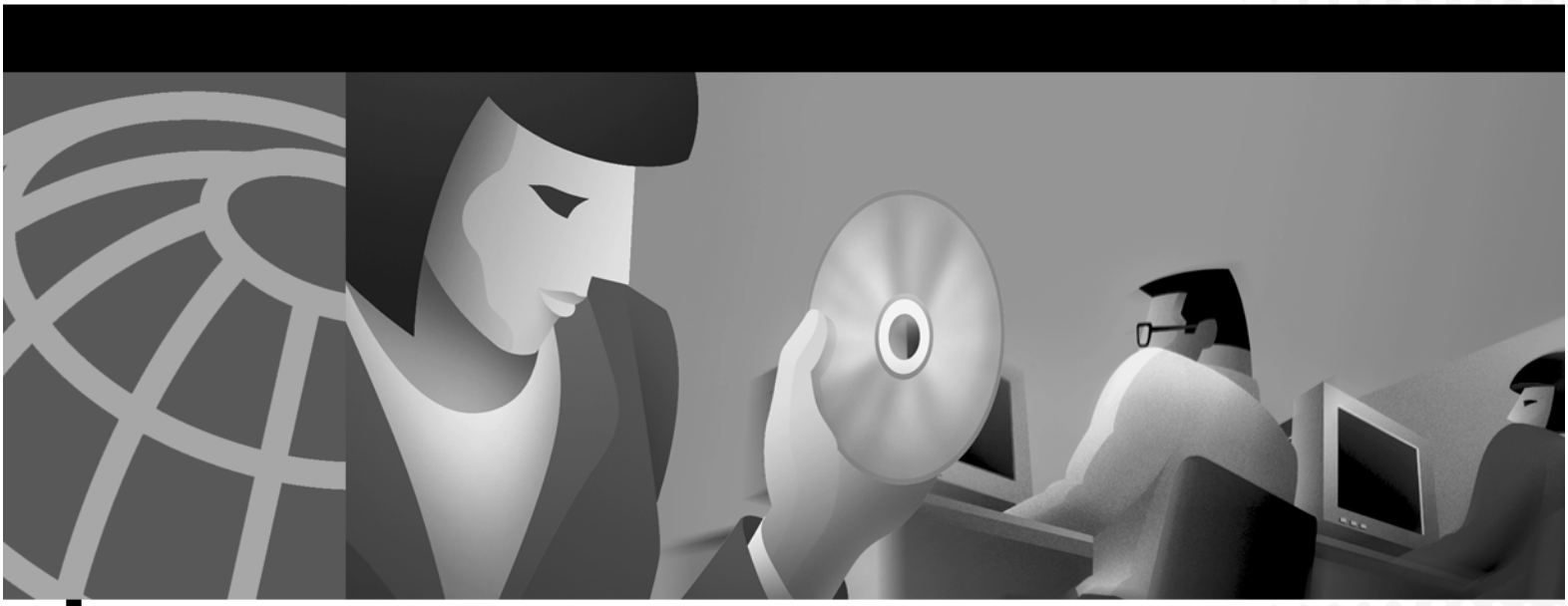
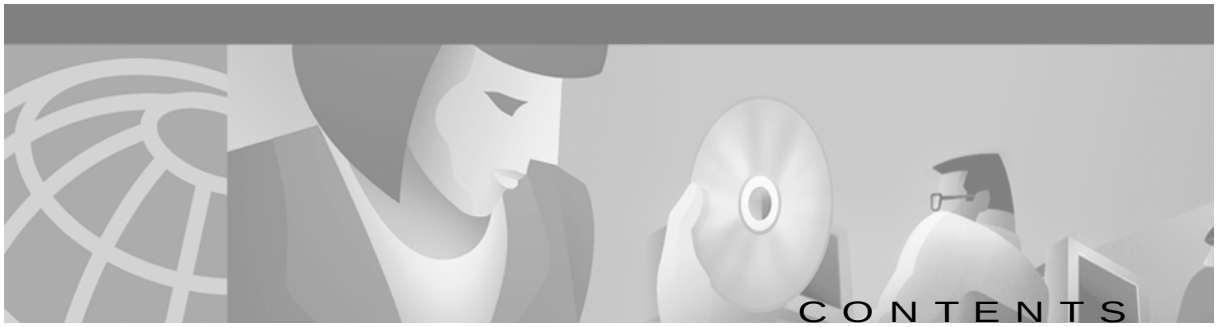


VPN Client User Guide for Windows

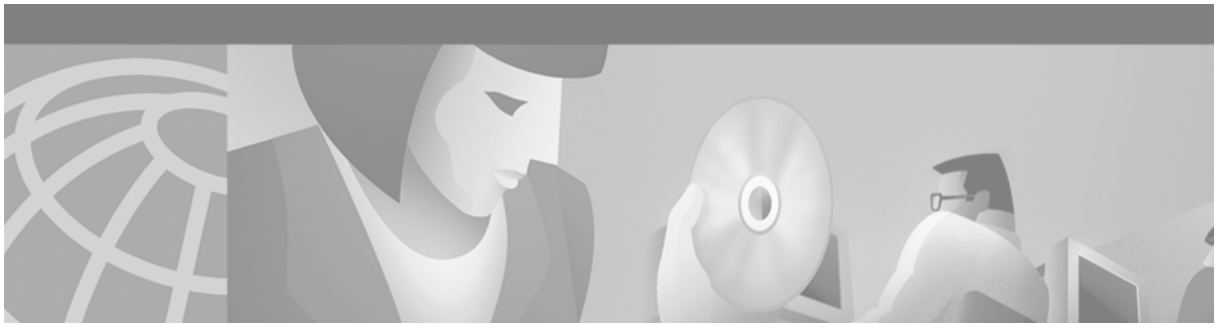
Release 3.5.1
January 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7813753=
Text Part Number: 78-13753-02



CONTENTS



Preface

This *VPN Client User Guide* tells you how to install, use, and manage the Cisco VPN Client with Cisco Systems products.

Audience

This guide is for remote clients who want to set up virtual private network (VPN) connections to a central site. Network administrators can also use this guide for information about configuring and managing VPN connections for remote clients. We assume that you are familiar with the Windows platform and know how to use Windows applications. A network administrator should be familiar with Windows system configuration and management and know how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices might be new to you.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Understanding the VPN Client	Briefly explains what the VPN Client is and how it works.
Chapter 2	Installing the VPN Client	Tells you how to install the VPN Client.
Chapter 3	Configuring the VPN Client	Tells you how to configure the VPN Client, including setting optional parameters.
Chapter 4	Connecting to a Private Network	Tells you how to connect to a private network using the VPN Client and an Internet connection; shows how to get status information on your connection.
Chapter 5	Managing the VPN Client	Tells you how to manage VPN Client connections, upgrade or uninstall VPN Client software, reconfigure the VPN Client automatically, use the Log Viewer application and set up special features such as Start Before Logon.

Chapter	Title	Description
Chapter 6	Enrolling and Managing Certificates	Tells you how to obtain digital certificates to use for authentication and how to manage these certificates on your system.
Appendix A	Copyrights and Licenses	Provides copyright and license information for software that the VPN Client uses.

Terminology

In this user guide, the term Cisco VPN device refers to the following Cisco products:

Cisco VPN 3000 Series Concentrator

Cisco VPN 5000 Series Concentrator

Cisco Secure PIX Firewall devices

IOS platform devices, such as the Cisco 7100 Series Routers

Related documentation

The VPN Client includes an extensive online HTML-based help system that you can access through a browser in several ways:

- Click the Help icon on the Cisco Systems VPN Client programs menu (Start > Programs > Cisco Systems VPN Client > Help).
- Press **F1** while using the applications.
- Click the **Help** button on screens that include it.

The *VPN Client Administrator Guide* tells how to:

- Configuration information for a VPN 3000 Concentrator network administrator:
  - Configuring a VPN 3000 Concentrator for remote access users
  - Configuring VPN Client firewall policy on a VPN 3000 Concentrator
  - Notifying remote users of a client update
  - Setting up Local LAN Access for the VPN Client
- Automate remote user profiles
- Use the VPN Client command-line interface
- Rebrand the VPN Client software (text, icons and so on)
- Use the SetMTU application
- Obtain troubleshooting information

The VPN Client guides are provided on the Cisco VPN 3000 Concentrator's software distribution CD-ROM in PDF format. To view the latest version on the Cisco Web site, go to the following site and click **VPN Clients**.

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm.

VPN 3000 Series Concentrator Documentation

The *VPN 3000 Concentrator Series Getting Started* guide explains how to unpack and install the VPN Concentrator, and how to configure the minimal parameters. This is known as *Quick Config*.

The *VPN 3000 Series Concentrator Reference Volume I: Configuration* explains how to start and use the VPN Concentrator Manager. It details the Configuration screens and explains how to configure your device beyond the minimal parameters you set during quick configuration.

The *VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring* provides guidelines for administering and monitoring the VPN Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

The VPN Concentrator Manager also includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

Other useful books, articles, and websites include:

- *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001
- Kosiur, Dave. *Building and Managing Virtual Private Networks*. Wiley: 1998.
- Sheldon, Tom. *Encyclopedia of Networking*. Osborne/McGraw-Hill: 1998.
- `www.ietf.org` for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).

Conventions

This document uses the following conventions:

Convention	Description
boldface font	User actions and commands are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. Cautions alert you to actions or conditions that could result in equipment damage or loss of data.

Data Formats

As you configure and manage the system, enter data in the following formats unless the instructions indicate otherwise:

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, `192.168.12.34`); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, `255.255.255.0`). Wildcard masks use the same notation (for example, `0.0.0.255`); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, `00.10.5A.1F.4F.07`).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, `VPN01`). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from `0` to `65535`. No commas or spaces are permitted in a number.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and might be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and choose **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check to see the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

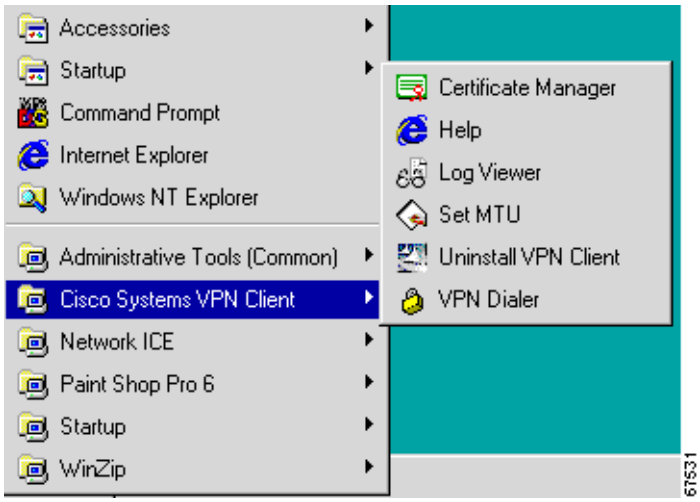
Understanding the VPN Client

The VPN Client is a software program that runs on a Microsoft® Windows®-based PC. The VPN Client on a remote PC, communicating with a Cisco VPN device on an enterprise network or with a service provider, creates a secure connection over the Internet. Through this connection you can access a private network as if you were an on-site user. Thus you have a Virtual Private Network (VPN).

As a remote user (low speed or high speed), you first connect to the Internet. Then you use the VPN Client to securely access the private enterprise network through a Cisco VPN device that supports the VPN Client.

The VPN Client comprises the following applications, which you select from the Program menu:

Figure 1-1 VPN Client Applications



In logical order of use, the applications are as follows:

- Help—Displays an online manual with instructions on using the applications.
- VPN Dialer—Lets you configure connections to a VPN device and lets you then start your connections.
- Certificate Manager—Lets you enroll for certificates to authenticate your connections to VPN devices.
- Log Viewer—Lets you display events from the log.
- Uninstall VPN Client—Lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations.
- SetMTU—Lets you manually change the size of the maximum transmission unit (see the *VPN Client Administrator Guide*, Chapter 5.)

How the VPN Client Works

The VPN Client works with a Cisco VPN device to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:

- Negotiating tunnel parameters—Addresses, algorithms, lifetime, and so on.
- Establishing tunnels according to the parameters.
- Authenticating users—Making sure users are who they say they are, by way of usernames, group names and passwords, and X.509 digital certificates.
- Establishing user access rights—Hours of access, connection time, allowed destinations, allowed protocols, and so on.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

For example, to use a remote PC to read e-mail at your organization, you connect to the Internet, then start the VPN Client and establish a secure connection through the Internet to your organization's private network. When you open your e-mail, the Cisco VPN device uses IPSec to encrypt the e-mail message. It then transmits the message through the tunnel to your VPN Client, which decrypts the message so you can read it on your remote PC. If you reply to the e-mail message, the VPN Client uses IPSec to process and return the message to the private network through the Cisco VPN device.

Connection Technologies

The VPN Client lets you use any of the following technologies to connect to the Internet:

- POTS (Plain Old Telephone Service)—Uses a dial-up modem to connect.
- ISDN (Integrated Services Digital Network)—May use a dial-up modem to connect.
- Cable—Uses a cable modem; always connected.
- DSL (Digital Subscriber Line)—Uses a DSL modem; always connected.

You can also use the VPN Client on a PC with a direct LAN connection.

VPN Client Features

The VPN Client includes the following features:

Program Features

- Complete browser-based context-sensitive HTML Help
- Support for VPN 3000 Series Concentrator platforms that run Release 3.0 and above. (VPN Client Release 3.0 and above will not work with Releases 2.x of the VPN 3000 Concentrator.)
- Command-line interface to the VPN Dialer
- Local LAN access—The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN device (if the central site grants permission)
- Automatic VPN Client configuration option—the ability to import a configuration file

- Log Viewer—An application that collects events for viewing and analysis
- Set MTU size—The VPN Client automatically sets a size that is optimal for your environment. However, you can set the MTU size manually as well. (For instructions on adjusting the MTU size, see the *VPN Client Administrator Guide)*.
- Application Launcher—The ability to launch an application or a third-party dialer from the VPN Client.
- Automatic uninstall of the Nortel Networks Extranet Access Client and the 5000 VPN Client software
- Automatic connection by way of Microsoft Dial-Up Networking or any other third-party remote access dialer
- Software update notifications from the VPN device upon connection
- Ability to launch a location site containing upgrade software from a VPN device notification

NT Features

- Password expiration information when authenticating through a RADIUS server that references an NT user database. When you log in, the VPN Concentrator sends a message that your password has expired and asks you to enter a new one and then confirm it. On pre-Release 3.5 VPN Clients, the prompt asks you to supply a PIN and to verify it. On a 3.5 VPN Client, the prompt asks you to enter and verify a password.
- Start Before Logon—The ability to establish a VPN connection before logging on to a Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP systems.
- Ability to disable automatic disconnect when logging off of a Windows NT platform. This allows for roaming profile synchronization.

IPSec Features

- IPSec tunneling protocol
- Transparent tunneling—IPSec over UDP for NAT and PAT, and IPSec over TCP for NAT, PAT, and firewalls
- IKE key management protocol
- IKE Keepalives—Monitoring the continued presence of a peer and reporting the VPN Client's continued presence to the peer. This lets the VPN Client notify you when the peer is no longer present. Another type of keepalives keeps NAT ports alive.
- Split tunneling—The ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel
- LZS data compression, which can benefit modem users

Authentication Features

- User authentication by way of VPN central-site device:
  - Internal through the VPN device's database
  - RADIUS (Remote Authentication Dial-In User Service)
  - NT Domain (Windows NT)
  - RSA (formerly SDI) SecurID or SoftID
- Certificate Manager—An application that lets you manage your identity certificates

- Ability to use Entrust Entelligence certificates
- Ability to authenticate using smart cards with certificates

Firewall Features

- Support for Cisco Secure PIX Firewall platforms that run Release 6.0 and higher

Note Instructions on configuring the VPN Client to interoperate with Cisco Secure PIX Firewall, Release 6.0, are available in *IPSec User Guide for Cisco Secure PIX Firewall.*

- Support for personal firewalls:
  - Cisco Integrated Firewall (CIC)
  - ZoneAlarmPro 2.6.3.57
  - ZoneAlarm 2.6.3.57
  - Zone Integrity
  - BlackIce Agent and BlackIce Defender 2.5
- Centralized Protection Policy—Support for firewall policies pushed to the VPN Client from a VPN 3000 Concentrator

VPN Client IPSec Attributes

The VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one of establishing ISAKMP Security Associations (SAs)
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs
- Authentication algorithms:
  - HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function
  - HMAC with SHA-1 (Secure Hash Algorithm) hash function
- Authentication Modes:
  - Preshared Keys
  - X.509 Digital Certificates
- Diffie-Hellman Groups 1, 2, and 5
- Encryption algorithms:
  - 56-bit DES (Data Encryption Standard)
  - 168-bit Triple-DES
- Extended Authentication (XAUTH)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

Installing the VPN Client

This chapter explains how to install the VPN Client on your PC and includes the following sections:

- Verifying System Requirements
- Gathering Information You Need
- Installing the VPN Client

To upgrade the VPN Client software, or to uninstall it, see "Managing the VPN Client."

Caution Installing the VPN Client software on Windows NT or Windows 2000 requires Administrator privileges. If you do not have Administrator privileges, you must have someone with Administrator privileges install the product for you.

Verifying System Requirements

Verify that your computer meets these requirements:

- Computer with a Pentium®-class processor or greater
- One of the following operating systems:
  - Microsoft®Windows® 95 (OSR2), Windows 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT® 4.0 (with Service Pack 3, or higher)
  - Windows 2000
  - Windows XP
- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 10 MB hard disk space.
- RAM:
  - 16 MB for Windows 95/98
  - 32 MB for Windows NT and Windows ME
  - 64 MB for Windows 2000
  - 128 MB for Windows XP

- To install the VPN Client:
  - CD-ROM drive
  - 3.5 inch high-density diskette drive
  - Administrator privileges if installing on Windows NT or Windows 2000
- To use the VPN Client:
  - Direct network connection (cable or DSL modem and network adapter/interface card)
  - Internal or external modem
  - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, www.microsoft.com. Windows 98 includes the DUN 1.3 functionality.)
- To connect using a digital certificate for authentication:
  - A digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:

    Baltimore Technologies (www.baltimoretechnologies.com)

    Entrust Technologies (www.entrust.com)

    Microsoft Certificate Services—Windows 2000

    Netscape (Security)

    Verisign, Inc. (www.verisign.com)

    A smart card

Gathering Information You Need

To configure and use the VPN Client, you may need the information listed in this section.

Ask for this information from the system administrator of the private network you want to access. Your system administrator may have preconfigured much of this data; if so, he or she will tell you which items you need.

- Hostname or IP address of the secure gateway to which you are connecting
- Your IPSec Group Name (for preshared keys)
- Your IPSec Group Password (for preshared keys)
- If authenticating with a digital certificate, the name of the certificate
- If authenticating through the secure gateway's internal server, your username and password
- If authenticating through a RADIUS server, your username and password
- If authenticating through an NT Domain server, your username, password, and domain name
- If authenticating through a token vendor, your username and PIN
- If authenticating through a smart card, your smart card, reader, PIN or passcode, and the name of the certificate stored on the smart card.
- If you should configure backup server connections, the hostnames or IP addresses of the backup servers

Installing the VPN Client

To install the VPN Client on your system, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.

Step 1 Exit all Windows programs, and disable any antivirus software.

Step 2 Start the appropriate VPN Client installation setup program:

- If VPN Client software is on CD-ROM:

a. Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.

b. Choose **Start** > **Run**. The Run dialog box appears.

c. Enter E:\VPN Client\CD-ROM\setup, where E: is your system's CD-ROM drive.

d. Click **OK**.

- If VPN Client software is on diskettes:

a. Insert Disk 1 (of three) in your system's diskette drive.

b. Choose **Start** > **Run**. The Run dialog box appears.

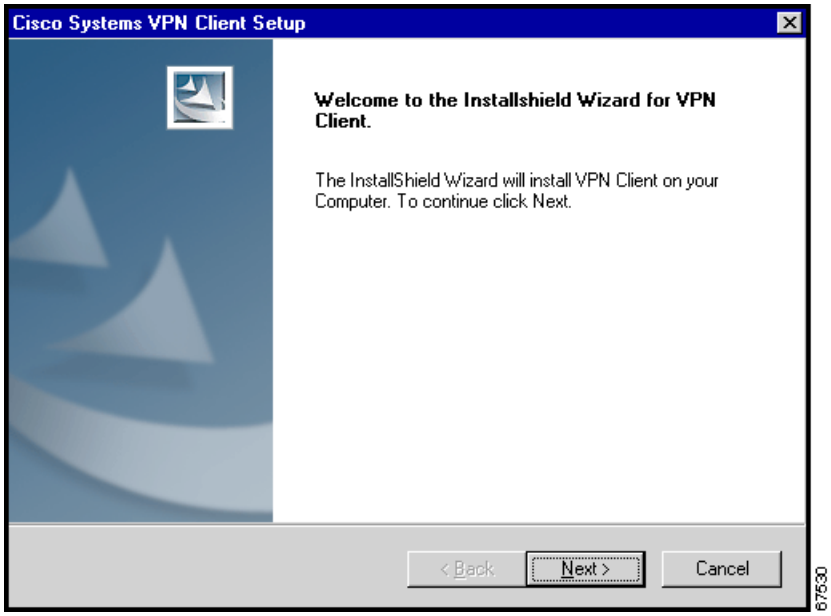
c. Enter `A:\setup`, where `A:` is your system's diskette drive.

d. Click **OK**.

Note Cisco does not allow you to install the VPN Client software from a network drive. If you attempt to do so, you receive an error message.

The program displays the Cisco Systems logo and InstallShield Setup window shown in Figure 2-1.

Figure 2-1 Initial VPN Client Installation Window



Step 3 If the InstallShield Wizard identifies an existing version of the VPN Client, the Cisco 5000 Client, or Nortel Networks Extranet Access Client, it displays a dialog box that asks if you want to uninstall the existing client program. To continue, choose **Yes**.

The VPN Client launches the appropriate uninstall wizard: the Cisco VPN Client uninstall wizard to uninstall a previous version of the VPN Client, the Extranet Access Client wizard program, or the Cisco 5000 wizard. Follow the instructions on the uninstall wizard dialog boxes to automatically uninstall the program and reboot.

Note Having more than one VPN client on your system is not advisable.

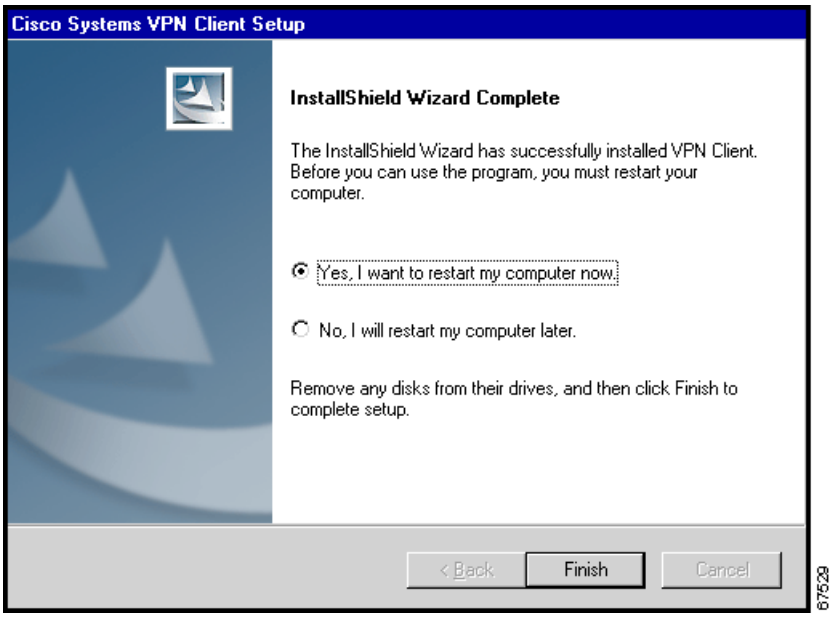
After your system reboots, our own Cisco Systems VPN Client Setup wizard resumes.

Step 4 Follow the instructions on the screens and enter the following information:

A destination folder for the VPN Client files (or click **Next>** to enter the default location C:\Program Files\Cisco Systems\VPN Client).

Step 5 After you have installed the VPN Client, the InstallShield Wizard displays the following screen. You must restart your computer before you can configure and use the VPN Client. (See Figure 2-2.)

Figure 2-2 Setup Complete Dialog Box



- To restart now, click **Finish**. Your system reboots. *Be sure to remove any diskette from the drive before you reboot.*
- To restart later, click the **No** radio button and then click **Finish**. The VPN Client Setup closes. Remember: *you must restart your computer before you can use the VPN Client.*

What Next?

The VPN Client software is now installed on your PC. To configure it, see “Configuring the VPN Client.”

Configuring the VPN Client

This chapter explains how to configure the VPN Client.

To configure the VPN Client, you enter values for a set of parameters known as a *connection entry*. The VPN Client uses a connection entry to identify and connect securely to a specific private network.

Parameters 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 preconfigured your connection entry, you can skip this chapter and go directly to "Connecting to a Private Network."

This chapter explains the following configuration tasks:

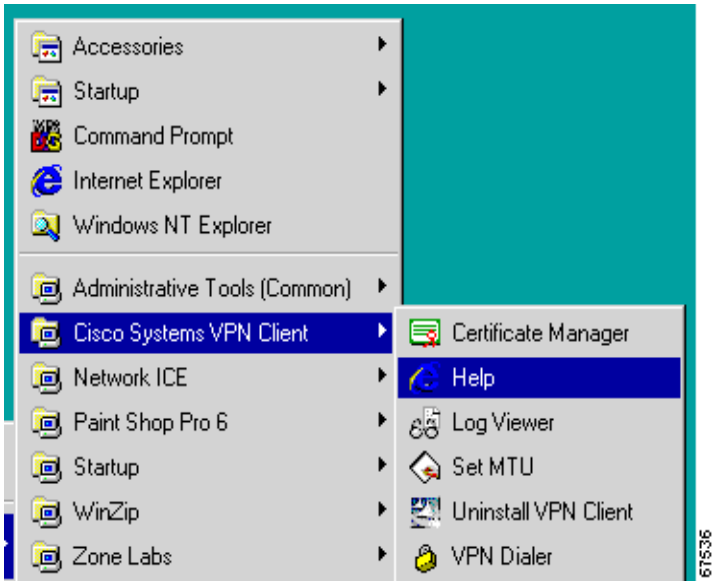
- How to Get Help
- What Is a Connection Entry?
- How To Create a New Connection Entry
- Setting or Changing Connection Entry Properties
- Changing the VPN Device Address for a Connection Entry

How to Get Help

The VPN Client comes with a complete, context-sensitive, browser-based help system. You can display help in the following ways:

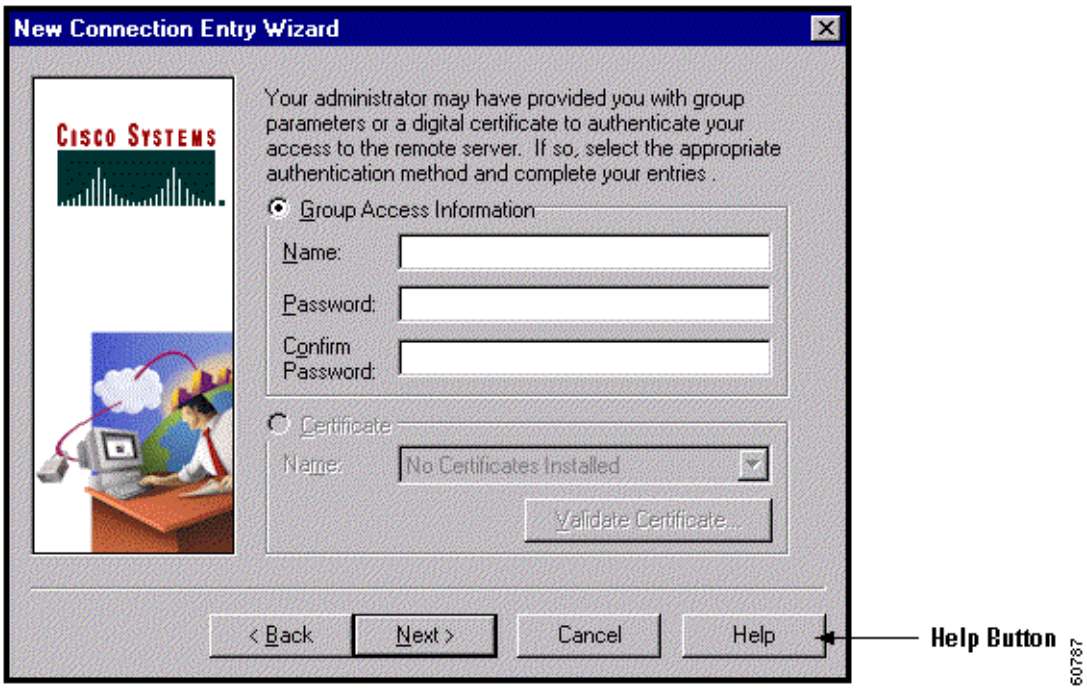
- On the Program Menu, choose **Start** > **Programs** > **Cisco Systems VPN Client** > **Help**. (See Figure 3-1.)

Figure 3-1 Choosing Help from the Cisco Systems VPN Client Program Menu



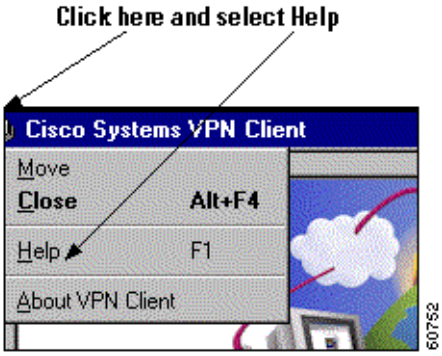
- Press **F1** at any window while using the VPN Client, including the main window of each application (VPN Dialer, Log Viewer, and Certificate Manager).
- Click the **Help** button on windows that display it. (See Figure 3-2.)

Figure 3-2 Help Button



- Choose **Help** from the menu that appears when you click on the icon in the title bar. (See Figure 3-3.)

Figure 3-3 Menu Containing Help Option



Determining the VPN Client Version

To display the version number of the software release you are currently using, follow these steps:

Step 1 Click the icon in the title bar. (See Figure 3-3.)

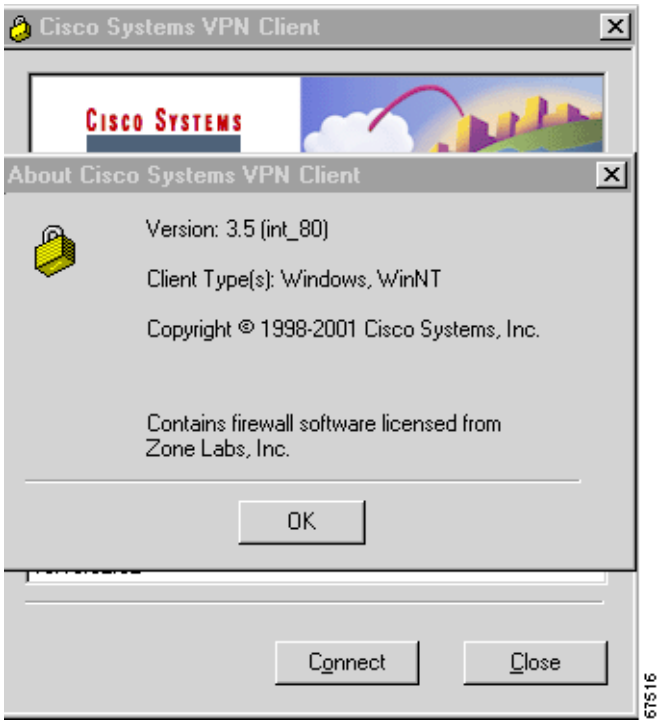
The VPN Client displays a menu.

Step 2 Click **About VPN Client** on the menu displayed.

The VPN Client displays the version you are currently using. (See Figure 3-4.)

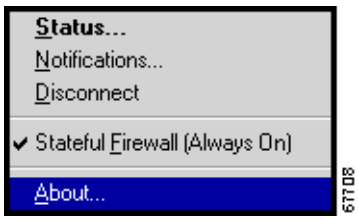
Step 3 After viewing the version number, click **OK**.

Figure 3-4 Displaying the VPN Client Software Version



When you are connected, you can display the software version by clicking **About...** on the menu you display by right clicking the Dialer icon in the system tray.

Figure 3-5 Displaying Version from Menu Available from System Tray



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.

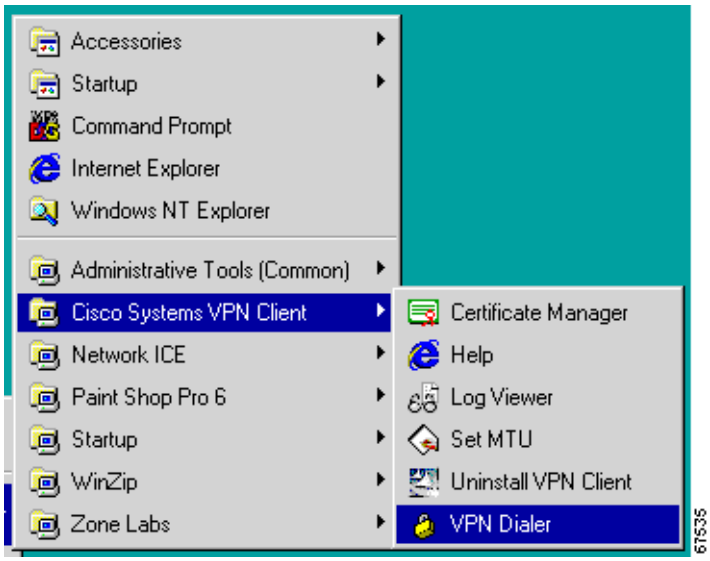
You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously) or if you belong to more than one VPN remote access group.

For connection entry parameters, refer to “Gathering Information You Need”.

How To Create a New Connection Entry

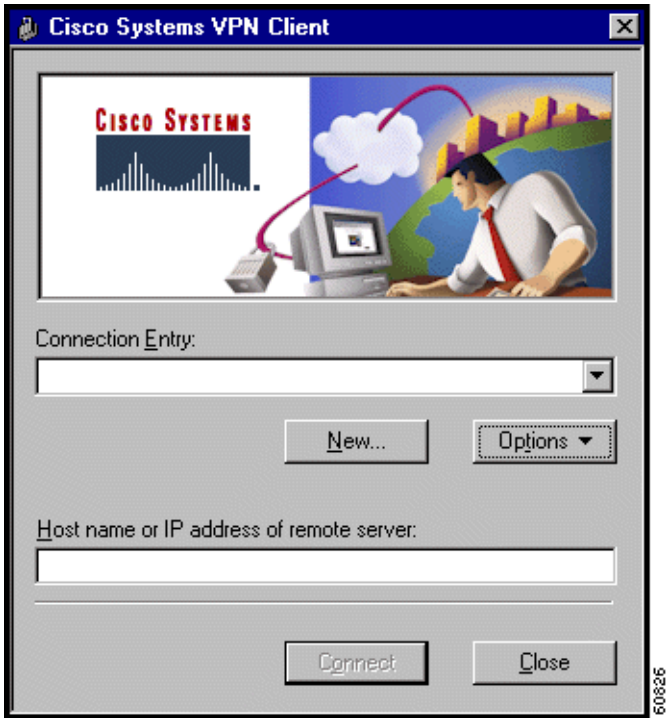
Start the VPN Client by choosing **Start** > **Programs** > **Cisco Systems VPN Client** > **VPN Dialer**.

Figure 3-6 Starting the VPN Dialer



The VPN Dialer application starts and displays its main dialog box. (See Figure 3-7.)

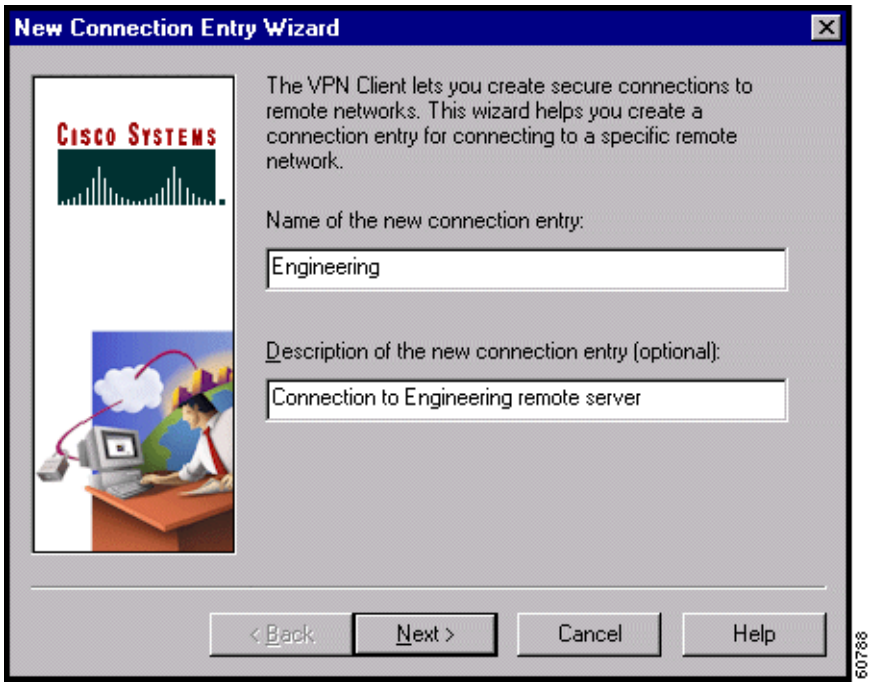
Figure 3-7 VPN Dialer Main Dialog Box



Step 1 At the main dialog, click **New**.

The first New Connection Entry Wizard dialog box appears. (See Figure 3-8.)

Figure 3-8 Entering Name and Description



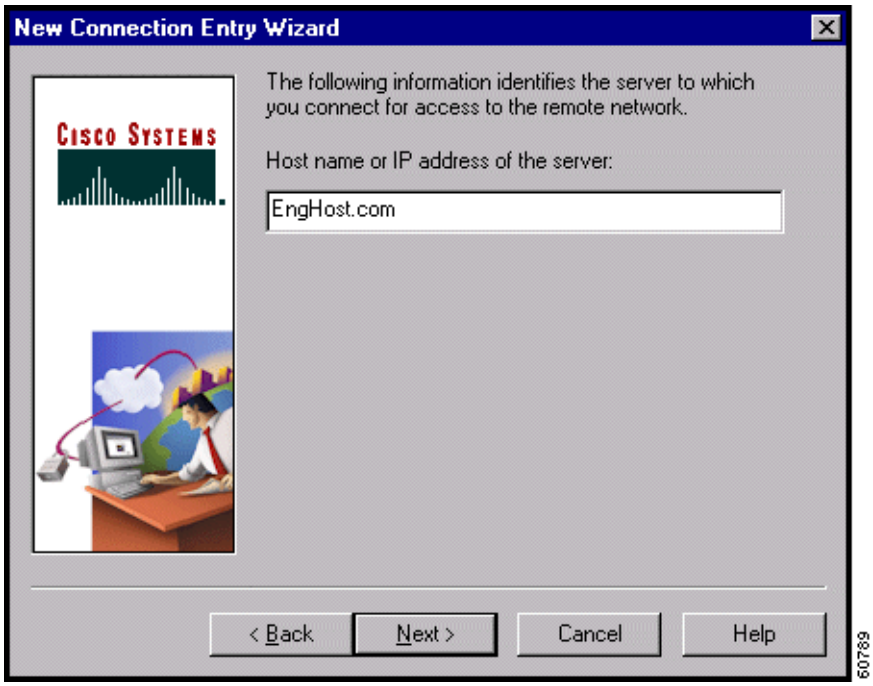
Step 2 Enter a unique name for this new connection. You can use any name to identify this connection; for example, Engineering. This name can contain spaces, and it is not case-sensitive.

Step 3 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 4 Click **Next**.

The second New Connection Entry Wizard dialog box appears. (See Figure 3-9.)

Figure 3-9 Identifying Server



Step 5 Enter the hostname or IP address of the remote VPN device you want to access, and click **Next**.

The third New Connection Entry Wizard dialog box appears. (See Figure 3-10.)

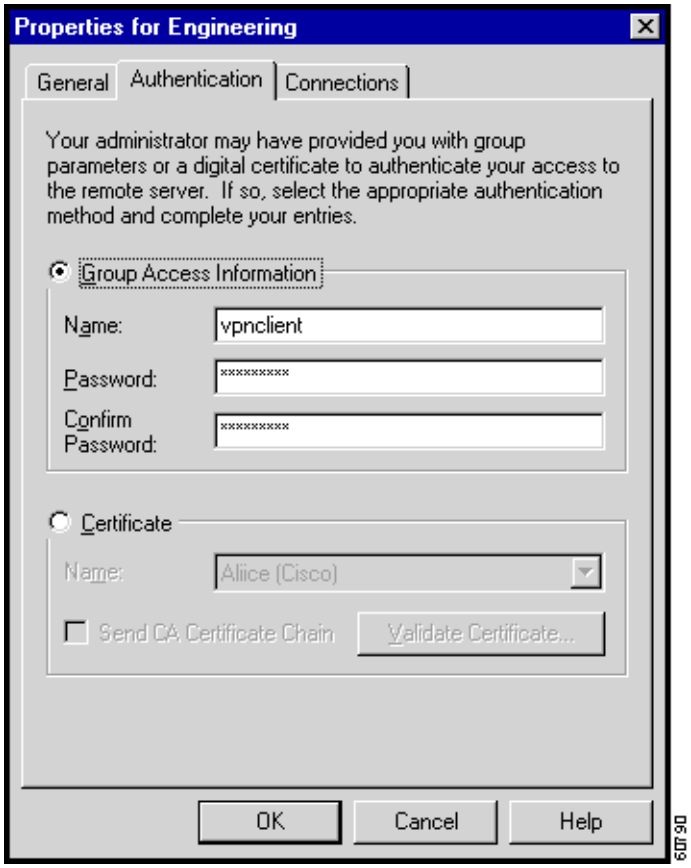
Choosing an Authentication Method

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, perform the following procedure: (See Figure 3-10.)

Figure 3-10 Group Authentication



Step 1 In the Name field, enter the name of the IPSec group to which you belong. This entry is case-sensitive.

Step 2 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

Step 3 Verify your password by entering it again in the Confirm Password field.

Step 4 To continue, click **Next**.

Certificate Authentication

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

Step 1 Click the **Certificates** radio button.

Step 2 Choose the name of the certificate you are using from the pull-down menu. (See Figure 3-11.)

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 Chapter 6, "Enrolling and Managing Certificates." Or, consult your network administrator.

Figure 3-11 Certificate Authentication

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 a 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 3-1 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 CA certificates, 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 To verify the validity of a certificate, click **Validate Certificate...** and enter the password.

The VPN Dialer might prompt for a password to secure the certificate. If so, enter the password.

You receive a report letting you know whether the certificate is valid. If the password is not valid, you need to try again. If you do not know the password, see your system administrator. An identity certificate has a public and private key, and a time period within which it is valid. Make sure the certificate is valid before you continue.

Step 2 After you have verified that the certificate is valid, click **Next**.

Configuring an Entrust Certificate for Authentication

If you have an Entrust Entelligence certificate enrolled, the pull-down menu includes the entry "Entelligence Certificate (Entrust)." (See Figure 3-12.)

Figure 3-12 Entrust Entelligence Certificate

An Entrust Entelligence certificate is stored in a *Profile*, which you obtain when you log in to Entrust Entelligence.

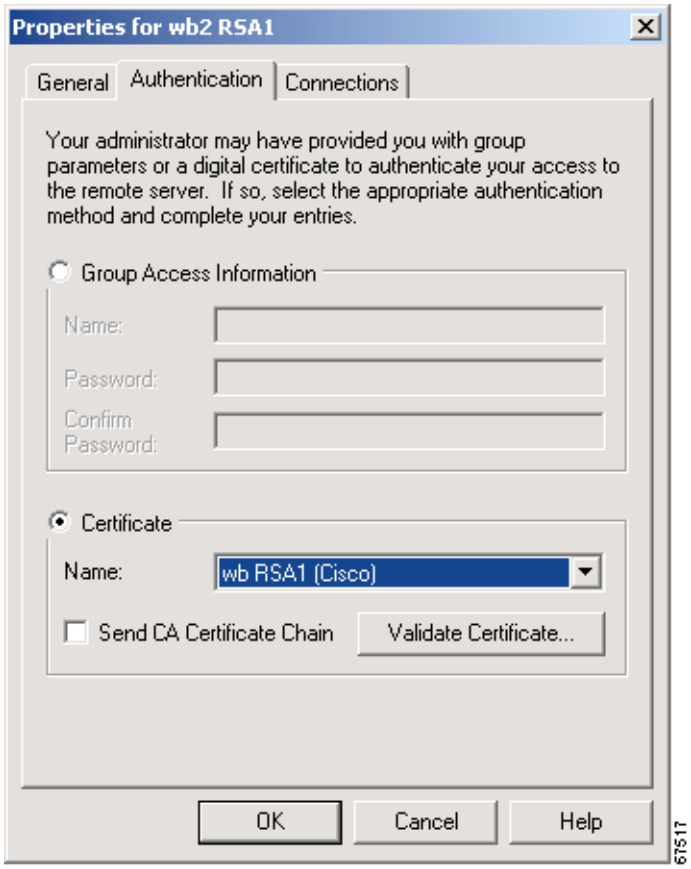
Choose **Entelligence Certificate (Entrust)** from the pull-down menu and click **Next**.

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, select that certificate. (See Figure 3-13.)

Figure 3-13 Creating a Connection Entry for a Smart Card



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:

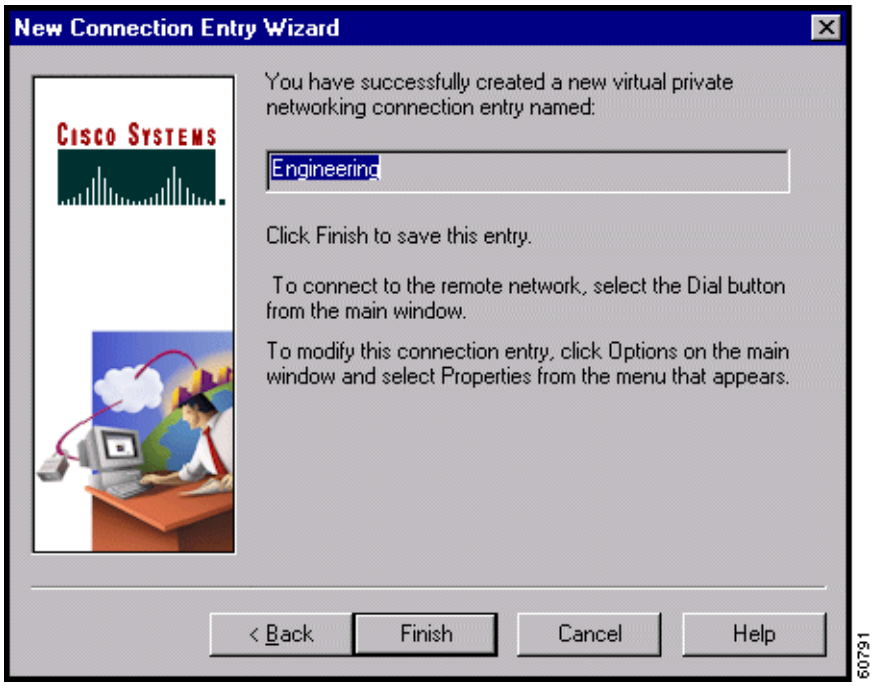
Vendor	Software and Version	Card/Token Tested	Vendor Web site
GemPLUS	GemSAFE Workstation 2.0 or later	GEM195	www.gemplus.com
Activcard	Activcard Gold version 2.0.1 or later	Palmera 32K	www.activcard.com
Aladdin	eToken Runtime Environment (RTE) version 2.6 or later	PRO and R2 tokens	www.ealaddin.com

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

Completing the Connection Wizard

After you enter authentication information and click **Next**, the fourth New Connection Entry Wizard dialog box appears. (See Figure 3-14.)

Figure 3-14 Completing the Connection Entry



To complete the connection entry configuration, use the following procedure.

Step 1 Review the connection entry name. If you want to change any previous entries, click **Back** until you get to the desired dialog box.

Step 2 To complete your entry, click **Finish**.

The final New Connection Entry Wizard dialog box closes. Your new connection entry now appears in the Connection Entry drop-down list on the VPN Client's main dialog box.

What Next?

If you need to configure optional connection entry parameters or change parameters for an existing connection entry, continue to the next section.

Otherwise, you can skip to "*Connecting to a Private Network.*"

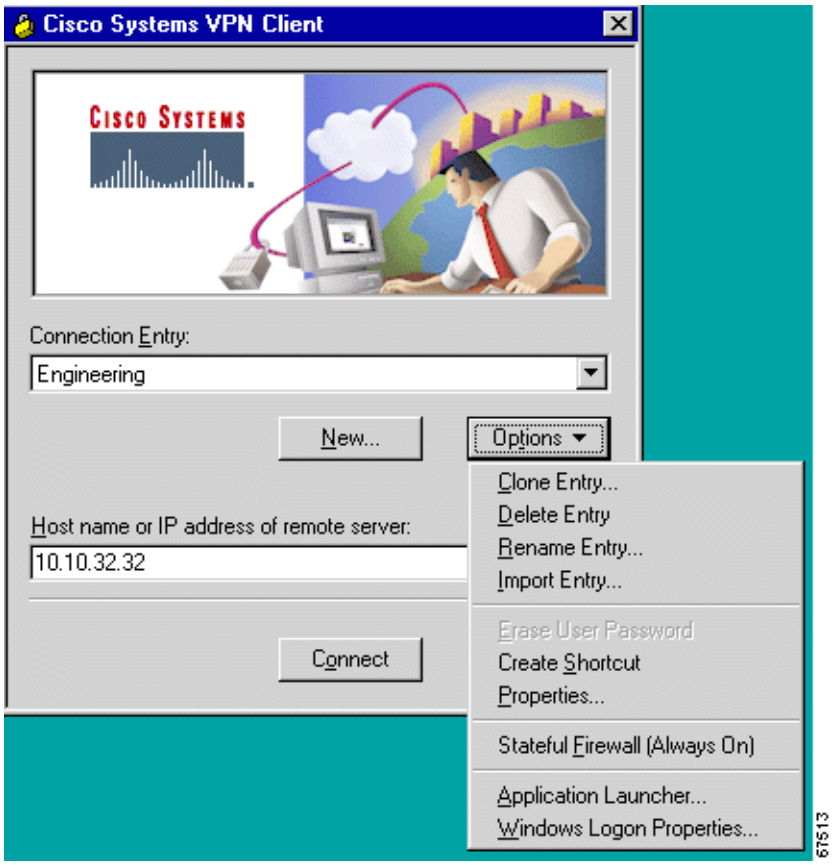
Setting or Changing Connection Entry Properties

To change parameters or to set optional parameters for an existing connection entry, follow these steps:

Step 1 In the VPN Client's main dialog box, click the Connection Entry drop-down menu button and choose the entry you want to configure.

Step 2 Then click **Options** and choose **Properties** from the menu. (See Figure 3-15.)

Figure 3-15 VPN Client Options Menu



The Properties dialog box appears. The fields in this dialog box differ according to the operating system you are using.

- If you are using Microsoft Windows 95, Windows 98, or Windows ME, you see a dialog box that resembles the one in Figure 3-16.
- If you are using Microsoft Windows NT, Windows 2000, or Windows XP, you see the dialog box in Figure 3-17.

Figure 3-16 Connection Entry Properties Dialog Box (Windows 95, Windows 98 and Windows ME)

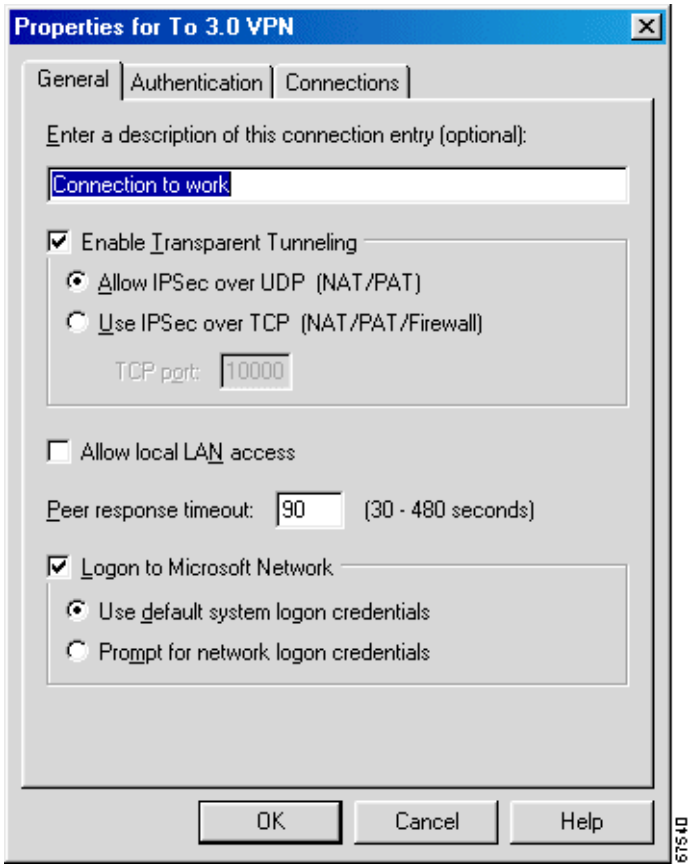
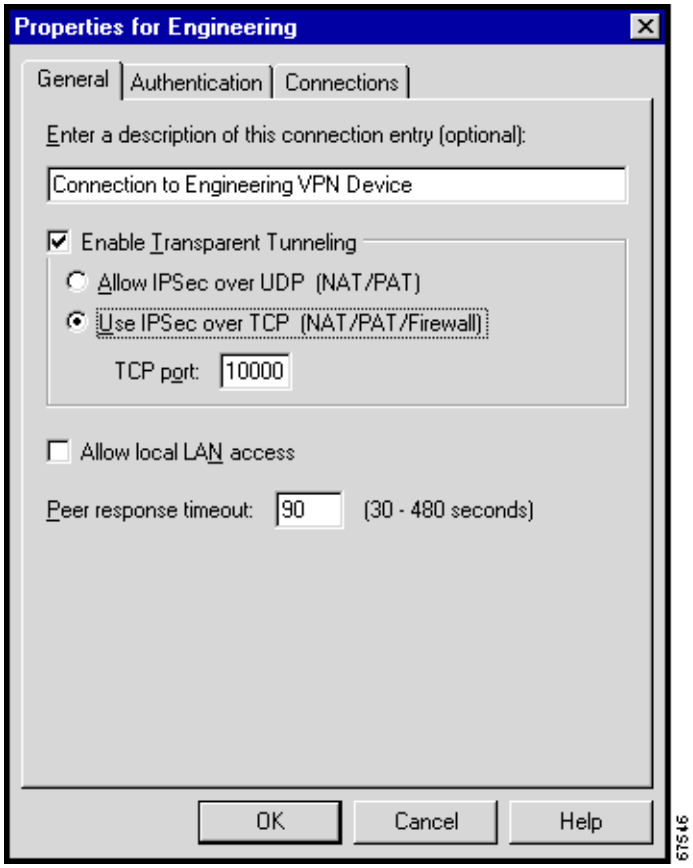


Figure 3-17 Connection Entry Properties Dialog Box (Windows NT, Windows 2000, and Windows XP)



Step 3 Click the tab for the parameters you want to change:

- General tab
  - Change the connection entry description
  - Enable transparent tunneling
  - Allow local LAN Access
  - Adjust the peer response time out
  - Log on to Microsoft Network
- Authentication tab
  - Change the group name or group password
  - Change the certificate you want to use
- Connections tab
  - Enable, add, and remove backup server connections
  - Connect to the Internet via Dial-Up Networking

See the appropriate section of this chapter for each tab and parameter.

Step 4 When you have finished setting parameters, click **OK**. The Properties dialog box closes and the VPN Dialer saves your changes.

To discard your changes, click **Cancel**. The Properties dialog box closes and discards all changes.

Changing General Settings

The Properties > General tab lets you set general parameters for this connection entry. (See Figure 3-17.)

Changing Connection Entry Description

To change the description of this connection entry, enter or edit the description field. This field is optional, but it can help you identify this connection.

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, 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, clear the check. We recommend that you always keep this parameter checked.

Then select 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.

Allow IPSec over UDP (NAT/PAT)

To enable **Allow IP over UDP**, click the radio button. With UDP, the port number is negotiated. UDP is the default mode.

Use IPSec over TCP (NAT/PAT/Firewall)

To enable **Use 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.

Note When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a client is idle, it does not send a keepalive until it sends data and gets no response.

To allow the VPN Client to work through ESP-aware NAT/Firewalls, add the ForceKeepAlives parameter to the *.pcf (profile configuration file) for the affected connection profile. This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

Use the following syntax when adding this parameter to the [Main] section of any *.pcf file:

ForceKeepAlives=1

For more information, see "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide*.

Allowing Local LAN Access

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, 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.

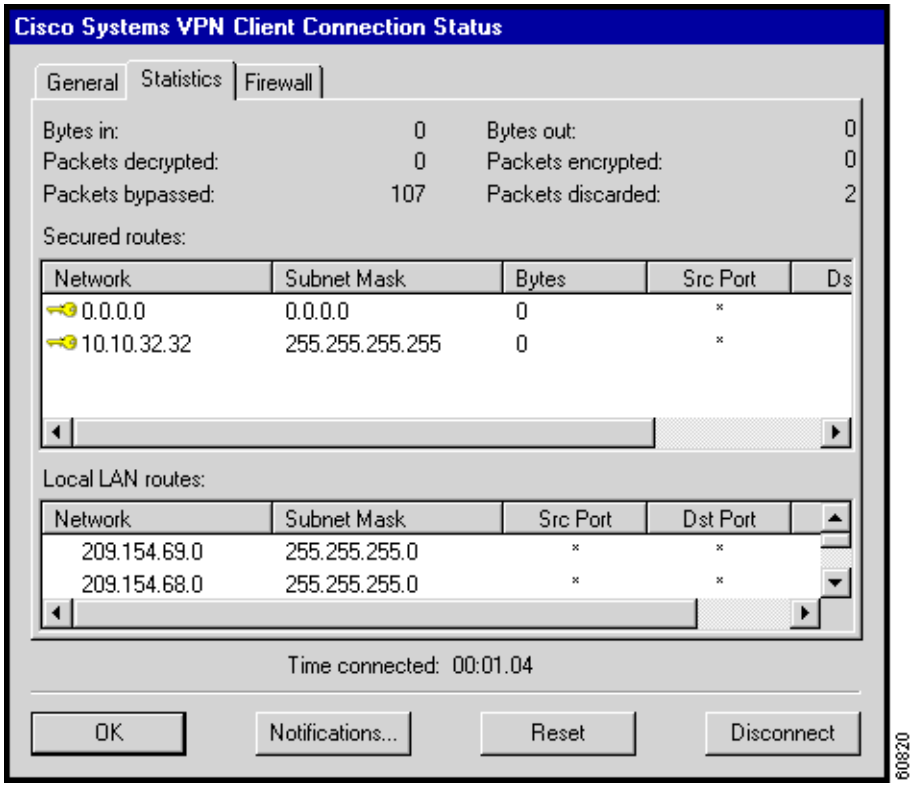
To enable this feature, check **Allow Local LAN Access**; to disable it, clear the check mark from the box. If the local LAN you are using is not secure, you should disable this feature. For example, you would disable this feature when you are using a local LAN in a hotel or airport.

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 on the Statistics tab on the Connection Status dialog box. (See Figure 3-18.)

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

Figure 3-18 Local LAN Access



The Local LAN routes section on the Connection Status dialog box lists the IP address and subnet mask of each available network. The Src Port and Dst Port fields are not currently used.

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 may 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.

Logging on to Microsoft Network (Windows 95, 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, clear the check.

Note This parameter appears only on VPN Clients installed on systems running Windows 95, 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.

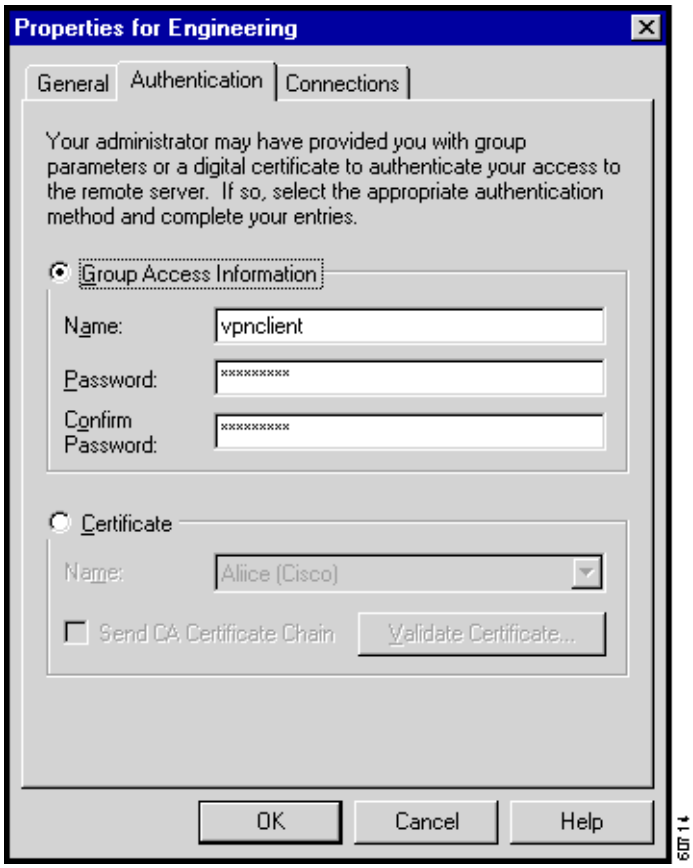
When you are done with the General tab, click **OK** or click another tab.

Changing Authentication Settings

The Properties > Authentication tab (see Figure 3-19) lets you change the name or password of the IPSec group to which you are assigned. Your group determines your access to, and use of, the remote network. The group name and password are essential parameters in authenticating you as a user of the remote network.

If you want to choose a different certificate, you also use this screen.

Figure 3-19 Changing Authentication Parameters from the Authentication Tab



Changing Group Name or Group Password

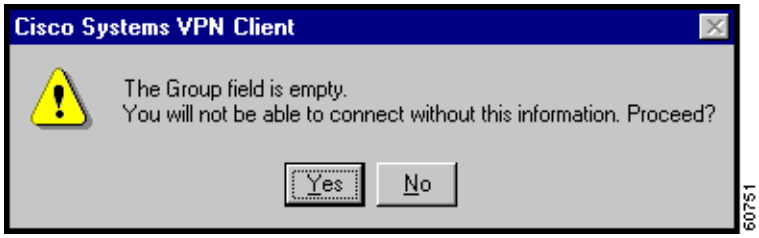
You usually specify a group name and group password when you create a connection entry. However, you can use the Authentication tab to change a group name or group password if your system administrator so instructs you; or to enter the group name and password if the connection entry does not already have them.

In the Name field, enter or edit the group name. This entry is case-sensitive.

In the Password field, enter or edit the group password. This entry is case-sensitive. The field displays only asterisks. Verify your password by entering it again in the Confirm Password field.

If either field is empty when you leave this dialog box, the VPN Client reminds you to enter missing group information. (See Figure 3-20.) To proceed, click **Yes**, or to terminate, click **No**.

Figure 3-20 Reminder Dialog Box

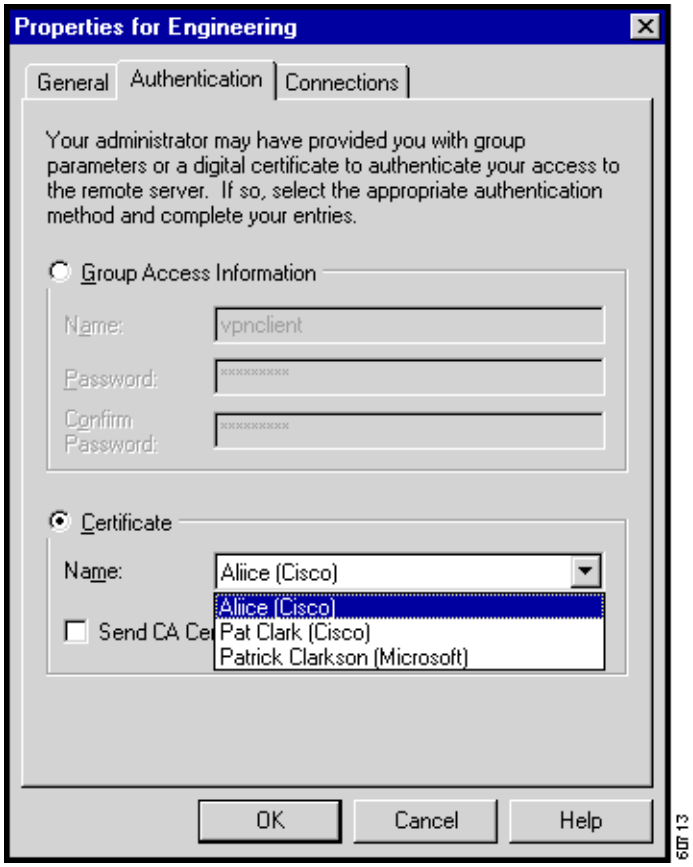


When you are done with the Authentication tab, click **OK** or click another tab.

Choosing a Different Certificate

To choose a different certificate, check the **Certificate** radio button, then click the drop-down menu of certificates installed on your PC and choose one. (See Figure 3-21.)

Figure 3-21 Choosing a Certificate

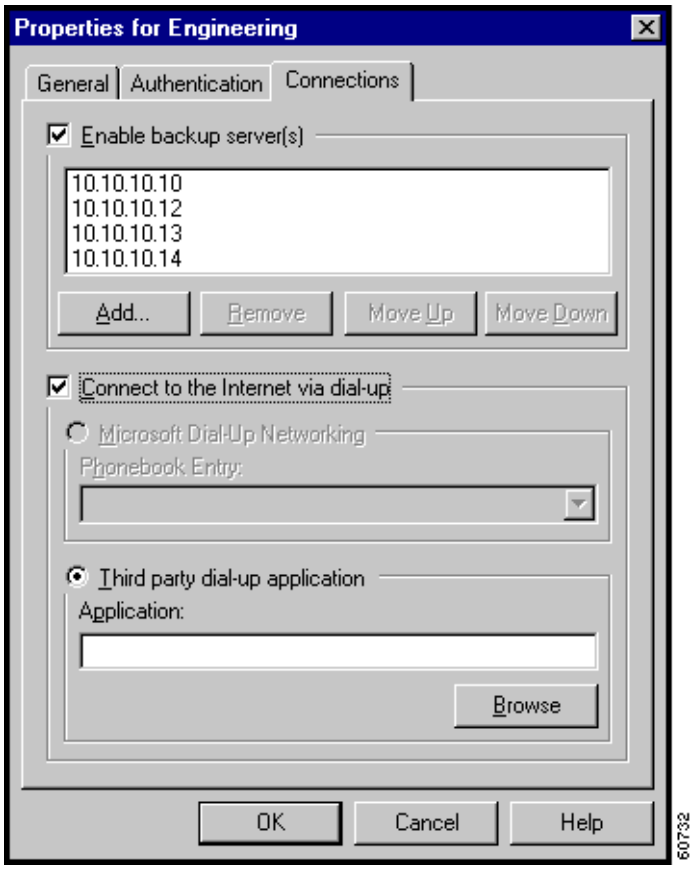


When you are done with the Authentication tab, click **OK** or click another tab.

Changing Connection Settings

The Properties > Connections tab (shown in Figure 3-22) lets you set parameters that govern how you connect to the private network. You can enable and configure backup server connections, and automatically launch a dial-up networking application to connect to the Internet.

Figure 3-22 Changing Parameter Values from the Connections tab



Enabling and Adding Backup Servers

The private network may include one or more backup VPN devices (servers) to use if the primary server is not available. Your system administrator tells you whether to enable a backup server and gives you its address. Refer to your entries in the "Gathering Information You Need".

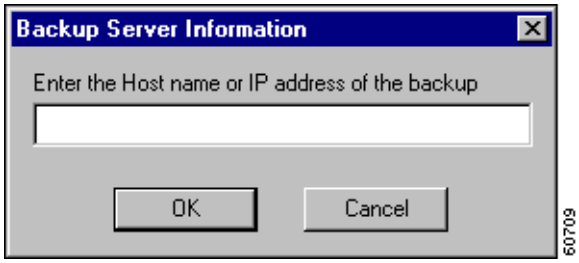
To enable backup servers, perform the following steps:

Step 1 Check **Enable backup server(s)**. This is not checked by default.

Step 2 Click **Add** to enter its address.

The Backup Server Information dialog box appears. (See Figure 3-23.)

Figure 3-23 Entering Backup Server Information



Step 3 Enter the hostname or IP address of the backup server. Use a maximum of 255 characters.

Step 4 Click **OK**.

The hostname or IP address appears in the Enable backup server(s) list. (See Figure 3-22.)

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

Removing Backup Servers

To remove a server from the backup list, choose the server from the list and click **Remove**. *There is no confirmation or undo.* The server name no longer appears in the list.

Changing the Order of the Servers

To reorder the servers in the list, choose a server and click **Move Up** to increase the server's priority or **Move Down** 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, clear the **Enable backup server(s)** check.

Configuring a Connection to the Internet Through Dial-up Networking

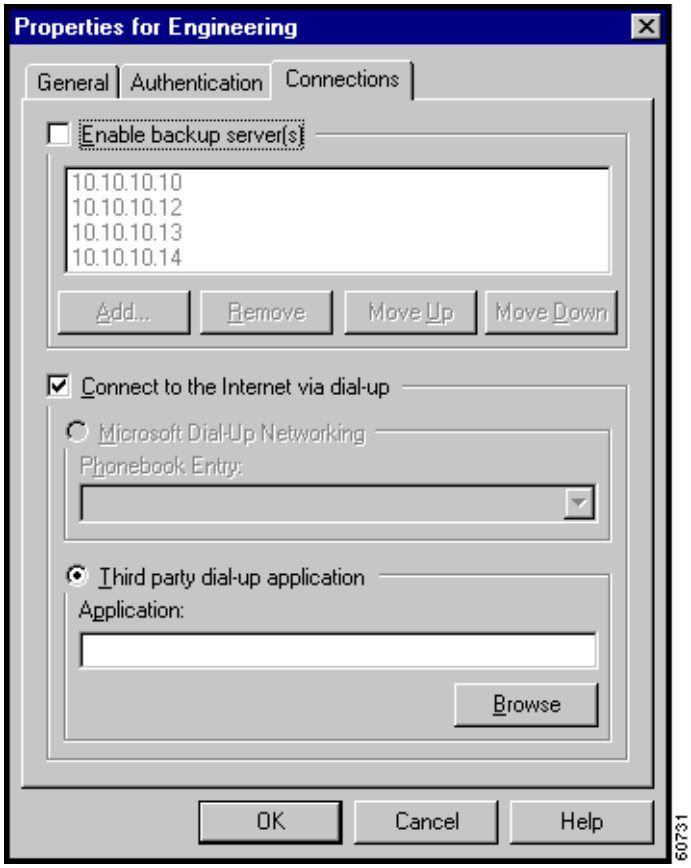
To connect to a private network using a dial-up connection, perform the following two steps:

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 **Connect to the Internet via dial-up**. This is not checked by default. (See Figure 3-24.)

Figure 3-24 Connecting to the Internet Through Dial-up



You can connect to the Internet using the VPN Dialer application in two different 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, perform the following steps:

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 drop-down 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.

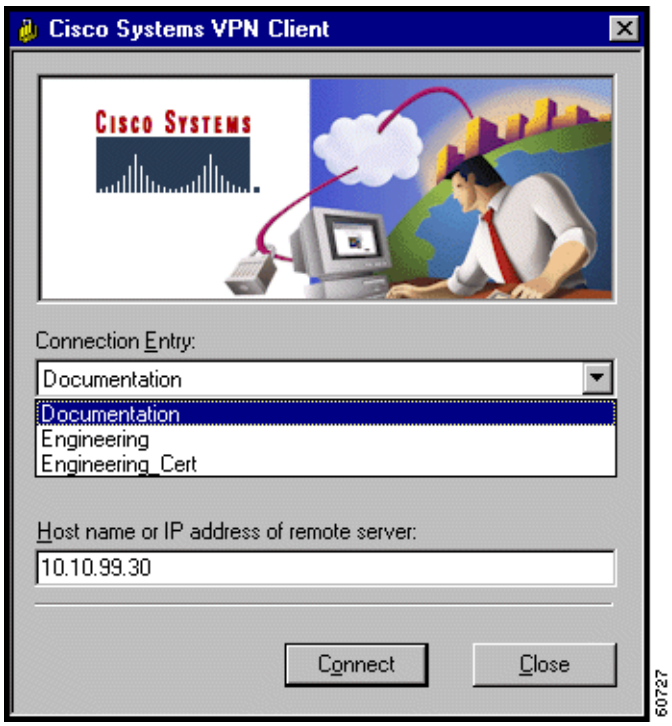
This string you choose or enter here is the pathname to the command that starts the application and the name of the command; for example: c:\isp\ispdialer.exe dialEngineering. Your network administrator may have set this up for you. If not, consult your network administrator.

Changing the VPN Device Address for a Connection Entry

To change the address of the VPN device in a connection entry, and to make the change temporary or permanent, follow these steps:

Step 1 On the VPN Client main dialog box shown in Figure 3-25, click the **Connection Entry** drop-down menu button and choose the entry, if it is not already displayed.

Figure 3-25 Choosing a Connection Entry



Step 2 Edit the address in the Host name or IP address of remote server field.

Step 3 Click **Connect**. The VPN Client displays a confirmation dialog box. (See Figure 3-26.)

Figure 3-26 Confirming Your Changes

Step 4 Click one of the following:

To use this address for the current session only, click **No**. The VPN Client begins connecting to the VPN device, but it does not save the change you have made to the connection entry.

To permanently change the address for this connection entry, click **Yes**. The VPN Client begins connecting to the VPN device, and it saves the new address with the connection entry.

For an explanation of the connection process, see “Connection Procedure”.

Connecting to a Private Network

This chapter explains how to connect to a private network with the VPN Client.

We assume you have configured at least one VPN Client connection entry as described in "Configuring the VPN Client." To connect to a private network, you also need the following information:

- ISP logon username and password, if necessary.
- User authentication information:
  - If you are authenticated via the VPN 3000 Concentrator internal server, your username and password.
  - If you are authenticated via a RADIUS server, your username and password.
  - If you are authenticated via an Windows NT Domain server, your username, password, and domain name.
  - If you are authenticated via RSA Data Security (formerly SDI) SecurID or SoftID, your username and PIN.
  - If you use a digital certificate for authentication, the name of the certificate and your username and password. If your private key is password protected for security reasons, you also need this password.

Refer to your entries in "Gathering Information You Need," as you complete the steps described here, which includes the following sections:

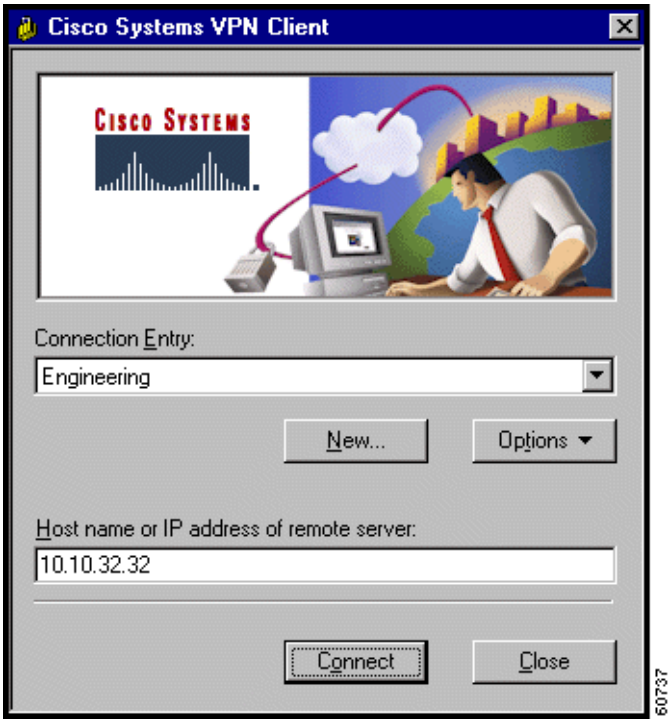
- Starting the VPN Dialer
- Using the VPN Client to Connect to the Internet via Dial-Up Networking
- Authenticating to Connect to the Private Network
- Connecting with Digital Certificates
- Completing the Private Network Connection
- Viewing Connection Status
- Closing the VPN Client
- Disconnecting your VPN Client Connection

Starting the VPN Dialer

Step 1 To start the VPN Dialer application, choose **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

The VPN Dialer displays the VPN Client's main dialog box. (See Figure 4-1.)

Figure 4-1 VPN Dialer Main Dialog Box



Step 2 If necessary, click the **Connection Entry** drop-down menu and choose the desired connection entry.

Connection Procedure

To connect to a private network, perform the following steps:

Step 1 Connect to the Internet, if necessary.

Step 2 Connect to the private network through the Internet.

- Systems with cable or DSL modems are usually connected to the Internet, so no additional action is necessary. Skip to "Authenticating to Connect to the Private Network."
- Systems with modems or ISDN modems must connect to the Internet via Dial-Up Networking:
  - If you connect to the Internet via Dial-up Networking, proceed to "Using the VPN Client to Connect to the Internet via Dial-Up Networking."

– If you must manually connect to the Internet, do it now. When your connection is established, skip to "Authenticating to Connect to the Private Network."

– If your system is already connected to the Internet via Dial-Up Networking, skip to "Authenticating to Connect to the Private Network."

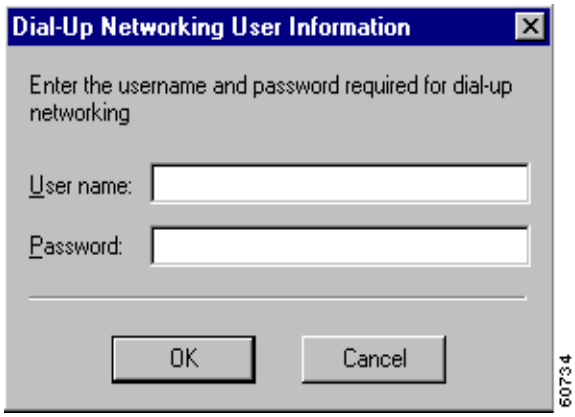
Using the VPN Client to Connect to the Internet via Dial-Up Networking

This section describes how to connect to the Internet via Dial-Up Networking by running only the VPN Client. Your connection entry must be configured with Connect to the Internet via Dial-Up Networking enabled; see "Configuring the VPN Client".

Step 1 Click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

If your credentials are not stored in the RAS database, the Dial-up Networking User Information dialog box appears. (See Figure 4-2.) This dialog box varies depending on the version of Windows you are using.

Figure 4-2 Entering User Information



Step 2 Enter your username and password to access your ISP. These entries may be case-sensitive. The Password field displays only asterisks.

Step 3 Click **OK**.

You see the Connection History dialog box. (See Figure 4-3.)

Figure 4-3 Confirming Connections to ISP

When the ISP connection is established, a Dial-Up Networking icon appears in the system tray on the Windows task bar. (See Figure 4-4.)

Figure 4-4 Dial-Up Networking task bar Icon

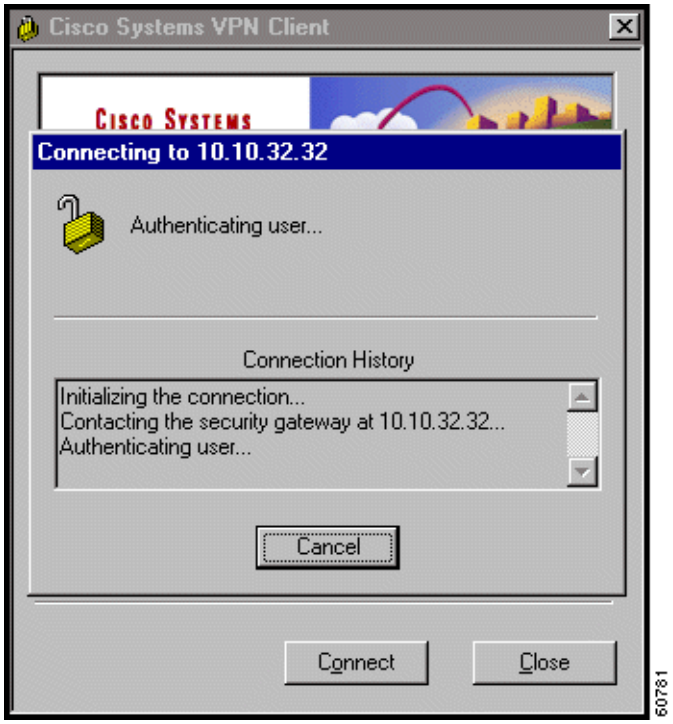
Authenticating to Connect to the Private Network

This section assumes you are connected to the Internet. If you connect using Dial-Up Networking, verify that its icon is visible in the Windows task bar system tray. (See Figure 4-4.) If not, your Dial-Up Networking connection is not active and you need to establish it before continuing.

If you did not do so earlier, click **Connect** on the VPN Client's main dialog box. (See Figure 4-1.)

The VPN Client starts tunnel negotiation and displays the Connection History dialog box. (See Figure 4-5.)

Figure 4-5 Negotiating Dialog Box



The next phase in tunnel negotiation is user authentication.

User Authentication

User authentication means proving that you are a valid user of this private network. User authentication is optional. Your administrator determines whether it is required.

The VPN Client displays a user authentication dialog box that differs according to the authentication that your IPSec group uses. Your system administrator tells you which method to use.

To continue, refer to your entries in “Gathering Information You Need” and go to the appropriate authentication section that follows.

Authenticating Through the VPN Device Internal Server or RADIUS Server

To display the user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

Figure 4-6 Authenticating Through an Internal or RADIUS Server

Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 Click **OK**.

Note If you cannot choose the Save Password option, your administrator does not allow this option. If you can choose this option, be aware that using it might compromise system security, since your password is then stored on your PC and is available to anyone who uses your PC.

If Save Password is checked and authentication fails, your password may be invalid. To eliminate a saved password, click **Options** > **Erase User Password**.

Proceed to the section "Completing the Private Network Connection."

Authenticating Through a Windows NT Domain

To display the Windows NT Domain user authentication dialog box, perform the following steps. The title bar identifies the connection entry name.

Figure 4-7 Authenticating Through a Windows NT Domain

Step 1 In the Username field, enter your username. This entry is case-sensitive.

Step 2 In the Password field, enter your password. This entry is case-sensitive. The field displays only asterisks.

Step 3 In the Domain field, enter your Windows NT Domain name, if it is not already there.

Step 4 Click **OK**.

Skip to "Completing the Private Network Connection."

Changing your Password

Your network administrator may have configured your group for RADIUS with Expiry authentication on the VPN 3000 Concentrator. If this feature is in effect and your password has expired, a dialog box prompts you to enter and confirm a new password.

After you have tried unsuccessfully to log in three times, you might receive one of the following login messages:

- Restricted login hours
- Account disabled
- No dial-in permission
- Error changing password
- Authentication failure

Authenticating Through RSA Data Security (RSA) SecurID

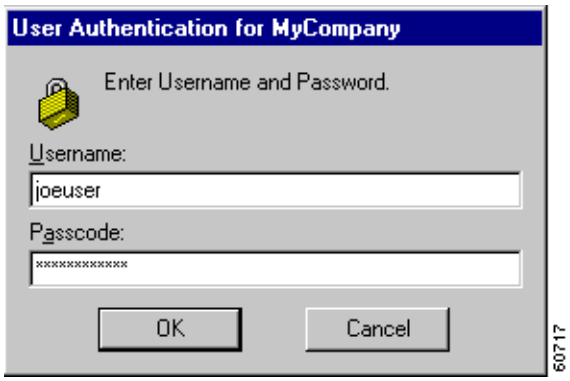
RSA (formerly SDI) SecurID authentication methods include physical SecurID cards and keychain fobs, and PC software called SoftID. SecurID cards also vary: with some cards, the passcode is a combination of a PIN and a cardcode; with others, you enter a PIN on the card and it displays a passcode. Ask your system administrator for the correct procedure.

Authentication via these methods also varies slightly for different operating systems. If you use an RSA method, the VPN Client displays the appropriate RSA user authentication dialog box. The title bar identifies the connection entry name.

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95, Windows 98, and Windows ME)

To display an authentication dialog box asking for your username and passcode, perform the following steps. (See Figure 4-8.) If you are using SoftID, it must be running on your PC.

Figure 4-8 Authenticating through RSA



Step 1 In the Username field, enter your username. This entry is case-sensitive.

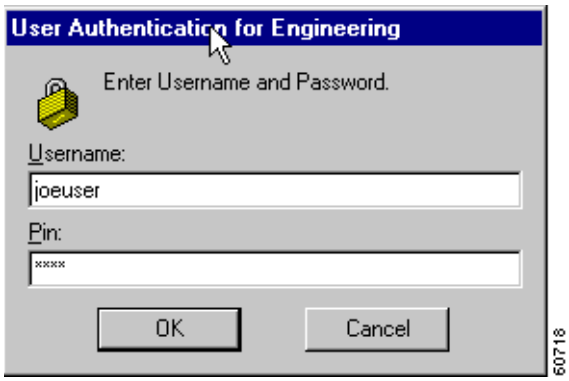
Step 2 In the Passcode field, enter a SecurID code. With SoftID, you can copy this code from the SoftID window and paste it here. Your administrator will tell you what you need to enter here, depending on the type of tokencard you are using.

Step 3 After entering the code, click **OK**.

RSA User Authentication: SoftID v1.x (Windows NT Only) and SoftID v2.0 (All Operating Systems)

If you are using SoftID under Windows NT, the VPN Client displays an authentication dialog box asking for your username and PIN. (See Figure 4-9).

Figure 4-9 Authenticating Through SoftID on Windows NT



Step 1 In the Username field, enter your username. This entry is case-sensitive.

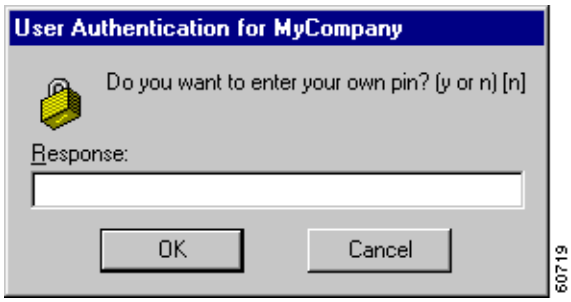
Step 2 In the PIN field, enter your SoftID PIN. The VPN Client gets the passcode from SoftID by communicating directly with SoftID. The SoftID application must be installed but does not have to be running on your PC.

Step 3 After entering the PIN, click **OK**.

RSA New PIN Mode

The first time you authenticate using SecurID or SoftID (all operating systems), or if you are using a new SecurID card, and if the RSA administrator allows you to create your own PIN, the authentication program asks if you want to create your own PIN. (See Figure 4-10.)

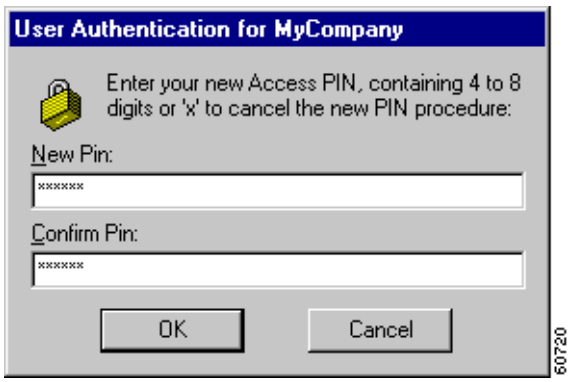
Figure 4-10 SecurID New PIN Request



Step 1 Enter your response **y** for yes or **n** for no. No is the default response. Then, click **OK**. What happens next depends on your response.

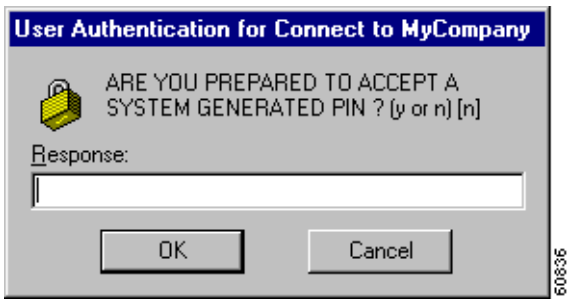
- If you responded yes—Enter your new PIN in the New PIN field and enter it again in the Confirm PIN field. Click **OK**. (See Figure 4-11.)

Figure 4-11 Entering a New PIN Yourself



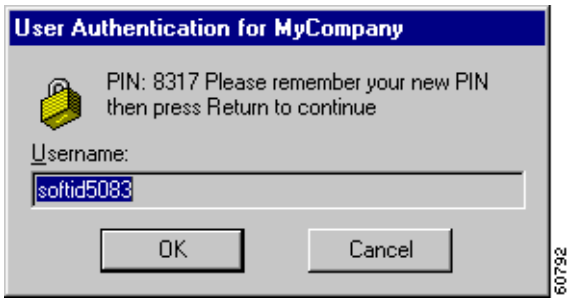
- If you responded no—the authentication program asks if you will accept a system-generated PIN. (See Figure 4-12.)

Figure 4-12 Accepting a PIN from the System



Step 2 To receive a PIN, you must respond **y** for yes and then click **OK**. When you do, the authentication program generates a PIN for you and displays it. (See Figure 4-13.) Be sure to remember your PIN.

Figure 4-13 New PIN Received



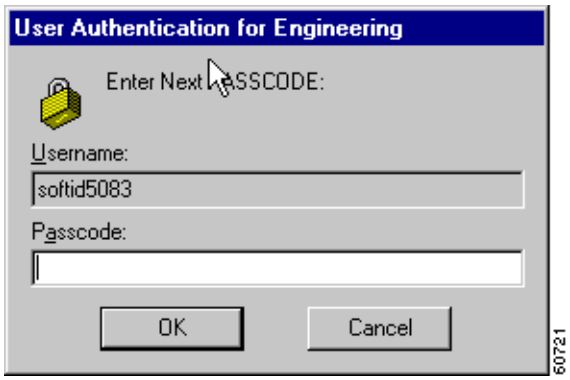
Step 3 To continue, click **OK**.

SecurID Next Cardcode Mode

Sometimes SecurID authentication prompts you to enter the next cardcode from your token card, as in Figure 4-14. SecurID displays this prompt either to resynchronize the token card with the RSA server, or because it noticed several unsuccessful attempts to authenticate with this username.

The SecurID Next Cardcode Mode dialog box might appear. (See Figure 4-14.)

Figure 4-14 Entering the Passcode for SecurID Next Card



In the Passcode field, enter the next code from your token card. This field requires only a cardcode. Do not include your PIN as part of the passcode.

Now continue to "Completing the Private Network Connection."

Connecting with Digital Certificates

Before you created a connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on your system. If this is not the case, then you need to obtain a digital certificate. In many cases, the network administrator of your organization can provide you with a certificate. If not, then you can obtain one by enrolling with a PKI directly using the Certificate Manager application, or you can obtain an Entrust profile through Entrust Entelligence™. Currently, we support the following PKIs:

- UniCERT from Baltimore Technologies (www.baltimoretechnologies.com)
- Entrust PKI™ from Entrust Technologies (www.entrust.com)
- Versign (www.verisign.com)
- Microsoft Certificate Services in Microsoft Windows 2000 Server
- Cisco Certificate Store

The websites listed in parentheses in this list contain information about the digital certificates that each PKI provides. The easiest way to enroll in a PKI or import a certificate is to use the Certificate Manager (see "Enrolling and Managing Certificates") or Entrust Entelligence (see Entrust documentation).

Note Every time you connect using a certificate, the VPN Client checks to verify that your certificate has not expired. If your certificate is within one month of expiring, the VPN Client displays a message when you attempt to connect or when you use the Properties option. The message displays the certificate common name, the "not before" date, the "not after" date, and the number of days until the certificate expires or since it has expired.

There is one exception to this rule. When you are authenticating with a Microsoft certificate, the VPN Dialer skips the automatic certificate validation process and starts the connection immediately. If there is a problem with the certificate, the connection attempt fails. To obtain information about the failure, look in the connection log file (see "Viewing and Managing the VPN Client Event Log"). To validate the certificate manually, choose Properties > Authentication > Validate Certificate.

What happens when you press **Connect** can depend on the level of private key protection on your certificate. If your certificate is password protected, you are prompted to enter the password.

Connecting with an Entrust Certificate

This section provides important information about what to expect when connecting with an Entrust certificate under certain conditions.

Accessing Your Profile

If you are not already logged in, you must log in to Entrust Entelligence to access your Entrust Entelligence certificate profile, using the following procedure:

After you choose **Connect** on the VPN Client main dialog box, the Entrust logon dialog box appears. (See Figure 4-15.)

Figure 4-15 Logging in to Entrust

Step 1 Choose a profile name from the pull-down menu.

Your network administrator has previously configured one or more profiles for you through Entrust Entelligence. If the software is installed on your system but there are no profiles available, then you need to get a profile from your network administrator or directly through Entrust. Refer to *Entrust Entelligence Quick Start Guide* for instructions on obtaining a profile. The *VPN Client Administrator Guide* contains supplementary configuration information.

Step 2 After choosing a profile, enter your Entrust password.

Check the Work offline field to use Entrust Entelligence without connecting to the Entrust PKI. If Work offline is checked and you press **OK**, the Entrust wizard displays the message shown in Figure 4-16.

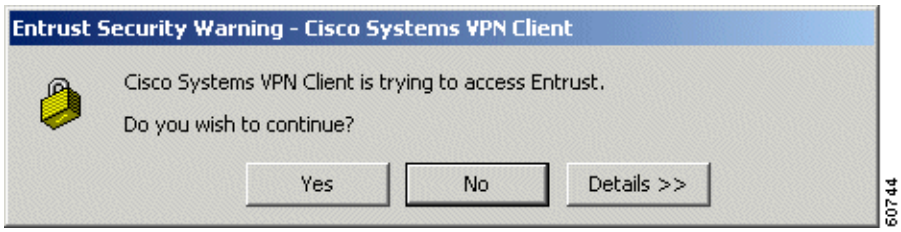
Figure 4-16 Entrust Login Message

You can ignore this message. Since you are connecting to your organization's private network using an existing certificate profile, you are not interacting with the Entrust PKI. If you see this message, click **OK** to continue.

Step 3 After completing the Entrust Login dialog box (see Figure 4-15), click **OK**.

You may receive a security warning message from Entrust. This warning occurs, for example, when an application attempts to access your Entelligence profile for the first time or when you are logging in after a VPN Client software update. The message happens because Entrust wants to verify that it is acceptable for the VPN Client to access your Entrust profile.

Figure 4-17 Entrust Security Warning



Step 4 At the warning message, click **Yes** to continue.

You can now use your Entrust certificate for authenticating your new connection entry.

Entrust Inactivity Timeout

If you have a secure connection and you see a padlock next to the Entelligence icon in the Windows system tray, Entelligence has timed out. However you have not lost your connection. If you see the Entelligence icon with an X next to it, you are logged out of Entrust and you did not have a secure connection initially. To make a new connection, start from the beginning (see "Accessing Your Profile").

Using Entrust SignOn and Start Before Logon Together

Entrust SignOn™ is an optional Entrust application that lets you use one login and password to access Microsoft Windows and Entrust applications. This application is similar to Start Before Logon, which is a VPN Client feature that enables you to dial in before logging on to Windows NT. For information about Start Before Logon, see "Starting a Connection Before Logging on to a Windows NT Platform".

If you want to use these two features together, you should make sure you have installed Entrust Entelligence with the Entrust SignOn module before installing the VPN Client. For information about installing Entrust SignOn, refer to Entrust documentation and the *VPN Client Administrator Guide*, Chapter 1.

To use these two features together, follow these steps:

Step 1 Start your system.

When the SignOn option is installed, Entrust displays its own Ctrl Alt Delete dialog box.

Step 2 Click **Ctrl Alt Delete**.

The Entrust Options dialog box and the VPN Dialer login dialog box both pop up. The VPN Dialer dialog box is active.

Step 3 To start your VPN connection, click **Connect** on the VPN Dialer main dialog box.

The Entrust login dialog box becomes active.

Step 4 To log in to your Entrust profile, enter your Entrust password.

The VPN Dialer password prompt dialog box becomes active.

Step 5 Enter your VPN dialer username and password.

The VPN Client authenticates your credentials and optionally displays a banner and/or a notification. Respond to the banner or notification as required. Then the Windows NT logon dialog box is active.

Step 6 To complete the connection, enter your Windows NT logon credentials in the Windows logon dialog box and you are done.

Connecting with a Smart Card or Token

The VPN Client supports authentication with digital certificates through a smart card or electronic token. There are several vendors that provide smart cards and tokens. For an up-to-date list of those that the VPN Client currently supports, see "Smart Cards Supported". Smart card support is provided through Microsoft Cryptographic API (MS CAPI). Any CryptoService provider you use must support signing with CRYPT_NOHASHOID.

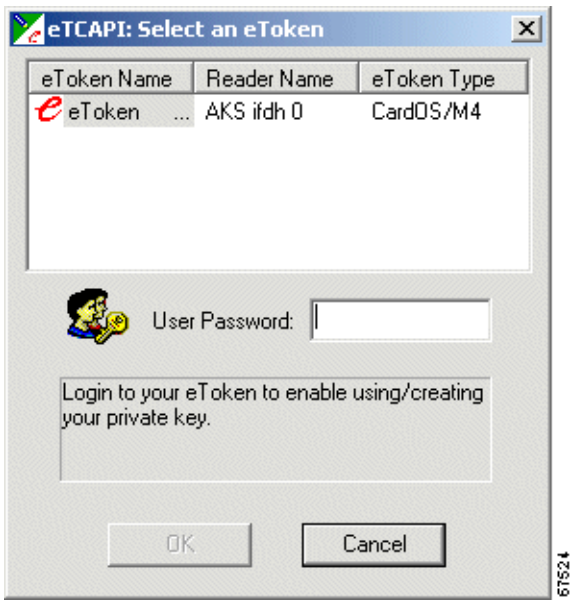
Once you or your network administrator has configured a connection entry that uses a Microsoft certificate provided by a smart card, you must insert the smart card into the receptor. When you start your connection, you are prompted to enter a password or PIN, depending on the vendor. For example, Figure 4-18 shows the authentication prompt from ActivCard Gold.

Figure 4-18 ActivCard Gold PIN Prompt

In above example, you would type your PIN code in the Enter PIN code field and click **OK**.

The next example shows how to log in to eToken from Aladdin. You select the token in the eToken Name column, type a password in the User Password field, and click **OK**.

Figure 4-19 eToken Prompt



Note If your smart card or token is not inserted, the authentication program displays an error message. If this occurs, insert your smart card or token and try again.

Completing the Private Network Connection

After completing the user authentication phase, the VPN Client continues negotiating security parameters and displays a dialog box. (See Figure 4-20.) The title bar identifies the remote Cisco VPN device to which you are connecting.

Figure 4-20 Completing Connection History

If the network administrator of the Cisco VPN device has created a client banner, you see a message designated for all clients connecting to that device; for example, `The Documentation Server will be down for routine maintenance on Sunday`.

After you complete your connection, the VPN Client minimizes to an icon in the system tray on the Windows task bar.

You are now connected securely to the private network via a tunnel through the Internet, and you can access the private network as if you were an onsite user.

Viewing Connection Status

The VPN Client icon on the task bar  lets you view the status of your private network connection.

- Double-click the icon, or
- Click the icon with the right mouse button and choose **Status** from the pop-up menu.

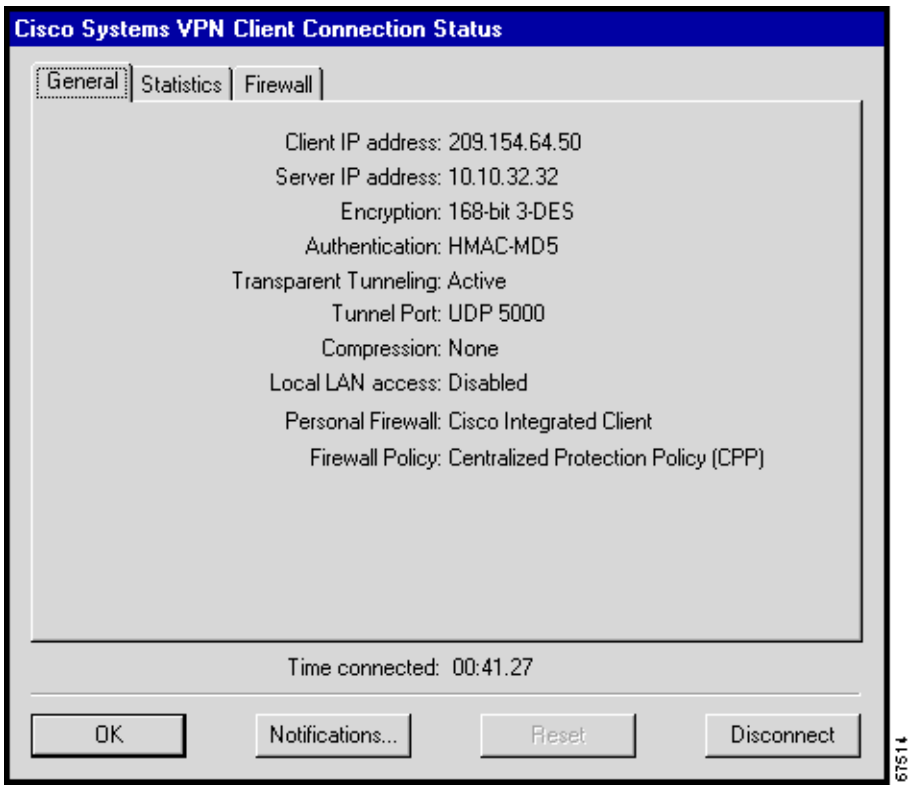
The VPN Client Connection Status dialog box appears. The dialog contains three tabs:

- General (See Figure 4-21.)
- Statistics (See Figure 4-22.)
- Firewall (See Figure 4-23).

General Information

The General tab on the Connection Status dialog box provides IP security information, listing the IPSec parameters that govern the use of this VPN tunnel to the private network.

Figure 4-21 Viewing IPSec Security Information



Theparameters are the following:

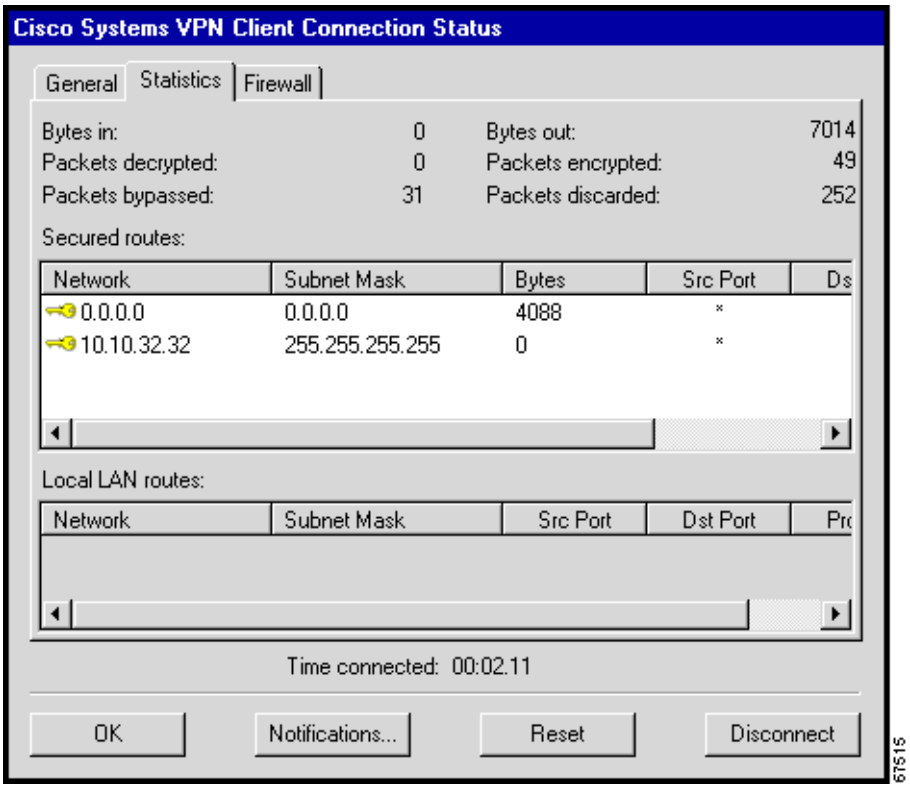
- Client IP address—The IP address assigned to the VPN Client for the current session.
- Server IP address—The IP address of the VPN device to which the VPN Client is connected.
- Encryption—The data encryption method for traffic through this tunnel. Encryption makes data unreadable if intercepted.
- Authentication—The data, or packet, authentication method used for traffic through this tunnel. Authentication verifies that no one has tampered with data.
- Transparent Tunneling—The status of tunnel transparent mode in the client, either active or inactive.
- Tunnel Port—If Transparent Mode is active, the tunnel port through which packets are passing. This field also identifies whether the VPN Client is sending packets through UDP or TCP. This port number comes from the VPN device. If UDP, the port is negotiated; if TCP the port is preconfigured. If Transparent Tunneling is inactive, then the value of Tunnel Port is zero.
- Compression—Whether data compression is in effect as well as the type of compression in use. Currently, LZS is the only type of compression that the VPN Client supports.

- Local LAN Access—Whether this parameter is enabled or disabled. (For information on configuring this feature, see "Allowing Local LAN Access".)
- Personal Firewall—The name of the firewall that the VPN Client is enforcing, such as the Cisco Integrated Client, Zone Labs ZoneAlarm, ZoneAlarm Pro, BlackICE Defender, and so on.
- Firewall Policy—The firewall policy in use:
  - AYT (Are You There) enforces the use of a specific personal firewall but does not require you to have a specific firewall policy.
  - Centralized Protection Policy (CPP) or "Policy Pushed" as defined on the VPN Concentrator lets you define a stateful firewall policy that the VPN Client enforces for Internet traffic while a tunnel is in effect. CPP is for use during split tunneling and is not relevant for a tunnel everything configuration. In a tunnel everything configuration, all traffic other than tunneled traffic is blocked during the tunneled connection.
  - Client/Server corresponding to "Policy from Server" (Zone Labs Integrity) on the VPN Concentrator

Statistics

The Statistics tab on the Connection Status dialog box shows statistics for data packets that the VPN Client has processed during the current session or since the statistics were reset. Reset affects only this tab.

Figure 4-22 Viewing Statistics



Bytes in—The total amount of data received after a secure packet has been successfully decrypted.

Bytes out—The total amount of encrypted data transmitted through the tunnel.

Packets decrypted—The total number of data packets received on the port.

Packets encrypted—The total number of secured data packets transmitted out the port.

Packets bypassed—The total number of data packets that the VPN Client did not process because they did not need to be encrypted. Local ARPs and DHCP fall into this category.

Packets discarded—The total number of data packets that the VPN Client rejected because they did not come from the secure VPN device gateway.

Secured Routes

The Secured Routes section lists the IPSec Security Associations (SAs).

In Figure 4-22 under Secured Routes, the columns show the following types of information:

Key icon—In the first row, you see a key at the start of the connection entry. This key shows that the route is secure. The software generates a key as soon as the client needs to send secure data through the tunnel to the networks on the other side. The absence of a key means that the SA is no longer active. The SA may have timed out due to inactivity. Sending data to this network re-establishes the SA, and the key reappears.

Network—The IP address of the remote private network with which this VPN Client has an SA.

Subnet Mask—The subnet mask of the IP address for this SA.

Bytes—The total amount of data this SA has processed. This includes data before encryption as well as encrypted data received.

Src Port, Dst Port, and Protocol are for future use.

Local LAN Routes

If active the Local LAN Routes box shows the network addresses of the networks you can access on your local LAN while you are connected to your organization's private network through an IPSec tunnel. You can access up to 10 networks on the client side of the connection. A network administrator at the central site must configure the networks you can access from the client side. For information on configuring Local LAN Access on the VPN 3000 Concentrator, refer to *VPN Client Administrator Guide*, Chapter 1.

Time Connected

The Statistics tab also displays the time in days, hours, minutes and seconds, that has elapsed since you initiated the connection.

Firewall Tab

The Firewall tab displays information about the VPN Client's firewall configuration.

The VPN Concentrator's network manager sets up the firewall policy under Configuration | User Management | Base Group or Group | Client FW tab. There are three options:

- Are You There—The supported personal firewall software on the VPN Client PC controls its own rules. The VPN Client polls the firewall every 30 seconds to make sure it is still running, but does not confirm that a specific policy is enforced.

- Centralized Protection Policy—This policy takes advantage of the Cisco Integrated Client. The policy rules are defined on the VPN Concentrator and sent to the VPN Client during each connection attempt. The VPN Client enforces these rules for all non-tunneled traffic while the tunnel is active.
- Client/Server—This policy relates to Zone Labs Integrity solution. The policy is defined on the Integrity Server in the private network and sent to the VPN Concentrator, which in turns sends it to the Integrity Agent on the VPN Client PC to implement. Since Integrity is a fully functional personal firewall, it can intelligently decide on network traffic based on applications as well as data.

Note CPP affects Internet traffic only. Traffic across the tunnel is unaffected by its policy rules. If you are operating in tunnel everything mode, enabling CPP has no affect.

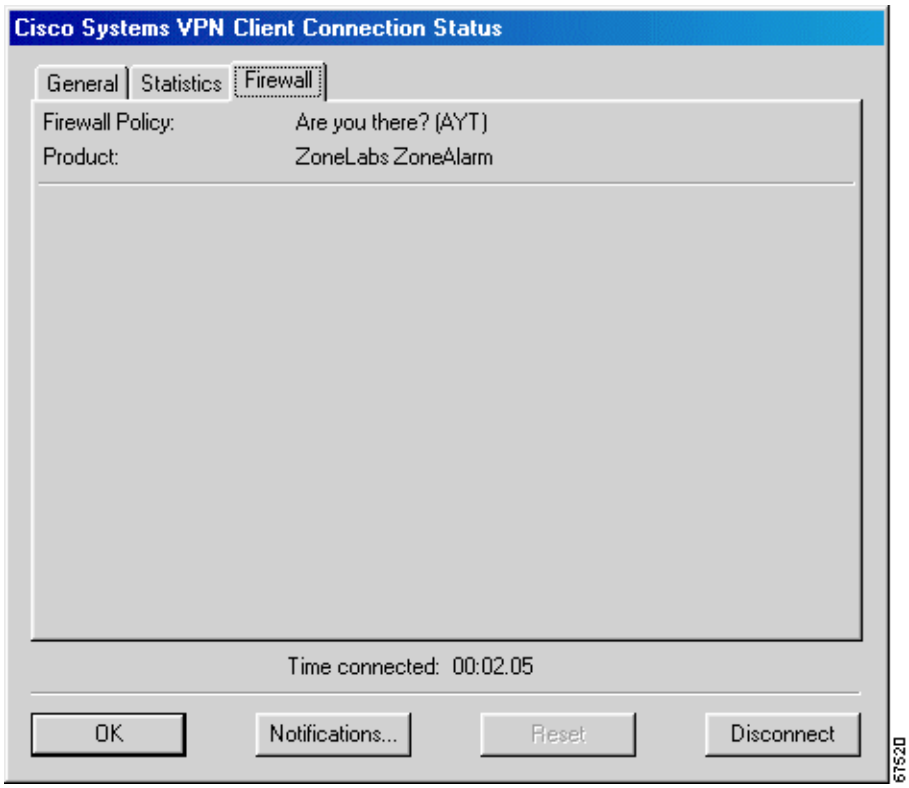
The information shown on this tab varies according to your firewall policy.

- AYT—When the Are You there (AYT) is the supported capability, the Firewall tab shows only the firewall policy (AYT) and the name of the firewall product (see Figure 4-23).
- Centralized Protection Policy (CPP)—When CPP is the supported capability, the Firewall tab includes the firewall policy, the firewall in use, and firewall rules (see Figure 4-23).
- Client/Server—When the Client/Server is the supported capability, the Firewall tab displays the the firewall policy as Client/Server, the name of the product as ZoneLabs Integrity Agent, the user ID, session ID, and the addresses and port numbers of the firewall servers (see Figure 4-25).

AYT Firewall Tab

The Firewall tab shows that AYT is running and displays the name of the firewall product that supports AYT.

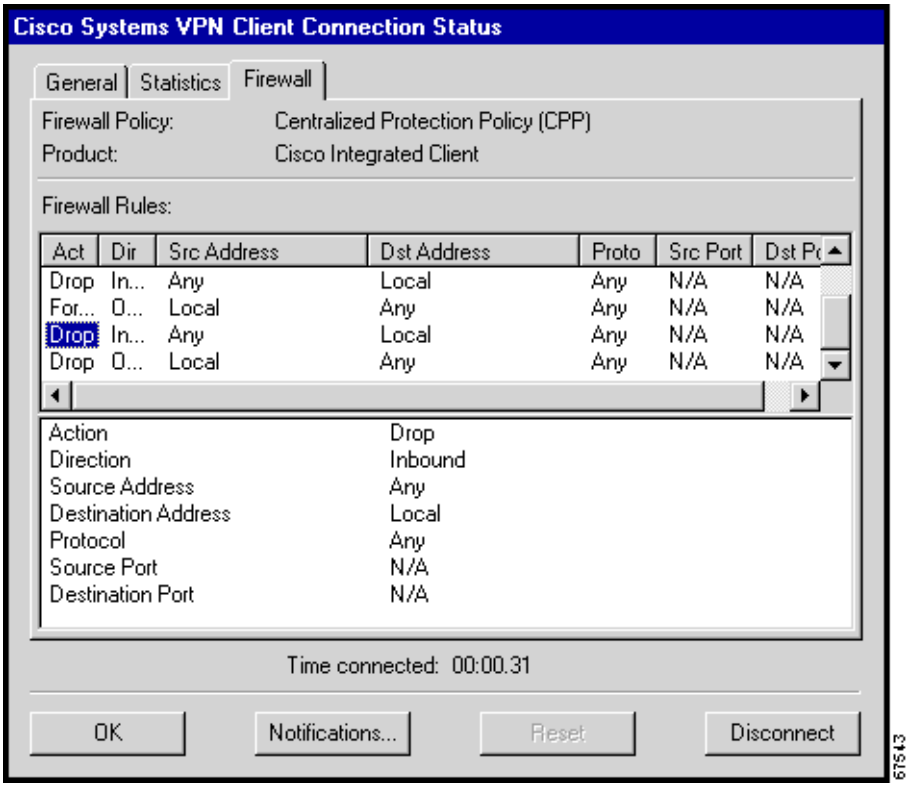
Figure 4-23 Firewall Tab for AYT capability



Centralized Protection Policy (CPP) Using the Cisco Integrated Client

CPP is a stateful firewall policy that is defined on and controlled from the VPN Concentrator. It can add protection for the VPN Client PC and private network from intrusion when split tunneling is in use. For CPP (see Figure 4-24), the Firewall tab shows you the firewall rules in effect. Firewall Tab for CPP.

Figure 4-24 Firewall Tab for CPP



This status screen lists the following information:

Firewall Policy—The policy established on the VPN Concentrator for this VPN Client.

Product—Lists the name of the firewall currently in use, such as Cisco Integrated Client, Zone Alarm Pro, and so on.

Firewall Rules

The Firewall Rules section shows all of the firewall rules currently in effect on the VPN Client. Rules are in order of importance from highest to lowest level. The rules at the top of the table allow inbound and outbound traffic between the VPN Client and the secure gateway and between the VPN Client and the private networks with which it communicates. For example, there are two rules in effect for each private network that the VPN Client connects to through a tunnel (one rule that allows traffic outbound and another that allows traffic inbound). These rules are part of the VPN Client software. Since they are at the top of the table, the VPN Client enforces them before examining CPP rules. This approach lets the traffic flow to and from private networks.

CPP rules (defined on the VPN Concentrator) are only for nontunneled traffic and appear next in the table. For information on configuring filters and rules for CPP, see *VPN Client Administrator Guide*, Chapter 1. A default rule “Firewall Filter for VPN Client (Default)” on the VPN Concentrator lets the VPN Client send any data out, but permits return traffic in response only to outbound traffic.

Finally, there are two rules listed at the bottom of the table. These rules, defined on the VPN Concentrator, specify the filter’s default action, either drop or forward. If not changed, the default action is drop. These rules are used only if the traffic does not match any of the preceding rules in the table.

Note The Cisco Integrated Client firewall is stateful in nature, where the protocols TCP, UDP, and ICMP allow inbound responses to outbound packets. For exceptions, refer to *VPN Client Administrator Guide*, Chapter 1. If you want to allow inbound responses to outbound packets for other protocols, such as HTTP, a network administrator must define specific filters on the VPN Concentrator.

You can move the bars on the column headings at the top of the box to expand their size; for example, to display the complete words Action and Direction rather than Act or Dir. However, each time you exit from the display and then open this status tab again, you must expand the columns again. Default rules on the VPN Concentrator (drop any inbound and drop any outbound) are always at the bottom of the list. These two rules act as a safety net and are in effect only when traffic does notmatch any of the rules higher in the hierarchy.

To display the fields of a specific rule, click on the first column and observe the fields in the next area below the list of rules. For example, the window section underneath the rules in Figure 4-24 displays the fields for the rule that is highlighted in the list.

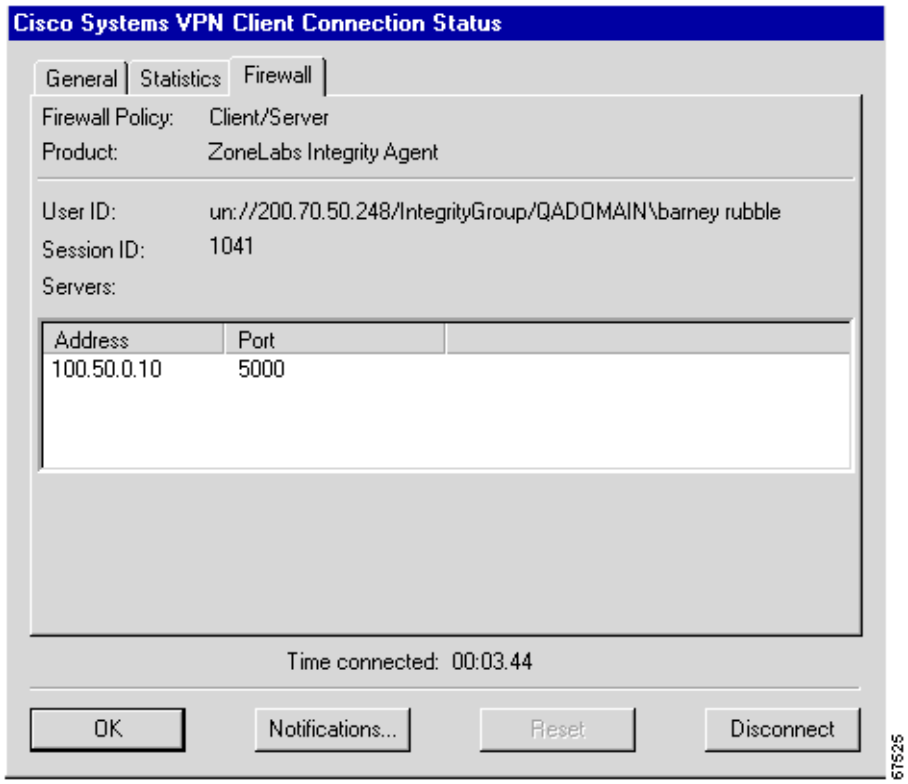
A firewall rule includes the following fields:

- Action—The action taken if the data traffic matches the rule:
  - Drop = Discard the session.
  - Forward = Allow the session to go through.
- Direction—The direction of traffic to be affected by the firewall:
  - Inbound = traffic coming into the PC, also called local machine.
  - Outbound = traffic going out from the PC to all networks while the VPN Client is connected to a secure gateway.
- Source Address—The address of the traffic that this rule affects:
  - Any = all traffic; for example, drop any inbound traffic.
  - This field can also contain a specific IP address and subnet mask.
  - Local = the local machine; if the direction is Outbound then the Source Address is local.
- Destination Address—The packet's destination address that this rule checks (the address of the recipient).
  - Any = all traffic; for example, forward any outbound traffic.
  - Local = The local machine; if the direction is Inbound, the Destination Address is local.
- Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP and so on).
- Source Port—Source port used by TCP or UDP.
- Destination Port—Destination port used by TCP or UDP.

Client/Server Firewall Tab

When Client/Server is the supported policy, the Firewall tab displays the name of the firewall policy, the name of the product, the user ID, session ID, and the addresses and port numbers of the firewall servers in the private network (see Figure 4-25). Zone Labs Integrity is a Client/Server firewall solution in which the Integrity Server (IS) acts as the firewall server that pushes firewall policy to the Integrity Agent (IA) residing on the VPN Client PC. Zone Labs Integrity can also provide a centrally controlled always on personal firewall.

Figure 4-25 Client/Server Firewall Tab



Firewall Policy—This field shows that Client/Server is the supported policy.

Product—Lists the name of the Client/Server solution currently in use, such as Zone Labs Integrity Client.

User ID—In the format *xx*://*IP address of the VPN Concentrator*/*group name and user name*

Where: *xx* can be **un** or **dn**:

un = The gateway-based ID is based on the group and user name.

dn = The gateway-based ID is based on the distinguished name (as is the case when using digital certificates).

The User ID is used to initialize the firewall client.

Session ID—The session ID of the connection between all of the entities. This is used to initialize the firewall client and is helpful for troubleshooting.

Servers—The IP address and port number of each firewall server. For Release 3.5, there is only one.

Resetting Statistics

To reset all connection statistics to zero, click **Reset**. *There is no undo*. Reset affects only the connection statistics, not the other sections of this dialog box.

Closing the VPN Client

You may want to close the VPN Client when it is running on your PC but not connected to a remote network.

To close the VPN Client when it is not connected to a remote network, do one of the following:

- Click **Close** on the VPN Dialer's main dialog box. (See Figure 4-1).
- Press **Esc** on your keyboard.
- Press **Alt-F4** on your keyboard.

Disconnecting your VPN Client Connection

To disconnect your PC from the private network, do one of the following:

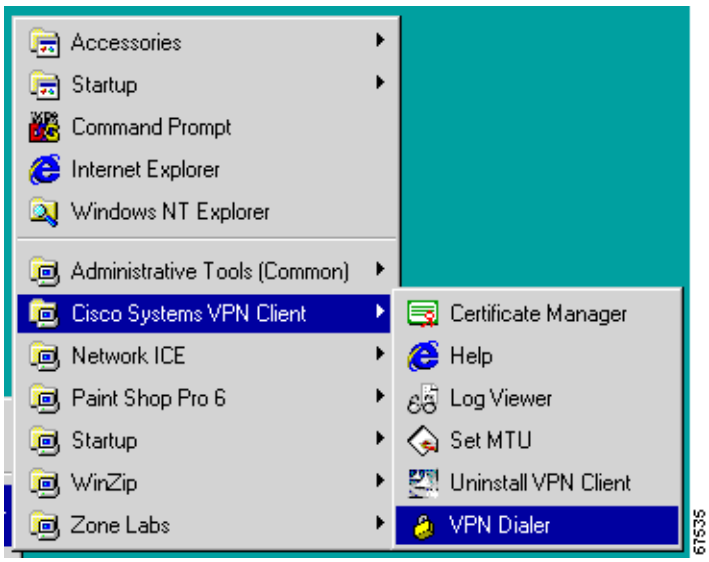
- Double-click the VPN Client icon on the Windows task bar. Click **Disconnect** on the Connection Status dialog box. (See Figure 4-21.)
- Click the VPN Client icon with the secondary mouse button and choose **Disconnect** from the pop-up menu.

Your IPSec session ends and the VPN Client closes. You must manually disconnect your dial-up networking connection (DUN).

Managing the VPN Client

This chapter explains the tasks you can perform to manage connection entries, view and manage event reporting, and upgrade or uninstall the VPN Client software. The management features are available from the Cisco Systems VPN Client applications menu. (See Figure 5-1.)

Figure 5-1 Cisco Systems VPN Client Menu of Applications



This chapter includes the following sections:

- Managing VPN Client Connection Entries
- Enabling Stateful Firewall (Always On)
- Launching an Application
- Managing Windows NT Logon Properties
- Viewing and Managing the VPN Client Event Log
- Receiving Notifications From a VPN Device
- Upgrading the VPN Client Software
- Uninstalling the VPN Client

To configure properties of connection entries, see “Configuring the VPN Client.”

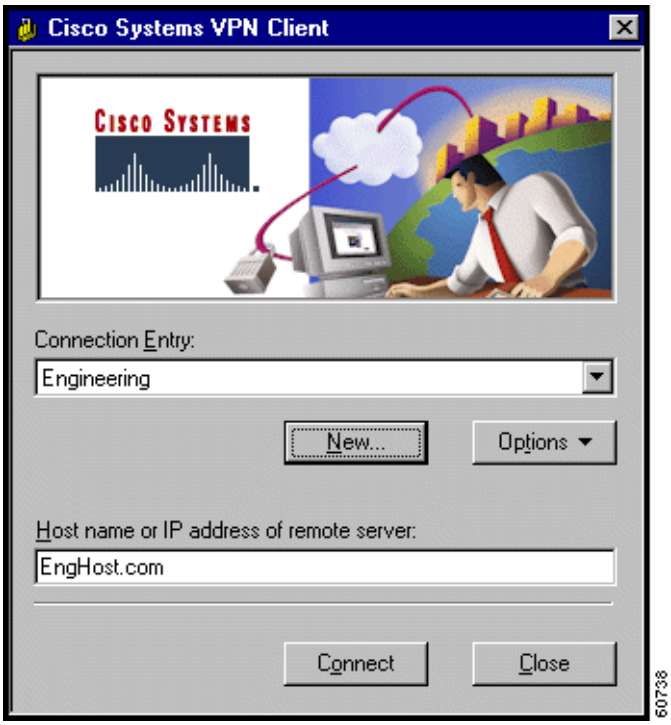
Note If you are a system administrator, refer to the *VPN Client Administrator Guide* for information on configuring the VPN 3000 Concentrator and preparing preconfigured profiles for VPN Client users.

Managing VPN Client Connection Entries

To manage a connection entry, start the Cisco VPN Client and choose **VPN Dialer** from the menu of applications.

The VPN Client main dialog box appears. (See Figure 5-2.)

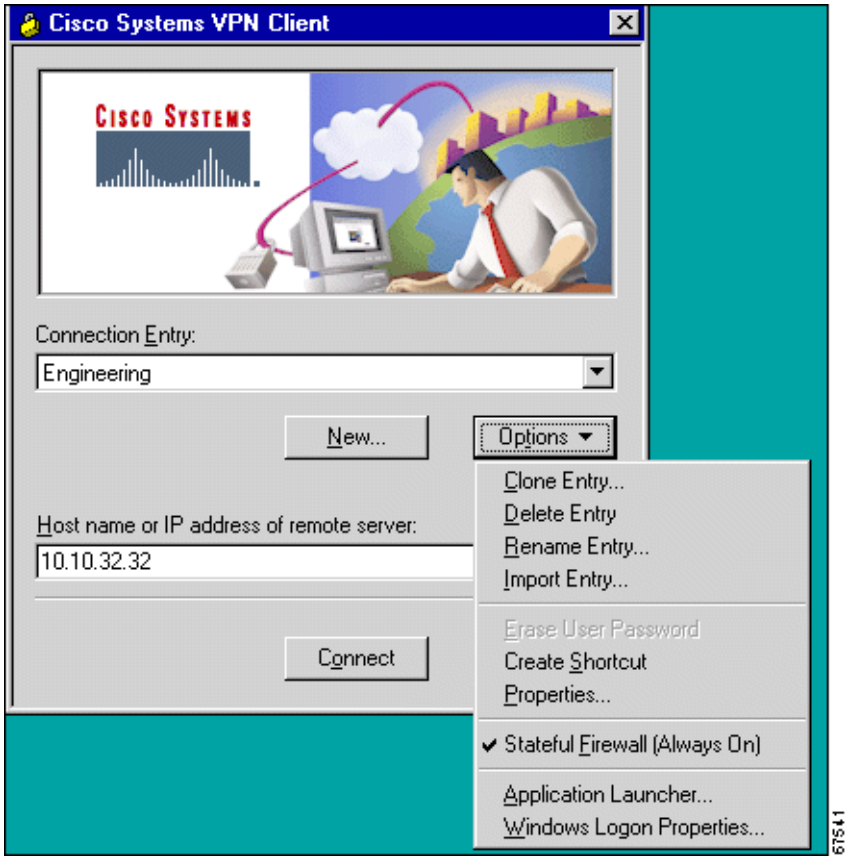
Figure 5-2 VPN Client Main Dialog Box (VPN Dialer)



Click the **Connection Entry** drop-down menu arrow and choose an entry.

Click **Options** to display the menu.

Figure 5-3 VPN Client Options Menu



Cloning a Connection Entry

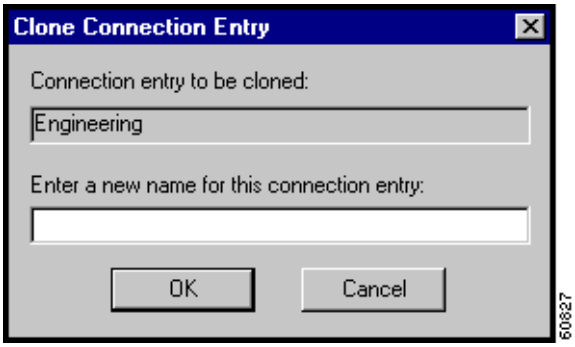
To clone a connection entry with all its properties and use it as the basis for creating a new entry, follow these steps:

Step 1 On the VPN Client's main dialog box, click the Connection Entry drop-down menu and choose the entry you want to clone.

Step 2 On the VPN Client Options menu, choose **Clone Entry**. (See Figure 5-3.)

The Clone Connection Entry dialog box appears. (See Figure 5-4.)

Figure 5-4 Clone Connection Entry Dialog Box



Step 3 Enter a name for the new connection entry in the field and click **OK**.

Step 4 The dialog box closes. The new name appears in the Connection Entry list in the VPN Client main dialog box.

Step 5 To configure the properties of this new connection entry, click **Options** > **Properties** on the VPN Client main dialog box and see the "Setting or Changing Connection Entry Properties".

Deleting a Connection Entry

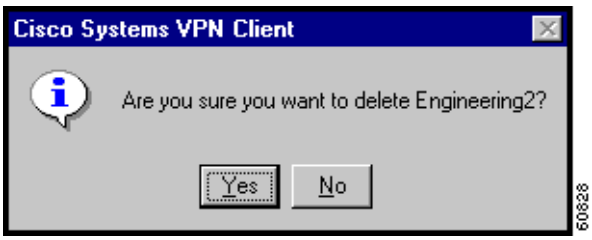
To delete a configured connection entry, follow these steps:

Step 1 On the VPN Client's main dialog box, click the Connection Entry drop-down menu arrow and choose the entry you want to delete.

Step 2 On the VPN Client Options menu, choose **Delete entry**. (See Figure 5-3.)

A confirmation dialog box appears. (See Figure 5-5.)

Figure 5-5 Confirming Deletion of a Connection Entry



Step 3 Click **Yes** or **No**:

- To permanently delete the connection entry, click **Yes.** *There is no undo.*
- To retain the connection entry, click **No**.

The VPN Client returns to its main dialog box.

Renaming a Connection Entry

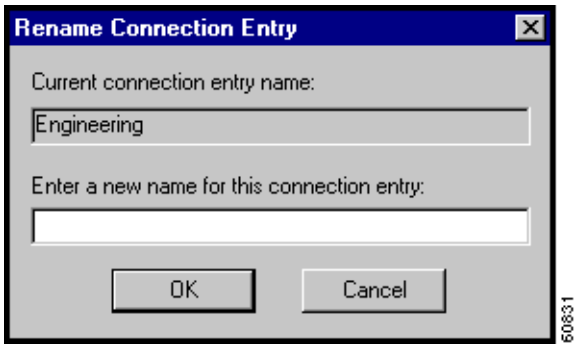
You can rename a connection entry and retain all its properties. Each connection entry name must be unique. Since these names are *not* case-sensitive, be sure the new name differs in content, not just case.

Step 1 On the VPN Client's main dialog box, click the Connection Entry drop-down menu and choose the entry you want to rename.

Step 2 On the VPN Client Options menu, choose **Rename Entry**. (See Figure 5-3.)

The Rename Connection Entry dialog box appears. (See Figure 5-6.)

Figure 5-6 Entering a New Name for a Connection Entry



Step 3 Enter a new name for this connection entry in the field and click **OK**.

The dialog box closes. The new name appears in the Connection Entry list in the VPN Client main dialog box.

Importing a VPN Client Configuration File

You can automatically configure your VPN Client with new settings by importing a new configuration file (a file with a `.pcf` extension, called a profile) that your system administrator supplies.

To automatically configure a VPN Client, perform the following steps:

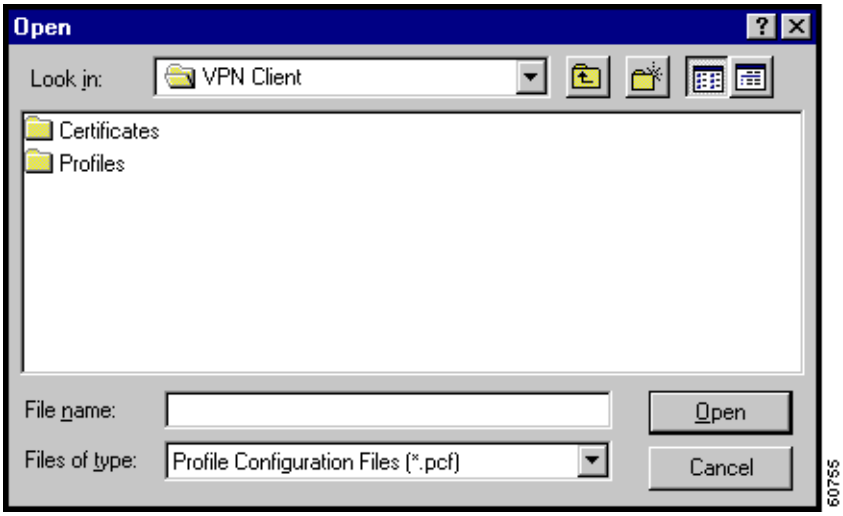
Step 1 Obtain a new VPN Client profile (`.pcf`) file from your system administrator.

Step 2 Load the file on your hard disk.

Step 3 On the VPN Client main dialog box, click **Options** and choose **Import Entry** from the menu.

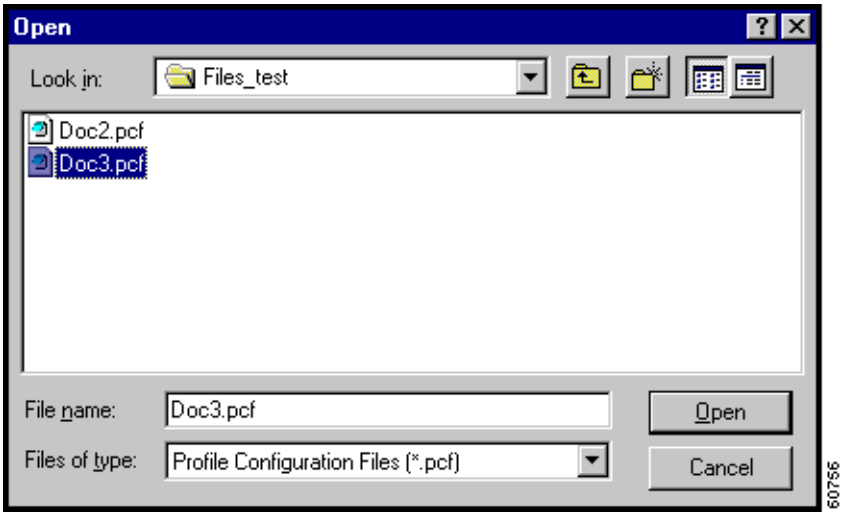
The VPN Client opens a window for you to choose the profile file. (See Figure 5-7.)

Figure 5-7 Choosing a File to Import



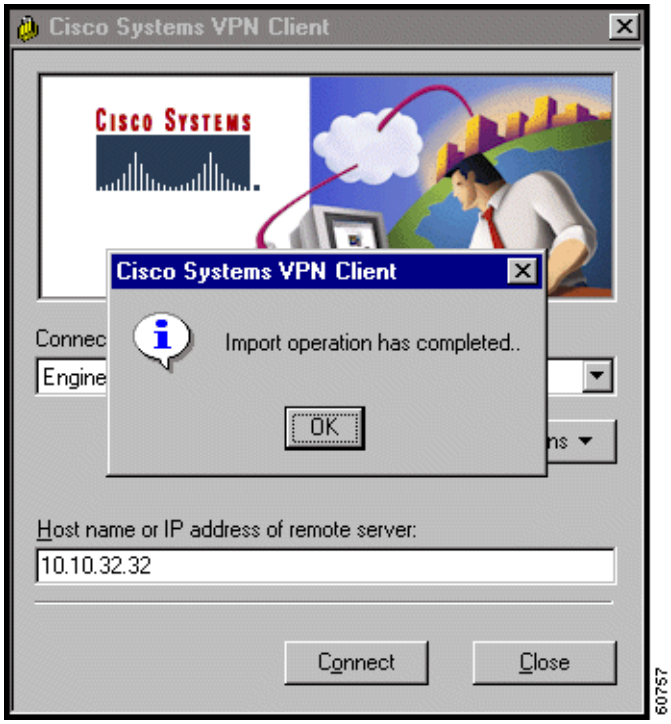
Step 4 Browse until you locate the profile file and when you have located it, choose it and click **Open.** (See Figure 5-8.)

Figure 5-8 Importing the Profile File



The VPN Client displays a message informing you that your file import was successful. (See Figure 5-9.) If the profile already exists, you receive a message asking if you want to overwrite it.

Figure 5-9 Import Successful



Step 5 To continue, click **OK**.

Alternatively, you can copy the .pcf file into the Profiles directory and restart the VPN Dialer application.

Your VPN Client is now configured with the connection entries and parameters specified by this new profile file. You can examine or modify the connection entries by clicking the Connection Entry drop-down menu on the main dialog box, choosing an entry, and clicking **Options** > **Properties**.

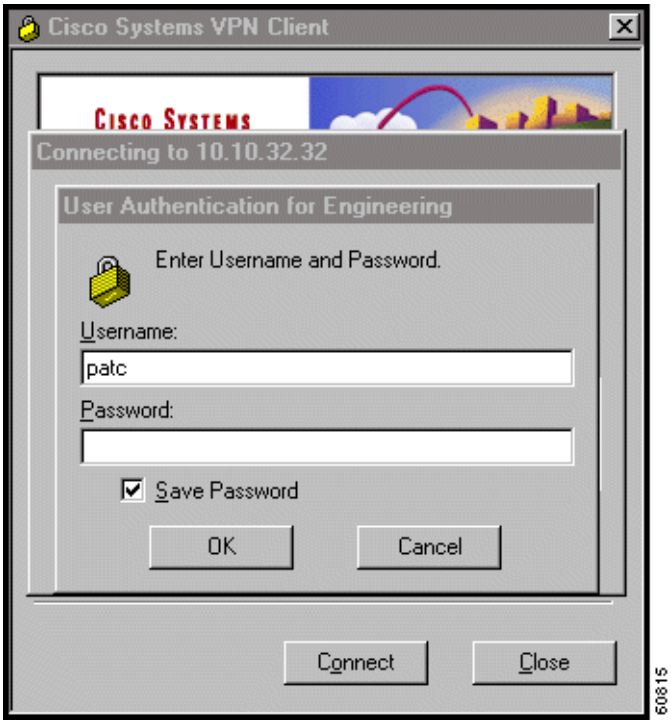
Erasing a Saved Password for a Connection Entry

You or your administrator may 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, use the Erase User Password feature on the Options menu. Erase User Password is available only when you have previously checked Save Password on the User Authentication dialog box. (See Figure 5-10.)

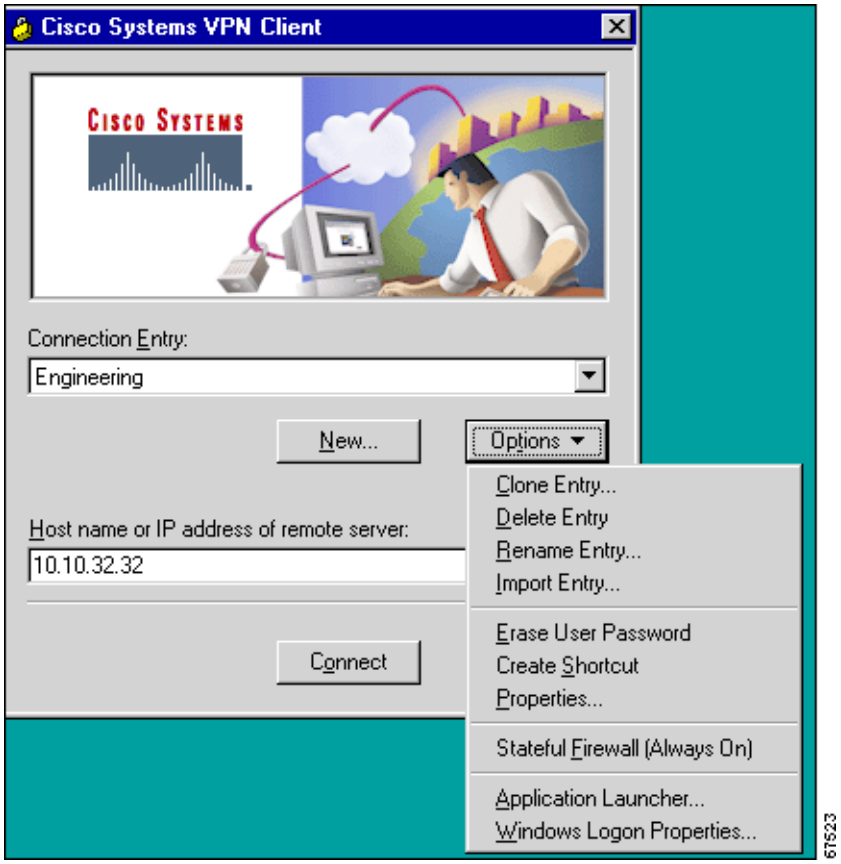
Figure 5-10 Saving Password During Authentication



When the VPN device allows saving passwords on the remote site and Save Password is in effect, then Erase User Password is available on the Options menu. (See Figure 5-11.)

Note If the IPSec group parameter **Reauthentication on Rekey** is enabled on a VPN 3000 Concentrator, you must enable **Erase User Password** on the VPN Client. Otherwise during every IKE Phase 1 rekey, the VPN Client user is automatically authenticated (no authentication dialog is displayed).

Figure 5-11 Erase User Password Available



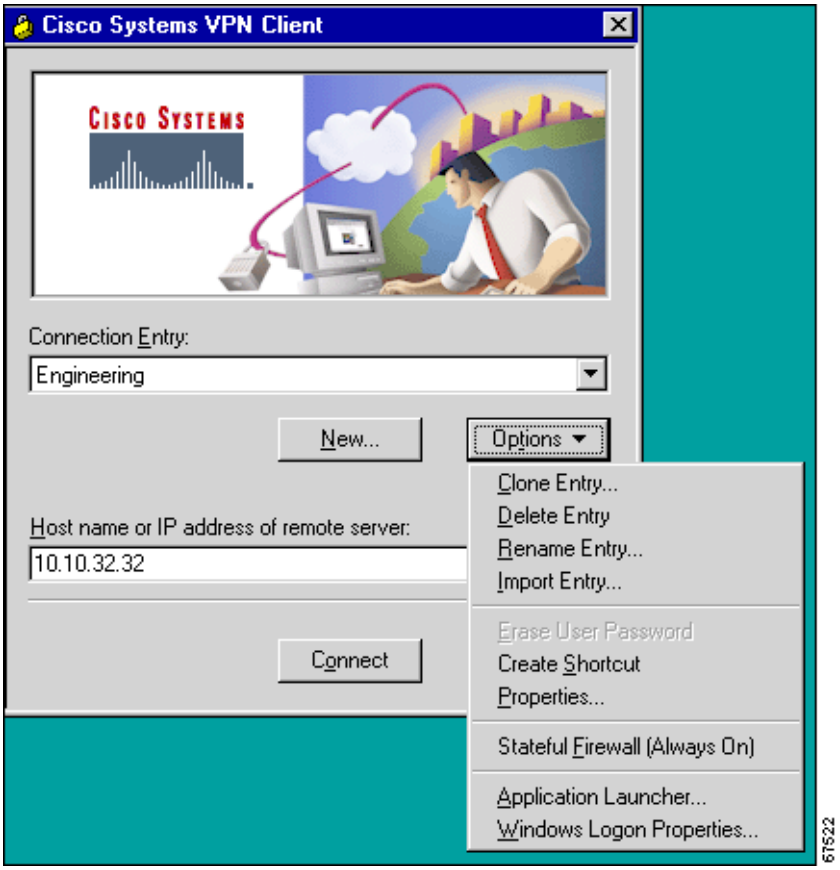
To enable this feature, click **Erase User Password**.

The VPN Client prompts you to confirm (See Figure 5-12.)

Figure 5-12 Verifying Erase User Password

With Erase User Password in effect, the next time you connect, the authentication dialog box prompts you to enter your password: on the Options menu, the Erase User Password feature is no longer available. (See Figure 5-13.)

Figure 5-13 Erase User Password Unavailable



Creating a Shortcut for a Connection Entry

You can create a shortcut on your desktop to quickly and directly launch a VPN Client connection entry that you use frequently.

Step 1 On the VPN Client's main dialog box, click the **Connection Entry** drop-down menu and choose an entry.

Step 2 On the VPN Client Options menu, choose **Create Shortcut**. (See Figure 5-3.)

The shortcut appears on your desktop, as in this example. (See Figure 5-14.)

Figure 5-14 Connection Entry Shortcut

The VPN Client main dialog box remains open.

Enabling Stateful Firewall (Always On)

The VPN Client includes an integrated stateful firewall that provides protection when split tunneling is in effect and protects the VPN Client PC from Internet attacks while the VPN Client is connected to a VPN Concentrator through an IPSec tunnel. This integrated firewall includes a feature called Stateful Firewall (Always On).

Stateful Firewall (Always On) provides even tighter security. When enabled, this feature allows *no* inbound sessions from all networks, whether or not a VPN connection is in effect. Also, the firewall is active for both encrypted and non encrypted traffic. There are two exceptions to this rule. The first is DHCP, which sends requests to the DHCP server out one port but receives responses from DHCP through a different port. For DHCP, the stateful firewall allows inbound traffic. The second is ESP. The stateful firewall allows ESP traffic from the secure gateway, because ESP rules are packet filters and not session-based filters. For the latest information on other exceptions, if any, refer to *Release Notes for Cisco VPN Client for Windows*.

To enable the stateful firewall, click **Stateful Firewall (Always on)**. When Stateful Firewall (Always On) is enabled, you see a check in front of the option. This feature is disabled by default. You can enable or disable this feature from the VPN Client Options menu. During a VPN connection, you can view the status of this feature by right-clicking the lock icon in the system tray. You can also enable or disable this feature from the same menu.

Launching an Application

You can configure the dialer to automatically launch an application before establishing a connection. Some examples of why you would want to use this feature follow:

- You are configured for Start Before Logon and you need to start an authentication application at the logon desktop.
- You want to launch a monitoring application such as the Log Viewer before each connection. (See Figure 5-15 to Figure 5-17.)

To configure the VPN Dialer to launch an application from the logon desktop, use the Application Launcher.

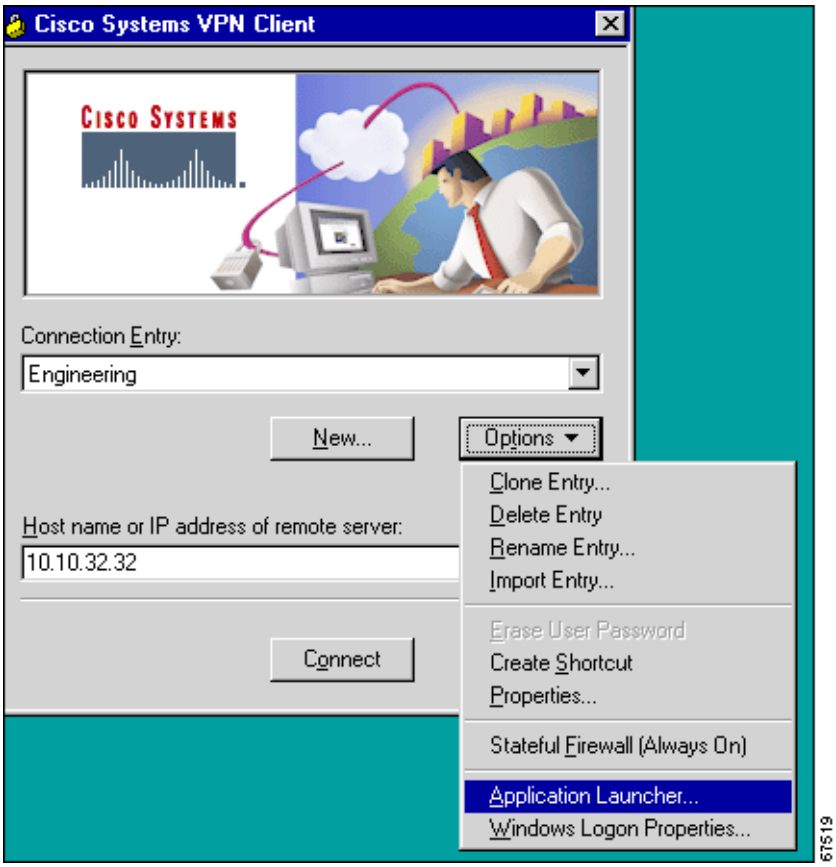
The Application Launcher starts the specified application once per session. To launch an application again, you must exit from the VPN Dialer, restart the VPN Dialer, and launch the application.

Note You cannot launch a batch file using Application Launcher.

To activate Application Launcher, follow these steps:

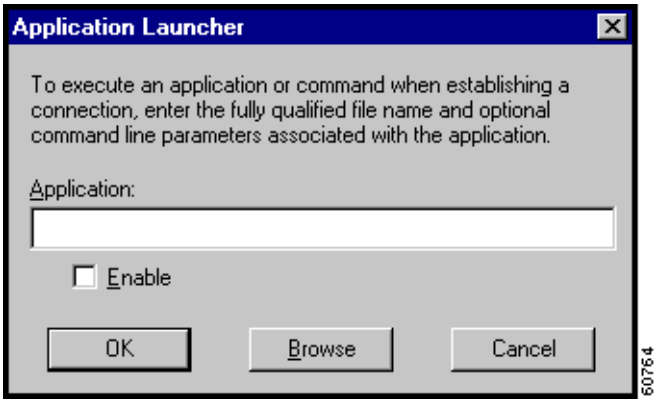
Step 1 Open the VPN Dialer Options pull-down menu (shown in Figure 5-3) and click **Application Launcher.** (See Figure 5-15.)

Figure 5-15 Application Launcher Option



The VPN Dialer displays a dialog box prompting for the name of the application. (See Figure 5-16.)

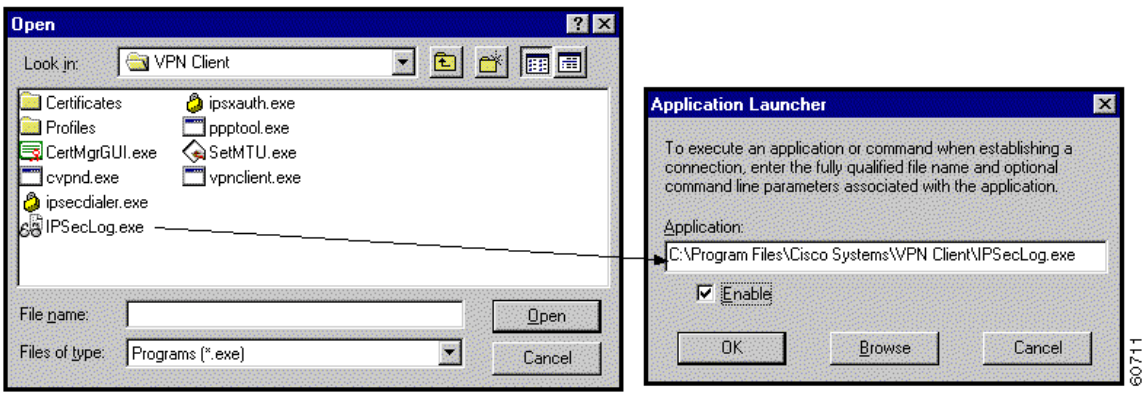
Figure 5-16 Entering the Name of the Application



Step 2 Click **Browse** to locate and then choose the complete pathname to the application as well as the name of the application. (See Figure 5-17.)

The application name appears in the Application Launcher dialog box. In this example, the VPN Dialer is configured to launch the Log Viewer before a connection.

Figure 5-17 Choosing an Application



Step 3 Click **Enable** and then click **OK**.

Turning Off Application Launcher

To disable Application Launcher, follow these steps:

Step 1 Open the Options pull-down menu and choose **Application Launcher**.

Step 2 When the Application Launcher dialog box displays, remove the check from in front of Enable.

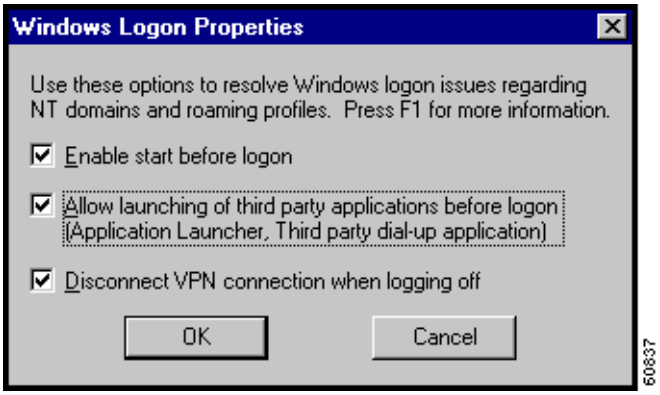
Managing Windows NT Logon Properties

This section describes special logon features for the Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP. These features include:

- Ability to start a connection before logging on to a Windows NT system
- Permission to launch a third party application before logging on to a Windows NT system
- Control over auto-disconnect when logging off of a Windows NT system

To access the Windows logon properties, open the VPN Client Options pull-down menu (shown in Figure 5-3) and choose **Windows Logon Properties**. The VPN Client displays a dialog box containing three parameters. (See Figure 5-18.)

Figure 5-18 Windows Logon Properties



Starting a Connection Before Logging on to a Windows NT Platform

On a Windows NT platform, you can connect to the private network before you log on to your system. This feature is called Start Before Logon and its purpose is primarily to let you log in to the domain and run login scripts.

Your administrator may have set this up for you. Once you establish a VPN connection, your credentials are sent to a domain controller for logging in to your system. If you need to launch an application before you logon, see the section “Launching an Application” for information.

When you have established a successful VPN connection, the VPN Dialer window closes and your logon window displays. If the connection is not successful, the VPN Dialer window continues to display. Your administrator may have set up a banner that lets you know when you have a successful connection.

To activate this feature, follow these two steps:

Step 1 Open the VPN Client Options pull-down menu (shown in Figure 5-3) and choose **Windows Logon Properties**.

Step 2 Check **Enable start before logon**. (See Figure 5-18.)

What Happens When You Use Start Before Logon

When Start Before Logon is active, the following events occur when your system starts:

- Your system logon dialog box displays. Other messages might display as well, depending on your setup. Wait until you see the VPN Dialer start.
- The VPN Dialer starts and displays the connection dialog box over the system logon dialog box.
- You establish your connection to the private network of the VPN Device.

You log on to your system.

Turning Off Start Before Logon

To turn this feature off, open the Options pull-down menu on the VPN Dialer connection dialog box and uncheck **Enable start before logon**. The next time you log on to your system, the VPN Dialer connection dialog box does not automatically display on your logon desktop.

Note You can use certificates for authentication with Start Before Logon when your personal certificate along with the CA or intermediary certificate(s) are in your Cisco certificate store but not your Microsoft store (CAPI certificates). However, to use a CAPI certificate, you can log in using cached credentials, make a VPN connection using your CAPI certificate, and disable the "Disconnect VPN connection when logging off" parameter (see "Disconnecting When Logging Off of a Windows NT Platform," following). This action keeps your connection open. Now you can log back in to the system.

For information on enrolling certificates and importing certificates into your Cisco store, see "Enrolling and Managing Certificates."

For information about using Start Before Logon with the Entrust SignOn feature, see "Connecting with Digital Certificates".

Permission to Launch an Application Before Log On

Your system administrator determines whether you can launch applications and third-party dialers before you log on to a Windows NT platform. To protect system and network security, your system administrator might have disabled this feature. If this feature is greyed out, you cannot launch applications and third-party dialers before logging on to a Windows NT platform. You must have system administrator privileges to change this parameter.

Disconnecting When Logging Off of a Windows NT Platform

This parameter controls whether your VPN Client connection automatically disconnects when you log off your Windows NT system.

To always automatically terminate your connection when you log off, check this parameter. This parameter is checked by default.

To disable auto-disconnect while logging off, remove the check from this parameter. When you remove the check, the VPN Client displays the warning message shown in Figure 5-19.

Figure 5-19 Auto-disconnect Warning Message

Disabling this parameter allows your connection to remain up during and after log off, which allows profiles or folders to be synchronized during log off. You would disable this parameter when using the Windows roaming profiles feature.

Note With this feature disabled, you must completely shut down your system to disconnect your VPN Client connection.

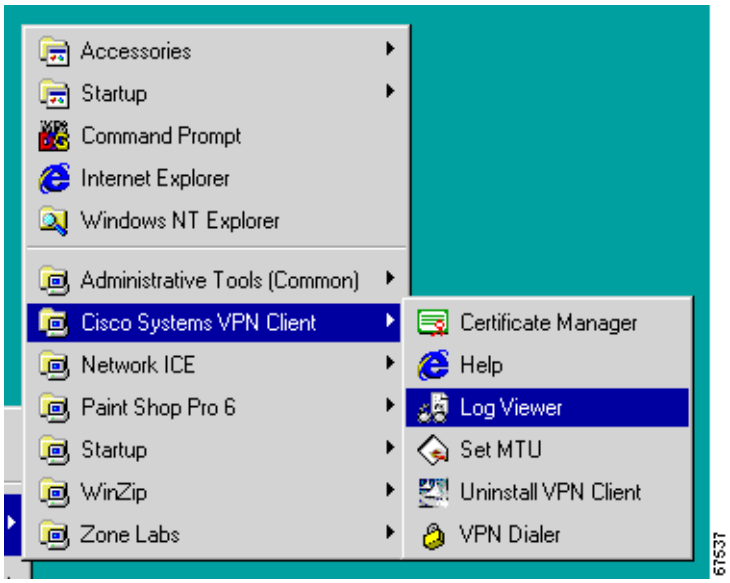
Viewing and Managing the VPN Client Event Log

Examining the event log can often help a network administrator diagnose problems with an IPSec connection between a VPN Client and a peer device. The log view application collects event messages from all processes that contribute to the client-peer connection. This section shows how to use the Log Viewer to retrieve and manage this information.

Starting the Log Viewer

To start the Log Viewer, use the following path from the Start menu:
Start > **Programs** > **Cisco Systems VPN Client** > **Log Viewer**. (See Figure 5-20.)

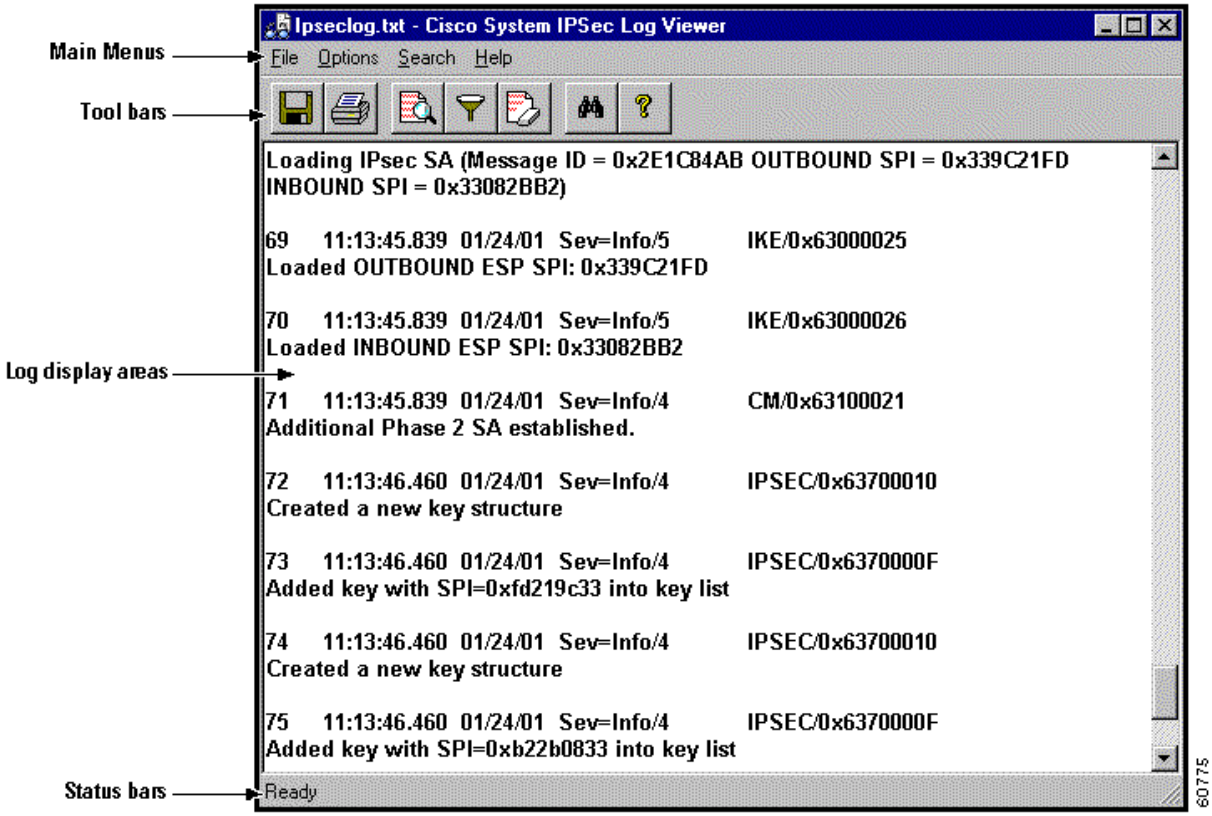
Figure 5-20 Starting the Log Viewer



The Log Viewer starts, displaying its main window. (See Figure 5-21.) By default, the filter is set to low, so you may not see any events displayed in this window (see the section “Filtering Events”).

For help on this window, press **F1**.

Figure 5-21 Log Viewer Main Window



Displaying the Version of the Software

To display a brief help message that gives you the version number of the software, choose **Help** from the main menu or click the **Help** icon.

Collecting Events

To start collecting event messages into the log file, choose **Options** > **Capture**. When a check mark appears in front of the Capture option, Log Viewer is collecting events. This option is off by default. Alternatively, you can click the Capture icon.

Each message in the log file comprises at least two lines containing the following fields:

```
Event# Time Date Severity/type/level EventClass/MessageID
Message text
```

Table 5-1 describes the fields in an event message. Table 5-2 describes Event types and severity levels.

Table 5-1 Fields in an Event Message

Field	Meaning
Event#	The first field shows the event number. Events are numbered incrementally and never reset.
Time	The Time field shows the time of the event: *hour:minutes:seconds*. The hour is based on a 24-hour clock. For example `15:25:09` identifies an event that occurred at 3:25:09 PM.
Date	The date field shows the date of the event: *MM/DD/YYYY*. For example, `2/03/2001` identifies an event that occurred on February 3, 2001.
Severity/type/level	This field reports the severity type and level of the event; for example, `Sev=Info/4`, which identifies an informational event, severity level 4. identifies event types and severity levels
Event Class and Message ID	This field shows the module or source of the event and the message identifier associated with the module. For example, `IPSEC/0x63700012`.
Message Text	A brief message describing the event. Usually this message is no more than 80 characters. For example, `Delete all keys associated with peer 10.10.99.40`. In a message containing arrows, the arrows indicate the direction of the transmission: >>> for sending and <<< for receiving.

Table 5-2 Event Types and Severity Levels

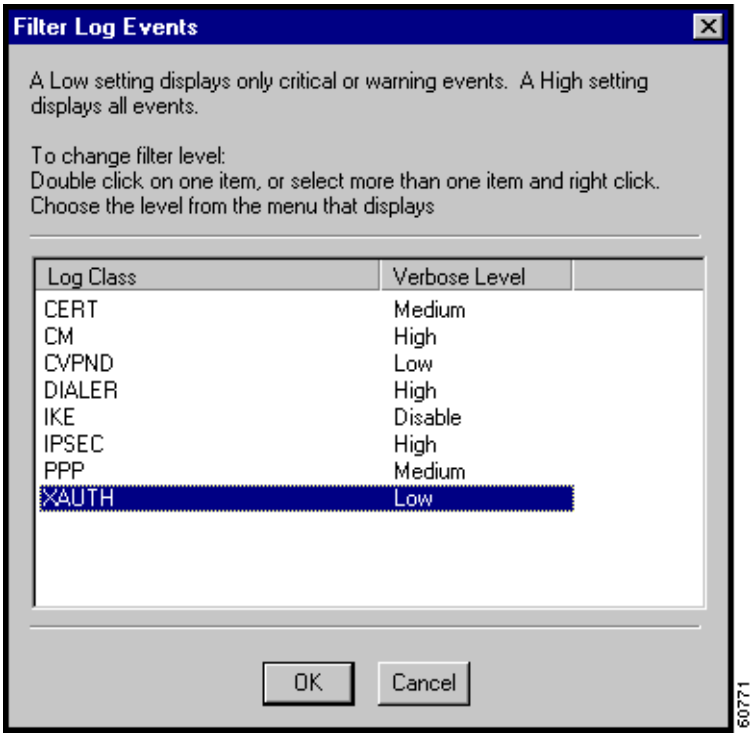
Type	Level	Meaning
Fault	1	A system failure or nonrecoverable error.
Warning	2 - 3	Imminent system failure or a serious problem that may require user intervention.
Informational	4 - 6	Level 4 provides the most general type (high level) information. Levels 5 and 6 provide more detailed information about the connection.

Filtering Events

To control the amount of information to view with the Log Viewer, choose **Options** > **Filter**. Alternatively, you can click the Filter icon.

The Log Viewer displays the Log Viewer Filter message to let you choose the amount of information you want to capture. (See Figure 5-22.)

Figure 5-22 Log Viewer Filter Message



To change the filter level, do the following:

Step 1 Double-click on one item, or choose more than one item and right click.

Step 2 Choose from the following options that the Log Viewer displays:

Disable—Inhibits event reporting for the chosen class.

Low—Provides the least amount of information. This choice includes severity levels 1 through 3 (all faults and warnings). Low is the default for all classes.

Medium—Includes severity levels 1 through 4; all in Low plus the first level informational events, which provide general information about the connection. Note that a first level informational event is level 4 and appears in the event display as Info/4.

High—Includes severity levels 1 through 6, thus adding two levels of informational events (Info/5 and Info/6). This setting can lower the performance of all applications on your system, so use it only when your network administrator or a support engineer suggests that you do so.

Table 5-3 defines the classes (modules) that generate events.

Table 5-3 Classes That Generate Events in the VPN Client

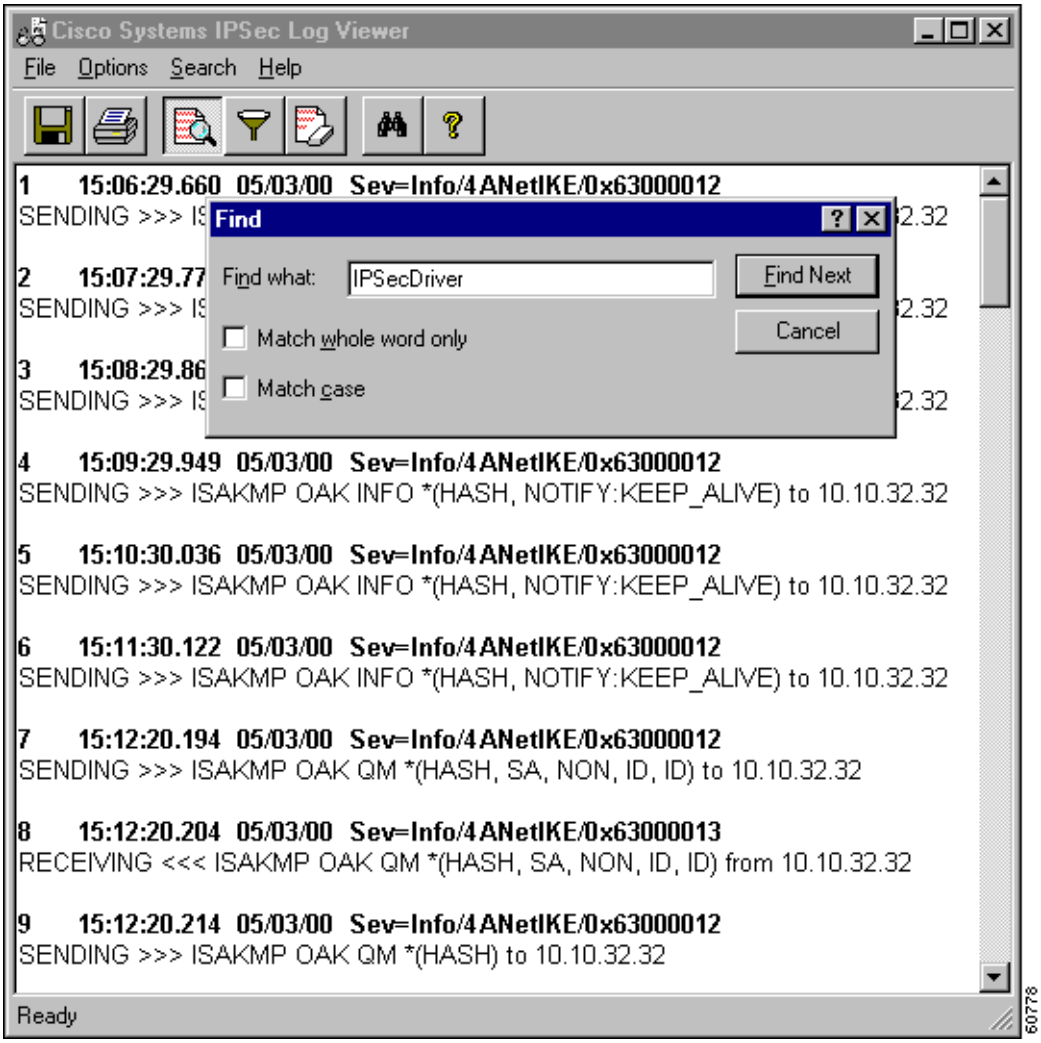
Class Name	Definition
CERT	Certificate management process (CERT), which handles getting, validating, and renewing certificates from certificate authorities. CERT also displays errors that occur as you use the application.
CM	Connection manager (CM), which drives VPN connections. (CM dials a PPP device, configures IKE for establishing secure connections, and manages connection states.
CVPND	Cisco VPN Daemon (main daemon), which initializes client service and controls messaging process and flow.
DIALER	Windows-only component, which handles configuring a profile, initiating a connection, and monitoring it.
IKE	Internet Key Exchange (IKE) module, which manages secure associations.
IPSEC	IPSec module, which obtains network traffic and applies IPSec rules to it.
PPP	Point to Point Protocol.
XAUTH	Extended authorization application, which validates a remote user's credentials.

Searching the Log File

To locate specific events or event types in the window, choose **Search** from the main menu. Alternatively, you can click on the Search icon.

The Log Viewer displays the **Find** message. (See Figure 5-23.) Enter a string to find and click **Find Next**. You can match on whole words and on case.

Figure 5-23 Searching the Log Display



Printing the Log File

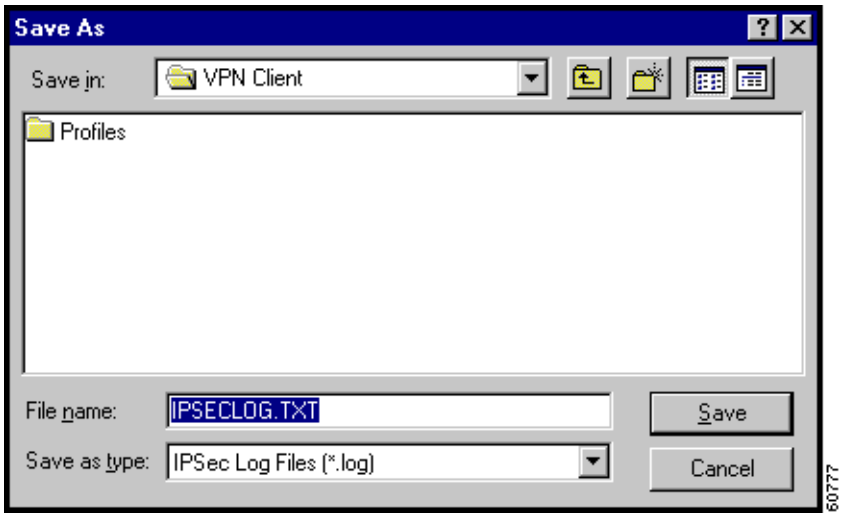
To print the events displayed in the current window, choose **File > Print** from the main menu. Alternatively, you can click the Printer icon. (See Figure 5-23.)

Saving the Log File

To save the currently displayed events in the `ipseclog` file on your hard drive, choose **File > Save as** from the main menu. Alternatively, click the Disk icon. (See Figure 5-23.)

The ipseclog file is a text (.txt) file in DOS format. The Log Viewer saves the information to the Client install directory, which by default is the pathname Program Files\Cisco Systems VPN Client\VPN Client\IPSECLOG.TXT. You can specify any directory and name. (See Figure 5-24.)

Figure 5-24 Saving a Log File



Clearing the Events Display

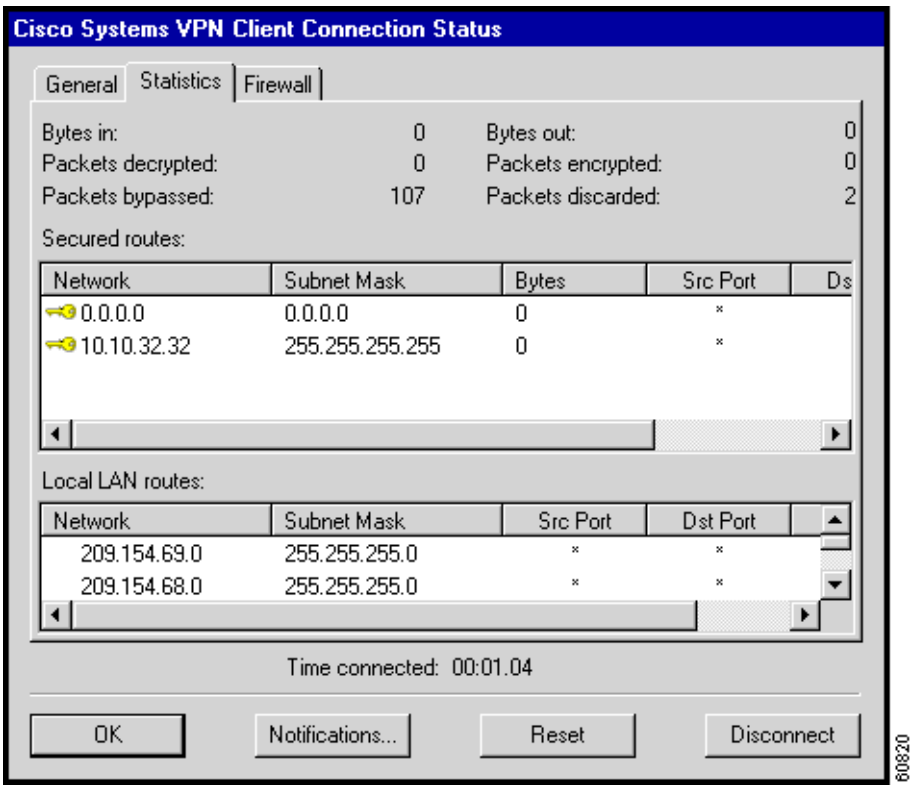
To eliminate all the events currently displayed in the Log Viewer main window, choose **Options > ClearLog Display** from the main menu. Alternatively, you can click the Erase All icon. (See Figure 5-23.)

If you want to store the event messages, be sure you save them before you clear the display. Clearing the display does not reset event numbering, nor does it clear the log file itself.

Receiving Notifications From a VPN Device

The VPN device (secure gateway) through which you connect to the private network at your organization can send you notifications. Typically, you might receive a notification from your network administrator when it is time to update the VPN Client software or when the VPN device that requires a specific firewall be running on the VPN Client PC detects that the firewall is not running. A notification typically shows up when you start your dialer connection. You can also display notifications while you are connected by clicking **Notifications** on the Connection Status dialog box. (See Figure 5-25.)

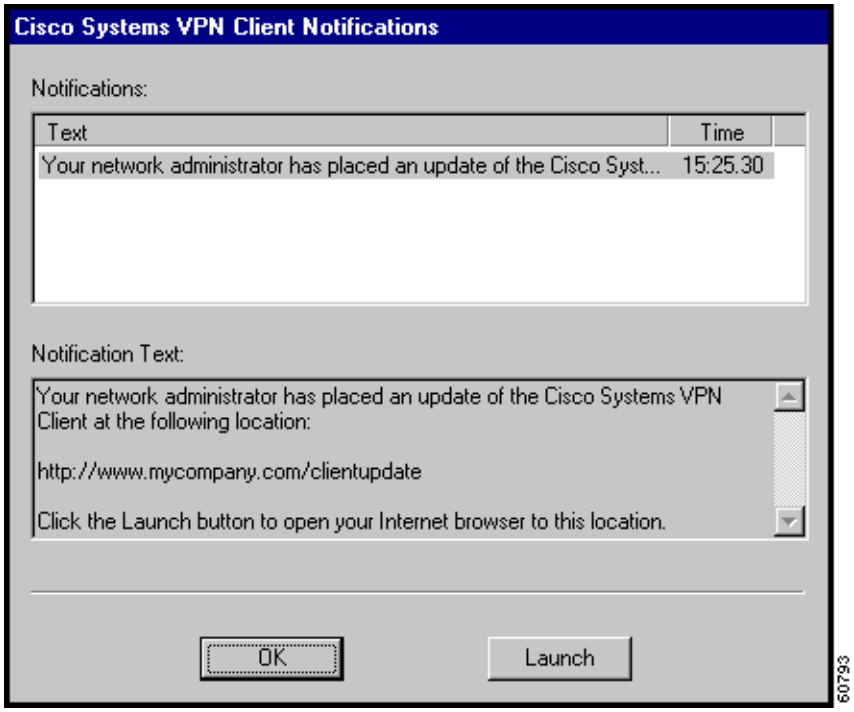
Figure 5-25 Displaying Notifications



Upgrade Notifications

The notification shown in Figure 5-26 informs a remote user that it is time to upgrade the VPN Client software. The notification includes the location where the remote user can obtain the upgrade. When you receive an upgrade notification that includes a URL, click **Launch** to go to the site and retrieve the upgrade software. You will receive an upgrade notification every time you connect until you have installed the upgrade software.

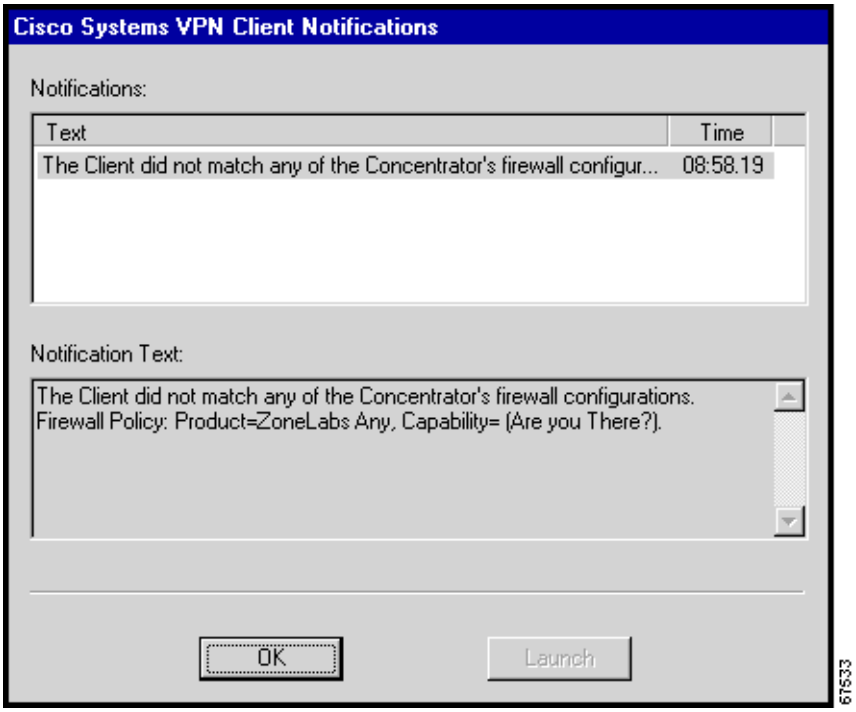
Figure 5-26 Notification of a Software Upgrade



Firewall Notifications

If the VPN Client and VPN Concentrator firewall configurations do not match, the VPN Concentrator notifies the VPN Client while negotiating the connection. The notification includes the policy that the VPN Concentrator requires. For example, the notification in Figure 5-27 shows an example firewall notification. The message states that the policy required is AYT and the firewall required is any Zone Labs product.

Figure 5-27 Firewall Notification



Upgrading the VPN Client Software

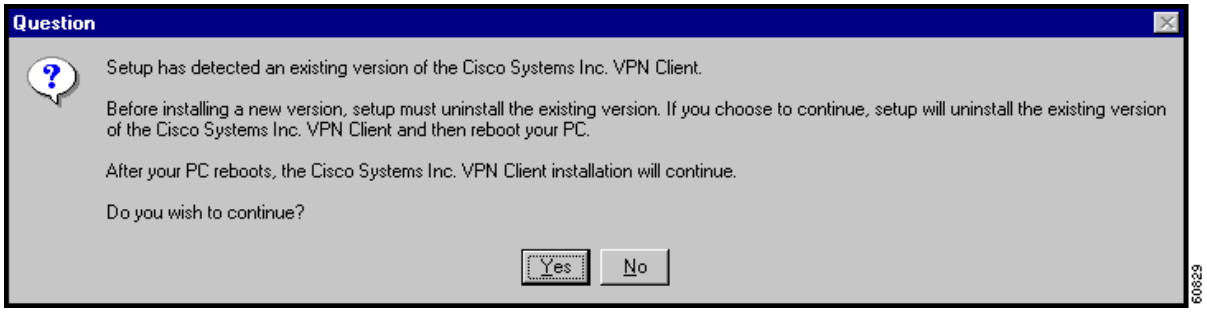
Upgrading the VPN Client software using this method retains existing connection entries and their parameters.

To install an upgrade of the VPN Client over an existing version on your system, use the following procedure, which first uninstalls the existing version, and then reboots your PC and installs the new version.

Step 1 To begin the procedure, follow the instructions in the “Installing the VPN Client” section in Chapter 2.

When it starts, the installation wizard detects the existing version and asks you to confirm that you want to remove that version and reboot your PC. (See Figure 5-28.)

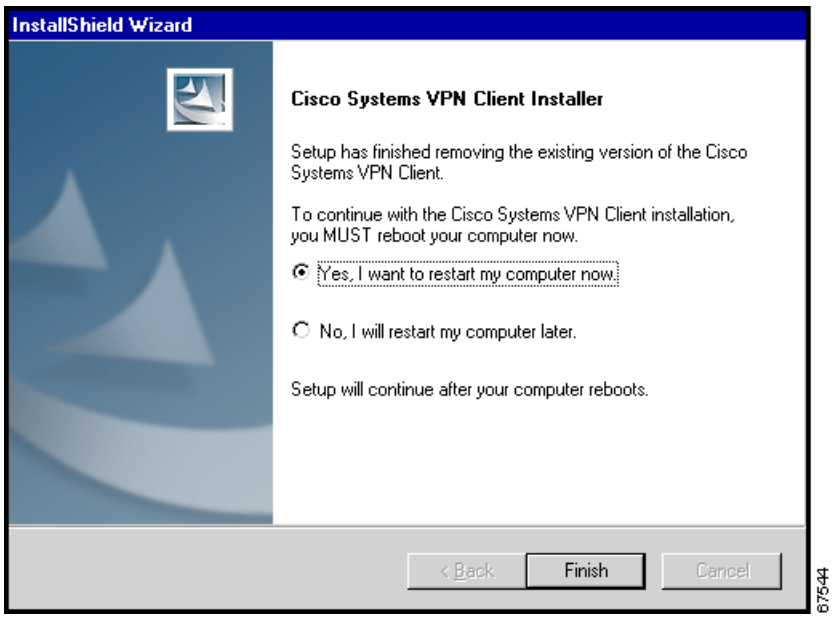
Figure 5-28 Uninstalling an Existing Version



Step 2 To continue, click **Yes**.

The installation program removes the old version and asks you to confirm the system restart. (See Figure 5-29.)

Figure 5-29 Confirming the System Restart



Be sure to remove any diskette from its drive before you restart your system.

If you are installing from diskettes, reinsert Disk 1 after your system restarts and displays the Windows logo screen, but *before* the desktop appears.

Step 3 To restart your system, click **Yes** (the default) and click **Finish**.

The installation wizard restarts your system. Once your system has restarted, installation continues automatically.

Step 4 Follow the instructions as if you were installing for the first time. See "Installing the VPN Client."

Uninstalling the VPN Client

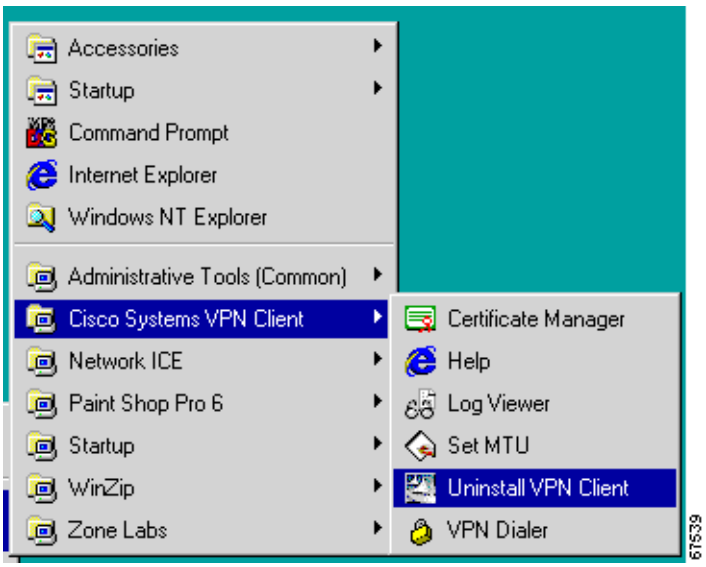
Uninstalling the VPN Client means completely removing all VPN Client software from your computer. For example, if you are changing or upgrading your PC, you might want to uninstall the VPN Client.

Note Do not attempt to uninstall or upgrade the VPN Client software from a mapped network drive.

Before you run the uninstall program, make sure you have closed all of your remote access (Dial-Up Networking) connections and all VPN Client applications. Then use the following procedure. (See Figure 5-30.)

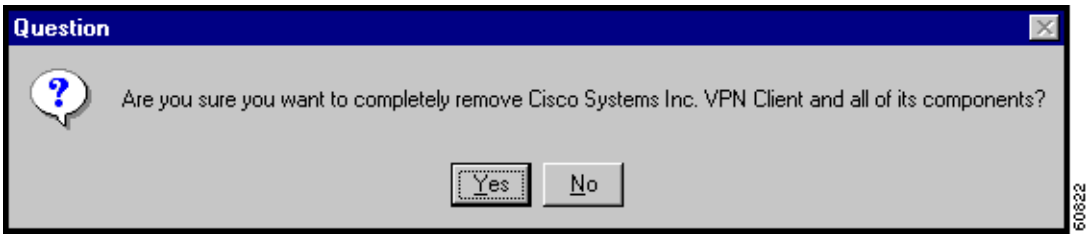
Step 1 Choose **Start** > **Programs** > **Cisco Systems VPN Client** > **Uninstall VPN Client**.

Figure 5-30 Running the Uninstall Program



The Uninstall Wizard runs and asks if you want to really want to remove the VPN Client applications. (See Figure 5-31.)

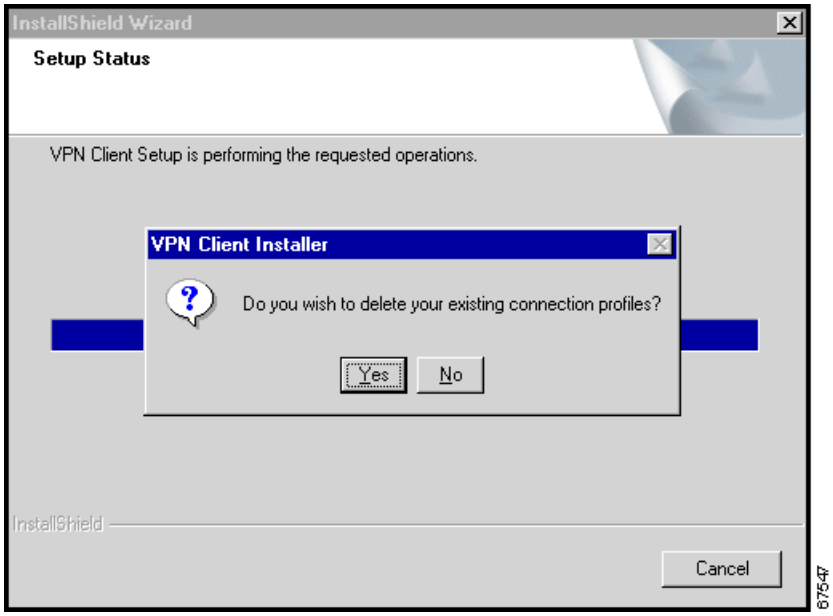
Figure 5-31 Confirming Uninstall



Step 2 To completely remove the VPN Client software from your system, click **Yes**. Otherwise, click **No**.

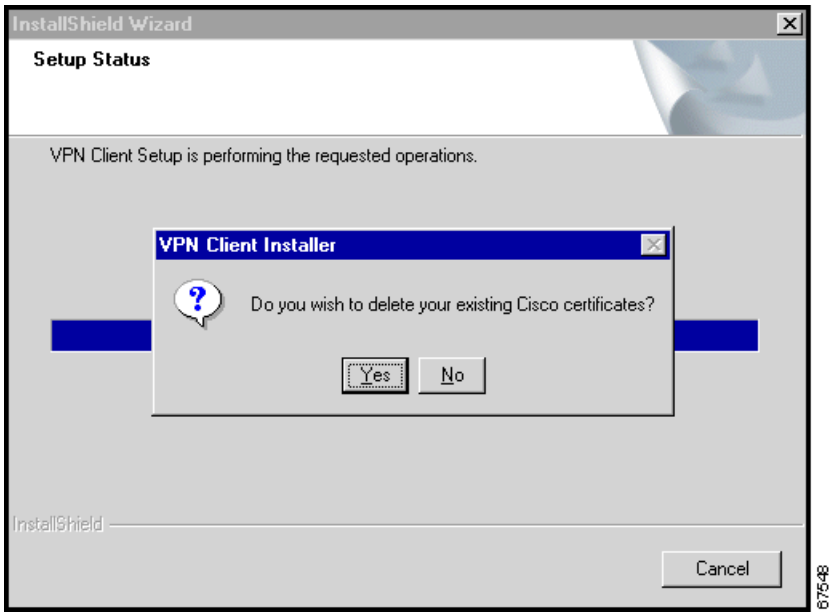
Next, the Uninstall Wizard asks if you want to delete your connection profiles. (See Figure 5-32.)

Figure 5-32 Confirming Your Connections



Step 3 To preserve your connection profiles (which contain configured connection entries), click **No**. Then the Uninstall Wizard asks if you want to delete your certificates. (See Figure 5-33.)

Figure 5-33 Confirming Your Certificates



Step 4 To keep your certificates, click **No**.

Finally, the Uninstall Wizard prompts you to restart your system. To complete the uninstallation, you must restart your system.

Step 5 To restart your system, click **Yes** (the default) and then click **Finish**.

The installation program restarts your system.

Be sure to remove any diskette from its drive before you restart your system.

Note When you uninstall the VPN Client software after you have run the Log Viewer and you have clicked yes to remove your certificate and profile directories, the vpnclient.ini and ipseclog.txt files remain on your system. Since these files were generated after you installed the software, they are not removed when you uninstall the software. You have to remove them manually.

Enrolling and Managing Certificates

This chapter explains how to enroll and manage personal certificates using the Certificate Manager application. Specifically, it describes 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.

  You can enroll for a certificate in two ways:

  – through the network (*online enrollment)*

  – through a file
- Import certificates
- Manage certificates

  – Viewing

  – Verifying

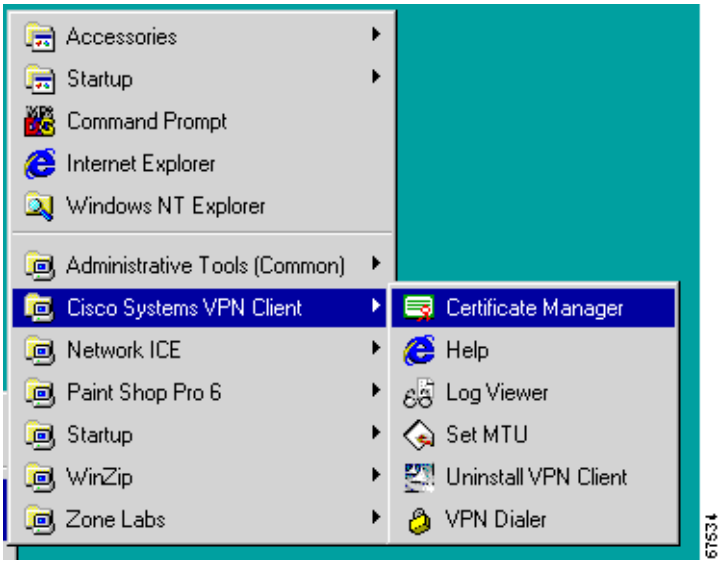
  – Deleting

  – Exporting
- Manage enrollment requests

To get started with certificates, go to the Cisco Systems VPN Client menu (the same menu that you use to start the client, shown in Figure 6-1).

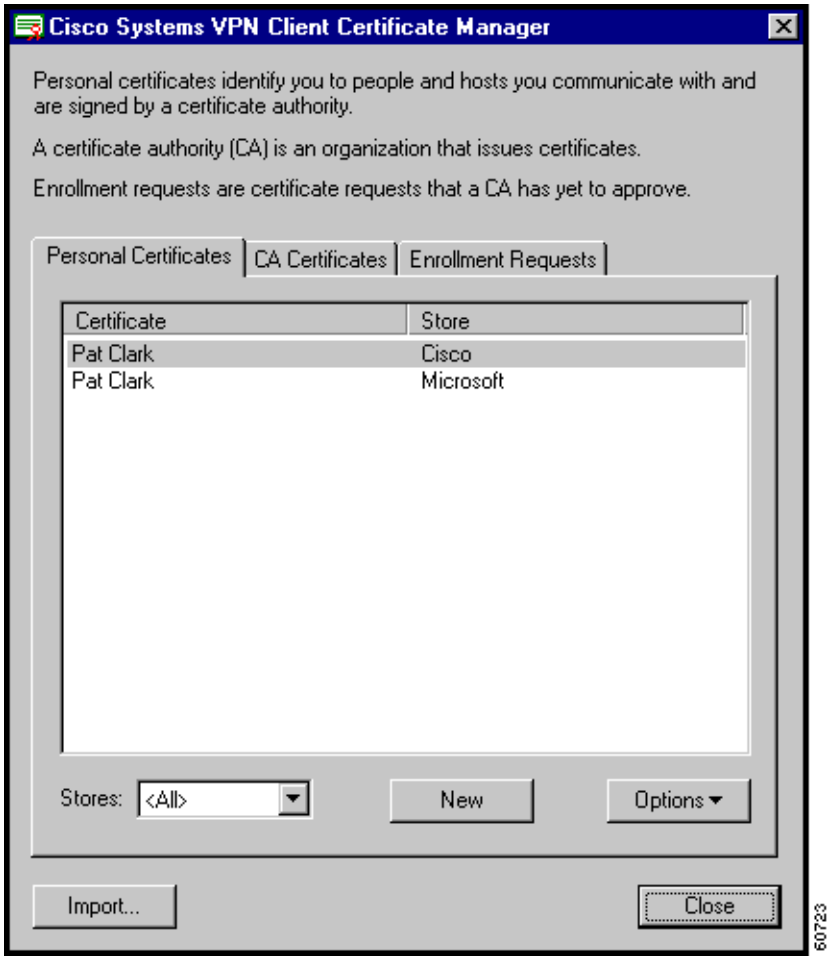
Choose **Start> Programs> Cisco Systems VPN Client> Certificate Manager.**

Figure 6-1 Choosing Certificate Manager



The Certificate Manager window opens. (See Figure 6-2.)

Figure 6-2 Certificate Manager Main Window



What are Certificate stores?

The Certificate Manager uses the notion of *store* to convey a location in your local file system for storing personal certificates. The major store for the VPN Client is the Cisco store. The Cisco store contains certificates you have enrolled for through the Simple Certificate Enrollment Protocol (SCEP). This application supports several standard enrollment protocols. 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.

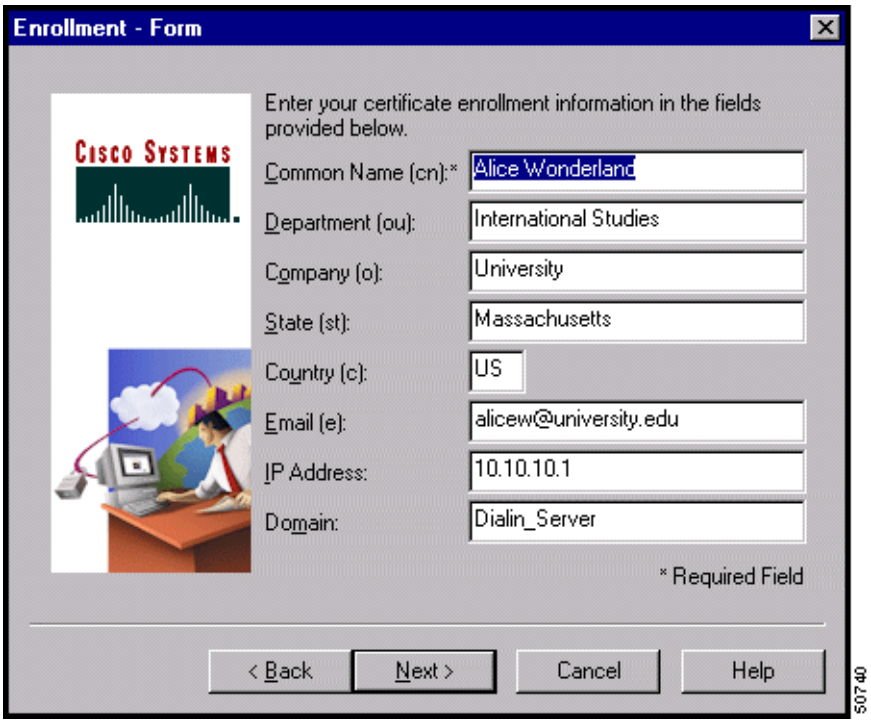
Enrolling for a Certificate

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. In both cases, you complete the same form (shown in Figure 6-3.)

Enrollment Form

This section describes the information required for filling out the certificate enrollment form. Make sure you have all of the following information before you start.

Figure 6-3 Enrollment Form



- Common Name—Your common name (CN), which is the unique name to use 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).

When you enroll a personal certificate, you either 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 6-2.)

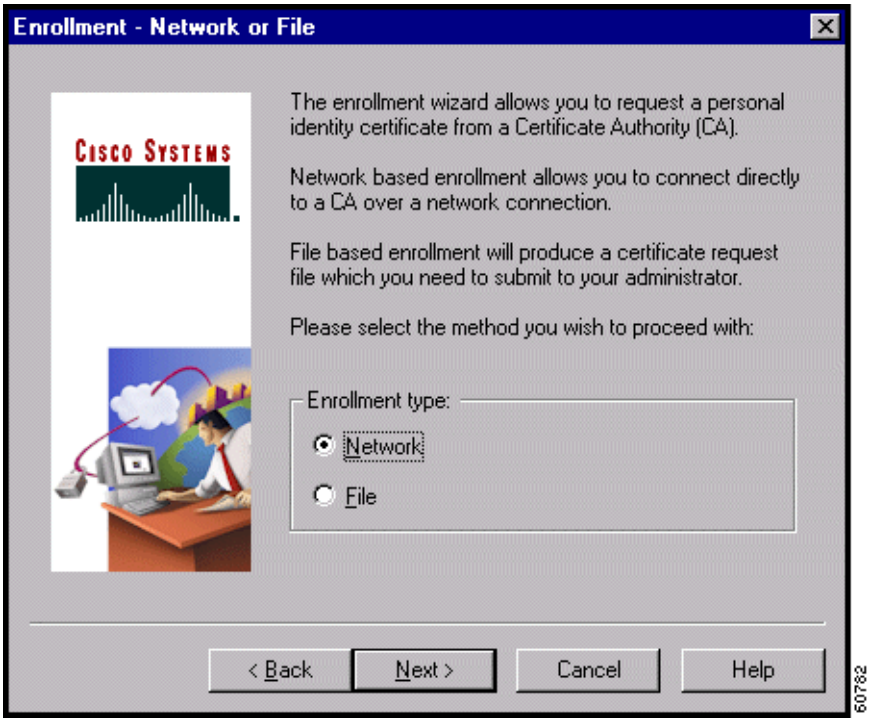
Starting Enrollment

To begin, click **New** on the Certificate Manager's main screen under the Personal Certificates tab. (See Figure 6-2.) The Certificate Manager prompts you to enter a password for the certificate you are enrolling. (See Figure 6-4.) The password is optional, but we recommend that you use one to protect your private key more effectively. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords. This password is called the *personal certificate password*.

Figure 6-4 Protecting a Certificate with a Password

After entering a password, click **Next** to continue. The Certificate Manager lets you choose between enrolling via the network or by creating a file. (See Figure 6-5.) Enrolling via the network is also called *online enrollment*.

Figure 6-5 Choosing Enrollment Method



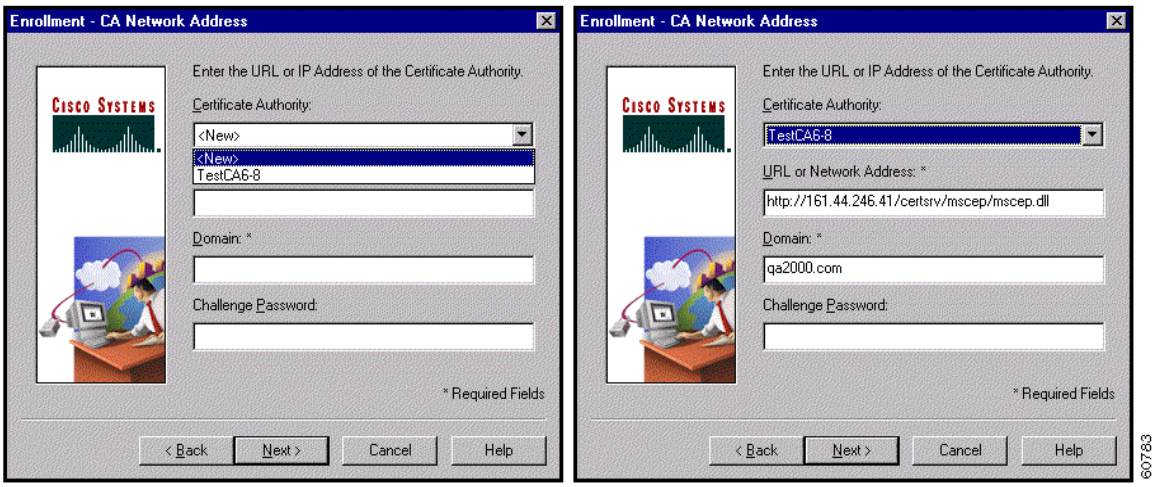
Enrolling Through the Network

To enroll through the network, retrieve a certificate from a CA, and place it in the Cisco store, using the following procedure:

Step 1 Click **Network** and click **Next**. (See Figure 6-5.)

The Certificate Manager asks you to enter the network address of the issuing certificate authority. (See Figure 6-6.)

Figure 6-6 Entering Network Address



Step 2 Choose one of the following procedures:

- Choose an existing Certificate Authority from the drop-down menu.
  - The URL or Network Address and Domain fields are automatically filled.
  - Renter the Challenge password or enter a new password, which you can obtain from the CA or your network administrator.
- Choose **<New>** from the drop-down menu.
  - Enter the URL or Network Address of the CA and the CA's Domain, both of which are required.
  - Some CAs require that you enter a password to access their site. If this is the case, enter the password in the Challenge Password field. You can get the password from the CA or from your network administrator.

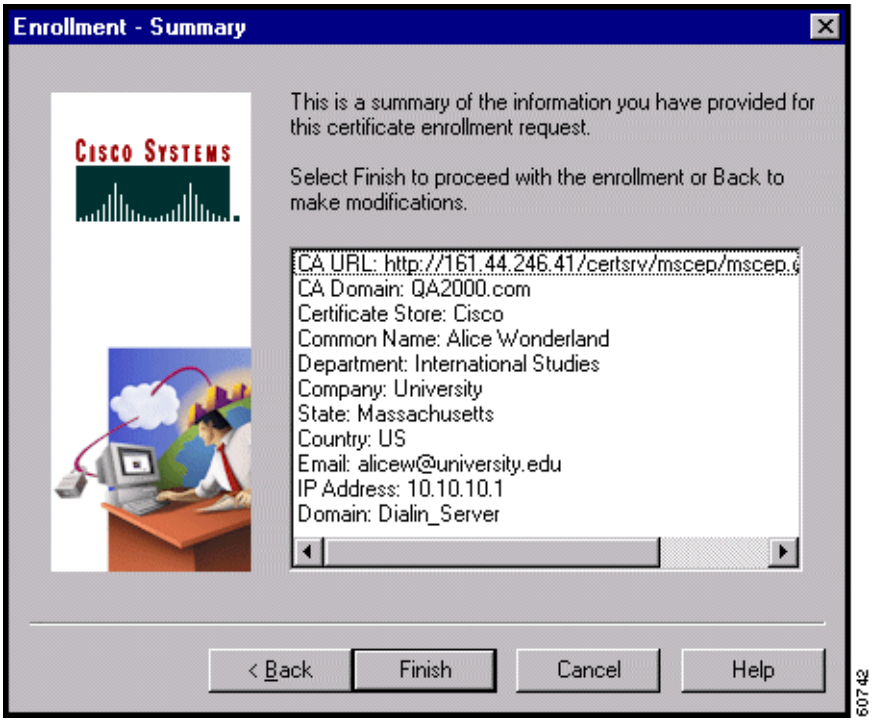
Step 3 When you have completed the network address information, click **Next>**.

The Certificate Manager displays the enrollment form for you to complete. (See Figure 6-3.)

Step 4 Enter the information you collected before you started the enrollment process. The only field that the Certificate Manager requires is Common Name. However the CA may require some or all of the other fields. Then click **Next>.**

After you enter the form, the Certificate Manager displays a summary that looks something like the one in Figure 6-7.

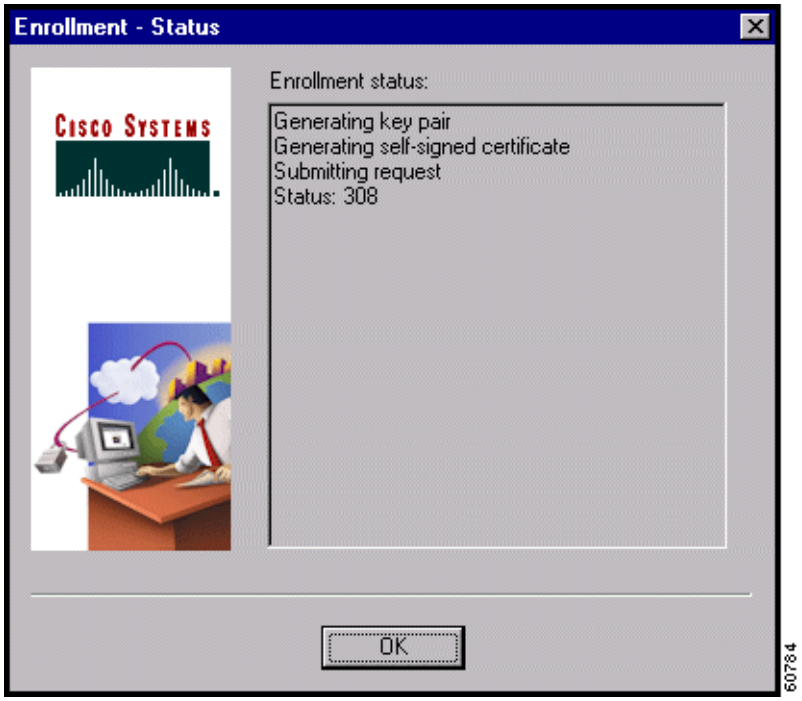
Figure 6-7 Enrollment Summary



Step 5 To complete the enrollment, click **Finish**.

The Certificate Manager displays a status window (shown in Figure 6-8) that lets you monitor the progress of the certificate retrieval. If the enrollment failed, the status window indicates the cause so you can fix the problem and try again.

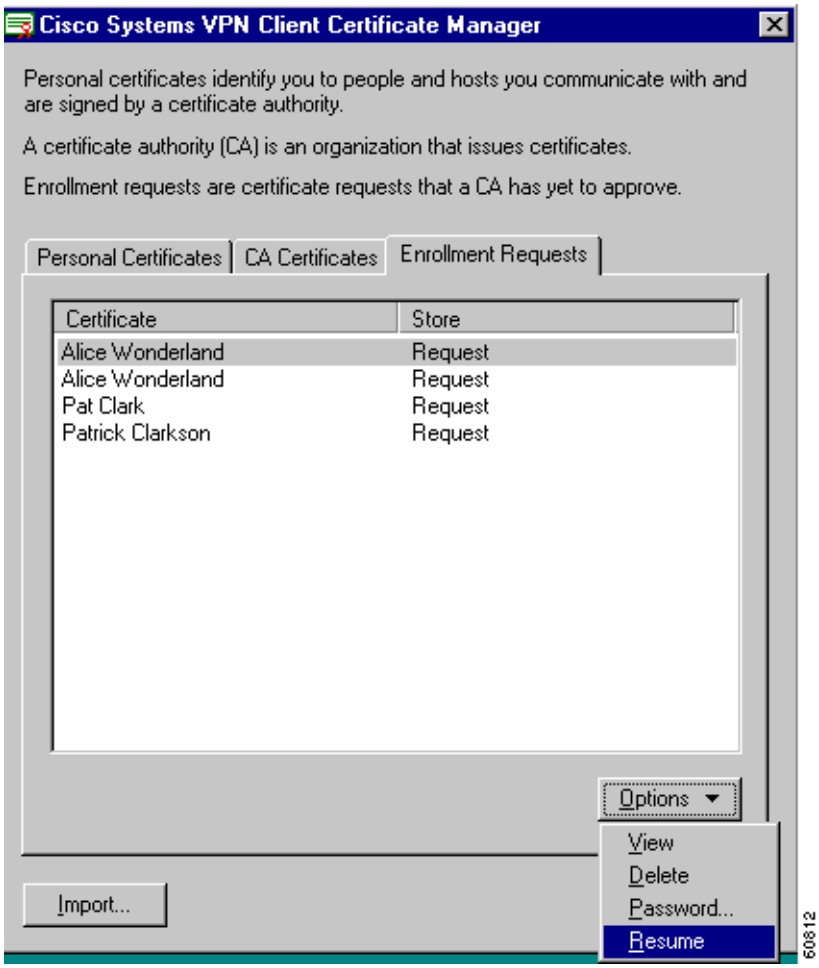
Figure 6-8 Certificate Status Messages



Step 6 What happens next depends on your CA. (See Figure 6-8):

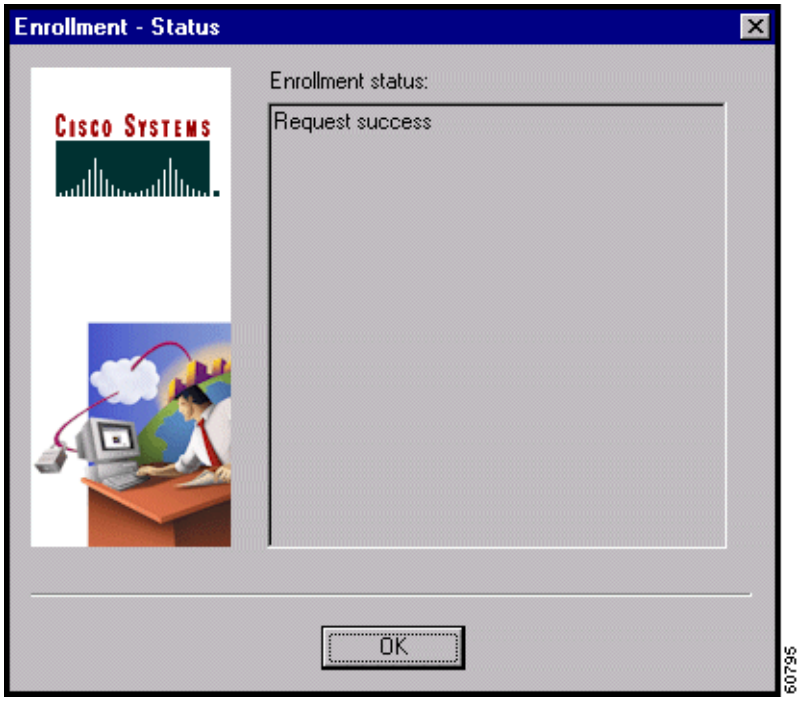
- Some CAs may provide immediate response. If so, the Enrollment - Status window reflects this fact and displays an OK button.
  - Click **OK** and you see a message that your enrollment succeeded. You can view and manage the certificate under the Personal Certificates tab.
- If the enrollment status is Request pending, your CA does not immediately approve your request and the Enrollment - Status window shows the Suspend button.
  - Click **Suspend**.
  - Your request appears under the Enrollment Requests tab, while you are waiting for the CA to issue the certificate.
  - When the CA issues your certificate, choose the certificate and then choose **Resume** from the Options pull-down menu to complete the enrollment. (See Figure 6-9.)

Figure 6-9 Resuming Enrollment Request



– After you have obtained the certificate, the status screen updates to show the result. (See Figure 6-10.) After viewing the screen, click **OK**.

Figure 6-10 Receiving Status Update



Enrolling Through a File Request

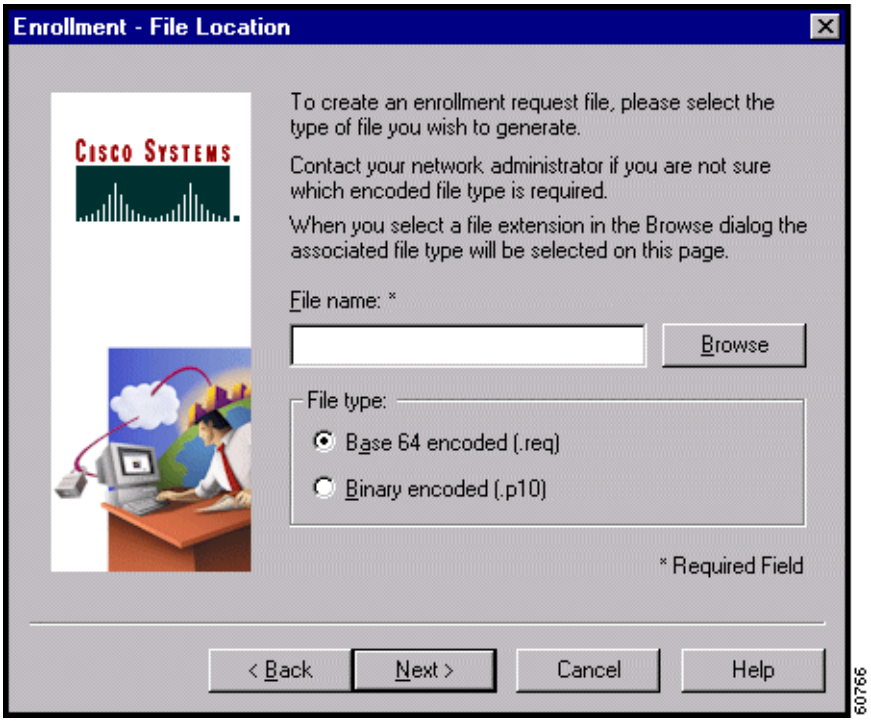
Alternatively, you can enroll by creating a file using the same form as network enrollment. (See Figure 6-3.) Once you have created a request file, you can either e-mail it to the CA and receive a certificate back or you can access the CA's website and cut and paste the enrollment request in the area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

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

Step 1 At the Enrollment - Network or File dialog box. (See Figure 6-5), click **File** and click **Next**.

The Certificate Manager prompts you to choose a file type for your file request and to specify a file name. (See Figure 6-11.)

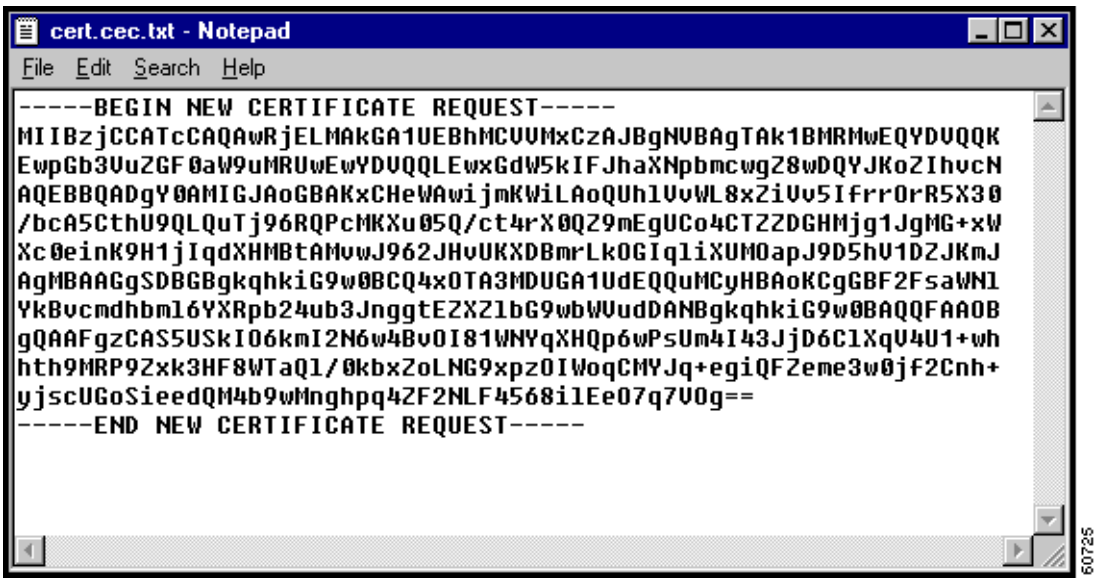
Figure 6-11 Choosing file type and location



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 6-12.) Choose this type when you want to cut and paste the text into the CA website.

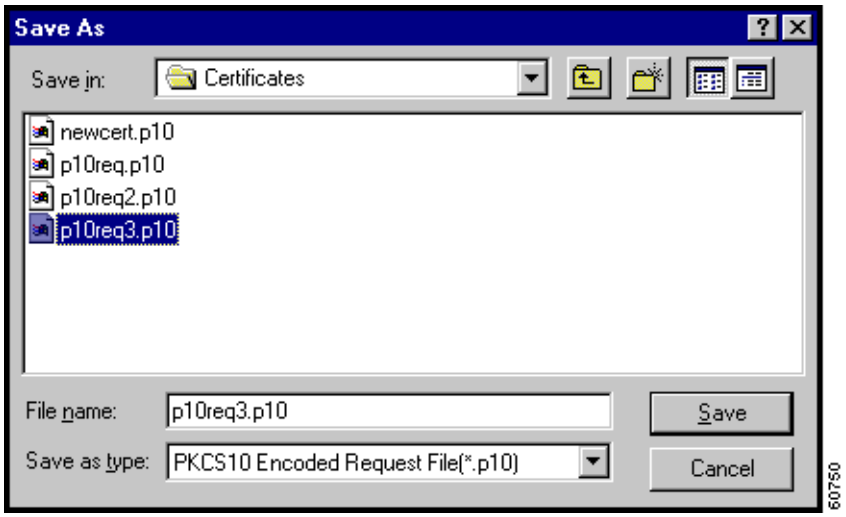
Figure 6-12 A PKCS10 Certificate Request



Step 3 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. (See Figure 6-13.) You can save your file enrollment requests in the Certificates directory, which is a subdirectory of the directory where the VPN Client is installed.

