Configurando o VPN Client 3.x para obter um certificado digital

Contents

Introduction

Este documento demonstra como configurar o Cisco VPN Client 3.x para obter um certificado digital.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em um PC que executa o 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.

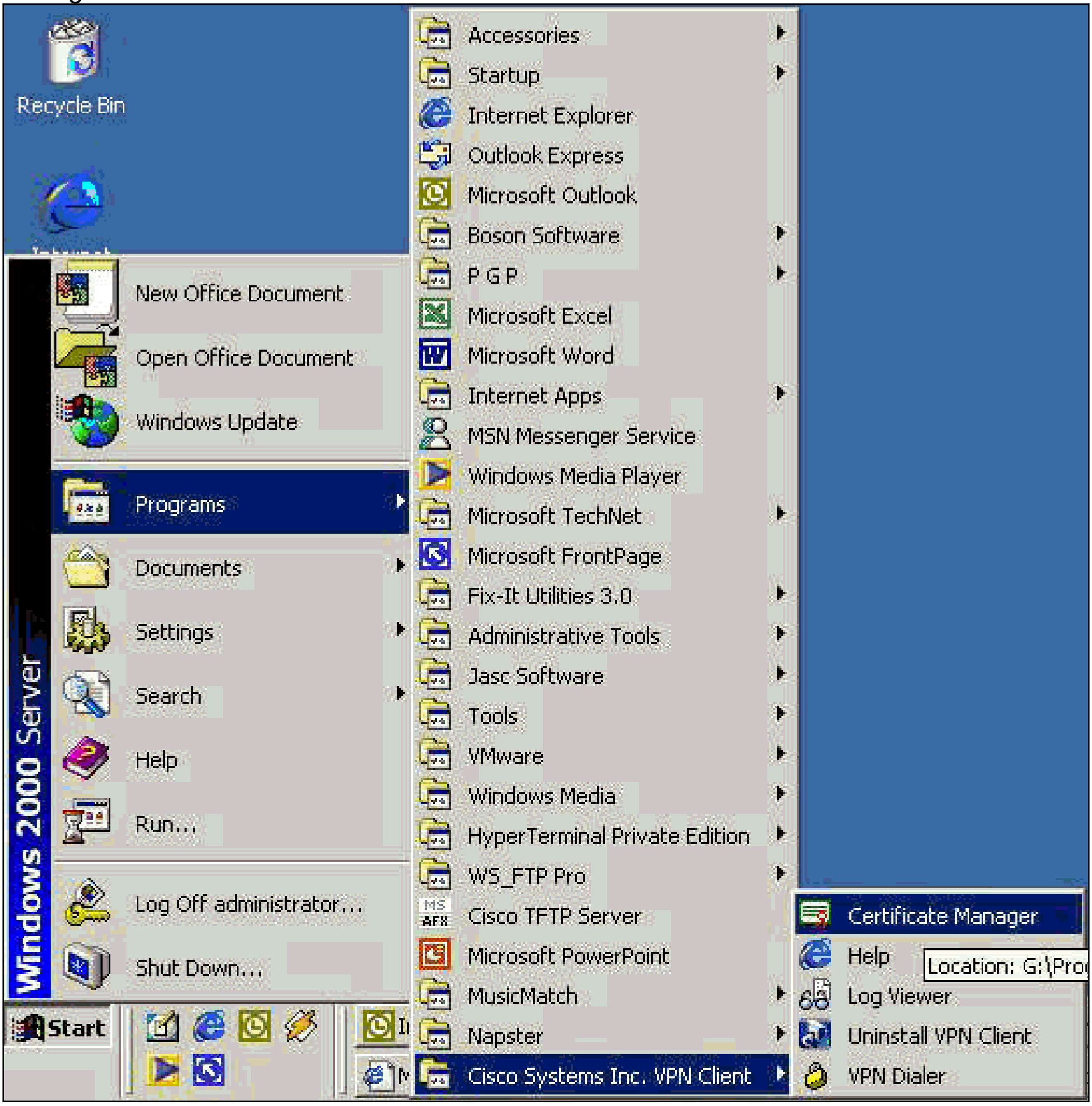
Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

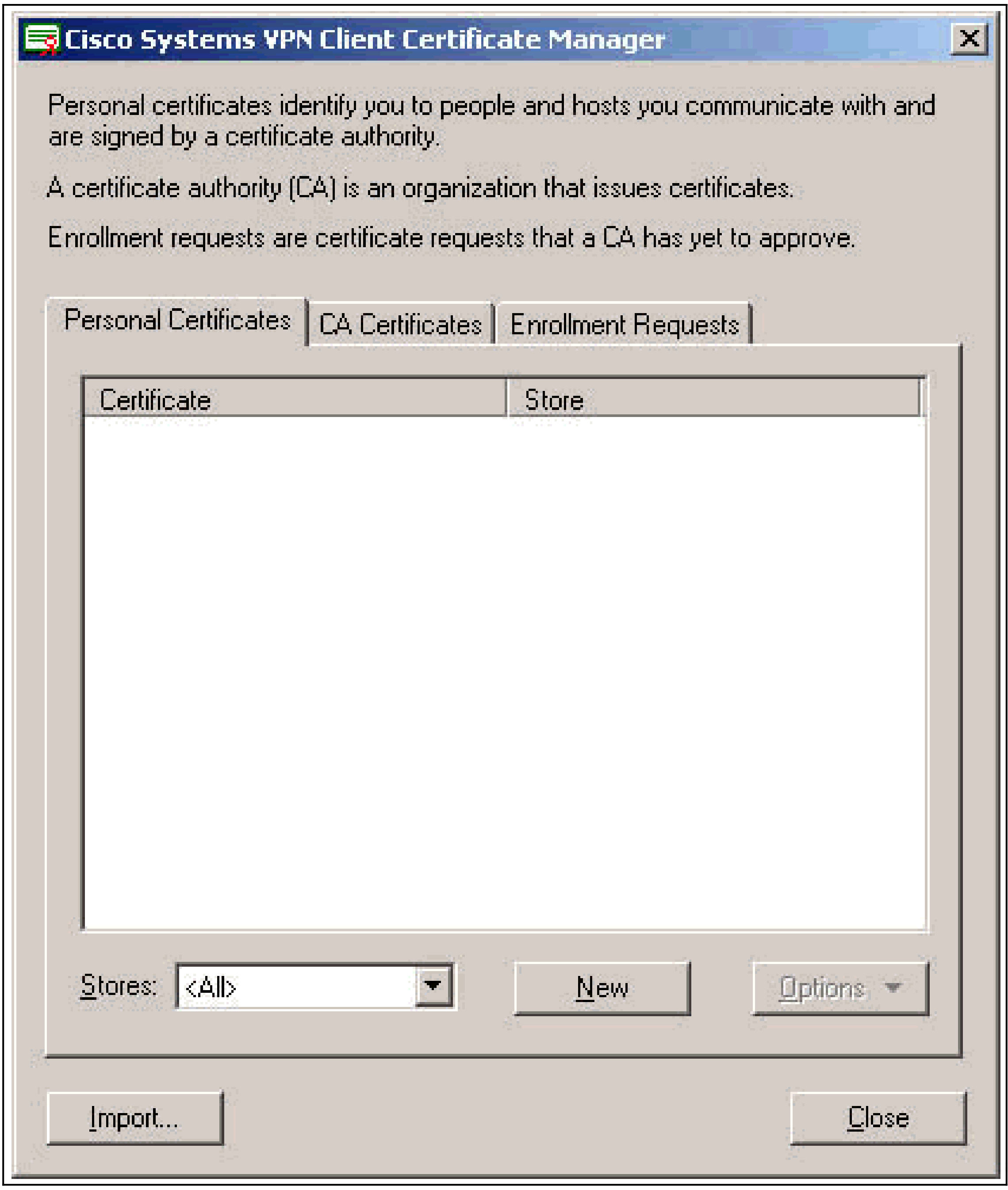
Configurar o VPN Client

Conclua estes passos para configurar o VPN Client.

1. Selecione **Start** > **Programs** > **Cisco Systems Inc. VPN client** > **Certificate Manager** para iniciar o VPN Client Certificate
   Manager.



