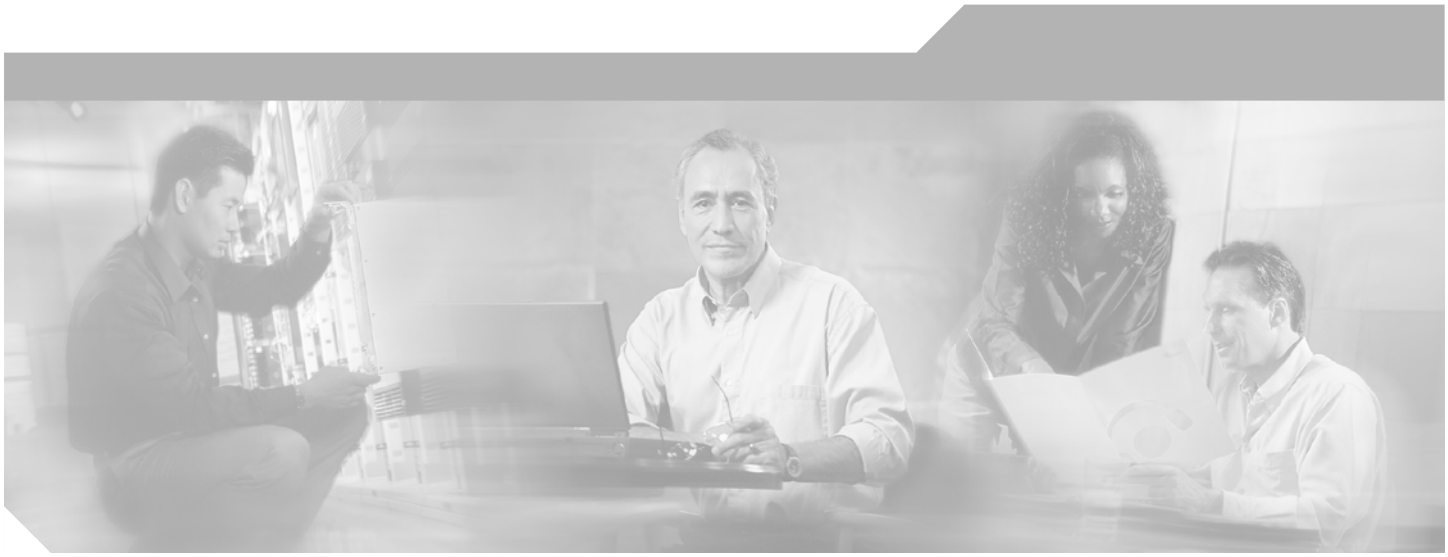


Cisco VPN Client User Guide for Mac OS X

Release 3.7

October 2002

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

Customer Order Number:
Text Part Number: OL-3138-01

Cisco VPN Client User Guide for Mac OS X

CONTENTS

About This Guide

This VPN client User Guide describes how to install, use, and manage the Cisco VPN Client for the Macintosh operating system, Version 10.1.0 or later. You can manage the VPN Client for Mac OS X from the graphical user interface or from the command-line interface.

The VPN client for Mac OS X installer program installs both the graphical user interface and the command-line version of the VPN client.

Audience

This guide is for remote clients who want to set up virtual private network (VPN) connections to a central site. Network administrators can also use this guide for information about configuring and managing VPN connections for remote clients. You should be familiar with the Macintosh platform and know how to use Macintosh applications. Network administrators should be familiar with Macintosh system configuration and management and know how to install, configure, and manage internetworking systems.

Contents

This guide contains the following chapters:

- Chapter 1, “Introduction to the VPN Client.” This chapter describes how the VPN client software works and lists the main features.
- Chapter 2, “Installing the VPN Client.” This chapter describes how to install the VPN client software application.
- Chapter 3, “Navigating the User Interface.” This chapter describes the main VPN client window and the tools, tabs, menus and icons for navigating the user interface.
- Chapter 4, “Configuring Connection Entries.” This chapter describes how to configure VPN client connection entries, including optional parameters.
- Chapter 5, “Establishing a VPN Connection.” This chapter describes how to connect to a private network using the VPN client, an Internet connection, and the user authentication methods supported by the VPN client.
- Chapter 6, “Managing Certificates.” This chapter describes how to obtain digital certificates to use for authentication and how to manage these certificates in the VPN client certificate store.

- Chapter 7, “Managing the VPN Client.” This chapter describes how to manage VPN client connections, use the event log, and view tunnel details, including packet and routing data.
- Index

Related Documentation

The following is a list of user guides and other documentation related to the VPN client for Mac OS X and the VPN devices that provide the connection to the private network.

- *Cisco VPN Client User Guide for Linux and Solaris, Release 3.7*
- *Release Notes for the Cisco VPN Client, Release 3.7 for Linux, Solaris, and Mac OS X*
- *Cisco VPN Client Administrator Guide*
- *Cisco VPN 3000 Series Concentrator Series Getting Started Guide*
- *Cisco VPN 3000 Series Concentrator Reference Volume I: Configuration*
- *Cisco VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*

Terminology

In this user guide:

- The term Cisco VPN device refers to the following Cisco products:
  - Cisco IOS devices that support Easy VPN server functionality
  - VPN 3000 Series Concentrators
  - Cisco PIX Firewall Series
- The term “PC” refers generically to any personal computer.
- The term click means click the left button on a normally-configured multi-button mouse. The term right-click means click the right button on a normally-configured multi-button mouse. If your mouse has only one button, use **Ctrl-Click** to access the right-click menus.

Document Conventions

This guide uses the following typographic conventions:

- **Boldface** font—Describes user actions and commands.
- *Italic* font—Describes arguments that you supply the values for.
- `Screen` font—Describes terminal sessions and information displayed by the system.
- **`Boldface screen`** font—Describes information that you must enter.

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

When you configure the VPN client, enter data in these formats unless the instructions indicate otherwise.

- IP Address—Use standard 4-byte dotted decimal notation (for example, 192.168.12.34). You can omit leading zeros in a byte position.
- Hostnames—Use legitimate network host or end-system name notation (for example, VPN01). Spaces are not allowed. A hostname must uniquely identify a specific system on a network. A hostname can be up to 255 characters in length.
- User names and Passwords—Text strings for user names and passwords use alphanumeric characters in both upper- and lower-case. Most text strings are case sensitive. For example, simon and Simon would represent two different user names. The maximum length of user names and passwords is generally 32 characters, unless specified otherwise.

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.

CHAPTER 1

Introduction to the VPN Client

The Cisco VPN Client for Mac OS X is a software application that runs on any Macintosh computer using operating system Version 10.1.0 or later. The VPN client on a remote PC, communicating with a Cisco VPN device on an enterprise network or with a service provider, creates a secure connection over the Internet. This connection allows you to access a private network as if you were an on-site user, creating a Virtual Private Network (VPN).

The following VPN devices can terminate VPN connections from VPN clients:

- Cisco IOS devices that support Easy VPN server functionality
- VPN 3000 Series Concentrators
- Cisco PIX Firewall Series, Version 6.2 or later

With the graphical user interface for the VPN Client for Mac OS X, you can establish a VPN connection to a private network, manage connection entries, certificates, events logging, and view tunnel routing data.

You can also manage the VPN client for Mac OS X using the command-line interface (CLI). If you are running Darwin, or if you prefer to manage the VPN client from the CLI, refer to the *Cisco VPN Client Adminstration Guide*.

This chapter contains the following sections:

VPN Client Overview

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

The steps used to establish a VPN connection can include:

- Negotiating tunnel parameters (addresses, algorithms, lifetime)
- Establishing VPN tunnels according to the parameters.
- Authenticating users (from usernames, group names and passwords, and X.509 digital certificates.)
- Establishing user access rights (hours of access, connection time, allowed destinations, allowed protocols)

- 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, the connection process might be similar to the following:

Step 1 Connect to the Internet.

Step 2 Start the VPN client.

Step 3 Establish a secure connection through the Internet to your organization's private network.

Step 4 When you open your e-mail

- The Cisco VPN device
  - Uses IPSec to encrypt the e-mail message
  - Transmits the message through the tunnel to your VPN client
- The VPN client
  - Decrypts the message so you can read it on your remote PC
  - Uses IPSec to process and return the message to the private network through the Cisco VPN device.

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 Main Features

Features	Description
Operating System	Mac OS Version 10.1.0 or later
Connection types	• async serial PPP • Internet-attached Ethernet
Protocol	IP
Tunnel protocol	IPSec
User Authentication	• RADIUS • RSA SecurID • VPN server internal user list • PKI digital certificates • 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
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 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*.
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.

IPSec Features

The VPN client supports the IPSec features listed in Table 1-3

Table 1-3 IPSec Features

IPSec Feature	Description
Tunnel Protocol	IPSec
Transparent tunneling	• IPSec over UDP for NAT and PAT • IPSec over TCP for NAT and PAT

Table 1-3 IPSec Features (continued)

IPSec Feature	Description
Key Management protocol	Internet Key Exchange (IKE)
IKE Keepalives	A tool for monitoring the continued presence of a peer and report 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 on the VPN client and configure the network list on the VPN device.
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 (VPN concentrator) and enabled on the VPN client by default. To use Split DNS, you must also have split tunneling configured.

VPN Client IPSec Attributes

The VPN client supports the IPSec attributes listed in Table 1-4.

Table 1-4 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 • X.509 Digital Certificates
Diffie-Hellman Groups	• 1 • 2
Encryption algorithms	• 56-bit DES (Data Encryption Standard) • 168-bit Triple-DES • AES 128-bit and 256-bit

Table 1-4 IPSec Attributes (continued)

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

Authentication Features

The VPN client supports the authentication features listed in Table 1-5.

Table 1-5 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 Management	Allows you to manage the certificates in the certificate stores.
Certificate Authorities (CAs)	CAs that support PKI SCEP enrollment.
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.

CHAPTER 2

Installing the VPN Client

This chapter describes how to install the VPN Client for the Mac OS X.

Verifying System Requirements

The VPN Client for Mac OS X runs on any Power Macintosh or compatible computer with the Macintosh operating system Versions 10.1.0 or later and 30 MB of hard disk space.

Obtaining the VPN Client Software

The VPN client software is available from the Cisco website and comes as a zipped file. Only system administrators can obtain and distribute the VPN client software.

To obtain the VPN client software from the system administrator:

Step 1 Download the zipped file to your desktop.

Step 2 Expand and extract the zipped file.

Your browser might automatically expand and extract the zipped files. If it does not, double-click the zipped file, or if the file is in a folder, you can use Unzip.

The VPN client installer is extracted to your desktop. The zipped file also remains on your desktop.

Preconfiguring the VPN Client

This section describes how to distribute preconfigured configuration files (user profiles) and GUI preference files to the VPN client installer.

Preconfiguring the User Profile

The VPN client uses parameters that must be uniquely configured for each remote user of the private network. Together these parameters make up a user profile, which is contained in a profile configuration file (.pcf file).

Note Refer to the *Cisco VPN Client Administrator Guide* for information on creating a user profile, configuration file parameters, keywords, and values.

To distribute custom user profiles to the installer program, place the files inside the installer application in the directory:

CiscoVPN.app/Contents/Resources/

To access the Resources folder, right-click (or Ctrl-click) the VPN client installer icon to access the installer menu (Figure 2-1).

Figure 2-1 Installer Menu

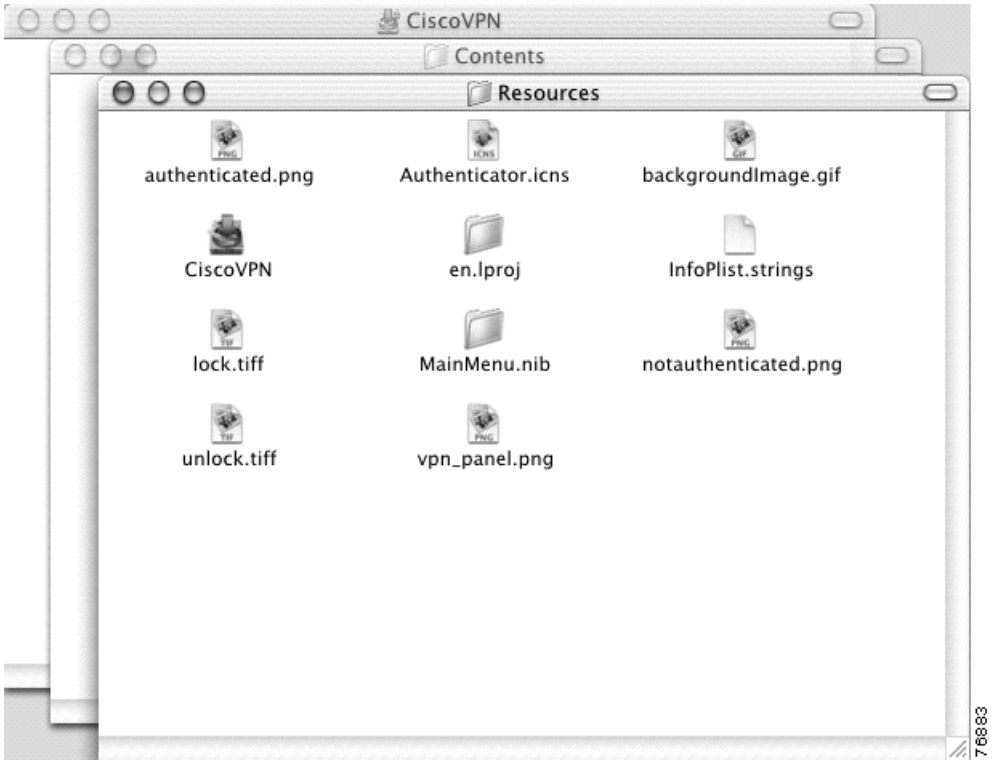
Step 3 Choose **Show Package Contents** to open the installer directory.

Step 4 Click on the Contents folder.

Step 5 Click on the Resources folder.

Figure 2-2 shows the Resources directory.

Figure 2-2 Resources Folder Contents



Step 6 Copy the configuration files (.pcf files) into the Resources directory.

Any file with a .pcf extension found in this folder is placed in the Profiles directory when the VPN client is installed.

Preconfigured GUI Preferences

VPN client GUI preferences, such as window locations and sizes, are stored in the file VPNClient.conf.

When you first open the VPN client, the GUI preferences file is populated with default settings. Each time you make changes to the GUI preferences, the VPNClient.conf file is updated and stored.

You can also distribute a preconfigured GUI preference file.

