
```

```
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4GA1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ21zY28gU3lzdGVtczEOMAwGA1UECmEwFVFNXRUIx
Oja4BgNVBASUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNpZ24uY29tL2Nwcy90ZjB20wgZ8wDQYJ
KoZiHvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxs1EgryosBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjaAMAsGA1UdDwQEAwIFoDBDBGNV
HR8EPDA6MDigNqA0hjJodHRWoi8vU1ZSU2VjdXJlLWNYbc52ZXJpc2lnbi5jb20v
U1ZSVHJpYWwyMDA1LmNybdBKBGNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYD
VR0lBBYwFAyIKWYBBQUHAWEGCCsGAQUFBwMCMCB8GA1UdIwQYMBaAFGYi joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwa jAkBggrBgEFBQcwAYYYaHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzACHjZodHRWoi8vU1ZSU2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYIKWYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGGQUS2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9n
bzEuZ2lmMA0GCSqGSIB3DQEBBQUAA4IBAQAAnym4GVThPIyL/9ylDBd8N7/yw3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q86ZiKyMIj
XM2VCmcHSa jmMMRy jpydxfk6CIdDMtMGotCavRHD9Tl2twvgrBock/v/54o02lkB
SmLzVV7crlyJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89Fsewy8MAIY
rtab5F+oiTc5xGy8w7NARafNgFXihqnLgWTtA35/oWuy86bje1IWbeyqj8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju50
-----END CERTIFICATE-----
quit
```

```
INFO: Certificate successfully imported
ciscoasa(config)#
```

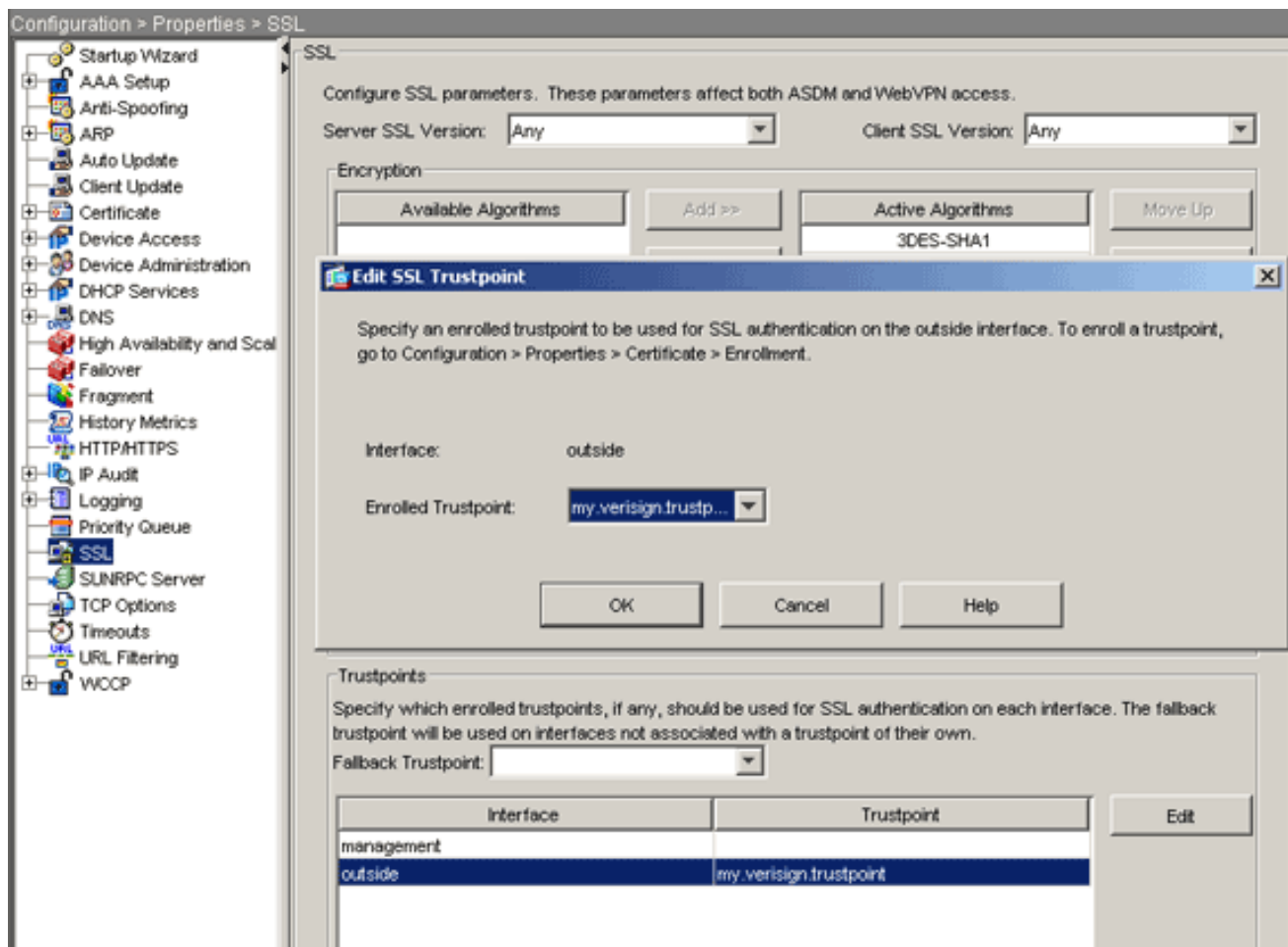
## Step 7. Configure WebVPN to Use the Newly Installed Certificate

### ASDM Procedure

1. Click **Configuration**, click **Properties**, and then choose **SSL**.
2. In the Trustpoints area, select the interface that will be used to terminate WebVPN sessions. (This example uses the outside interface.)
3. Click **Edit**.

The Edit SSL Trustpoint dialog box appears.

[+] Show Image [\[ASDM\]](#)



4. From the Enrolled Trustpoint drop-down list, choose the trustpoint you created in [Step 3](#).
5. Click **OK**, and then click **Apply**.

Your new certificate should now be utilized for all WebVPN sessions that terminate on the interface specified. See the [Verify](#) section in this document for information on how to verify a successful installation.

## Command Line Example

