Configuration de VPN Client 3.x pour obtenir un certificat numérique

Contenu

Introduction

Ce document explique comment configurer le client VPN Cisco 3.x pour obtenir un certificat numérique.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur un PC qui exécute Cisco VPN Client 3.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

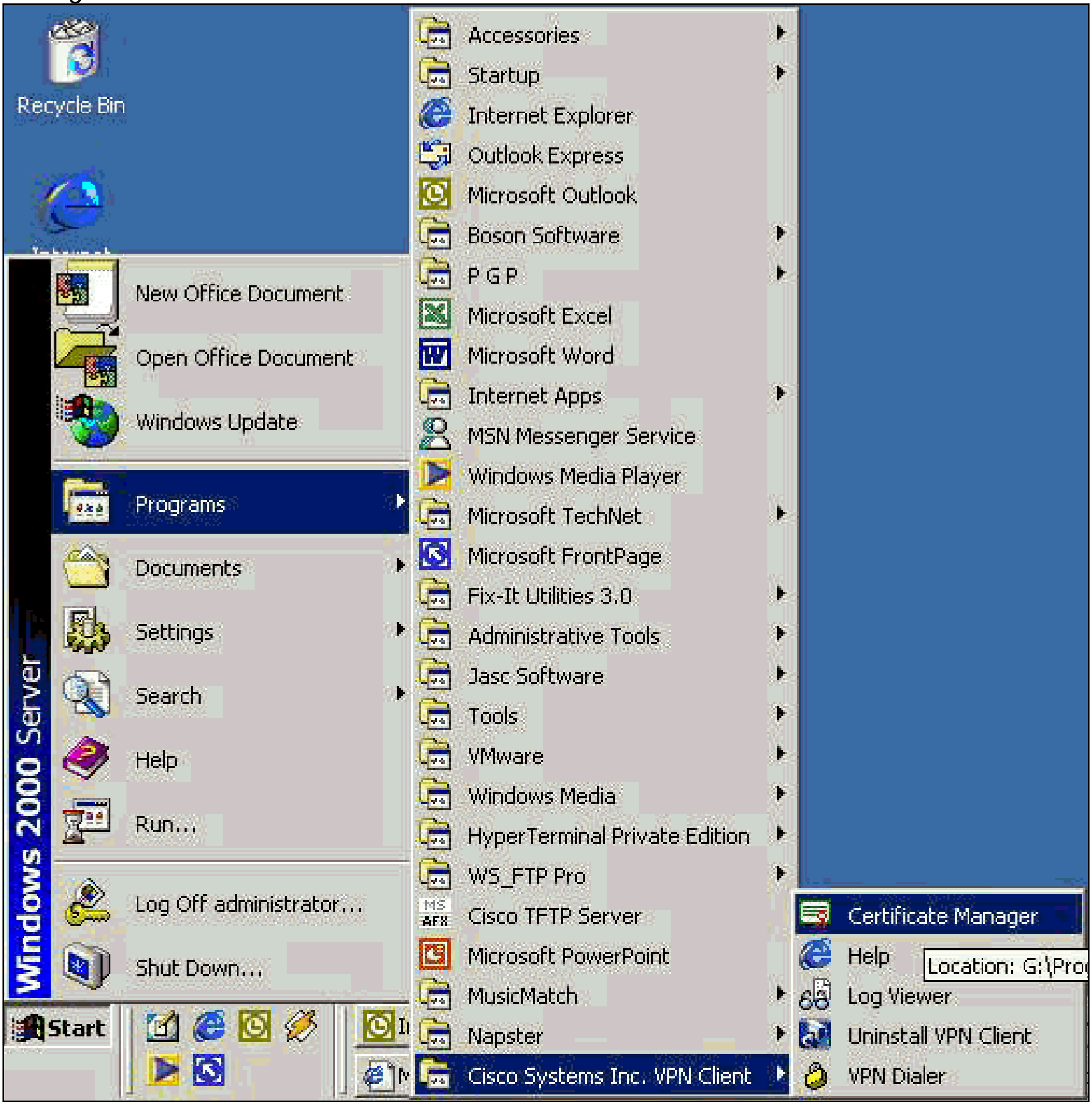
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

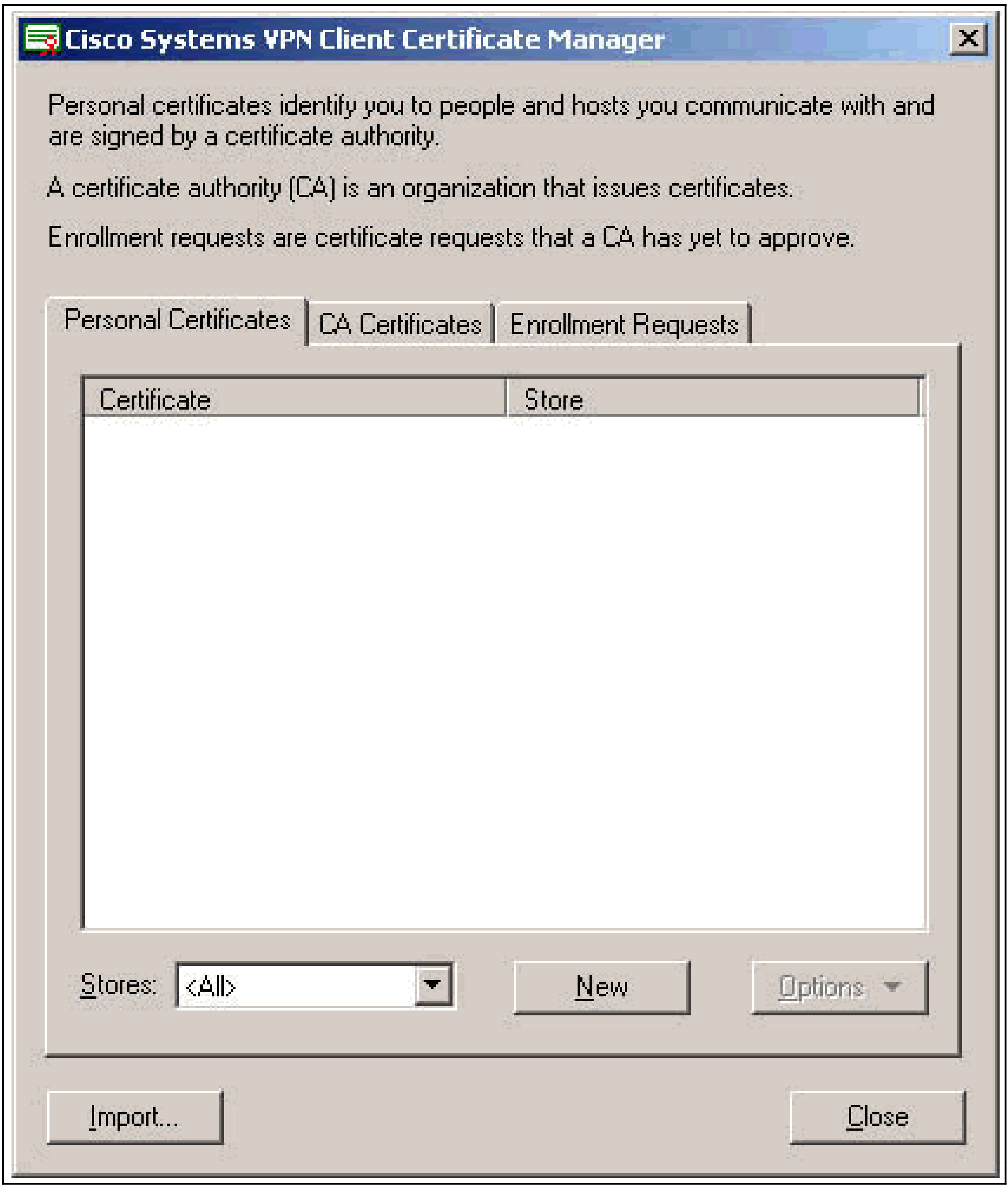
Configurer le client VPN

Complétez ces étapes pour configurer le client VPN.

1. Sélectionnez **Start** > **Programs** > **Cisco Systems Inc. VPN client** > **Certificate Manager** pour lancer VPN Client Certificate Manager.



