

# 配置VPN client 3.x获得数字证书

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置 VPN 客户端](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文档演示如何配置Cisco VPN Client 3.x以获取数字证书。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于运行Cisco VPN Client 3.x的PC。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

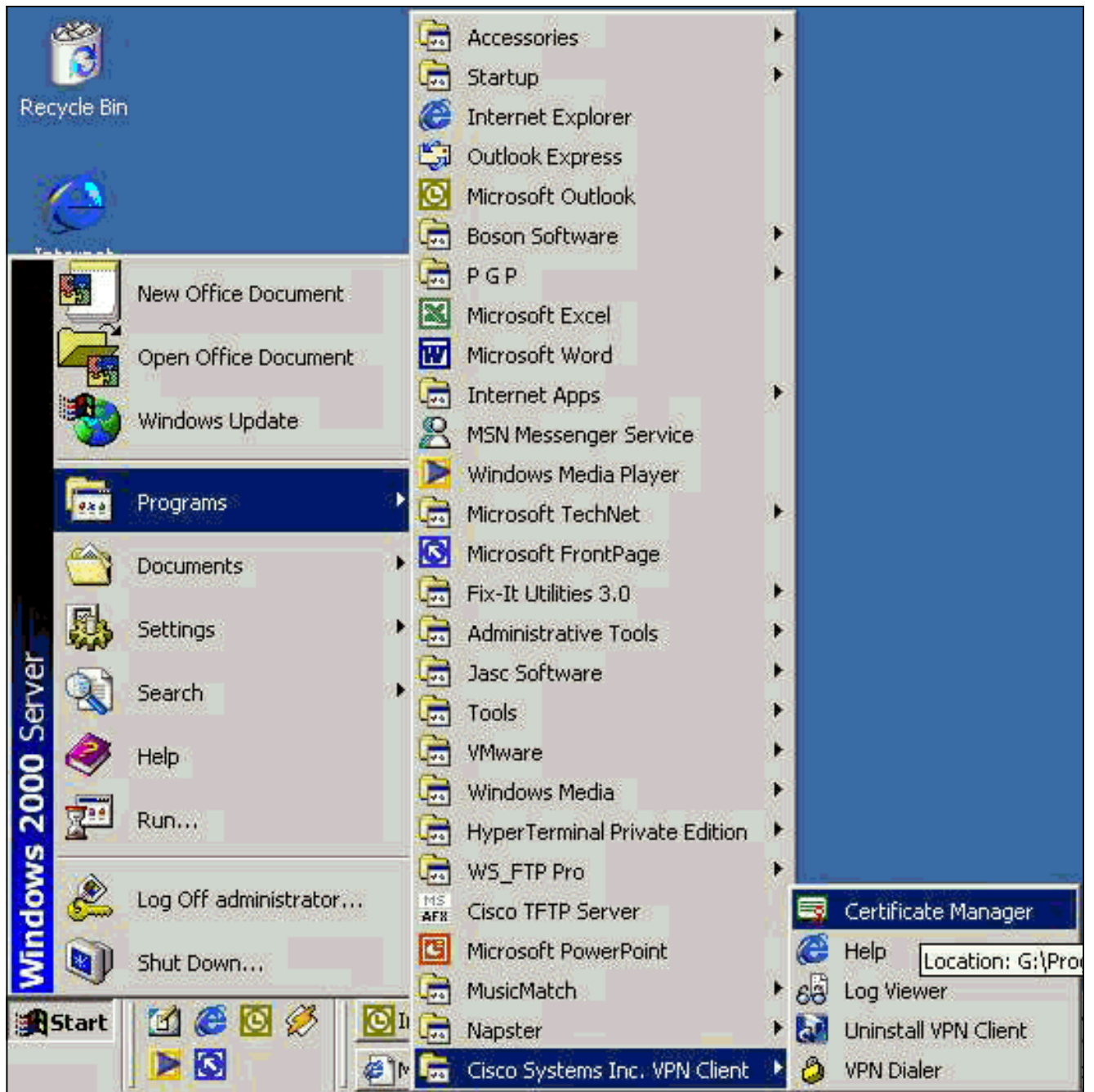
### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

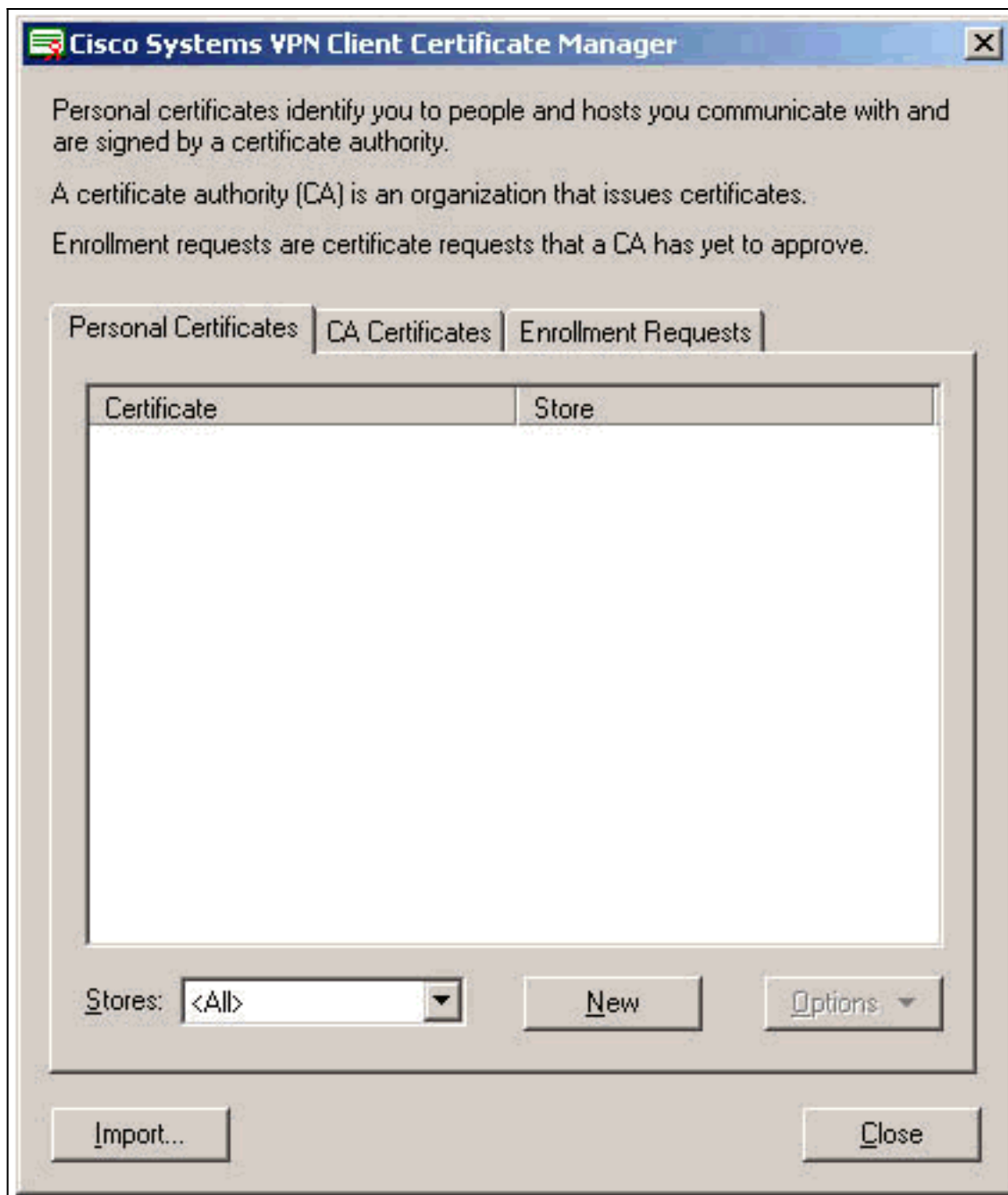
## 配置 VPN 客户端

要配置 VPN 客户端，请完成以下步骤。

1. 选择**Start > Programs > Cisco Systems Inc. VPN client > Certificate Manager**以启动VPN Client Certificate Manager。



2. 选择“个人证书”选项卡，然后单击“新建”。



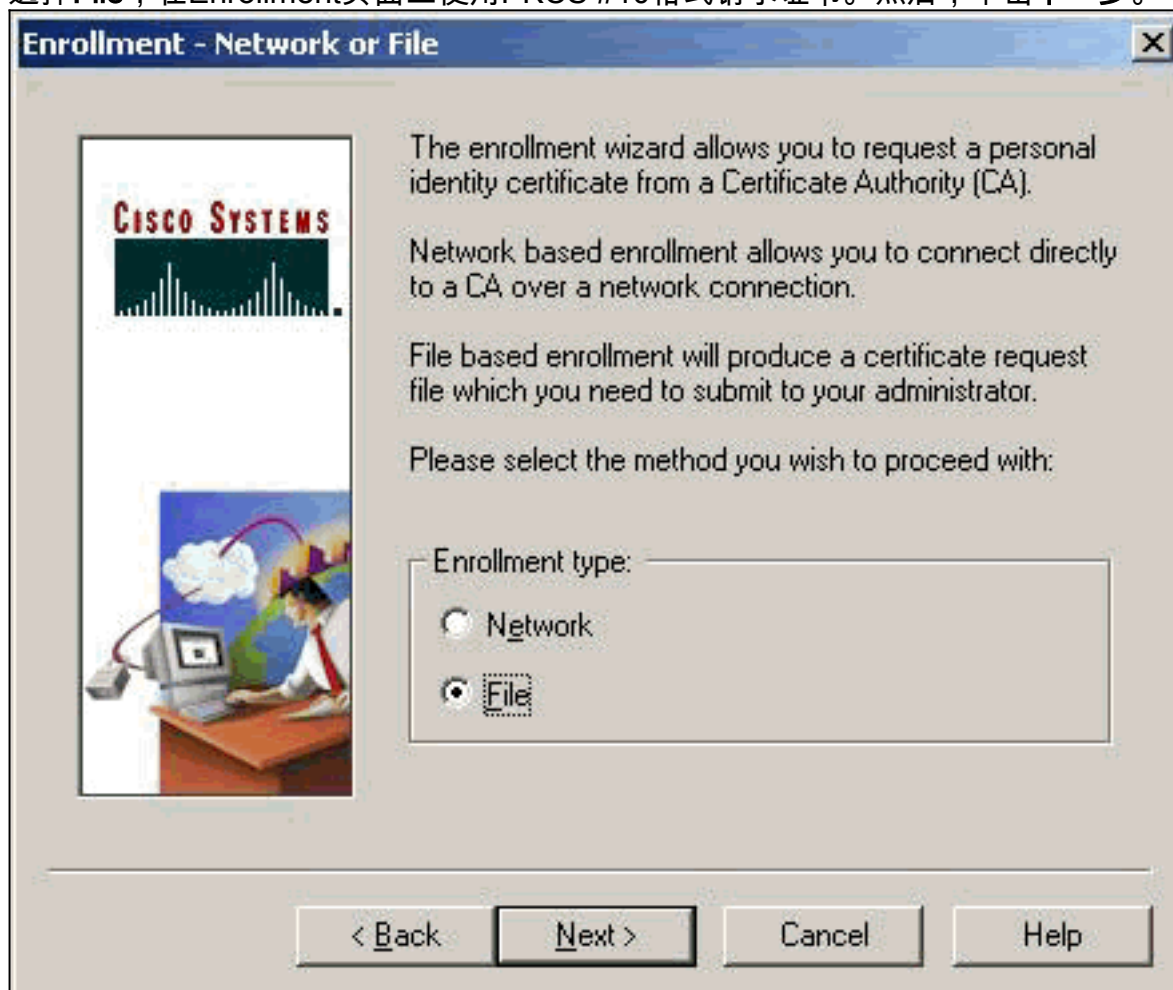
注意

: IPsec无法完成对用户进行VPN连接身份验证的计算机证书。

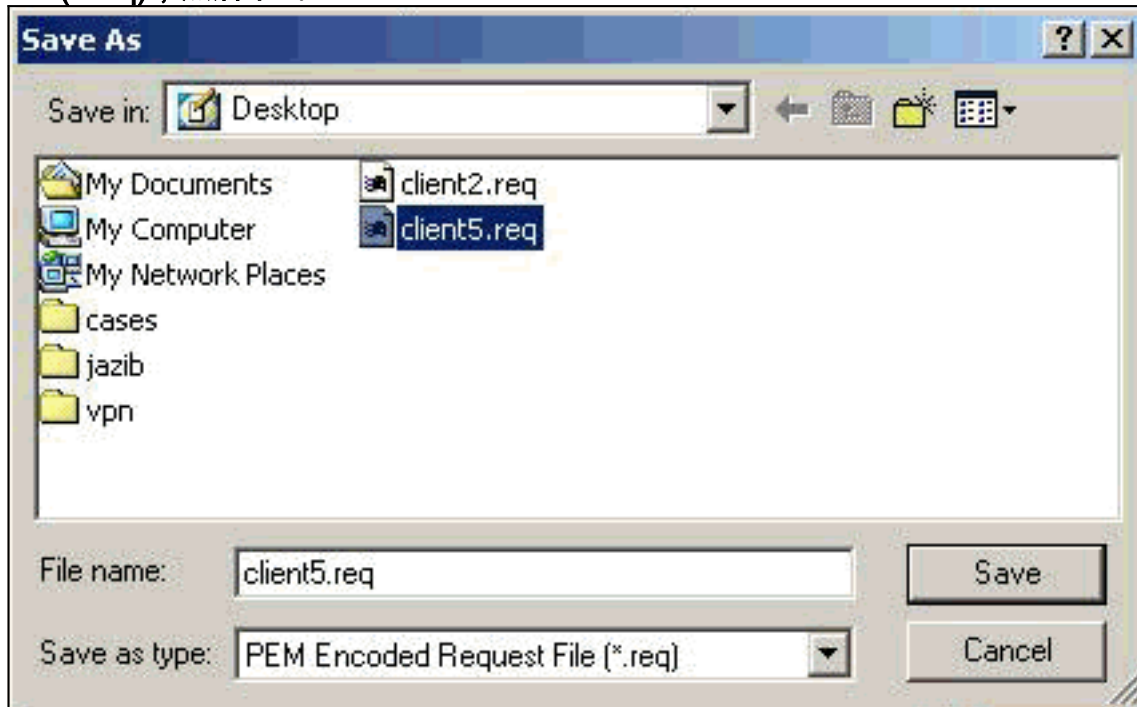
3. 当VPN客户端提示您输入密码时，请指定密码以保护证书。任何需要访问证书私钥的操作都需要指定的密码才能继续。



4. 选择**File**，在Enrollment页面上使用PKCS #10格式请求证书。然后，单击**下一步**。



5. 单击**Browse**，然后为证书请求文件指定文件名。对于文件类型，选择**PEM Encoded Request File(\*.req)**，然后单击“**Save**”。



6. 在VPN Client Enrollment页面上单击**Next**。





7. 填写登记表上的字段。此示例显示字段：公用名=用户1部门= IPSECCERT(这应与VPN 3000集中器上的组织单位(OU)和组名称匹配。)公司=思科系统州=北卡罗来纳州国家/地区=美国电邮= User1@email.com IP地址=(可选；用于指定证书请求的IP地址)域= cisco.com完成后单击“下一步”。



**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



< Back Next > Cancel Help

8. 单击Finish继续注册。

**Enrollment - Summary**

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

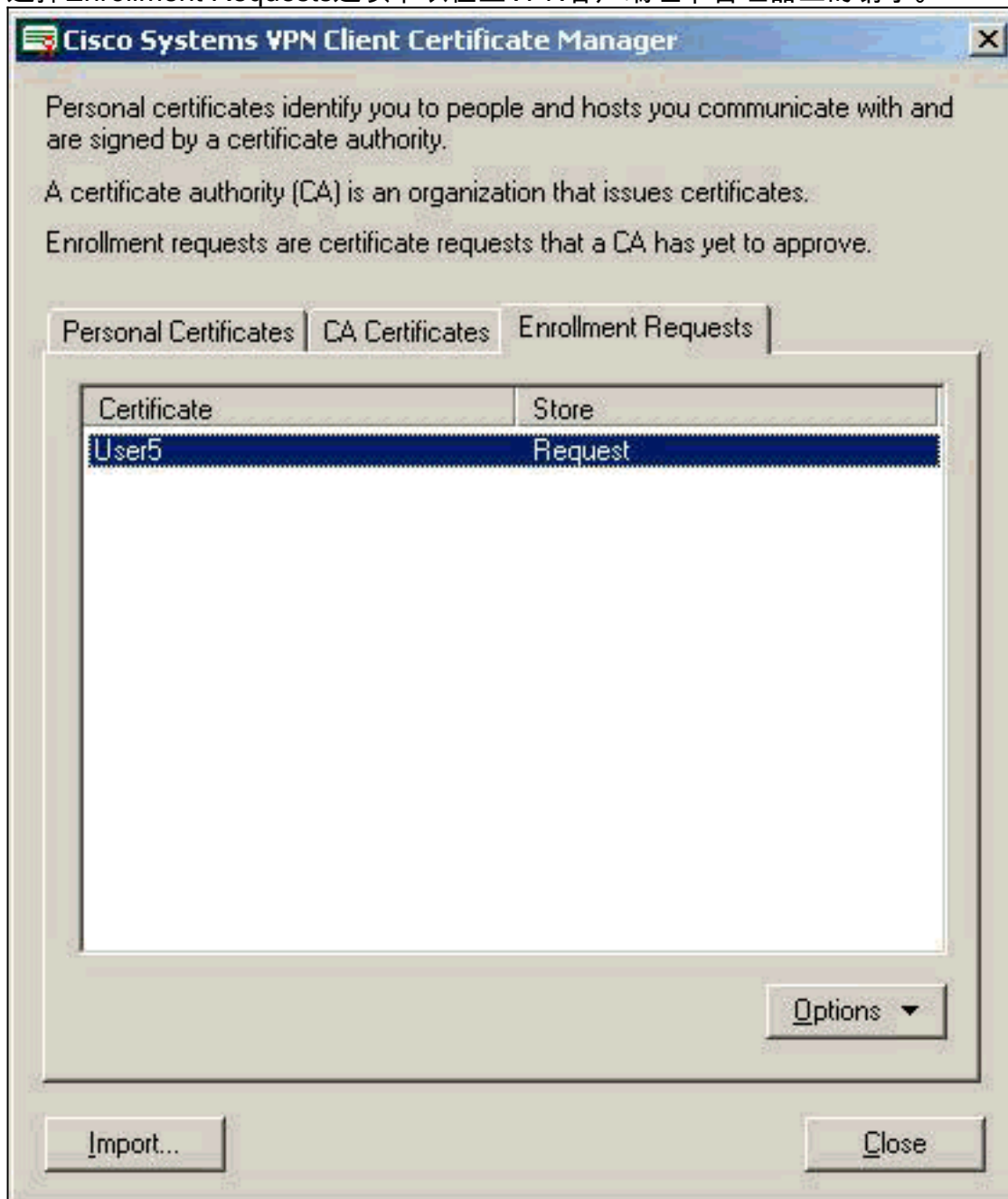
Select Finish to proceed with the enrollment or Back to make modifications.

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

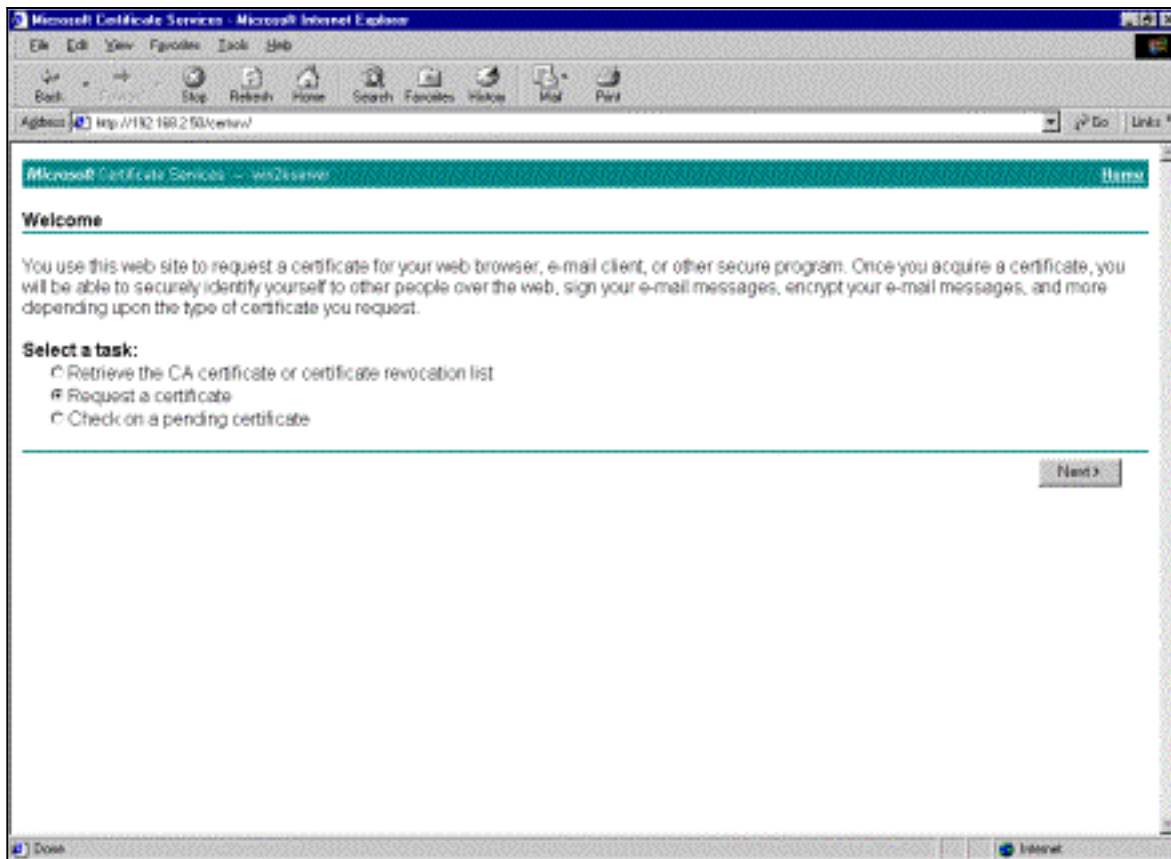
< Back Finish Cancel Help

9. 选择Enrollment Requests选项卡以检查VPN客户端证书管理器上的请求。

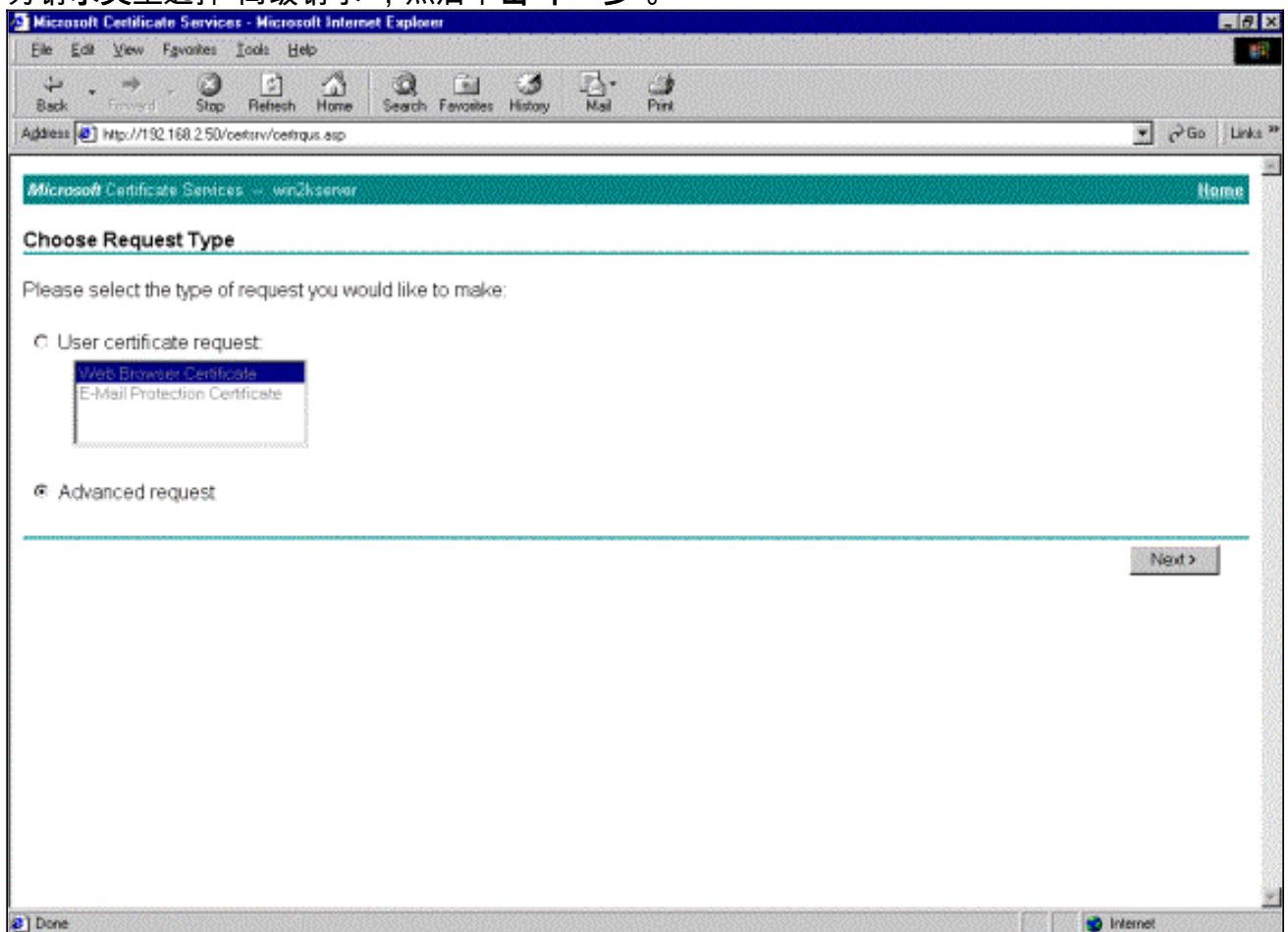


10. 同时启动证书颁发机构(CA)服务器和VPN客户端接口以提交请求。

11. 选择Request a certificate(请求证书), 然后单击CA服务器上的Next ( 下一步 )。

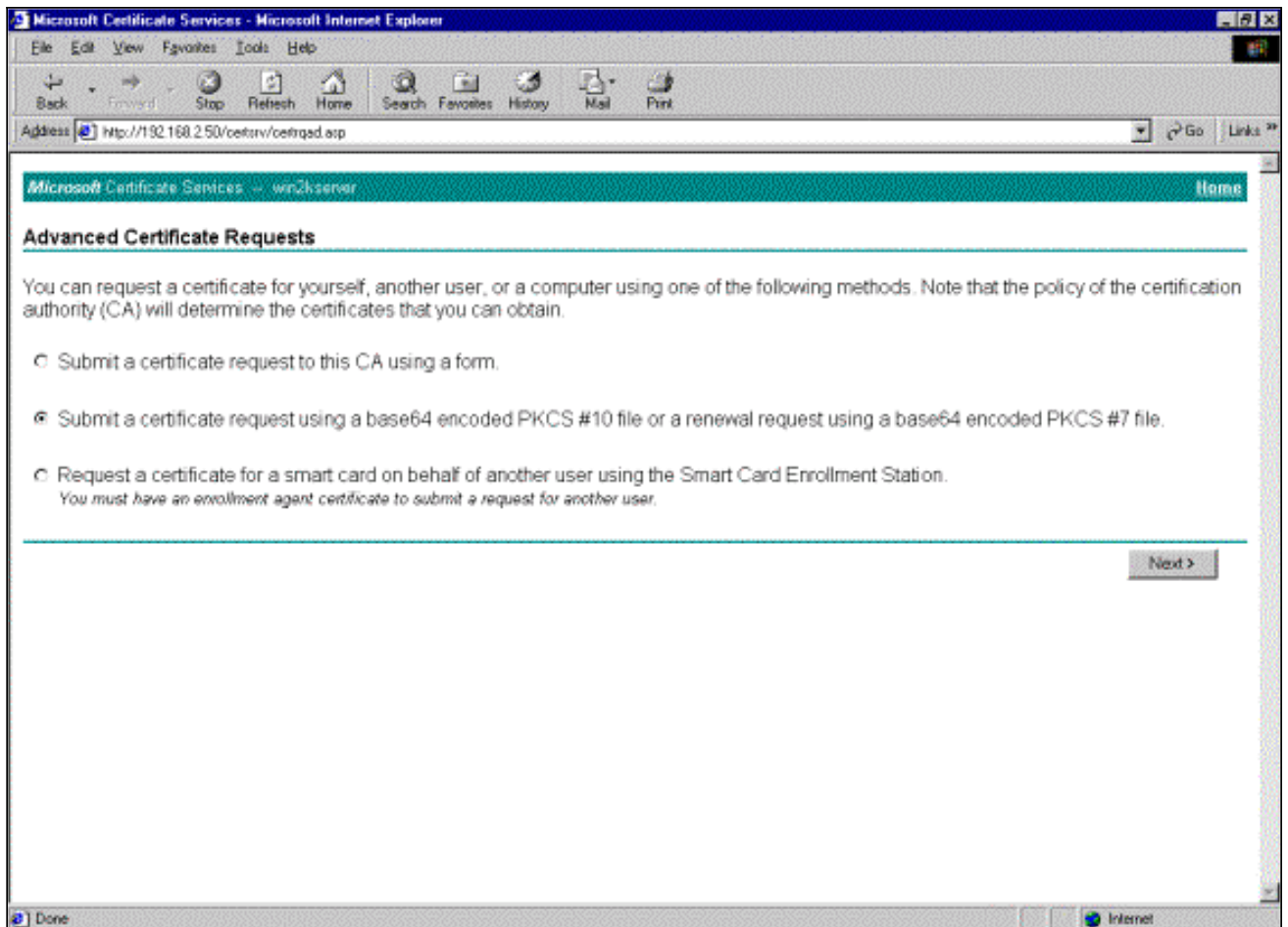


12. 为请求类型选择“高级请求”，然后单击“下一步”。

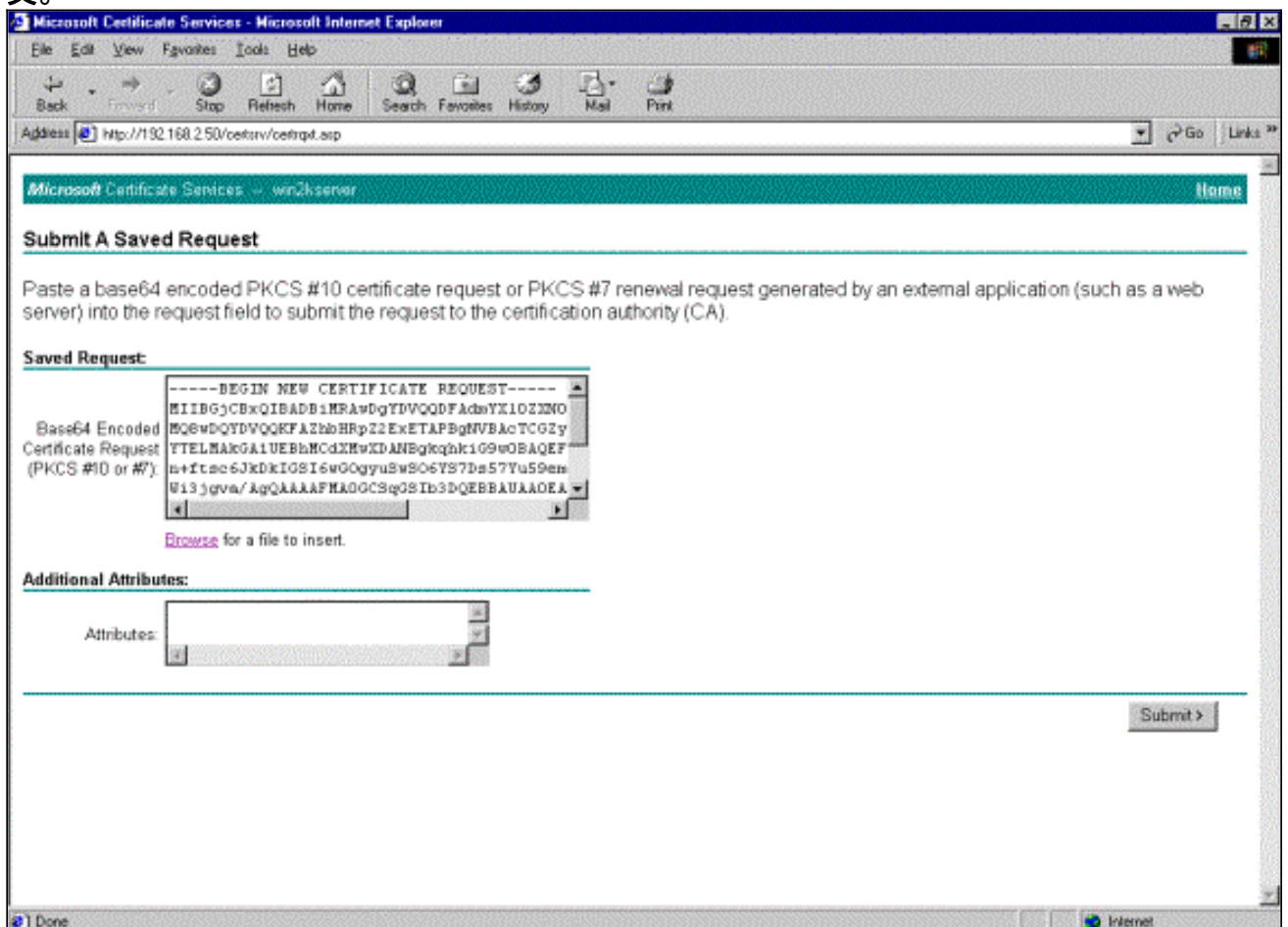


13. 在“Advanced Certificate Requests”下，选择“Submit a certificate request using a base64 encoded PKCS #10 file”或“renewal request using a base64 encoded PKCS #7 file”，然后单击Next。

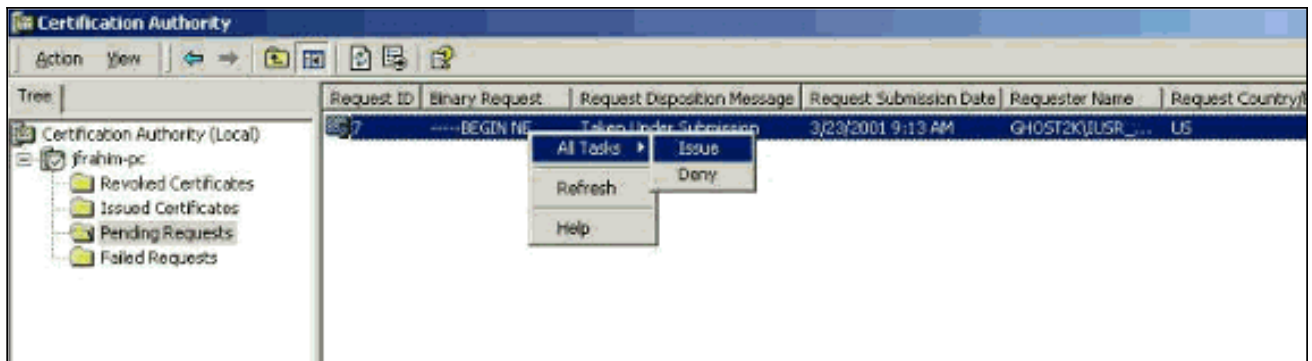




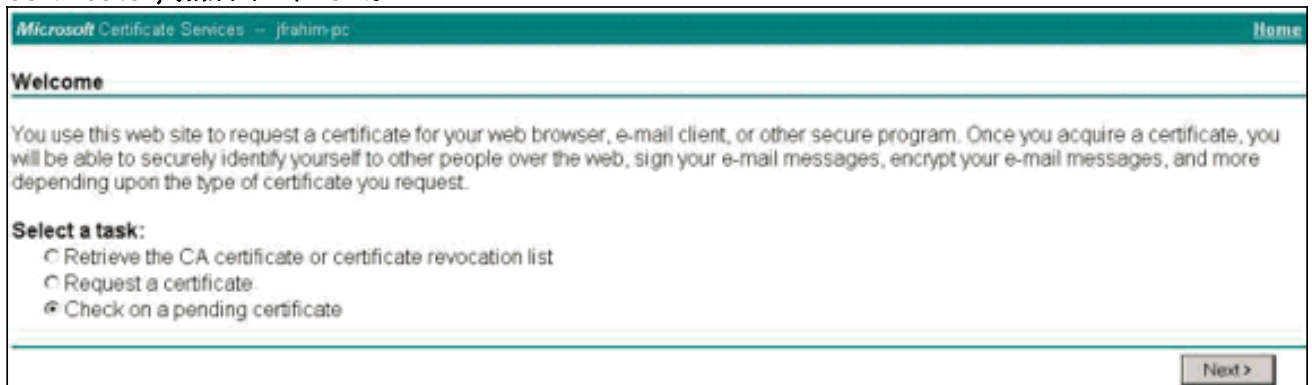
14. 突出显示VPN Client请求文件，并将其粘贴到Saved Request下的CA服务器。然后请点击提交。



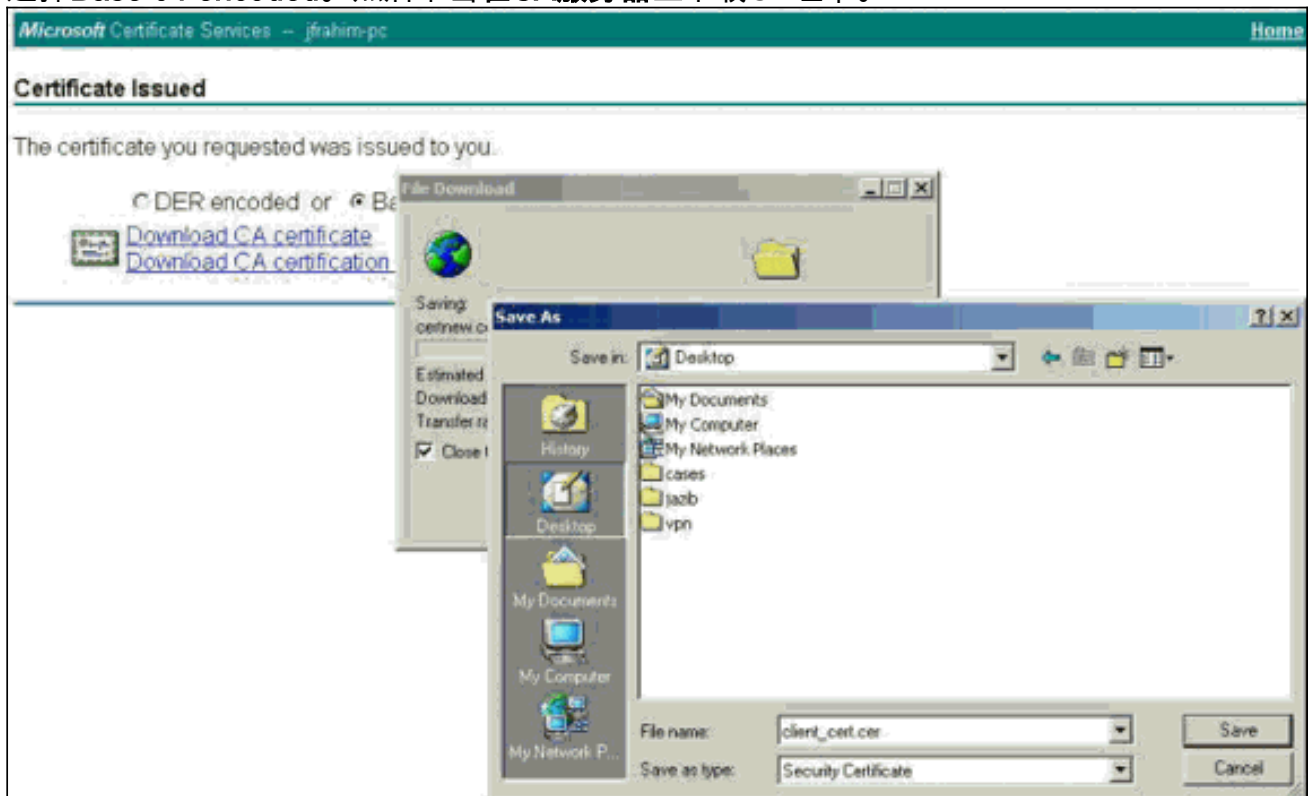
15. 在CA服务器上，为VPN客户端请求颁发身份证书。



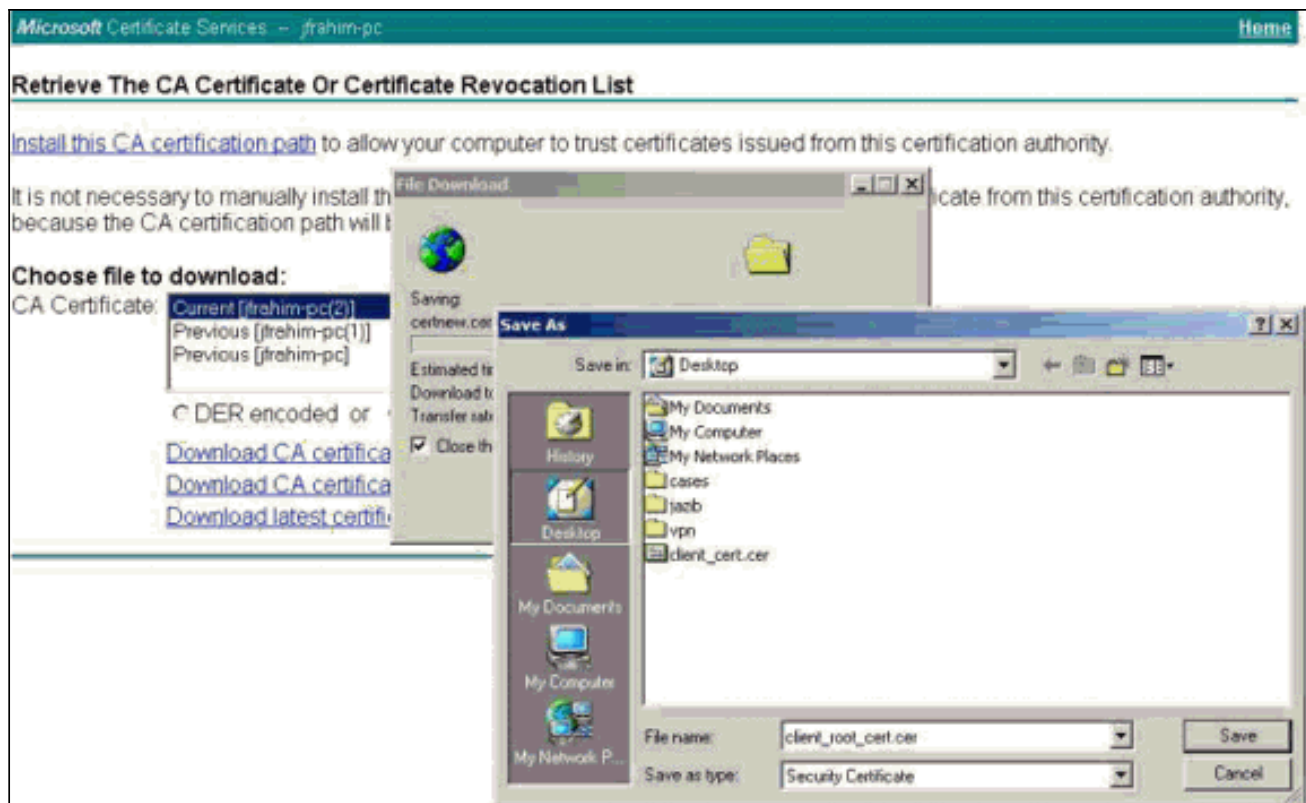
16. 将根证书和身份证书下载到VPN客户端。在CA服务器上，选择Check on a pending certificate，然后单击Next。



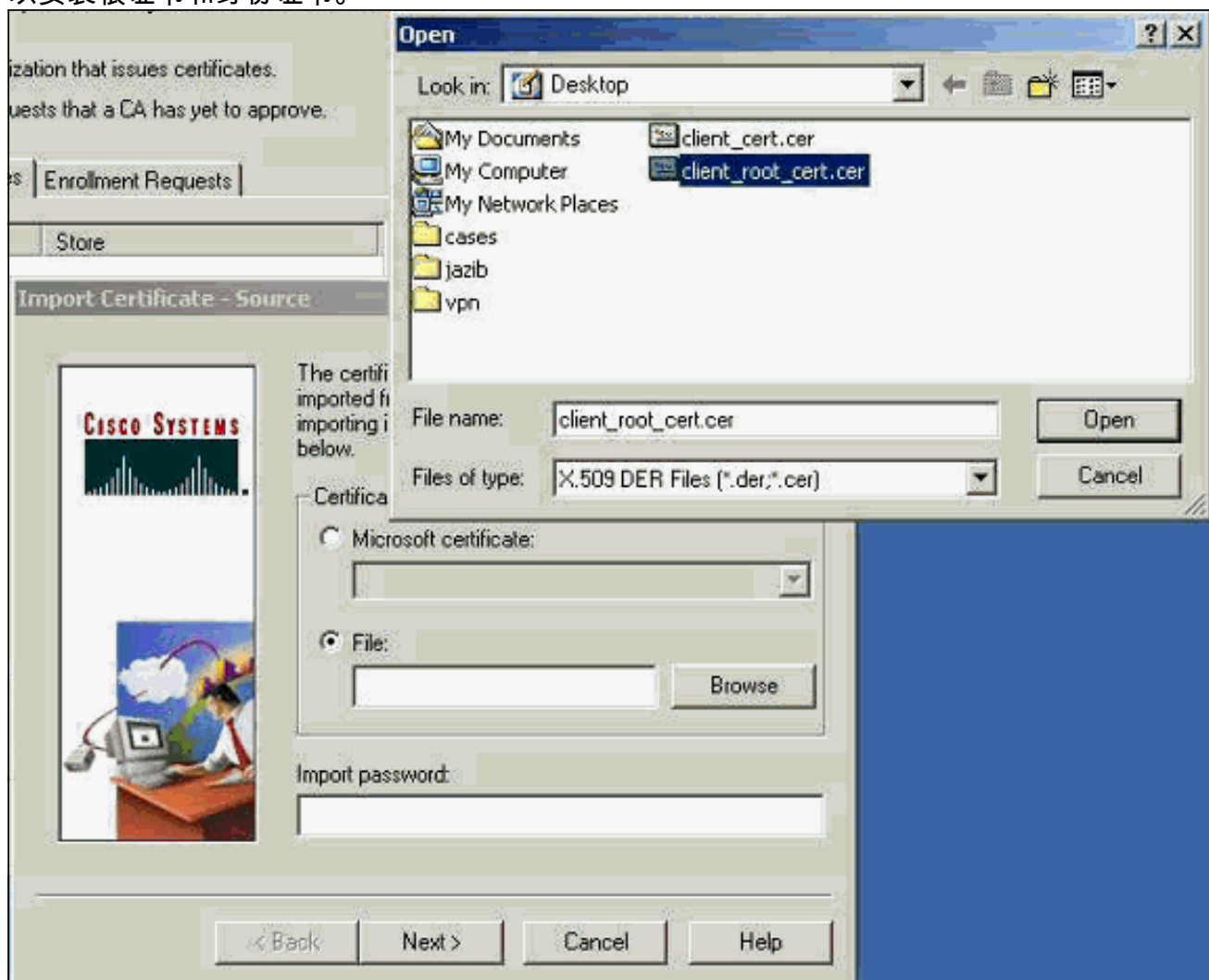
17. 选择Base 64 encoded。然后单击在CA服务器上下载CA证书。



18. 从Retrieve the CA Certificate or Certificate Revocation List页面选择要下载的文件，以获取CA服务器上的根证书。然后，单击下一步。



19. 选择Certificate Manager > CA Certificate > Import on the VPN Client，然后选择根CA文件以安装根证书和身份证书。

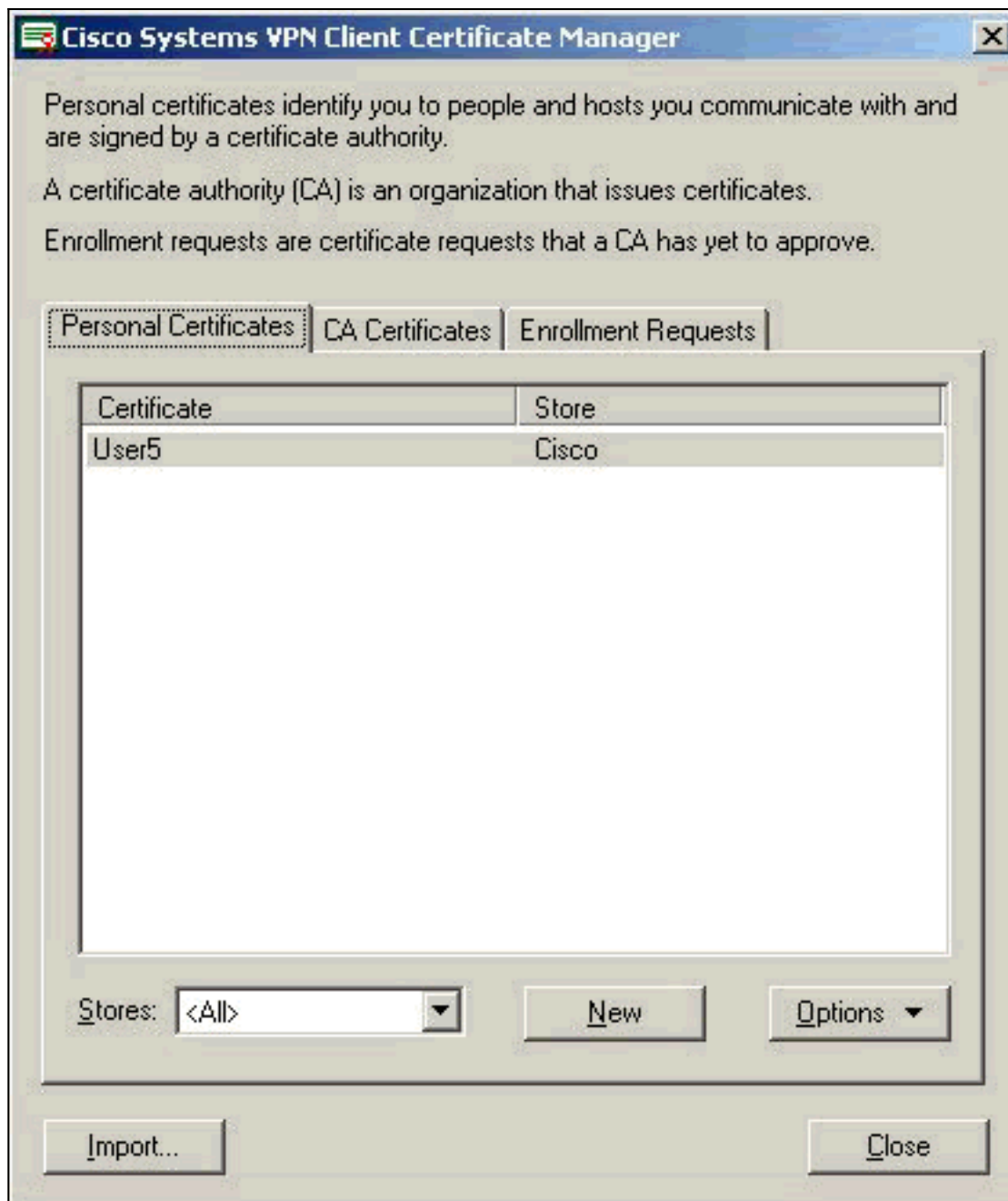


20. 选择Certificate Manager > Personal Certificates > Import，然后选择身份证书文件。



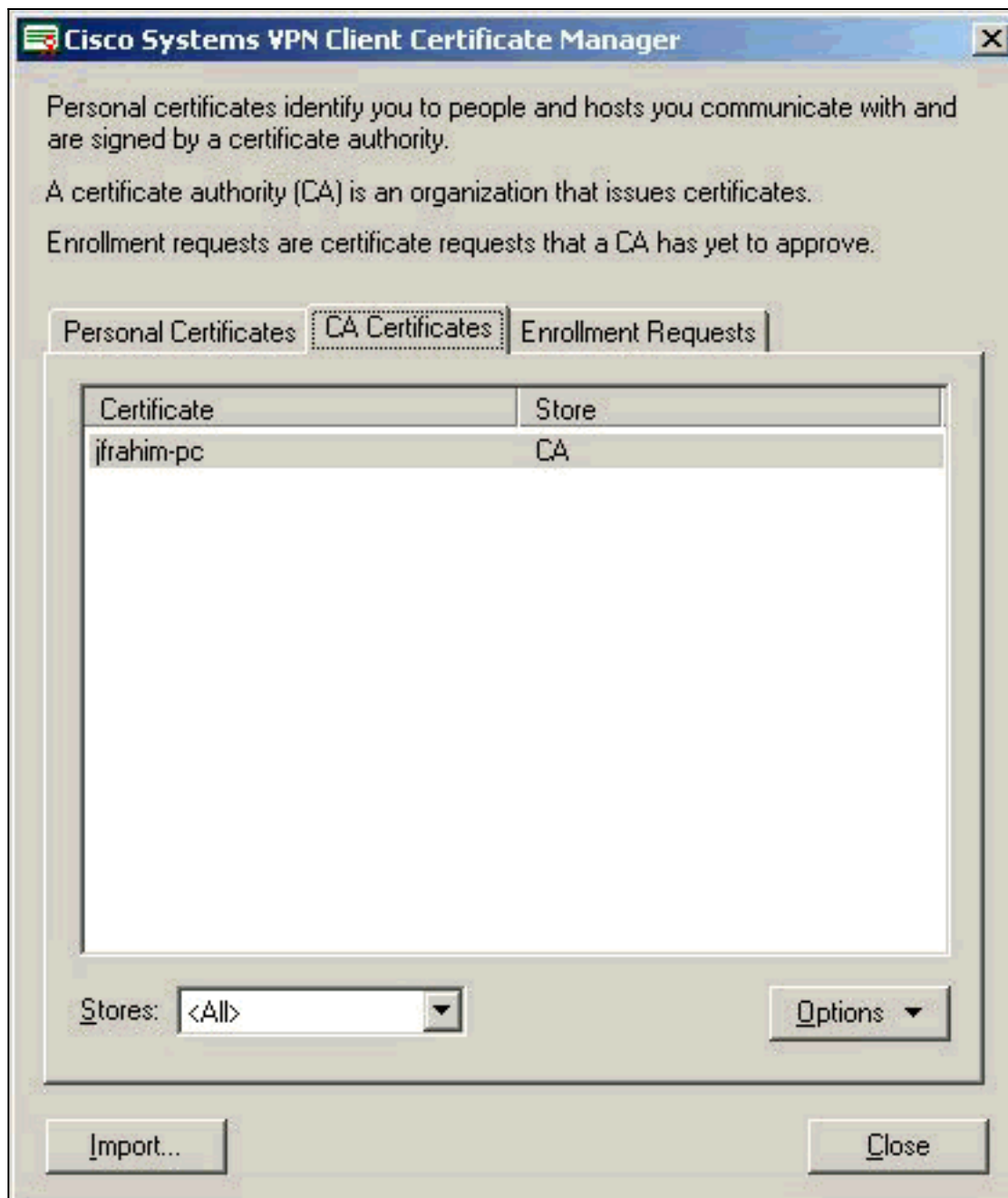
21. 确保身份证书显示在“个人证书”选项卡下。





22. 确保根证书出现在CA Certificates选项卡下。





## 验证

当前没有可用于此配置的验证过程。

## 故障排除

当您尝试向Microsoft CA服务器注册时，它可能会生成此错误消息。

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

如果收到此错误消息，请参阅Microsoft CA日志了解详细信息，或参阅这些资源了解详细信息。

- [Windows找不到处理请求的证书颁发机构](#)
- [XCCC:当您请求安全会议的证书时，会出现“Your Certificate Request was Denied”错误消息](#)

## 相关信息

- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)