```

ciscoasa
-----
ciscoasa(config)#ssl trust-point my.verisign.trustpoint outside

! Specifies the trustpoint that will supply the SSL
! certificate for the defined interface.

ciscoasa(config)#write memory

Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08

8808 bytes copied in 3.630 secs (2936 bytes/sec)
[OK]
ciscoasa(config)#

! Save configuration.

```

# Verify

This section describes how to confirm that the installation of your 3rd party vendor certificate was successful.

## Replace Self-Signed Certificate from ASA

This section describes how to replace the installed self-signed certificate from the ASA.

1. Issue a certificate signing request to Verisign.

After you receive the requested certificate from Verisign, you can install it directly under the same trustpoint.

2. Type this command: **crypto ca enroll Verisign**

You are prompted to answer questions.

3. For *Display Certificate Request to terminal*, enter **yes**, and send the output to Verisign.

4. Once they give you the new certificate, type this command: **crypto ca import Verisign certificate**

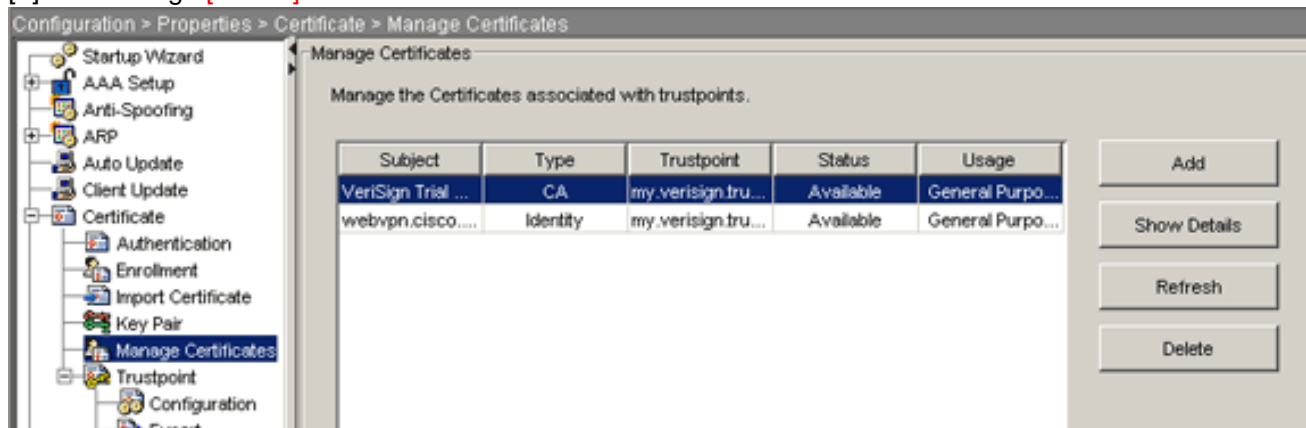
## View Installed Certificates

### ASDM Procedure

1. Click **Configuration**, and click **Properties**.
2. Expand **Certificate**, and choose **Manage Certificates**.

The CA certificate used for Trustpoint authentication and the identity certificate that was issued by the 3rd party vendor should appear in the Manage Certificates area.

[+] Show Image [ASDM]



### Command Line Example

```
ciscoasa(config)#show crypto ca certificates
```

*! Displays all certificates installed on the ASA.*

#### Certificate

Status: Available

Certificate Serial Number: 32cfe85eebbd2b5e1e30649fd266237d

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=webvpn.cisco.com

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

ou=TSWEB

o=Cisco Systems

l=Raleigh

st=North Carolina

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 Jul 19 2007

end date: 23:59:59 UTC Aug 2 2007

Associated Trustpoints: my.verisign.trustpoint

*! Identity certificate received from 3rd party vendor displayed above.*

#### 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

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: my.verisign.trustpoint
```

*! CA intermediate certificate displayed above.*

## Verify Installed Certificate for WebVPN with a Web Browser

In order to verify that WebVPN uses the new certificate, complete these steps:

1. Connect to your WebVPN interface through a web browser. Use https:// along with the FQDN you used to request the certificate (for example, https://webvpn.cisco.com).

If you receive one of these security alerts, perform the procedure that corresponds to that alert:

- o **The Name of the Security Certificate Is Invalid or Does Not Match the Name of the Site**

Verify that you used the correct FQDN/CN in order to connect to the WebVPN interface of the ASA. You must use the FQDN/CN that you defined when you requested the identity certificate. You can use the **show crypto ca certificates *trustpointname*** command in order to verify the certificates FQDN/CN.

- o **The security certificate was issued by a company you have not chosen to trust...**

Complete these steps in order to install the 3rd party vendor root certificate to your web browser:

1. In the Security Alert dialog box, click **View Certificate**.
2. In the Certificate dialog box, click the **Certificate Path** tab.
3. Select the CA certificate located above your issued identity certificate, and click **View Certificate**.
4. Click **Install Certificate**.
5. In the Certificate Install Wizard dialogue box, click **Next**.
6. Select the **Automatically select the certificate store based on the type of certificate** radio button, click **Next**, and then click **Finish**.
7. Click **Yes** when you receive the Install the certificate confirmation prompt.
8. At the *Import operation was successful* prompt, click **OK**, and then click **Yes**.

**NOTE:** Since this example uses the Verisign Trial Certificate the Verisign Trial CA Root Certificate must be installed in order to avoid verification errors when users connect.

2. Double-click the lock icon that appears in the lower-right corner of the WebVPN login page.

The installed certificate information should appear.

3. Review the contents to verify that it matches your 3rd party vendors certificate.

[+] Show Image [\[ASDM\]](#)



## Steps To Renew the SSL Certificate

Complete these steps in order to renew the SSL certificate:

1. Select the trust-point you need to renew.
2. Choose **enroll**.

This message appears:

*If it is successfully enrolled again, the current cert will be replaced with the new ones. Do you want to continue?*

3. Choose **yes**.

This will generate a new CSR.

4. Send the CSR to your CA and then import the new ID cert when you get it back.

5. Remove and reapply the trust-point to the outside interface.

## Commands

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

- **show crypto ca trustpoint** — Displays configured trustpoints.
- **show crypto ca certificate** — Displays all the certificates installed on the system.
- **show crypto ca crls** — Displays cached certificate revocation lists (CRL).
- **show crypto key mypubkey rsa** — Displays all generated crypto key pairs.

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

## Troubleshoot

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

Here are some possible errors that you might encounter:

- **% Warning: CA cert is not found. The imported certs might not be usable.INFO: Certificate successfully imported**

CA certificate was not authenticated correctly. Use the **show crypto ca certificate *trustpointname*** command in order to verify that the CA certificate was installed. Look for the line that begins with **CA Certificate**. If the CA certificate is installed, verify that it references the correct trustpoint.

ciscoasa

```
ciscoasa#show crypto ca certificate my.verisign.trustpoint | b CA Certificate
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
  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: 19:00:00 EST Feb 8 2005
  end   date: 18:59:59 EST Feb 8 2015
Associated Trustpoints: my.verisign.trustpoint
ciscoasa#
```

- **ERROR: Failed to parse or verify imported certificate**

This error can occur when you install the identity certificate and do not have the correct intermediate or root CA certificate authenticated with the associated trustpoint. You must remove and reauthenticate with the correct intermediate or root CA certificate. Contact your 3rd party vendor in order to verify that you received the correct CA certificate.

- **Certificate does not contain general purpose public key**

This error can occur when you attempt to install your identity certificate to the wrong Trustpoint. You attempt to install an invalid identity certificate, or the key pair associated with the Trustpoint does not match the public key contained in the identity certificate. Use the **show crypto ca certificates *trustpointname*** command in order to verify you installed your identity certificate to the correct trustpoint. Look for the line stating **Associated Trustpoints:** If the wrong trustpoint is listed, use the procedures described in this document in order to remove and reinstall to the appropriate trustpoint, also Verify the keypair has not change since the CSR was generated.

- **Error Message: %PIX|ASA-3-717023 SSL failed to set device certificate for trustpoint [trustpoint name]**

This message displays when a failure occurs when you set a device certificate for the given trustpoint in order to authenticate the SSL connection. When the SSL connection comes up, an attempt is made to set the device certificate that will be used. If a failure occurs, an error message is logged that includes the configured trustpoint that should be used to load the device certificate and the reason for the failure.

*trustpoint name*—Name of the trustpoint for which SSL failed to set a device certificate.

**Recommended Action:** Resolve the issue indicated by the reason reported for the failure.

1. Ensure that the specified trustpoint is enrolled and has a device certificate.
2. Make sure the device certificate is valid.
3. Reenroll the trustpoint, if required.

---

## Related Information

- [How to obtain a Digital Certificate from a Microsoft Windows CA using ASDM on an ASA](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation - Cisco Systems](#)

---

<a href="#">Home</a>
----------------------

<a href="#">How to Buy</a>
----------------------------

<a href="#">Login</a>
-----------------------

<a href="#">Profile</a>
-------------------------

<a href="#">Feedback</a>
--------------------------

<a href="#">Site Map</a>
--------------------------

<a href="#">Help</a>
----------------------

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).