2. Selecione a guia Certificados pessoais e clique em



Cisco Systems VPN Client Certificate Manager

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

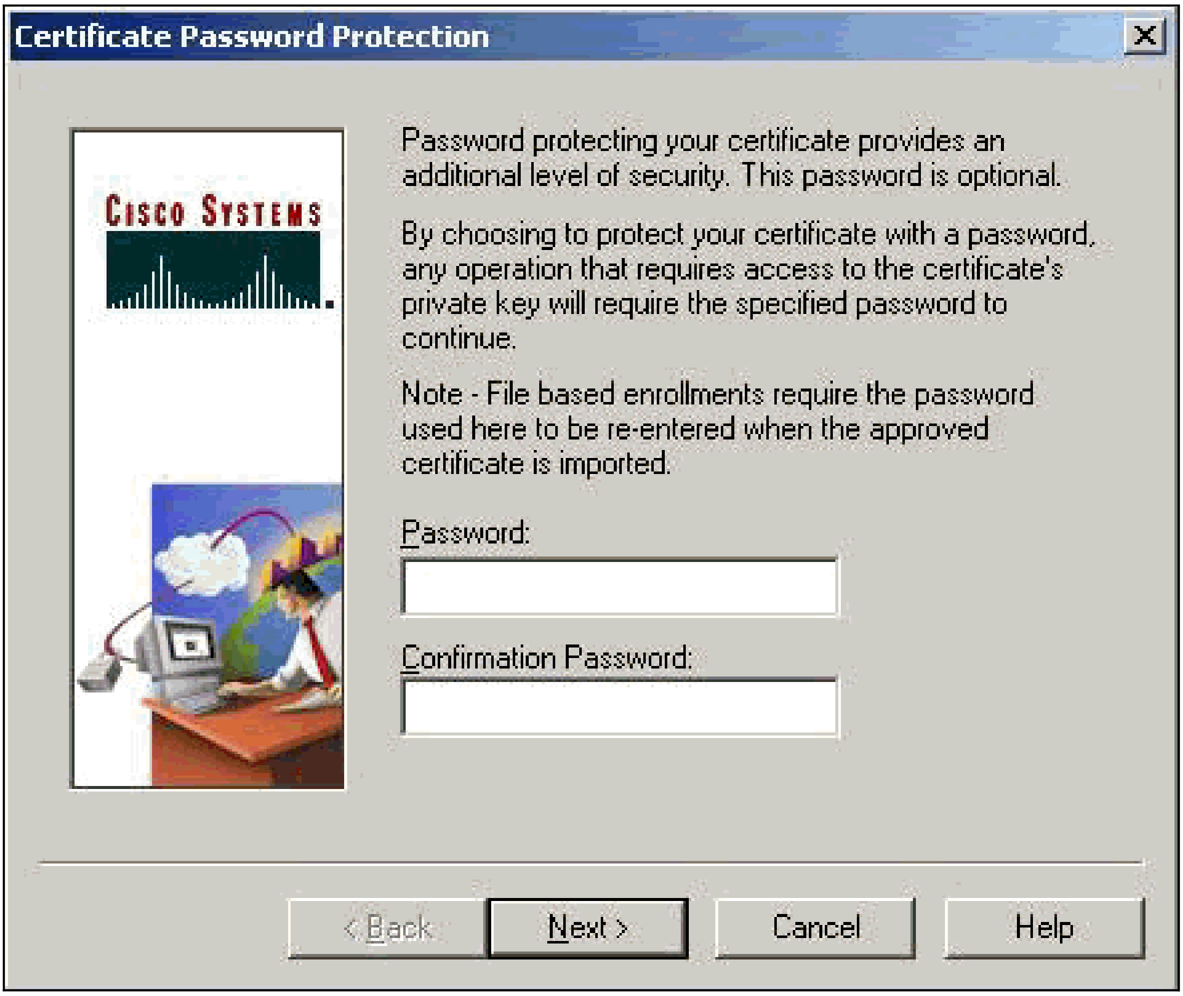
A certificate authority (CA) is an organization that issues certificates.

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

Novo. **Observação:** certificados de máquina para autenticar usuários para conexões VPN não podem ser feitos com o IPsec.

3. Quando o VPN Client solicitar uma senha, especifique uma senha para proteger o certificado. Qualquer operação que exija acesso à chave privada do certificado requer que a senha especificada

continue.



Certificate Password Protection

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

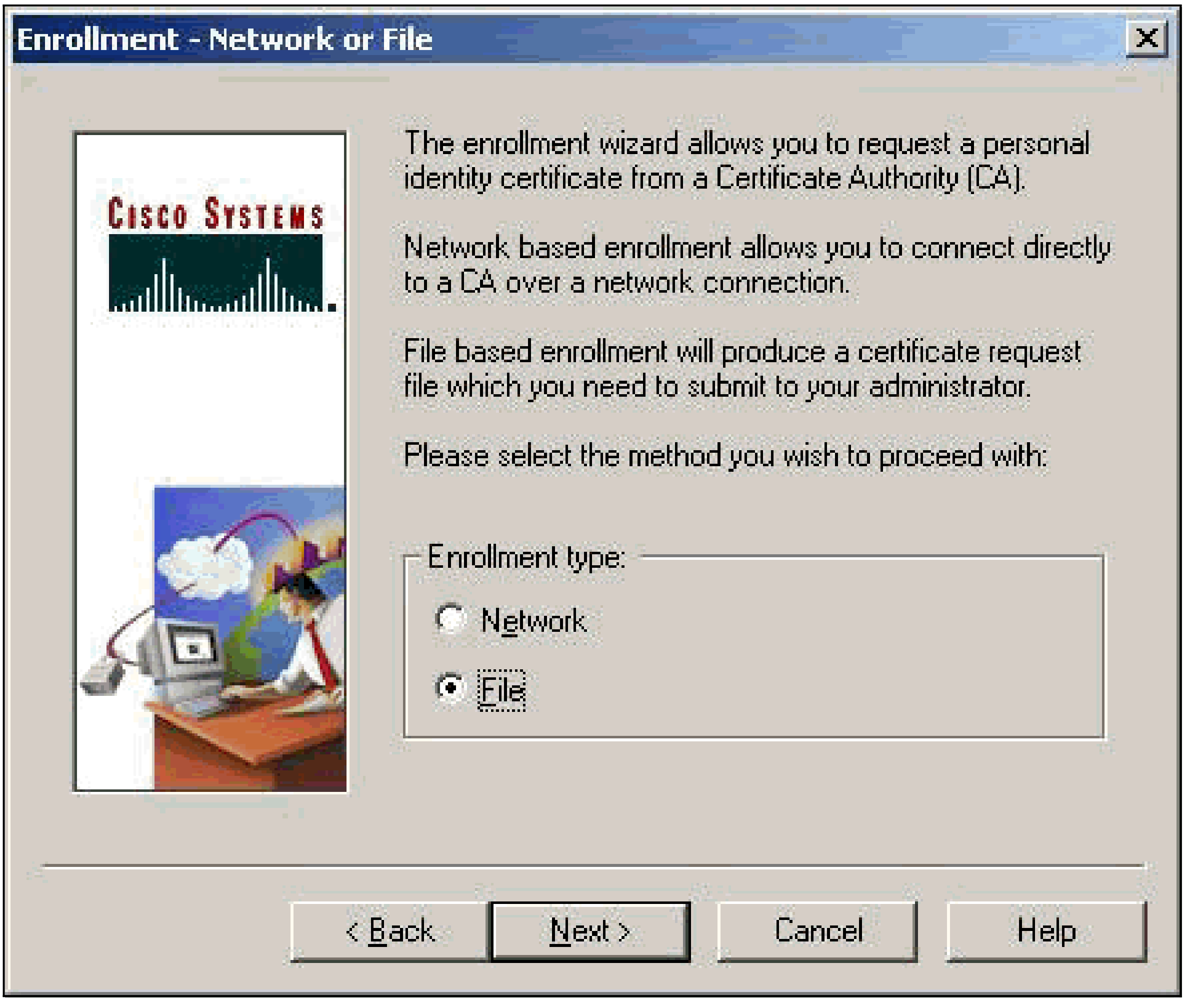
By choosing to protect your certificate with a password, any operation that requires access to the certificate's private key will require the specified password to continue.

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

Password:

Confirmation Password:

4. Selecione **File** para solicitar um certificado usando o formato PKCS #10 na página Enrollment. Em seguida, clique em



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:

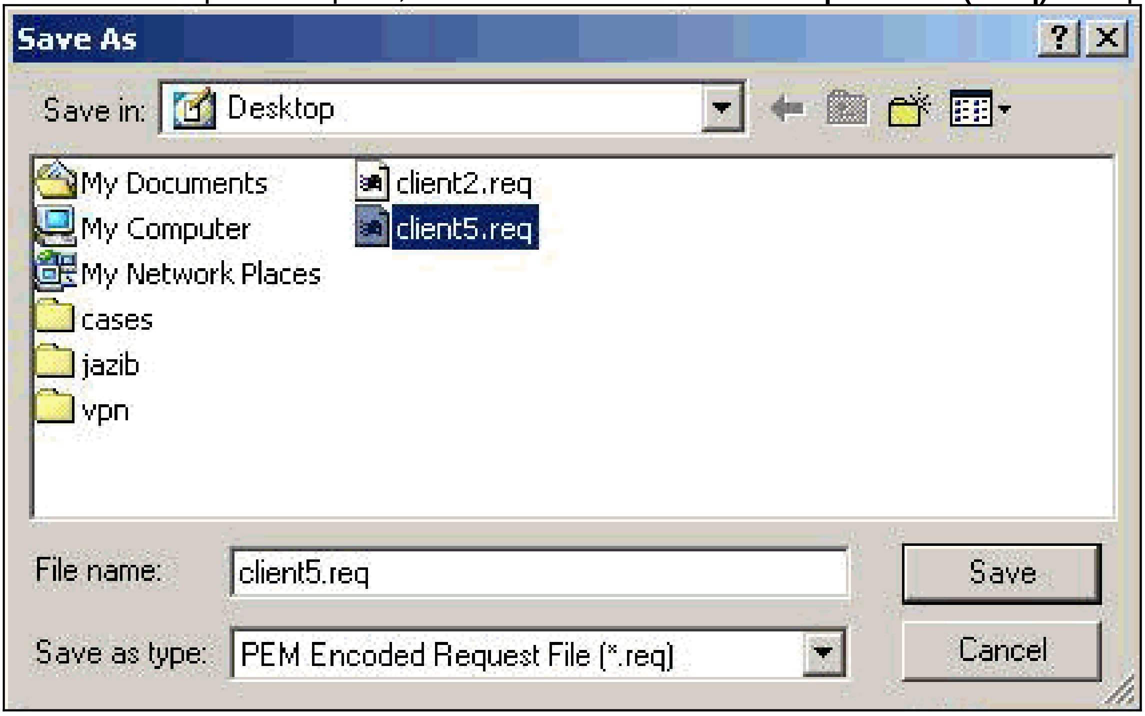
Enrollment type:

○ Network

● File

Avançar.

5. Clique em **Procurar** e especifique um nome de arquivo para o arquivo de solicitação de certificado. Para o tipo de arquivo, selecione **PEM Encoded Request File (*.req)** e clique em



Save As

Save in: Desktop

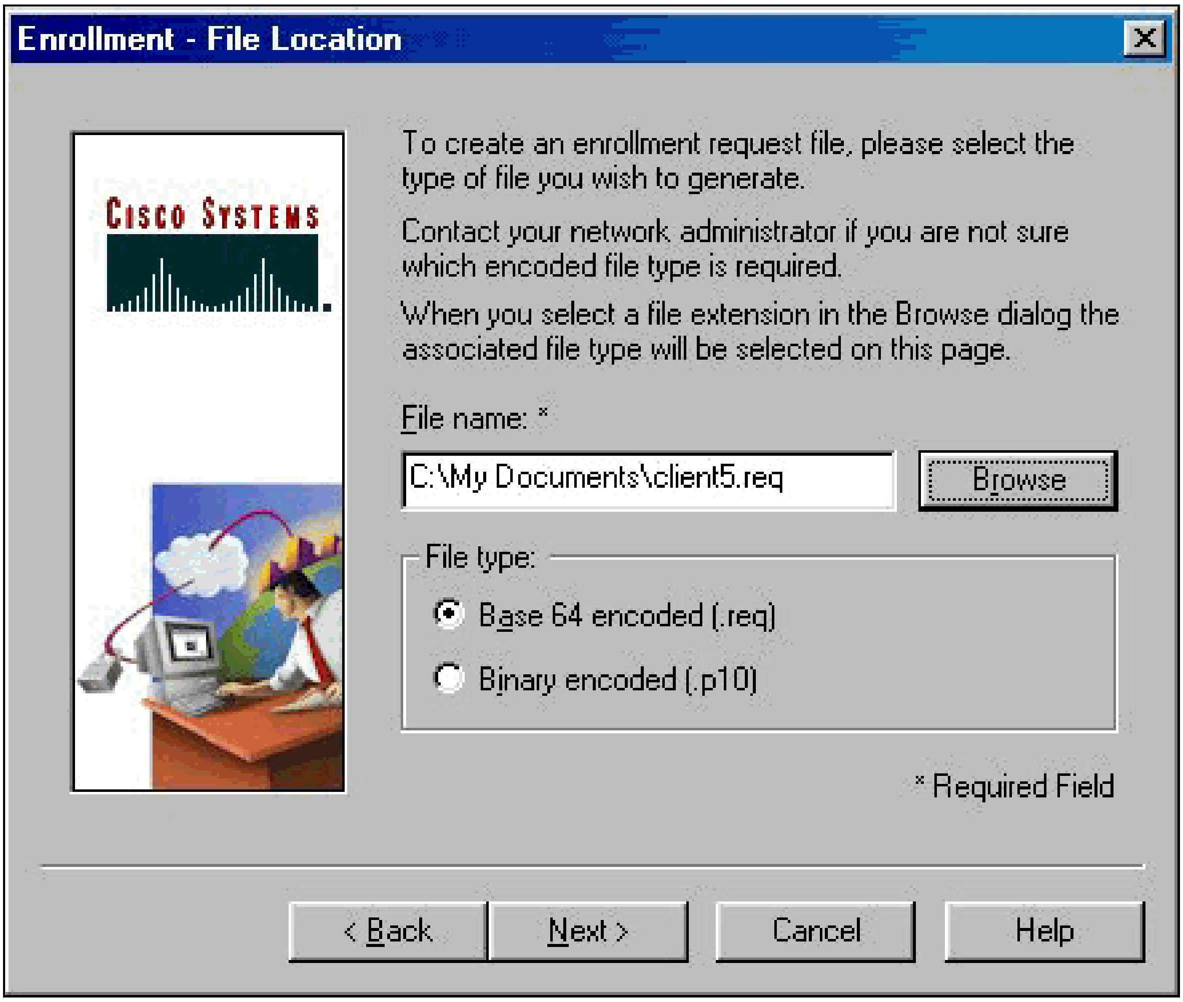
My Documents
My Computer
My Network Places
cases
jazib
vpn
client2.req
client5.req

File name: client5.req

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

Save.

6. Clique em **Next** na página VPN Client Enrollment.



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

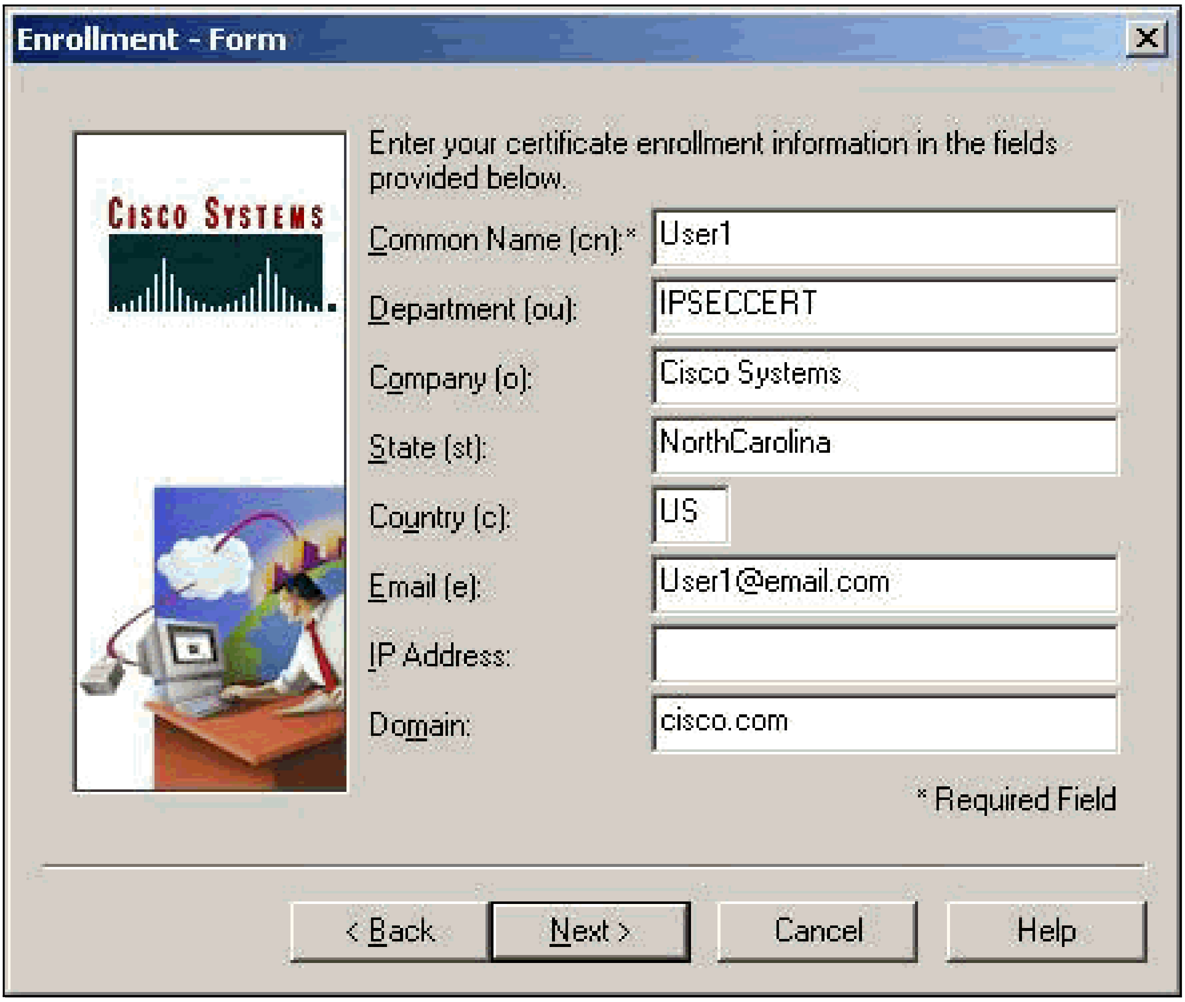
File type:

● Base 64 encoded (.req)

○ Binary encoded (.p10)

* Required Field

7. Preencha os campos no Formulário de inscrição.Este exemplo mostra os campos:Nome Comum = Usuário1Departamento = IPSECCERT (Deve corresponder à unidade organizacional (OU) e ao nome do grupo no VPN 3000 Concentrator.)Empresa = Cisco SystemsEstado = Carolina do NortePaís = EUAE-mail = User1@email.comEndereço IP = (opcional; usado para especificar o endereço IP na solicitação do certificado)Domain=cisco.comClique em **Avançar** quando



Enrollment - Form

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

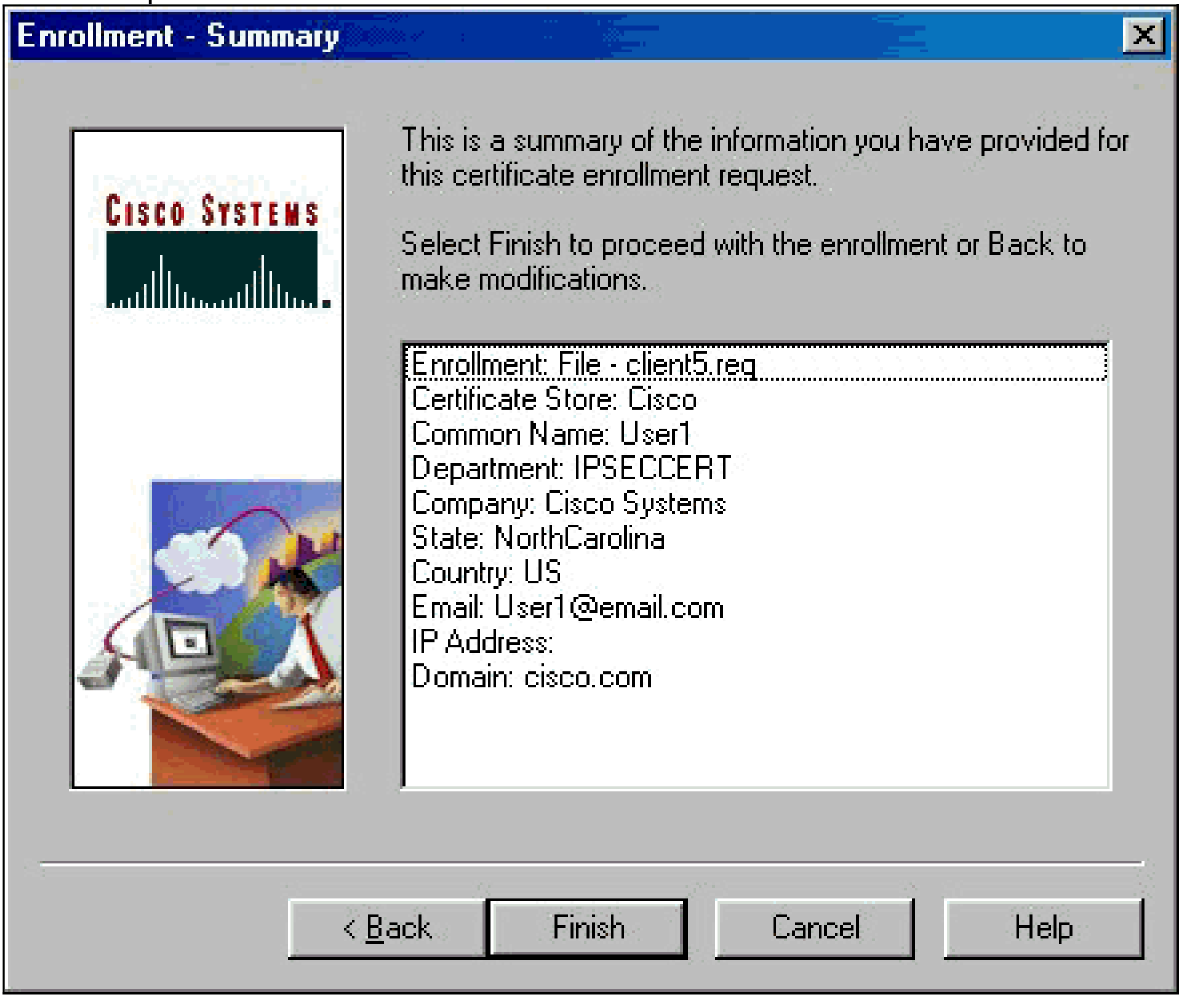
IP Address:

Domain: cisco.com

* Required Field

terminar.

8. Clique em **Concluir** para continuar a inscrição.



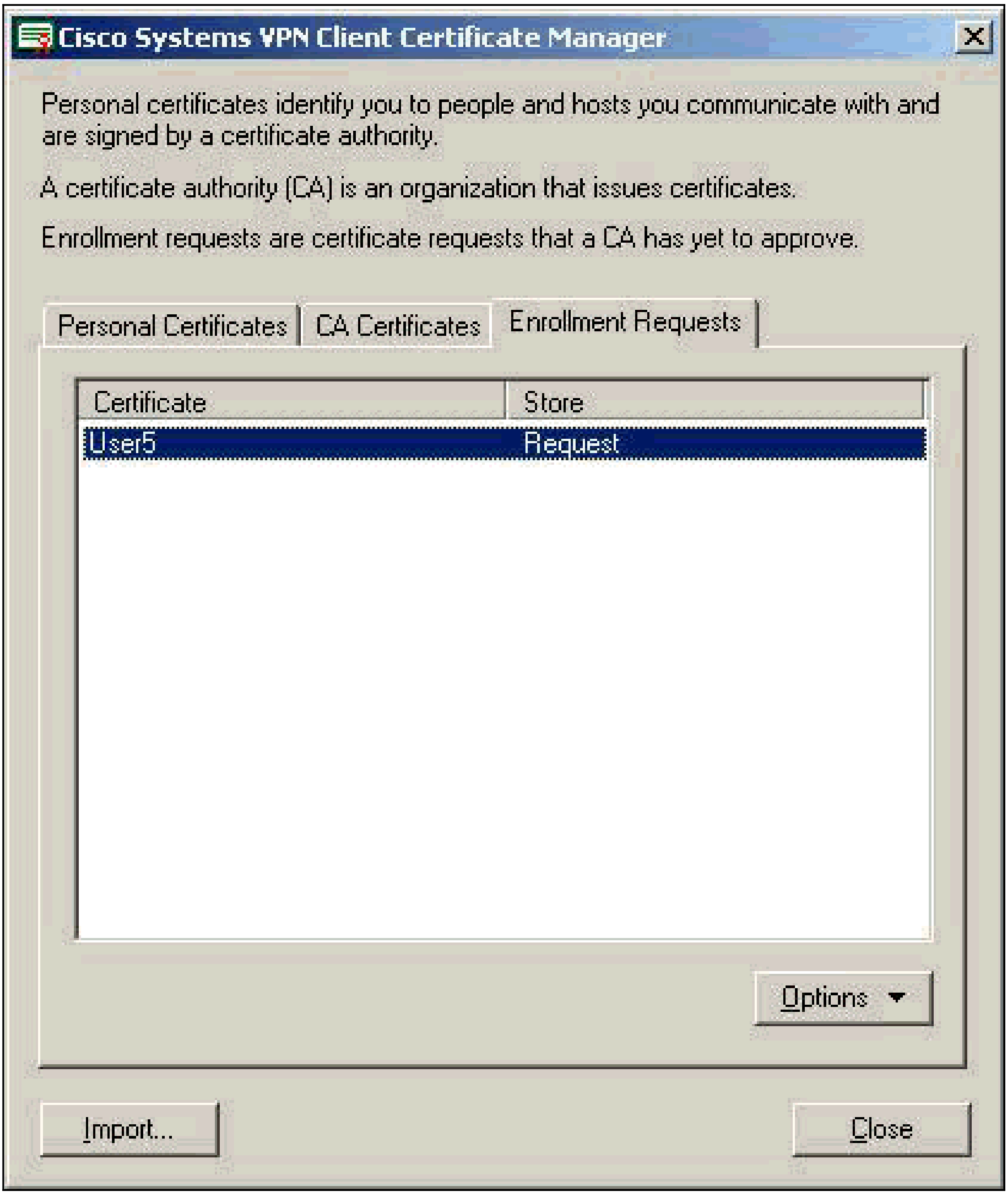
Enrollment - Summary

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. Selecione a guia Solicitações de inscrição para verificar a solicitação no Gerenciador de certificados do cliente VPN.



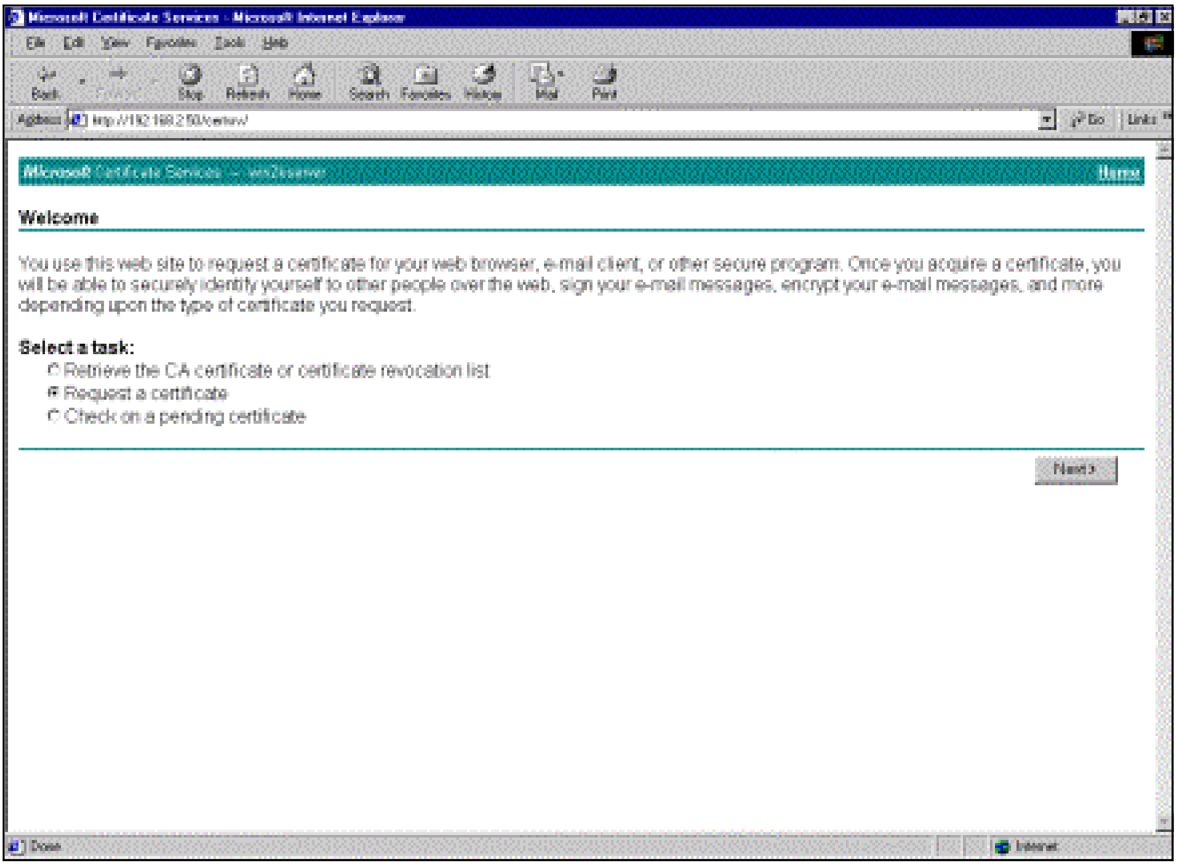
Personal certificates identify you to people and hosts you communicate with and are signed by a certificate authority.

