

Configuring the VPN Client 3.x to Get a Digital Certificate

Document ID: 4302

Contents

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure the VPN Client

Verify

Troubleshoot

Related Information

Introduction

This document demonstrates how to configure the Cisco VPN Client 3.x to get a digital certificate.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on a PC that runs 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.

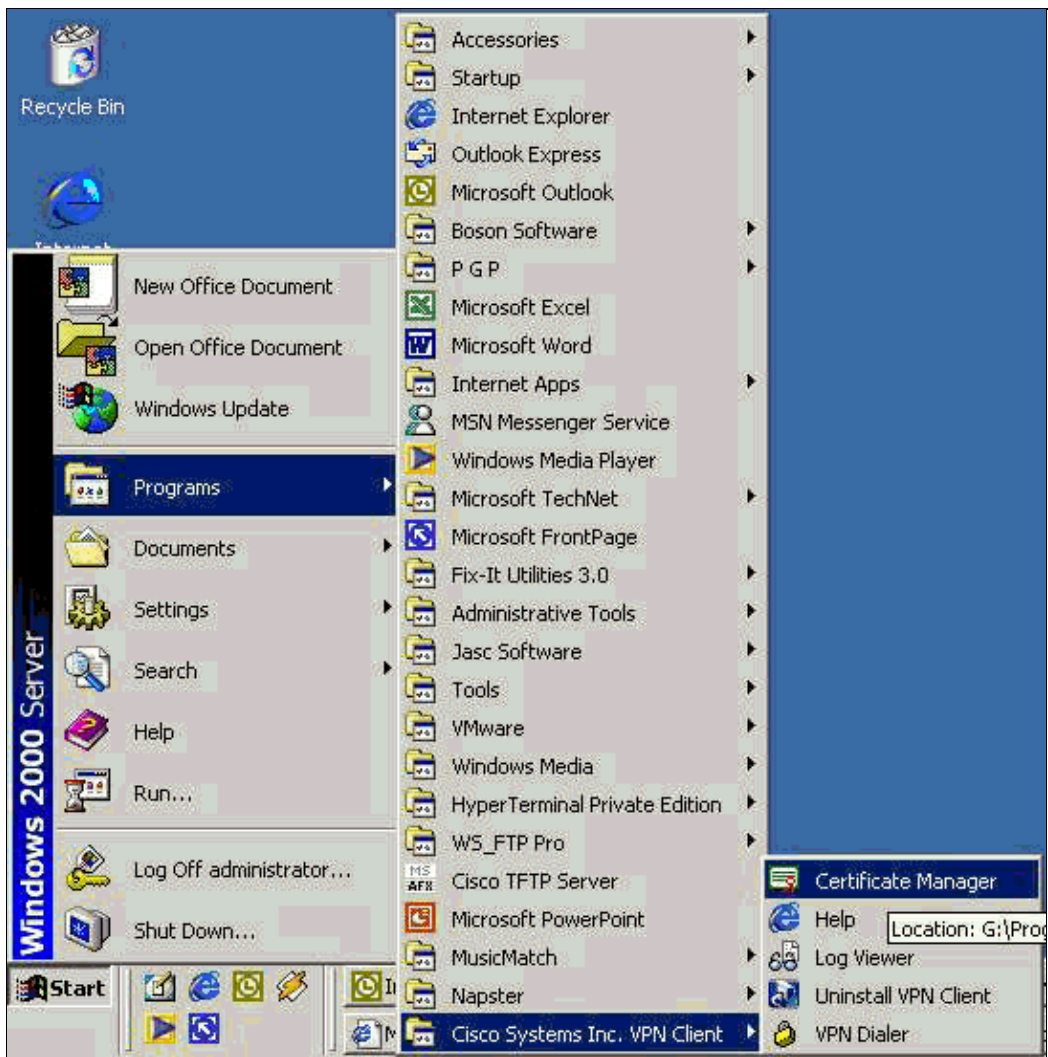
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

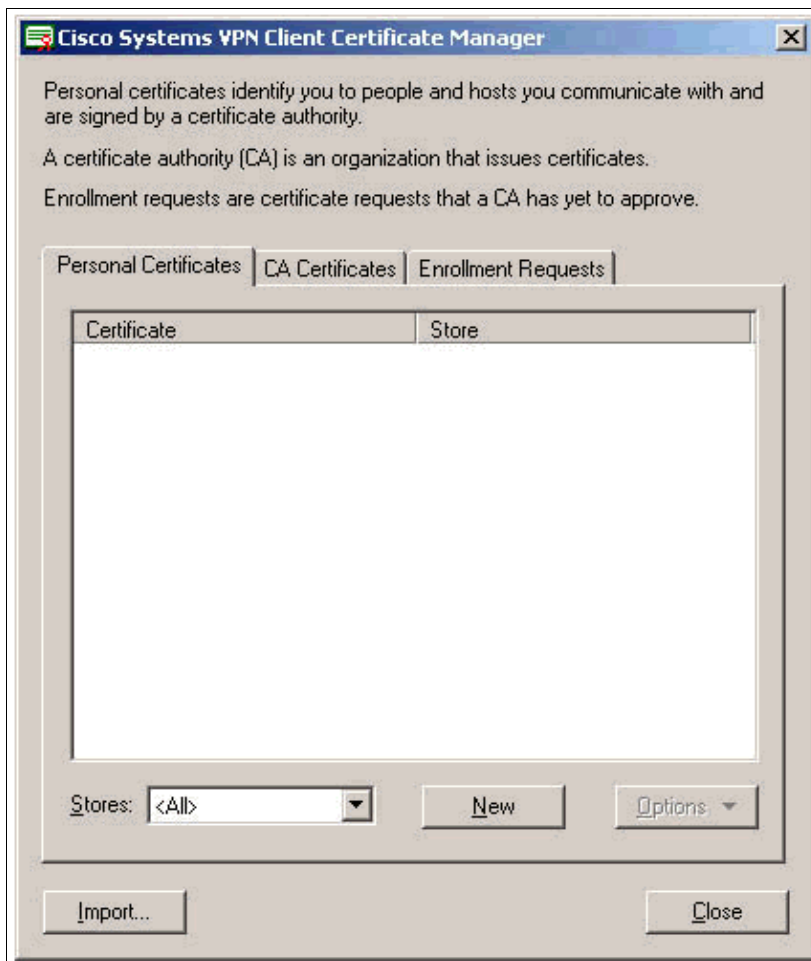
Configure the VPN Client

Complete these steps to configure the VPN Client.

1. Select **Start > Programs > Cisco Systems Inc. VPN client > Certificate Manager** to launch the VPN Client Certificate Manager.



2. Select the Personal Certificates tab and click **New**.



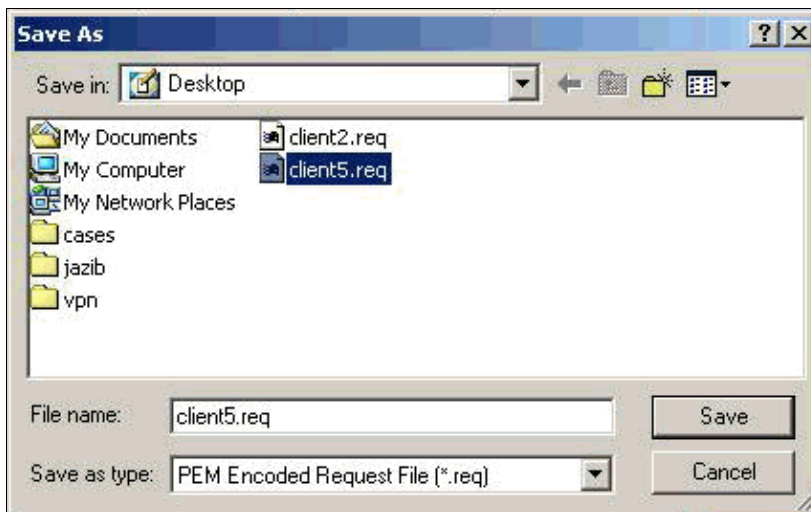
- Note:** Machine certificates to authenticate users for VPN connections cannot be done with IPsec.
3. When the VPN Client prompts you for a password, specify a password to protect the certificate. Any operation that requires access to the certificate's private key requires the specified password to continue.



4. Select **File** to request a certificate using PKCS #10 format on the Enrollment page. Then click **Next**.



5. Click **Browse**, and specify a filename for the certificate request file. For the file type, select **PEM Encoded Request File (*.req)** and click **Save**.



6. Click **Next** on the VPN Client Enrollment page.

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

< Back Next > Cancel Help

7. Fill out the fields on the Enrollment Form.

This example shows the fields:

- ◆ Common Name = User1
- ◆ Department = IPSECCERT (This should match the organizational unit (OU) and the group name on the VPN 3000 Concentrator.)
- ◆ Company = Cisco Systems
- ◆ State = NorthCarolina
- ◆ Country = US
- ◆ Email = User1@email.com
- ◆ IP Address = (optional; used to specify the IP address on the certificate request)
- ◆ Domain = cisco.com

Click **Next** when you are done.

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. Click **Finish** to proceed with the enrollment.

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

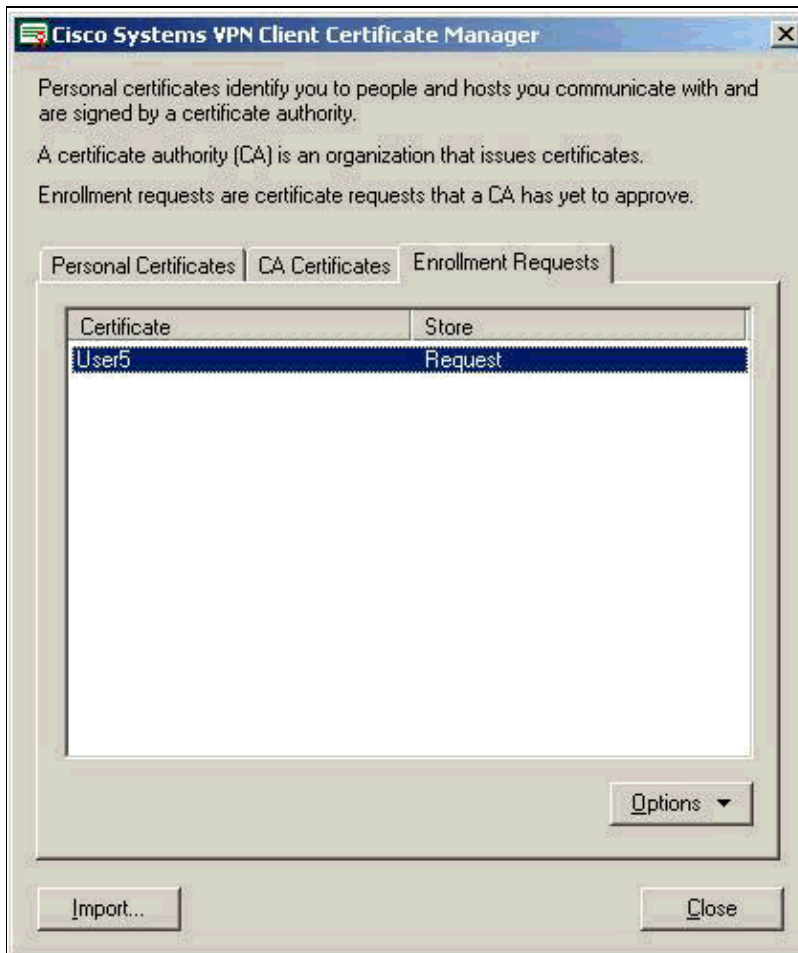
Email: User1@email.com

IP Address:

