Configurazione di VPN Client 3.x per ottenere un certificato digitale

Sommario

Introduzione

Questo documento mostra come configurare Cisco VPN Client 3.x per ottenere un certificato digitale.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato un PC con Cisco VPN Client 3.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

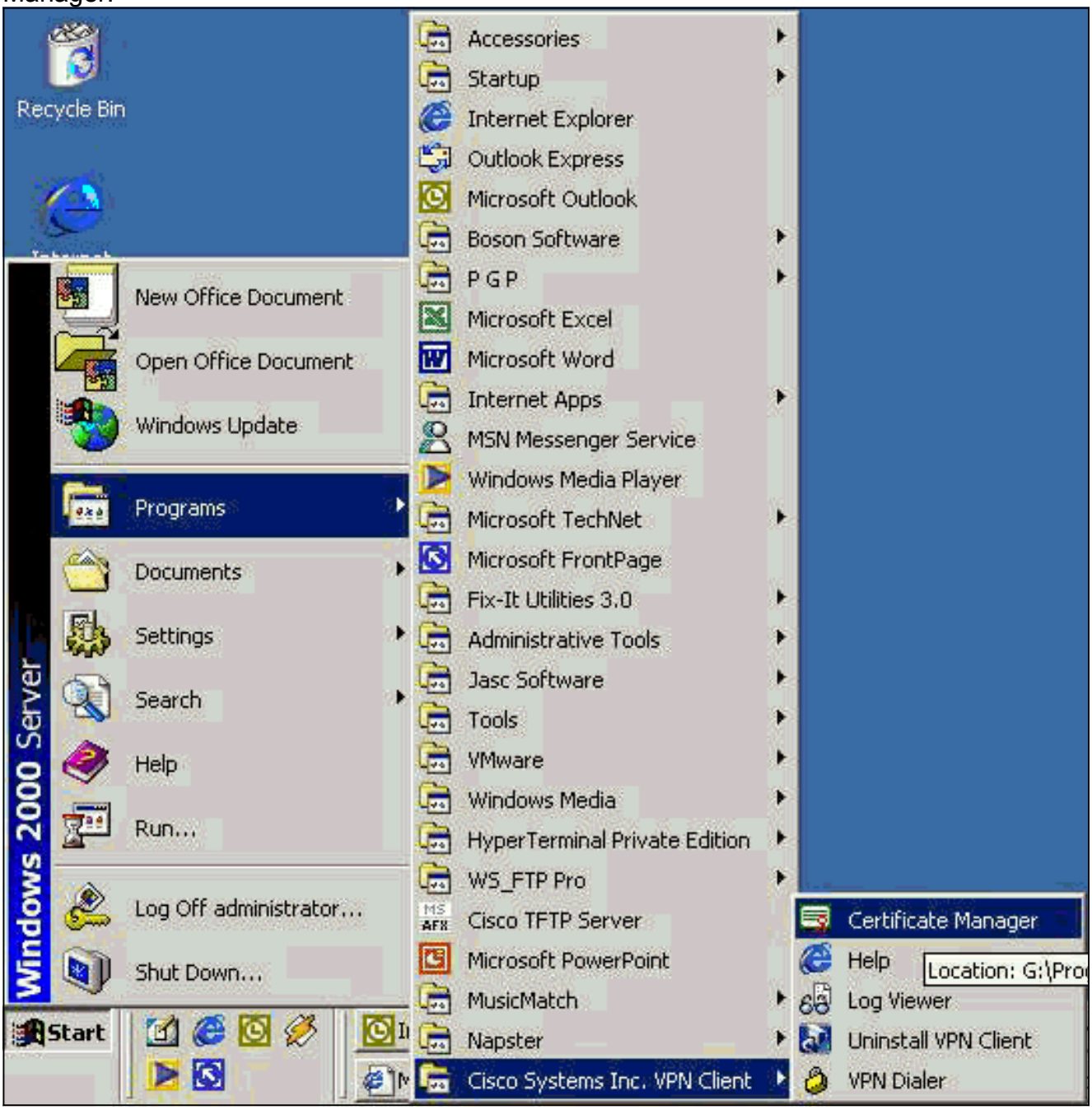
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

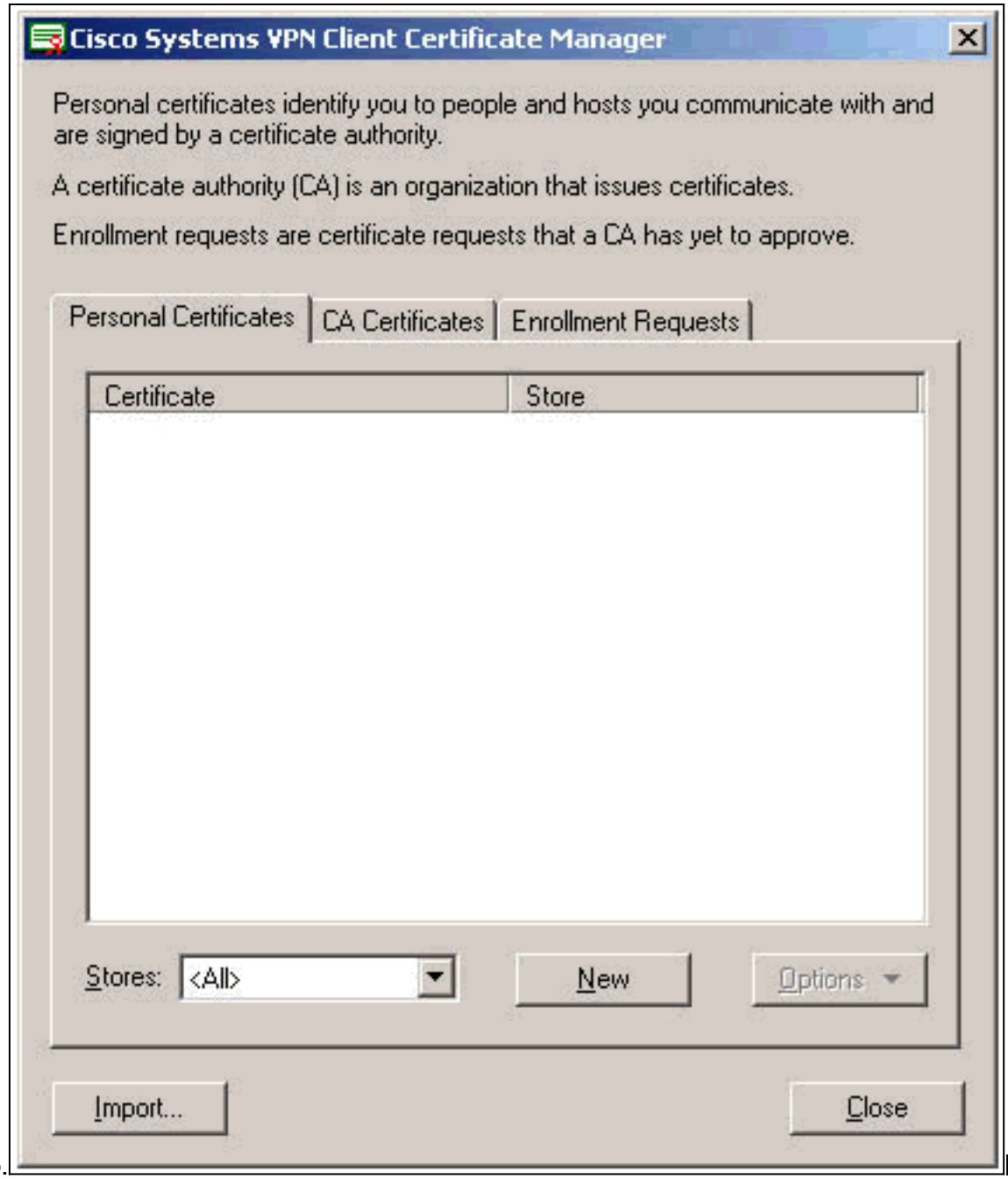
Configurare il client VPN

Completare questa procedura per configurare il client VPN.

1. Selezionare **Start > Programmi > Cisco Systems Inc. VPN client > Certificate Manager** per avviare VPN Client Certificate Manager.



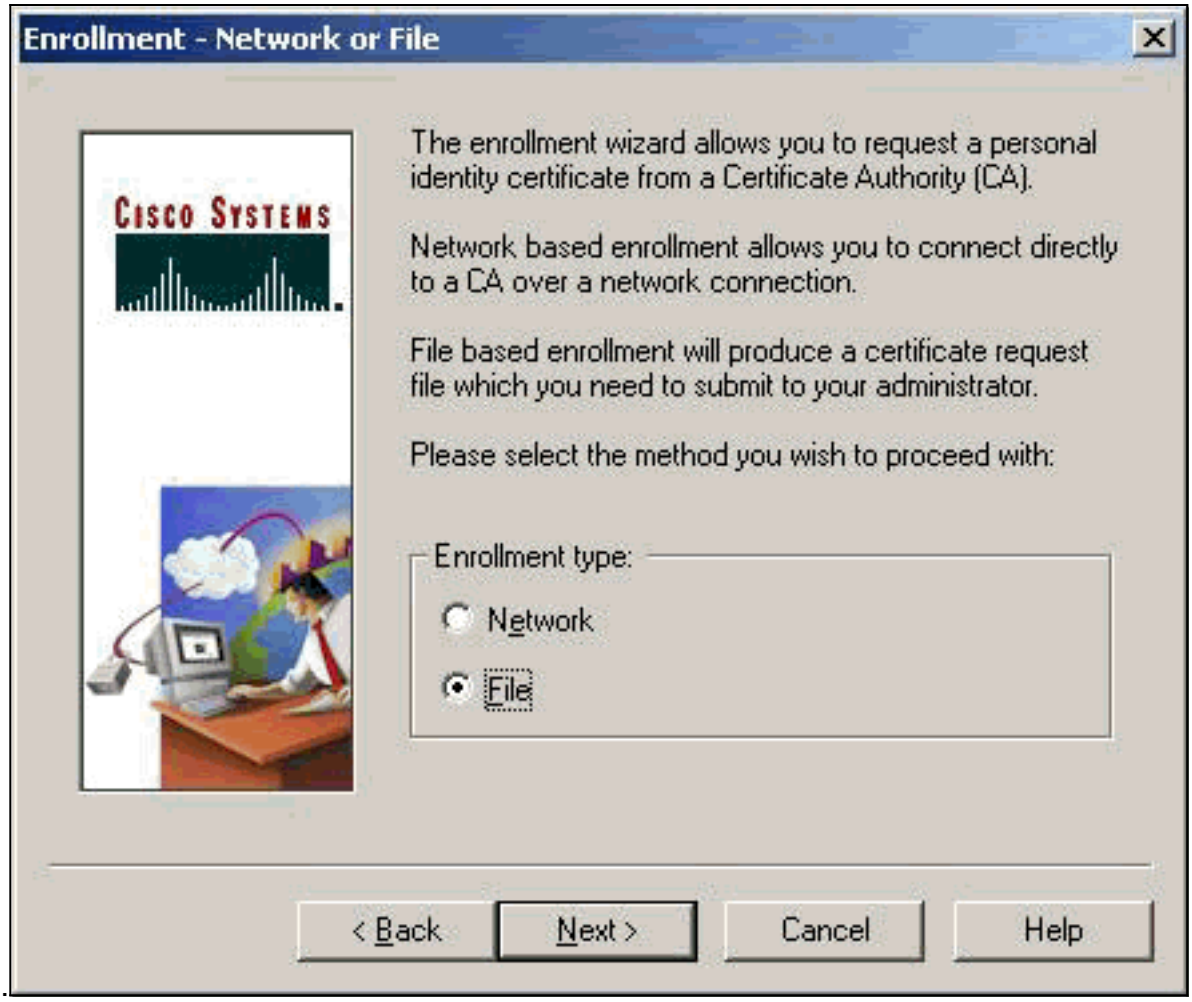
2. Selezionare la scheda Certificati personali e fare clic su



Nuovo.**Nota:** i certificati del computer per l'autenticazione degli utenti per le connessioni VPN non possono essere eseguiti con IPSec.

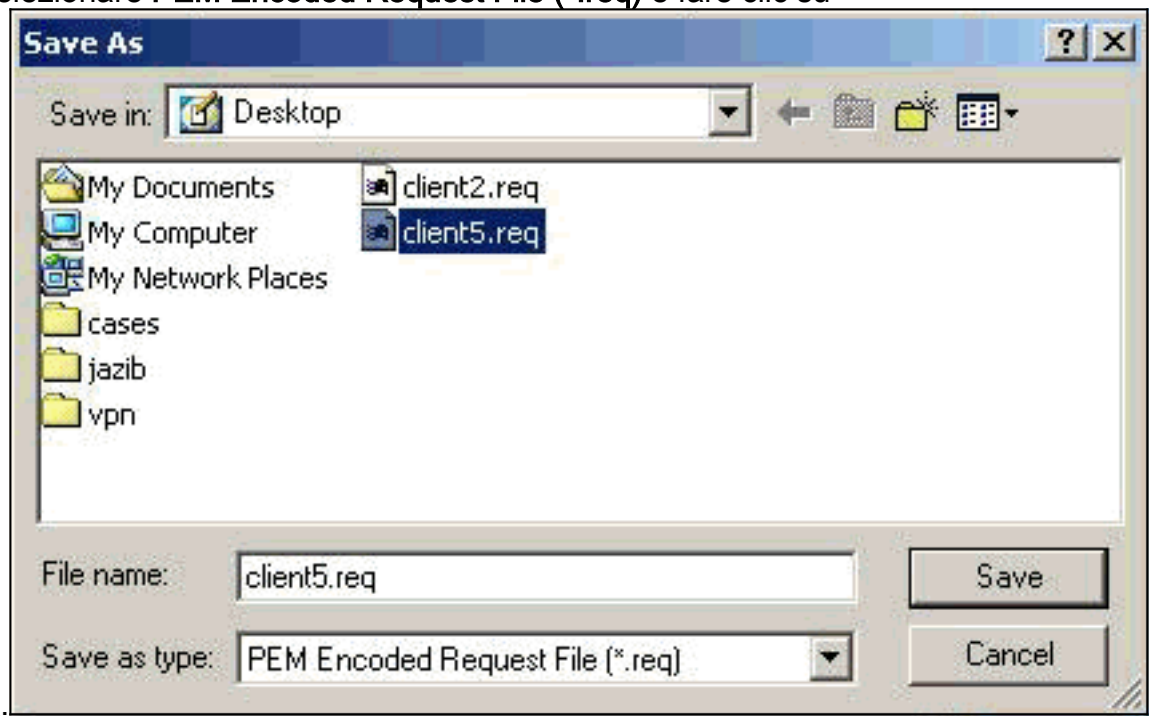
3. Quando il client VPN richiede una password, specificare una password per proteggere il certificato. Qualsiasi operazione che richiede l'accesso alla chiave privata del certificato richiede la password specificata per
continuare.

4. Selezionare **File** per richiedere un certificato utilizzando il formato PKCS #10 nella pagina Registrazione. Quindi fare clic su



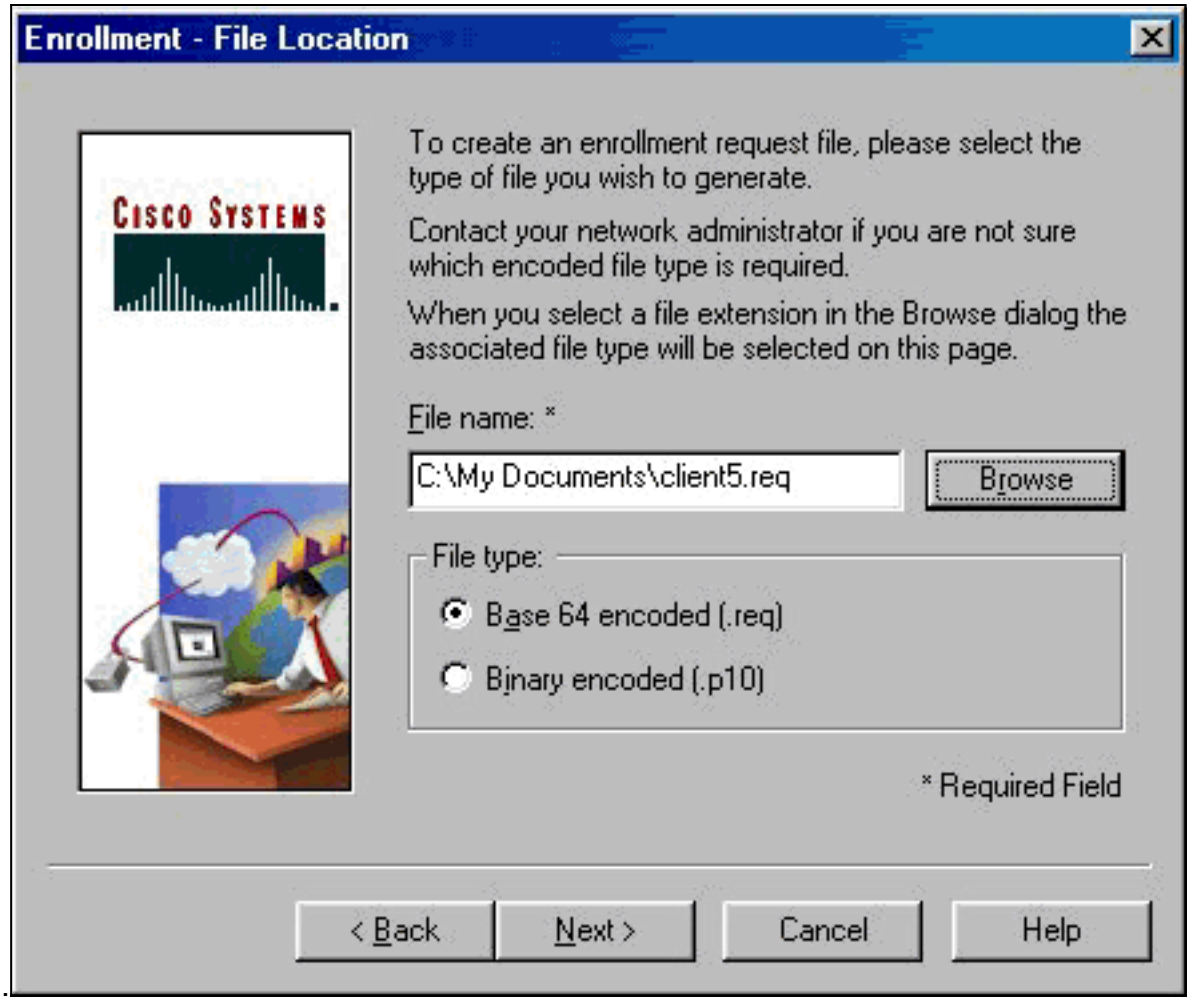
Avanti.

5. Fare clic su **Sfoglia** e specificare un nome file per il file di richiesta del certificato. Per il tipo di file, selezionare **PEM Encoded Request File (*.req)** e fare clic su



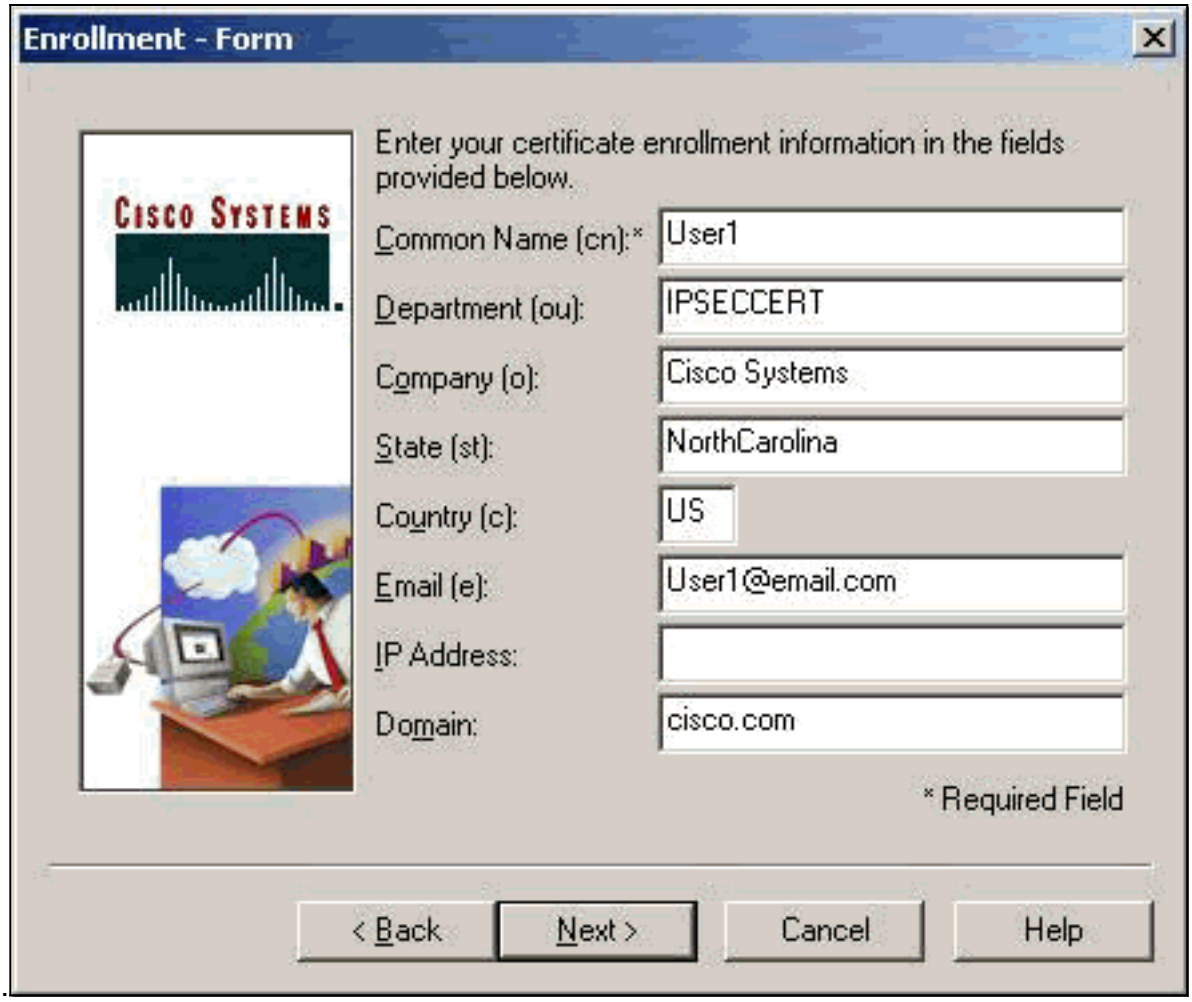
Salva.

6. Fare clic su **Avanti** nella pagina Registrazione client



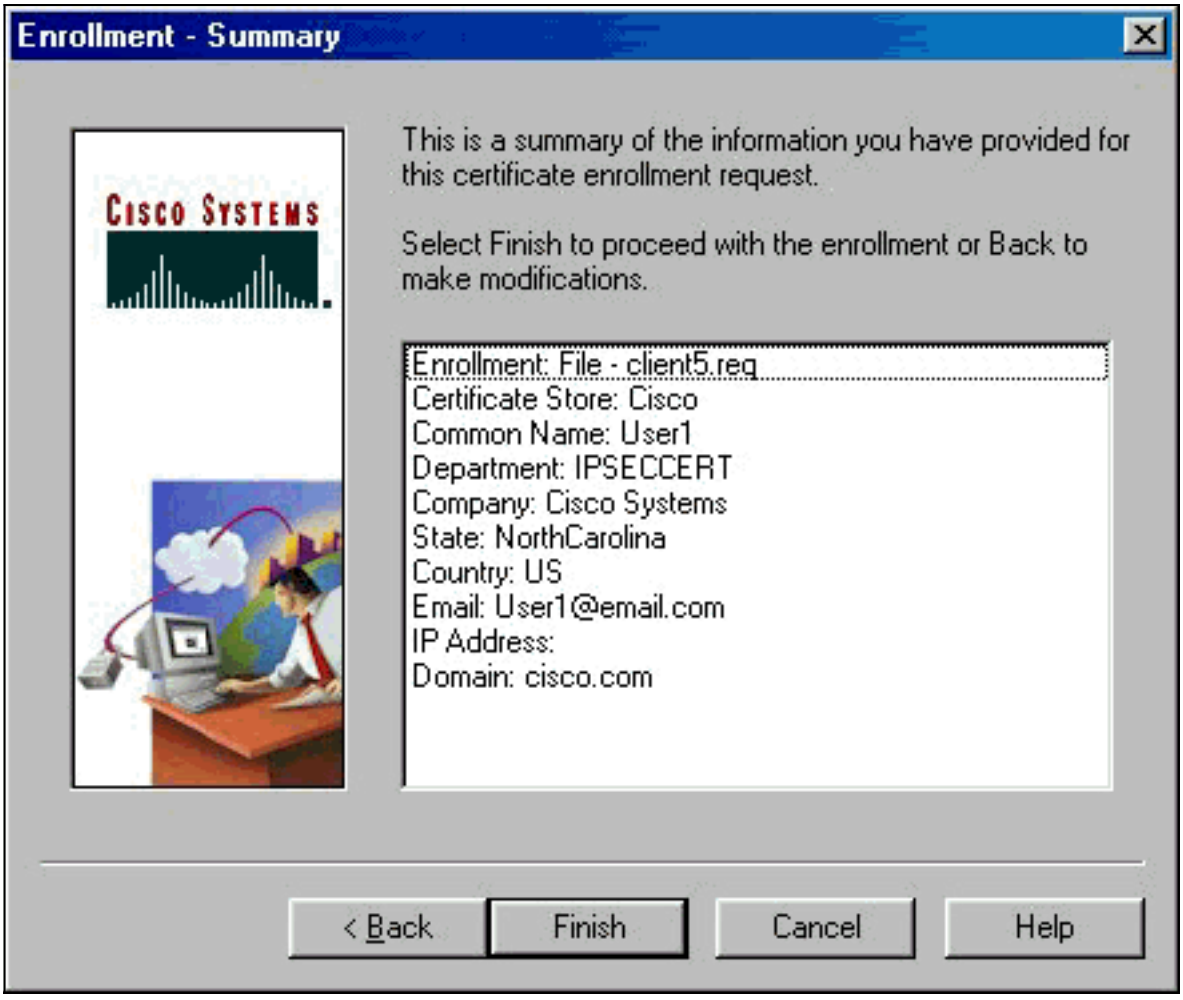
VPN.

7. Compilare i campi del modulo di registrazione.Nell'esempio vengono mostrati i campi:Nome comune = Utente1Department = IPSECCERT (deve corrispondere all'unità organizzativa e al nome del gruppo nel concentratore VPN 3000).Azienda = Cisco SystemsStato = Carolina del NordPaese = USE-mail = User1@email.comIndirizzo IP = (facoltativo; utilizzato per specificare l'indirizzo IP nella richiesta di certificatoDomain = cisco.comAl termine, fare clic su

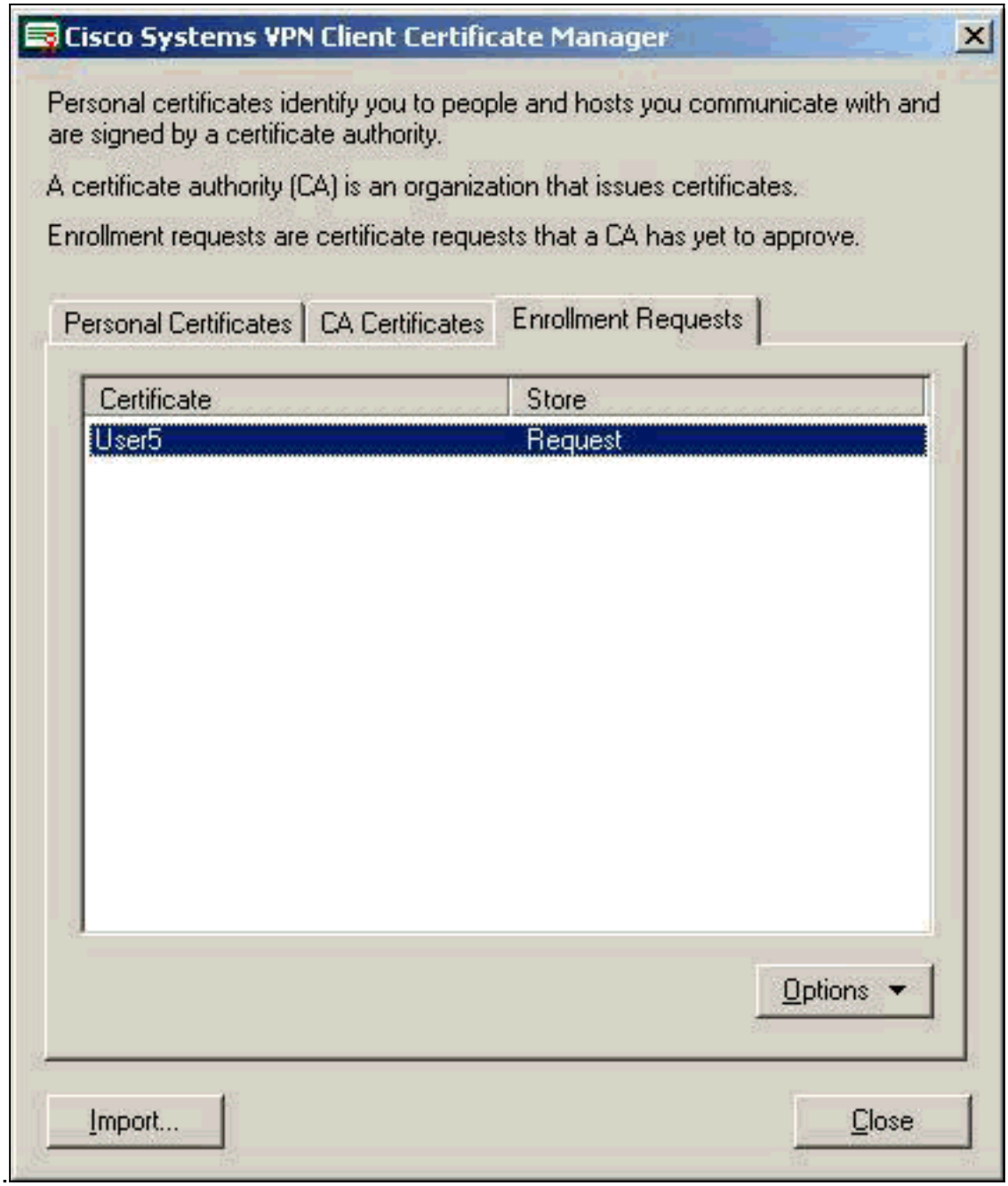


Avanti.

8. Fare clic su **Fine** per procedere con l'iscrizione.

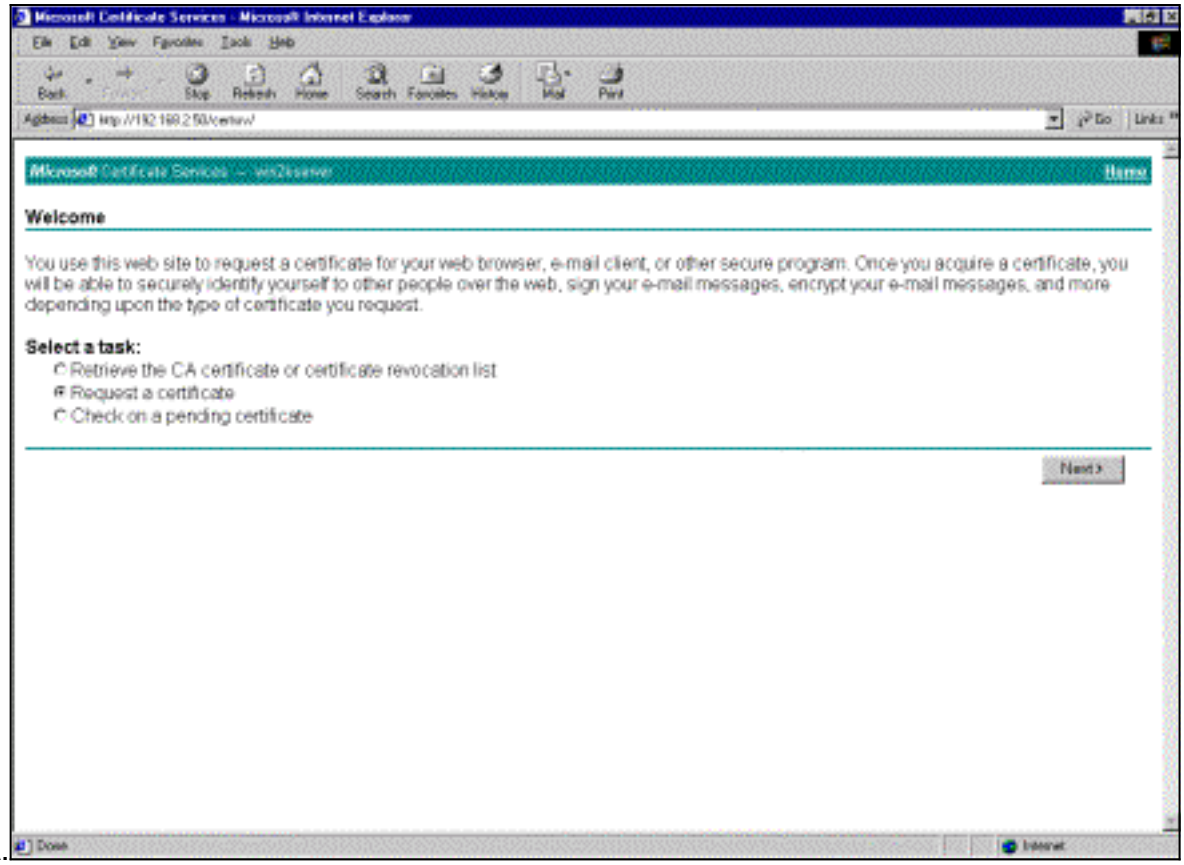


9. Selezionare la scheda Richieste di registrazione per controllare la richiesta in Gestione certificati client



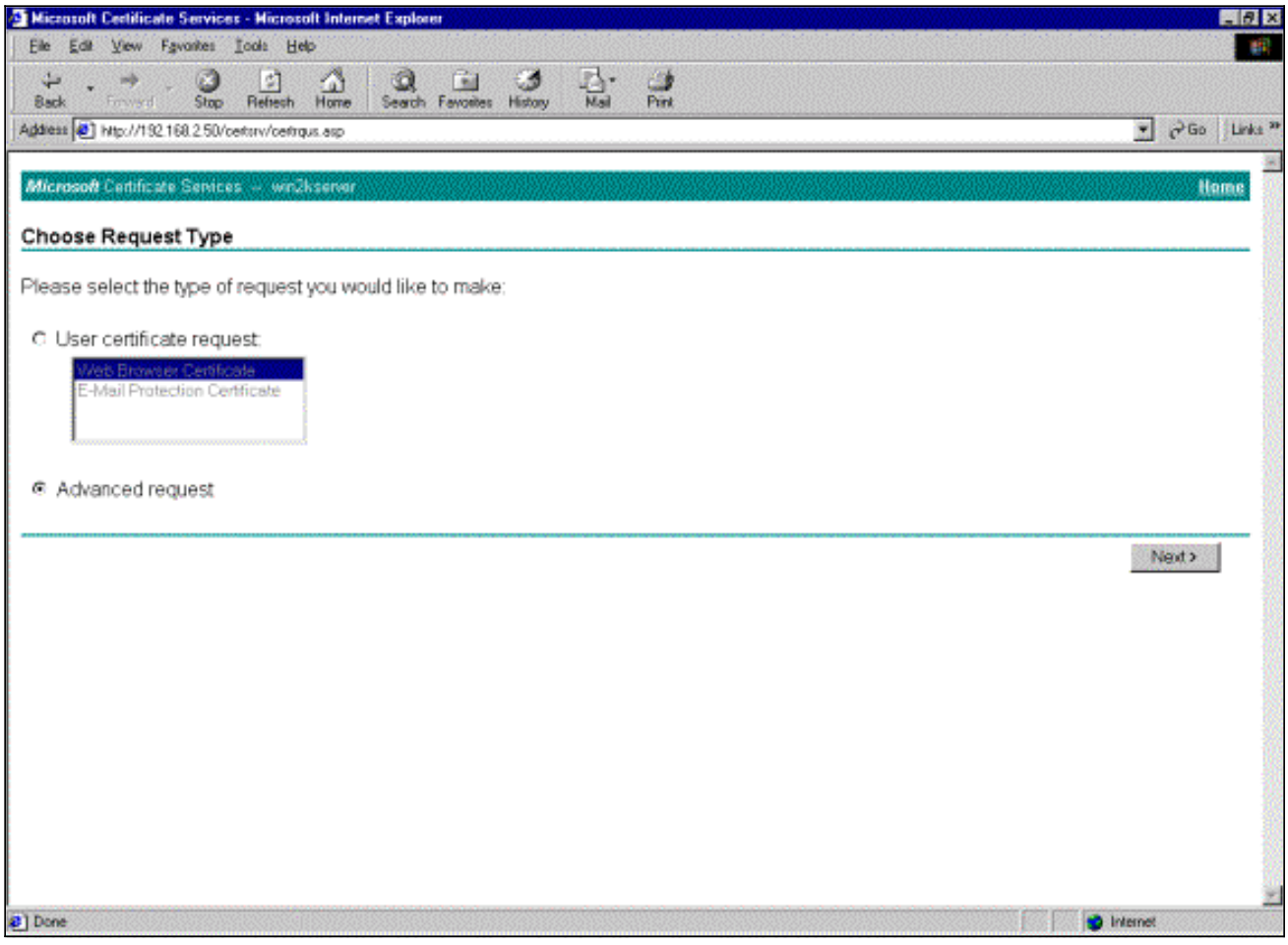
VPN.

10. Per inviare la richiesta, attivare contemporaneamente il server Autorità di certificazione (CA) e le interfacce client VPN.
11. Selezionare **Request a certificate** (Richiedi un certificato) e fare clic su **Next** (Avanti) sul server



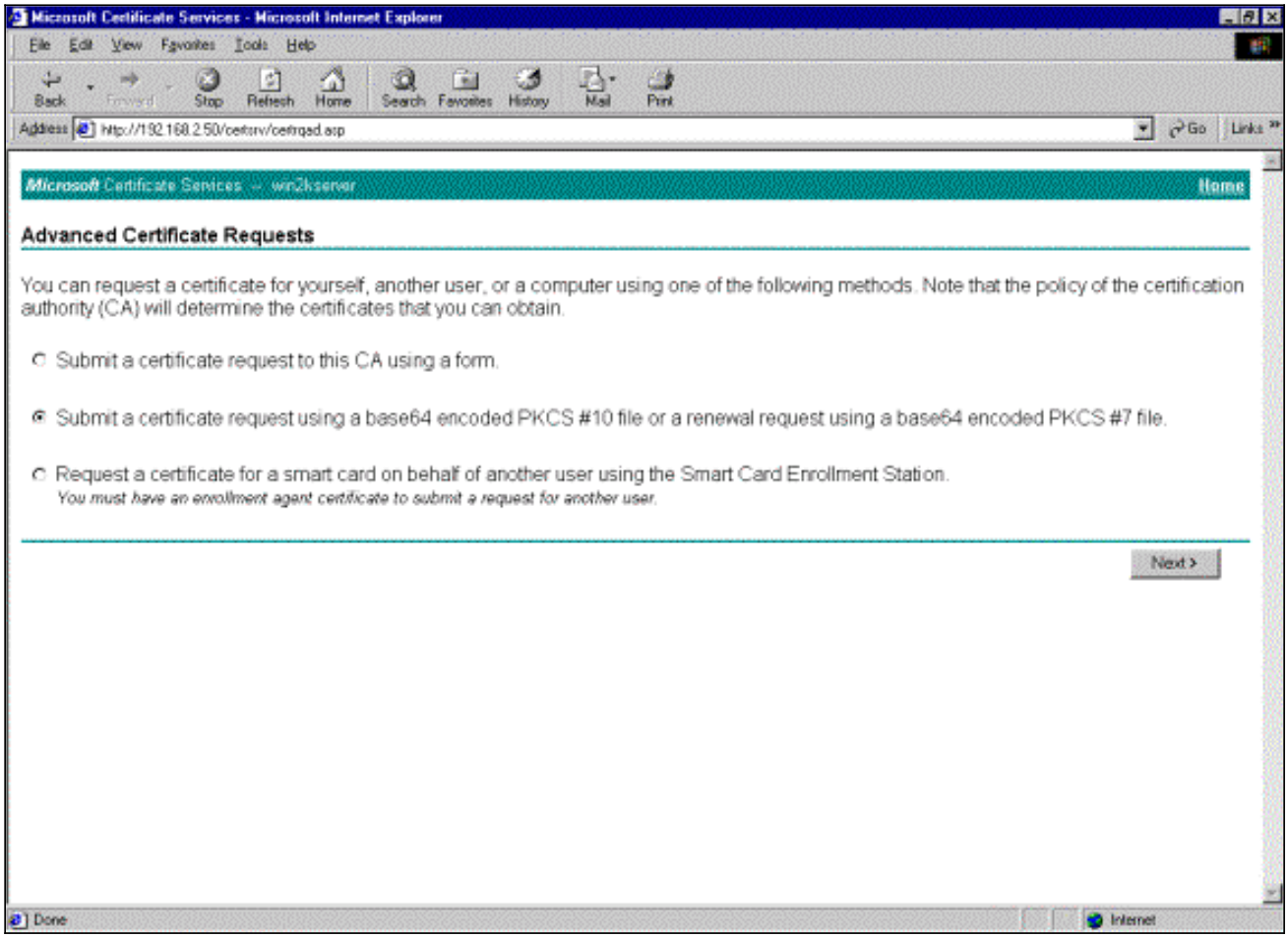
CA.

12. Selezionare **Richiesta avanzata** per il tipo di richiesta e fare clic su **Avanti**.

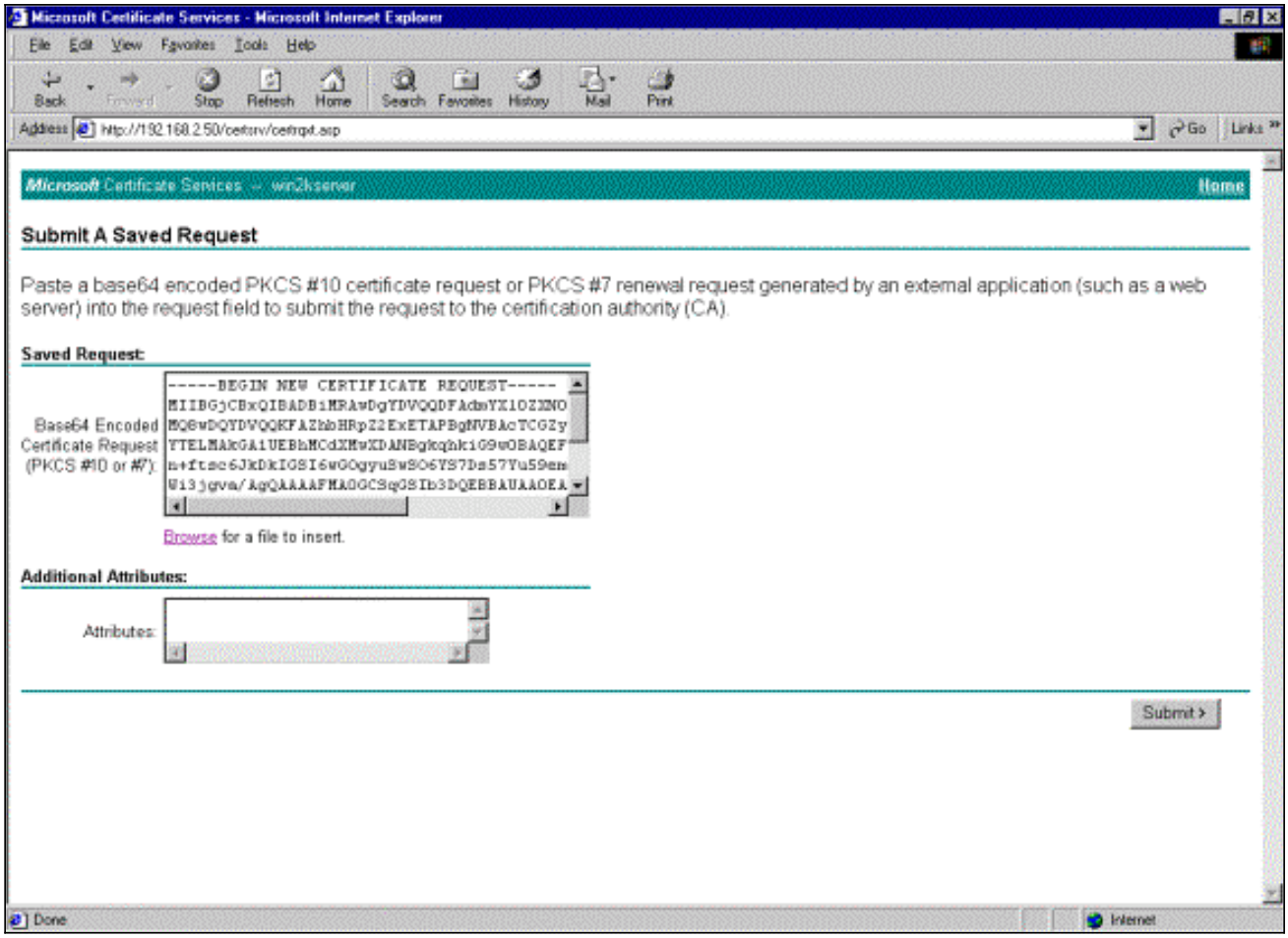


13. Selezionare **Inviare una richiesta di certificato utilizzando un file PKCS #10 con codifica Base64 o una richiesta di rinnovo utilizzando un file PKCS #7 con codifica Base64** in Richieste di certificato avanzate e quindi fare clic su

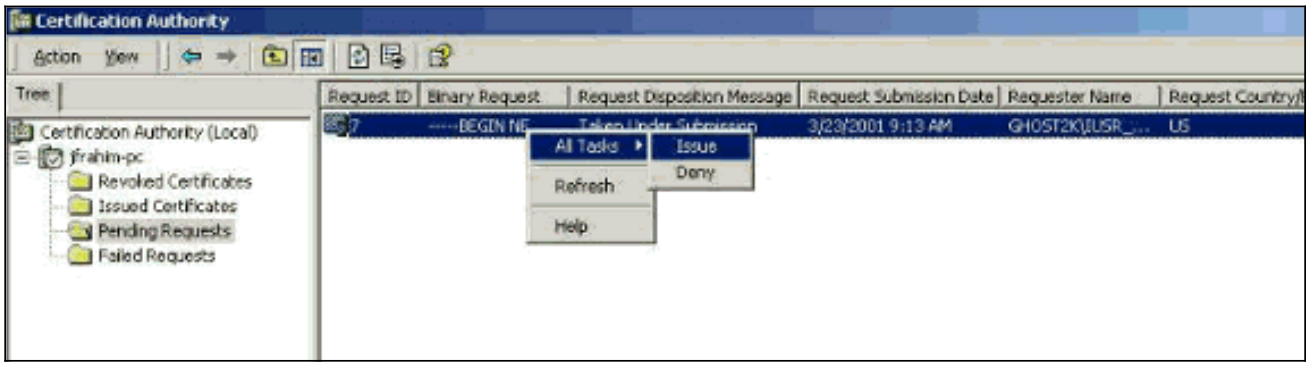
Avanti.



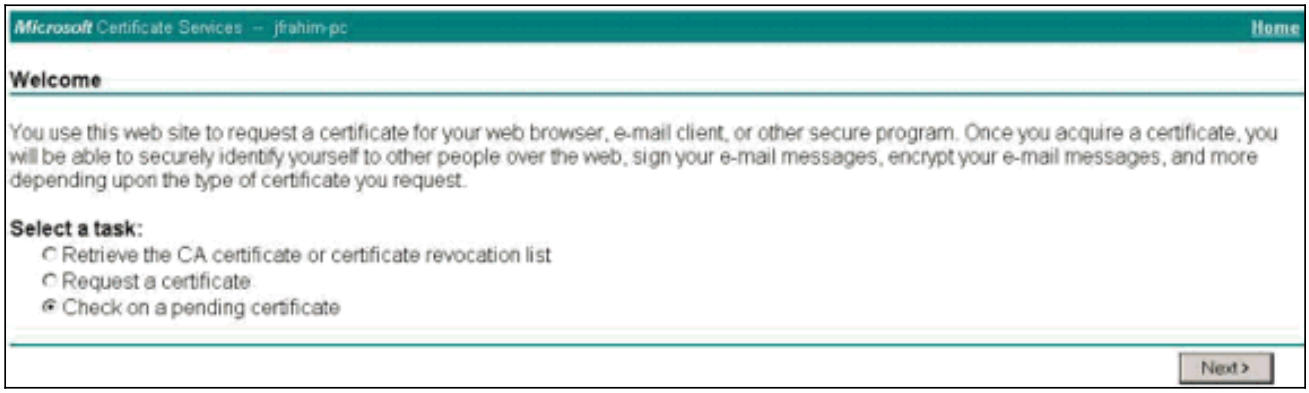
14. Evidenziare il file di richiesta del client VPN e incollarlo nel server CA in Richiesta salvata. Quindi fare clic su
Invia.



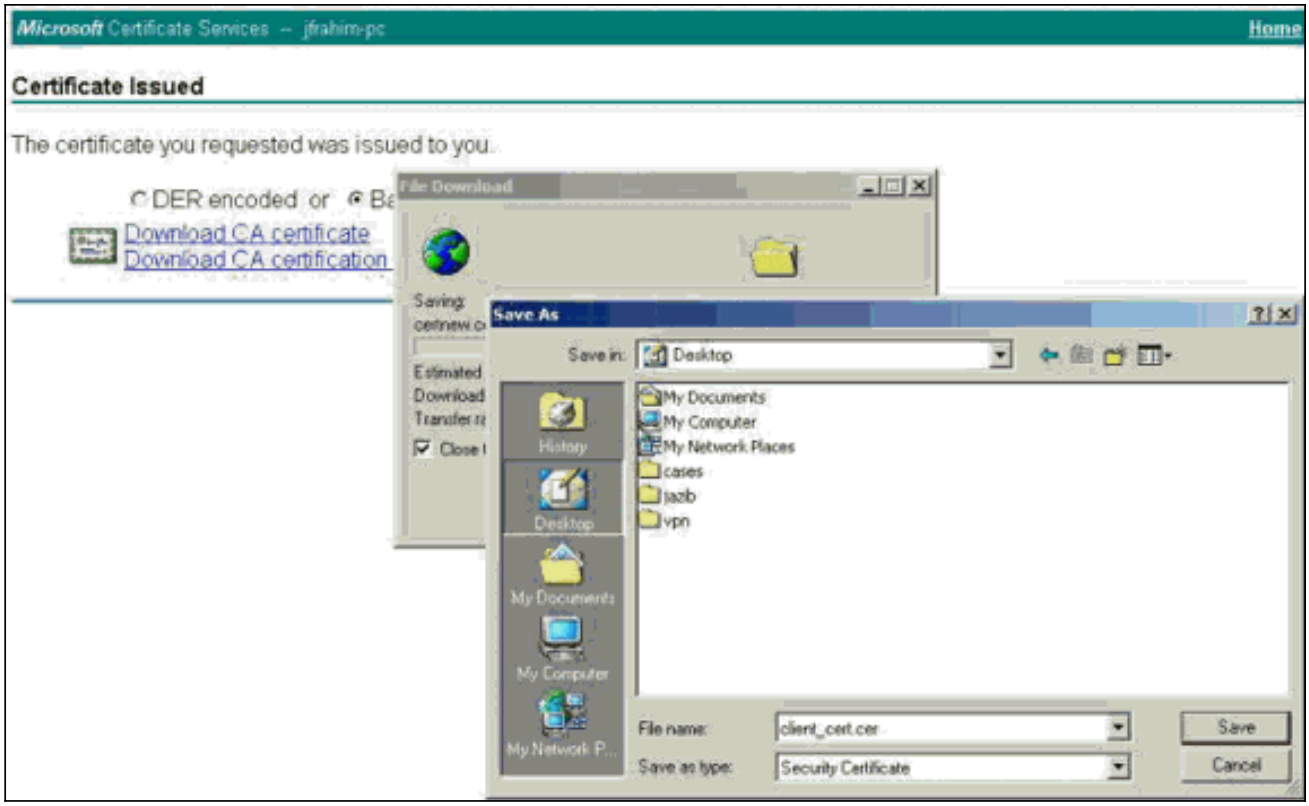
15. Sul server CA, emettere il certificato di identità per la richiesta del client VPN.



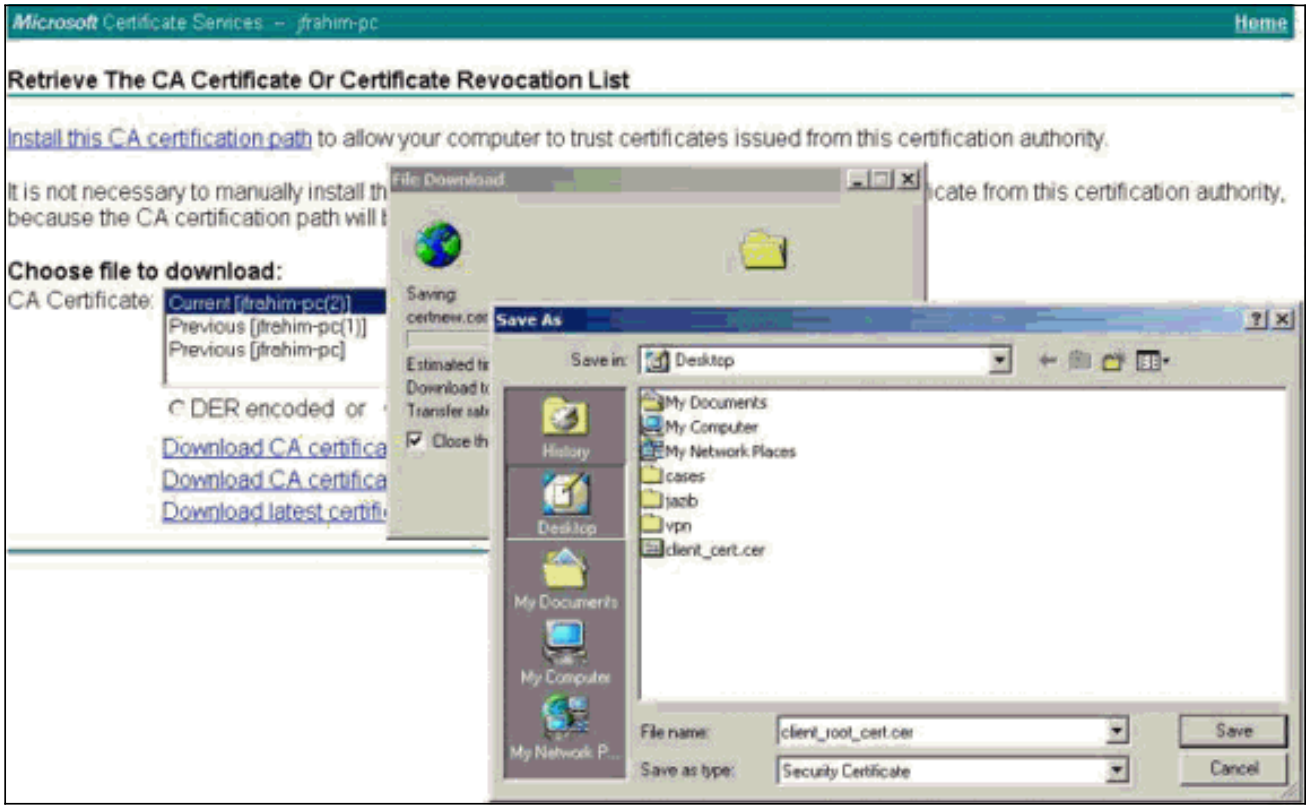
16. Scaricare i certificati radice e di identità nel client VPN. Nel server CA selezionare **Verifica un certificato in sospeso** e quindi fare clic su **Avanti**.



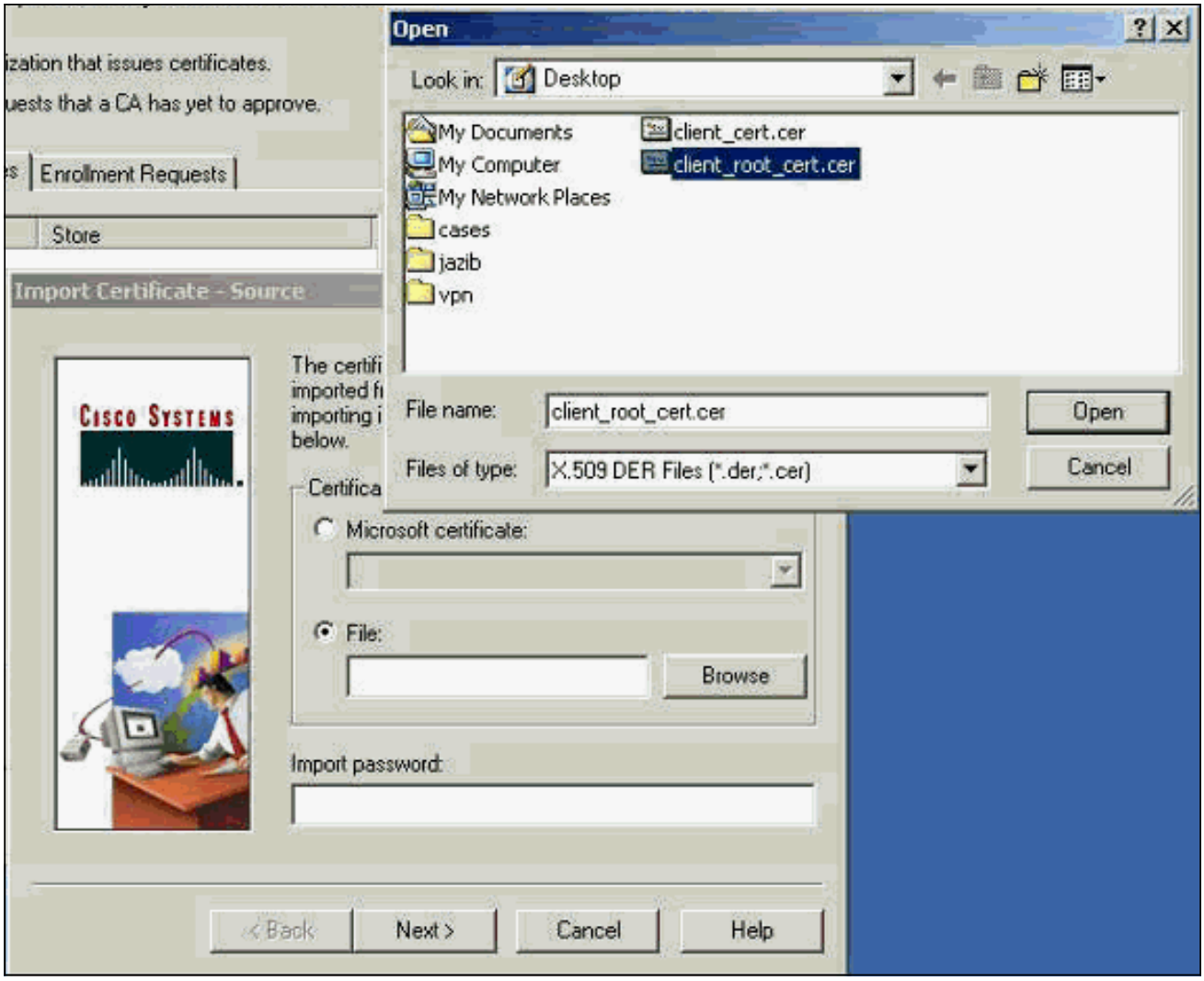
17. Selezionare **Codificato Base 64**. Quindi fare clic su **Scarica certificato CA** sul server CA.



18. Selezionare un file da scaricare dalla pagina Recupera il certificato CA o l'elenco di revoche di certificati per ottenere il certificato radice sul server CA. Quindi fare clic su **Avanti**.



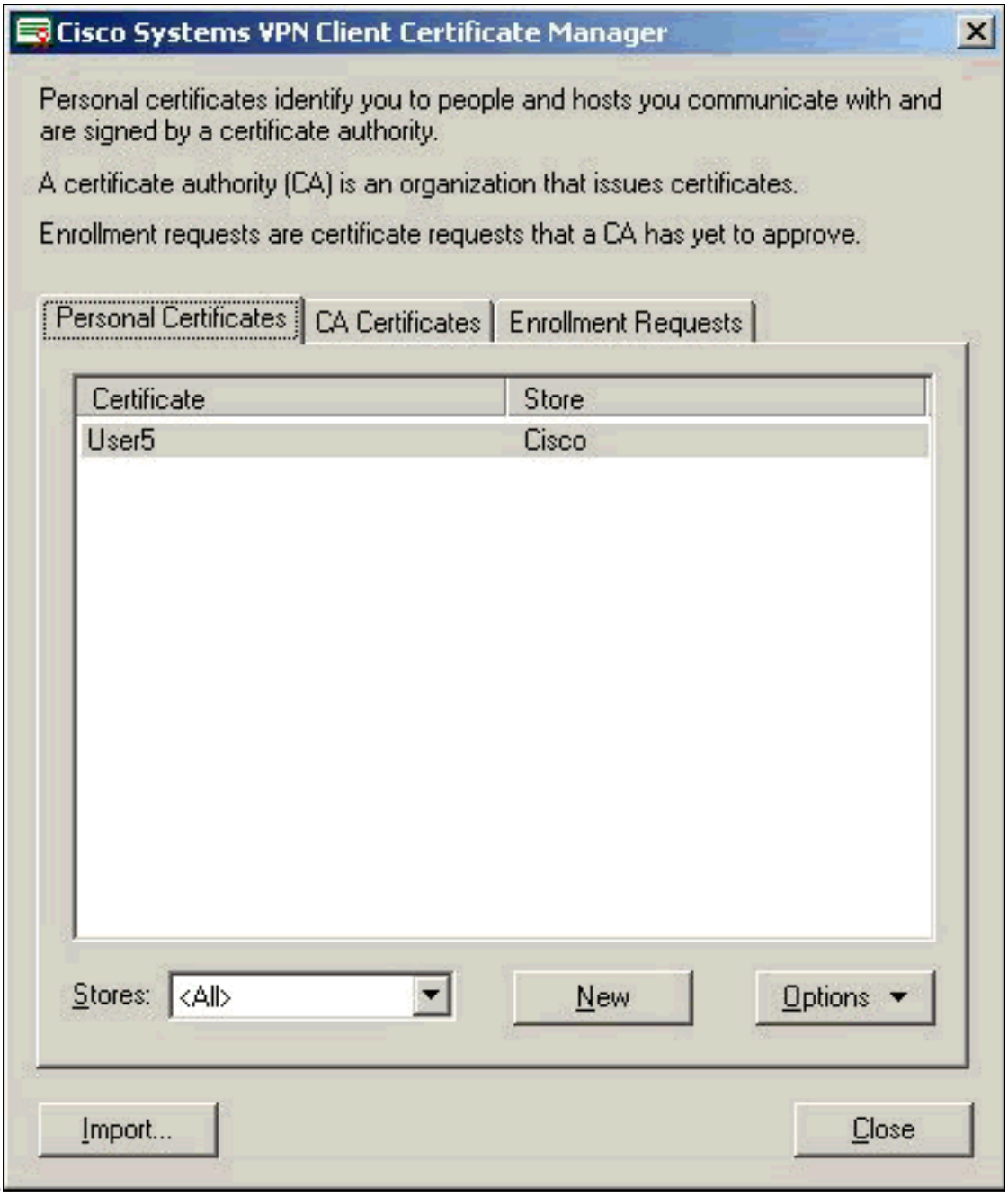
19. Selezionare **Gestione certificati > Certificato CA > Importa nel client VPN** e quindi selezionare il file CA radice per installare i certificati radice e di identità.



20. Selezionare **Gestione certificati > Certificati personali > Importa**, quindi scegliere il file del certificato di

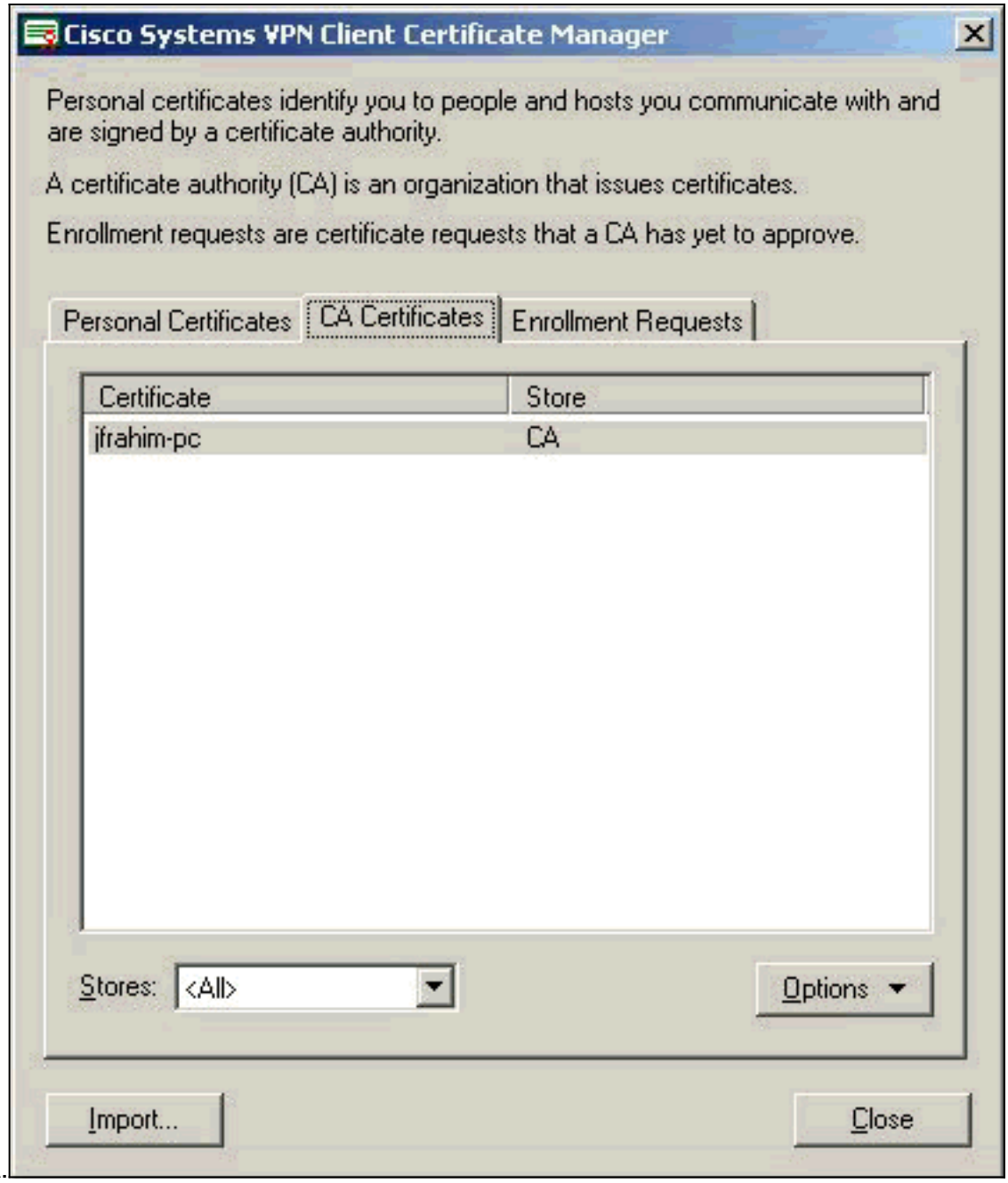
identità.

21. Assicurarsi che il certificato di identità venga visualizzato nella scheda Certificati



personali.

22. Verificare che il certificato radice venga visualizzato nella scheda Certificati



CA.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Quando si tenta di eseguire la registrazione al server CA Microsoft, è possibile che venga generato questo messaggio di errore.

```
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 viene visualizzato questo messaggio di errore, vedere i registri CA di Microsoft per ulteriori informazioni oppure fare riferimento a queste risorse per ulteriori informazioni.

- Impossibile trovare un'Autorità di certificazione che elabori la richiesta
- XCCC: Quando Si Richiede Un Certificato Per Conferenze Protette, Viene Visualizzato Il Messaggio Di Errore "Richiesta Di Certificato Negata"

Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems