

使用數位證書和Microsoft CA的ASA/PIX 8.x和VPN客戶端IPSec身份驗證配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[ASA配置](#)

[ASA配置摘要](#)

[VPN客戶端配置](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何手動在思科安全裝置(ASA/PIX)8.x以及VPN客戶端上安裝第三方供應商數位證書，以便使用Microsoft證書頒發機構(CA)伺服器驗證IPSec對等體。

必要條件

需求

本文檔要求您擁有證書註冊證書頒發機構的訪問許可權。支援的第三方CA供應商包括Baltimore、Cisco、Entrust、iPlanet/Netscape、Microsoft、RSA和VeriSign。

本文檔假設ASA/PIX中沒有預先存在的VPN配置。

注意：本文檔使用Microsoft Windows 2003伺服器作為方案的CA伺服器。

注意：有關如何將Windows 2003伺服器配置為CA的完整資訊，請參閱[在Windows伺服器上配置CA](#)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 5510(運行軟體版本8.0(2)和ASDM版本6.0(2))
- 運行軟體版本4.x及更高版本的VPN客戶端

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。

相關產品

ASA配置還可以與運行軟體版本8.x的Cisco 500系列PIX一起使用。

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。

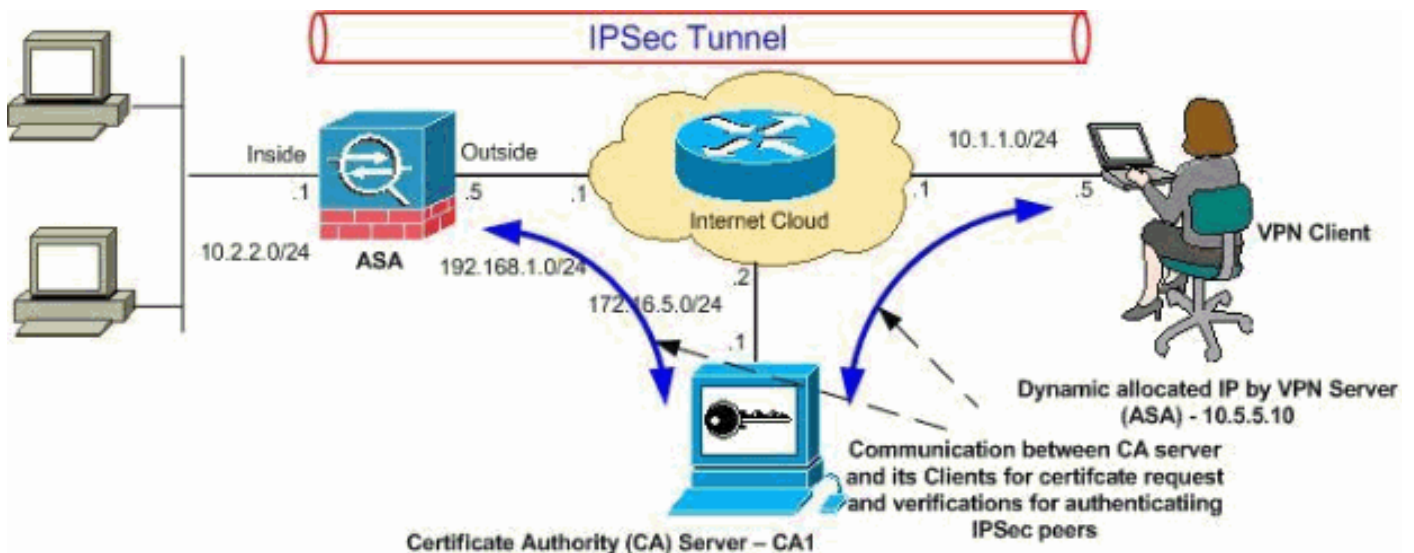
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅限[註冊](#)客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

組態

本檔案會使用以下設定：

- [ASA配置](#)
- [ASA配置摘要](#)

- [VPN客戶端配置](#)

ASA配置

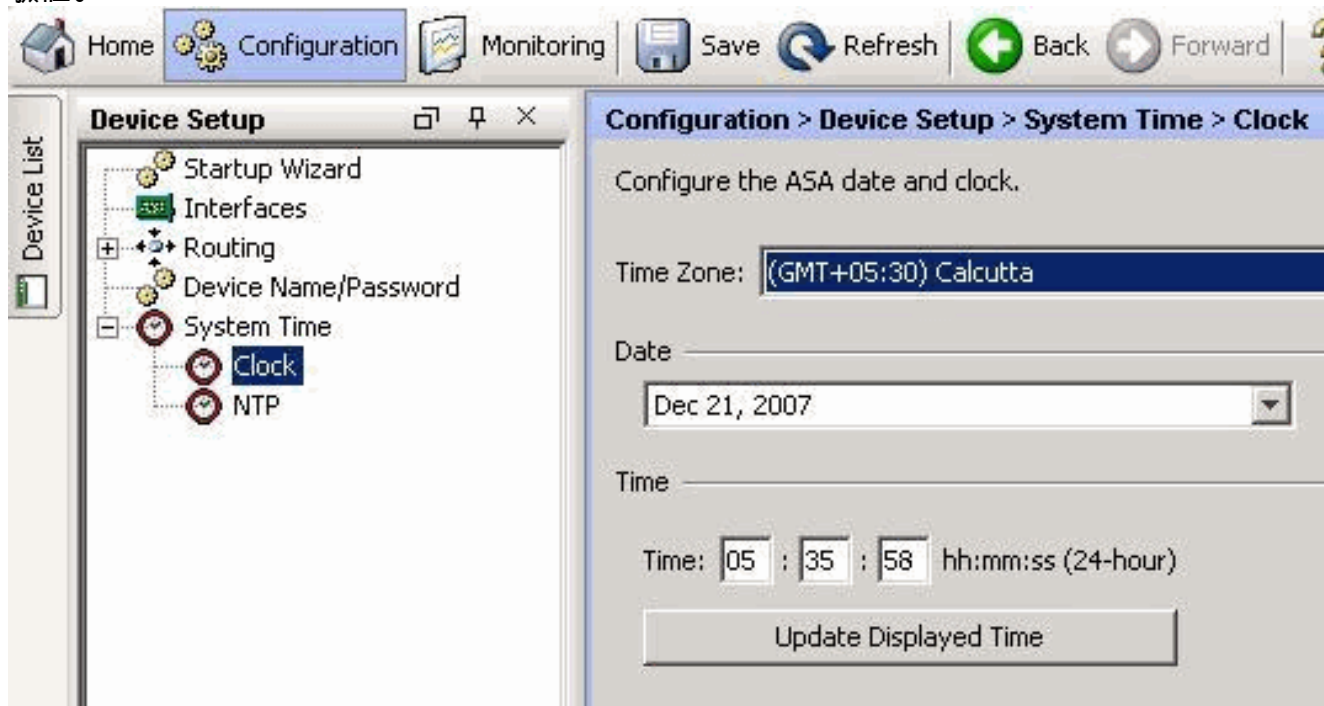
要在ASA上安裝第三方供應商數位證書，請完成以下步驟：

- [步驟1.檢驗日期、時間和時區值是否準確](#)
- [步驟2.生成證書簽名請求](#)
- [步驟3.驗證信任點](#)
- [步驟4.安裝證書](#)
- [步驟5.將遠端訪問VPN\(IPSec\)配置為使用新安裝的證書](#)

步驟1.檢驗日期、時間和時區值是否準確

ASDM過程

1. 按一下**Configuration**，然後按一下**Device Setup**。
2. 展開**System Time**，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  
05:37:37.904 UTC Fri Dec 21 2007
```

步驟2.生成證書簽名請求

需要證書簽名請求(CSR)，第三方CA才能頒發身份證書。CSR包含您的ASA的可分辨名稱(DN)字串以及ASA生成的公鑰。ASA使用生成的私鑰對CSR進行數位簽章。

ASDM過程

1. 按一下**Configuration**，然後按一下**Device Management**。
2. 展開**Certificate Management**，然後選擇**Identity Certificates**。
3. 按一下「**Add**」。

Add Identity Certificate

Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

4. 按一下**Add a new identity certificate**單選按鈕。
5. 對於金鑰對，按一下**New**。

Add Key Pair

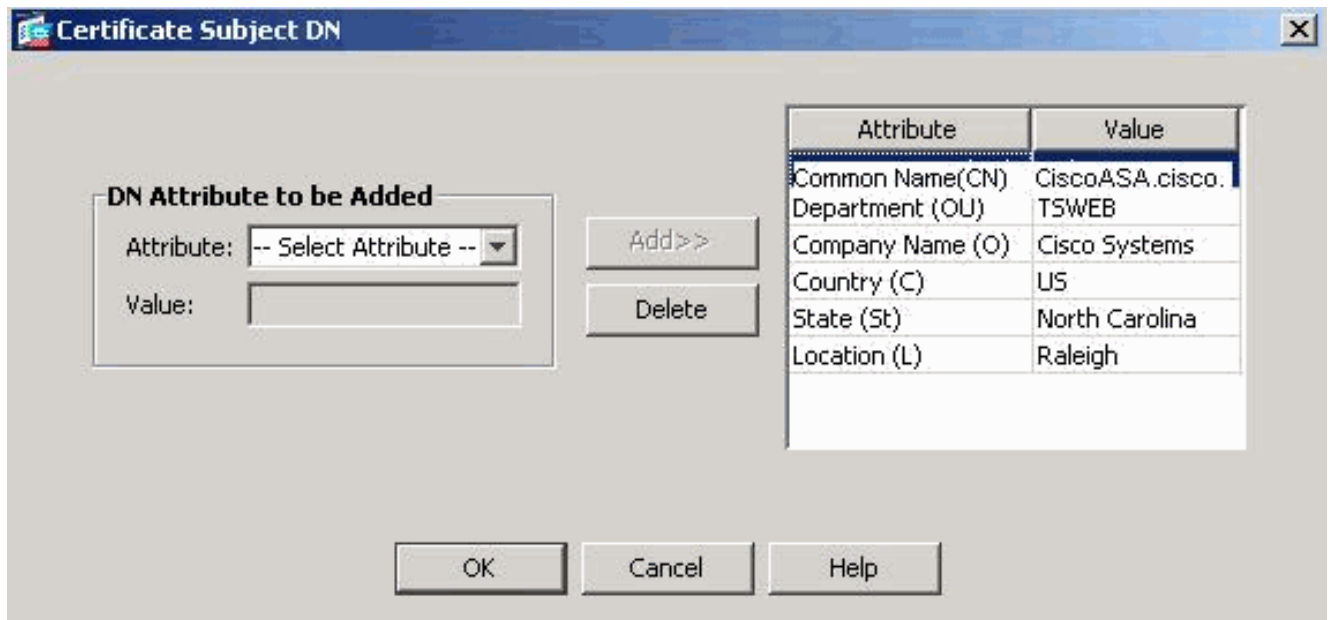
Name: Use default key pair name

Enter new key pair name:

Size:

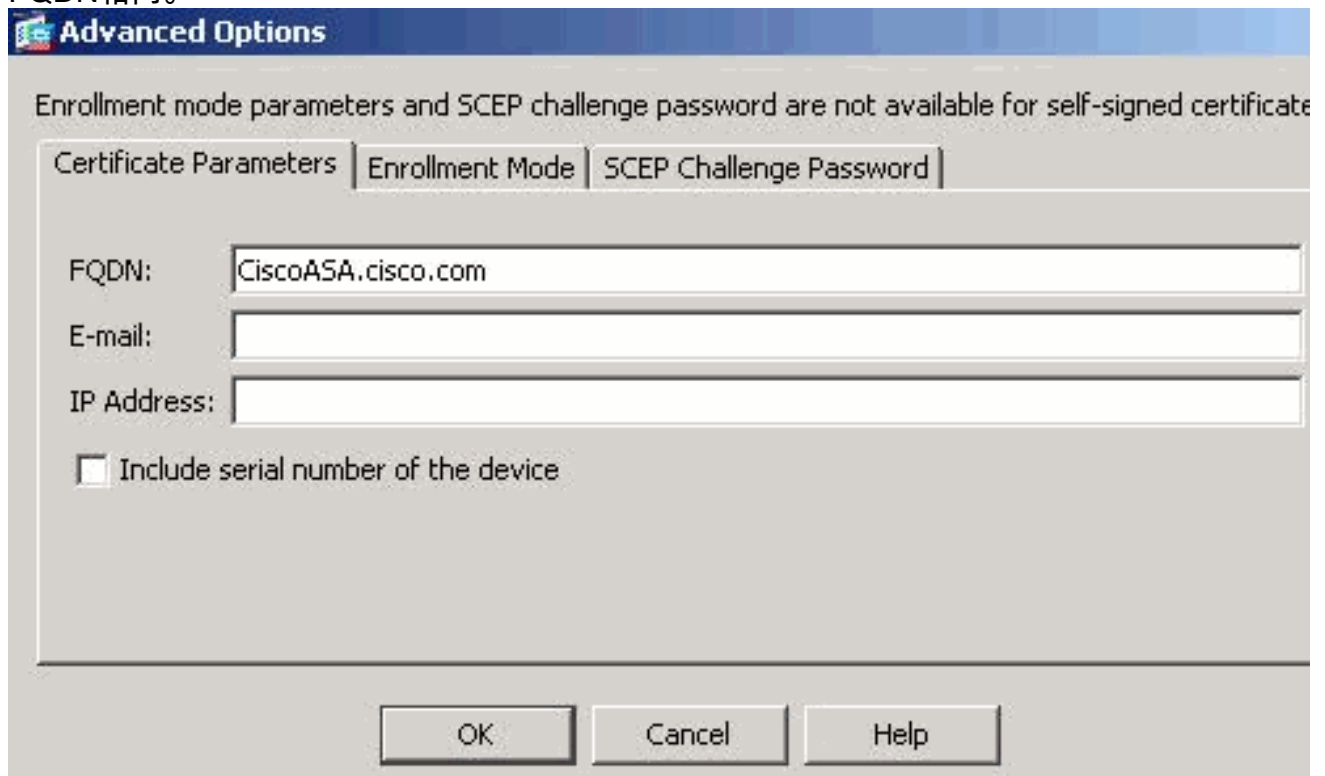
Usage: General purpose Special

6. 按一下**Enter new key pair name**單選按鈕。出於識別目的，必須明確標識金鑰對名稱。
7. 按一下「**Generate Now**」。現在必須建立金鑰對。
8. 要定義證書使用者DN，請按一下**選擇**，然後配置下表列出的屬性：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**。

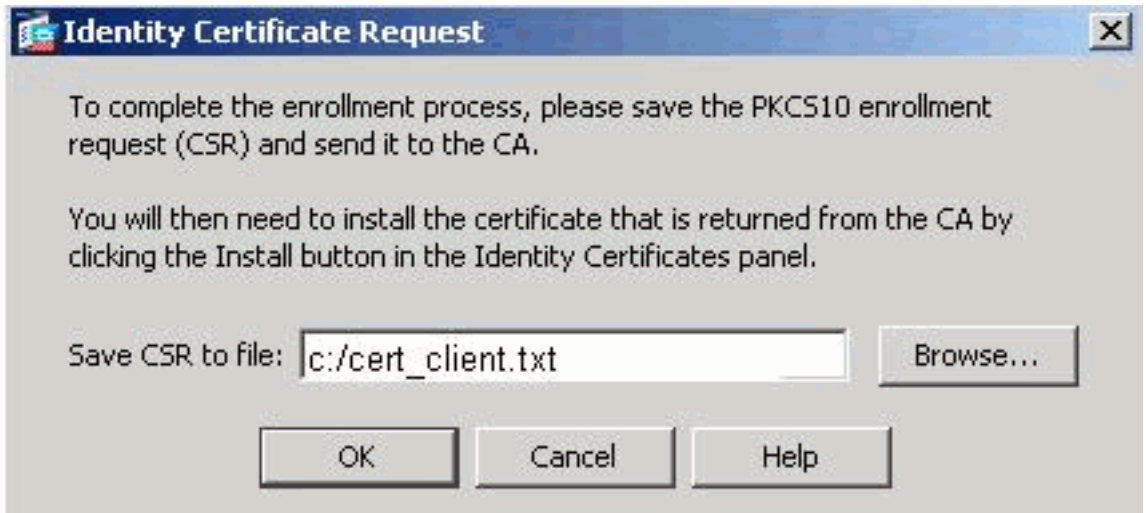


注意：某些第三方供應商要求在頒發身份證書之前包含特定屬性。如果您不確定所需的屬性，請與您的供應商聯絡以瞭解詳細資訊。

9. 新增適當的值後，按一下**確定**。系統將顯示Add Identity Certificate對話方塊，其中填充了Certificate Subject DN欄位。
10. 按一下「**Advanced**」。
11. 在FQDN欄位中，輸入用於從Internet訪問裝置的FQDN。此值必須與用於公用名(CN)的FQDN相同。



12. 按一下「**OK**」，然後按一下「**Add Certificate**」。系統將提示您將CSR儲存到本地電腦上的

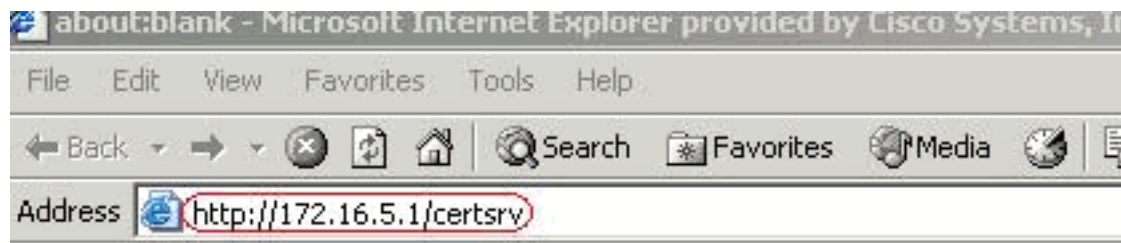


檔案中。

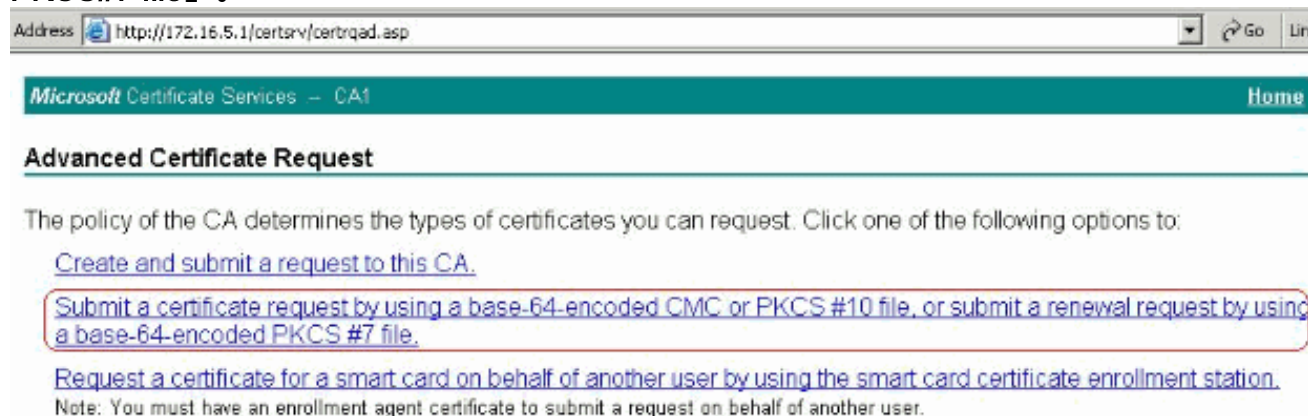
13. 按一下「Browse」，選擇要儲存CSR的位置，並以.txt副檔名儲存檔案。注意：使用.txt副檔名儲存檔案時，可以使用文本編輯器（如記事本）開啟該檔案並檢視PKCS#10請求。



14. 將儲存的CSR提交給您的第三方供應商（例如Microsoft CA），如下所示。使用為vpnservice提供的使用者憑據執行Web登入CA伺服器172.16.5.1。



注意：確保您在CA伺服器中擁有ASA (vpn伺服器) 的使用者帳戶。按一下「Request a certificate > advanced certificate request」，以選擇「Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file」。



將編碼的資訊複製並貼上到**Saved Request**框中，然後按一下**Submit**。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded C source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
lvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAO  
4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8  
D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+  
8Ux9emhFHpGHnQ/MpSfUOdQ==  
not part of the certificate request---
```

[Browse for a file to insert.](#)

Certificate Template:

IPSEC

Additional Attributes:

Attributes:

Submit >

按一下

「Base 64 encoded」單選按鈕，然後按一下「Download certificate」。

Microsoft Certificate Services -- CA1

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

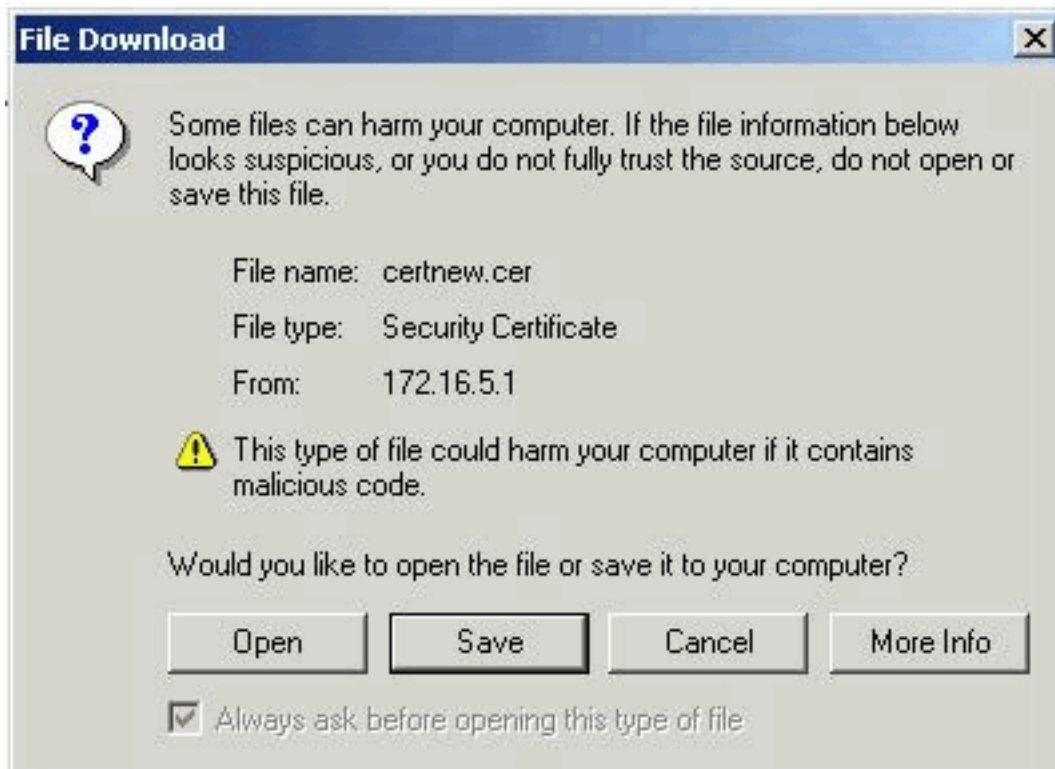


[Download certificate](#)

[Download certificate chain](#)

出現「File

Download (檔案下載)」視窗。使用cert_client_id.cer名稱儲存該證書，該名稱是要安裝在ASA上的身份證書。



命令列示例

CiscoASA

```
CiscoASA# configure terminal

CiscoASA(config)#crypto key generate rsa label my.ca.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.CA.key Keypair generation process begin.
Please wait... ciscoasa(config)#crypto ca trustpoint CA1
ciscoasa(config-ca-trustpoint)# subject-name
CN=CiscoASA.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 as a guide. CiscoASA(config-
ca-trustpoint)#keypair my.CA.key

!--- Specifies key pair generated in Step 3
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.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 CA1
!--- Initiates certificate signing request. This is the
request to be !--- submitted via Web or Email to the
third party vendor. % Start certificate enrollment .. %
The subject name in the certificate will be:
cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems,
```

```

C=US,St=North Carolina,L=Raleigh % The fully-qualified
domain name in the certificate will be:
CiscoASA.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]: y
!--- 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 third party CA. Certificate Request follows:
MIICKzCCAzQCAQAwga0xEDA0BgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEWJVUzEWMBQGA1UEChMNQ2l2Y28gU3l2
dGVtczEk
MCIGA1UEAxMbQ2l2Y29BU0EuY2l2Y28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkcr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXTlPgNAaFMwB2YsTIOh+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBxl/LVLTy3ORqcy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIB3DQEJJDjEuMCwwCwYDVR0PBAQD
AgWgMB0G
A1UdEQQWMBSEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF
AAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd20LCbXAoP5LlKbPaEeaCkfn/Pp5mATA
sG832TBm
bsxSvljSSXQsQlSb842D6MEG6cu7Bxj/KlZ6MxafUvCHROPYWVU1wgRJ
Gh+ndCZK j89/Y4S8XhQ79fvBwB8Ux9emhFHpGHnQ/MpSfU0dQ== --
--End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: n
CiscoASA(config)#

```

步驟3. 驗證信任點

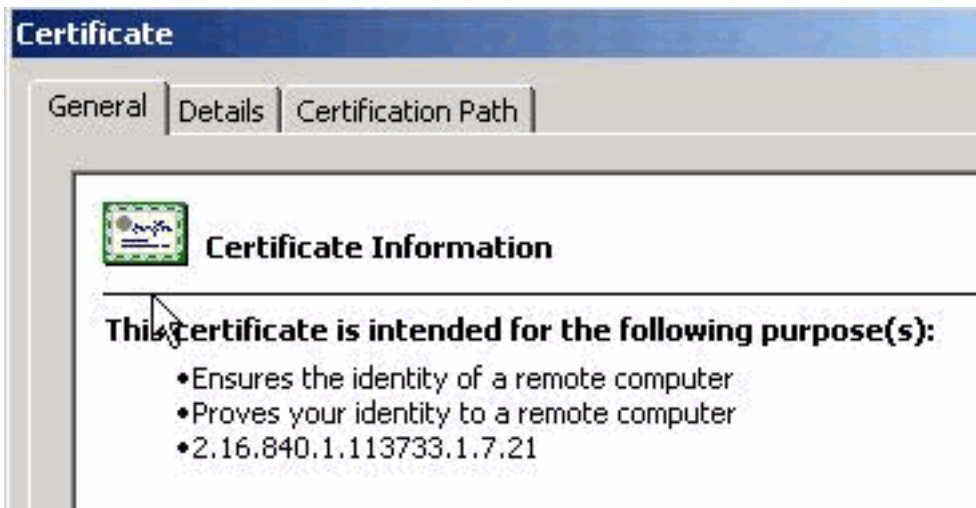
收到來自第三方供應商的身份證書後，您可以繼續執行此步驟。

ASDM過程

1. 將身份證書儲存到本地電腦。
2. 如果為您提供了base64編碼的證書，並且該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. 使用.cer副檔名重新命名檔案**注意**：使用.cer副檔名重新命名檔案後，檔案圖示將顯示為證書



，如圖所示。



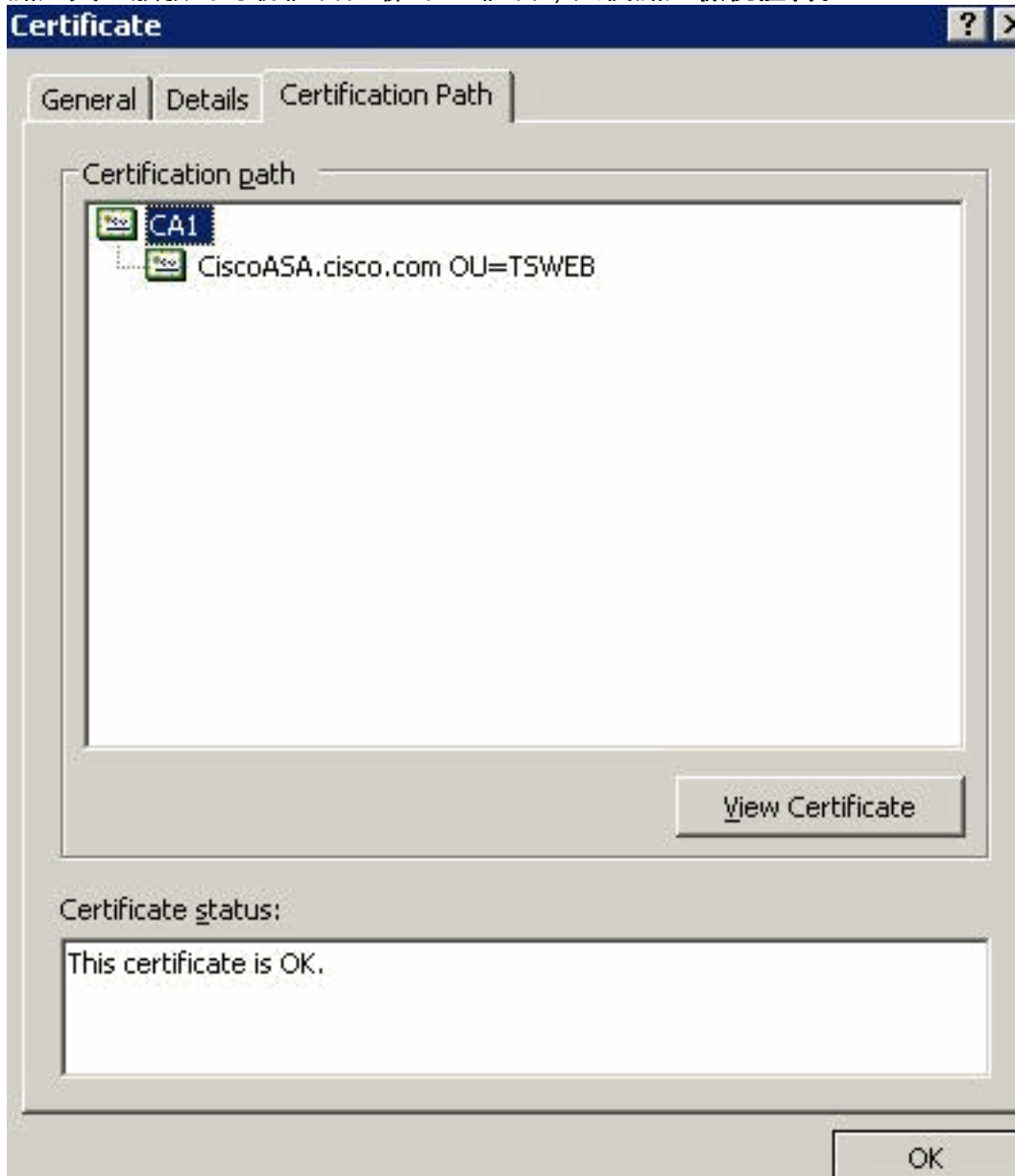
4. 按兩下證書檔案。

注意

：如果Windows沒有足夠的資訊來驗證此證書消息出現在「常規」選項卡中，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。

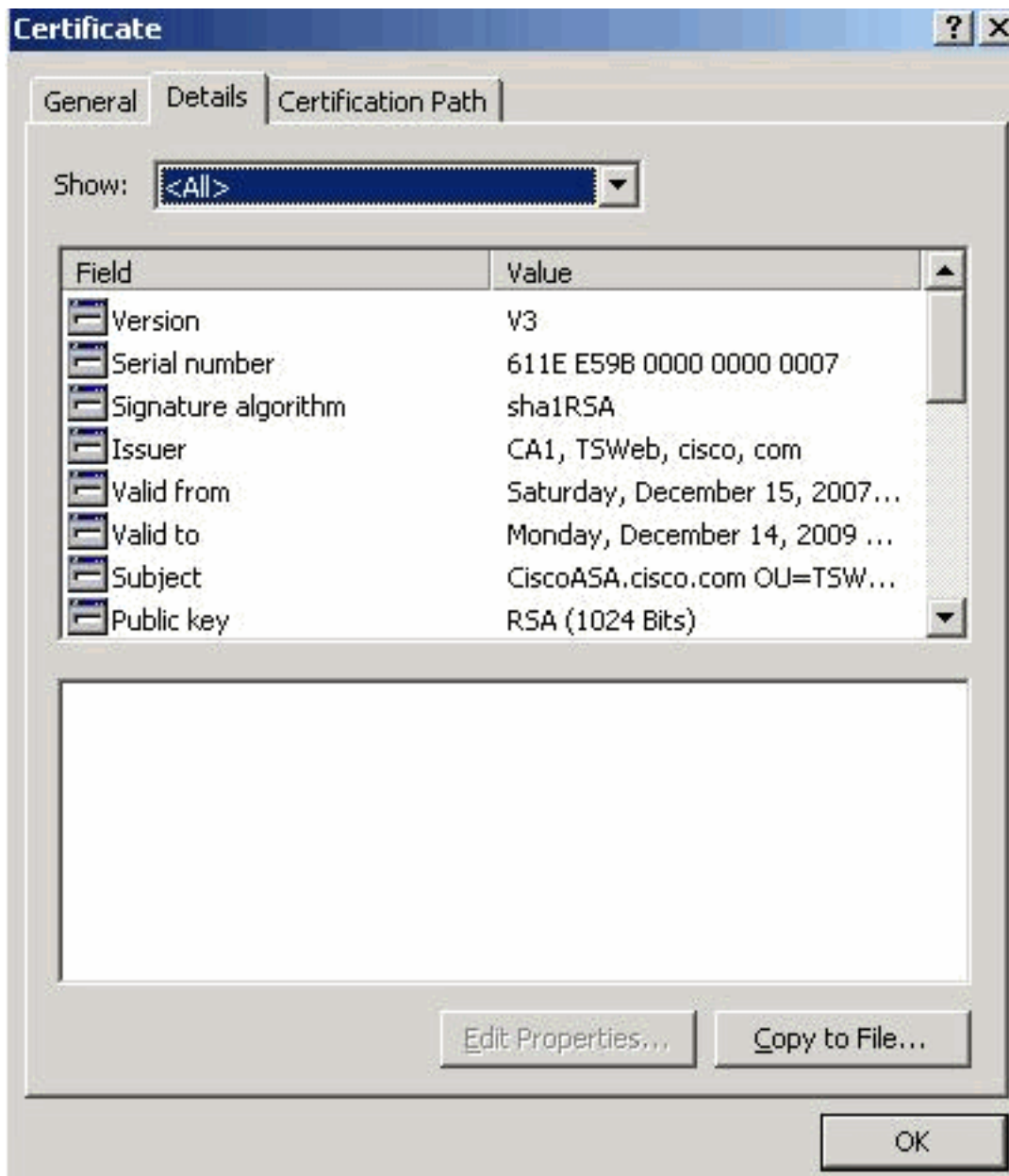
6. 點選與您頒發的身份證書關聯的CA證書，然後點選**檢視證書**。



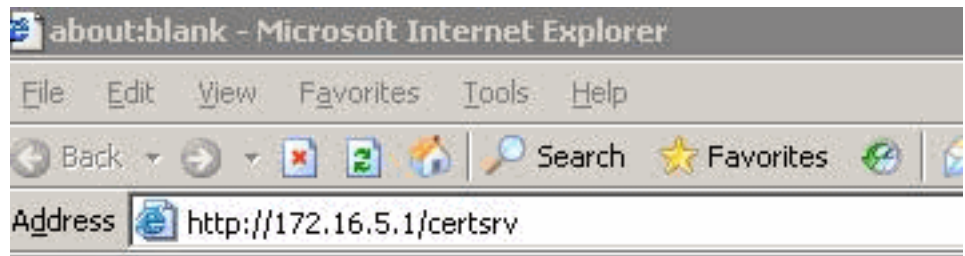
此時將顯示有關

CA證書的詳細資訊。

7. 按一下**Details**以瞭解有關身份證書的詳細資訊。



8. 在安裝身份證書之前，必須從CA伺服器下載CA證書並將其安裝在ASA中，如圖所示。完成這些步驟，從名為**CA1**的CA伺服器下載CA憑證。使用提供給VPN伺服器的憑據執行Web登入



CA伺服器172.16.5.1。

按一下「Download a CA certificate, certificate chain or CRL」以開啟視窗，如下所示。按一下 Base 64 單選按鈕作為編碼方法，然後按一下 Download CA certificate。

按

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
- Base 64

- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

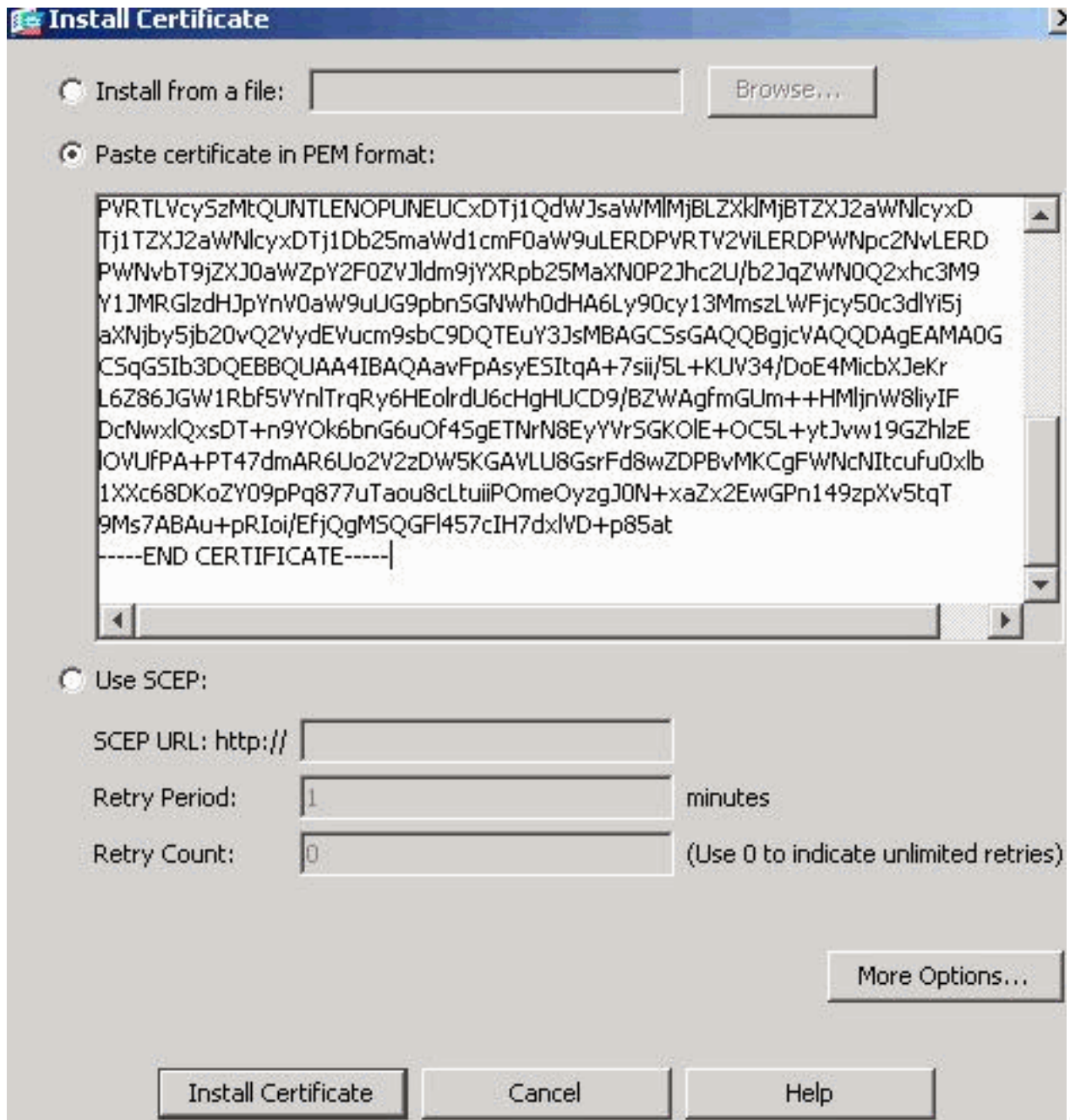
在電腦上使用certnew.cer名稱儲存CA證書。



9. 瀏覽到儲存CA證書的位置。
10. 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」。
11. 系統會顯示與圖中的憑證類似的base64編碼訊息
：

```
certnew.cer - Notepad
File Edit Format Help
-----BEGIN CERTIFICATE-----
MIIEHTCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBRI
MRMwEQYKZImiZPyLQBGGRYDY29tMRUwEwYKZImiZPyLQBGGRYFY2IzY28xFTAT
BgoJkiajk/IsZAEZFGVUU1dIYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
M1oXDTEyMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCgms
JomT8ixkARKwBWNpc2NvMRUwEwYKZImiZPyLQBGGRYFVFNXZWIxDDAKBgnVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgntjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vweMijcQnwdOq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhdbMivwqYBXWkh4u04xxQmr//Sct1tdwQcvk2V
uBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wggFrMBMGCSSGAQQBgjCUAgQHgQAQwBBMASGA1UddwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZXk1MjBTZXJ2awNlcYxD
Tj1TZXJ2awNlcYxDTj1Db25maWd1cmF0aw9uLERDPVRTV2ViLERDPWNpc2NvLERD
PWNvbT9jZXJ0awZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNWw0dHA6Ly90cy13MmszLWwFjcy50c3dlYi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGCSsGAQQBgjCVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MibXJekr
L6Z86JGw1Rbf5vynlTrqRy6HEo1rdU6cHgHUCD9/BZWagfmGUM++HMLjnw8liyIF
DcnwxlQxsDT+n9Yok6bnG6uof4SgETNrN8EyyVrSGK0lE+OC5L+ytJvw19Gzh1ze
lOVUfPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCGFWNCNItcufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPN149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
```

12. 在ASDM中，按一下**Configuration**，然後按一下**Device Management**。
13. 展開**Certificate Management**，然後選擇**CA Certificates**。
14. 按一下「**Add**」。
15. 按一下**Paste certificate in PEM Format**單選按鈕，然後將第三方供應商提供的base64 CA證書貼上到文本欄位中。
16. 按一下「**Install Certificate**」。



出

現一個對話方塊，確認安裝成功。

命令列示例

```

CiscoASA
CiscoASA(config)#crypto ca authenticate CA1
!--- Initiates the prompt for paste-in of base64 CA
intermediate certificate. ! This should be provided by
the third party vendor. Enter the base 64 encoded CA
certificate. End with the word "quit" on a line by
itself -----BEGIN CERTIFICATE-----
MIIE nTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLQG BGRYDY29tMRUwEwYKCZImiZPyLQG BGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0E xMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNvowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQG BGRYFVFNXZWI xDDAK

```



```

BgNVBAMT
A0NBMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGAPAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuAhpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAQOQHQAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMM1mjBLZXk1mjBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDtj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNO
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFwcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAghmGUm++HM1j
nW81iyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGK0LE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPvMKCGFWNcNIt
cufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqT
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dxlVD+p85at
-----END CERTIFICATE-----
quit
!--- Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
CiscoASA(config)#

```

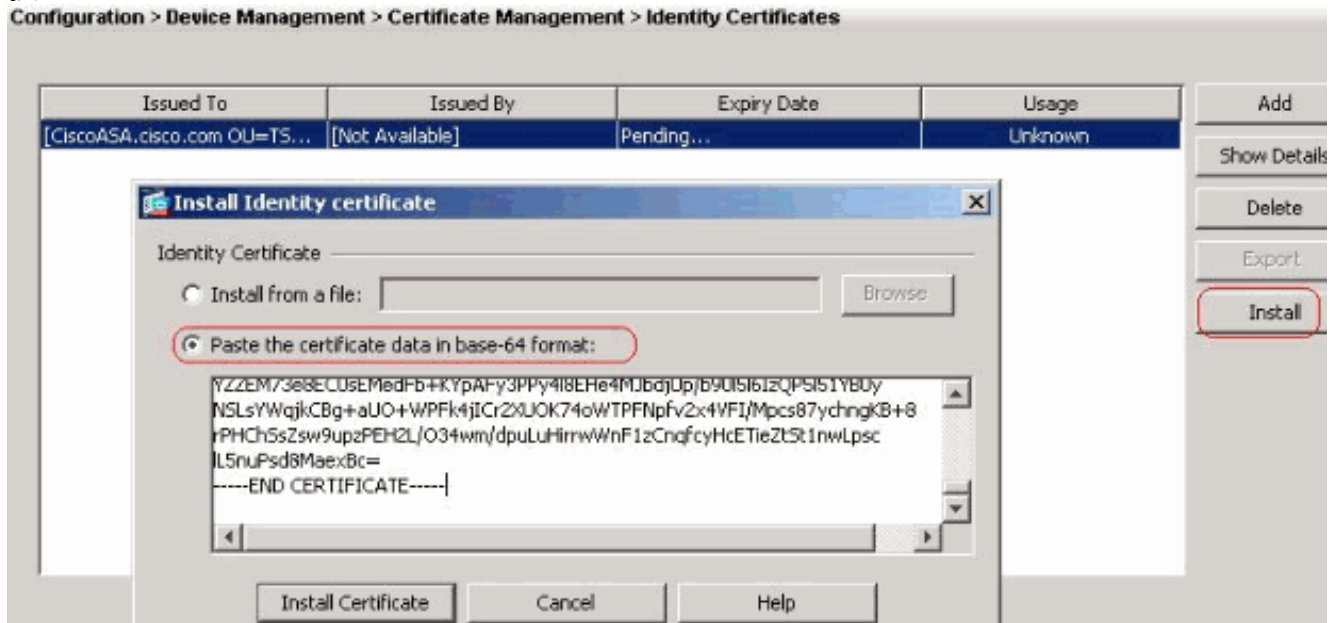
步驟4. 安裝證書

ASDM過程

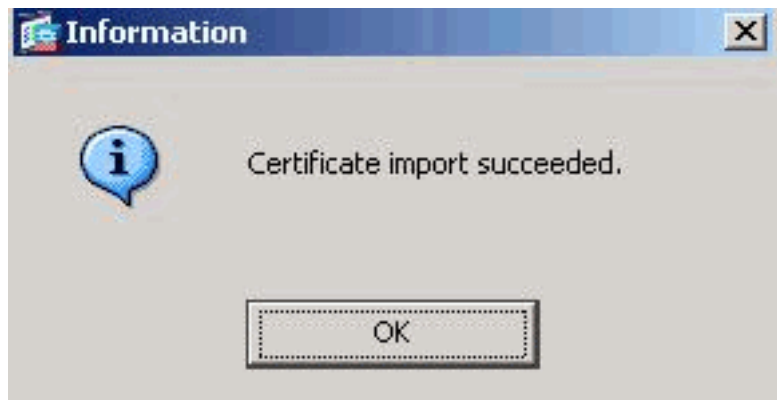
使用第三方供應商提供的身份證書來完成以下步驟：

1. 按一下 **Configuration**，然後按一下 **Device Management**。
2. 展開 **Certificate Management**，然後選擇 **Identity Certificates**。
3. 選擇您在步驟2中建立的 **身份證書**。註：到期日期顯示為待定。

4. 按一下「Install」。



按一下 **Paste the certificate data in base-64 format** 單選按鈕，然後將第三方供應商提供的身份證書貼上到文本欄位中。



5. 按一下「Install Certificate」。

一個對話方塊，以確認匯入成功。

將出現

命令列示例

```
CiscoASA
CiscoASA(config)#crypto ca import CA1 certificate
!--- Initiates prompt to paste the base64 identity !---
certificate provided by the third party vendor. %The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself !--- Paste the base 64 certificate provided by
the third party vendor. -----BEGIN CERTIFICATE-----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLQQBGRYDY29tMRUwEwYKCZImiZPyLQQBGRYFY21zY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0EzMB4XDTA3MTIxNTA4MzUz
OVoXDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxZjZlY28xFTAT
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXNO
ZW1zMSQw
IgwYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUlwgZ8wDQYJ
KoZlIhvcN
```

```
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QUUsKMgWqBT7EXiRkgGBvjKf/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBAAwHQYDVR0RBBywFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDgQWBbQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWGBTZrb8I8jqI8RRDL3mYfNqJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
aWM1MjBLZXklMjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnsG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEgEgEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUESQ049UHvibGljJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UUy1XMksZLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBIAFMAZQByAHYAZQByMAWGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAWEdQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzCWAEVRXCyBlx0NpR/j1ocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtz5vBjG1cROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpFv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc
1L5nuPsd8MaexBc=
-----END CERTIFICATE-----
quit

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

步驟5.將遠端訪問VPN(IPSec)配置為使用新安裝的證書

ASDM過程

完成以下步驟以配置遠端訪問VPN:

1. 選擇 Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > IKE Policies > Add 以建立 ISAKMP 策略配置，如 65535 所示。

Add IKE Policy

Priority: 65535 Authentication: rsa-sig

Encryption: 3des D-H Group: 2

Hash: md5 Lifetime: Unlimited
 86400 seconds

OK Cancel Help

按一下「OK」和「Apply」。

2. 選擇 Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > IPsec Transform Sets > Add 以建立 myset 轉換集，如下所示。

Add Transform Set

Set Name: myset

Properties

Mode: Tunnel Transport

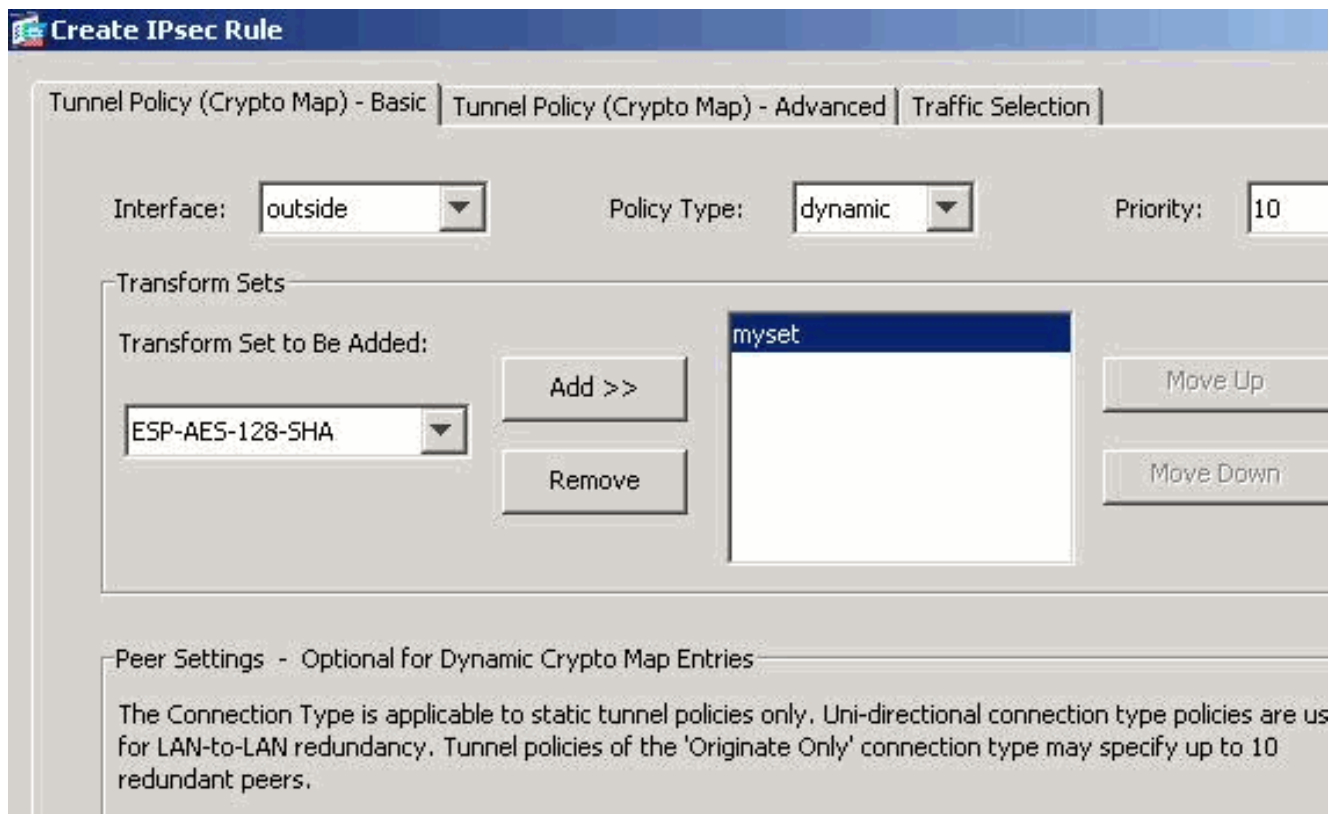
ESP Encryption: 3DES

ESP Authentication: MD5

OK Cancel Help

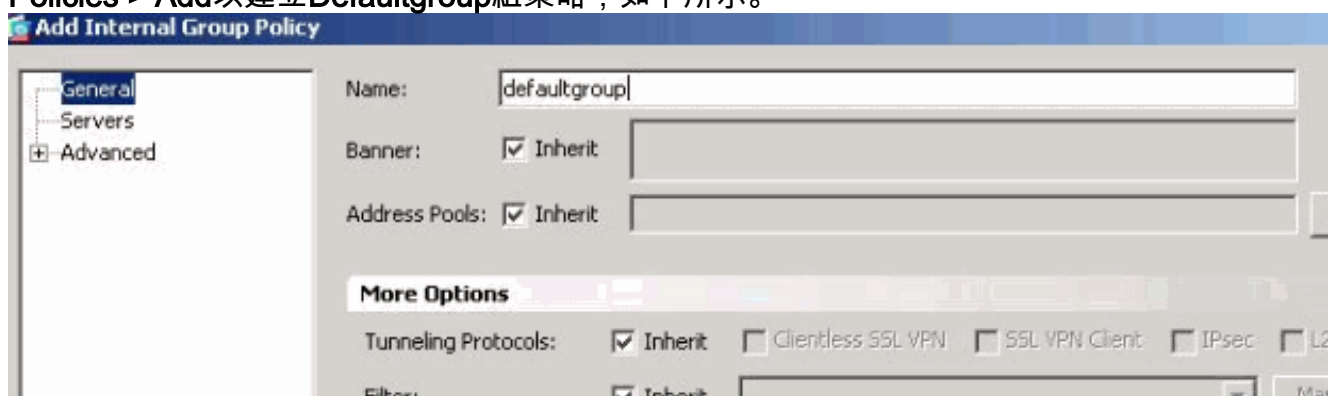
按一下「OK」和「Apply」。

3. 選擇 Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > Crypto Maps > Add，以便使用優先順序為 10 的動態策略建立加密對映，如下所示。



按一下「OK」和「Apply」。注意：ASA 8.0不支援SHA 2。此外，不支援使用具有256雜湊值的證書的IPSec客戶端。

4. 選擇Configuration > Remote Access VPN > Network(Client)Access > Advanced > Group Policies > Add以建立Defaultgroup組策略，如下所示。



按一下「OK」和「Apply」。

5. 選擇Configuration > Remote Access VPN > Network(Client)Access > Address Assignment > Address Pools > Add，為要動態分配的VPN客戶端使用者配置vpnpool地址池。

Add IP Pool

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

OK Cancel Help

按一下「OK」和「Apply」。

6. 選擇 **Configuration > Remote Access VPN > AAA Setup > Local Users > Add**，以便為VPN客戶端訪問建立vpnpool使用者帳戶。此外，將此使用者設為DefaultRAGroup的成員。

Add User Account

Identity

VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of:

Member-of: Add >> Delete

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

7. 選擇 **Configuration > Remote Access VPN > Network(Client)Access > IPSec Connection Profiles > Edit**以編輯DefaultRAGroup，如下所示。從IKE Peer Authentication欄位的下拉選單

中選擇適當的身份證書。在User Authentication欄位中選擇伺服器組作為LOCAL。選擇vpnpool作為Client Address Assignment欄位的Client Address Pool。為「預設組策略」欄位選擇defaultgroup作為「組策略」。

The screenshot shows the configuration interface for an IPsec Remote Access Connection Profile. The 'Advanced' tab is active, and the 'IPsec' sub-tab is selected. The configuration includes:

- Name: DefaultRAGroup
- IKE Peer Authentication: (empty)
- Pre-shared Key: (empty)
- Identity Certificate: [cn=CiscoASA.cisco.com OU]=TSWEB, o=Cisco Systems, ...
- User Authentication: Server Group: LOCAL
- Fallback: Use LOCAL if Server Group fails
- Client Address Assignment: Client Address Pools: vpnpool
- Default Group Policy: Group Policy: defaultgroup
- Client Protocols: IPsec L2TP over IPsec

按一下「OK」和「Apply」。

命令列示例

CiscoASA

```
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)#exit
CiscoASA(config)#crypto isakmp identity auto

!--- Phase 1 Configurations CiscoASA(config)#crypto
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map dynmap 10 set
transform-set myset
CiscoASA(config)#crypto map mymap 10 ipsec-isakmp
dynamic dynmap
CiscoASA(config)#crypto map mymap interface outside

!--- Phase 2 Configurations CiscoASA(config)#group-
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value
cisco.com
CiscoASA(config-group-policy)# exit

!--- Create a group policy "defaultgroup" with domain
```

```

name !--- cisco.com CiscoASA(config)#username vpnuser
password Cisco123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#memberof DefaultRAGroup
CiscoASA(config-username)#exit

!--- Create a user account "vpnuser" and added to !---
"DefaultGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes

!--- The Security Appliance provides the default tunnel
groups !--- for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)#address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the
address pool. CiscoASA(config-tunnel-general)#default-
group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the
tunnel group. CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-
attributes
CiscoASA(config-tunnel-ipsec)#trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer !---
authentication

```

ASA配置摘要

CiscoASA

```

CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 90
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3

```



```
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
access-list 100 extended permit ip 10.2.2.0
255.255.255.0 10.5.5.0
255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ip local pool vpnpool 10.5.5.10-10.5.5.20
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
route outside 172.16.5.0 255.255.255.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
crypto ca trustpoint CA1
enrollment terminal
subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco
Systems, C=US,
St=North Carolina,L=Rale
serial-number
keypair my.CA.key
crl configure
crypto ca certificate chain CA1
certificate 611ee59b000000000007
308205a7 3082048f a030201 02020a61 1ee59b00
00000000 07300d06 092a8648
```

86f70d01 01050500 30513113 3011060a 09922689
93f22c64 01191603 636f6d31
15301306 0a099226 8993f22c 64011916 05636973
636f3115 3013060a 09922689
93f22c64 01191605 54535765 62310c30 0a060355
04031303 43413130 1e170d30
37313231 35303833 3533395a 170d3039 31323134
30383335 33395a30 76310b30
09060355 04061302 55533117 30150603 55040813
0e4e6f72 74682043 61726f6c
696e6131 10300e06 03550407 13075261 6c656967
68311630 14060355 040a130d
43697363 6f205379 7374656d 73312430 22060355
0403131b 43697363 6f415341
2e636973 636f2e63 6f6d204f 553d5453 57454230
819f300d 06092a86 4886f70d
01010105 0003818d 00308189 02818100 b8e20aa8
332356b7 5b660073 5008d373
5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754
5e7f98d3 d4239b42 ab8faf0b
e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a
b94b18ef 308eb12f 22ab1a8e
db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9
03f722bd 414b0a32 05aa053e
c45e2464 80606f8e 417f09a7 aa9c644d 02030100
01a38202 de308202 da300b06
03551d0f 04040302 05a0301d 0603551d 11041630
14821243 6973636f 4153412e
63697363 6f2e636f 6d301d06 03551d0e 04160414
2c242ddb 490cdela fe2d63e3
1e1fb28c 974c4216 301f0603 551d2304 18301680
14d9adbf 08f23a88 f114432f
79987cd4 09a403e5 58308201 03060355 1d1f0481
fb3081f8 3081f5a0 81f2a081
ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43
4e3d5453 2d57324b 332d4143
532c434e 3d434450 2c434e3d 5075626c 69632532
304b6579 25323053 65727669
6365732c 434e3d53 65727669 6365732c 434e3d43
6f6e6669 67757261 74696f6e
2c44433d 54535765 622c4443 3d636973 636f2c44
433d636f 6d3f6365 72746966
69636174 65526576 6f636174 696f6e4c 6973743f
62617365 3f6f626a 65637443
6c617373 3d63524c 44697374 72696275 74696f6e
506f696e 74863568 7474703a
2f2f7473 2d77326b 332d6163 732e7473 7765622e
63697363 6f2e636f 6d2f4365
7274456e 726f6c6c 2f434131 2e63726c 3082011d
06082b06 01050507 01010482
010f3082 010b3081 a906082b 06010505 07300286
819c6c64 61703a2f 2f2f434e
3d434131 2c434e3d 4149412c 434e3d50 75626c69
63253230 4b657925 32305365
72766963 65732c43 4e3d5365 72766963 65732c43
4e3d436f 6e666967 75726174
696f6e2c 44433d54 53576562 2c44433d 63697363
6f2c4443 3d636f6d 3f634143
65727469 66696361 74653f62 6173653f 6f626a65
6374436c 6173733d 63657274
69666963 6174696f 6e417574 686f7269 7479305d
06082b06 01050507 30028651
68747470 3a2f2f74 732d7732 6b332d61 63732e74
73776562 2e636973 636f2e63

6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b
332d4143 532e5453 5765622e
63697363 6f2e636f 6d5f4341 312e6372 74302106
092b0601 04018237 14020414
1e120057 00650062 00530065 00720076 00650072
300c0603 551d1301 01ff0402
30003013 0603551d 25040c30 0a06082b 06010505
07030130 0d06092a 864886f7
0d010105 05000382 0101008a 82680f46 fbc87edc
84bc45f5 401b3716 0045515c
2c81971d 0da51fe3 96870627 b41b4319 23284b30
5eafcedb 10clef05 d0686a61
cd1ab877 100b965d 499088e1 7de418fb b5529199
46129b81 9c4353a2 1761b61c
f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433
bddef040 b4b0431e 7456fe29
8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74
97997a23 340fe65e 75601d32
3522ec61 6aa39020 60f9a50e f963c593 88c80abd
9750e2bb e285933c 53697efd
b1e15148 fcca5cb3 cef27219 e0281fbc acf1c285
2b19b30f 6ea733c4 1f62ff3b
7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87
7044e279 9b52b759 f02e9b1c
94be67b8 fb1df0c6 9ec417
quit
certificate ca 7099f1994764e09c4651da80a16b749c
3082049d 30820385 a0030201 02021070 99f19947
64e09c46 51da80a1 6b749c30
0d06092a 864886f7 0d010105 05003051 31133011
060a0992 268993f2 2c640119
1603636f 6d311530 13060a09 92268993 f22c6401
19160563 6973636f 31153013
060a0992 268993f2 2c640119 16055453 57656231
0c300a06 03550403 13034341
31301e17 0d303731 32313430 36303134 335a170d
31323132 31343036 31303135
5a305131 13301106 0a099226 8993f22c 64011916
03636f6d 31153013 060a0992
268993f2 2c640119 16056369 73636f31 15301306
0a099226 8993f22c 64011916
05545357 6562310c 300a0603 55040313 03434131
30820122 300d0609 2a864886
f70d0101 01050003 82010f00 3082010a 02820101
00ea8fee c7ae56fc a22e603d
0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d
28ece906 02902f9a d1eb2b8d
f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
ale906ec 88b32a19 38e5353e
6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621
876bd678 c8a37109 f074eabe
2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7
24b9e054 063c60a4 9b8d3c09
351bc630 05f69357 833b9197 f875b408 cb71a814
69a1f331 b1eb2b35 0c469443
1455c210 db308bf0 a9805758 a878b82d 38c71426
afffd272 dd6d7564 1cbe4d95
b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67
94b97ac7 63249009 fa05ca4d
6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b
5f020301 0001a382 016f3082
016b3013 06092b06 01040182 37140204 061e0400
43004130 0b060355 1d0f0404
03020186 300f0603 551d1301 01ff0405 30030101

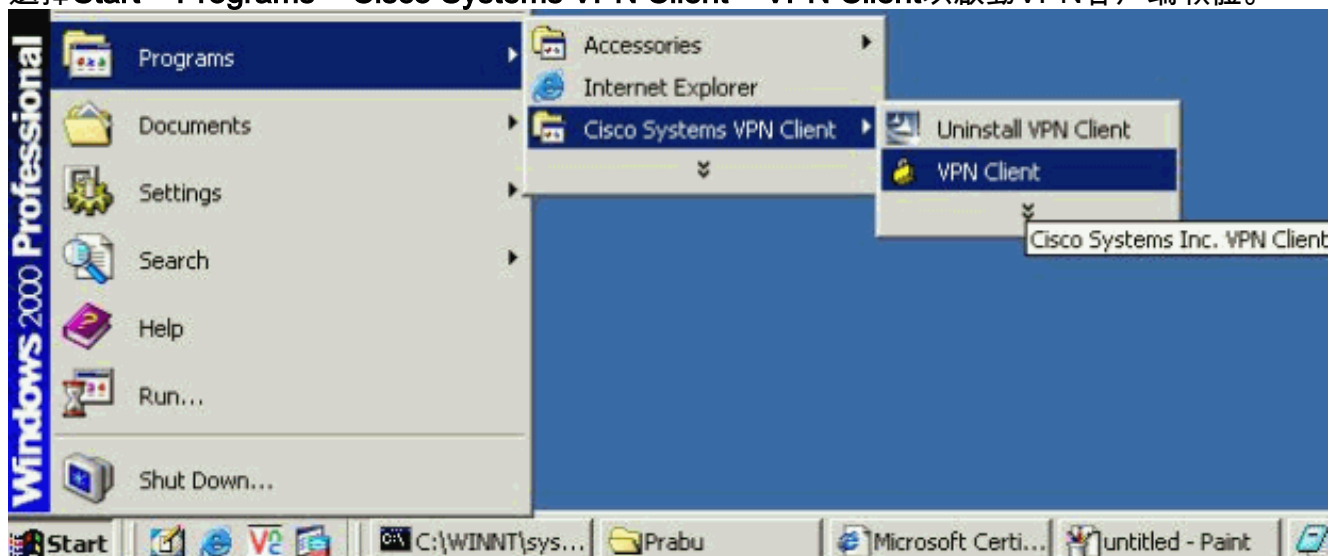
```
ff301d06 03551d0e 04160414
  d9adbf08 f23a88f1 14432f79 987cd409 a403e558
30820103 0603551d 1f0481fb
  3081f830 81f5a081 f2a081ef 8681b56c 6461703a
2f2f2f43 4e3d4341 312c434e
  3d54532d 57324b33 2d414353 2c434e3d 4344502c
434e3d50 75626c69 63253230
  4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f
  6e666967 75726174 696f6e2c 44433d54 53576562
2c44433d 63697363 6f2c4443
  3d636f6d 3f636572 74696669 63617465 5265766f
63617469 6f6e4c69 73743f62
  6173653f 6f626a65 6374436c 6173733d 63524c44
69737472 69627574 696f6e50
  6f696e74 86356874 74703a2f 2f74732d 77326b33
2d616373 2e747377 65622e63
  6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f
4341312e 63726c30 1006092b
  06010401 82371501 04030201 00300d06 092a8648
86f70d01 01050500 03820101
  001abc5a 40b32112 22da80fb bb228bfe 4bf8a515
df8fc3a0 4e0c89c6 d725e2ab
  2fa67ce8 9196d516 dfe55627 953aea47 2e871289
6b754e9c 1e01d408 3f7f0595
  8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b
  ab8e7f84 a011336b 37c13261 5ad218a3 a513e382
e4bfb2b4 9bf0d7d1 99865cc4
  94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92
860152d4 f06b2b15 df306433
  c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d
  aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76
13018f9f 5e3dce95 efe6da93
  f4cb3b00 102efa94 48a22fc4 7e342031 2406165e
39edc207 eddc6554 3fa9f396 ad
quit
crypto isakmp enable outside
crypto isakmp policy 65535
  authentication rsa-sig
  encryption 3des
  hash md5
  group 2
  lifetime 86400
crypto isakmp identity auto
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
```

```
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
group-policy defaultgroup internal
group-policy defaultgroup attributes
  default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
  memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
  address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
  trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#
```

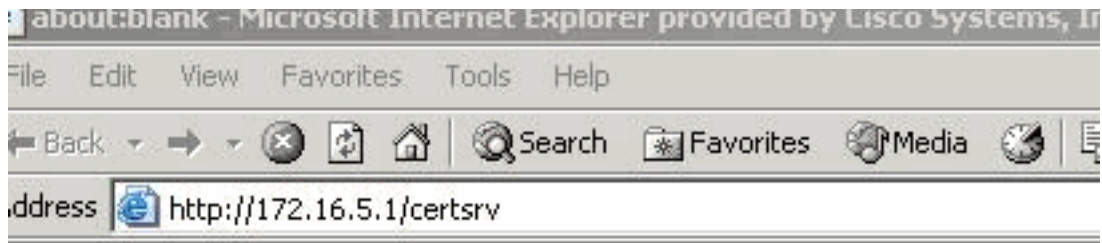
VPN客戶端配置

完成以下步驟以配置VPN客戶端。

1. 選擇Start > Programs > Cisco Systems VPN Client > VPN Client以啟動VPN客戶端軟體。



2. 完成這些步驟，從名為CA1的CA伺服器下載CA憑證，並將其安裝到Cisco VPN使用者端。使用提供給vpnuser的憑據執行Web登入CA伺服器172.16.5.1。



Enter Network Password

Please type your user name and password.

Site: 172.16.5.1

User Name: vpnuser

Password: xxxxxxxx

Domain:

Save this password in your password list

OK Cancel

注意：確保您在CA伺服器中擁有VPN客戶端使用者的使用者帳戶。按一下「**Download a CA certificate, certificate chain or CRL**」以開啟視窗，如下所示。按一下**Base 64**單選按鈕作為編碼方法，然後按一下**Download CA certificate**。

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

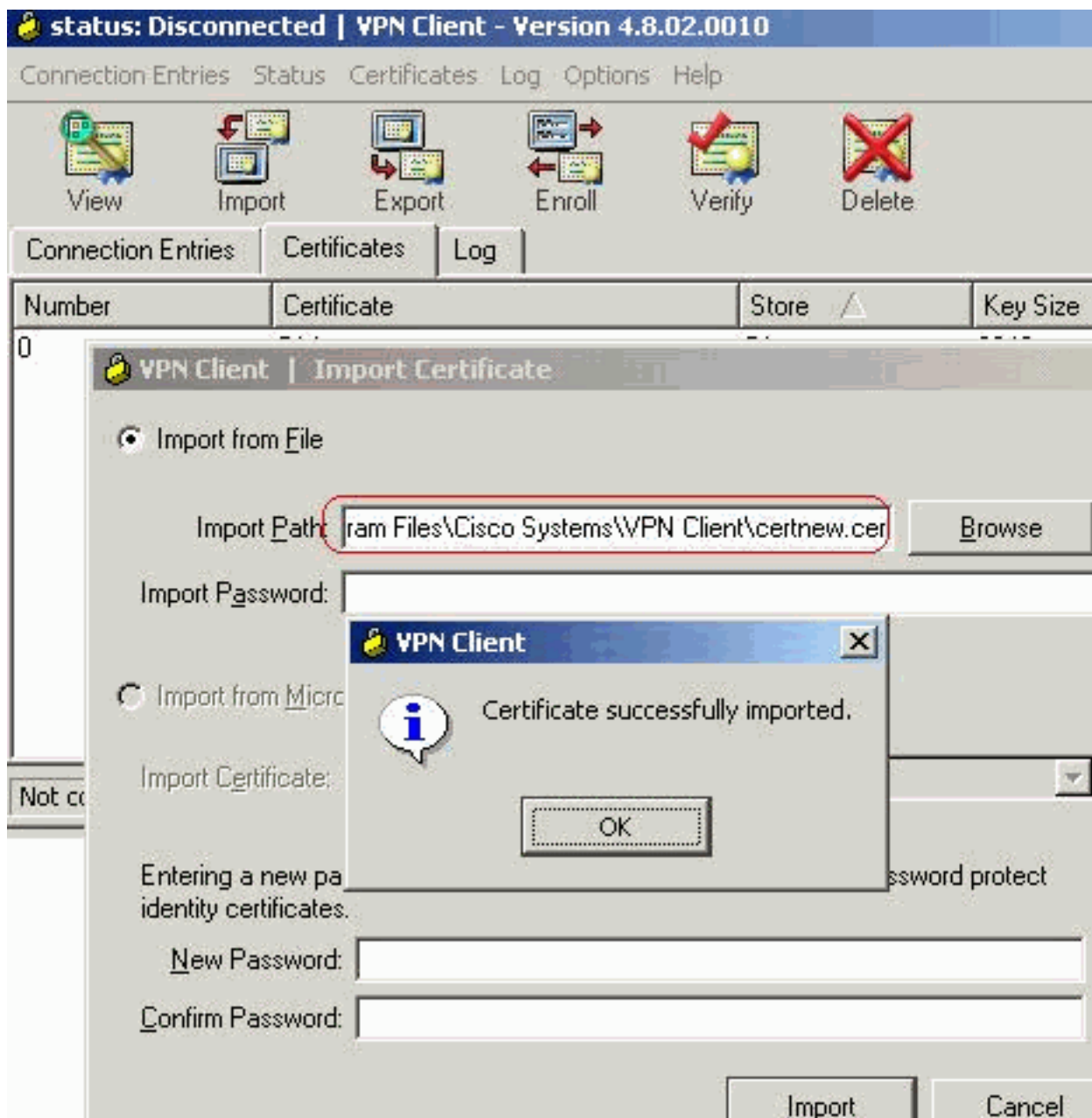
- DER
- Base 64

- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)

在電腦上使用 **certnew.cer** 名稱儲存 CA 證書。預設情況下，它儲存在 `C:\Program Files\Cisco Systems\VPN Client` 路徑中。



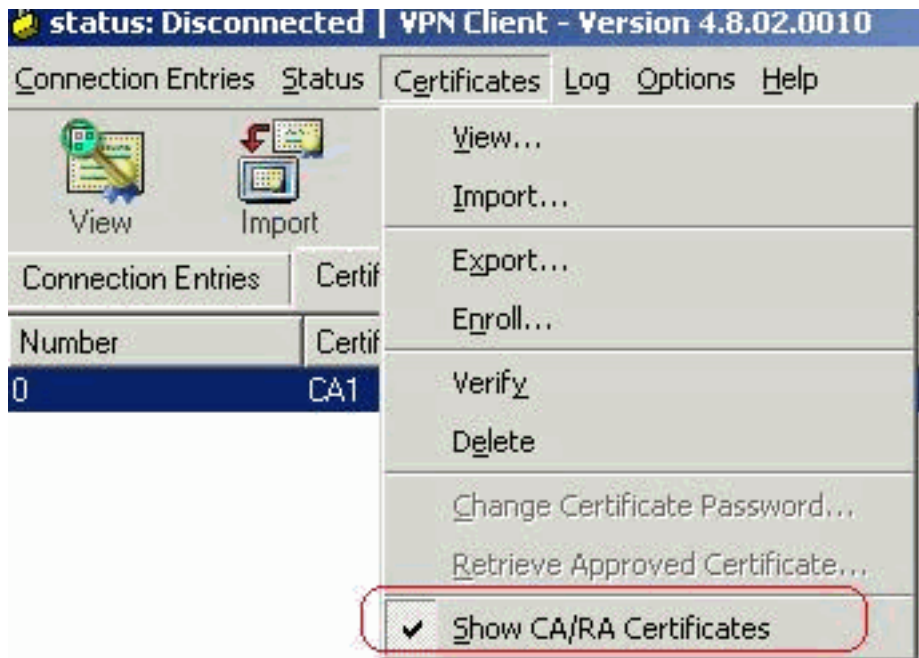
在VPN客戶端中，選擇 **Certificates 頁籤 > Import**，然後按一下 **Import from Fileradio** 按鈕。按一下 **Browse** 以從儲存位置 `C:\Program Files\Cisco Systems\VPN Client` 匯入 CA 證書，如下所示。按一下「**Import**」（匯入）。此時將顯示成功視窗，如圖所示。



在 Certificates 頁籤中，出現 CA Certificates CA1，如下所示。



注意：確保已選擇 Show CA/RA Certificates 選項（如圖所示），否則 CA 證書不得出現在證書



視窗中。

3. 完成以下步驟，即可下載身份證書並將其安裝到VPN客戶端。在CA伺服器CA1中，選擇 **Request a Certificate > advanced certificate request > Create**並向此CA提交請求以註冊身份證書。按一下「Submit」。

Certificate Template:

User ▼

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

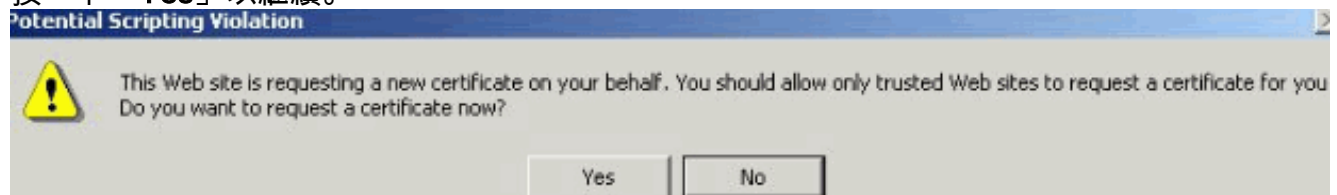
Request Format: CMC PKCS10

Hash Algorithm: MD5 ▼

Only used to sign request.

Save request to a file

按一下「Yes」以繼續。



按一下「Install this Certificate」。

Microsoft Certificate Services -- CA1

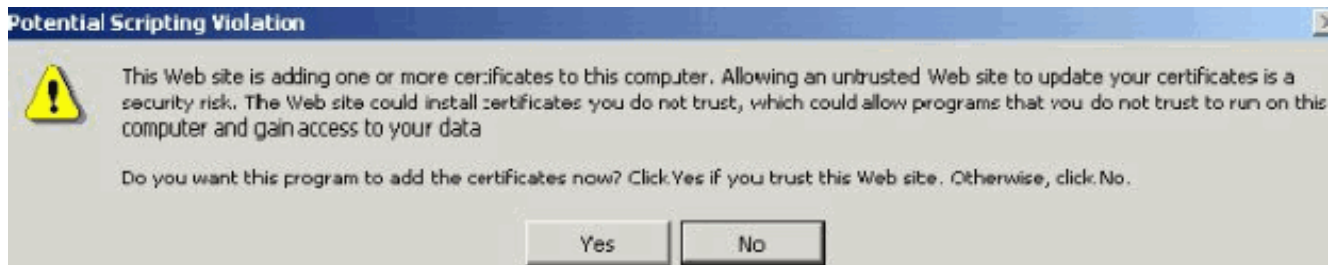
Certificate Issued

The certificate you requested was issued to you.



[Install this certificate](#)

按一下「Yes」以繼續。



您必須收到證書安裝消息，如圖所示。

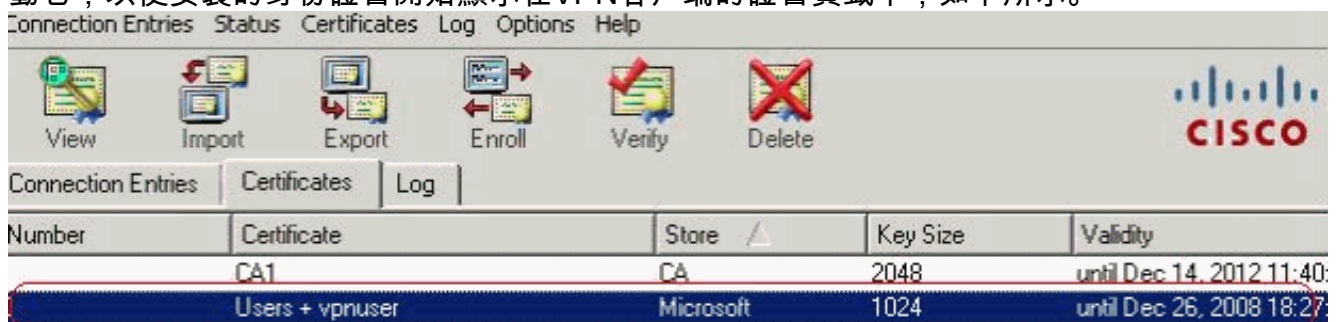
Microsoft Certificate Services -- CA1

Certificate Installed

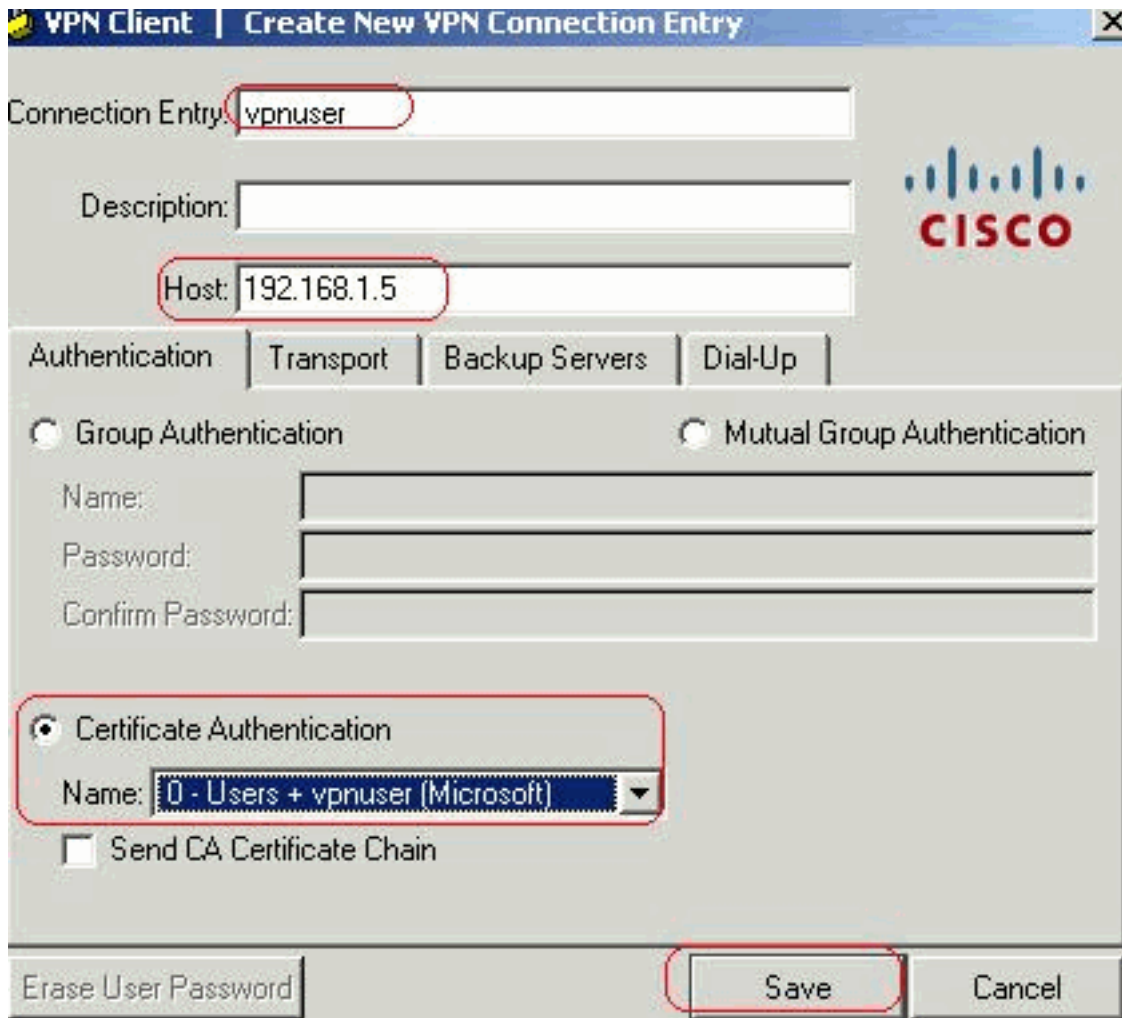
Your new certificate has been successfully installed.

退出VPN客戶端並重新啟

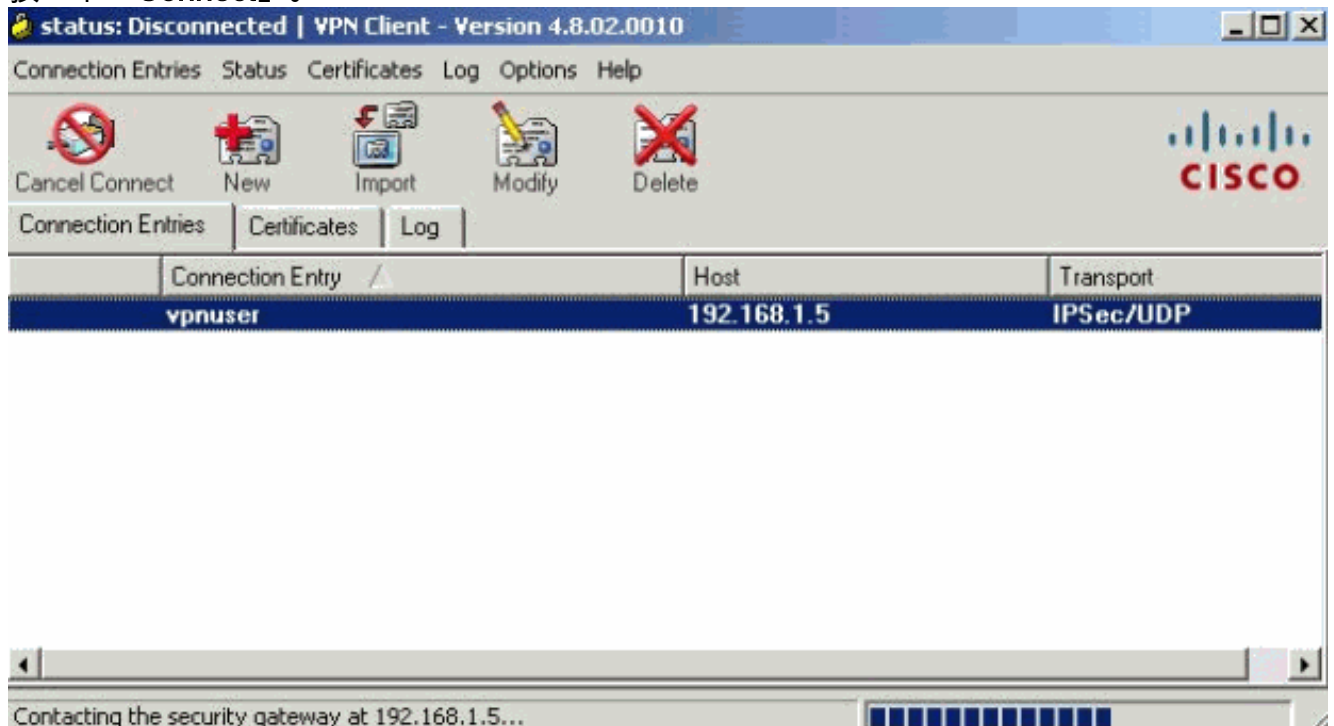
動它，以使安裝的身份證書開始顯示在VPN客戶端的證書頁籤中，如下所示。



4. 在Connection entries頁籤中，按一下**New**以建立連線條目**vpnuser**，如下所示。在Host欄位中輸入遠端對等IP地址（可路由）。按一下**Certificate Authentication**單選按鈕，然後從下拉式清單中選擇身分憑證，如下所示。按一下「**Save**」。



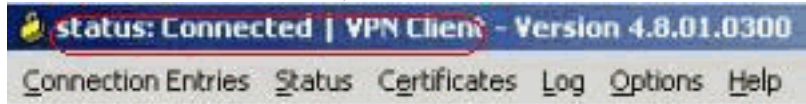
5. 按一下「Connect」。



6. 出現提示時，輸入xauth的使用者名稱和密碼資訊，然後按一下OK以連線到遠端網路。



7. VPN客戶端連線到ASA，如圖所示。



驗證

在ASA上，您可以在命令列發出幾個show命令，以驗證證書的狀態。

使用本節內容，確認您的組態是否正常運作。

- **show crypto ca trustpoint**命令顯示已配置的信任點。

```
CiscoASA#show crypto ca trustpoints
```

```
Trustpoint CA1:
```

```
Subject Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Serial Number: 7099f1994764e09c4651da80a16b749c
```

```
Certificate configured.
```

- **show crypto ca certificate**命令會顯示系統上安裝的所有證書。

```
CiscoASA# show crypto ca certificate
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 3f14b70b00000000001f
```

```
Certificate Usage: Encryption
```

```
Public Key Type: RSA (1024 bits)
```

```
Issuer Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Subject Name:
```

```
cn=vpnserver
```

```
cn=Users
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
PrincipalName: vpnserver@TSWeb.cisco.com
```

```
CRL Distribution Points:
```

```
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,  
CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
```

```
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

```
[2] http://ts-w2k3-acis.tsweb.cisco.com/CertEnroll/CA1.crl
```

```
Validity Date:
```

```
start date: 14:00:36 UTC Dec 27 2007
```

```
end date: 14:00:36 UTC Dec 26 2008
```

```
Associated Trustpoints: CA1
```

CA Certificate

```
Status: Available
Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Issuer Name:
  cn=CA1
  dc=TSWeb
  dc=cisco
  dc=com
Subject Name:
  cn=CA1
  dc=TSWeb
  dc=cisco
  dc=com
CRL Distribution Points:
  [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
      CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
      DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
Validity Date:
  start date: 06:01:43 UTC Dec 14 2007
  end date: 06:10:15 UTC Dec 14 2012
Associated Trustpoints: CA1
```

Certificate

```
Subject Name:
  Name: CiscoASA.cisco.com
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
Associated Trustpoint: CA1
```

- **show crypto ca crls**命令會顯示快取的憑證撤銷清單(CRL)。
- **show crypto key mypubkey rsa**命令顯示所有生成的加密金鑰對。

```
CiscoASA# show crypto key mypubkey rsa
Key pair was generated at: 01:43:45 UTC Dec 11 2007
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
Key pair was generated at: 06:36:00 UTC Dec 15 2007
Key name: my.CA.key
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
Key pair was generated at: 07:35:18 UTC Dec 21 2007
CiscoASA#
```

- **show crypto isakmp sa**命令顯示IKE 1隧道資訊。

```
CiscoASA#show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 10.1.1.5
Type      : user          Role       : responder
Rekey     : no           State      : MM_ACTIVE
```

- **show crypto ipsec sa**命令顯示IPSec隧道資訊。

```
CiscoASA#show crypto ipsec sa
interface: outside
Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
current_peer: 10.1.1.5, username: vpnuser
dynamic allocated peer ip: 10.5.5.10

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: FF3EEE7D

inbound esp sas:
spi: 0xEFDF8BA9 (4024404905)
transform: esp-3des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: dynmap
sa timing: remaining key lifetime (sec): 28314
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xFF3EEE7D (4282314365)
transform: esp-3des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 4096, crypto-map: dynmap
sa timing: remaining key lifetime (sec): 28314
IV size: 8 bytes
replay detection support: Y
```

[輸出直譯器工具\(僅供已註冊客戶使用\)\(OIT\)](#)支援某些show命令。使用OIT檢視show指令輸出的分析

。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

以下是您可以遇到的一些可能錯誤：

- **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。發出**show crypto ca certificates trustpointname**命令，以驗證您是否將身份證書安裝到正確的信任點。查詢說明**Associated Trustpoints**:如果列出的信任點不正確，請使用本文檔中介紹的過程來刪除並重新安裝適當的信任點。此外，請確認自產生CSR後，金鑰對沒有變更。
- **錯誤：ASA/PIX。Sev=Warning/3 IKE/0xE:3000081程憑證ID無效**：如果證書存在身份驗證問題，此錯誤消息可能出現在VPN客戶端中。在ASA/PIX配置中使用命令**crypto isakmp identity auto**以解決此問題。

相關資訊

- [思科自適應安全裝置支援頁面](#)
- [Cisco VPN使用者端支援頁面](#)
- [將Microsoft Server配置為證書頒發機構\(CA\)](#)
- [技術支援與文件 - Cisco Systems](#)