2. Sélectionnez l'onglet Certificats personnels et cliquez sur



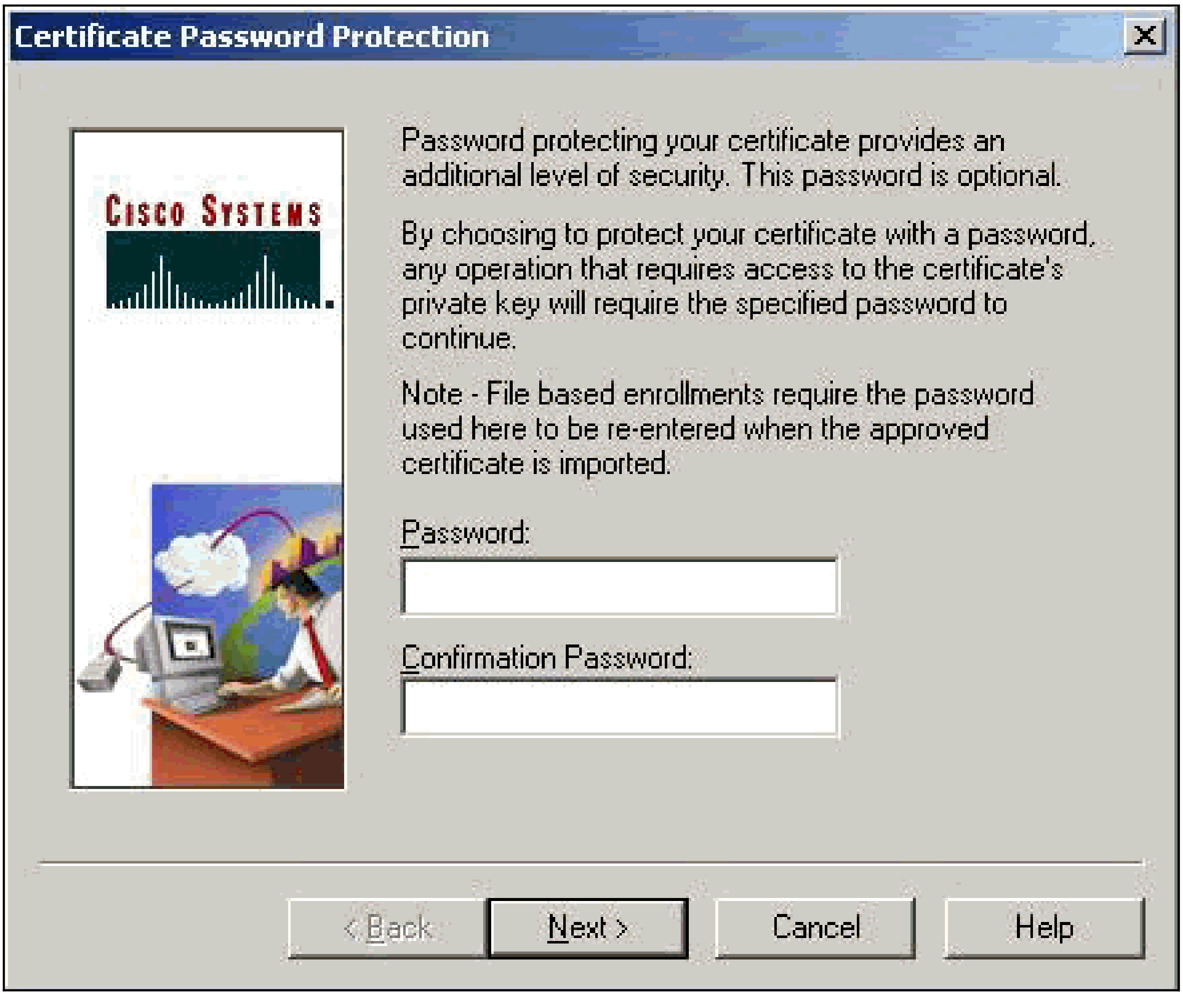
Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

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

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

Nouveau. **Remarque :** les certificats d'ordinateur pour authentifier les utilisateurs pour les connexions VPN ne peuvent pas être effectués avec IPsec.

3. Lorsque le client VPN vous demande un mot de passe, spécifiez un mot de passe pour protéger le certificat. Toute opération nécessitant l'accès à la clé privée du certificat nécessite que le mot de passe spécifié



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.

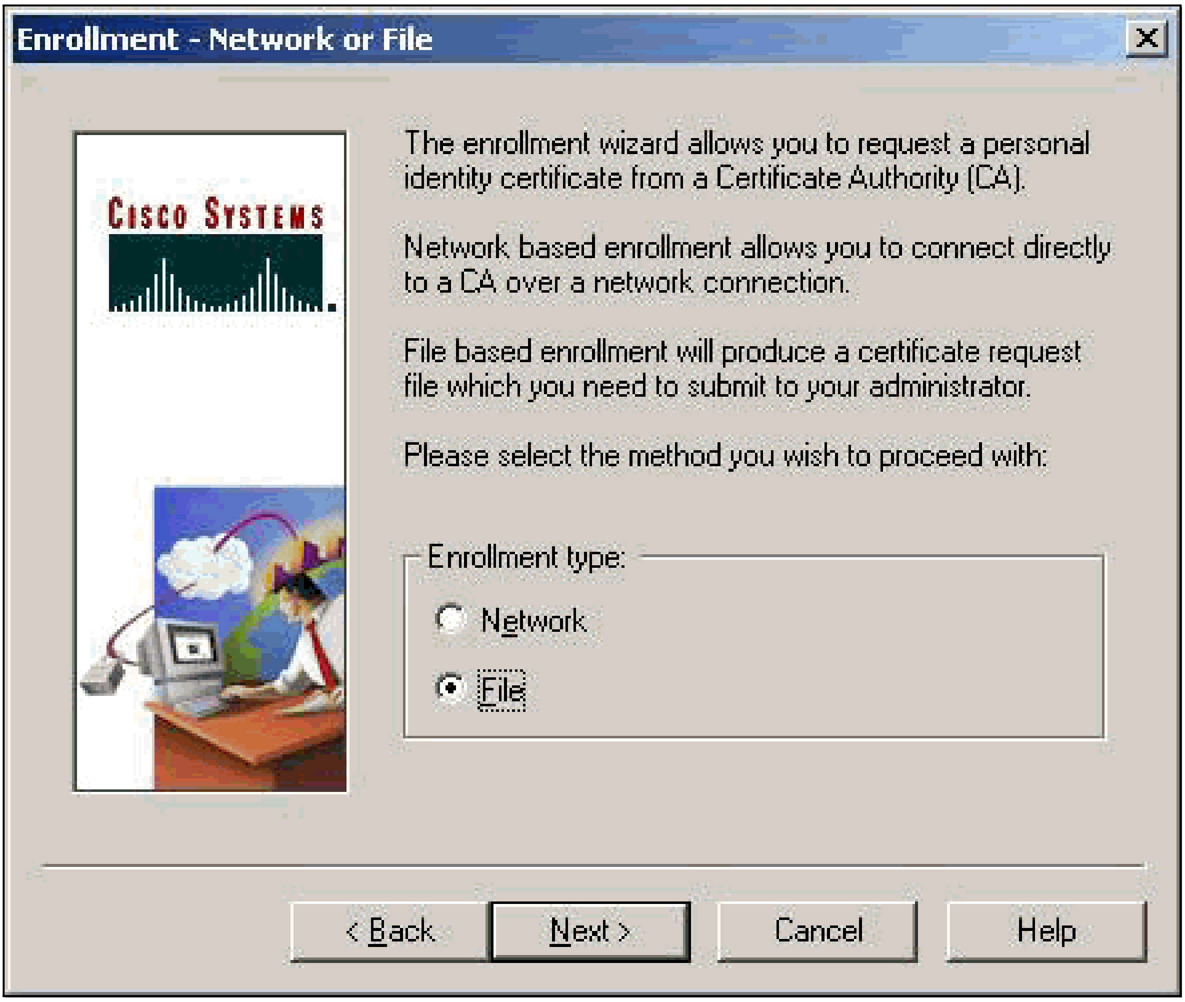
Password:

Confirmation Password:

continue.

4. Sélectionnez **Fichier** pour demander un certificat au format PKCS #10 sur la page Inscription. Cliquez ensuite

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.

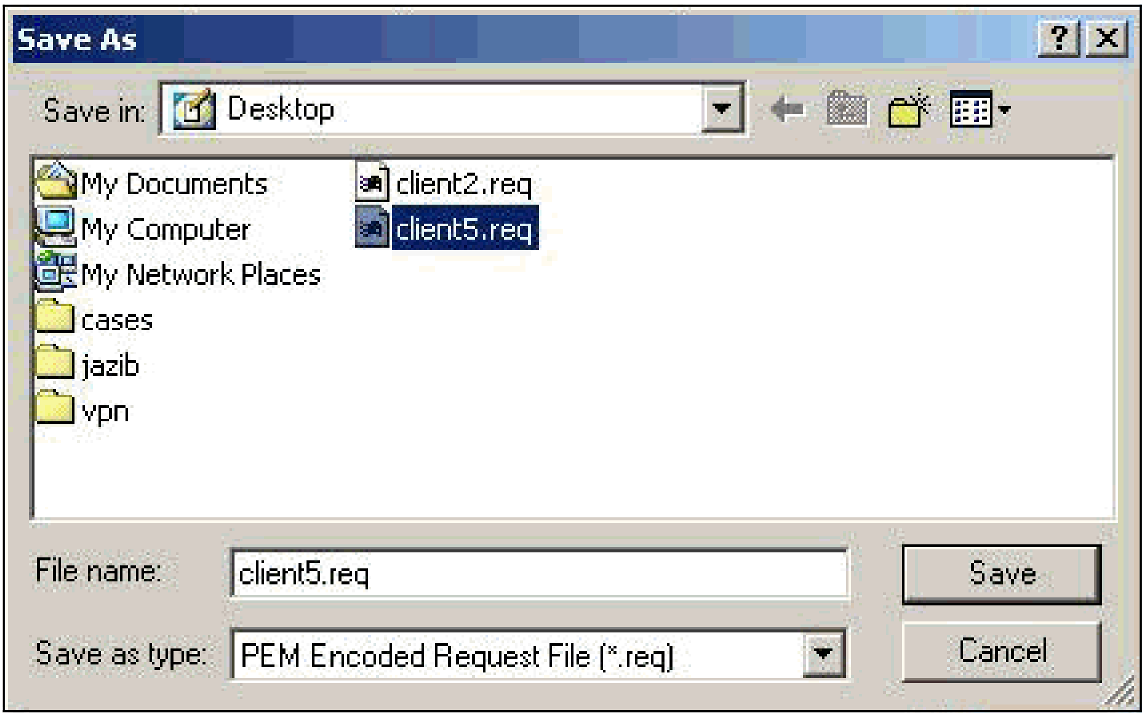
Please select the method you wish to proceed with:

Enrollment type:

○ Network

● File

5. Cliquez sur **Parcourir**, puis spécifiez un nom de fichier pour le fichier de demande de certificat. Pour le type de fichier, sélectionnez **Fichier de demande codée PEM (*.req)** et cliquez sur **Enregistrer**.



