在 ASA 7.x 上手动安装第三方供应商证书以便与 WebVPN 一起使用的配置示例

目录

简介

此配置示例描述如何在 ASA 上手动安装第三方供应商数字证书，以便与 WebVPN 一起使用。此示例中使用 Verisign Trial Certificate。每个步骤都包含 ASDM 应用程序步骤和 CLI 示例。

先决条件

要求

本文档要求您能够访问证书机构 (CA) 以便进行证书注册。支持的第三方 CA 供应商有 Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA 和 Verisign。

使用的组件

本文档使用运行软件版本 7.2(1) 和 ASDM 版本 5.2(1) 的 ASA 5510。但是，本文档中的过程对于运行 7.x 和任何可兼容 ASDM 版本的任何 ASA 设备都有效。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

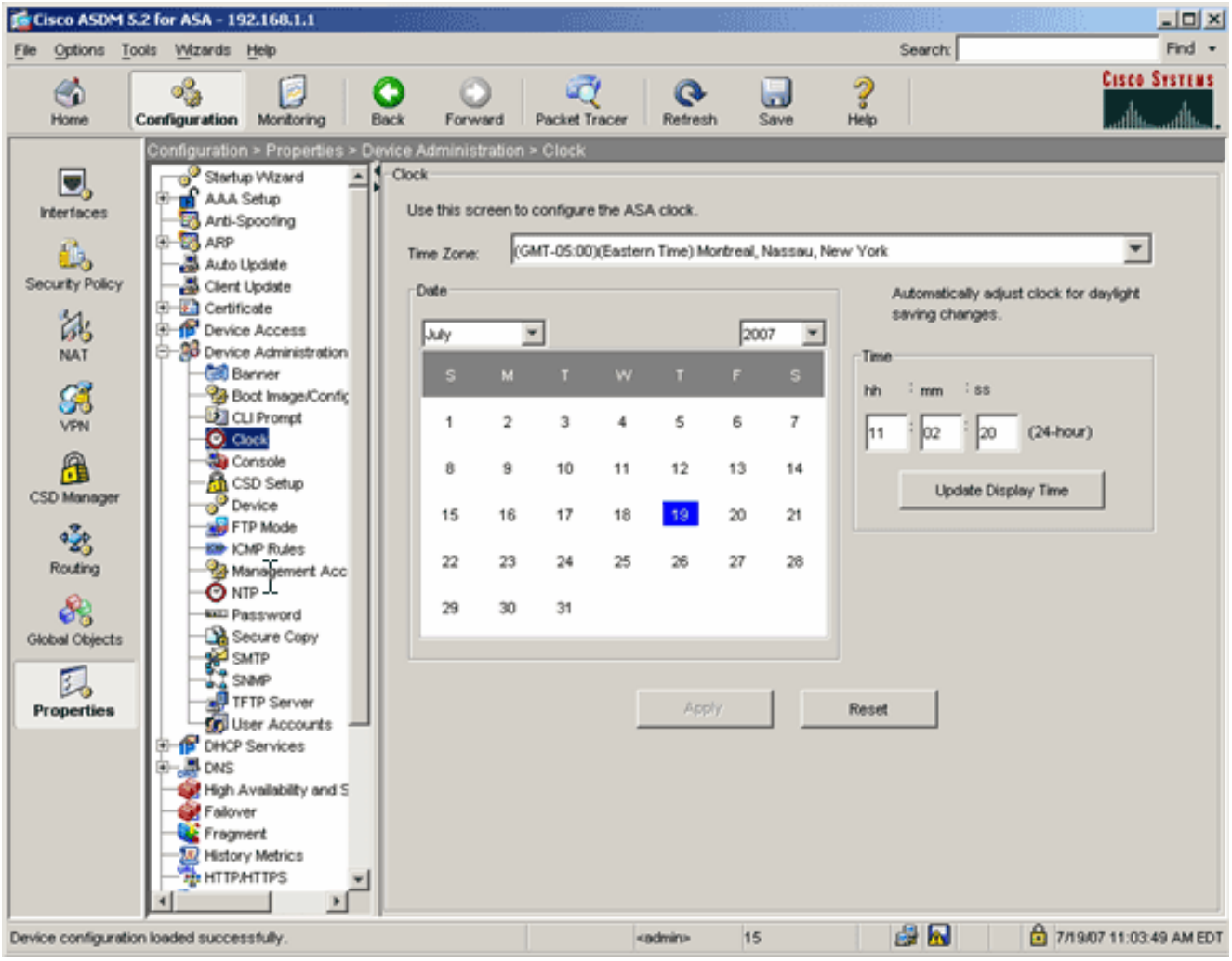
要在 PIX/ASA 上安装第三方供应商数字证书，请完成以下步骤：

1. 验证日期、时间和时间区域值是准确的。
2. 生成 RSA 密钥对。
3. 创建信任点。
4. 生成证书登记。
5. 验证信任点。
6. 安装证书。
7. 配置WebVPN最近使用预装证书。

步骤 1. 验证 Date、Time 和 Time Zone 值是否准确

ASDM 步骤

1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Device Administration**，然后选择 Clock。
3. 验证列出的信息是否准确。要正确通过证书验证，Date、Time 和 Time Zone 值必须准确。



命令行示例

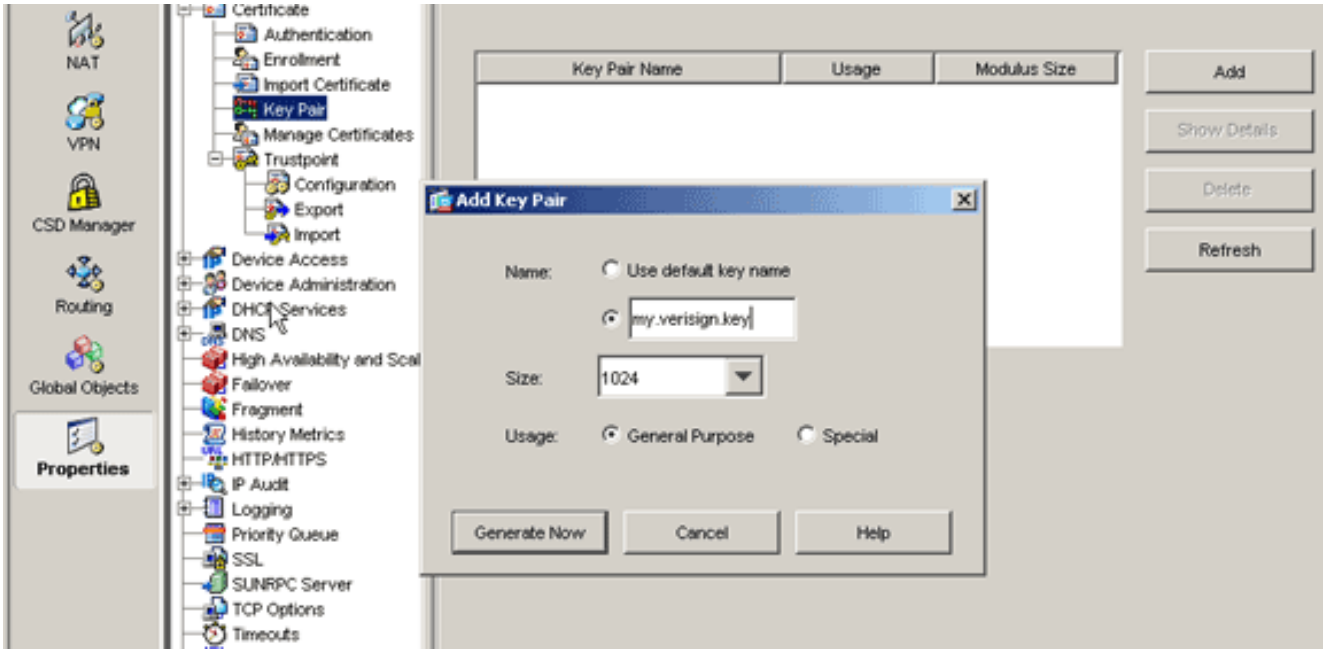
ciscoasa
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa

步骤 2. 生成 RSA 密钥对

生成的 RSA 公钥将与 ASA 的身份信息组合在一起形成 PKCS#10 证书请求。您应明确指出要为其创建密钥对的信任点的密钥名称。

ASDM 步骤

1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Certificate**，然后选择 Key Pair。
3. 单击 **Add**。



4. 输入密钥名称，选择系数大小，然后选择使用类型。**注意**：推荐的密钥对大小是 1024。
5. 单击生成。您创建的密钥对应在 Key Pair Name 列中列出。

命令行示例

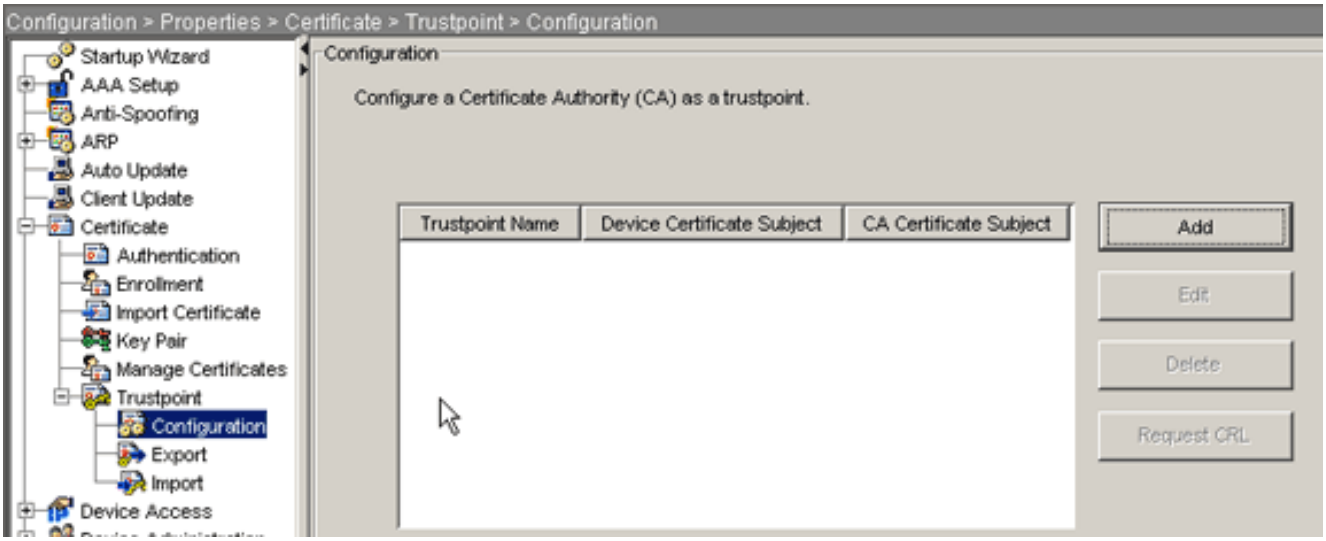
ciscoasa
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024** *! Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#

步骤 3. 创建信任点

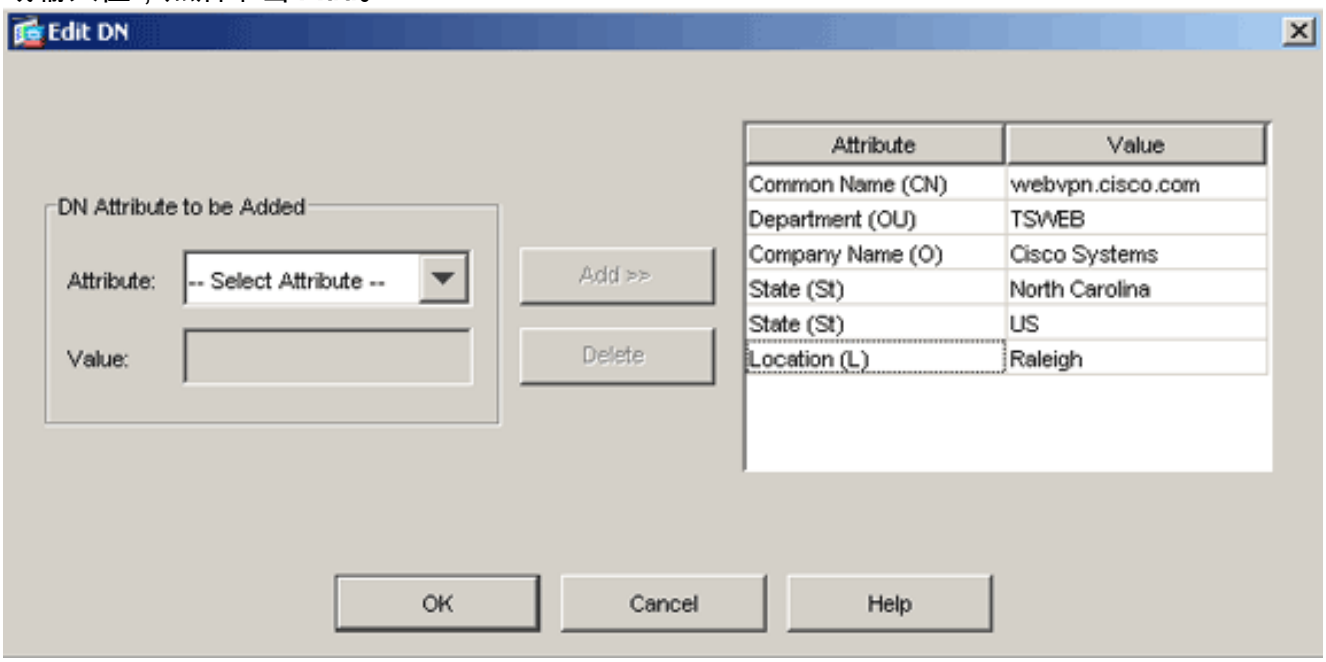
要声明 ASA 将使用的证书机构 (CA)，必须提供信任点。

ASDM 步骤

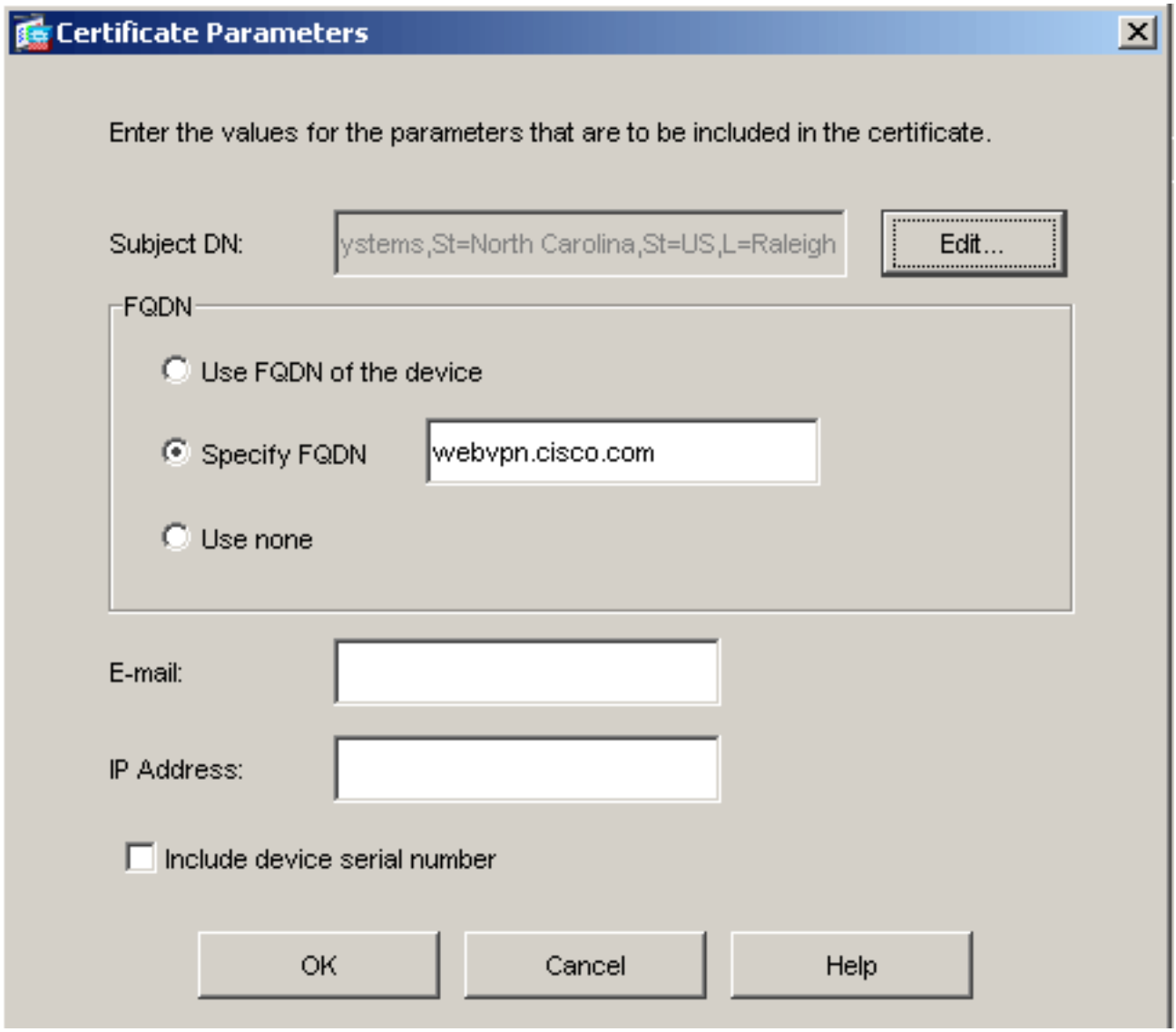
1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Certificate**，然后展开 Trustpoint。
3. 选择 **Configuration**，然后单击 Add。



