

Konfigurieren des VPN Client 3.x zum Abrufen eines digitalen Zertifikats

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren des VPN-Clients](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird veranschaulicht, wie der Cisco VPN Client 3.x so konfiguriert wird, dass er ein digitales Zertifikat erhält.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf einem PC, auf dem Cisco VPN Client 3.x ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

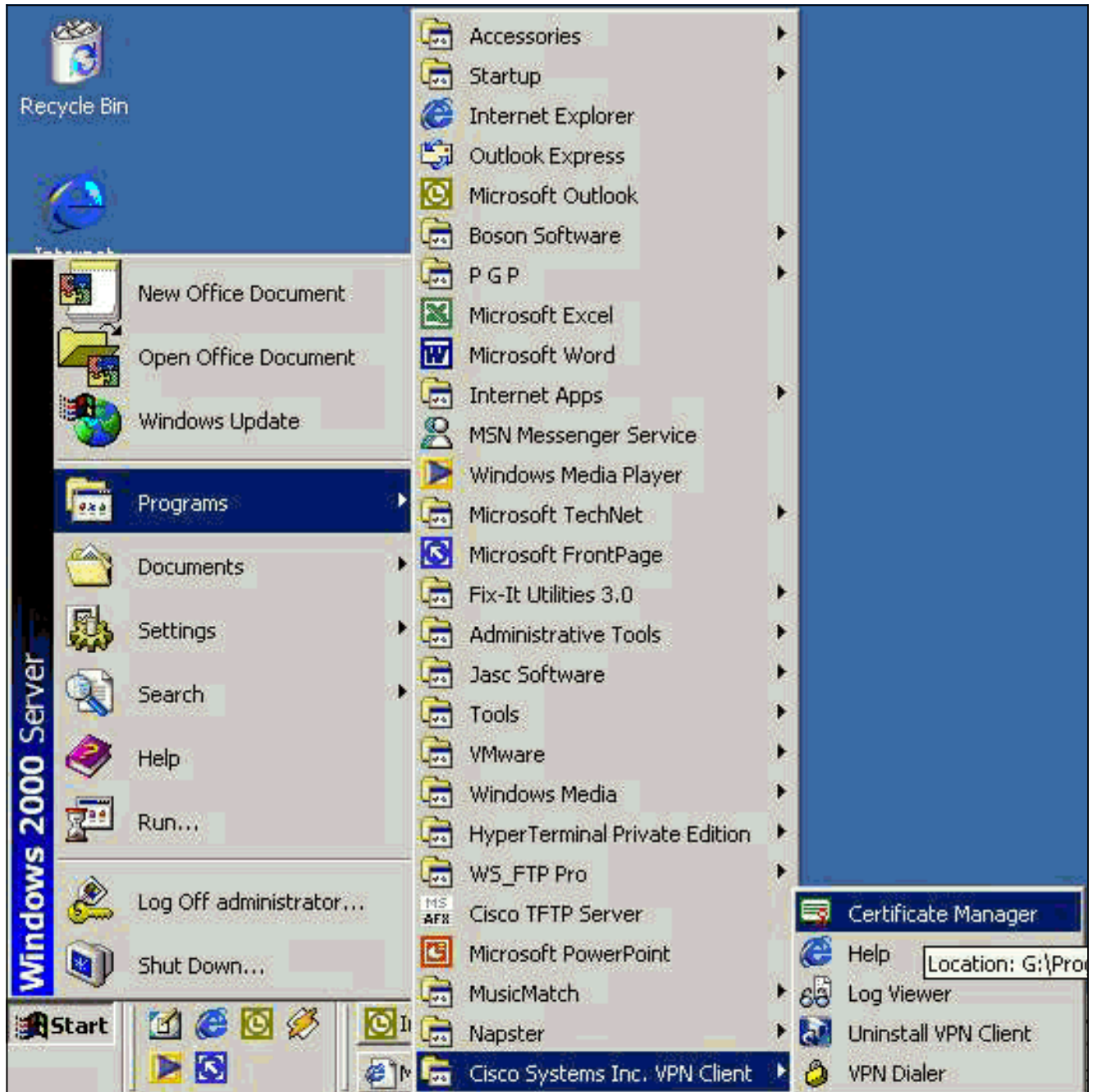
[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

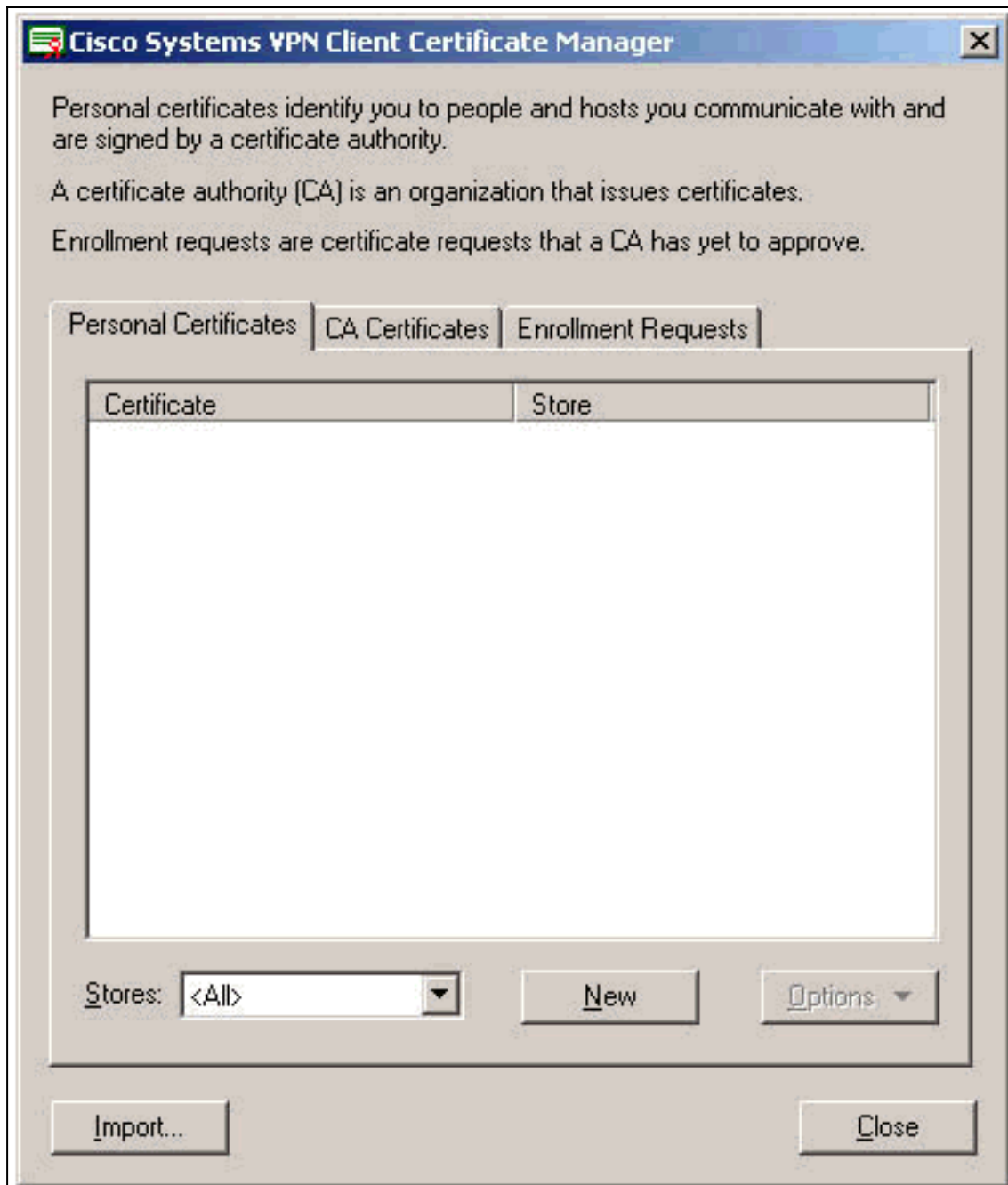
Konfigurieren des VPN-Clients

Führen Sie diese Schritte aus, um den VPN-Client zu konfigurieren.

