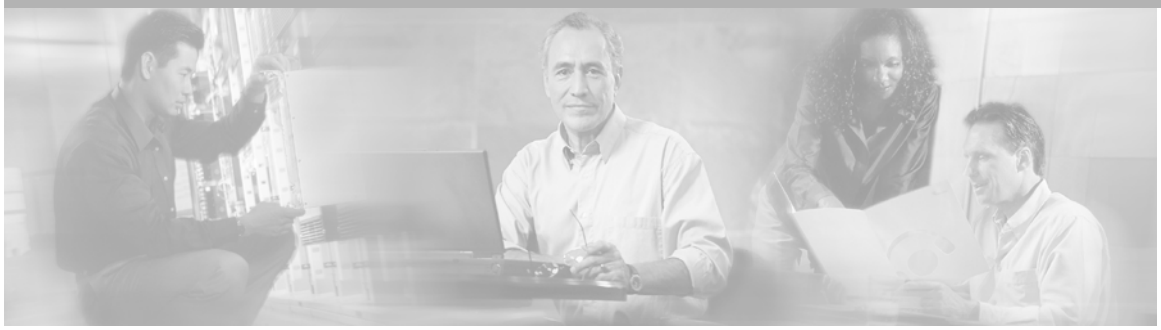


VPN Client User Guide for Windows

Release 4.6
August 2004

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-OL-5489-01

VPN Client User Guide for Windows

Preface

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

Audience

This guide is for users of 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. For information specific to a network administrator, see *VPN Client Administrator Guide*.

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Understanding the Cisco VPN Client	Explains briefly 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	Navigating the User Interface	Describes the main VPN Client window and the tools, tabs, menus and icons for navigating the user interface, including accessibility features.
Chapter 4	Configuring and Managing Connection Entries	Tells you how to configure the VPN Client, including setting optional parameters.
Chapter 5	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, and how to use automatic VPN initiation.

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.
Chapter 7	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, and set up special features such as Start Before Logon.
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 Concentrators
- 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, including a pdf version of the manual, 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.
- Select Help > Help VPN Client from the Help menu.

The *VPN Client Administrator Guide* tells a network administrator how to:

- Configure a VPN 3000 Concentrator for several specific features:
  - Configure a VPN 3000 Concentrator for remote access users
  - Configure VPN Client firewall policy on a VPN 3000 Concentrator
  - Notify remote users of a client update
  - Set up Local LAN Access for the VPN Client
  - Configure the VPN Concentrator to update VPN Client backup servers
  - Set up the VPN Concentrator and the VPN Client for NAT Transparency
  - Configure Entrust Entelligence for the VPN Client
  - Set up authentication using Smart Cards.
- Automate remote user profiles
- Configure auto initiation
- Use the VPN Client command-line interface

- Customize the VPN Client software (text, icons and installation)
- Use the SetMTU application
- Obtain troubleshooting information
- Work with Microsoft Windows Installer

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 Client**.

http://www.cisco.com/en/US/products/sw/secursw/ps2308/prod_technical_documentation.html

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).

Cisco PIX Firewall Documentation

The VPN Client can also interact with the Cisco PIX Firewall. For information about using the PIX Firewall product, see the following documents.

- *Cisco PIX Firewall and VPN Configuration Guide, Version 6.3*
- *Cisco PIX Firewall Command Reference, Version 6.3*

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.

Type of Data	Format
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

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

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

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: 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 online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Understanding the Cisco VPN Client

The Cisco VPN Client for Windows (referred to in this user guide as *VPN Client*) is software that runs on a Microsoft® Windows®-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN server 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). The server verifies that incoming connections have up-to-date policies in place before establishing them. Cisco IOS, VPN 3000 Series Concentrators, and PIX central-site servers can all terminate VPN connections from VPN Clients.

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

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

Figure 1-1 VPN Client Applications as Installed by the Install Shield Wizard

The applications are as follows:

- Help—Displays an online manual with instructions on using the applications.
- SetMTU—Lets you manually change the size of the maximum transmission unit (see the *VPN Client Administrator Guide*, Chapter 6.)
- VPN Client—Lets you configure connections to a VPN server, start connections, enroll for certificates to authenticate connections to VPN servers, and 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.

Note You can install the VPN Client through either the InstallShield wizard or the Microsoft Installer. If you install the VPN Client through the Microsoft Installer, the Programs menu shown in Figure 1-1 does not contain the Uninstall application.

How the VPN Client Works

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

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 tables in the following sections describe the VPN Client features.

Table 1-1 lists the VPN Client main features.

Table 1-1 VPN Client for Windows Main Features

Features	Description
Operating System	Windows 98, Windows NT, Windows ME, Windows 2000, Windows XP
Connection types	• async serial PPP • Internet-attached Ethernet
Protocol	IP

Table 1-1 VPN Client for Windows Main Features (continued)

Features	Description
Tunnel protocol	IPSec
User Authentication	• RADIUS • RSA SecurID • VPN server internal user list • PKI digital certificates • Smart cards • NT Domain (Windows NT)

Program Features

The VPN Client supports the program features listed in Table 1-2.

Table 1-2 Program Features

Program Feature	Description
On-line Help	• Complete browser-based context-sensitive Help
Servers supported	• Cisco IOS devices that support Easy VPN server functionality • VPN 3000 Series Concentrators • Cisco PIX Firewall Series, Version 6.2 or later
Interface supported	• Graphical user interface • Command line interface
Local LAN access	The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission).
Automatic VPN Client configuration option	The ability to import a configuration file.
Event logging	The VPN Client log collects events for viewing and analysis.
NAT Transparency (NAT-T)	Enables the VPN Client and the VPN device to automatically detect when to use IPSec over UDP to work properly in Port Address Translation (PAT) environments.
Update of centrally controlled backup server list	The VPN Client learns the backup VPN server list when the connection is established. This feature is configured on the VPN device and pushed to the VPN Client. The backup servers for each connection entry are listed on the Backup Servers tab.
Set MTU size	The VPN Client automatically sets a maximum transmission unit (MTU) size that is optimal for your environment. However, you can also set the MTU size manually. For information on adjusting the MTU size, see the *VPN Client Administrator Guide*.

Table 1-2 Program Features (continued)

Program Feature	Description
Support for Dynamic DNS (DDNS hostname population)	The VPN Client sends its hostname to the VPN device when the connection is established. If this occurs, the VPN device can send the hostname in a DHCP request. This causes the DNS server to update its database to include the new hostname and VPN Client address.
Application Launcher	The ability to launch an application or a third-party dialer from the VPN Client.
Uninstall package (InstallShield)	Automatic uninstall of the 5000 VPN Client software with the InstallShield installation package.
Automatic dialup connection	Automatic connection by way of Microsoft Dial-Up Networking or any other third-party remote-access dialer.
Notifications	Software update notifications from the VPN server upon connection.
Launching from notification	Ability to launch a location site containing upgrade software from a VPN server notification.
Auto initiation	The ability to automatically initiate secure wireless VPN connections seamlessly.
Virtual adapter	Available on Windows 2000 and Windows XP, this software-only driver acts as a valid interface in the system to solve application incompatibly problems.
Alerts (Delete with reason)	The VPN Client can display to the user the reason for a VPN 3000 Concentrator-initiated disconnection, if that information is available. If the VPN 3000 Concentrator disconnects the VPN Client and tears down the tunnel, the VPN Client displays a pop-up window showing the reason for the disconnect and also logs a message to the Notifications log and the IPSec log file. IPSec deletes that do not tear down the connection, generate an event message only in the log file.
Single-SA	The ability to support a single SA per VPN connection. Rather than creating a host-to-network security association (SA) pair for each split-tunneling network, this feature provides a host-to-ALL approach, creating one tunnel for all appropriate network traffic apart from whether split-tunneling is in use.
Coexistence with third-party client software	Compatibility with Microsoft, Nortel, Checkpoint, Intel, and other VPN clients -- the ability to use other VPN products while the VPN Client is installed. This does *not* allow each VPN Client to make connections simultaneously.
Automatic updates	The VPN device pushes an automatic update to the VPN Client to implement. When the VPN Client connects to the VPN device, it receives a location from which to download an update. The VPN Client then connects through a VPN tunnel to this location and downloads the update, which comprises VPN Client files and profiles. When the download has completed, the VPN Client verifies the integrity of the files and installs them. This feature is for Windows 2000 and Windows XP only.

Table 1-2 Program Features (continued)

Program Feature	Description
Browser proxy configuration for Internet Explorer	When connecting to the secure gateway at a central location, the VPN Client changes the web browser proxy to accommodate the organization's environment. When disconnecting, the software returns to the user's default browser application. This feature applies to Internet Explorer only. The VPN Concentrator administrator configures this feature in the VPN Concentrator Manager (see *VPN Client Administrator Guide*, Chapter 1).
Connect on open	This feature lets a user connect to the default user profile when starting the VPN Client (limited to the vpngui.exe program).
508 accessibility compliance	Starting with 4.6, the VPN Client complies with all 508 standards for accessibility. For information about activating the accessibility features before you progress any further, refer to Configuring the VPN Client for Accessibility.
VPN Client API	VPN Client provides an application programming interface for performing VPN Client tasks without using the command-line or graphical interfaces that Cisco provides. This API comes with a user guide for programmers, which is in a format that can be edited.

Authentication Features

The VPN Client supports the authentication features listed in Table 1-3.

Table 1-3 Authentication Features

Authentication Feature	Description
User authentication through 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 Authorities (CAs)	CAs that support PKI SCEP enrollment.
Entrust Entelligence	Ability to use Entrust Entelligence certificates
Certificate Management	Ability to manage the certificates in the certificate stores.
Smart cards	Ability to authenticate using smart cards with certificates
Peer Certificate Distinguished Name Verification	Prevents a VPN Client from connecting to an invalid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the VPN Client connection also fails.

Firewall Features

The VPN Client supports the firewall features listed in Table 1-4.

Table 1-4 Firewall Features

Firewall Feature	Description
Support for firewalls	• Cisco Integrated Firewall • Cisco Security Agent • ZoneAlarmPro 2.6.3.57 and higher • ZoneAlarm 2.6.3.57 and higher • ZoneLabs Integrity 1.0 and higher • BlackIce Agent and BlackIce Defender 2.5 and higher. • Sygate Personal Firewall and Sygate Personal Firewall Pro, Version 5.0, Build 1175 and higher
Centralized Protection Policy	• Support for firewall policies pushed to the VPN Client from a VPN Concentrator
Stateful Firewall	Command-line enable/disable Stateful Firewall
ICMP permission	Configurable on the VPN Client

IPSec Features

The VPN Client supports the IPSec features listed in Table 1-5

Table 1-5 IPSec Features

IPSec Feature	Description
Tunnel Protocol	IPSec
Transparent tunneling	• IPSec over UDP for NAT and PAT • IPSec over TCP for NAT, PAT, and firewalls
Key Management protocol	Internet Key Exchange (IKE)
IKE Keepalives	A tool for 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. The VPN device supplies a list of networks to the VPN Client for tunneled traffic. You enable split tunneling and configure the network list on the VPN device.

Table 1-5 IPSec Features (continued)

IPSec Feature	Description
Support for Split DNS	The ability to direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS. The VPN server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network. For example, a query for a packet destined for corporate.com would go through the tunnel to the DNS that serves the private network, while a query for a packet destined for myfavoritesearch.com would be handled by the ISP's DNS. This feature is configured on the VPN server and enabled on the VPN Client by default. To use Split DNS, you must also have split tunneling configured.
LZS data compression	A feature that benefits modem users.

VPN Client IPSec Attributes

The VPN Client supports the IPSec attributes listed in Table 1-6.

Table 1-6 IPSec Attributes

IPSec Attribute	Description
Main Mode and Aggressive Mode	Ways to negotiate phase one of establishing ISAKMP Security Associations (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 • Mutual Group Authentication • X.509 Digital Certificates
Diffie-Hellman Groups	• Group 1 = 768-bit prime modulus • Group 2 = 1024-bit prime modulus • Group 5 = 1536-bit prime modulus
Encryption algorithms	• 56-bit DES (Data Encryption Standard) • 168-bit Triple-DES • AES 128-bit and 256-bit
Extended Authentication (XAUTH)	The capability of authenticating a user within IKE. This authentication is in addition to the normal IKE phase 1 authentication, where the IPSec devices authenticate each other. The extended authentication exchange within IKE does not replace the existing IKE authentication.
Mode Configuration	Also known as ISAKMP Configuration Method

Table 1-6 IPSec Attributes (continued)

IPSec Attribute	Description
Tunnel Encapsulation Modes	• IPSec over UDP (NAT/PAT) • IPSec over TCP (NAT/PAT) • IPSec over NAT-T
IP compression (IPCOMP) using LZS	Data compression algorithm

Windows Features Supported

The VPN Client supports the Windows NT, Windows 2000, and Windows XP features listed in Table 1-7.

Table 1-7 Windows NT Features

Windows NT Feature	Description
Password expiration information	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 a Release 3.5 or higher 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.
Automatic VPN disconnect on logoff	The ability to enable or disable automatic disconnect when logging off a Windows NT platform. Disabling this feature allows for roaming profile synchronization.

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 Through InstallShield
- Installing the VPN Client Through Microsoft Windows Installer

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

Caution Installing the VPN Client software using InstallShield 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.

Installation Applications

You can install the VPN Client on your system through either of two different applications: InstallShield and Microsoft Windows Installer (MSI). Both applications use installation wizards to walk you through the installation. Installing the VPN Client through InstallShield includes an Uninstall icon in the program group; MSI does not. In the latter case, to manually remove VPN Client applications, you can use the Microsoft Add/Remove Programs utility.

Verifying System Requirements

Verify that your computer meets these requirements:

- A single, Pentium®-class processor.
- One of the following operating systems:
  - Microsoft®Windows® 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT 4.0 (with Service Pack 6, or higher)
  - Windows 2000
  - Windows XP

- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 50 MB hard disk space.
- RAM:
  - 32 MB for Windows 98
  - 64 MB for Windows NT and Windows ME
  - 64 MB for Windows 2000 (128 MB recommended)
  - 128 MB for Windows XP (256 MB recommended)
- 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
- 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)
  - Or a digital certificate stored on a smart card; the VPN Client supports smart cards via the MS CAPI Interface

Gathering Information You Need

To configure and use the VPN Client, you might 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 might 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 and password.

- 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 Through InstallShield

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

Step 3 Choose **Start > Run**. The Run dialog box appears.

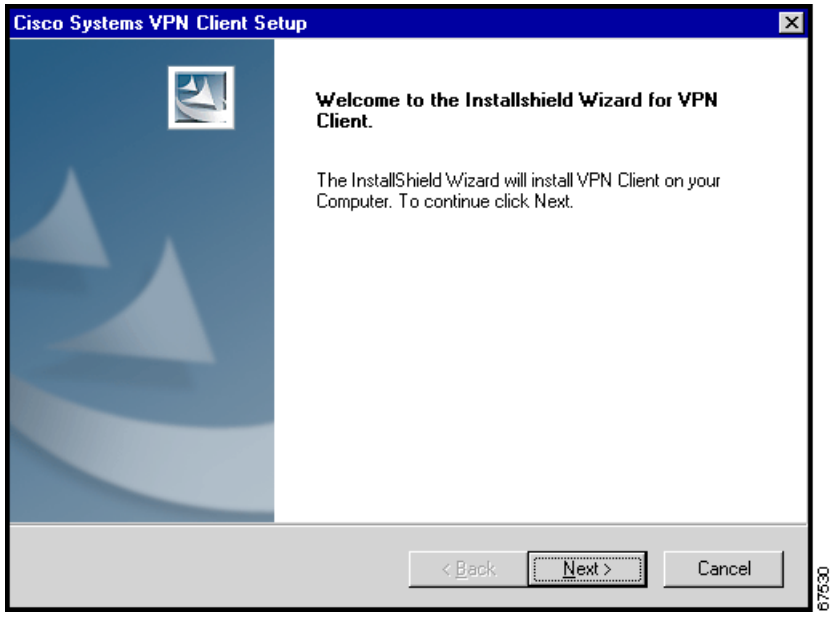
Step 4 Enter E:\VPN Client\CD-ROM\InstallShield\setup.exe, where E: is your system's CD-ROM drive.

Step 5 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 Starting InstallShield Installation



Step 6 If the InstallShield Wizard identifies an existing version of either the VPN 3000 Client or the Cisco 5000 VPN Client, it displays a dialog box that asks if you want to uninstall the existing client program. To continue, click **Yes**.

The VPN Client launches the appropriate uninstall wizard: the Cisco VPN Client uninstall wizard to uninstall a previous version of the VPN 3000 Client or the Cisco 5000 VPN Client. Follow the instructions on the uninstall wizard dialog boxes to automatically uninstall the program and reboot.

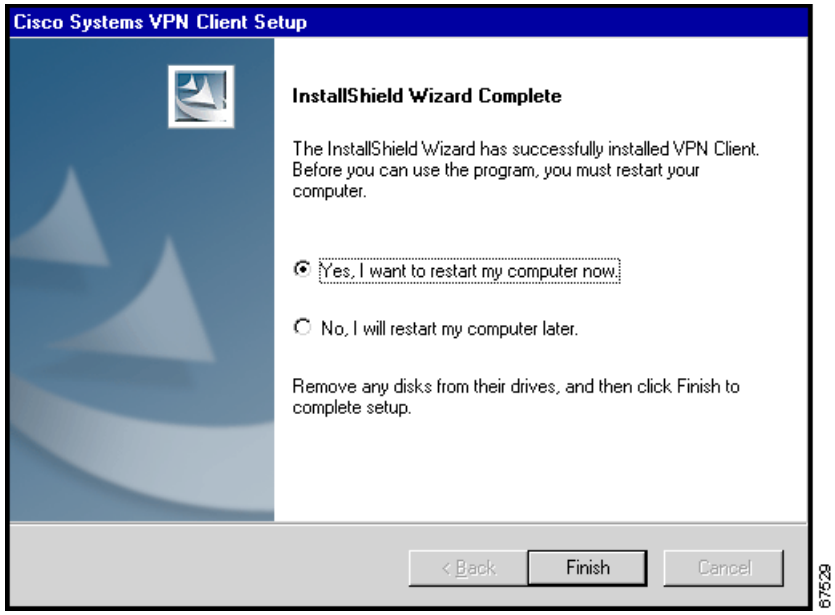
After your system reboots, the Cisco Systems VPN Client Setup wizard resumes.

Step 7 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 8 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 Completing InstallShield Installation



- 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.*

Installing the VPN Client Through Microsoft Windows Installer

Microsoft Windows Installer (MSI) is available for Windows NT, Windows 2000, and Windows XP.

Note If you are using the MSI installer, you must have Windows NT-based products such as Windows NT 4.0 (with SP6), Windows 2000, or Windows XP. Installing with MSI also requires administrator privileges.

Windows Installer 2.0 must be installed on a Windows NT or Windows 2000 PC before configuring the PC for a Restricted User with Elevated Privileges (CSCea37900).

To install the VPN Client using MSI, use the following procedure.

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

Step 2 Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.

Step 3 Choose **Start > Run**. The Run dialog box appears.

Step 4 Enter E:\VPN Client\CD-ROM\Msi\vpclient_en.exe, where E: is your system's CD-ROM drive.

Step 5 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 Microsoft Installer Setup window. Click **Next** to start the installation and then follow the instructions on the dialog boxes.

MSI installs the VPN Client in the default location C:\Program Files\Cisco Systems\VPN Client. If you want a different destination folder for the VPN Client files, enter the alternative location when prompted to do so.

When the installation has completed, the installer displays a confirmation dialog box.

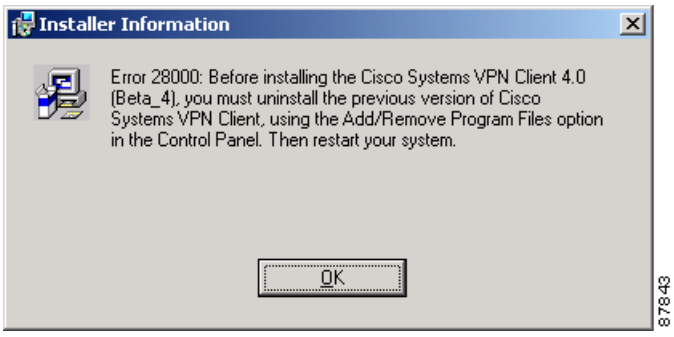
Step 6 Click **Finish**. MSI prompts you to restart your system.

Step 7 Click **Yes** to restart your system.

Note If you have not removed a previously installed VPN Client, when you execute the vpnclient_en.exe command or vpnclien_en.msi, an error message displays. See Figure 2-3. You must uninstall the previously installed VPN Client before proceeding with the new installation.

To remove a VPN Client installed with the MSI installer, use the Windows Add/Remove Programs control panel. To remove a VPN Client installed with InstallShield, select **Uninstall Client** on the Programs > VPN Client > Uninstall Client menu sequence.

Figure 2-3 Uninstall Error Message

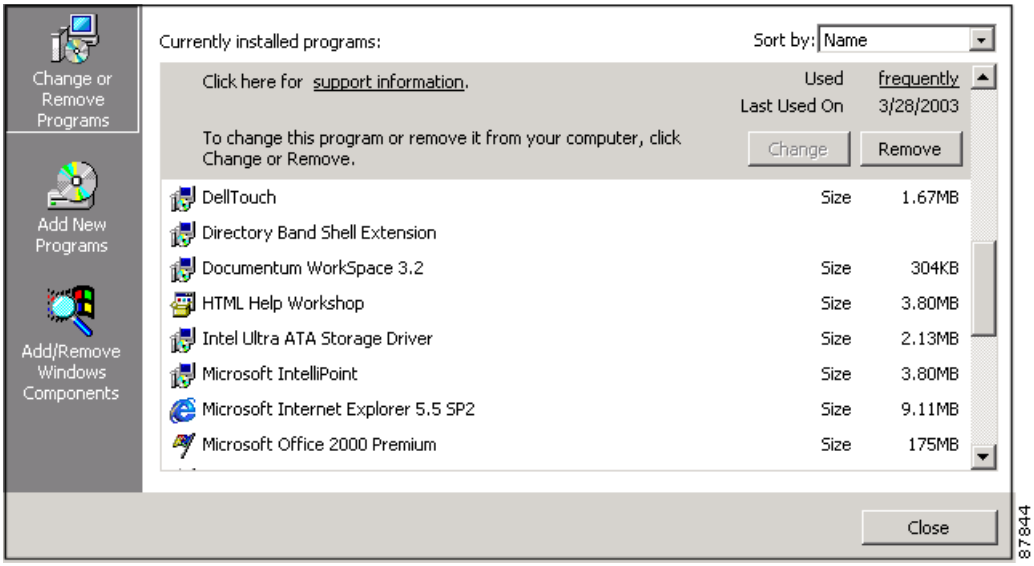


Removing a VPN Client Version Installed with MSI Installer

To uninstall a VPN Client version that was installed with the MSI installer, follow these steps:

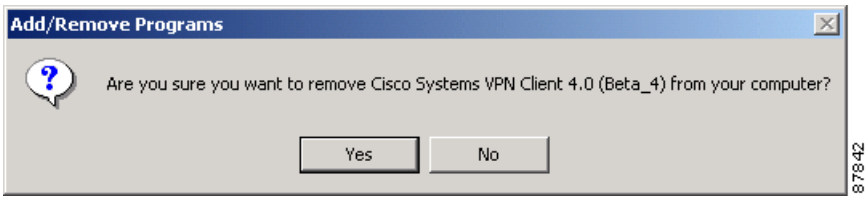
Step 1 Double-click the Add/Remove Programs control panel and select Cisco VPN Client. (See Figure 2-4.)

Figure 2-4 Removing Cisco VPN Client



Step 2 Click Remove. You see a dialog box asking you to confirm that you want to remove the VPN Client from your PC. (See Figure 2-5.)

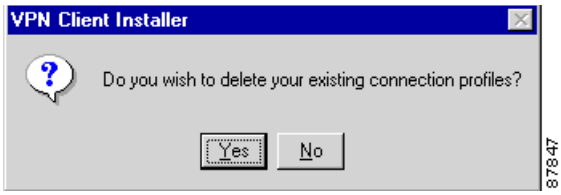
Figure 2-5 Uninstall Confirmation Dialog Box



Step 3 Click **Yes**. The Installer displays a dialog box (Figure 2-6) asking whether you want to delete your existing connection profiles.

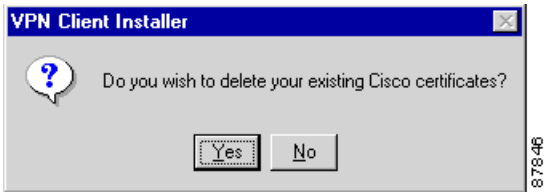
Step 4 Click **Yes** (the default) if you want to remove your connection profiles or **No** to retain them.

Figure 2-6 Uninstall Dialog Box - Delete Connection Profiles



Step 5 The wizard displays a dialog box asking whether you want to delete your existing Cisco certificates. (See Figure 2-7.) Click **Yes** (the default) to delete them or **No** to retain them.

Figure 2-7 Uninstall Dialog Box - Delete Certificates



Step 6 To remove the Cisco VPN Client, click **Next**. Or to halt the wizard, click **Cancel**.

When you respond to this dialog box, the wizard removes the Cisco VPN Client. If you elected to remove your connection profiles and/or certificates, these files are also removed; otherwise, these files remain on your system.

Step 7 To make these changes take effect, you must restart your computer. When it finishes uninstalling the VPN Client, the wizard asks whether you want to restart your computer now or restart later. Select the appropriate radio button and click **Finish**.

If you select **Restart Now**, the wizard exits and restarts your computer. If you select **Restart Later**, the wizard simply exits.

Automatically Installing a Root Certificate on the VPN Client PC

Some types of authentication, such as mutual or hybrid authentication, require that the VPN Client's PC have a root certificate installed. To have a root certificate automatically installed during installation follow these steps:

Step 1 Place the root certificate in a file named rootcert (without an extension).

Step 2 Place the rootcert file in your installation directory.

What Next?

When the VPN Client software is installed on your PC, to configure it, see "Configuring and Managing Connection Entries."

Navigating the User Interface

This chapter describes the main VPN Client window and the tools, tabs, menus and icons for navigating the user interface. This chapter contains the following sections:

Configuring the VPN Client for Accessibility

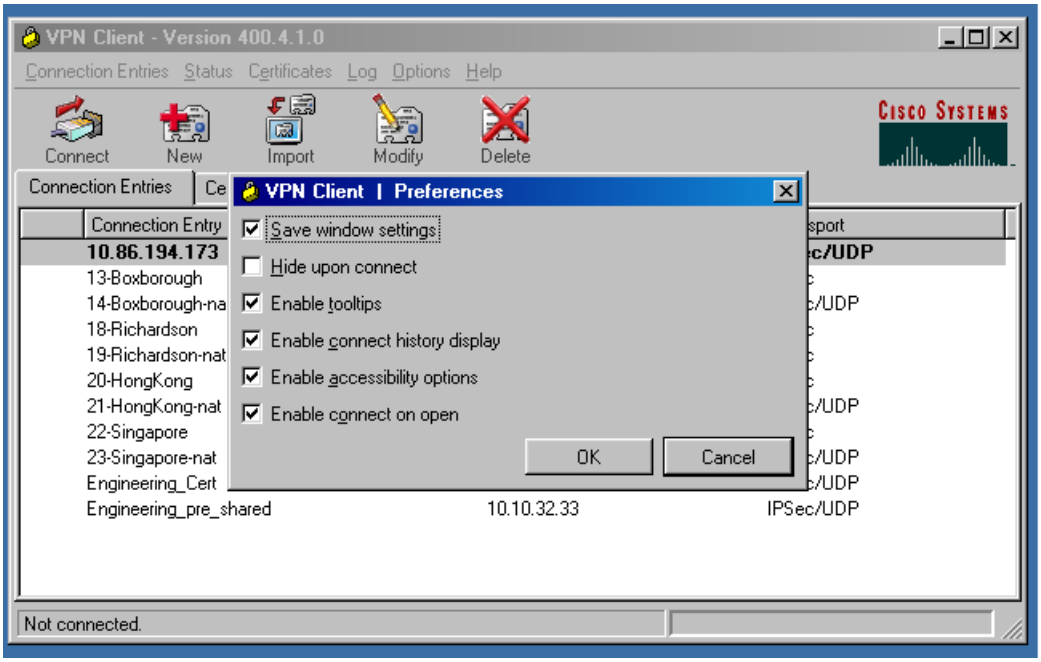
You can activate accessibility features in the VPN Client for Windows user interface. Accessibility features include the following:

- No system tray icon. When connected, the VPN Client is minimized and you can access it with the key combination **Alt Tab**.
- Sound and visual notifications for all dialogs and text edit boxes
- Sound and visual notifications when connecting and disconnecting

To activate the accessibility features, use this procedure.

Step 1 Open the Options menu and display the Preferences menu.

Figure 3-1 Enabling Accessibility Options



Step 2 Check Enable accessibility options and click OK.

Step 3 Restart the VPN Client to activate the accessibility features.

Choosing a Run Mode

You can run the VPN Client in simple mode or in advanced mode. The default is advanced mode, although your network administrator might have configured simple mode as the default.

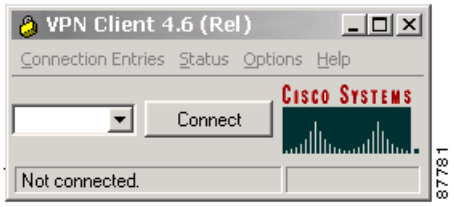
- Use simple mode if you want only to start the VPN Client application and connect to a VPN device using the default connection entry.
- Use advanced mode for the following tasks:
  - Managing the VPN Client
  - Configuring connection entries
  - Enrolling for and managing certificates
  - Viewing and managing event logging
  - Viewing tunnel routing data

To toggle between advanced mode and simple mode, press **Ctrl-M**. Alternately, you can choose a mode from the Options menu.

VPN Client Window—Simple Mode

In simple mode, you work with a scaled-down version of the VPN Client user interface (Figure 3-2).

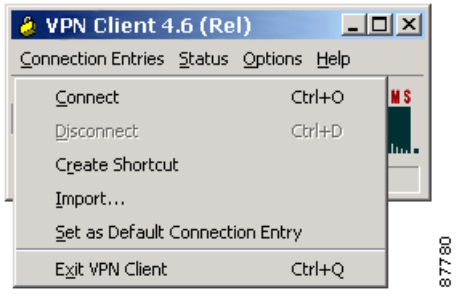
Figure 3-2 VPN Client Window—Simple Mode



The VPN Client main window shows the version information, the current connection entry, the connect button, and the status bar. Use the down arrow to display other connection entries.

- From the Connection Entries menu (Figure 3-3), you can
  - Connect to or disconnect from the connection entry shown in the box
  - Create a shortcut for the connection entry shown in the box
  - Import a new connection profile
  - Set the current connection entry as the default connection entry
  - Exit from the VPN Client

Figure 3-3 Simple Mode Connection Entries Menu



- From the Status menu, you can display notifications.
- From the Options menu, you can switch to Advanced Mode, and you can set the following preferences:
  - Save window settings—Saves any changes you make to the VPN Client window
  - Minimize upon connect—Places the VPN Client closed lock icon in the system tray when the VPN connection is established
  - Enable tool tips—Activates tool tips for the toolbar action buttons
  - Enable connect history display—Displays connection history information
  - Enable accessibility options—Places the VPN Client in the task bar rather than the system tray for easier access, and sounds a beep to indicate that a connection has been made
  - Enable connect on open—Connects to the default connection entry when you start the VPN Client (when you open or double click the VPN Client icon)

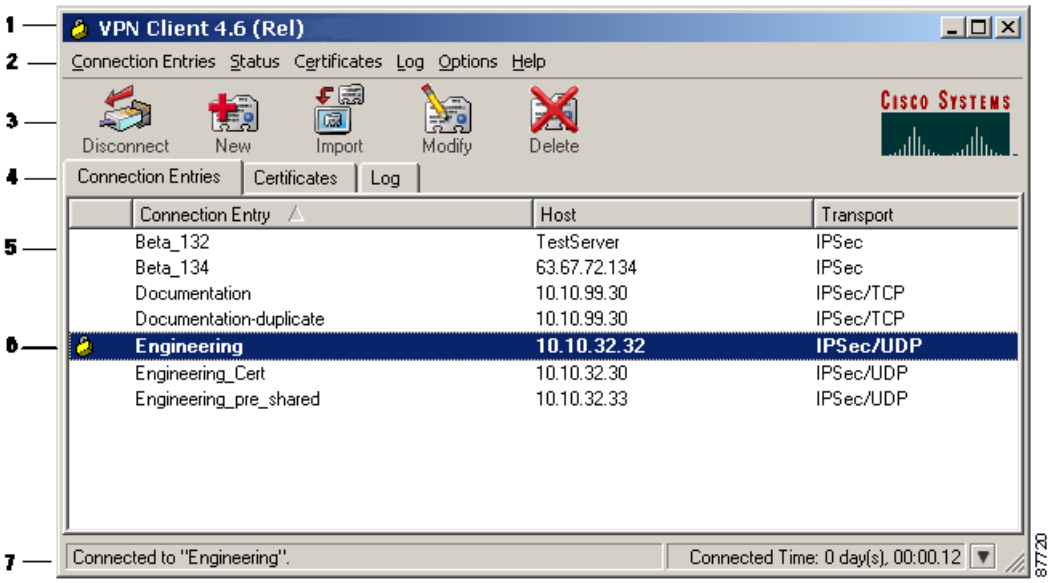
- From the Help menu, you can display context-sensitive, browser-based online Help.

VPN Client Window—Advanced Mode

The following sections describe the VPN Client main window in Advanced Mode, the primary buttons and tabs for navigating the user interface, the main menu options, and the right-click menu options.

Figure 3-4 shows the VPN Client window and the primary navigation areas.

Figure 3-4 VPN Client Main Window in Advanced Mode



1	VPN Client version information.	**5**	Display area for the main tabs.
2	Menu bar.	**6**	The currently active connection entry (if the Connection Entry area is showing).
3	Toolbar action buttons. The buttons that are available depend on which tab is forward.	**7**	Connection status bar. The left side of the status bar shows the connection entry name and connection status. When connected, the right side shows the connection time for this VPN session. Use the down arrow to display the number of bytes in and out, and the IP address of the VPN device.
4	Main tabs for managing the VPN Client.		

Toolbar Action Buttons—Advanced Mode

The action buttons at the top of the VPN Client window vary depending on which tab is forward.

- If the **Connection Entries** tab is forward, the Connect, New, Import, Modify, and Delete buttons control operations for the selected connection entry (Figure 3-4).
- If the **Certificates** tab is forward, the View, Import, Export, Enroll, Verify, and Delete buttons control operations for the selected certificate (Figure 3-5).

Figure 3-5 Toolbar Buttons—Certificates Tab

- If the **Log** tab is forward, the Disable, Clear, Log Settings, and Log Window buttons control the logging operations (Figure 3-6).

Figure 3-6 Toolbar Buttons—Log Tab

Main Tabs—Advanced Mode

This section describes the main tabs for managing the VPN Client (Figure 3-4).

The main tabs are:

- Connection Entries tab—Displays the list of current connection entries, the host, which is the VPN device each connection entry uses to gain access to the private network, and the transport properties that are set for each connection entry. Refer to "Configuring and Managing Connection Entries" for details on the Connection Entries tab.
- Certificates tab— Displays the list of certificates in the VPN Client certificate store. Use this tab to manage certificates. Refer to "Enrolling and Managing Certificates" for more details on the Certificates tab.
- Log tab—Displays event messages from all processes that contribute to the client-peer connection: enabling logging, clearing the event log, viewing the event log in an external window, and setting logging levels. Refer to "Managing the VPN Client" for more information.

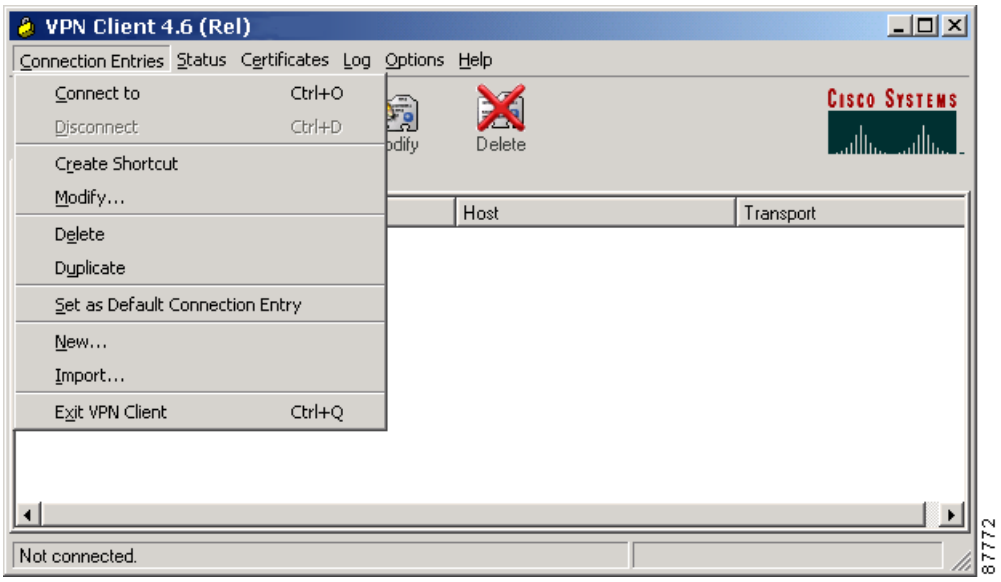
Menus—Advanced Mode

The following sections describe the VPN Client menus, located at the top of your screen, when the VPN Client application is active on your desktop.

Connection Entries Menu

Use the Connection Entries menu (Figure 3-7) as a shortcut to frequently-used connection entry operations.

Figure 3-7 Connection Entries Menu



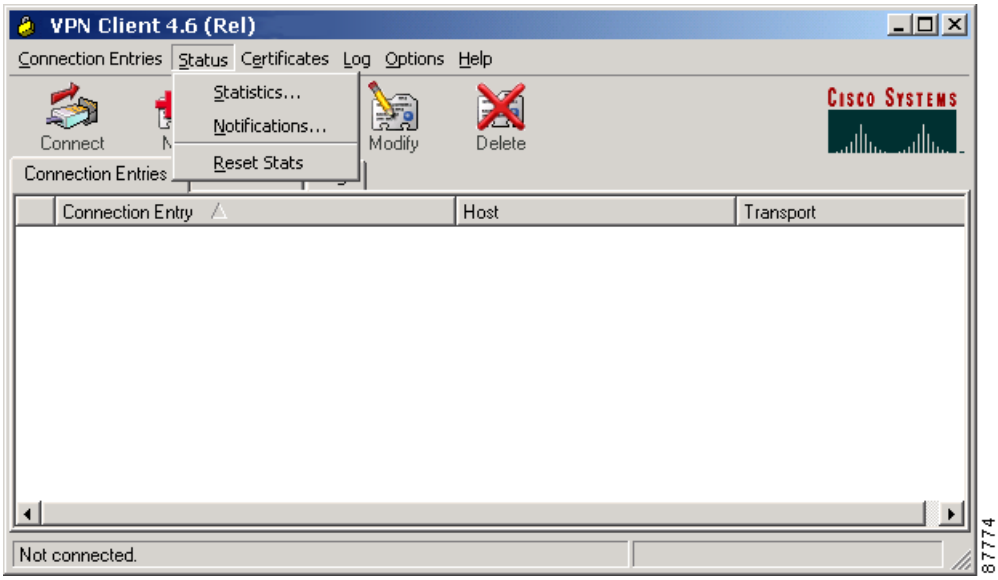
- Connect to—Connect to a VPN device using the selected connection entry. If the Connections tab is not selected, a submenu, which lists all available connection entries, is displayed.
- Disconnect—End your current VPN session.
- Create Shortcut—Create a shortcut on your desktop for the current connection entry.
- Modify—Edit the current connection entry.
- Delete—Remove the current connection entry.
- Duplicate—Make a copy of the selected connection entry. This menu choice lets you create a new connection entry using the configuration from a current connection entry as a template.
- Set as Default Connection Entry—Make the current connection entry the default.
- New—Create a new connection entry.
- Import—Bring in a new connection entry profile from a file.
- Exit VPN Client—Close the VPN Client application.

To configure a connection entry, see "Configuring and Managing Connection Entries".

Status Menu

Use the Status menu (Figure 3-8) to display routes and notifications, and to reset the statistics display.

Figure 3-8 Status Menu

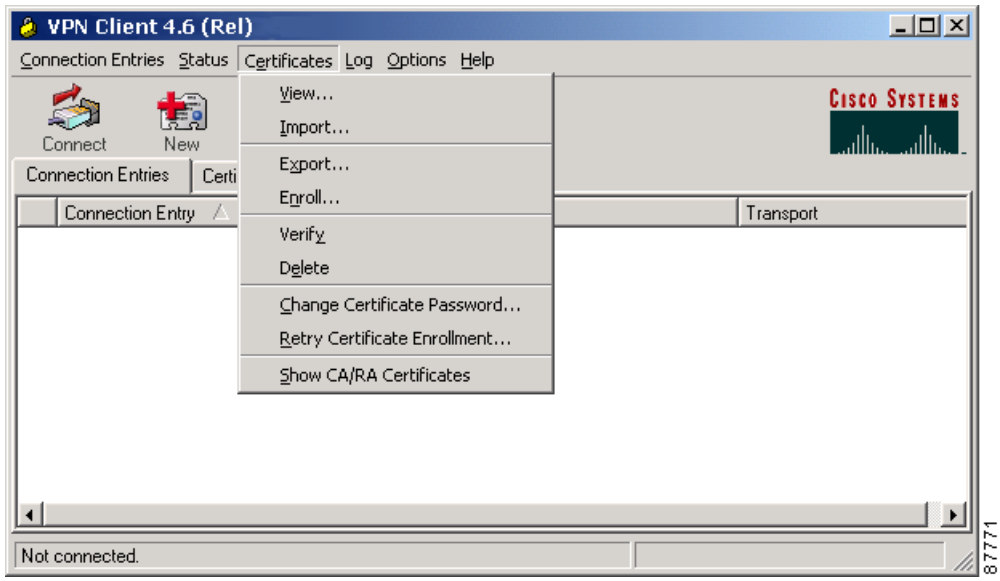


- Statistics—View tunnel details, route details and firewall information for the current VPN session.
- Notifications—View notices from the VPN device you are currently connected to.
- Reset Stats—Clear the statistics from the statistics displays and start over.

Certificates Menu

Use the Certificates menu (Figure 3-9) to enroll and manage certificates.

Figure 3-9 Enrolling and Managing Certificates

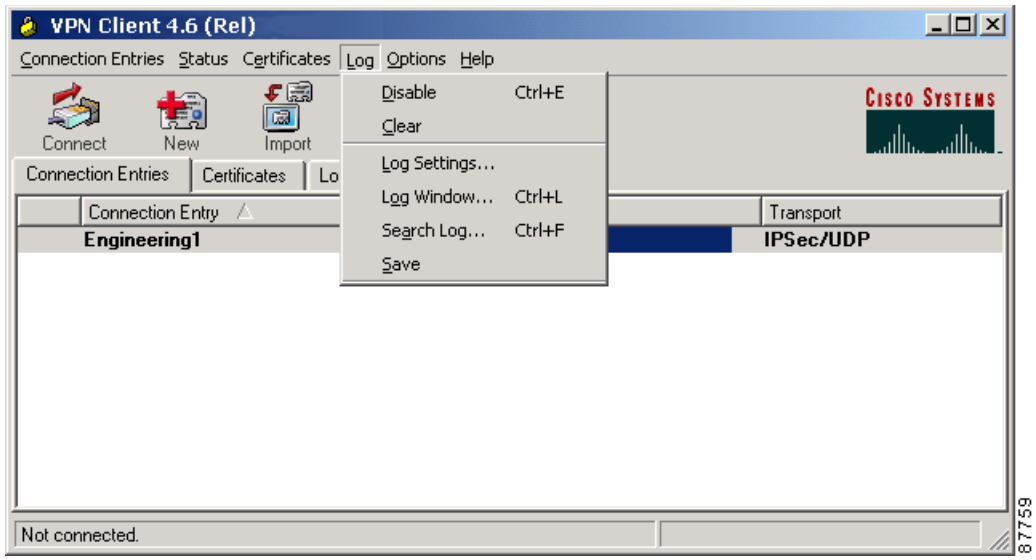


- View—Display the properties of the selected certificate.
- Import—Bring in a certificate file from a specified file location.
- Export—Send the selected certificate to a specified file location.
- Enroll—Sign up with a Certificate Authority (CA) to obtain a certificate.
- Verify—Make sure that a certificate is still valid.
- Delete—Remove the selected certificate.
- Change Certificate Password—Update the password that protects the selected certificate in the VPN Client certificate store.
- Retry Certificate Enrollment—Try a previously attempted certificate enrollment again.
- Show CA/RA Certificates—Display digital certificates issued by either a Certificate Authority (CA) or a Registration Authority (RA).

Log Menu

Use the Log menu (Figure 3-10) to manage the log.

Figure 3-10 Managing the IPSec Log

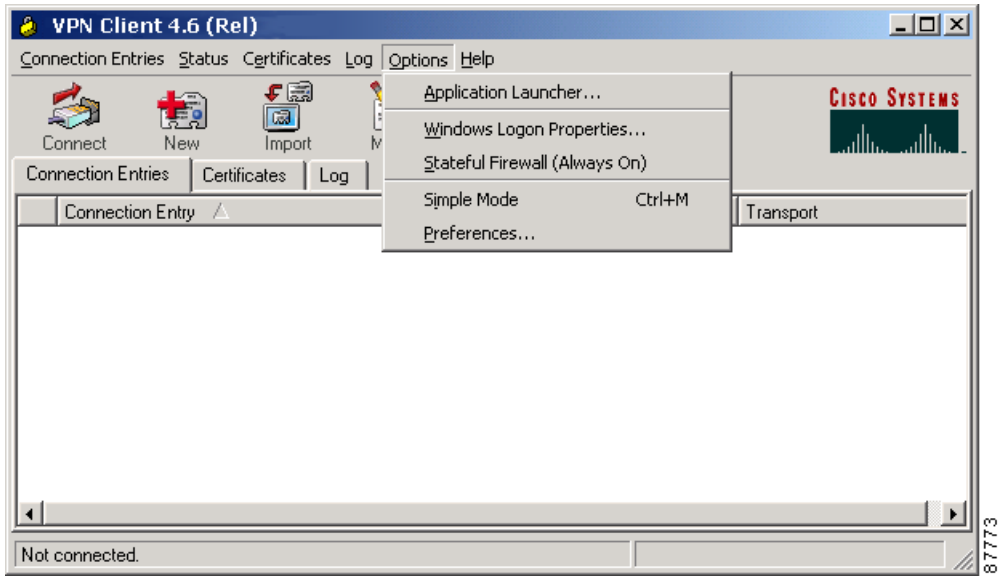


- Enable/Disable—Start collecting events (Enable); stop collecting events (Disable).
- Clear—Erase the events displayed on the log tab (and log window).
- Log Settings—Change the logging levels of event classes.
- Log Window—Bring up a separate window that displays events. From this window you can save the display, edit logging levels by event class, and clear both log displays. The window shows more events than the display area of the main advanced mode window.
- Search Log—Bring up a dialog box into which you enter the exact string to be matched. The search string is not case-sensitive, and wildcards are not supported. Matched instances are highlighted on the log tab, not the log window.
- Save—Store the current log in a specified log file.

Options Menu

Use the Options menu to perform various actions such as launching an application. Figure 3-11 shows the choices available from the Options menu.

Figure 3-11 Controlling VPN Client Options



- Application Launcher—Start an application before connecting to a VPN device.
- Windows Logon Properties—Control logon features for the Windows NT platform:
  - 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 of auto-disconnect behavior when logging off
- Stateful Firewall (Always On)—Enable/disable the internal stateful firewall.
- Simple Mode—Switch to simple mode.
- Preferences—Set the following features:
  - Save window settings—Save any changes you make to the VPN Client window
  - Hide upon connect—Place the VPN Client window in the dock when the VPN connection is established
  - Enable tool tips—Enable tool tips for the toolbar action buttons
  - Enable connect history display—Enable the display of connection history information
  - Enable accessibility options—Activate 508 accessibility features on the VPN Client graphical user interface
  - Enable connect on open—Causes the VPN Client to connect to the default profile when it activates

Right-Click Menus

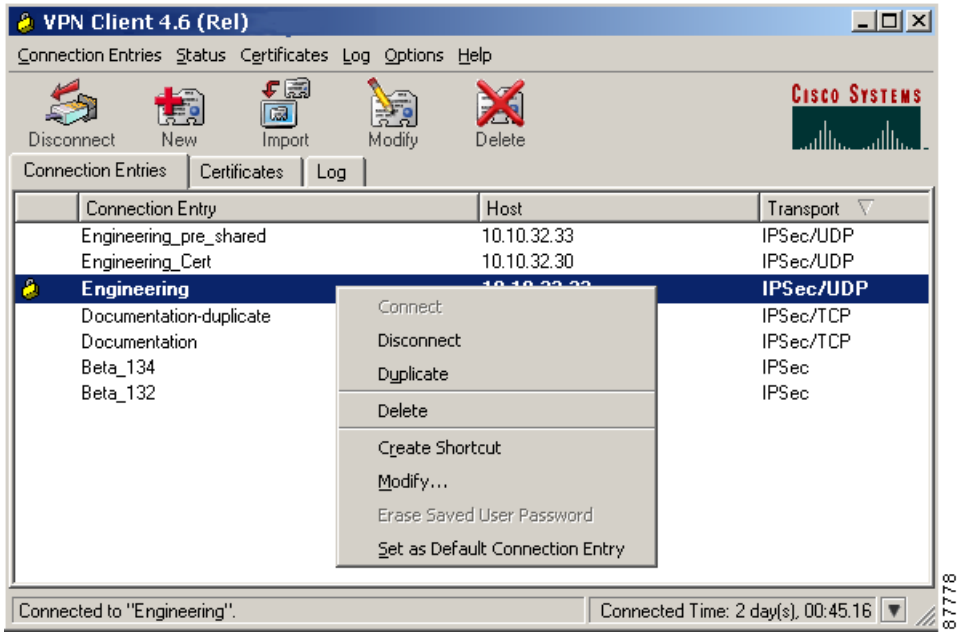
Use the right-click Menus from the Connection Entries tab, the Certificates tab, or the Log tab for frequently performed operations. The sections that follow introduce the features you can use from right-click menus for the following operations:

- Connection entries
- Certificates
- Log

Connection Entries Tab Right-Click Menu

Figure 3-12 shows the right-click menu options available when a connection entry is highlighted on the Connection Entries tab display.

Figure 3-12 Connection Entries Right-Click Menu



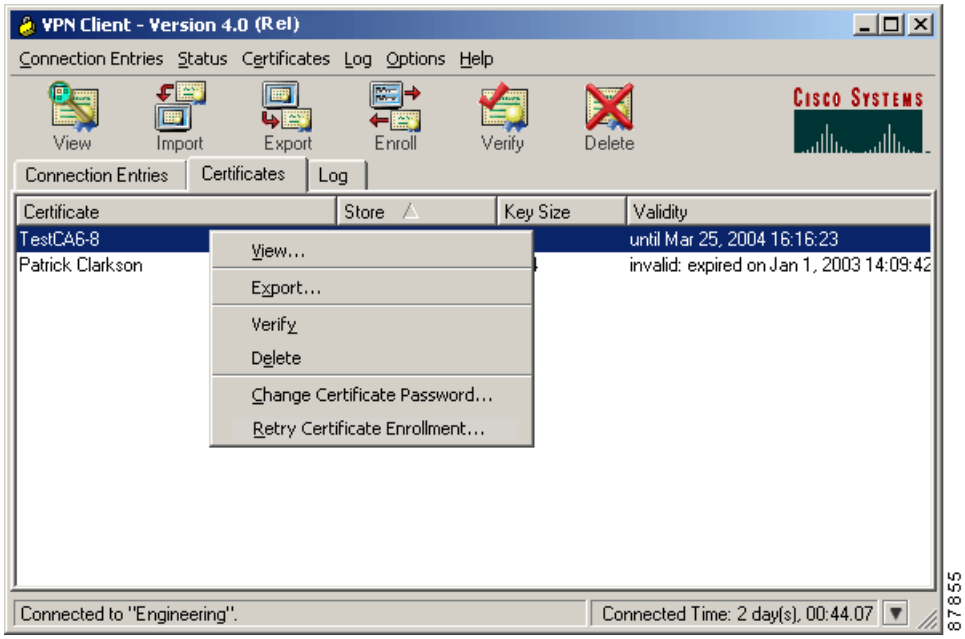
- Connect—Use the selected connection entry to connect to a VPN device.
- Disconnect—End the current VPN session.
- Duplicate—Made a copy of the selected connection entry. This action allows you to create a new connection entry using the configuration from a current connection entry as a template.
- Delete—Erase the selected connection entry.
- Create Shortcut—Place a link to the connection entry on your desktop.
- Modify—Edit the properties of the current connection entry (for example, its name, hostname, and so on).

- Erase Saved User Password—Delete the user password that is saved on the VPN Client workstation, forcing the VPN Client to prompt you for a password each time you establish a connection.
- Set as Default Connection Entry—Use the selected connection entry as the default.

Certificates Tab Right-Click Menu

Figure 3-13 shows the right-click menu options available when the Certificates tab is forward and a certificate entry is highlighted.

Figure 3-13 Certificates Tab Right-Click Menu

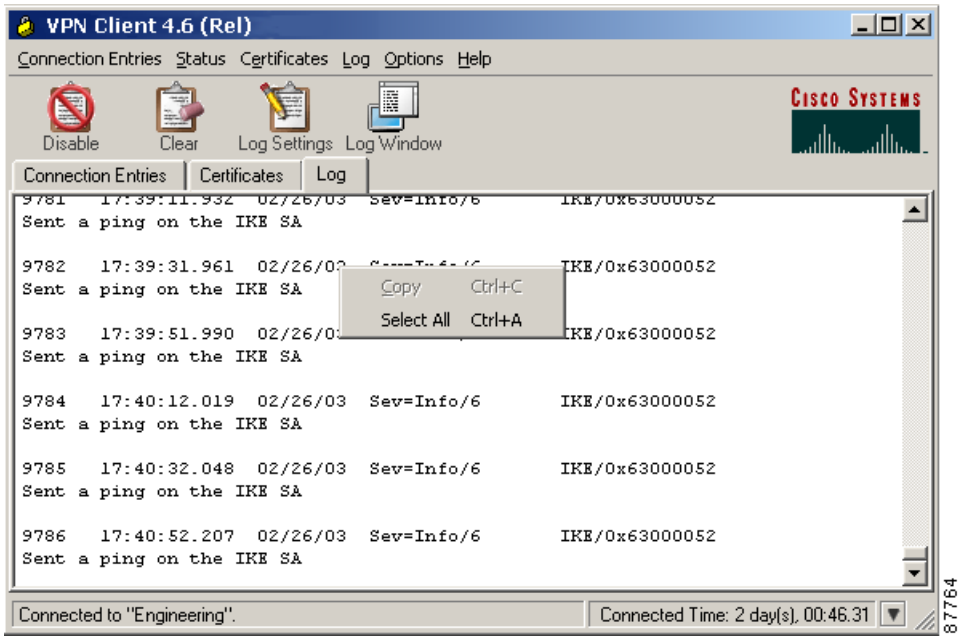


- Verify—Make sure that the selected certificate is valid.
- View—Look at the properties of the selected certificate.
- Delete—Erase the selected certificate.
- Export—Send the selected certificate to a specified file location.
- Change Certificate Password—Update the password that protects the certificate in the VPN Client certificate store.
- Retry Certificate Enrollment—try a previous certificate enrollment again.

Log Tab Right-Click Menu

Figure 3-14 shows the right-click menu options available when the Log tab is forward.

Figure 3-14 Log Tab Right-Click Menu



- Cut—Removes the selected item from the current context and saves a copy to the clipboard.
- Select All—Selects the entire contents of the log file, usually in preparation for another operation.

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**. This method displays the entire help file beginning with a list of topics.
- Press **F1** at any window while using the VPN Client. This method displays context-sensitive information.
- Click the **Help** button on windows that display it. This method displays context-sensitive information.
- Choose **Help VPN Client** from the menu that appears when you click the Help menu in the Menu bar.

Determining the VPN Client Version

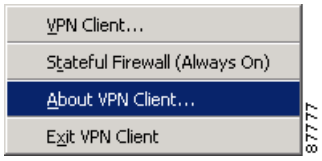
You can determine the version of the VPN Client and the VPN Client type from the system tray or from the Help menu.

- From the system tray:

Step 1 Right-click the closed padlock icon.

Step 2 Choose **About VPN Client** from the menu shown in Figure 3-15.

Figure 3-15 Displaying Version from Right-Click Menu



Note The menu you see when you are not connected differs from the menu that displays when the connection is active, but you can display version information from both menus.

- From the Help menu as follows:

Step 1 Click **Help**.

Step 2 Select **About VPN Client**.

Configuring and Managing Connection Entries

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

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

This chapter explains the following configuration tasks:

What Is a Connection Entry?

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

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

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

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

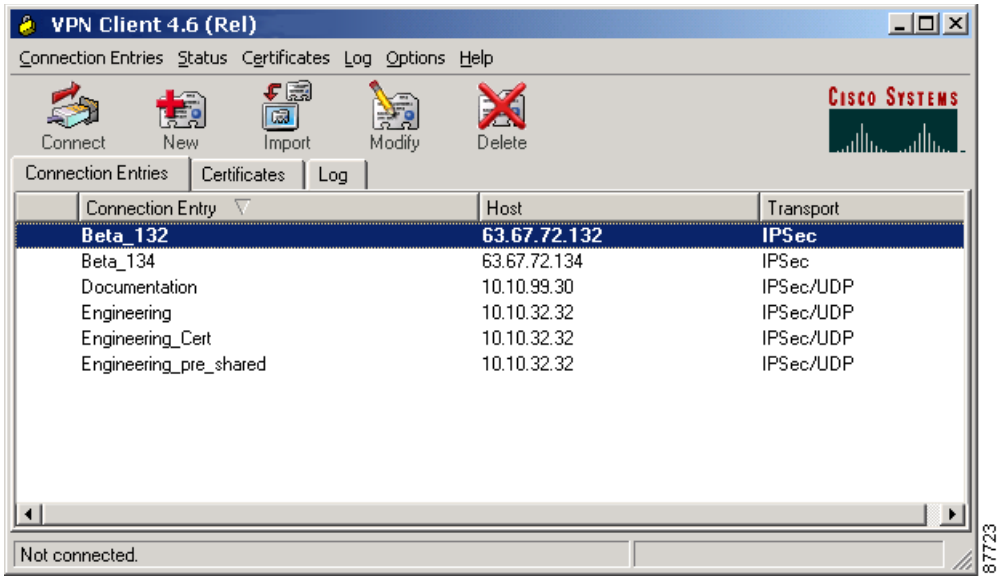
Creating a New Connection Entry

Use the following procedure to create a new connection entry.

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

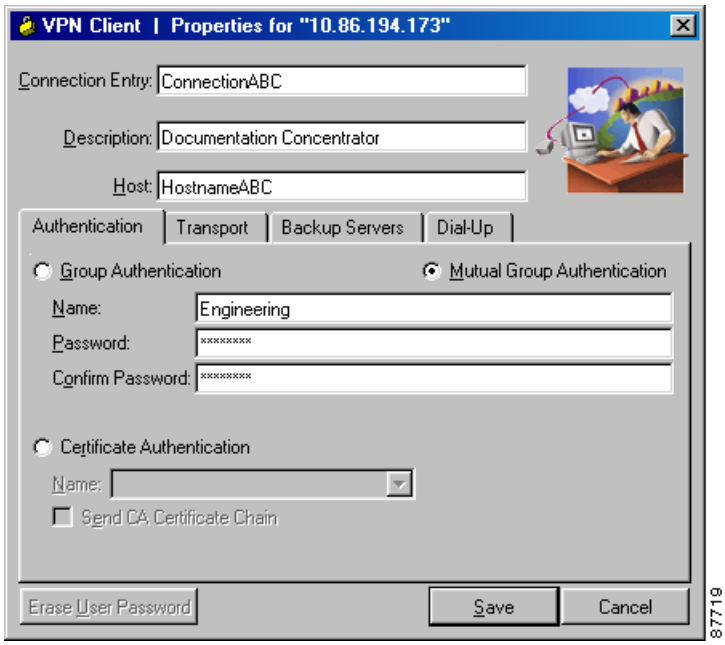
Step 2 The VPN Client application starts and displays the advanced mode main window (Figure 4-1). If you are not already there, open the Options menu in simple mode and choose **Advanced Mode** or press **Ctrl-M.**

Figure 4-1 VPN Client Main Window.



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

Figure 4-2 Creating a New Connection Entry



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

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

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

Choosing an Authentication Method

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

Group Authentication

Your network administrator usually configures group authentication for you. If this is not the case, use the following procedure:

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

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

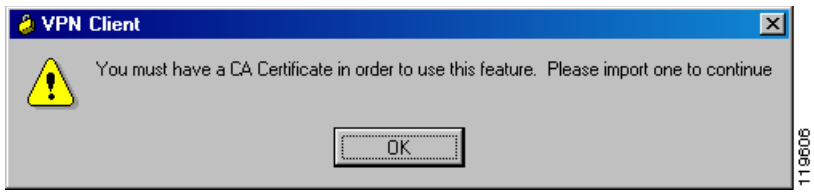
Step 3 In the Password field, enter the password (which is also case-sensitive) for your IPSec group. The field displays only asterisks.

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

Mutual Group Authentication

To use mutual group authentication, you need a root certificate that is compatible with the central-site VPN installed on your system. Your network administrator can load a root certificate on your system during installation. When you select mutual group authentication, the VPN Client software verifies whether you have a root certificate installed. If not, it prompts you to install one.

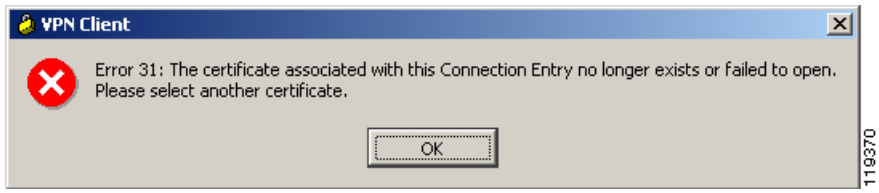
Figure 4-3 Mutual Group Authentication Prompt



Before you continue, you must import a root certificate. For information on importing a certificate, see Importing a Certificate File.

When you have installed a root certificate (if required), follow the steps in Group Authentication.

If you delete the root certificate from the user profile and you try to connect without it, the VPN Client displays the following error message:



Certificate Authentication

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

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

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

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

Sending a Certificate Authority Certificate Chain

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

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

Example 4-1 CA Certificate Chains

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

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

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

Validating a Certificate

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

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

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

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

Configuring an Entrust Certificate for Authentication

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

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

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

Configuring a Connection Entry for a Smart Card

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

Smart Cards Supported

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

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

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

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

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

To disable this parameter, uncheck the check box.

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

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

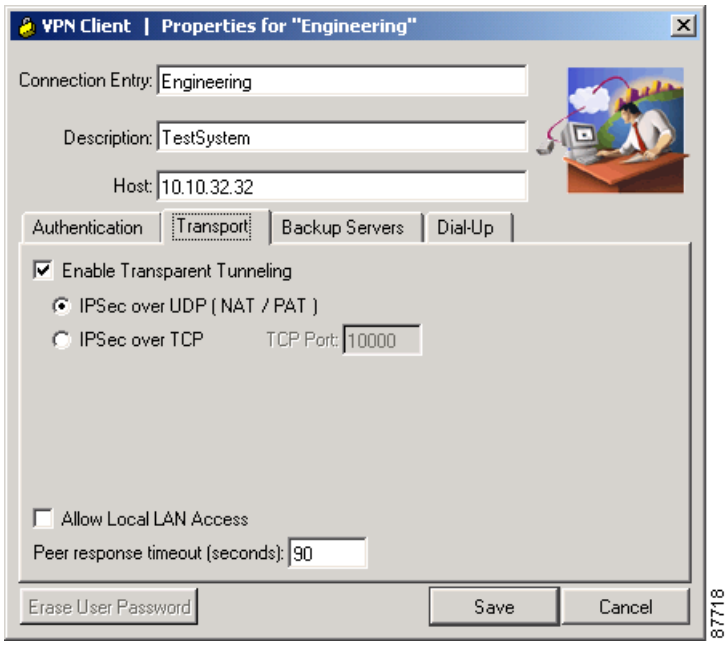
If you enable this parameter, click one of the radio buttons to choose the logon process:

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

Configuring Transparent Tunneling

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

Figure 4-4 Configuring Transport Parameters



Enabling Transparent Tunneling

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

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

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

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

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

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

Using IPSec over UDP (NAT/PAT)

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

Using IPSec over TCP (NAT/PAT/Firewall)

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

Allowing Local LAN Access

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

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

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

When this feature is enabled and configured on the VPN Client and permitted on the central-site VPN device, you can see a list of the local LANs available by looking at the Routes table. (See Figure 4-5.)

To display the Routes table, use the following procedure:

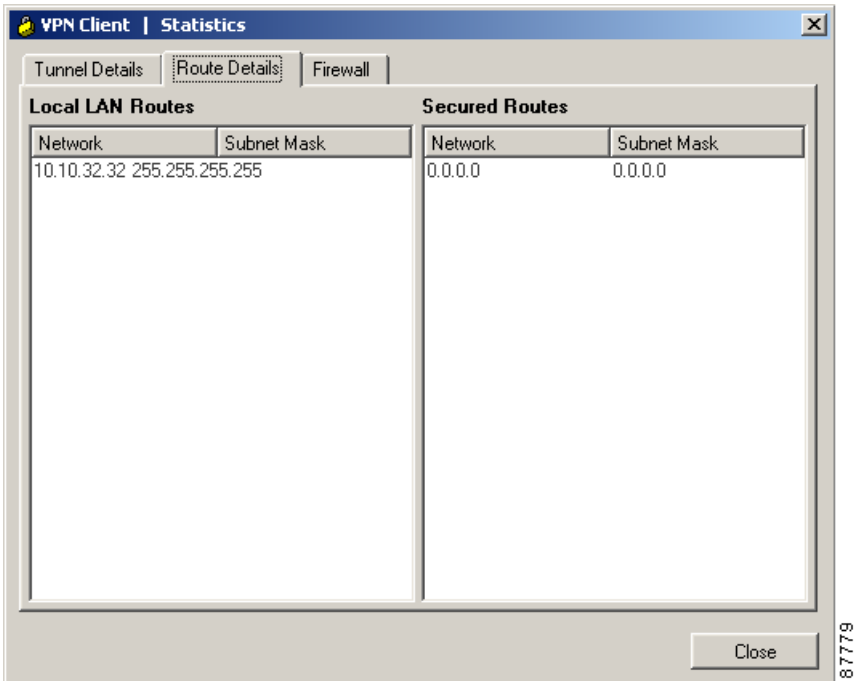
Step 1 Display the Status menu and choose **Statistics.**

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

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

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

Figure 4-5 Routes Table



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

Adjusting the Peer Response Timeout Value

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

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

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

Enabling and Adding Backup Servers

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

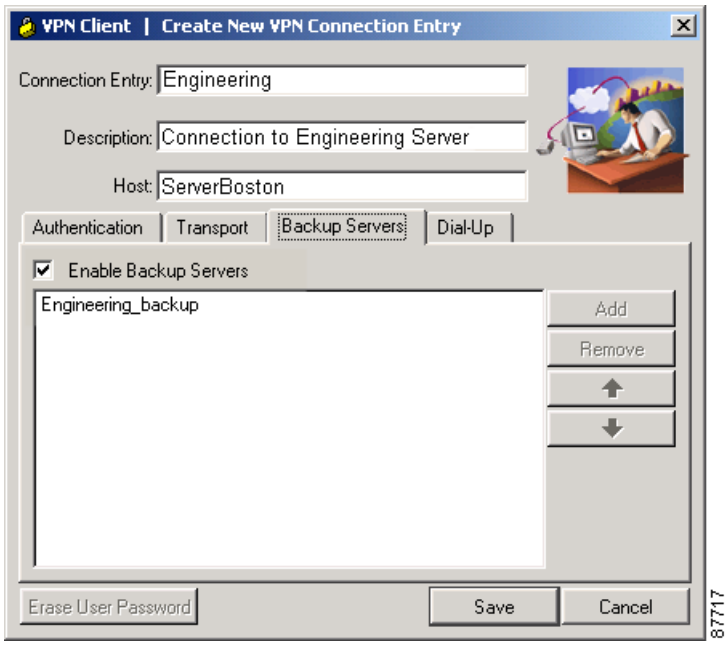
To enable backup servers from the VPN Client, use the following procedure:

Step 1 Open the Backup Servers tab (Figure 4-6).

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

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

Figure 4-6 Adding Backup Server Information



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

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

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

Removing Backup Servers

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

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

Changing the Order of the Servers

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

Disabling Backup Servers

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

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

Configuring a Connection to the Internet Through Dial-up Networking

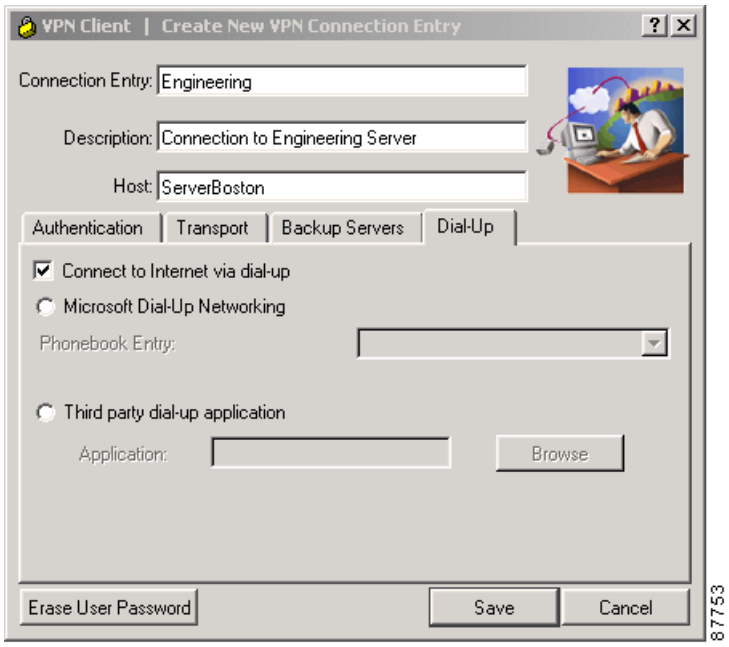
To connect to a private network using a dial-up connection, perform the following steps:

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

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

To enable and configure this feature, check the **Connect to the Internet via dial-up** check box. This feature is not checked by default. (See Figure 4-7.)

Figure 4-7 Connecting to the Internet Through Dial-up



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

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

Microsoft Dial-up Networking

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

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

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

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

Third Party Dial-up Program

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

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

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

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

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

Completing a Connection Entry

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

Setting a Default Connection Entry

If you have a default connection entry (also known as *default profile*) configured, the VPN Client opens the default connection entry when you launch it. To make one of your connection entries the default connection entry, use the following procedure:

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

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

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

Creating a Shortcut for a Connection Entry

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

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

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

The VPN Client places the shortcut on your desktop.

Duplicating a Connection Entry

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

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

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

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

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

a. Right-click on the new connection entry.

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

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

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

Modifying a Connection Entry

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

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

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

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

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

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

Deleting a Connection Entry

To delete a connection entry, use the following procedure:

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

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

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

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

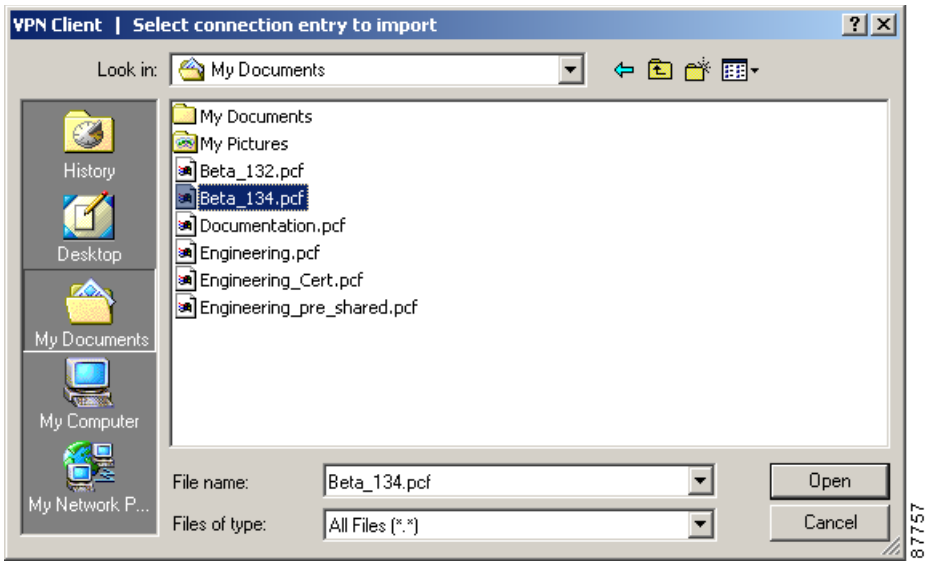
Importing a New Connection Entry

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

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

Step 2 Type the file name (a file with a .pcf extension) in the File Name box or browse to find the file you want to import (Figure 4-8).

Figure 4-8 Choosing a Profile to Import



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

Erasing a Saved Password for a Connection Entry

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

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

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

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

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

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

Step 3 Click **Erase User Password**.

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

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

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

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 and Managing Connection Entries." 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 (if necessary) 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 include the following sections:

Starting the VPN Client

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

The VPN Client displays the VPN Client's main window in either simple mode (Figure 5-1) or advanced mode (Figure 5-2), which is the default.

Figure 5-1 Connecting from Simple Mode

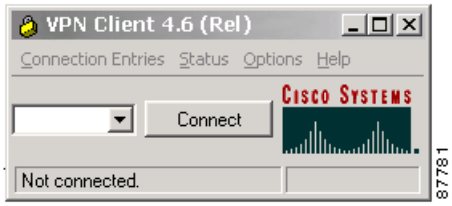
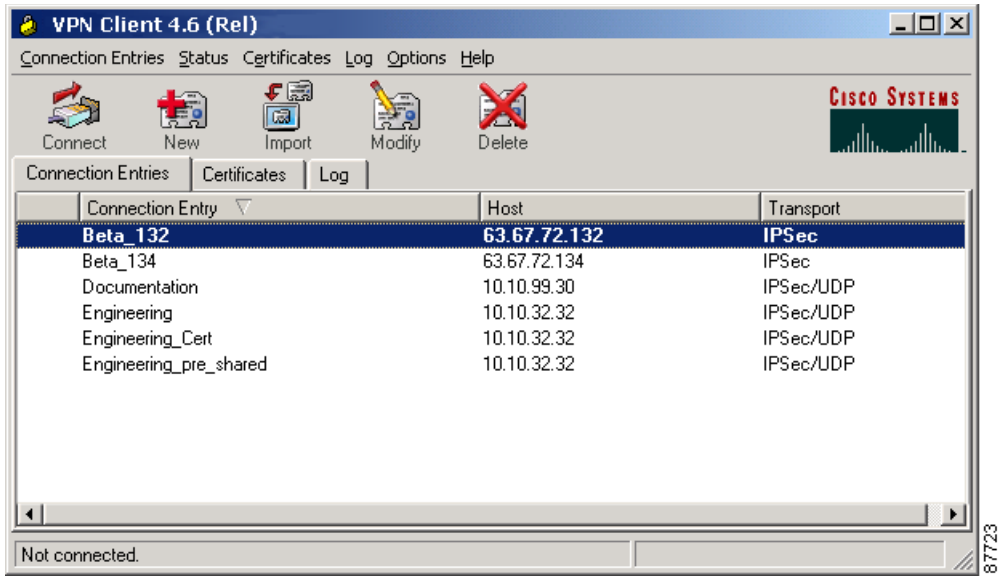


Figure 5-2 Connecting from Advanced Mode



Connecting to a Default Connection Entry

If you have configured a default connection entry (sometimes called *default user or default profile*), the VPN Client uses this connection entry when it starts. The name of this feature is *Connect on Open*. An administrator configures this feature for you. For information, see the *VPN Client Administrator Guide*. For information on setting a connection entry to be the default, see "Setting a Default Connection Entry".

Connecting from Simple Mode

To connect to a VPN device through simple mode, follow these steps:

Step 1 If necessary, click the drop-down menu showing connection entries and choose the desired connection entry.

Step 2 Click **Connect**. The VPN Client displays a window to ask for authentication information.

Step 3 Enter your authentication information; for example, your username and password. (See "Authentication Alternatives").

Connecting from Advanced Mode

To connect to a VPN device through advanced mode, follow these steps:

Step 1 Using advanced mode, you can connect in one of the following ways.

- Display the Connection Entries menu and choose **Connect**.
- Click the **Connect** icon on the tool bar above the Connection Entries tab.
- Double-click a connection entry in the list of connection entries.

Step 2 Enter your authentication information; for example, your username and password. (See "Authentication Alternatives")

Authentication Alternatives

To connect to a private network through the Internet, you must authenticate the connection request:

- 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."

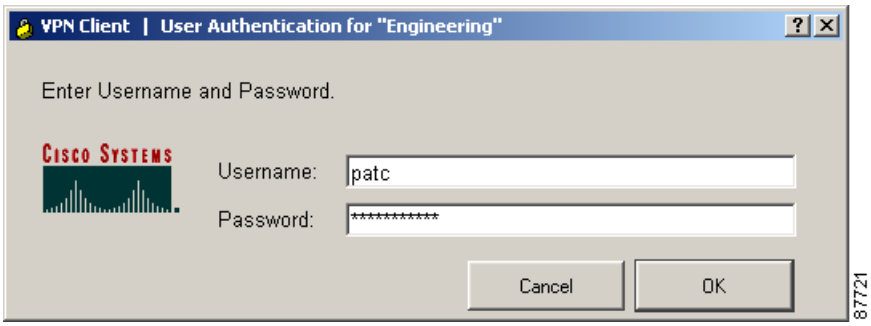
Using the VPN Client to Connect to the Internet via Dial-Up Networking

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 and Managing Connection Entries".

Step 1 Click **Connect** on the VPN Client's main window. (See Figure 5-1 and Figure 5-2.)

If your credentials are not stored in the RAS database, the Dial-up Networking User Information dialog box appears. (See Figure 5-3.) This dialog box varies, depending on the version of Windows you are using.

Figure 5-3 Entering User Information



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

Step 3 Click **OK**.

When the ISP connection is established, the status line on the Connection window changes to show that the status is "connected", and a Dial-Up Networking icon appears in the system tray on the Windows task bar. (See Figure 5-4.)

Figure 5-4 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 5-4.) If not, your Dial-Up Networking connection is not active, and you must establish it before continuing.

If you did not do so earlier, click **Connect** on the VPN Client's main window. (See Figure 5-1 or Figure 5-2.)

The VPN Client starts tunnel negotiation and displays the status in the Status area (bottom left of the window).

The next phase in tunnel negotiation is 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 window 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 window, perform the following steps. The title bar identifies the connection entry name.

Figure 5-5 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, go to advanced mode, and click **Erase User Password**.

Proceed to the section "Viewing Connection Information."

Authenticating Through a Windows NT Domain

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

Figure 5-6 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.

Note If you are connecting to a legacy server (that is, to a VPN 3000 Concentrator running a software version prior to Release 4.0), you might also be prompted for a domain name. If you see this field in the dialog box, enter your Windows NT Domain name in the Domain field, if it is not already there.

Step 3 Click **OK**.

Skip to "Viewing Connection Information."

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 window 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

These messages let you know the cause of your inability to log in. For help, contact your network administrator.

Authenticating Through RSA Data Security (RSA) SecurID (SDI)

RSA (formerly SDI) SecurID authentication methods include physical SecurID cards and keychain fobs, and SecurID PC software (formerly 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 window. The title bar identifies the connection entry name.

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

To display an authentication window asking for your username and passcode, perform the following steps. (See Figure 5-7.) If you are using SoftID, it must be running on your PC.

Figure 5-7 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 SecurID v2.0 (All Operating Systems)

If you are using SoftID version 1.x under Windows NT or SecurID version 2.0 under any operating system, the VPN Client displays an authentication window asking for your username and PIN. (See Figure 5-8.)

Figure 5-8 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 or SecurID PIN. The VPN Client gets the passcode from SoftID or SecurID by communicating directly with SoftID or SecurID. The SoftID or SecurID 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

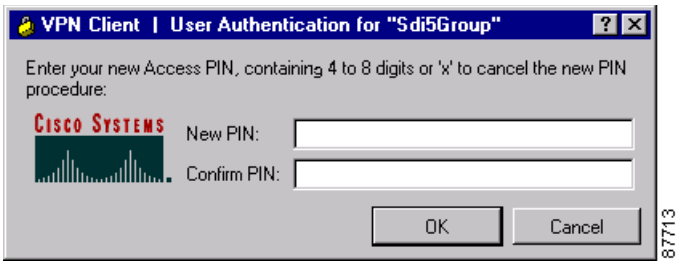
The first time you authenticate using SecurID or SoftID (all operating systems), or if you are using a new SecurID card, and if the RSA administrator allows you to create your own PIN, the authentication program asks if you want to create your own PIN. (See Figure 5-9.)

Figure 5-9 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 5-10.)

Figure 5-10 Entering a New PIN Yourself

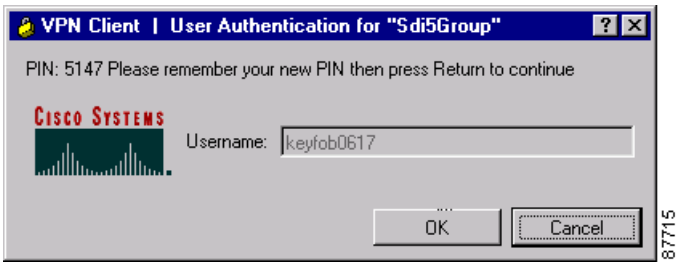


- If you responded no—the authentication program asks if you will accept a system-generated PIN. (See Figure 5-11.)

Figure 5-11 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 5-12.) Be sure to remember your PIN.

Figure 5-12 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 5-13. 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 window might appear. (See Figure 5-13.)

Figure 5-13 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 "Viewing Connection Information."

Connecting with Digital Certificates

Before you create 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 Web sites 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 verifies 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.

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

Note Because each certificate is associated with a connection profile, you can create different connection profiles with different certificates.

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 window, the Entrust logon window appears. (See Figure 5-14.)

Figure 5-14 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 5-15.

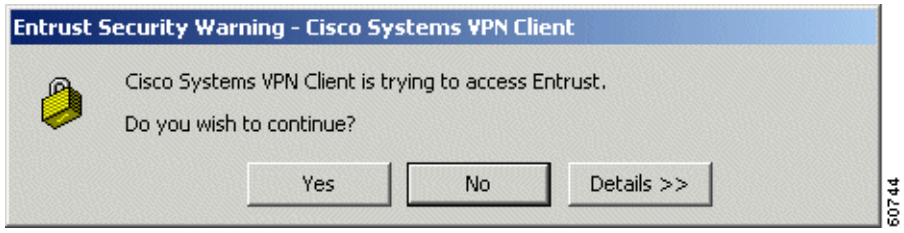
Figure 5-15 Entrust Login Message

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 window (see Figure 5-14), 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 5-16 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 window.

Step 2 Click **Ctrl Alt Delete**.

The Entrust Options window and the VPN Client login window both pop up. The VPN Client window is active.

Step 3 To start your VPN connection, click **Connect** on the VPN Client main window.

The Entrust login window becomes active.

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

The VPN Client password prompt window 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 window is active.

Step 6 To complete the connection, enter your Windows NT logon credentials in the Windows logon window, then 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. Several vendors 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.

Note Smart cards generally have only the private key associated with a certificate, so even without having the smart card inserted, you can still create an individual certificate-authentication profile. You must insert the smart card, however, to complete the authentication process.

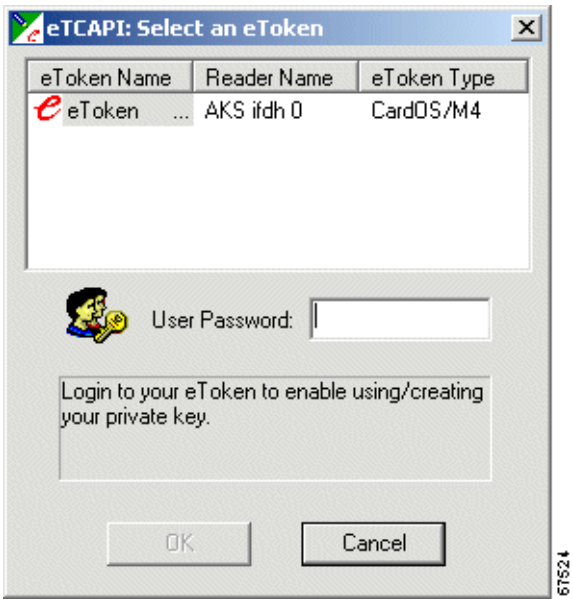
Once you or your network administrator has configured a connection entry that uses a Microsoft certificate provided by a smart card, you must insert the smart card into the receptor. When you start your connection, you are prompted to enter a password or PIN, depending on the vendor. For example, Figure 5-17 shows the authentication prompt from ActivCard Gold.

Figure 5-17 ActivCard Gold PIN Prompt

In this 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 5-18 eToken Prompt



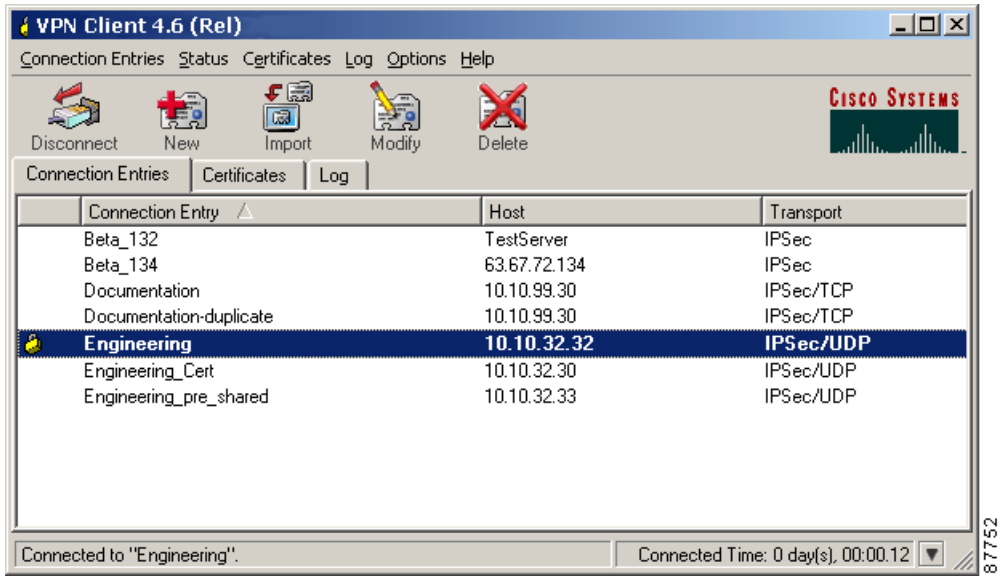
Note If your smart card or token is not inserted, the authentication program displays an error message. If this occurs, insert your smart card or token and try again.

Completing the Private Network Connection

After completing the user authentication phase, the VPN Client continues negotiating security parameters and displays a window. The connection entry display now indicates which connection entry is active. In Figure 5-19, a yellow lock icon indicates the Engineering connection entry is active and the

status line shows Connected to “Engineering”. Clicking the down arrow icon at the lower-right corner of the status line toggles a statistics display to show, in turn, the connect time, bytes in and out, and the IP address.

Figure 5-19 Completing the Private Network Connection



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 a closed-lock icon in the system tray on the Windows task bar.

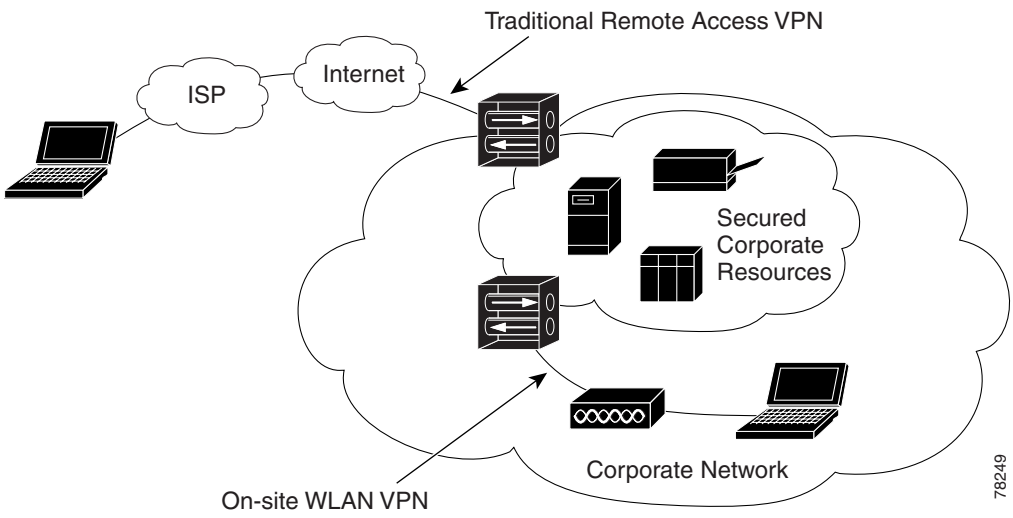
You are now connected securely to the private network via a tunnel through the Internet, and you can access the private network as if you were an onsite user.

Using Automatic VPN Initiation

Your VPN Client can automatically initiate a VPN connection based on the network to which your machine is connected. This feature is called *auto initiation* for on-site Wireless LANs (WLANs). Auto initiation makes the user experience resemble a traditional wired network in which VPNs secure WLANs. These environments are also known as WLANs.

On-site WLAN VPNs are similar to remote access VPNs with an important distinction. In an on-site wireless VPN environment, enterprise administrators have deployed wireless 802.11x networks in corporate facilities, and these networks use VPNs to secure the wireless part of the network link. In this case, if your PC is on a WLAN without VPN, you cannot access network resources. If a VPN exists, your access is similar to what it is with wired Ethernet connections. Figure 5-20 shows the two different types of VPN access.

Figure 5-20 Remote Access VPN Versus On-Site Wireless Access VPN



In your connection profile, your network administrator can configure a list of up to 64 matched networks (address/subnet masks) and corresponding connection profiles (.pcf files). When the VPN Client detects that your PC's network address matches one of the address/subnet mask pairs in the auto initiation network list, it checks whether the network administrator has configured that profile to allow (the default) or prohibit auto initiation. If auto initiation is allowed, the VPN Client automatically establishes a VPN connection using the matching profile for that network.

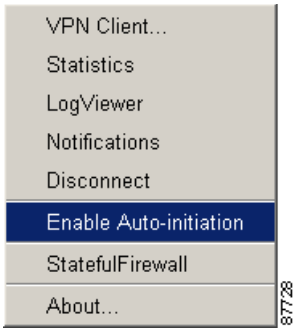
While auto initiation is primarily for an on-site WLAN application, you can also use auto initiation in any situation based on the presence of a specific network. For example, in your home office, you may want to create an entry for your VPN to auto initiate from your corporate PC whenever you are connected to your home network, whether that network is a wireless or a wired LAN.

The VPN Client lets you know when your connection is auto initiating and informs you of various stages in the process of an auto initiated connection. You can suspend, resume, disconnect or disable auto initiation. When you disconnect or the connection attempt fails, the VPN Client automatically retries auto initiation using a configured interval called the retry interval. From The VPN Client Options menu, you can disable auto initiation, and you can change the interval between connection attempts.

Enabling Automatic VPN Initiation

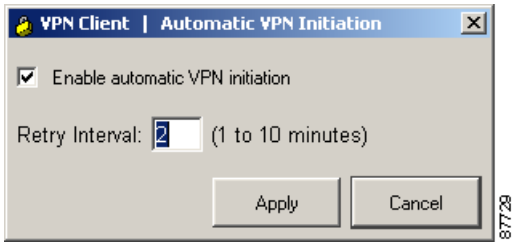
After you have established a connection, right-click the yellow lock icon in the system tray and select Enable Auto-initiation from the menu that appears (see Figure 5-21).

Figure 5-21 Enabling Auto Initiation



The VPN Client displays a dialog box (Figure 5-22) asking whether you want to enable auto initiation and asking you to specify the number of minutes between retries.

Figure 5-22 Auto Initialization Dialog



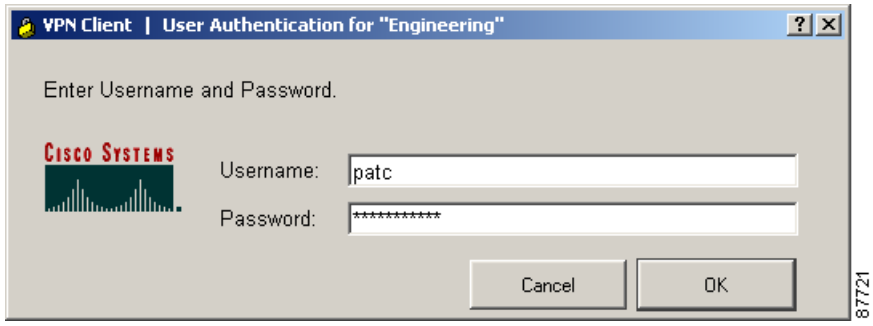
Check the check box to enable auto initiation and specify an retry interval ranging from 1 to 10 minutes. After you have enabled auto initiation, if you close or lose your connection, auto initiation automatically attempts to reconnect at the specified interval until you exit the VPN Client, or disable or suspend auto initiation.

Connecting Through Automatic VPN Initiation

Typically when you start your wireless system (normally, a laptop), your connection initiates automatically. You do not see the VPN Client's main dialog. As the connection goes forward, the VPN Client displays a sequence of screens.

The VPN Client also displays an authentication dialog, such as the one shown in Figure 5-23.

Figure 5-23 Authenticating Automatic VPN Initialized Connection



When you enter your authentication information, your connection starts immediately, as indicated by the closed yellow lock icon in the system tray.

Figure 5-24 Closed Lock—Connected

If your network administrator has defined a banner, you'll also see that banner displayed.

To cancel the connection attempt, click **Cancel Connect** on the toolbar. When you cancel the connection attempt, the VPN Client displays a message requesting you to confirm the cancellation.

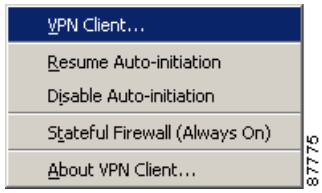
To cancel, click **No**. The Log tab or Log Window shows the event log message "Connection canceled."

To suspend auto initiation, right-click the yellow lock icon in the system tray and select **Suspend Auto-initiation** from the menu. In the event log, you see the message "Auto-initation has been suspended". When suspended, also in the system tray, you see that the yellow lock icon is now open.

Figure 5-25 Open Lock—Suspended Auto Initiation

To resume auto initiation after suspending, right-click on the open yellow lock icon and select **Resume Auto-initiation** from the menu.(See Figure 5-26.)

Figure 5-26 Resuming Auto Initiation

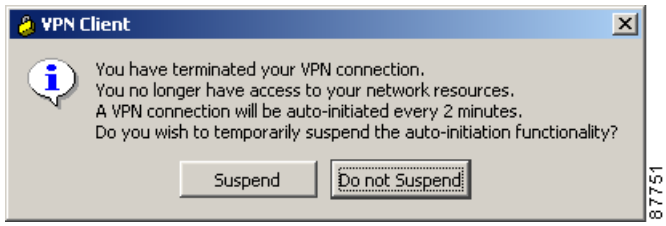


Auto initiation resumes. This is the simplest scenario of what happens during auto initiation. At various points, depending on the actions you take, you see messages, changes in the color of the icon in the system tray, and differences in choices you can make. The rest of this section describes these various alternatives.

Disconnecting Your Session

To disconnect your session, either double-click the lock icon in the system tray and click the **Disconnect** button or right-click the lock and select **Disconnect** from the menu (in the standard way). The VPN Client displays the following message. (See Figure 5-27.)

Figure 5-27 Disconnecting Your Session



To suspend auto initiation, click **Yes**. Auto initiation suspends until you resume it, disable it, or log off.

When you click **No**, auto initiation stays in effect and the VPN Client automatically retries auto initiation according to the retry interval; for example, every minute.

Changing Option Values While Auto Initiation is Suspended

When auto initiation is suspended, you can change VPN Client options as follows:

Step 1 Double-click yellow lock icon in the system tray.

Step 2 Click **Options**. The VPN Client displays the Options menu.

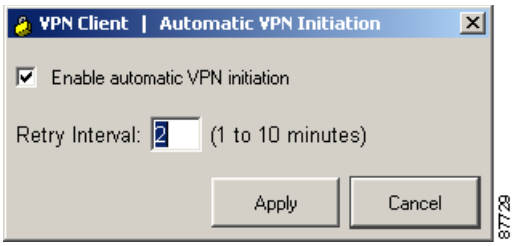
Disabling Automatic VPN Initiation

To completely shut down auto initiation, you can disable it through the Options menu by following these steps:

Step 1 Display the VPN Client main window and click **Options**.

Step 2 Select **Automatic VPN Initiation**. The VPN Client displays the window shown in Figure 5-28.

Figure 5-28 Setting Auto Initiation Parameters



Step 3 Click to remove the check mark from **Enable** and click **OK**. The log displays a message, "Auto-initiation has been disabled," and auto initiation terminates.

Note Unchecking Enable does not remove Automatic VPN Initiation option from the Options menu. This option always shows up in the menu as long as the feature has been configured by your network administrator.

Disabling While Suspended

Alternatively, when auto initiation is suspended and you want to disable it, follow these steps:

Step 1 Right-click the yellow lock icon in the system tray.

Step 2 Select **Disable Auto-initiation**. The VPN Client displays a message asking whether you are sure that you want to disable auto initiation.

Step 3 To completely disable auto initiation and eliminate further automatic retries, click **Yes**. To cancel the action and keep auto initiation enabled, click **No**.

Restarting After Disabling Automatic VPN Initiation

When you want to restart auto initiation, follow these steps:

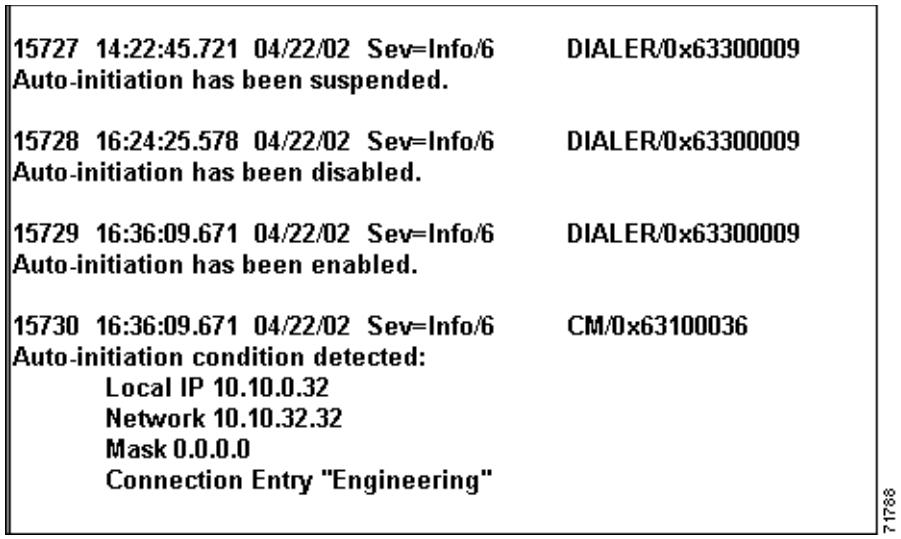
Step 1 Launch the **VPN Client** from the Start > Programs > Cisco Systems VPN Client menu.

Step 2 Click **Options**.

Step 3 Select **Automatic VPN Initiation**.

Step 4 Check the **Enable** check box, set the retry interval, and click **OK**. The log shows that auto initiation is now in effect. For an example, see Figure 5-29.

Figure 5-29 Auto Initation Log Messages

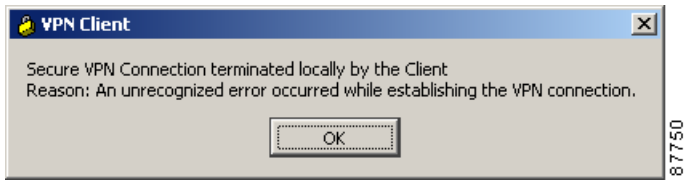


Step 5 Close the VPN Client dialog. The Authentication window displays.

Connection Failures

If the auto initiation attempt fails, the VPN Client notifies you with a dial status dialog and a warning message.

Figure 5-30 Auto Initiation Failure Message



Viewing Connection Information

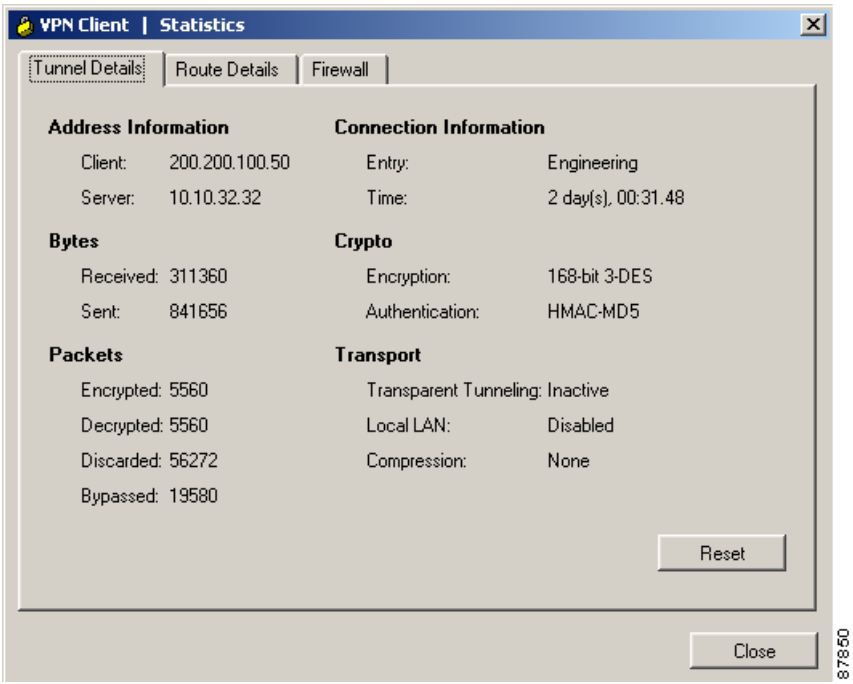
From the Status menu, you can view the following information about your private network connection:

- Tunnel details
- Routing information
- Firewall information
- Notifications

Viewing Tunnel Details

To display information about your IPSec tunnel, pull down the Status menu and choose **Statistics**. Then click the Tunnel Details tab. The VPN Client shows IP security information, listing the IPSec statistics for this VPN tunnel to the private network.

Figure 5-31 Viewing Tunnel Information



The statistics are the following:

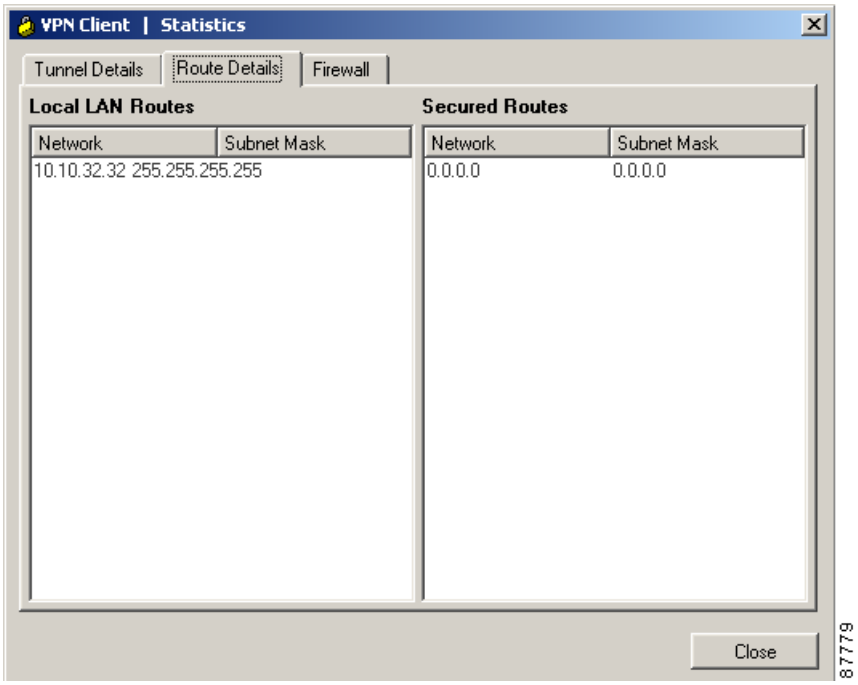
- Address Information:
  - Client IP address—The IP address assigned to the VPN Client for the current session.
  - Server IP address—The IP address of the VPN device to which the VPN Client is connected.
- Connection Information
  - Connection Entry—The name of the profile you are using to establish the connection.
  - Time—Length of time the connection has been up.
- Bytes
  - Received—The total amount of data received after a secure packet has been successfully decrypted.
  - Sent—The total amount of encrypted data transmitted through the tunnel.
- Crypto
  - 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.

- Packets
  - Packets encrypted—The total number of secured data packets transmitted out the port.
  - Packets decrypted—The total number of data packets received on the port.
  - Packets discarded—The total number of data packets that the VPN Client rejected because they did not come from the secure VPN device gateway.
  - 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.
- Transport
  - Transparent Tunneling—The status of tunnel transparent mode in the VPN Client, either active or inactive.
  - Local LAN Access—Whether access to your local area network while the tunnel is active is enabled or disabled. (For information on configuring this feature, see "Allowing Local LAN Access".)
  - 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.

Viewing Routing Information

To display routing information, pull down the Status menu and choose **Statistics**. Then click the **Route Details** tab.

Figure 5-32 Viewing Routing Information



In Figure 5-32, the columns show the following types of information.

Local LAN Routes

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.

- Network—The IP address of the excluded route.
- Subnet Mask—The subnet mask of the IP address for this route.

Secured Routes

The Secured Routes box shows the following information:

- Network—The IP address of the remote private network with which this VPN Client has a security association (SA).
- Subnet Mask—The subnet mask of the IP address for this SA.

Firewall Tab

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

Configuring the Firewall on the Concentrator

The VPN Concentrator's network manager specifies 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, and sets up the firewall policy under the Configuration | User Management | Base Group or Group | Client FW tab. The following firewall policy options exist:

- AYT (Are You There) enforces the use of a specific firewall but does not require you to have a specific firewall policy. The supported 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 (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. 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.

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

- Client/Server, corresponding to "Policy from Server" (Zone Labs Integrity) on the VPN Concentrator, 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.

Table 5-1 summarizes the policy options available for the various supported firewalls.

Table 5-1 Firewalls and Policy Options Summary

Firewall	Policy Options		
	AYT	Pushed (CPP)	From Server
Cisco Integrated Firewall		X	
Network Ice BlackICE Defender	X		
Zone Labs ZoneAlarm	X	X	
Zone Labs ZoneAlarm Pro	X	X	
Zone Labs ZoneAlarm or ZoneAlarm Pro	X	X	
Zone Labs Integrity			X
Sygate Personal Firewall	X		
Sygate Personal Firewall Pro	X		
Sygate Security Agent	X		
Cisco Intrusion Prevention Security Agent	X		
Custom Firewall	X	X	X

Viewing Firewall Information on the VPN Client

The Firewall tab displays information about the VPN Client's firewall configuration, including the firewall policy and the configured firewall product. The remaining contents of the Firewall tab depend on these two configured options.

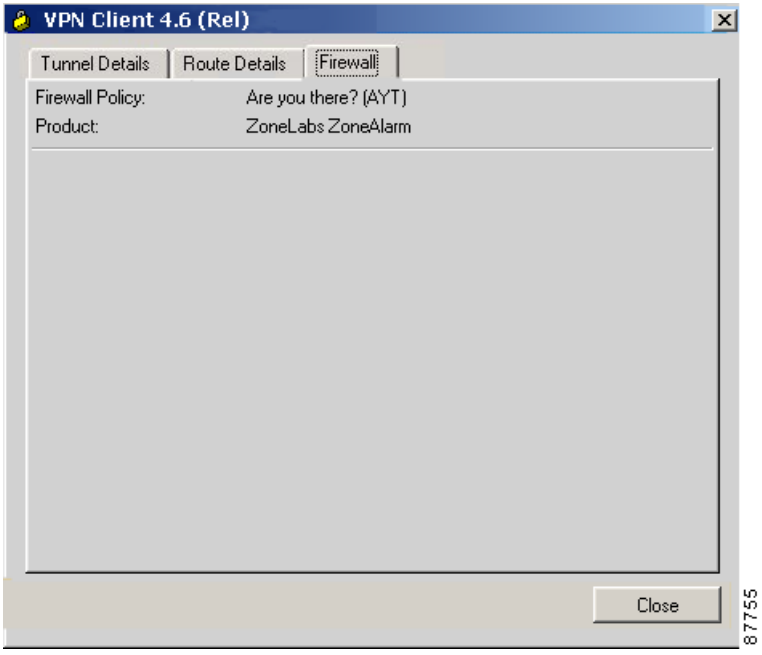
The information shown on this tab varies according to your firewall policy.

- 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 5-33). AYT enforces the use of a specific personal firewall but does not require you to have a specific firewall policy.
- 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 5-34).
- Client/Server—When the Client/Server is the supported capability, the Firewall tab displays 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 5-35).

AYT Firewall Tab

The Firewall tab shows that AYT is running and displays the name of the firewall product that supports AYT. AYT is used in conjunction with Cisco Intrusion Prevention Security Agent or Zone Labs Zone Alarm or Zone Alarm Pro to ensure that the firewall is enabled and running on a system, but not to confirm that a specific policy is enforced.

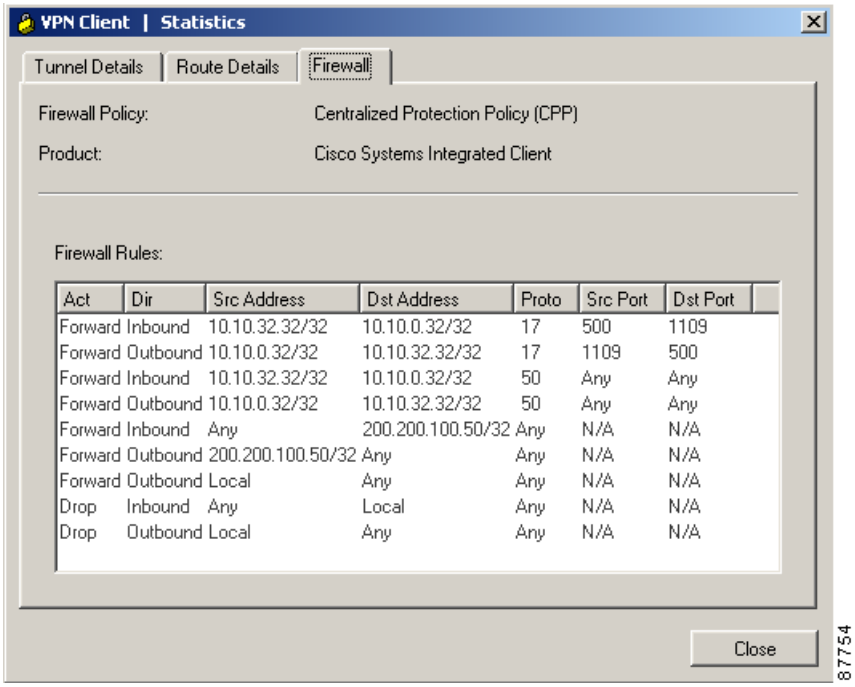
Figure 5-33 Firewall Tab for AYT capability



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. CPP sends down a stateful firewall policy for the integrated firewall in the VPN Client for use while connected with split tunneling. For CPP (see Figure 5-34), the Firewall tab shows you the firewall rules in effect.

Figure 5-34 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—The name of the firewall currently in use, such as Cisco Integrated Client, Zone Alarm Pro, and so on.
- Firewall Rules—Information about the firewall rules currently in effect, as described in the following section.

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 width; 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, the columns revert to their original width. 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 not match 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 5-34 displays the fields for the rule that is highlighted in the list.

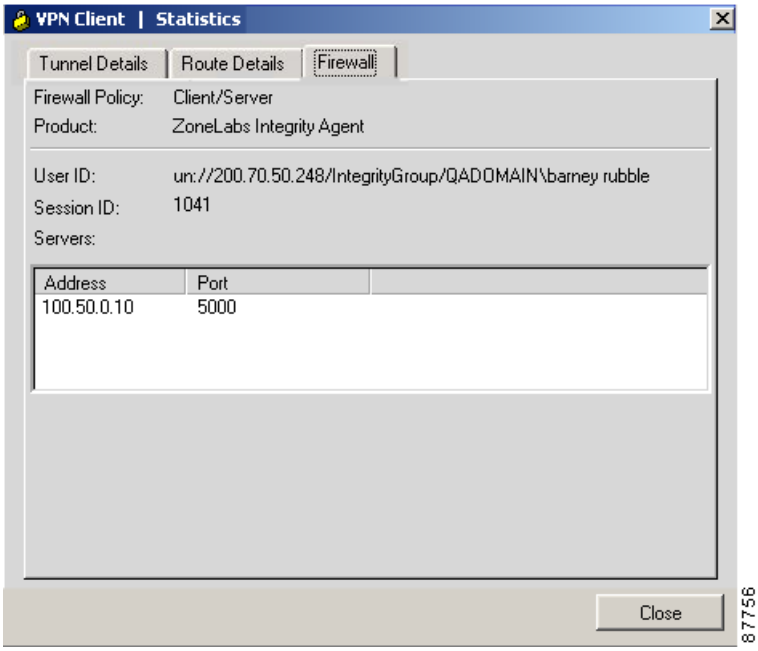
A firewall rule includes the following fields:

- 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 5-35). 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 5-35 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.

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 window.

Disconnecting your VPN Client Connection

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

- From the Connection Entries menu on the VPN Client's main window, select **Disconnect**. (See Figure 5-1.)
- Right-click the yellow lock icon in the system tray. Click **Disconnect** on the menu.

Your IPSec session ends, but the VPN Client does not automatically close. You must manually disconnect your dial-up networking connection (DUN).

Closing the VPN Client

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

- From the Connection Entries menu on the VPN Client's main window, select **Exit VPN Client**. (See Figure 5-1.)
- Press **CTRL+Q** on your keyboard.
- Press **Alt-F4** on your keyboard.

Enrolling and Managing Certificates

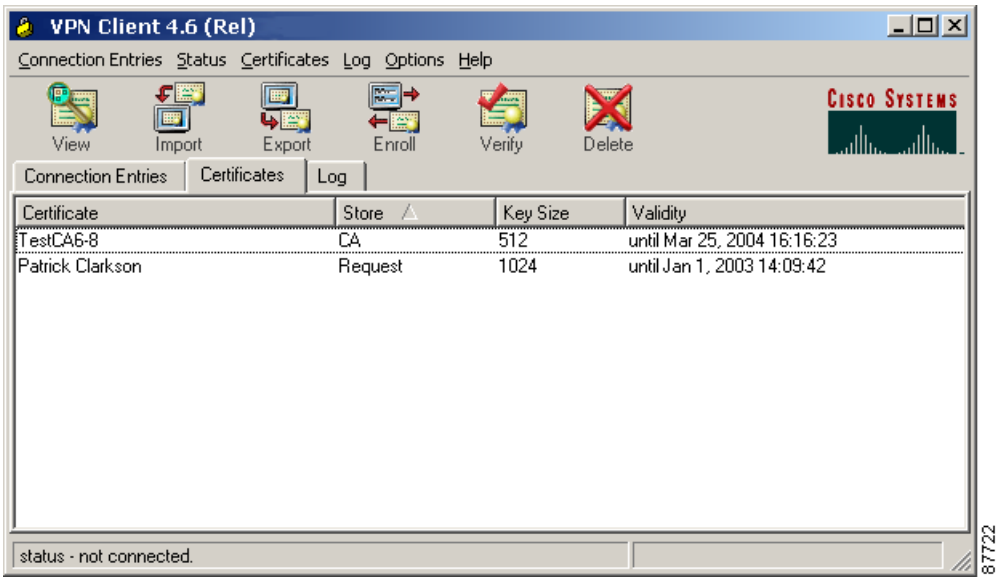
This chapter explains how to enroll and manage personal certificates, specifically, how to perform the following tasks:

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

This chapter includes the following sections:

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

Figure 6-1 Managing Certificates



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

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

Using Certificate Stores

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

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

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

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

- Certificate—The name of the certificate

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

Enrolling for a Certificate

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

Enrolling Through the Network

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

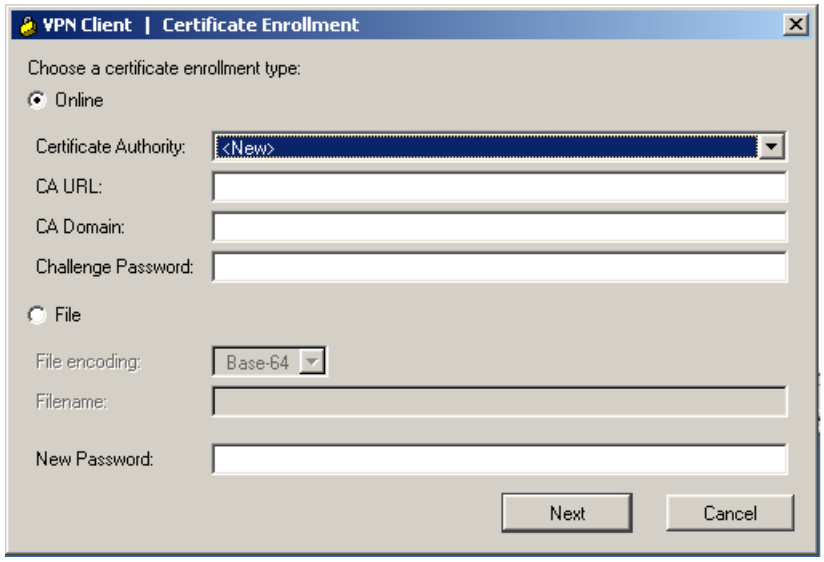
Use this section to gather the information before you begin. To enroll for a certificate with a CA over the network, follow this procedure:

Step 1 In advanced mode, either click the **Enroll** icon on the toolbar above the Certificates tab or display the Certificates menu and choose **Enroll**.

Step 2 Click **Online** as the certificate type. There are two forms to fill out.

Step 3 Fill out the first form (Figure 6-2) as follows.

Figure 6-2 Online Enrollment Form

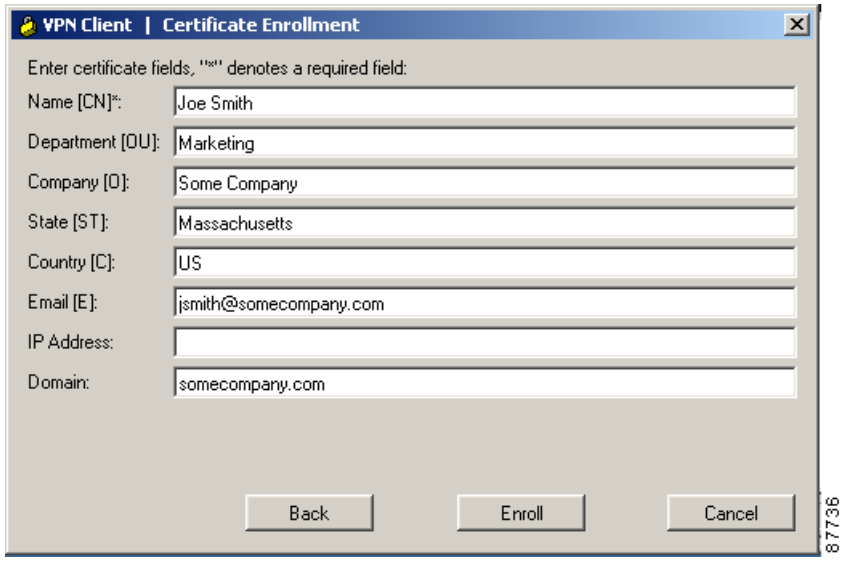


- CA URL—The URL or network address of the CA. This parameter is required.
- CA Domain—The CA's domain name. This parameter is required.

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

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

Figure 6-3 Online Enrollment Form Page Two



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

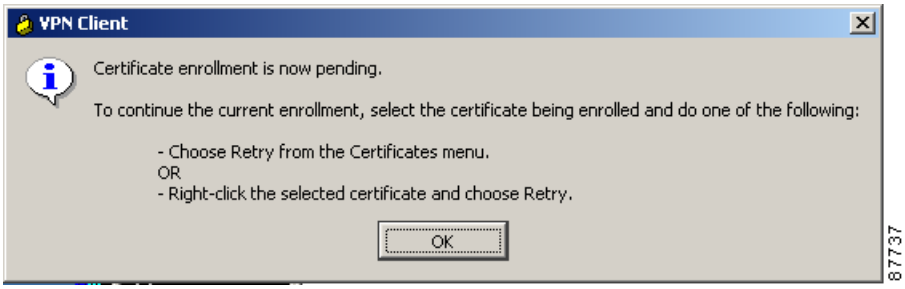
Together, all these fields except IP address and domain comprise your distinguished name (DN).

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

What happens next depends on your CA.

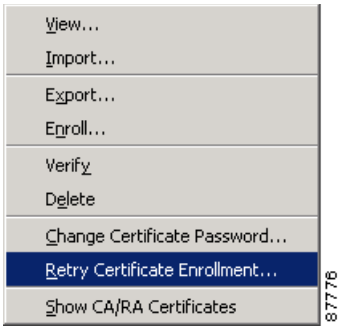
- Some CAs provide immediate response. If so, you see a message that your enrollment succeeded. You can view and manage the certificate under the Certificates tab.
- If the enrollment status is Request pending, your CA does not immediately approve your request. You see a status pending pop up window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

Figure 6-4 Enrollment Request Pending Message



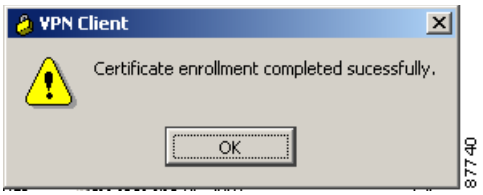
  - While you are waiting for the CA to issue the certificate, your request appears in the certificates list under the Certificates tab as a request. (The store column shows "Request".)
  - When the CA issues your certificate, choose the certificate and then choose **Retry Certificate Enrollment** from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

Figure 6-5 Retrying Enrollment Request



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

Figure 6-6 Enrollment Request Succeeded Message



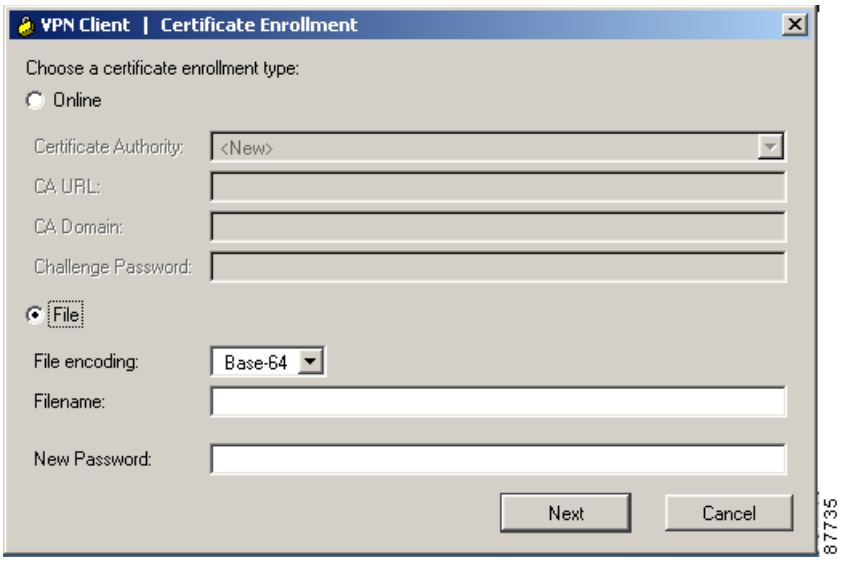
Enrolling Through a File Request

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

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

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

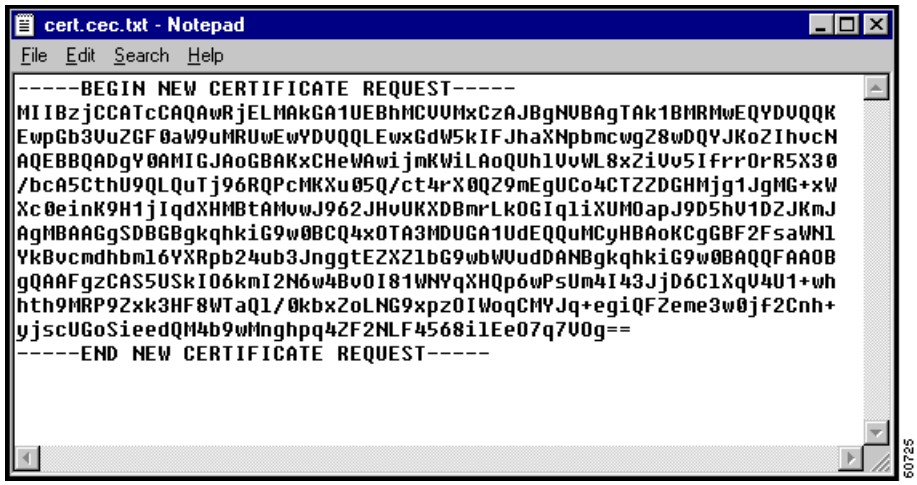
Figure 6-7 Enrolling a Certificate Using a File Request



Step 2 Click one of the following file types:

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

Figure 6-8 A PKCS10 Certificate File



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

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

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

An example of a complete pathname is c:\program files\cisco systems\vpn client\certificates\p10req3.p10.

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

Step 5 Click **Next**. The VPN Client displays page two of the form. This form is the same as the one used for enrolling via the network. See "Enrolling Through the Network".

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

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

Figure 6-9 Enroll File Success Message

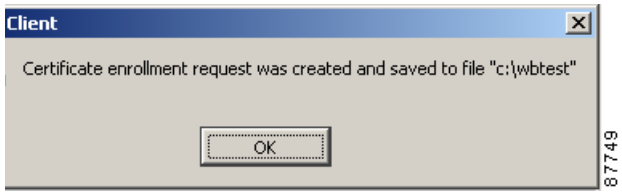
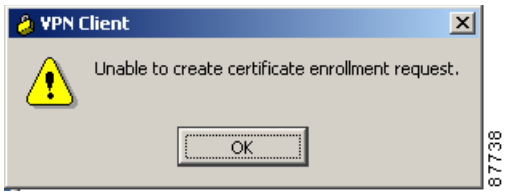


Figure 6-10 Enrollment Request Failed Message



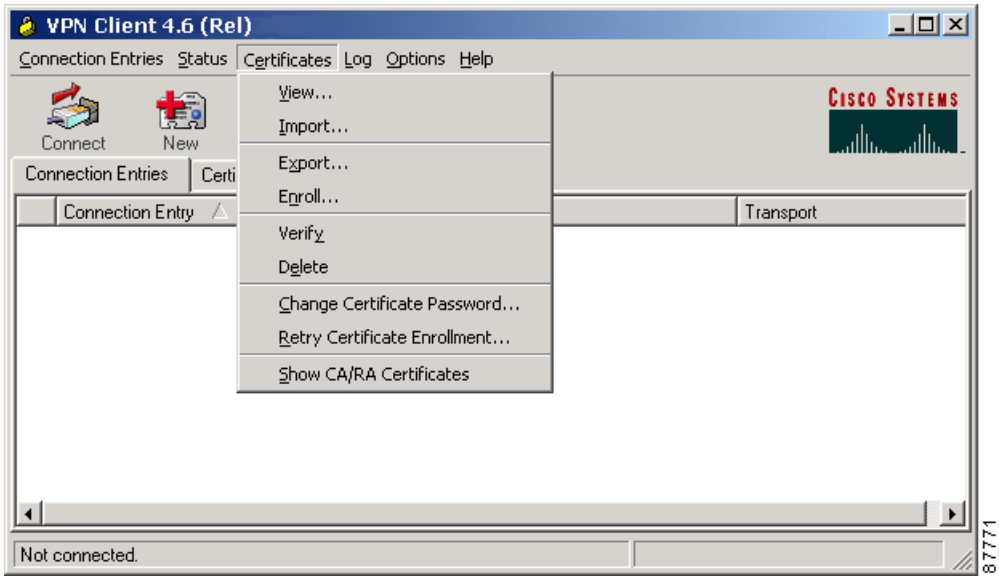
Step 7 Click **OK** to complete the file enrollment request.

Managing Personal and CA/RA Certificates

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

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

Figure 6-11 Certificates Menu



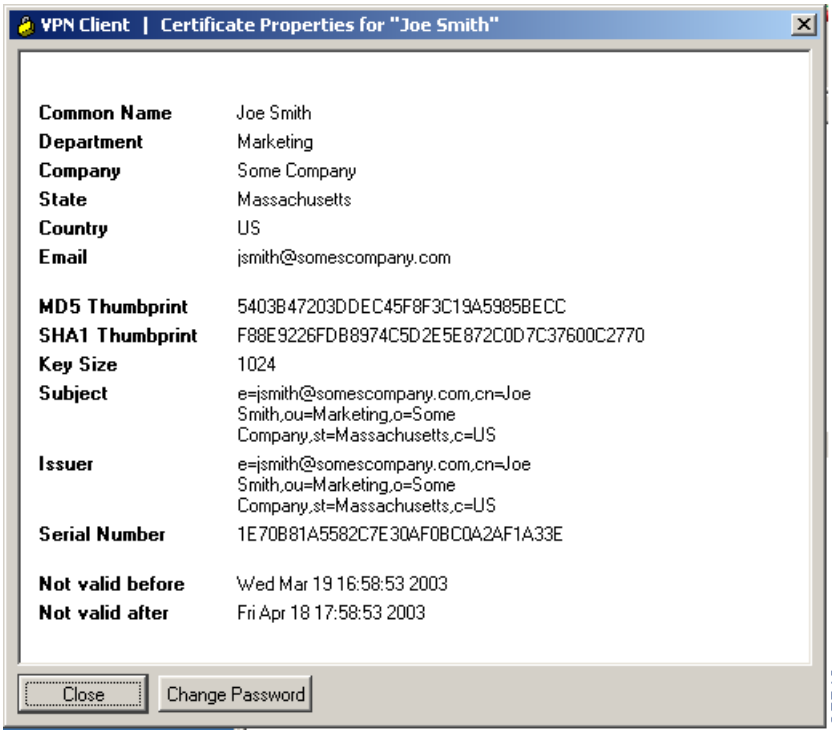
Viewing a Certificate

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

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

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

Figure 6-12 Viewing a Certificate



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

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

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

Importing a Certificate File

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

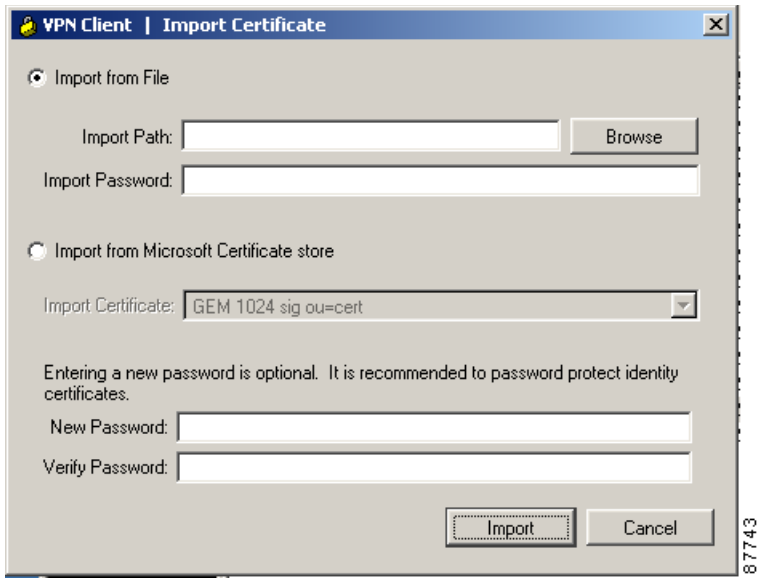
Importing a Certificate from a File

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

Step 1 Display the Certificates menu and choose **Import** or click the **Import** icon above the Certificates tab.

The Certificate Manager displays the Import Certificate Source dialog box. (See Figure 6-13.)

Figure 6-13 Importing a Certificate from File



Step 2 Select Import from File (the default).

Step 3 Complete the Import Certificate form:

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

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

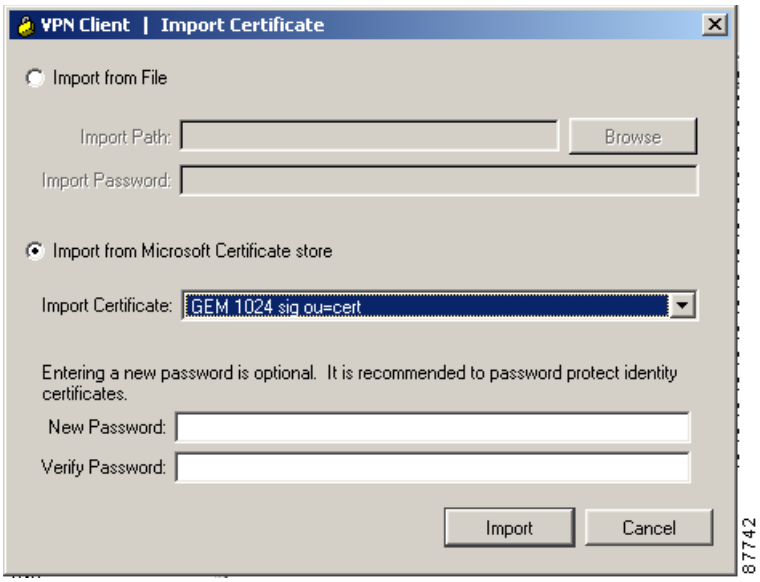
Importing a Certificate from the Microsoft Certificate Store

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

Step 1 Display the Certificates menu and choose **Import** or click the **Import** icon above the Certificates tab.

The Certificate Manager displays the Import Certificate dialog box. (See Figure 6-14.)

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



Step 2 Select Import from Microsoft Certificate store.

Step 3 New Password—The case-sensitive password to be stored with the certificate. This password is optional but we recommend that you always protect your certificate with a password.

Step 4 Verify Password—The password that you enter here must match what you entered in the New Password field.

Step 5 To complete the import request, click **Import** or to cancel your request click **Cancel**.

Verifying a Certificate

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

Step 1 Select the certificate from the certificate store under the Certificates tab

Step 2 Display the Certificates menu, and choose **Verify** or click the **Verify** icon on the toolbar above the Certificates tab.

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

Figure 6-15 Verifying a Certificate's Validity

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

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

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

Deleting a Certificate

To delete a certificate, follow this procedure:

Step 1 Select the certificate from the certificate store under the Certificates tab (certificate store).

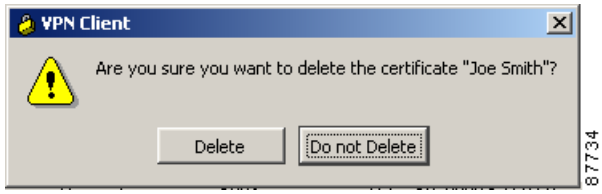
Step 2 Display the Certificates menu and choose **Delete**, or click the **Delete** icon in the toolbar above the Certificates tab.

If the certificate has a password, the VPN Client prompts you to enter it.

Step 3 In the Password field, type the password given to the certificate during enrollment and click **OK**.

Step 4 The VPN Client asks you to confirm that you want to delete this certificate (Figure 6-16). To delete the certificate, click **Delete**. To cancel the deletion, click **Do Not Delete** (the default).

Figure 6-16 Confirming Certificate Deletion



Changing the Password on a Personal Certificate

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

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

Step 2 Display the Certificates menu and choose **Change Certificate Password**

The VPN Client displays the Change Certificate Password dialog box. In the Current field, type the password you are currently using to protect your private key.

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

Step 4 In the Confirm field, type the same password again.

Step 5 Click **OK**. The VPN Client confirms that you have successfully changed your password (Figure 6-17).

Figure 6-17 Certificate Password Change Success Message

Exporting a Certificate

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

To export a certificate, follow these steps:

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

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

Figure 6-18 Exporting a Certificate

Step 2 In the Export path field, enter the path for the exported certificate or use the Browse feature to locate a target directory for the exported certificate.

Step 3 To export the CA and/or RA certificate with your personal certificate, check the **Export entire certificate chain** check box.

Step 4 In the Password field, enter an optional password to protect the export file. Then enter it again in the Verify Password field.

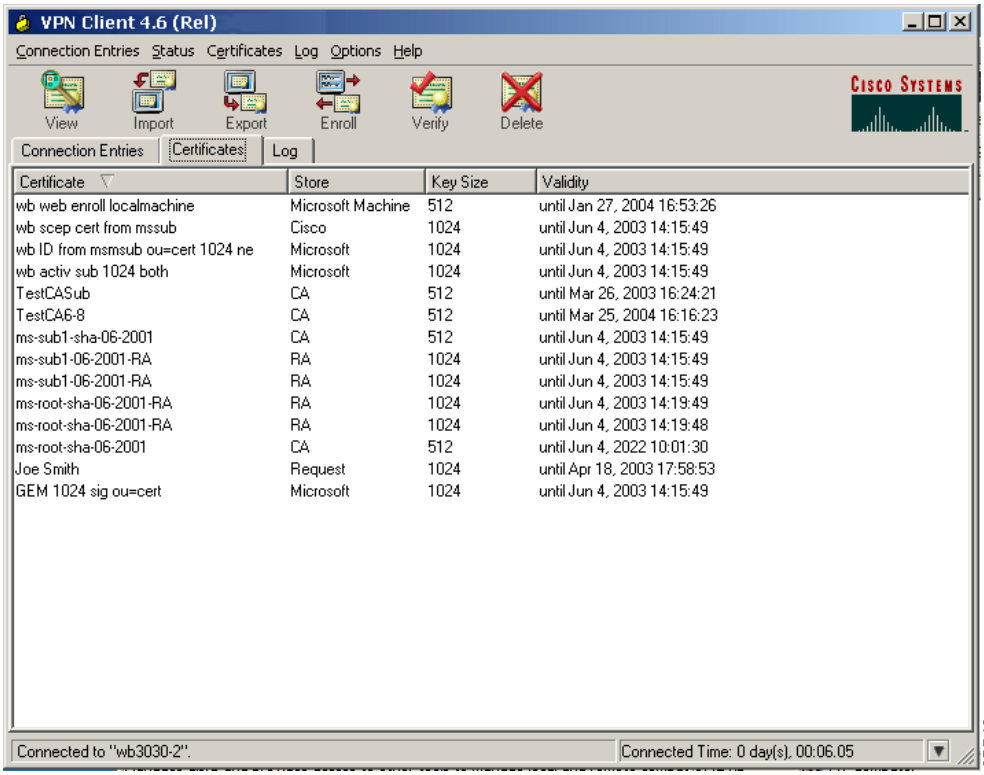
Step 5 After completing all the information, click **Export**.

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

Showing CA/RA Certificates

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

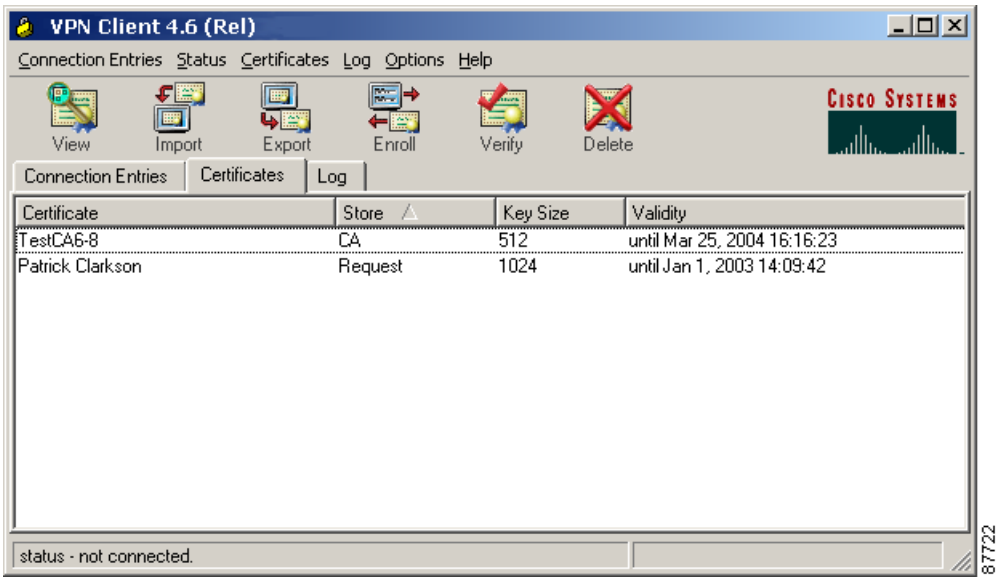
Figure 6-19 CA/RA Certificates List



Managing Enrollment Requests

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

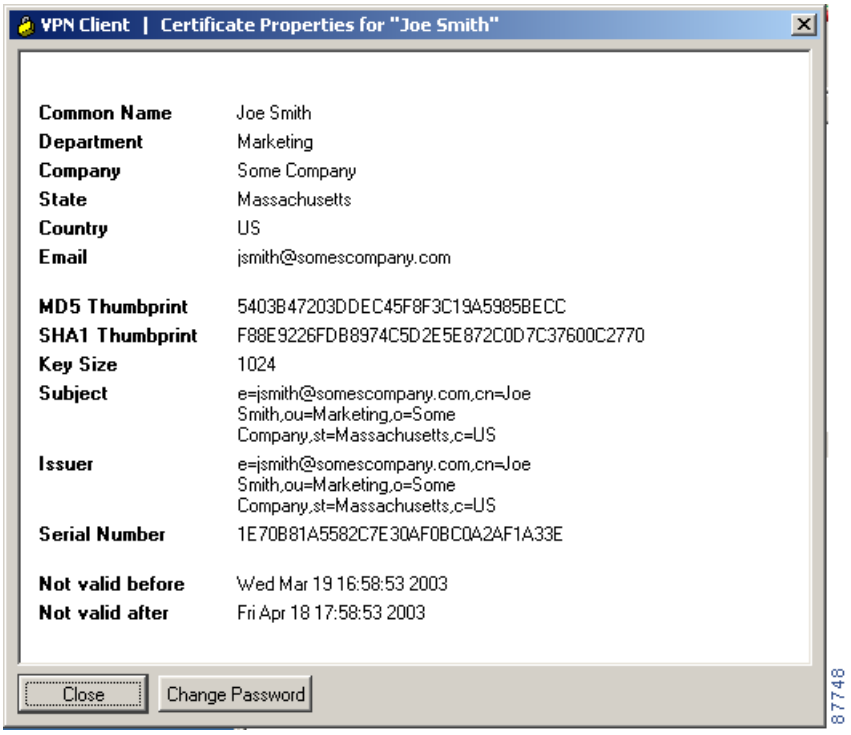
Figure 6-20 Managing Enrollment Requests



Viewing the Enrollment Request

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

Figure 6-21 Viewing an Enrollment Request



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

You can change the certificate request password from this screen.

Deleting an Enrollment Request

To delete an enrollment request, follow these steps:

Step 1 Select the enrollment request, display the Certificates menu and choose **Delete**.

The VPN Client prompts you for a password.

Step 2 Type the password in the Password field (if there is one) and click **OK**.

The VPN Client verifies the password. If the password is correct, the VPN Client deletes the request.

Changing the Password on an Enrollment Request

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

Step 1 Select the certificate request in the list under the Certificates tab.

Step 2 Display the Certificates menu and choose **Change Certificate Password**.

The VPN Client displays the Certificate Password dialog box. (See Figure 6-22.)

Figure 6-22 Changing a Certificate Password

Step 3 Type in the password you are currently using and click **OK**.

Step 4 At the prompt, type the new password and click **OK**.

Step 5 At the next prompt, type your new password again to verify it and click **OK**.

The VPN Client responds with a success message.

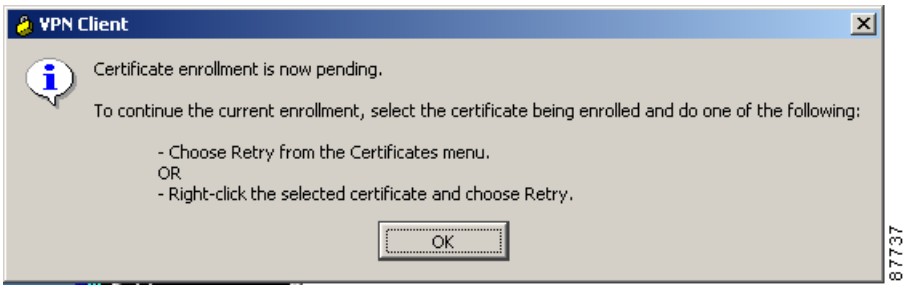
Note You can also change the password from the **View** dialog box.

Completing an Enrollment Request

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

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

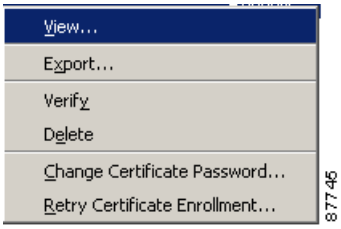
Figure 6-23 Completing a Pending Online Certificate Enrollment Request



Step 2 Select the certificate being enrolled, then do one of the following:

- Choose **Retry** from the Certificates menu.
- Right-click the selected certificate on the Certificates tab and choose **Retry** from the menu that appears (Figure 6-24).

Figure 6-24 Right-Click Certificate Menu



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

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.

This chapter includes the following sections:

To configure properties of connection entries, see "Configuring and Managing Connection Entries."

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.

Note The VPN Client displays Windows Logon Properties only on Windows NT, Windows 2000, and Windows XP systems.

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, regardless of whether a VPN connection is in effect. Also, the firewall is active for both encrypted and unencrypted traffic. There are two exceptions to this rule:

- 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.
- 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 or disable the stateful firewall, use the following procedure:

Step 1 Display the Options menu and click **Stateful Firewall (Always on)**. Or right-click the lock icon in the system tray, and choose **Stateful Firewall**.

When the stateful firewall is enabled, you see a check in front of the option. This feature is disabled by default.

Step 2 During a VPN connection, to view the status of this feature, right-click the lock icon in the system tray.

Launching an Application

You can configure the dialer to launch an application automatically 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 before each connection.

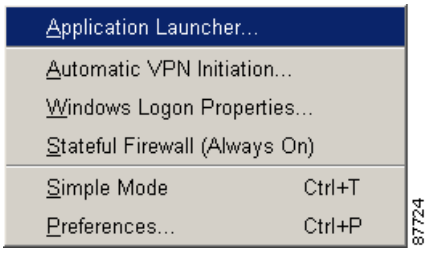
To configure the VPN Client to launch an application from the logon desktop, use the Application Launcher.

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

To activate Application Launcher, follow these steps:

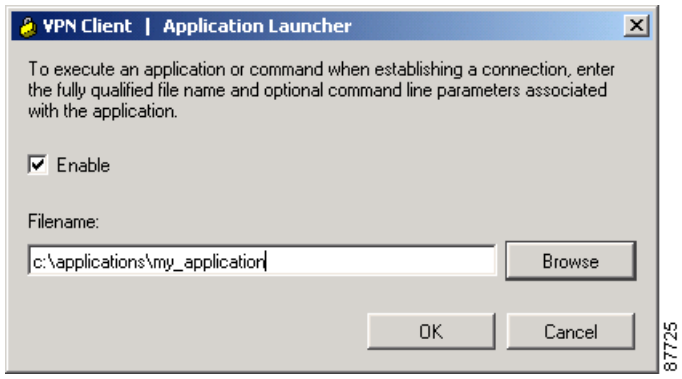
Step 1 Open the VPN Client Options menu (shown in Figure 7-1) and choose **Application Launcher.**

Figure 7-1 Choosing Application Launcher



The VPN Client displays a dialog box prompting for the name of the application. (See Figure 7-2.)

Figure 7-2 Entering the Name of the Application



Step 2 To enable the feature, click **Enable**.

Step 3 Either type the complete pathname of the application or click **Browse** to locate the application. (See Figure 7-2.)

Step 4 Click **Apply** to activate the application or click **Cancel** to cancel the operation.

Turning Off Application Launcher

To disable Application Launcher, follow these steps:

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

Step 2 When the Application Launcher dialog box displays, click the **Enable** check box to uncheck it.

Managing Windows NT Logon Properties

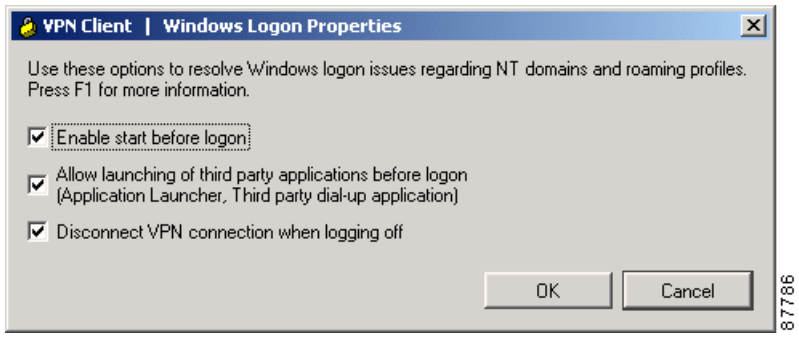
This section describes special logon features for the Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP. These features include:

- 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 menu (shown in Figure 7-1) and choose **Windows Logon Properties**. The VPN Client displays a dialog box containing three parameters. (See Figure 7-3.)

Note The VPN Client displays Windows Logon Properties only on Windows NT, Windows 2000, and Windows XP.

Figure 7-3 Controlling 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 on to your system. If you need to launch an application before you log on, see the section "Launching an Application" for information.

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

To activate start before logon, follow these steps:

Step 1 Open the VPN Client Options menu (shown in Figure 7-1) and choose **Windows Logon Properties**.

Step 2 Click **Enable start before logon** and then click **OK** or to cancel the operation, click **Cancel**. (See Figure 7-3.)

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 Client start.
- The VPN Client starts and displays the connection dialog box over the system logon dialog box.
- You connect to the private network of the VPN Device. The connection dialog box goes away.
- You log on to your system.

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 and the Microsoft local machine but not your personal Microsoft store (CAPI certificates). However, to use a CAPI certificate, you can log on using cached credentials, connect 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 on 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 an Entrust Certificate."

Turning Off Start Before Logon

To turn this feature off, use the following procedure:

Step 1 Open the VPN Client Options menu (shown in Figure 7-1) and choose **Windows Logon Properties**.

Step 2 Click to uncheck **Enable start before logon** and then click **OK** or to cancel, thus keeping the feature enabled, click **Cancel**.

Step 3 To make these changes take effect, reboot your PC.

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.

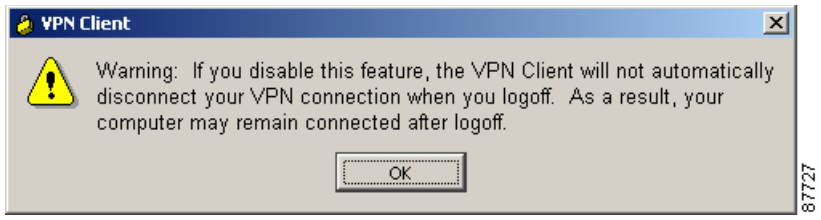
Disconnecting When Logging Off of a Windows NT Platform

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, uncheck this parameter. When you uncheck the parameter, the VPN Client displays the warning message shown in Figure 7-4.

Figure 7-4 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.

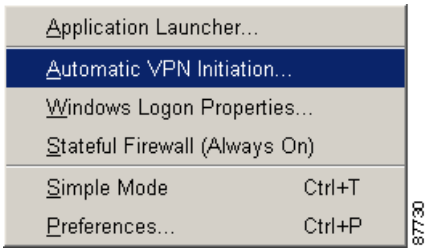
Note With this feature disabled, you must completely shut down your system to disconnect your VPN Client connection.

Managing Automatic VPN Initiation

When your network administrator has configured your VPN Client for automatic VPN initiation (by including it in the vpnclient.ini file), the Options menu includes the option Automatic VPN Initiation (auto initiation). (See Figure 7-5.) When you select this option, the VPN Client displays a dialog box that lets you enable/disable auto initiation and change the setting of the retry interval. Disabling auto initiation in this way does not remove it from your configuration. If you need to enable auto initiation after you have disabled it, you can return to this dialog box and enable it again. The only way you can remove auto initiation from your configuration is through editing the vpnclient.ini file.

For complete information on auto initiation, see "Using Automatic VPN Initiation".

Figure 7-5 Choosing Automatic VPN Initiation

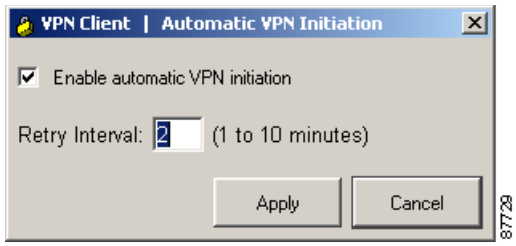


To disable or enable auto initiation, follow these steps:

Step 1 Choose **Automatic VPN Initiation** from the Options menu.

The VPN Client displays the Automatic VPN Initiation Dialog Box (Figure 7-6).

Figure 7-6 Automatic VPN Initiation Dialog Box



Step 2 To enable auto initiation after it has been disabled, click **Enable automatic VPN initiation** (or to disable auto initiation, click to uncheck **Enable automatic VPN initiation**).

Step 3 To change the setting of the retry interval, enter the new value (1 to 10) in the **Retry Interval** box.

Step 4 Click **Apply**.

Step 5 If you are enabling auto initiation, you then must close the VPN Client. The authentication dialog then prompts you to enter your authentication information.

Note You can also enable/disable, resume, and suspend auto initiation from the right-click menu, depending on the state of your connection.

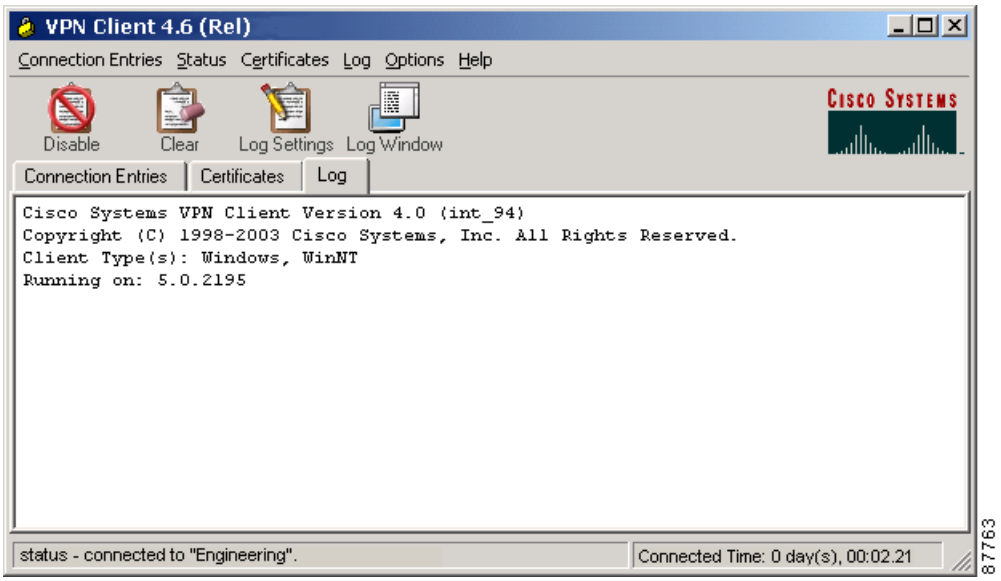
Viewing and Managing the VPN Client Event Log

When you start the VPN Client and enable logging, the VPN Client creates a new, empty log file for your session. The log collects event messages from all processes that contribute to the client-peer connection. Examining the event log can often help a network administrator diagnose problems with an IPSec connection between a VPN Client and a peer device. During a session, you can view the log from the Log tab and the Log Window. You can also view a saved log file with a text editor. This section shows how to use the log to retrieve and manage this information.

The Log Tab

You can manage and also view the log from the Log tab (Figure 7-7).

Figure 7-7 Viewing and Managing Events using the Log Tab



This window lets you

- View the log in the Log tab screen
- Enable or disable logging events
- Clear the log display in both the Log tab screen and the Log Window
- Change the log filtering settings
- Display the complete log in the log window and within the window perform the following actions:
  - Search the log
  - Save the messages to the log file
  - Change log filter settings
  - Clear the log display

Enabling or Disabling the Log

Enabling and disabling the log does not clear the events from the log file. To control the flow of information logged, use the following procedure. You can also control the amount of information collected by changing the log filtering settings.

Step 1 To start collecting event messages into the log file, you must enable the log in one of the following ways:

- Click **Enable** on the toolbar above the Log tab
- Display the Log menu and choose **Enable**

The log is disabled by default.

Step 2 To end collecting event messages into the log file, you must disable the log in one of the following ways:

- Click **Disable** on the toolbar above the Log tab

- Display the Log menu and choose **Disable**

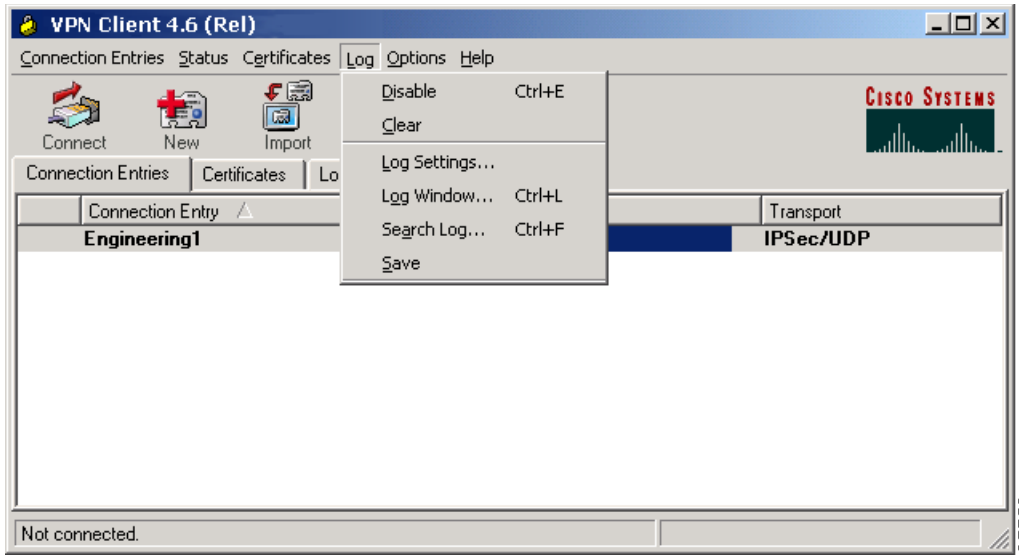
Displaying the Log Window

You can see a complete view of the log file by using the Log Window, which is scrollable.

Step 1 Display the Log Window in one of the following ways:

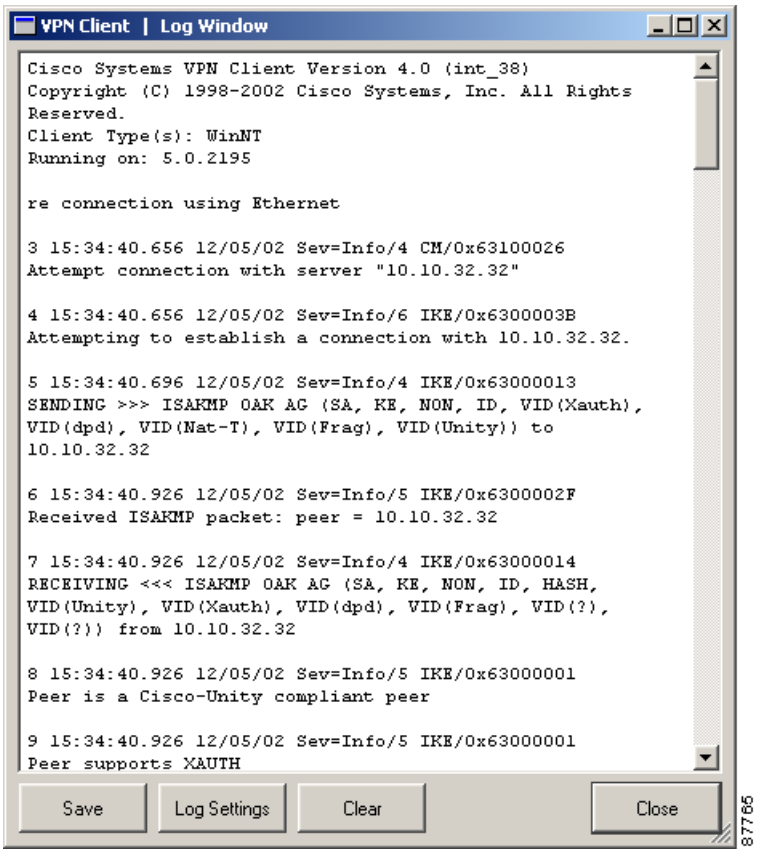
- Display the Log menu and choose **Log Window** (Figure 7-8)
- Press **Ctrl-L**
- Click the **Log Window** icon on the toolbar above the Log tab(Figure 7-7)

Figure 7-8 Displaying Log Messages from the Log Menu



The Log Window appears on the screen. (See Figure 7-9.) By default, the filter is set to low, so you might not see any events displayed in this window (see "Filtering Events").

Figure 7-9 Log Window



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 7-1 describes the fields in an event message. Table 7-2 describes Event types and severity levels.

Table 7-1 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, `2/03/2003` identifies an event that occurred on February 3, 2003.
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

Table 7-1 Fields in an Event Message

Field	Meaning
Event Class/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 7-2 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

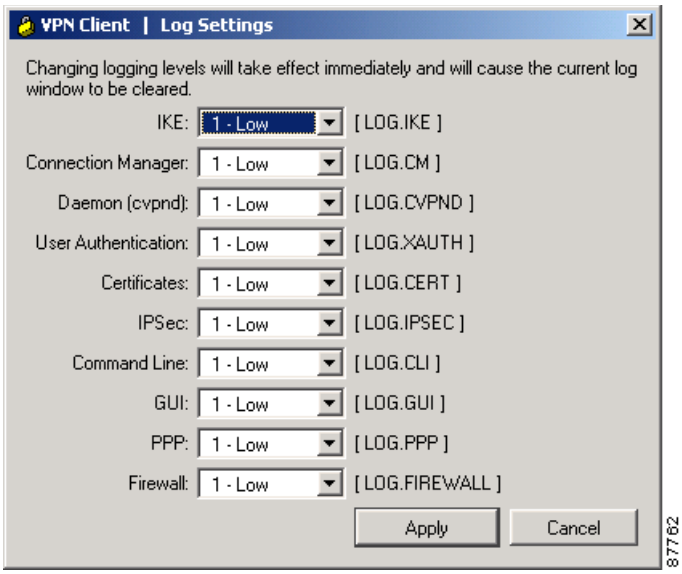
To control the amount of information collected in the log, use the following procedure:

Step 1 To change logging settings do one of the following:

- Display the Log menu and choose **Log Settings**
- Click the **Log Settings** icon in the toolbar above the Log tab
- Click **Log Settings** on the Log Window

The VPN Client displays the log settings dialog box (See Figure 7-10.)

Figure 7-10 Displaying and Changing Log Settings



To change the filter level, do the following:

Step 2 For each of the logs you want to change, click the down arrow and choose from the following options that the Log Settings dialog box displays:

Disabled—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.

Step 3 After making your changes, click **Apply** to save or **Cancel** to cancel your changes.

Table 7-3 defines the classes (modules) that generate events.

Table 7-3 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.
CLI	Command Line Interface, which lets managers start and end connections, get status information and so on through a command line rather than using the VPN Client graphical user interface.
CM	Connection manager (CM), which drives VPN connections. (CM dials a PPP device, configures IKE for establishing secure connections, and manages connection states.

Table 7-3 Classes That Generate Events in the VPN Client (continued)

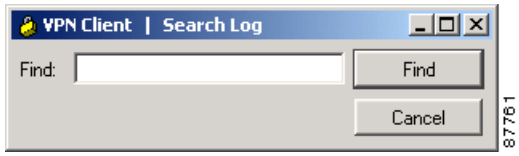
Class Name	Definition
CVPND	Cisco VPN Daemon (main daemon), which initializes client service and controls messaging process and flow.
GUI	Windows-only component, which handles configuring a profile, initiating a connection, and monitoring it.
FIREWALL	Firewall component, which generates events related to connections through a firewall.
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.

If you change the log filter levels, the change takes effect immediately for the events shown in both the Log Window and the Log tab, but while this change clears the events display on the Log tab, it does not clear the events in the log file.

Searching the Log File

You can search the log file for the occurrence of a string of characters. From the Log menu, select Search Log. This displays a dialog box (Figure 7-11) into which you enter the exact string to be matched.

Figure 7-11 Log Search Dialog Box



The search string is not case-sensitive, and wildcards are not supported. Search terms are highlighted only on the log tab display, not in the log window, even if the log tab was not the active tab.

Saving the Log File

To save the currently displayed events in the log file on your hard drive, use the following procedure:

Step 1 Either display the Log menu and choose **Save**, or click **Save** on the Log Window.

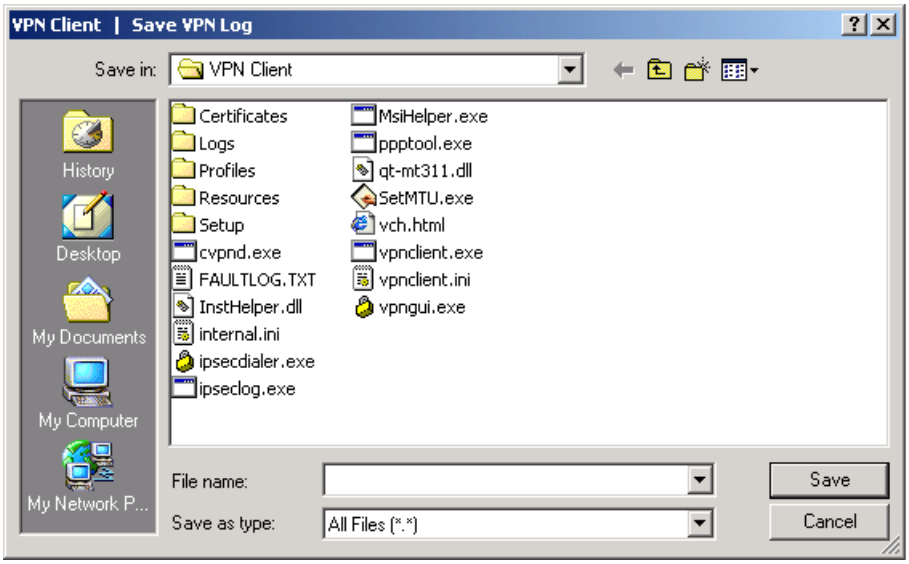
The VPN Client saves the information to the Client install directory, which by default is the pathname Program Files\Cisco Systems VPN Client\VPN Client\Logs. The default file name includes the word "LOG" and is based on the date and time (in 24-hour format) that the log file was created; for example, LOG-yyyy-MM-dd-hh-mm-ss.txt. This new format complies with the ISO 8601 extended specification for representations of dates and times and avoids issues with localization.

The new log file names have a chronological order that is the same as their alphanumeric order. This provides for a method of enumerating only the log files generated by the GUI.

Note You can save the contents of the present log to a different directory and filename, but you cannot change the default log directory and filename. (See Figure 7-12.)

Step 2 After typing in the name of the file, click **Save** or **Cancel**.

Figure 7-12 Saving a Log File



Clearing the Events Display in the Log Window and Log Tab

To eliminate all the events currently displayed in the Log Window and the Log tab, do one of the following:

- Click the **Clear** icon in the toolbar above the Log tab
- Open the Log menu and choose **Clear**.
- Click **Clear** on the Log Window.

Clearing the log display does not reset event numbering, nor does it clear the log file itself.

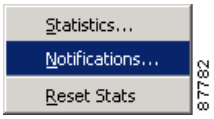
Receiving Notifications From a VPN Device

The VPN device (secure gateway) through which you connect to the private network at your organization can send you notifications. You can receive a notification from your network administrator when it is time to update the VPN Client software, when the VPN device detects that a required firewall is not running, or when the VPN Client receives a disconnect-with-reason notification. Other notifications are essentially documentary and can include connection history, client disconnect notices, and an administrator-defined banner. A notification showing the login sequence typically appears when you start your dialer connection.

Step 1 To display notifications, do one of the following:

- Open the Status menu, and click **Notifications**. (See Figure 7-13)

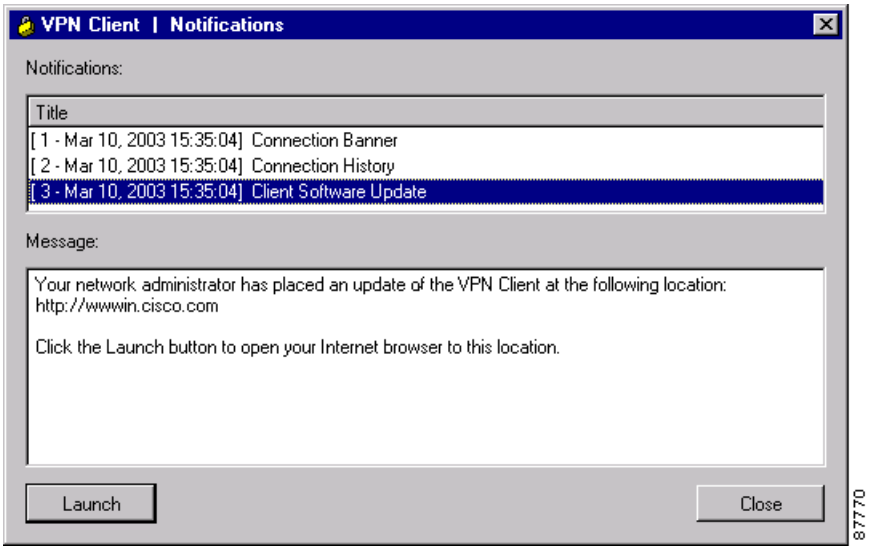
Figure 7-13 Displaying Notifications from the Status Menu



- While connected, right-click the VPN Client icon in the system tray, and click **Notifications**.

Figure 7-14 shows the Notifications dialog box.

Figure 7-14 Displaying Notifications



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. The message states that the policy required is AYT and the firewall required is any Zone Labs product.

Disconnect-with-Reason Messages

In addition, in Release 4.0, when a VPN 3000 Concentrator disconnects the VPN Client and tears down the tunnel, the VPN Client displays a popup window showing the reason for the disconnect and also logs a message to the Notifications log and the IPSec log file. For IPSec deletes that do not tear down the connection, the event message appears only in the log file. These disconnect events include:

- Administrative disconnect.

- VPN 3000 Concentrator shutdown or reboot.
- Idle-time disconnect.
- Maximum connection time disconnect.

For a shutdown or reboot scheduled at a future time, the VPN 3000 Concentrator sends the disconnect notification at the time of the actual shutdown or reboot. This feature does not provide advanced or early notification of a future event; for example, it does not send messages such as "The Concentrator is going to shut down in 30 minutes."

The disconnect-with-reason feature is enabled by default, but an administrator can configure the VPN 3000 Concentrator to turn off these disconnect notifications. This feature is not configurable on the VPN Client. When this feature is enabled, the VPN 3000 Concentrator and the VPN Client negotiate whether to display these messages.

Upgrading VPN Client Software

There are several ways to update VPN Client Software. For all Windows platforms, you can update software manually, using either the MSI installer or the InstallShield installer. If you are on a Windows 2000 or Windows XP system, updating VPN Client software and profiles occurs automatically. This section supplies instructions for all the various ways you can upgrade your software.

All Windows Platforms

If you are using a Windows 95, Windows 98, or Windows NT platform, you must update the VPN Client software manually. Generally, an administrator sends a notification to inform you that you must upgrade.

Upgrade Notifications

Remote users receive a notification message when 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. For an example of an upgrade notification, see Figure 7-14.

Upgrading the VPN Client Software Using MSI

Upgrading the VPN Client software using MSI in this recommended way retains existing connection entries and their parameters. You must remove any version of the Cisco VPN Client or any other VPN Client before upgrading the Cisco VPN Client with MSI.

To install an upgrade of the VPN Client to replace an existing version on your system, use the following procedure.

Step 1 Remove any existing version of the VPN Client software through the Add/Remove available from the Windows Control Panel.

Step 2 Install the VPN Client using the MSI installer (vpnclient_en.msi).

Step 3 Reboot your PC.

Upgrading the VPN Client Software Using InstallShield

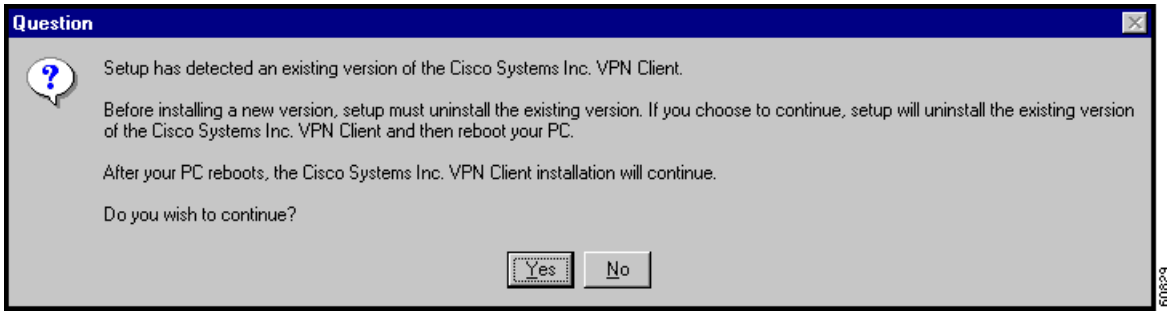
Upgrading the VPN Client software using this method retains existing connection entries and their parameters.

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 Through InstallShield" I 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 7-15.)

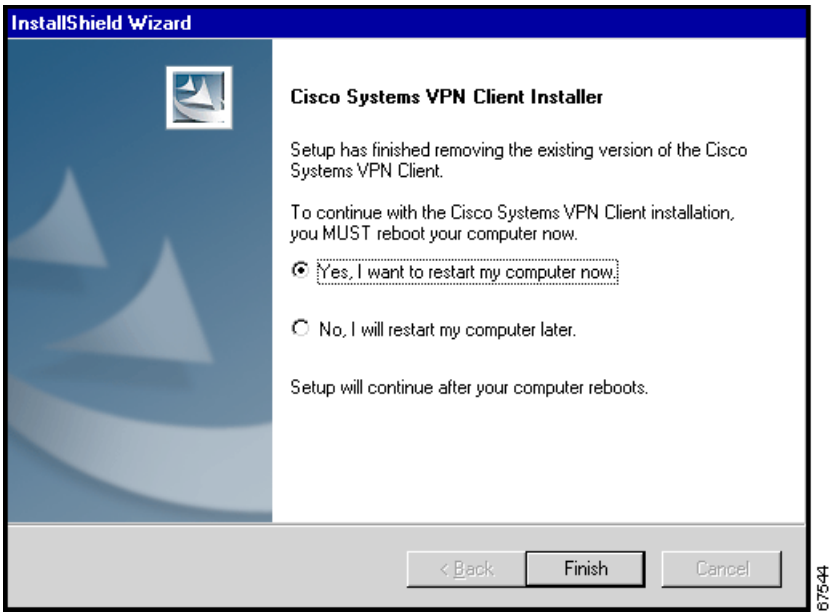
Figure 7-15 Uninstalling an Existing Version



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

The installation program removes the old version and asks you to confirm the system restart. (See Figure 7-16.)

Figure 7-16 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, I want to restart my computer now** (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 Through InstallShield."

Uninstalling the VPN Client with the Uninstall Application

This option is available only if you have installed the VPN Client via InstallShield. 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. Also, if you are getting ready to install Cisco VPN Client 4.0 using Microsoft Windows Installer (MSI), you can run the Uninstall application to remove previous versions of the Cisco 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 7-17.)

Note If you installed the VPN Client via the Microsoft Windows Installer, the Cisco Systems VPN Client menu does not include the Uninstall VPN Client option. Remove a previous version with Add/Remove Software.

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

Figure 7-17 Running the Uninstall Program

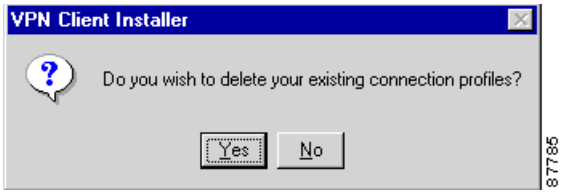
The Uninstall Wizard runs and asks if you want to really want to remove the VPN Client applications. (See Figure 7-18.)

Figure 7-18 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 7-19.)

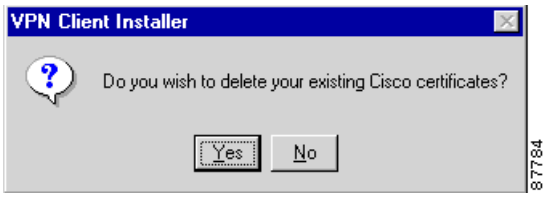
Figure 7-19 Confirming Your Connections



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 7-20.)

Figure 7-20 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 and you have clicked yes to remove your certificate and profile directories, the vpnclient.ini and log 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 must remove them manually.

Updating the VPN Client Software Automatically—Windows 2000 and Windows XP Systems

Beginning with VPN Client Release 4.6, the VPN Client software can install new releases, updates to releases, and new or modified profiles automatically on Windows 2000 and Windows XP systems. For information on how to manage this feature, refer to *VPN Client Administrator Guide*. Autoupdate can reduce or eliminate the need for rebooting during installation. For MSI installation, autoupdate removes the old version of the VPN Client software automatically and then resumes installation (in the same manner as InstallShield).

When a new version or update is available, the autoupdate program displays a dialog (for an example, see Figure 7-21) that lets you choose to install it right away, install it later, or not to install the package at all. In the later case, however, every time you connect to the VPN Concentrator you see the dialog asking you to install the update until you finally install it. If an administrator requires that you install the update, your choices are limited to Install Now or Install Later.

Figure 7-21 Automatic Installation—Full Install

There are three types of automatic installs: Full Installation, minor update, profile update.

Full Installation

For a major update, you do a full installation. Full installations can be either optional or required. Major updates require a reboot.

- An optional full installation—The update package is a new major release. Figure 7-21 shows your choices: Install Now, Install Later, Don't Install.
  - To install the update, close all programs and choose **Install Now**.
  - To install the update when you exit from the VPN Client, select **Install Later**.
  - To reject the installation, choose **Don't Install**. If you choose Don't Install, autoupdate prompts you again next time you start the VPN Client.
- A required full installation—The update package is a major update. You can choose from only two options, Install Now or Install Later.
  - To install the update, close all programs and choose **Install Now**.
  - To install the update when you exit from the VPN Client, select **Install Later**. If you choose Install Later, when you exit from the VPN Client, autoupdate installs the update.

Minor Update

The update is a minor release (a point release or a patch release). Minor updates can be optional or required. They may or may not require a reboot.

- An optional minor update— The update package is not a new major release. Figure 7-22 shows your choices: Install Now, Install Later, Don't Install.

Figure 7-22 Automatic Installation—Minor Update

  - To install the update, close all programs and choose **Install Now**.
  - To install the update when you exit from the VPN Client, select **Install Later**.
  - To reject the installation, choose **Don't Install**. If you choose Don't Install, autoupdate prompts you again next time you start the VPN Client.
- A required minor update—The update package is a minor update. You can choose from only two options, Install Now or Install Later.
  - To install the update, close all programs and choose **Install Now**.
  - To install the update when you exit from the VPN Client, select **Install Later**. If you choose Install Later, when you exit from the VPN Client, autoupdate installs the update.

Profile Update

Profile updates distribute new and/or modified user profiles and can also contain updated software. Profile updates can be either optional or required. They may or may not require a reboot.

- An optional profile update—The profile update distributes new or modified profiles. Figure 7-23 shows your choices: Install Now, Install Later, Don't Install.

Figure 7-23 Automatic Installation—Profile Update

  - To install the update, close all programs and choose **Install Now**.
  - To install the update when you exit from the VPN Client, select **Install Later**.

  - To reject the installation, choose **Don't Install**. If you choose Don't Install, autoupdate prompts you again next time you start the VPN Client.

- A required profile update—The profile update distributes new or modified profiles. You can choose from only two options, Install Now or Install Later.
  - To install the update, close all programs and choose **Install Now**.
  - To install the update when you exit from the VPN Client, select **Install Later**. If you choose Install Later, when you exit from the VPN Client, autoupdate installs the update.

If the update does not succeed, autoupdate displays an error message identifying the problem.

Figure 7-24 Automatic Installation—Error Message

When this happens, click **Finish** and then contact your system administrator.

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

1. 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

2. 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

3. You may also 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.

4. You may copy and distribute the Software to your third party business partners and customers solely and exclusively for the purposes of accessing your Cisco VPN concentrators and thereby gaining remote access to your secure network. Each such distribution of the Software to a third party must be accompanied by a copy of this Client Software License Agreement. You may not copy or transfer the Software for any purpose, other than as specified in this Agreement, without the express written consent of Cisco. Without intending to limit the foregoing, you shall not post or otherwise make publicly available the Software to any external web site, file server, or other location to which there is unrestricted access.

5. Cisco Systems will not provide end-user support (including Technical Assistance or TAC support) to any third party that receives the Software in accordance with Section 4 hereof. You shall be responsible for providing all support to each such third party. 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. (For reference purposes only, see the Cisco Encryption Tool Quick Reference Guide currently located at http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.)

6. 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.

7. 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 in your possession. You must also use commercially reasonable efforts to notify the third parties to whom you have distributed the Software that their rights of access and use of the Software have also ceased. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.

8. 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 through 4 hereof.

9. 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

10. 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 USE OF THE SOFTWARE BY YOU OR ANY THIRD PARTY.

RSA software

Zone Labs

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z