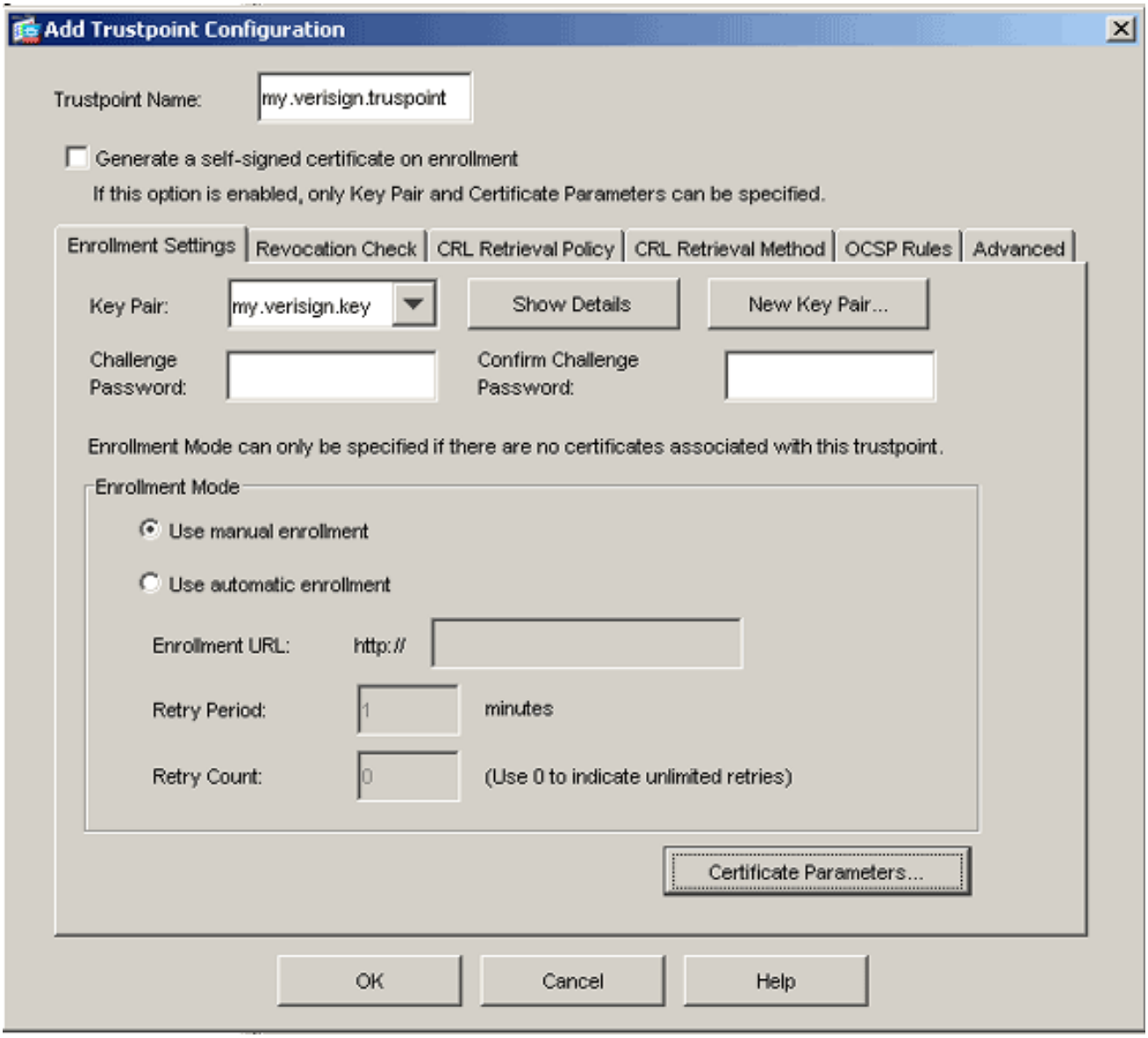
4. 配置以下值：**Trustpoint Name**:信任点名称应与目标用途相关。（此示例使用 *my.verisign.trustpoint*。）**Key pair**:选择在步骤 2 中生成的密钥对 (*my.verisign.key*)。
5. 确保选中 Manual Enrollment。
6. 单击 **Certificate Parameters**。将会出现 Certificate Parameters 对话框。
7. 单击 **Edit**，然后配置下表中列出的属性：要配置这些值，可以从 Attribute 下拉列表中选择值或输入值，然后单击 **Add**。



8. 添加相应的值之后，单击 **OK**。
9. 在 Certificate Parameters 对话框的 Specify FQDN 字段中，输入 FQDN。此值应与用于公用名称 (CN) 的 FQDN 相同。



10. 单击 **Ok**。
11. 验证是否选择了正确的密钥对，然后单击 **Use manual enrollment** 单选按钮。
12. 单击 **OK**，然后单击 Apply。



命令行示例

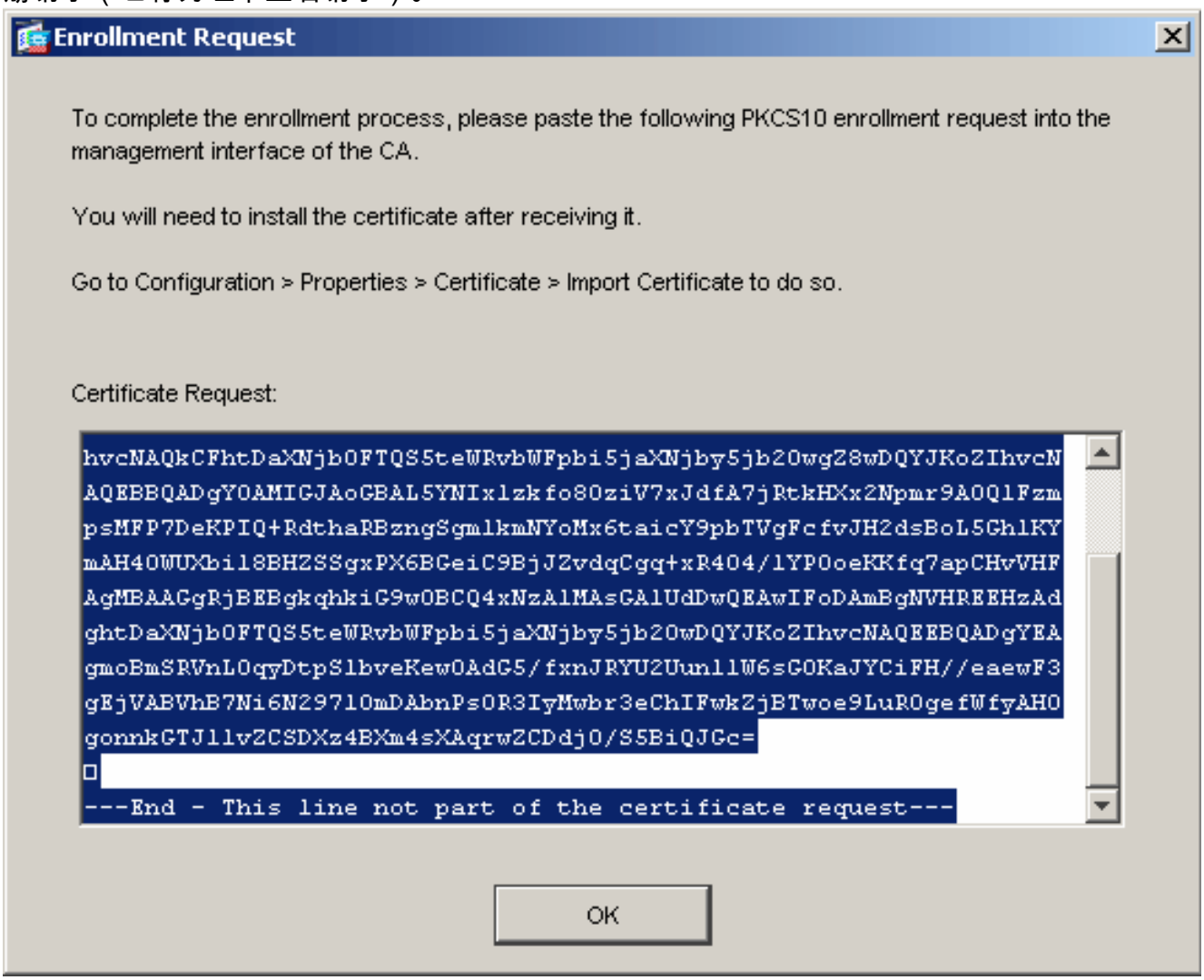
ciscoasa
ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** **! Creates the trustpoint.** ciscoasa(config-ca-trustpoint)#**enrollment terminal** *! Specifies cut and paste enrollment with this trustpoint.* ciscoasa(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco 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 webvpn.cisco.com** *! Specifies subject alternative name (DNS:).*

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

步骤 4. 生成证书注册

ASDM 步骤

1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Certificate**，然后选择 Enrollment。
3. 确认选择了在第 3 步中创建的信任点，然后单击 **Enroll**。将会出现一个对话框，并列出证书注册请求（也称为证书签名请求）。