Save As

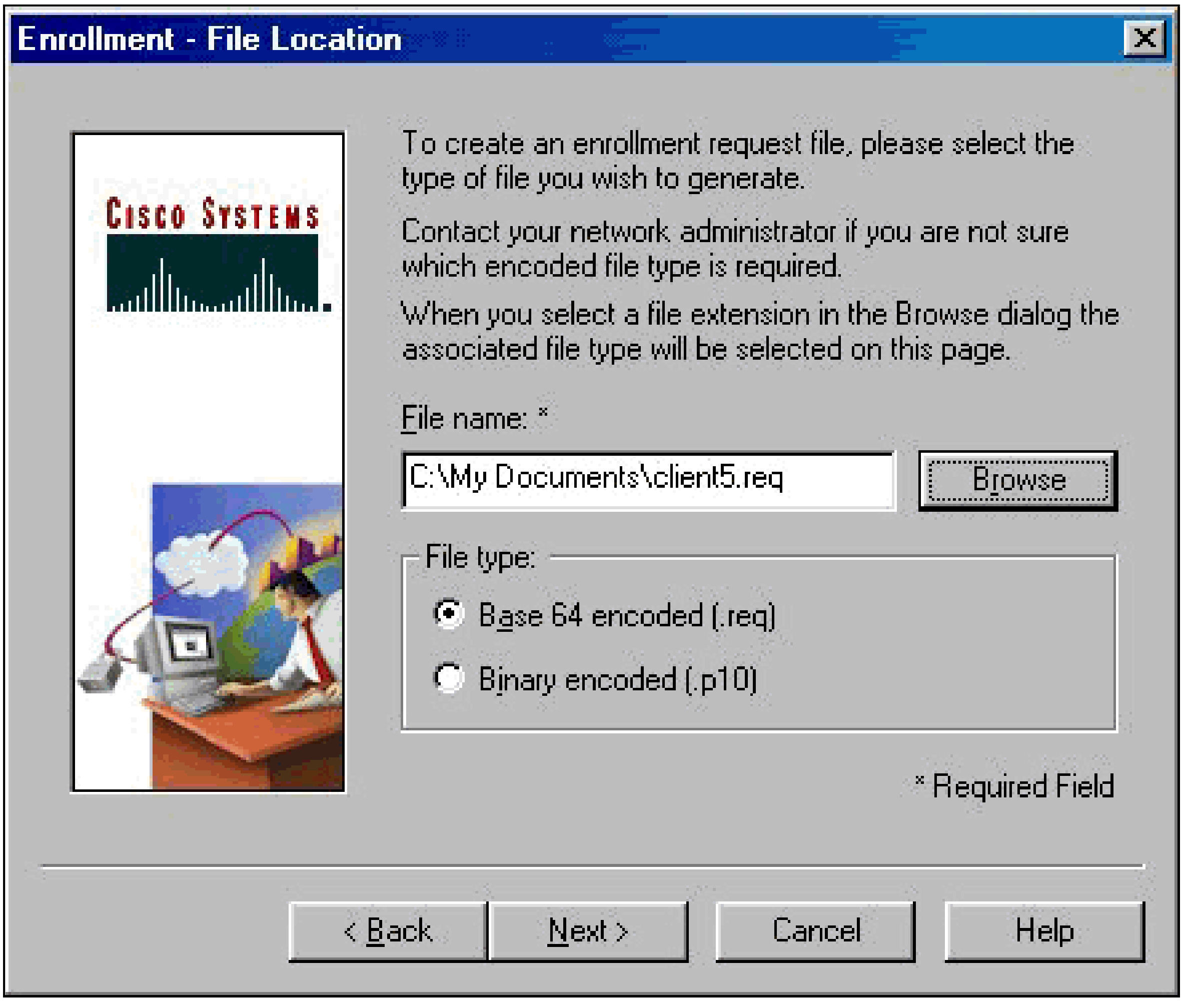
Save in: Desktop

My Documents
My Computer
My Network Places
cases
jazib
vpn
client2.req
client5.req

File name: client5.req

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

6. Cliquez sur **Next** sur la page VPN Client Enrollment.



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

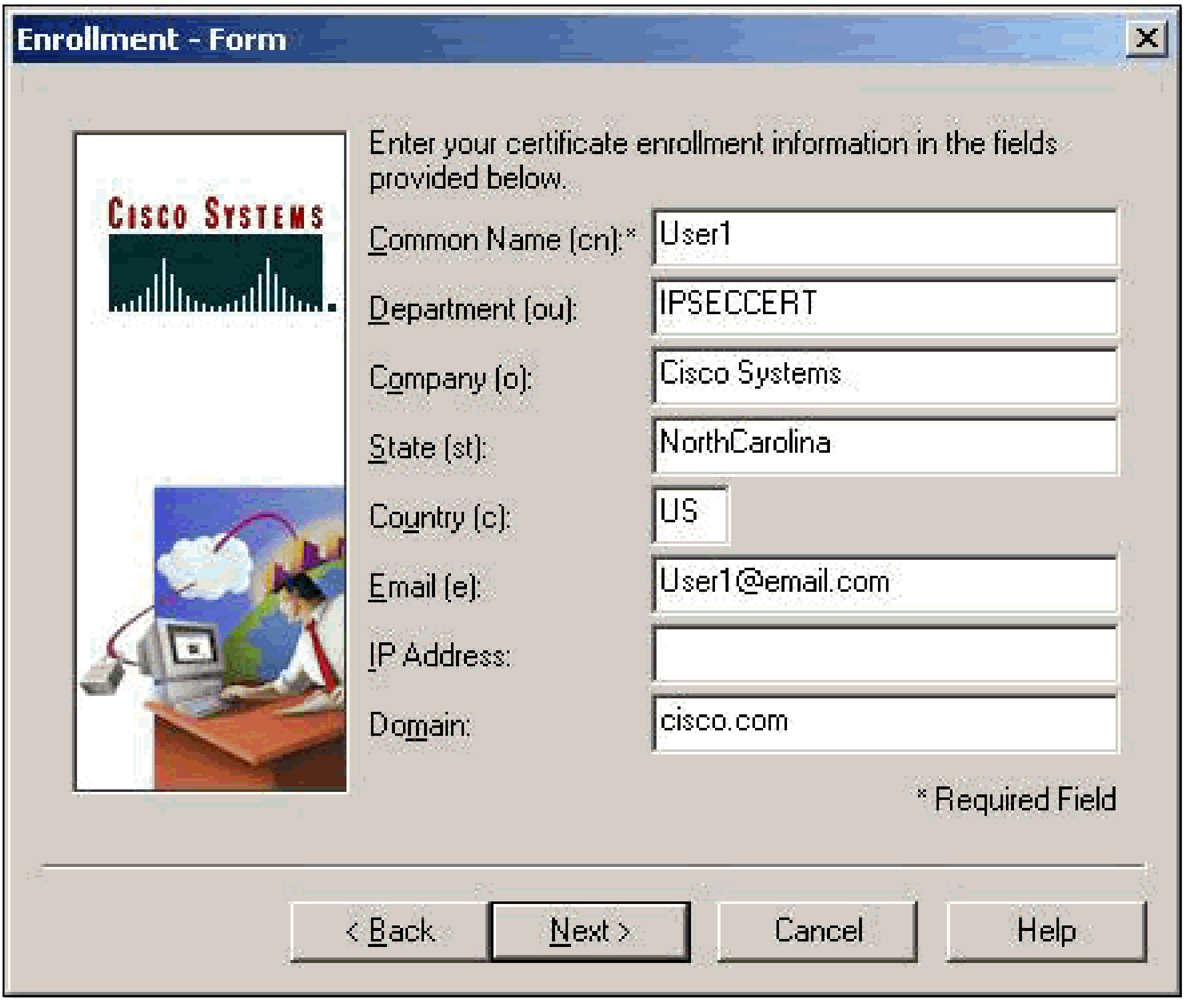
File type:

● Base 64 encoded (.req)

○ Binary encoded (.p10)

* Required Field

7. Remplissez les champs du formulaire d'inscription.Cet exemple montre les champs suivants :Nom commun = Utilisateur1Département = IPSECCERT (cette valeur doit correspondre à l'unité d'organisation (OU) et au nom du groupe sur le concentrateur VPN 3000.)Société = Cisco SystemsÉtat = Caroline du NordPays = États-UnisE-mail = User1@email.comAdresse IP = (facultatif); utilisé pour spécifier l'adresse IP sur la demande de certificat)Domaine = cisco.comCliquez sur **Suivant** lorsque vous avez



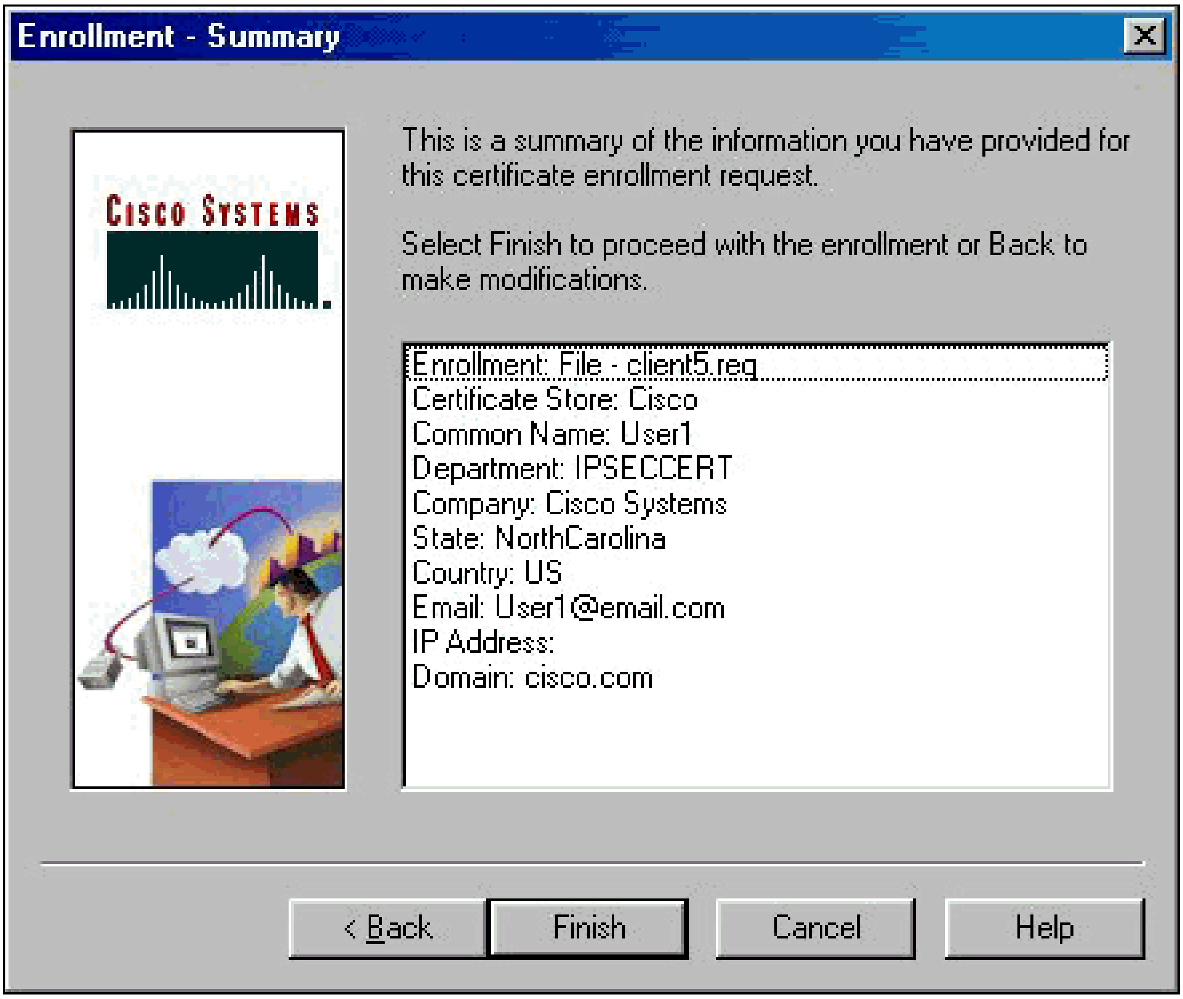
Enter your certificate enrollment information in the fields provided below.

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

terminé.

8. Cliquez sur **Terminer** pour poursuivre l'inscription.



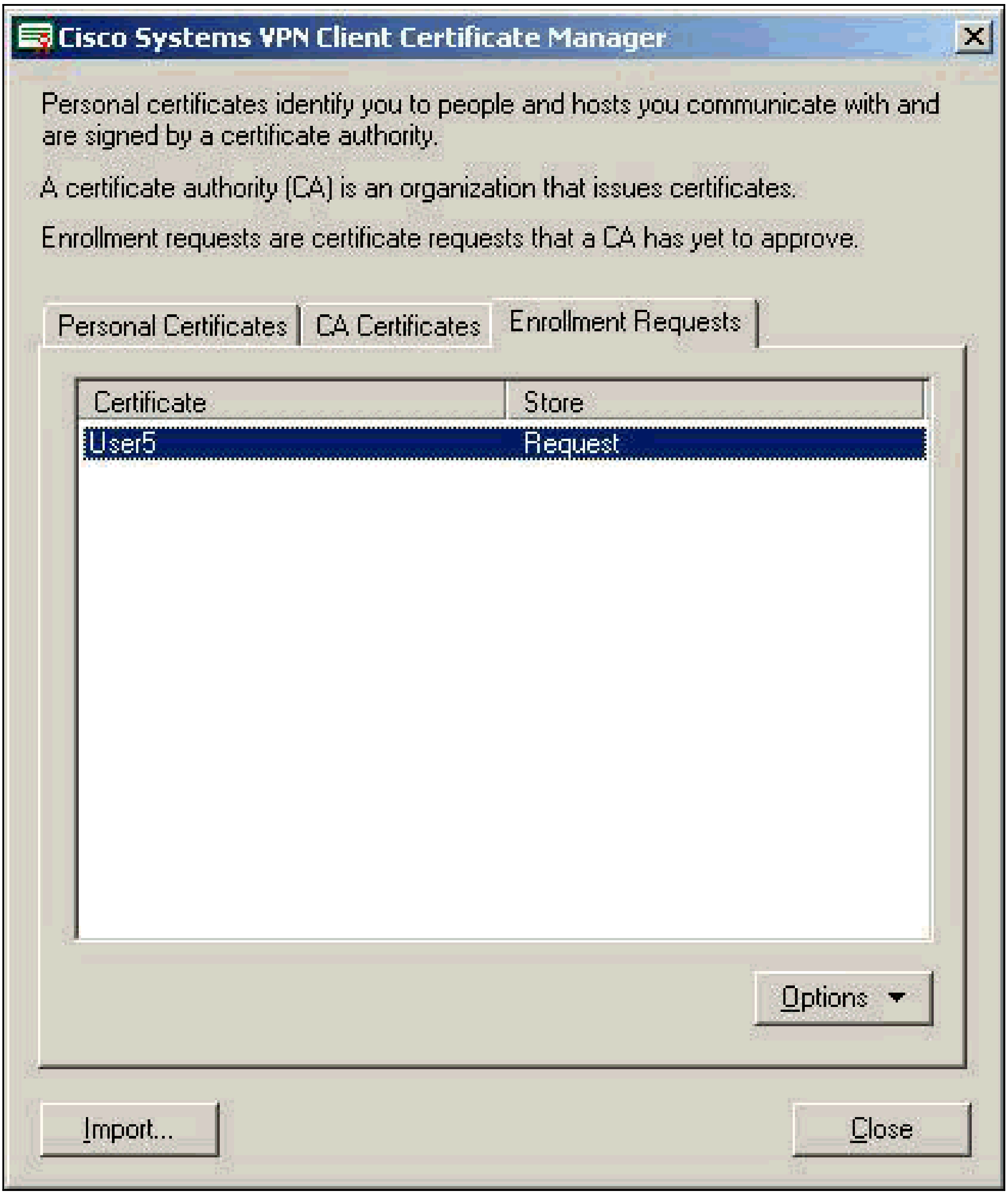
This is a summary of the information you have provided for this certificate enrollment request.

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. Sélectionnez l'onglet Demandes d'inscription pour vérifier la demande sur le gestionnaire de certificats client

VPN.



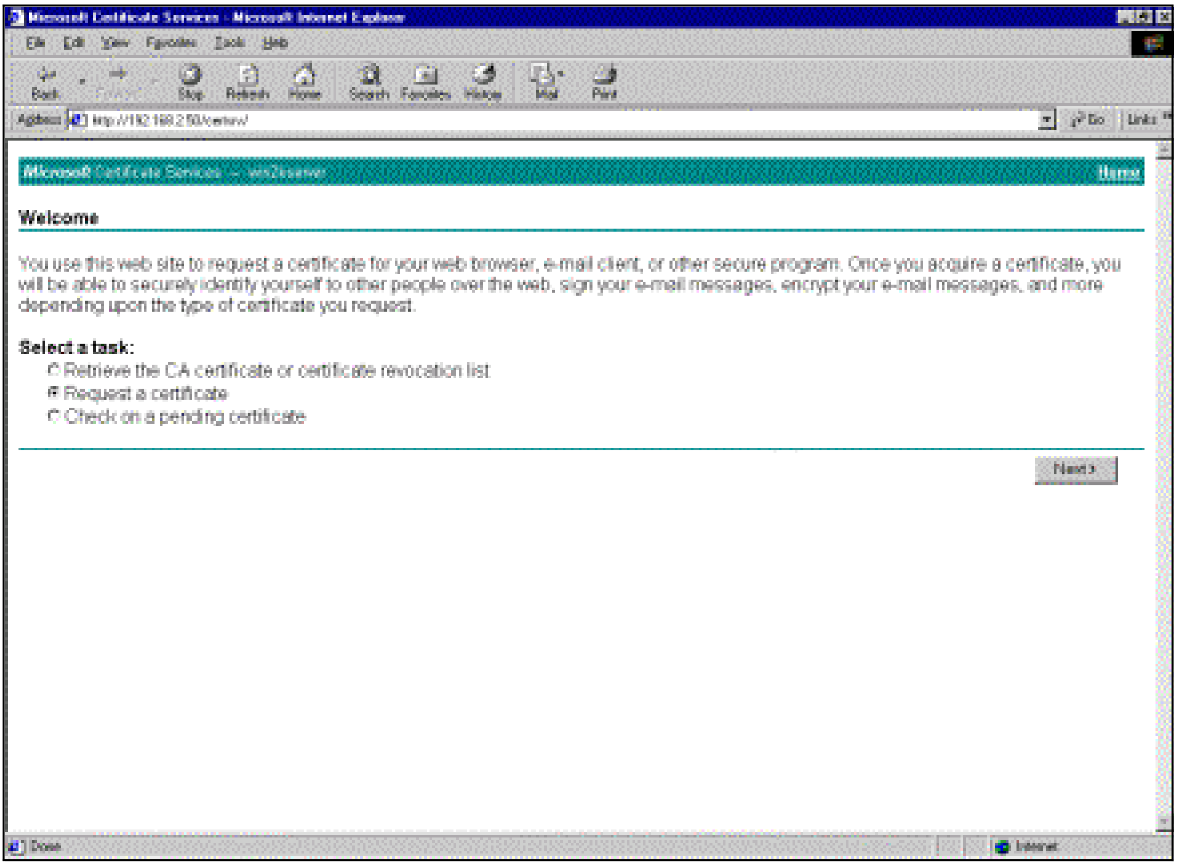
Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

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. Activez simultanément le serveur de l'autorité de certification (CA) et les interfaces du client VPN pour soumettre la demande.
11. Sélectionnez **Demander un certificat** et cliquez sur **Suivant** sur le serveur


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.

