

ASA 7.x手動安裝第三方供應商證書以用於WebVPN配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[步驟1.檢驗日期、時間和時區值是否準確](#)

[步驟2.生成RSA金鑰對](#)

[步驟3.建立信任點](#)

[步驟4.生成證書註冊](#)

[步驟5.驗證信任點](#)

[步驟6.安裝證書](#)

[步驟7.配置WebVPN以使用新安裝的證書](#)

[驗證](#)

[替換來自ASA的自簽名證書](#)

[檢視安裝的證書](#)

[使用Web瀏覽器驗證WebVPN的安裝證書](#)

[更新SSL證書的步驟](#)

[指令](#)

[疑難排解](#)

[相關資訊](#)

簡介

此配置示例描述如何在ASA上手動安裝第三方供應商數位證書以用於WebVPN。本示例中使用的是Verisign試用證書。每個步驟都包含ASDM應用程式過程和CLI示例。

必要條件

需求

本文檔要求您有權訪問證書頒發機構(CA)進行證書註冊。受支援的第三方CA供應商包括Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA和VeriSign。

採用元件

本文使用的是運行軟體版本7.2(1)和ASDM版本5.2(1)的ASA 5510。但是，本文檔中的過程適用於任何運行7.x且帶有任何相容ASDM版本的ASA裝置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

設定

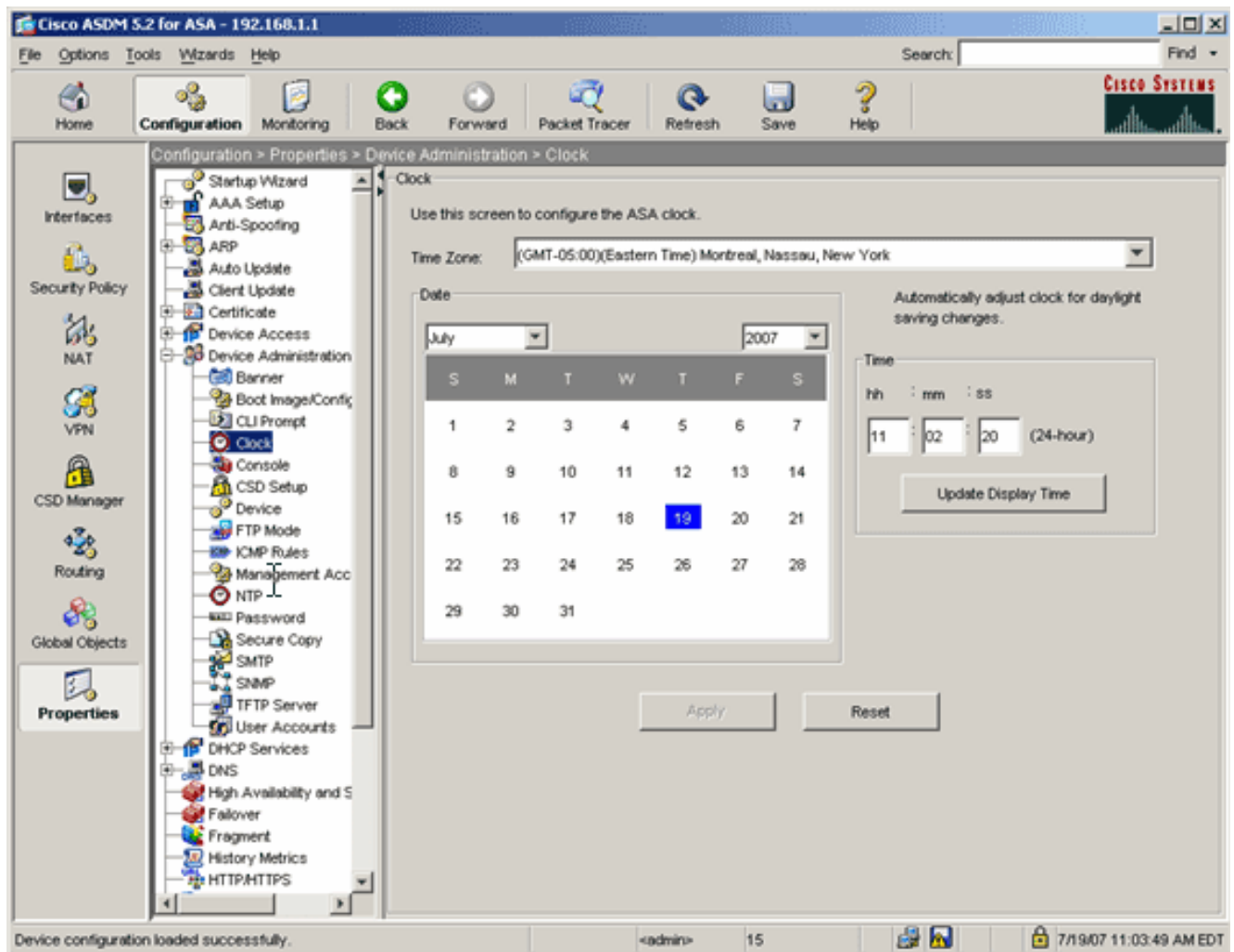
要在PIX/ASA上安裝第三方供應商數位證書，請完成以下步驟：

1. [驗證日期、時間和時區值是否準確。](#)
2. [生成RSA金鑰對。](#)
3. [建立信任點。](#)
4. [生成證書註冊。](#)
5. [驗證信任點。](#)
6. [安裝證書。](#)
7. [配置WebVPN以使用新安裝的證書。](#)

步驟1.檢驗日期、時間和時區值是否準確

ASDM過程

1. 按一下配置，然後按一下屬性。
2. 展開Device Administration，然後選擇Clock。
3. 驗證列出的資訊是否準確。Date、Time和Time Zone的值必須準確無誤，才能進行正確的證書驗證。



命令列示例

```
ciscoasa
```

```
ciscoasa#show clock
```

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

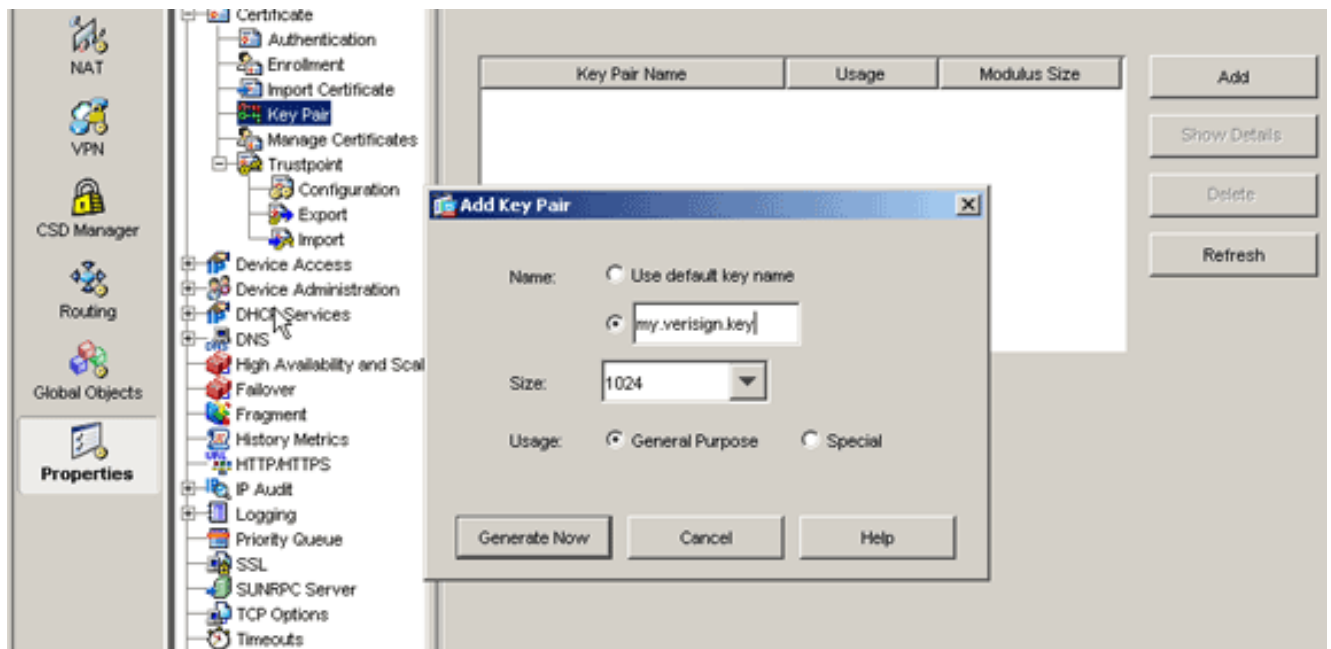
```
ciscoasa
```

步驟2.生成RSA金鑰對

生成的RSA公鑰與ASA的身份資訊結合起來形成PKCS#10證書請求。您應該使用為其建立金鑰對的信任點明確標識金鑰名稱。

ASDM過程

1. 按一下**Configuration**，然後按一下**Properties**。
2. 展開**Certificate**，然後選擇**Key Pair**。
3. 按一下「**Add**」。



4. 輸入金鑰名稱，選擇模數大小，然後選擇使用型別。附註：建議的金鑰對大小為1024。
5. 按一下「Generate」。您建立的金鑰對應該列在「金鑰對名稱」列中。

命令列示例

```

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)#

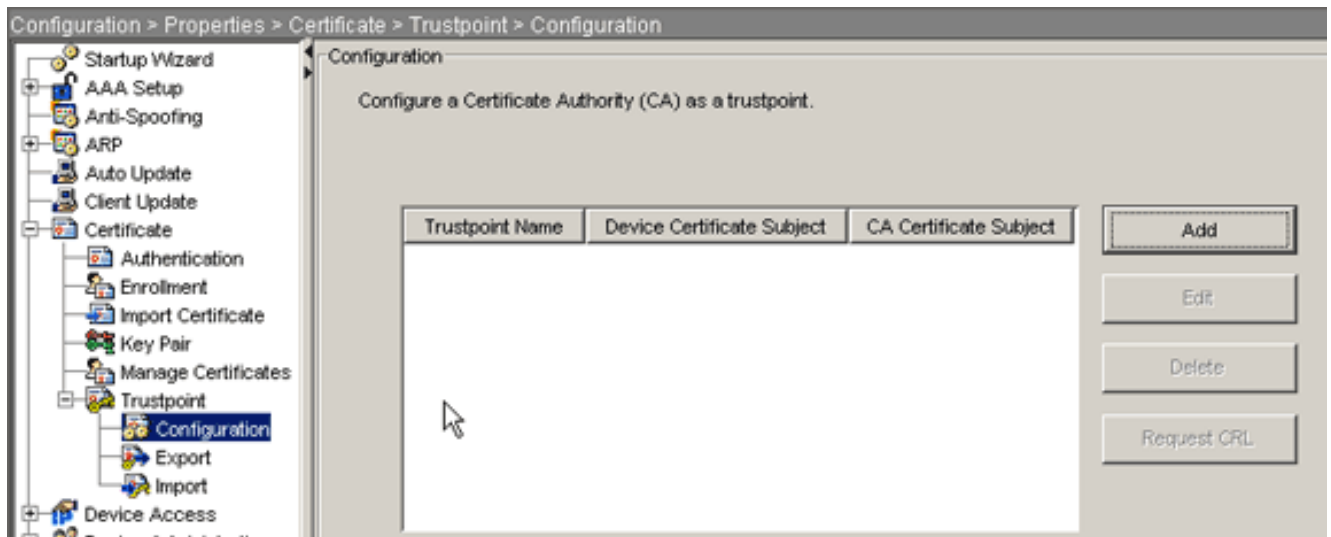
```

步驟3.建立信任點

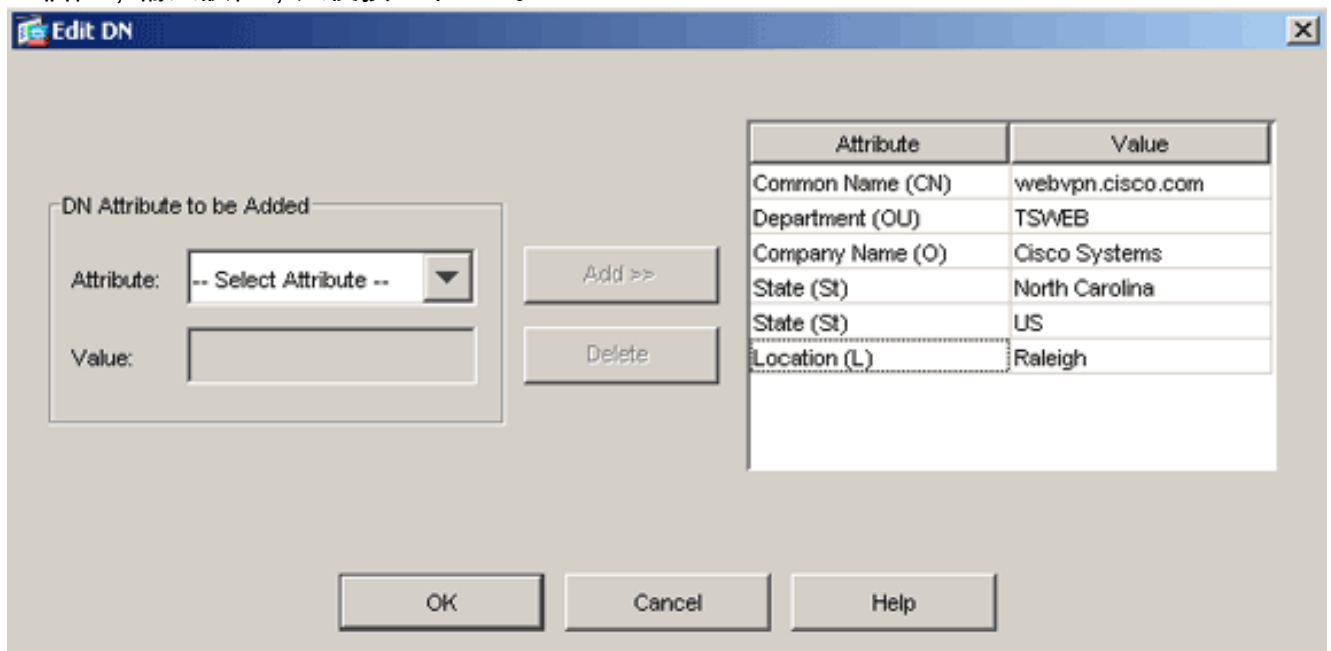
需要信任點來宣告您的ASA將使用的證書頒發機構(CA)。

ASDM過程

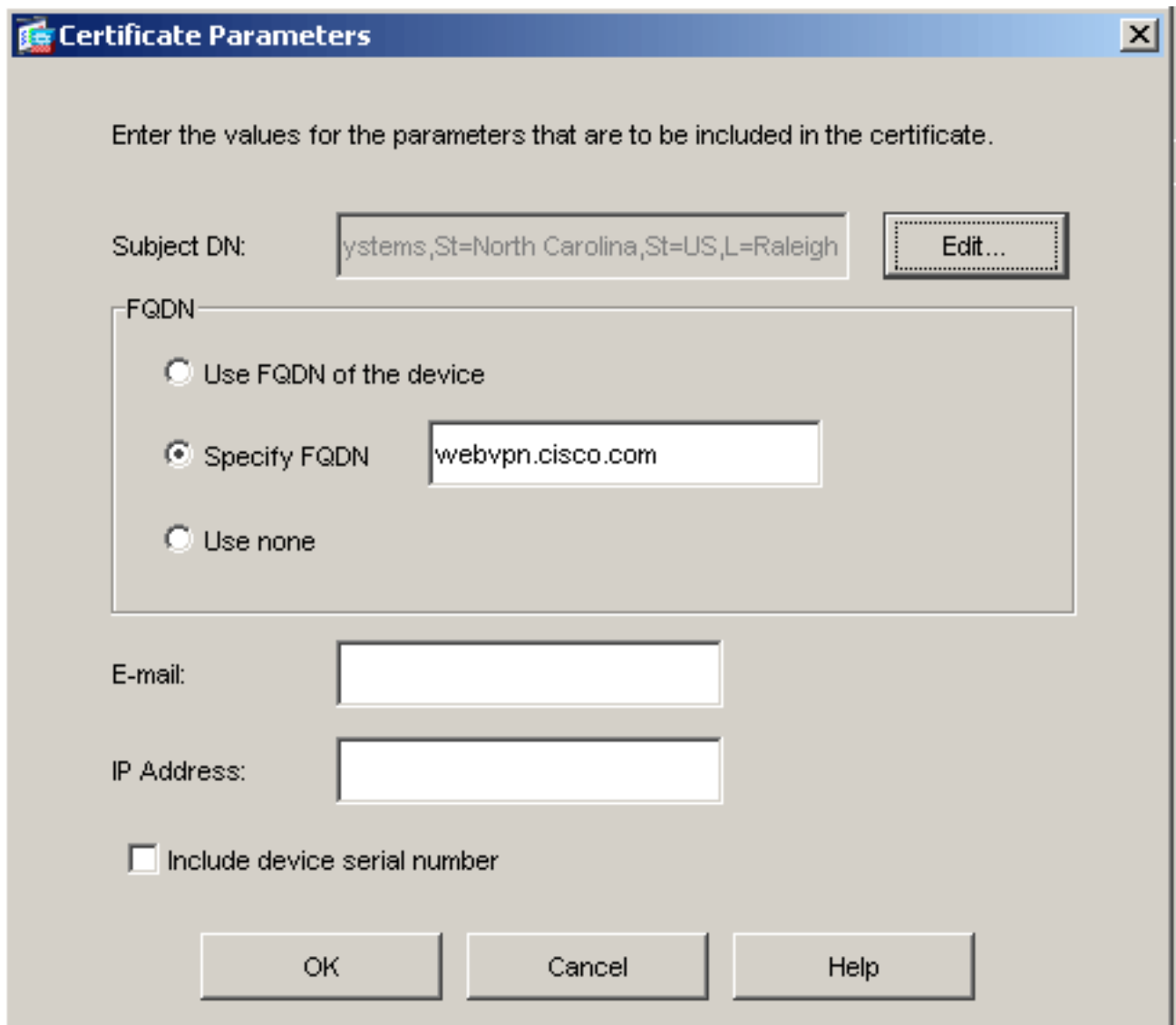
1. 按一下Configuration，然後按一下Properties。
2. 展開Certificate，然後展開Trustpoint。
3. 選擇Configuration，然後點選Add。



4. 配置以下值：**信任點名**:信任點名稱應與預期用途相關。(此示例使用*my.verisign.trustpoint*。)
金鑰對:選擇[步驟2](#)中生成的金鑰對。(i.e. *my.verisign.key*)
5. 確保選中「**手動註冊**」。
6. 按一下「**Certificate Parameters**」。系統將顯示Certificate Parameters對話方塊。
7. 按一下**Edit**，然後配置下表中列出的屬性：若要設定這些值，請從「屬性」下拉式清單中選擇一個值，輸入該值，然後按一下**Add**。



8. 新增適當的值後，按一下**確定**。
9. 在「證書引數」對話方塊中，在「指定FQDN」欄位中輸入FQDN。此值應與用於公用名 (CN)的FQDN相同。



The image shows a Windows-style dialog box titled "Certificate Parameters". At the top, it says "Enter the values for the parameters that are to be included in the certificate." Below this, there are several input fields and options:

- Subject DN:** A text box containing "ystems,St=North Carolina,St=US,L=Raleigh" and an "Edit..." button to its right.
- FQDN:** A section with three radio button options:
 - Use FQDN of the device
 - Specify FQDN: A text box containing "webvpn.cisco.com"
 - Use none
- E-mail:** An empty text box.
- IP Address:** An empty text box.
- Include device serial number

At the bottom, there are three buttons: "OK", "Cancel", and "Help".