4. 将 PKCS#10 注册请求复制到一个文本文件中，然后将 CSR 提交给相应的第三方供应商。第三方供应商在收到 CSR 后应颁发一个用于安装的身份证书。

命令行示例

设备名称 1

```
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
```

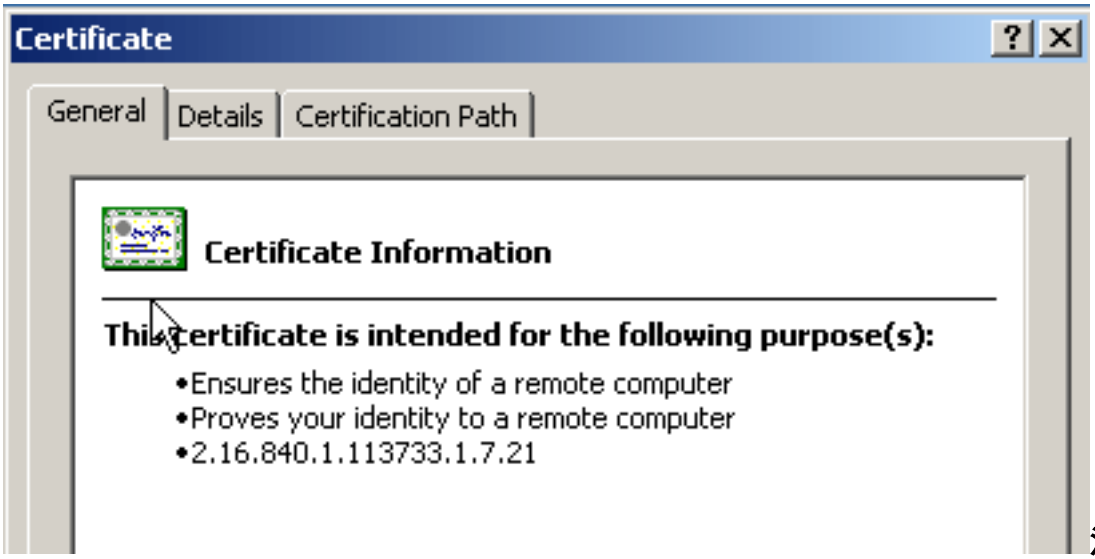
```
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes

! 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:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#
```

步骤 5. 验证信任点

从第三方供应商处收到身份证书后，您可以继续执行此步骤。

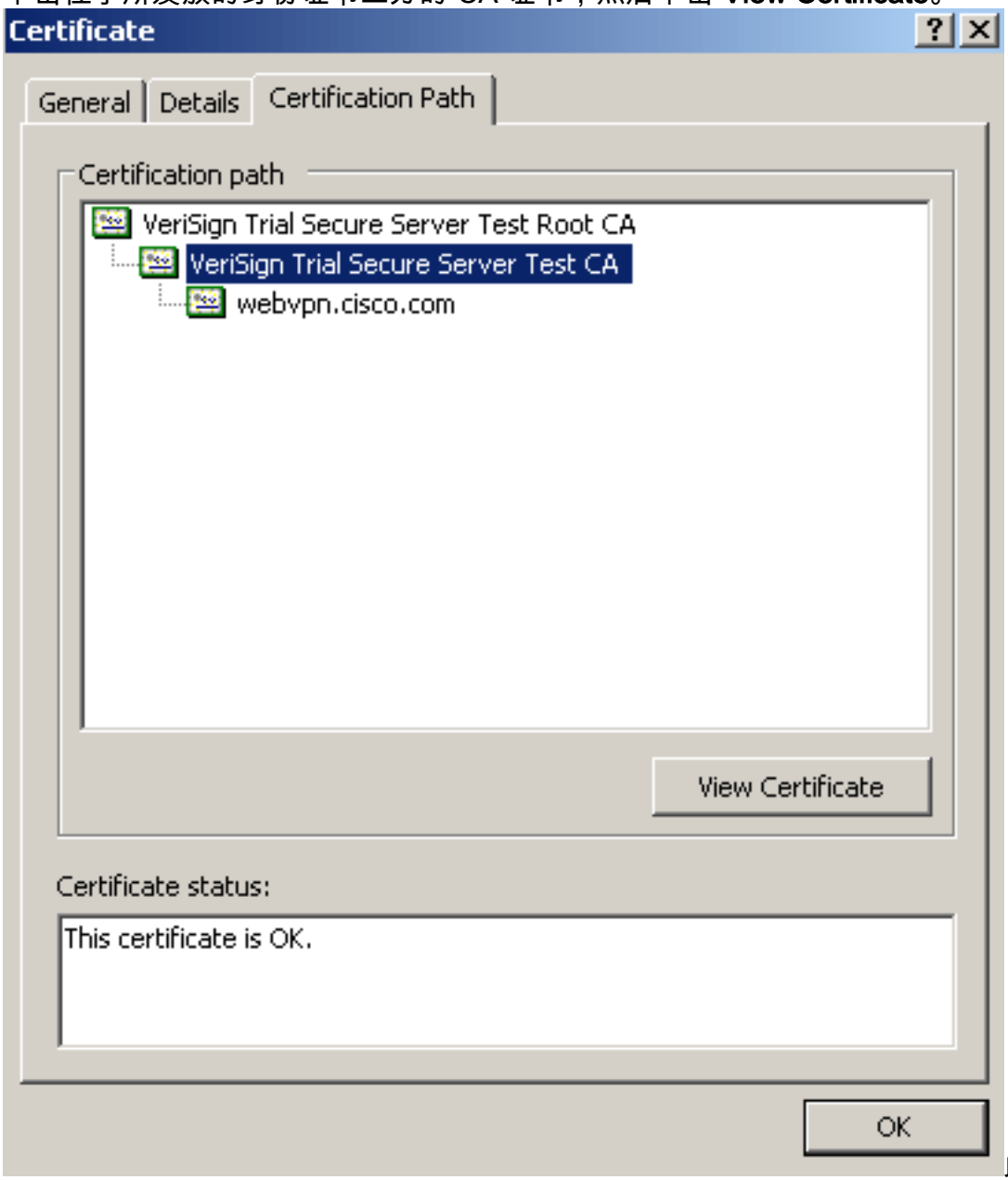
ASDM 步骤

1. 将身份证书保存到本地计算机中。
2. 如果您收到的是非文件形式的 base64 加密证书，则您必须复制此 base64 信息，并将其粘贴到文本文件中。
3. 将文件扩展名改为 .cer。**注意：** 使用扩展名 .cer 重命名文件后，文件图标将显示为证书。
4. 双击此证书文件。此时，将显示“Certificate”对话框。



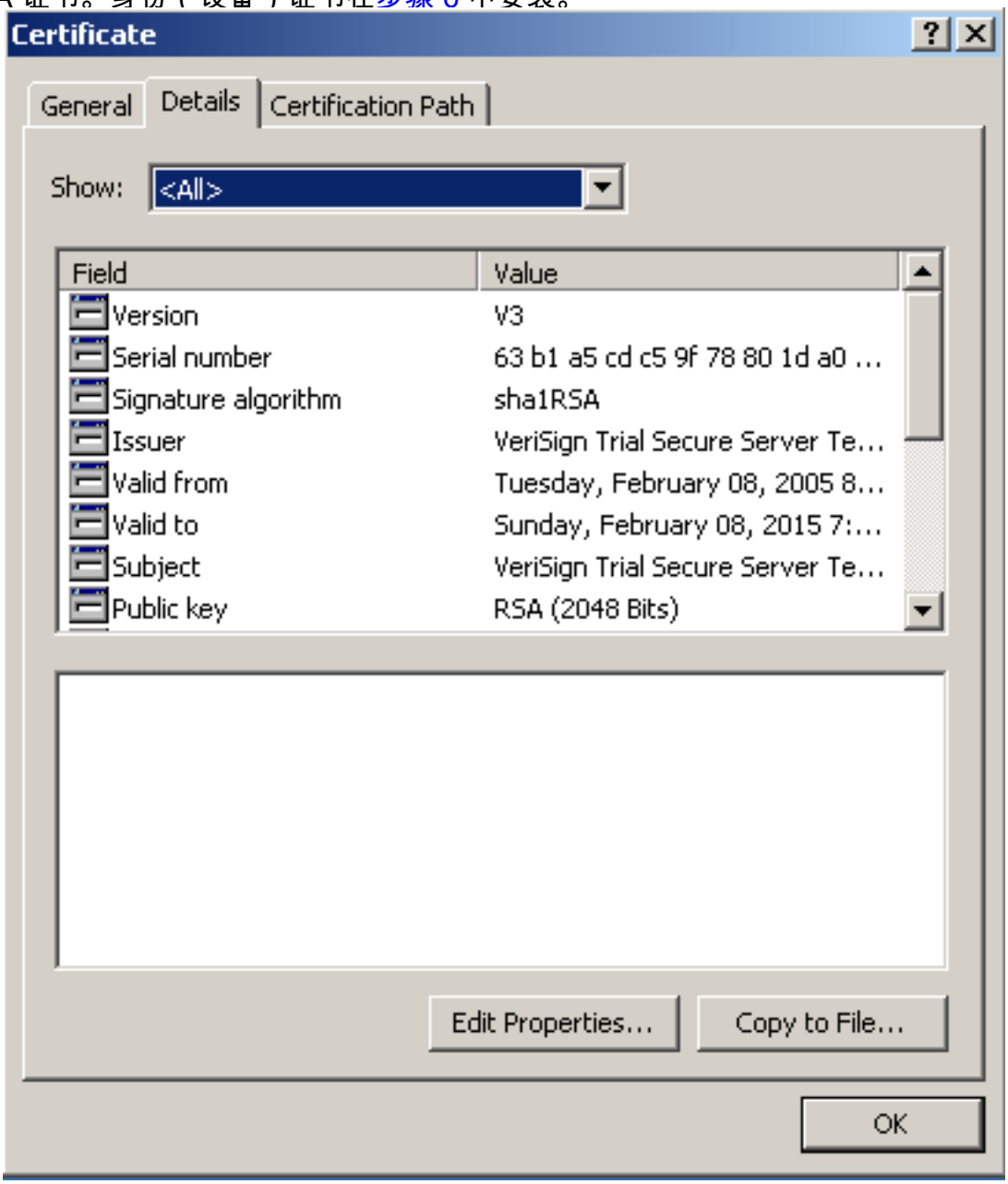
注意： 如果 General 选项卡中显示“Windows does not have enough information to verify this certificate”信息，则在继续执行此步骤之前，您必须获取第三方供应商的根 CA 或中间 CA 证书。请与第三方供应商或 CA 管理员联系，以获得其发放的根 CA 或中间 CA 证书。

