デジタル証明書を取得するための VPN Client 3.x の設定

目次

はじめに

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関しては個別の要件はありません。

使用するコンポーネント

この 文書に記載されている 情報は Cisco VPN Client 3.x を実行する PC に基づいています

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

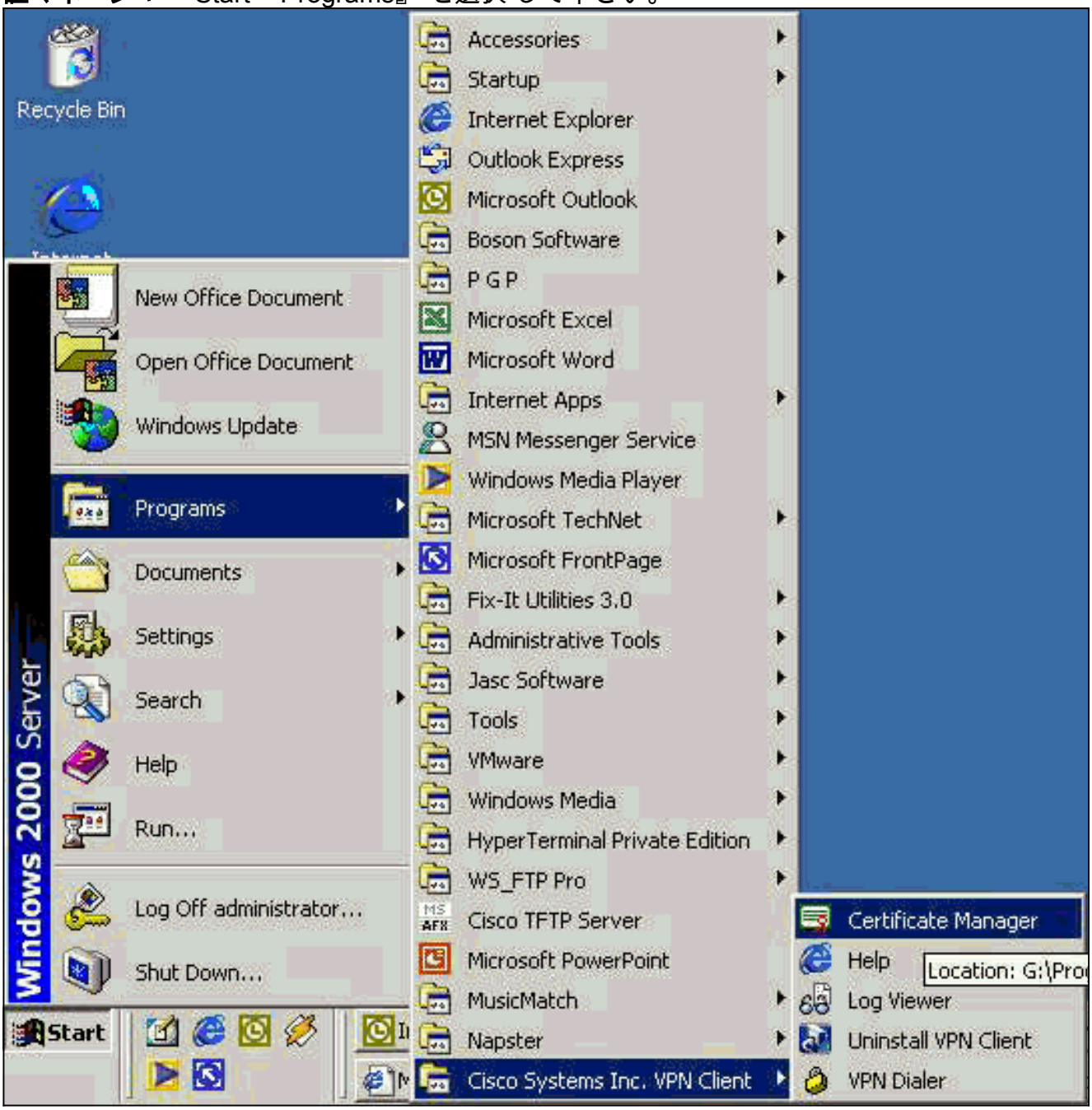
表記法

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。

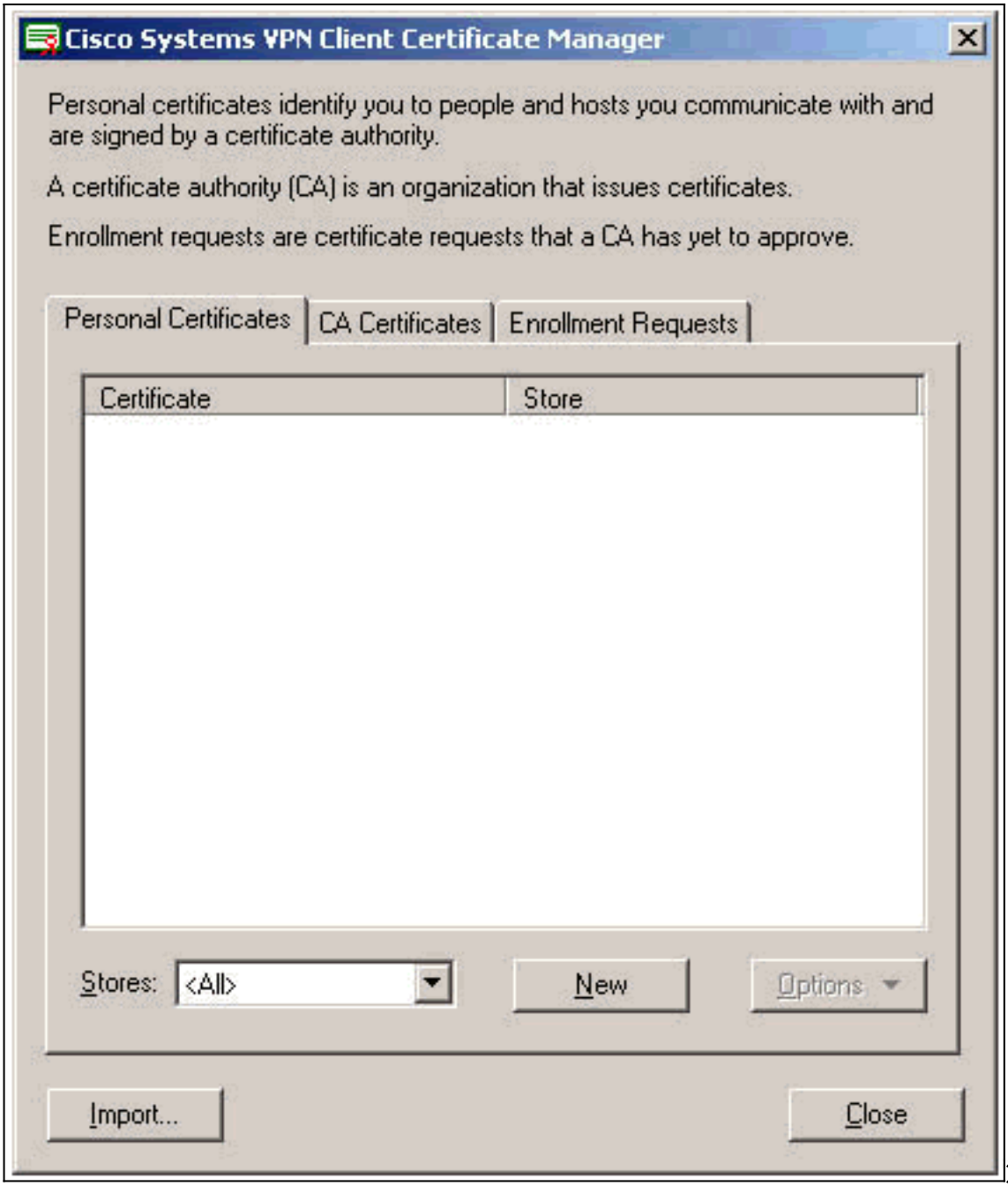
VPN クライアントの設定

VPN クライアントを設定するためにこれらのステップを完了して下さい。

1. >VPN クライアント 認証マネージャを起動させる **Cisco 社株式会社 VPN クライアント > 認証マネージャ** 『Start > Programs』 を選択 して下さい。



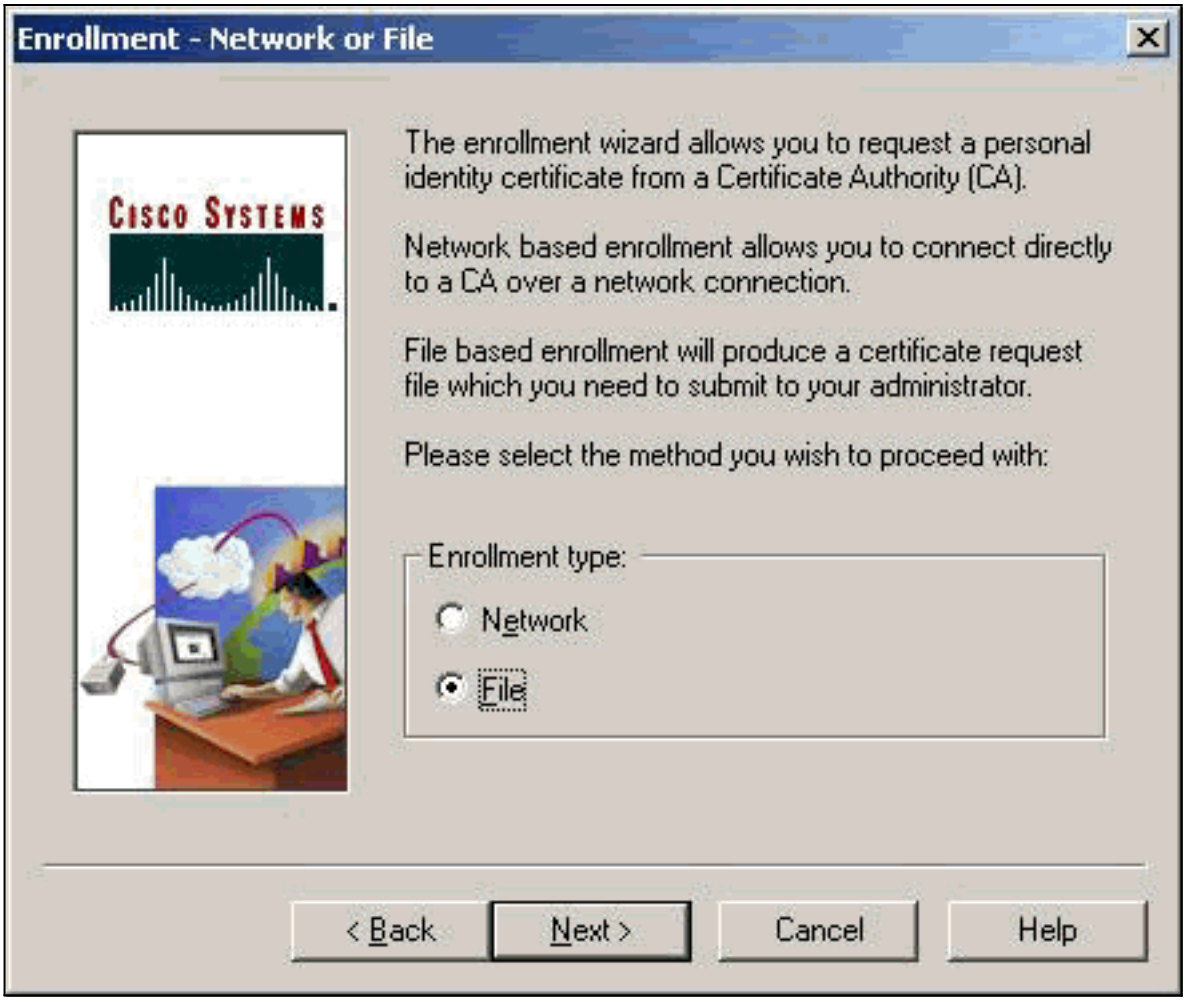
2. Personal Certificates タブを選択し、『New』 をクリック して下さい。



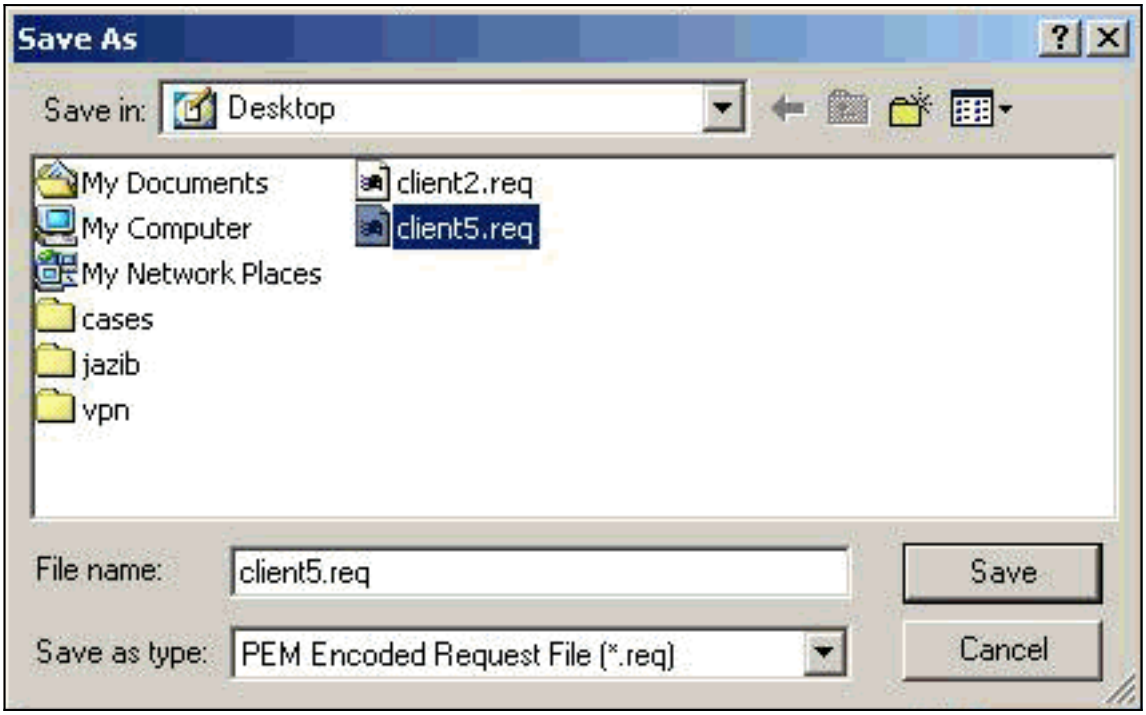
注: VPN 接続のためのユーザを認証するマシン認証は IPsec とすることができません。

3. VPN クライアントがパスワードのためにプロンプト表示するとき、証明書を保護するためにパスワードを規定 して下さい。 証明書のプライベートキーへのアクセスを必要とするどのオペレーションでも規定 されたパスワードが続くように要求します。

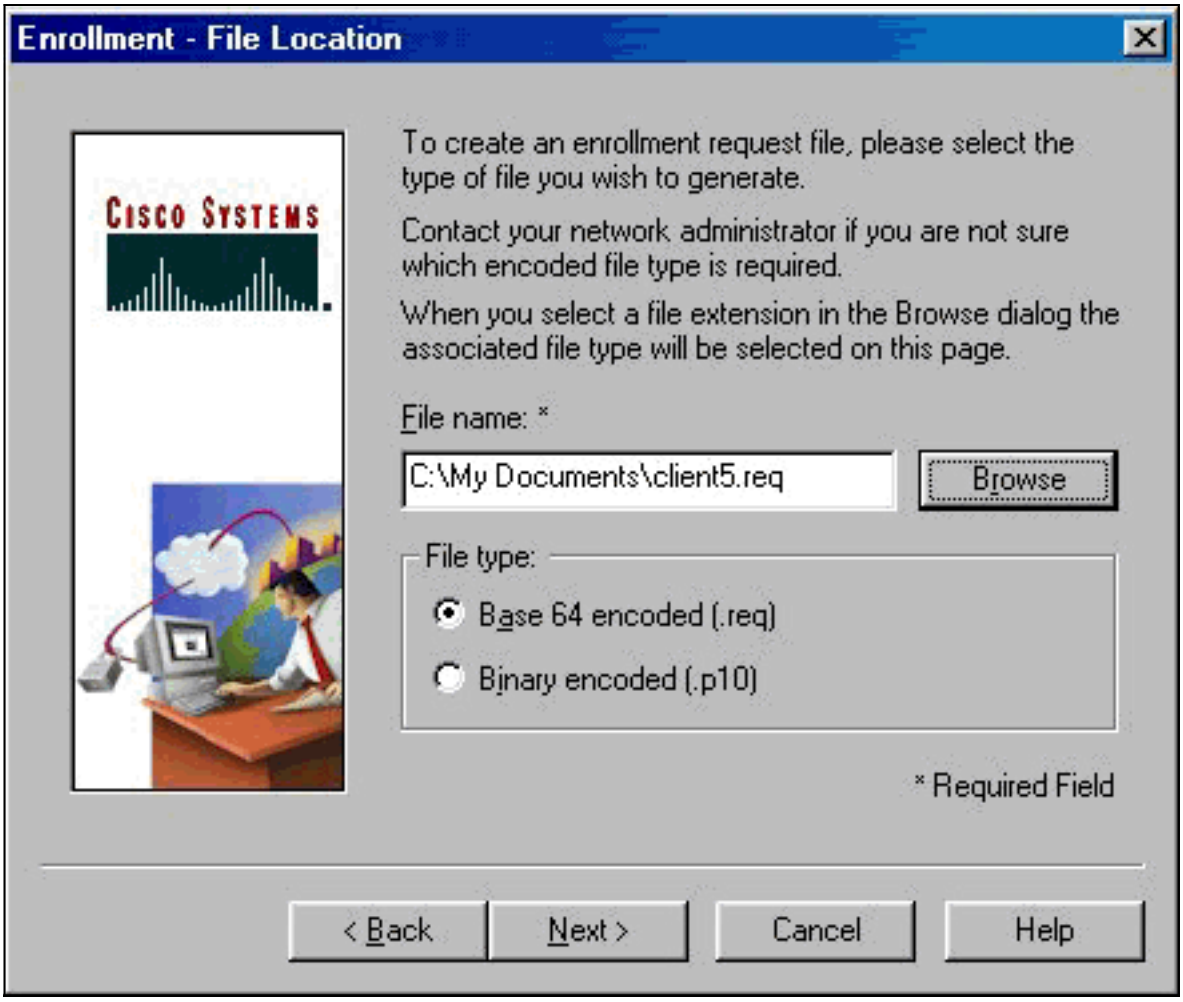
4. 登録ページの PKCS #10 フォーマットを使用して証明書を要求するために『File』 を選択して下さい。 次に [Next] をクリックします。



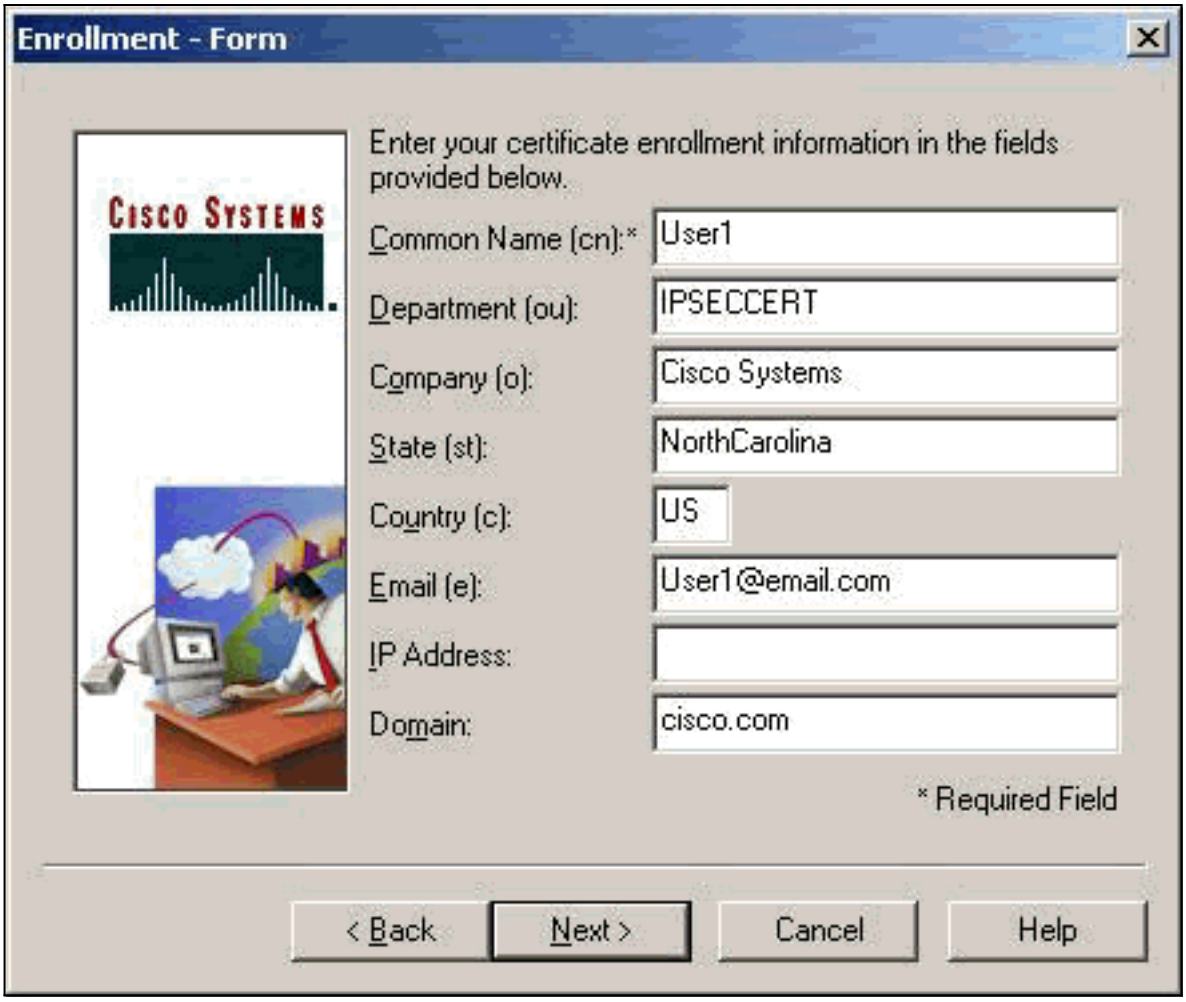
5. 『Browse』 をクリック し、証明書要求ファイルのためのファイル名を指定して下さい。 ファイルタイプに関しては、選定された **PEM は符号化された要求ファイル (*.req)** および『SAVE』 をクリック します。



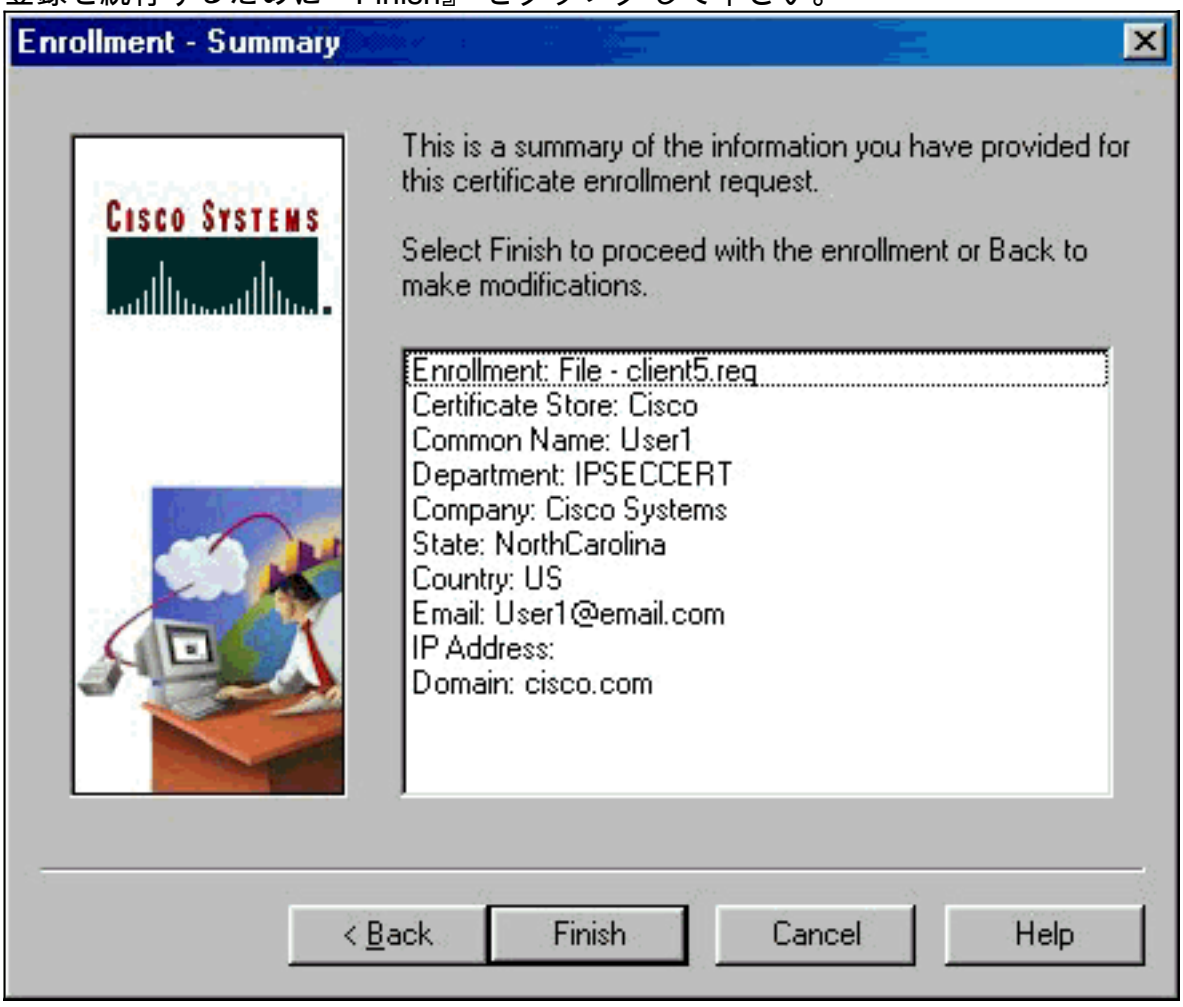
6. VPN クライアント登録ページで『Next』 をクリック して下さい。



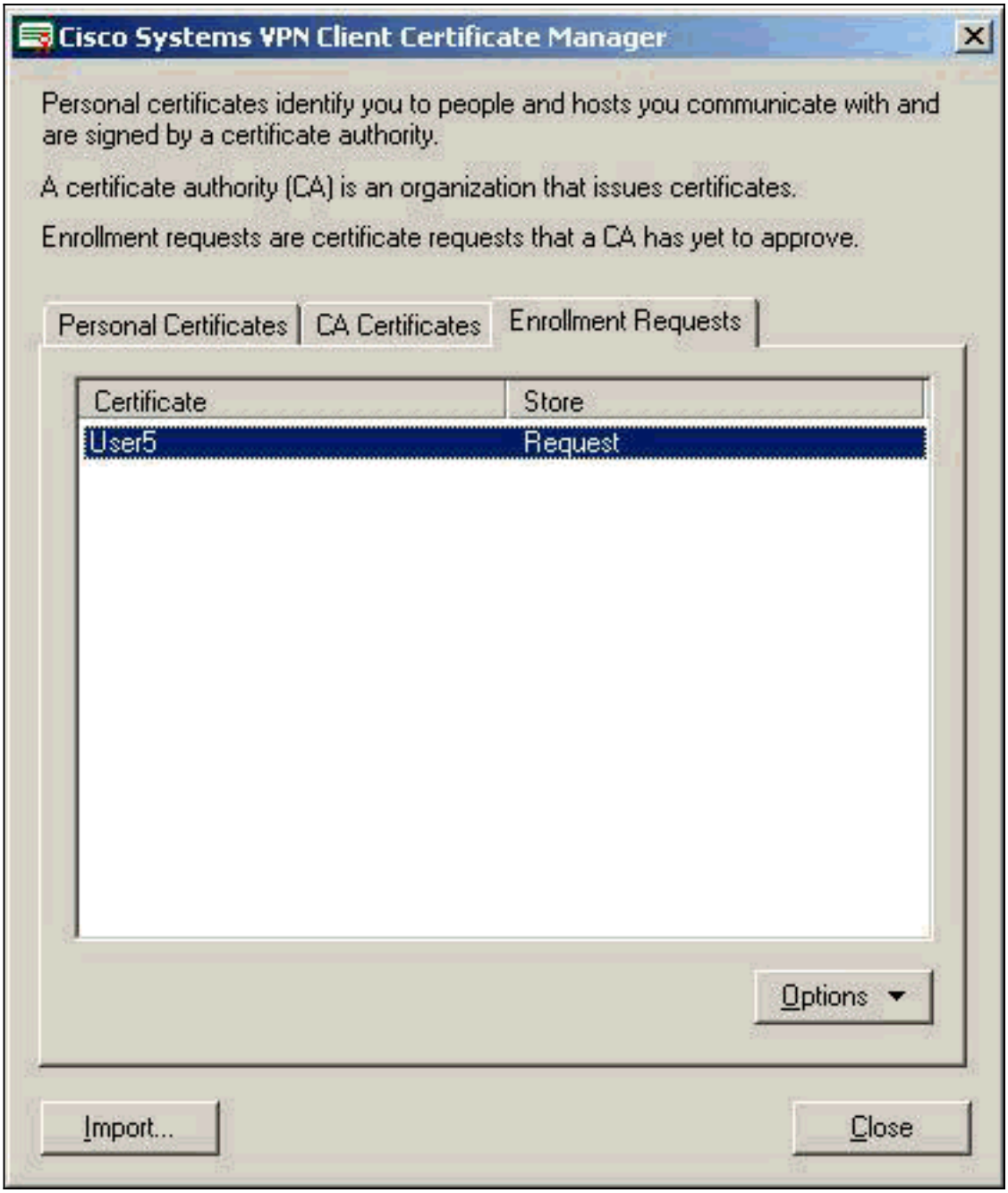
7. 登録形式のフィールドに記入して下さい。この例はフィールドを示したものです:Common Name = User1部門 = IPSECCERT（これは VPN 3000 コンセントレータの Organizational Unit（OU）およびグループ名を一致する必要があります。）会社 = Cisco 社状態 = ノースカロライナ国 = 米国メール = User1@email.comIP アドレス =（オプション; 証明書要求の IP アドレスを規定 するのに使用しました）ドメイン = cisco.com読み終わったら [Next] をクリックします。



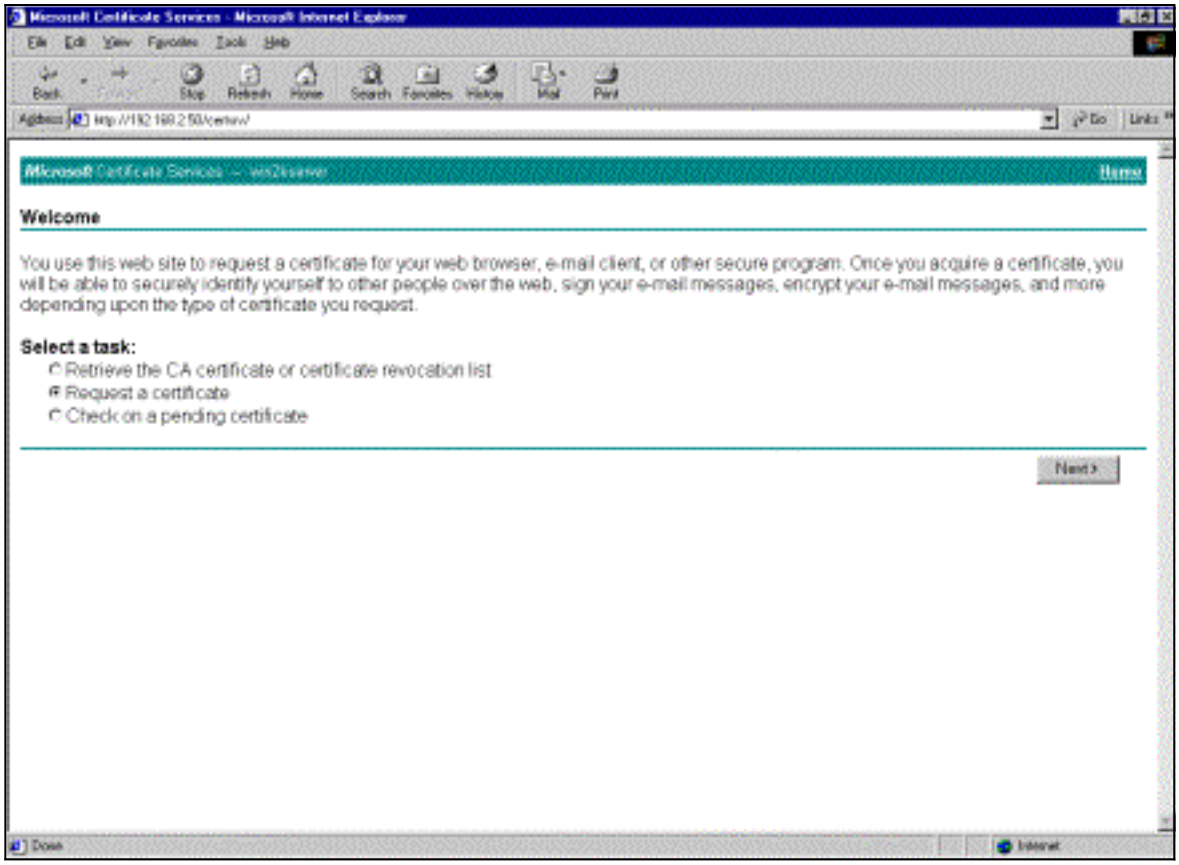
8. 登録を続行するために『Finish』 をクリック して下さい。



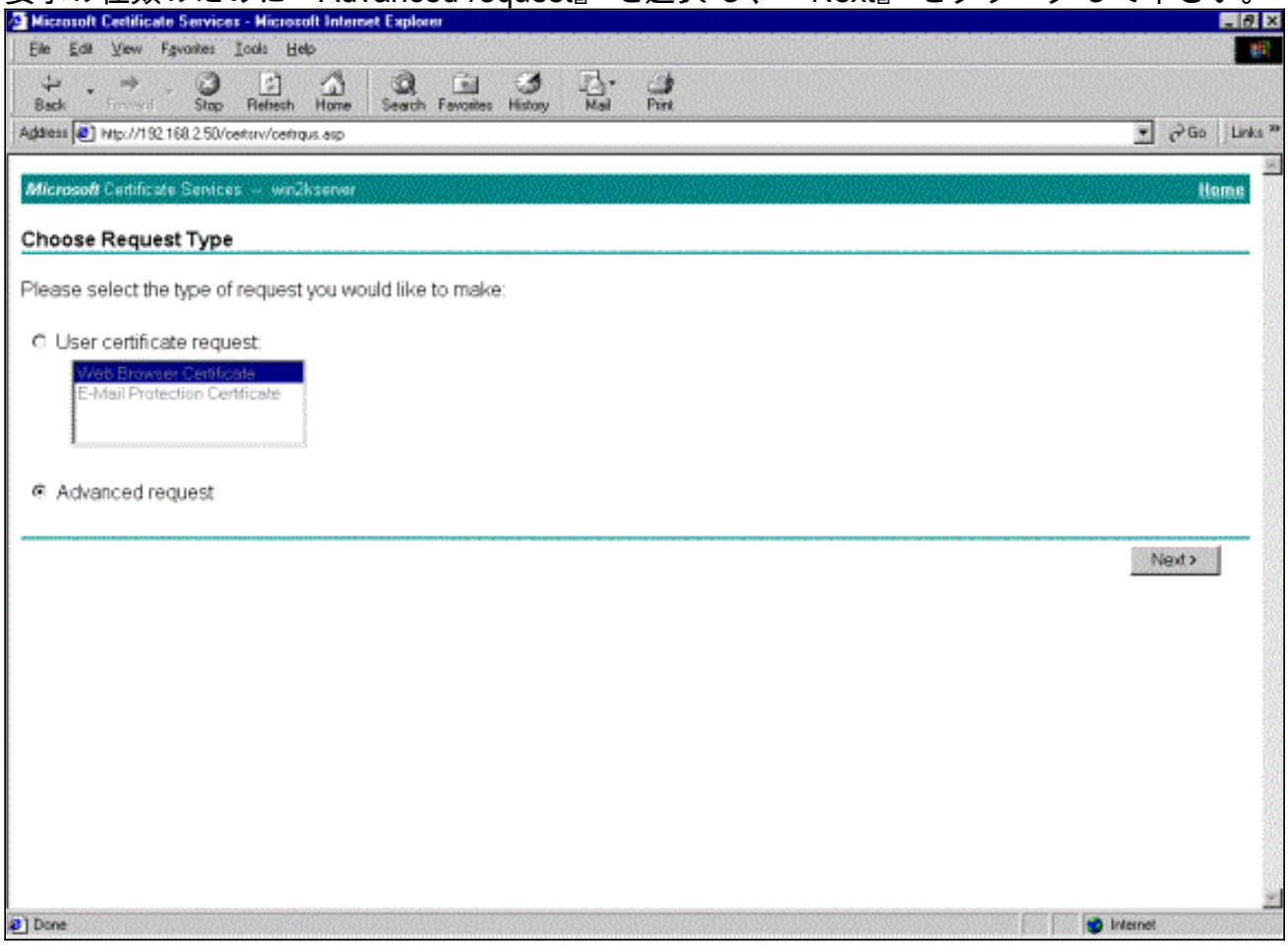
9. VPN クライアント 認証マネージャの要求をチェックするために Enrollment Requests タブを選択して下さい。



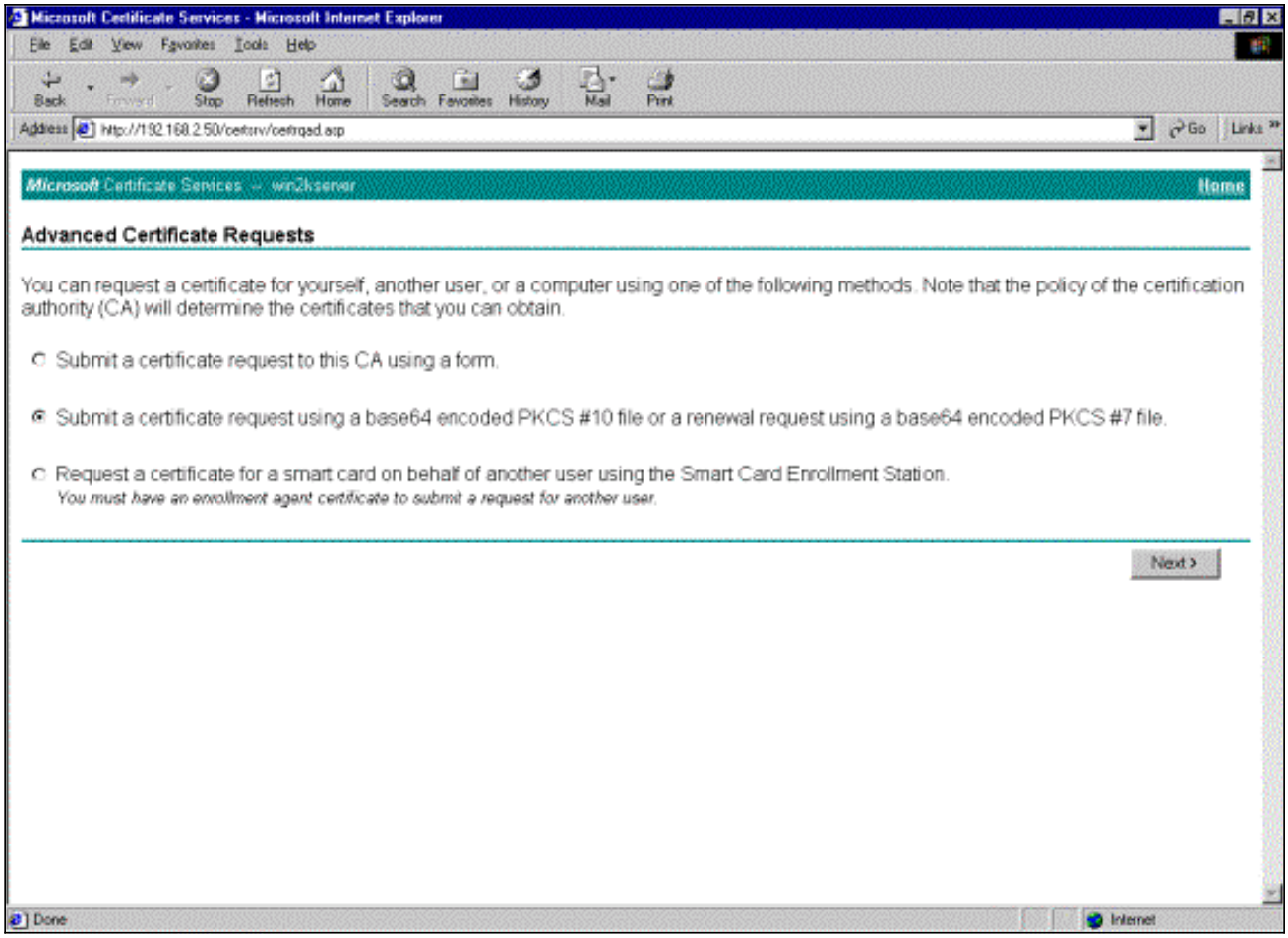
10. 始動は Certification Authority（CA）サーバおよび VPN クライアント要求を入れるために同時にインターフェイスします。
11. CA サーバで『Request a certificate』 を選択 し、『Next』 をクリック して下さい。



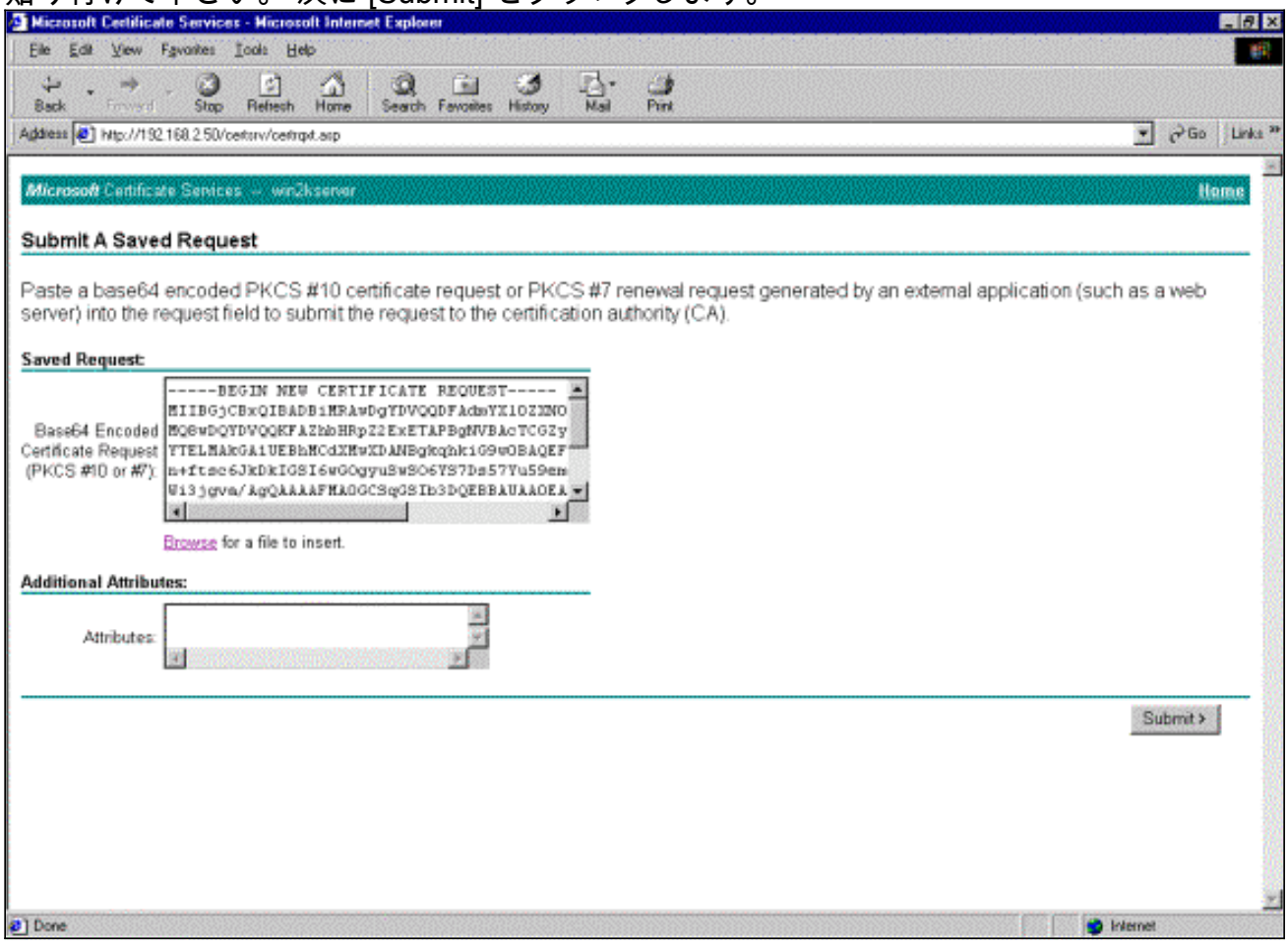
12. 要求の種類のために『Advanced request』 を選択 し、『Next』 をクリック して下さい。



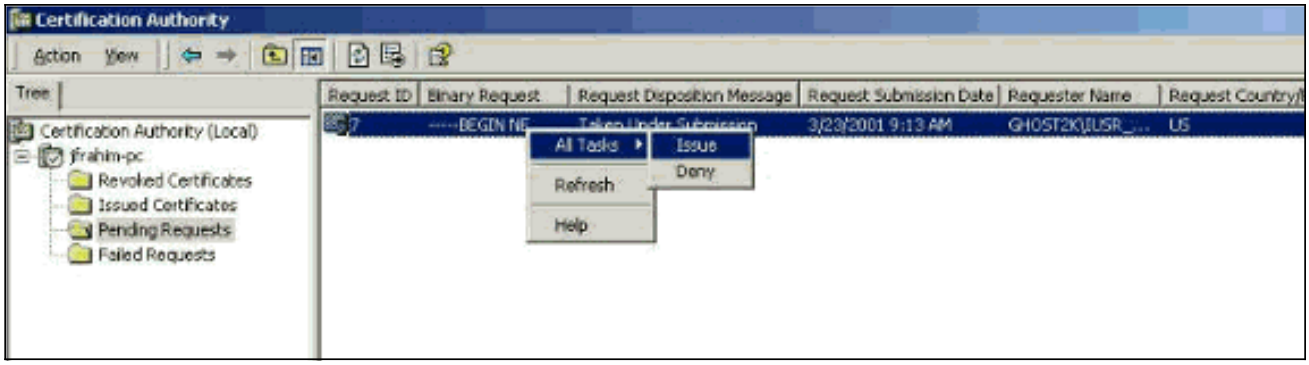
13. 高度証明書要求の下で『Submit a certificate request using a base64 encoded PKCS -10 file or a renewal request using a base64 encoded PKCS -7 file』 を選択 し、次に『Next』 をクリック して下さい。



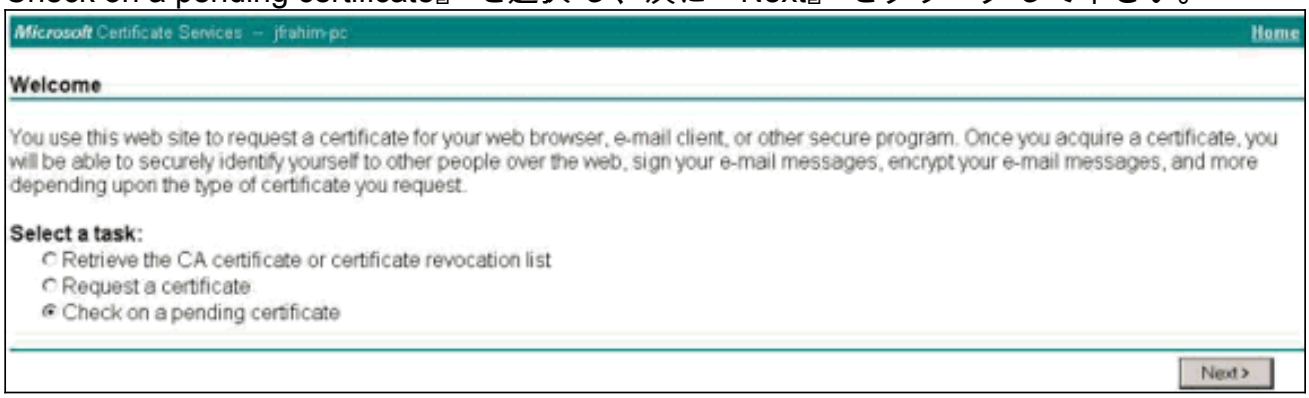
14. VPN クライアント要求ファイルをハイライト表示し、CA サーバに保存 された 要求の下に貼り付けて下さい。 次に [Submit] をクリックします。



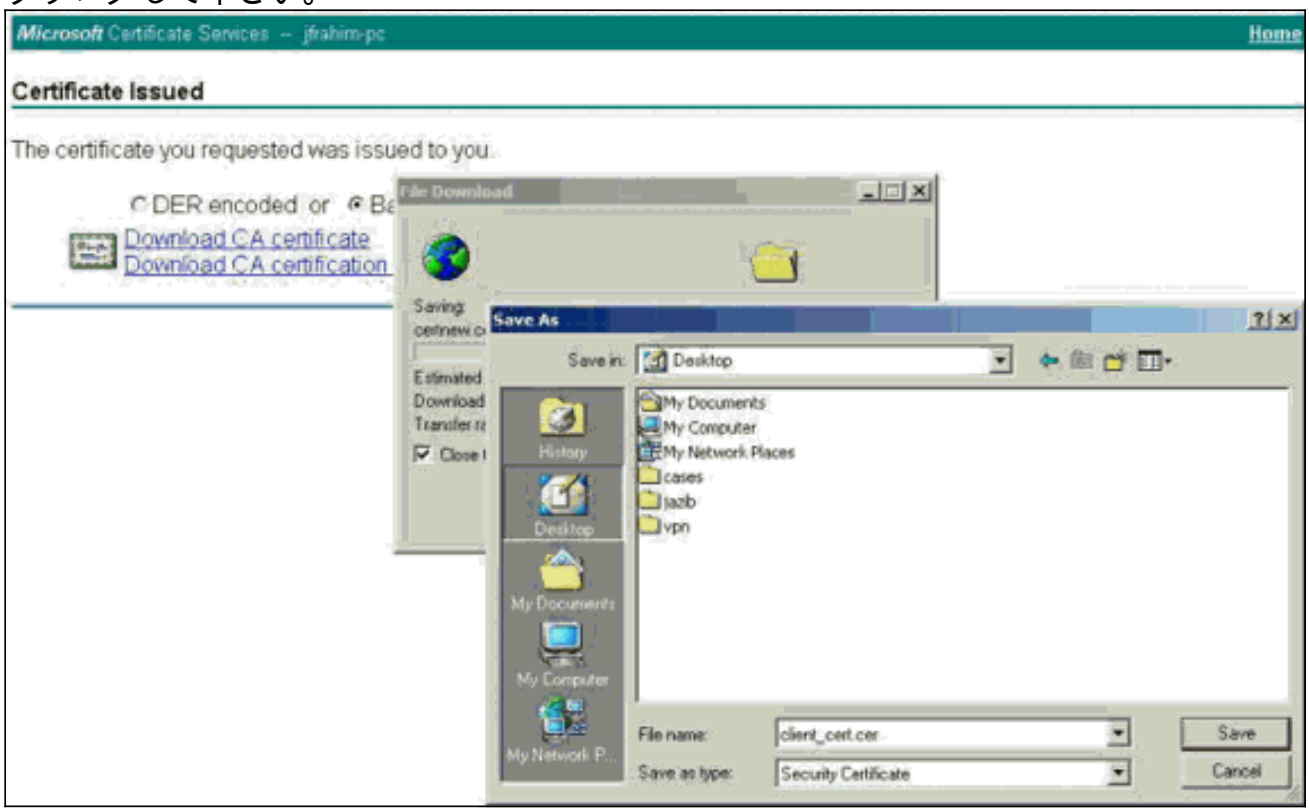
15. CA サーバで、VPN クライアント要求のための ID証明を発行して下さい。



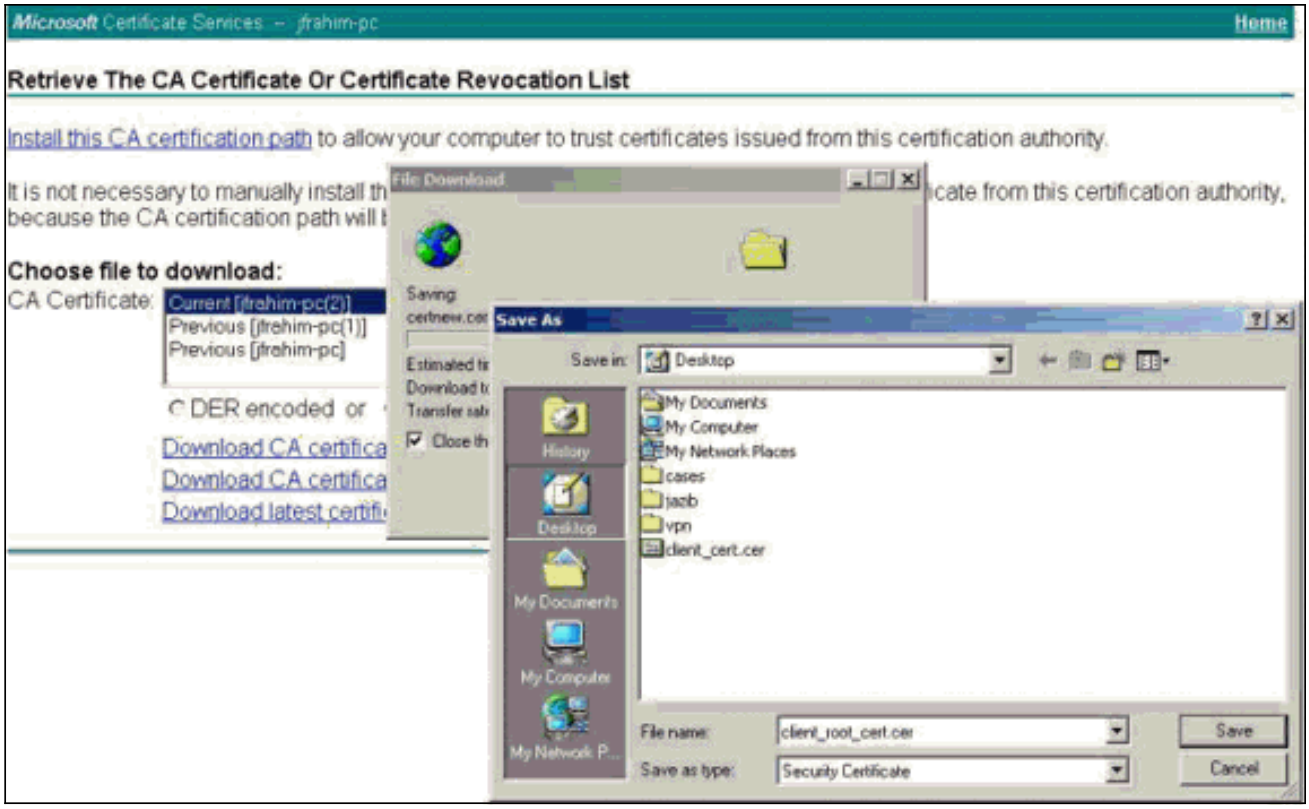
16. VPN クライアントにルートおよび ID証明をダウンロードして下さい。 CA サーバで、『Check on a pending certificate』 を選択 し、次に『Next』 をクリック して下さい。



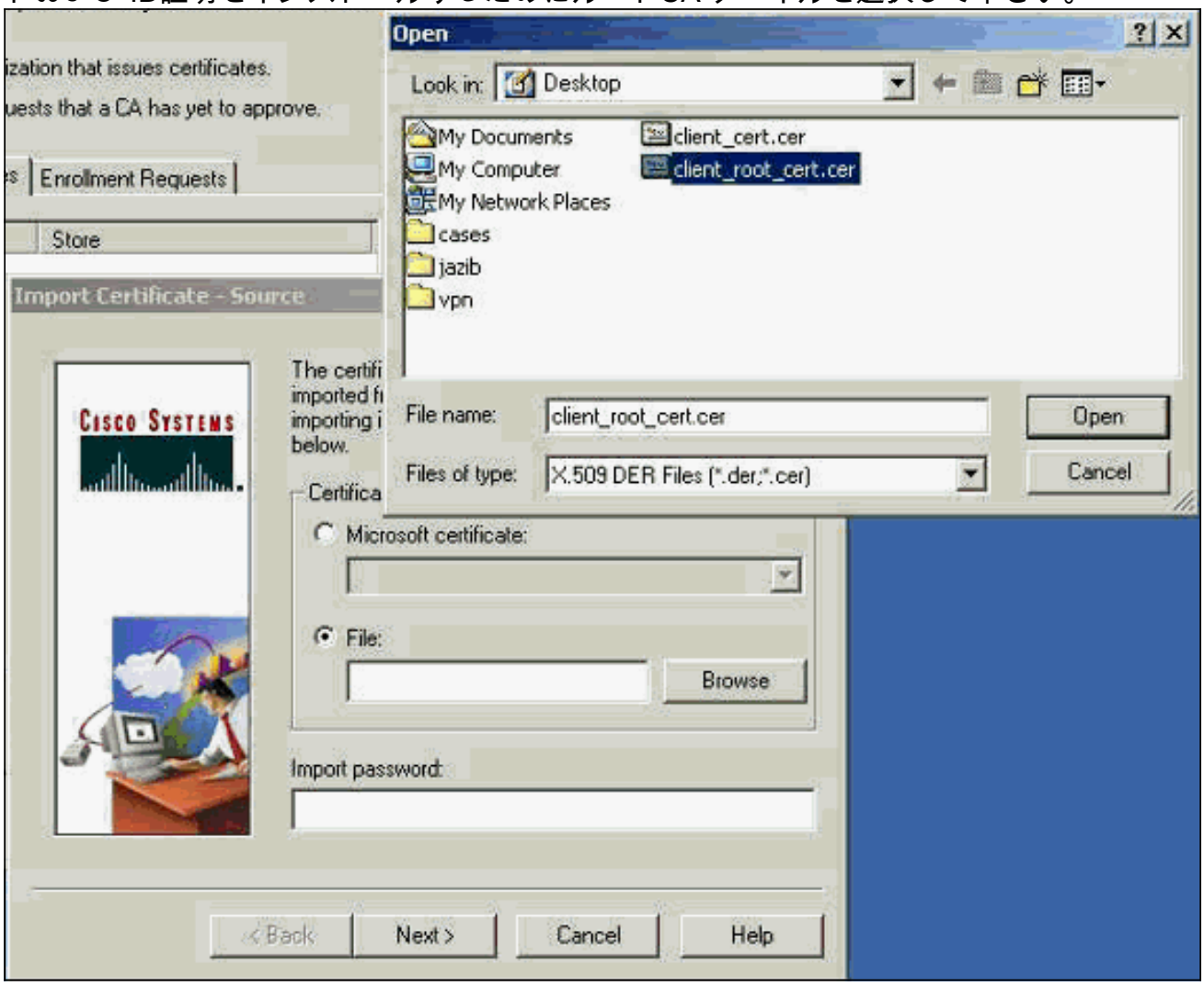
17. [Base 64 encoded] を選択します。 それから CA サーバで『Download CA certificate』 をクリック して下さい。



18. Retrieve the CA certificate or certificate revocation list ページから CA サーバのルート証明を得るためにダウンロードするようにファイルを選択して下さい。 次に [Next] をクリックします。

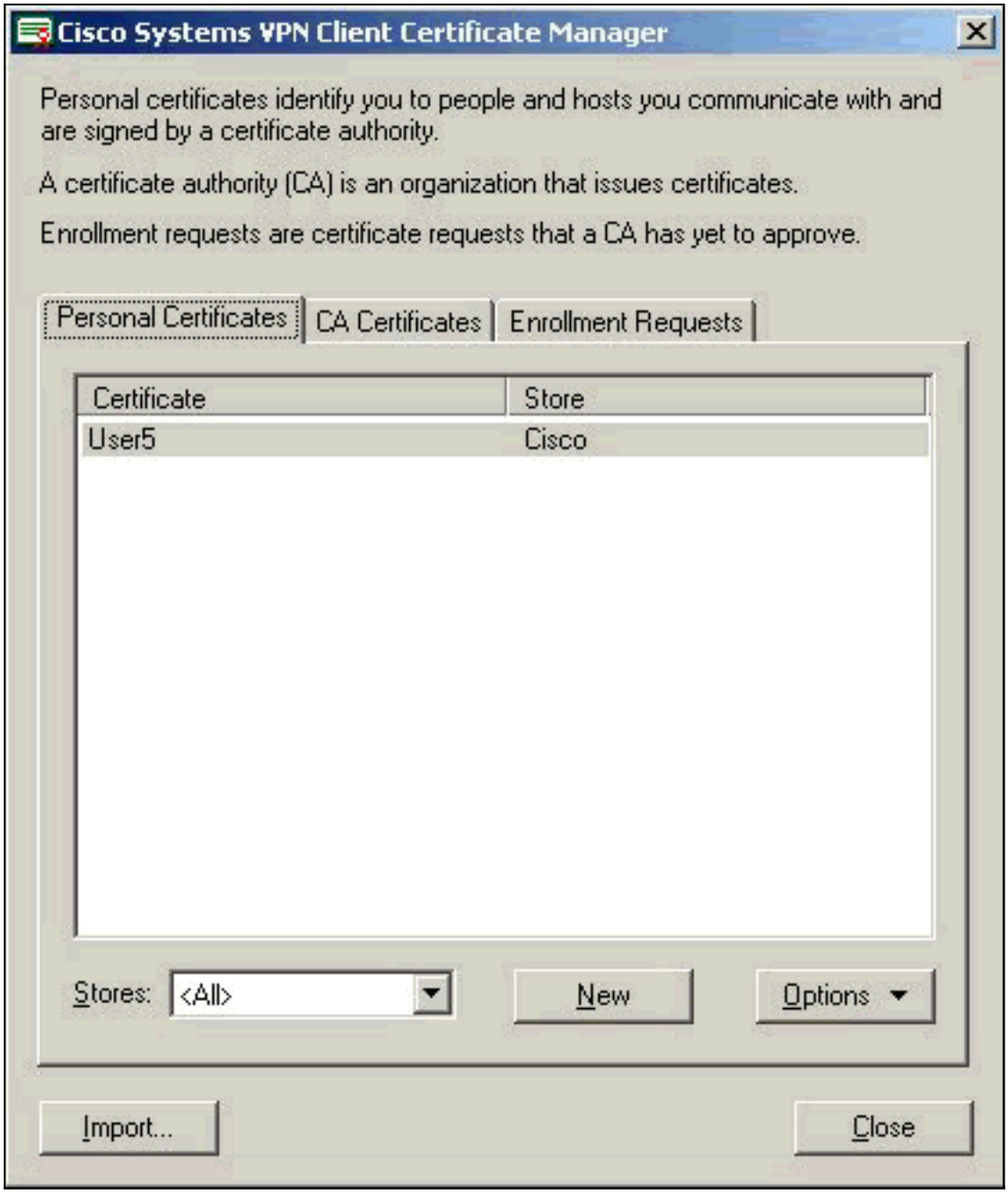


19. Certificate Manager > CA Certificate > Import on the VPN Client の順に選択 し、次にルートおよび ID証明をインストールするためにルートCA ファイルを選択して下さい。

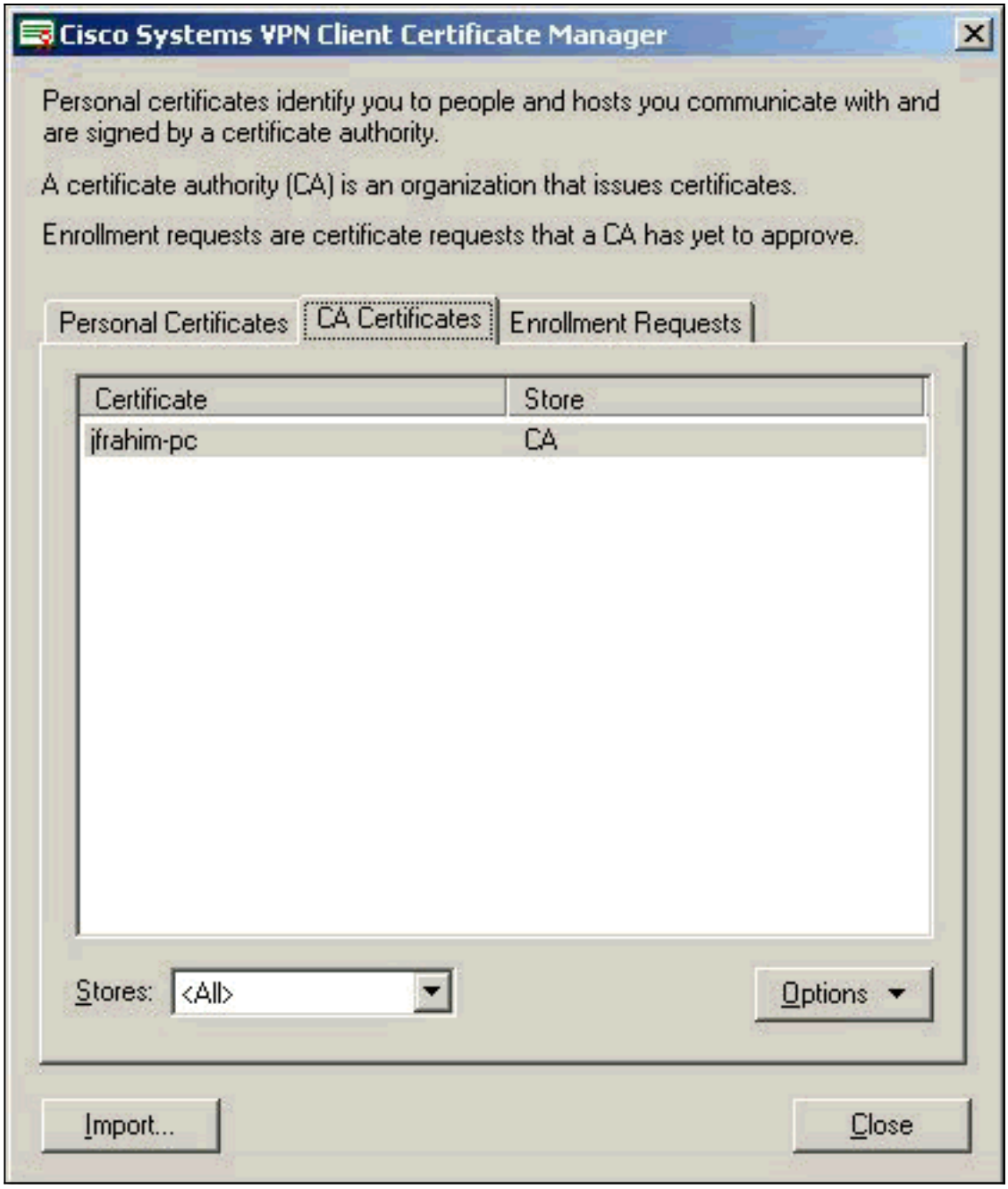


20. Certificate Manager > Personal Certificates > Import の順に選択 し、ID証明ファイルを選択して下さい。

21. ID証明が Personal Certificates タブの下で現われるようにして下さい。



22. ルート証明が CA Certificates タブの下で現われるようにして下さい。



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 サーバによって登録するように試みるときこのエラーメッセージを生成できます。

```
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を受け取る場合、詳細については Microsoft CA ログを参照するか、または詳細についてはこれらのリソースを参照して下さい。

- Windows は要求を処理する認証局を見つけることができません
- XCCC: " Your Certificate Request was Denied " エラーメッセージはセキュア会議のために証明書を要求すると発生します

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