

ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example

Document ID: 98596

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Step 1. Verify that the Date, Time, and Time Zone Values are Accurate
- Step 2. Generate a Certificate Signing Request
- Step 3. Authenticate the Trustpoint
- Step 4. Install the Certificate
- Step 5. Configure WebVPN to Use the Newly Installed Certificate

Verify

- View Installed Certificates
- Verify Installed Certificate for WebVPN with a Web Browser
- Commands

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. Examples of 3rd party CA vendors include, but are not limited to, Baltimore, Cisco, Entrust, Geotrust, Godaddy, iPlanet/Netscape, Microsoft, RSA, Thawte, and VeriSign.

Components Used

This document uses an ASA 5510 that runs software version 8.0(2) and ASDM version 6.0(2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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 ASA, complete these steps:

1. Verify that the Date, Time, and Time Zone Values are Accurate
2. Generate a Certificate Signing Request
3. Authenticate the Trustpoint
4. Install the Certificate
5. Configure WebVPN to Use the Newly Installed Certificate

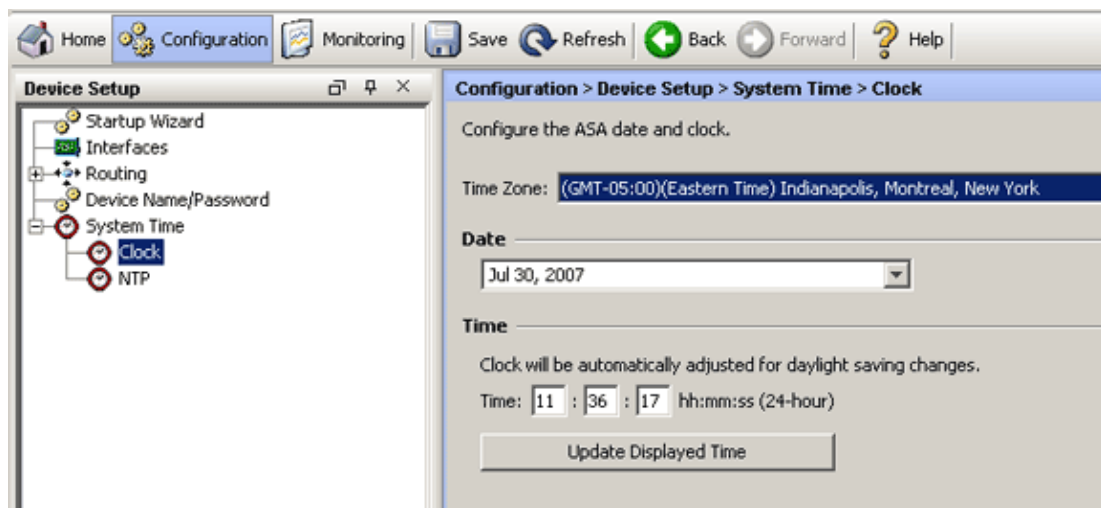
Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

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

ASDM Procedure

1. Click **Configuration**, and then click **Device Setup**.
2. Expand **System Time**, 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.



Command Line Example

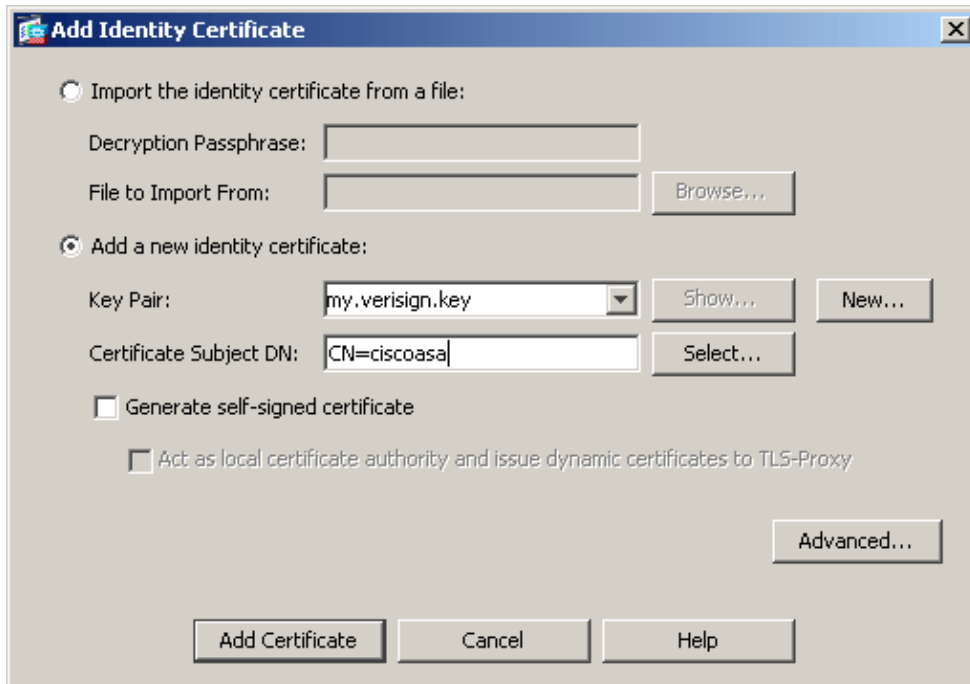
```
ciscoasa
ciscoasa#show clock
11:02:20.244 UTC Thu Jul 19 2007
ciscoasa#
```

Step 2. Generate a Certificate Signing Request

A certificate signing request (CSR) is required in order for the 3rd party CA to issue an identity certificate. The CSR contains your ASA's distinguished name (DN) string along with the ASA's generated public key. The ASA uses the generated private key to digitally sign the CSR.

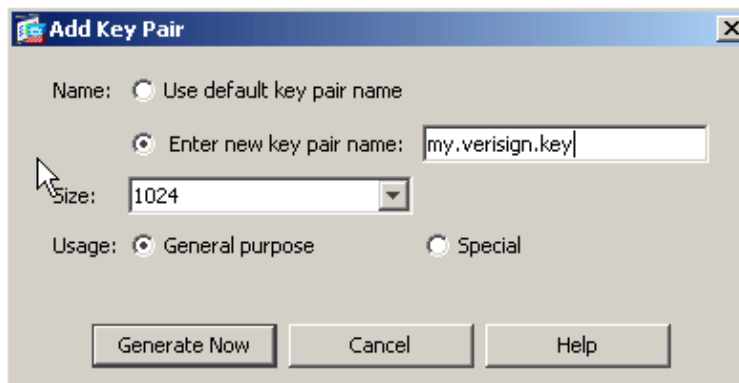
ASDM Procedure

1. Click **Configuration**, and then click **Device Management**.
2. Expand **Certificate Management**, and choose **Identity Certificates**.
3. Click **Add**.



The screenshot shows the "Add Identity Certificate" dialog box. It has two radio buttons: "Import the identity certificate from a file:" (unselected) and "Add a new identity certificate:" (selected). Under the first option, there are fields for "Decryption Passphrase:" and "File to Import From:" with a "Browse..." button. Under the second option, there is a "Key Pair:" dropdown menu showing "my.verisign.key", a "Show..." button, and a "New..." button. Below that is a "Certificate Subject DN:" field containing "CN=ciscoasa" and a "Select..." button. There are two checkboxes: "Generate self-signed certificate" (unchecked) and "Act as local certificate authority and issue dynamic certificates to TLS-Proxy" (unchecked). An "Advanced..." button is at the bottom right. At the very bottom are "Add Certificate", "Cancel", and "Help" buttons.

4. Click the **Add a new identity certificate** radio button.
5. For the Key Pair, click **New**.



The screenshot shows the "Add Key Pair" dialog box. It has two radio buttons for "Name": "Use default key pair name" (unselected) and "Enter new key pair name:" (selected). The "Enter new key pair name:" field contains "my.verisign.key". There is a "Size:" dropdown menu set to "1024". There are two radio buttons for "Usage": "General purpose" (selected) and "Special" (unselected). At the bottom are "Generate Now", "Cancel", and "Help" buttons.

Note: If you use a 2048 bit certificate, generate a 2048 bit key as well.

6. Click the **Enter new key pair name** radio button. You should distinctly identify the key pair name for recognition purposes.
7. Click **Generate Now**.

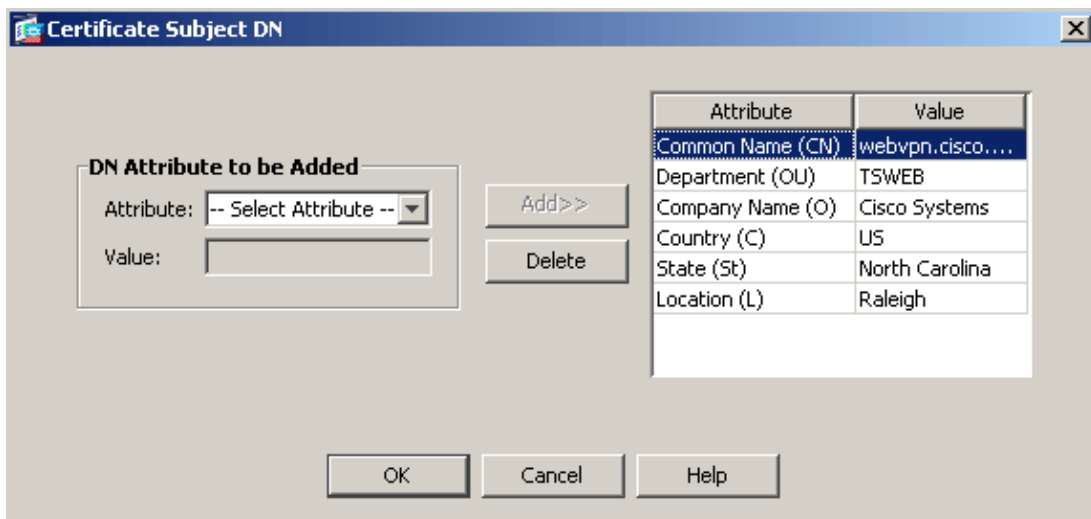
The key pair should now be created.

8. To define the Certificate Subject DN, click **Select**, and configure the attributes listed in this table:

Table 4.1: DN Attributes

Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. 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**.