5. 单击 **Certificate Path** 选项卡。
6. 单击位于所发放的身份证书上方的 CA 证书，然后单击 **View Certificate**。

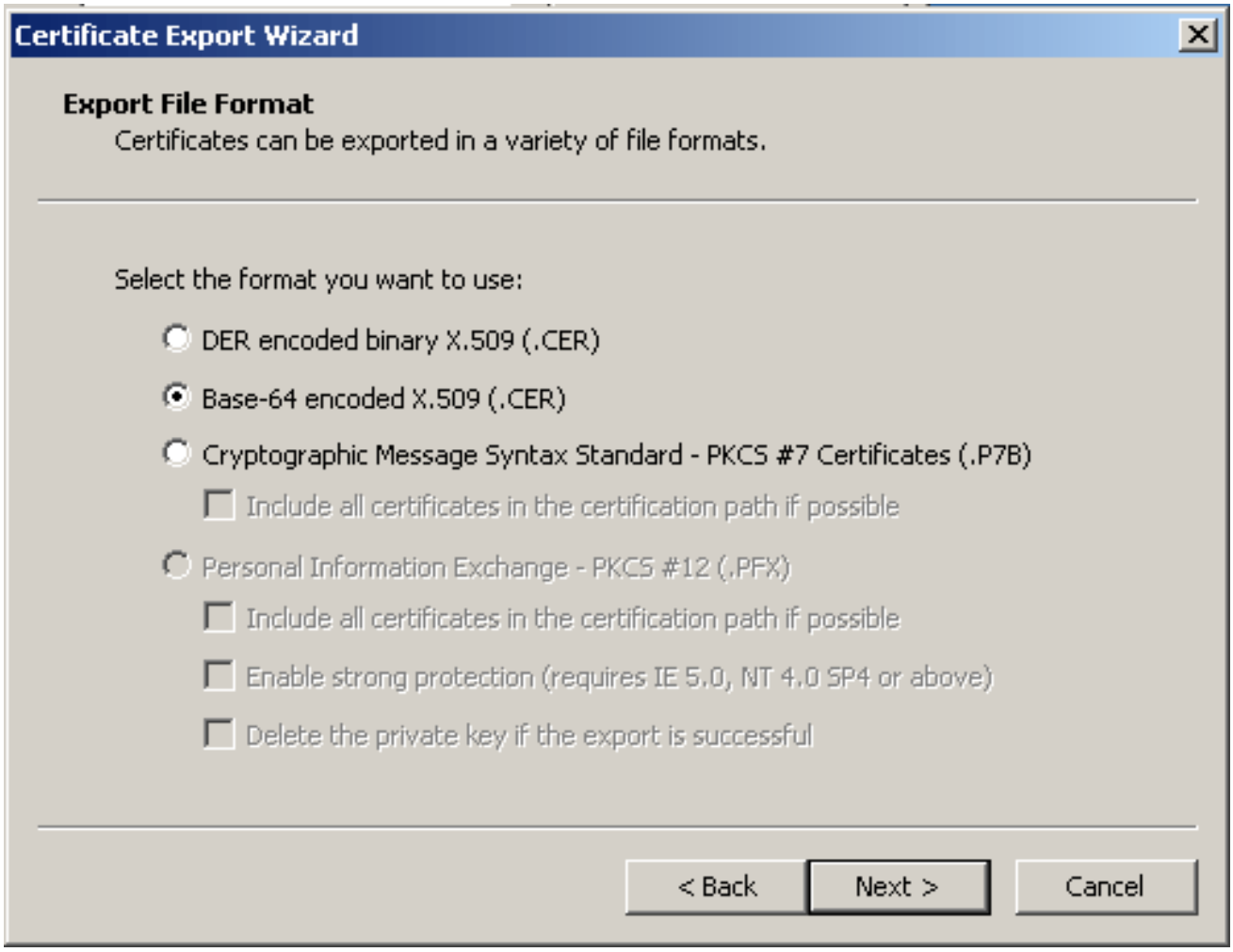


此时，将显示中

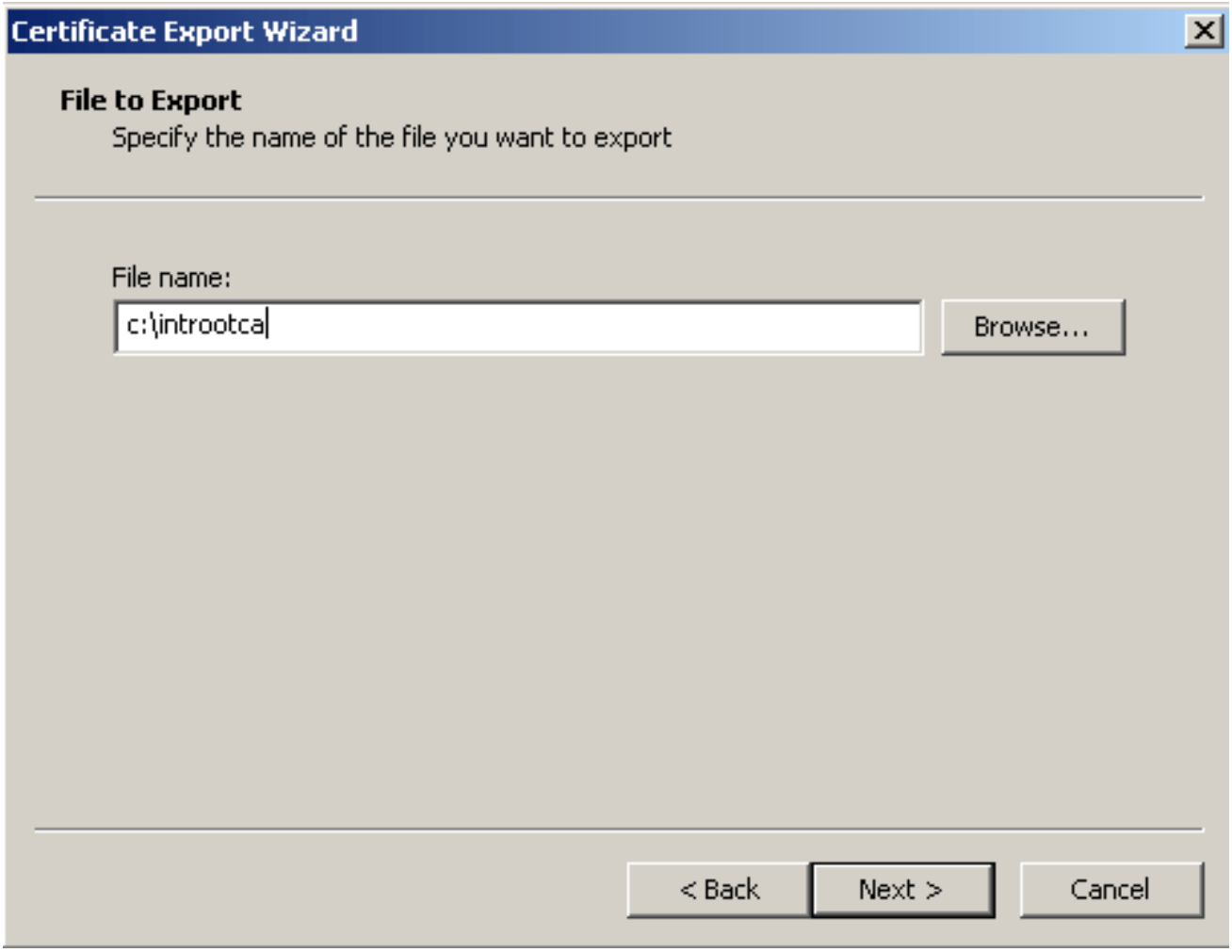
间 CA 证书的详细信息。**警告：** 请勿在此步骤中安装身份（设备）证书。在此步骤中仅添加根、辅助根或 CA 证书。身份（设备）证书在步骤 6 中安装。