1. Wählen Sie **Start > Programme > Cisco Systems Inc. VPN-Client > Certificate Manager** aus, um den VPN Client Certificate Manager zu starten.



2. Wählen Sie die Registerkarte **Persönliche Zertifikate** aus, und klicken Sie auf



Neu.

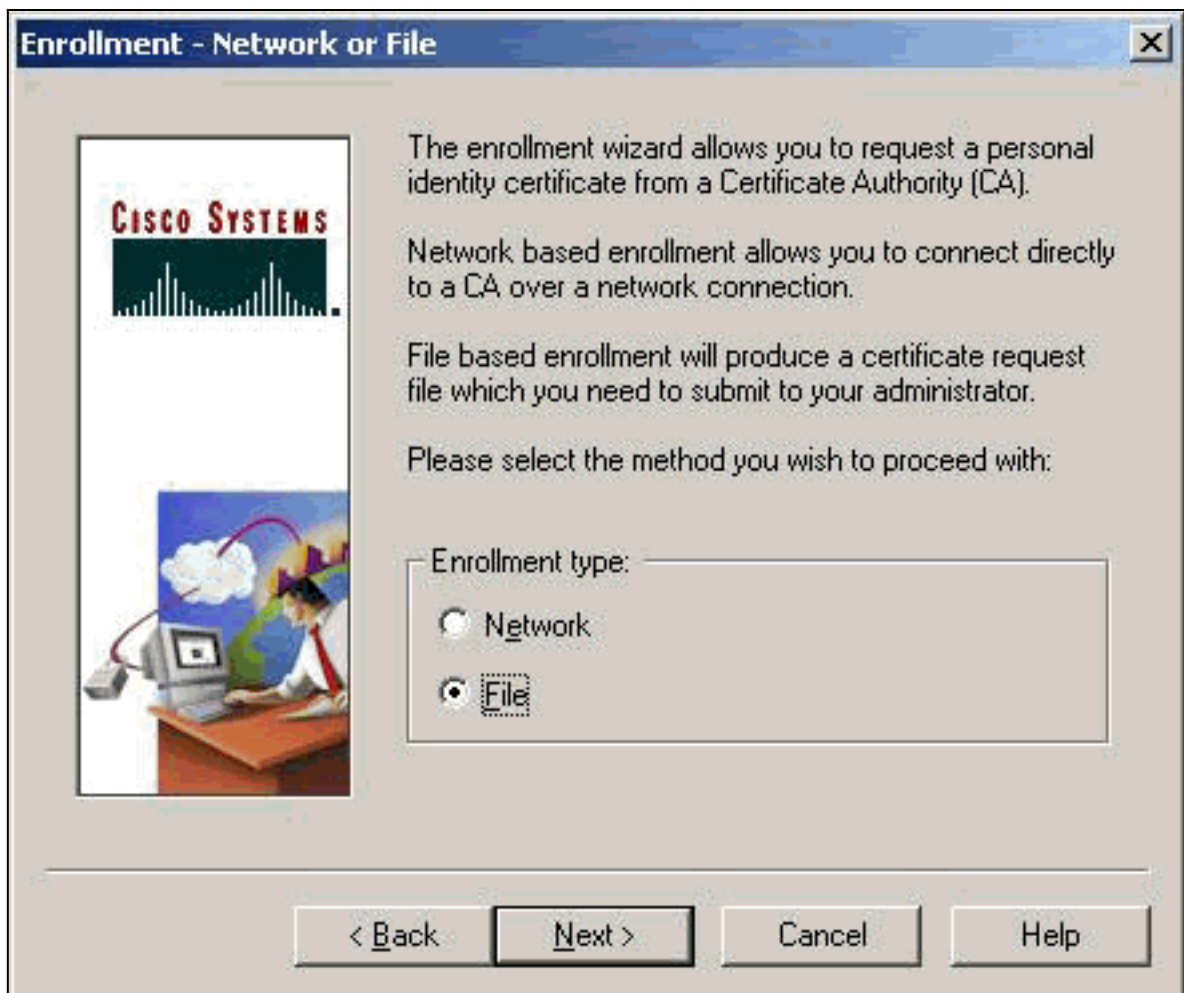
Hinweis

: Computerzertifikate zur Authentifizierung von Benutzern für VPN-Verbindungen können nicht mit IPsec erstellt werden.

3. Wenn Sie vom VPN-Client zur Eingabe eines Kennworts aufgefordert werden, geben Sie ein Kennwort zum Schutz des Zertifikats an. Bei jeder Operation, die Zugriff auf den privaten Schlüssel des Zertifikats erfordert, muss das angegebene Kennwort eingegeben werden, um fortzufahren.

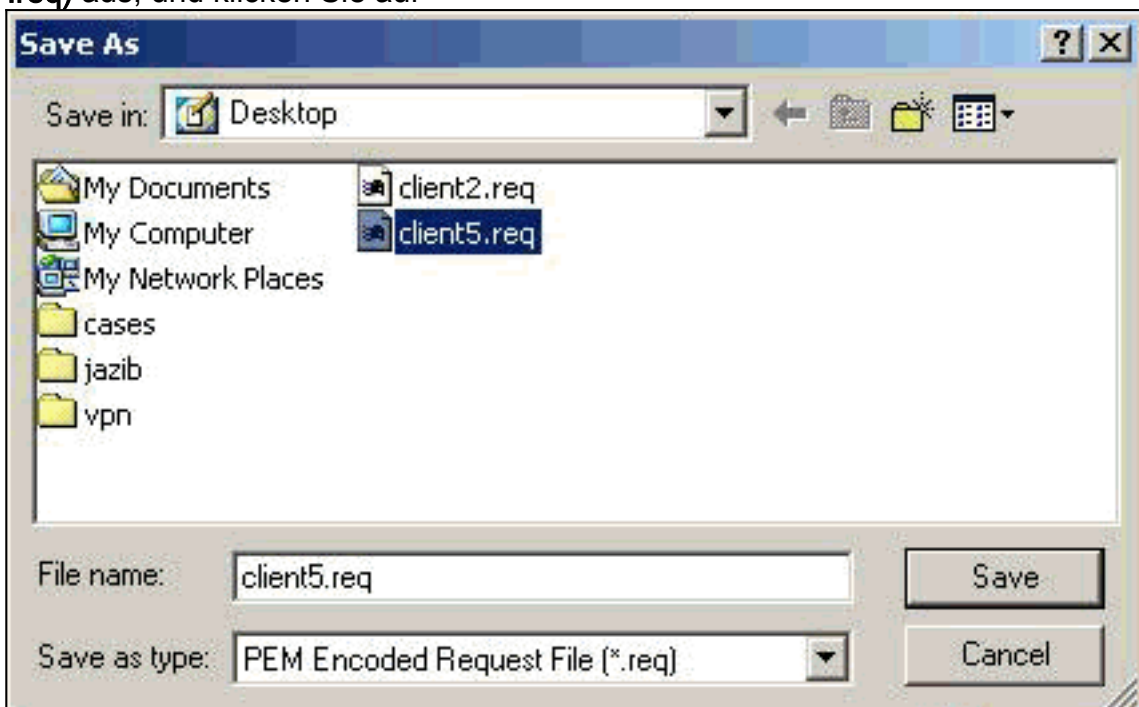


4. Wählen Sie **File (Datei)** aus, um ein Zertifikat im PKCS #10-Format auf der Anmeldeseite anzufordern. Klicken Sie anschließend auf



Weiter.

5. Klicken Sie auf **Durchsuchen**, und geben Sie einen Dateinamen für die Zertifikatsanforderungsdatei an. Wählen Sie als Dateityp die Option **PEM Encoded Request File (*.req)** aus, und klicken Sie auf



Save.

6. Klicken Sie auf der Seite "VPN Client Enrollment" auf

Enrollment - File Location [X]



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 Browse

File type:

Base 64 encoded (.req)

Binary encoded (.p10)

* Required Field


< Back
Next >
Cancel
Help

Weiter.

7. Füllen Sie die Felder im Anmeldeformular aus. Dieses Beispiel zeigt die Felder: Common Name = User1 Abteilung = IPSECCERT (Dies muss mit der Organisationseinheit (OU) und dem Gruppennamen im VPN 3000-Konzentrator übereinstimmen.) Unternehmen = Cisco Systems State = North Carolina Land = USA E-Mail = User1@email.com IP-Adresse = (optional) wird verwendet, um die IP-Adresse auf der Zertifikatsanforderung anzugeben.) Domain = cisco.com Klicken Sie abschließend auf

Enrollment - Form [X]

Enter your certificate enrollment information in the fields provided below.

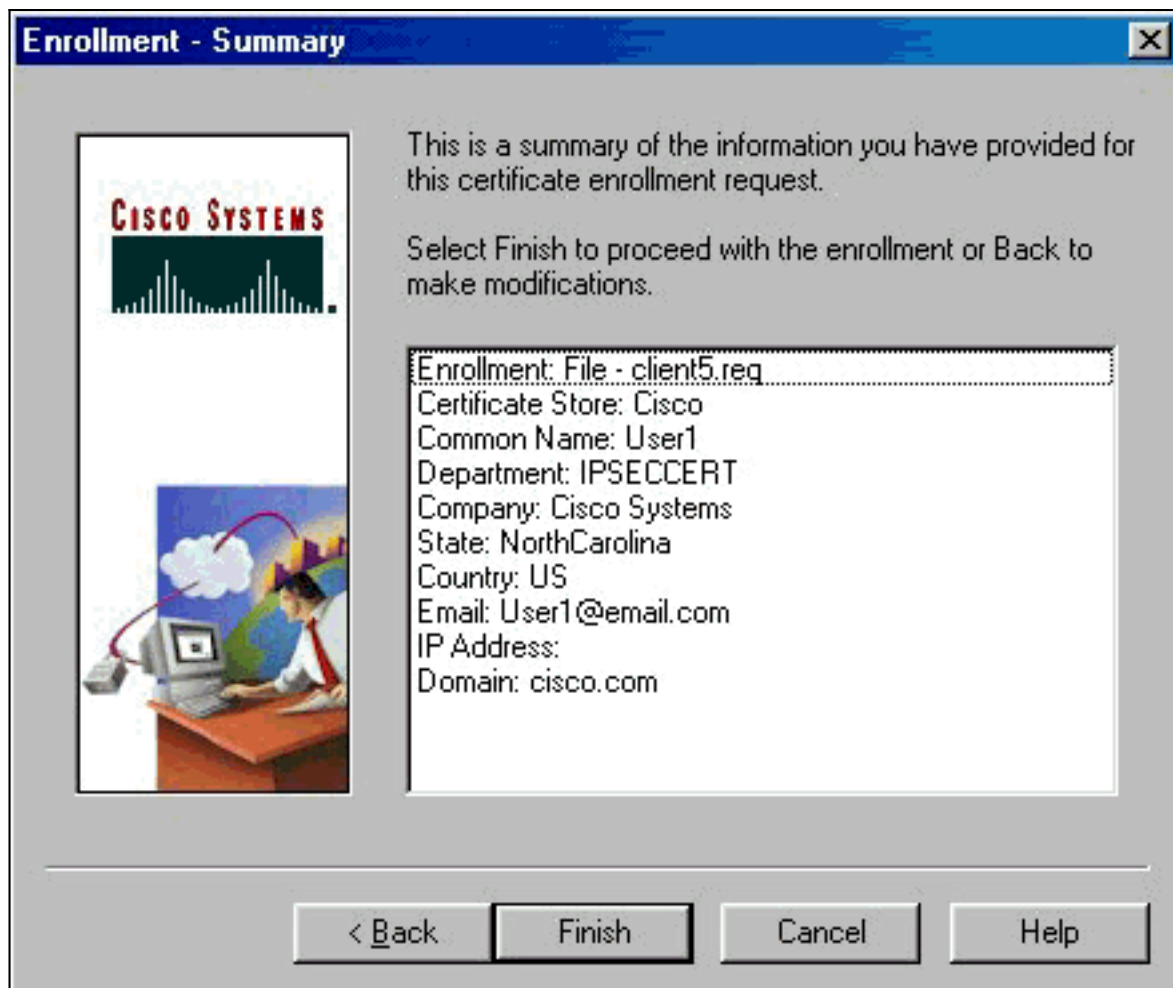
	<u>C</u> ommon Name (cn):*	User1
	<u>D</u> ePARTMENT (ou):	IPSECCERT
	<u>C</u> ompany (o):	Cisco Systems
	<u>S</u> tate (st):	NorthCarolina
	<u>C</u> ountry (c):	US
	<u>E</u> mail (e):	User1@email.com
	<u>I</u> P Address:	
	<u>D</u> omain:	cisco.com

* Required Field

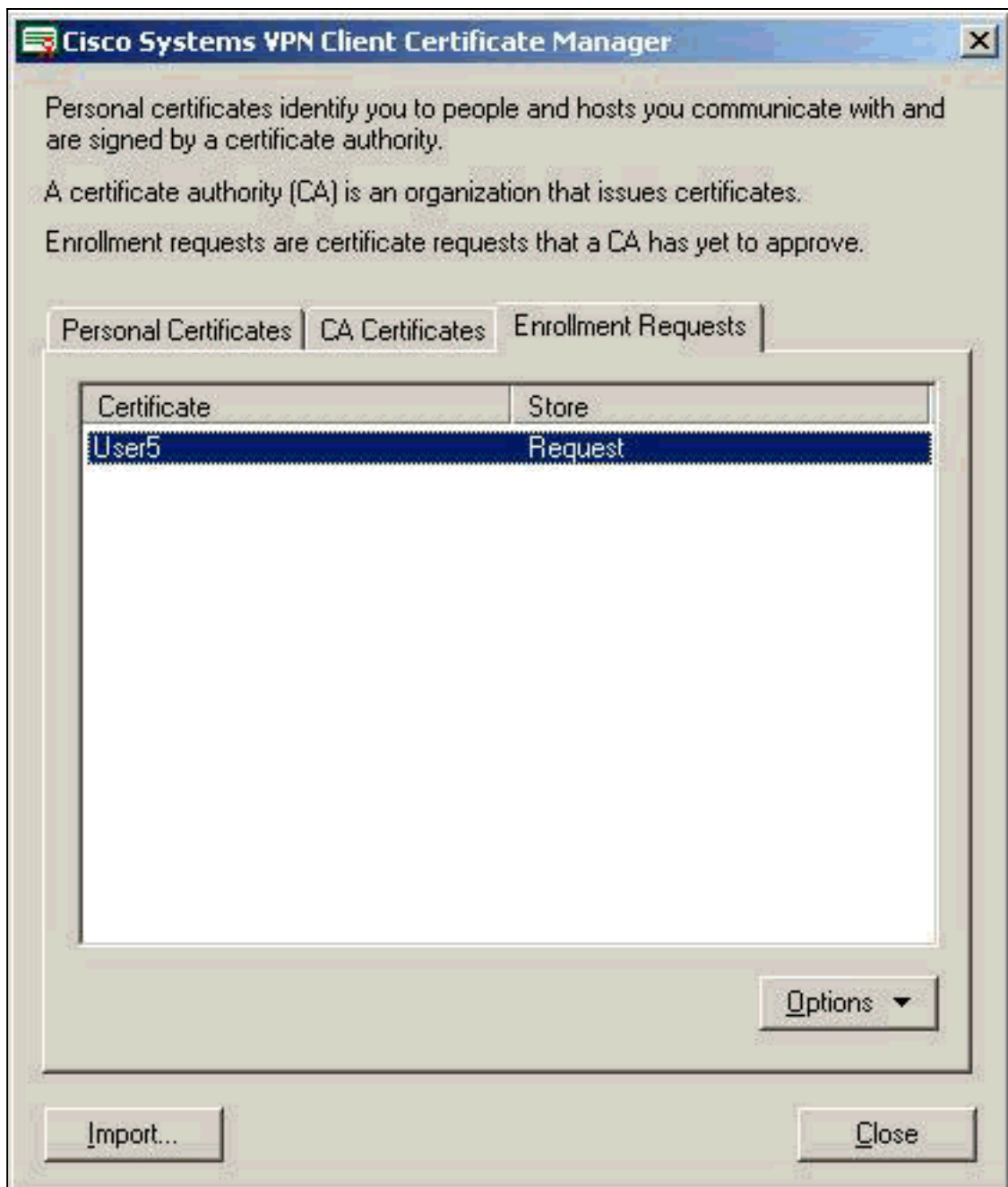
< Back Next > Cancel Help

Weiter.

8. Klicken Sie auf **Fertig stellen**, um mit der Registrierung fortzufahren.

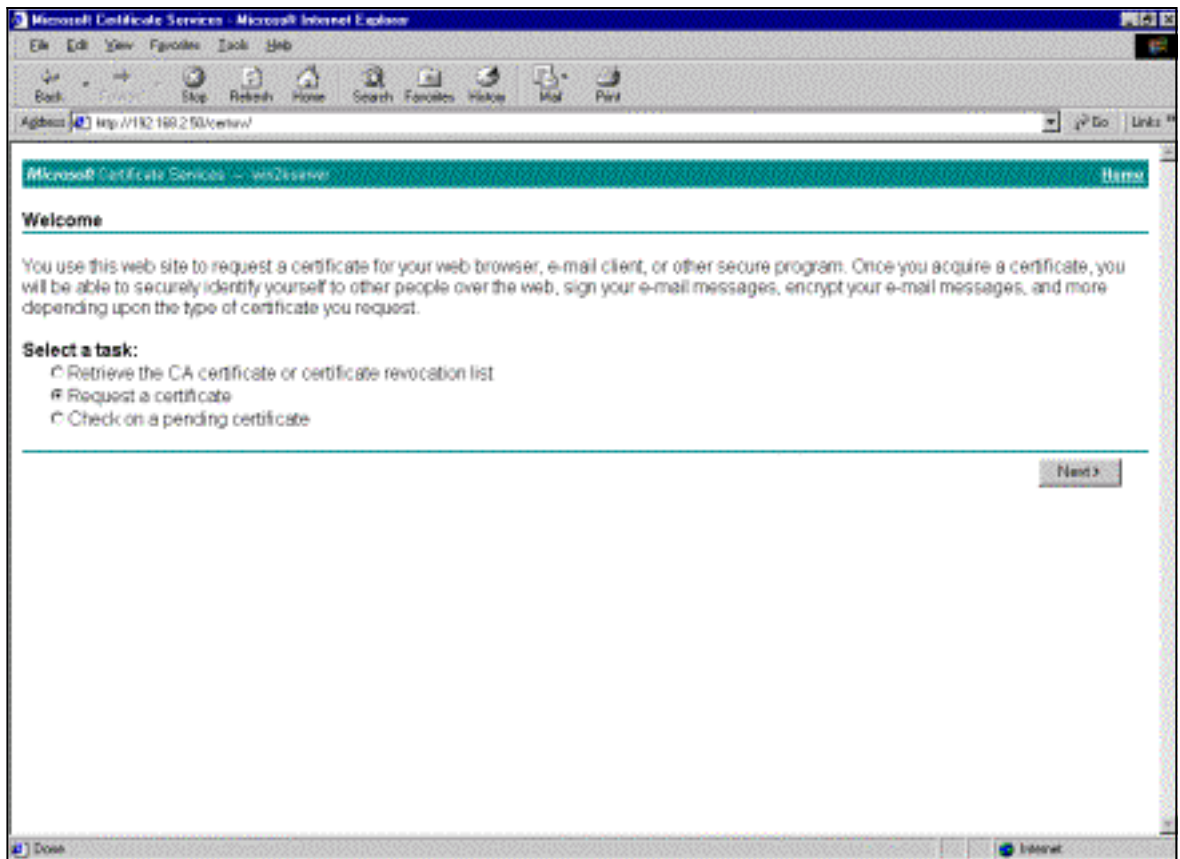


9. Wählen Sie die Registerkarte Registrierungsanfragen aus, um die Anforderung im VPN Client Certificate Manager zu



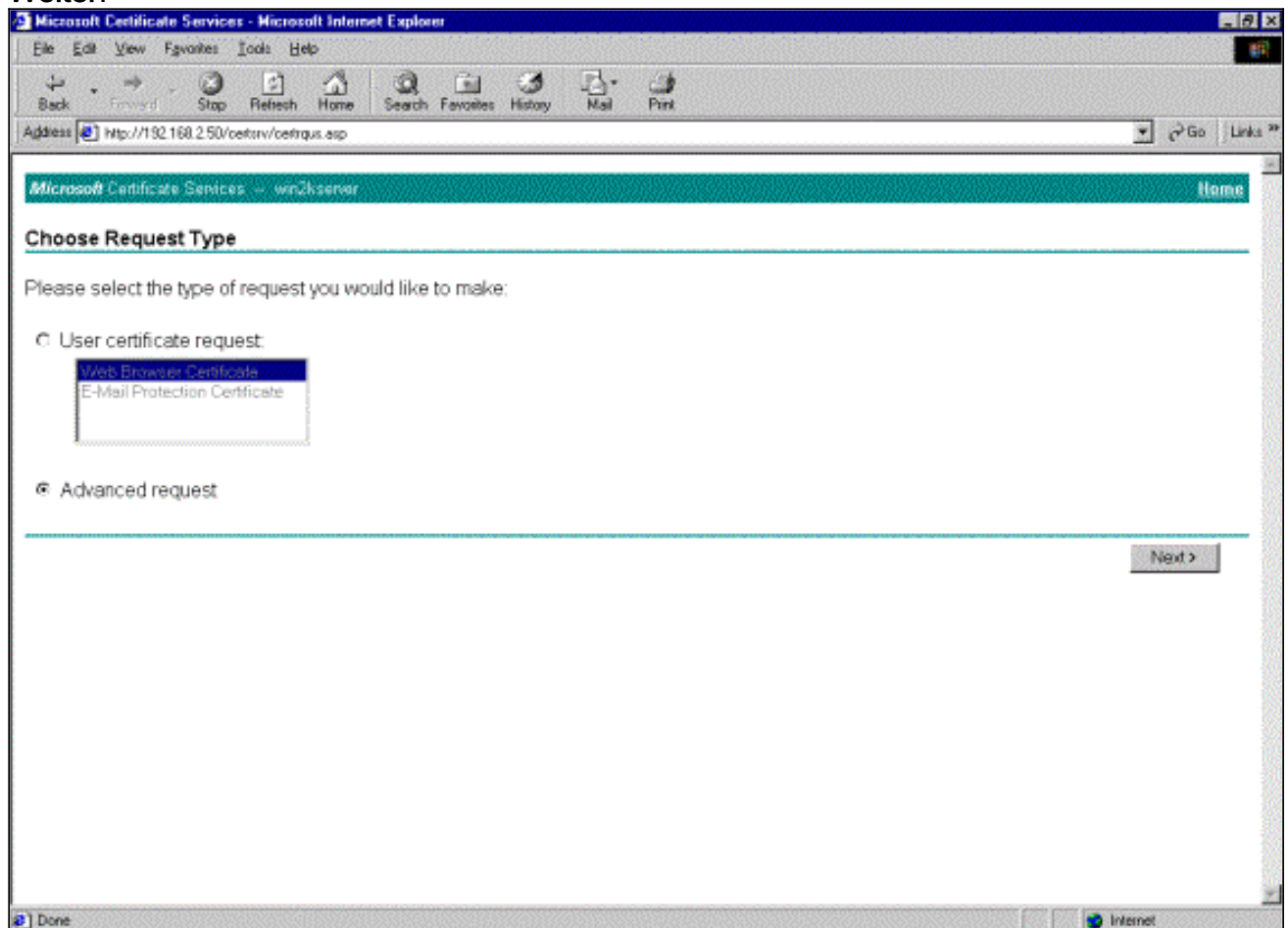
überprüfen.

10. Stellen Sie den CA-Server (Certification Authority) und die VPN-Client-Schnittstellen gleichzeitig ein, um die Anfrage zu senden.
11. Wählen Sie **Zertifikat anfordern aus**, und klicken Sie auf **Weiter** auf dem CA-



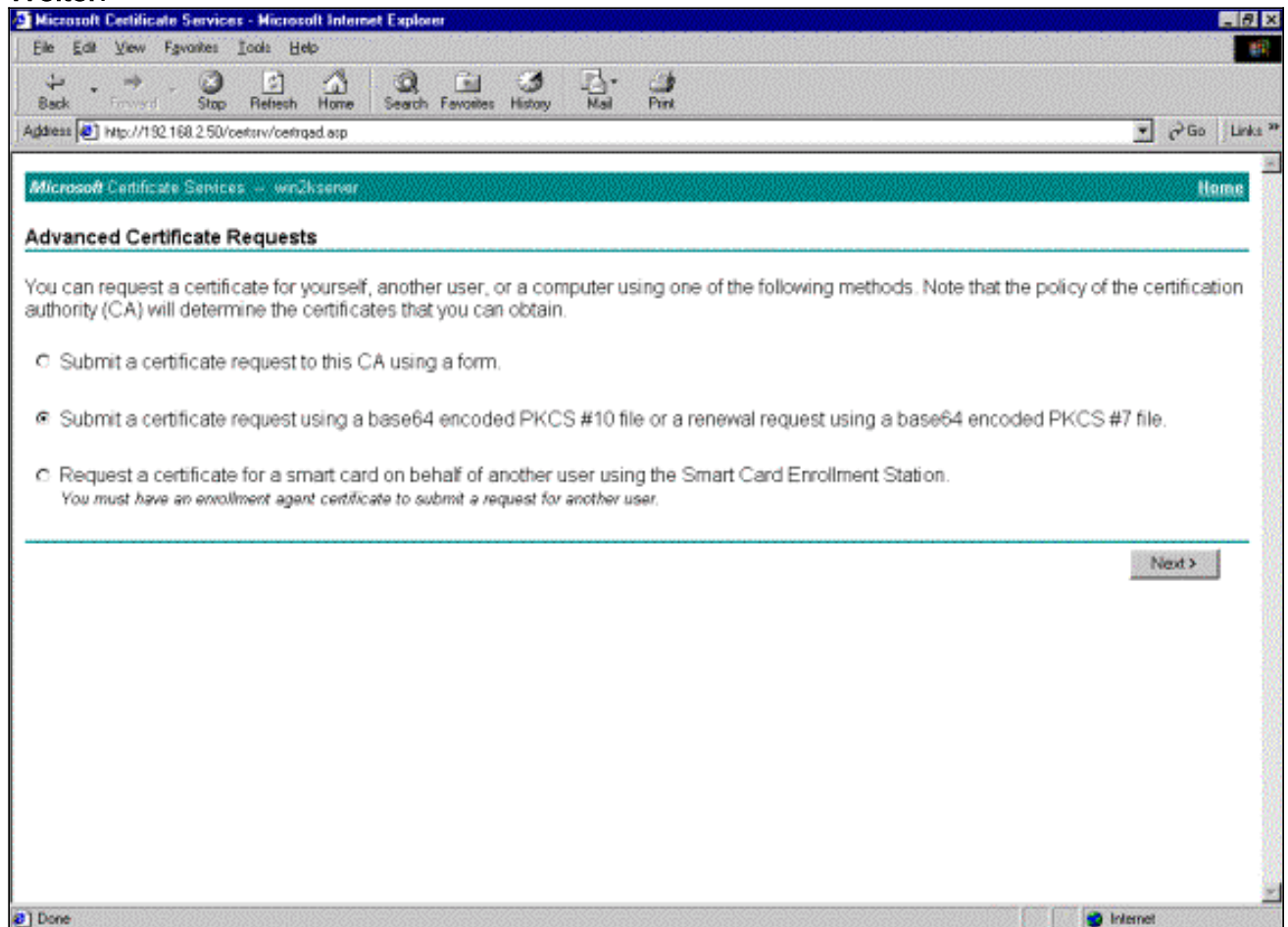
Server.

12. Wählen Sie **Erweiterte Anforderung** für die Art der Anfrage aus, und klicken Sie auf **Weiter**.

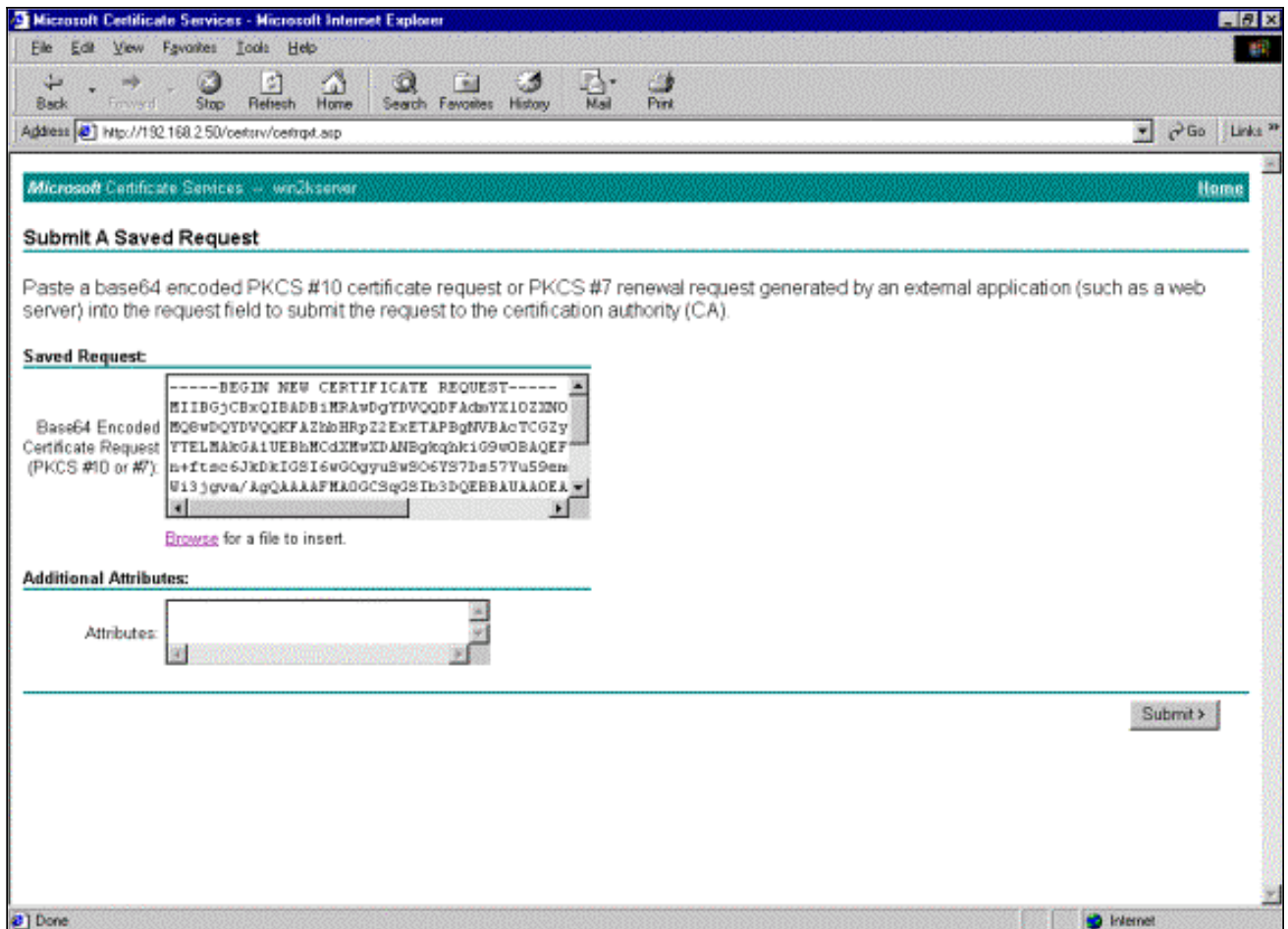


13. Wählen Sie **unter** Erweiterte Zertifikatsanforderungen **eine** unter **Base64 verschlüsselte PKCS #10-Datei** oder eine **Verlängerungsanfrage** unter Verwendung einer **Base64-kodierten PKCS #7-Datei** einreichen aus, und klicken Sie dann auf

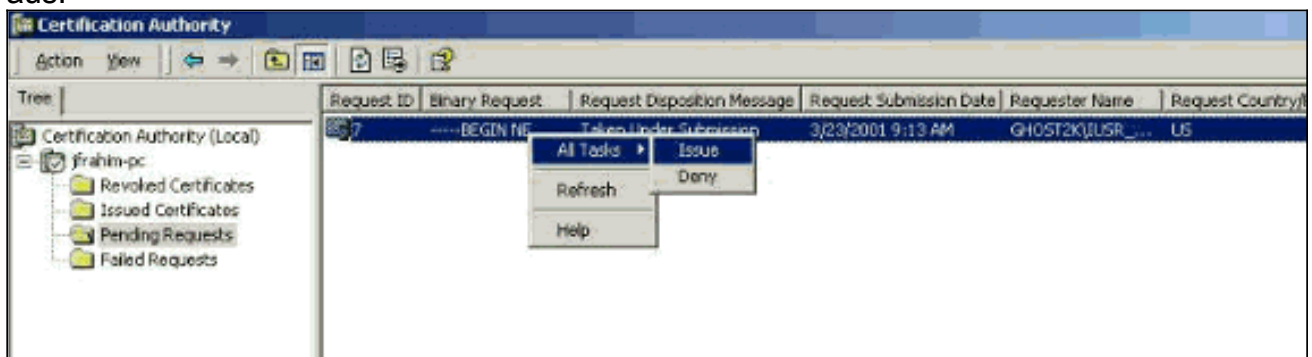
Weiter.



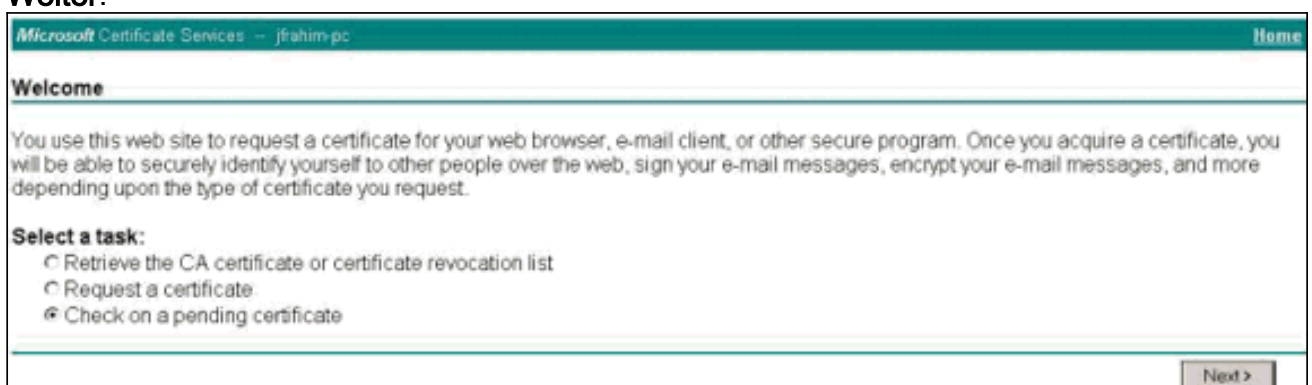
14. Markieren Sie die VPN Client-Anforderungsdatei, und fügen Sie sie unter "Gespeicherte Anforderung" auf den CA-Server ein. Klicken Sie anschließend auf **Senden**.



15. Stellen Sie auf dem CA-Server das Identitätszertifikat für die VPN-Client-Anforderung aus.

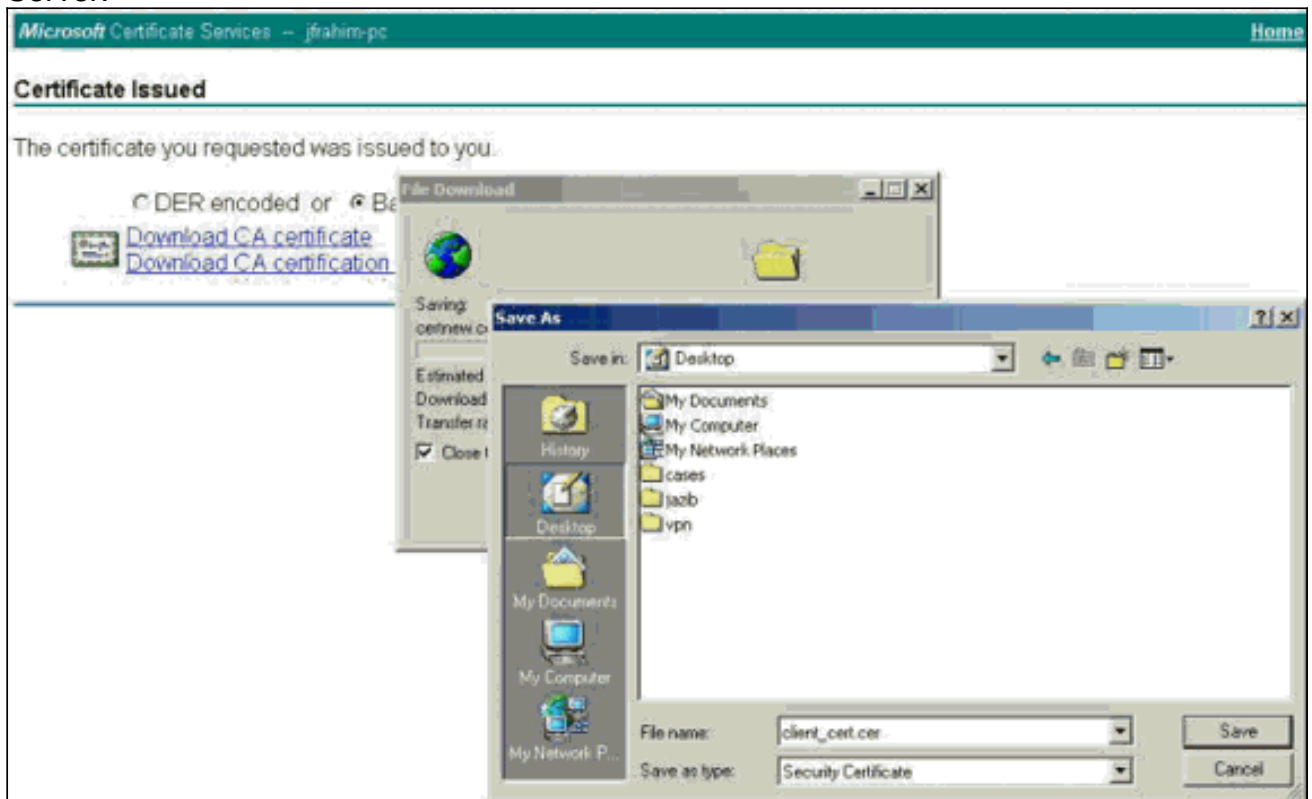


16. Laden Sie die Root- und Identitätszertifikate auf den VPN-Client herunter. Wählen Sie auf dem CA-Server die Option **Auf ausstehendem Zertifikat prüfen** aus, und klicken Sie dann auf **Weiter**.

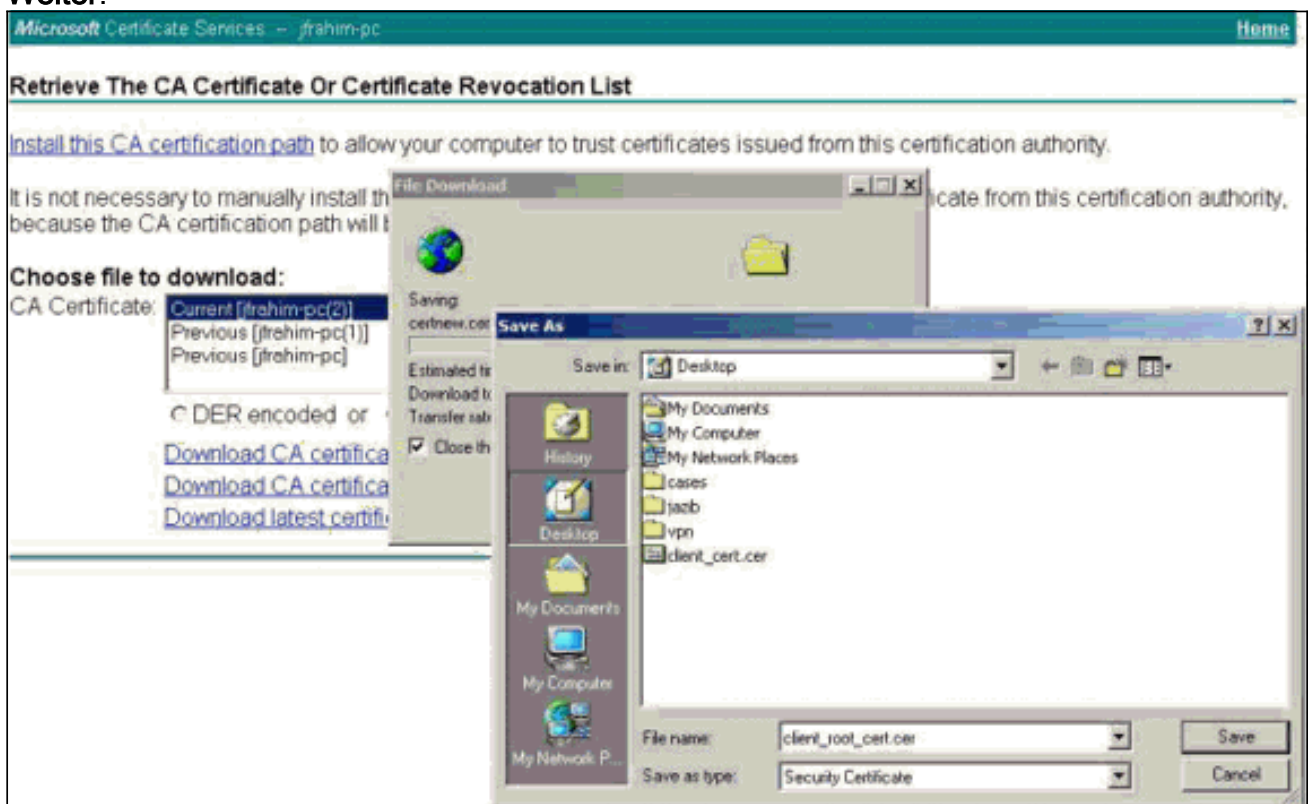


17. Wählen Sie **Base 64-verschlüsselt** aus. Klicken Sie dann auf **Zertifizierungsstellenzertifikat herunterladen** auf dem CA-

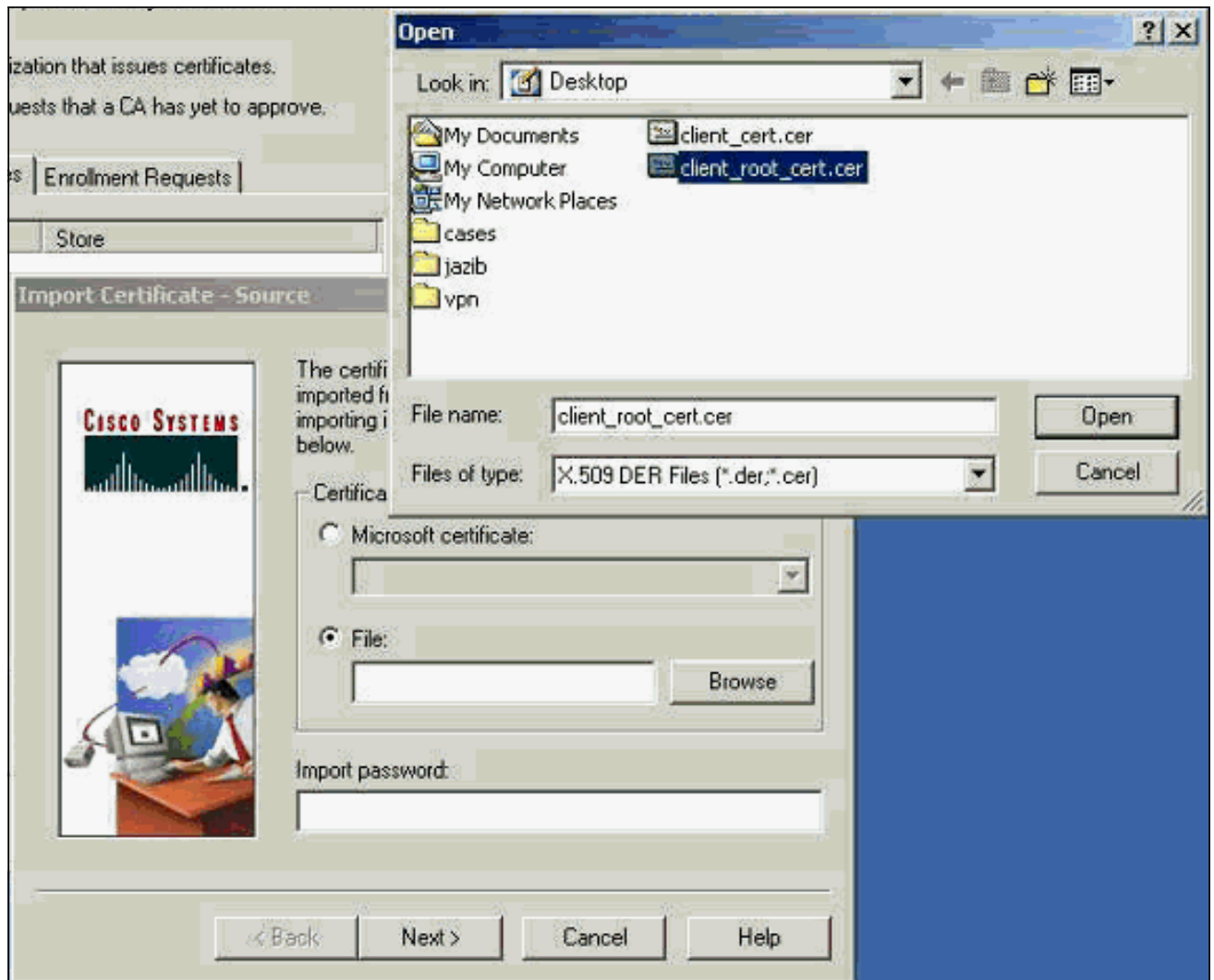
Server.



18. Wählen Sie eine Datei aus, die Sie von der Seite Zertifikat oder Zertifikatswiderrufliste abrufen möchten, um das Stammzertifikat auf dem CA-Server abzurufen. Klicken Sie anschließend auf **Weiter**.



19. Wählen Sie **Certificate Manager > CA Certificate > Import on the VPN Client** aus, und wählen Sie dann die Root CA-Datei aus, um die Root- und Identitätszertifikate zu installieren.

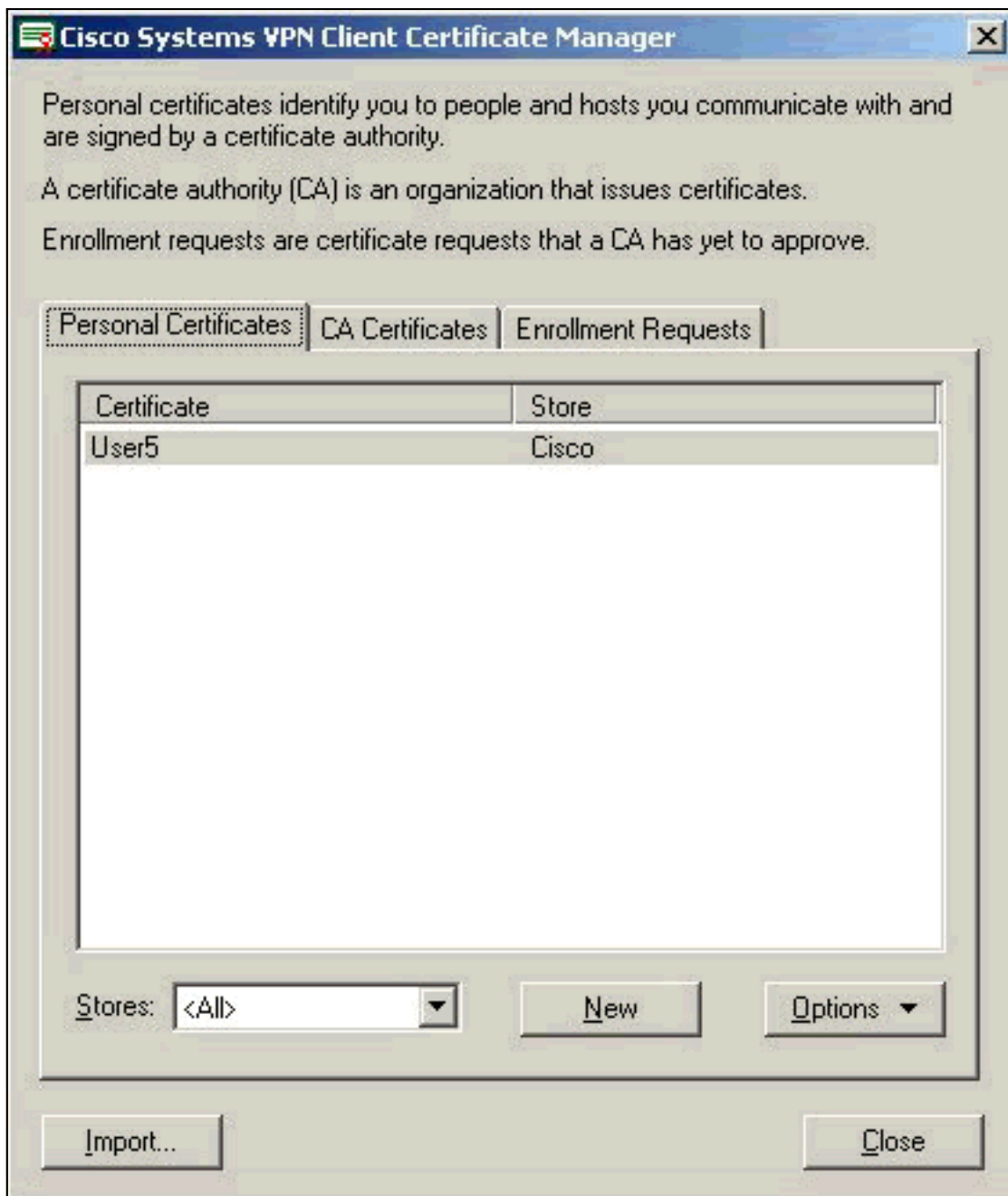


20. Wählen Sie **Zertifikatsmanager > Persönliche Zertifikate > Importieren aus**, und wählen Sie die Identitätszertifikatdatei



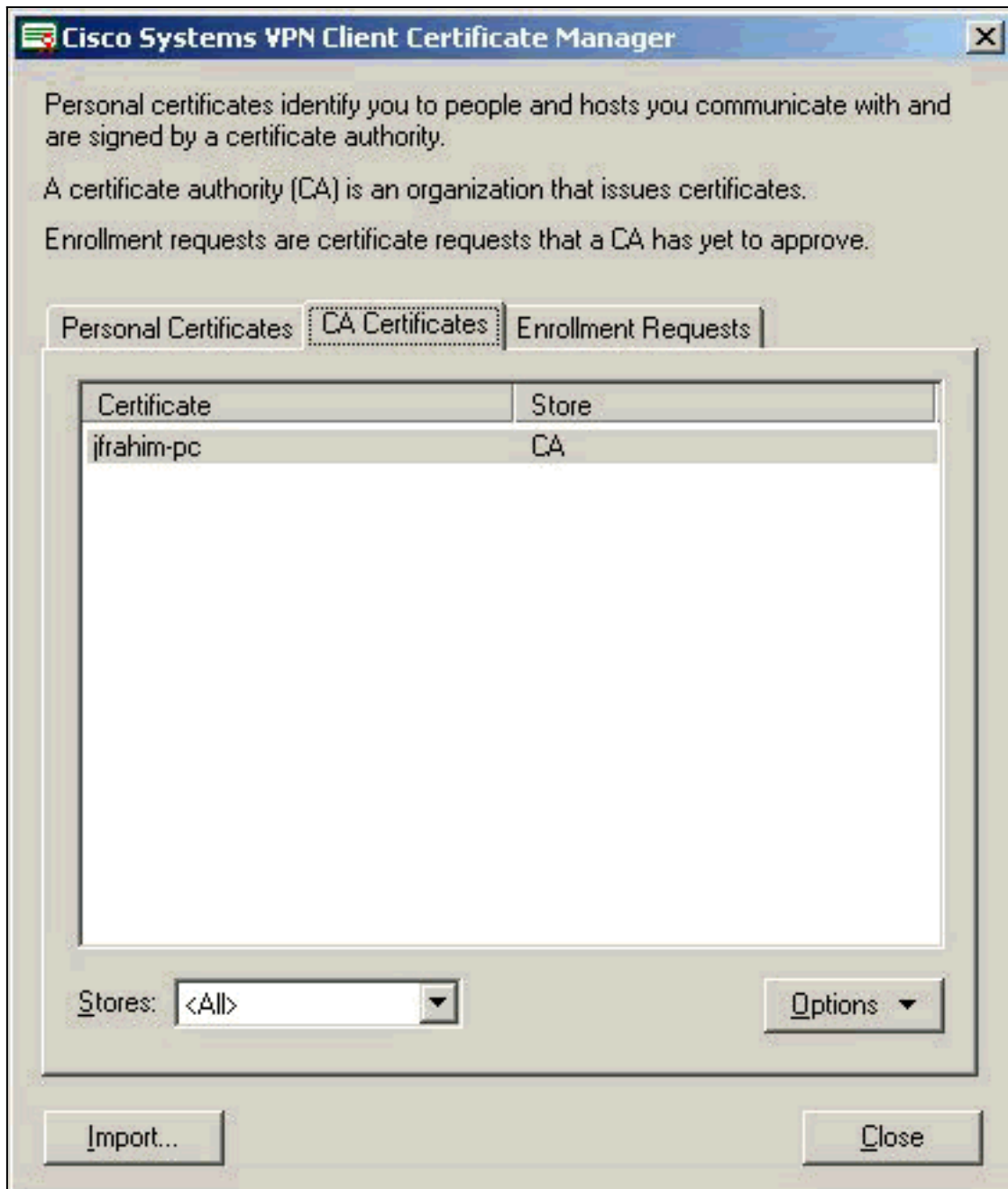
aus.

21. Stellen Sie sicher, dass das Identitätszertifikat auf der Registerkarte "Persönliche Zertifikate" angezeigt



wird.

22. Stellen Sie sicher, dass das Stammzertifikat auf der Registerkarte Zertifizierungsstellen angezeigt



wird.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Wenn Sie versuchen, sich beim Microsoft CA Server anzumelden, kann diese Fehlermeldung generiert werden.

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

Wenn Sie diese Fehlermeldung erhalten, finden Sie weitere Informationen in den Microsoft CA-Protokollen oder in diesen Ressourcen.

- [Windows kann keine Zertifizierungsstelle finden, die die Anforderung verarbeitet.](#)
- [XCCC: Wenn Sie ein Zertifikat für sichere Konferenzen anfordern, wird die Fehlermeldung "Ihre Zertifikatsanforderung wurde abgelehnt" angezeigt.](#)

Zugehörige Informationen

- [IPsec-Aushandlung/IKE-Protokolle](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)