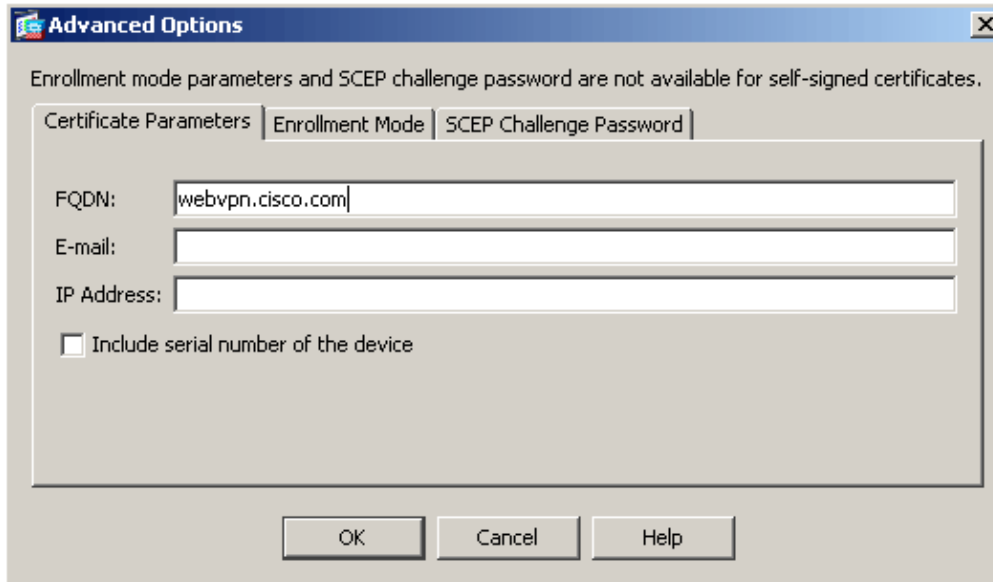


Note: Some 3rd party vendors require particular attributes to be included before an identity certificate is issued. If you are unsure of the required attributes, check with your vendor for details.

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

The Add Identity Certificate dialog box appears with the Certificate Subject DN field populated.

10. Click **Advanced**.

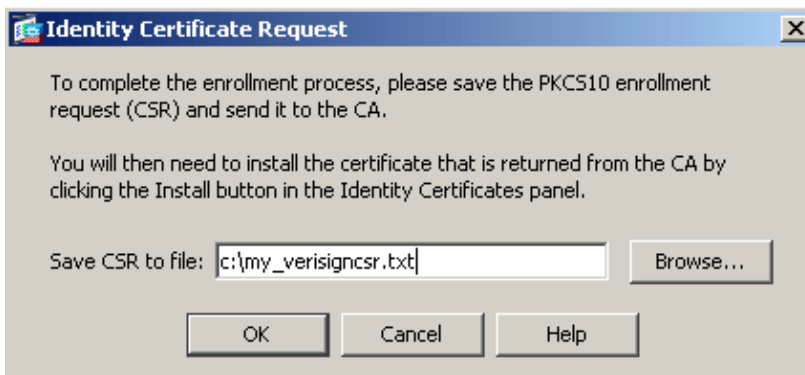


11. In the FQDN field, enter the FQDN that will be used to access the device from the internet.

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

12. Click **OK**, and then click **Add Certificate**.

You are prompted to save the CSR to a file on your local machine.



13. Click **Browse**, choose a location in which to save the CSR, and save the file with the .txt extension.

Note: When you save the file with a .txt extension, you can open the file with a text editor (such as Notepad) and view the PKCS#10 request.

14. Submit the saved CSR to your 3rd party vendor. Once you submit the CSR to your 3rd party vendor, they will provide you the identity certificate to be installed on the ASA.

Command Line Example

In ASDM 6.x, the trustpoint is automatically created when a CSR is generated or when the CA certificate is installed. In the CLI, the trustpoint must be created manually.

```

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

```
! Defines x.500 distinguished name. Use the attributes
! defined in table 4.1 in Step 2 as a guide.
```

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

```
! Specifies key pair generated in Step 3.
```

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

```
! Specifies the FQDN (DNS:) to be used as the subject
! alternative name.
```

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

```
! Specifies manual enrollment.
```

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

```
! Initiates certificate signing request. 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:
```

```
MIICHjCCAYcCAQAwgaAxEDA0BgNVBACTB1JhbGVpZ2gxZmZAVBgNVBAGTDk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEWJVUzEWMBQGA1UEChMNQ2l5Y28gU31zdGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNlLnNpc2NvLmNvbTEhMB8G
```