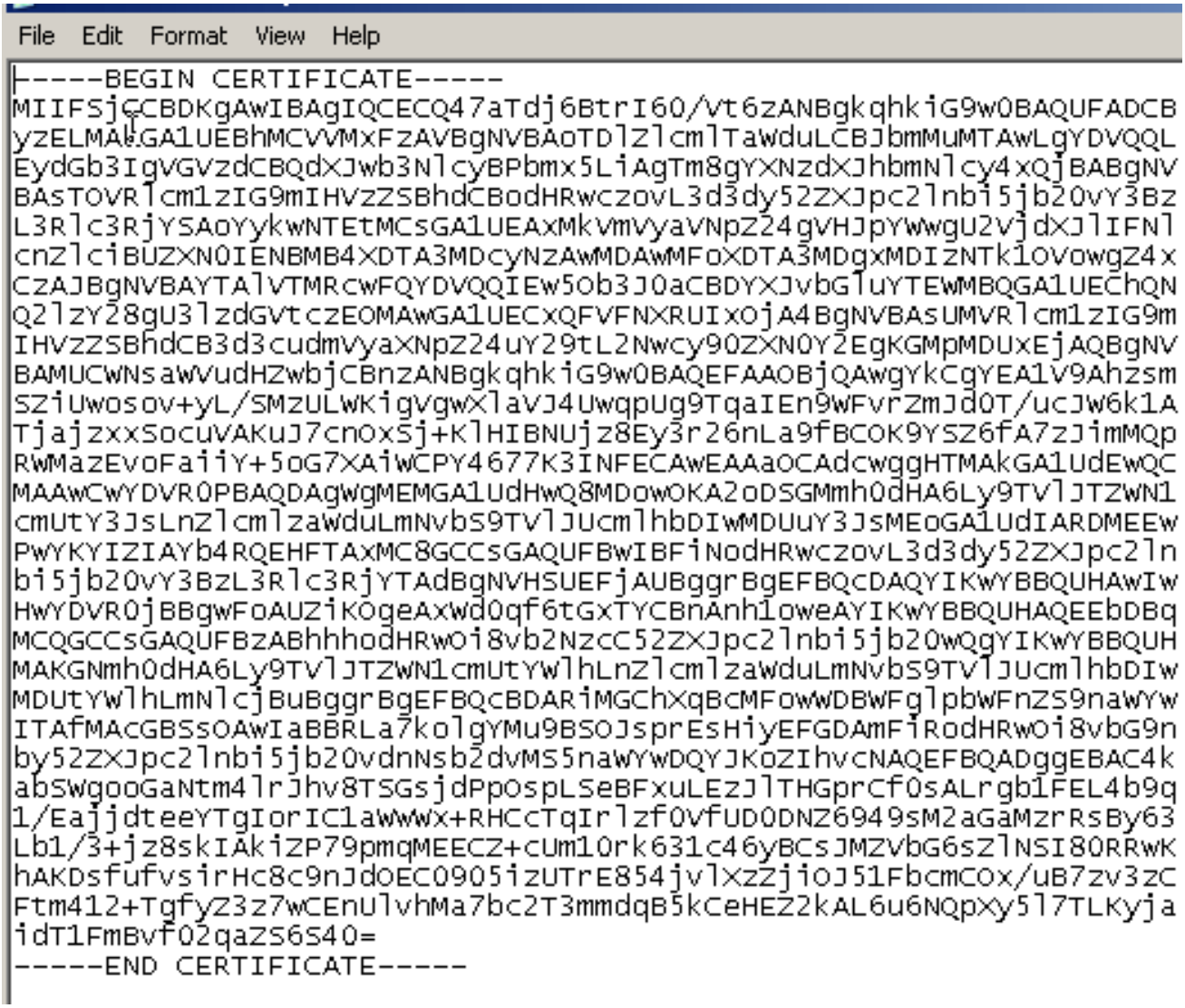
7. 单击 **Details**。
8. 单击 **Copy to File**。
9. 在“Certificate Export Wizard”中，单击 **Next**。
10. 在“Export File Format”对话框中，单击 **Base-64 encoded X.509 (.CER)** 单选按钮，然后单击“Next”。



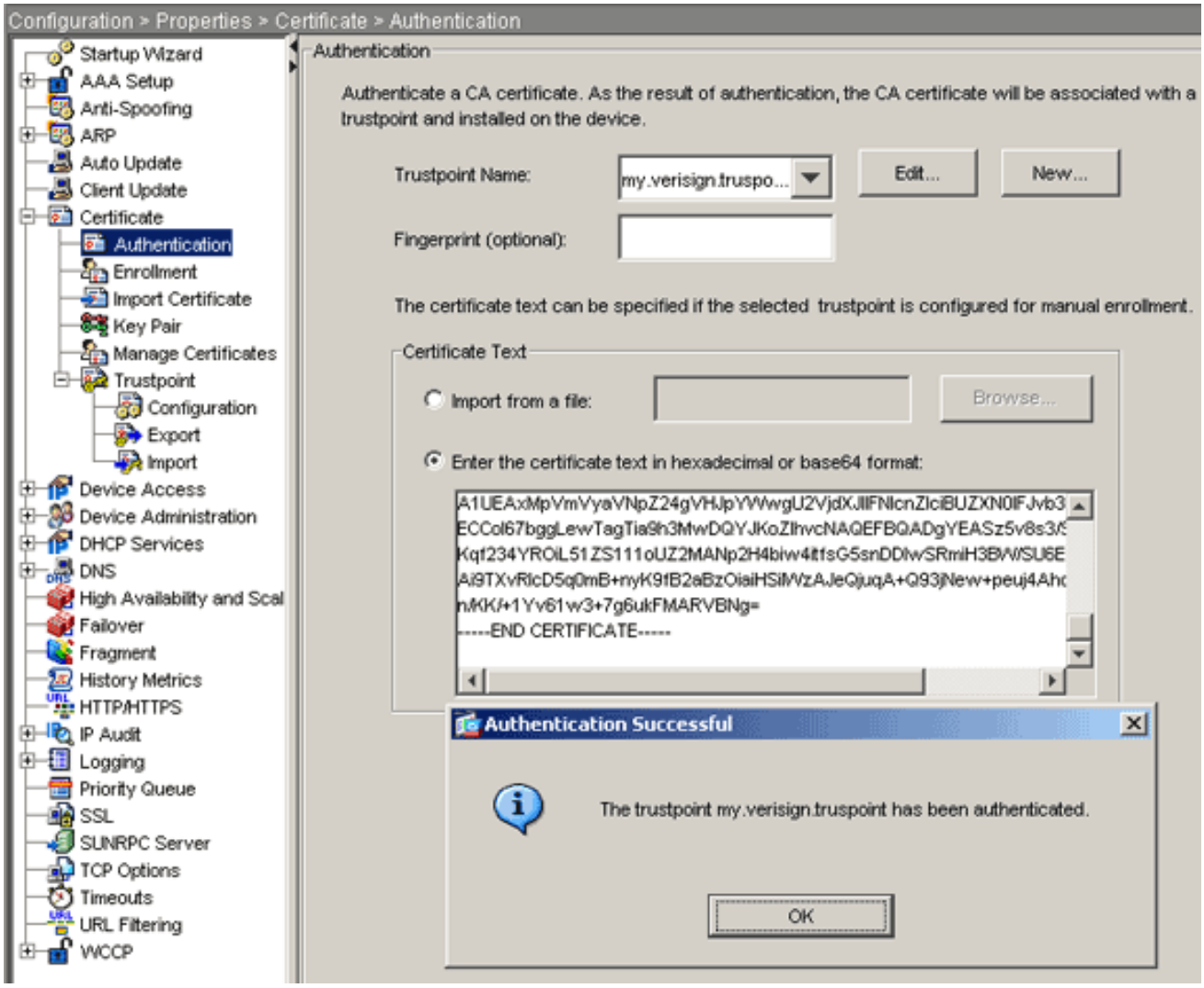
11. 输入文件名以及要用于保存 CA 证书的位置。
12. 单击 **Next**，然后单击“Finish”。



13. 在“Export Successful”对话框中，单击 **OK**。
14. 浏览到 CA 证书的保存位置。
15. 使用文本编辑器打开文件，例如记事本。（右键单击文件，然后选择 **Send To > Notepad**。）将会显示类似于下图中证书的 base64 编码信息：



16. 在 ASDM 中，单击 **Configuration**，然后单击 Properties。
17. 展开 **Certificate**，然后选择 Authentication。
18. 单击 **Enter the certificate text in hexadecimal or base64 format** 单选按钮。
19. 将 base64 格式的 CA 证书从文本编辑器中粘贴到文本区域。
20. 单击 **Authenticate**。



