

デジタル証明書を取得するための VPN Client 3.x の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[VPN クライアントの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、デジタル証明書を取得するように Cisco VPN Client 3.x を設定する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN Client 3.xが稼働するPCに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

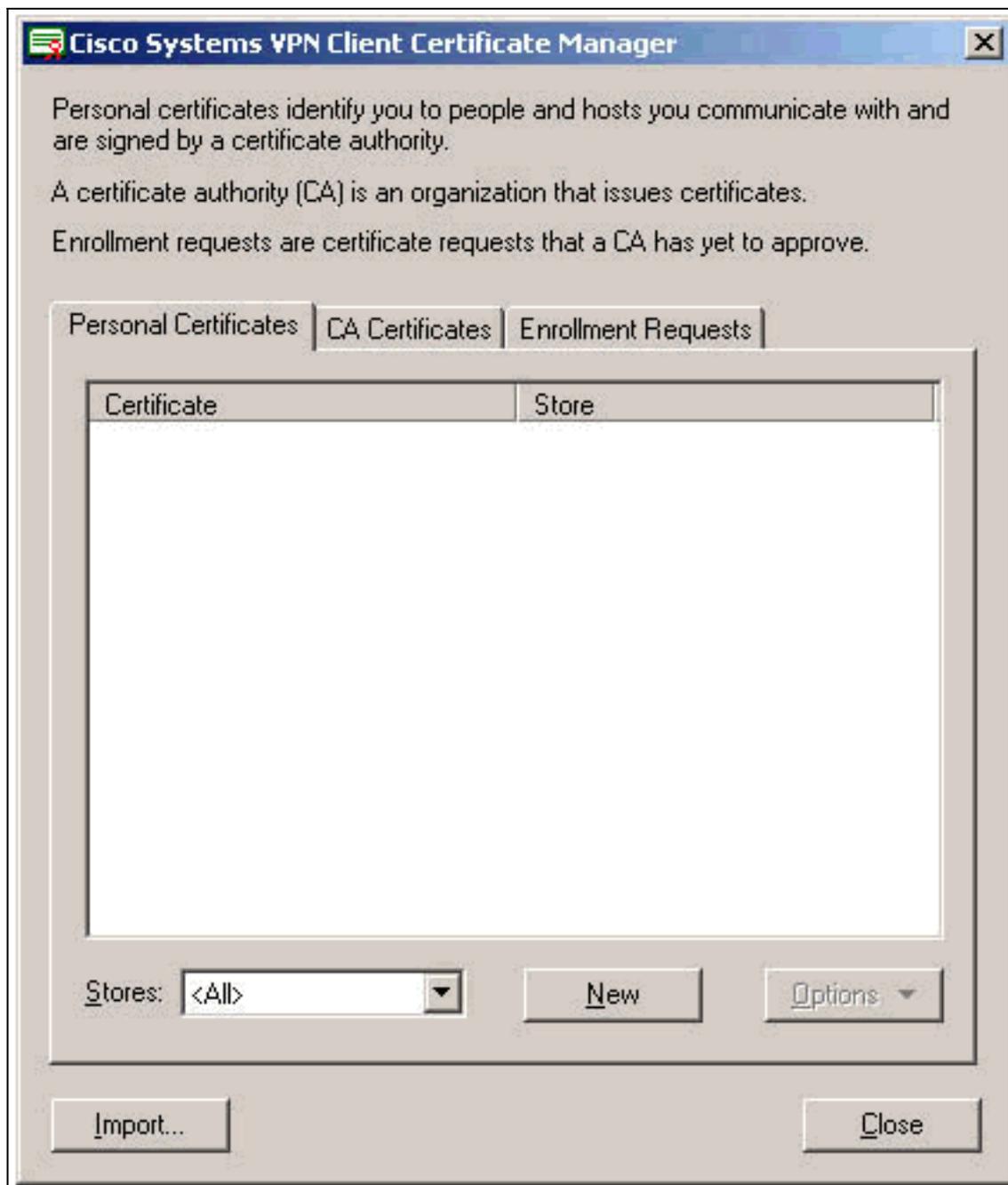
VPN クライアントの設定

VPN Clientを設定するには、次の手順を実行します。

1. [Start] > [Programs] > [Cisco Systems Inc. VPN client] > [Certificate Manager] の順に選択して、VPN Client Certificate Managerを起動します。



2. [Personal Certificates]タブを選択し、[New]をクリックします。



注：VPN接

続のユーザを認証するマシン証明書は、IPsecでは実行できません。

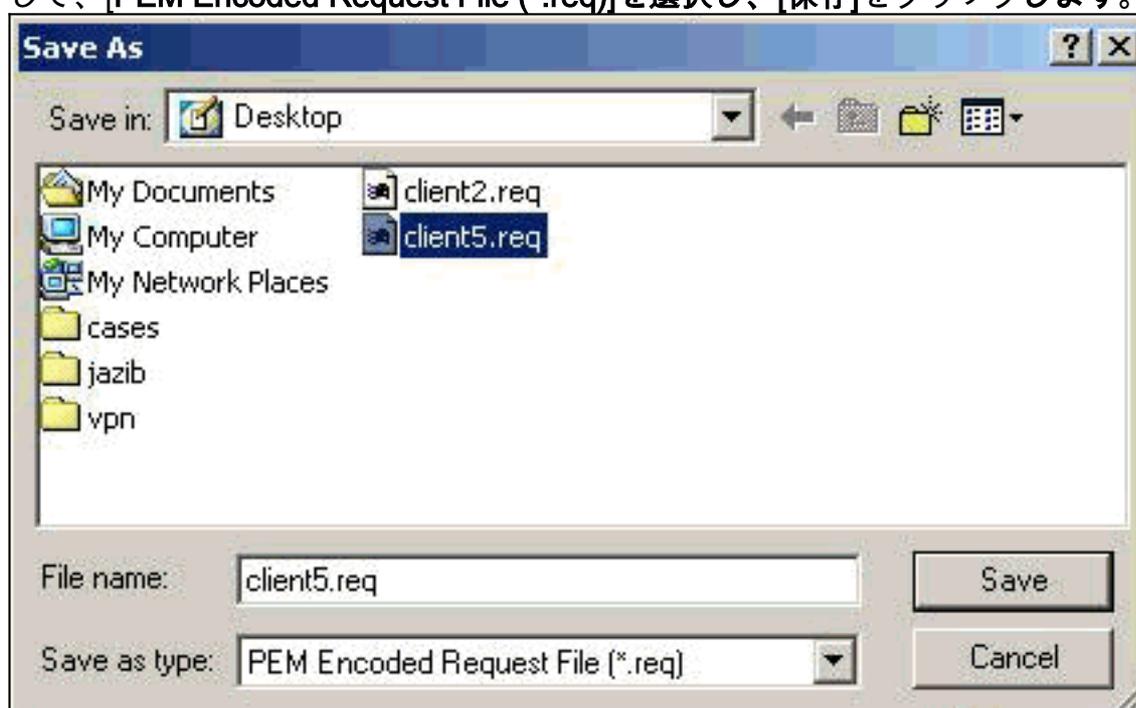
3. VPN Clientからパスワードの入力を求められたら、証明書を保護するためのパスワードを指定します。証明書の秘密キーへのアクセスを必要とする操作を続行するには、指定されたパスワードが必要です。



4. [Enrollment] ページで[File]を選択し、PKCS #10形式を使用して証明書を要求します。次に、[Next] をクリックします。

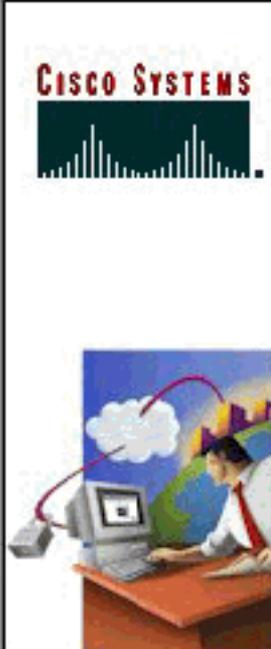


5. [Browse]をクリックし、証明書要求ファイルのファイル名を指定します。ファイルの種類として、[PEM Encoded Request File (*.req)]を選択し、[保存]をクリックします。



6. [VPN Client Enrollment]ページで[Next]をクリックします。

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. 登録フォームのフィールドに入力します。次の例は、フィールドを示しています。共通名= User1部門= IPSECCERT(これは、VPN 3000コンセントレータの組織単位(OU)とグループ名と一致する必要があります)。会社=シスコ州=ノースカロライナ国=米国電子メール= User1@email.comIPアドレス=(オプション；証明書要求のIPアドレスを指定するために使用される)ドメイン= cisco.com完了したら、[Next] をクリックします。

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. [完了]をクリックして、登録を続行します。

Enrollment - Summary

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

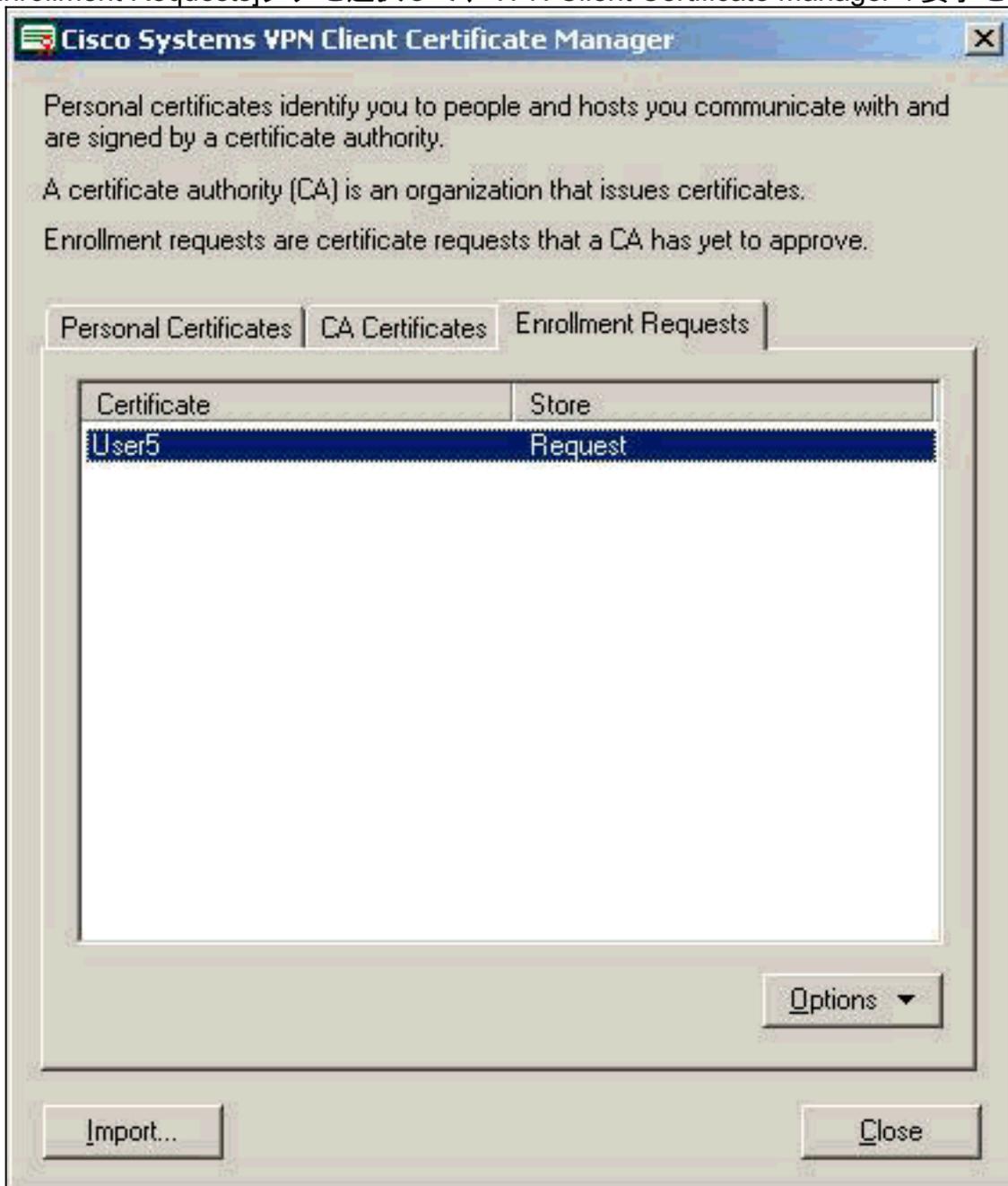
Select Finish to proceed with the enrollment or Back to make modifications.




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

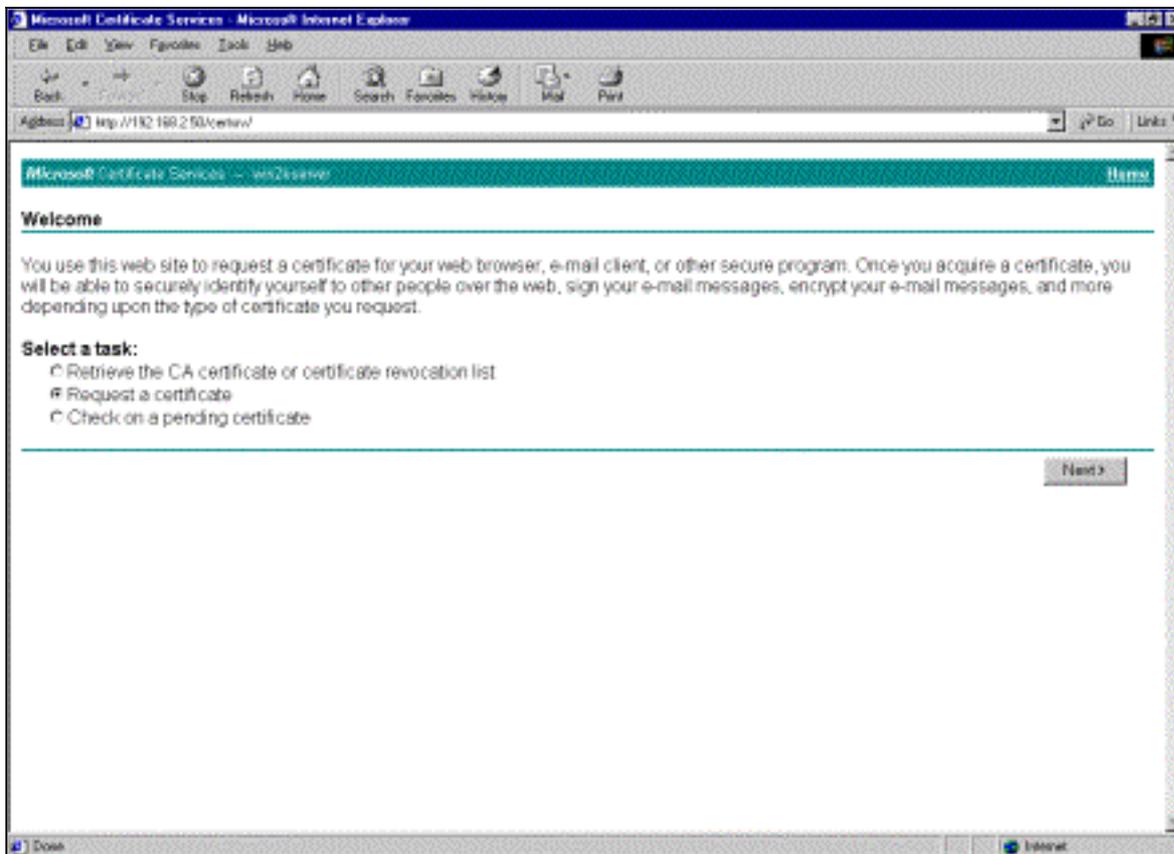
< Back Finish Cancel Help

9. [Enrollment Requests]タブを選択して、VPN Client Certificate Managerの要求を確認します

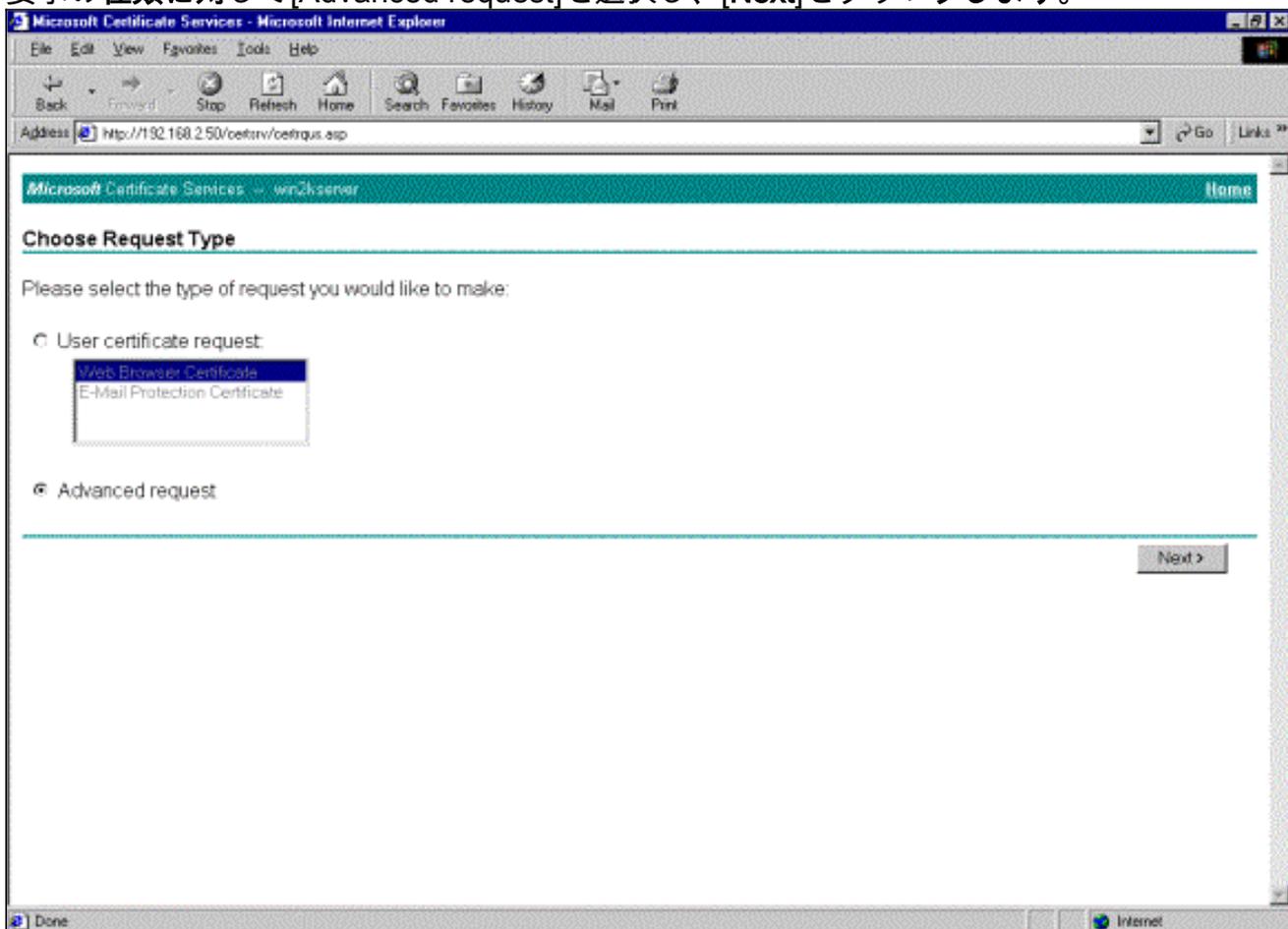


10. 認証局(CA)サーバとVPN Clientインターフェイスを同時に起動して、要求を送信します。

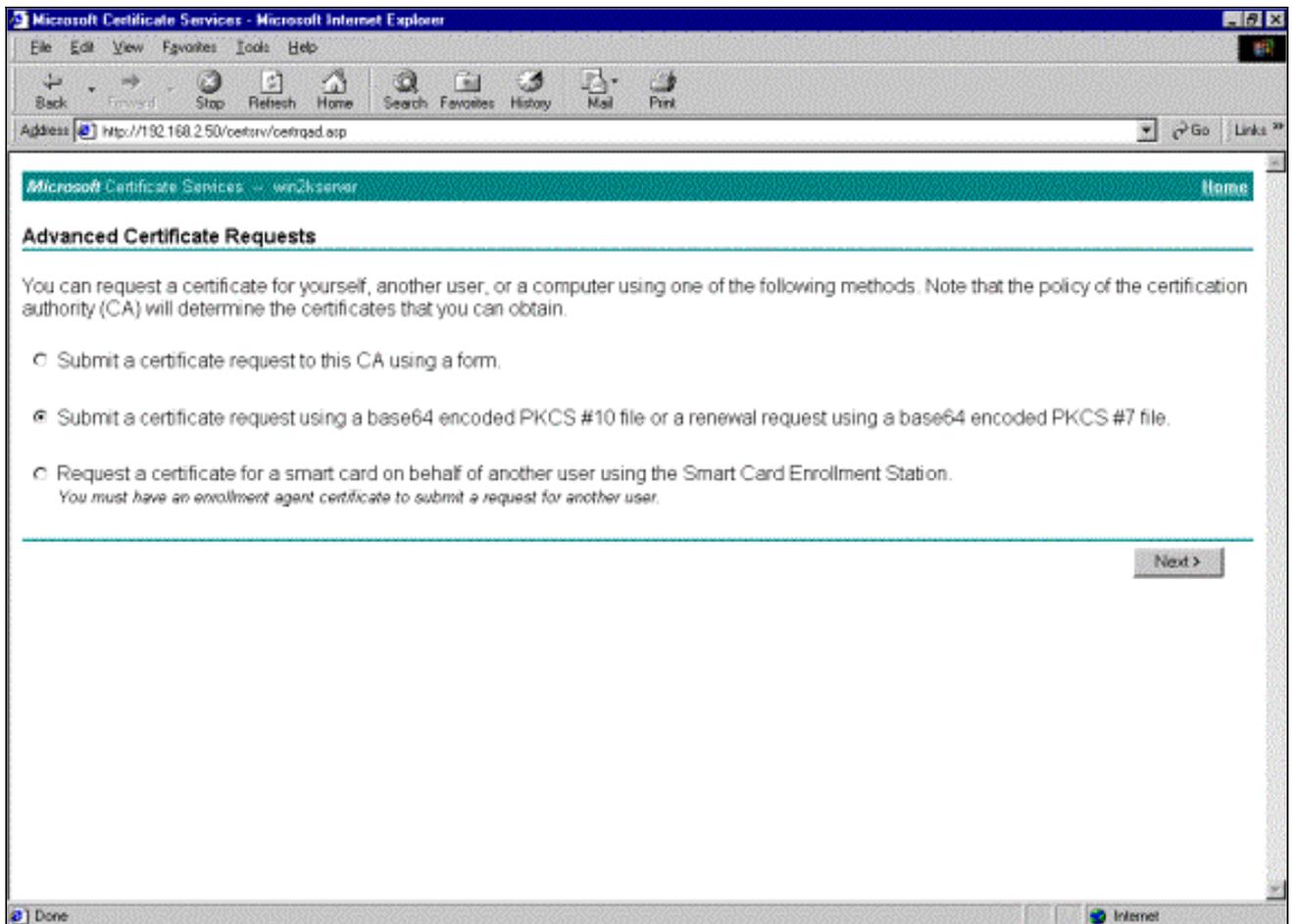
11. [Request a certificate]を選択し、CAサーバで[Next]をクリックします。



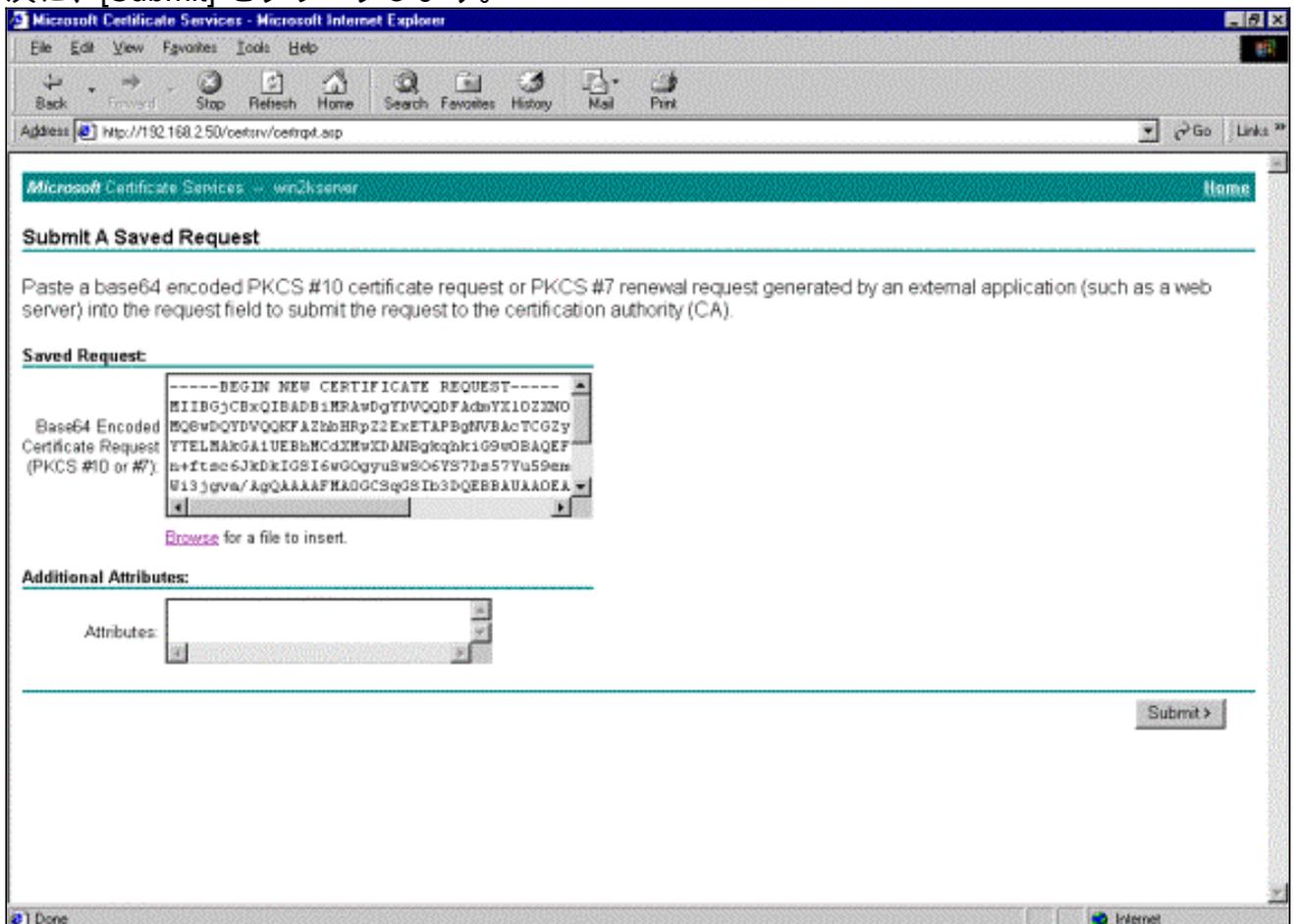
12. 要求の種類に対して[Advanced request]を選択し、[Next]をクリックします。



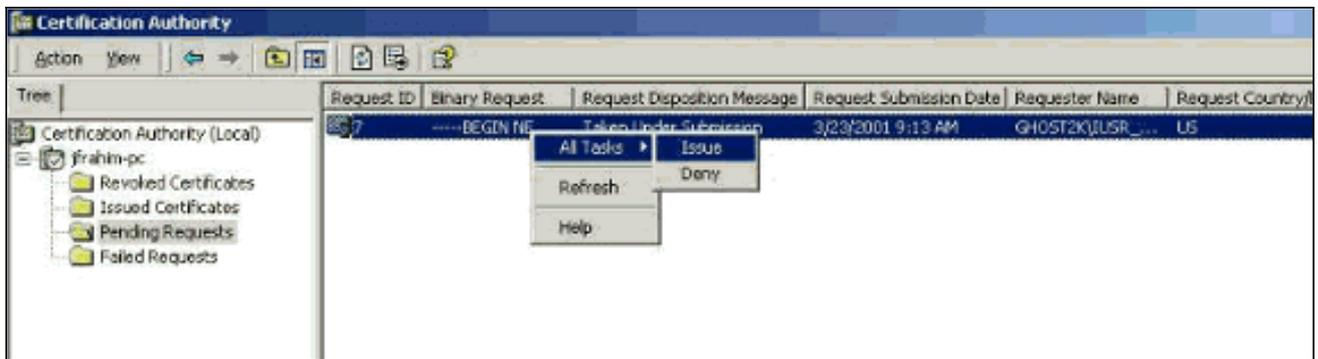
13. [Advanced Certificate Requests]で、[Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file]を選択し、[Next]をクリックします。



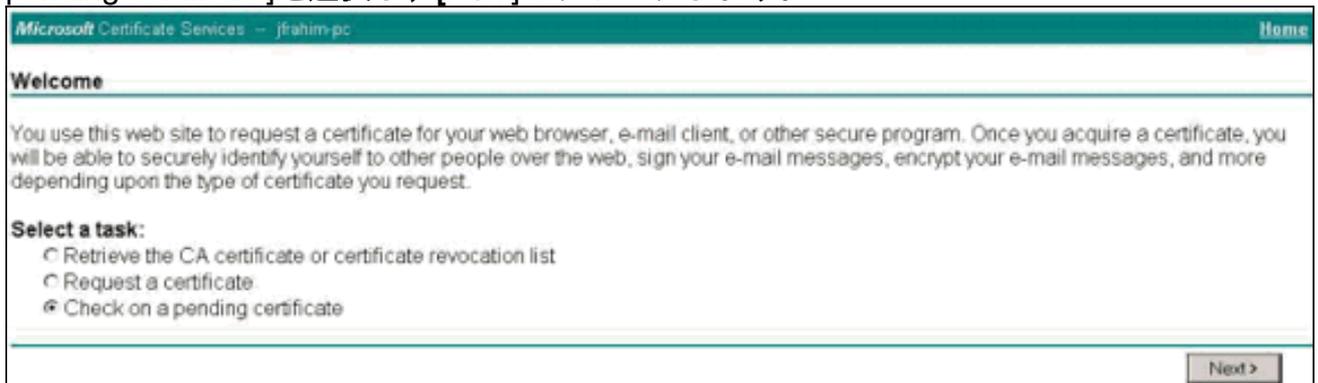
14. VPN Client要求ファイルを強調表示し、[Saved Request]の下のCAサーバに貼り付けます。次に、[Submit] をクリックします。



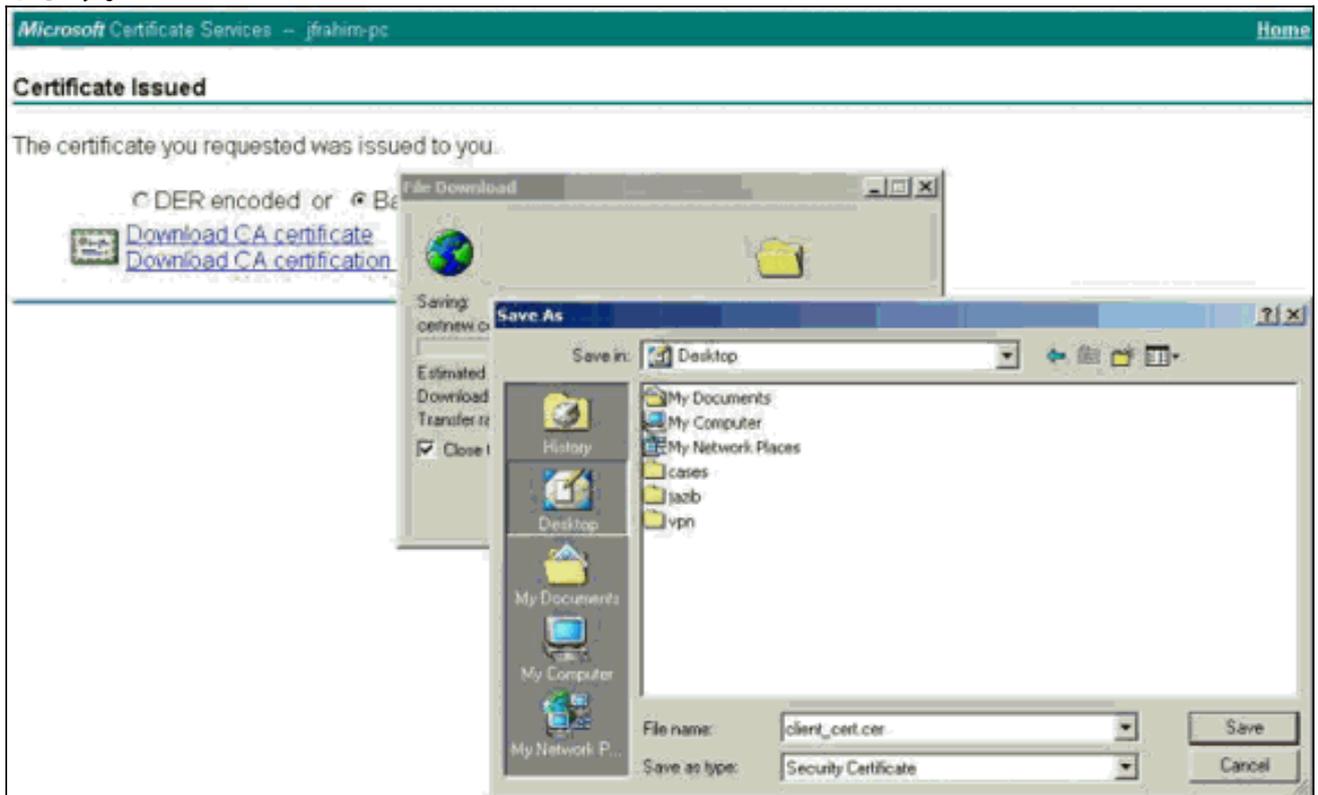
15. CAサーバで、VPN Client要求のID証明書を発行します。



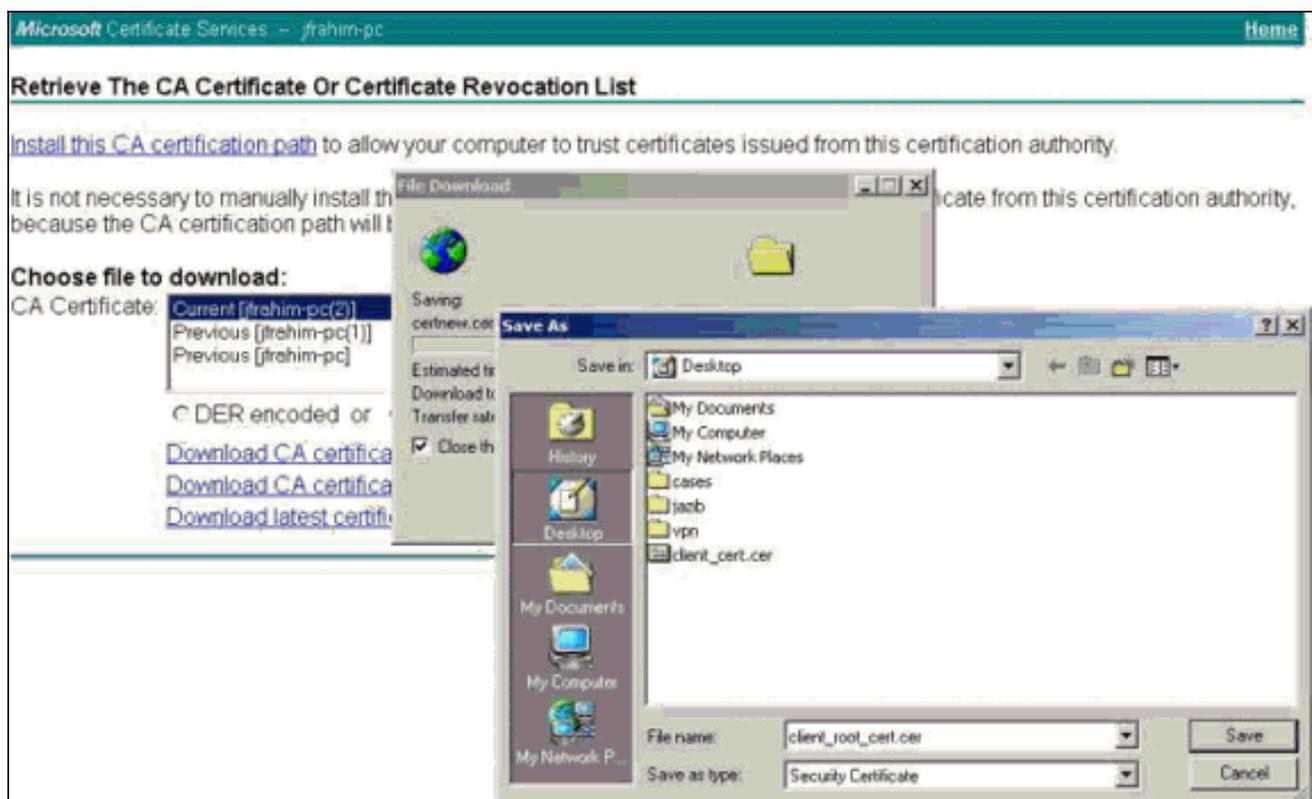
16. ルート証明書とID証明書をVPN Clientにダウンロードします。CAサーバで、[Check on a pending certificate]を選択し、[Next]をクリックします。



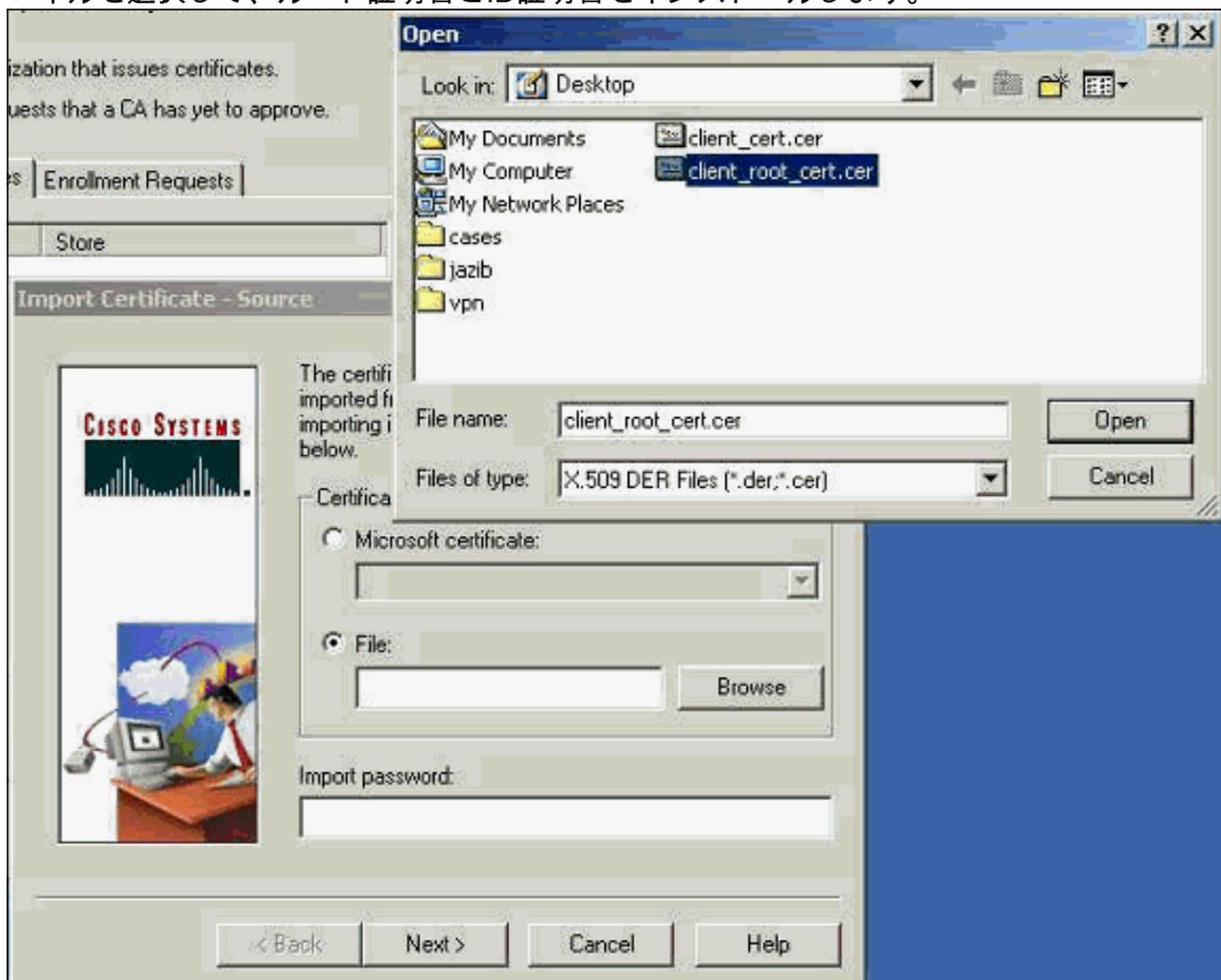
17. [Base 64 encoded] を選択します。次に、CAサーバで[Download CA certificate]をクリックします。



18. [Retrieve the CA Certificate or Certificate Revocation List]ページからダウンロードするファイルを選択し、CAサーバのルート証明書を取得します。次に、[Next] をクリックします。



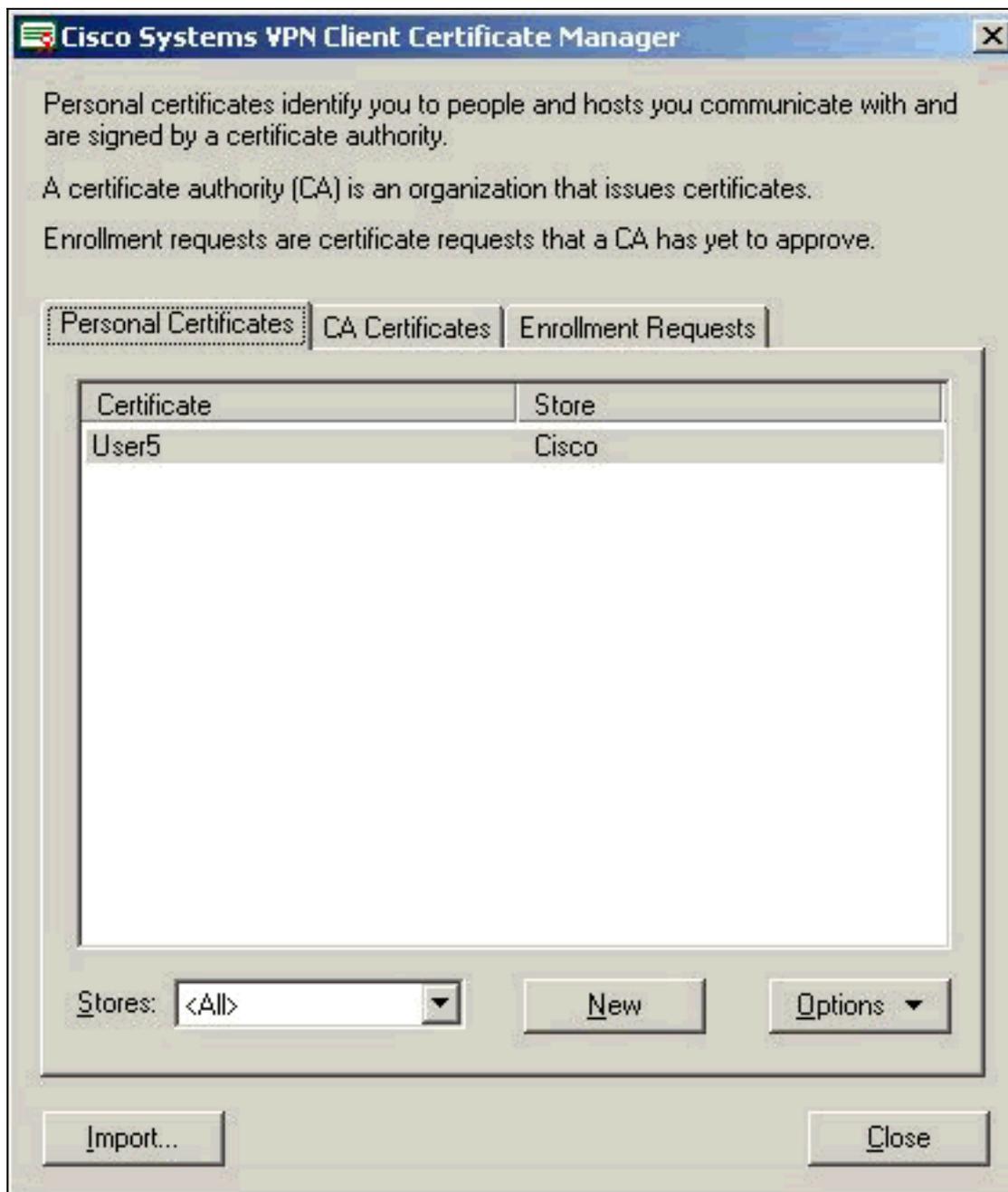
19. [Certificate Manager] > [CA Certificate] > [Import on the VPN Client] を選択し、ルートCAファイルを選択して、ルート証明書とID証明書をインストールします。



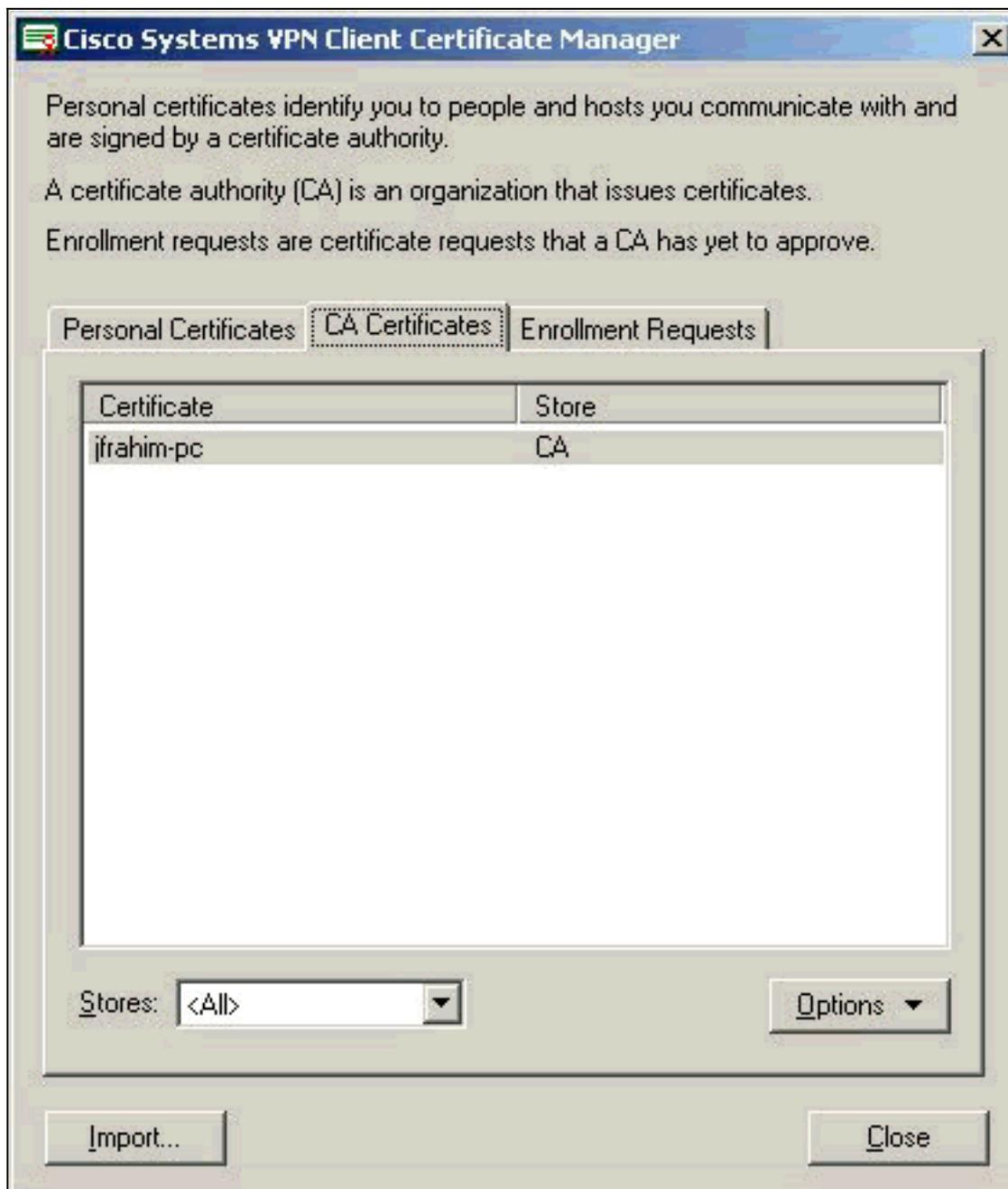
20. [Certificate Manager] > [Personal Certificates] > [Import] を選択し、ID証明書ファイルを選択します。



21. ID証明書が[Personal Certificates]タブに表示されていることを確認します。



22. ルート証明書が[CA Certificates]タブに表示されていることを確認します。



確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

Microsoft CAサーバに登録しようとする、次のエラーメッセージが生成される可能性があります。

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

このエラーメッセージが表示された場合は、Microsoft CAのログで詳細を確認するか、これらの

リソースで詳細を確認してください。

- [要求を処理する認証局が見つかりません](#)
- [XCCC:セキュアな会議の証明書を要求すると、「Your Certificate Request was Denied」エラーメッセージが表示される](#)

関連情報

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)