```
CSqGSIB3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIB3DQEBAQUA
A4GNADCBiQKBgQcmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB9M4yTx5b
Fm886s8F73WsfQPynBDFBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt3oMXSNPO
mldZ0xJVnrIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKargwIDAQAB
oD0wOwYJKoZIHvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBywFIIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIB3DQEBBAUAA4GBABrXPY0q7SeOHZf3yEJq
po6wG+oZpsvpYI/HemKUlARc783w4BMO51ulIEnHgRqAxrTbQn0B7JPibkc2ykkm
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)#
```

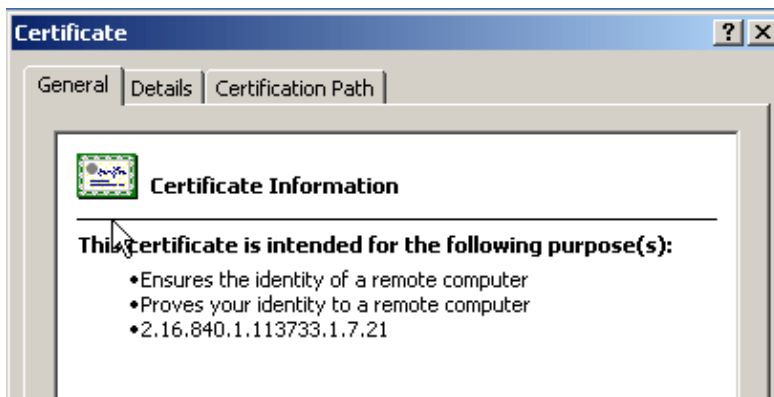
Step 3. Authenticate the Trustpoint

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

ASDM Procedure

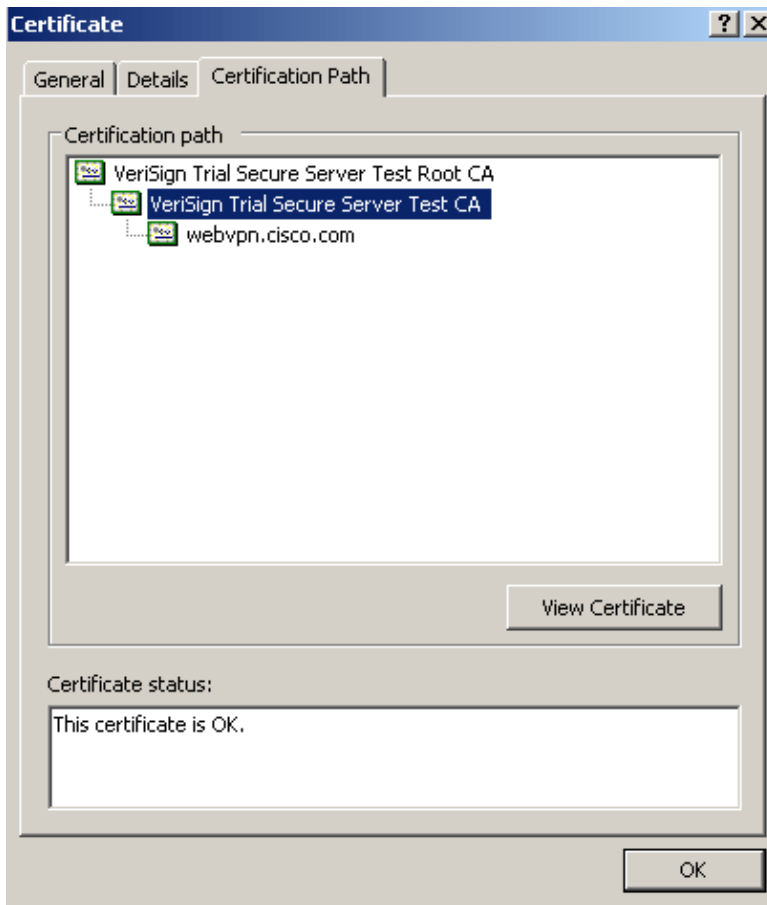
1. Save the identity certificate to your local computer.
2. If your were provided a base64–encoded certificate that did not come as a file, you must copy the base64 message, and paste it into a text file.
3. Rename the file with a .cer extension. Note: Once the file is renamed with the .cer extension, the file icon should display as a certificate.
4. Double–click the certificate file.

The Certificate dialog box appears.



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.

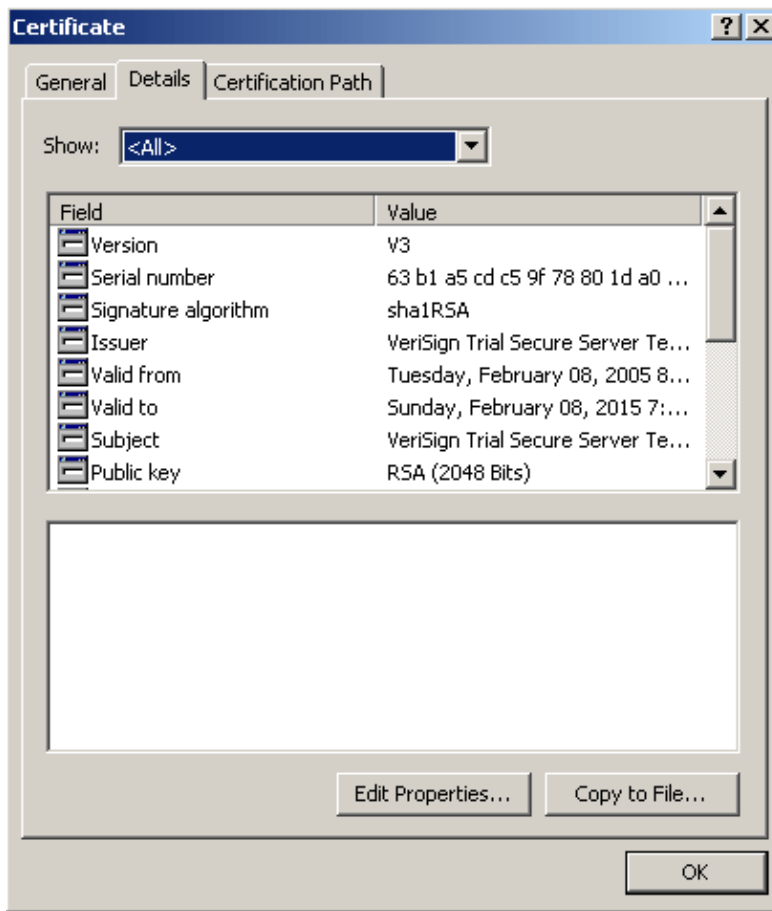
5. Click the **Certificate Path** tab.
6. Click the CA certificate located above your issued identity certificate, and click **View Certificate**.



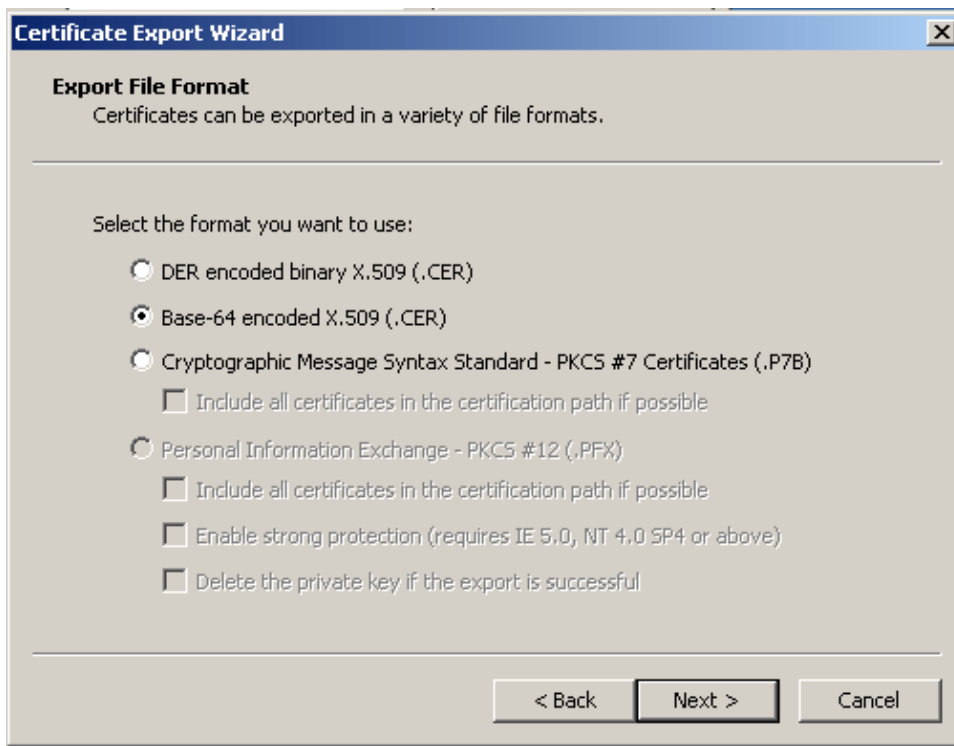
Detailed information about the intermediate CA certificate appears.



- 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 4.
7. Click **Details**.

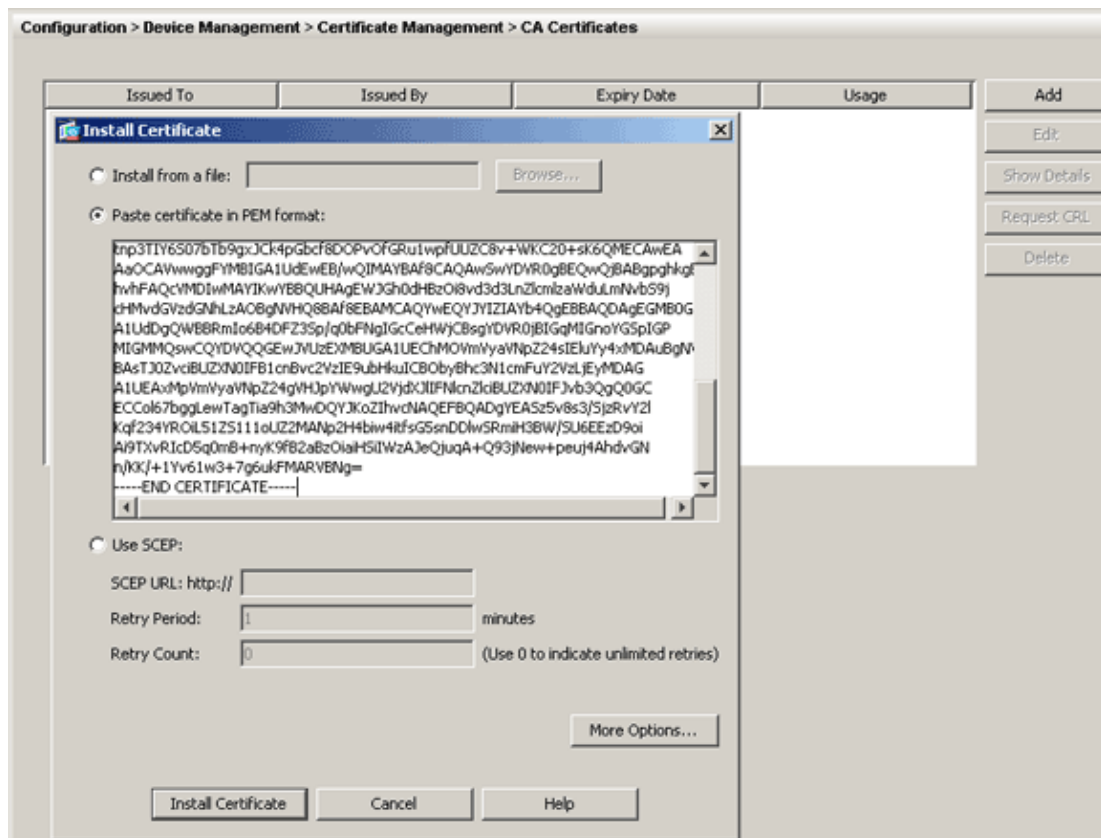


8. Click **Copy to File**.
9. Within the Certificate Export Wizard, click **Next**.



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

16. Within ASDM, click **Configuration**, and then click **Device Management**.
17. Expand **Certificate Management**, and choose **CA Certificates**.
18. Click **Add**.
19. Click the **Paste certificate in PEM Format** radio button, and paste the base64 CA certificate provided by the 3rd party vendor into the text field.
20. Click **Install Certificate**.



A dialog box appears that confirms the installation was successful.

Command Line Example

```

ciscoasa
-----BEGIN CERTIFICATE-----
MIIEwDCCBCmgAwIBAgIQY7G1zcWfeIAdoGNs+XVGezANBgkqhkiG9w0BAQUFADCB
jDELMAkGA1UEBhmCVVMxZAVBgnVBAoTD1Zlcm1TaWduLCBjbmuMTAwLgYDVQQL
EydG3IgvGVzdCBQdXJwb3NlcYBPbm55LiAgTm8gYXNzdXJhbmNlcY4xMjAwBjNV
BAMTKVZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgvGVzdCBsb290IENBMB4X
DTA1MDIwOTAwMDAwMfoXDTE1MDIwODIzNTk1OVowgcsxZAJBgnVBAwYTA1VTMRcw
FQYDVQQKEw5WZXXJpU2lnbiwSW5jLjEwMjAwMjAwLgYDVQQLZS1UZXRyYyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxLTAr
BgNVBAMTJFZlcm1TaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgvGVzdCBDbDQCCASiW

```

```
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAuwElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE61BBD6Zqk
d851P1/6Xxk0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n451P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1D/OCCmZO
5RmNqLLKSvYHhJ25EskFhgR2qCxx2EQJdnDXuTw0+4t1qj97ydk5iDoxjKfV6sb
tnp3TIY6S07bTb9gxJcK4pGbcf8DOPvOfGRulwpfUuzC8v+WKC20+sK6QMECAwEA
AaOCAVwgggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBABgppghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9j
cHMvdGVzdG9hLzAObG9NVH08BAf8EBAMCAQYwEYJYIZIAIYb4QgEBBAQDAgEGMB0G
A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgiGcCeHWjCBsgYDVR0jBIGqMIGnoYGSPIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNPZ24sIEluYy4xMDAuBGNV
BASTJ0ZvciBUZXR0IFB1cnBvc2VzIE9ubHkuICB0byBhc3N1cmFuY2VzLjEjEYMDAG
A1UEAxMpVmVyaVNPZ24gVHJpYWwgU2VjdXJlIFNlcnZlcjBUZXR0IFJvb3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/SjzRvY21
Kqf234YROI51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU6EEZD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaHSiIWzAJeQjuqA+Q93jNew+peuj4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBng=
-----END CERTIFICATE-----
quit
```

! Manually pasted certificate into CLI.

INFO: Certificate has the following attributes:

Fingerprint: 8de989db 7fcc5e3b fdde2c42 0813ef43

Do you accept this certificate? [yes/no]: **yes**

Trustpoint 'my.verisign.trustpoint' is a subordinate CA and
holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported

ciscoasa(config)#

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

Step 4. Install the Certificate

ASDM Procedure

Use the identity certificate provided by the 3rd party vendor to perform these steps:

1. Click **Configuration**, and then click **Device Management**.
2. Expand **Certificate Management**, and then choose **Identity Certificates**.
3. Select the identity certificate you created in Step 2. (The Expiry Date should display *Pending*.)
4. Click **Install**.


```
L3Rlc3RjYSAoYykwNTEtMCSGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
cnZlciBUZXR0IEIENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4GA1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ21zY28gU31zdGVtczEOMAwGA1UECzQVFNXRUIx
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90
ZXR0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNlMS5jaXNjby5jb20wgZ8wDQYJ
KoZIHvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R
IaUE8/LiAZba70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJZa1hJTxs1EgryosBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjaAMAsGA1UdDwQEAwIFoDBDBgNV
HR8EPDA6MDignQa0hjJodHRwOi8vU1ZSU2VjdXJlLWNYbC52ZXJpc2lnbi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBGgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXR0Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYijoHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwaJkBggrBgEFBQcwAYYYaHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJl
LWFPYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFPYS5jZXIwbgYIKwYBBQUH
AQWEYjBgoV6gXDBAMFgwVhYJaW1hZ2UvZ2lmMCEwHZAHBGUrdgMCGgQUS2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9n
bzEuY2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAAnym4GVThPIyL/9ylDBd8N7/yW3Ov3
bIirHfHJyfpJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q86ZiKyMIj
XM2VCmcHsaJmMMRjypydxfk6CidDMtMGotCavRHD9T12tvwgrBock/v/54o021kB
SmLzVV7crlYjEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FsewY8MAIY
rtab5F+oiTc5xGy8w7NARAFNGFXihqnLgWTtA35/oWuy86bje1IWbeyqj8ePM9Td
0LdAw6kUULPNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
quit
```

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

Step 5. Configure WebVPN to Use the Newly Installed Certificate

ASDM Procedure

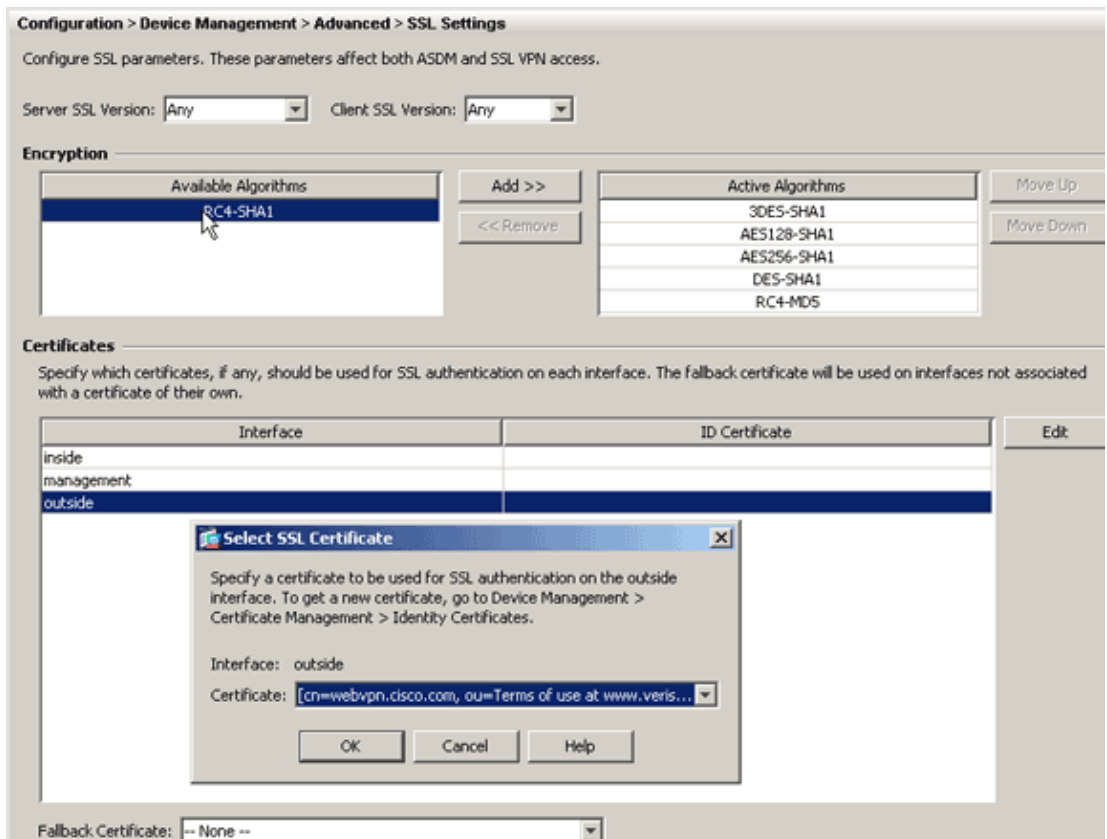
1. Click **Configuration**, and then click **Device Management**.
2. Expand **Advanced**, and then expand **SSL Settings**.
3. Under Certificates, select the interface that is used to terminate WebVPN sessions.

In this example, the outside interface is used.

4. Click **Edit**.
5. In the Certificate drop-down list, choose the certificate installed in Step 4.
6. Click **OK**.
7. Click **Apply**.

Your new certificate should now be utilized for all WebVPN sessions that terminate on the interface specified.

8. See the Verify section in order to confirm that the installation process was successful.



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)# wr mem
Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08

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

! Save configuration.

```

Verify

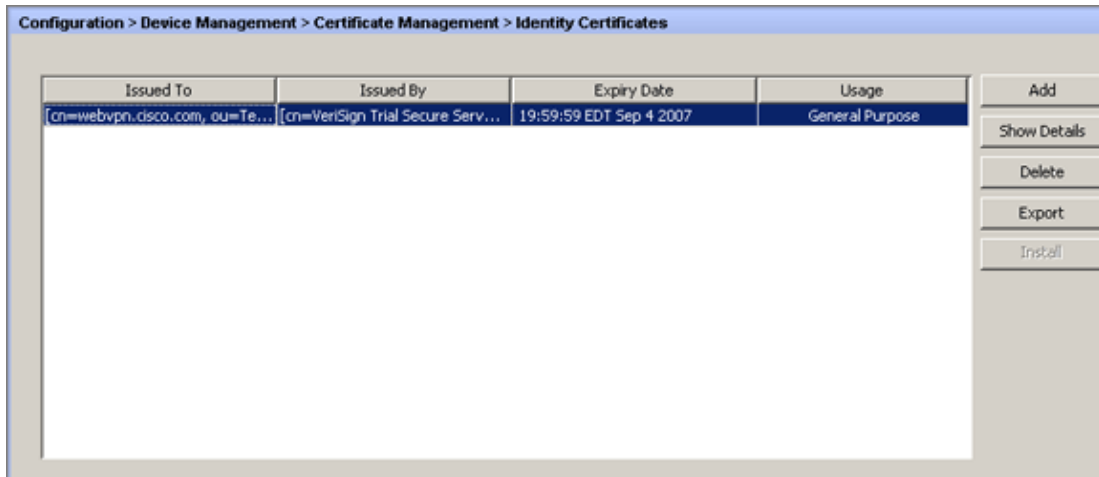
Use the following steps to verify successful installation of the 3rd Party Vendor Certificate and use for WebVPN connections.

View Installed Certificates

ASDM Procedure

1. Click Configuration, and click Device Management.
2. Expand Certificate Management, and choose Identity Certificates.

The identity certificate issued by your 3rd party vendor should appear.



Command Line Example

```
ciscoasa
-----
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 ©)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 ©)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 ©)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 the following security alerts, perform the procedure that corresponds to that alert:

◆ 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.

◆ The security certificate was issued by a company you have not chosen to trust...

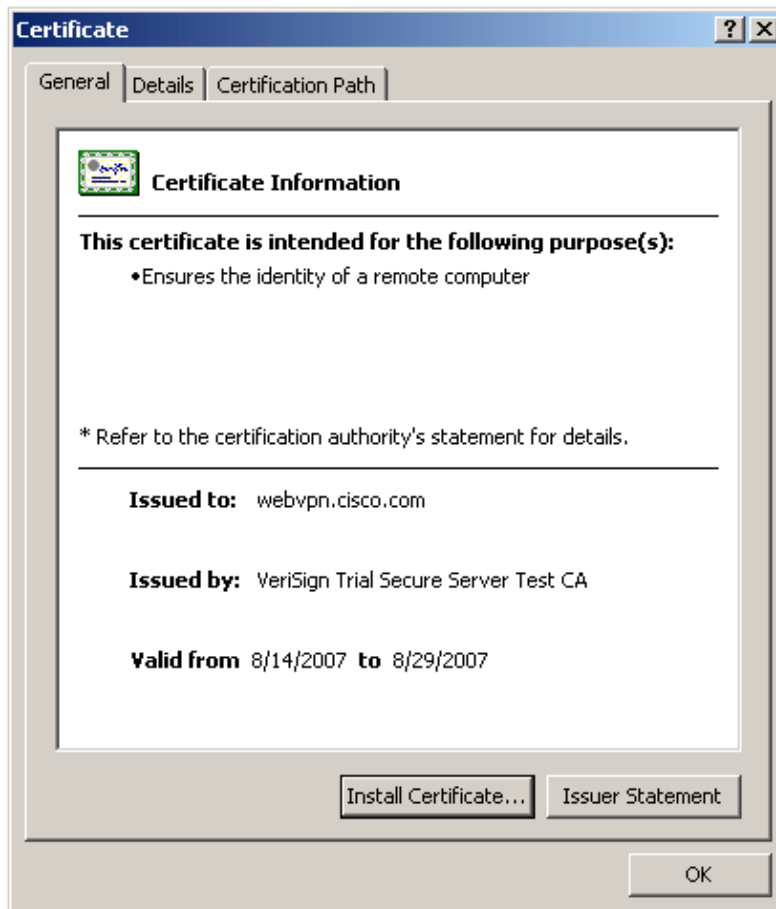
Complete these steps in order to install the 3rd party vendor root certificate to your web browser:

- a. In the Security Alert dialog box, click **View Certificate**.
- b. In the Certificate dialog box, click the **Certificate Path** tab.
- c. Select the CA certificate located above your issued identity certificate, and click **View Certificate**.
- d. Click **Install Certificate**.
- e. In the Certificate Install Wizard dialogue box, click **Next**.

- f. Click the **Automatically select the certificate store based on the type of certificate** radio button, click **Next**, and then click **Finish**.
 - g. Click **Yes** when you receive the Install the certificate confirmation prompt.
 - h. 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.



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. If the CA certificate exists, verify it references the correct trustpoint.

```

ciscoasa
-----
ciscoasa#show crypto ca certificate my.verisign.trustpoint | b CA Certificate
CA Certificate
  Status: Available
  Certificate Serial Number: 63bla5cdc59f78801da0636cf975467b
  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 ©)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

!!! Line above lists associated trustpoints.

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 the appropriate trustpoint. Also, verify the key pair has not changed 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](#)

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 04, 2007

Document ID: 98596
