



Enrolling and Managing Certificates

This chapter explains how to enroll and manage personal certificates, specifically, how to perform the following tasks:

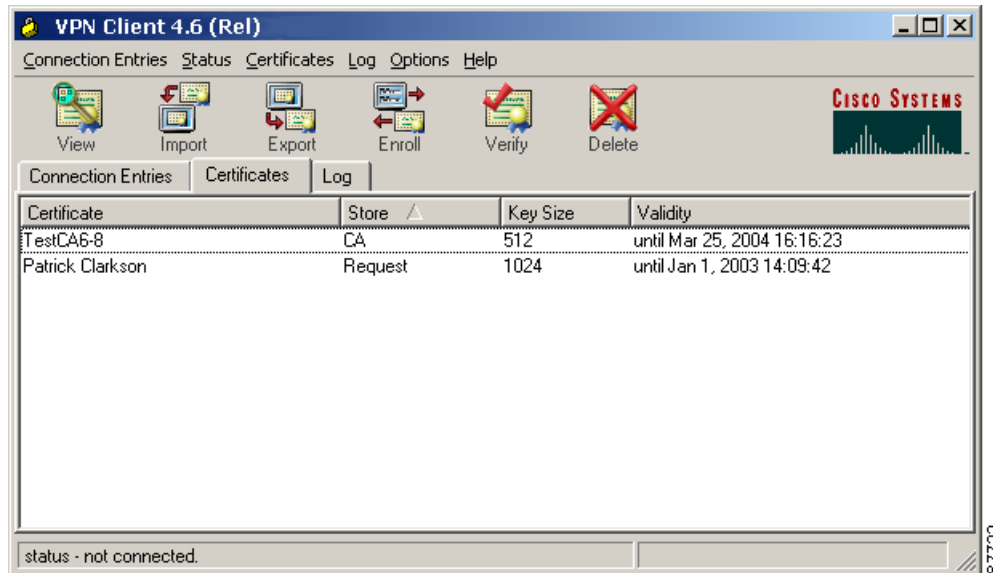
- Obtain personal certificates through enrollment with a certificate authority (CA), which is an organization that issues digital certificates that verify that you are who you say you are. (See [Using Certificate Stores](#) for a description of personal certificates.)
- Import certificates
- Manage certificates and enrollment requests

This chapter includes the following sections:

- [Using Certificate Stores](#)
- [Enrolling for a Certificate](#)
- [Managing Personal and CA/RA Certificates](#)
- [Managing Enrollment Requests](#)

To get started with certificates, open the Certificates tab on the VPN Client main window in advanced mode ([Figure 6-1](#)). The Certificates tab lists the certificates you currently have enrolled. If there are no certificate showing, you need to enroll with a CA or contact your system administrator.

Figure 6-1 Managing Certificates



The toolbar displays the tasks you can perform from the Certificates tab:

- View—Displays the details of the currently selected certificate (for example, common name, department and so on)
- Import—Imports a certificate from a file or certificate store
- Export—Exports the currently selected certificate
- Enroll—Enrolls for a certificate with a certificate authority via the network or a file
- Verify—Checks to see if the currently selected certificate has expired
- Delete—Removes the currently selected certificate or certificate request from the certificate store

Using Certificate Stores

A certificate *store* is a location in your local file system that contains personal certificates. The major store for the VPN Client is the Cisco store, which contains certificates you have enrolled for through the Simple Certificate Enrollment Protocol (SCEP). Your system also includes a Microsoft certificate store that may contain certificates that your organization provides or that you have installed previously. You can manage them just like the certificates in your Cisco store, or you can import them to your Cisco store. New certificates obtained through enrollment or importing go into the Cisco store.

There are two types of Microsoft certificates: certificates for individuals to use and a Microsoft certificate for your local PC itself. So, if several people are using the same PC, each person can have his or her own certificate, and there can also be a certificate for the local system on Windows 2000 and Windows XP. On a Windows 98 system, you can use only non-exportable certificates with Internet Explorer version 5.1 SP2.

Microsoft certificates with non-exportable private keys are also available.

The Certificates tab displays a list of the certificates currently in your certificate stores (Figure 6-1). The display shows the following information:

- Certificate—The name of the certificate

- **Store**—The name of the store that contains the certificate; this can be Cisco, Microsoft, Microsoft machine, Request, CA, or RA
- **Key Size**—The size of the key pair in bits (512, 1024, and so on) that protects the certificate
- **Validity**—Expiration date of the certificate

Enrolling for a Certificate

Your system administrator may have already set up your VPN Client with digital certificates. If not, or if you want to add certificates, you can obtain a certificate by enrolling with a Certificate Authority (CA) over the network or by creating a file request.

Enrolling Through the Network

When you enroll for a personal certificate, either you go through a CA from which your system already has a root certificate or you obtain a root certificate from the CA as part of the enrollment process. The CA Certificates tab displays the current list of CA certificates. (See [Figure 6-1](#).)

Use this section to gather the information before you begin. To enroll for a certificate with a CA over the network, follow this procedure:

-
- Step 1** In advanced mode, either click the **Enroll** icon on the toolbar above the Certificates tab or display the Certificates menu and choose **Enroll**.
- Step 2** Click **Online** as the certificate type. There are two forms to fill out.
- Step 3** Fill out the first form ([Figure 6-2](#)) as follows.

Figure 6-2 Online Enrollment Form

- **CA URL**—The URL or network address of the CA. This parameter is required.
- **CA Domain**—The CA's domain name. This parameter is required.

- **Challenge Password**—Some CA's require a password to access their site. If such is the case with this CA, enter the password in the Challenge Password field. To find out the password, contact the CA or your network administrator.
- **New Password**—The password that protects this certificate. If your connection entry requires certificate authentication, you must enter this password each time you connect. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords.

Step 4 Click **Next**. The VPN Client displays page two of the enrollment request (Figure 6-3).

Figure 6-3 Online Enrollment Form Page Two

Enter certificate fields, "*" denotes a required field:

Name [CN]*: Joe Smith

Department [OU]: Marketing

Company [O]: Some Company

State [ST]: Massachusetts

Country [C]: US

Email [E]: jsmith@somecompany.com

IP Address:

Domain: somecompany.com

Back Enroll Cancel

87736

- **Common Name**—Your common name (CN), which is the unique name for this certificate. This field is required. The common name can be the name of a person, system, or other entity; it is the most specific level in the identification hierarchy. The common name becomes the name of the certificate; for example, Alice Wonderland.
- **Department**—The name of the department to which you belong; for example, International Studies. This field correlates to the Organizational Unit (OU). The OU is the same as the Group Name configured in a VPN 3000 Series Concentrator, for example.
- **Company**—The name of the company or organization (O) to which you belong; for example, University.
- **State**—The name of your state (ST); for example, Massachusetts.
- **Country**—The 2-letter country code for your country (C); for example, US. This two-letter country code must conform to ISO 3166 country abbreviations.
- **Email**—Your email address (e); for example, alicew@university.edu.
- **IP Address**—The IP address of your system, for example, 10.10.10.1.
- **Domain**—The Fully Qualified Domain Name of the host for your system; for example, Dialin_Server.

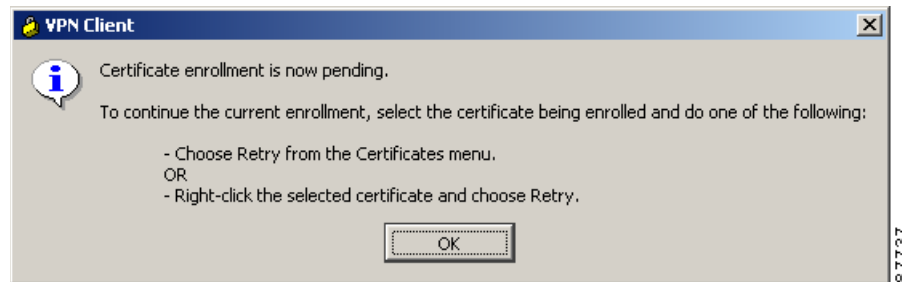
Together, all these fields except IP address and domain comprise your distinguished name (DN).

Step 5 To complete the enrollment, click **Enroll**. (Or to edit the form click **Back**).

What happens next depends on your CA.

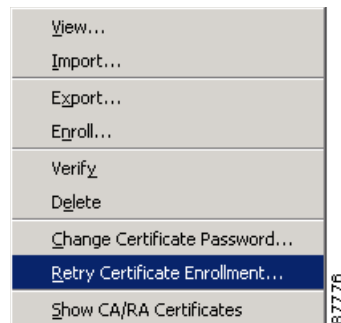
- Some CAs provide immediate response. If so, you see a message that your enrollment succeeded. You can view and manage the certificate under the Certificates tab.
- If the enrollment status is Request pending, your CA does not immediately approve your request. You see a status pending pop up window (Figure 6-4).

Figure 6-4 Enrollment Request Pending Message



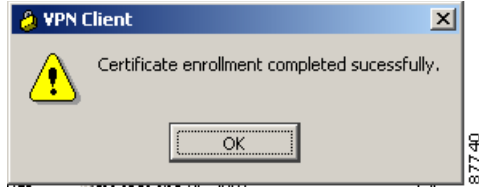
- While you are waiting for the CA to issue the certificate, your request appears in the certificates list under the Certificates tab as a request. (The store column shows “Request”.)
- When the CA issues your certificate, choose the certificate and then choose **Retry Certificate Enrollment** from the Certificates menu to complete the enrollment. (See Figure 6-5.)

Figure 6-5 Retrying Enrollment Request



- After you have obtained the certificate, you see a message that your enrollment succeeded (Figure 6-6).

Figure 6-6 Enrollment Request Succeeded Message



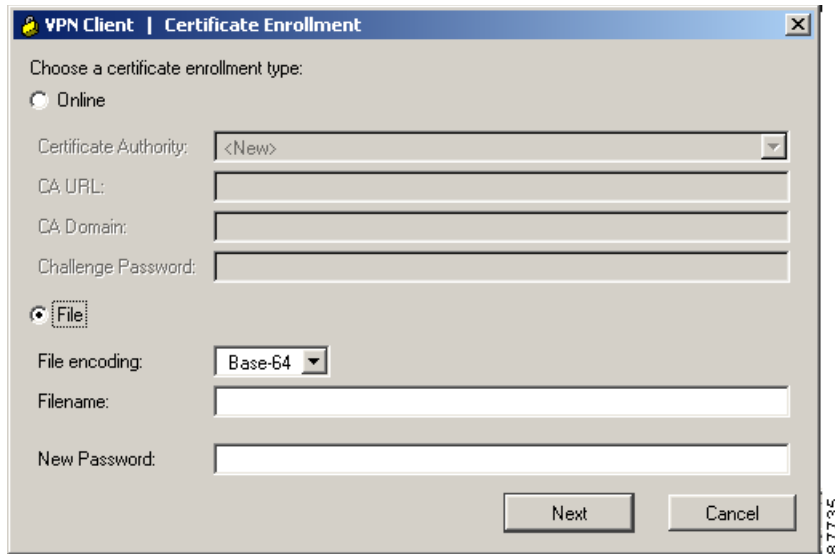
Enrolling Through a File Request

Alternatively, you can enroll by creating a file using much the same form as for online enrollment. (See [Figure 6-3](#).) Once you have created a request file, you can either e-mail it to the CA and receive a certificate back or you can access the CA's Web site and cut and paste the enrollment request in the area that the CA provides.

To enroll through a file request, use the following procedure:

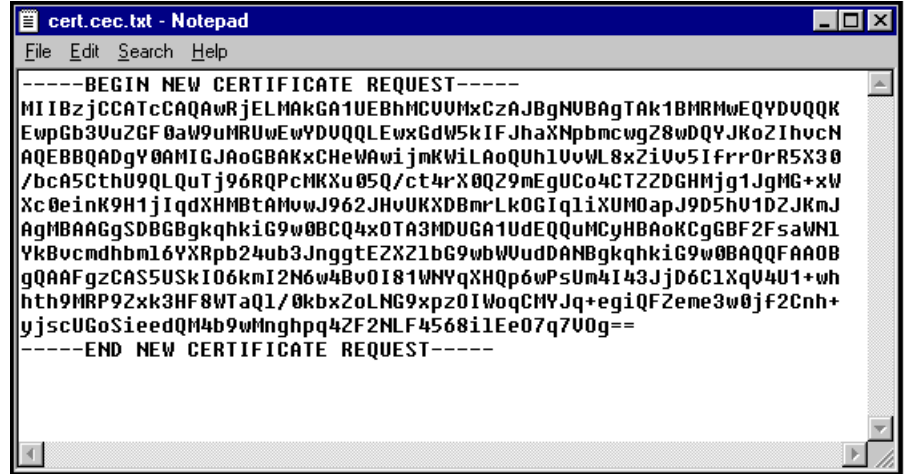
-
- Step 1** On the Certificate Enrollment dialog box (see [Figure 6-7](#)), click **File** as the certificate type.

Figure 6-7 Enrolling a Certificate Using a File Request



- Step 2** Click one of the following file types:
- **Binary encoded**—A base-2 PKCS10 file (Public Key Cryptography Standard; for example, an X.509 DER file). You cannot display a binary-encoded file.
 - **Base 64 encoded**—An ASCII-encoded PKCS10 file that you can display in text format (for example, the request shown in [Figure 6-8](#)). Choose this type when you want to cut and paste the text into the CA Web site.

Figure 6-8 A PKCS10 Certificate File



Step 3 In the Filename field, enter the full pathname for the file request.

When you browse for an appropriate directory for placing the file request, the Certificate Manager shows only the files of the chosen file type.

You can save your file enrollment requests in the Certificates directory, which is a subdirectory of the directory where the VPN Client is installed.

An example of a complete pathname is c:

\program files\cisco systems\vpn client\certificates\p10req3.p10.

Step 4 In the New Password field, enter the password that protects this certificate. If your connection entry requires certificate authentication, you must enter this password each time you connect. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords.

Step 5 Click **Next**. The VPN Client displays page two of the form. This form is the same as the one used for enrolling via the network. See “[Enrolling Through the Network](#)”.

Step 6 After completing the page two of the form, click **Enroll**.

The VPN Client displays a message to let you know whether your request succeeded. If successful, the message contains the name of the file. (See [Figure 6-9](#) and [Figure 6-10](#).)

Figure 6-9 Enroll File Success Message

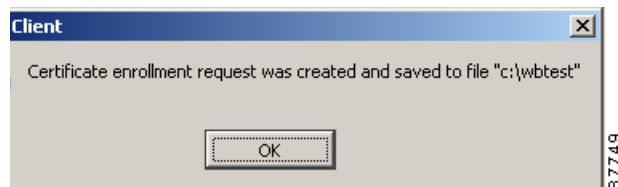
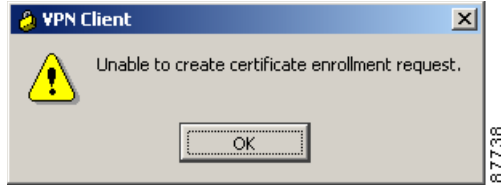


Figure 6-10 Enrollment Request Failed Message



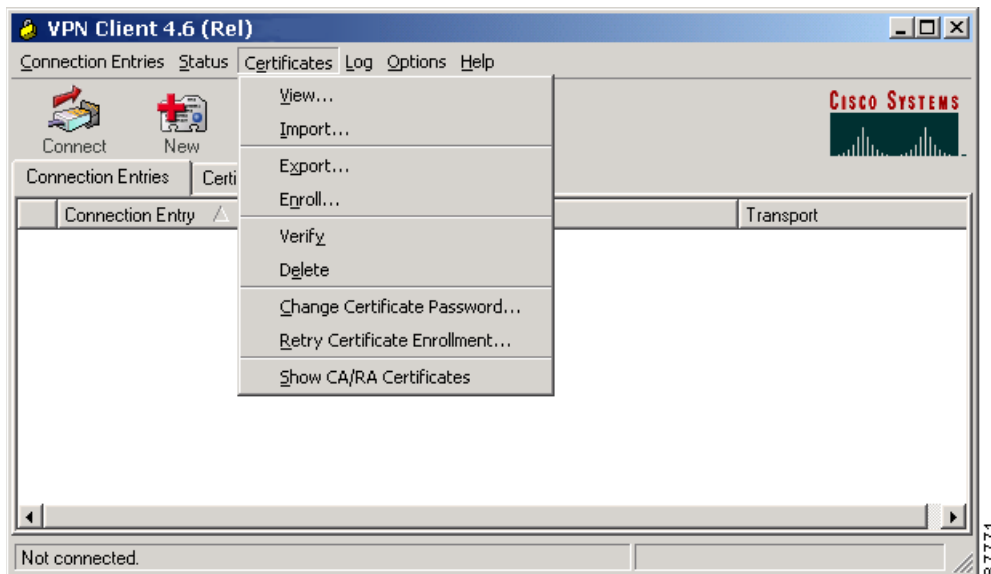
Step 7 Click **OK** to complete the file enrollment request.

Managing Personal and CA/RA Certificates

From the Certificates menu (Figure 6-11) or the toolbar above the Certificates tab, you can perform the following tasks to manage personal and CA/RA certificates.

- View a certificate
- Verify that a certificate is still valid (within the dates assigned to it and has not been revoked)
- Export a certificate to a file that you can e-mail
- Delete a certificate
- For personal certificates only, change the certificate password (Certificates menu only)
- For personal certificates only, retry certificate enrollment
- Show or hide CA/RA certificates

Figure 6-11 Certificates Menu



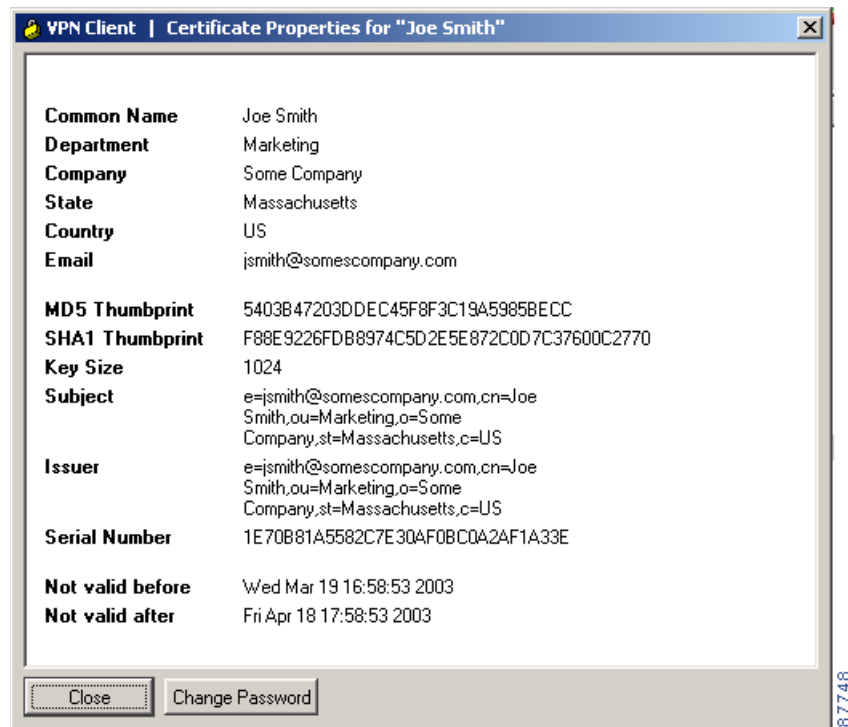
Viewing a Certificate

To display a certificate, select it in the certificate store, then do one of the following:

- Open the Certificates menu and choose **View**
- Click **View** on the toolbar above the Certificates tab
- Double-click the certificate

Figure 6-12 shows a sample certificate from a Microsoft certificate service provider. This is only an example. Not all certificates are guaranteed to look like this one.

Figure 6-12 Viewing a Certificate



A typical certificate such as that shown in Figure 6-12 contains the following information.

- **Common Name**—The name of the owner, usually the first name and last name. This field identifies the owner within the Public Key Infrastructure (PKI organization).
- **Department**—The name of the owner's department, which is same as the Organizational Unit (OU). Note that when connecting to a VPN 3000 Concentrator, the OU should generally match the Group Name configured for the owner in the VPN 3000 Concentrator.
- **Company**—The organization where the owner is using the certificate.
- **State**—The state where the owner is using the certificate.
- **Country**—The two-character country code where the owner's system is located.
- **Email**—The email address of the owner of the certificate.

- **Thumbprint**—The MD5 and SHA-1 hash to the certificate’s complete contents. This provides a way to validate the certificate’s authenticity. For example, if you contact the issuing CA, you can use this identifier to verify that this is the correct certificate to use.
- **Key Size**—The size of the signing key pair in bits; for example, 1024.
- **Subject**—The fully qualified distinguished name (DN) of certificate’s owner. This specific example includes the following parts. Other items may be included, depending on the certificate type. However, these fields are fairly standard.
 - cn is the common name.
 - ou is the organizational unit (department)
 - o is the organization
 - l is the locality (city or town).
 - st is the state or province of the owner.
 - c is the country.
 - e is the email address of the owner.
- **Issuer**—The fully qualified distinguished name (DN) of the source that provided the certificate. The fields in this example are the same as for Subject.
- **Serial Number**—A unique identifier used for tracking the validity of the certificate on Certificate Revocation Lists (CRLs).
- **Not Before**—The beginning date that the certificate is valid.
- **Not After**—The end date beyond which the certificate is no longer valid.

Importing a Certificate File

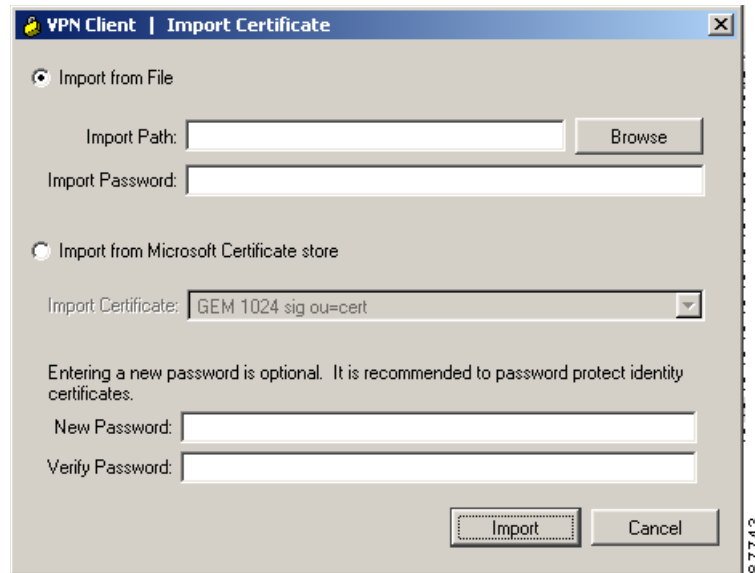
You can import a certificate into the Cisco store from the Microsoft store or from a file. The procedures vary slightly.

Importing a Certificate from a File

To import a certificate from a file, use the following procedure:

-
- Step 1** Display the Certificates menu and choose **Import** or click the **Import** icon above the Certificates tab. The Certificate Manager displays the Import Certificate Source dialog box. (See [Figure 6-13](#).)

Figure 6-13 Importing a Certificate from File



Step 2 Select **Import from File** (the default).

Step 3 Complete the **Import Certificate** form:

- **Import Path**—The complete pathname for the certificate. You can type the name or browse your file system to locate the file.
- **Import Password**—This password must exactly match the password given during enrollment (online) or given when exported (if a file), including upper and lower case letters. For example, *sKate8* is not exactly the same as *Skate8*. In online enrollment, this password is kept with the certificate; in file enrollment, this password is not retained.
- **New Password**—The password to be stored with the certificate. Use this password to protect the certificate while it is in the certificate store. This password is optional but we recommend that you always protect your certificate with a password.
- **Verify Password**—The password that you enter here must match what you entered in the **New Password** field.

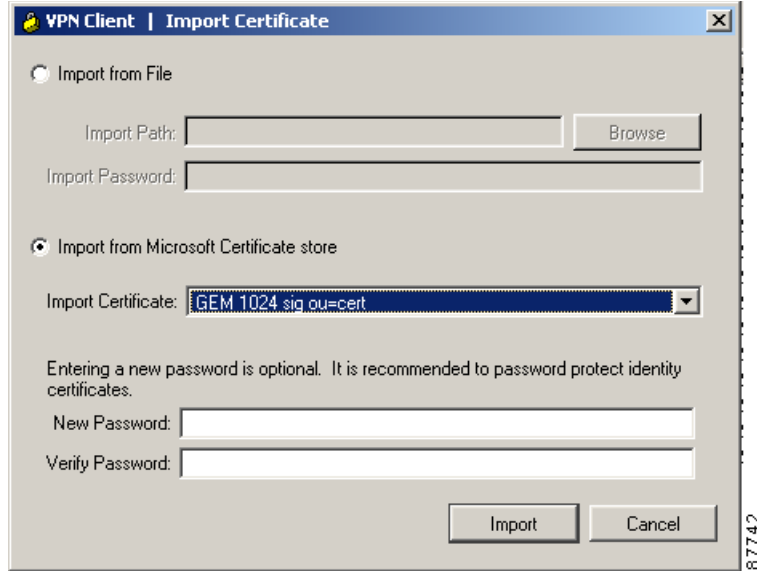
Step 4 To complete the import request, click **Import** or to cancel your request click **Cancel**.

Importing a Certificate from the Microsoft Certificate Store

To import a certificate from the Microsoft Certificate store, use the following procedure:

- Step 1** Display the **Certificates** menu and choose **Import** or click the **Import** icon above the **Certificates** tab. The Certificate Manager displays the **Import Certificate** dialog box. (See [Figure 6-14](#).)

Figure 6-14 Importing a Certificate from the Microsoft Certificate Store



- Step 2 Select Import from Microsoft Certificate store.
- Step 3 New Password—The case-sensitive password to be stored with the certificate. This password is optional but we recommend that you always protect your certificate with a password.
- Step 4 Verify Password—The password that you enter here must match what you entered in the New Password field.
- Step 5 To complete the import request, click **Import** or to cancel your request click **Cancel**.

Verifying a Certificate

To see whether the certificate is valid, choose it in the certificate store, follow these steps:

- Step 1 Select the certificate from the certificate store under the Certificates tab
- Step 2 Display the Certificates menu, and choose **Verify** or click the **Verify** icon on the toolbar above the Certificates tab.

The VPN Client displays a message such as the one in [Figure 6-15](#) indicating whether the certificate is still valid.

Figure 6-15 Verifying a Certificate's Validity



The following table shows the messages you might see when you check the validity of your certificate

Message	Description
Certificate is not valid yet	The current date is prior to the certificate's valid start date. You must wait until the certificate becomes valid.
Certificate has expired	The current date is after the certificate's valid end date. You need to enroll for a new certificate.
Certificate signature is not valid	You do not have the CA certificate, or the CA certificate that you have may have expired. You might need to download or import the CA certificate.
Certificate <name> is valid	You have a working certificate enrolled.

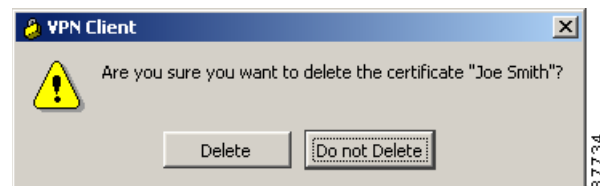
Step 3 After viewing the message, click **OK**.

Deleting a Certificate

To delete a certificate, follow this procedure:

- Step 1** Select the certificate from the certificate store under the Certificates tab (certificate store).
- Step 2** Display the Certificates menu and choose **Delete**, or click the **Delete** icon in the toolbar above the Certificates tab.
- If the certificate has a password, the VPN Client prompts you to enter it.
- Step 3** In the Password field, type the password given to the certificate during enrollment and click **OK**.
- Step 4** The VPN Client asks you to confirm that you want to delete this certificate (Figure 6-16). To delete the certificate, click **Delete**. To cancel the deletion, click **Do Not Delete** (the default).

Figure 6-16 Confirming Certificate Deletion



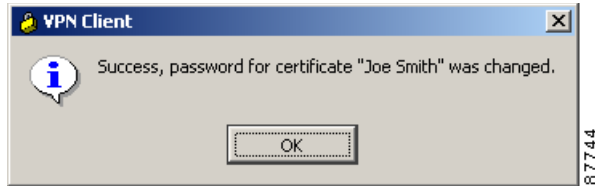
Changing the Password on a Personal Certificate

To change the password on a personal certificate, use this procedure:

- Step 1** Select a certificate from the certificate store under the Certificates tab.

- Step 2** Display the Certificates menu and choose **Change Certificate Password**
- The VPN Client displays the Change Certificate Password dialog box. In the Current field, type the password you are currently using to protect your private key.
- Step 3** In the New field, type the new password.
- Step 4** In the Confirm field, type the same password again.
- Step 5** Click **OK**. The VPN Client confirms that you have successfully changed your password (Figure 6-17).

Figure 6-17 Certificate Password Change Success Message



Exporting a Certificate

You may want to export a certificate, primarily for backing up your certificate and private key or moving them to another system. When you export a certificate, you are making a copy of it.

To export a certificate, follow these steps:

- Step 1** Display the Certificates menu and choose **Export** or click the **Export** icon on the toolbar above the Certificates tab.

The VPN Client displays the Export Certificate dialog box (Figure 6-18).

Figure 6-18 Exporting a Certificate



- Step 2** In the Export path field, enter the path for the exported certificate or use the Browse feature to locate a target directory for the exported certificate.
- Step 3** To export the CA and/or RA certificate with your personal certificate, check the **Export entire certificate chain** check box.
- Step 4** In the Password field, enter an optional password to protect the export file. Then enter it again in the Verify Password field.

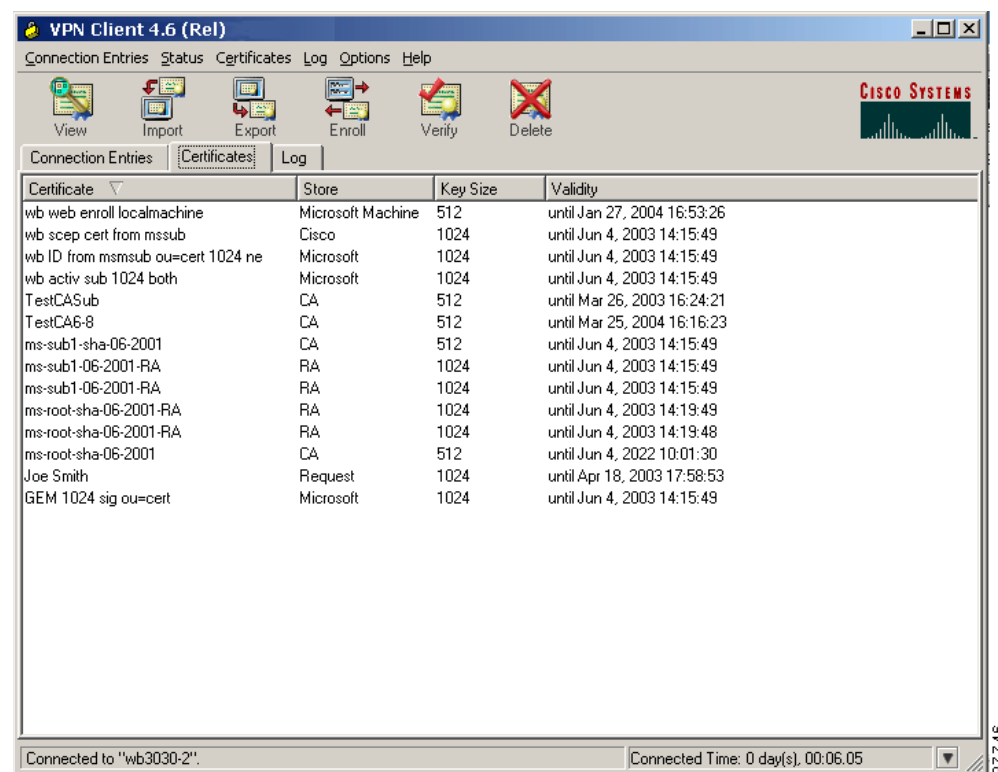
Step 5 After completing all the information, click **Export**.

The VPN Client displays a message indicating whether your certificate export was successful.

Showing CA/RA Certificates

You can view, but not modify, the current list of CA and RA certificates by selecting **Show CA/RA Certificates** from the Certificates menu. The VPN Client displays the list in a new window (Figure 6-19).

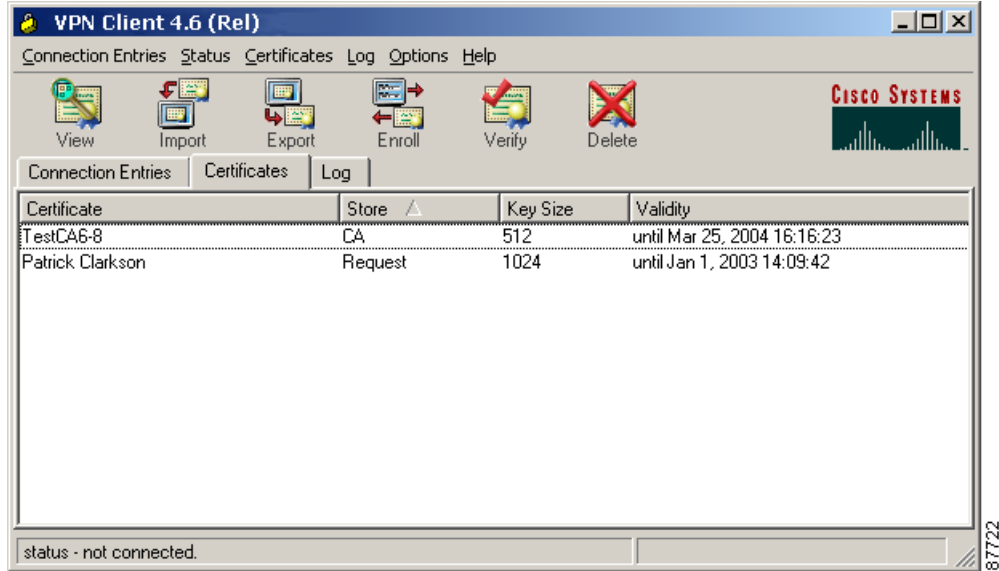
Figure 6-19 CA/RA Certificates List



Managing Enrollment Requests

While a request is pending approval by the CA administration, the VPN Client places the enrollment request in the list under the Certificates tab. You can view, delete, or change the password on any request in the list; or you can retry a network enrollment request. To perform any of these actions, click the Certificates tab and select the action on the Certificates menu. (See Figure 6-20.)

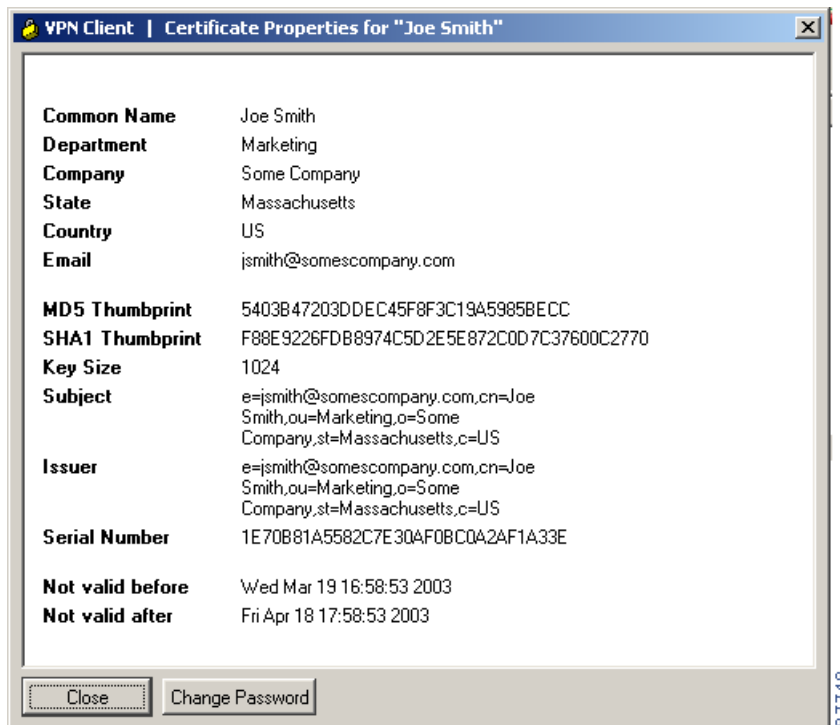
Figure 6-20 Managing Enrollment Requests



Viewing the Enrollment Request

To display the enrollment request, select the request, display the Certificates menu and choose **View** from the Certificates menu. The VPN Client displays the pending request. (See [Figure 6-21](#).)

Figure 6-21 Viewing an Enrollment Request



Note that the Issuer field shows the subject name and not the name of the CA, since the CA has not yet issued the certificate.

You can change the certificate request password from this screen.

Deleting an Enrollment Request

To delete an enrollment request, follow these steps:

-
- Step 1** Select the enrollment request, display the Certificates menu and choose **Delete**.
The VPN Client prompts you for a password.
- Step 2** Type the password in the Password field (if there is one) and click **OK**.
The VPN Client verifies the password. If the password is correct, the VPN Client deletes the request.
-

Changing the Password on an Enrollment Request

To change the certificate password on an enrollment request, use this procedure:

-
- Step 1** Select the certificate request in the list under the Certificates tab.
- Step 2** Display the Certificates menu and choose **Change Certificate Password**.
The VPN Client displays the Certificate Password dialog box. (See [Figure 6-22](#).)

Figure 6-22 Changing a Certificate Password



- Step 3** Type in the password you are currently using and click **OK**.
- Step 4** At the prompt, type the new password and click **OK**.
- Step 5** At the next prompt, type your new password again to verify it and click **OK**.
The VPN Client responds with a success message.



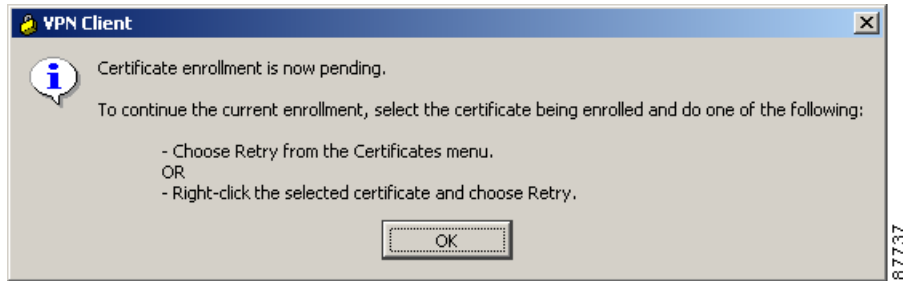
Note You can also change the password from the **View** dialog box.

Completing an Enrollment Request

To complete a pending online enrollment request, use the following procedure

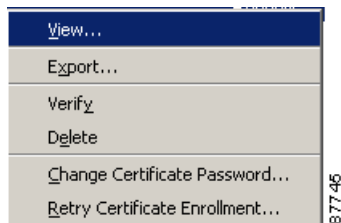
- Step 1** Select the request under the Certificates tab. The VPN Client displays a dialog box confirming the certificate's pending status and describing how to complete the enrollment procedure (Figure 6-23).

Figure 6-23 *Completing a Pending Online Certificate Enrollment Request*



- Step 2** Select the certificate being enrolled, then do one of the following:
- Choose **Retry** from the Certificates menu.
 - Right-click the selected certificate on the Certificates tab and choose **Retry** from the menu that appears (Figure 6-24).

Figure 6-24 *Right-Click Certificate Menu*



- Step 3** Click **OK** to close the dialog box.