10. 按一下「OK」(確定)。
11. 驗證是否選擇了正確的金鑰對，然後按一下**Use manual enrollment**單選按鈕。
12. 按一下「OK」，然後按一下「Apply」。

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:

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)

命令列示例

```

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=webvpn.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:).

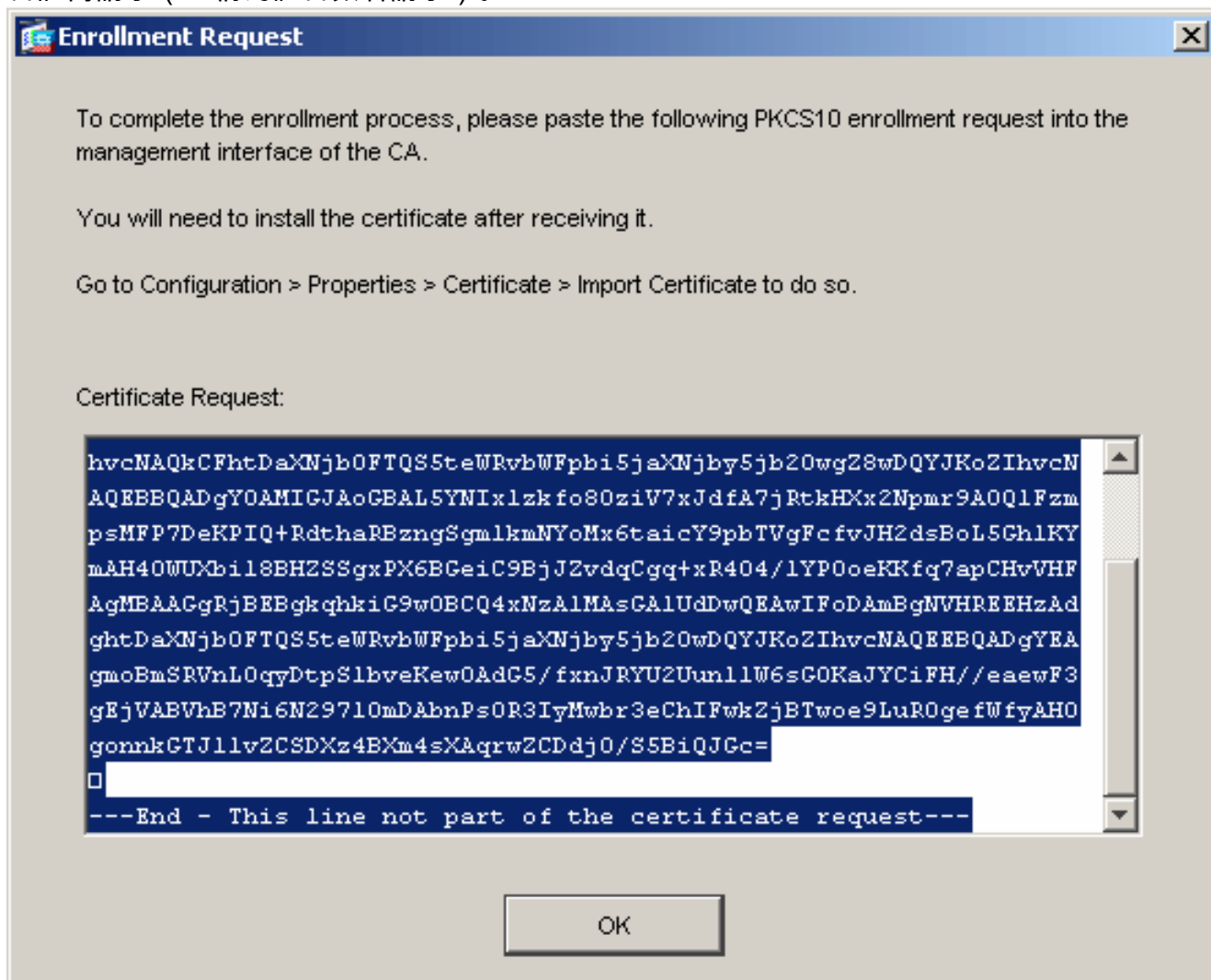
```

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

步驟4.生成證書註冊

ASDM過程

1. 按一下**Configuration**，然後按一下**Properties**。
2. 展開**Certificate**，然後選擇**Enrollment**。
3. 驗證是否已選中**步驟3**中建立的信任點，然後按一下**Enroll**。出現一個對話方塊，其中列出了證書註冊請求（也稱為證書簽名請求）。