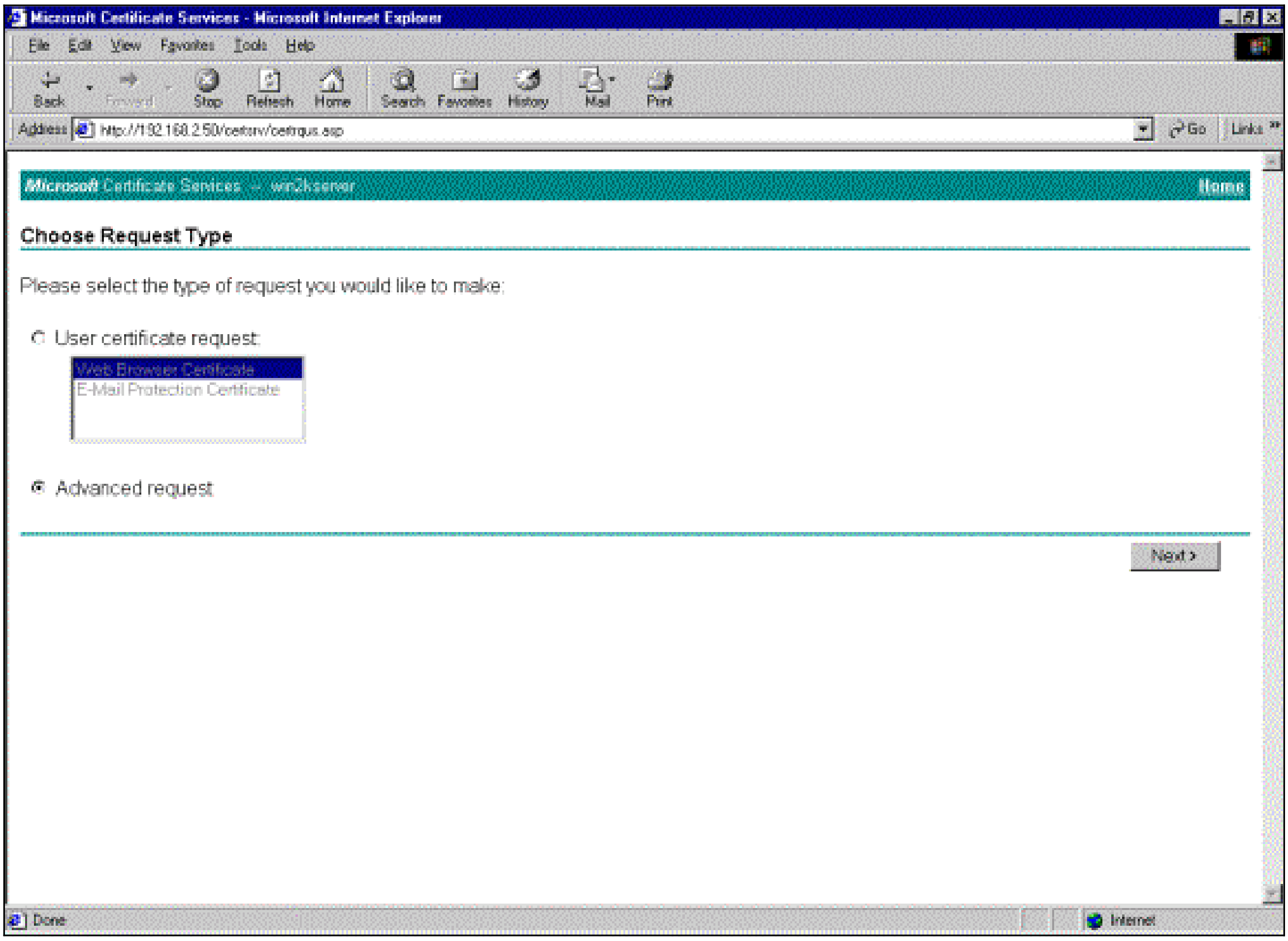
Select a task:

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

Next >

AC.

12. Sélectionnez **Demande avancée** pour le type de demande et cliquez sur **Suivant**.


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:

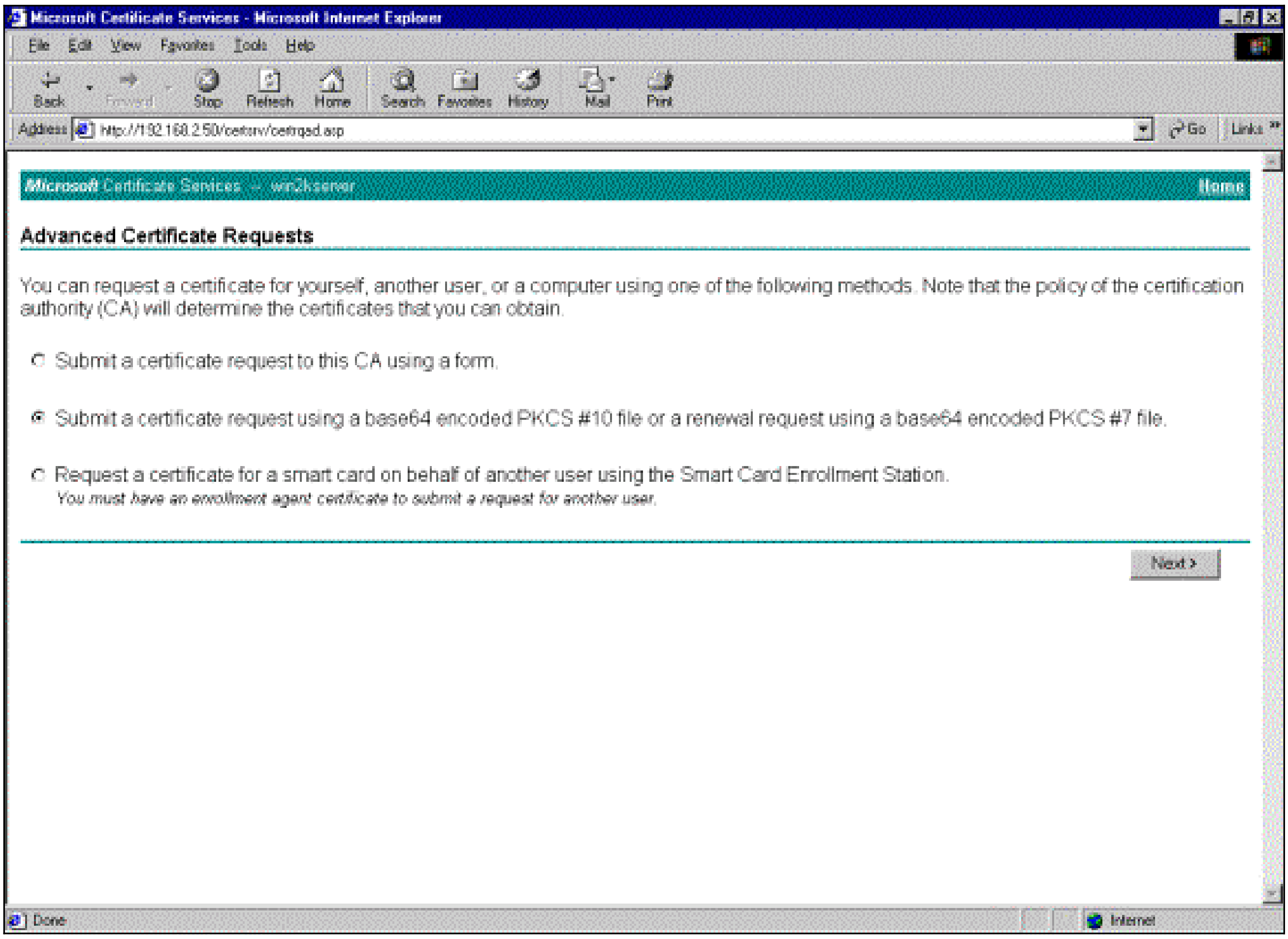
○ User certificate request:
Web Browser Certificate
E-Mail Protection Certificate

● Advanced request

Next >

13. Sélectionnez **Soumettre une demande de certificat à l'aide d'un fichier PKCS #10 codé en base64 ou d'une demande de renouvellement à l'aide d'un fichier PKCS #7 codé en base64** sous Demandes de certificat avancées, puis cliquez sur

Suivant.



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
Done
Internet

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.

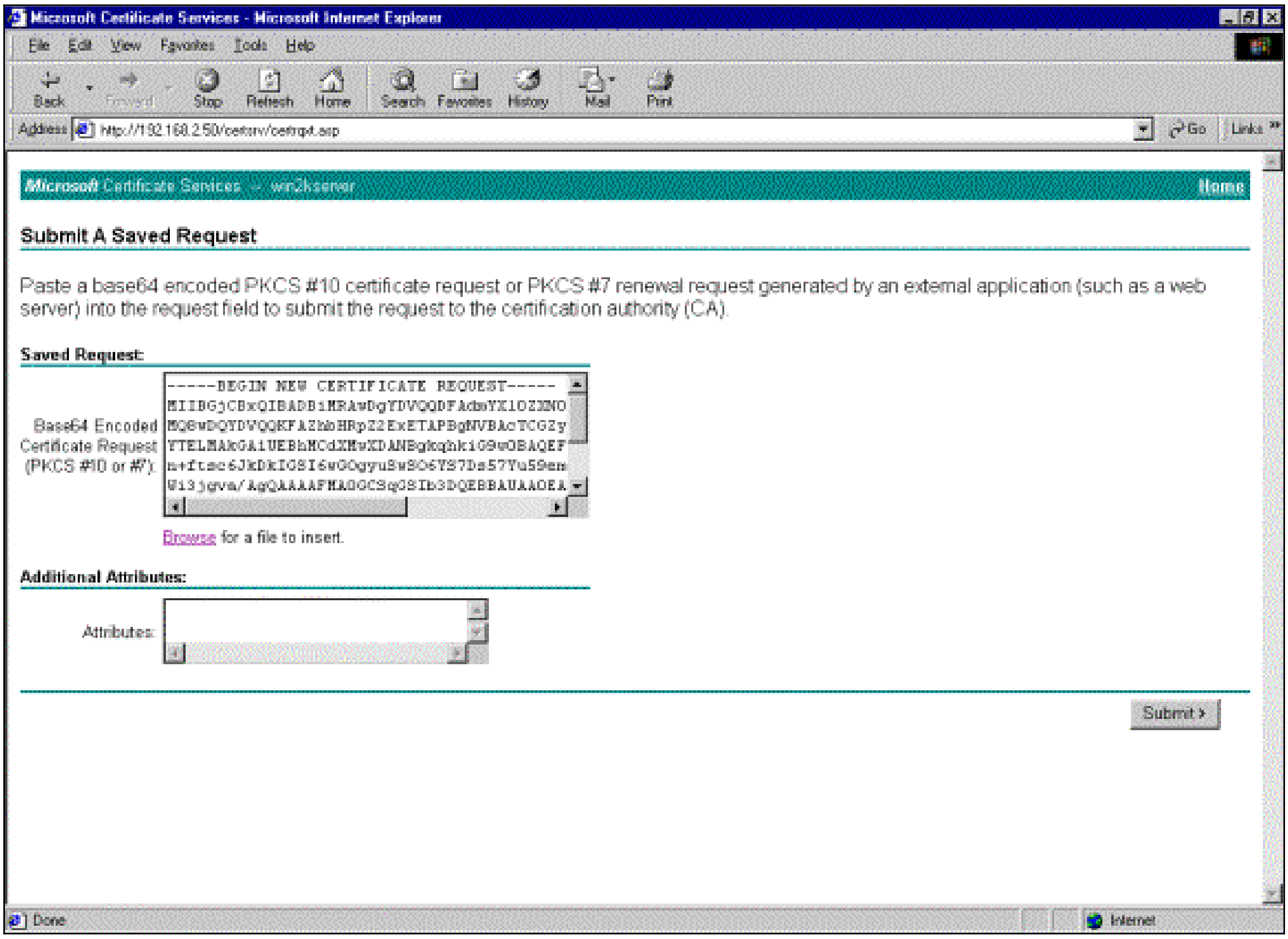
○ Submit a certificate request to this CA using a form.