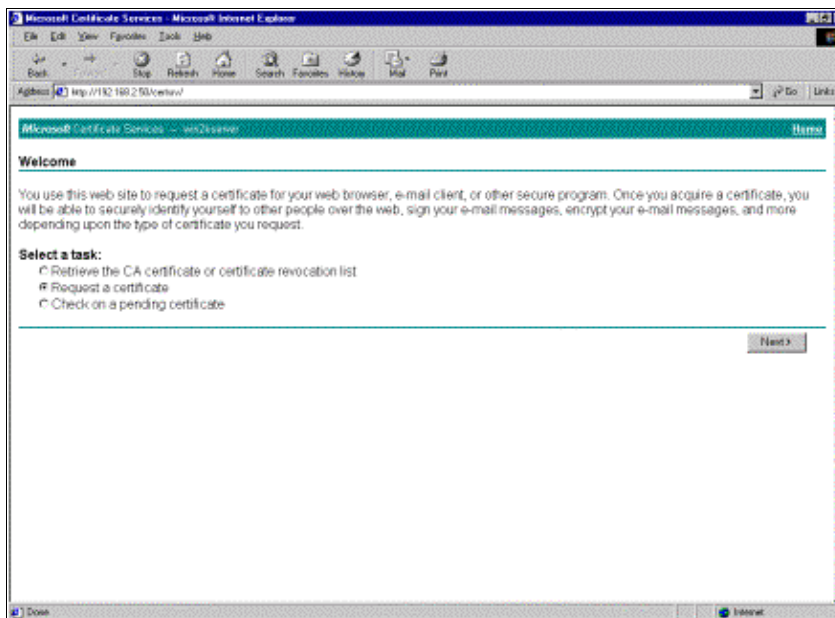
Domain: cisco.com

< Back Finish Cancel Help

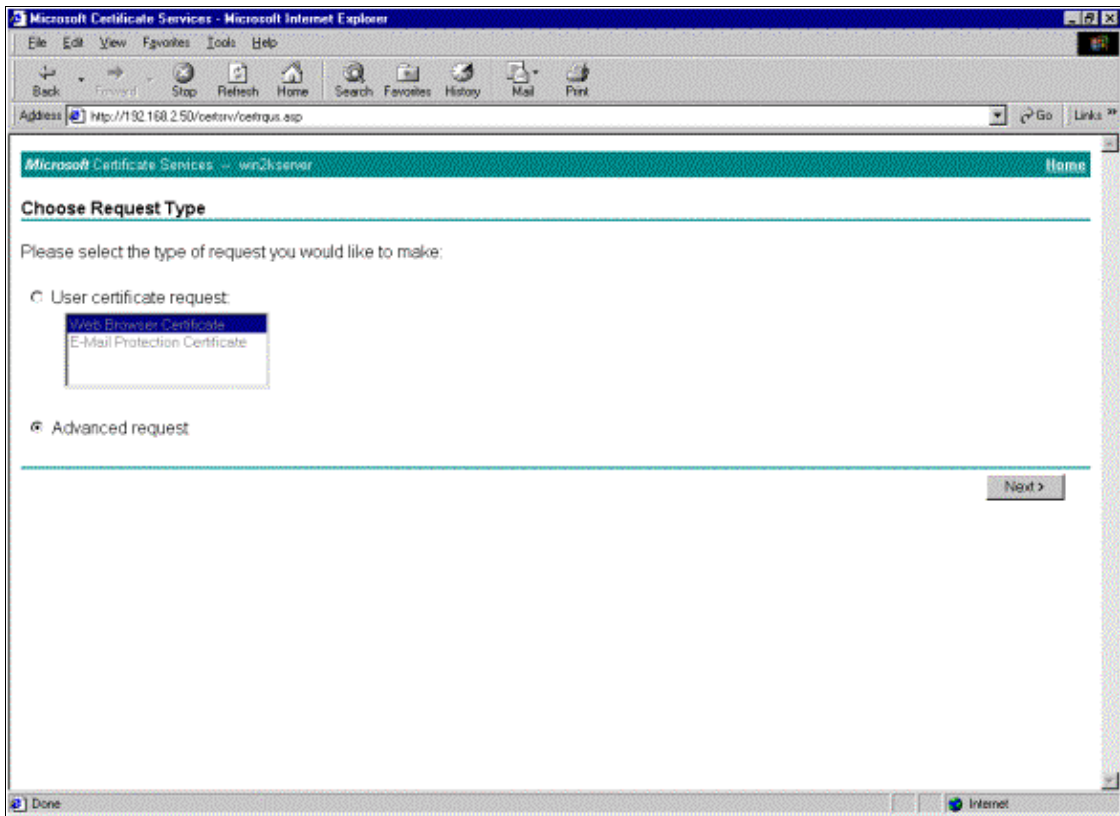
9. Select the Enrollment Requests tab to check the request on the VPN Client Certificate Manager.



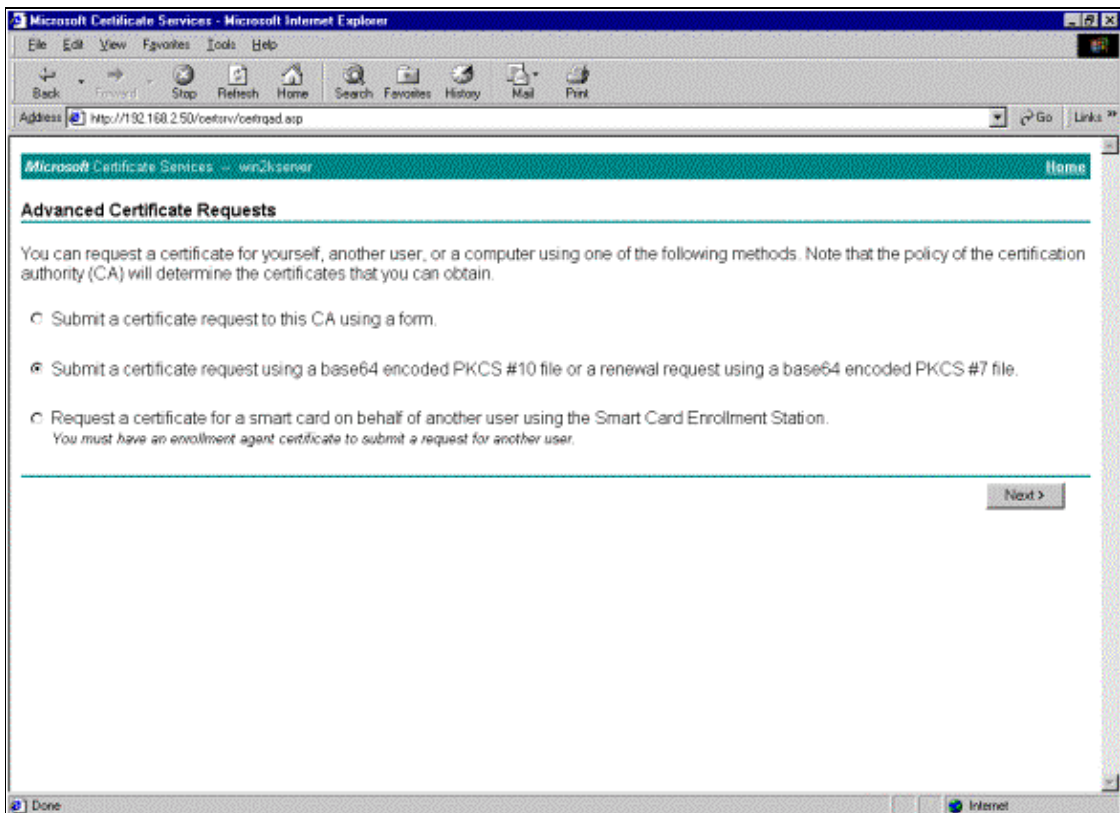
10. Bring up the Certification Authority (CA) server and the VPN Client interfaces concurrently to submit the request.
11. Select **Request a certificate** and click **Next** on the CA server.



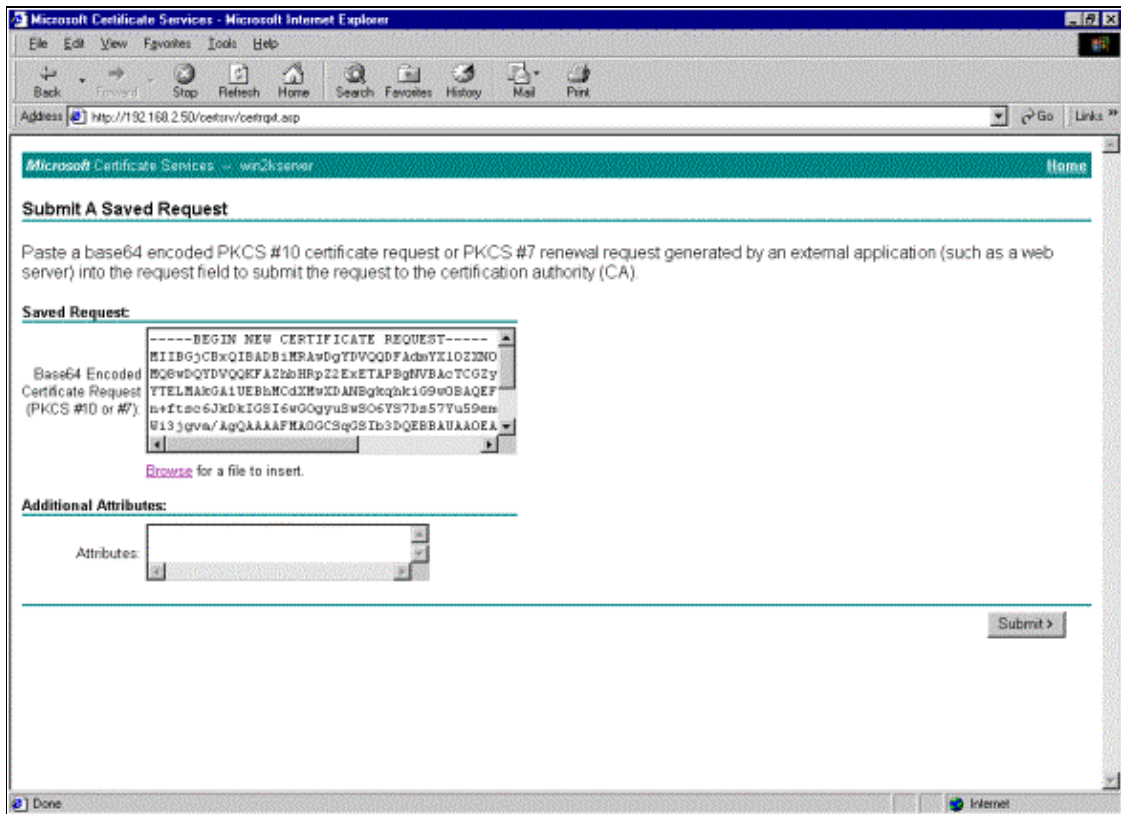
12. Select **Advanced request** for the type of request and click **Next**.



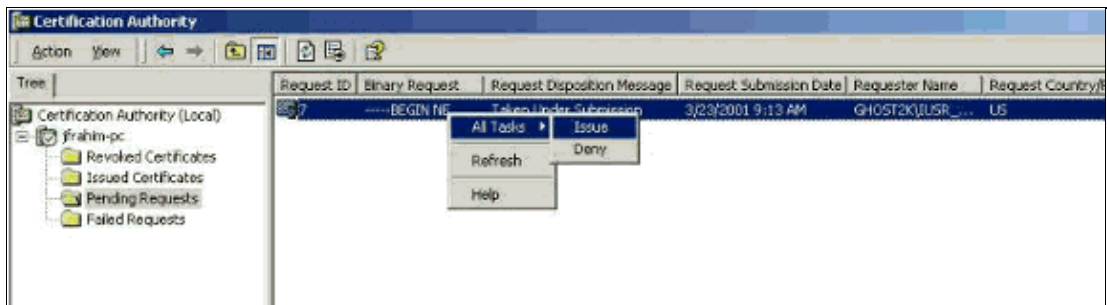
13. Select **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file** under Advanced Certificate Requests, and then click **Next**.



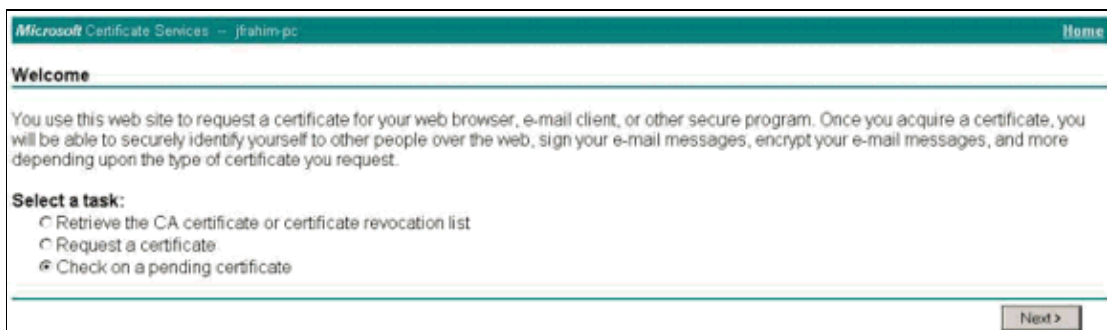
14. Highlight the VPN Client request file, and paste it to the CA server under Saved Request. Then click **Submit**.



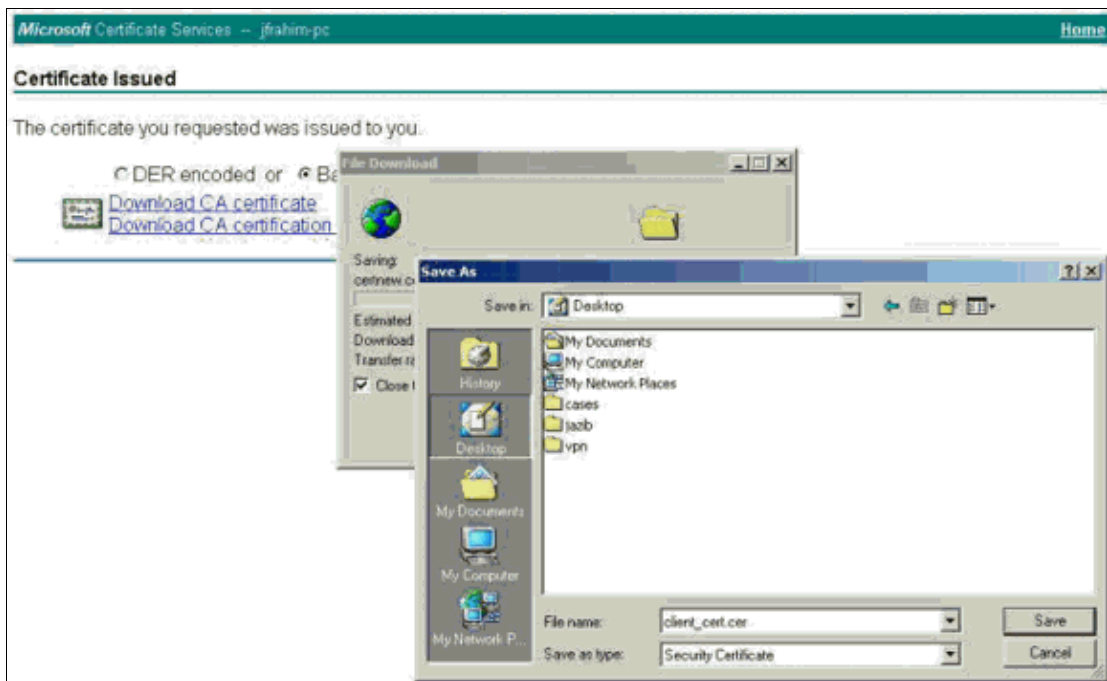
15. On the CA server, issue the identity certificate for the VPN Client request.



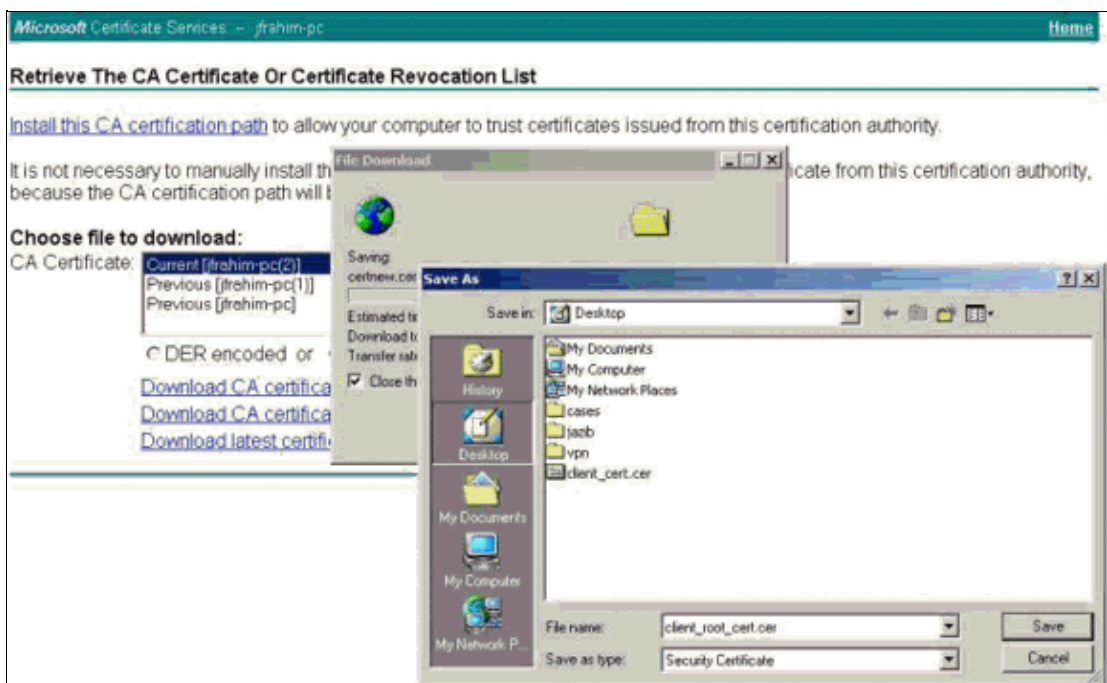
16. Download the root and identity certificates to the VPN Client. On the CA server, select **Check on a pending certificate**, and then click **Next**.



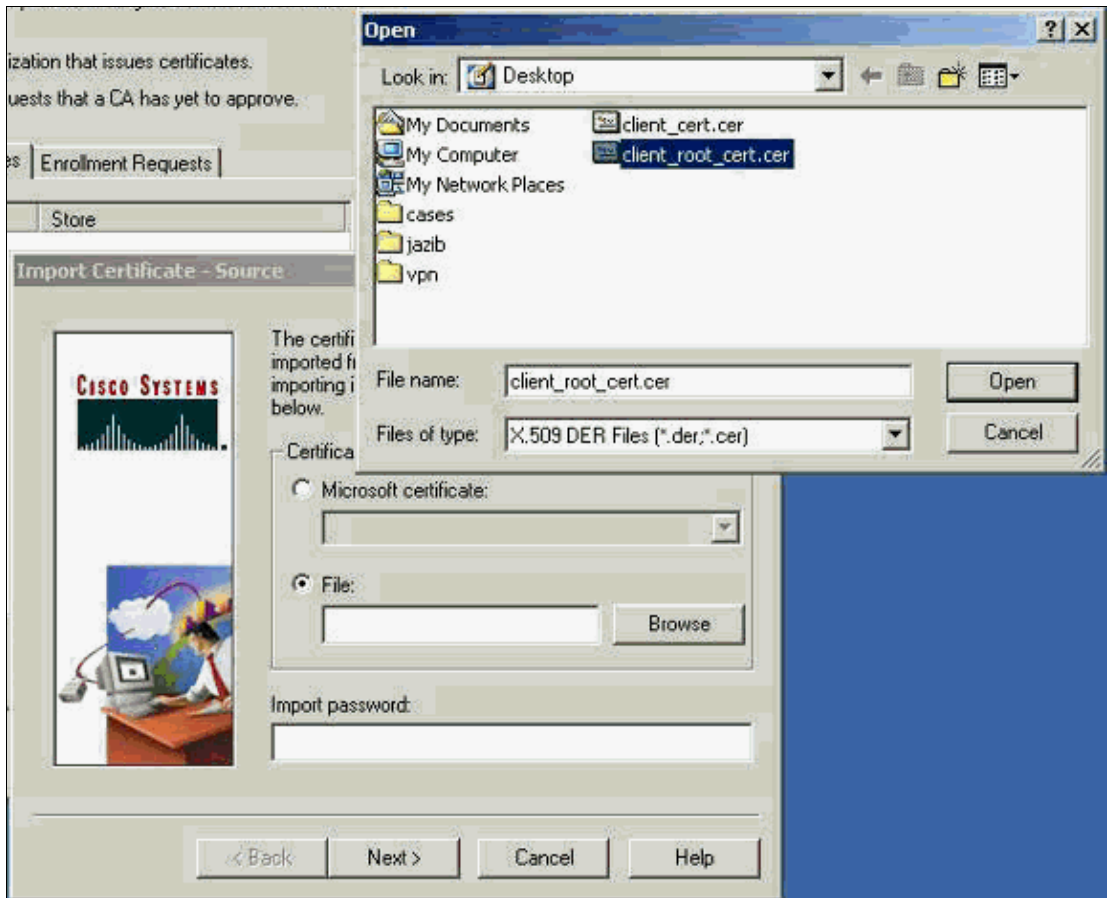
17. Select **Base 64 encoded**. Then click **Download CA certificate** on the CA server.



18. Select a file to download from the Retrieve the CA Certificate or Certificate Revocation List page to get the root certificate on the CA server. Then click **Next**.



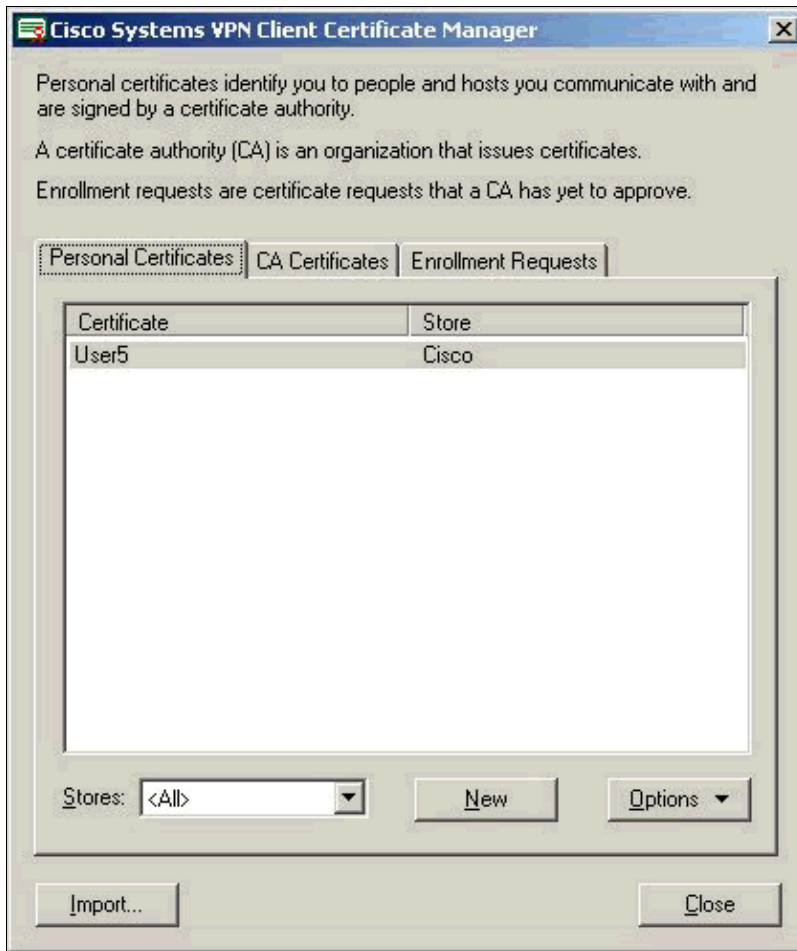
19. Select **Certificate Manager > CA Certificate > Import on the VPN Client**, and then select the root CA file to install the root and identity certificates.



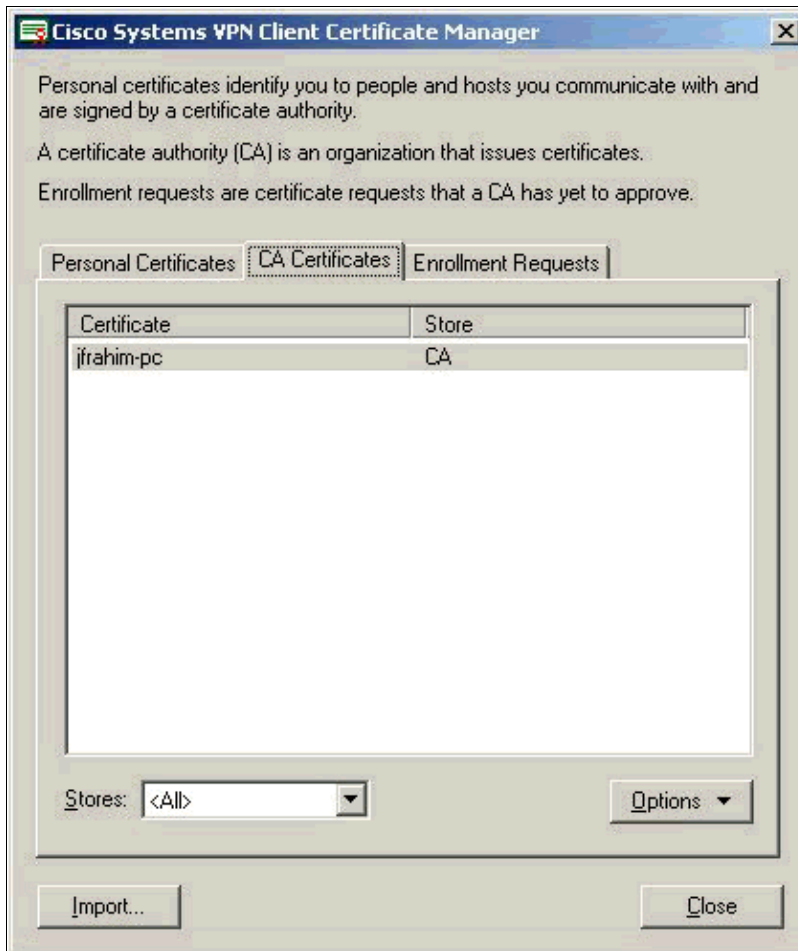
20. Select **Certificate Manager > Personal Certificates > Import**, and choose the identity certificate file.



21. Ensure that the identity certificate appears under the Personal Certificates tab.



22. Ensure that the root certificate appears under the CA Certificates tab.



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

When you attempt to enroll with the Microsoft CA Server, it can generate this error message.

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

If you receive this error message, refer to the Microsoft CA logs for details, or refer to these resources for more information.

- [Windows Cannot Find a Certificate Authority That Processes the Request](#)
- [XCCC: "Your Certificate Request was Denied" Error Message Occurs When You Request a Certificate for Secure Conferences](#)

Related Information

- [Cisco VPN 3000 Product Documentation](#)
- [IPsec Negotiation/IKE Protocols](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 4302
