配置VPN客戶端3.x以獲取數位證書

目錄

簡介

本文檔演示如何配置Cisco VPN客戶端3.x以獲取數位證書。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據執行Cisco VPN Client 3.x的PC。

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。

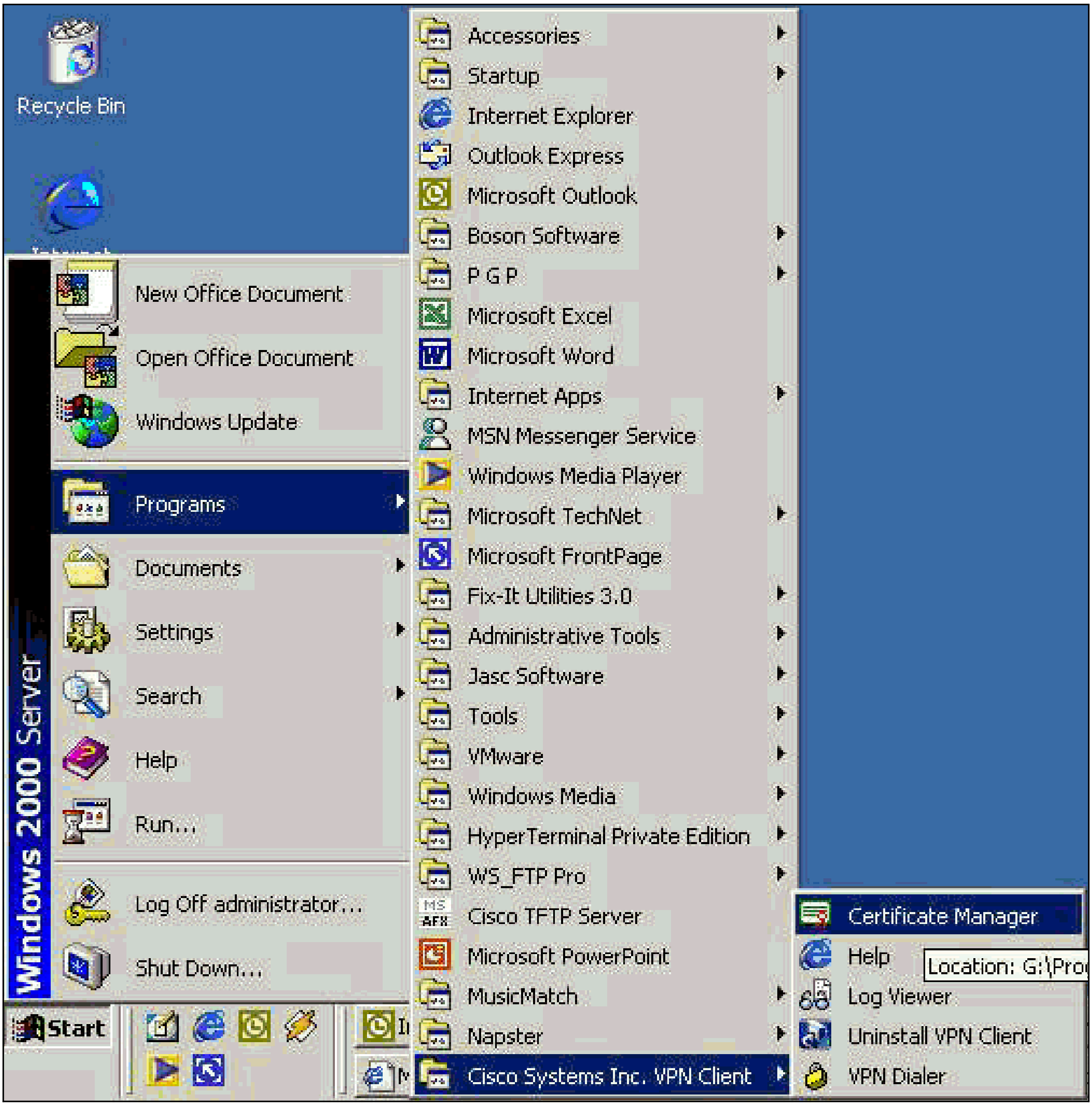
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

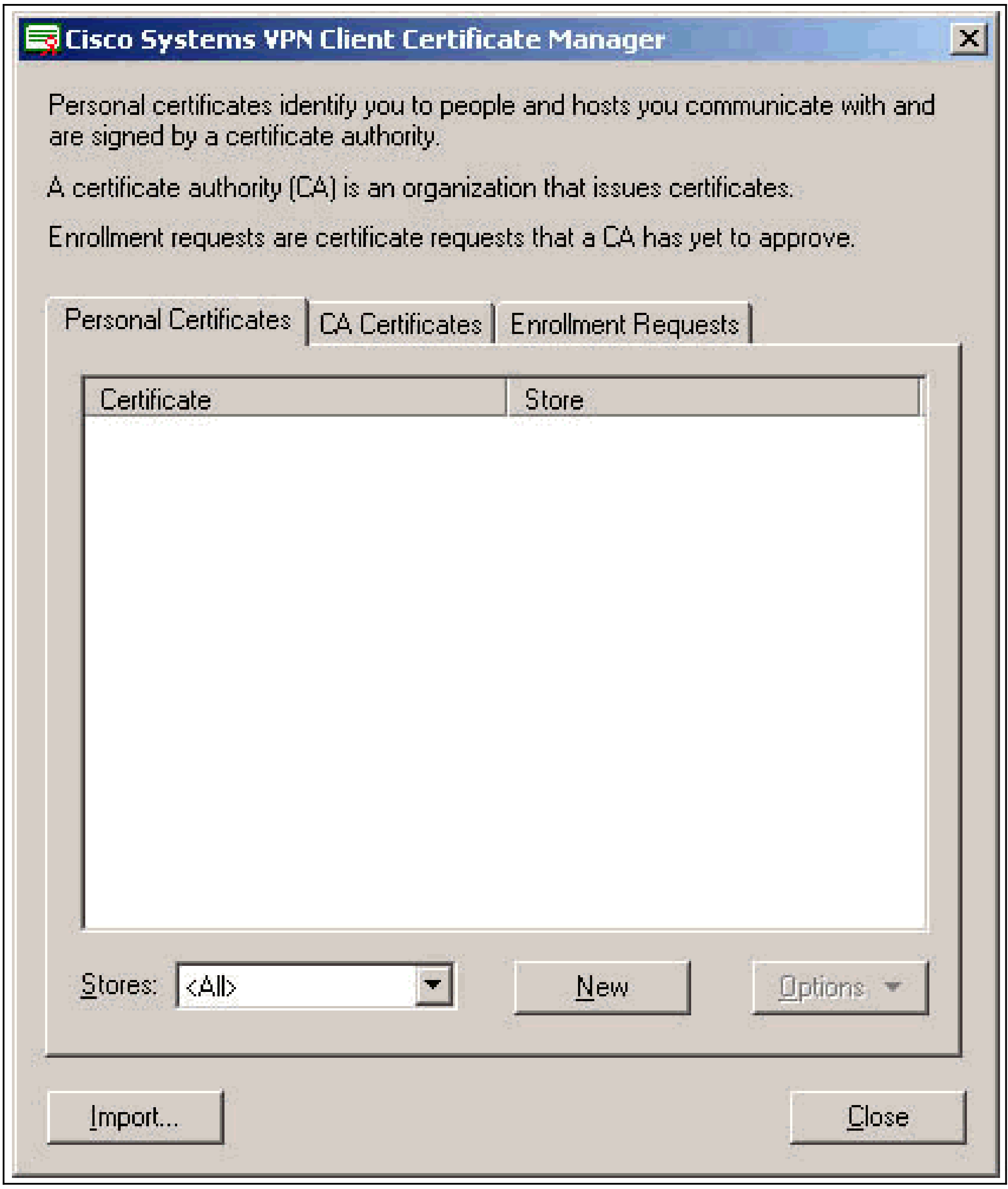
配置VPN客戶端

完成以下步驟以配置VPN客戶端。

1. 選擇**Start** > **Programs** > **Cisco Systems Inc. VPN client** > **Certificate Manager**以啟動VPN Client Certificate Manager。



2. 選擇個人證書頁籤，然後按一下**新建**。



Cisco Systems VPN Client Certificate Manager

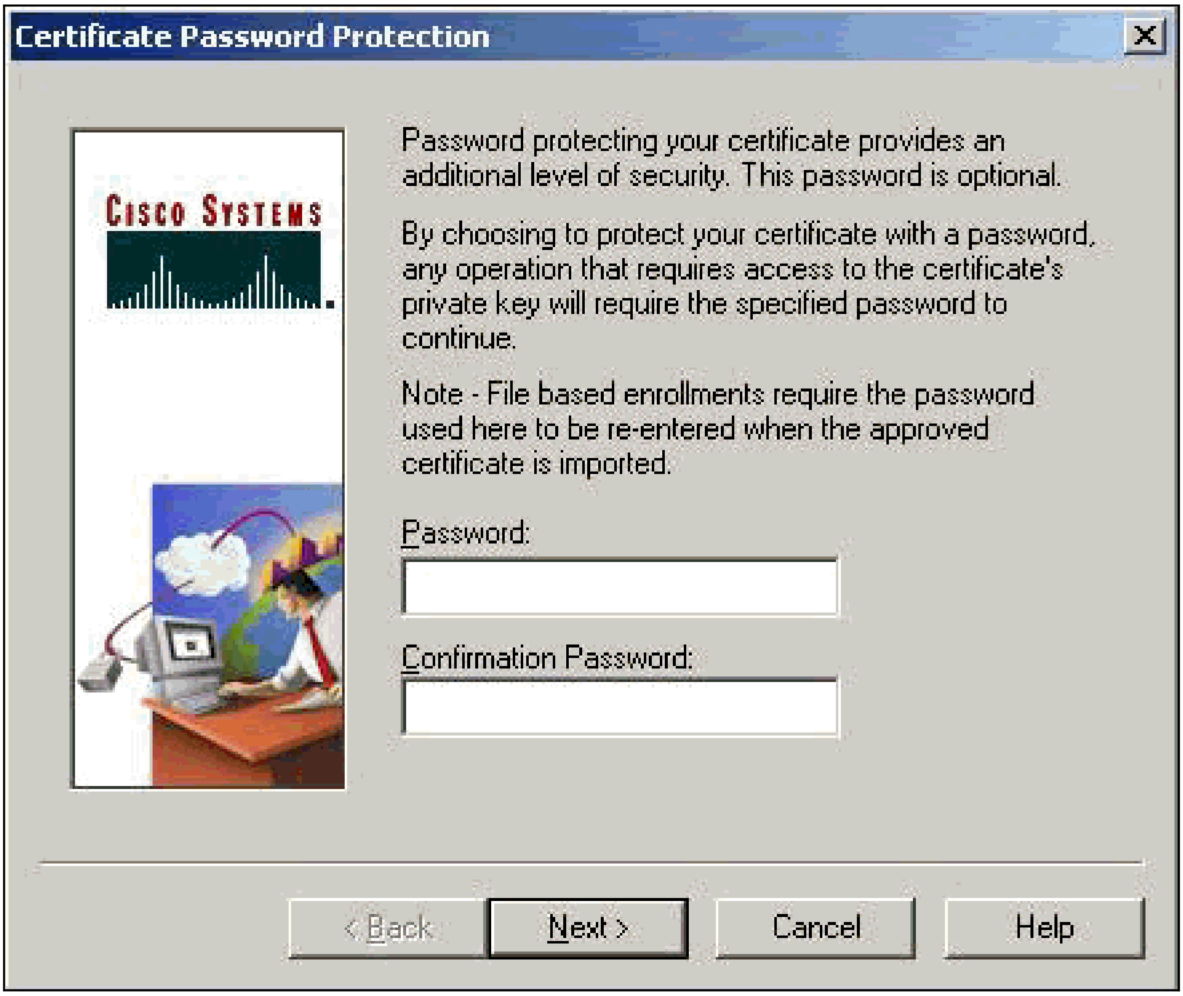
Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

A certificate authority (CA) is an organization that issues certificates.

Enrollment requests are certificate requests that a CA has yet to approve.

注意：無法使用IPsec完成對VPN連線的使用者進行身份驗證的電腦證書。

3. 當VPN客戶端提示您輸入密碼時，請指定密碼以保護證書。任何需要訪問證書私鑰的操作都需要指定的密碼才能繼續。



Certificate Password Protection

Password protecting your certificate provides an additional level of security. This password is optional.

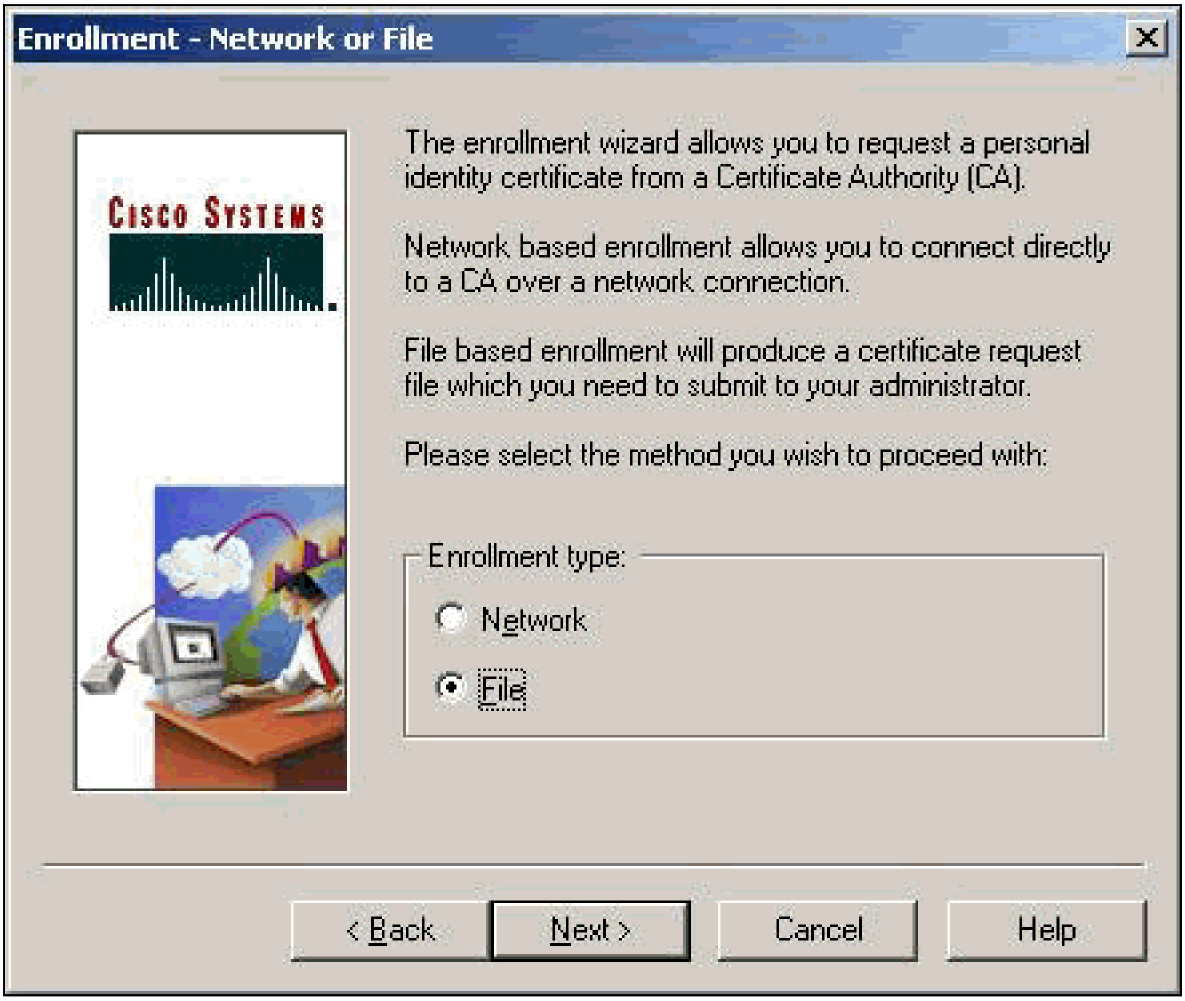
By choosing to protect your certificate with a password, any operation that requires access to the certificate's private key will require the specified password to continue.

Note - File based enrollments require the password used here to be re-entered when the approved certificate is imported.

Password:

Confirmation Password:

4. 在Enrollment頁面上選擇**File**以使用PKCS #10格式請求證書。然後按一下**Next**。



Enrollment - Network or File

The enrollment wizard allows you to request a personal identity certificate from a Certificate Authority (CA).

Network based enrollment allows you to connect directly to a CA over a network connection.

File based enrollment will produce a certificate request file which you need to submit to your administrator.

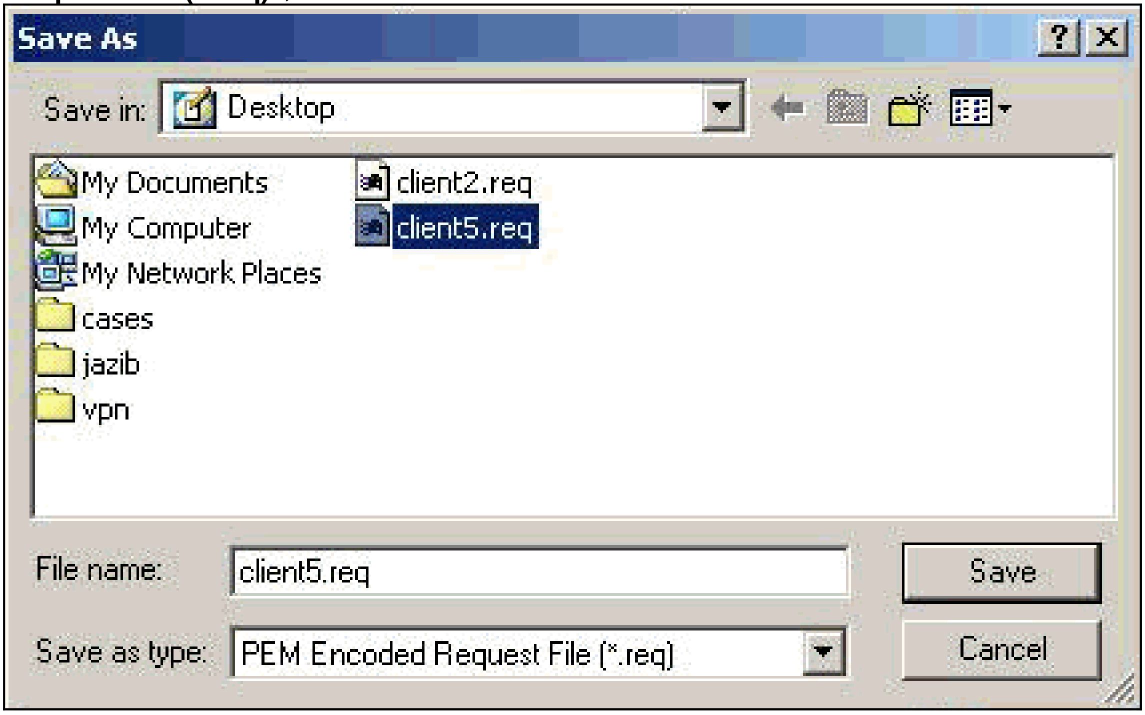
Please select the method you wish to proceed with:

Enrollment type:

○ Network

● File

5. 按一下「**Browse**」，並為憑證請求檔案指定檔案名稱。對於檔案型別，選擇**PEM Encoded Request File(*.req)**，然後按一下**Save**。



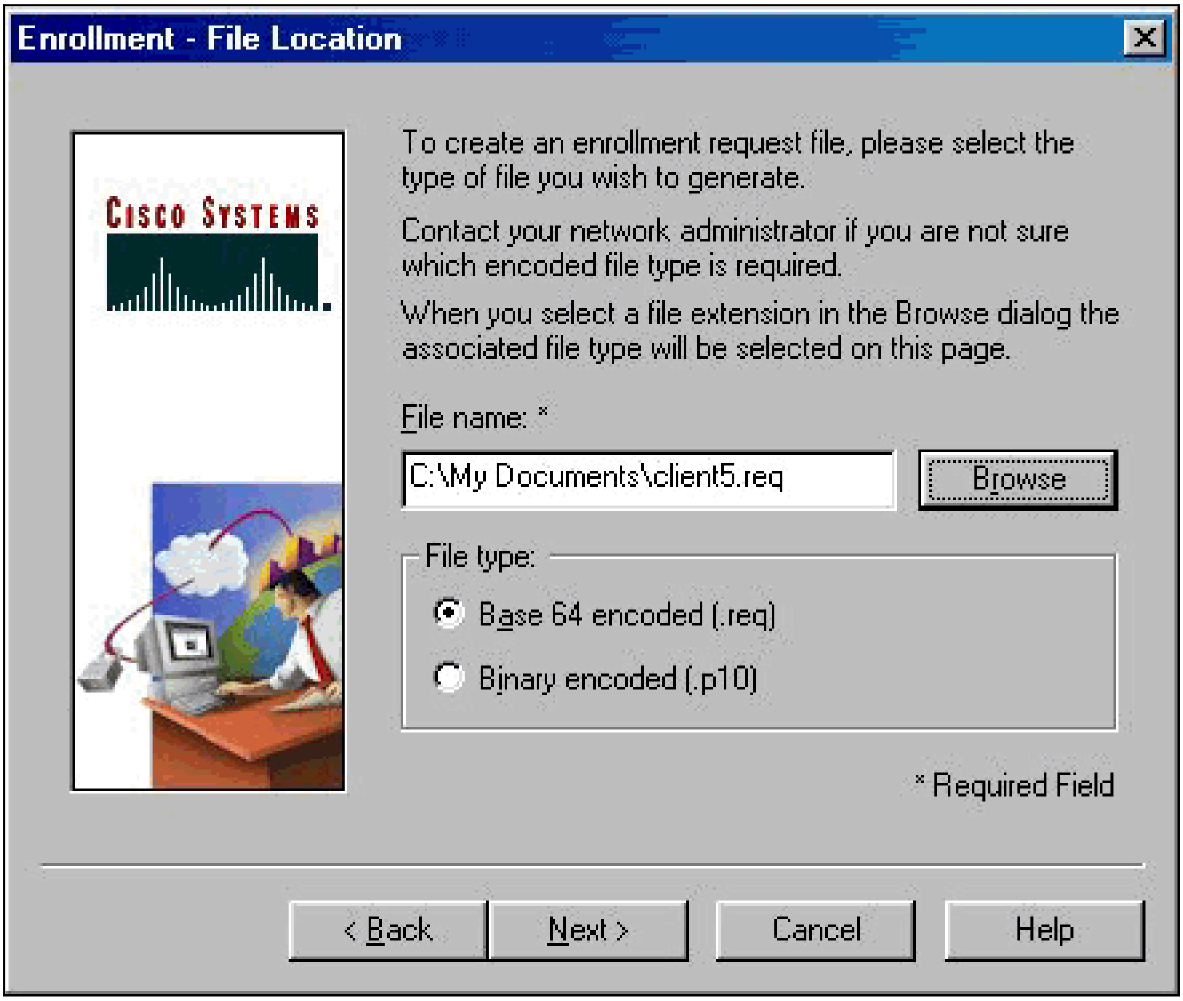
Save As

Save in: Desktop

File name: client5.req

Save as type: PEM Encoded Request File (*.req)

6. 在VPN Client Enrollment頁面上按一下**Next**。



Enrollment - File Location

To create an enrollment request file, please select the type of file you wish to generate.

Contact your network administrator if you are not sure which encoded file type is required.

When you select a file extension in the Browse dialog the associated file type will be selected on this page.

File name: * C:\My Documents\client5.req

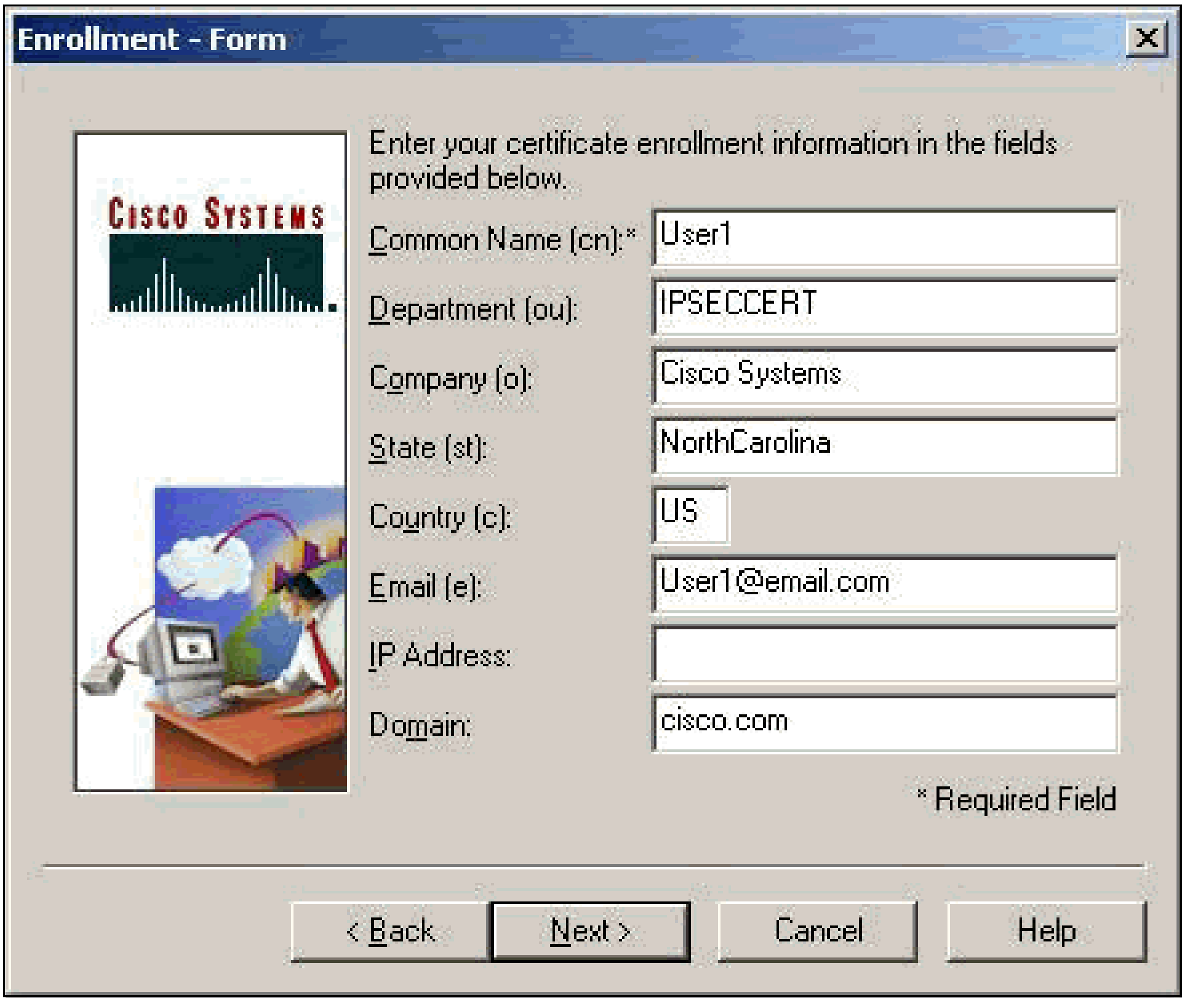
File type:

● Base 64 encoded (.req)

○ Binary encoded (.p10)

* Required Field

7. 填寫登記表上的欄位。此範例顯示欄位：公用名=使用者1Department = IPSECCERT(這應與VPN 3000 Concentrator上的組織單位(OU)和組名稱匹配。)公司=思科系統公司州=北卡羅萊納州國家/地區=美國電子郵件= User1@email.comIP地址=(可選；用於指定證書請求上的IP地址)域= cisco.com完成後按一下**Next**。



Enter your certificate enrollment information in the fields provided below.

Common Name (cn):* User1

Department (ou): IPSECCERT

Company (o): Cisco Systems

State (st): NorthCarolina

Country (c): US

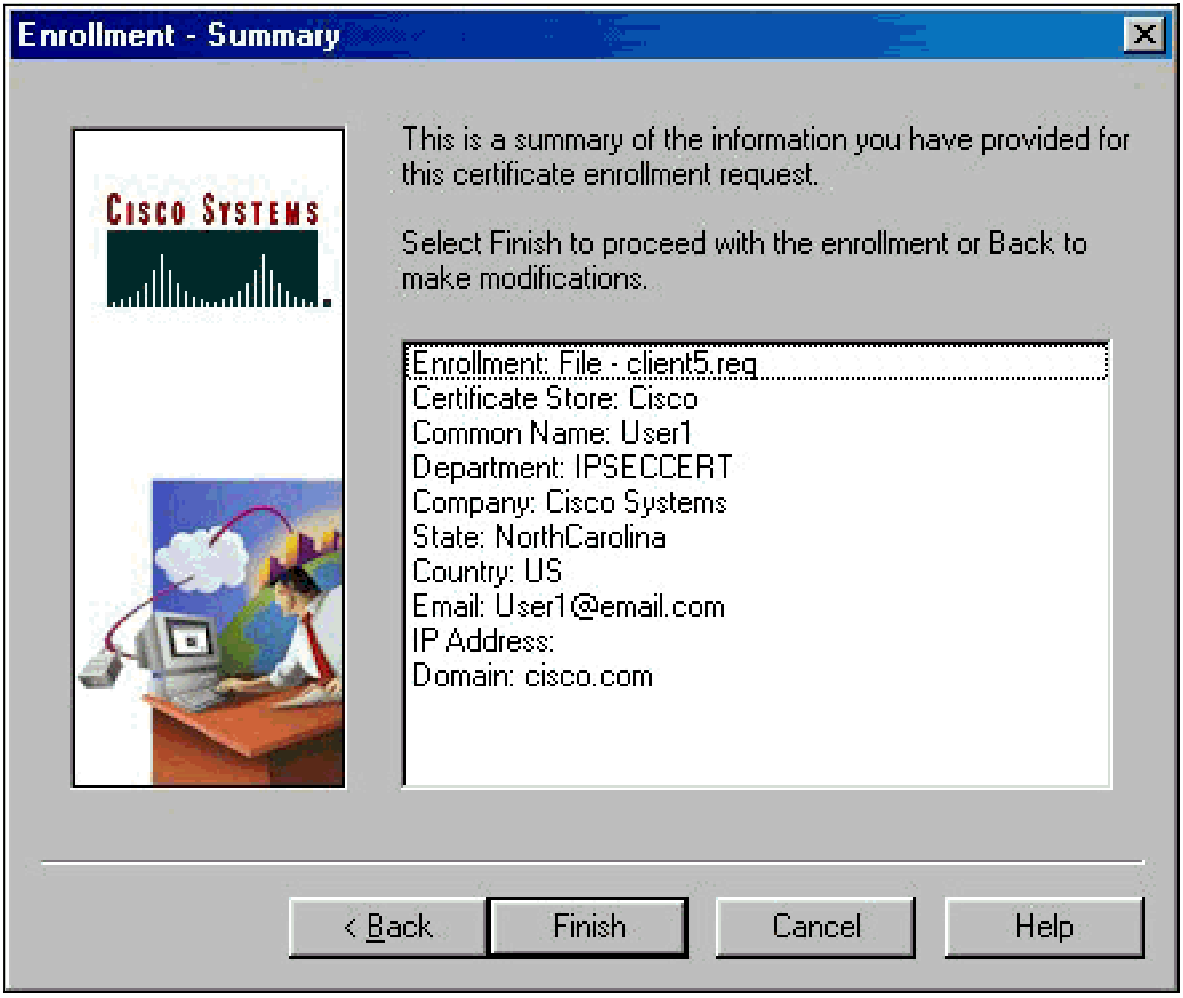
Email (e): User1@email.com

IP Address:

Domain: cisco.com

* Required Field

8. 按一下**完成**繼續註冊。

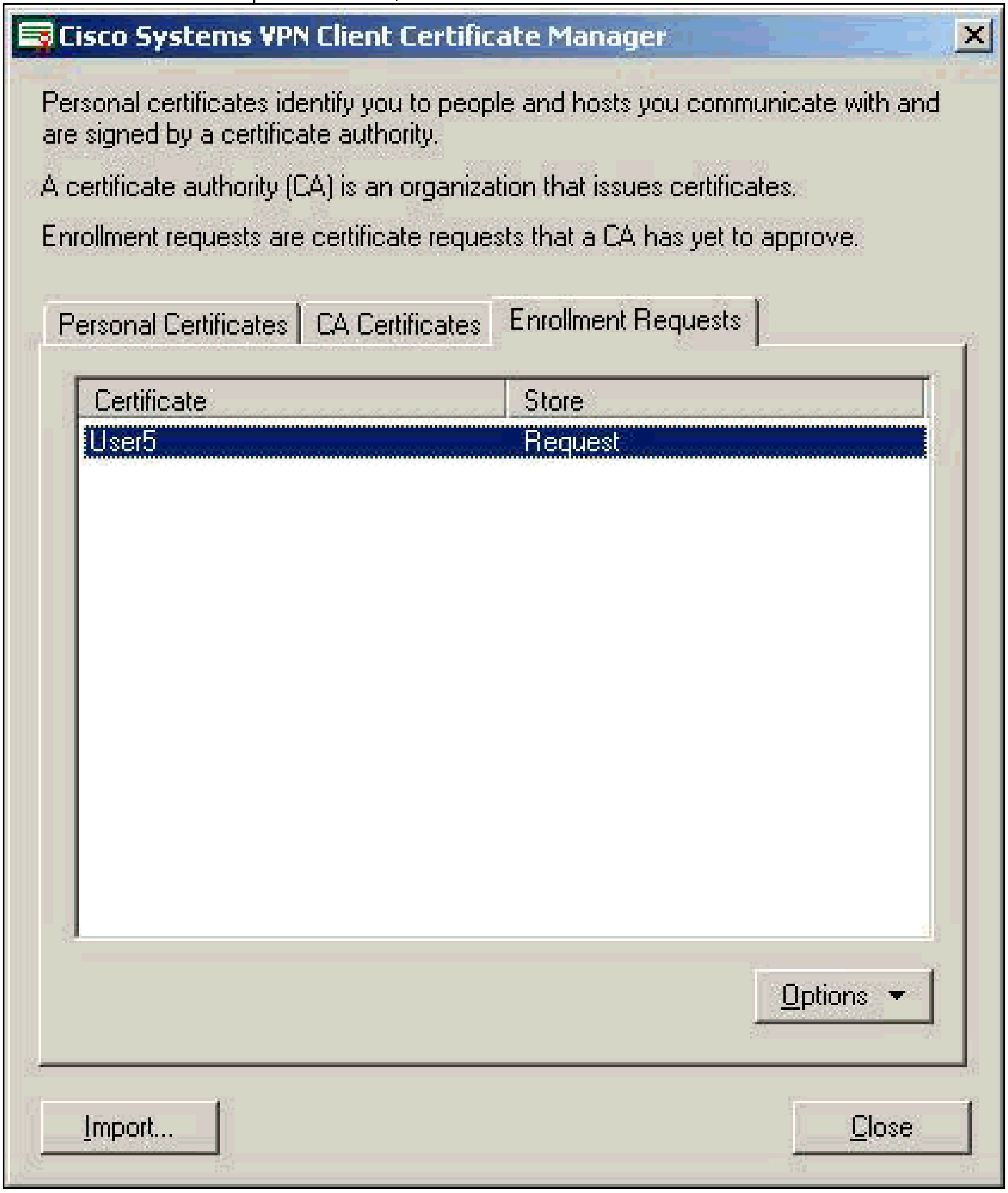


This is a summary of the information you have provided for this certificate enrollment request.

Select Finish to proceed with the enrollment or Back to make modifications.

Enrollment: File - client5.req
Certificate Store: Cisco
Common Name: User1
Department: IPSECCERT
Company: Cisco Systems
State: NorthCarolina
Country: US
Email: User1@email.com
IP Address:
Domain: cisco.com

9. 選擇Enrollment Requests頁籤，在VPN客戶端證書管理器上檢查請求。



Cisco Systems VPN Client Certificate Manager

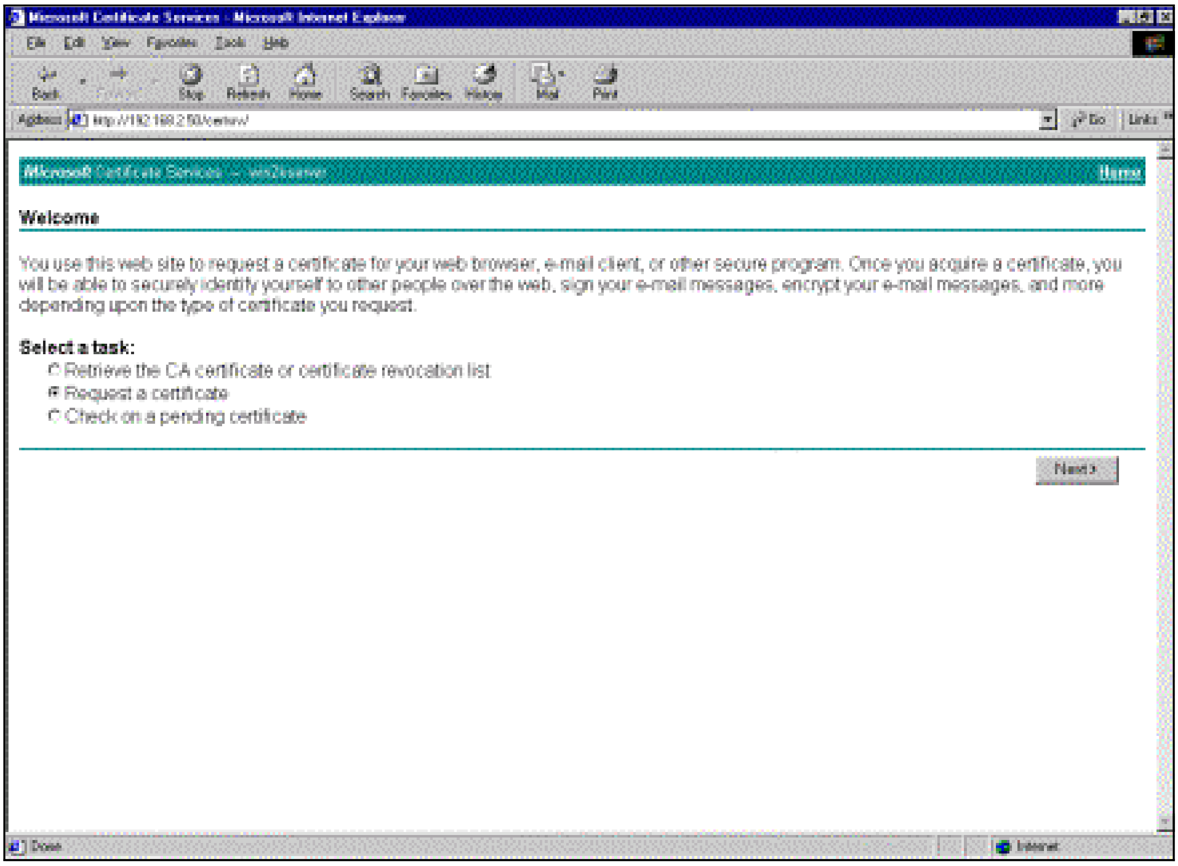
Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

A certificate authority (CA) is an organization that issues certificates.

Enrollment requests are certificate requests that a CA has yet to approve.

Certificate	Store
User5	Request

10. 同時開啟證書頒發機構(CA)伺服器和VPN客戶端介面以提交請求。
11. 選擇**Request a certificate**，然後在CA伺服器上按一下**Next**。


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.2.50/certsrv/
Go Links
Done
Internet

Microsoft Certificate Services -- win2kserver **Home**

Welcome

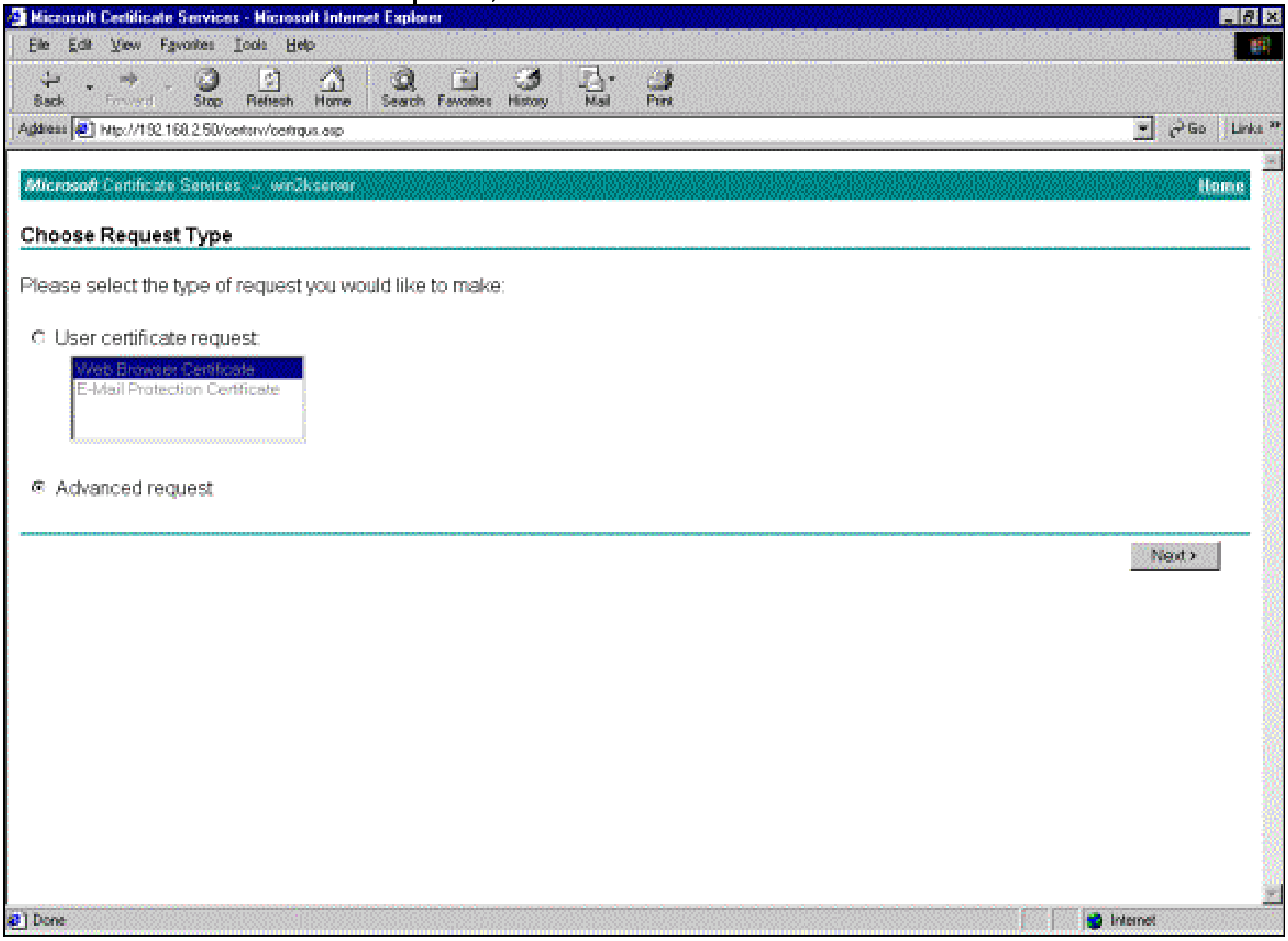
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Next >

12. 為請求型別選擇**Advanced request**，然後按一下**Next**。


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.2.50/certsrv/certrqus.asp
Go Links
Done
Internet

Microsoft Certificate Services -- win2kserver **Home**

Choose Request Type

Please select the type of request you would like to make:

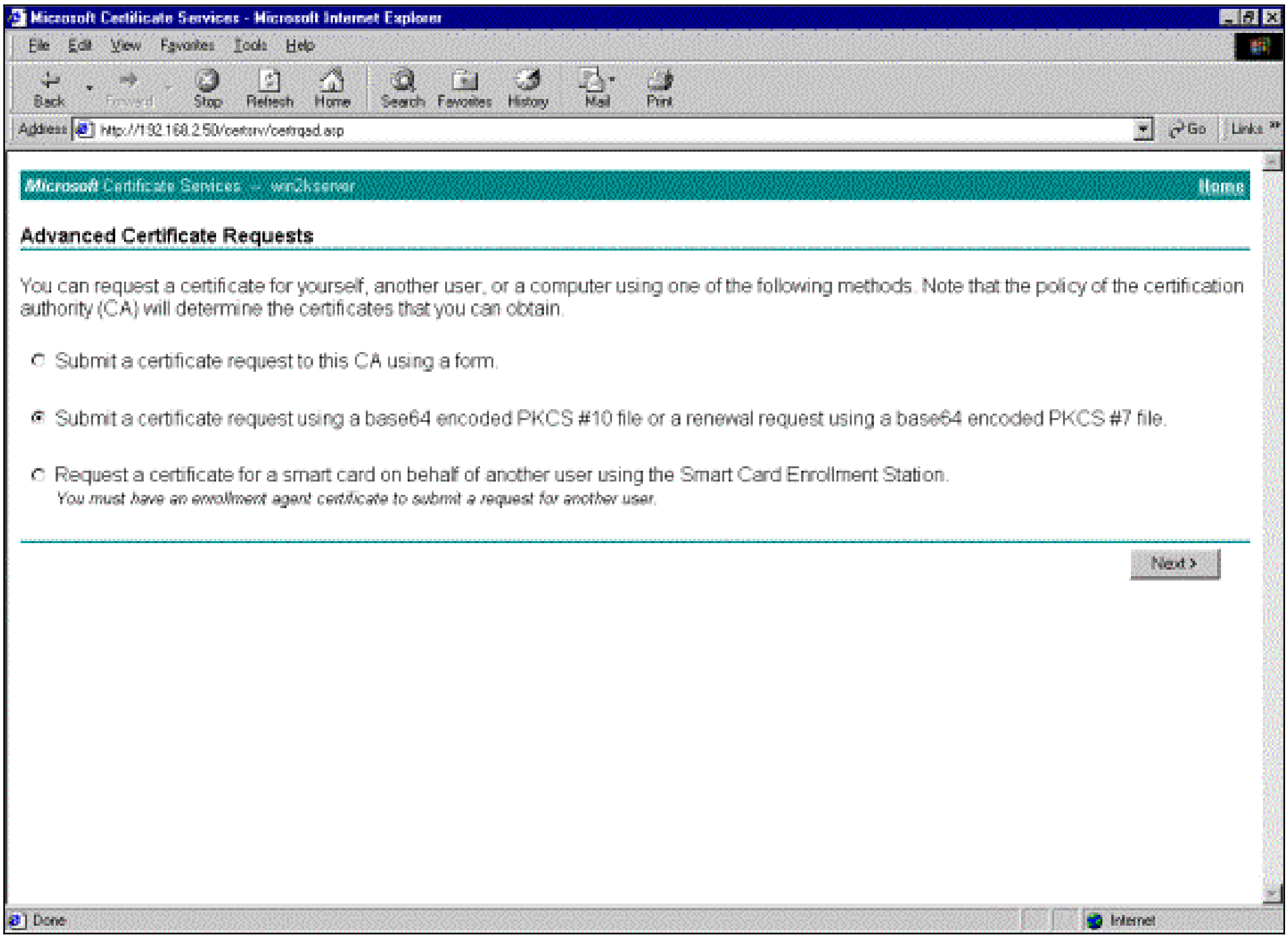
○ User certificate request:

Web Browser Certificate
E-Mail Protection Certificate

● Advanced request

Next >

13. 在Advanced Certificate Requests下，選擇**Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**，然後按一下**Next**。


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.2.50/certsrv/certrqad.asp
Go Links
Microsoft Certificate Services -- win2kserver
Home

Advanced Certificate Requests

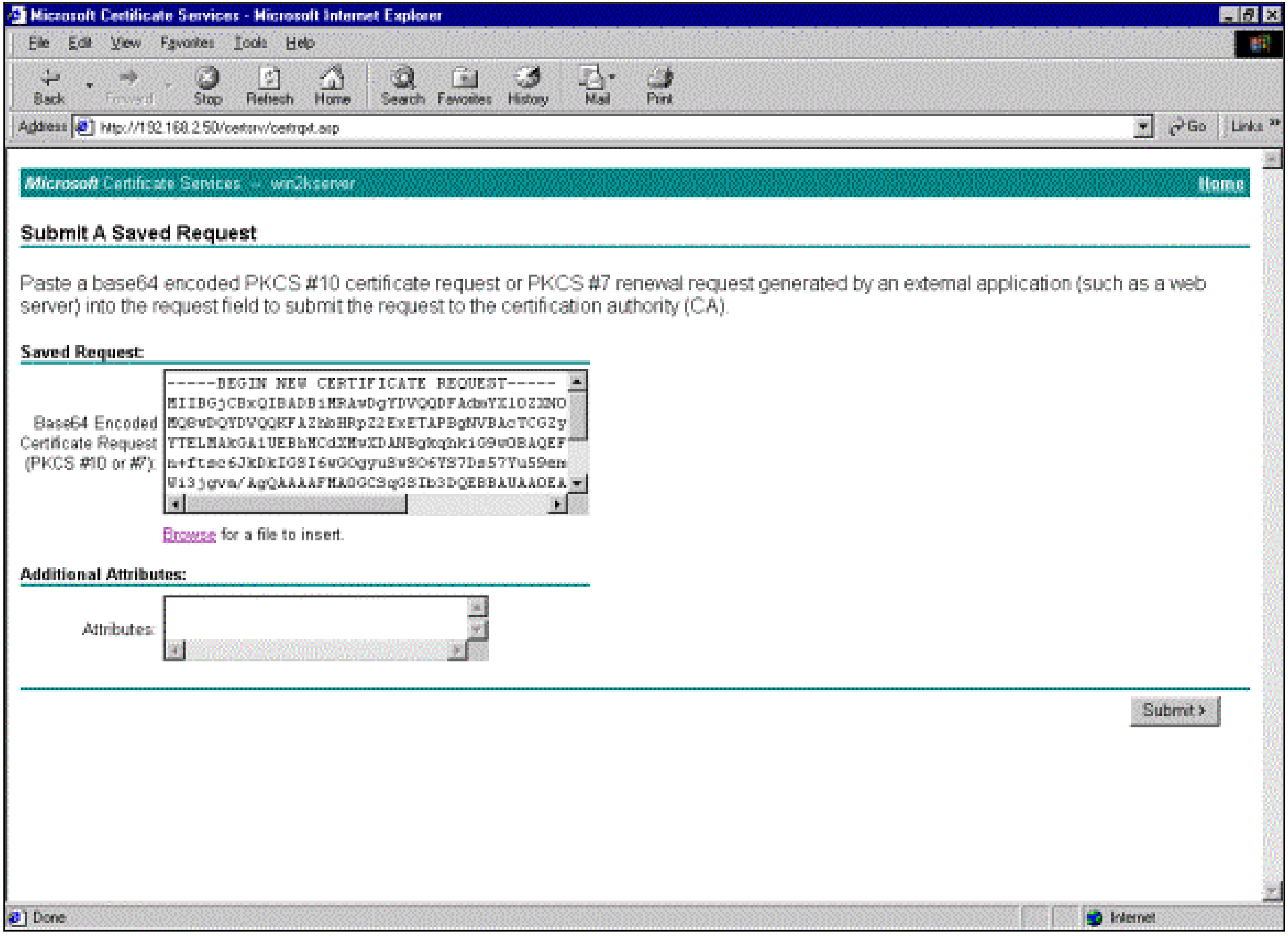
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

14. 突出顯示VPN客戶端請求檔案，並將其貼上到CA伺服器儲存的請求下。然後按一下**Submit**。


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.2.50/certsrv/certrqxt.asp
Go Links
Microsoft Certificate Services -- win2kserver
Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

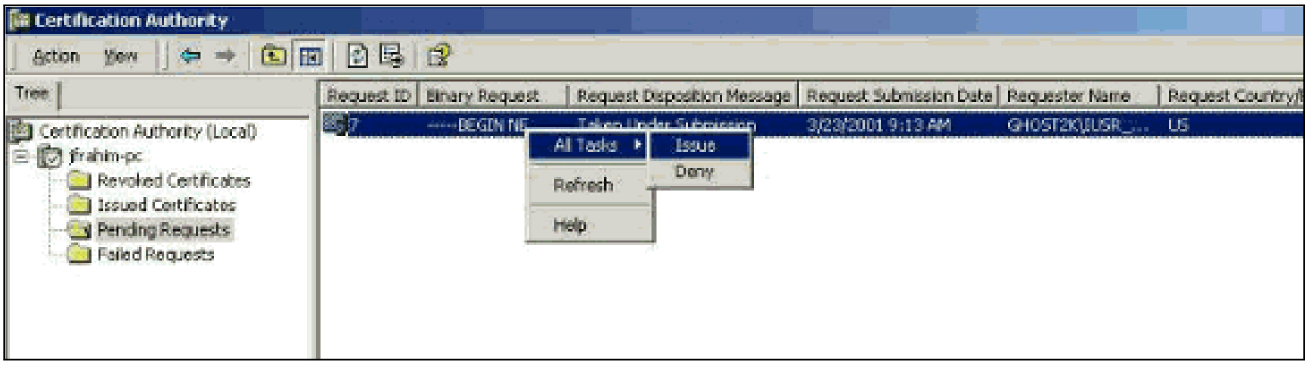
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBGjCBxQIBADB1MRAwDgYDVQQDFAdmYXl0ZXN0
MQ8wDQYDVQQKFAZmbHRpZ2ExETAPBgNVBAcTCGZy
YTELMAkGA1UEBhMCdXMwXDANBgkqhkiG9w0BAQEF
n+ftmc6JkDkIG8I6wGOgyu8w8O6Y87Ds57Yu59em
W13jgva/AgQAAAAFMA0GCSqGSIb3DQEBBAUAA0EA
```

Browse for a file to insert.

Additional Attributes:

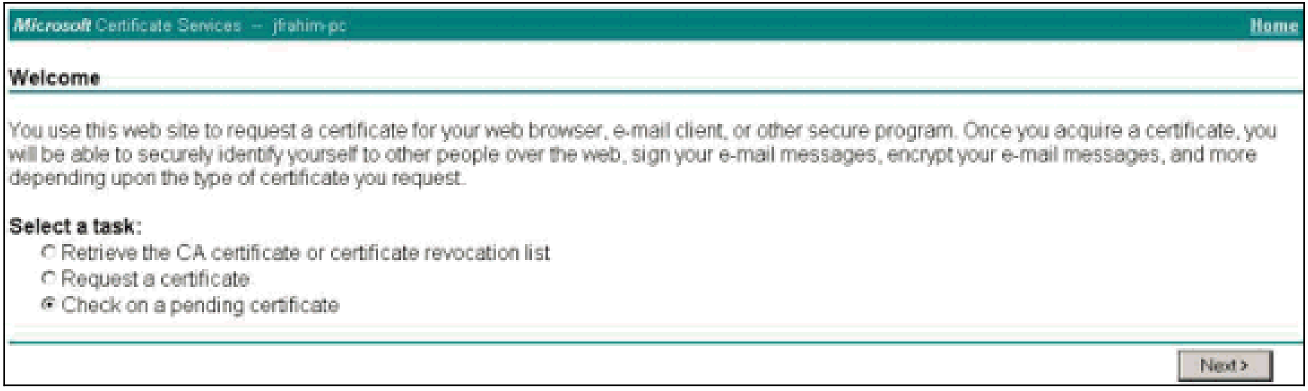
Attributes:

15. 在CA伺服器上，為VPN客戶端請求頒發身份證書。



Request ID	Binary Request	Request Disposition Message	Request Submission Date	Requester Name	Request Country/I
7	-----BEGIN NE	Taken Under Submission	3/23/2001 9:13 AM	GHOST2K\IUSR_...	US

16. 將根證書和身份證書下載到VPN客戶端。在CA伺服器上，選擇**Check on a pending certificate**，然後按一下**Next**。

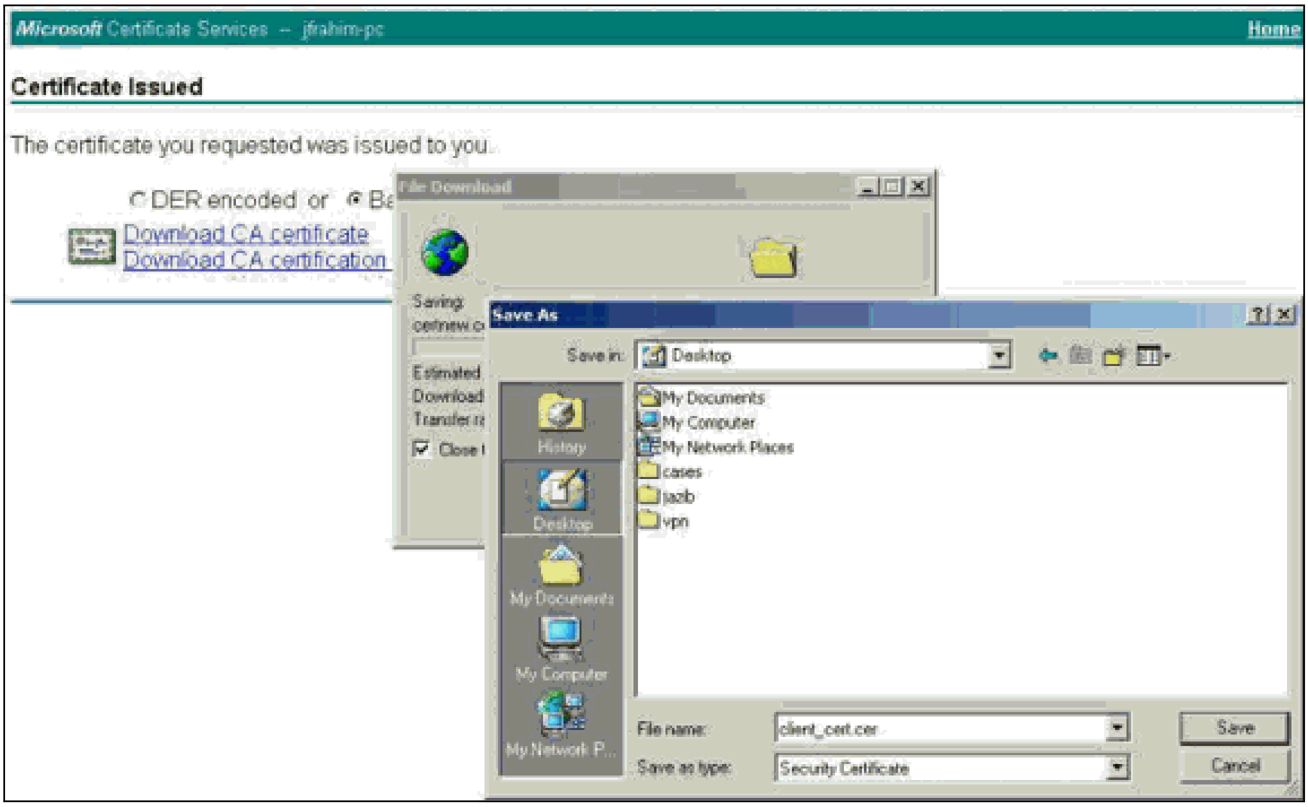


Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:
○ Retrieve the CA certificate or certificate revocation list
○ Request a certificate
● Check on a pending certificate

17. 選擇**Base 64 encoded**。然後按一下CA伺服器上的**Download CA certificate**。



Certificate Issued

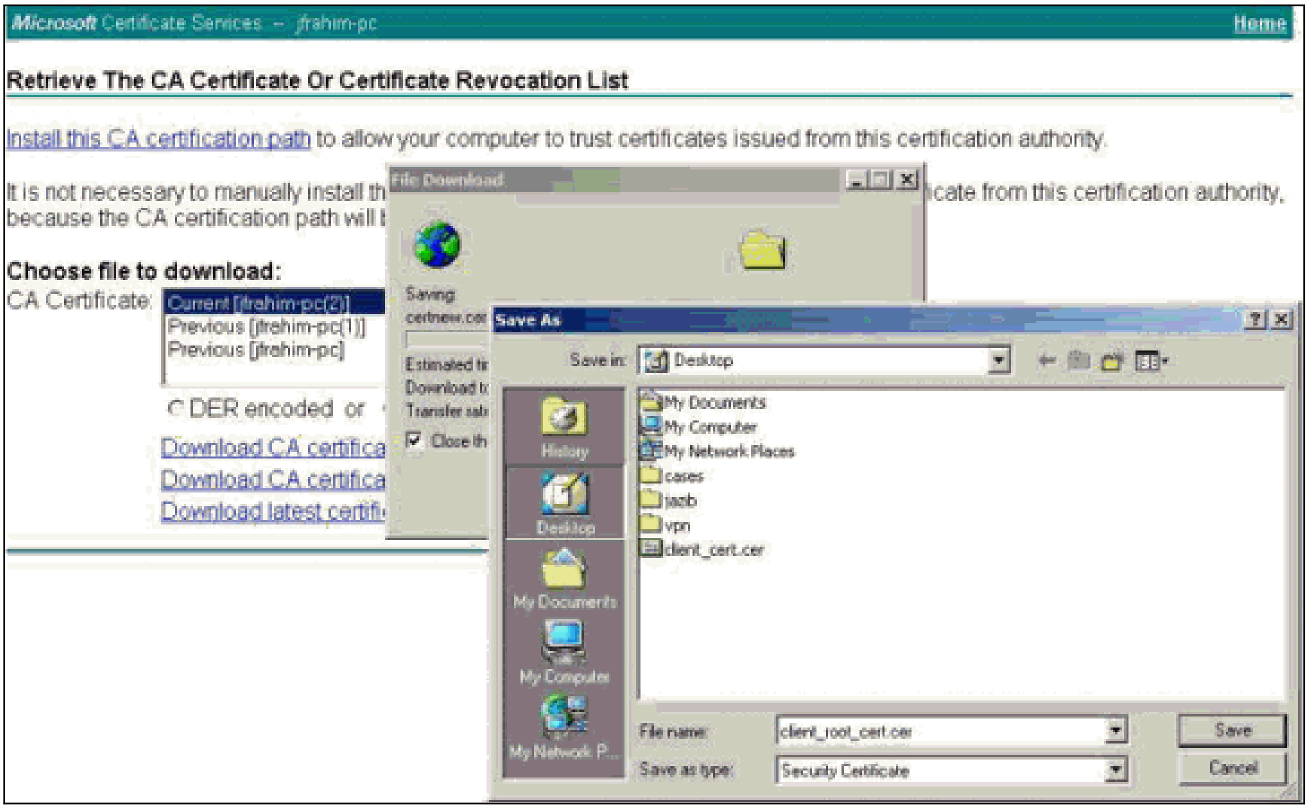
The certificate you requested was issued to you.

○ DER encoded or ● Ba

Download CA certificate
Download CA certification

File name: client_cert.cer
Save as type: Security Certificate

18. 從Retrieve the CA Certificate or Certificate Revocation List頁選擇要下載的檔案，以獲取CA伺服器上的根證書。然後按一下**Next**。



Microsoft Certificate Services -- jfrahim-pc

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install th… cate from this certification authority, because the CA certification path will b…

Choose file to download:

CA Certificate: Current [jfrahim-pc(2)] Previous [jfrahim-pc(1)] Previous [jfrahim-pc]

○ DER encoded or

Download CA certifica…
Download CA certifica…
Download latest certifi…

File Download

Saving: certnew.cer

☑ Close th…

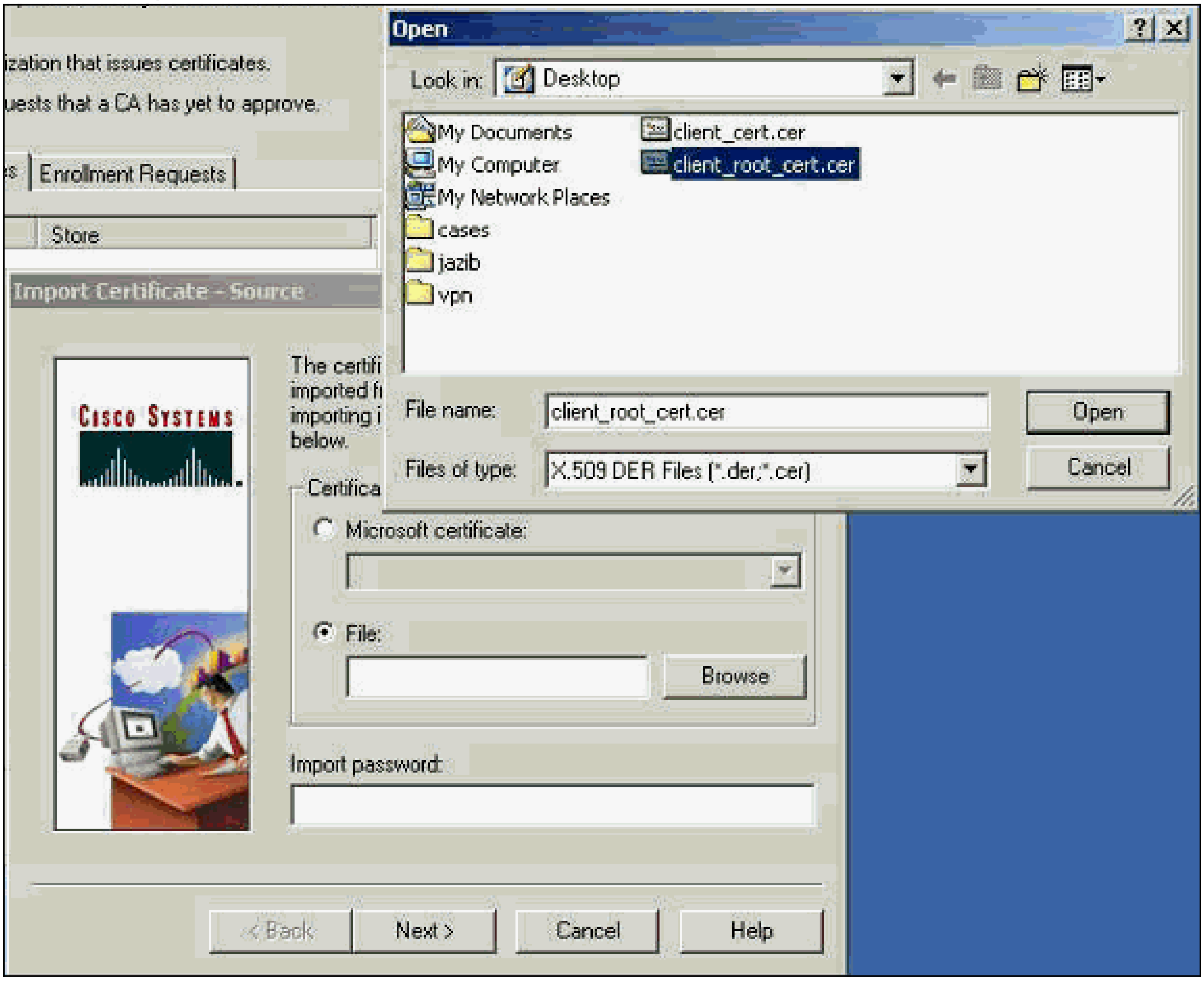
Save As

Save in: Desktop

File name: client_root_cert.cer

Save as type: Security Certificate

19. 選擇**Certificate Manager** > **CA Certificate** > **Import on the VPN Client**，然後選擇根CA檔案以安裝根和身份證書。



…ization that issues certificates.
…uests that a CA has yet to approve.

Import Certificate - Source

The certifi… imported fr… importing i… below.

Certifica…

○ Microsoft certificate:

● File:

Import password:

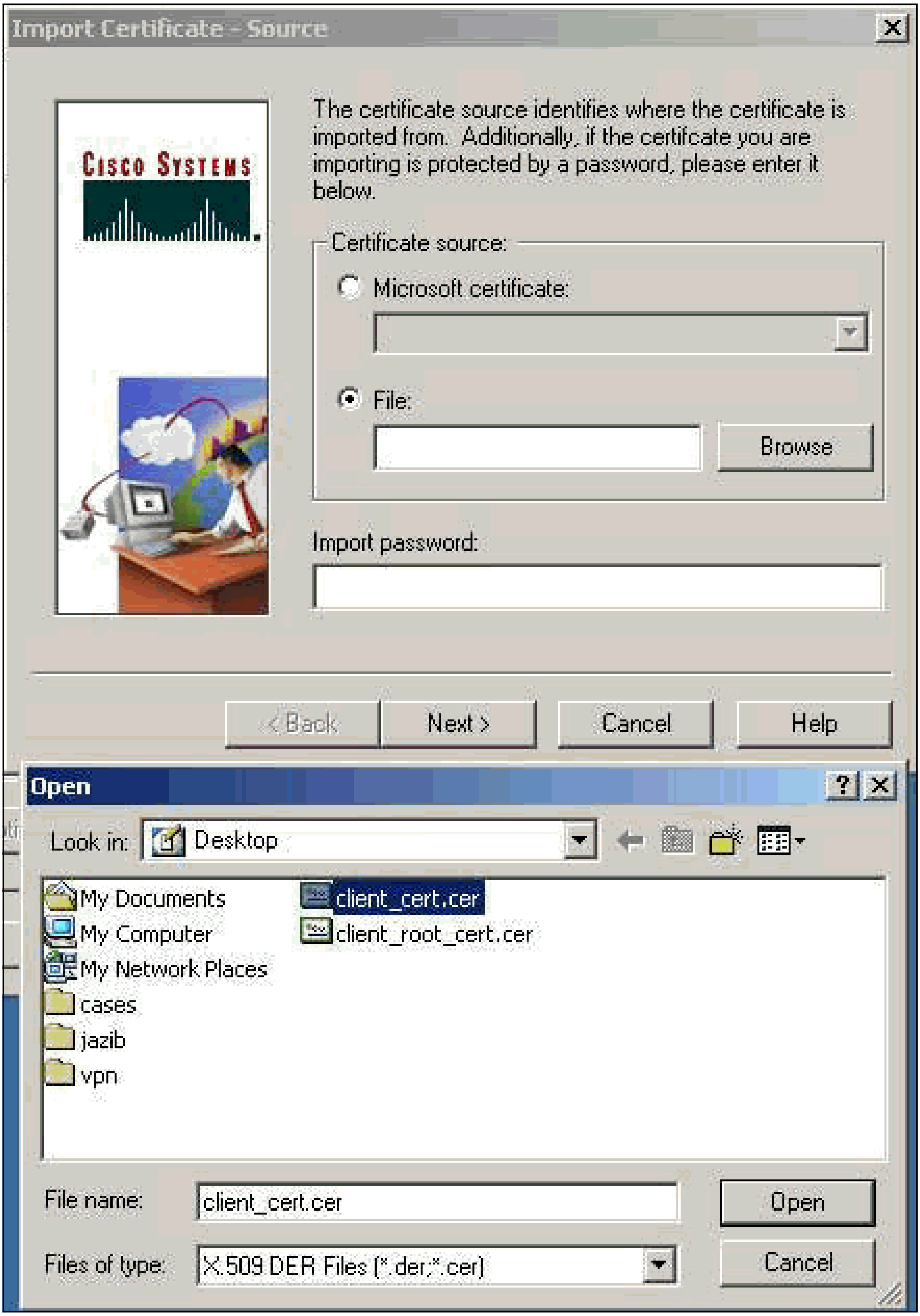
Open

Look in: Desktop

File name: client_root_cert.cer

Files of type: X.509 DER Files (*.der;*.cer)

20. 選擇**Certificate Manager** > **Personal Certificates** > **Import**，然後選擇身份證書檔案。



Import Certificate - Source

The certificate source identifies where the certificate is imported from. Additionally, if the certifcate you are importing is protected by a password, please enter it below.

Certificate source:

○ Microsoft certificate:

● File:

Import password:

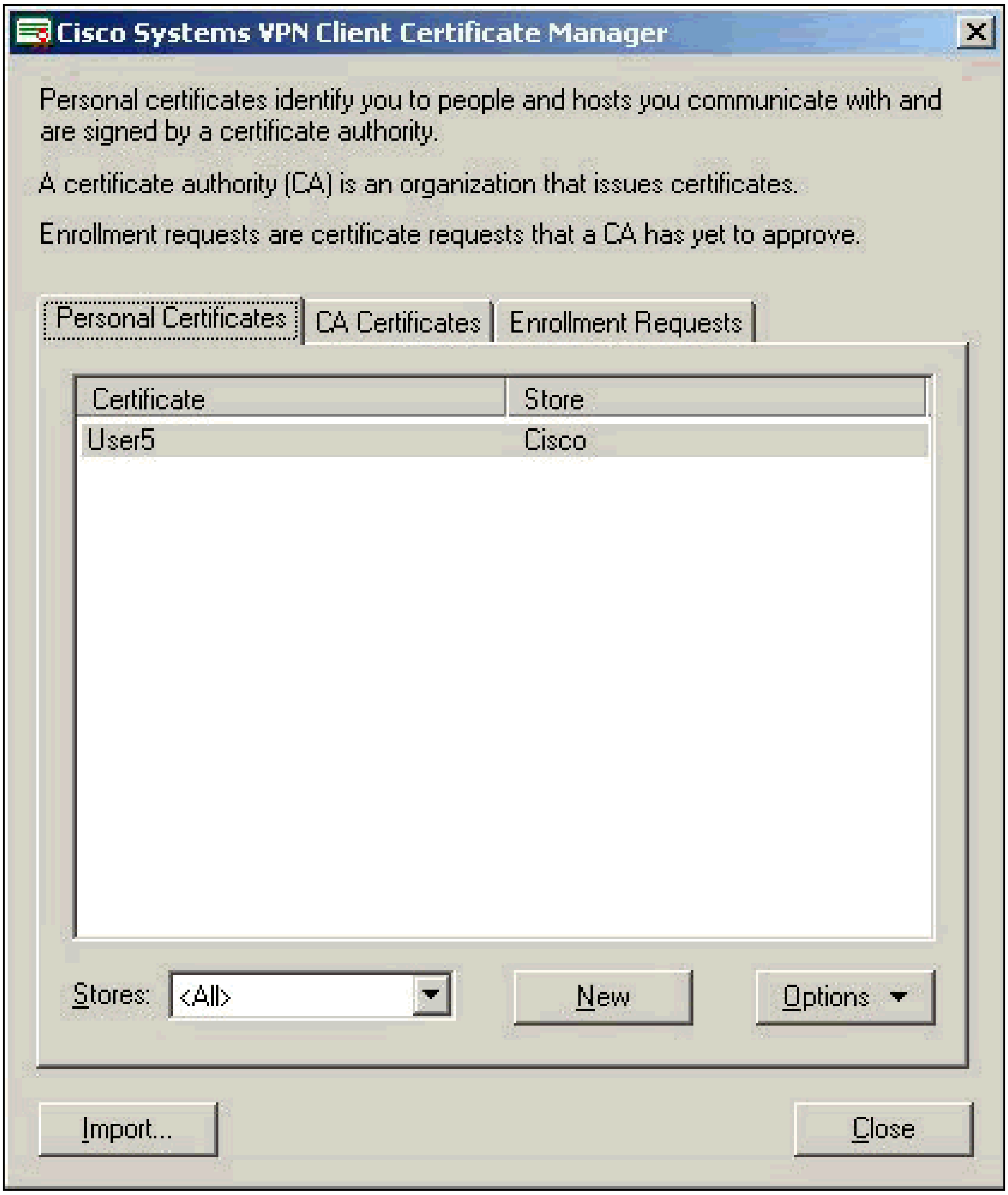
Open

Look in: Desktop

File name: client_cert.cer

Files of type: X.509 DER Files (*.der;*.cer)

21. 確保身份證書顯示在「個人證書」頁籤下。



Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

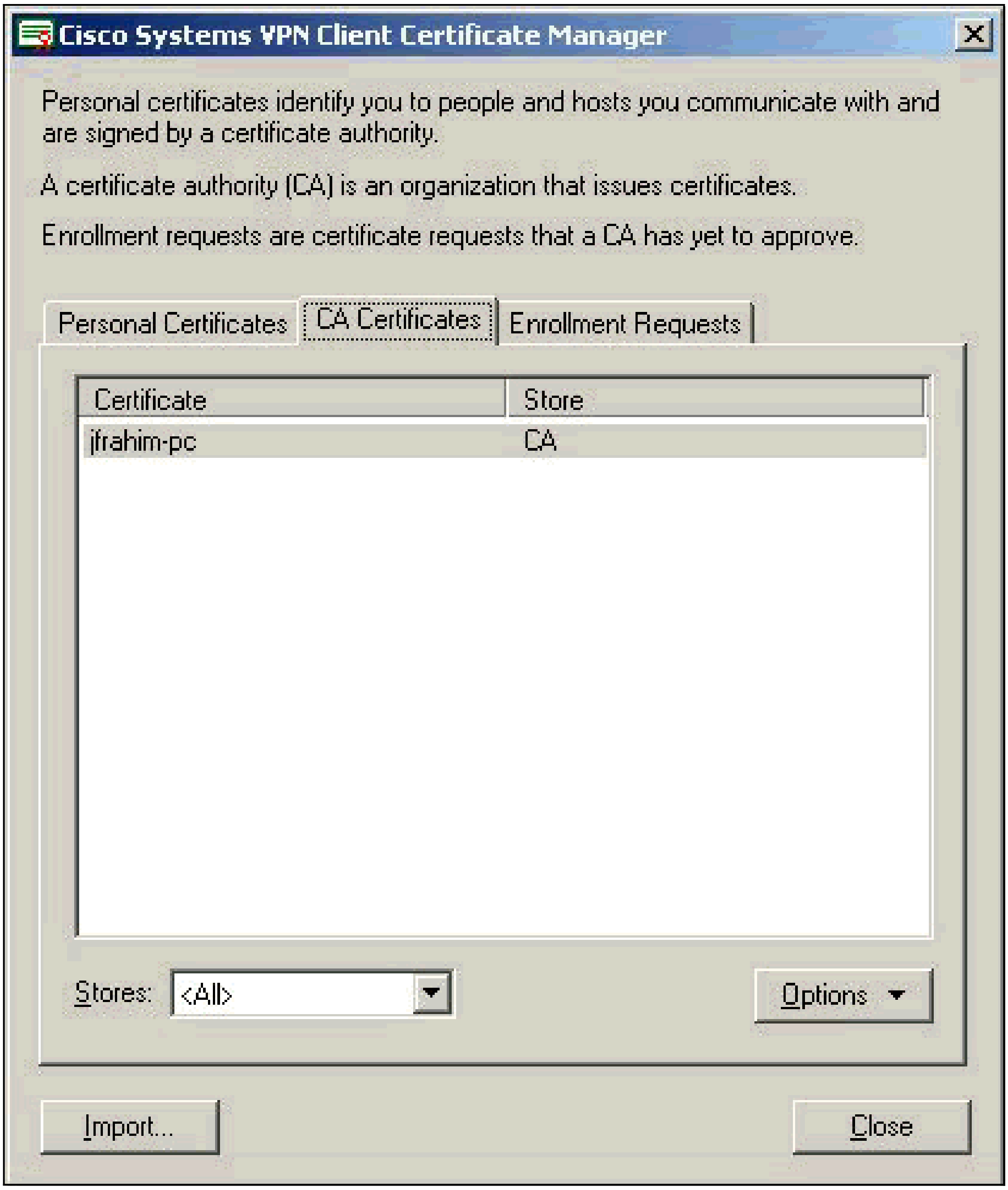
A certificate authority (CA) is an organization that issues certificates.

Enrollment requests are certificate requests that a CA has yet to approve.

Certificate	Store
User5	Cisco

Stores: <All>

22. 確保根證書顯示在CA Certificates頁籤下。



Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

A certificate authority (CA) is an organization that issues certificates.

Enrollment requests are certificate requests that a CA has yet to approve.

Certificate	Store
jfrahim-pc	CA

Stores: <All>

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

嘗試向Microsoft CA Server註冊時，可能會生成此錯誤消息。

```
Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied
```

如果您收到此錯誤消息，請參閱Microsoft CA日誌瞭解詳細資訊，或參閱這些資源瞭解詳細資訊。

- Windows找不到處理請求的證書頒發機構
- XCCC:當您請求安全會議的證書時，會出現「Your Certificate Request was Denied」錯誤消息

相關資訊

- **IPSec 協商/IKE 通訊協定**
- **技術支援與文件 - Cisco Systems**