● 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.

Next >

14. Mettez en surbrillance le fichier de demande du client VPN et collez-le sur le serveur AC sous Requête enregistrée. Cliquez ensuite sur
Soumettre.


Microsoft Certificate Services - Microsoft Internet Explorer

Address http://192.168.2.50/certsrv/certrqxt.asp

Microsoft Certificate Services -- win2kserver

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-----
MIIBGjCBxQIBADB1MRAwDgYDVQQDFAdmYX1OZ3NO
MQ8wDQYDVQQKFAZhbHRpZ2ExETAPBgNVBAcTCGZy
YTELMAkGA1UEBhMCdXMwXDANBgkqhkiG9w0BAQEF
m+ftmc6JkDkIG8I6wGOgyu8wSO6YS7Ds57Yu59em
W13jgva/AgQAAAAFMA0GCSqGSIb3DQEBBAUAA0EA
```

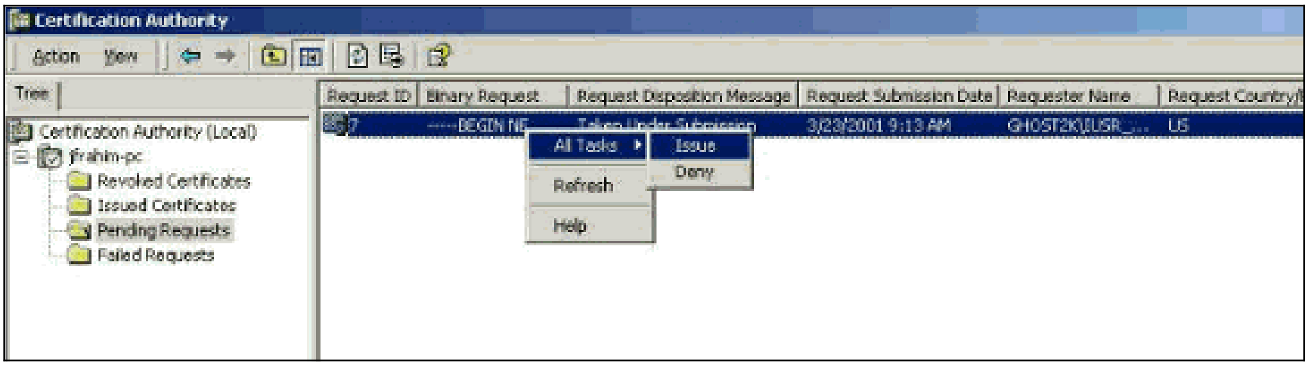
Browse for a file to insert.

Additional Attributes:

Attributes:

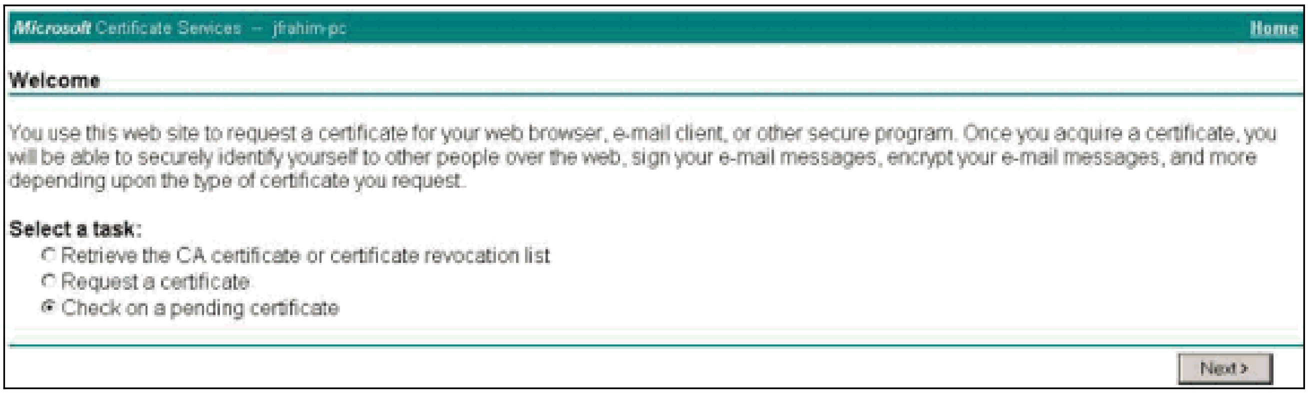
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Go Links
Home
Submit >
Done
Internet

15. Sur le serveur AC, émettez le certificat d'identité pour la demande du client VPN.


Certification Authority

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

16. Téléchargez les certificats racine et d'identité sur le client VPN. Sur le serveur AC, sélectionnez **Vérifier un certificat en attente**, puis cliquez sur **Suivant**.


Microsoft Certificate Services -- jfrahim-pc

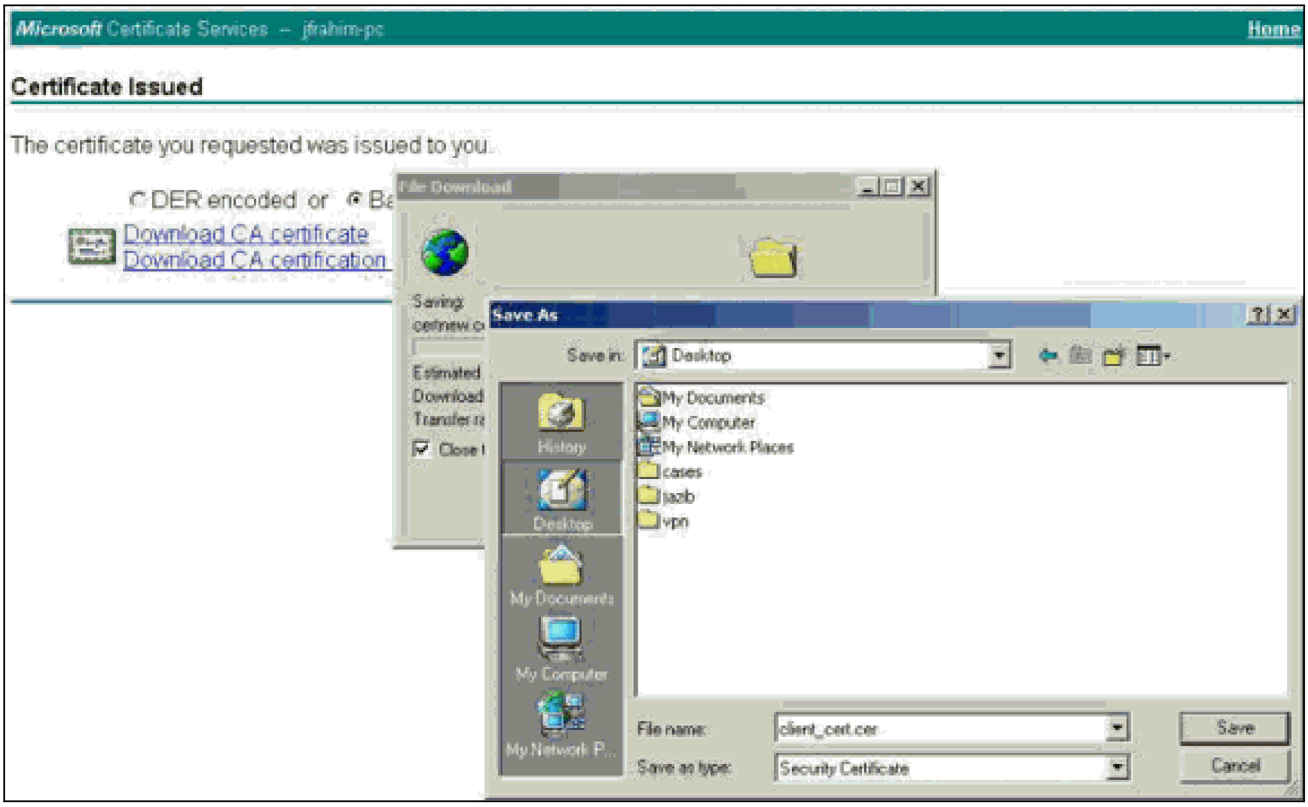
Welcome

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. Sélectionnez **Codé Base 64**. Cliquez ensuite sur **Télécharger le certificat de l'Autorité de certification** sur le serveur de l'Autorité de certification.



Microsoft Certificate Services -- jfrahim-pc

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Ba

Download CA certificate

Download CA certification

Saving:

certnew.c

Estimated

Download

Transfer r

☑ Close t

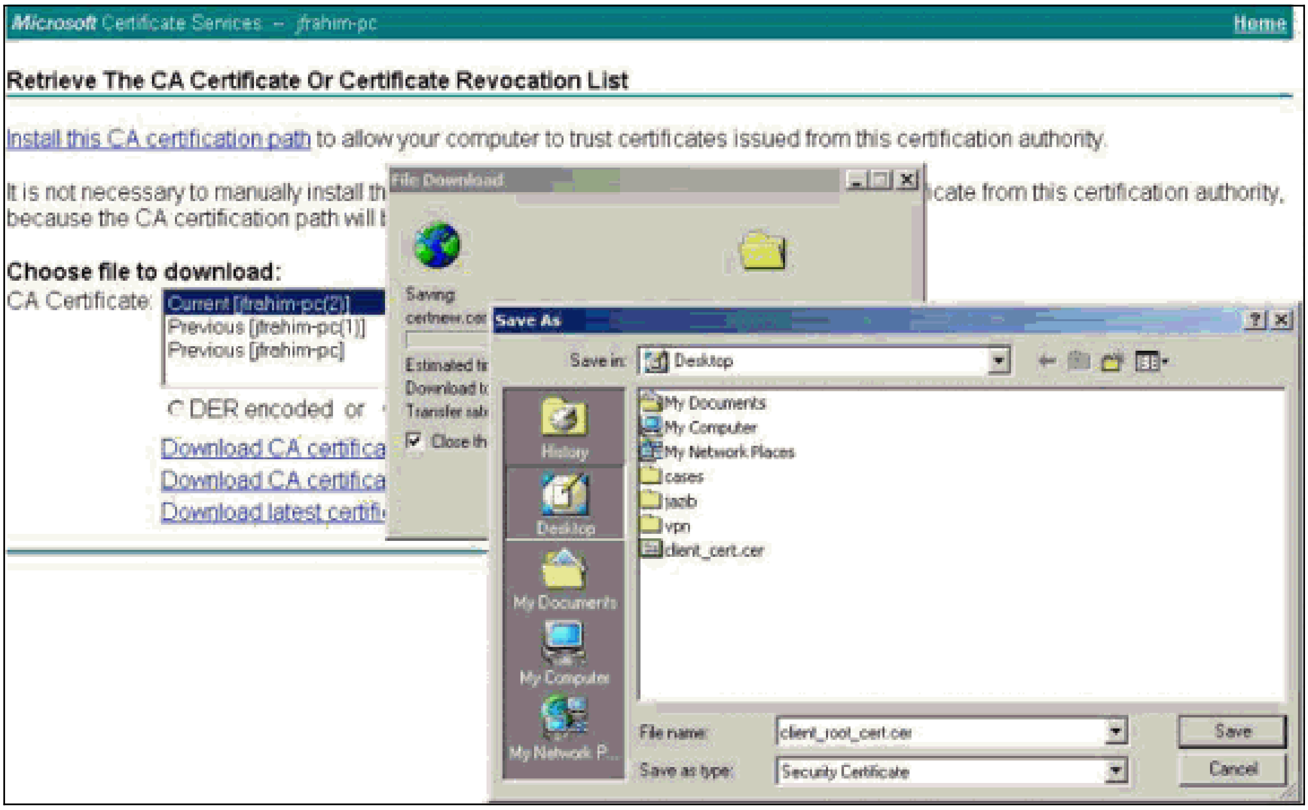
Save As

Save in: Desktop

File name: client_cert.cer

Save as type: Security Certificate

18. Sélectionnez un fichier à télécharger à partir de la page Récupérer le certificat CA ou la liste de révocation de certificat pour obtenir le certificat racine sur le serveur AC. Cliquez ensuite **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... icate 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

Saving:

certnew.cer

Estimated ti

Download t

Transfer rat

☑ Close th

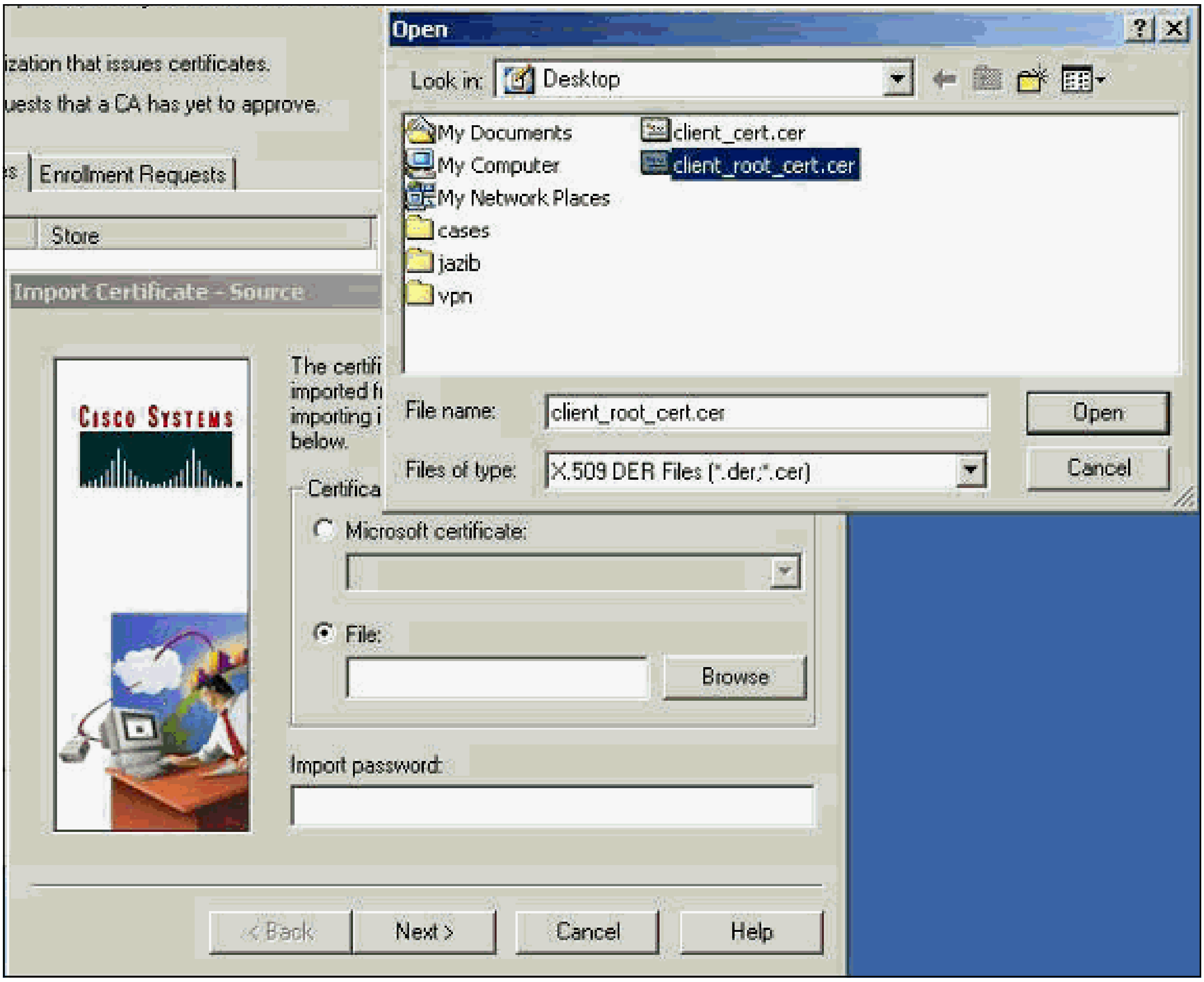
Save As

Save in: Desktop

File name: client_root_cert.cer

Save as type: Security Certificate

19. Sélectionnez **Certificate Manager** > **CA Certificate** > **Import sur le client VPN**, puis sélectionnez le fichier AC racine pour installer les certificats racine et d'identité.



ization that issues certificates.

uests that a CA has yet to approve.

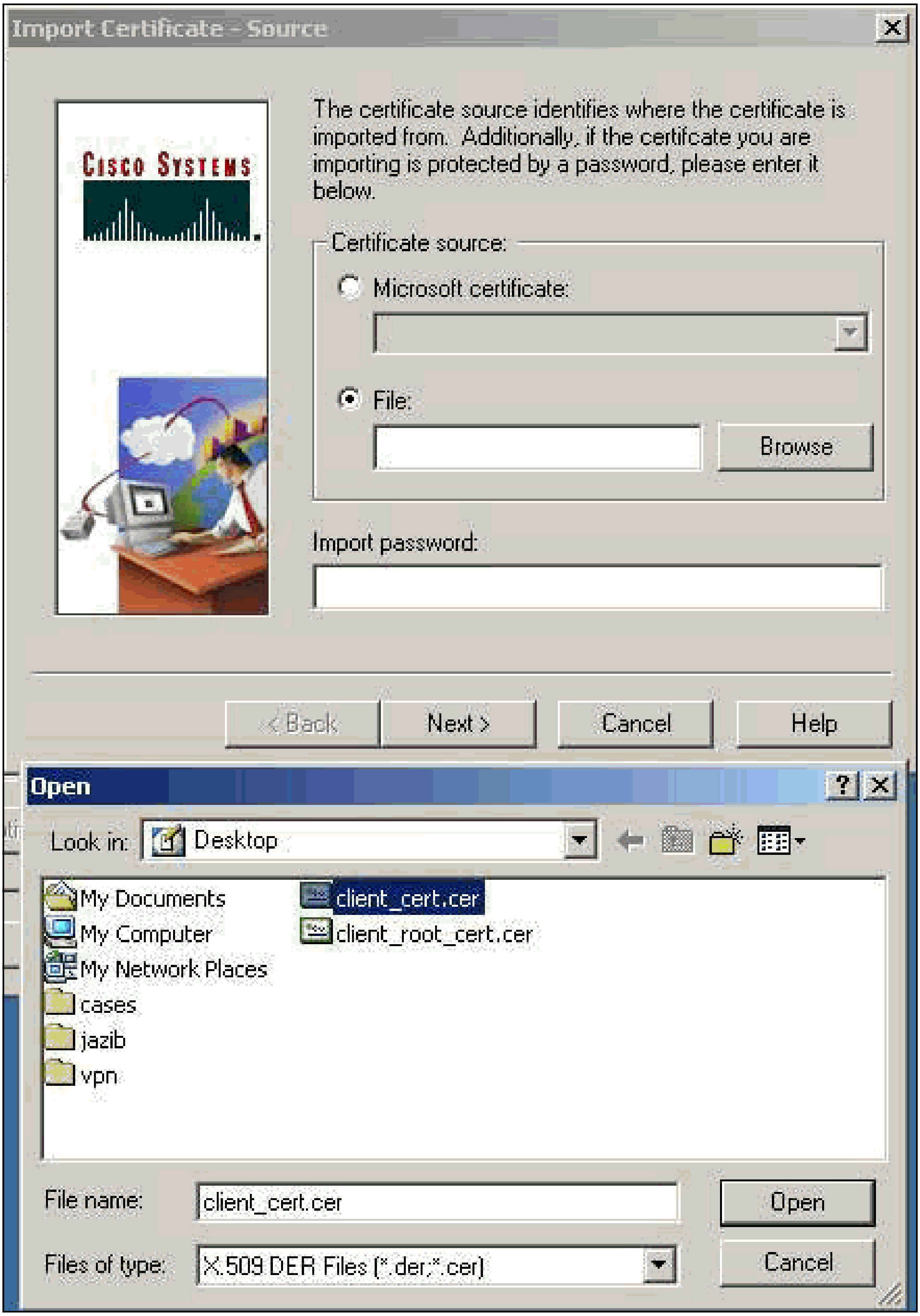
Look in: Desktop

File name: client_root_cert.cer

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

The certifi imported fi importing i below.

20. Sélectionnez **Gestionnaire de certificats** > **Certificats personnels** > **Importer** et choisissez le fichier de certificat d'identité.



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:

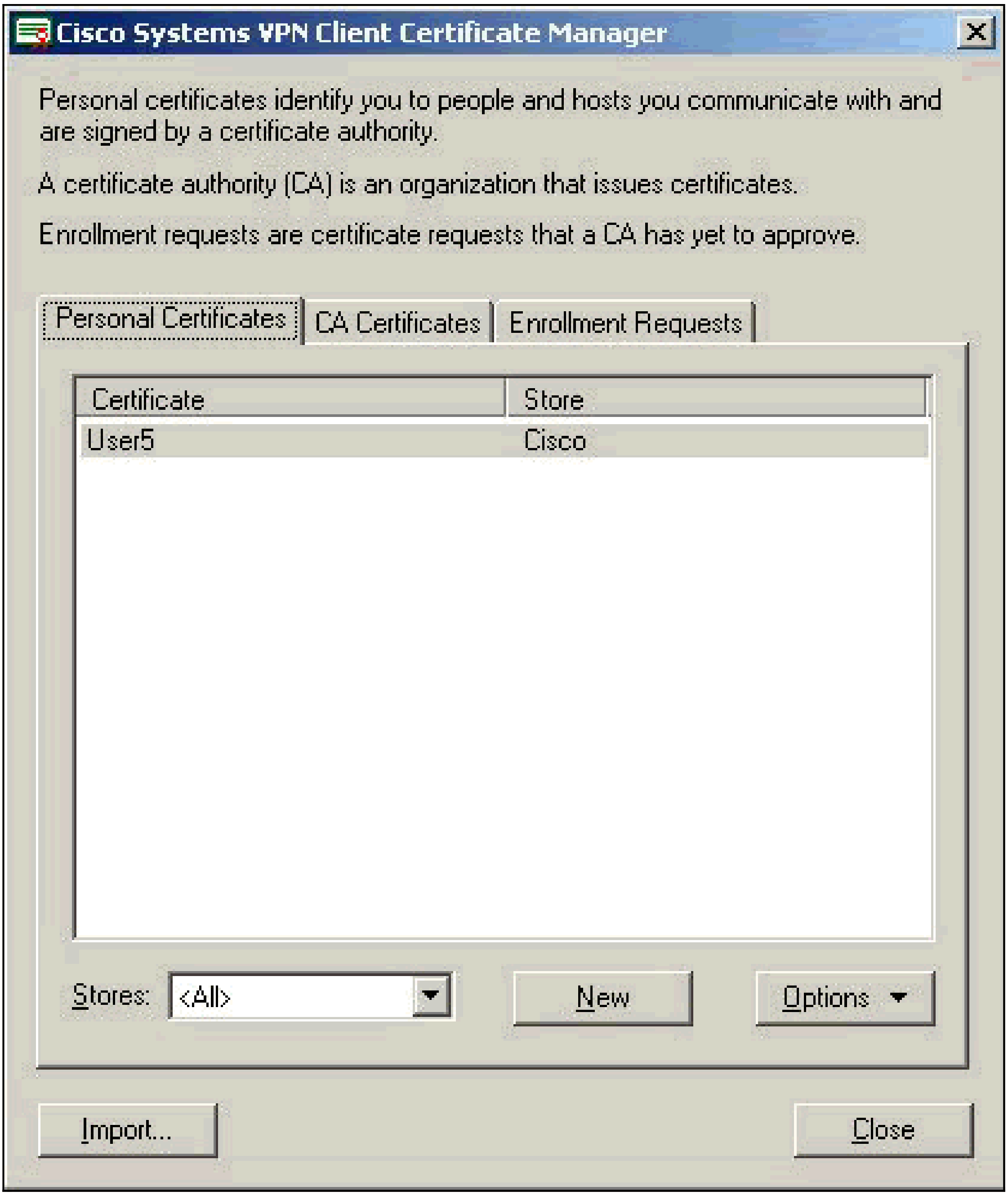
Open

Look in: Desktop

File name: client_cert.cer

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

21. Vérifiez que le certificat d'identité apparaît sous l'onglet Certificats



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.

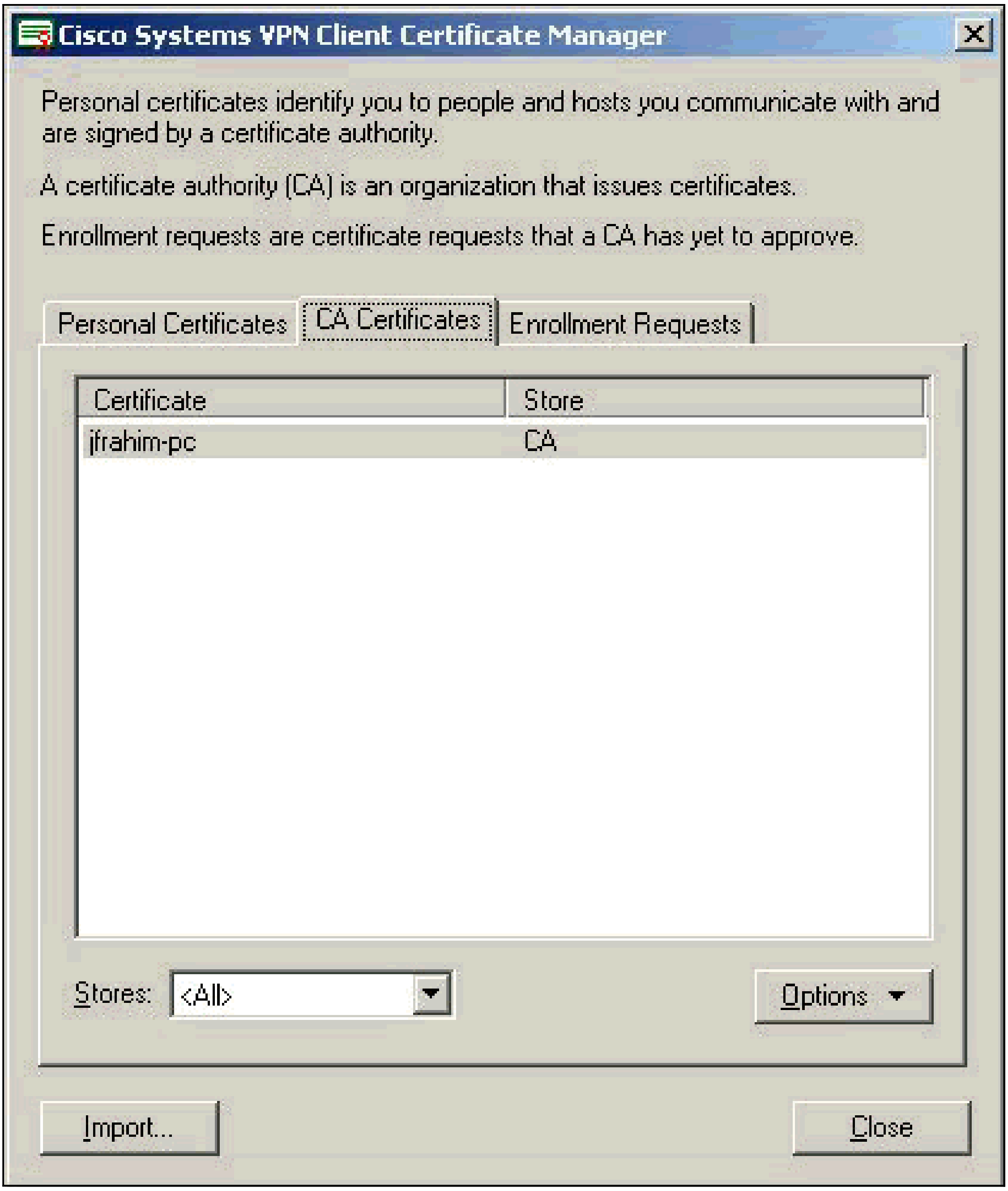
Certificate	Store
User5	Cisco

Stores: <All>

personnels.

22. Assurez-vous que le certificat racine apparaît sous l'onglet Certificats

CA.



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

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Lorsque vous tentez de vous inscrire à Microsoft CA Server, il peut générer ce message d'erreur.

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

Si vous recevez ce message d'erreur, reportez-vous aux journaux de l'Autorité de certification

Microsoft pour plus d'informations ou reportez-vous à ces ressources pour plus d'informations.

- Windows ne trouve pas d'autorité de certification qui traite la demande
- XCCC : Le message d'erreur « Votre demande de certificat a été refusée » se produit lorsque vous demandez un certificat pour des conférences sécurisées

Informations connexes

- **Négociation IPSec/Protocoles IKE**
- **Support et documentation techniques - Cisco Systems**