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. Ative o servidor da Autoridade de Certificação (CA) e as interfaces do VPN Client simultaneamente para enviar a solicitação.
11. Selecione **Solicitar um certificado** e clique em **Avançar** no servidor


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
Microsoft Certificate Services -- win2kserver
Home
Next >
Done
Internet

Welcome

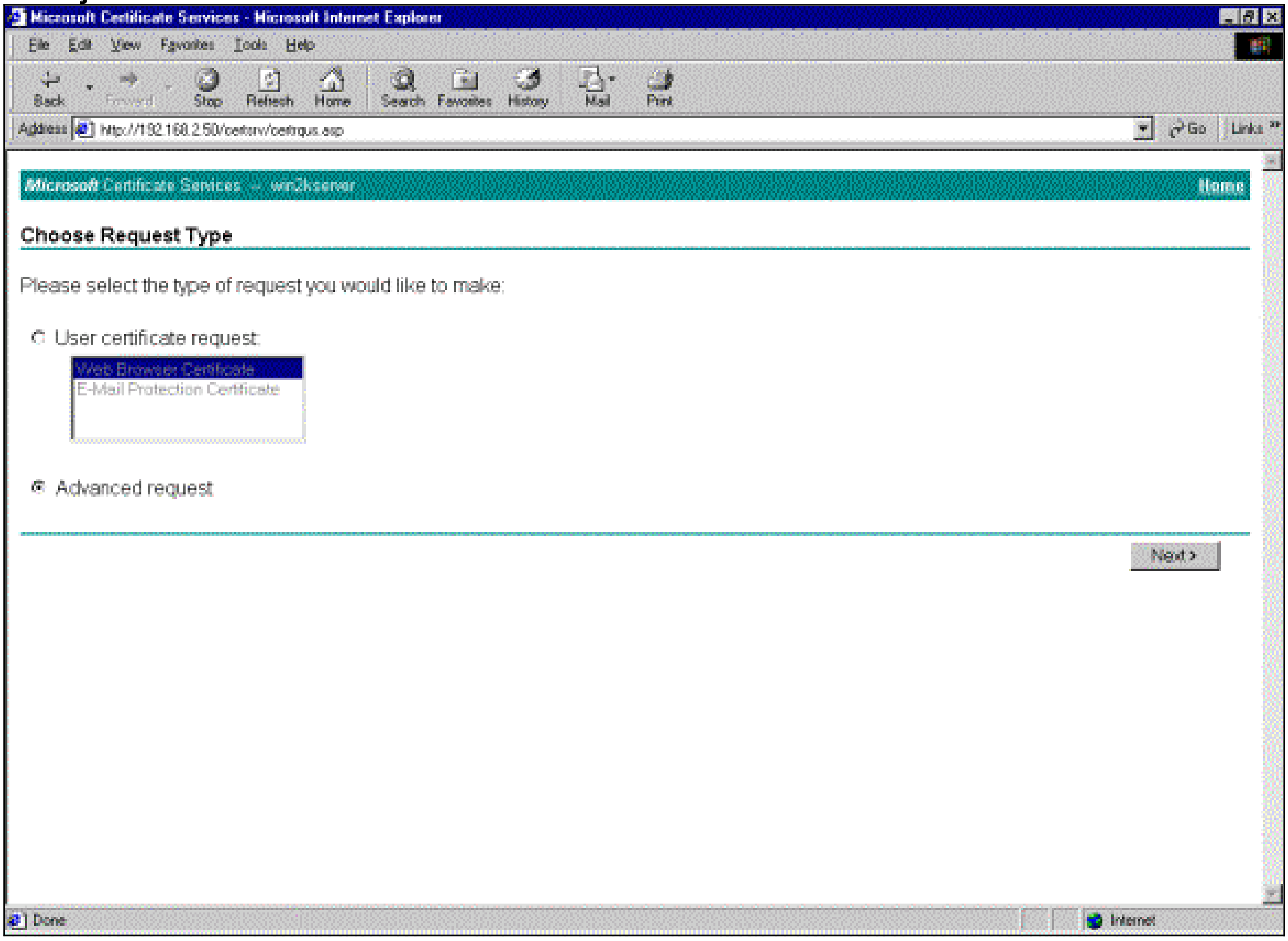
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the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

Select a task:

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

CA.

12. Selecione **Solicitação avançada** para o tipo de solicitação e clique em **Avançar**.


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
Microsoft Certificate Services -- win2kserver
Home
Next >
Done
Internet

Choose Request Type

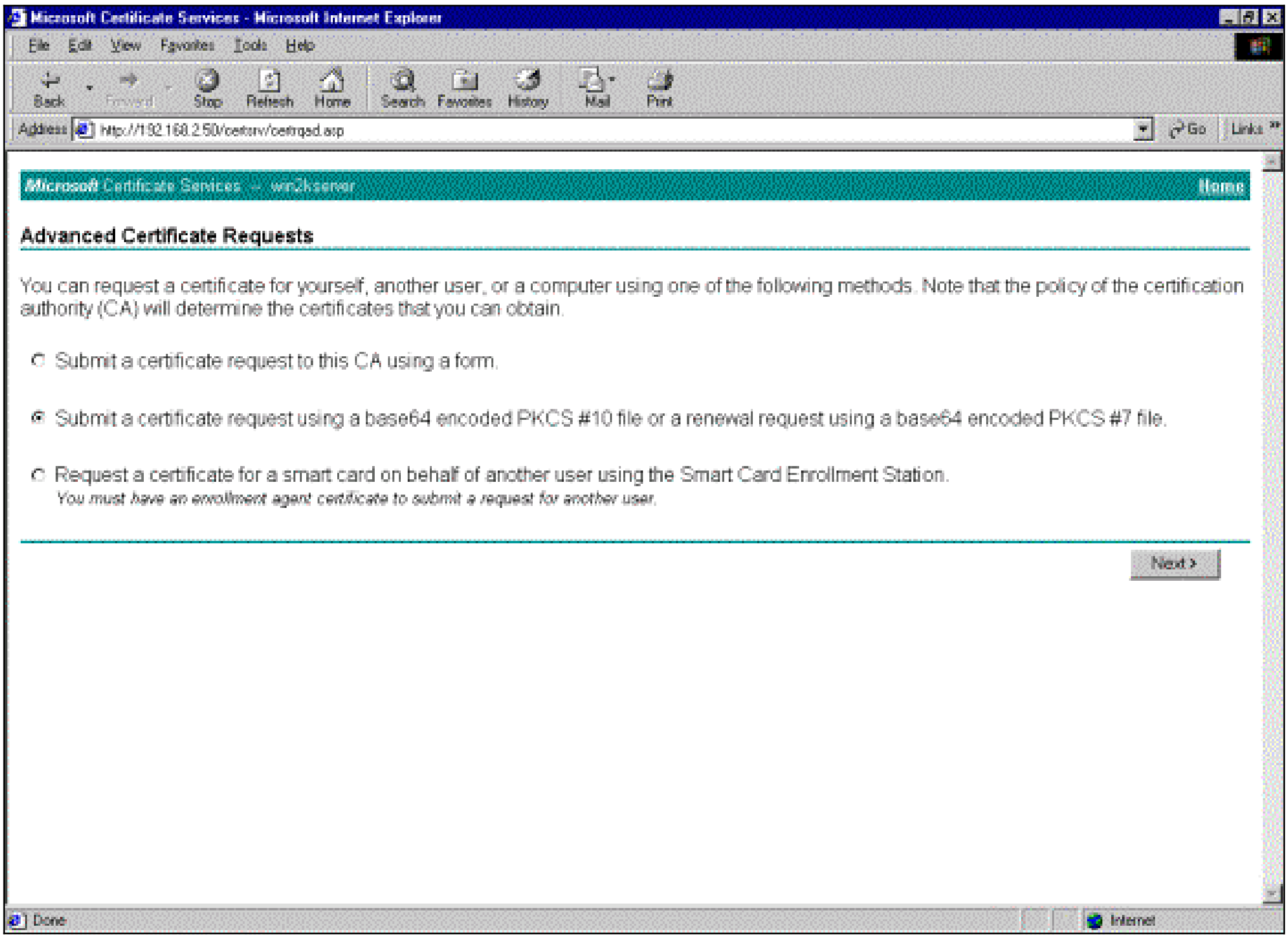
Please select the type of request you would like to make:

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

● Advanced request

13. Selecione **Submit a certificate request using a base64 encoded PKCS #10 file or a renew request using a base64 encoded PKCS #7 file** em Advanced Certificate Requests e clique em

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

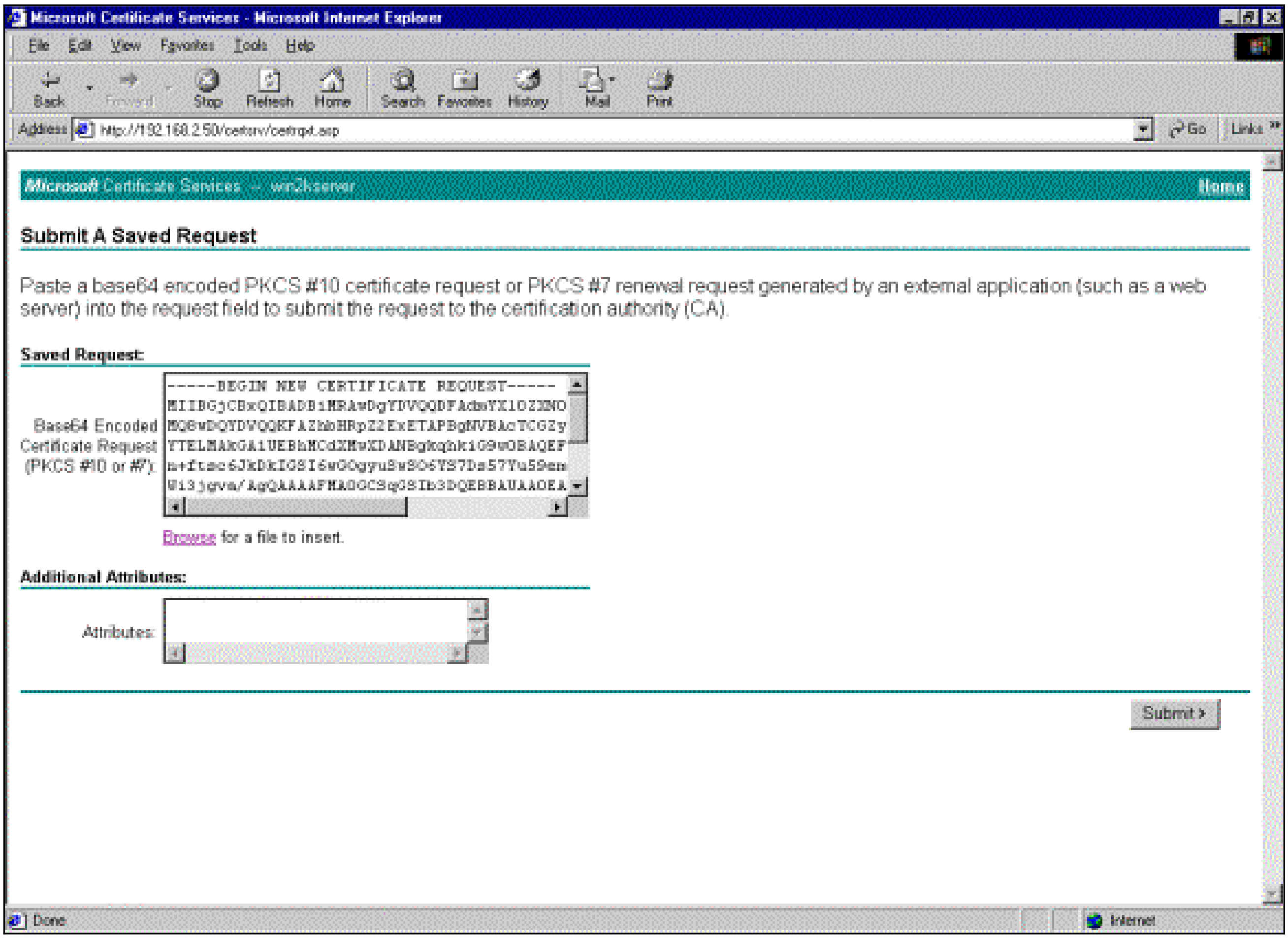
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ 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. Destaque o arquivo de solicitação do VPN Client e cole-o no servidor CA em Solicitação salva. Em seguida, clique em
Enviar.



Microsoft Certificate Services - Microsoft Internet Explorer

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

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-----
MIIBGjCBxQIBADB1MRAwDgYDVQQDFAdmYX1OZXNO
MQ8wDQYDVQQKFAZhbHRpZ2ExETAPBgNVBAcTCGZy
YTELMAkGA1UEBhMCdXMwXDANBgkqhkiG9w0BAQEF
n+ftmc6JkDkIGSI6wGOgyu8wSO6YS7Ds57Yu59en
W13jgva/AgQAAAAFMADGCSqGSIb3DQEBBAUAA0EA
```

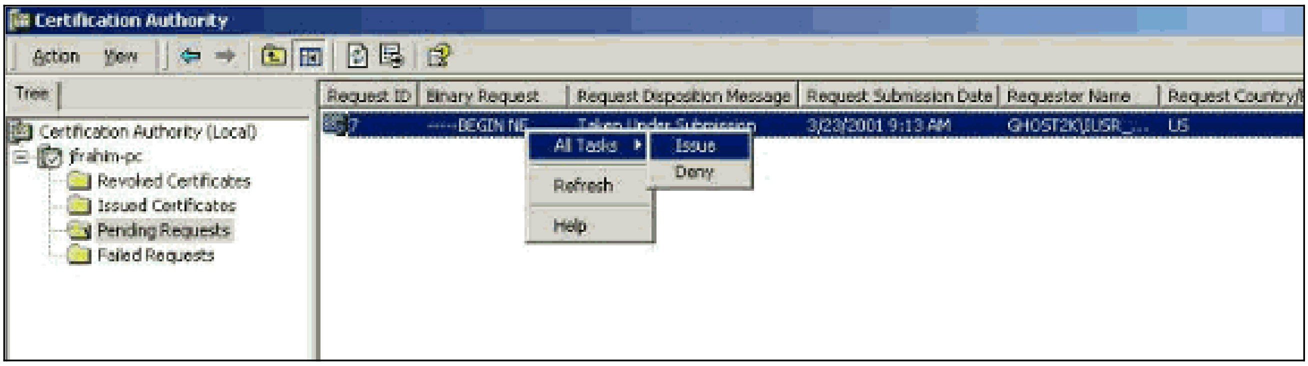
Browse for a file to insert.

Additional Attributes:

Attributes:

Submit >

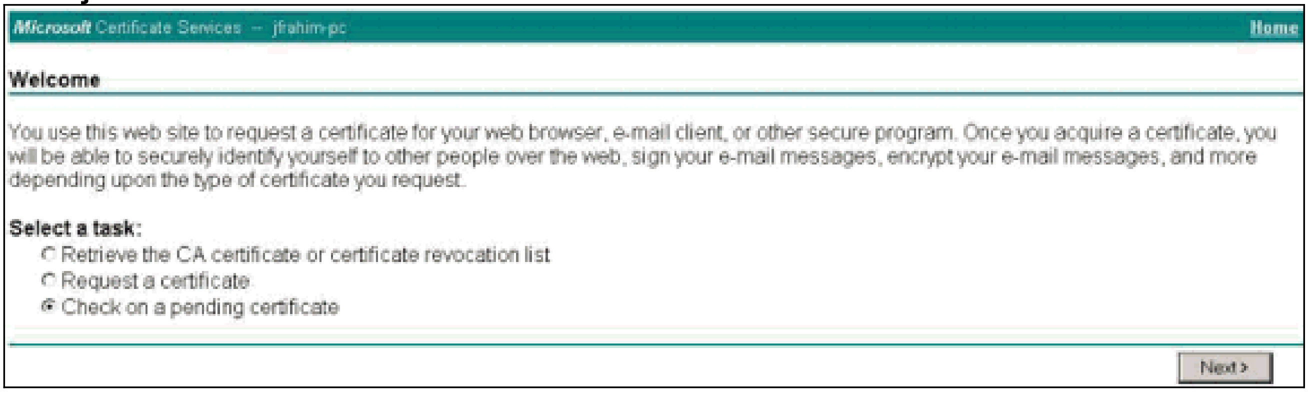
15. No servidor CA, emita o certificado de identidade para a solicitação do VPN Client.



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. Faça o download dos certificados raiz e de identidade para o VPN Client. No servidor CA, selecione **Verificar um certificado pendente** e clique em **Avançar**.



Microsoft Certificate Services -- jfrahim-pc — Home

Welcome

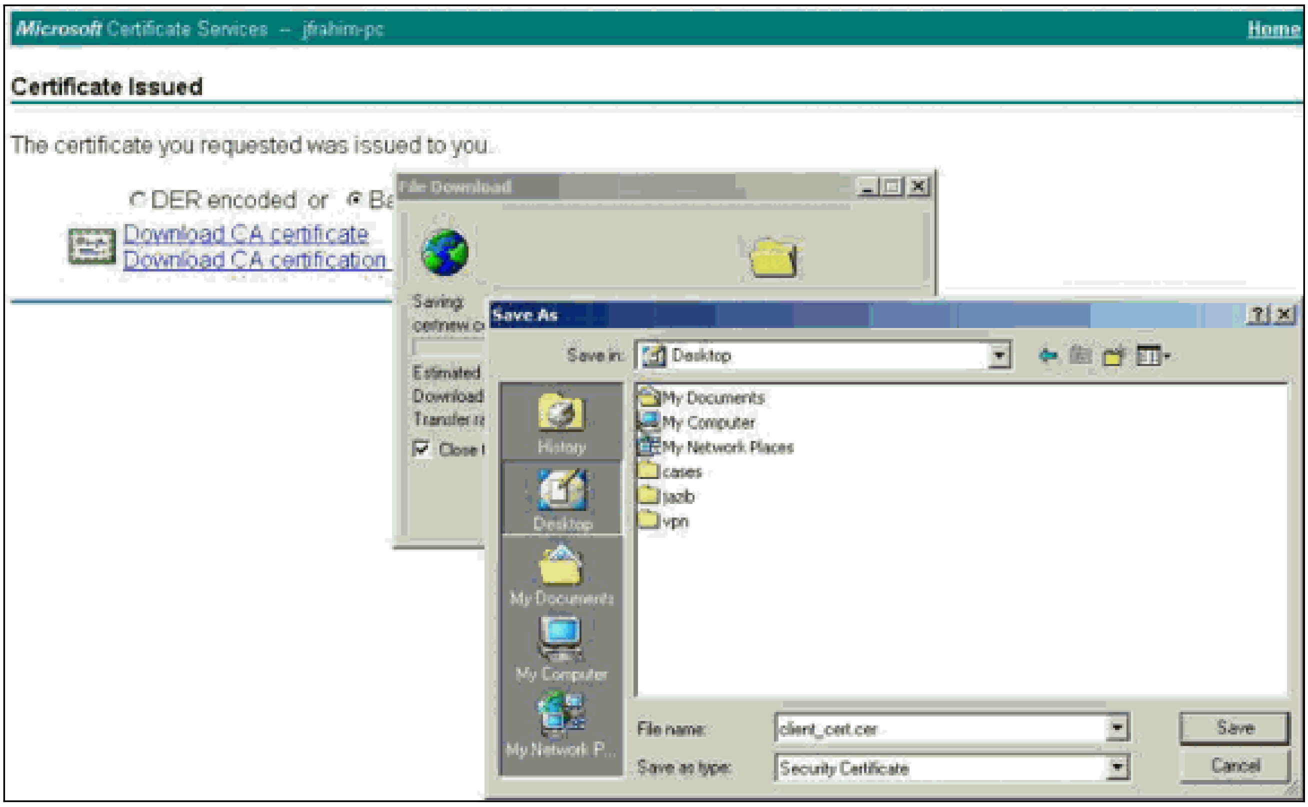
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the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

17. Selecione **Base 64 codificada**. Em seguida, clique em **Transferir certificado CA** no servidor CA.



Microsoft Certificate Services -- jfrahim-pc

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Ba

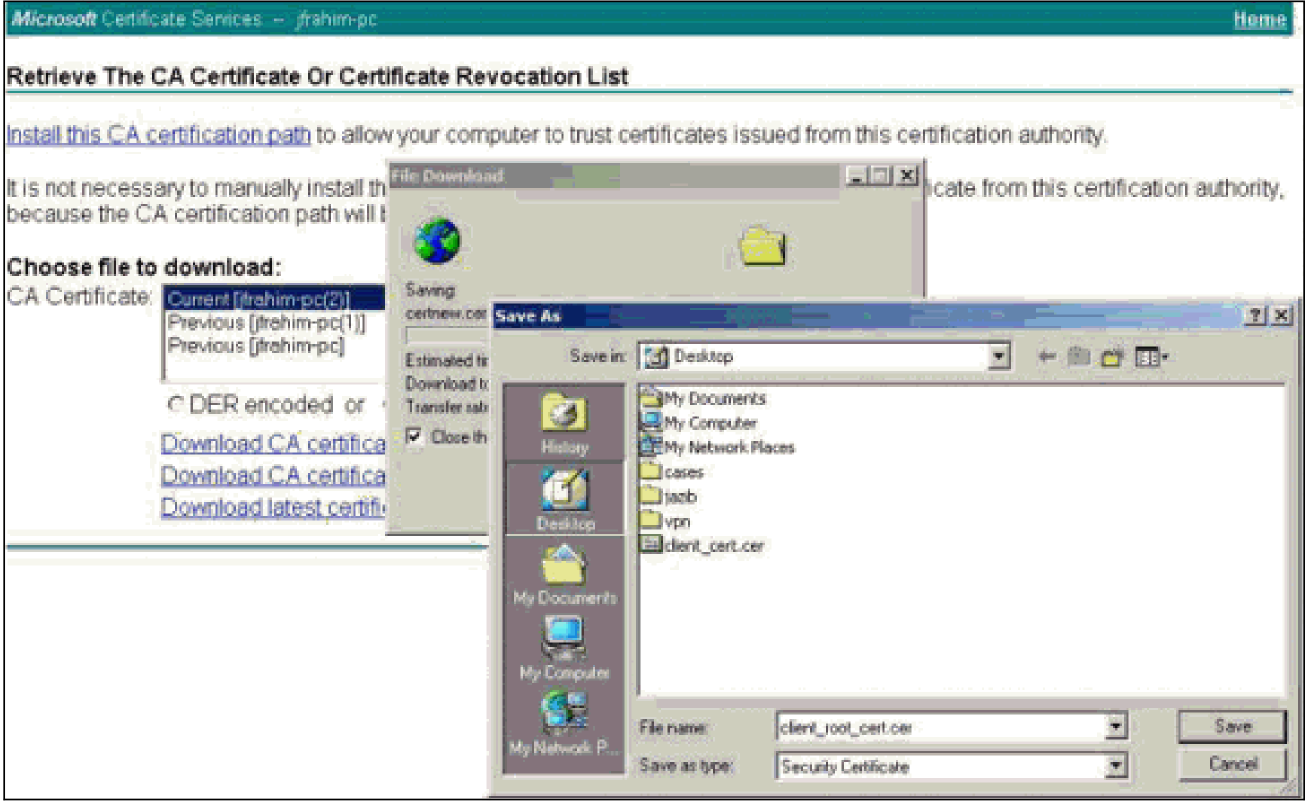
Download CA certificate
Download CA certification

Save in: Desktop

File name: client_cert.cer

Save as type: Security Certificate

18. Selecione um arquivo para baixar na página Recuperar certificado CA ou lista de revogação de certificado para obter o certificado raiz no servidor CA. Em seguida, clique em
Avançar.



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

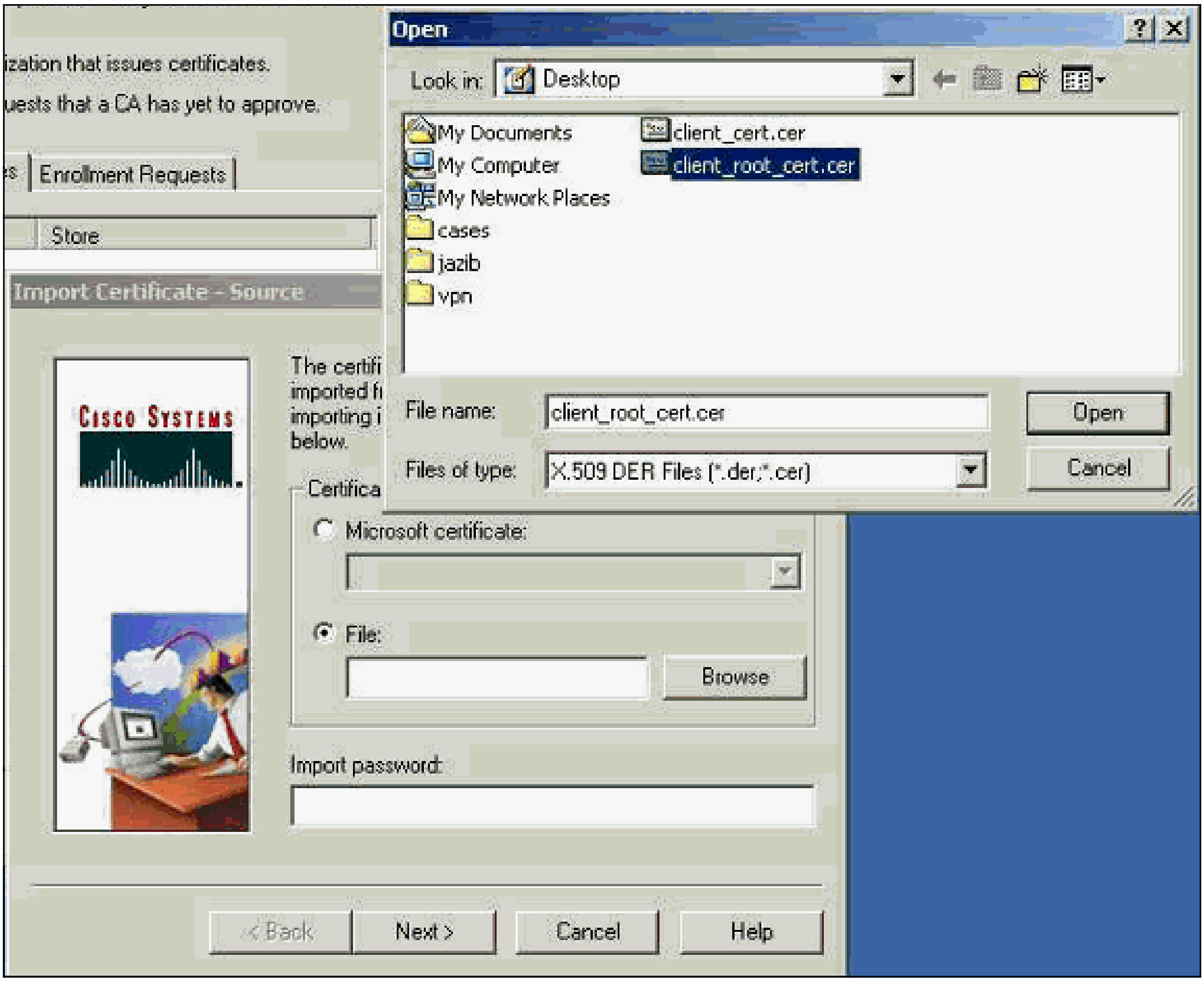
Download CA certifica
Download CA certifica
Download latest certifi

Save in: Desktop

File name: client_root_cert.cer

Save as type: Security Certificate

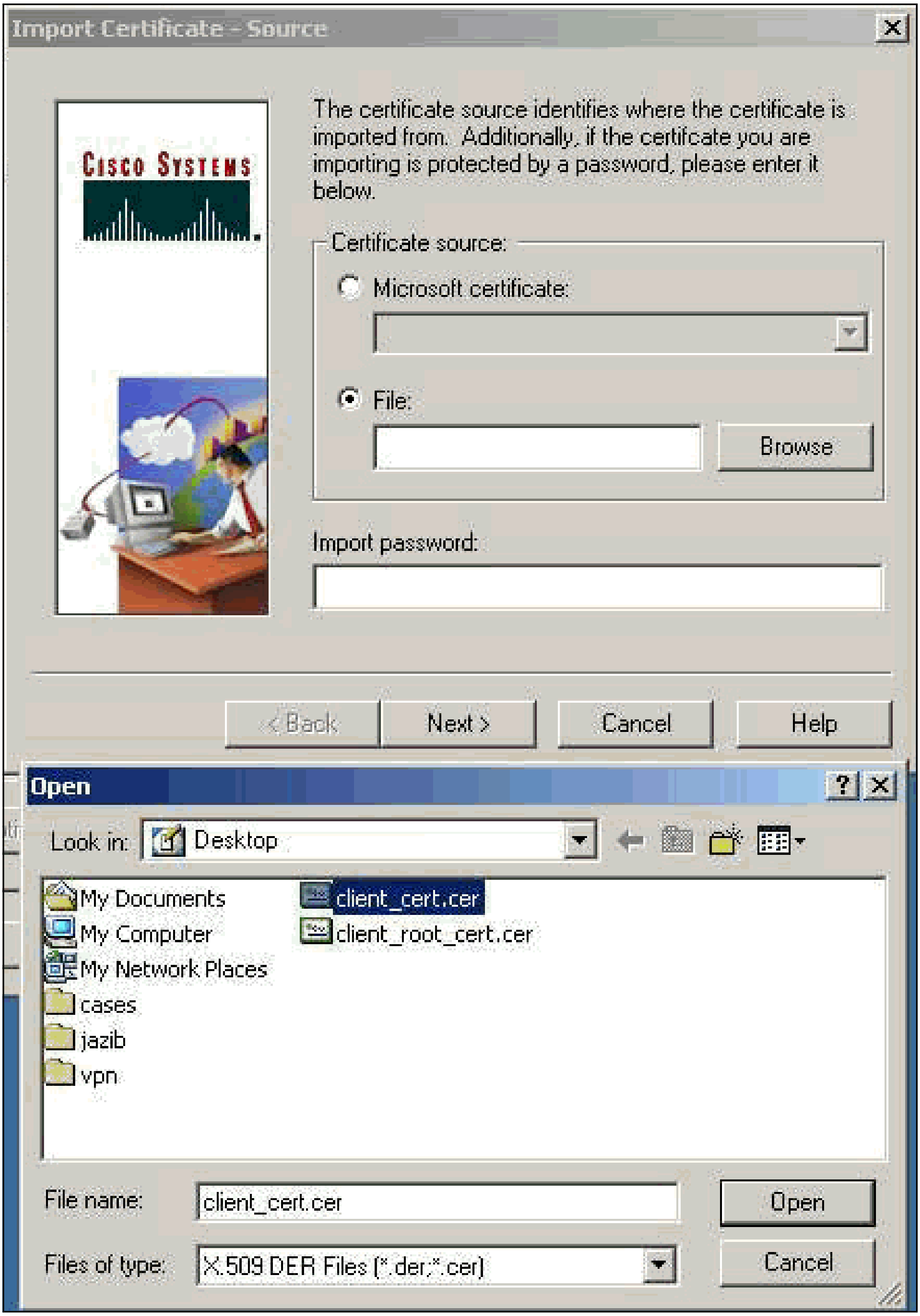
19. Selecione **Certificate Manager** > **CA Certificate** > **Import on the VPN Client** e, em seguida, selecione o arquivo CA raiz para instalar a raiz e os certificados de
identidade.



File name: client_root_cert.cer

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

20. Selecione **Gerenciador de Certificados** > **Certificados Pessoais** > **Importar** e escolha o arquivo de certificado de identidade.



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

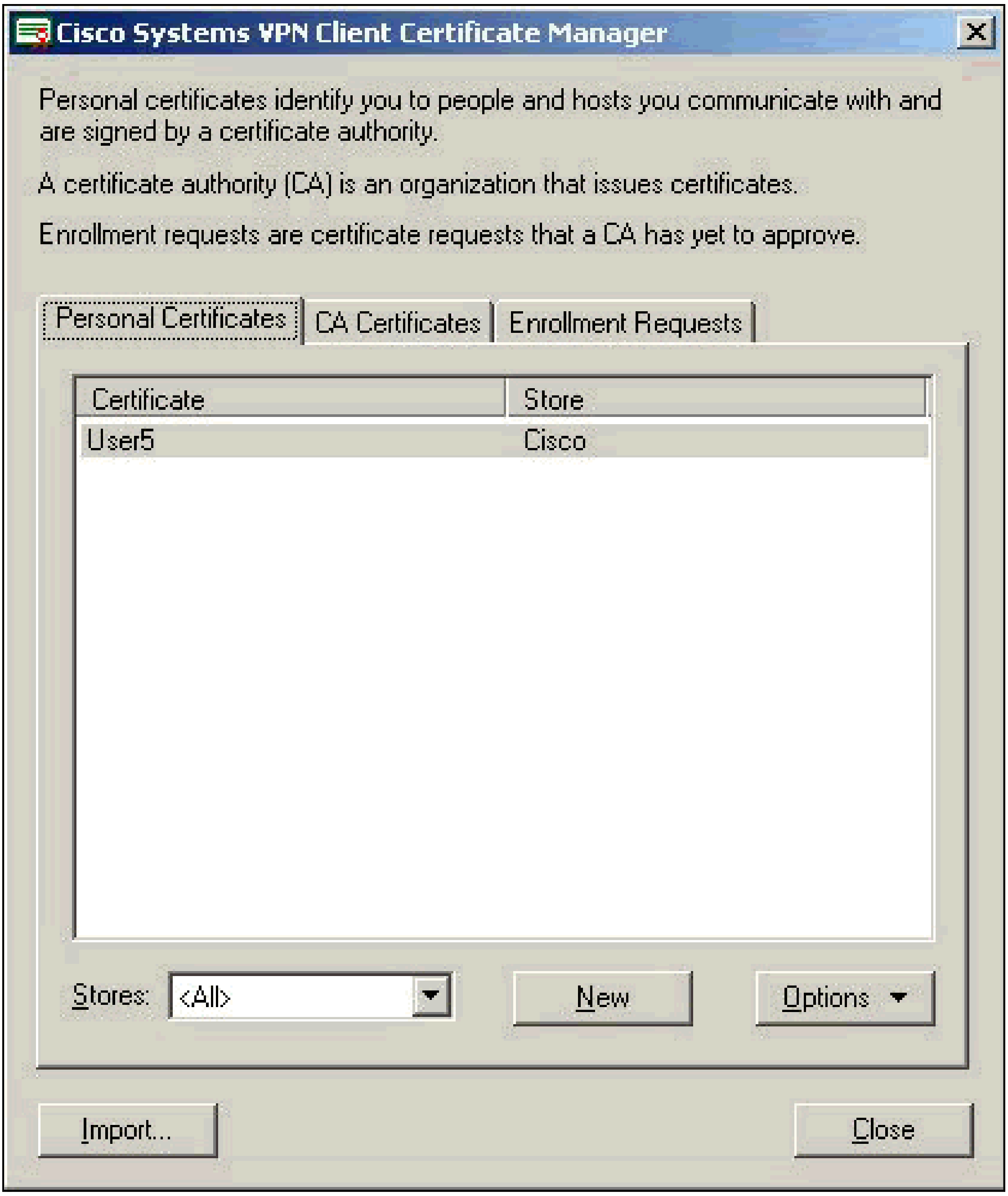
Look in: Desktop

File name: client_cert.cer

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

21. Certifique-se de que o certificado de identidade aparece na guia Certificados

pessoais.



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.

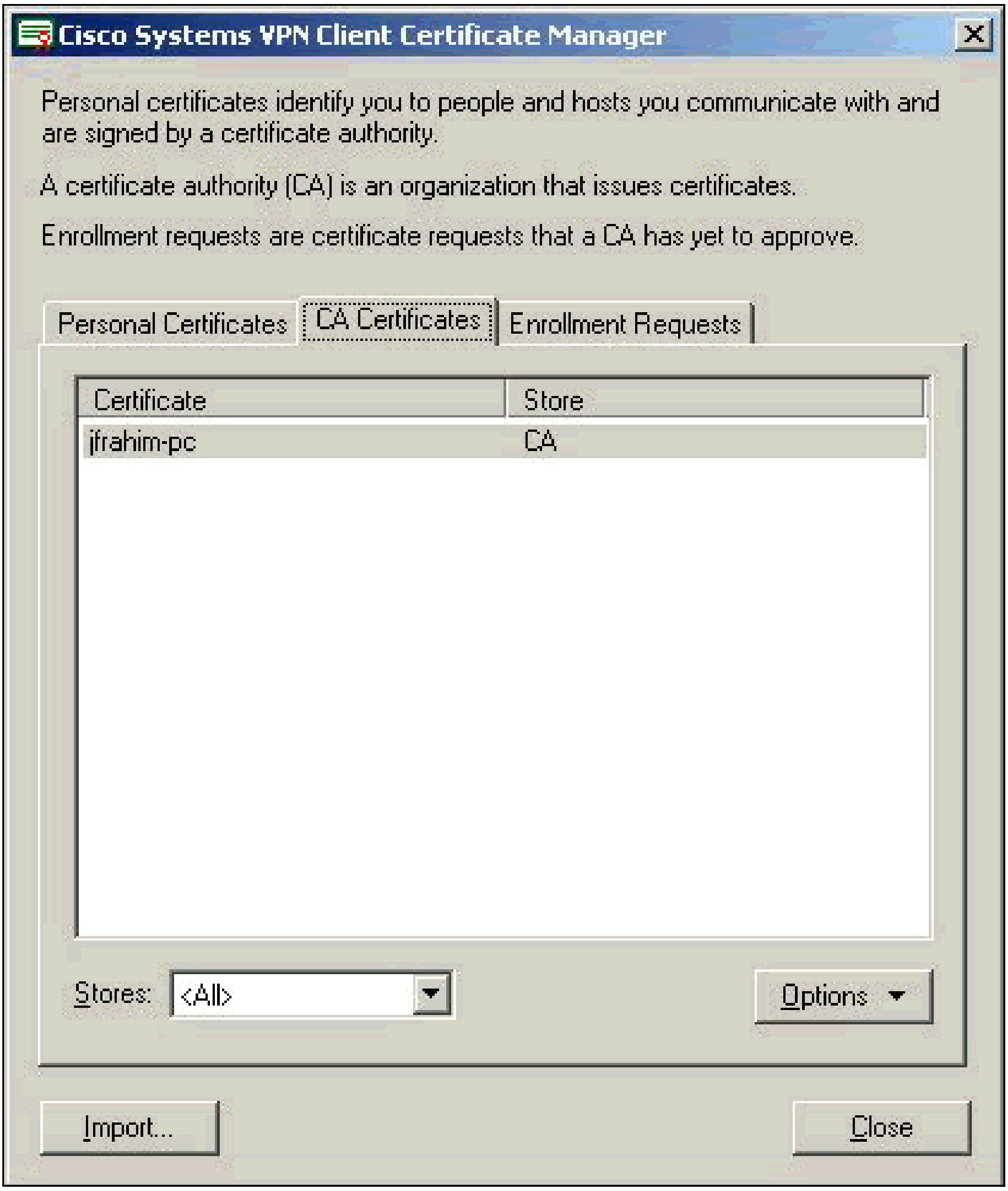
Enrollment requests are certificate requests that a CA has yet to approve.

Certificate	Store
User5	Cisco

Stores: <All>

22. Verifique se o certificado raiz é exibido na guia Certificados

CA.



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
jfrahim-pc	CA

Stores: <All>

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Quando você tenta se inscrever no Microsoft CA Server, ele pode gerar esta mensagem de erro.

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

Se você receber essa mensagem de erro, consulte os registros do Microsoft CA para obter detalhes ou consulte esses recursos para obter mais informações.

- O Windows não consegue localizar uma autoridade de certificado que processa a solicitação
- XCCC: A mensagem de erro "Sua solicitação de certificado foi negada" ocorre quando você solicita um certificado para conferências seguras

Informações Relacionadas

- **Negociação IPsec/Protocolos IKE**
- **Suporte Técnico e Documentação - Cisco Systems**