4. 將PKCS#10註冊請求複製到文本檔案，然後將CSR提交給相應的第三方供應商。在第三方供應商收到CSR後，他們應該發出身份證書以進行安裝。

命令列示例

裝置名稱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

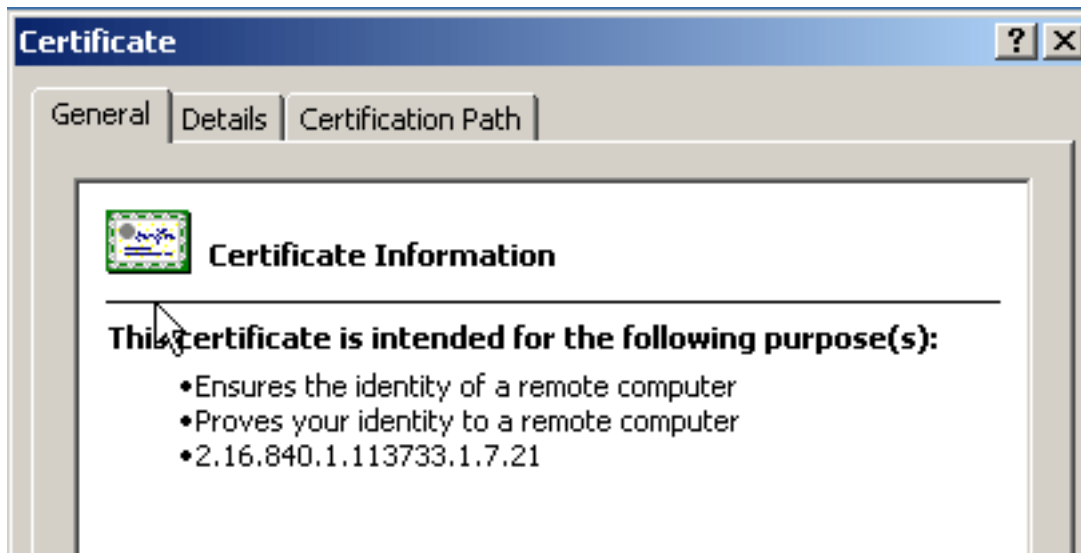
! Displays the PKCS#10 enrollment request to the
terminal. ! You will need to copy this from the terminal
to a text ! file or web text field to submit to the 3rd
party CA. Certificate Request follows:
MIICHjCCAYcCAQAwgAAXEDAOBgNVBACTB1JhbGVpZ2gxZzAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECXMVFVNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQpynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRip9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5Q1Kx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#
```

步驟5. 驗證信任點

收到來自第三方供應商的身份證書後，您可以繼續執行此步驟。

ASDM過程

1. 將身份證書儲存到本地電腦。
2. 如果您獲得的base64編碼證書不是作為檔案提供的，則必須複製base64消息並將其貼上到文本檔案中。
3. 將檔案重新命名為.cer副檔名。注意：使用.cer副檔名重新命名檔案後，檔案圖示應顯示為證書。
4. 按兩下證書檔案。出現「Certificate (證書)」對話方塊。

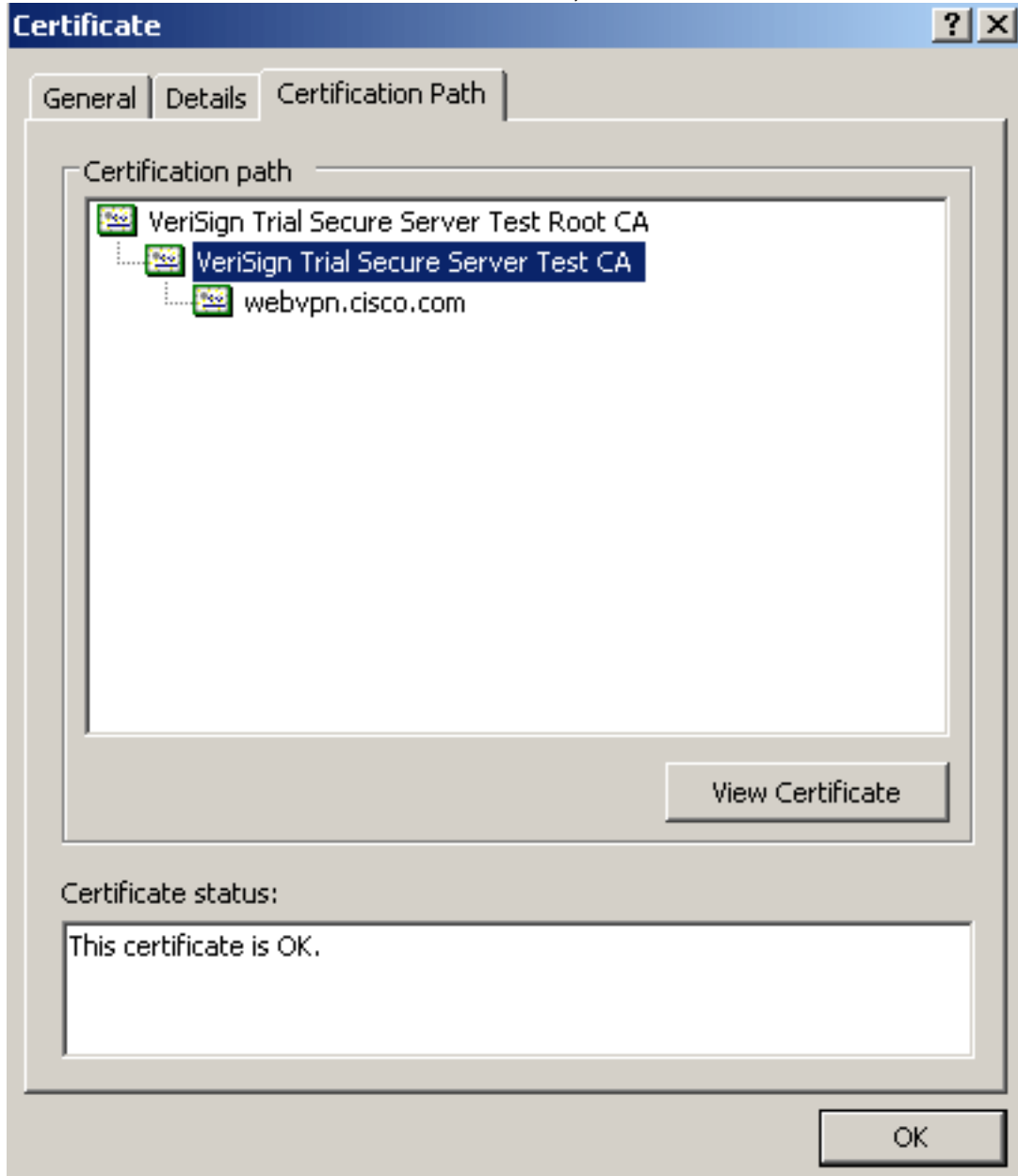


註：如果「

General」頁籤中顯示「Windows does not have enough information to verify this certificate」消息，則必須先獲取第三方供應商根CA或中間CA證書，然後才能繼續此過程。請聯絡您的第三方供應商或CA管理員，以獲取頒發的根CA或中間CA證書。

5. 按一下**Certificate Path**頁籤。

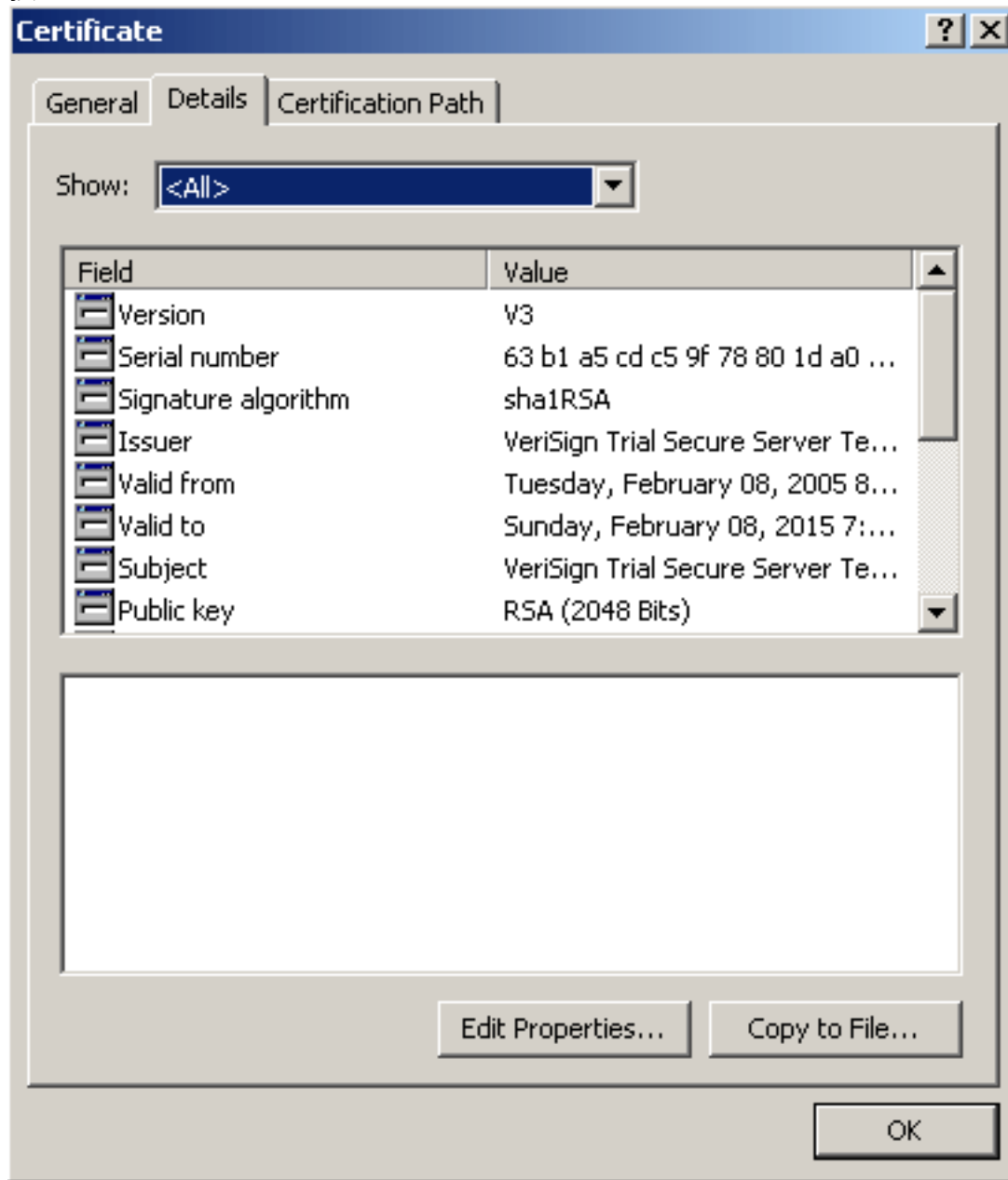
6. 按一下位於已頒發身份證書上方的CA證書，然後按一下**View Certificate**。



將顯示中間CA證

書的詳細資訊。**警告**：不要在此步驟中安裝身份（裝置）證書。在此步驟中只新增根、從根或 CA證書。身份（裝置）證書安裝在**步驟6**中。

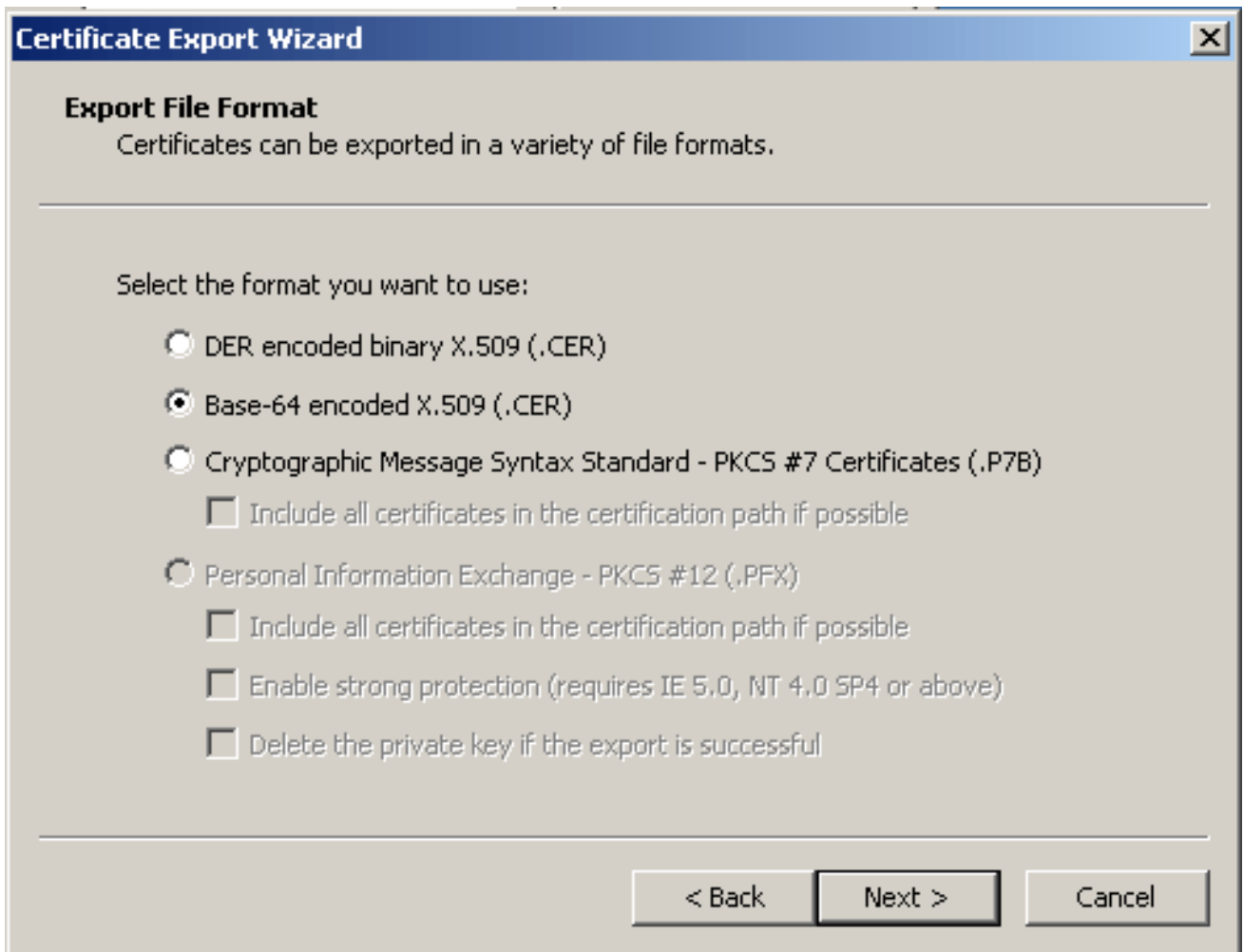
7. 按一下「**Details**」。



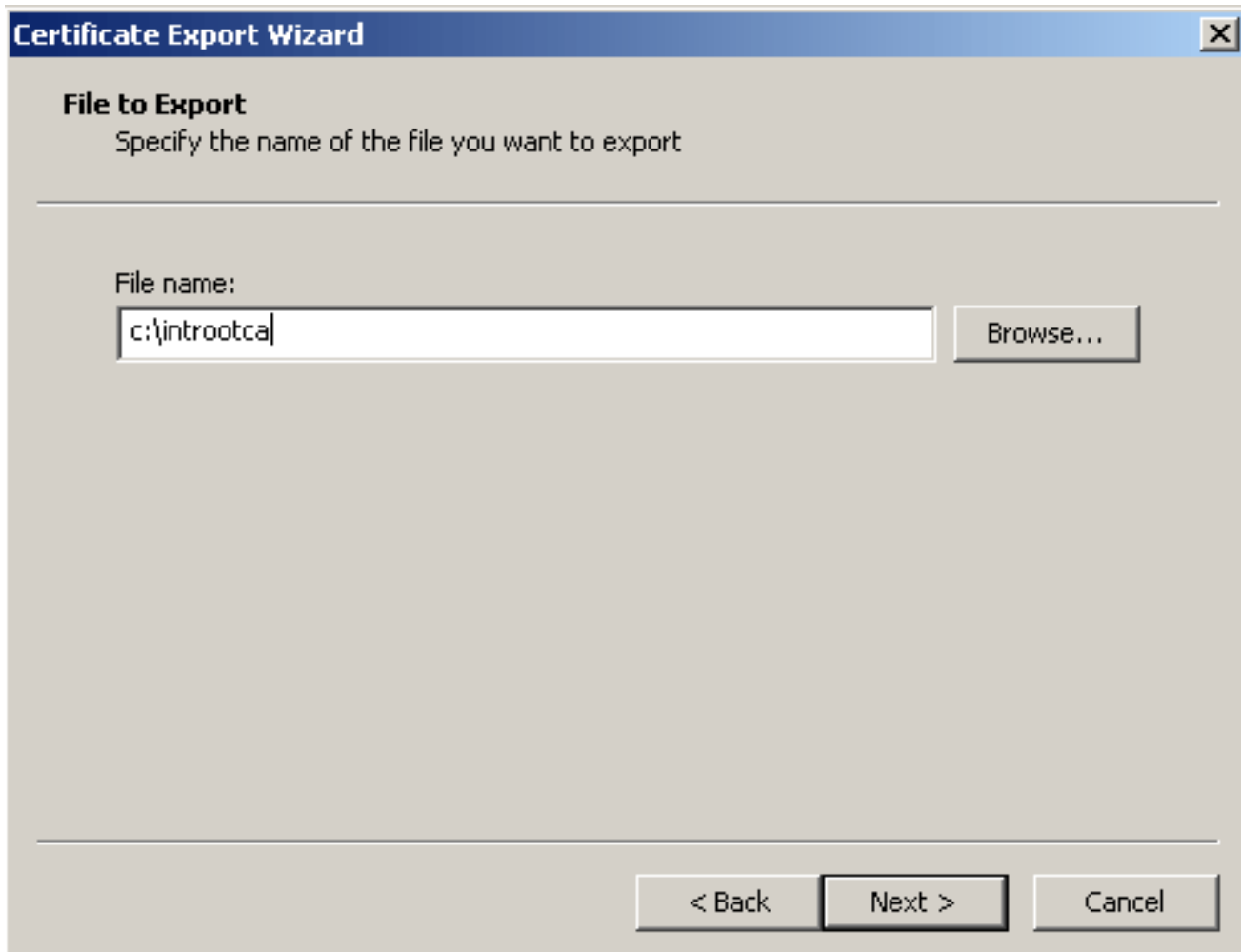
8. 按一下「**Copy to File**」。

9. 在「Certificate Export Wizard (證書匯出嚮導)」中，按一下「**Next (下一步)**」。

10. 在「匯出檔案格式」對話方塊中，按一下**Base-64 encoded X.509(.CER)**單選按鈕，然後按一下**下一步**。



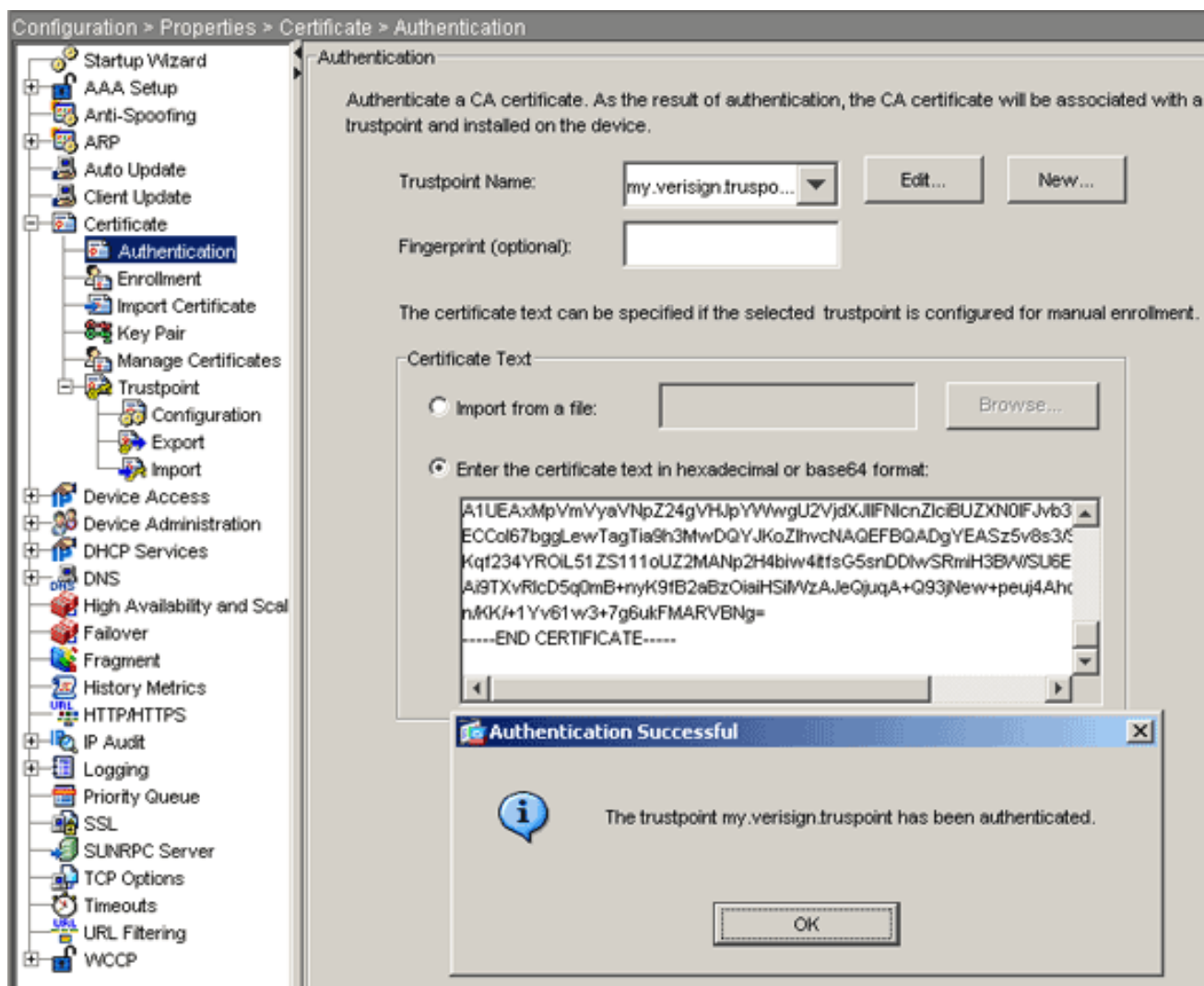
11. 輸入要儲存CA證書的檔名和位置。
12. 按一下**Next**，然後按一下**Finish**。



13. 在「匯出成功」對話方塊中按一下**確定**。
14. 瀏覽到儲存CA證書的位置。
15. 使用文字編輯器（例如記事本）開啟檔案。（按一下右鍵該檔案，然後選擇「傳送到」>「記事本」。）Base64編碼的訊息應該顯示與此圖中的憑證類似：
：

```
-----BEGIN CERTIFICATE-----
MIIFSjCCBDKgAwIBAgIQCECQ47aTdj6BtrI60/vt6zANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMXFZAVBgnVBAoTDIzIcm1TawduLCBjbmMuMTAwLgYDVQQQL
EydGb3IgvGVzdCBQdXJwb3NlcyBpbmx5LjAgTm8gYXNzdXJhbmNlcy4xQjBAGNV
BASTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vy3Bz
L3Rlc3RjYSAoYykwNTetMCSGA1UEAxMkVmvyavNpZ24gVHJpYXVwU2VjdxJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDg0MDIzNTk1OVowgZ4x
CZAJBgNVBAYTA1VTMRcwFQYDVQQIEW50b3J0aCBDYXJvbG1uYUwTEWMBQGA1UEChQN
Q2IzY28gU3IzdGvtcZEOMAwGA1UECxQVFNXRUIxojA4BgNVBASUMVRlcm1zIG9m
IHVzZSBhdCB3d3cudmvyaxNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUXEjAQBGNV
BAMUCWNSawVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA1v9Ahzsm
SZiUwosov+yL/SMZULWkigvgwX1avJ4UwqpuG9TgaIEn9wFvrZmJd0T/ucJW6k1A
TjajzxSocuvAKUj7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimmQp
RWMazevoFaiiy+5oG7XAiwCPY4677K3INFECAWEAAaOCAdcwggHTMAkGA1UdEwQC
MAAwCwYDVR0PBAQDAgwgMEMGA1UdHwQ8MDowOKA2oDSGMMh0dHA6Ly9TVlJTZWNI
cmUtY3JzLnZlcm1zawduLmNvbS9TVlJUCm1hbDIwMDUuY3JSMEOGA1UdIARDMEEW
PwYKYIZIAyB4RQEHTAXMC8GCCSGAQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2ln
bi5jb20vy3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQCDAQYIKwYBBQUHAWIw
HwYDVR0jBBgwFoAUZikOgeAXwd0qf6tGxTYCBnAnhIoweAYIKwYBBQUHAQEEdBq
MCQGCSGAQUFBzABhhodHRwoi8vb2Nzcc52ZXJpc2lnbi5jb20wQGYIKwYBBQUH
MAKGNmh0dHA6Ly9TVlJTZWNIcmUtYw1hLnZlcm1zawduLmNvbS9TVlJUCm1hbDIw
MDUuYw1hLmNlcm1zBuBgggrBgEFBQCBDARiMGChxqBcMFowWDBWfGlpbwFnZS9nawYw
ITAFMACGBSSoAwIaBBRLa7ko1gYMU9BSOJsprEsHiyEFGDAmFiRodHRwoi8vbG9n
by52ZXJpc2lnbi5jb20vdnnsb2dvMS5nawYwDQYJKoZIhvcNAQEFBQADggEBAC4k
abswgoogAntm4lrJhv8TSGsjdPpospLseBFxuLEzJlTHGprcf0sALrgbIFEL4b9q
l/EajjdtEeyTgIorIC1awwwx+RHCCtqIr1zf0vfUD0DNZ6949sM2agAmzrRsBy63
Lb1/3+jz8skIAkizP79pmqMEECZ+cum10rk631c46yBCsJMzVbG6sZlNSI80RRwK
hAKdsfufvsirHc8c9nJdOEC0905izUTRE854jv1XzZjioJ51FbcmCox/ub7zv3zC
Ftm412+TgfyZ3z7wCENulvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpxy5l7TLkyja
idT1FmBvf02qaZS6S40=
-----END CERTIFICATE-----
```

16. 在ASDM中，按一下**Configuration**，然後按一下**Properties**。
17. 展開**Certificate**，然後選擇**Authentication**。
18. 按一下**Enter the certificate text in hexadecimal or base64 format**單選按鈕。
19. 從文本編輯器將base64格式的CA證書貼上到文本區域。
20. 按一下「**Authenticate**」。



21. 按一下「OK」(確定)。

命令列示例

```

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-----
MIIEwDCCBCmgAwIBAgIQY7G1zcWfeIAdoGNs+XVGezANBgkqhkiG9w0B
AQUFADCB
jDELMAkGA1UEBhmCVVMxZAVBgNVBAoTD1ZlcmlTaWduLCBjb250aWwv
LgYDVQQL
EydG93IGVGVzdCBQdXJwb3N1cyBpbm51LiAgTm8gYXNzdXJhbmN1cy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFSIFN1Y3VyZSBTZXJ2ZXIgaGVhZG93ZD90
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowGcsxCzAJBgNVBAYT
A1VTMRcw
FQYDVQQKEw5WZXJpU21nbW5jLjEwMC4GA1UECzMmRm9yIFRlc3Qg
UHVycG9z
ZXMGt25seS4gIE5vIGFzc3VyYW5jZXMUMUwQAYDVQQLEz1UZXR1cm91
ZiB1c2Ug
YXQgHR0cHM6Ly93d3cuZmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFSIFN1Y3VyZSBTZXJ2ZXIgaGVhZG93ZD90

```

```
QTCCASIW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxx2EQJdnDXuTw0+4t1qj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJcK4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwgggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEwJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
cHMvdGVzdGhLzAObG9vNHQ8BAf8EBAMCAQYwEYJYIZIAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBRRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGN
oYGSPIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAstJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICB0byBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFN1cnZlcmlBUZXN0IFJv
b3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY2l
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDD1wSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaIHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN
n/KK/+1Yv61w3+7g6ukFMARVBNG=
-----END CERTIFICATE-----
quit
```

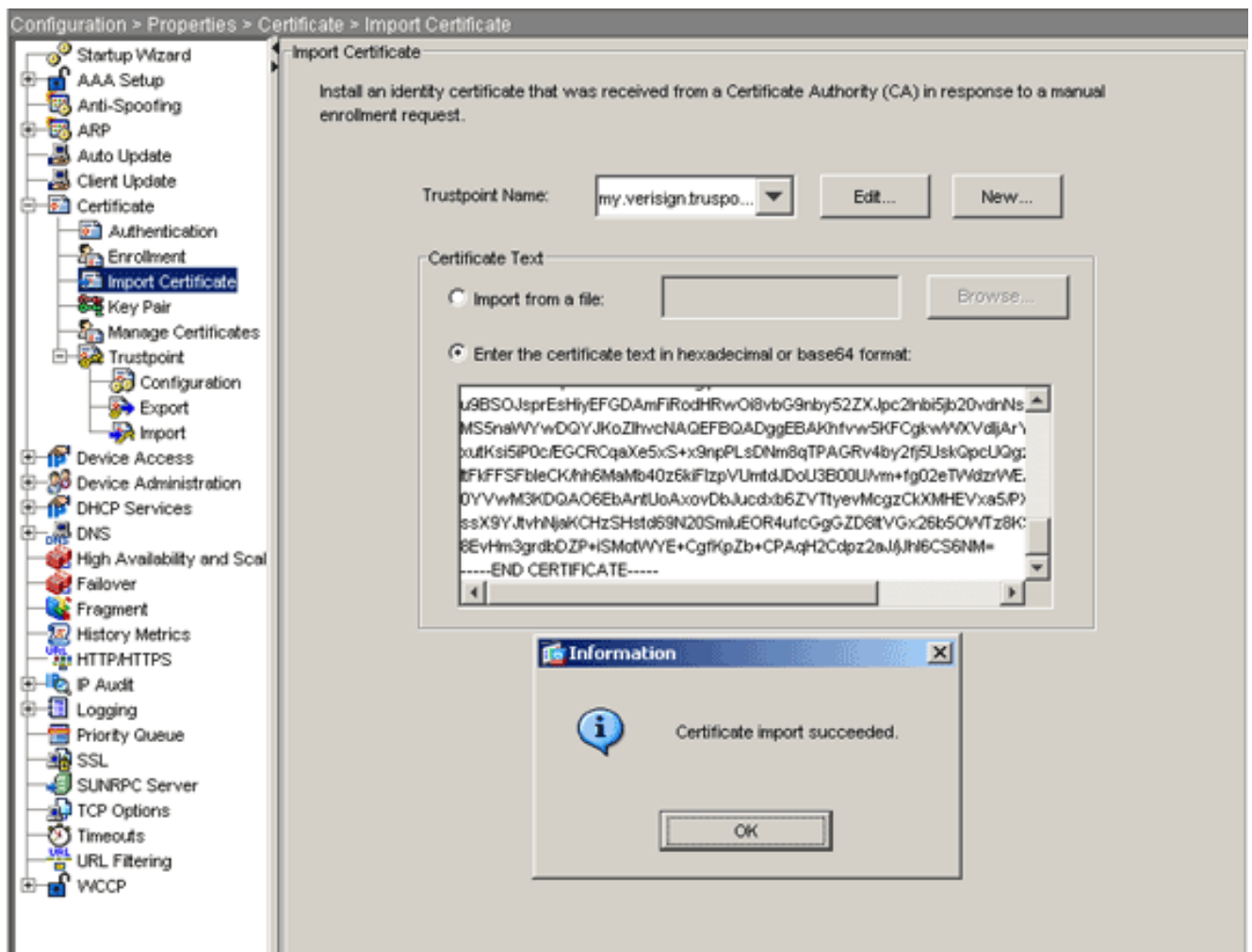
```
! Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
8de989db 7fcc5e3b fdde2c42 0813ef43 Do you accept this
certificate? [yes/no]: yes Trustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non self-signed certificate. Trustpoint CA certificate
accepted. % Certificate successfully imported
ciscoasa(config)#
```

步驟6. 安裝證書

ASDM過程

使用第三方供應商提供的身份證書執行以下步驟：

1. 按一下 **Configuration**，然後按一下 **Properties**。
2. 展開 **Certificate**，然後選擇 **Import Certificate**。
3. 按一下 **Enter the certificate text in hexadecimal or base64 format** 單選按鈕，然後將 base64 身份證書貼上到文本欄位中。



4. 按一下Import，然後按一下OK。

命令列示例

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
yzELMAkGA1UEBhMCVVMxFTZAVBgNVBAoTDlZlcm1TaWduLCBjb20vY3Bz
LgYDVQQL
EydgB3IgvGVzZCBQdXJwb3NlcYBPbm5LiAgTm8gYXNzdXJhbmNlcY4x
QjBAbgNV
BAStOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCSGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTA1VTMRcwFQYDVQIEw5OjB3J0aCBDYXJvbGluYTEQM4G
A1UEBxQH
UmFsZWlnaDEwBQGA1UEChQzY28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUlx
```

```

OjA4BgNVBAsUMVR1cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZKN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNlMS5jaXNjby5jb20w
gZ8wDQYJ
KoZlHvcNAQEBBQADgY0AMIGJAoGBAL56EvorHH1sIB/VRKaR1JeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxs1Egry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjaAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJ1LWNyC52ZXJpc2ln
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBGNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZKN0
Y2EwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJ1
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFGwVhYJaW1hZ2UvZ2lmMCEwHZAHBgUrDgMCGGQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAAnym4GVThPIyL/9y1DBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIddMtMGotCavRHD9T12tvwgrBock/v/
54o021kB
SmLzVV7crlYJEUhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARafNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
quit

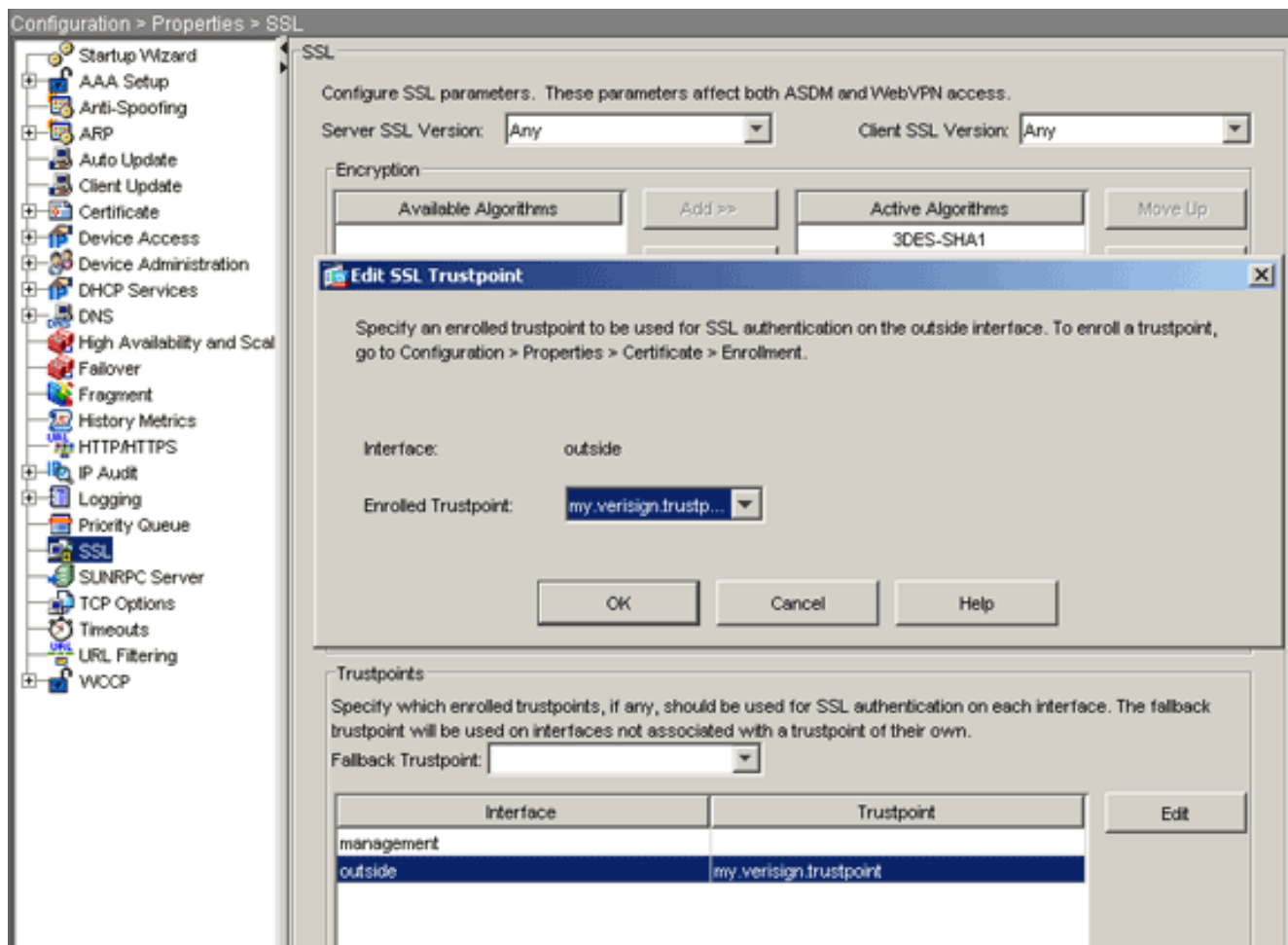
INFO: Certificate successfully imported
ciscoasa(config)#

```

步驟7.配置WebVPN以使用新安裝的證書

ASDM過程

1. 按一下「Configuration」，按一下「Properties」，然後選擇「SSL」。
2. 在Trustpoints區域中，選擇將用於終止WebVPN會話的介面。（此示例使用外部介面。）
3. 按一下「Edit」。系統將顯示Edit SSL Trustpoint對話方塊。



4. 從Registered Trustpoint下拉選單中，選擇您在步驟3中建立的信任點。

5. 按一下「OK」，然後按一下「Apply」。

現在，您的新證書應該用於終止於指定介面的所有WebVPN會話。有關如何驗證成功安裝的資訊，請參閱本文檔中的驗證部分。

命令列示例

```

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.

```

驗證

本節介紹如何確認第三方供應商證書安裝成功。

替換來自ASA的自簽名證書

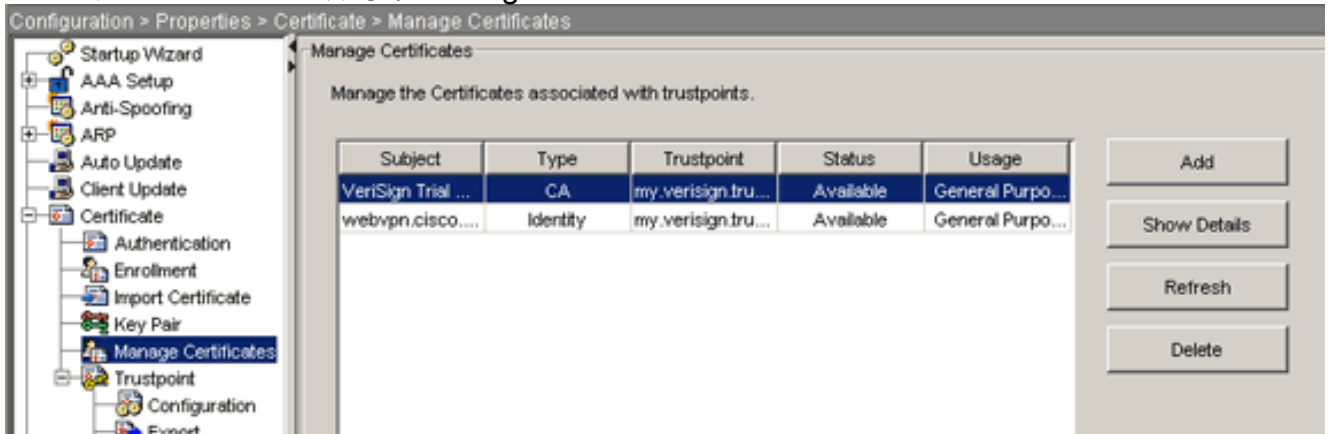
本節介紹如何從ASA替換已安裝的自簽名證書。

1. 向Verisign發出證書簽名請求。從Verisign收到請求的證書後，可以直接在同一信任點下安裝。
2. 鍵入以下命令：`crypto ca enroll Verisign`系統將提示您回答問題。
3. 對於終端顯示證書請求，輸入`yes`，並將輸出傳送到Verisign。
4. 一旦他們向您提供新證書，請鍵入以下命令：`crypto ca import Verisign certificate`

檢視安裝的證書

ASDM過程

1. 按一下**Configuration**，然後按一下**Properties**。
2. 展開**Certificate**，然後選擇**Manage Certificates**。用於Trustpoint身份驗證的CA證書和第三方供應商頒發的身份證書應顯示在Manage Certificates區域中。



命令列示例

ciscoasa

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

! Displays all certificates installed on the ASA.

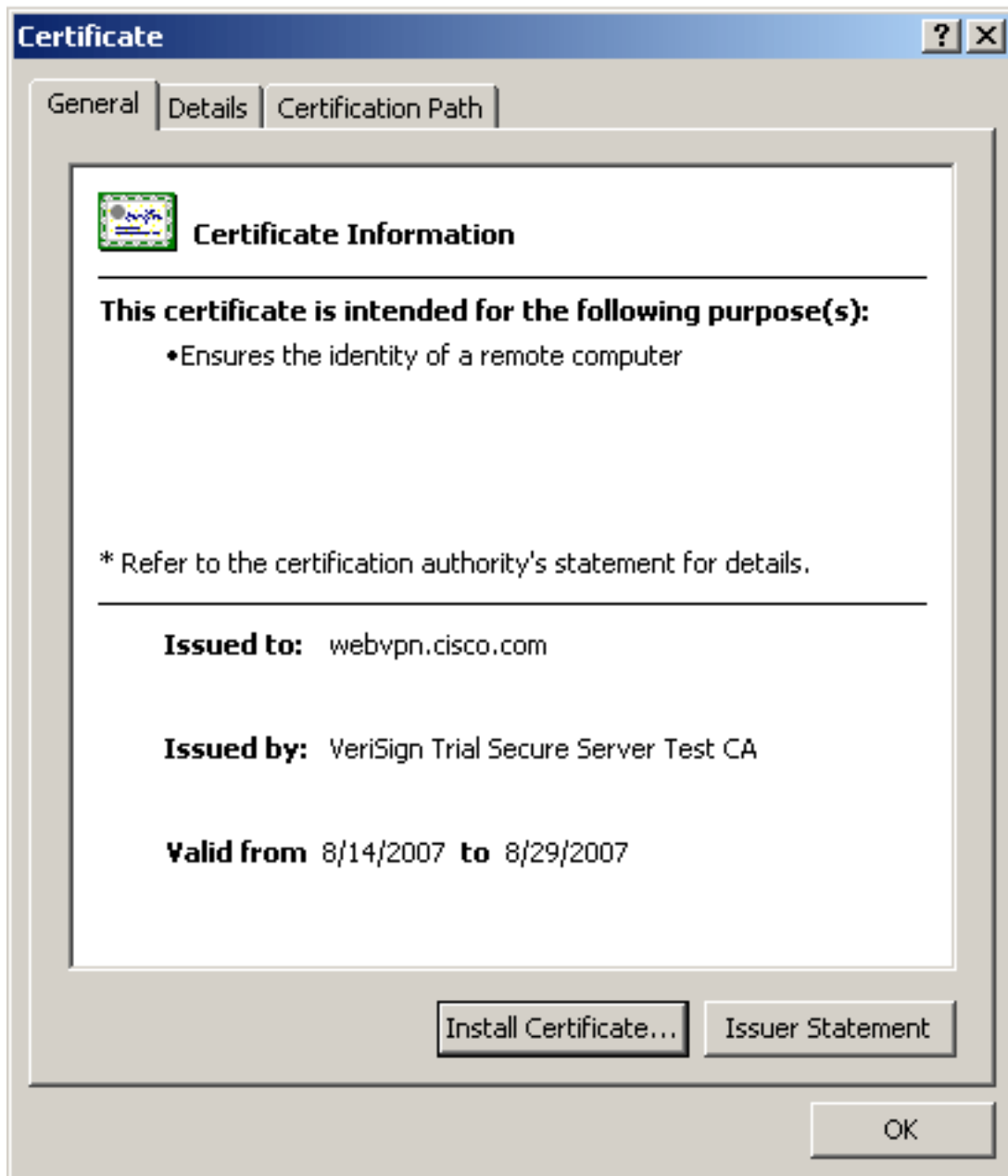
```
Certificate Status: Available Certificate Serial Number:
32cfe85eebbd2b5e1e30649fd266237d Certificate Usage:
General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test CA ou=Terms
of use at https://www.verisign.com/cps/testca (c)05
ou=For Test Purposes Only. 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 OSCP
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瀏覽器驗證WebVPN的安裝證書

若要確認WebVPN是否使用新憑證，請完成以下步驟：

1. 通過Web瀏覽器連線到WebVPN介面。使用https://以及您用來請求證書的FQDN(例如https://webvpn.cisco.com)。如果收到以下安全警報之一，請執行與該警報對應的過程：**安全證書的名稱無效或與站點名稱不匹配**驗證您使用正確的FQDN/CN以連線到ASA的WebVPN介面。必須使用您在請求身份證書時定義的FQDN/CN。您可以使用**show crypto ca certificates trustpointname**命令驗證證書FQDN/CN。**安全證書由您未選擇信任的公司頒發**.....完成以下步驟，將第三方廠商根憑證安裝到Web瀏覽器中：在「安全警報」對話方塊中，按一下**檢視證書**。在「證書」對話方塊中，按一下**證書路徑頁籤**。選擇位於您頒發的身份證書上方的CA證書，然後按一下**View Certificate**。按一下「**Install Certificate**」。在「證書安裝嚮導」對話方塊中，按一下**下一步**。選擇**Automatically select the certificate store based on the type of certificate**單選按鈕，按一下**Next**，然後按一下**Finish**。當您收到Install the certificate confirmation提示時，按一下**Yes**。在「匯入操作成功」提示符下，按一下**OK**，然後按一下**Yes**。**注意**：由於此示例使用Verisign試用證書，因此必須安裝Verisign試驗CA根證書，以避免使用者連線時出現驗證錯誤。
2. 按兩下WebVPN登入頁面右下角顯示的鎖定圖示。應顯示安裝的證書資訊。
3. 檢視內容，確認其與您的第三方供應商證書相匹配。



更新SSL證書的步驟

完成以下步驟即可續訂SSL憑證：

1. 選擇需要續訂的信任點。
2. 選擇**enroll**。出現以下消息：*如果再次成功註冊，則當前證書將替換為新證書。是否要繼續？*
3. 選擇**yes**。這會產生新的CSR。
4. 將CSR傳送到CA，然後在您傳回新ID憑證時將其匯入。
5. 刪除信任點並將其重新應用到外部介面。

指令

在ASA上，您可以在命令列中使用幾個show命令來驗證證書的狀態。

- **show crypto ca trustpoint** — 顯示已配置的信任點。
- **show crypto ca certificate** — 顯示系統上安裝的所有證書。
- **show crypto ca crls** — 顯示快取的證書吊銷清單(CRL)。

- `show crypto key mypubkey rsa` — 顯示所有生成的加密金鑰對。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

以下是您可能會遇到的一些可能錯誤：

- **%警告：未找到CA證書。**匯入的證書可能不是usable.INFO:已成功匯入證書CA證書未正確驗證。使用`show crypto ca certificate trustpointname`命令以驗證CA證書是否已安裝。尋找以CA憑證開頭的行。如果安裝了CA證書，請驗證它是否引用了正確的信任點。
- **錯誤：無法分析或驗證匯入的證書安裝身份證書並且沒有用關聯的信任點進行身份驗證的正確的中間或根CA證書時，**可能出現此錯誤。您必須移除並使用正確的中間CA或根CA證書重新進行身份驗證。請與您的第三方供應商聯絡，以驗證您是否收到了正確的CA證書。
- **證書不包含通用公鑰**當您嘗試將身份證書安裝到錯誤的信任點時，可能會發生此錯誤。您試圖安裝無效的身份證書，或者與信任點關聯的金鑰對與身份證書中包含的公鑰不匹配。使用`show crypto ca certificates trustpointname`命令以驗證您的身份證書是否已安裝到正確的信任點。查詢說明*Associated Trustpoints*:如果列出錯誤的信任點，請使用本文檔中介紹的過程以刪除並重新安裝到適當的信任點，同時驗證金鑰對自生成CSR以來是否未更改。
- **錯誤消息：%PIX|ASA-3-717023 SSL無法為信任點[trustpoint name]設定裝置證書**當您為給定信任點設定裝置證書以驗證SSL連線時，將顯示此消息。當SSL連線啟動時，將嘗試設定將使用的裝置證書。如果發生故障，則會記錄一條錯誤消息，其中包括用於載入裝置證書的已配置信任點和故障原因。*trustpoint name - SSL無法為其設定裝置證書的信任點的名稱*。**建議的操作**：解決故障報告原因所指示的問題。確保指定的信任點已註冊並具有裝置證書。確保裝置證書有效。如果需要，重新註冊信任點。

相關資訊

- [如何使用ASA上的ASDM從Microsoft Windows CA獲取數位證書](#)
- [安全產品現場通知](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)