To distribute the preconfigured file, place the VPNClient.conf file inside the installer application in the Resources directory:

CiscoVPN.app/Contents/Resources/

During installation, the file is installed in /etc/CiscoSystemsVPNClient/Resources/VPNClient.conf.

Installing the VPN Client

The following sections describe how to install the VPN client software. The VPN client for Mac OS X installer program installs both the graphical user interface and the command-line version of the VPN client.

Note You must uninstall any previous version of the VPN client for Mac OS X before you install a new version. For more information, see "Uninstalling the VPN Client" section on page 2-13.

Authentication

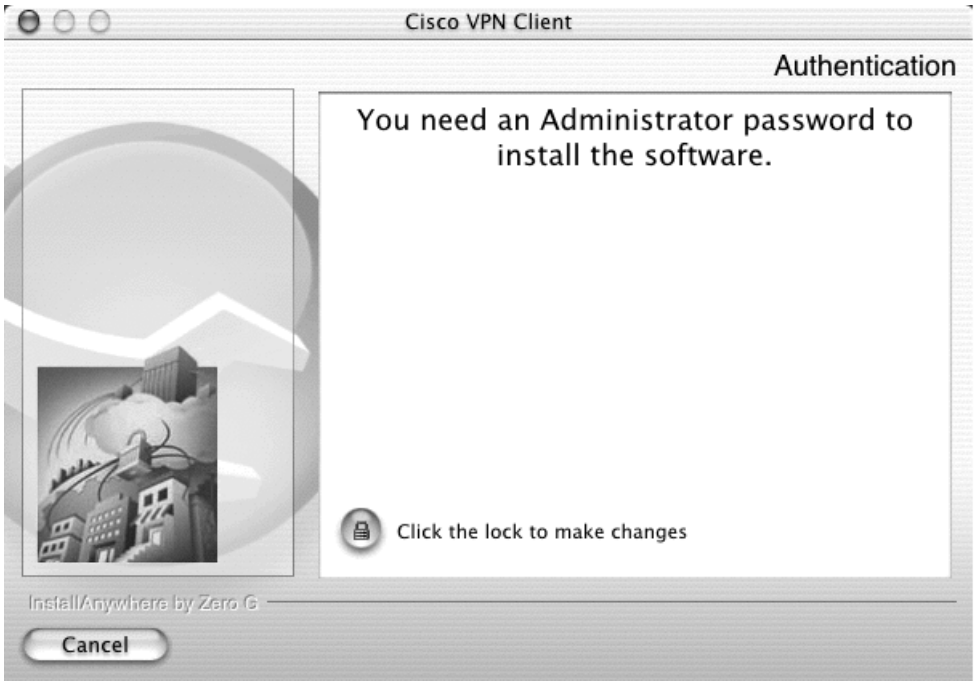
Before you can start the installation process, you must show that you have installation privileges.

Step 1 Open the installer by double-clicking the installer icon on your desktop (Figure 2-3).

Figure 2-3 VPN Installer Icon

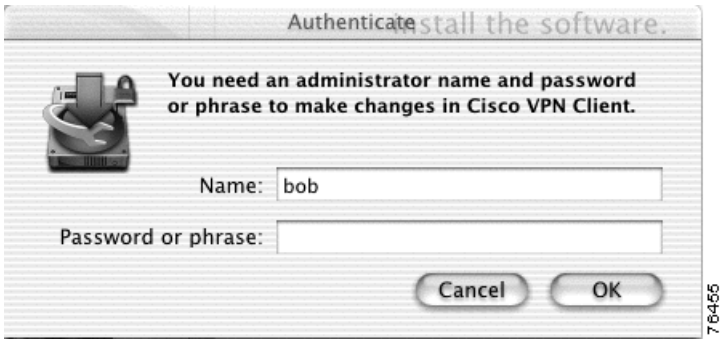
The Authentication window appears (Figure 2-4). You must have an Administrator password to install the VPN client application.

Figure 2-4 Cisco VPN Client—Authentication Window



Step 2 Click the lock at the bottom left corner of the Authentication window. The Authenticate dialog box appears (Figure 2-5).

Figure 2-5 Authenticate Dialog Box



Step 3 Enter your administrator username and a password or challenge phrase.

Step 4 Click **OK**.

If the authentication is successful, continue to the installation process. Contact your network administrator if you cannot authenticate for installation.

VPN Client Installation Process

You must complete all steps in the VPN client installation process before you can use the VPN client software.

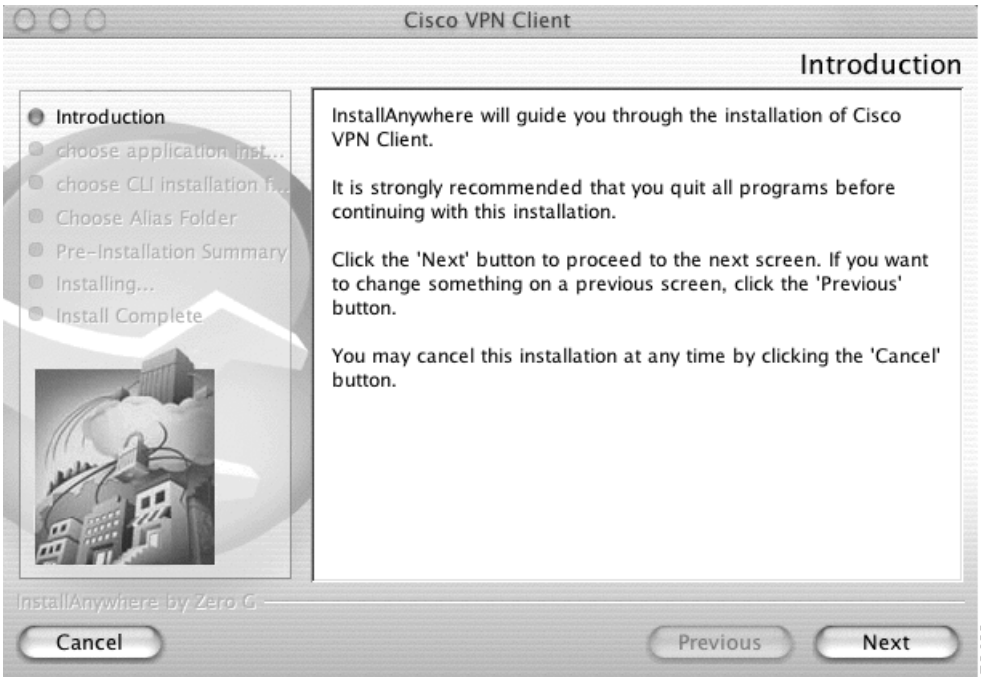
At any time during the installation process, you can go back to a previous step and adjust your selections or restore the default selections.

The installation process includes the following steps:

Introduction

The first window that appears during the installation process is the introduction. The right pane of the Introduction window (Figure 2-6) describes the installation process and lists any preinstallation recommendations. The left pane displays each of the installation steps. As you complete each step, it is highlighted with a blue bullet.

Figure 2-6 Cisco VPN Client—Introduction Window

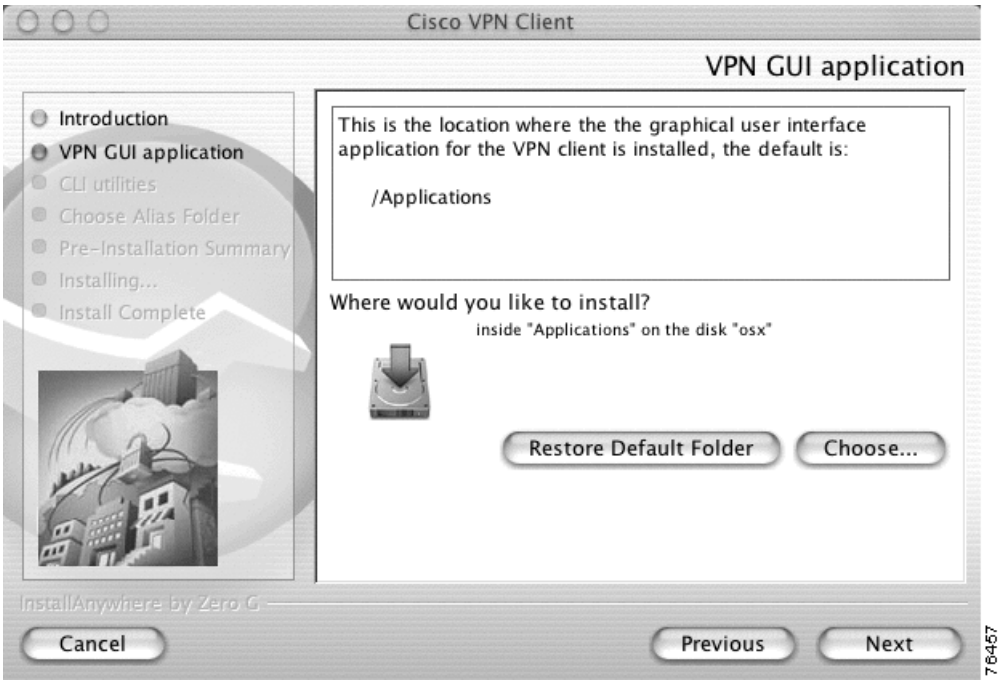


Click **Next** to continue or **Cancel** to quit the installation process.

Choosing the Application Location

Install the VPN client application in the default folder, /Applications, or choose another folder. If you choose another folder, a browser window appears. Locate a new directory for the VPN client application and click **Choose**. The new application folder is listed on the VPN GUI Application window (Figure 2-7).

Figure 2-7 Cisco VPN Client—VPN GUI Application Window



Click **Next** to continue, **Previous** to go back to a previous step, or **Cancel** to quit the installation process.

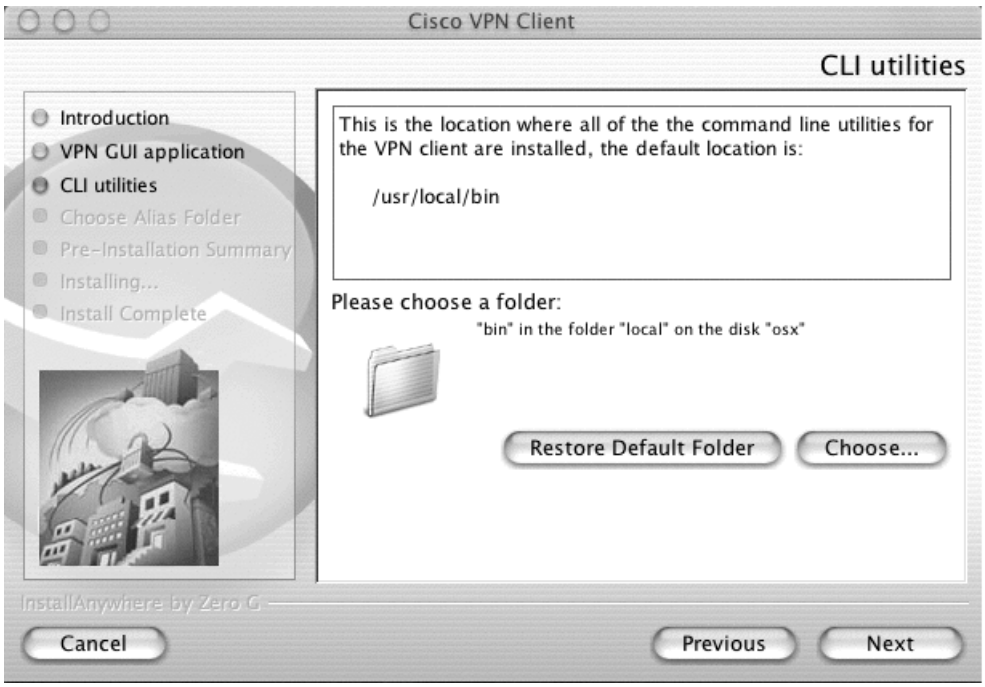
Choosing the CLI Utilities Location

Install the VPN client command-line utilities in the default folder /usr/local/bin, or choose another folder. If you choose another folder, a browser window appears. Locate the directory for the CLI installation and click **Choose**. The new CLI utilities folder is listed on the CLI Utilities window (Figure 2-8).

Note If you choose a different folder for the CLI utilities, you must update your paths or use the full path when you run the VPN client application.

Note If you are running Macintosh OS Version 10.2, /usr/local/bin is not provided as the default path.

Figure 2-8 Cisco VPN Client—CLI Utilities Window



Click **Next** to continue, **Previous** to go back to a previous step, or **Cancel** to quit the installation process.

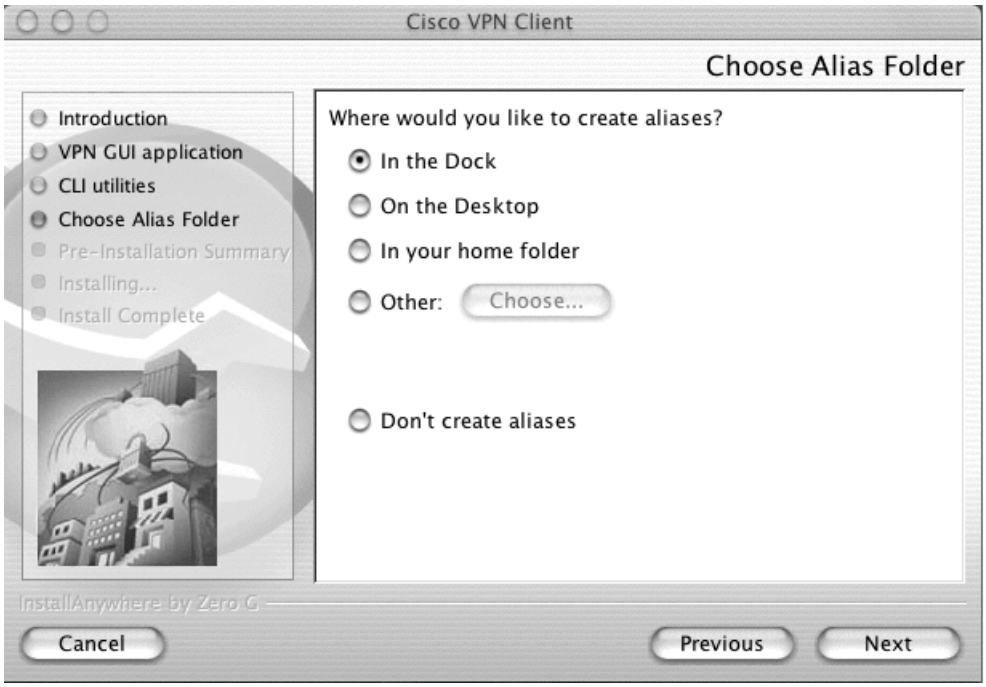
Choosing the Alias Folder

The alias folder contains the shortcut to VPN client application. You can store aliases:

- In the dock
- On the desktop
- In your home folder
- In a different directory. Click **Browse** to locate a folder in a different directory. Locate the new directory for the VPN client aliases and click **Choose**. The new alias folder is listed on the Choose Alias Folder window (Figure 2-9).

Creating aliases is optional. If you do not want to create aliases, select the **Don't create aliases** radio button.

Figure 2-9 Cisco VPN Client—Choose Alias Folder Window

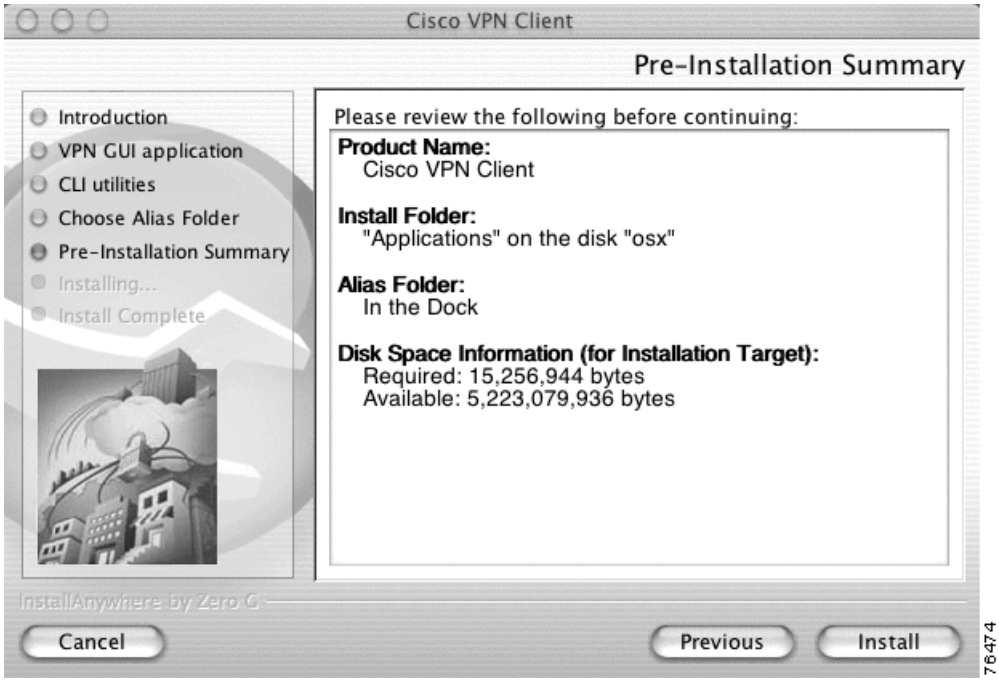


Click **Next** to continue, **Previous** to go back to a previous step, or **Cancel** to quit the installation process.

Checking the Preinstallation Summary

The Preinstallation Summary window (Figure 2-10) lists the installation selection that were chosen in the previous installation steps.

Figure 2-10 Cisco VPN Client—Preinstallation Summary Window



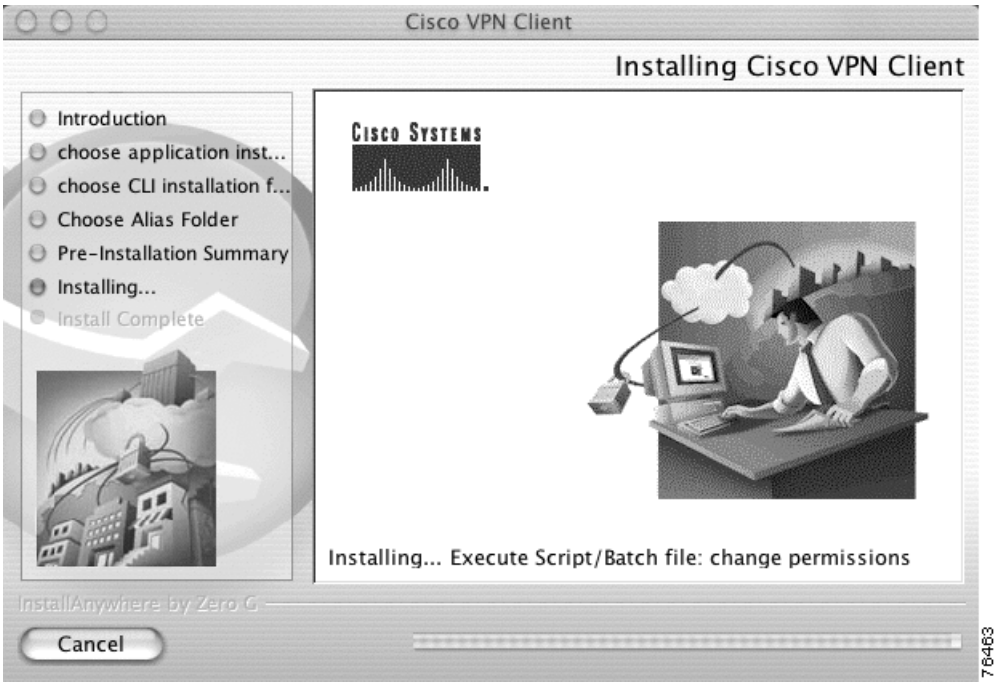
Be sure that all of the installation selections are correct.

- If the summary information is correct, click **Install** to continue.
- If it is not correct, click **Previous** to return to any of the previous installation windows to adjust your selections. Alternately, you can return to a previous step by clicking the radio button next to that step.

Installing the VPN Client Application

During the application installation, the operations taking place are displayed above the blue progress bar at the bottom of the Installing Cisco VPN Client window (Figure 2-11).

Figure 2-11 Cisco VPN Client—Installing Cisco VPN Client Window



The VPN client application installation process includes the following:

- Creating custom VPN initialization file
- Installing packaged profiles
- Installing packaged images
- Installing images

To stop the installation process, click **Cancel**. A warning prompt appears (Figure 2-12) to remind you that the installation is not complete.

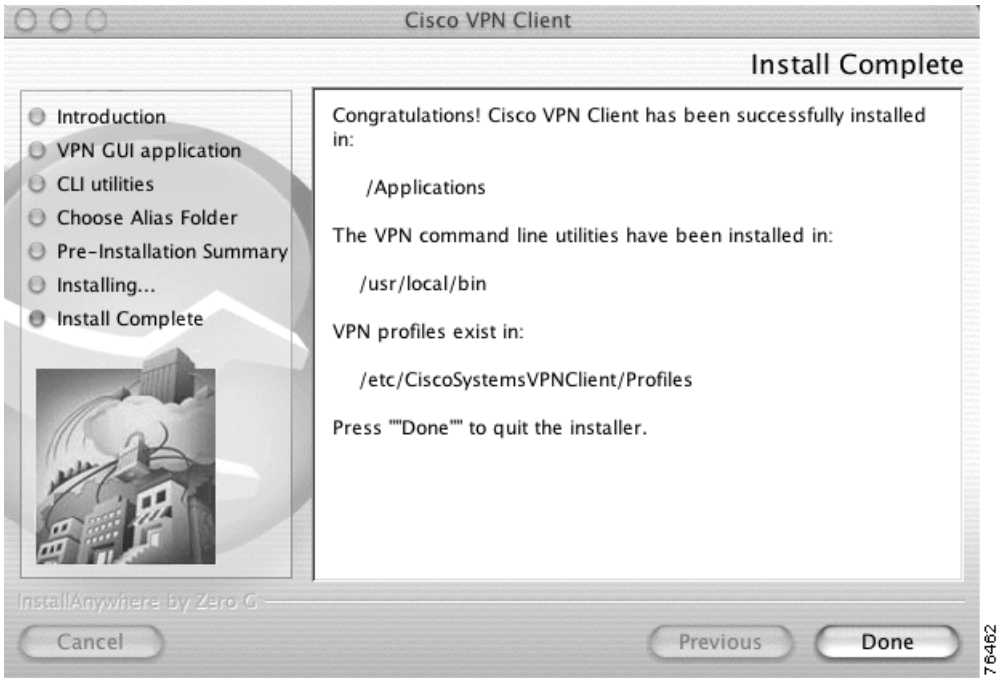
Figure 2-12 Cancel Installation Warning

If you choose:

- **Quit**, the VPN client installer closes. You must restart the installation process from the beginning before you can begin using the VPN client.
- **Resume**, the installation process continues.

The Install Complete window appears (Figure 2-13) when the installation is complete.

Figure 2-13 Cisco VPN Client—Install Complete Window



Click **Done** to close the installer.

If you do not receive this confirmation, the installation was not successful. You must start the installation process again from the beginning or contact your network administrator for assistance.

CLI Version Install Script Notes

The VPN client installer includes both the graphical user interface and the command-line version of the VPN Client for Mac OS X. You can choose to manage the VPN client using only the command-line.

Use the following commands to start, stop, and restart VPN service:

- /System/Library/StartupItems/CiscoVPN/CiscoVPN start
- /System/Library/StartupItems/CiscoVPN/CiscoVPN stop
- /System/Library/StartupItems/CiscoVPN/CiscoVPN restart

During the installation process, the application binaries are copied to the specified destination directory.

Uninstalling the VPN Client

The following sections describe how to uninstall the VPN client.

Note You must uninstall any previous version of the VPN client for Mac OS X before you install a new version.

Uninstalling the CLI-Only Version

To uninstall the VPN client for Mac OS X (CLI version—Release 3.6.x or earlier):

a. Locate the script vpn_uninstall.

   This file must be run as root.

b. You are prompted to remove all profiles and certificates.

   – If you answer yes, all binaries, startup scripts, certificates, profiles, and any directories that were created during the installation process are removed.

   – If you answer no, all binaries and startup scripts are removed, but certificates, profiles, and the vpnclient.ini file remain.

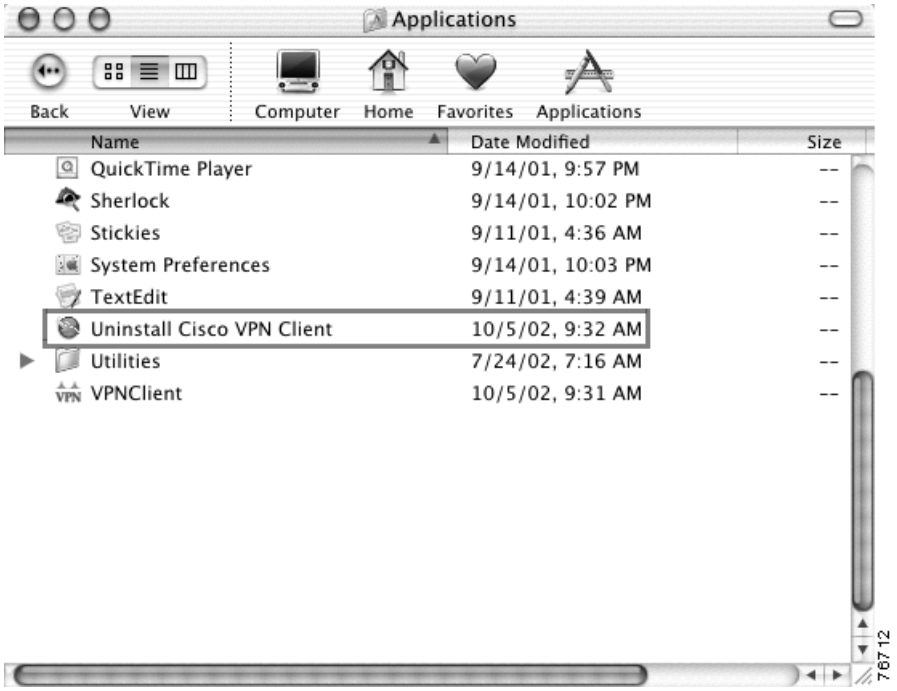
Uninstalling the GUI Version

To uninstall the VPN client (GUI-based— Release 3.7):

Step 1 Open the Applications folder from the Finder.

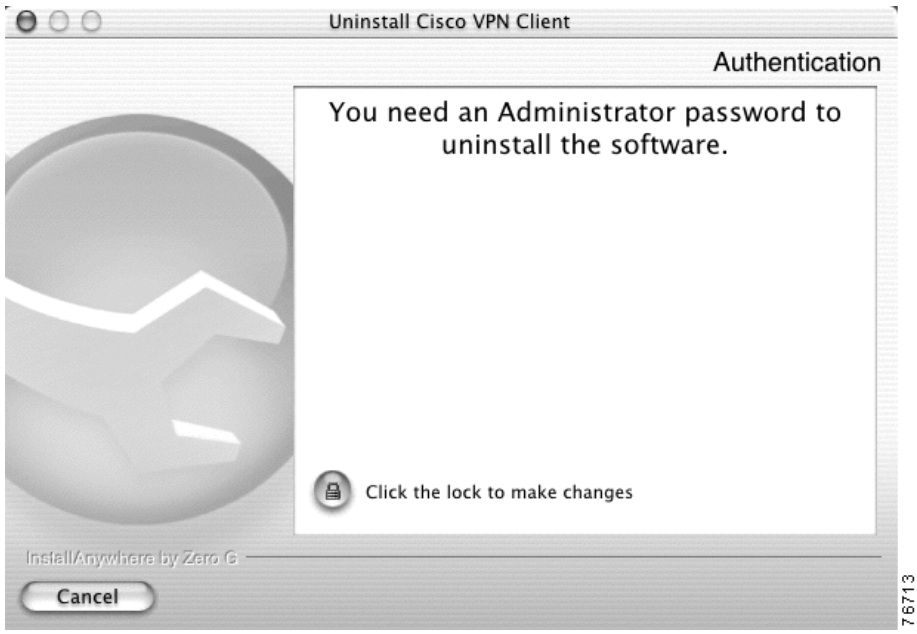
Step 2 Double-click the Uninstall Cisco VPN Client file, located above the Utilities folder (Figure 2-14).

Figure 2-14 Uninstall Cisco VPN Client File



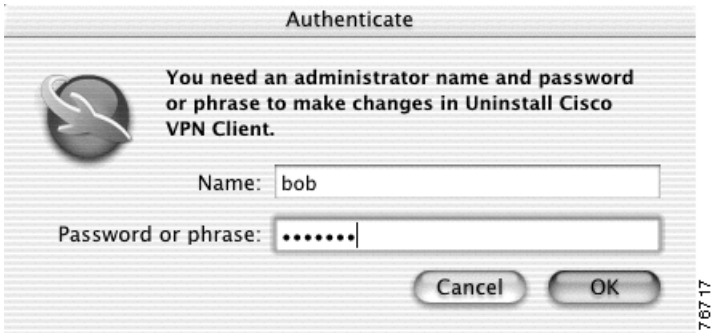
The Authentication window appears (Figure 2-15). You must have an administrator password to uninstall the VPN client.

Figure 2-15 Uninstall Cisco VPN Client



Step 3 Click the lock at the bottom left corner of the Authentication window. The Authenticate dialog box appears (Figure 2-16).

Figure 2-16 Authenticate Dialog Box

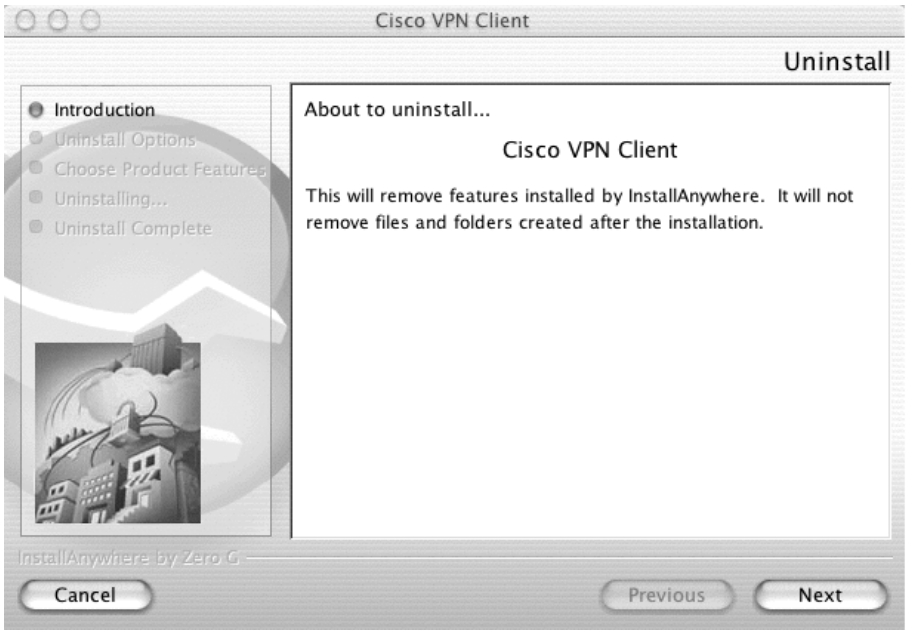


Step 4 Enter your administrator username and a password or challenge phrase.

Step 5 Click **OK**. If the authentication is successful, you can continue to uninstall the VPN client. Contact your network administrator if you cannot authenticate for an uninstall.

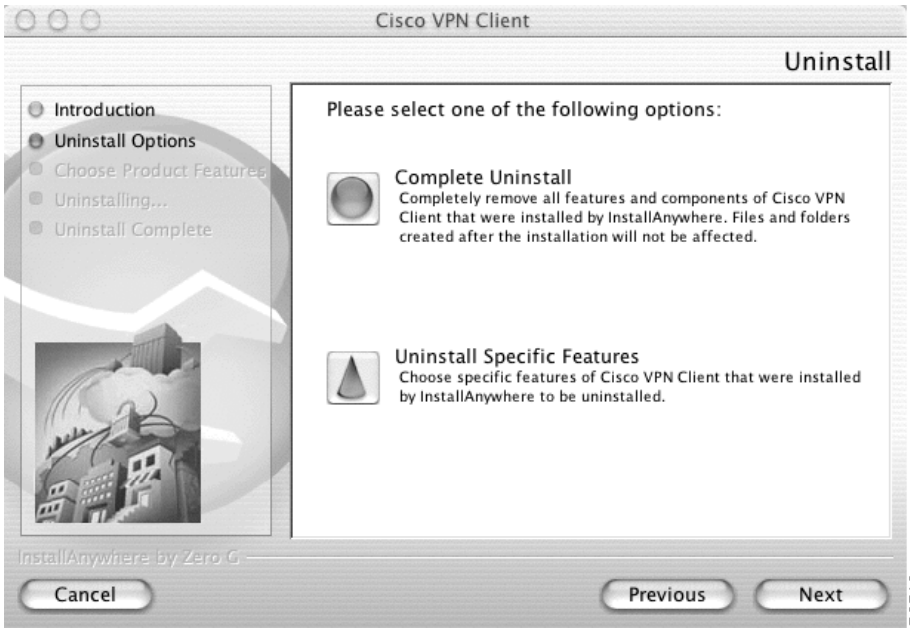
Step 6 The Uninstall Introduction window appears (Figure 2-17)

Figure 2-17 Uninstall Introduction Window



Step 7 Click **Next** to continue. The Uninstall Options window appears (Figure 2-18).

Figure 2-18 Cisco VPN Client—Uninstall Options Window

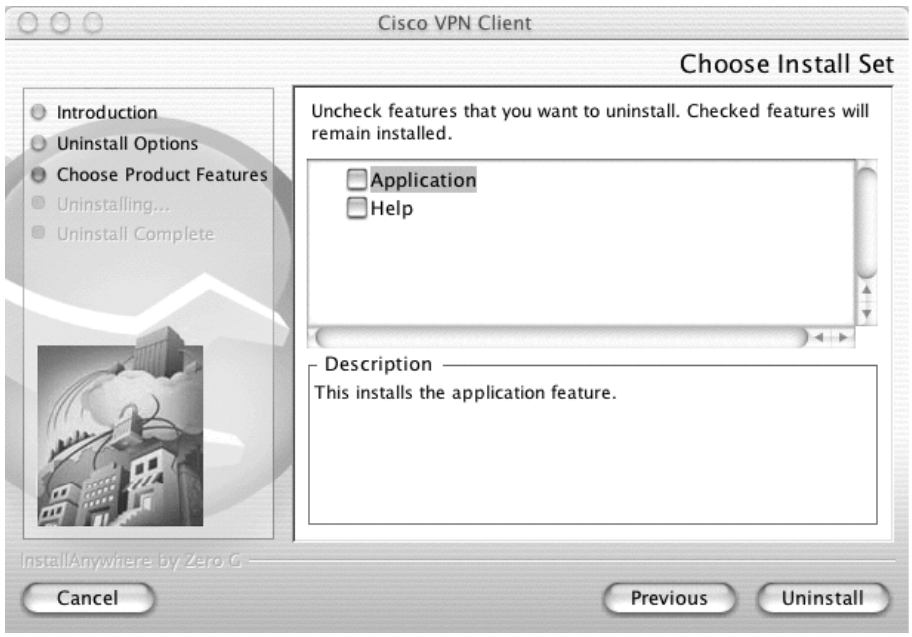


Step 8 Select your Uninstall option. Click **Next** to continue.

If you choose:

- Complete Uninstall, all features and components associated with the VPN client are uninstalled.
- Uninstall Specific Features, the Choose Install Set window appears (Figure 2-19).

Figure 2-19 Cisco VPN Client—Choose Install Set Window



Step 9 Uncheck features to uninstall. Any feature that is checked will remain installed.

- Application—Uninstalls the VPN client application.
- Help—Uninstalls the Help system (not available in Release 3.7).

Step 10 Click **Uninstall**. The VPN client application, folders, and aliases are uninstalled.

If you receive an error while uninstalling the VPN client software, contact your network administrator for assistance.

To reinstall the VPN client software, return to the "Installing the VPN Client" section on page 2-4.

CHAPTER 3

Navigating the User Interface

This chapter describes the main VPN client window and the tools, tabs, menus and icons for navigating the user interface.

Choosing a Run Mode

You can run the VPN client in simple mode or in advanced mode. The default is simple mode.

- Use simple mode if you only want to start the VPN client application and establish a connection to a VPN device using the default connection entry.
- Use Advanced mode to manage the VPN client, configure connection entries, manage certificates, to view and manage event logging, or to view tunnel routing data.

To toggle between advanced mode and simple mode, press **Command-T**. Alternately, you can choose your mode from the view menu.

VPN Client Window—Simple Mode

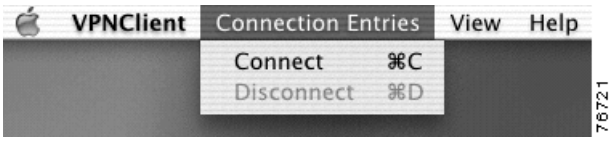
When you run in simple mode, you are presented with a scaled-down version of the VPN client user interface (Figure 3-1).

Figure 3-1 VPN Client Window—Simple Mode

The main VPN client window shows only the version information, the default connection entry, the connect button, and the status bar.

The Connection Entries menu also changes according to which mode you are running in (Figure 3-2).

Figure 3-2 Simple Mode Connection Entries Menu



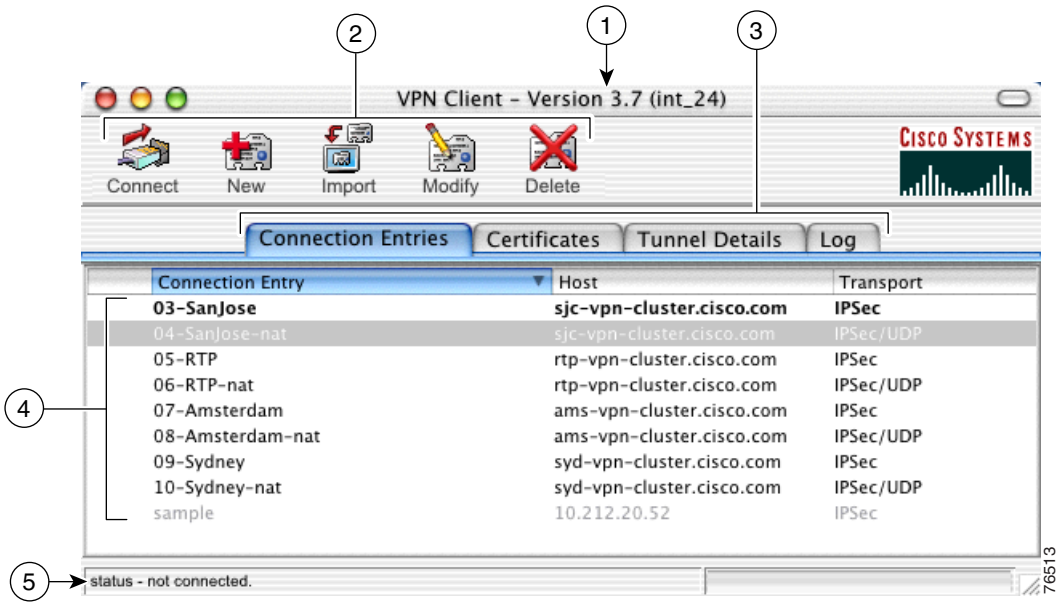
In simple mode, only the Connect/Disconnect choices are available. You can choose to connect or disconnect the default connection entry.

VPN Client Window—Advanced Mode

The following sections describe the main VPN client 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 3-3 shows the VPN client window and the primary navigation areas.

Figure 3-3 Main VPN Client Window



1	VPN client version information.	**4**	Display area for the main tabs.
2	Toolbar action buttons. The buttons that are available depend on which tab is forward.	**5**	Connection status bar. The left side of the status bar indicates the connection entry name and connection status. When connected, the right side displays the amount of time that this VPN session has been established.
3	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.

For example, if the **Connections** tab is forward, the Connect, New, Import, Modify, and Delete buttons control operations for the selected connection entry (see Figure 3-3 above). If the **Certificates** tab is forward, the View, Import, Export, Enroll, Verify, and Delete buttons control operations for the selected certificate (Figure 3-4).

Figure 3-4 Toolbar Buttons—Certificates Tab

Main Tabs—Advanced Mode

This section describes the four main tabs for managing the VPN client (Figure 3-5).

Figure 3-5 VPN Client GUI Main Tabs

The four main tabs include:

- 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 Chapter 4, “Configuring Connection Entries” for more 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 Chapter 6, “Managing Certificates” for more details on the Certificates tab.
- Tunnel Details tab—Displays information related to the active VPN session. This includes IP addresses assigned for this session, byte and packet transfer statistics, encryption and authentication algorithms, and tunneling options. Refer to Chapter 7, “Managing the VPN Client” for more information.
- Log tab—Displays event messages from all processes that contribute to the client-peer connection, including enabling logging, clearing the event log, viewing the event log in an external window, and setting logging levels. Refer to Chapter 7, “Managing the VPN Client” for more information.

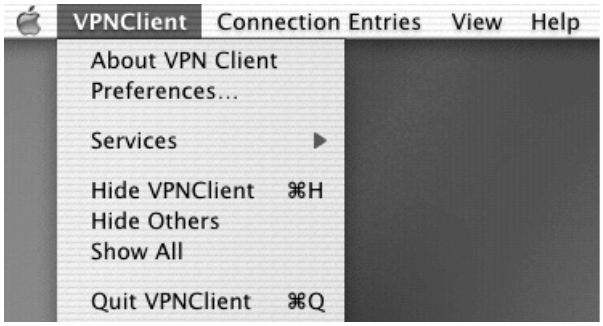
Main Menus—Advanced Mode

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

VPN Client Menu

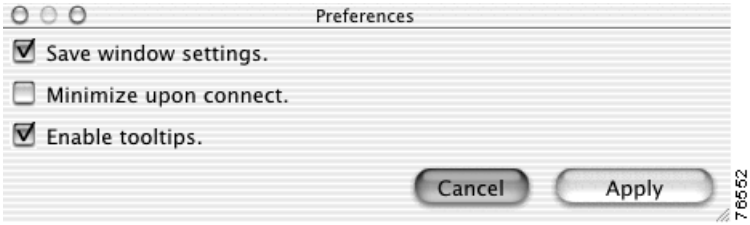
Use the VPN client menu (Figure 3-6) to manage the VPN client application and main window settings.

Figure 3-6 VPN Client Menu



- About VPN Client—Displays the current VPN client version, the VPN client type (platform), and the copyright information.
- Preferences—Sets VPN client window preferences (Figure 3-7).

Figure 3-7 VPN Client Window Preferences

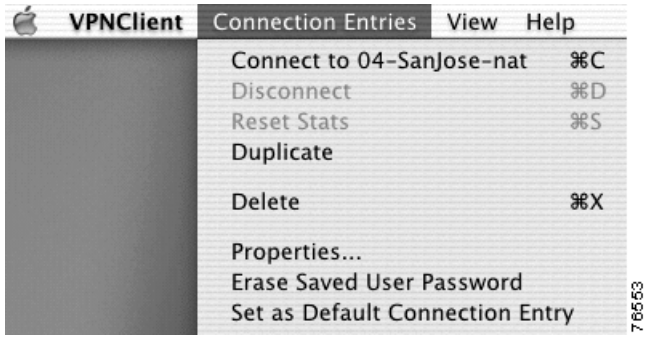


  - Save window settings—Saves any changes you make to the VPN client window
  - Minimize upon connect—Places the VPN client window in the dock when the VPN connection is established
  - Enable tooltips—Enables tool tips for the toolbar action buttons
- Services—Access standard Mac OS X services.
- Hide VPN Client—Remove the VPN client window from your screen. This option does not close the application or minimize the screen.
- Hide Others—Remove all windows except the VPN client from your screen.
- Show All—Displays all windows that were previously hidden.
- Quit VPN Client—Closes the VPN client application.

Connection Entries Menu

Use the Connection Entries menu (Figure 3-8) as a shortcut to frequently-used connection entry operations.

Figure 3-8 Connection Entries Menu



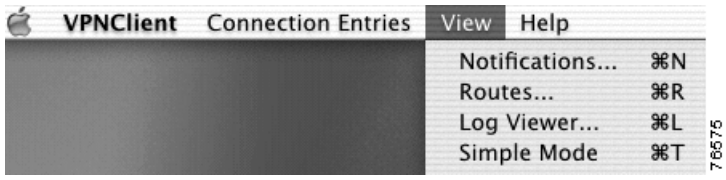
- Connect to—Establish a VPN connection using the selected connection entry. If the Connections tab is not selected, a submenu, which lists all available connection entries, is displayed.
- Disconnect—Disconnect the current VPN session.
- Reset Stats—Reset the VPN session statistics on the Tunnel Details tab.
- Delete—Delete the selected connection entry.
- Properties—Display the properties of the selected connection entry. This action opens the VPN Client Properties window.
- Duplicate—Duplicate the selected connection entry. This menu choice allows you to create a new connection entry using the configuration from a current connection entry as a template.
- Erase Saved User Password—Erases 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.

To configure a connection entry, see Chapter 4, “Configuring Connection Entries.”

View Menu

Use the View menu (Figure 3-9) to display the event log or tunnel details in a separate window.

Figure 3-9 View Menu



- Notifications—Open the Notifications window to view notices from the VPN device.
- Routes—Open the Routes window to view excluded and secured routes for the current VPN session.

- Show Log Viewer—Open the External Log View window.
- Simple Mode/Advanced Mode—Toggle between Simple Mode and Advanced Mode.

Note The Help menu is not available with Release 3.7.

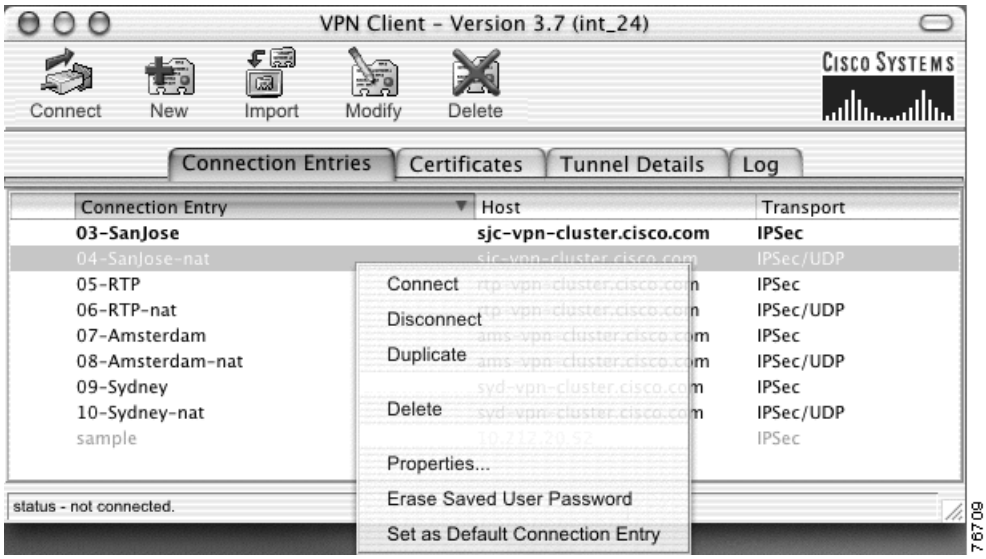
Right-Click Menus

Use the right-click menus from the Connection Entries tab or the Certificates tab as an alternate method for performing frequent VPN client operations. If your mouse has only one button, use **Ctrl-Click** to access the right-click menus.

Connection Entries Tab Right-Click Menu

Figure 3-10 shows the right-click menu options that are available when the Connection Entries tab is selected.

Figure 3-10 Connection Entries Right-Click Menu



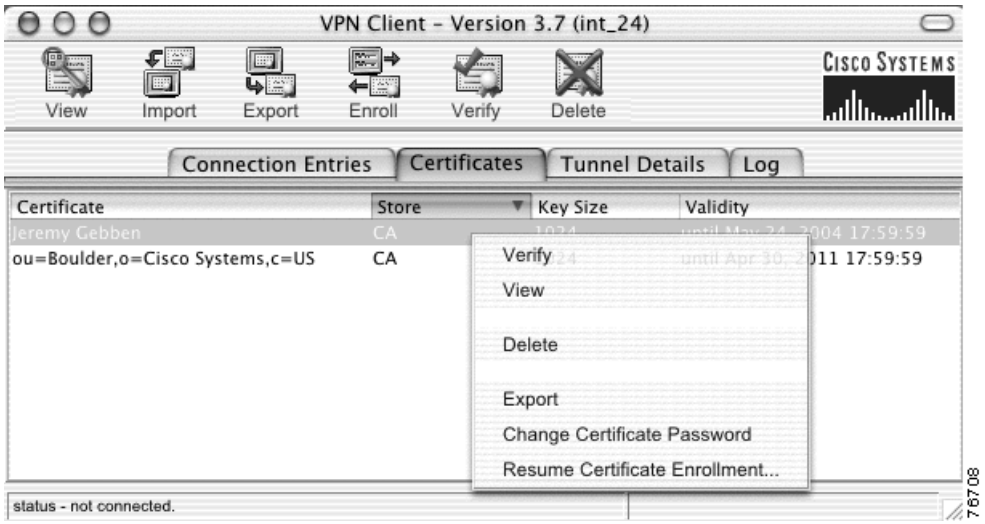
- Connect—Establish a VPN connection using the selected connection entry.
- Disconnect—Disconnect the current VPN session.
- Duplicate—Duplicate the selected connection entry. This action allows you to create a new connection entry using the configuration from a current connection entry as a template.
- Delete—Delete the selected connection entry.
- Properties—Display the properties of the selected connection entry. This action opens the VPN Client Properties window.

- Erase Saved User Password—Erases 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 3-11 shows the right-click menu options that are available when the Certificates tab is forward.

Figure 3-11 Certificates Tab Right-Click Menu



- Verify—Verify that the selected certificate is valid.
- View—View the properties of the selected certificate.
- Delete—Delete the selected certificate
- Export—Export the selected certificate to a specified file location
- Change Certificate Password—Change the password used to protect the certificate while it is in the VPN client certificate store.
- Resume Certificate Enrollment—Resume a previously started certificate enrollment.

Configuring Connection Entries

A connection entry is a set of parameters that the VPN client uses to identify and connect to a specific private network.

Connection entry parameters include a name and description for the connection, the name or address of the VPN device (the remote server providing the connection), and authentication information that identifies you as a valid user to the VPN device.

This chapter describes how to configure the parameters for a VPN client connection entry.

Creating a Connection Entry

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

- The VPN device that is providing access to the network.
- Preshared keys—The IPSec group that you have been assigned to. Your IPSec group determines the set of privileges you have for accessing and using the private 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 IPSec group.

To create a connection entry:

Step 1 Open the VPN client application. The VPN client window appears (Figure 4-1).

Figure 4-1 VPN Client Window

Step 2 Click the Connection Entries tab.

Step 3 Click **New** at the top of the VPN client window. The Create New VPN Connection Entry dialog box appears (Figure 4-2).

Figure 4-2 Create New VPN Connection Entry

Step 4 Enter a unique connection entry name. You can use any name to identify this connection. 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 to further identify this connection. For example, Connection to Engineering remote server.

Step 6 Enter the Host name or IP address of the remote VPN device that is providing access to the private network.

Step 7 Use the Authentication tab to select an authentication method. You can connect as part of a group, which is configured on the VPN device, or by supplying an identity digital certificate. See the "Authentication Methods" section on page 4-4 for more information.

Step 8 Use the Transport tab to set transport parameters. See the "Transport Parameters" section on page 4-6 for more information.

Step 9 Use the Backup Servers tab to view the current list of backup servers or to manually add a backup server. See the "Backup Servers" section on page 4-8 for more information.

Step 10 The **Erase User Password** button at the bottom of this dialog box erases 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.

Step 11 Click **Save**. The Connection Entry dialog box closes and you return to the Connection Entries tab.

Authentication Methods

You can configure a connection entry to authenticate as part of a group, which is configured on the VPN device, or by supplying an identity digital certificate. The Authentication tab on the Connection Entry Settings dialog box must be forward to select an authentication method for a connection entry.

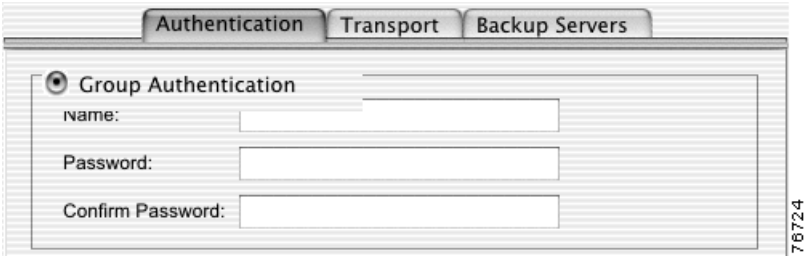
Group Authentication

Use this procedure if you plan to use group authentication for this connection entry.

To configure group authentication:

Step 1 From the Authentication tab, click the **Group Authentication** radio button (Figure 4-3).

Figure 4-3 Group Authentication



Step 2 Enter the name of the IPSec group you belong to.

Step 3 Enter the password for your IPSec group. The field displays only asterisks.

Step 4 Confirm the password by entering it again.

Step 5 Click **Save**. The Connection Entry dialog box closes and you return to the Connection Entries tab.

Certificate Authentication

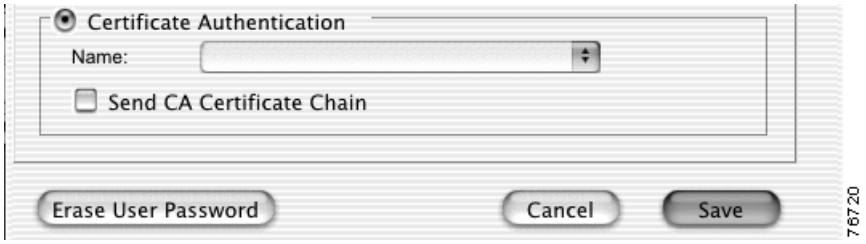
Use this procedure if you plan to use digital certificates for authenticating for this connection entry.

You can obtain a digital certificate for use with the VPN client by enrolling with a Public Key Infrastructure (PKI) or by importing a certificate from a file.

To configure this connection entry for a digital certificate:

Step 1 From the Authentication tab, click the **Certificate Authentication** radio button (Figure 4-4).

Figure 4-4 Certificate Authentication



Step 2 Select a certificate from the **Name** drop-down menu.

If the **Name** field displays No Certificates Installed, you must first enroll or import a certificate before you can use this feature. See the "Enrolling Certificates" section on page 6-2 or "Importing a Certificate" section on page 6-5 for more information.

Step 3 To send CA certificate chains, check the **Send CA Certificate Chain** check box. This parameter is disabled by default.

A CA certificate chain includes all CA certificates in the certificate hierarchy from the root certificate. This must be installed on the VPN client to identify each certificate. This feature enables a peer VPN Concentrator to trust the VPN client's identity certificate given the same root certificate, without having the same subordinate CA certificates actually installed.

The following is an example of a certificate chain:

- On the VPN client, you have this chain in the certificate hierarchy:
  a. Root Certificate
  b. CA Certificate 1
  c. CA Certificate 2
  d. Identity Certificate
- On the VPN Concentrator, you have this chain in the certificate hierarchy
  a. Root Certificate
  b. CA Certificate
  c. Identity Certificate

Though the identity certificates are issued by different CA certificates, the VPN device can still trust the VPN client's identity certificate, because it has received the chain of certificates installed on the VPN client PC.

This feature provides flexibility because the intermediate CA certificates do not need to be installed on the peer.

Step 4 Click **Save**. The Connection Entry dialog box closes and you return to the Connection Entries tab.

Transport Parameters

This section describes transport parameters you can configure for a connection entry.

The transport parameters include:

- Enable Transport Tunneling, page 4-7
- Transparent Tunneling Mode, page 4-7
- Allow Local LAN Access, page 4-7
- Peer Response Timeout, page 4-8

To configure transport parameters:

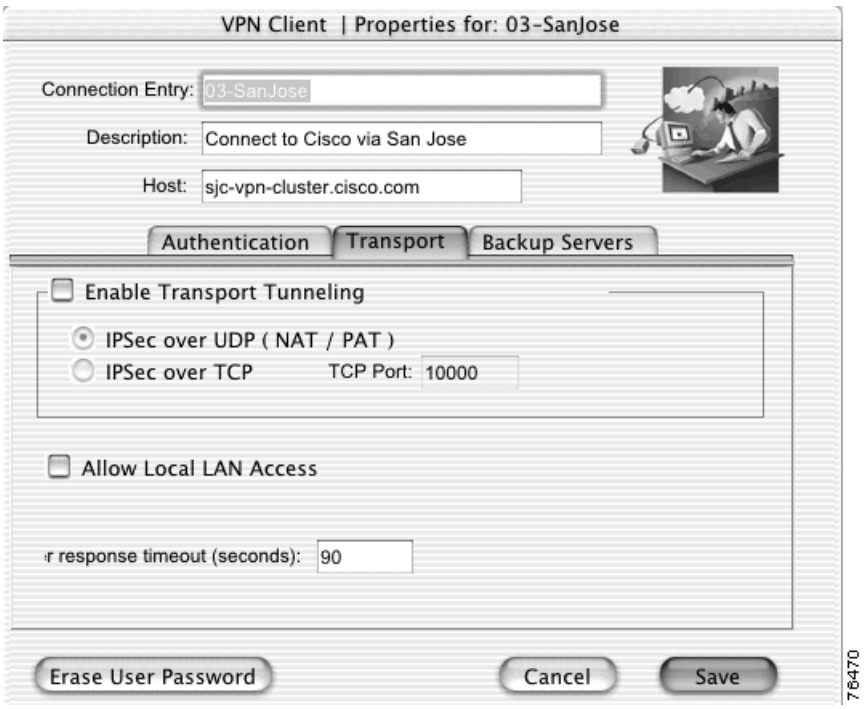
Step 1 Open the VPN client application.

Step 2 Select a connection entry.

Step 3 Click **Modify** at the top of the VPN client window to access the VPN Client Properties dialog box.

Step 4 Click the **Transport** tab (Figure 4-5) to display the existing transport parameters configured for this connection entry.

Figure 4-5 Transport Settings



Step 5 Select your transport settings. Refer to the following sections for more information on transport settings.

Step 6 Click **Save**. The VPN Client Properties dialog box closes and you return to the Connection Entries tab.

Enable Transport Tunneling

Transparent tunneling allows secure transmission between the VPN client and a secure gateway through a router serving as a firewall. The router might also be configured for Network Address Translation (NAT) or Port Address Translations (PAT).

Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets. It allows 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.

Not all devices support multiple simultaneous connections behind them. Some cannot map additional sessions to unique source ports. Check with your device's vendor to see if this limitation exists. Some vendors support Protocol 50 (ESP) PAT, which might let you operate without enabling transparent tunneling.

- To use transparent tunneling, the IPSec group in the Cisco VPN device must be configured to support it.
- Transparent Tunneling is enabled by default. To disable this parameter, clear the check box. We recommend that you keep this parameter enabled.

Transparent Tunneling Mode

The transparent tunneling mode you select must match the mode used by the VPN device providing your connection to the private network.

- If you select IPSec over UDP (NAT/PAT), the default mode, the port number is negotiated.
- If you select TCP, you must enter the port number for TCP in the TCP port field. This port number must match the port number configured on the VPN device. The default port number is 10000.

Note Either mode operates properly through a PAT device. Multiple simultaneous connections might work better with TCP, and if you are in an extranet environment, TCP mode is preferable. UDP does not operate with stateful firewalls. Use TCP with this configuration.

Allow Local LAN Access

The Allow Local LAN Access parameter gives you access to resources on your local LAN when you are connected through a secure gateway to a central-site VPN device.

- When this parameter is enabled:
  - You can access local resources (printer, fax, shared files, other systems) while connected.
  - You can access up to 10 networks. A network administrator at the central site configures a list of networks at the VPN client side that you can access.
  - If 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).
  - If enabled on the VPN client and permitted on the central-site VPN device, you can see a list of the local LANs that are available by clicking the **Routes** button on the **Tunnel Details** tab. For more information, see the "Routes" section on page 7-6.

- When this parameter is disabled, all traffic from your client system goes through the IPSec connection to the secure gateway.

If the local LAN you are using is not secure, you should not enable local LAN access. For example, do not enable this feature when you are using a local LAN in a hotel or airport.

To enable this feature, check the **Allow Local LAN Access** check box.

Peer Response Timeout

The VPN client uses DPD to check the availability of the VPN device on the other side of an IPSec tunnel. 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.

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.

To adjust the setting, enter the number of seconds in the **Peer response timeout** field. The configuration range for this parameter is 30 to 480 seconds. The default number of seconds the VPN client waits before terminating a connection is 90.

Backup Servers

The private network you are connecting to might include one or more backup VPN devices (servers) to use if the primary server is not available. The list of available backup servers is pushed to the VPN client when the connection is established, or you can add a backup server to the list manually.

The list of existing backup servers is found on the Backup Servers tab for each connection entry. Your network administrator can provide information regarding backup servers.

To use backup servers, you must enable this parameter.

To enable backup servers:

Step 1 Open the VPN client application.

Step 2 Select a connection entry.

Step 3 Click **Modify** at the top of the VPN client window. The VPN Client Properties dialog box appears.

Step 4 Click the **Backup Servers** tab (Figure 4-6).

Figure 4-6 Backup Servers Tab

Step 5 Check the **Enable Backup Servers** check box. This parameter is not enabled by default. The list of available backup servers is displayed.

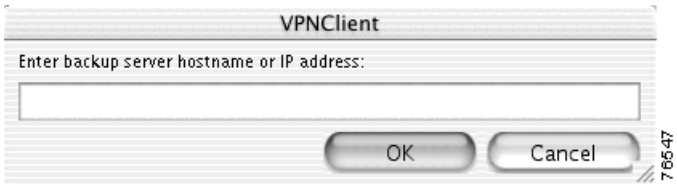
Backup servers are used in the order presented in the list. To change the order in which the backup servers are used, select a backup server and use the arrow buttons to move the server up or down in the list.

Step 6 Click **Save**. The VPN Client Properties dialog box closes and you return to the Connection Entries tab.

If there are no backup servers listed, or if you want to manually add a server to the list, use the following procedure.

Step 1 Click the **Add** button on the **Backup Servers** tab. The VPN client dialog box appears (Figure 4-7).

Figure 4-7 Add Backup Server



Step 2 Enter the hostname or IP address of the backup server to add.

Step 3 Click **OK**. The backup server is added to the list of available backup servers.

To remove a backup server, return to the **Backup Server** tab, select a server from the list, and click **Remove**.

CHAPTER 5

Establishing a VPN Connection

This chapter describes how to establish a VPN connection with a private network using the VPN client and the user authentication methods supported by the VPN device that is providing your connection.

Checking Prerequisites

Before you can establish a VPN connection, you must have:

- At least one connection entry configured on the VPN client. See Chapter 4, "Configuring Connection Entries" for more information.
- User authentication information. This includes your username and password, and depending on the configuration of your connection entry, might also include:
  - Passwords for RADIUS authentication
  - VPN group name and password for connections to VPN devices
  - PINs for RSA Data Security
  - Digital certificates and associated passwords
- An Internet connection

Contact your network administrator for prerequisite information.

Establishing a Connection

To establish a VPN connection:

Step 1 Double-click the VPN client icon to open the application (Figure 5-1). The icon should be located on the desktop or in the dock. Alternately, you can choose VPN Client from the Applications menu.

Figure 5-1 VPN Client Icon

The main VPN client window appears. Figure 5-2 shows the VPN client window in simple mode.

Figure 5-2 VPN Client Window—Simple Mode

Figure 5-3 shows the VPN client window in advanced mode.

Figure 5-3 VPN Client Window—Advanced Mode

See Chapter 3, "Navigating the User Interface" for more information on simple mode and advanced mode.

Step 2 From the Connection Entries tab, select the connection entry to use for this VPN session (advanced mode only).

Step 3 Click **Connect** at the top of the VPN client window or double-click the selected connection entry (for simple mode, click the **Connect** button).

Step 4 Respond to all user authentication prompts.

The user authentication prompts that appear depend on the configuration for this connection entry. See the "Choosing Authentication Methods" section on page 5-3 for information about the user authentication methods the VPN client supports.

The status bar at the bottom of the main VPN client window displays your connection status. When connected, the left side of the status bar indicates the connection entry name and the right side displays the amount of time that the VPN tunnel has been established.

Choosing Authentication Methods

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

The VPN client supports:

- Shared key or VPN group name and group password for authenticating the VPN device
- RADIUS server, RSA Security (SecurID), Digital Certificates for authenticating the user.

The authentication prompts displayed during the connection process depend on the configuration of your IPSec group. Refer to appropriate section in this chapter for more information on the user authentication method configured for each connection entry.

Note User names and passwords are case-sensitive. You have three opportunities to enter the correct information before an error message indicates that authentication failed. Contact your network administrator if you cannot pass user authentication.

The following sections describe each user authentication method that the VPN client supports.

Shared Key Authentication

The shared key authentication method uses the username and shared key password for authentication (Figure 5-4). The shared key password must be the same as the shared key password configured on the VPN device that is providing the connection to the private network.

Figure 5-4 Shared Key Authentication

Enter your Username and Password and click **OK**.

VPN Group Name and Password Authentication

The VPN group login method uses your VPN group name and password for authentication (Figure 5-5). You can use VPN group authentication alone or with other authentication methods.

Figure 5-5 VPN Group Authentication

Enter your group name and password and click **OK**. The group name is the name of the IPSec group configured on the VPN device for this connection entry.

RADIUS Server Authentication

You can use RADIUS server authentication with VPN group authentication. With this type of authentication, two prompts appear. The first prompt is for the VPN group name and password, and the RADIUS user authentication prompt follows (Figure 5-6).

Figure 5-6 User Authentication for RADIUS

Enter your username and password and click **OK**.

Check the **Save Password** check box if you do not want to be prompted for your RADIUS password each time you start a VPN session using this connection entry.

Note If you cannot choose the Save Password option, your system administrator does not allow this option. If you can choose this option, be aware that using it might compromise system security, because your password is 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, choose Erase User Password from the Connection Entries menu.

SecurID Authentication

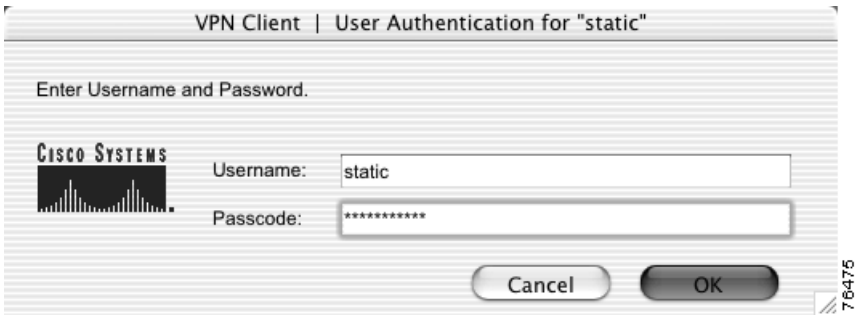
RSA SecurID authentication methods include physical SecurID cards and keychain fobs, and PC software called SoftID for passcode generation. SecurID cards can vary. The passcode might be combination of a PIN and a card code, or you might be required to enter a PIN on the card to display the passcode. Ask your network administrator for the correct procedure.

When you use SecurID passcodes for authentication:

- The process varies slightly for different operating systems.
- If you use physical SecurID cards or keychain fobs, the VPN client displays the appropriate RSA user authentication dialog box.
- If you use SoftID for passcode generation, it must be running on your workstation.

In most configurations, you use SecurID with VPN group authentication. With this type of authentication, two prompts appear. The first prompt is for the VPN group name and password, and the SecurID user authentication prompt follows (Figure 5-7).

Figure 5-7 User Authentication for SecurID



Enter your username and SecurID passcode and click **OK**.

Using Digital Certificates

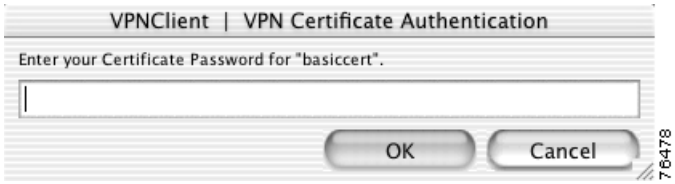
The VPN client works with Certificate Authorities (CAs) that support SCEP, manual enrollment, or PKCS import.

Each time you establish a VPN connection using a certificate, the VPN client verifies that your certificate is not expired.

- Valid— A message appears that indicates the validation period for this certificate.
- Expired—A warning appears that indicates when the certificate expired.

Each digital certificate is protected by a password. If the connection entry you are using requires a digital certificate for authentication, the VPN Certificate Authentication dialog box appears (Figure 5-8).

Figure 5-8 Certificate Password



Enter the certificate password and click **OK**.

For more information on digital certificates, see Chapter 6, “Managing Certificates.”

CHAPTER 6

Managing Certificates

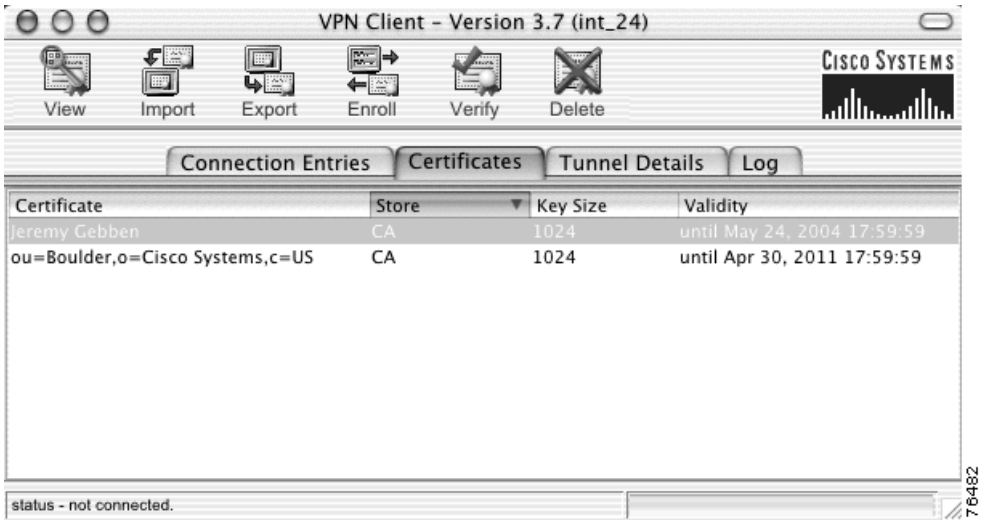
This chapter describes how to enroll and manage digital certificates for the VPN Client for Mac OS X.

Certificate Stores

The VPN client uses the notion of *store* to convey a location in your local file system for storing personal certificates. The main store for the VPN client is the Cisco store.

The Certificates tab on the VPN client window displays the list of certificates in your certificate store (Figure 6-1).

Figure 6-1 Certificate Store



For each certificate, the following information is listed:

- Certificate—The name of the certificate.
- Store—The certificate store where this certificate resides. If you enroll a certificate from a Certificate Authority, the store is CA. If you import a certificate from a file, the store is Cisco.

- Key Size—The size, in bits, of the signing key pair.
- Validity—The date and time when this certificate expires.

The Cisco store contains certificates enrolled through the Simple Certificate Enrollment Protocol (SCEP) and certificates that have been imported from a file.

Enrolling Certificates

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).

To enroll a digital certificate you must enroll using the PKI Framework standards, receive approval from the CA, and have the certificate installed on your system.

You can enroll a digital certificate:

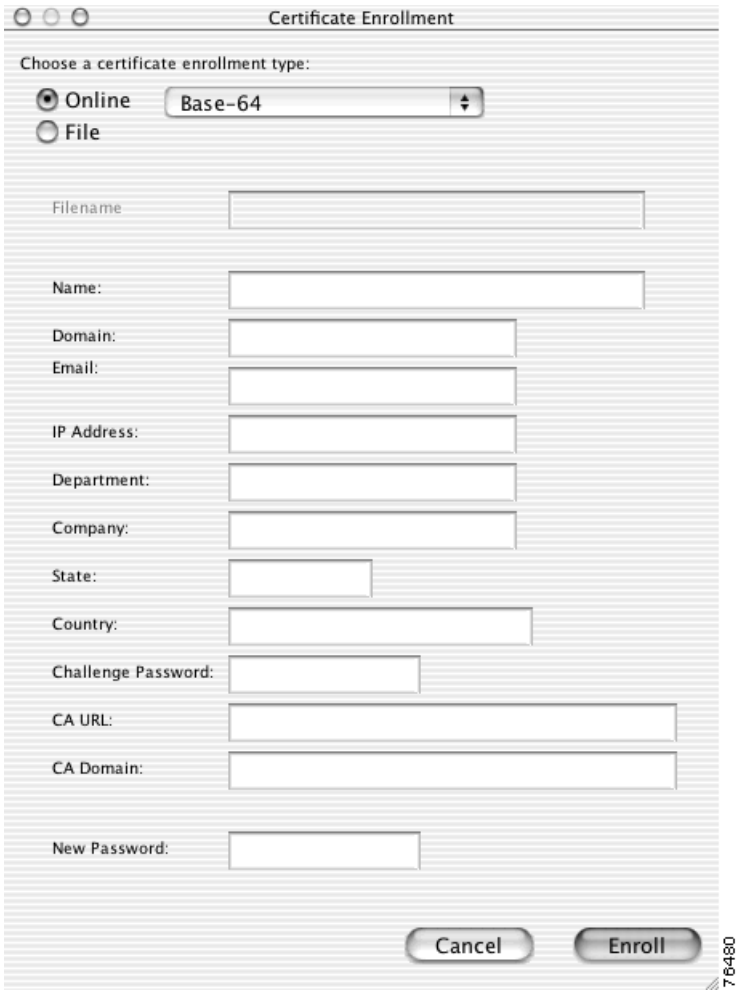
- Over the network from a CA
- From an enrollment request file

To enroll a digital certificate for user authentication:

Step 1 Click the Certificates tab.

Step 2 Click **Enroll** at the top of the VPN client window. The Certificate Enrollment dialog box appears (Figure 6-2).

Figure 6-2 Certificate Enrollment



Step 3 Choose a certificate enrollment type.

- If you choose **Online**, you obtain a certificate by enrolling with a CA over the network.

  Choose the encoding type of the output file from the drop-down menu.

  - Base-64, the default, is an ASCII-encoded PKCS10 file that you can display because it is in a text format. Use this type when you want to cut and paste the text into the CA's website.

- If you choose **File,** the VPN client generates an enrollment request file that you can email to a CA or post into a webpage form.

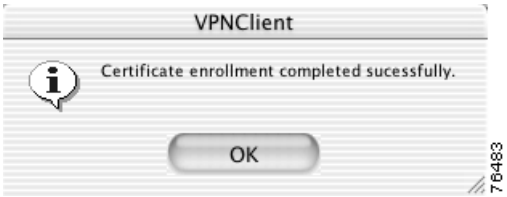
Step 4 Enter the certificate enrollment parameters. All fields are required unless they are grayed out. Table 6-1 describes the entry fields.

Table 6-1 Certificate Enrollment Parameters

Entry Field	Description
Filename	The full pathname for the file request. For example, /Users/Anna/Documents/Certificates/mycert.p10. This field is only available when you select a **File** enrollment type.
Name	The common name for the certificate. 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, Fred Flinstone.
Domain	The Fully Qualified Domain Name (FQDN) of the host for your system. For example, Dialin_Server.
Email	The user e-mail address for the certificate. email@company.com
IP Address	The IP address of the user's system. For example, 192.168.23.9
Department	The VPN group that this user belongs to. 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 company name for the certificate.
State	The state for the certificate.
Country	The 2-letter country code for your country. For example, US. This two-letter country code must conform to ISO 3166 country abbreviations.
Challenge Phrase	Some CAs require that you enter a password to access their site. Enter this password in the Challenge Phrase field. You can obtain the challenge phrase from your administrator or from the CA.
CA URL	The URL or network address of the CA. For example, http://198.162.41.9/certsrv/mcep/mcep.dll.
CA Domain	The CA's domain name. For example, qa2000.com.
New Password	The password for this certificate. Each digital certificate is protected by a password. If you create a connection entry that requires a digital certificate for authentication, you must enter the certificate password each time you attempt a connection.

Step 5 Click **Enroll** to enroll a certificate from a CA. A prompt indicates whether the certificate enrollment is successful (Figure 6-3).

Figure 6-3 Enrollment Complete



If the certificate enrollment is not successful, contact your network administrator.

Importing a Certificate

A network administrator might place a certificate in a file. This certificate must be imported in to the certificate store before you can use it for authenticating the VPN client to a VPN device.

To import a certificate from a file:

Step 1 Click the Certificates tab.

Step 2 Click **Import** at the top of the VPN client window. The Import Certificate dialog box appears (Figure 6-4).

Figure 6-4 Import Certificate

Step 3 Enter the path to the certificate you want to import. If you do not know the location, browse to the folder where the certificate is located and click **Open** on the browser window. The import path is automatically entered in the Import Certificate dialog box.

To import a digital certificates you need two different passwords.

- The first password is the one used to protect the certificate file, called the import password, and is assigned by the system administrator.
- The second password is assigned by you to protect the certificate while it is in your certificate store. This password is optional but we recommend that you always protect your certificate with a password.

Step 4 Enter the import password.

Step 5 Enter a password to protect the certificate while it is in the VPN client certificate store.

Step 6 Verify the certificate store password.

Step 7 Click **Import**. The certificate is installed in the VPN client certificate store.

Viewing a Certificate

To view the contents of a certificate in the certificate store:

Step 1 Click the Certificates tab.

Step 2 Select the certificate you want to view.

Step 3 Click **View** at the top of the VPN client window or double-click the certificate. The Certificate Properties window appears (Figure 6-5).

Figure 6-5 Certificate Properties

A typical digital certificate contains the following information:

- Common name—The name of the owner, usually both the first and last names. This field identifies the owner within the Public Key Infrastructure (PKI organization).
- Department—The name of the owner's department. This is the same as the organizational unit in the Subject field.
- Company—The company in which the owner is using the certificate. This is the same as the organization in the Subject field.
- State—The state in which the owner is using the certificate.
- Country—The 2-character country code in which the owner's system is located.
- Email—The e-mail address of the owner of the certificate.
- Thumbprint—An MD5 hash of the certificate's complete contents. This provides a means for validating the authenticity of the certificate. For example, if you contact the issuing CA, you can use this identifier to verify that this certificate is the correct one to use.
- Key size—The size of the signing key pair in bits.

- Subject—The fully qualified distinguished name (FQDN) of the certificate's owner. This field uniquely identifies the owner of the certificate in a format that can be used for LDAP and X.500 directory queries. A typical subject includes the following fields:
  - common name (**cn**)
  - organizational unit, or department (**ou**)
  - organization or company (**o**)
  - locality, city, or town (**l**)
  - state or province (**st)**
  - country (**c)**
  - e-mail address (**e)**

  Other items might be included in the Subject, depending on the certificate.
- Issuer—The fully qualified distinguished name (FQDN) of the source that provided the certificate.
- Serial number—A unique identifier used for tracking the validity of the certificate on the Certificate Revocation Lists (CRLs).
- Not valid before—The beginning date that the certificate is valid.
- Not valid after—The end date beyond which the certificate is no longer valid.

Step 4 Click **Close** to return to the VPN client window.

Exporting a Certificate

To export a certificate from the certificate store to a specified file:

Step 1 Click the Certificates tab.

Step 2 Click **Export** at the top of the VPN client window. The Export Certificate dialog box appears (Figure 6-6).

Figure 6-6 Export Certificate

Step 3 Enter the path for the export certificate. If you do not know the export path, browse to the export directory and click **Open** on the browser window. The export path is automatically entered in the Export Certificate dialog box.

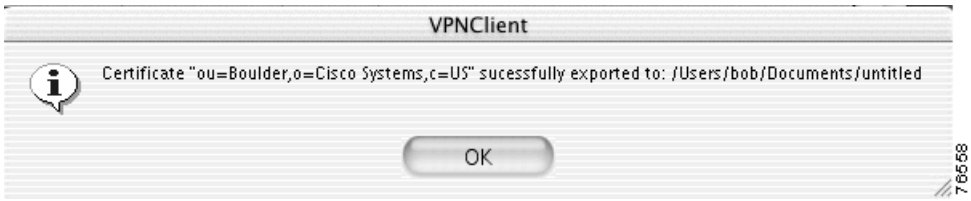
Step 4 To export the entire certificate chain, check the box next to this parameter.

Step 5 Enter a password to protect the exported certificate file. We recommend that you always enter a password to protect your certificates.

Step 6 Verify the exported certificate file password.

Step 7 Click **Export**. The certificate is copied to the selected directory and a prompt (Figure 6-7) indicates whether the export is successful.

Figure 6-7 Successful Export Prompt



Step 8 Click **OK** to return to the VPN client window.

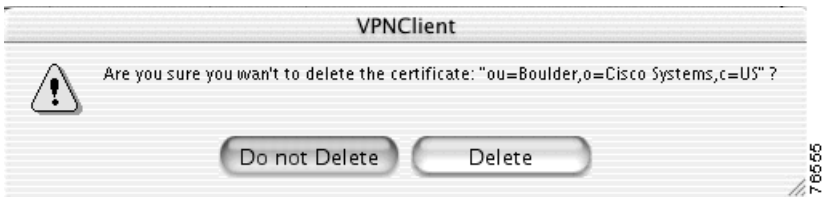
Deleting a Certificate

To delete a certificate from your certificate store:

Step 1 Click the Certificates tab.

Step 2 Click **Delete** at the top of the VPN client window. A warning prompt appears (Figure 6-8).

Figure 6-8 Delete Certificate Warning



Caution You cannot retrieve a certificate that has been deleted.

Step 3 Verify the name of the certificate and click **Delete**. The selected certificate is deleted from the certificate store.

Click **Do not Delete** to return to the VPN client window without deleting the selected certificate.

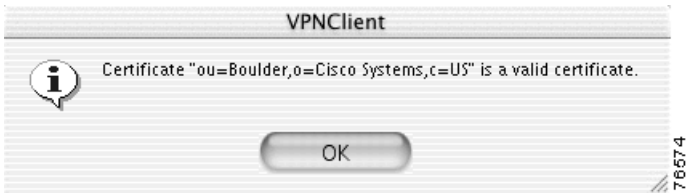
Verifying a Certificate

To verify that a certificate is valid:

Step 1 Click the Certificates tab.

Step 2 Click **Verify** at the top of the VPN client window. A prompt appears (Figure 6-9) to indicate the validity of the certificate.

Figure 6-9 Verify Certificate



Step 3 Click **OK** to return to the VPN client window.

If your certificate is invalid, contact the network administrator for instructions.

CHAPTER 7

Managing the VPN Client

This chapter describes how to manage connection entries, and view and manage the event logging.

Managing Connection Entries

The following sections describe the operations used to manage connection entries. This includes how to import, modify, and delete a connection entry.

Importing a Connection Entry

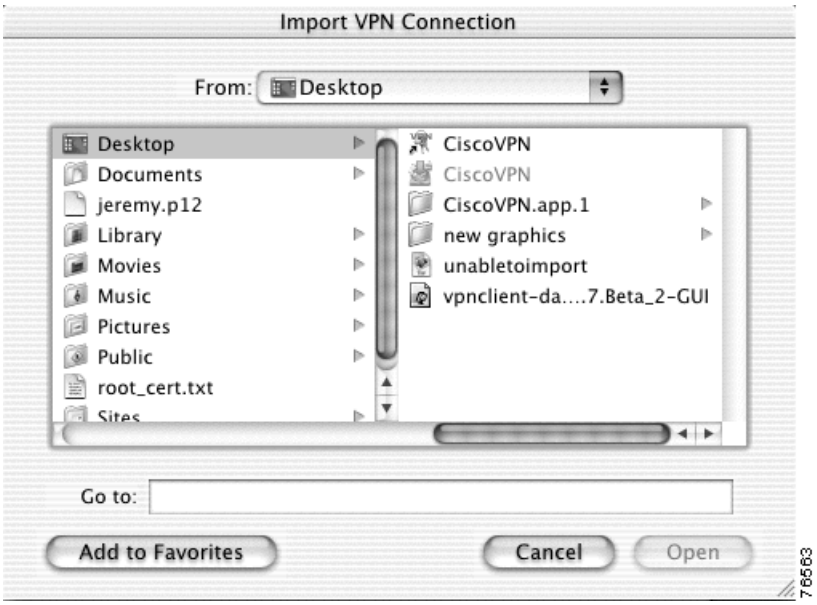
You can automatically configure your VPN client with new settings by importing a new configuration file (a file with a .pcf extension, called a profile) supplied by your network administrator.

To import a stored profile:

Step 1 Click the Connection Entries tab.

Step 2 Click **Import** at the top of the VPN client window. The Import VPN Connection dialog box appears (Figure 7-1).

Figure 7-1 Import VPN Connection



Step 3 Locate the connection entry to import. A valid connection entry configuration file must have a .pcf extension.

Step 4 Click **Open**. The connection entry is added to the list of available profiles and you return to the Connection Entries tab.

Alternately, you can copy the .pcf file into the profiles directory and restart the VPN client application.

Modifying a Connection Entry

You can make changes to a connection entry at any time. The new configuration is stored in the profiles directory and is applied during the next connection attempt.

To modify a connection entry:

Step 1 Click the Connection Entries tab.

Step 2 Select the connection entry to modify.

Step 3 Click **Modify** at the top of the VPN client window. The VPN Client Properties dialog box appears (Figure 7-2).

Figure 7-2 Connection Entry Settings

The existing configuration for this connection entry is displayed.

Step 4 Make adjustments to this connection entry configuration.

Step 5 Click **Save**. The VPN Client Properties dialog box closes and you return to the Connection Entries tab.

Deleting a Connection Entry

You can delete any connection entry that does not have an active VPN connection.

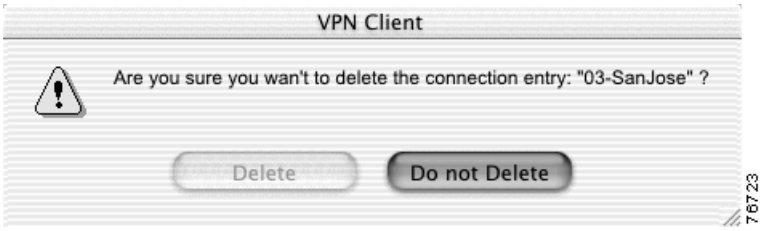
To delete a connection entry:

Step 1 The Connection Entries tab must be forward.

Step 2 Select the connection entry to delete.

Step 3 Click **Delete** at the top of the VPN client window. You are prompted to confirm the connection entry to delete (Figure 7-3).

Figure 7-3 Confirm Delete



Caution You cannot retrieve a connection entry that has been deleted.

Step 4 Click **Delete** to delete this connection entry. The connection entry is removed from the profiles directory and you are returned to the Connection Entries tab.

Click **Do not Delete** to return to the VPN client window without deleting the selected connection entry.

Viewing Tunnel Details

The Tunnel Details tab displays information related to the active VPN session, including:

- IP addresses assigned for this session
- Byte and packet transfer statistics
- Encryption and authentication algorithms
- Split tunneling
- NAT transparency
- Data compression

Figure 7-4 shows the Tunnel Details tab display, which includes the IP addresses assigned for this session and byte and packet statistics.

Figure 7-4 Tunnel Details Tab

Use the **Reset** button at the top of the VPN client window to clear the fields in the tunnel details display. Alternately, you can reset the statistics by choosing **Reset Stats** from the Connection Entries menu.

Table 7-1 describes the Tunnel Details statistics.

Table 7-1 Tunnel Details

Field	Description
Client	IP address assigned to the client for this VPN session
Server	IP address of the VPN device you are connected to.
Packets Encrypted	Number of packets encrypted during this VPN session.
Packets Decrypted	Number of packets decrypted during this VPN session.
Packets Discarded	Number of packets discarded during this VPN session.
Packets Bypassed	Number of packets bypassed during this VPN session.
Bytes Received	Number of bytes received by the client during the active session.
Bytes Sent	Number of bytes sent by the client during the active session.
Encryption	Encryption algorithm used for this VPN session. The VPN client supports: • 56-bit DES (Data Encryption Standard) • 168-bit Triple-DES • AES 128-bit and 256-bit **Note** The VPN client continues to support DES/MD5. However, support for DES/SHA is no longer available, and Release 3.7 VPN clients cannot connect to any central-site device group that is configured for (or proposing) DES/SHA. The VPN client must either connect to a different group or the system administrator for the central-site device must change the configuration from DES/SHA to DES/MD5 or another supported configuration. The *Cisco VPN Client Administrator Guide* lists all supported encryption configurations.
Authentication	Authentication algorithm used for this VPN session. The VPN client supports: • HMAC-MD 5 (Hashed Message Authentication Coding with Message Digest 5 hash function) • HMAC-SHA-1 (Secure Hash Algorithm hash function)
NAT	Displays whether NAT is enabled; if enabled, lists the protocol and port number.
Local LAN	Displays whether Local LAN access (split tunneling) is enabled.
Compression	Displays what type of data compression is used, if any.

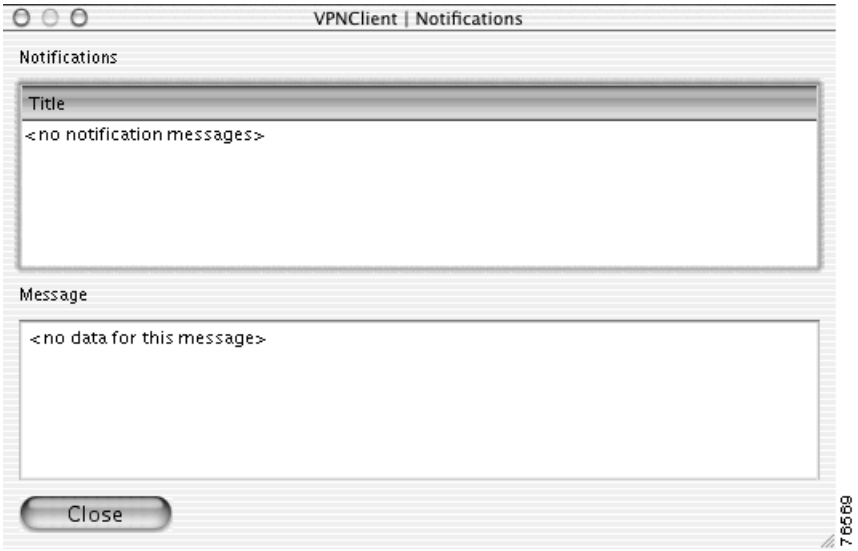
Notifications

The VPN device that provides your connection to the private network might send notifications to the VPN client. These notifications appear on the Notifications window. To display the notifications window (Figure 7-5), click **Notifications** on the **Tunnel Connections** tab.

When you first establish a VPN connection, you receive a notification regarding your connection. This is typically the login banner or connection history.

Other notifications might include messages from your network administrator about upgrades to the VPN client software or information regarding the specific VPN device you are connected to.

Figure 7-5 Notifications Window



The top pane of the Notifications window lists the title of each stored notification. The bottom pane displays the notification message associated with the selected title.

All notifications from the VPN device are stored in this display during the VPN session. Every VPN session contains at least one notification, the connection history.

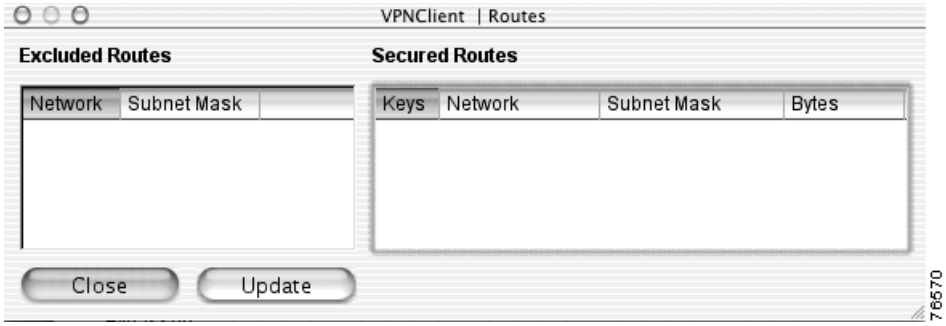
Routes

The routes window displays the routes that VPN traffic takes into the network, which can be either excluded routes or secured routes.

- Excluded routes are routes that are excluded from the Local LAN.
- Secured routes are routes that go through the secured VPN tunnel.

To display route data during an active VPN session, click **Routes** on the **Tunnel Connections** tab. The Routes window appears (Figure 7-6).

Figure 7-6 VPN Client Routes



The excluded routes pane displays:

- Network—The IP address of the VPN device providing the excluded route to the network.
- Subnet Mask—The subnet mask applied to the excluded route.

The secured routes pane displays:

- Keys—An established Security Association (SA). When you establish a connection using a secured route, an SA is created, and a key appears next to that route to represent that keys have been established.
- Network—The IP address of the VPN device providing the secured route to the network.
- Subnet Mask—The subnet mask applied to the secured route
- Bytes—The number of bytes passed through the secured route.

Event Logging

The following sections describe how to view and manage the VPN client event log.

The event log can help you diagnose problems with an IPSec connection between the VPN client and a peer VPN device. The log collects event messages from all processes that contribute to the client-peer connection.

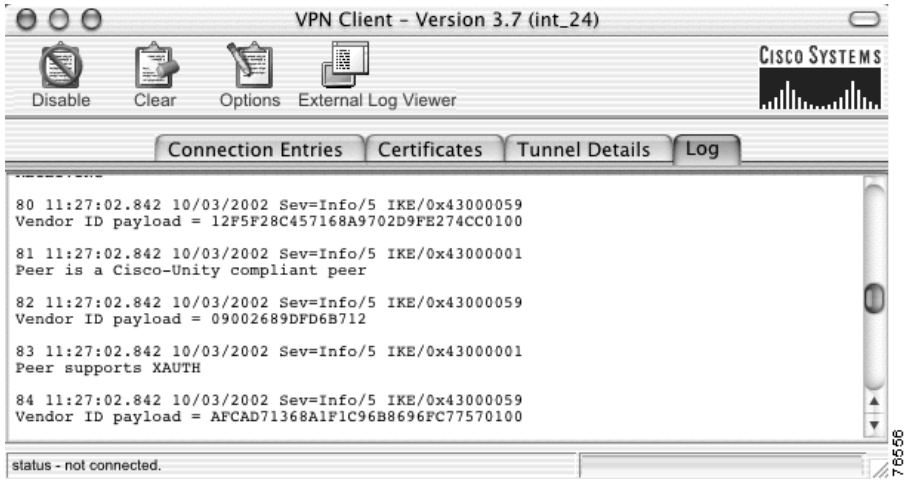
From the Log tab on the VPN client window you can:

- Enable logging
- Clear the logging display
- View the event log in an external window
- Set or change the logging levels.

Enable Logging

To enable logging, click **Enable** at the top of the VPN client window. The event logging window displays (Figure 7-7).

Figure 7-7 Event Log



Every VPN session contains at least one log entry, the connection history.

To disable logging, click the **Disable** button at the top of the VPN client window.

Clear Logging

To clear the event messages from the logging window, click **Clear** at the top of the VPN client window. Clearing the display does not reset event numbering or clear the log file itself.

Note If you want to store the event messages, you must manually copy and paste them into a text file before you clear the display.

Set Logging Options

Logging options apply to the active VPN session. Changing the logging settings clears the event log and the new logging settings take effect immediately.

To set logging options for the VPN client:

Step 1 Click the Log tab.

Step 2 Click **Options** at the top of the VPN client window. The Logging Options dialog box appears (Figure 7-8).

Figure 7-8 Logging Options

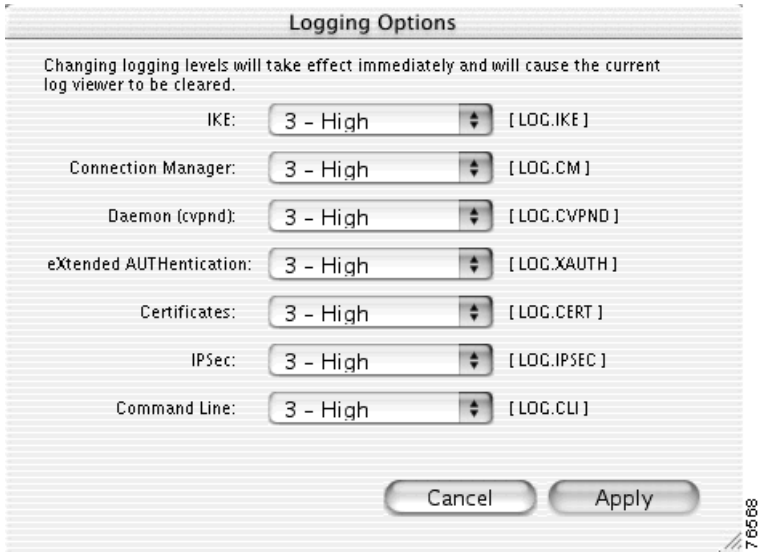


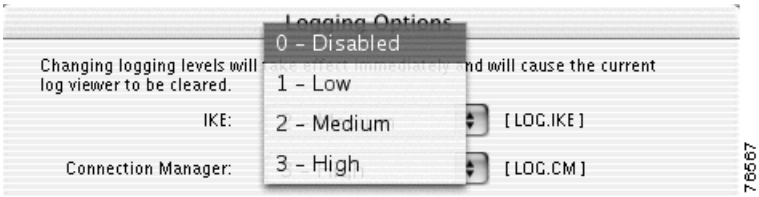
Table 7-2 describes the log classes that generate events in the VPN client log viewer.

Table 7-2 VPN Client Logging Classes

Log Class	Description	Module
[LOG.IKE]	Internet Key Exchange module, which manages secure associations.	IKE
[LOG.CM]	Connection Manager (CM), which drives VPN connections. (CM dials a PPP device, configures IKE for establishing secure connections, and manages connection states.)	Connection Manager
[LOG.CVPND]	Cisco VPN Daemon, which initializes client service and controls the messaging process and flow.	Daemon (cvpnd)
[LOG.XAUTH]	Extended authorization application, which validates a remote user's credentials.	eXtended AUTHentication
[LOG.CERT]	Certificate management process, which handles obtaining, validating, and renewing certificates from certificate authorities. CERT also displays errors that occur as you use the application.	Certificates
[LOG.IPSEC]	IPSec module, which obtains network traffic and applies IPSec rules to it.	IPSec
[LOG.CLI]	Command-Line Interface, which allows you to perform certain operations from the command line rather than using the VPN client graphical user interface.	Command Line

Step 3 Select the logging level for each module that uses logging services.The logging levels allow you to choose the amount of information you want to capture. Figure 7-8 shows the logging levels.

Figure 7-9 Logging Levels



There are four logging levels:

- **0**—Disables logging services for the specified [LOG] class.
- **1**—Low, displays only critical and warning events. This is the default.
- **2**—Medium, displays critical, warning, and informational events.
- **3**—High, displays all events.

Step 4 Click **Apply**. This clears the event log and immediately applies the new logging levels.

External Log Viewer

To display the events log in a separate window, click **External Log Viewer** at the top of the VPN client window. The VPN client Connection Log window appears (Figure 7-10).

Figure 7-10 Connection Log

To save the data in the event log, copy and paste the log into a text file.

INDEX

Symbols

A

B

C

K

L

M

N

O

P

R

S

T

U

V

W

X