21. 单击 Ok。

命令行示例

ciscoasa

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

! Initiates the prompt to paste in the base64 CA root !
or intermediate certificate. Enter the base 64 encoded
CA certificate. End with the word "quit" on a line by
itself -----BEGIN CERTIFICATE-----
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFN1Y3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEzlUZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFN1Y3VyZSBTZXJ2ZXIgVGVzdCBD
```

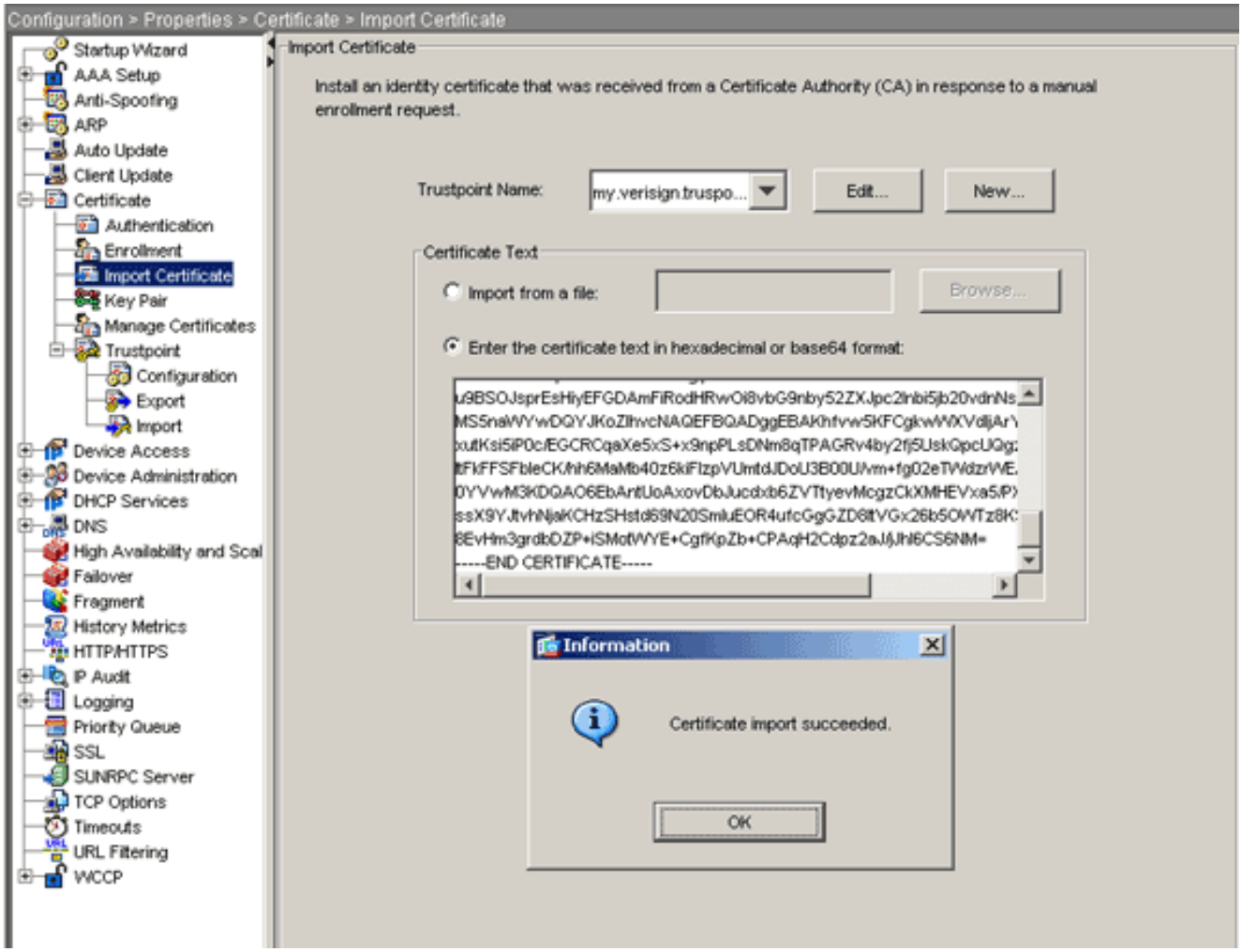
```
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
oYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IFJv
b3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY2l
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
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)#
```

步骤 6. 安装证书

ASDM 步骤

使用第三方供应商提供的身份证书执行以下步骤：

1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Certificate**，然后选择 Import Certificate。
3. 单击 **Enter the certificate text in hexadecimal or base64 format** 单选按钮，然后将 base64 身份证书粘贴到文本字段中。



4. 单击 Import，然后单击 OK。

命令行示例

ciscoasa

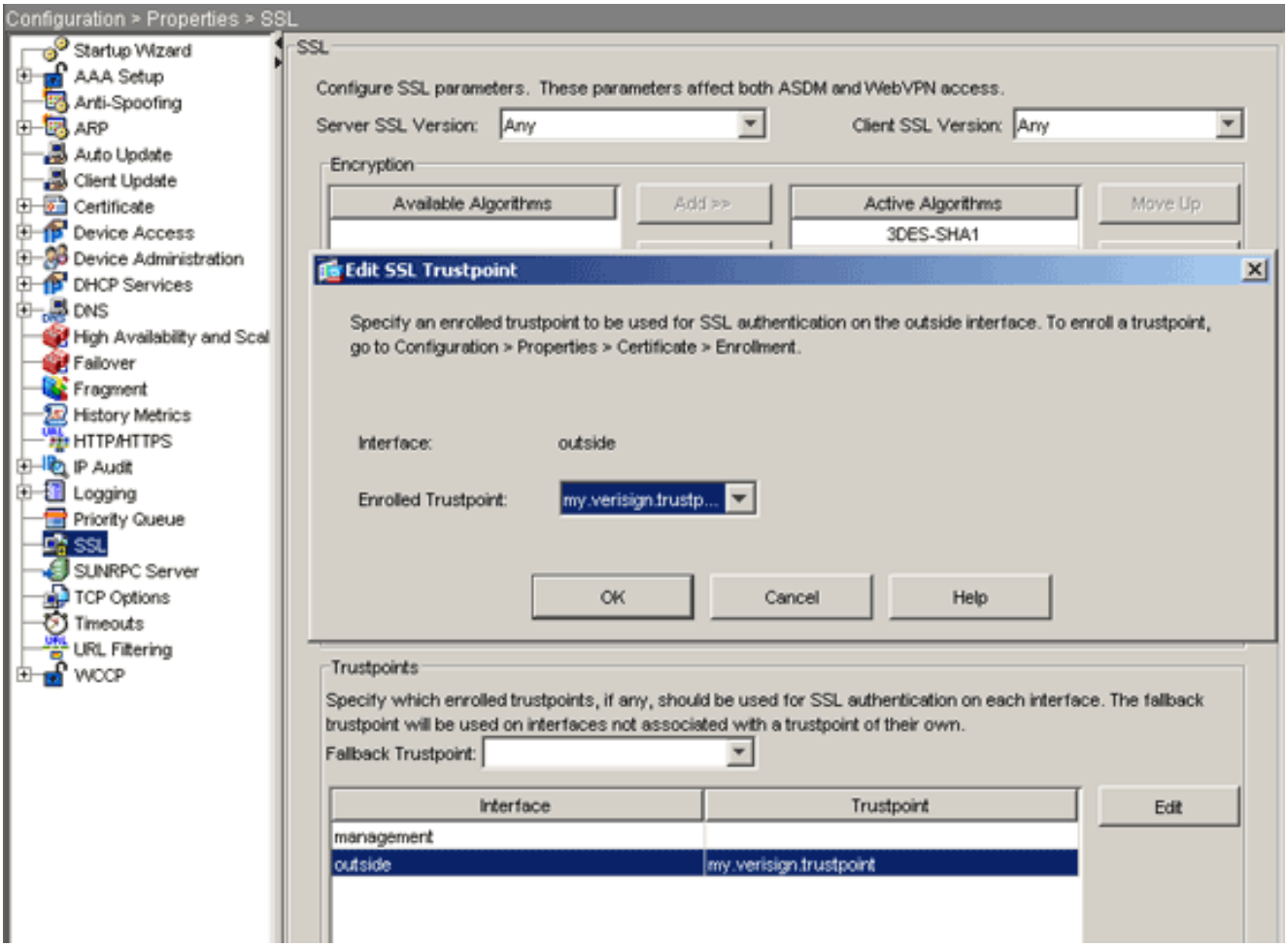
```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate

! 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/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
QjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFN1
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4G
A1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUIx
```

```
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2ln
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
quit

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

步骤 7. 将 WebVPN 配置为使用新安装的证书

ASDM 步骤

1. 单击 **Configuration**，单击 Properties，然后选择 SSL。
2. 在 Trustpoints 区域中，选择将用于终止 WebVPN 会话的接口。（本示例使用外部接口。）
3. 单击 **Edit**。此时将显示 Edit SSL Trustpoint 对话框。



4. 从 Enrolled Trustpoint 下拉列表中，选择在步骤 3 中创建的信任点。
5. 单击 **OK**，然后单击 Apply。

现在，在指定接口上终止的所有 WebVPN 会话应该已使用新的证书。有关如何验证安装是否成功的信息，请参阅本文档中的验证部分。

命令行示例

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.
```

验证

本部分描述如何确认已成功安装第三方供应商证书。

替换 ASA 的自签名证书

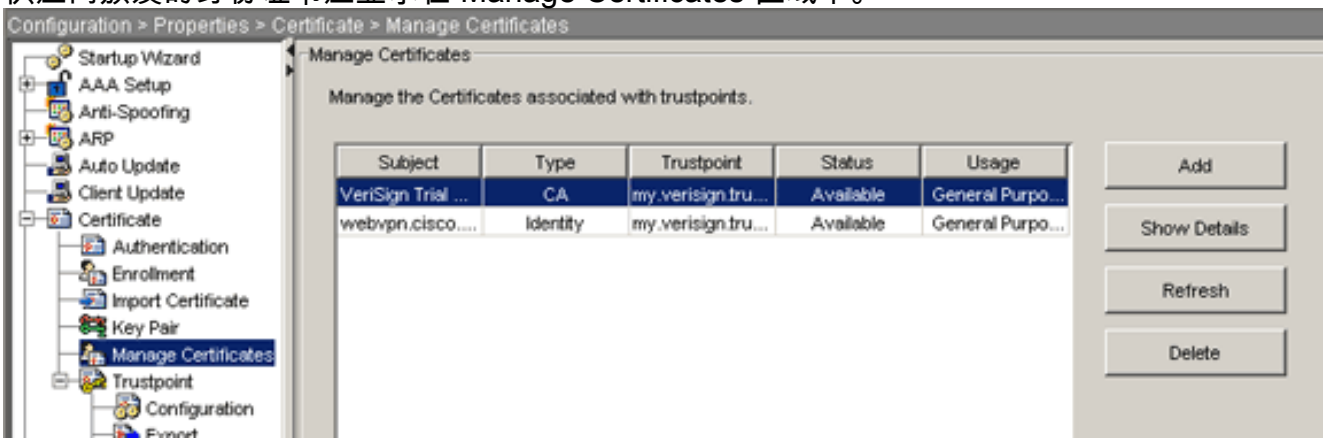
本部分描述如何替换已安装的 ASA 自签名证书。

1. 向 Verisign 发送证书签名请求。从 Verisign 收到请求的证书后，便可在同一个信任点下直接安装它。
2. 键入以下命令：**crypto ca enroll Verisign**系统将提示您回答问题。
3. 对于 *Display Certificate Request to terminal*，输入 **yes**，并将输出发送给 Verisign。
4. 在他们为您提供新证书后，键入以下命令：**crypto ca import Verisign certificate**

查看已安装的证书

ASDM 步骤

1. 单击 **Configuration**，然后单击 Properties。
2. 展开 **Certificate**，然后选择 Manage Certificates。用于信任点身份验证的 CA 证书和由第三方供应商颁发的身份证书应显示在 Manage Certificates 区域中。



命令行示例

ciscoasa

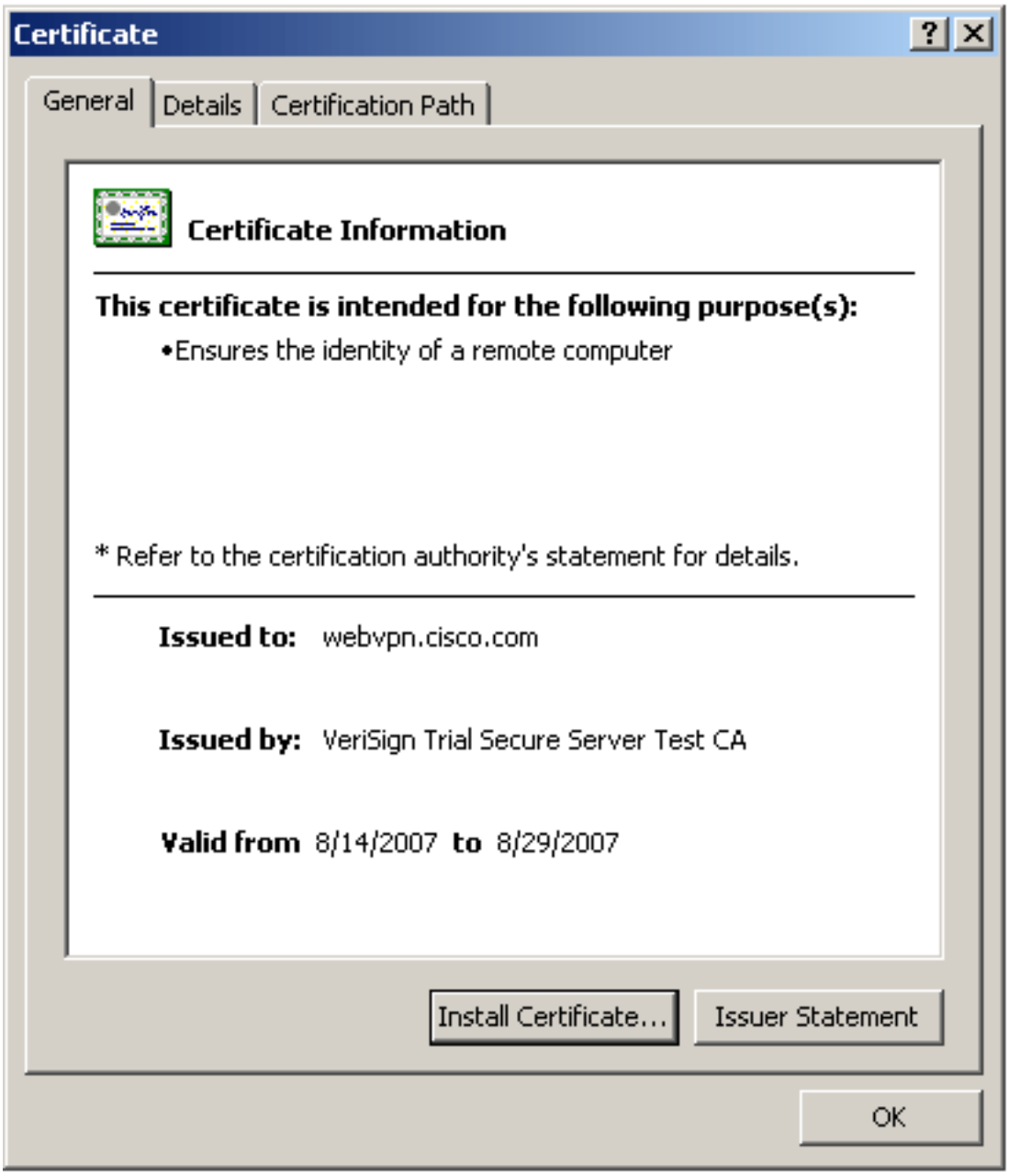
```
ciscoasa(config)#show crypto ca certificates

! 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 (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 (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.
```

使用 Web 浏览器验证为 WebVPN 安装的证书

要验证 WebVPN 是否使用新证书，请完成以下步骤：

1. 通过 Web 浏览器连接到 WebVPN 接口。将 https:// 以及用于请求证书的 FQDN（例如，https://webvpn.cisco.com）。如果收到下列安全警报之一，请执行与该警报对应的过程：**The Name of the Security Certificate Is Invalid or Does Not Match the Name of the Site**验证您使用的 FQDN/CN 是否正确，以便连接到 ASA 的 WebVPN 接口。必须使用请求身份证书时定义的 FQDN/CN。可以使用 **show crypto ca certificates** *trustpointname* 命令验证证书 FQDN/CN。**The security certificate was issued by a company you have not chosen to trust...**要将第三方供应商根证书安装到 Web 浏览器，请完成以下步骤：在“Security Alert”对话框中，单击 **View Certificate**。在“Certificate”对话框中，单击 **Certificate Path** 选项卡。选择位于为您颁发的身份证书上方的 CA 证书，然后单击 **View Certificate**。单击 **Install Certificate**。在“Certificate Install Wizard”对话框中，单击 **Next**。选择 **Automatically select the certificate store based on the type of certificate** 单选按钮，单击“Next”，然后单击“Finish”。当收到安装证书确认提示时，单击 **Yes**。显示 *Import operation was successful* 提示时，单击 **OK**，然后单击“Yes”。**注意：** 由于此示例使用 Verisign Trial Certificate，因此必须安装 Verisign Trial CA Root Certificate，以避免用户连接时出现验证错误。
2. 双击 WebVPN 登录页右下角显示的锁图标。此时应显示已安装证书的信息。
3. 查看这些内容，以验证是否与您的第三方供应商证书相匹配。



续订 SSL 证书的步骤

要续订 SSL 证书，请完成以下步骤：

1. 选择需要续订的信任点。
2. 选择 **enroll**。将显示以下消息：*If it is successfully enrolled again, the current cert will be replaced with the new ones.是否要继续？*
3. 选择**是**。这将生成一个新 CSR。
4. 将此 CSR 发送给您的 CA，在返回证书后导入新 ID 证书。
5. 在外部接口上删除并重新应用信任点。

命令

在 ASA 上，可以在命令行中使用一些 show 命令来验证证书的状态。

- **show crypto ca trustpoint** — 显示已配置的信任点。
- **show crypto ca certificate** — 显示系统上安装的所有证书。

- **show crypto ca crls** — 显示缓存的证书撤销列表 (CRL)。
- **show crypto key mypubkey rsa** — 显示所有生成的加密密钥对。

故障排除

本部分提供的信息可用于对配置进行故障排除。

以下是您可能会遇到的一些可能的错误：

- **%警告：CA cert is not found.The imported certs might not be usable.INFO:Certificate successfully imported**对 CA 证书的身份验证不正确。请使用 **show crypto ca certificate** *trustpointname* 命令验证是否安装了 CA 证书。查找以 **CA Certificate** 开头的行。如果已安装 CA 证书，请验证它是否引用了正确的信任点。
- ERROR:Failed to parse or verify imported certificate在安装身份证书时，如果您不具有通过相关信任点验证的正确的中间或根 CA 证书验证，则可能会出现此错误。您必须删除此身份证书，然后使用正确的中间或根 CA 证书重新验证身份。请与您的第三方供应商联系以验证您收到的 CA 证书是否正确。
- Certificate does not contain general purpose public key当您尝试将身份证书安装到错误的信任点时，可能会出现此错误。这是因为您尝试安装无效的身份证书，或者与信任点关联的密钥对不匹配身份证书中包含的公钥。请使用 **show crypto ca certificates** *trustpointname* 命令以验证您是否将身份证书安装到正确的信任点。请查找以 **Associated Trustpoints** 开头的行：如果列出了错误的信任点，则使用本文档中所述的过程删除并重新安装适当的信任点，并验证密钥对自生成 CSR 以来是否未发生过更改。
- **错误消息**：**%PIX|ASA-3-717023 SSL失败设置信任点[trustpoint name]的设备证书**当为给定信任点设置设备证书以对 SSL 连接进行身份验证时，如果发生故障，则会显示此消息。当 SSL 连接恢复正常时，会尝试设置将要使用的设备证书。如果发生故障，则会记录一条错误消息，其中包括将用于加载设备证书的已配置信任点以及发生故障的原因。*信任点名称—SSL 未能设置设备证书的信任点名称。***建议操作**：解决所报告的故障原因指出的问题。确保指定的信任点已注册并具有设备证书。确保设备证书有效。重新注册信任点（如果需要）。

相关信息

- 如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书
- 安全产品售后通知
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems