使用數位證書和Microsoft CA的ASA/PIX 7.x和VPN客戶端IPSec身份驗證配置示例

目錄

簡介

本文說明如何手動在思科安全裝置(ASA/PIX)7.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。

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

注意：本文檔假設ASA/PIX中沒有預先存在的VPN配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA 5510，執行軟體版本7.2(2)和ASDM版本5.2(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7.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。

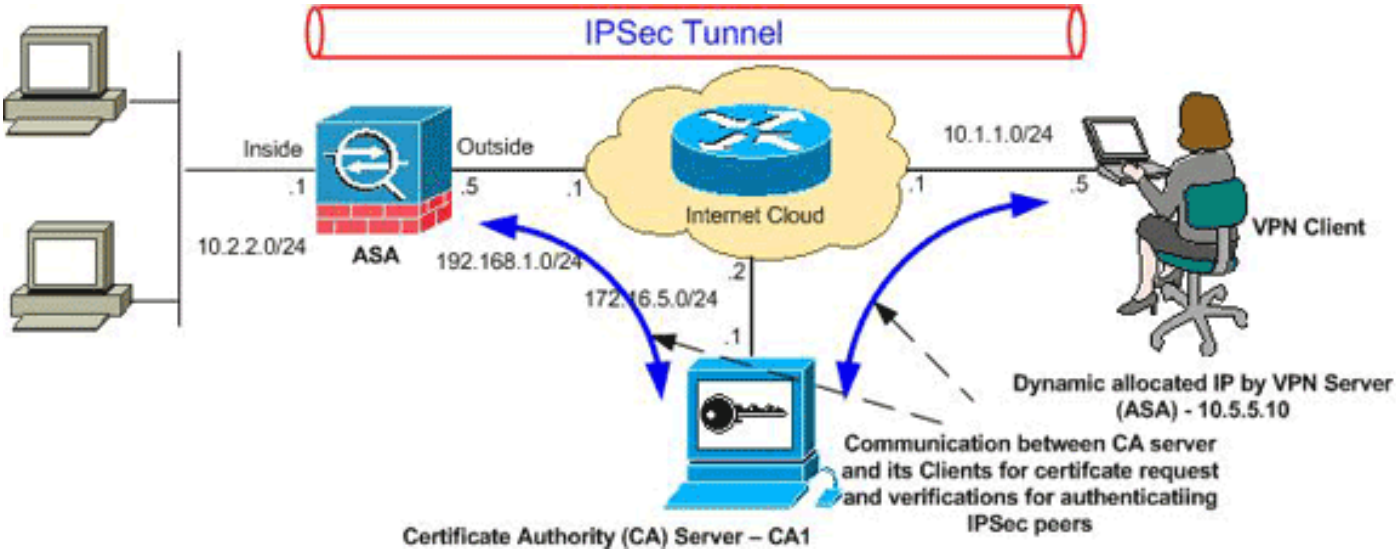
設定

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(僅供已註冊客戶使用)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。這些地址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

完成以下步驟，以便在ASA上安裝第三方供應商數位證書：

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

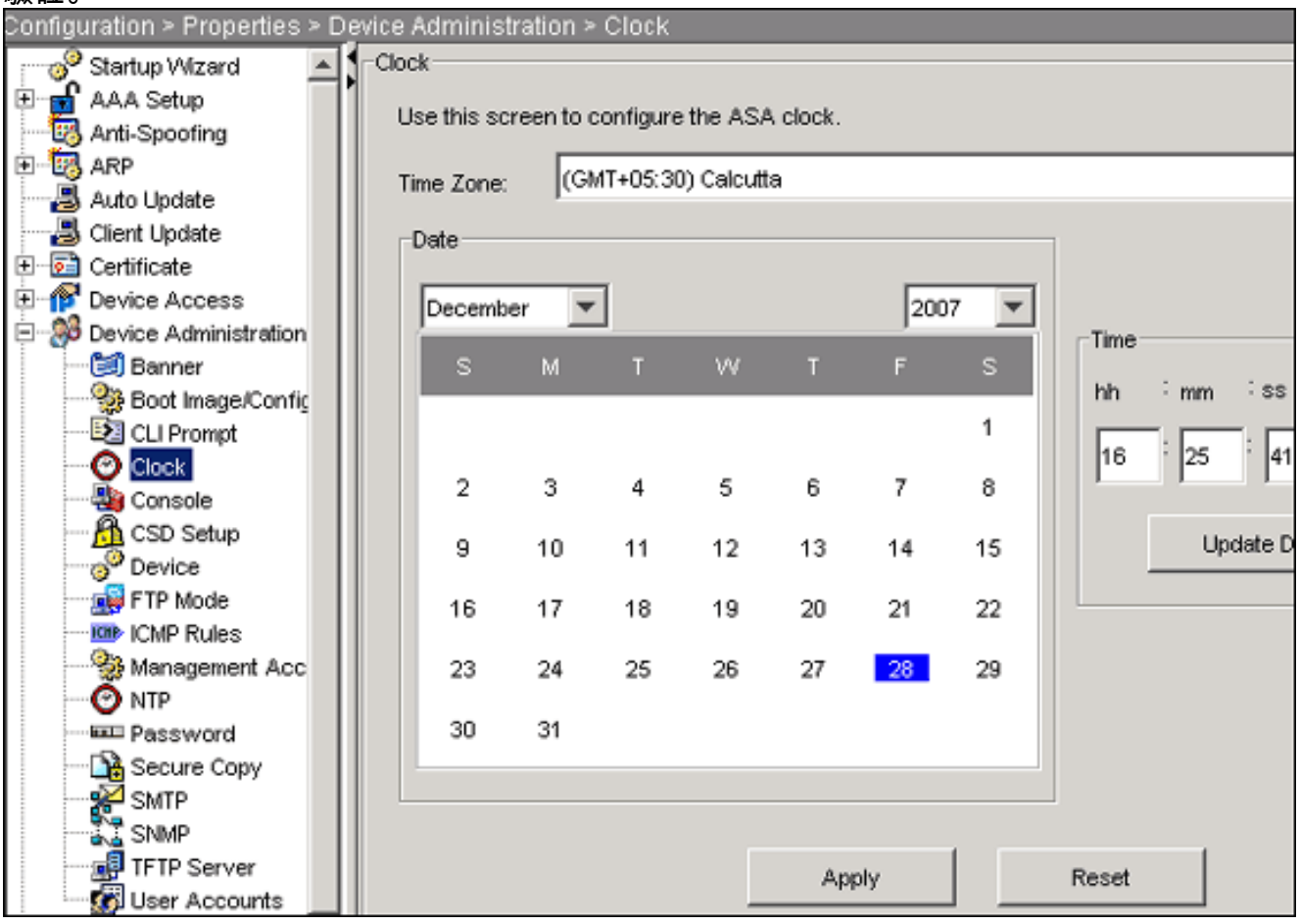
步驟6.安裝證書

步驟7.配置遠端訪問VPN(IPSec)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**Configuration**，然後按一下**Properties**。
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

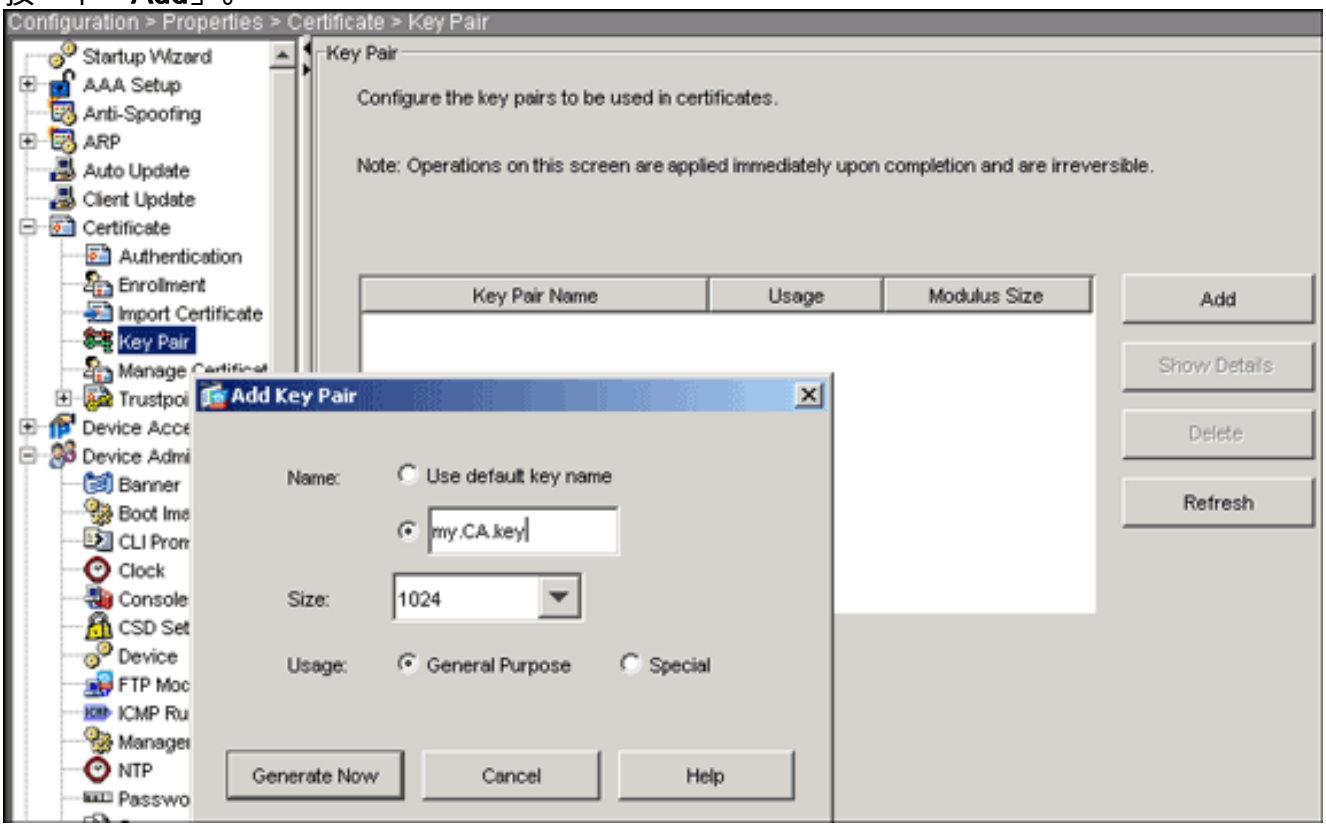
CiscoASA
CiscoASA#**show clock** 16:25:49.580 IST Fri Dec 28 2007

步驟2.生成RSA金鑰對

生成的RSA公鑰與來自ASA的身份資訊相結合，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。**注意**：建議的金鑰對大小為1024。
5. 按一下「**Generate Now**」。您建立的金鑰對應該列在「金鑰對名稱」列中。

命令列示例

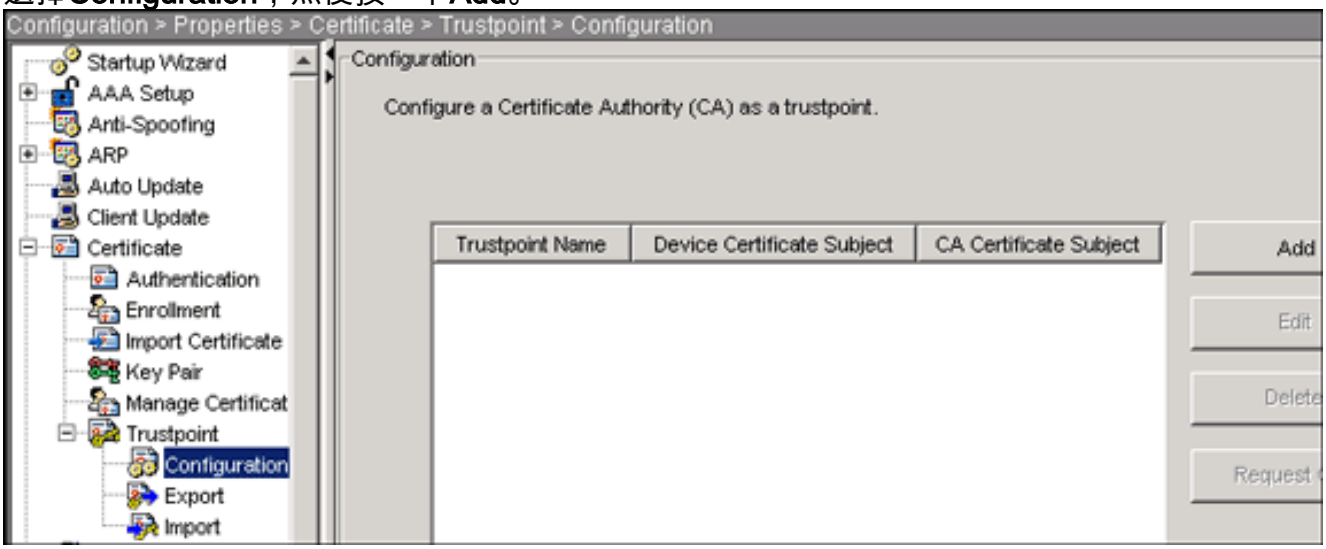
CiscoASA
CiscoASA#**configure terminal** CiscoASA(config)#**crypto key generate rsa label my.CA.key modulus 1024** *!--- Generates 1024 bit RSA key pair. "label" defines the name of the key pair.* INFO: The name for the keys will be: my.CA.key Keypair generation process begin. Please wait... ciscoasa(config)#

步驟3.建立信任點

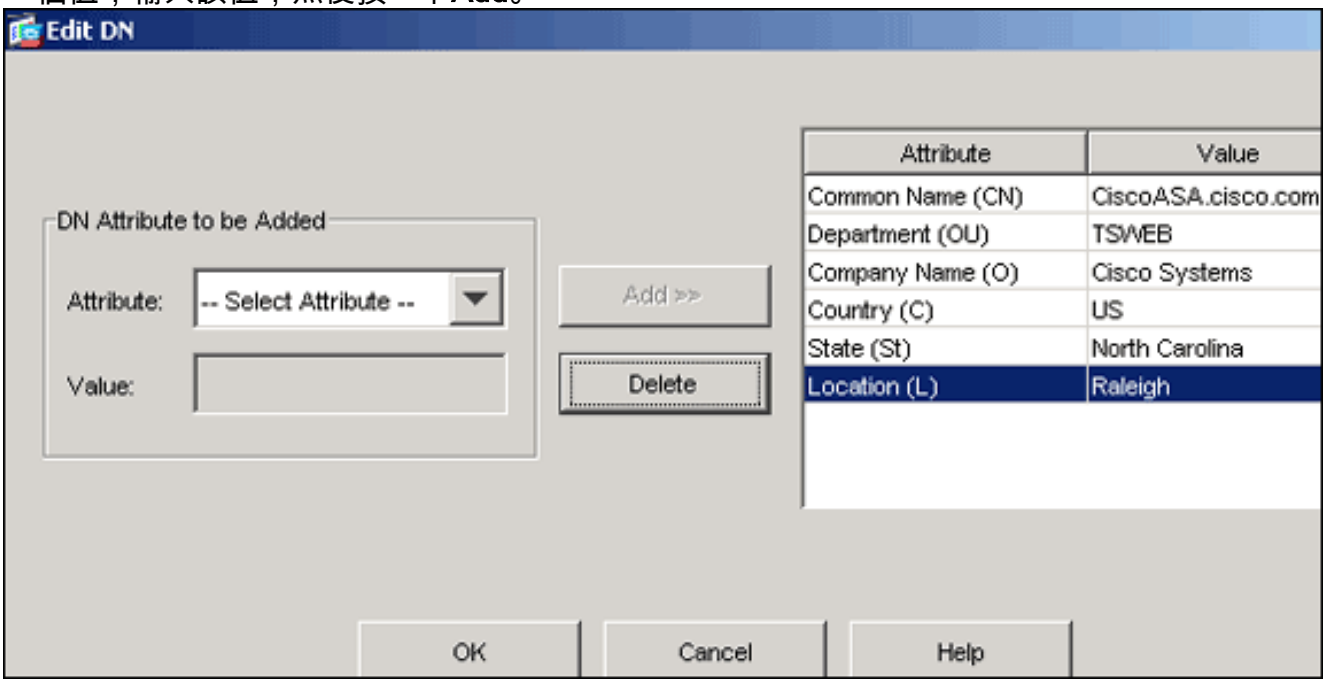
需要信任點來宣告您的ASA將使用的證書頒發機構(CA)。

ASDM過程

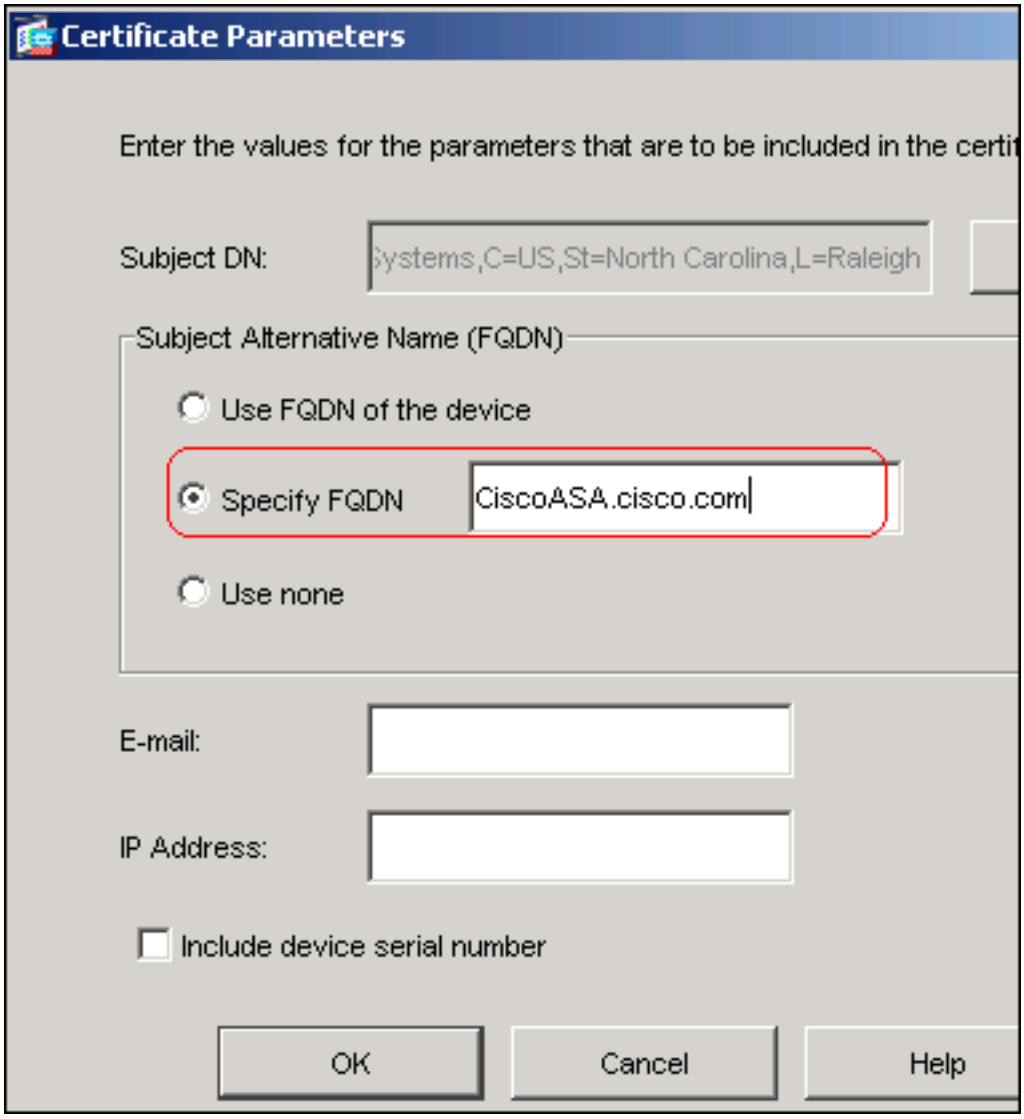
1. 按一下**Configuration**，然後按一下**Properties**。
2. 展開**Certificate**，然後展開**Trustpoint**。
3. 選擇**Configuration**，然後按一下**Add**。



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*CA1*。)**金鑰對**:選擇在步驟2中生成的金鑰對。(my.CA.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**。

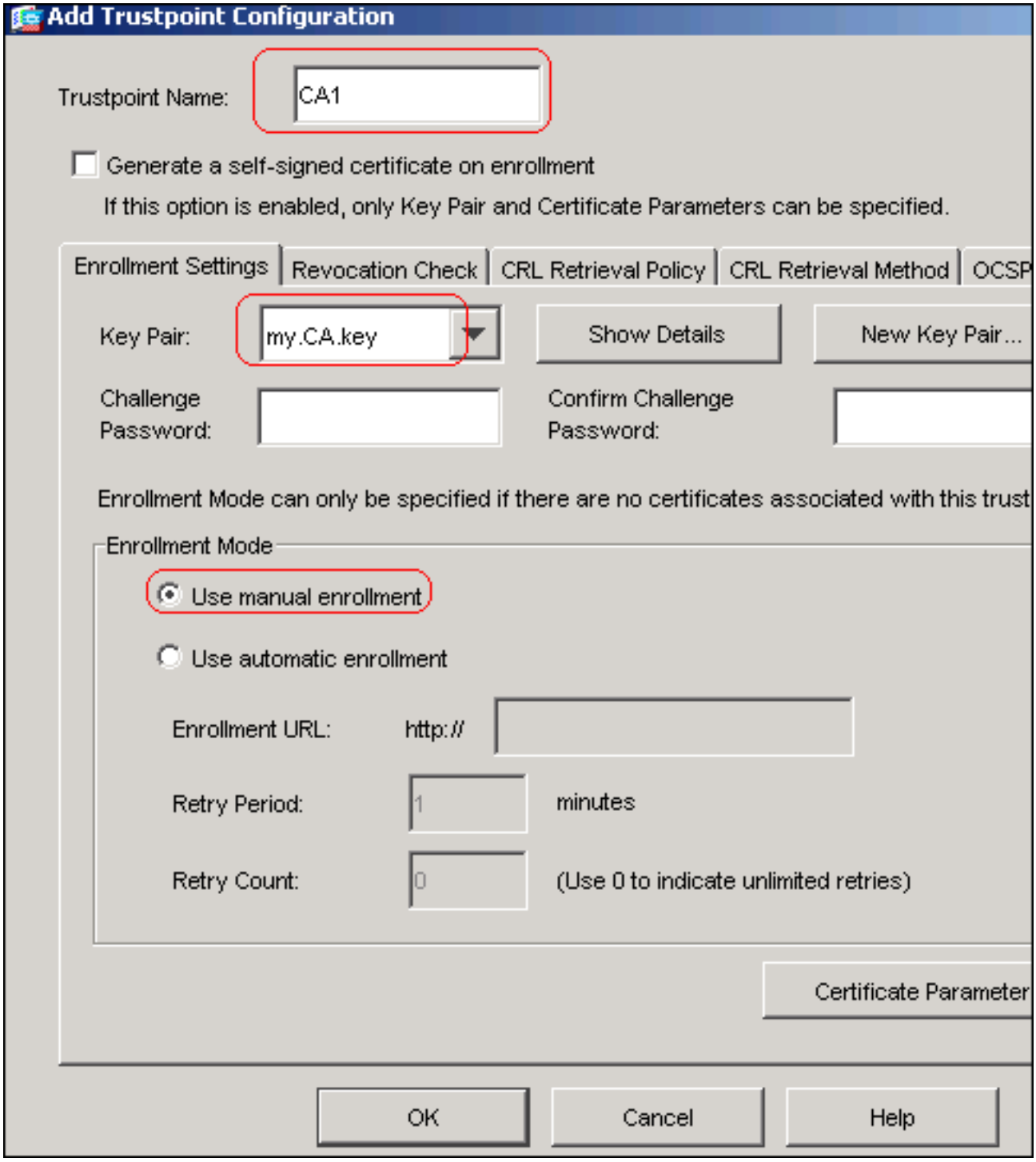


8. 新增適當的值後，按一下**確定**。
9. 在「證書引數」對話方塊中，在「指定FQDN」欄位中輸入FQDN。此值應與用於公用名



(CN)的FQDN相同。

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**」。



命令列示例

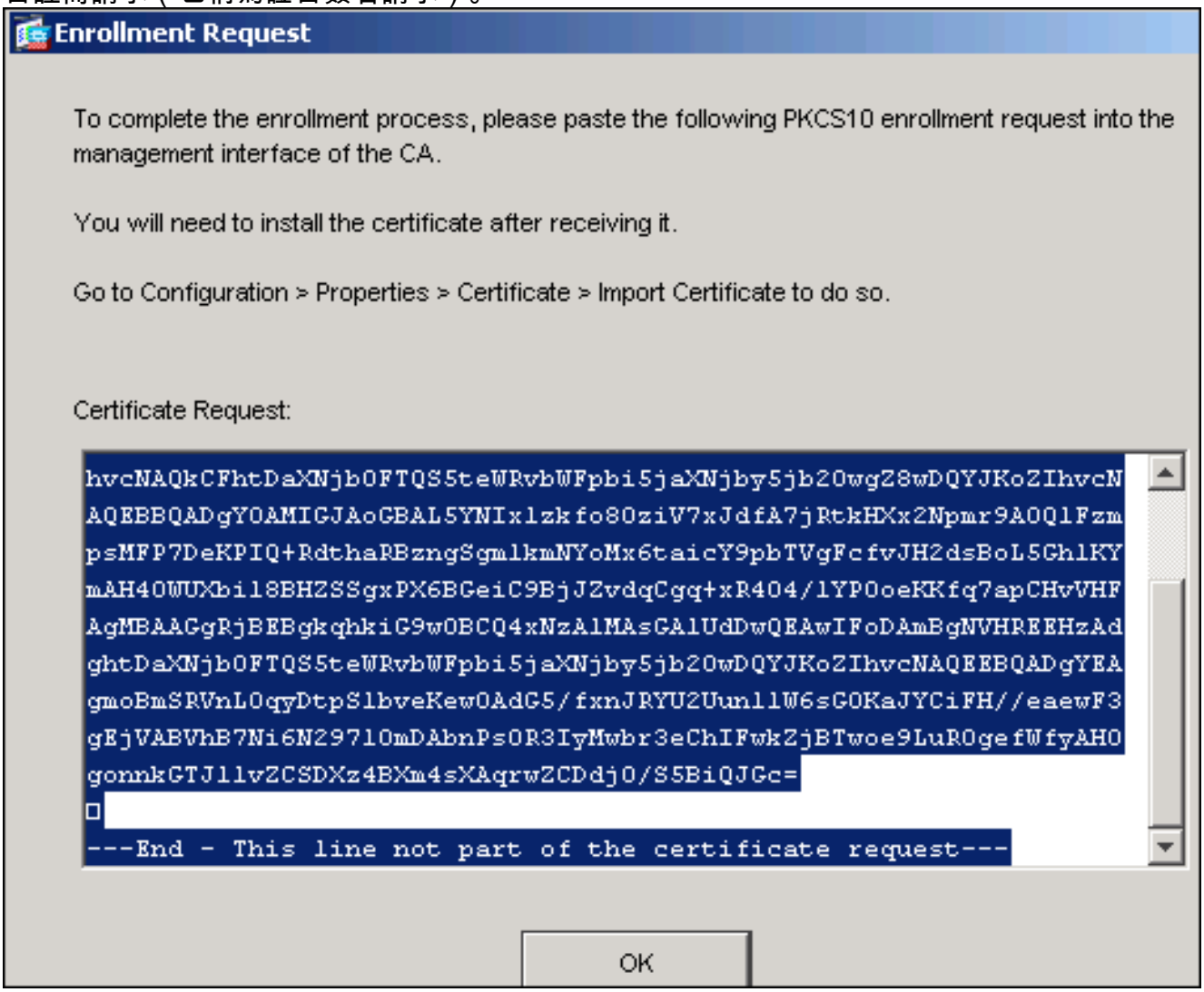
CiscoASA
CiscoASA(config)#**crypto ca trustpoint CA1** *!--- Creates the trustpoint.* CiscoASA(config-ca-trustpoint)#**enrollment terminal** *!--- Specifies cut and paste enrollment with this trustpoint.* CiscoASA(config-ca-trustpoint)#**subject-name CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh** *!--- Defines x.500 distinguished name.* CiscoASA(config-

```
ca-trustpoint)#keypair my.CA.key

!--- Specifies key pair generated in Step 2.
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com


!--- Specifies subject alternative name (DNS:).
CiscoASA(config-ca-trustpoint)#exit
```

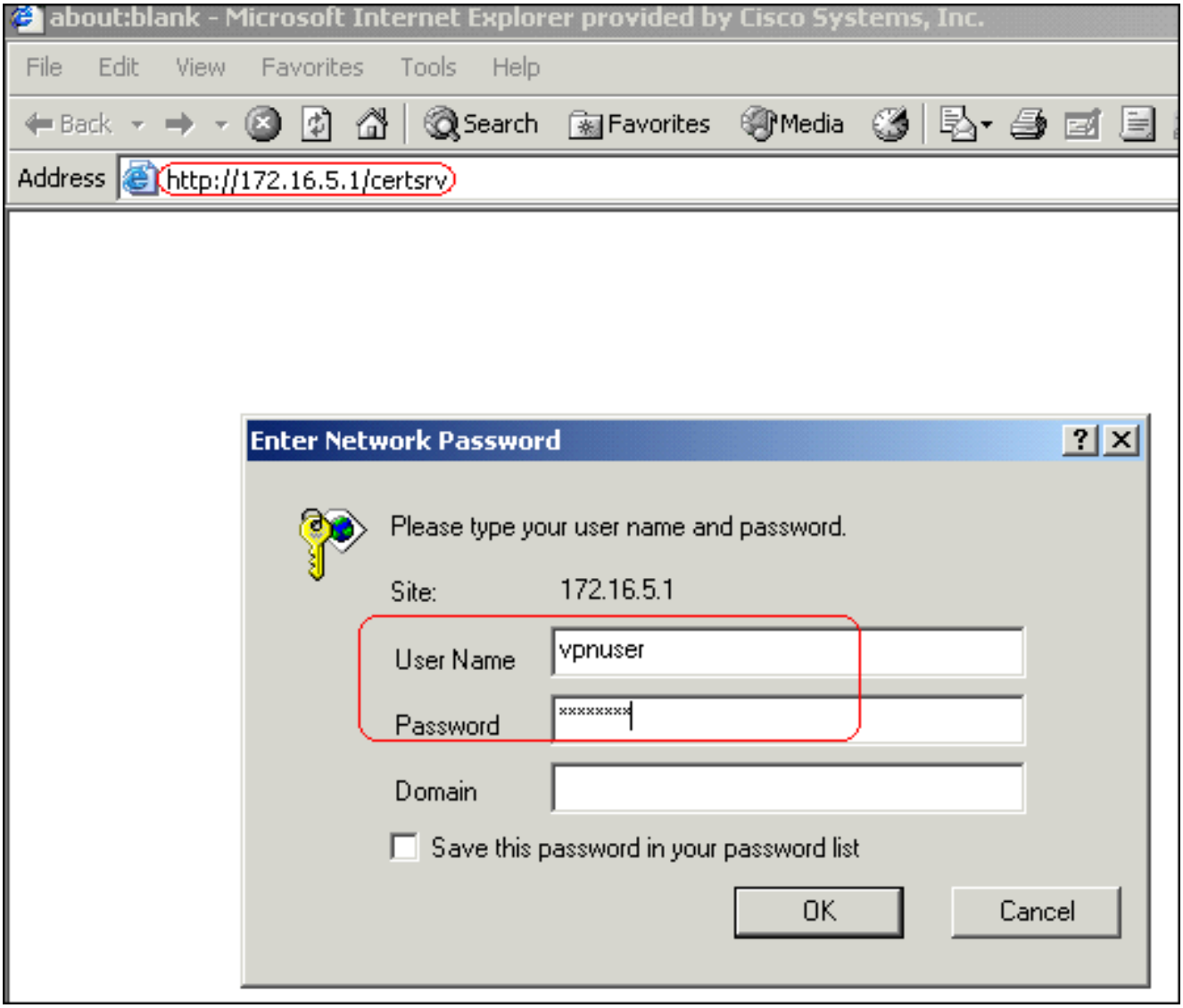
步驟4.生成證書註冊

ASDM過程

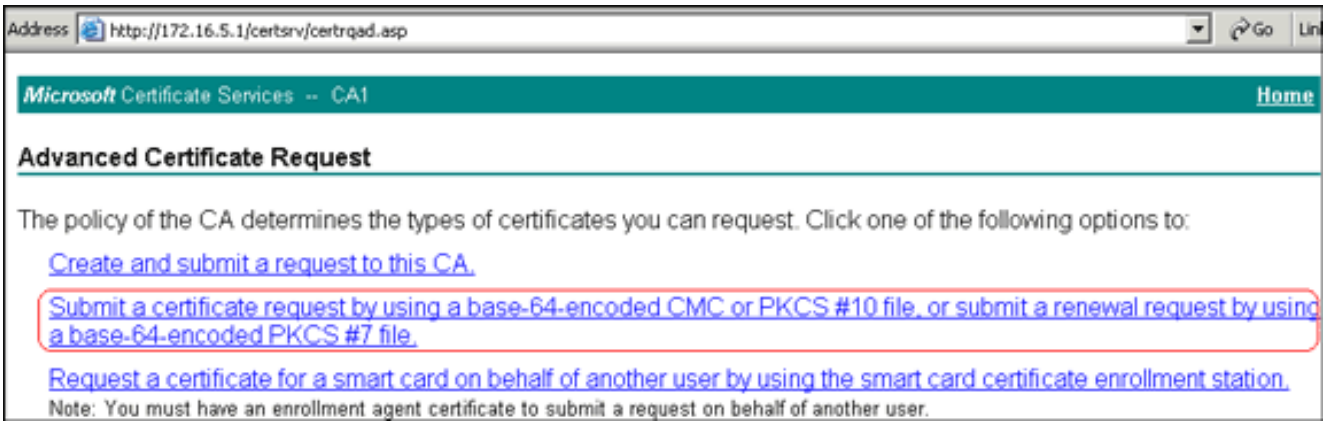
1. 按一下**Configuration**，然後按一下**Properties**。
2. 展開**Certificate**，然後選擇**Enrollment**。
3. 驗證是否已選中步驟3中建立的信任點，然後按一下**Enroll**。出現一個對話方塊，其中列出了證書註冊請求（也稱為證書簽名請求）。



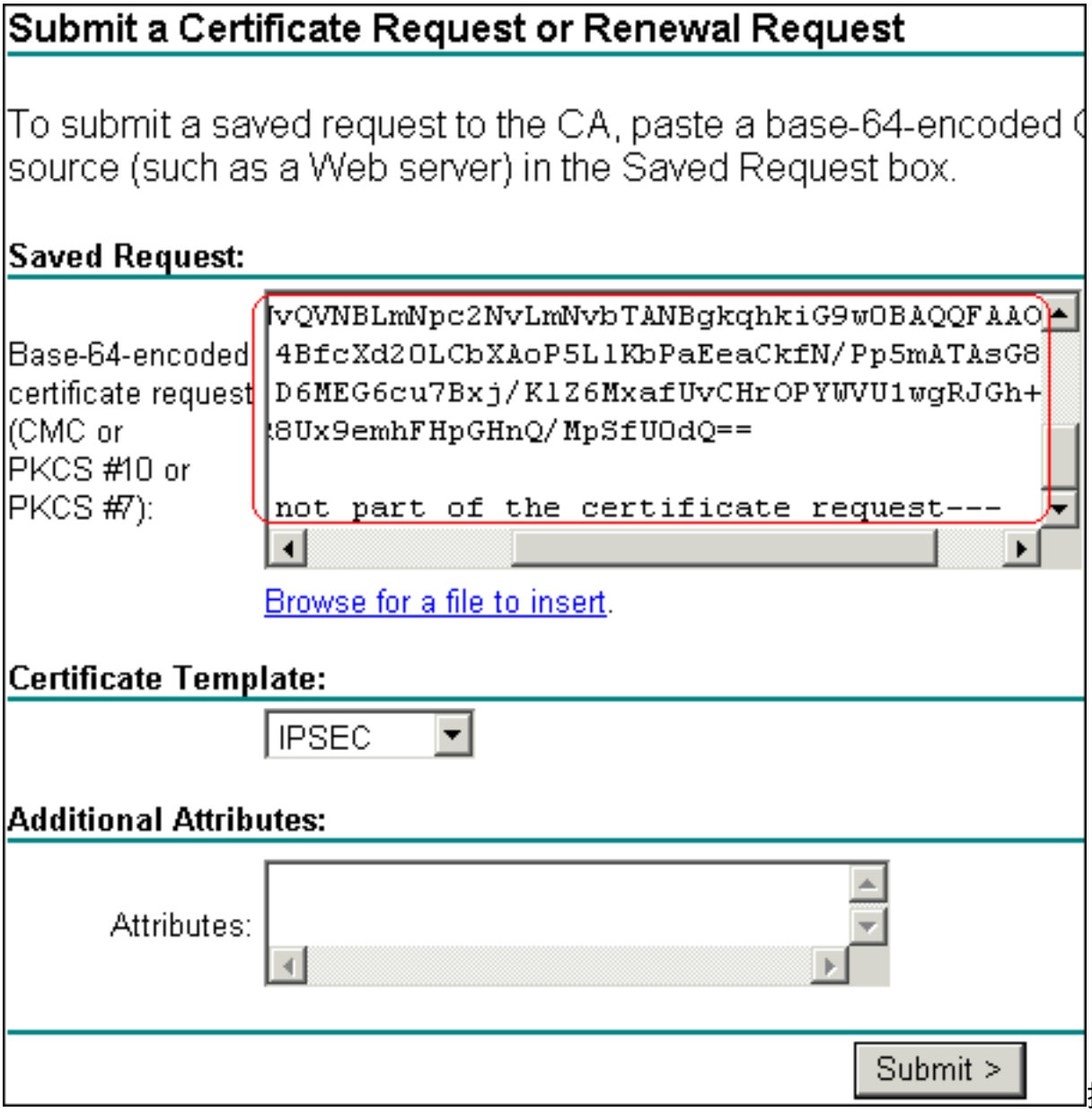
4. 將PKCS#10註冊請求複製到文本檔案，然後將儲存的CSR提交給您的第三方供應商（例如Microsoft CA），如以下過程所示：使用提供給vpn伺服器的使用者憑據登入到CA伺服器172.16.5.1。



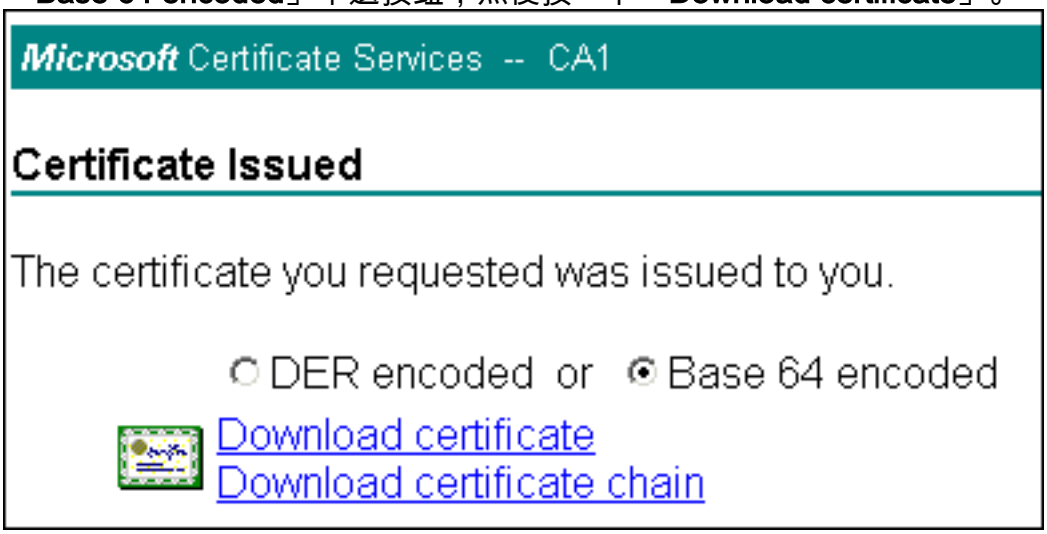
注意：確保您在CA伺服器中擁有ASA（vpn伺服器）的使用者帳戶。按一下**Request a certificate > advanced certificate request**，然後選擇**Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file**。



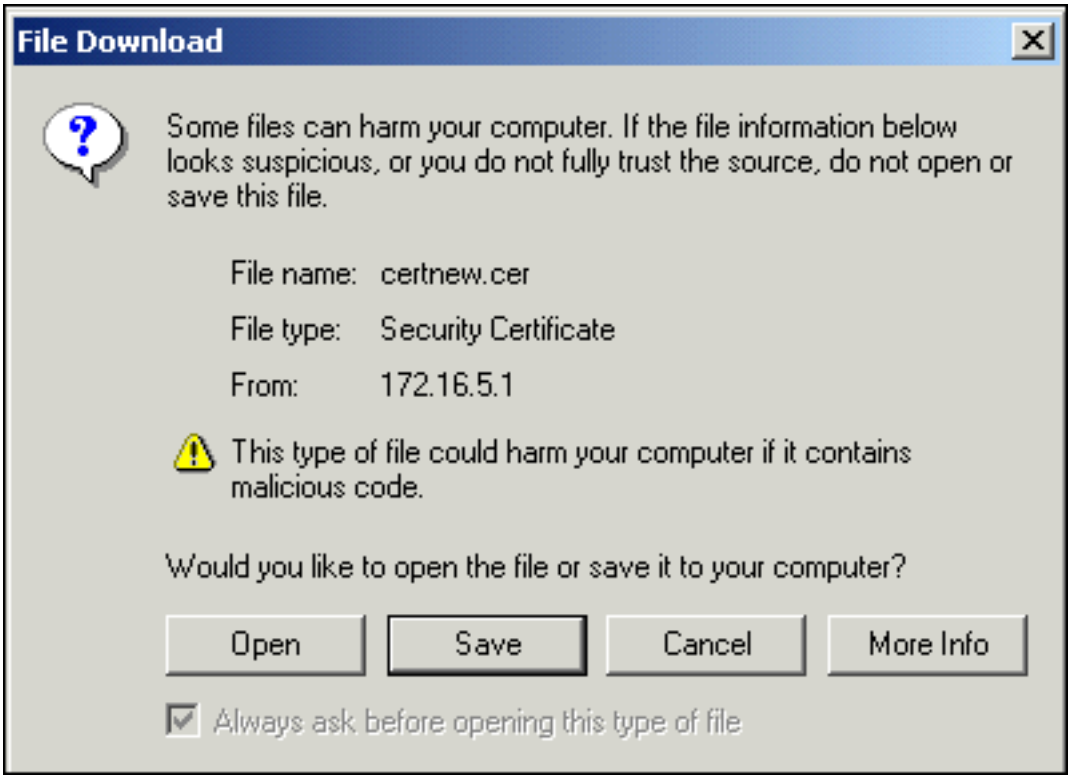
將編碼的資訊複製並貼上到**Saved Request**文本欄位中，然後按一下**Submit**。



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



出現「File Download（檔案下載）」對話方塊時，使用**cert_client_id.cer**名稱儲存該對話方塊，該名稱是要安裝在ASA上的身份證書。



命令列示例

CiscoASA

```
CiscoASA(config)#crypto ca enroll CA1

!--- 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=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]: 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]: no
ciscoasa(config)#
```

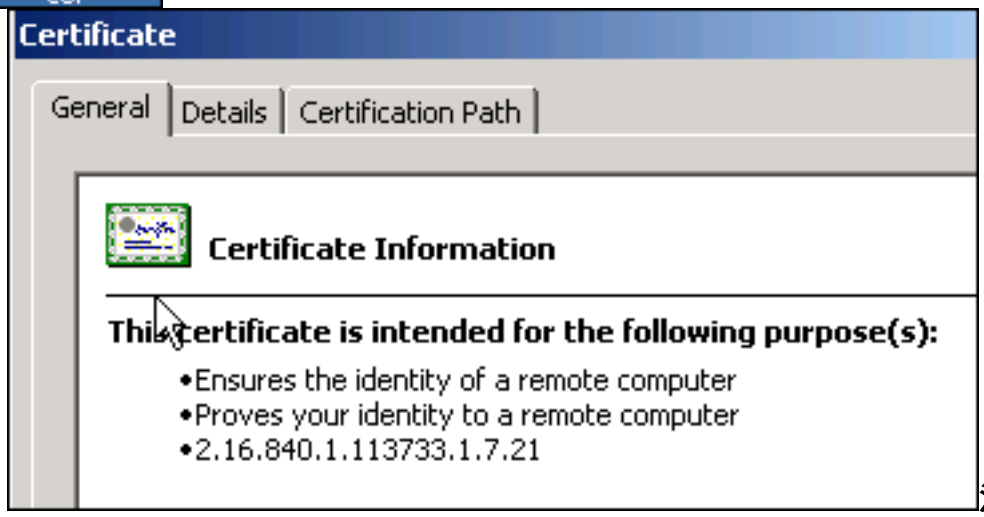
步驟5.驗證信任點

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

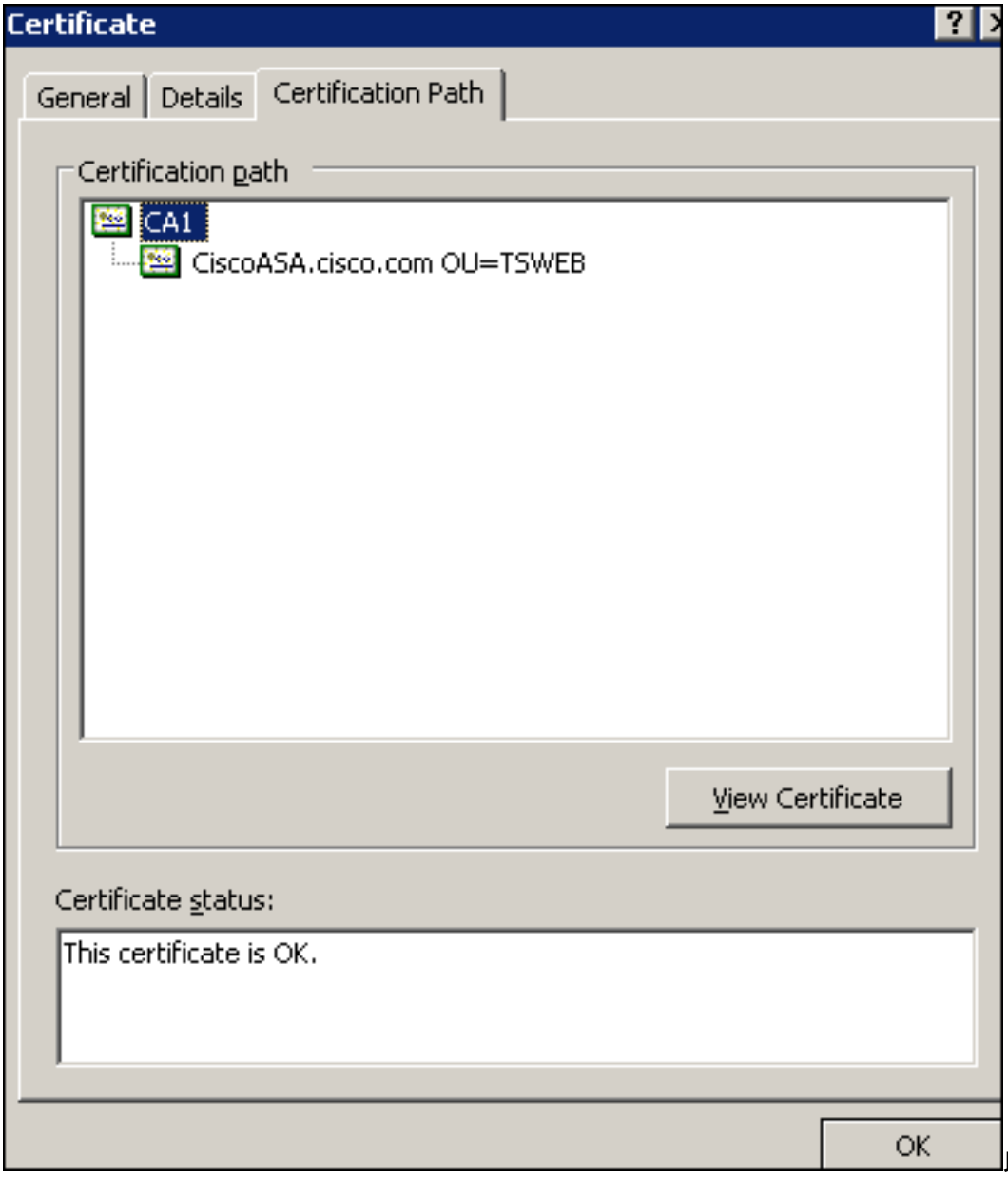
1. 將身份證書儲存到本地電腦。
2. 如果您獲得的base64編碼證書不是作為檔案提供的，則必須複製base64消息並將其貼上到文本檔案中。
3. 將檔案重新命名為.cer副檔名。**注意**：使用.cer副檔名重新命名檔案後，檔案圖示應顯示為證書，如圖所示。

4. 按兩下證書檔案。



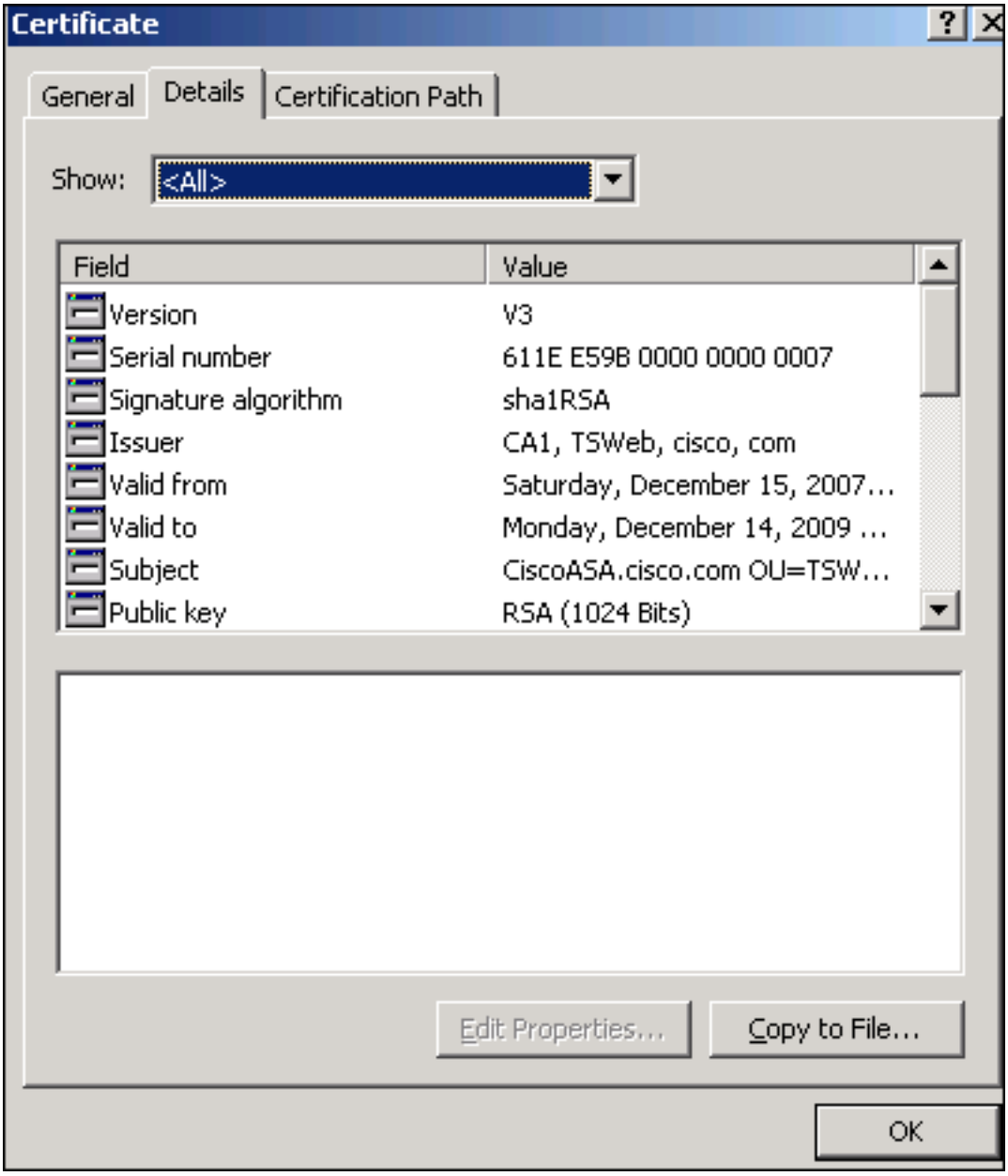
注意：如果「常規」頁籤中出現「Windows does not have enough information to verify this certificate」消息，則必須先獲取第三方供應商根CA或中間CA證書，然後才能繼續此過程。請聯絡您的第三方供應商或CA管理員，以獲取頒發的根CA或中間CA證書。

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**。

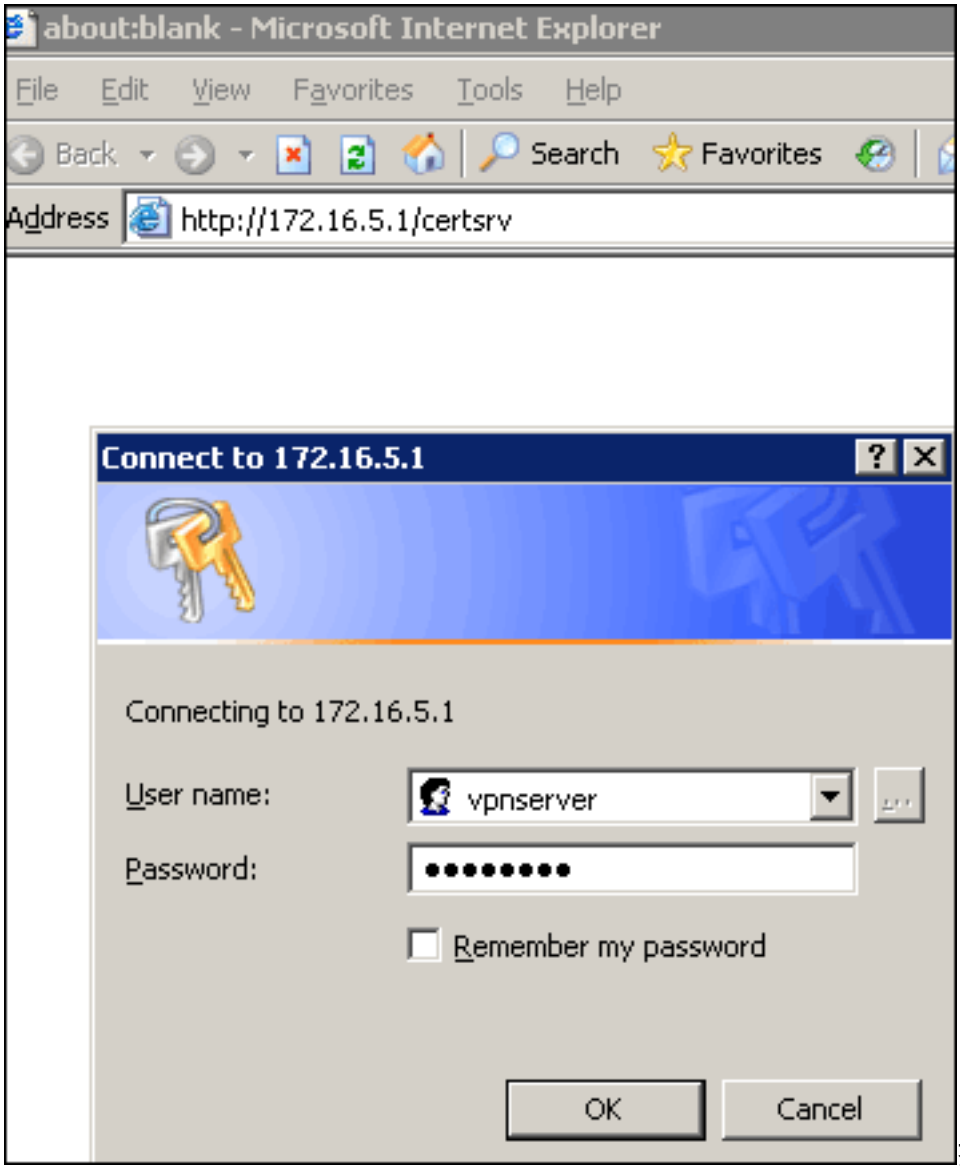


此時將顯示有關CA證書的詳細資訊。

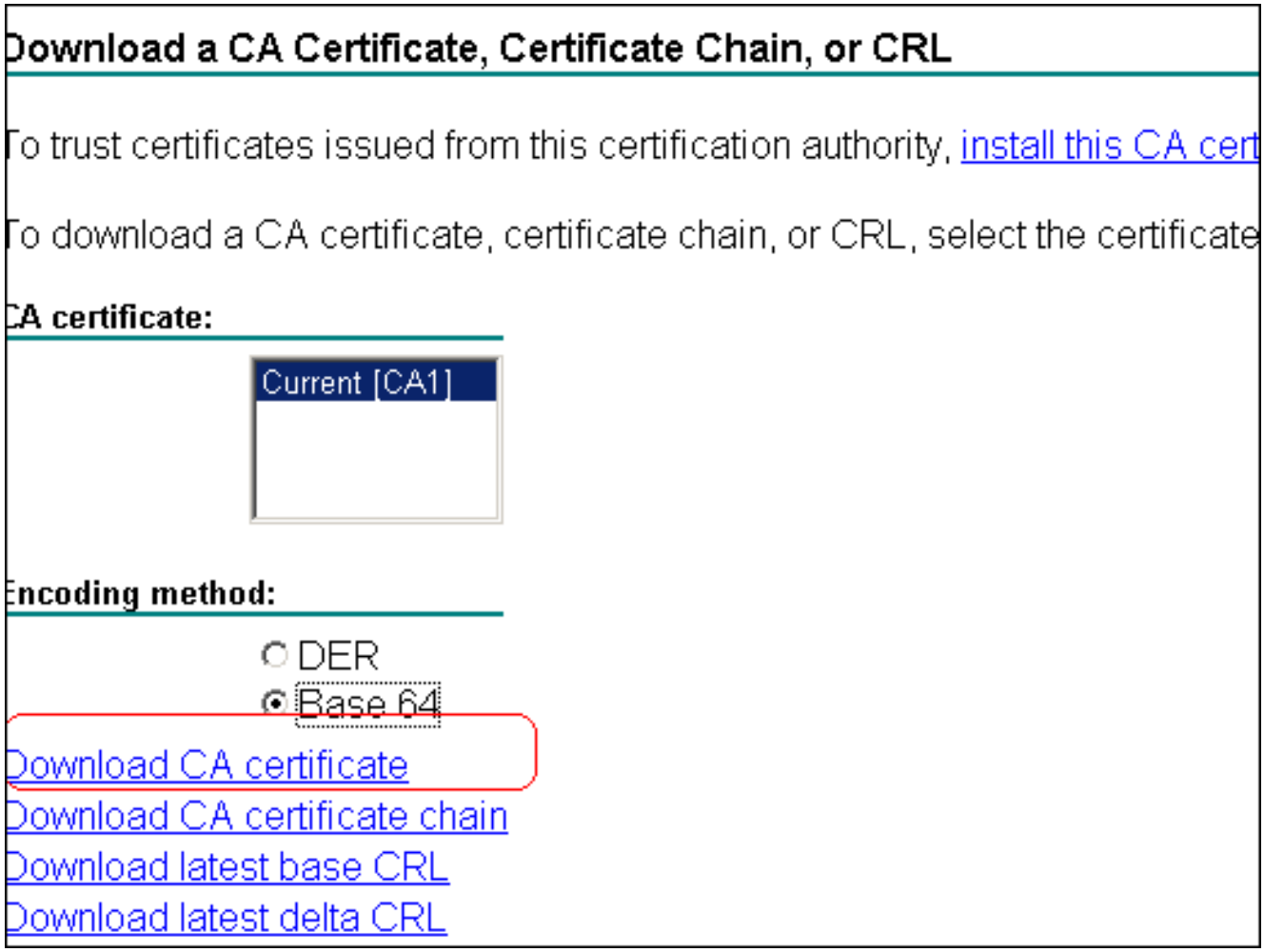
7. 按一下**Details**以瞭解有關身份證書的詳細資訊。



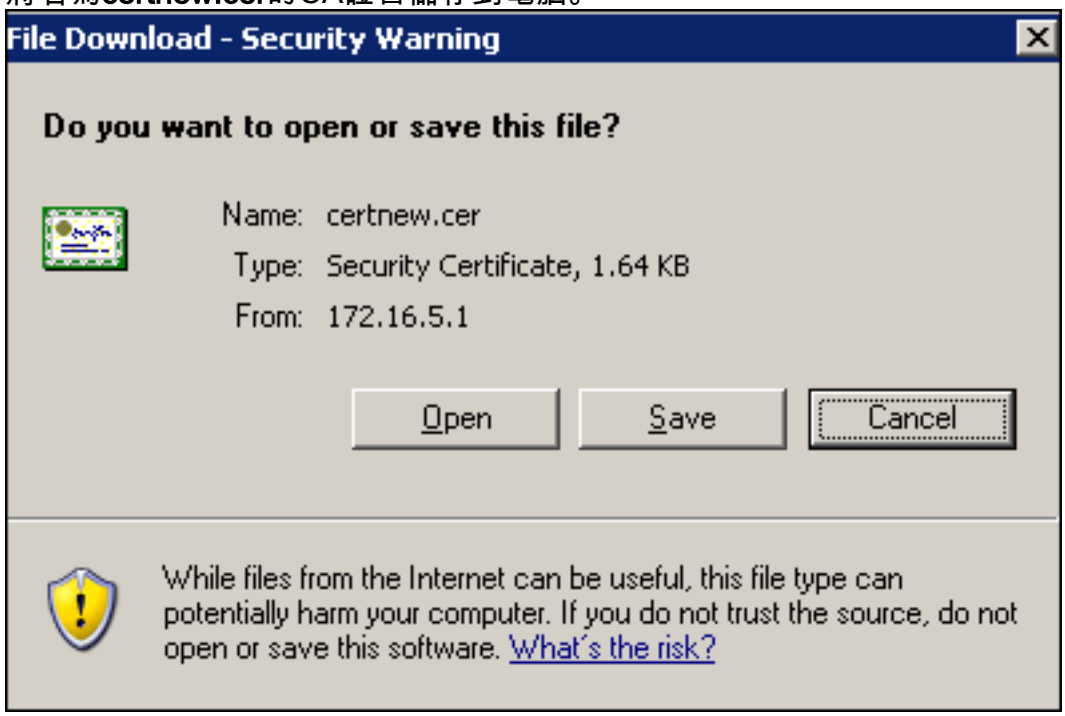
8. 在安裝身份證書之前，必須從CA伺服器下載CA證書並將其安裝在ASA中。完成以下步驟，從名為*CA1*的CA伺服器下載CA憑證：使用向vpn伺服器提供的使用者憑據登入到CA伺服器



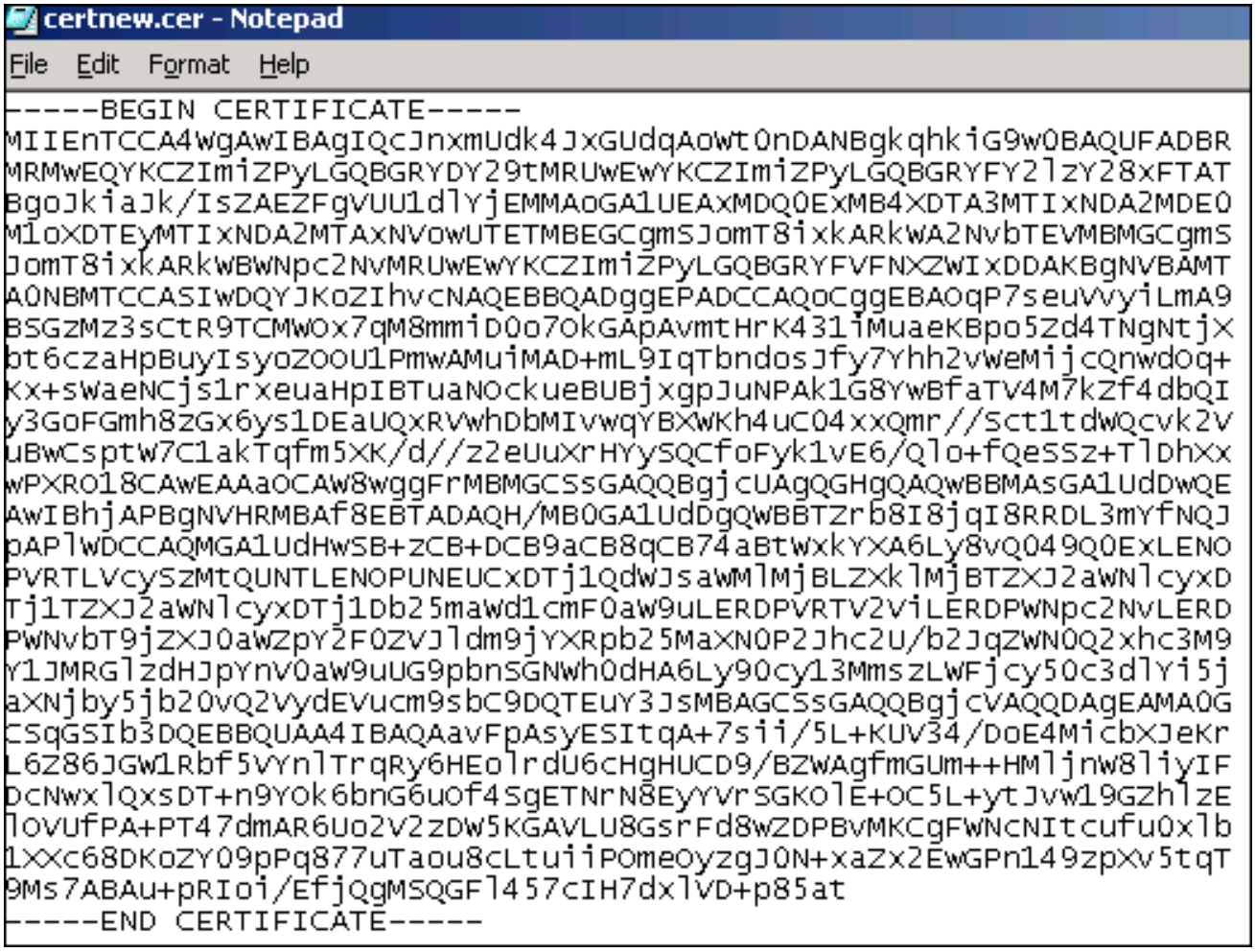
172.16.5.1。按一下「**Download a CA certificate， certificate chain or CRL**」，然後選擇「**Base 64**」單選按鈕以指定編碼方法。按一下「**Download CA certificate**」。



將名為**certnew.cer**的CA證書儲存到電腦。



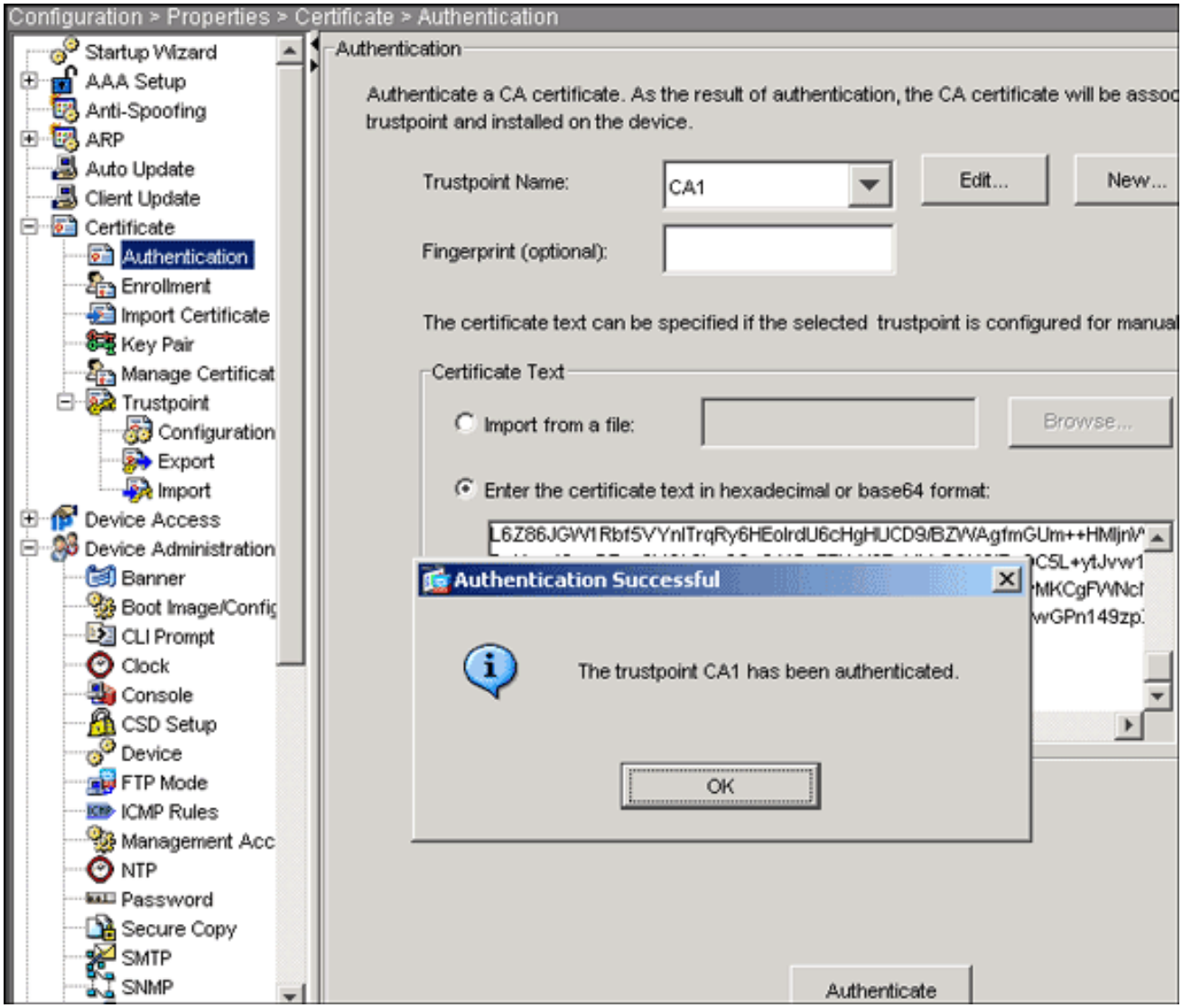
9. 瀏覽到儲存CA證書的位置。
10. 使用文字編輯器（例如記事本）開啟檔案。(按一下右鍵該檔案，然後選擇**「傳送到」>「記事本」**。)
11. Base64編碼的訊息應該顯示與此圖中的憑證類似
    :


certnew.cer - Notepad

File Edit Format Help

```
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAKBgNVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuVvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMijcQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1tdWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMASGA1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNwh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMljnW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw19GZhlzE
lOvUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8WZDPBvMKCgFWNcNItcufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+p85at
-----END CERTIFICATE-----
```

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



17. 按一下「OK」（確定）。

命令列示例

CiscoASA

```
CiscoASA(config)#crypto ca authenticate CA1


!--- 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-----
MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lz
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK
BgNVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
```

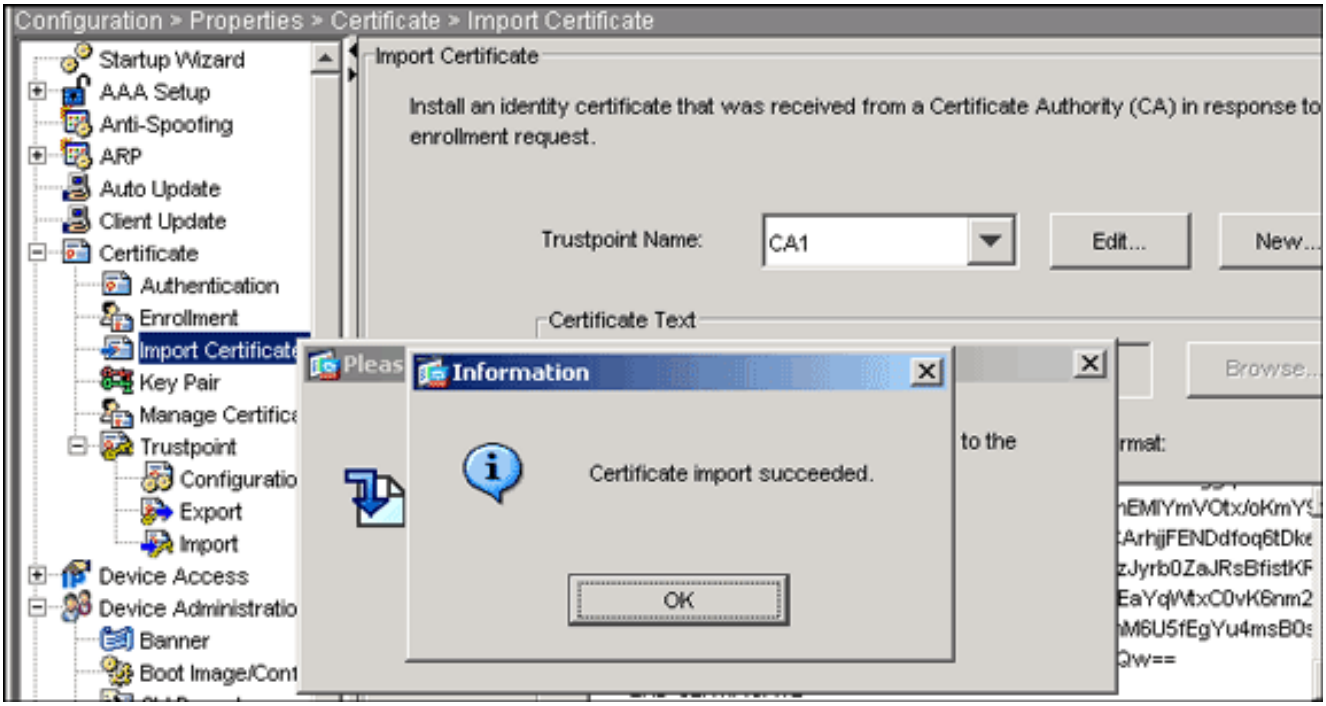
```
cQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSS
z+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
L3mYfNQJ
pAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2
aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMlj
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
cufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
zpXv5tqT
9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+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 CA1 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:
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 3rd party vendor. -----BEGIN CERTIFICATE-----
MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoXDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0
ZW1zMSQw
IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
KoZIhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ2lz
Y29BU0Eu
Y2lzY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KMl0xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAPlWDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
```

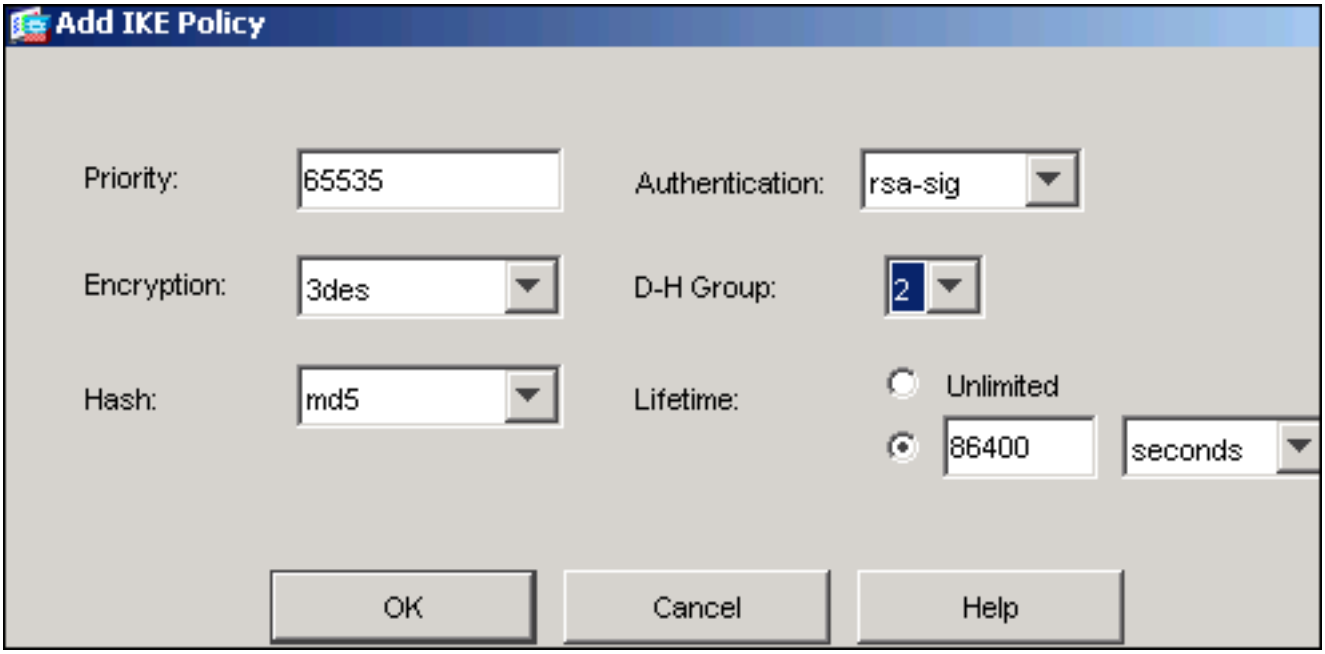
```
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy4l8EHe4MJbdjUp/b90l5l6IzQP
5l51YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc
lL5nuPsd8MaexBc=
-----END CERTIFICATE-----
quit

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

步驟7.配置遠端訪問VPN(IPSec)以使用新安裝的證書

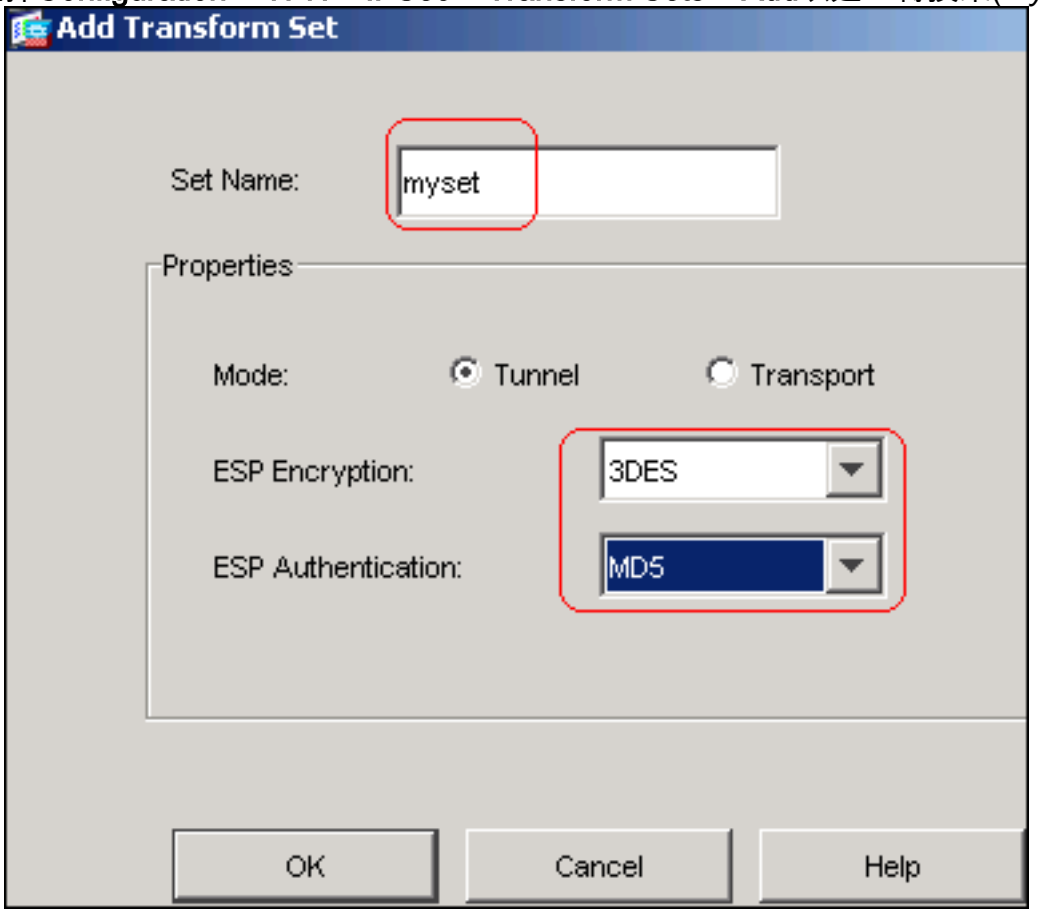
ASDM過程

完成以下步驟以配置遠端訪問VPN:

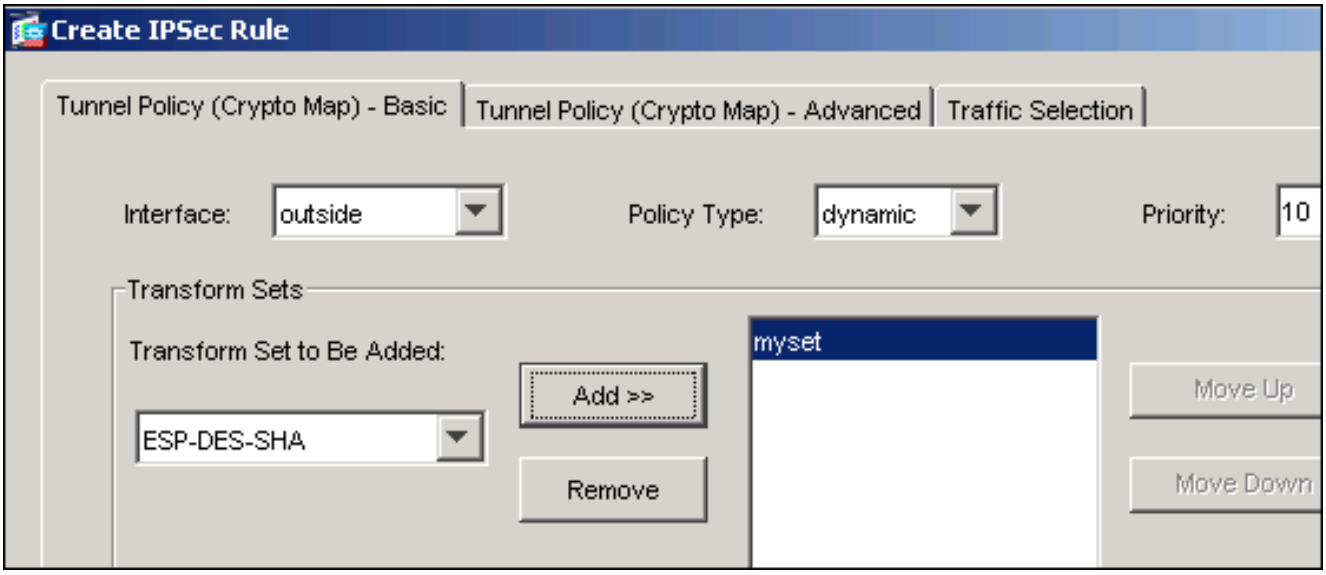
1. 選擇**Configuration > VPN > IKE > Policies > Add**以建立ISAKMP策略組65535，如下圖所示。



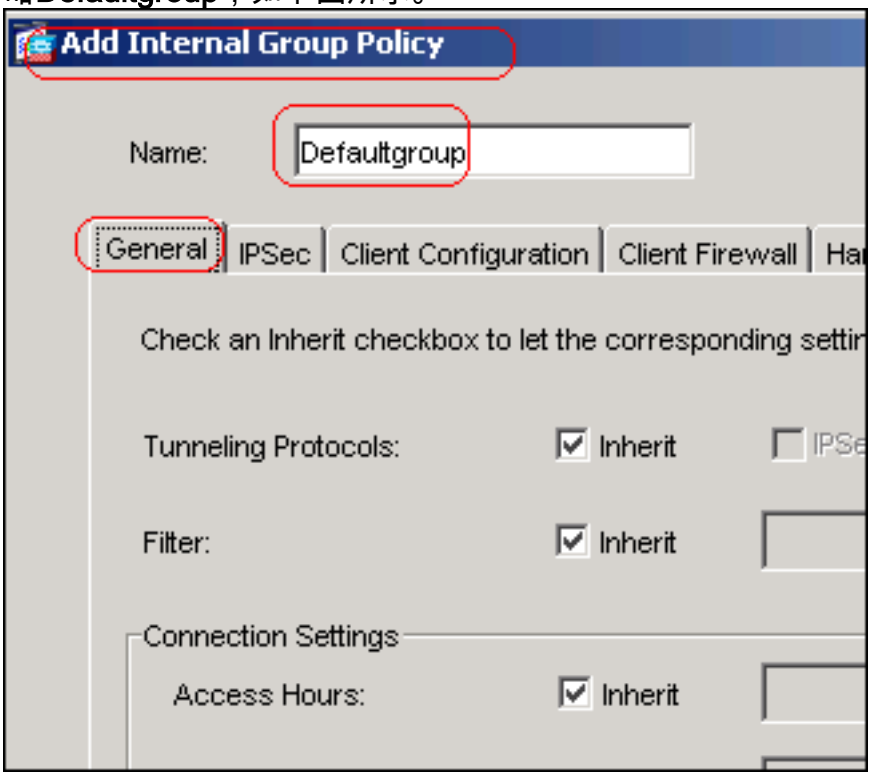
2. 按一下「**OK**」，然後按一下「**Apply**」。
3. 選擇**Configuration > VPN > IPSec > Transform Sets > Add**以建立轉換集(*myset*)，如下圖所示：

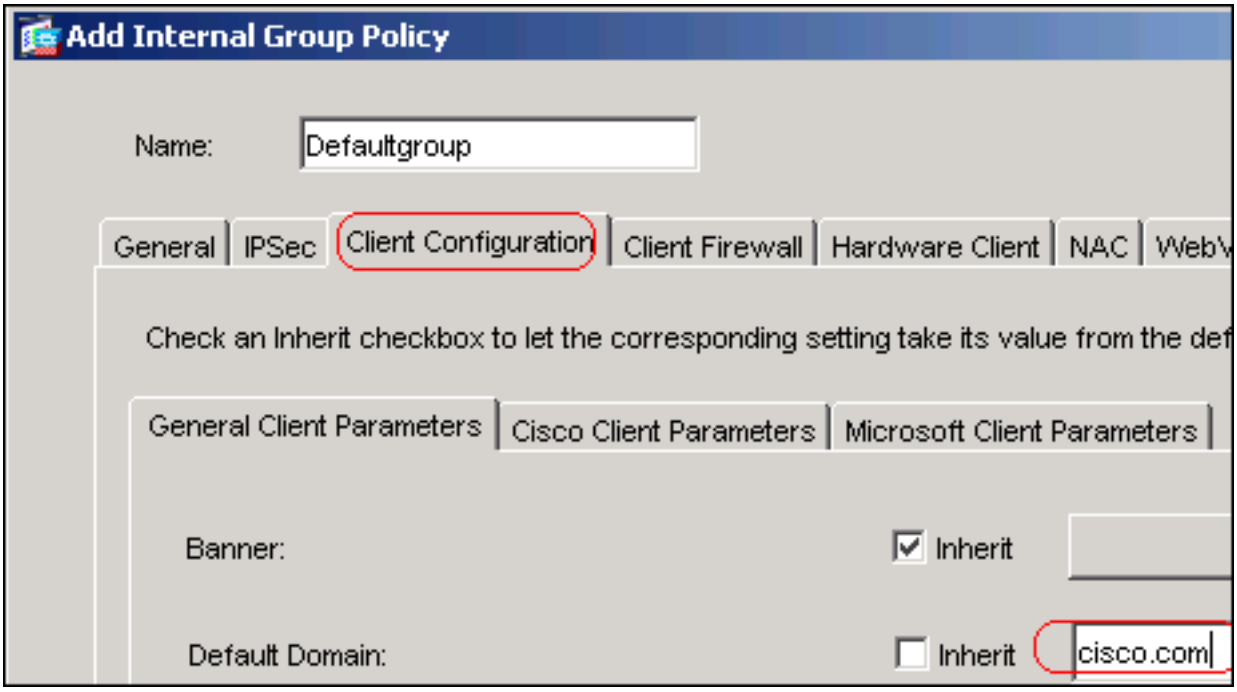


4. 按一下「**OK**」，然後「**Apply**」
5. 選擇**Configuration > VPN > IPSec > IPSec Rules > Add**，以使用優先順序為10的動態策略建立加密對映，如下圖所示：

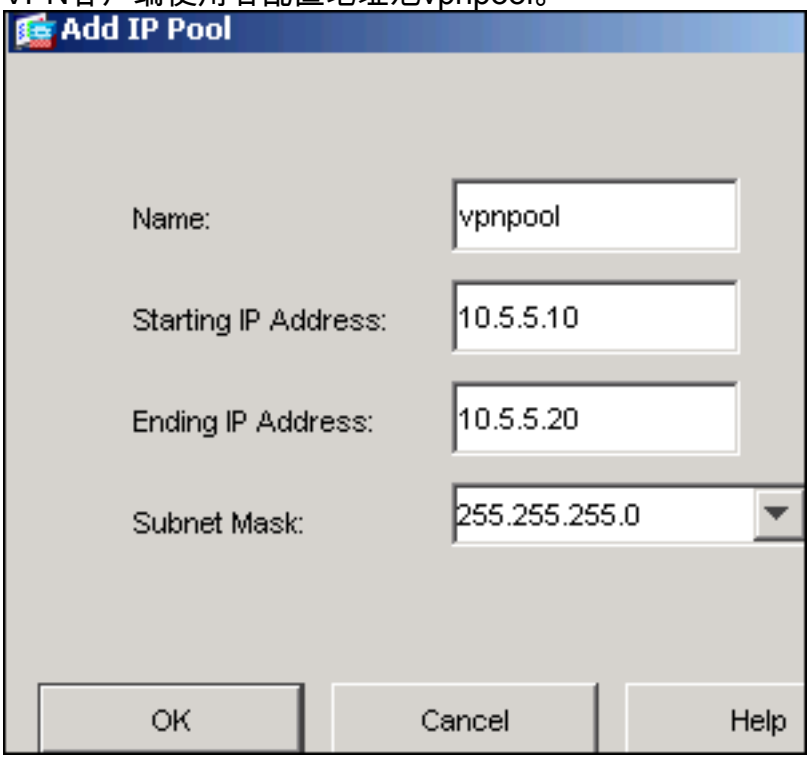


6. 按一下「**OK**」，然後「**Apply**
7. 選擇**Configuration > VPN > General > Group Policy > Add Internal Group Policy**，以建立組策略**Defaultgroup**，如下圖所示。

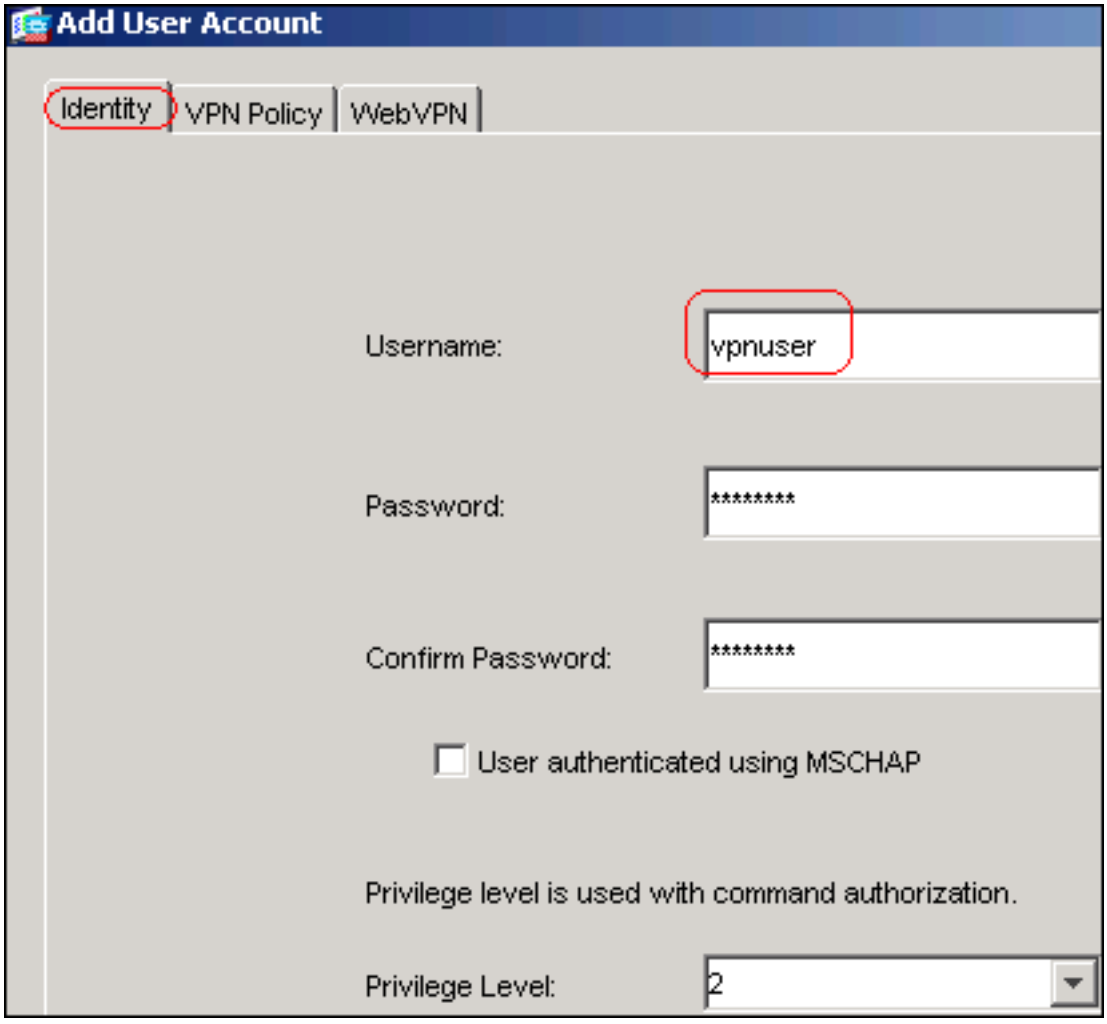




8. 按一下「**OK**」，然後「**Apply**
9. 選擇**Configuration > VPN > IP Address Management > IP Pools > Add**，為要動態分配的VPN客戶端使用者配置地址池vpnpool。

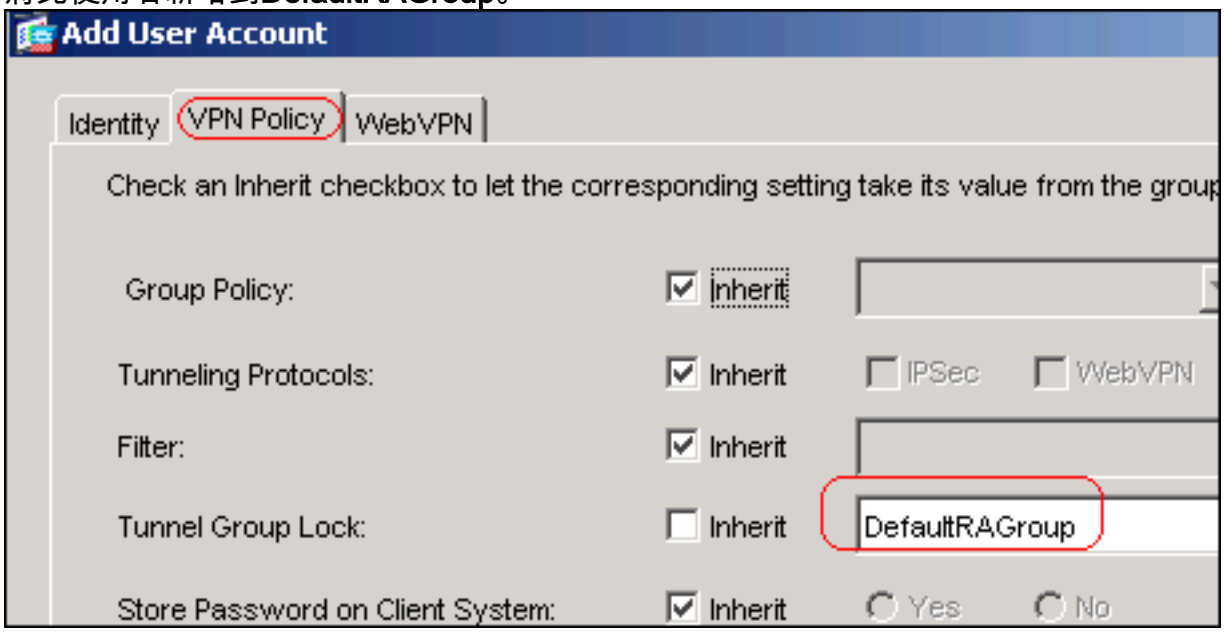


10. 按一下「**OK**」，然後「**Apply**
11. 選擇**Configuration > VPN > General > Users > Add**，以便為VPN客戶端訪問建立使用者帳戶

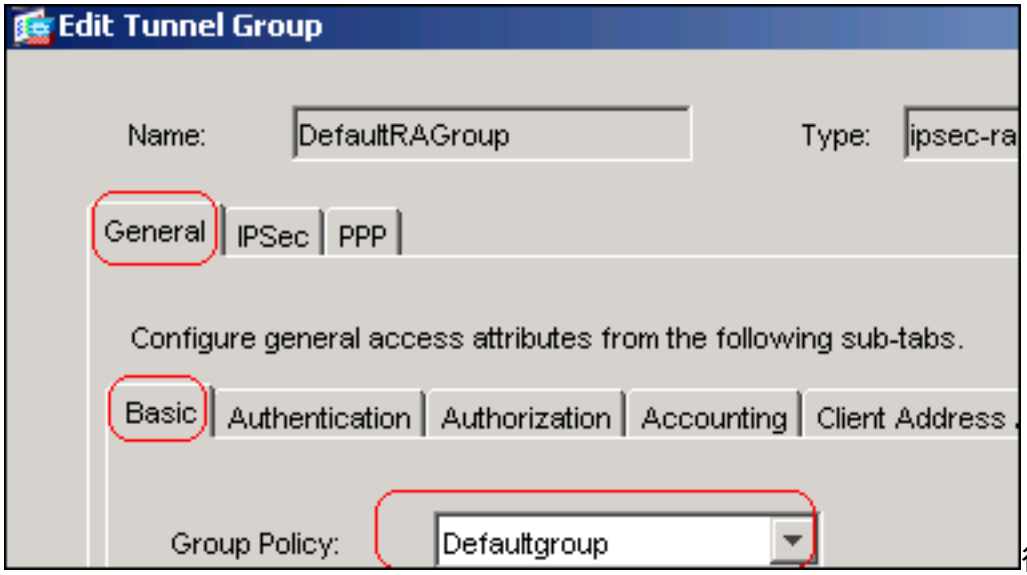


vpnuser。

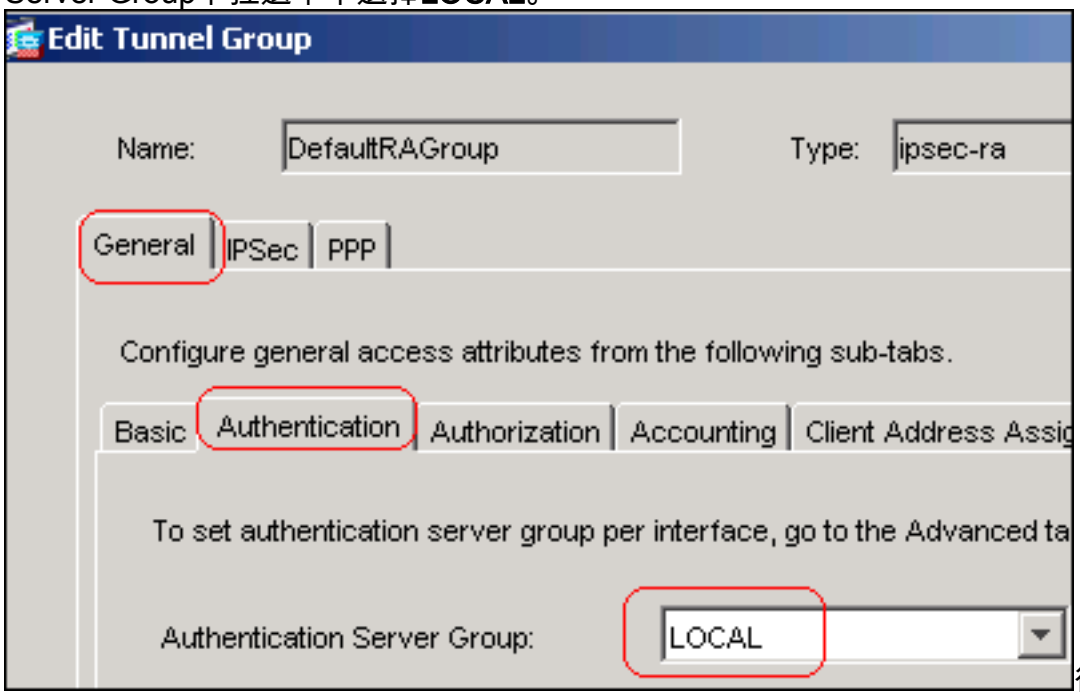
12. 將此使用者新增到**DefaultRAGroup**。



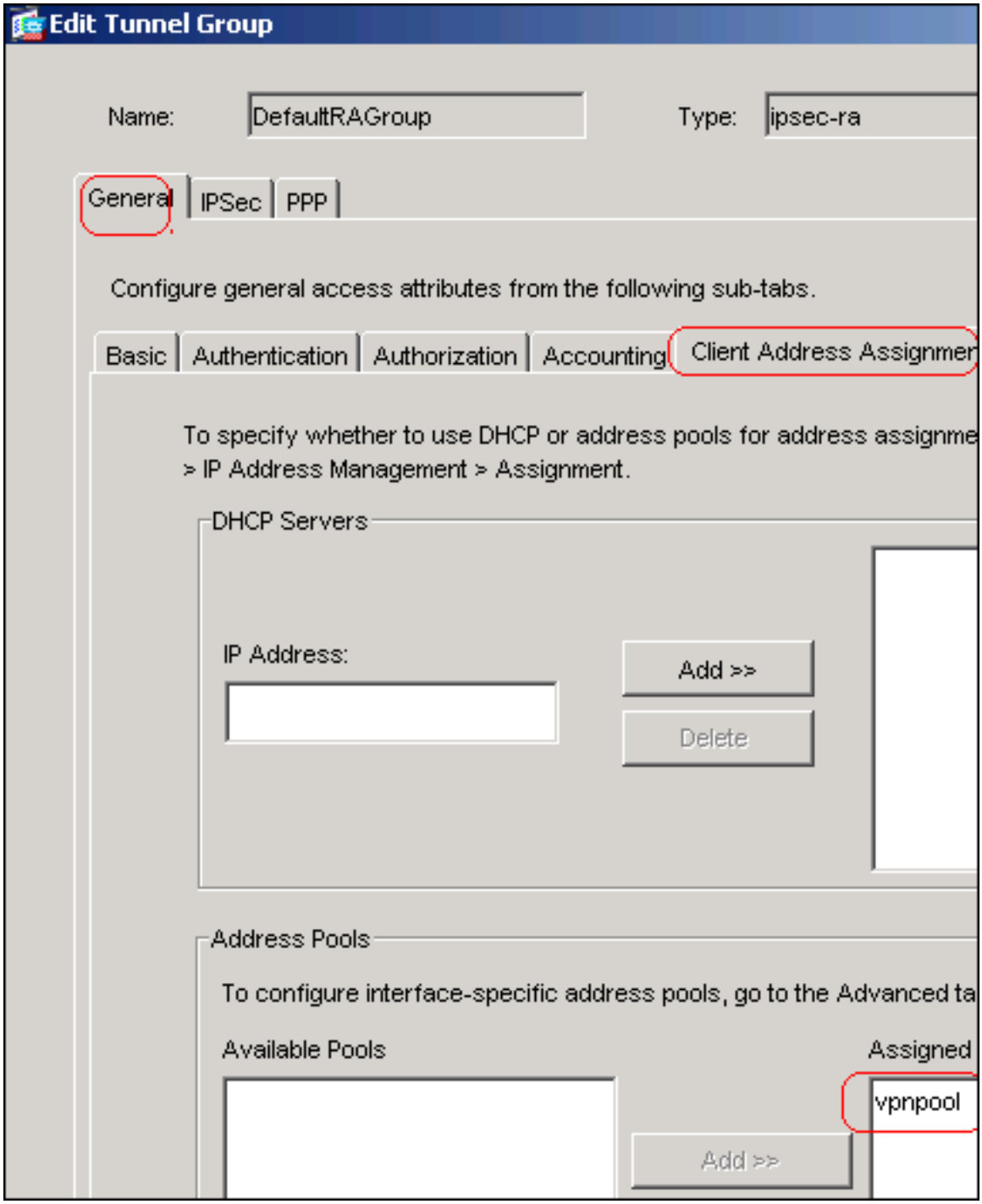
13. 按一下「**OK**」，然後「**Apply**
14. 按以下步驟所述編輯DefaultRAGroup:選擇**Configuration > VPN > General > Tunnel Group > Edit**。從Group Policy下拉選單中選擇**Defaultgroup**。



從Authentication Server Group下拉選單中選擇**LOCAL**。



從Client Address Assignment下拉選單中選擇**vpnpool**。



15. 按一下「**OK**」，然後「**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 outside_dyn_map 10**

```
set transform-set myset
CiscoASA(config)#crypto map outside_map 65535 ipsec-
isakmp dynamic outside_dyn_map
CiscoASA(config)#crypto map outside_map 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 password123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#group-lock value
DefaultRAGroup
CiscoASA(config-username)#exit

!--- Create an user account "vpnuser" and added to
"DefaultRAGroup" 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 7.2(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
boot system disk0:/asa722-k8.bin
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 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
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
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 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
group-policy Defaultgroup internal
group-policy Defaultgroup attributes
 default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
 group-lock value DefaultRAGroup
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 DMZ
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 outside_dyn_map 10 set transform-set
myset
crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map 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=Raleigh
 keypair my.CA.key
 crl configure
crypto ca certificate chain CA1
 certificate 3f14b70b00000000001f
    308205eb 308204d3 a0030201 02020a3f 14b70b00
00000000 1f300d06 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
    37313232 37313430 3033365a 170d3038 31323236
31343030 33365a30 67311330
    11060a09 92268993 f22c6401 19160363 6f6d3115
3013060a 09922689 93f22c64
    01191605 63697363 6f311530 13060a09 92268993
f22c6401 19160554 53576562
    310e300c 06035504 03130555 73657273 31123010
06035504 03130976 706e7365
    72766572 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 0001a382 03313082 032d300b 0603551d
0f040403 02052030 34060355
    1d11042d 302ba029 060a2b06 01040182 37140203
a01b0c19 76706e73 65727665
    72405453 5765622e 63697363 6f2e636f 6d301d06
03551d0e 04160414 2c242ddb
    490cde1a 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 74301506 092b0601
    04018237 14020408 1e060045 00460053 300c0603
551d1301 01ff0402 30003015
    0603551d 25040e30 0c060a2b 06010401 82370a03
04304406 092a8648 86f70d01
    090f0437 3035300e 06082a86 4886f70d 03020202
0080300e 06082a86 4886f70d
    03040202 00803007 06052b0e 03020730 0a06082a
864886f7 0d030730 0d06092a
    864886f7 0d010105 05000382 010100bf 99b9daf2
e24f1bd6 ce8271eb 908fadb3
    772df610 0e78b198 f945f379 5d23a120 7c38ae5d
8f91b3ff 3da5d139 46d8fb6e
    20d9a704 b6aa4113 24605ea9 4882d441 09f128ab
4c51a427 fa101189 b6533eef
    adc28e73 fcfed3f1 f4e64981 0976b8a1 2355c358
a22af8bb e5194b42 69a7c2f6
    c5a116f6 d9d77fb3 a7f3d201 e3cff8f7 48f8d54e
243d2530 31a733af 0e1351d3
    9c64a0f7 4975fc66 a017627c cfd0ea22 2992f463
9412b388 84bf8b33 bd9f589a
    e7087262 a4472e69 775ab608 e5714857 4f887163
705220e3 aca870be b107ab8d
    73faf76d b3550553 1a2b873f 156f9dff 5386c839
1380fda8 945a7f6c c2e9d5c8
    83e2e761 394dd4da 63eaefc6 a44df5
  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
```

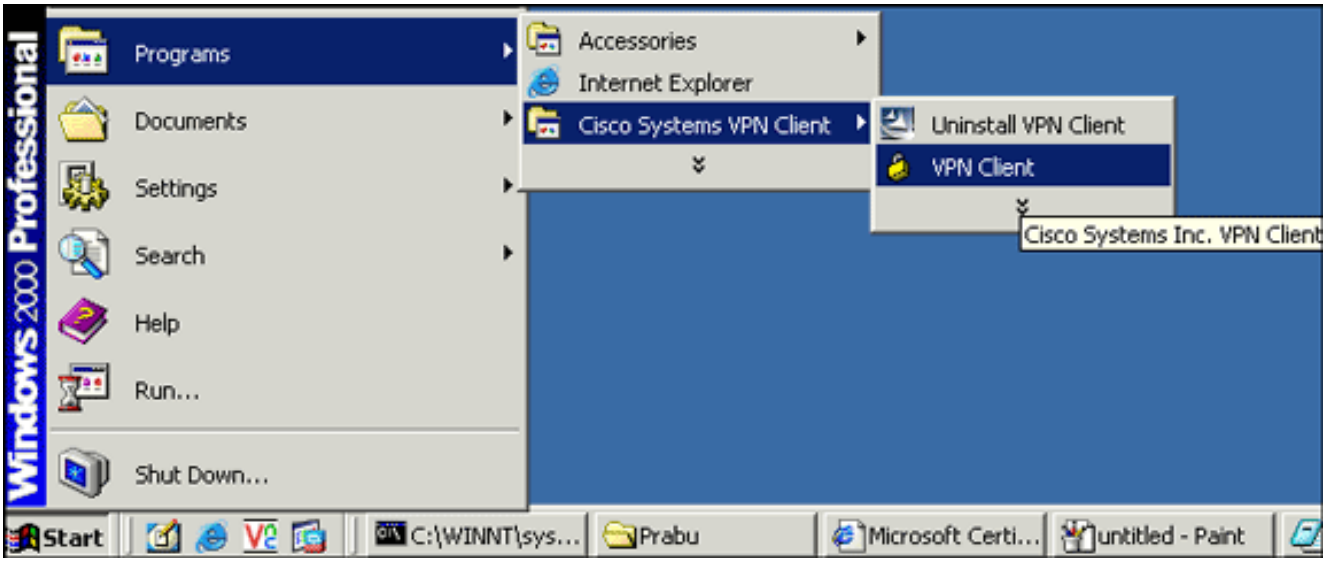
```
0a099226 8993f22c 64011916
    05545357 6562310c 300a0603 55040313 03434131
30820122 300d0609 2a864886
    f70d0101 01050003 82010f00 3082010a 02820101
00ea8fee c7ae56fc a22e603d
    0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d
28ece906 02902f9a d1eb2b8d
    f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
a1e906ec 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
tunnel-group DefaultRAGroup general-attributes
 address-pool vpnpool
 default-group-policy Defaultgroup
tunnel-group DefaultRAGroup ipsec-attributes
 trust-point CA1
telnet timeout 5
ssh timeout 5
console timeout 0
!
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
prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0
: end
CiscoASA#
```

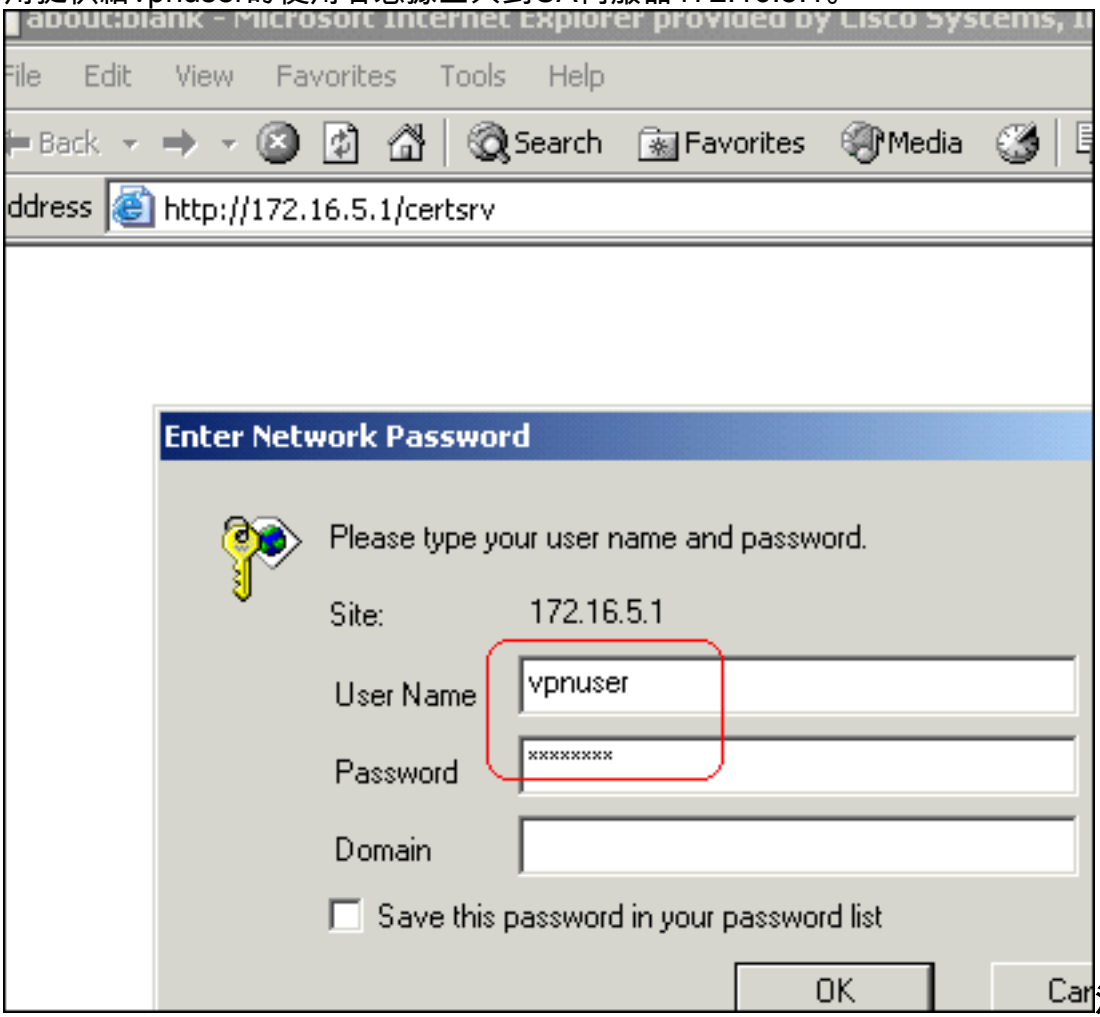
VPN客戶端配置

完成以下步驟以配置VPN客戶端：

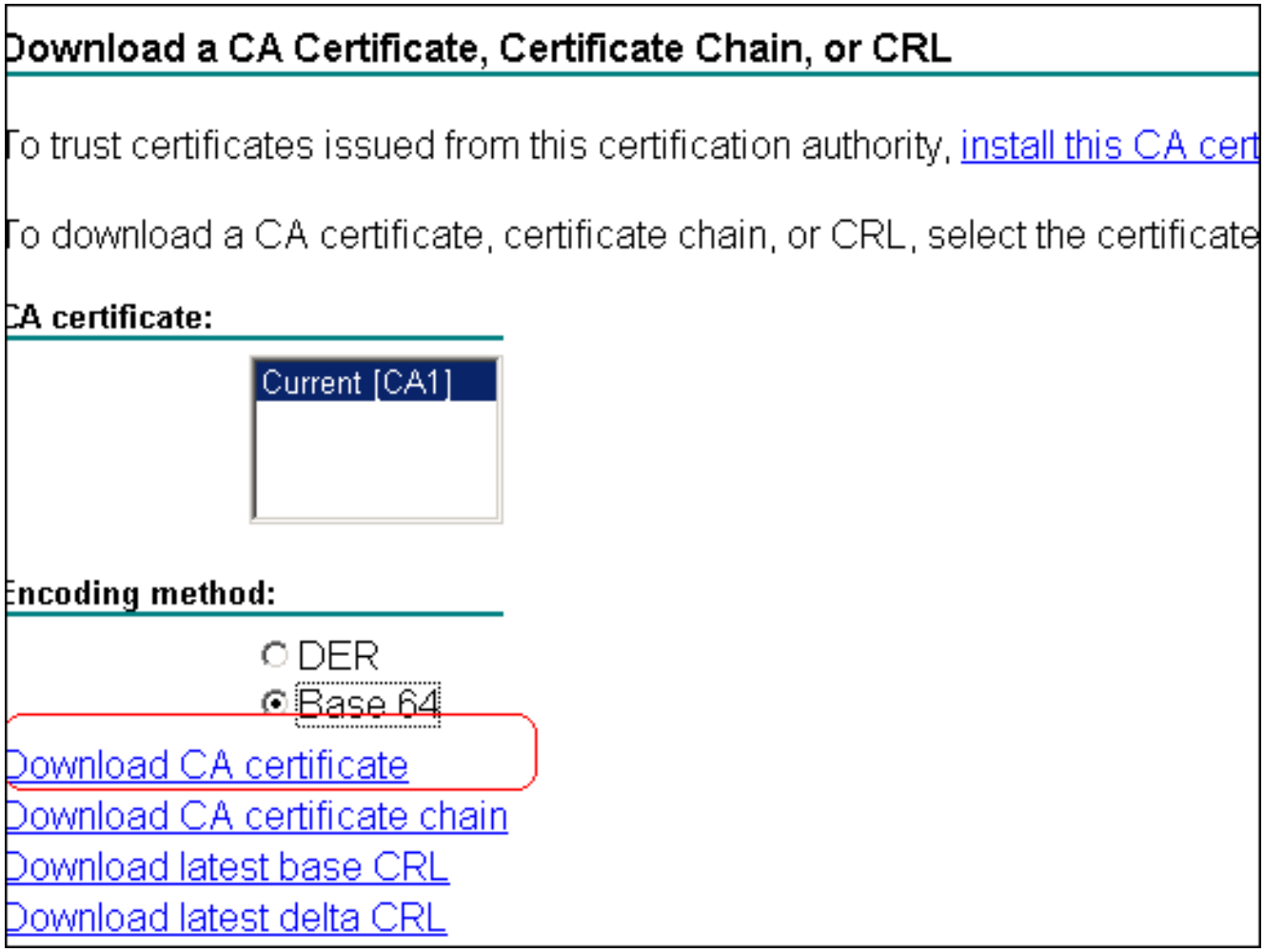
1. 選擇**Start > Programs > Cisco Systems VPN Client > VPN Client**以啟動VPN客戶端軟體。



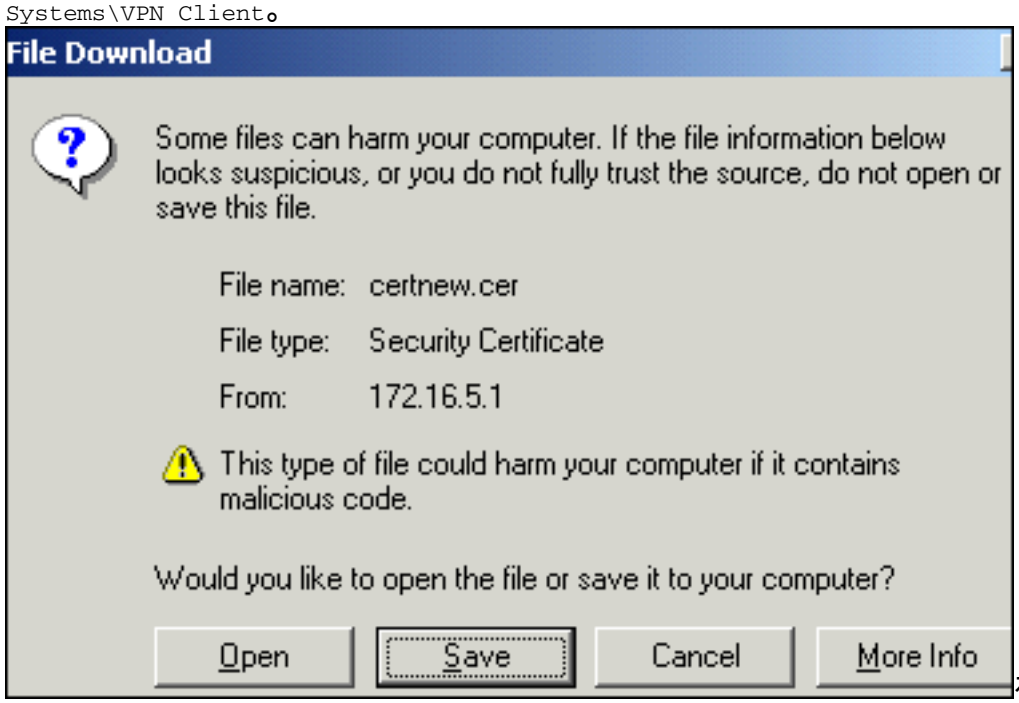
2. 完成以下步驟，從名為**CA1**的CA伺服器下載CA憑證，並將其安裝到Cisco VPN使用者端：使用提供給vpnuser的使用者憑據登入到CA伺服器172.16.5.1。



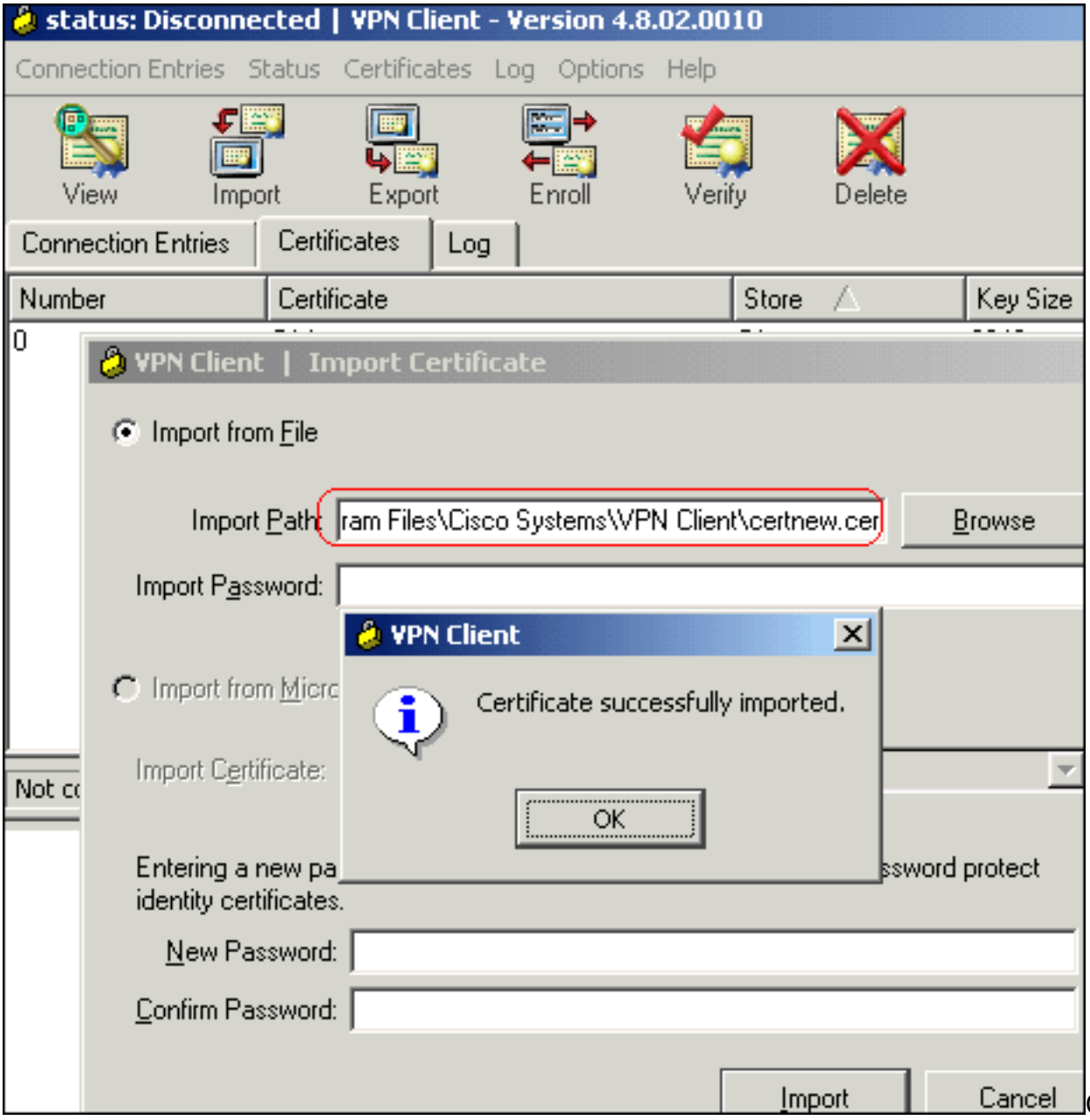
注意：確保您在CA伺服器中擁有VPN客戶端使用者的使用者帳戶。按一下「**Download a CA certificate, certificate chain or CRL**」，然後選擇「**Base 64**」單選按鈕以指定編碼方法。按一下「**Download CA certificate**」。



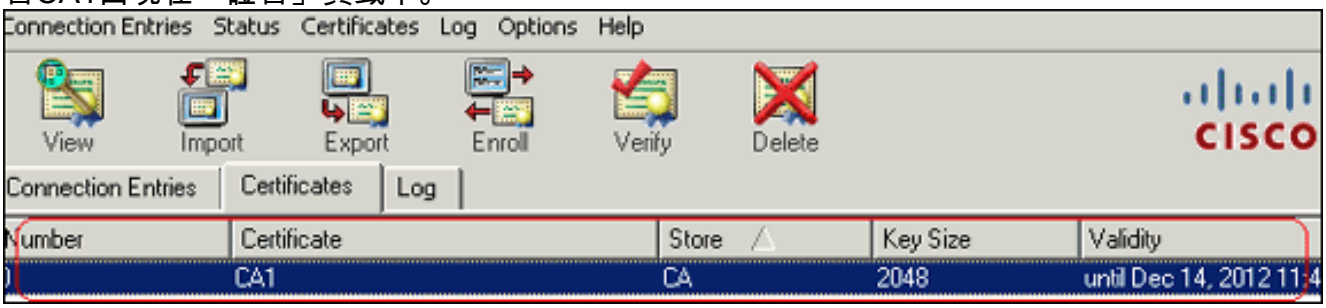
將名為**certnew.cer**的CA證書儲存到電腦。預設情況下，檔案儲存到`C:\Program Files\Cisco Systems\VPN Client`。



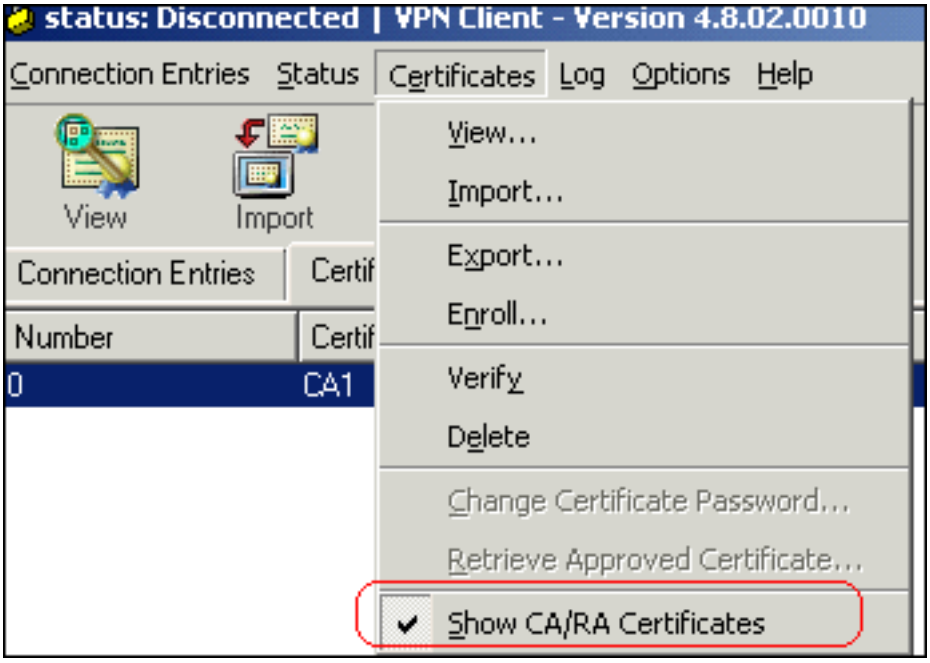
在VPN客戶端中，按一下**Certificates**頁籤，然後選擇**Import**。按一下**Import from File**單選按鈕，然後按一下**Browse**以從儲存位置`C:\Program Files\Cisco Systems\VPN Client`匯入CA證書。按一下「**Import**」（匯入）。系統將顯示一個對話方塊，說明已成功匯入證書。



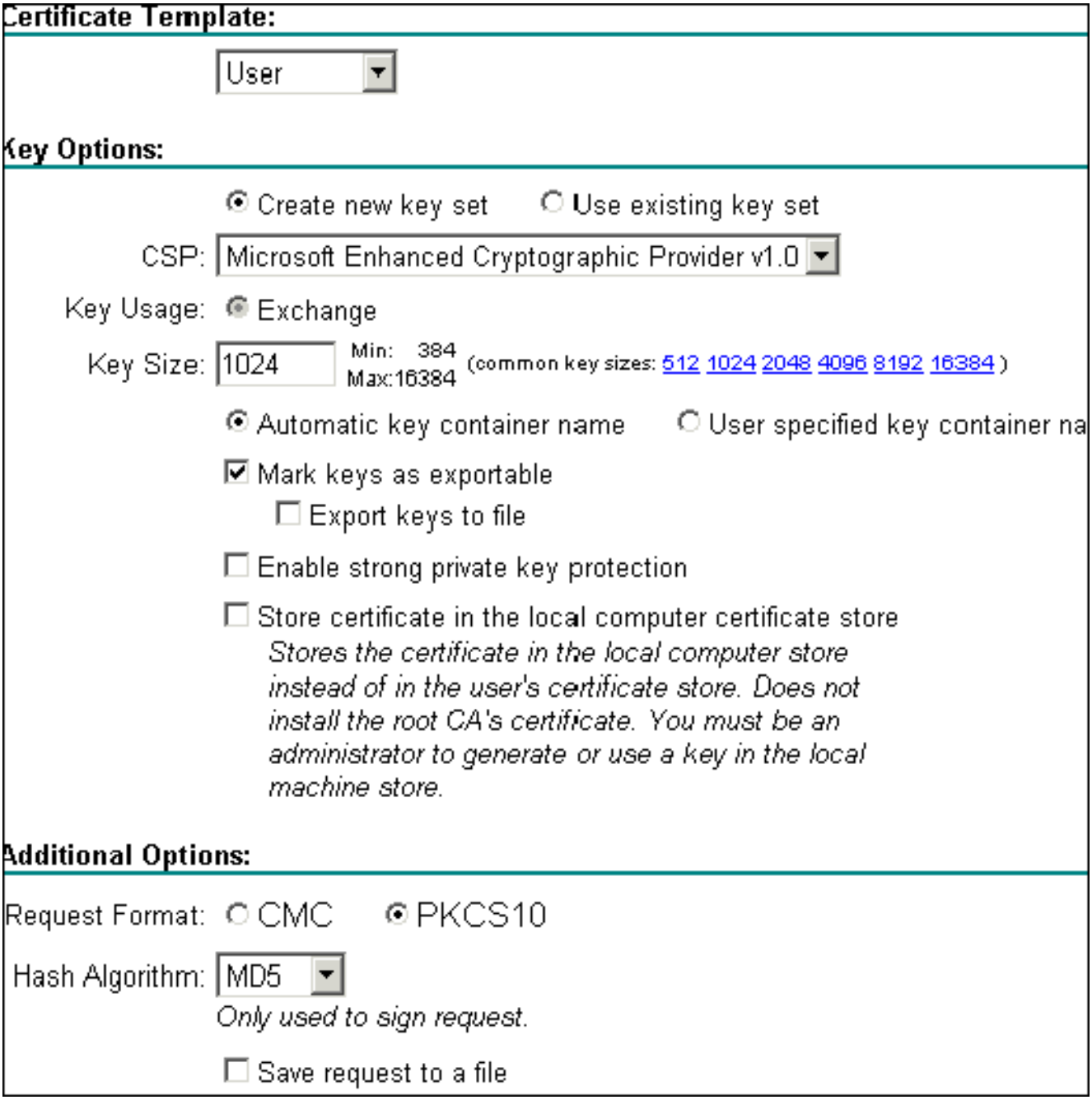
CA證書CA1出現在「證書」頁籤中。



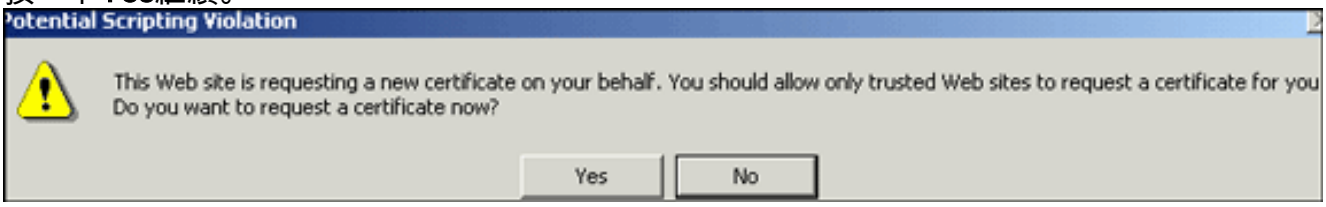
注意：確保選中**Show CA/RA Certificates**選項；否則，CA證書將不會出現在證書視窗中。



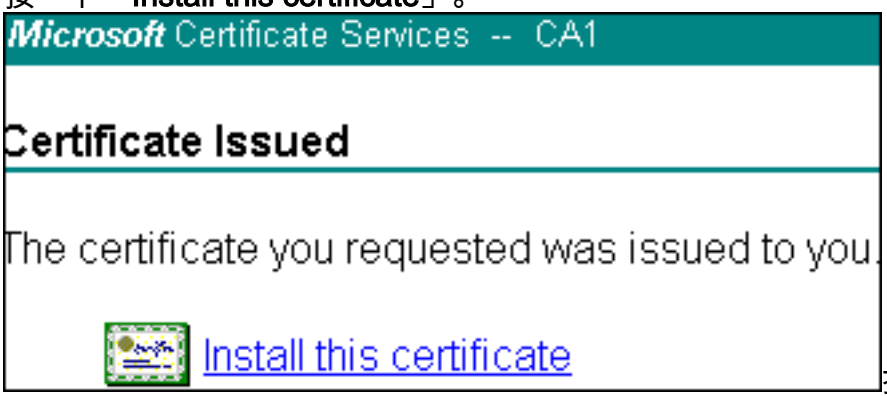
3. 完成以下步驟，即可下載身分憑證並將其安裝到VPN使用者端：在CA伺服器CA1中，選擇**Request a Certificate > advanced certificate request > Create並向此CA提交請求以註冊身份證書**。按一下「**Submit**」。



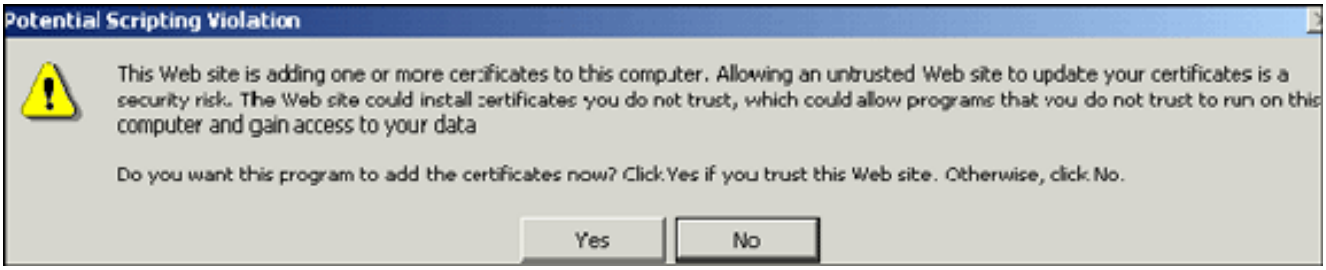
按一下**Yes**繼續。



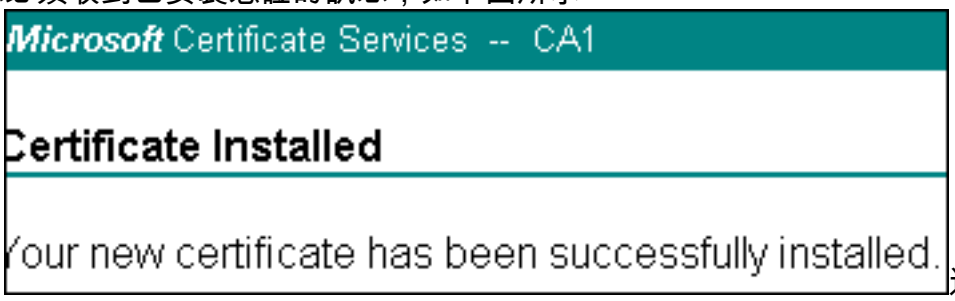
按一下「**Install this certificate**」。



按一下**Yes**繼續。

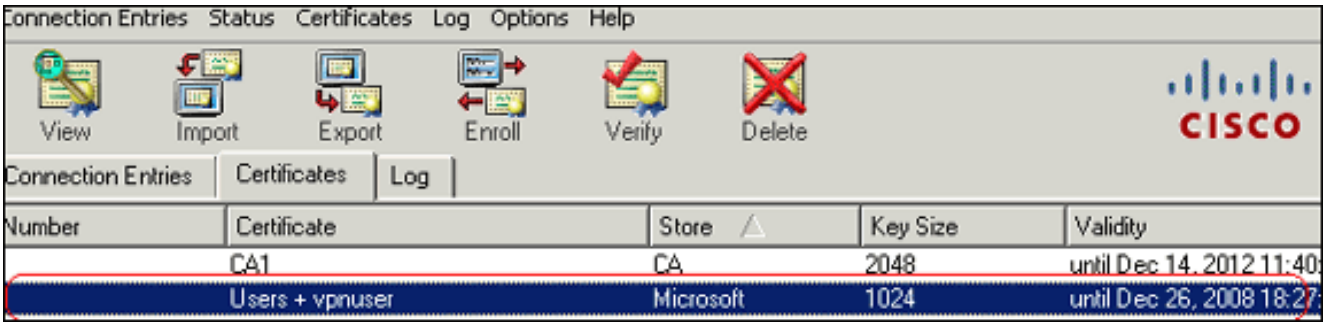


您必須收到已安裝憑證的訊息，如下圖所示

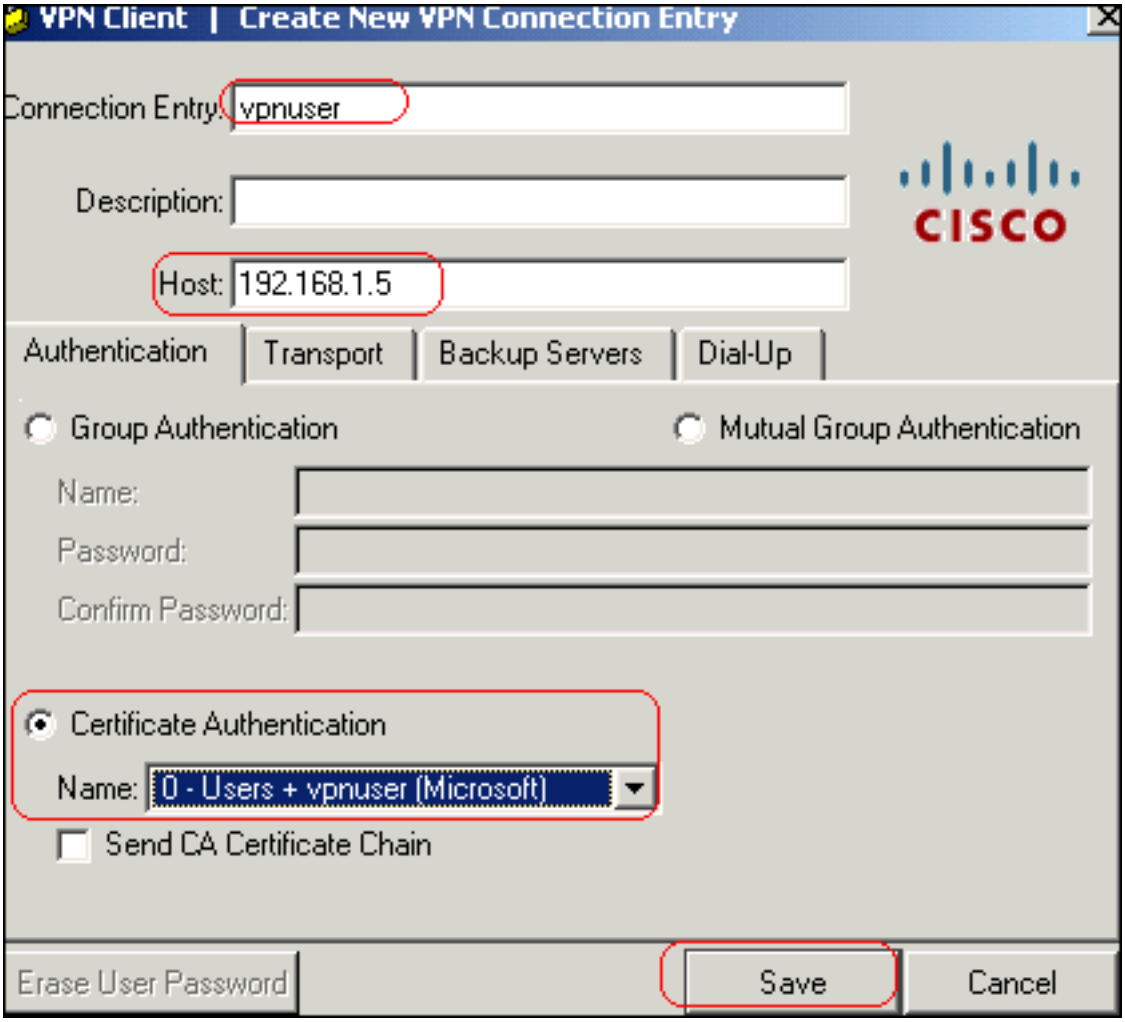
： 

退出VPN客戶端，然後重新啟動VPN客戶端，以允許已安裝的身份證書顯示在VPN客戶端的「證書」頁籤中，如下圖所示

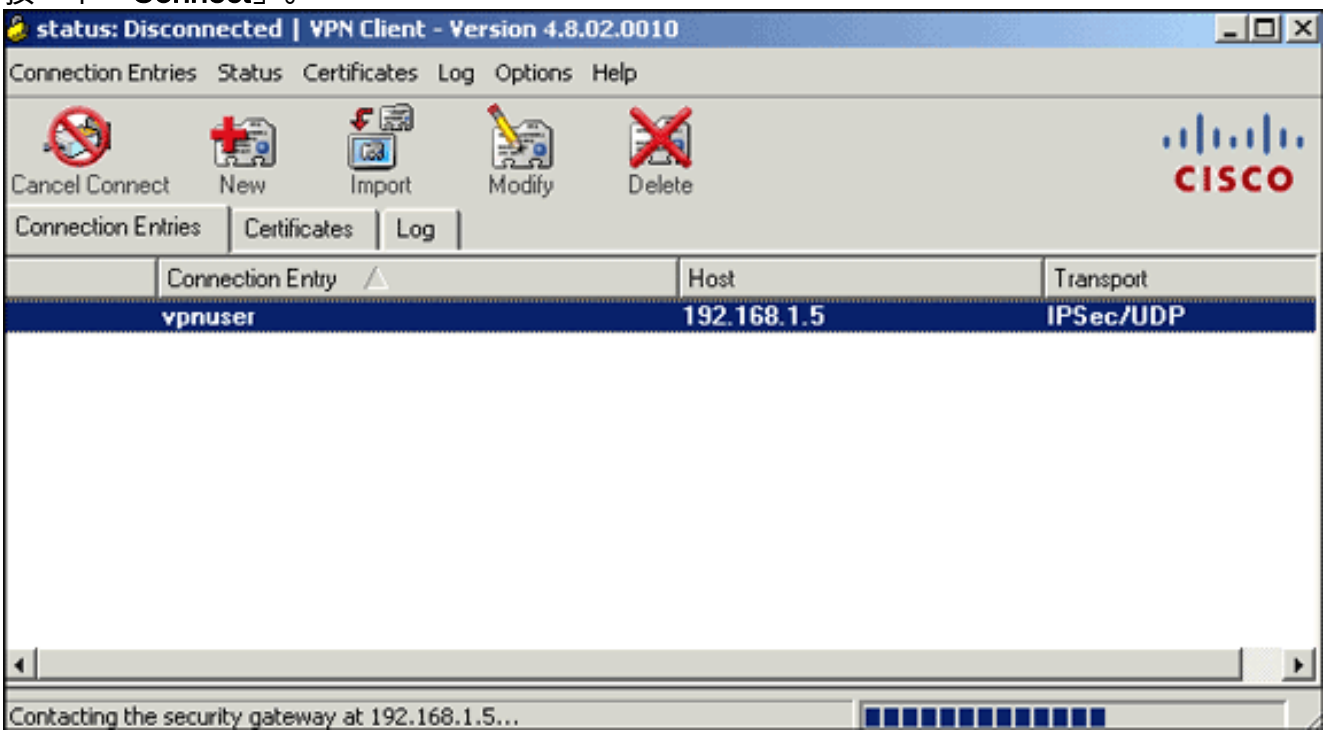
：



4. 完成以下步驟以建立連線條目(*vpnuser*):按一下Connection Entries頁籤，然後按一下**New**。在Host欄位中輸入遠端對等IP地址（可路由）。選擇**Certificate Authentication**單選按鈕，然後從下拉選單中選擇身份證書。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，如下圖所示：

驗證

在ASA上，您可以在命令列中使用多個show命令來驗證證書的狀態。

使用本節內容，確認您的組態是否正常運作。

- **show crypto ca trustpoint** — 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** — 顯示系統上安裝的所有證書。

```
CiscoASA#show crypto ca certificates
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=Configuratio
n,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: 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=Configuratio
n,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
```

- **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。

```
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** — 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** — 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命令輸出的分析。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

以下是您可能會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。使用**show crypto ca certificates trustpointname**命令以驗證您已將身份證書安裝到正確的信任點。查詢說明**Associated Trustpoints**的行。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**：如果在身份驗證期間證書出現問題，您可能會在VPN客戶端中收到此錯誤。要解決此問題，請在ASA/PIX配置中使用**crypto isakmp identity auto**命令。

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
- Cisco PIX 500系列安全裝置
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems