VPN-client 3.x configureren om een digitaal certificaat te verkrijgen

Inhoud

Inleiding

Dit document toont aan hoe u de Cisco VPN-client 3.x kunt configureren om een digitaal certificaat te verkrijgen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op een PC waar Cisco VPN-client 3.x actief is.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

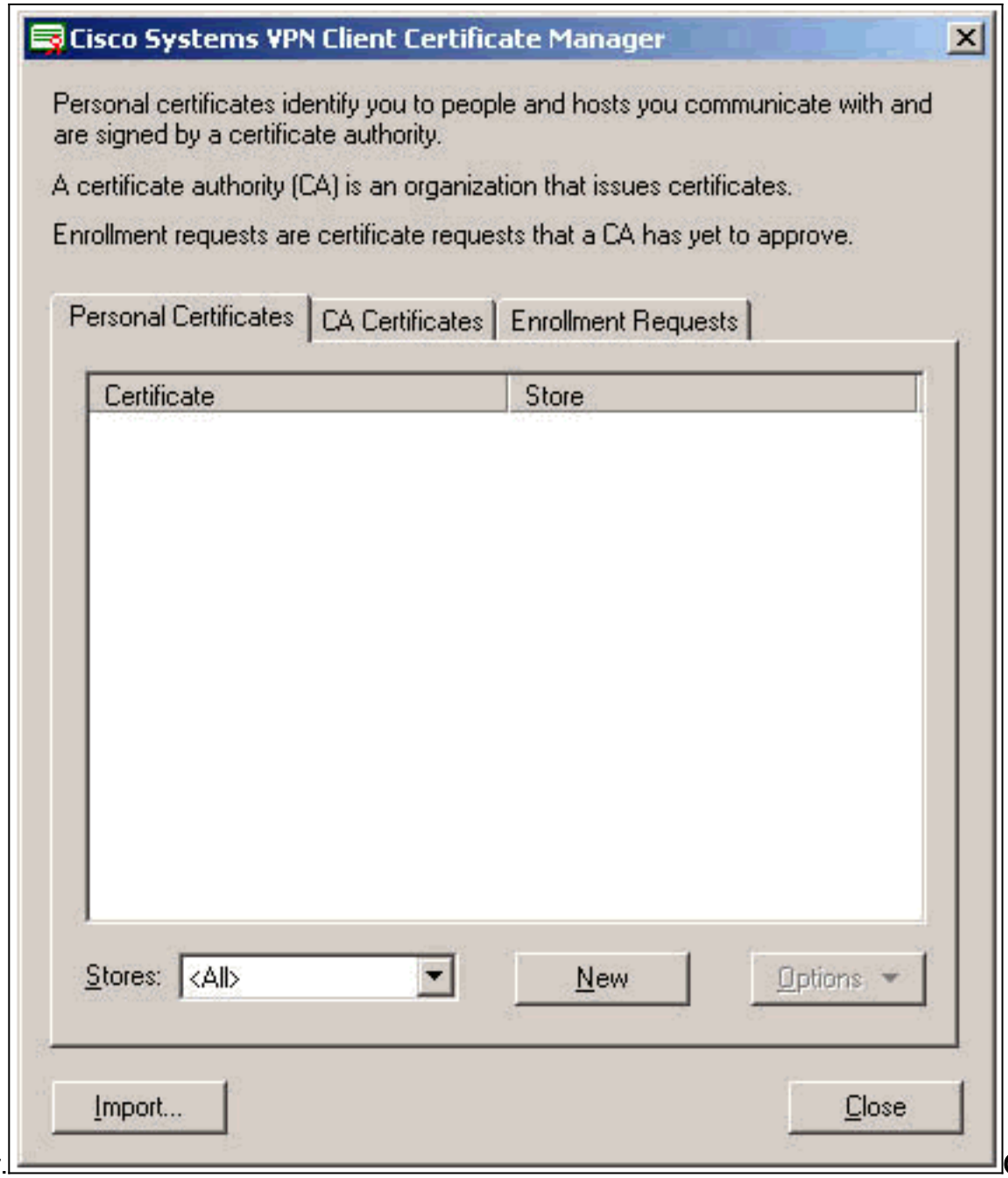
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

VPN-client configureren

Volg deze stappen om de VPN-client te configureren.

1. Selecteer **Start > Programma's > Cisco Systems Inc. VPN-client > certificaatbeheer** om VPN-clientcertificaatbeheer te
   starten.

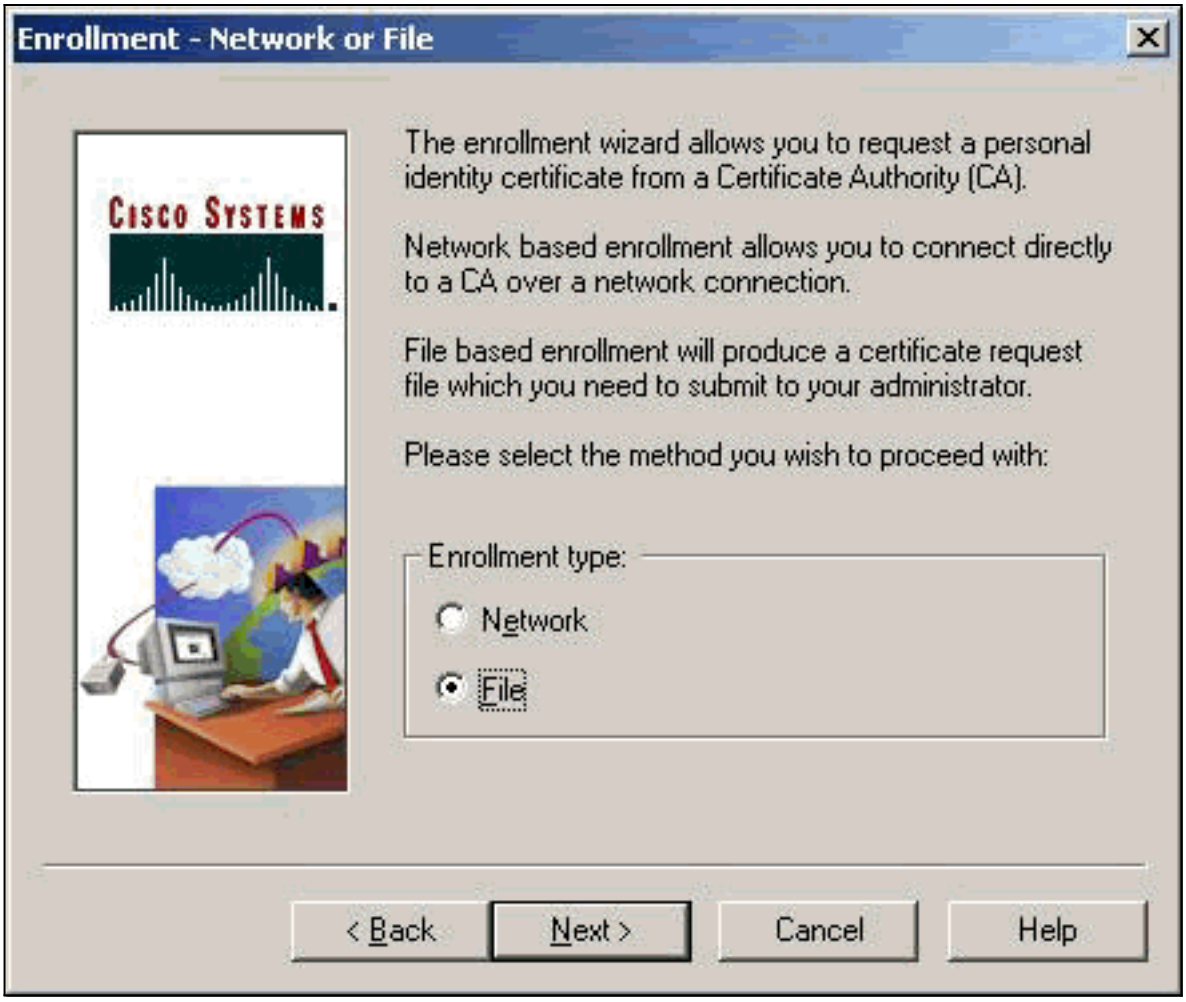
2. Selecteer het tabblad Persoonlijke certificaten en klik op



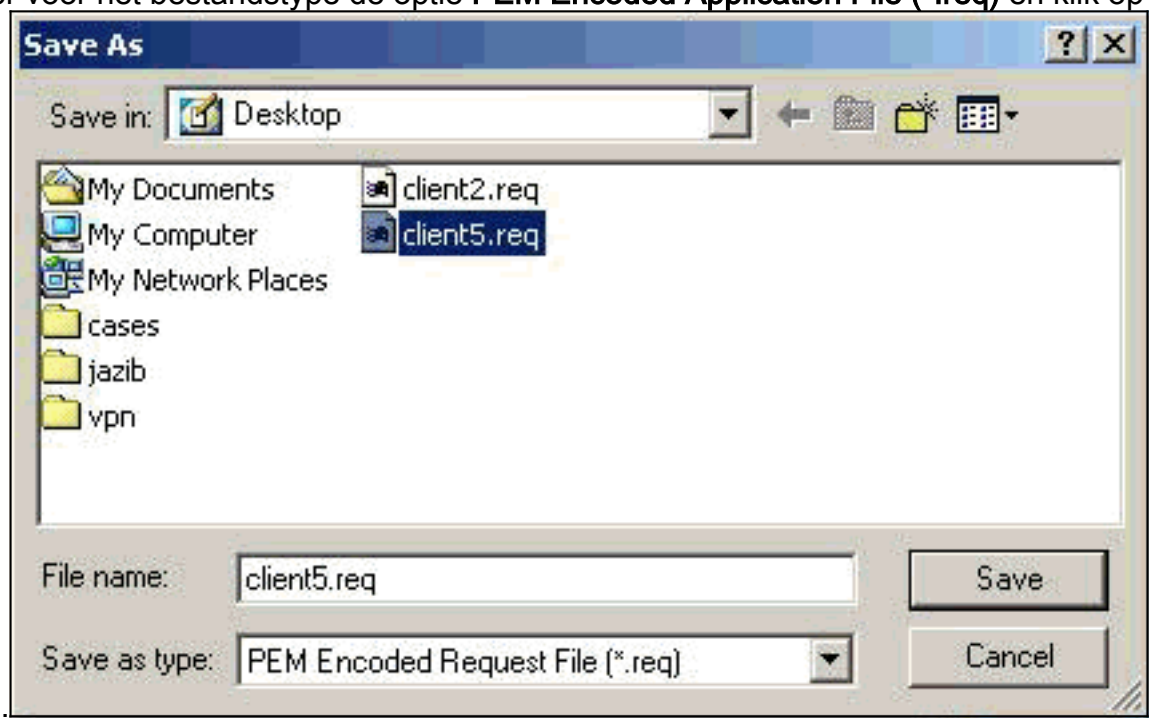
Nieuw.**Opmerking:** Machinecertificaten om gebruikers voor VPN-verbindingen te authentiseren kunnen niet met IPsec worden uitgevoerd.

3. Wanneer de VPN-client u om een wachtwoord vraagt, specificeert u een wachtwoord ter bescherming van het certificaat. Elke handeling waarvoor toegang tot de privé-toets van het certificaat vereist is, vereist dat het gespecificeerde wachtwoord wordt voortgezet.

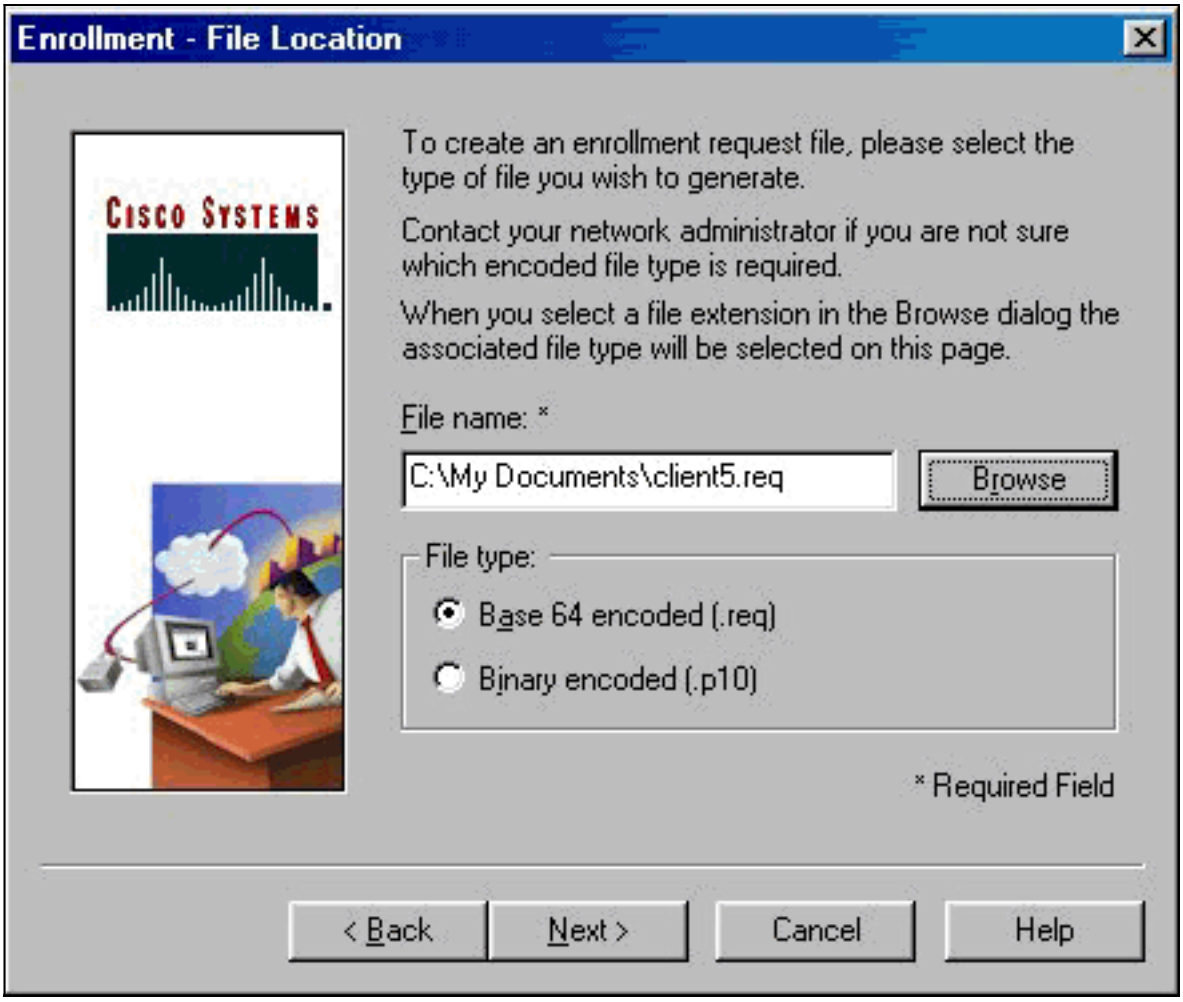
4. Selecteer **Bestand** om een certificaat aan te vragen met de PKCS #10-indeling op de pagina Inschrijven. Klik op
Volgende.



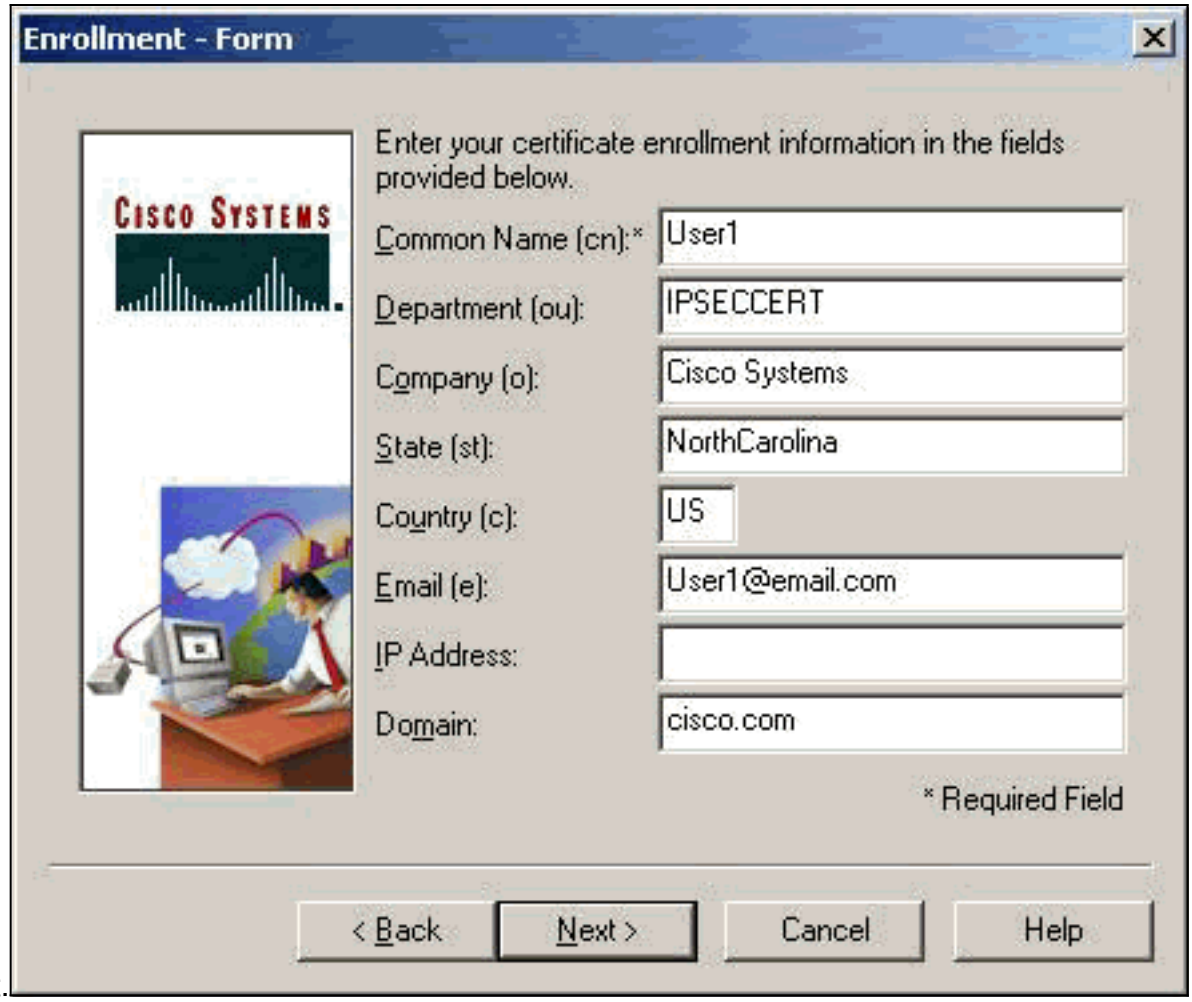
5. Klik op **Bladeren** en specificeer een bestandsnaam voor het bestand met certificaataanvraag. Selecteer voor het bestandstype de optie **PEM Encoded Application File (*.req)** en klik op **Opslaan**.



6. Klik op **Volgende** op de pagina VPN-clientinschrijving.

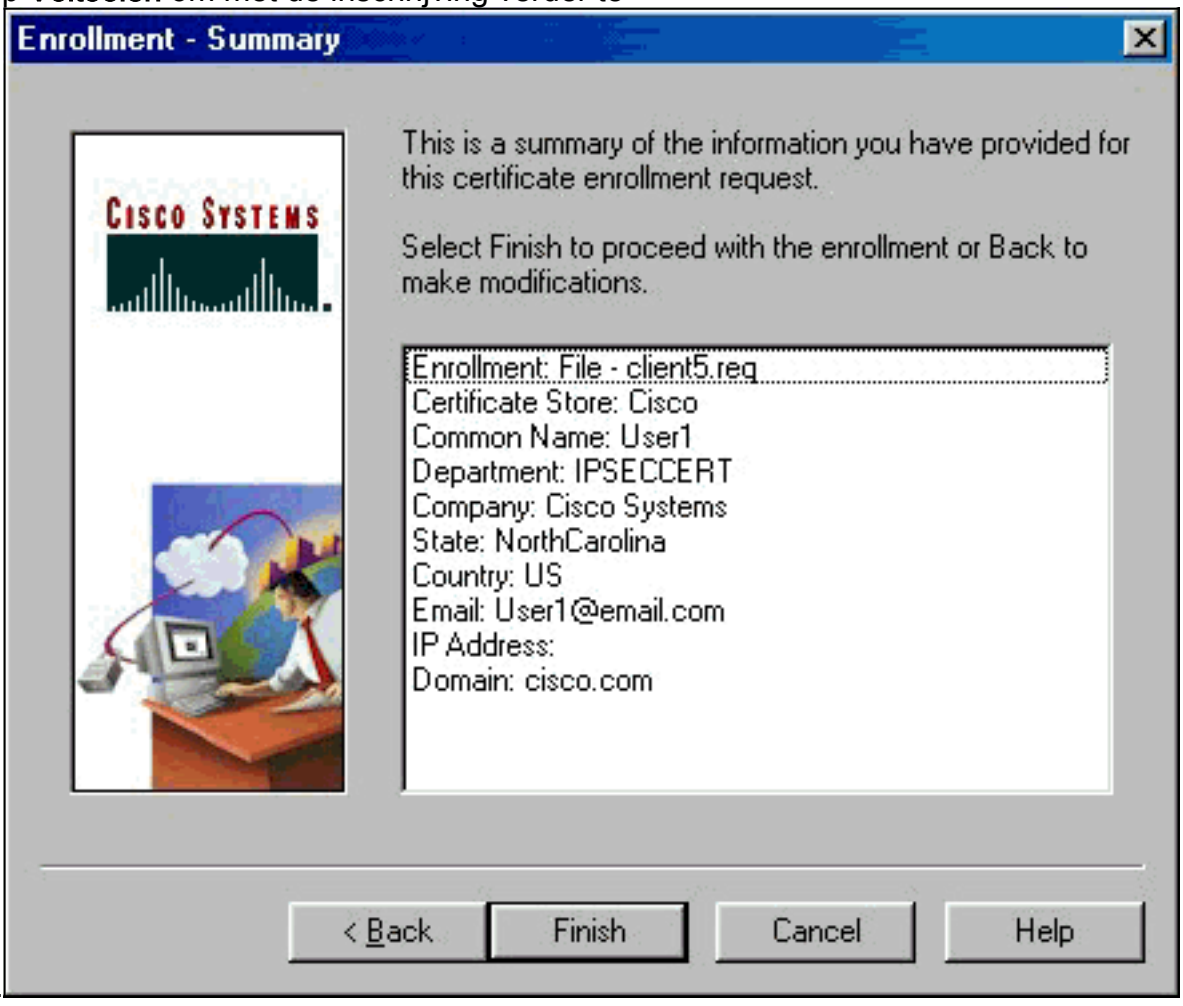


7. Vul de velden in op het Invoerformulier.Dit voorbeeld toont de velden:Gemeenschappelijke naam = Gebruiker1Departement = IPSECCERT (Dit moet overeenkomen met de organisatorische eenheid (OU) en de groepsnaam op de VPN 3000 Concentrator.)Bedrijf = Cisco-systemenStaat = NorthCarolinaLand = VSE-mail = User1@email.comIP-adres = (optioneel) gebruikt om het IP-adres op het certificaatverzoek te specificeren)Domain = cisco.comKlik op **Volgende** als u klaar



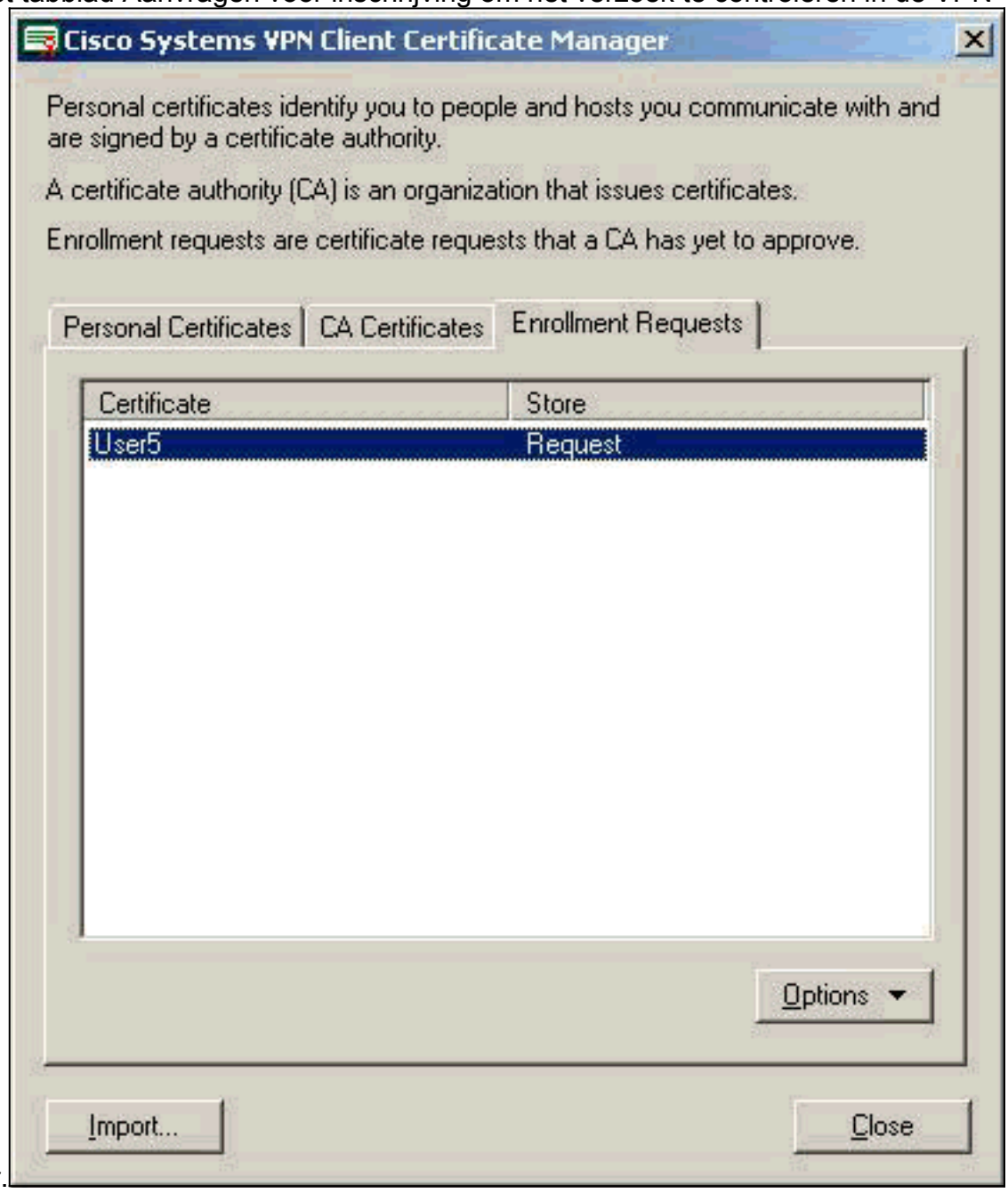
bent.

8. Klik op **Voltooien** om met de inschrijving verder te

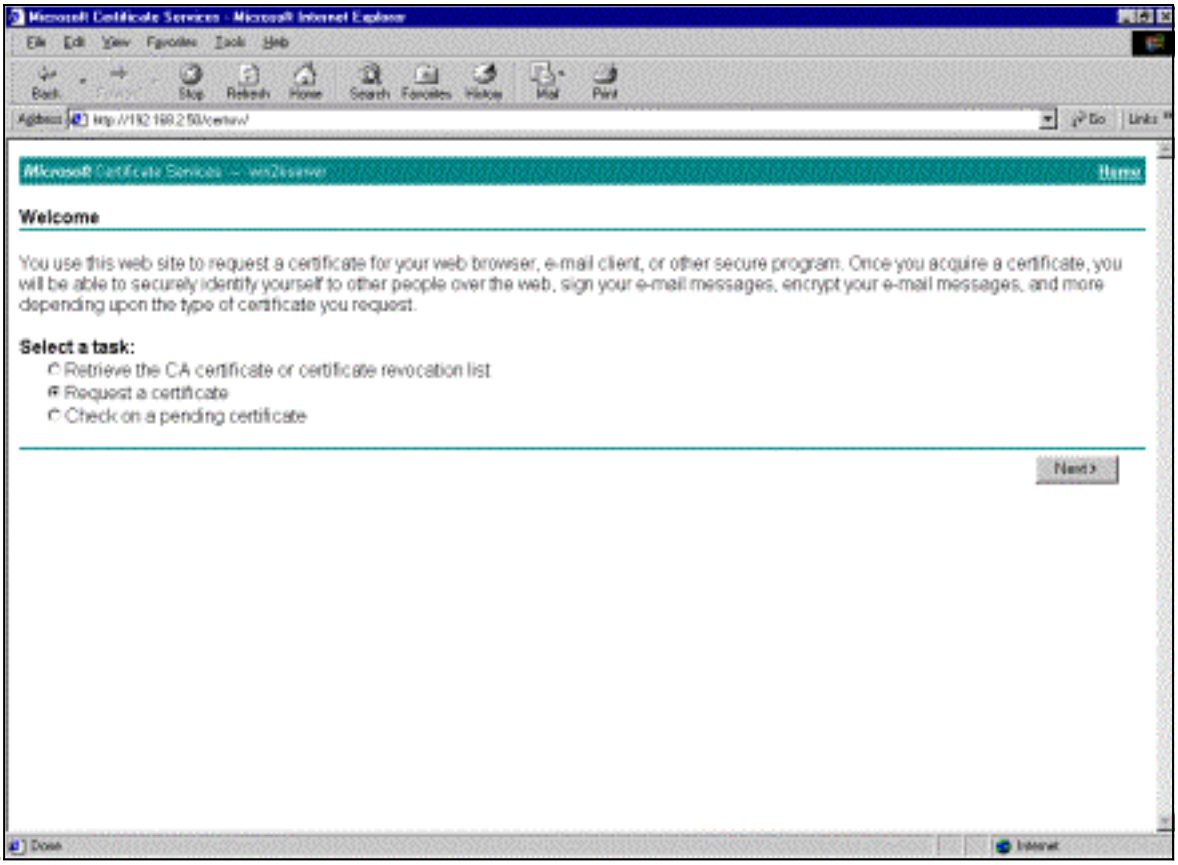


gaan.

9. Selecteer het tabblad Aanvragen voor inschrijving om het verzoek te controleren in de VPN-clientbeheer.

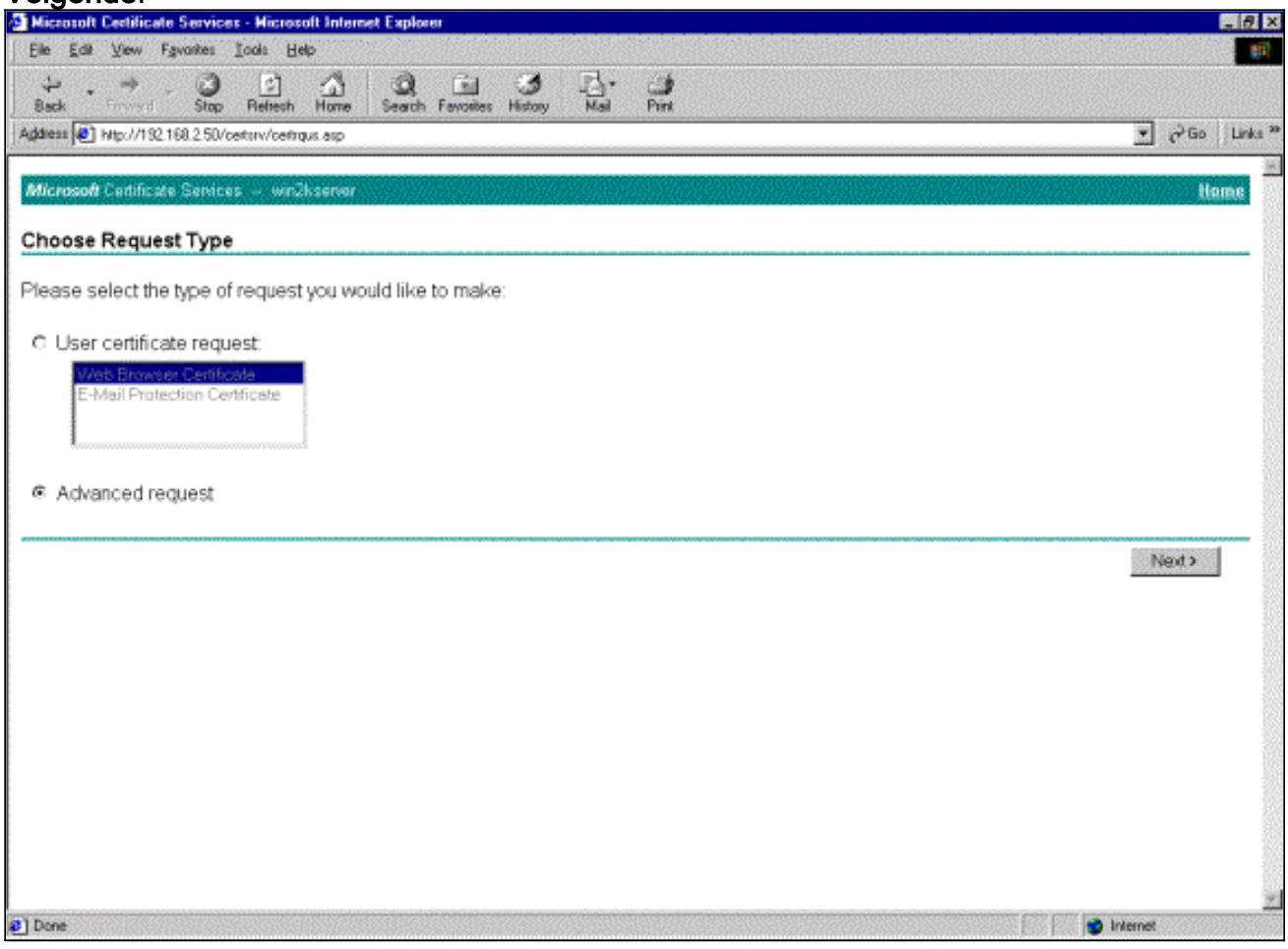


10. Breng de CA-server (Certified Authority) en de VPN-clientinterfaces tegelijkertijd aan om het verzoek in te dienen.
11. Selecteer **Aanvragen een certificaat** en klik op **Volgende** op de CA



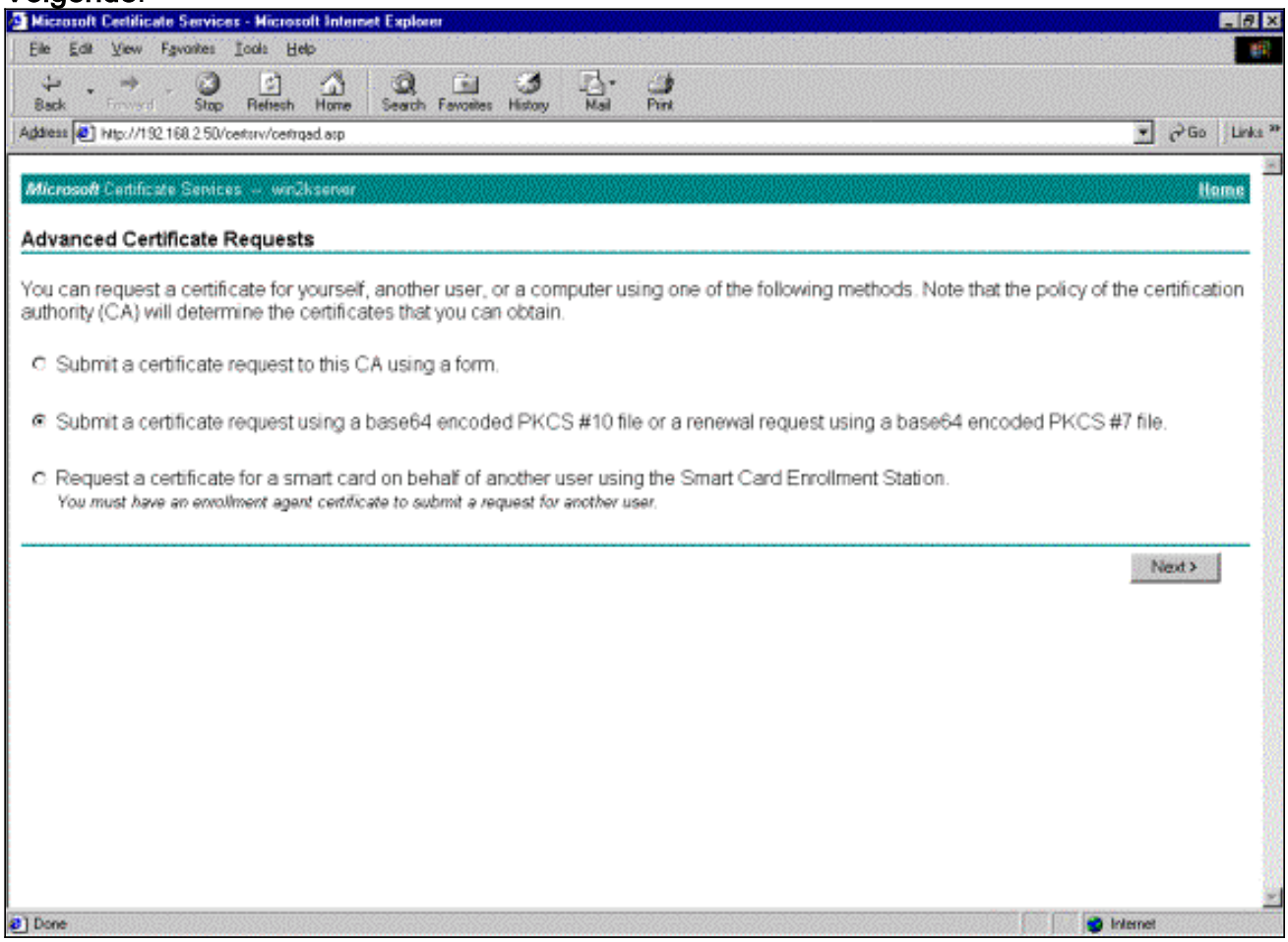
server.

12. Selecteer **Geavanceerd verzoek** voor het type verzoek en klik op **Volgende**.

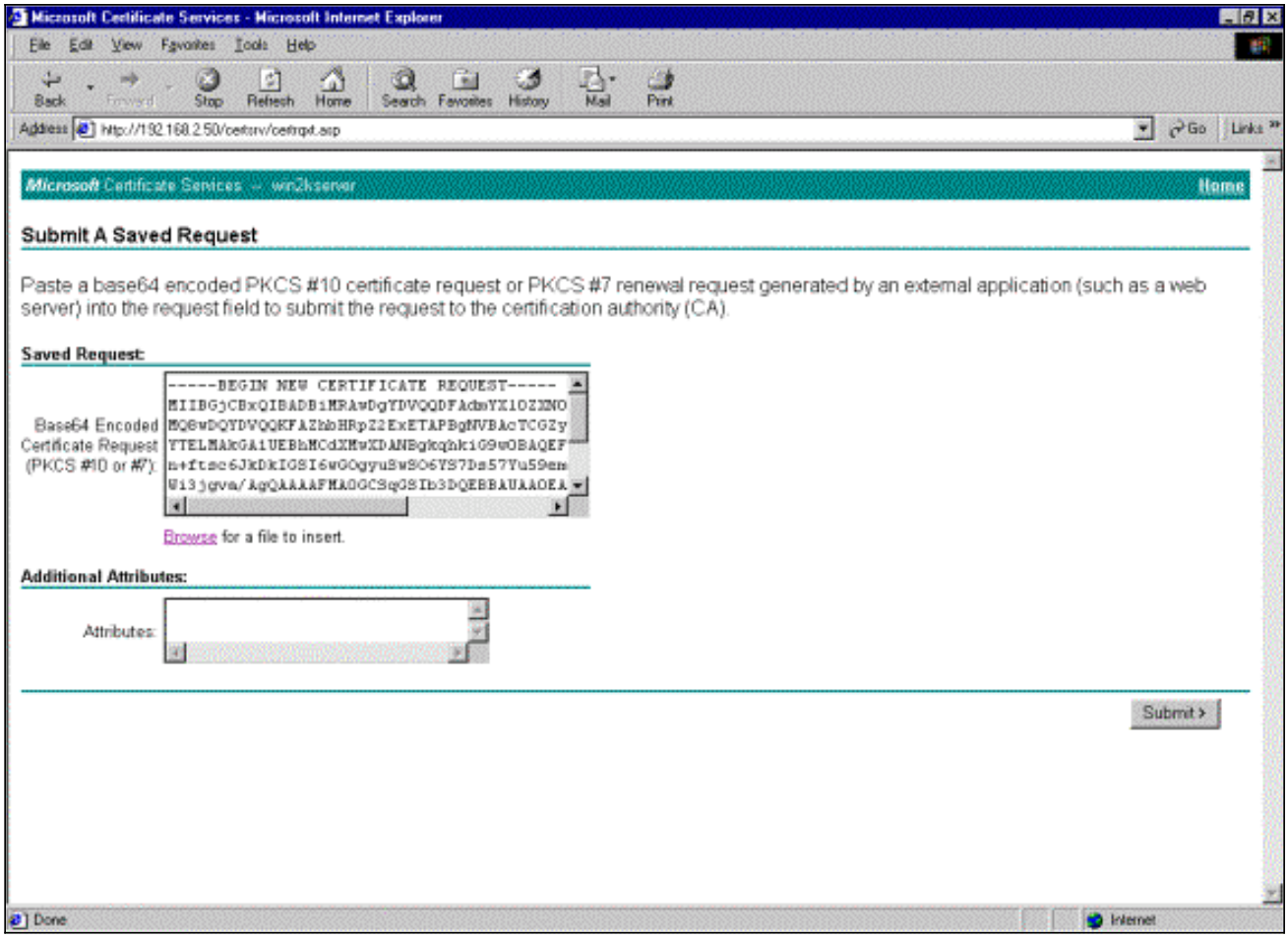


13. Selecteer **Een certificaataanvraag indienen met behulp van een Base64 gecodeerde PKCS #10-bestand of een vernieuwingsaanvraag met behulp van een Base64 gecodeerde PKCS #7-bestand** onder Geavanceerde certificaataanvragen en klik vervolgens op

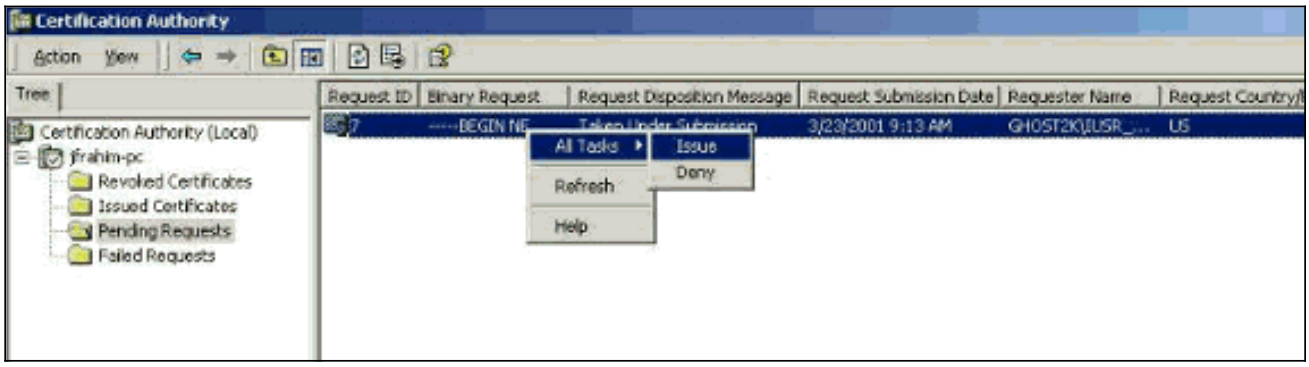
Volgende.



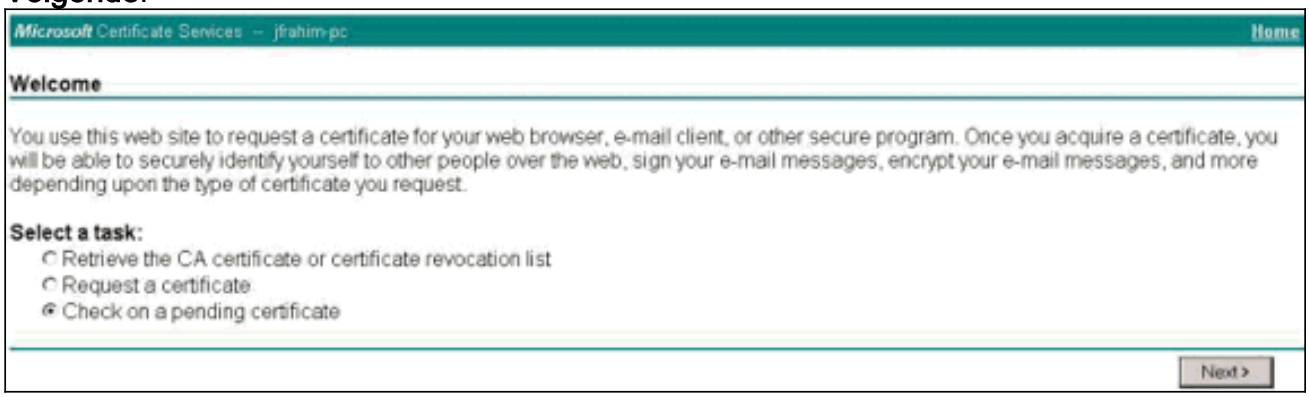
14. Markeer het VPN Client-aanvraagbestand en plak het op de CA-server onder Opgeslagen aanvraag. Klik vervolgens op
Inzenden.



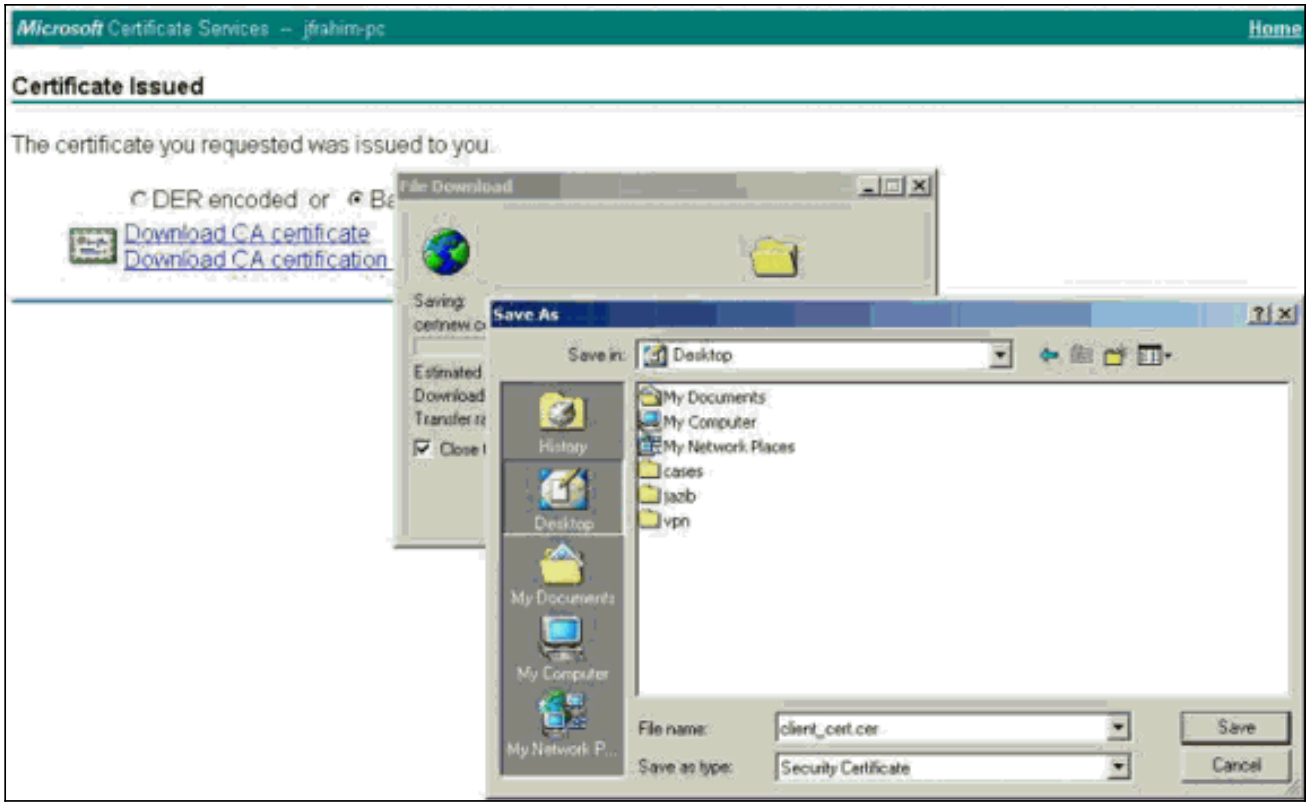
15. Geef op de CA server het identiteitsbewijs voor het verzoek van de VPN-client af.



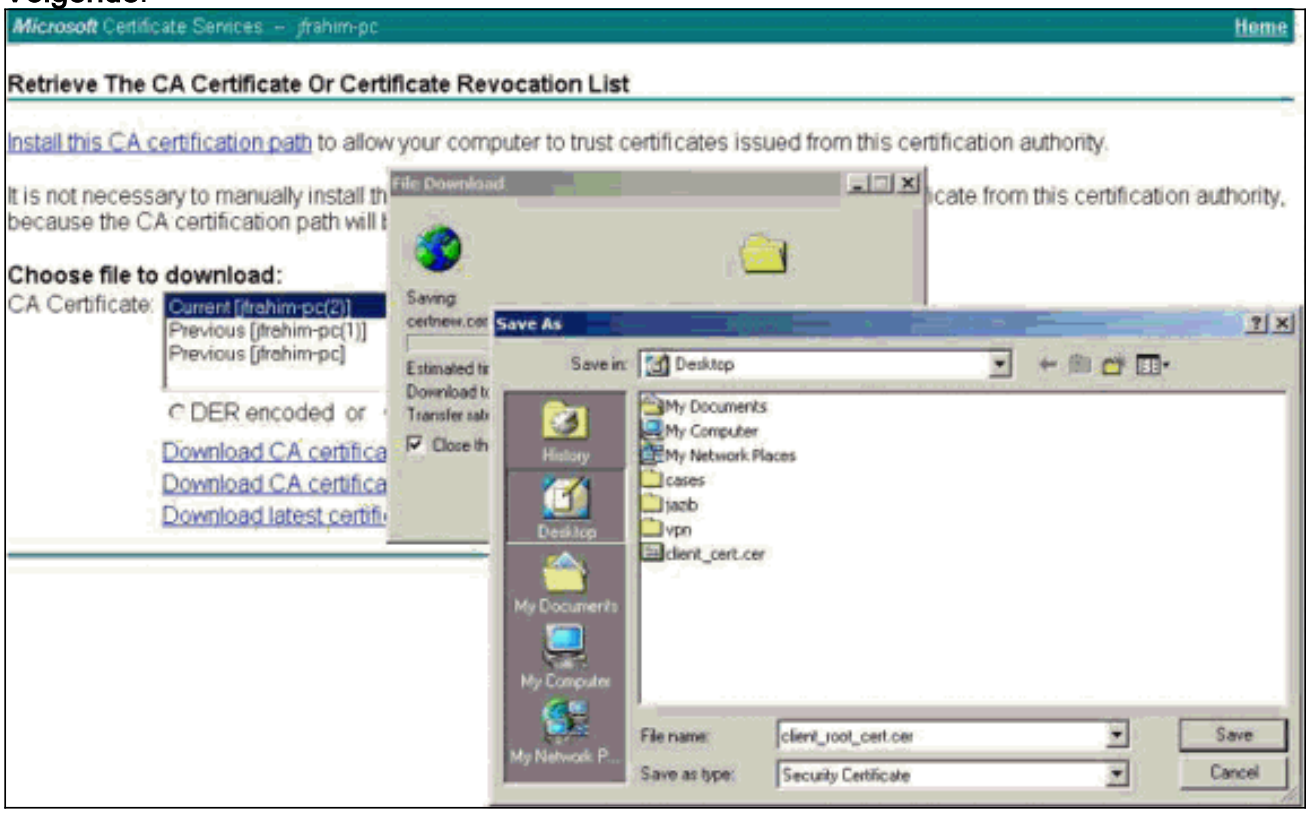
16. Download de wortel en de identiteit certificaten aan de VPN client. Selecteer op de CA-server **de optie controleren op een hangend certificaat** en klik vervolgens op **Volgende**.



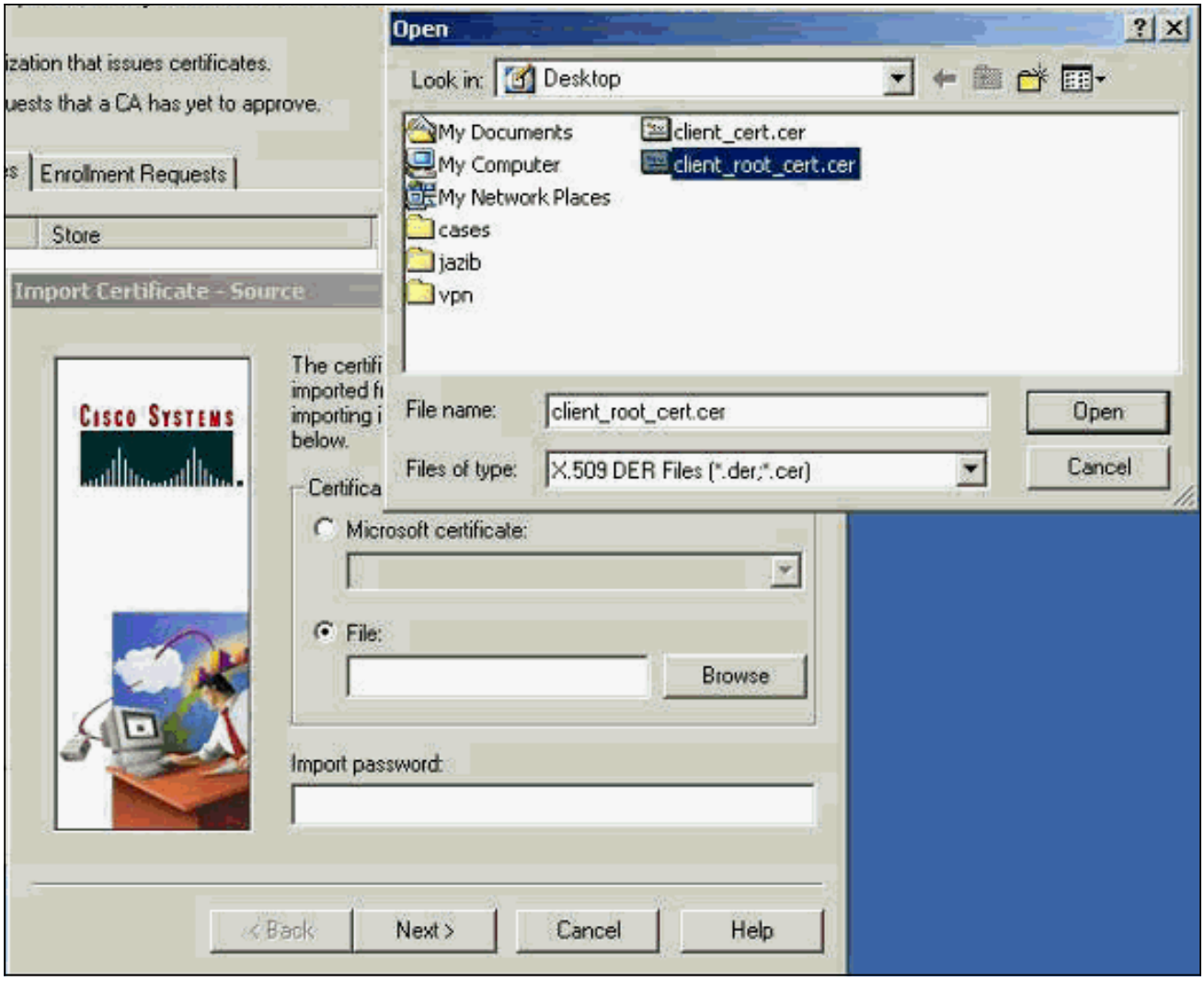
17. Selecteer **Base 64 gecodeerd**. Klik vervolgens op **CA-certificaat** op de CA-server.



18. Selecteer een bestand dat u kunt downloaden van de pagina CA-certificaat of lijst met certificaatherroeping om het basiscertificaat op de CA-server te verkrijgen. Klik op **Volgende**.

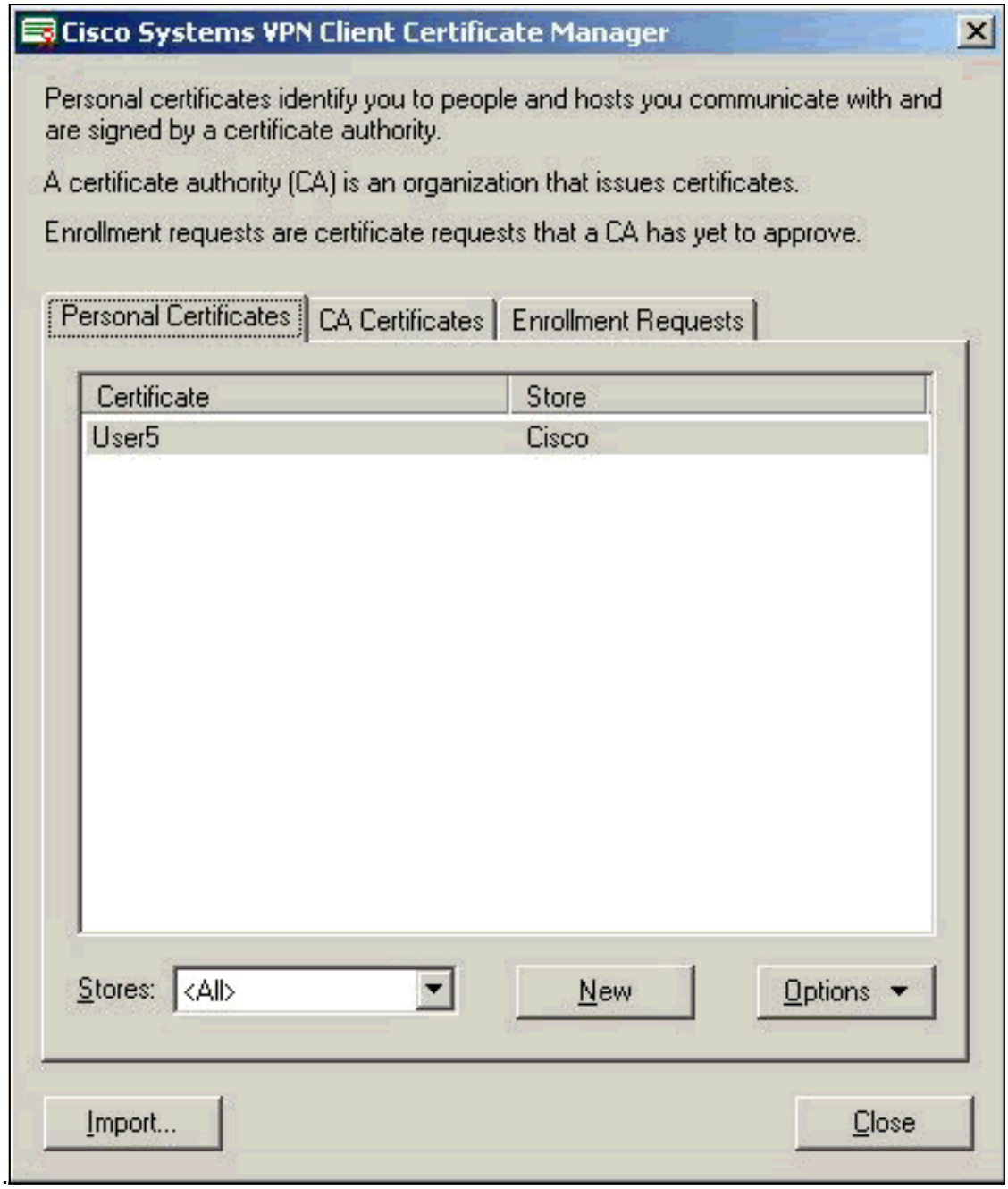


19. Selecteer **certificaatbeheer > CA-certificaat > Importeren op de VPN-client** en selecteer vervolgens het basisbestand CA-bestand voor het installeren van de wortel- en identiteitscertificaten.



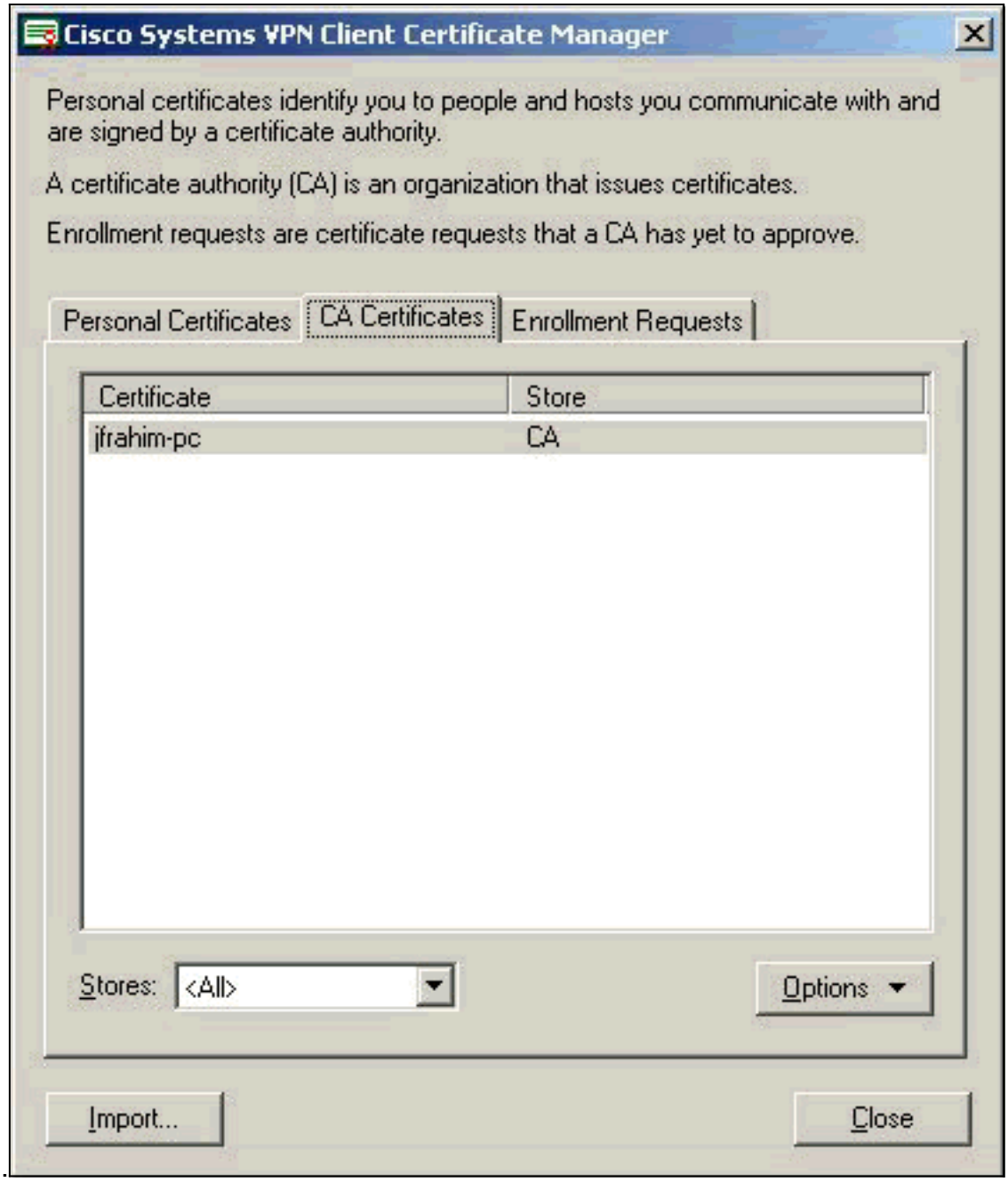
20. Selecteer **certificaatbeheer > Persoonlijke certificaten > Importeren** en kies het bestand met identiteitsbewijzen.

21. Zorg ervoor dat het identiteitsbewijs verschijnt onder het tabblad Persoonlijke



certificaten.

22. Zorg ervoor dat het basiscertificaat verschijnt onder het tabblad CA-

certificaten. 

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Wanneer u probeert zich in te schrijven bij de Microsoft CA Server, kan deze foutmelding worden gegenereerd.

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

Als u deze foutmelding ontvangt, raadpleegt u de Microsoft CA-logbestanden voor meer informatie of raadpleegt u deze bronnen voor meer informatie.

- Windows kan geen certificaatinstantie vinden die het verzoek verwerkt
- XCCC: Er wordt een foutmelding "Uw certificaataanvraag is afgewezen" weergegeven wanneer u een certificaat aanvraagt voor beveiligde conferencing

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems