Configuring and Managing Connection Entries

This chapter explains how to configure a connection entry for the VPN Client. The VPN Client uses a connection entry to identify and connect securely to a specific private network. To configure a connection entry, you enter values for a set of parameters, which include a name and description for the connection, the name or address of the VPN device (remote server), and information that identifies you to the VPN device.

Note If your system administrator has completely configured your connection entry for you, you can skip this chapter and go directly to "Connecting to a Private Network."

This chapter explains the following configuration tasks:

What Is a Connection Entry?

To use the VPN Client, you must create at least one connection entry, which identifies the following information:

- The VPN device (the remote server) to access
- Preshared keys—The IPSec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPSec algorithms your VPN Client uses.
- Certificates—The name of the certificate you are using for authentication
- Optional parameters that govern VPN Client operation and connection to the remote network

You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously) or if you belong to more than one VPN remote access group.

For connection entry parameters, see "Gathering Information You Need".

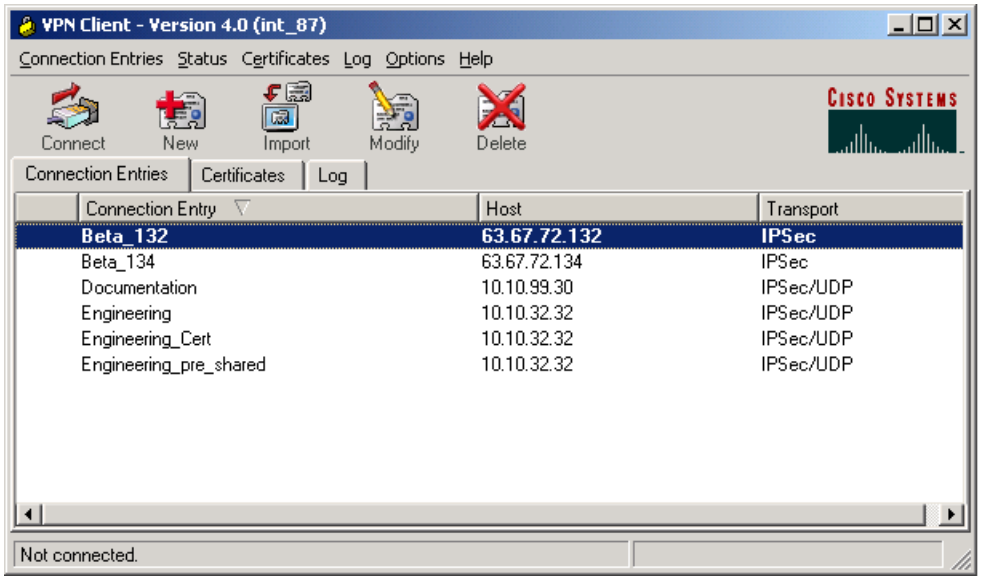
Creating a New Connection Entry

Use the following procedure to create a new connection entry.

Step 1 Start the VPN Client by choosing **Start > Programs > Cisco Systems VPN Client > VPN Client**.

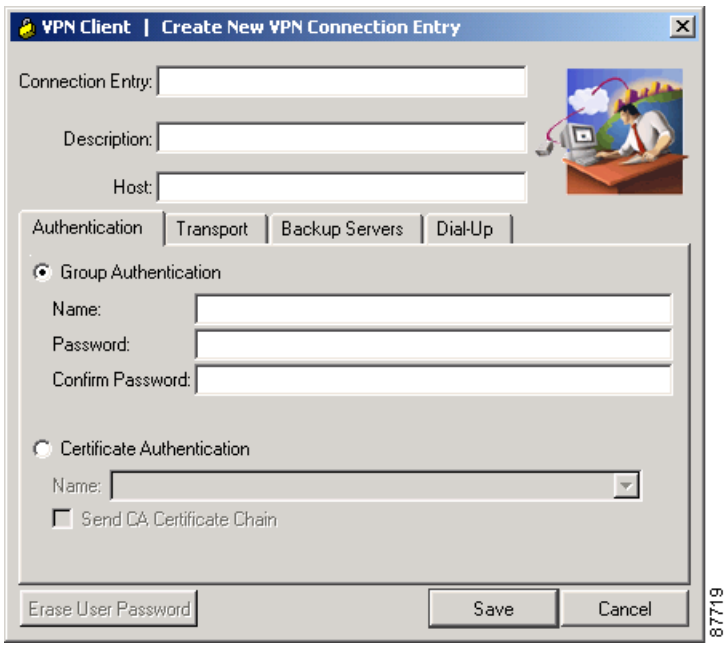
Step 2 The VPN Client application starts and displays the advanced mode main window (Figure 4-1). If you are not already there, open the Options menu in simple mode and choose **Advanced Mode** or press **Ctrl-M.**

Figure 4-1 VPN Client Main Window.



Step 3 Select **New** from the toolbar or the Connection Entries menu. The VPN Client displays a form (Figure 4-2).

Figure 4-2 Creating a New Connection Entry



Step 4 Enter a unique name for this new connection. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case-sensitive.

Step 5 Enter a description of this connection. This field is optional, but it helps further identify this connection. For example, Connection to Engineering remote server.

Step 6 Enter the hostname or IP address of the remote VPN device you want to access.

Choosing an Authentication Method

Under the Authentication tab, enter the information for the method you want to use. You can connect as part of a group (configured on a VPN device) or by supplying an identity digital certificate.

Group Authentication

For group authentication, use the following procedure:

Step 1 Click the **Group Authentication** radio button.

Step 2 In the Name field, enter the name of the IPSec group to which you belong. This entry is case-sensitive.

Step 3 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

Step 4 Verify your password by entering it again in the Confirm Password field.

Certificate Authentication

For certificate authentication, perform the following procedure, which varies according the type of certificate you are using:

Step 1 Click the **Certificate Authentication** radio button.

Step 2 Choose the name of the certificate you are using from the menu.

If the field says No Certificates Installed and is shaded, then you must first enroll for a certificate before you can use this feature. For information on enrolling for a certificate, see "Enrolling and Managing Certificates" or consult your network administrator.

Sending a Certificate Authority Certificate Chain

To send CA certificate chains, click **Send CA Certificate Chain**. This parameter is disabled by default.

The CA certificate chain includes all CA certificates in the hierarchy of certificates from the root certificate, which must be installed on the VPN Client, to the identity certificate. This feature enables the peer VPN Concentrator to trust the VPN Client's identity certificate given the same root certificate, without having all the same subordinate CA certificates actually installed.

Example 4-1 CA Certificate Chains

1. On the VPN Client, you have this chain in the certificate hierarchy:
   - Root Certificate
   - CA Certificate 1
   - CA Certificate 2
   - Identity Certificate
2. On the VPN Concentrator, you have this chain in the certificate hierarchy
   - Root Certificate
   - CA Certificate 3
   - Identity Certificate
3. Though the identity certificates are issued by different CAs, the VPN Concentrator can still trust the VPN Client's identity certificate, since it has received the chain of certificates installed on the VPN Client PC.

This feature provides flexibility since the intermediate CA certificates don't need to be actually installed on the peer.

Note Certificate chains are not supported for Entrust Entelligence. Therefore the Send CA Certificate Chain checkbox on the Authentication Tab is unchecked and disabled when you select Entelligence Certificate.

Validating a Certificate

Optionally you might want to verify that the certificate you are using is still valid, using the following procedure:

Step 1 Select the certificate in the list of certificates underneath the Certificates tab.

Step 2 Display the Certificates menu or right click on the certificate name, and choose **Verify.**

The VPN Client displays a message to let you know whether the certificate is valid.

Configuring an Entrust Certificate for Authentication

If you have an Entrust Entelligence certificate enrolled, the menu includes the entry "Entelligence Certificate (Entrust)." An Entrust Entelligence certificate is stored in a *Profile*, which you obtain when you log in to Entrust Entelligence.

Choose **Entelligence Certificate (Entrust)** from the menu.

For more information about connecting with Entrust Entelligence, see "Connecting with an Entrust Certificate."

Configuring a Connection Entry for a Smart Card

If you are using a smart card or electronic token to authenticate a connection, create a connection entry that defines the certificate provided by the smart card. For example, if you are using ActivCard Gold, an accompanying certificate is in the Microsoft Certificate Store. When you create a new connection entry for using the smart card, choose that certificate.

Smart Cards Supported

The VPN Client supports authentication with digital certificates through a smart card or an electronic token. There are several vendors that provide smart cards and tokens, including the following:

Vendor	Software and Version	Card/Token Tested	Vendor Web site
GemPLUS	GemSAFE Workstation 2.0 or later	GEM195	www.gemplus.com
Activcard	Activcard Gold version 2.0.1 or later	Palmera 32K	www.activcard.com
Aladdin	eToken Runtime Environment (RTE) version 2.6 or later	PRO and R2 tokens	www.ealaddin.com

The VPN Client works only with smart cards and tokens that support CRYPT_NOHASHOID.

Configuring Microsoft Network Access (Windows 98, and Windows ME)

The **Logon to Microsoft Network** parameter registers your PC on the private Microsoft network and lets you browse and use network resources after the VPN Client establishes a secure connection. This parameter is enabled by default.

To disable this parameter, uncheck the check box.

Note This parameter appears only on VPN Clients installed on systems running Windows 98 and Windows ME. For information on logging on to Windows NT and Windows 2000 systems, see the section "Starting a Connection Before Logging on to a Windows NT Platform."

If you do not need or do not have privileges for Microsoft Windows resources on the private network, disable this parameter. For example, if you require only FTP access to the private network, you could disable this parameter.

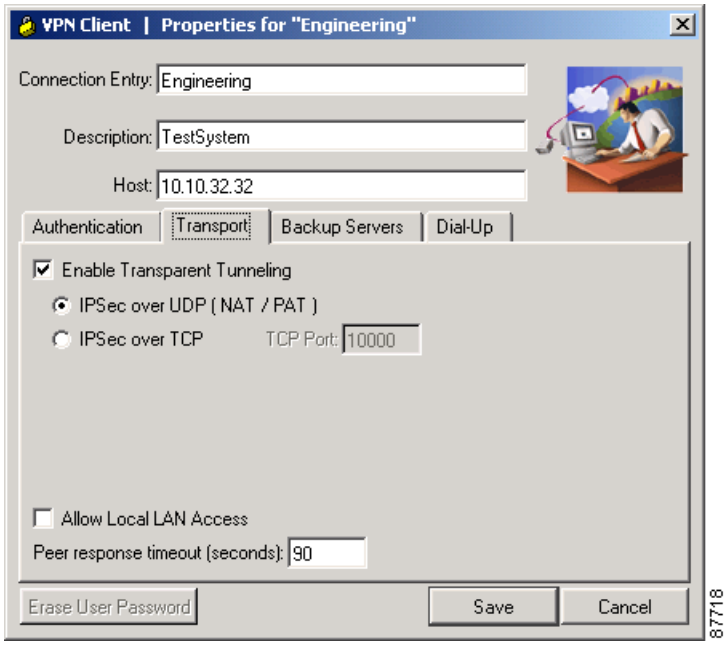
If you enable this parameter, click one of the radio buttons to choose the logon process:

- Use default system logon credentials—Use the Windows logon username and password on your PC to log on to the private network. With this option, you do not need to manually enter your logon username and password each time you connect to the private network. This is the default selection.
- Prompt for network logon credentials—The private network prompts you for a username and password to use its resources. If the logon username or password on your PC differs from those on the private network, use this option.

Configuring Transparent Tunneling

Next, configure the transparent tunneling by completing the fields on the Transport tab (Figure 4-3).

Figure 4-3 Configuring Transport Parameters



Enabling Transparent Tunneling

Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT). Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices and/or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.

The VPN Client also sends keepalives frequently, ensuring that the mappings on the devices are kept active.

Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Be sure to check with your device's vendor to verify whether this limitation exists. Some vendors support Protocol-50 (ESP) Port Address Translation (IPSec passthrough), which might let you operate without enabling transparent tunneling.

To use transparent tunneling, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the VPN 3000 Concentrator Manager, Configuration | User Management | Groups | IPSec tab (refer to *VPN 3000 Series Concentrator Reference Volume 1: Configuration* or Help in the VPN 3000 Concentrator Manager browser).

This parameter is enabled by default. To disable this parameter, uncheck the check box. We recommend that you always keep this parameter checked.

Then choose a mode of transparent tunneling, over UDP or over TCP. The mode you use must match that used by the secure gateway to which you are connecting. Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, then in general, TCP mode is preferable. UDP does not operate with stateful firewalls, so in this case, you should use TCP.

Using IPSec over UDP (NAT/PAT)

To enable **IPSec over UDP (NAT/PAT)**, click the radio button. With UDP, the port number is negotiated. UDP is the default mode.

Using IPSec over TCP (NAT/PAT/Firewall)

To enable **IPSec over TCP**, click the radio button. When using TCP, you must also enter the port number for TCP in the TCP port field. This port number must match the port number configured on the secure gateway. The default port number is 10000.

Allowing Local LAN Access

In a multiple-NIC configuration, Local LAN access pertains only to network traffic on the interface on which the tunnel was established. The Allow Local LAN Access parameter gives you access to the resources on your local LAN (printer, fax, shared files, other systems) when you are connected through a secure gateway to a central-site VPN device. When this parameter is enabled and your central site is configured to permit it, you can access local resources while connected. When this parameter is disabled, all traffic from your Client system goes through the IPSec connection to the secure gateway.

To enable this feature, check **Allow Local LAN Access**; to disable it, uncheck the check box. If the local LAN you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

A network administrator at the central site configures a list of networks at the Client side that you can access. You can access up to 10 networks when this feature is enabled. When Allow Local LAN Access is enabled and you are connected to a central site, all traffic from your system goes through the IPSec tunnel except traffic to the networks excluded from doing so (in the network list).

When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the Routes table. (See Figure 4-4.)

To display the Routes table, use the following procedure:

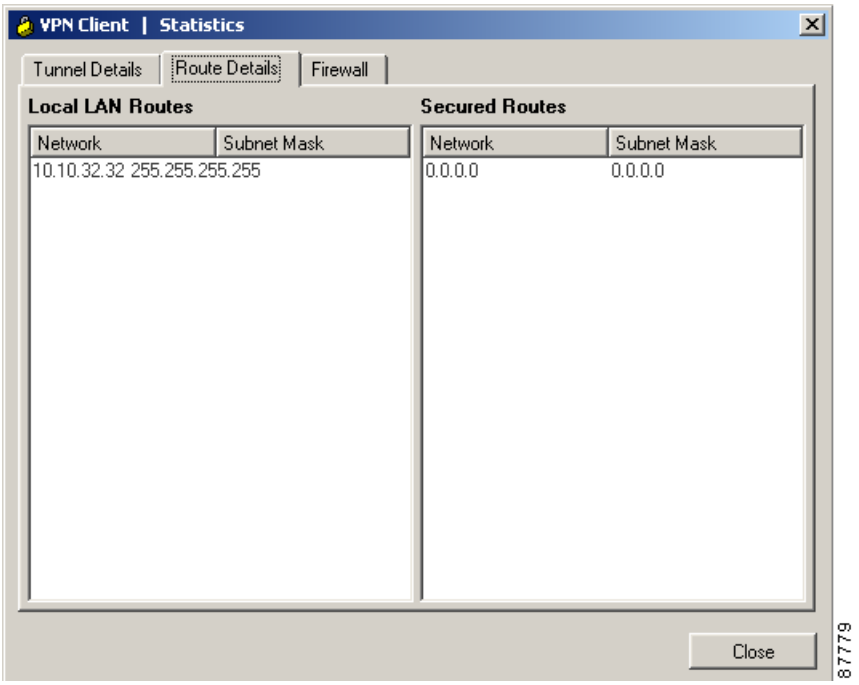
Step 1 Display the Status menu and choose **Statistics.**

Step 2 Choose **Route Details** from the Statistics dialog box.

The routes table shows local LAN routes, which do not traverse and IPSec tunnel and secured routes, which do traverse an IPSec tunnel to a central-site device. The routes in the local LAN routes column are for locally available resources.

Note This feature works only on one NIC card, the same NIC card as the tunnel.

Figure 4-4 Routes Table



Note While connected, you cannot print or browse the local LAN by name; when disconnected, you can print and browse by name. For more information on this limitation refer to *VPN Client Administrator Guide*, Chapter 1.

Adjusting the Peer Response Timeout Value

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to check the availability of the VPN device on the other side of an IPSec tunnel. If the network is unusually busy or unreliable, you might need to increase the number of seconds to wait before the VPN Client decides that the peer is no longer active. The default number of seconds to wait before terminating a connection is 90 seconds. The minimum number of seconds you can configure is 30 seconds and the maximum is 480 seconds.

To adjust the setting, enter the number of seconds in the **Peer response timeout** field.

The VPN Client continues to send DPD requests every 5 seconds, until it reaches the number of seconds specified by the Peer response timeout value.

Enabling and Adding Backup Servers

The private network may include one or more backup VPN servers to use if the primary server is not available.Your system administrator tells you whether to enable backup servers. Information on backup servers can download automatically from the VPN Concentrator, or you can manually enter this information.

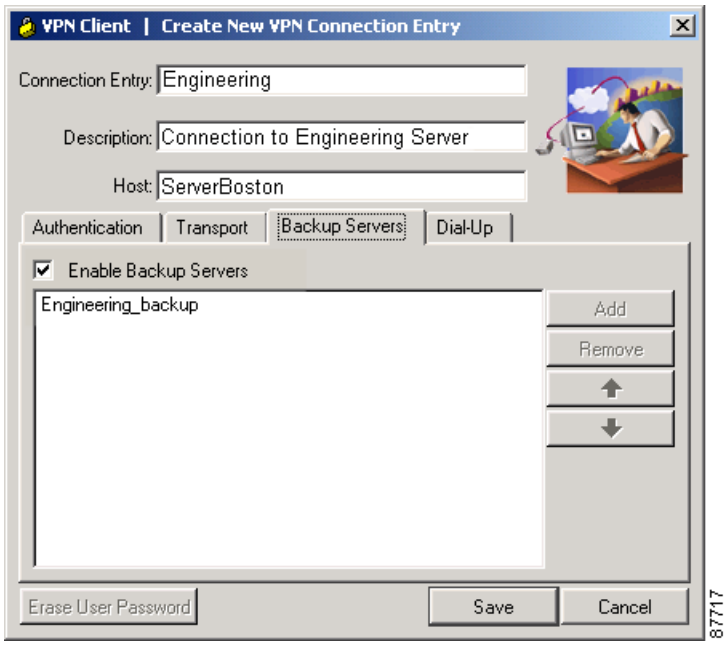
To enable backup servers from the VPN Client, use the following procedure:

Step 1 Open the Backup Servers tab (Figure 4-5).

Step 2 Check **Enable Backup Server(s)**. This is not checked by default.

Step 3 Click **Add** to enter a backup server's address.

Figure 4-5 Adding Backup Server Information



Step 4 Enter the hostname or IP address of the backup server. Use a maximum of 255 characters.

The hostname or IP address appears in the Enable backup server(s) list.

Step 5 To add more backup devices, repeat Steps 2, 3, and 4.

Removing Backup Servers

To remove a server from the backup list, select the server in the list and click **Remove**. The VPN Client displays a dialog box asking you to confirm the deletion. The server name no longer appears in the list.

Note If you click Cancel in the dialog box after a modification like Remove, the item is *not* removed from the .pcf file. You must click Save to make any changes on any of the tabs permanent.

Changing the Order of the Servers

When necessary, the VPN Client tries the backup servers in the order in which they appear in the backup servers list, starting at the top. To reorder the servers in the list, select a server and click the up arrow to increase the server's priority or the down arrow to decrease the server's priority.

Disabling Backup Servers

You can disable using backup servers without removing backup servers from the list.

To disable using backup servers, uncheck the **Enable backup server(s)** check box.

Configuring a Connection to the Internet Through Dial-up Networking

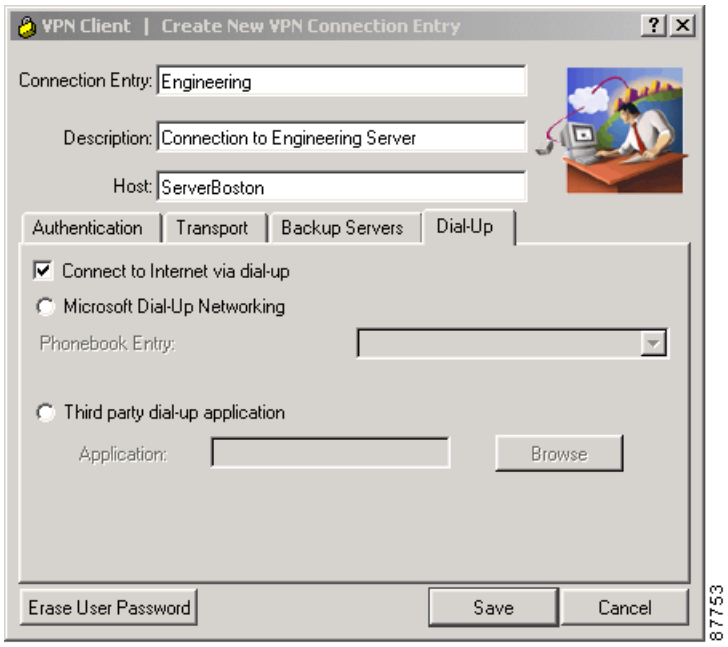
To connect to a private network using a dial-up connection, perform the following steps:

Step 1 Use a dial-up connection to your Internet service provider (ISP) to connect to the Internet.

Step 2 Use the VPN Client to connect to the private network through the Internet.

To enable and configure this feature, check the **Connect to the Internet via dial-up** check box. This feature is not checked by default. (See Figure 4-6.)

Figure 4-6 Connecting to the Internet Through Dial-up



You can connect to the Internet using the VPN Client application in either of the following ways:

- Microsoft Dial-up Networking (DUN)
- Third party dial-up program

Microsoft Dial-up Networking

If you have DUN phonebook entries and have enabled Connect to the Internet via dial-up, Microsoft Dial-up Networking is enabled by default. To link a VPN Client connection entry to a Dial-Up Networking phonebook entry, use the following procedure:

Step 1 Click **Microsoft Dial-up Networking** (if it is not already enabled).

Step 2 To link your VPN Client connection entry to a DUN entry, click the down arrow next to the Phonebook entry field and choose an entry from the menu.

The VPN Client then uses this DUN entry to automatically dial into the Microsoft network before making the VPN connection to the private network.

Third Party Dial-up Program

If you have no DUN phonebook entries and have enabled Connect to the Internet via dial-up, then Third party dial-up application is enabled by default.

To connect to the Internet using a third party dial-up program, follow these steps:

Step 1 Click **Third party dial-up application**, if it is not already enabled.

Step 2 Use **Browse** to enter the name of the program in the **Application** field. This application launches the connection to the Internet.

This string you choose or enter here is the pathname to the command that starts the application and the name of the command; for example: c:\isp\ispdialer.exe dialEngineering. Your network administrator might have set this up for you. If not, consult your network administrator.

Completing a Connection Entry

To complete the connection entry, click **Save**. The VPN Client stores your new connection entry in the Cisco Systems\VPN Client\Profiles directory.

Setting a Default Connection Entry

If you have a default connection entry configured, when you start the Client, you can just press Enter and the Client connects using that connection entry. To make one of your connection entries the default connection entry, use the following procedure:

Step 1 Select a connection entry in the list underneath the Connection Entries tab.

Step 2 Display the Connection Entries menu or right-click the connection entry name and choose **Set as Default Connection Entry**.

The default connection entry appears as bold in the list of connection entries.

Creating a Shortcut for a Connection Entry

To create a shortcut to a connection entry to appear on your desktop, use the following procedure:

Step 1 Select a connection entry in the list underneath the Connection Entries tab.

Step 2 Display the Connection Entries menu or right-click the connection entry name, and choose **Create Shortcut**.

The VPN Client places the shortcut on your desktop.

Duplicating a Connection Entry

You can duplicate an existing connection entry to serve as the basis of a new connection entry. To make a duplicate connection entry, use the following procedure:

Step 1 Select a connection entry in the list underneath the Connection Entries tab.

Step 2 Display the Connection Entries menu or right-click the connection entry name, and choose **Duplicate.**

The VPN Client enters the duplicate into the list as "*name*-duplicate."

Step 3 To change the name of the duplicate connection entry, follow these steps:

a. Right-click on the new connection entry.

b. Choose **Modify** from the menu.

c. Type a new name into the Connection Entry box.

Step 4 To save the new name, click **Save** or to cancel the change, click **Cancel**.

Modifying a Connection Entry

To change your connection entry settings, perform the following steps:

Step 1 Select a connection entry in the list underneath the Connection Entries tab.

Step 2 To modify the selected connection entry, do one of the following actions:

- Display the Connection Entries menu and choose **Modify**
- Click the **Modify** icon on the toolbar above the Connection Entries tab
- Right-click the selected entry and choose **Modify** from the menu

Step 3 Modify the information in the fields you want to change.

Step 4 To save your changes, click **Save** or to cancel your changes, click **Cancel**.

Deleting a Connection Entry

To delete a connection entry, use the following procedure:

Step 1 Select a connection entry in the display underneath the Connection Entries tab.

Step 2 To delete the selected entry, do one of the following actions:

- Display the Connection Entries menu and choose **Delete**
- Click the **Delete** icon on the toolbar above the Connection Entries tab
- Right-click the selected entry and choose **Delete** from the menu

Step 3 To confirm the deletion, choose **Delete** from the pop-up window or to cancel the deletion and keep the connection entry, choose **Do not Delete**.

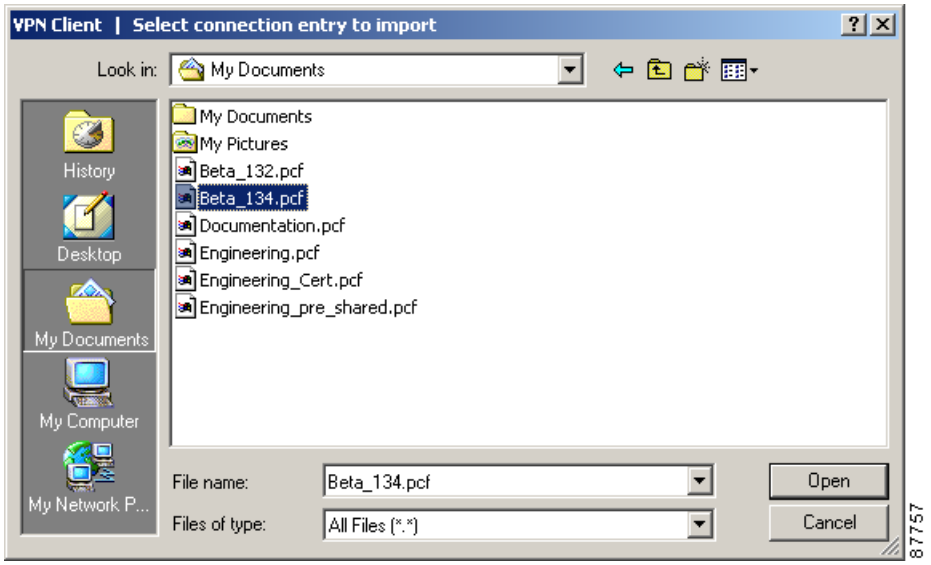
Importing a New Connection Entry

Your network administrator might have created other connection entry profiles for you. To use such a profile, you must first import that profile to the Profiles directory on your PC. To import a new connection entry profile from a file, use the following procedure:

Step 1 Either display the Connection Entries menu and choose **Import** or click the **Import** icon on the toolbar above the Connection Entries tab. The VPN Client displays the Import VPN Connection dialog box.

Step 2 Type the file name (a file with a .pcf extension) in the File Name box or browse to find the file you want to import (Figure 4-7).

Figure 4-7 Choosing a Profile to Import



The VPN Client displays a message to let you know that the import action succeeded and places the imported profile in the Cisco Systems\VPN Client\Profiles directory.

Erasing a Saved Password for a Connection Entry

You or your administrator might have configured an entry to save the authentication password on your PC so you do not have to enter a password when you are connecting to the VPN device. Normally we recommend that you not use this feature, because storing the password on the PC can compromise security, and requiring a password to authenticate you every time you attempt to connect to the VPN device is fundamental to maintaining security on the private network. However, there may be reasons for temporarily bypassing the authentication dialog box; for example, when you want to create a batch file for your PC to log in to a VPN device to accomplish some task that requires using the private network behind the VPN device.

If there is a password saved on your system, and authentication fails, your password might be invalid.

To eliminate a saved password, you need to modify the connection entry profile; use the following procedure:

Step 1 Select a connection entry in the display underneath the Connection Entries tab.

Step 2 To modify the selected connection entry, do one of the following actions:

- Display the Connection Entries menu and choose **Modify**
- Click the **Modify** icon on the toolbar above the Connection Entries tab
- Right-click the selected entry and choose **Modify** from the menu

Step 3 Click **Erase User Password**.

Step 4 To save your changes, click **Save,** or to cancel your changes, click **Cancel**.

Note If you get a failed-to-authenticate message, you should enable **Erase User Password** on the VPN Client and verify that your password is valid. When you attempt to connect, the VPN Client prompts you to enter your password.

With Erase User Password in effect, the next time you connect, the authentication dialog box prompts you to enter your password.