Figure 6-13 Specifying a Filename

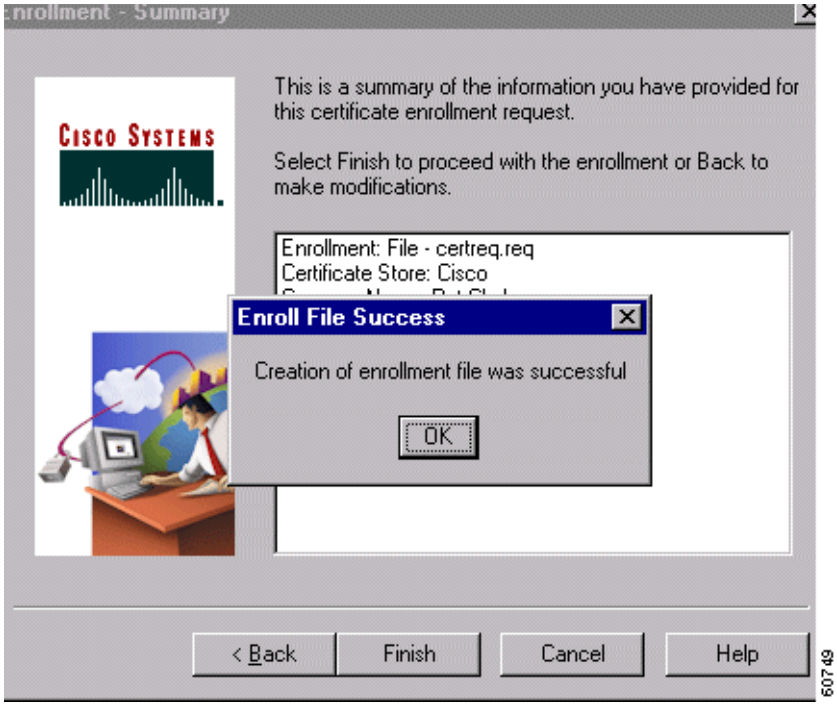


In this example, the complete pathname is C:\Program Files\Cisco Systems\VPN Client\Certificates\p10req3.p10.

Step 4 Complete the form (see the "Enrollment Form" section) and click **Next>**.

The Certificate Manager displays the summary screen and a message to let you know that your request succeeded. (See Figure 6-14.)

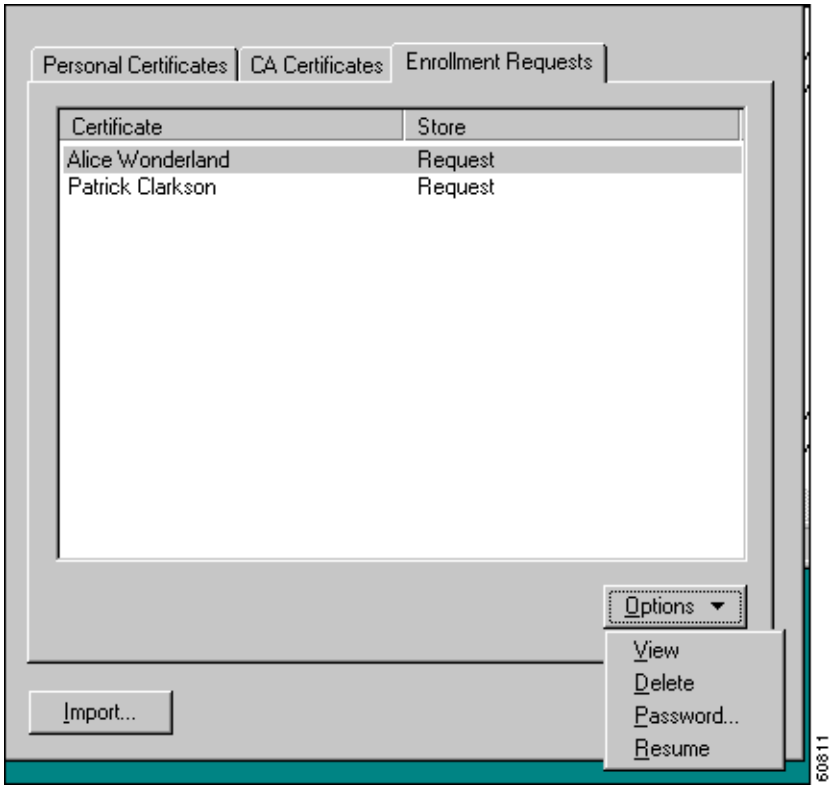
Figure 6-14 Enroll File Success Message



Step 5 Click **OK** on the message screen then click **Finish** on the summary screen.

You can view the file request under the Enrollment Requests tab. (See Figure 6-15.)

Figure 6-15 File Enrollment Requests



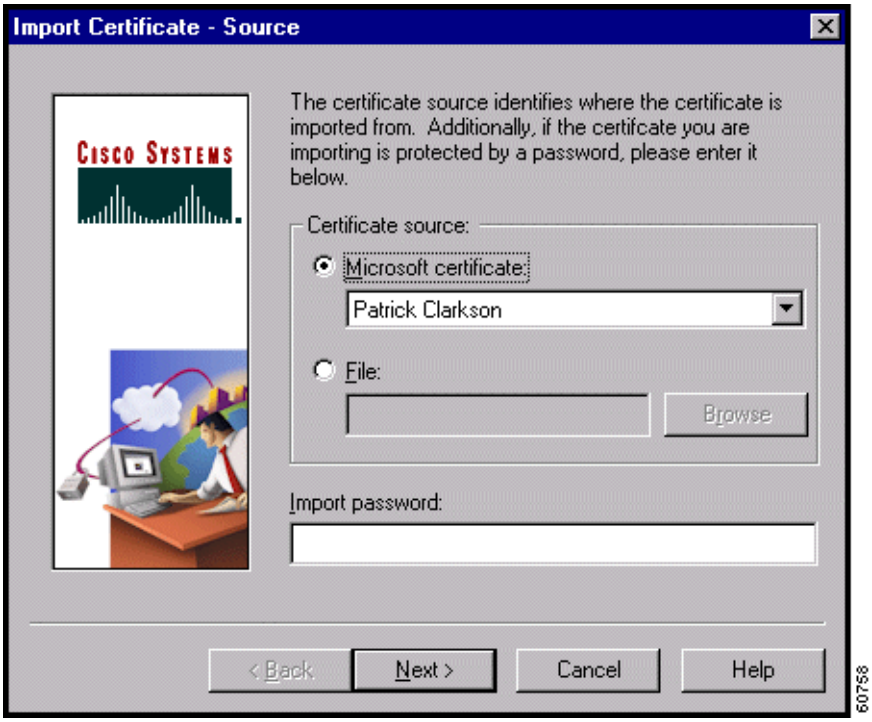
Importing a Certificate File

You can import a certificate into the Cisco store from the Microsoft store or from a file. To import a certificate, use the following procedure:

Step 1 On the Certificate Manager main window under the Personal Certificates tab, click **Import**.

The Certificate Manager displays the Import Certificate - Source dialog box. (See Figure 6-16.)

Figure 6-16 Importing a Certificate



Step 2 To import a certificate do one of the following depending on where your certificate resides:

- Importing from the Microsoft store—Click **Microsoft certificate** and choose the certificate from the drop-down menu. The certificate must already be in your Microsoft store.
- Importing from a file—Click **File** and enter the pathname of the file into the field.

Step 3 If a password is used to protect this certificate, type the password into the Import Password: field.

This is the password assigned to protect the certificate's private key.

- If you are importing from the Microsoft store, this password is the one you (or the network administrator) entered during enrollment.
- If you are importing a certificate from a file, this is the password specified when the certificate was exported.

Step 4 Click **Next>**.

The Certificate Manager prompts for a password to be stored with the certificate. (See Figure 6-17.)

Figure 6-17 Destination Password for Importing Certificate

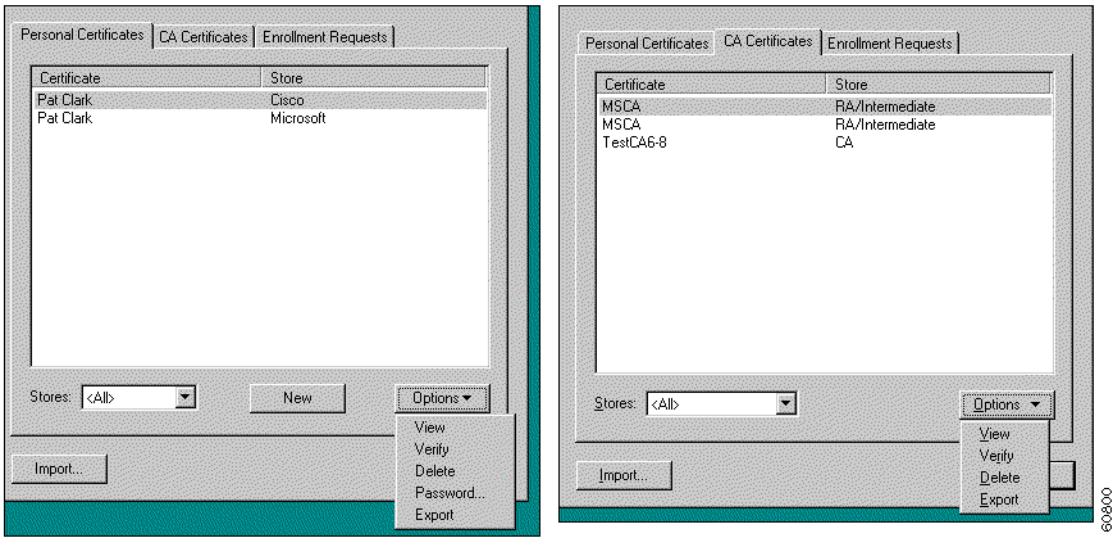
Step 5 Type a password into the Password field, and click **Finish**.

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.

Managing Personal and CA/RA Certificates

Using the Certificate Manager, you can view a certificate, verify that the certificate is still valid (within the dates assigned to it and has not been revoked), delete a certificate, and export the certificate to a file that you can e-mail. For personal certificates only, you can also change the certificate password. To perform any of these actions, use the Options menu on the main window. (See Figure 6-18.)

Figure 6-18 Certificate Manager Options Menu

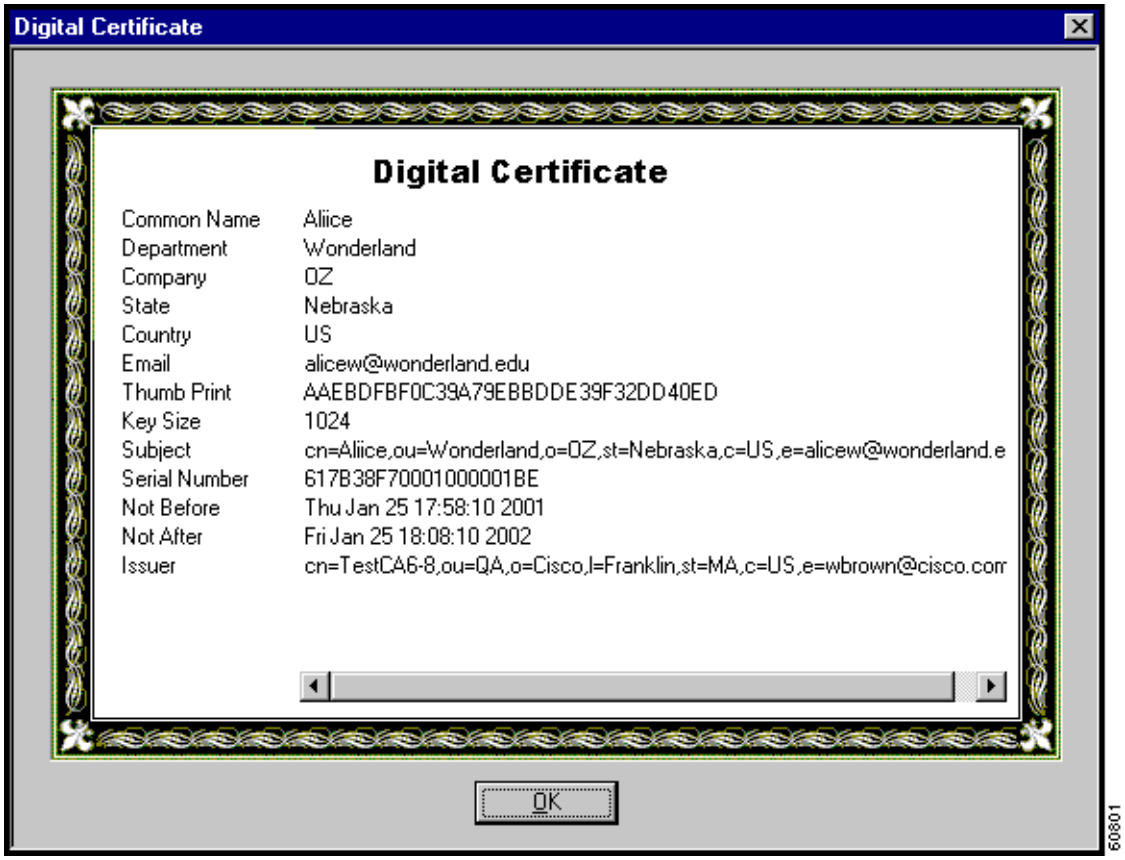


Viewing a Certificate

To display a certificate, choose it in the certificate store, open the Options pull-down menu and choose **View**. Or, you can double-click on the certificate to display it.

Figure 6-19 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 6-19 Displaying a Certificate



A typical certificate shown in Figure 6-19 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 must 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—An MD5 hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. For example, you can contact the issuing CA and use this identifier to verify that this certificate is indeed the right one.
- Key Size—The size of the signing key pair in bits; for example, 512.

- 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.
- 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.
- 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.

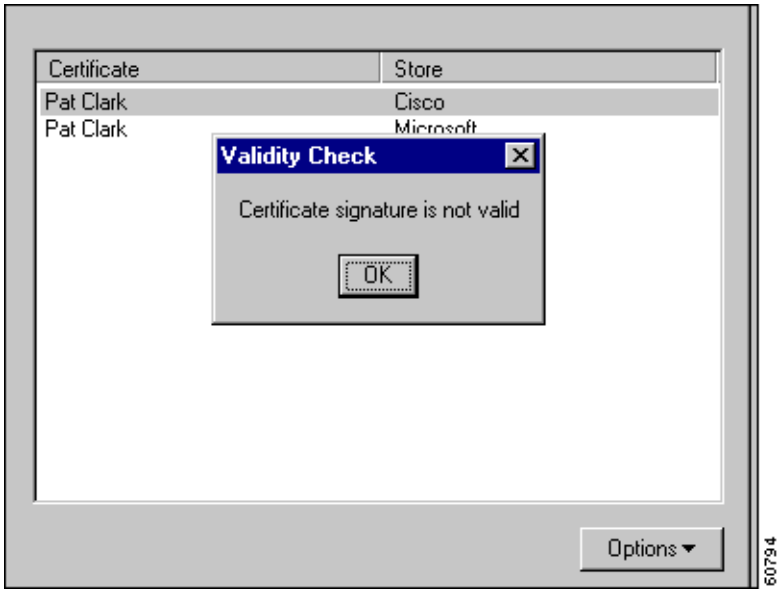
After you have finished viewing the certificate, click **OK** to close it.

Verifying a Certificate

The Certificate Manager provides a quick way for you to check the validity of a certificate; for example, to see if it is within the valid beginning and ending date range. To see if the certificate is valid, choose it in the certificate store, display the Options pull-down menu, and choose **Verify**.

The Certificate Manager displays a message such as the one in Figure 6-20 indicating whether the certificate is still valid.

Figure 6-20 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 is valid`	You have a working certificate enrolled.

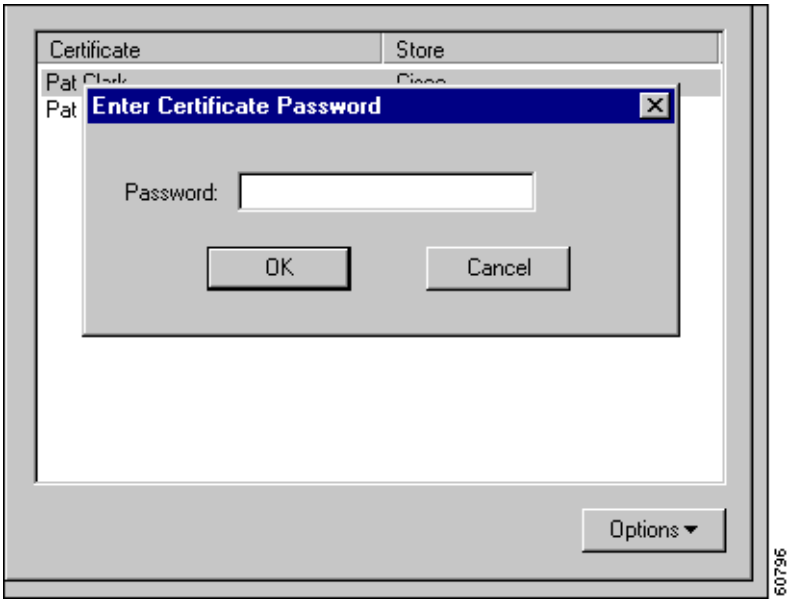
Deleting a Certificate

To delete a certificate, follow this procedure:

Step 1 Choose the certificate in the certificate store, display the Options pull-down menu, and choose **Delete**.

If the certificate has a password, the Certificate Manager prompts you to enter it. (See Figure 6-21.)

Figure 6-21 Entering Password for Deleting a Certificate



Step 2 In the Password field, type the password given to the certificate during enrollment and click **OK**. Next, the Certificate Manager asks you to confirm. (See Figure 6-22.)

Figure 6-22 Confirming Deletion

Step 3 To complete the deletion, click **Yes**. If you decide not to delete this certificate, click **No**.

Changing the Password on a Personal Certificate

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

Step 1 Display the Options pull-down menu and choose **Password...**.

The Certificate Manager displays the Change Certificate Password dialog box. (See Figure 6-23.)

Figure 6-23 Changing a Certificate Password

Step 2 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**.

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 Options pull-down menu and choose **Export**.

The Certificate Manager displays the Export Certificate dialog box. (See Figure 6-24.)

Figure 6-24 Exporting a Certificate

Step 2 In the Certificate password field, enter the password initiated during enrollment.

The Certificate password protects the certificate in the certificate store (so an unauthorized individual can not use it). This is the password you *optionally* entered when you enrolled for the certificate.

Step 3 In the Export password field, enter an optional password to protect the export file. Then enter it again in the Confirm password field.

Step 4 In the Export filename field, enter the filename for the exported certificate. Only the filename is required. Use the Browse feature to locate a target directory for the exported certificate.

Step 5 To export the CA and/or RA certificate with your personal certificate, check the **Export certificate chain** option.

Step 6 After completing all the information, click **OK**.

The Certificate Manager displays a message indicating whether your certificate export was successful. (See Figure 6-25.)

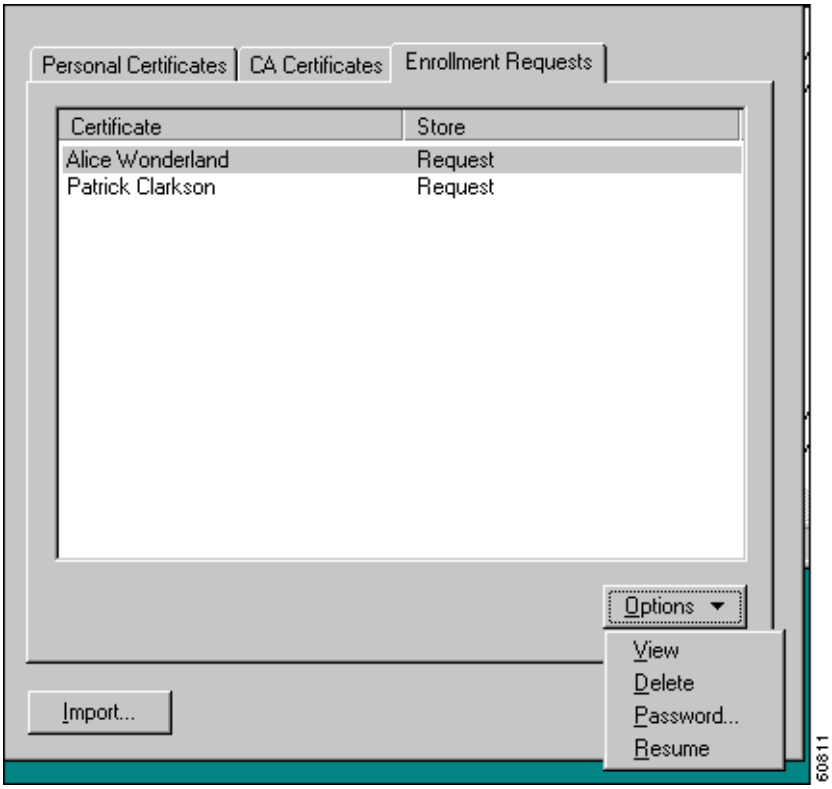
Figure 6-25 Export Message

Step 7 To continue, click **OK**.

Managing Enrollment Requests

While a request is pending approval by the CA administration, the Certificate Manager places the enrollment request under the Enrollment Requests tab. You can view, delete, or change the password on any request in the list; or you can resume a network enrollment request. To perform any of these actions, choose the Enrollment Requests tab and click on the Options pull-down menu. (See Figure 6-26.)

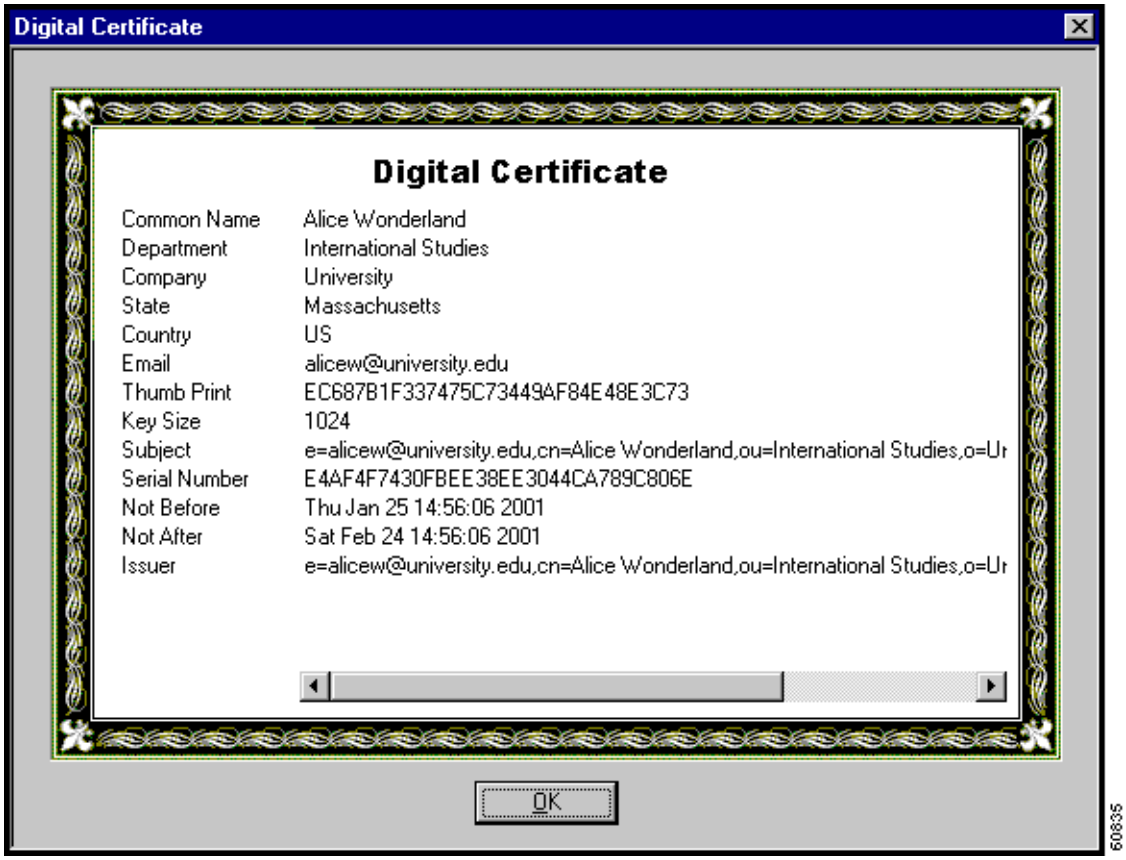
Figure 6-26 Managing Enrollment Requests



Viewing the Enrollment Request

To display the enrollment request, click on its name in the list and choose **View** from the Options pull-down menu. The Certificate Manager displays the pending request. (See Figure 6-27.)

Figure 6-27 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.

Deleting an Enrollment Request

To delete an enrollment request, follow these steps:

Step 1 Click on the enrollment request in the list and choose **Delete** from the Options pull-down menu.

The Certificate manager prompts you for a password.

Step 2 Type the password in the Password field and click **OK**.

The Certificate Manager verifies the password. If the password is correct, the Certificate Manager asks you to confirm that you really want to delete the enrollment request.

Step 3 To complete the deletion, click **Yes**. If you decide not to delete this certificate, click **No**.

Changing the Password on an Enrollment Request

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

Step 1 Display the Options pull-down menu and choose **Password...**.

The Certificate Manager displays the Change Certificate Password dialog box. (See Figure 6-28.)

Figure 6-28 Changing a Certificate Password

Step 2 In the Current field, type the password you are currently using.

Step 3 In the New field, type the new password.

Step 4 In the Confirm field, type your new password again.

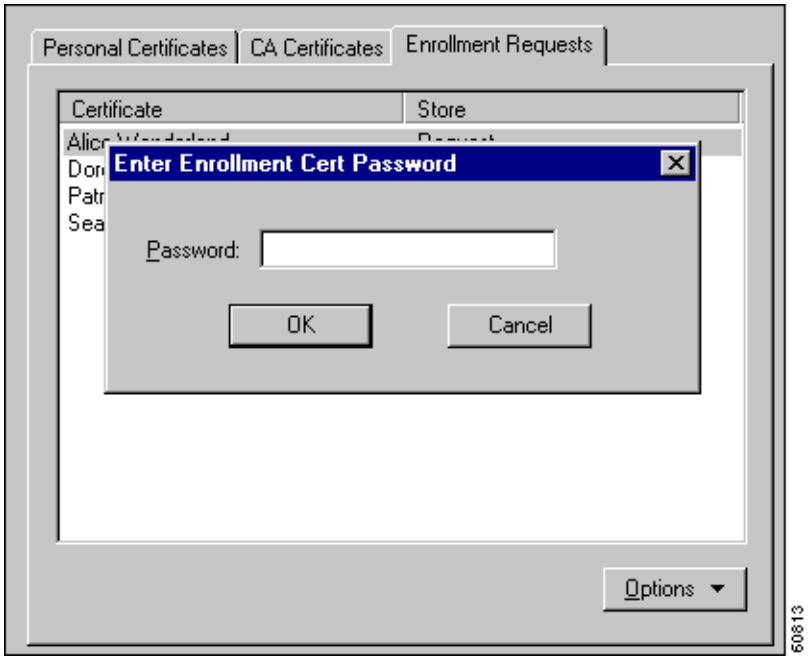
Step 5 Click **OK**.

Completing an Enrollment Request

To complete a pending enrollment request, choose the request under the Enrollment Requests tab, and choose **Resume** from the Options pull-down menu.

The Certificate Manager prompts you to enter a password. (See Figure 6-29.) This password must match the password you are using to protect the certificate's private key, if any.

Figure 6-29 Entering Password to Resume Online Enrollment



Enter the password and click **OK** to resume enrollment.

Copyrights and Licenses

Client Software License Agreement of Cisco Systems

THE SOFTWARE TO WHICH YOU ARE REQUESTING ACCESS IS THE PROPERTY OF CISCO SYSTEMS. THE USE OF THIS SOFTWARE IS GOVERNED BY THE TERMS AND CONDITIONS OF THE AGREEMENT SET FORTH BELOW. BY CLICKING “YES” ON THIS SCREEN, YOU INDICATE THAT YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THAT AGREEMENT. THEREFORE, PLEASE READ THE TERMS AND CONDITIONS CAREFULLY BEFORE CLICKING ON “YES”. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE AGREEMENT, CLICK “NO” ON THIS SCREEN, IN WHICH CASE YOU WILL BE DENIED ACCESS TO THE SOFTWARE.

Ownership of the Software

The software contained in the Cisco Systems VPN Client (“the Software”), to which you are requesting access, is owned or licensed by Cisco Systems and is protected by United States copyright laws, laws of other nations, and/or international treaties.

Grant of License

Cisco Systems hereby grants to you the right to install and use the Software on an unlimited number of computers, provided that each of those computers must use the Software only to connect to Cisco Systems products, and subject to export restrictions in paragraph 4 hereof. You may make one copy of the Software for each such computer for the purpose of installing the Software on that computer. The Software is licensed for use only with Cisco Systems products, and for no other use.

Restrictions on Use and Transfer

You may not otherwise copy the Software, except that you may make one copy of the Software solely for backup or archival purposes. To this end, you may transfer the Software to a single set of disks provided you keep the disks solely for backup or archival purposes. You may not use the backup or archival copy of the Software except in conjunction with Cisco Systems products.

You may not transfer the Software to any third party without the express written permission of Cisco Systems. For permitted transfers, you may not export the Software to any country for which the United States requires any export license or other governmental approval at the time of export without first obtaining the requisite license and/or approval. Furthermore, you may not export the Software in violation of any export control laws of the United States or any other country.

You may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from, the Software or any accompanying documentation or any copy thereof, in whole or in part.

The subject license will terminate immediately if you do not comply with any and all of the terms and conditions set forth herein. Upon termination for any reason, you (the licensee) must immediately destroy the Software, any accompanying documentation, and all copies thereof. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.

You may not remove or alter any copyright, trade secret, patent, trademark, trade name, logo, product designation or other proprietary and/or other legal notices contained in or on the Software and any accompanying documentation. These legal notices must be retained on any copies of the Software and accompanying documentation made pursuant to paragraphs 2 and 3 hereof.

You shall acquire no rights of any kind to any copyright, trade secret, patent, trademark, trade name, logo, or product designation contained in, or relating to, the Software or accompanying documentation and shall not make use thereof except as expressly authorized herein or otherwise authorized in writing by Cisco Systems.

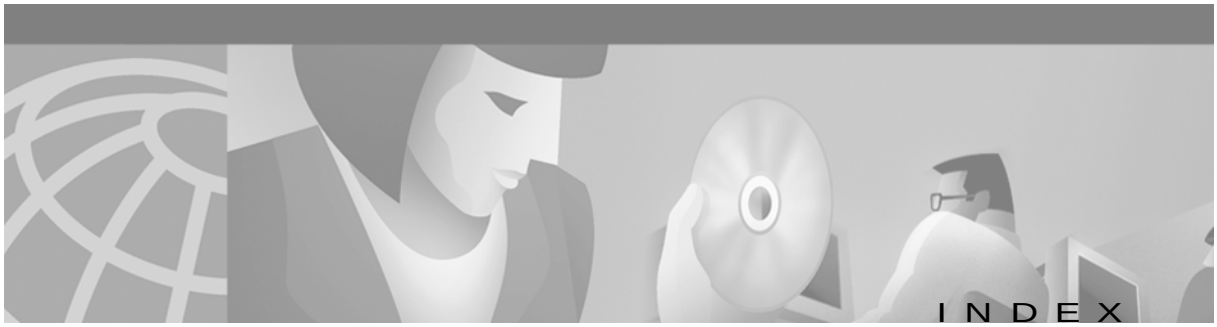
Limitation Of Liabilities

INSTALLATION AND USE OF THE SOFTWARE IS ALSO GOVERNED BY A SEPARATE LICENSE AGREEMENT BETWEEN CISCO SYSTEMS AND THE PURCHASER OF THE CISCO SYSTEMS VPN CLIENT PRODUCT. THAT SEPARATE LICENSE AGREEMENT CONTAINS A DESCRIPTION OF ALL WARRANTIES PROVIDED BY CISCO SYSTEMS FOR THE SOFTWARE. CISCO SYSTEMS PROVIDES NO WARRANTIES FOR THE SOFTWARE OTHER THAN THOSE SET FORTH IN THAT AGREEMENT, AND ASSUMES NO LIABILITIES WITH RESPECT TO YOUR USE OF THE SOFTWARE.

RSA software

The RSA Public Key Cryptosystem is protected by U.S. Patent #4,405,829.

Zone Labs



A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z