



VPN Client User Guide for Mac OS X

Release 4.6

August 2004

Corporate Headquarters

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

Customer Order Number:
Text Part Number: OL-5490-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

VPN Client User Guide for Mac OS X
Copyright © 2004, Cisco Systems, Inc.
All rights reserved.



About This Guide	vii
Audience	vii
Contents	vii
Related Documentation	viii
Terminology	viii
Document Conventions	viii
Data Formats	ix
Obtaining Documentation	ix
Cisco.com	ix
Documentation CD-ROM	ix
Ordering Documentation	x
Documentation Feedback	x
Obtaining Technical Assistance	x
Cisco.com	x
Technical Assistance Center	xi
Cisco TAC Website	xi
Cisco TAC Escalation Center	xii
Obtaining Additional Publications and Information	xii

CHAPTER 1

Understanding the VPN Client	1-1
Connection Technologies	1-1
VPN Client Overview	1-2
VPN Client Features	1-3
Program Features	1-3
Authentication Features	1-5
IPSec Features	1-5
VPN Client IPSec Attributes	1-6

CHAPTER 2

Installing the VPN Client	2-1
Verifying System Requirements	2-1
Gathering Information You Need	2-1
Obtaining the VPN Client Software	2-2
Preconfiguring the VPN Client	2-2

- Preconfiguring the User Profile 2-3
- Preconfiguring the Global Profile 2-3
- Bundling a Root Certificate with the Installation Package for Darwin 2-4
- Installing the VPN Client 2-4
 - Authentication 2-4
 - VPN Client Installation Process 2-6
 - Introduction 2-6
 - Accepting the License Agreement 2-7
 - Selecting the Application Destination 2-7
 - Choosing the Installation Type 2-8
 - CLI Version Install Script Notes 2-12
- Uninstalling the VPN Client 2-12

CHAPTER 3

Navigating the User Interface 3-1

- VPN Client Menu 3-1
- Choosing a Run Mode 3-2
- Operating in Simple Mode 3-2
 - VPN Client Window—Simple Mode 3-2
 - Main Menus—Simple Mode 3-3
 - Connection Entries Menu 3-3
 - Status Menu 3-3
- Operating in Advanced Mode 3-4
 - VPN Client Window—Advanced Mode 3-4
 - Toolbar Action Buttons—Advanced Mode 3-5
 - Main Tabs—Advanced Mode 3-5
 - Main Menus—Advanced Mode 3-6
 - Connection Entries Menu 3-6
 - Status Menu 3-7
 - Certificates Menu 3-7
 - Log Menu 3-8
 - Right-Click Menus 3-8
 - Connection Entries Tab Right-Click Menu 3-9
 - Certificates Tab Right-Click Menu 3-10

CHAPTER 4

Configuring Connection Entries 4-1

- Creating a Connection Entry 4-1
- Authentication Methods 4-3
 - Group Authentication 4-3

Mutual Group Authentication	4-4
Certificate Authentication	4-4
Transport Parameters	4-6
Enable Transport Tunneling	4-7
Transparent Tunneling Mode	4-7
Allow Local LAN Access	4-7
Peer Response Timeout	4-8
Backup Servers	4-8

CHAPTER 5

Establishing a VPN Connection	5-1
Checking Prerequisites	5-1
Establishing a Connection	5-1
Connecting to a Default Connection Entry	5-3
Choosing Authentication Methods	5-3
Shared Key Authentication	5-3
VPN Group Name and Password Authentication	5-4
RADIUS Server Authentication	5-4
SecurID Authentication	5-5
Using Digital Certificates	5-6

CHAPTER 6

Enrolling and Managing Certificates	6-1
Using the Certificate Store	6-1
Enrolling Certificates	6-2
Managing Enrollment Requests	6-5
Viewing the Enrollment Request	6-5
Deleting an Enrollment Request	6-5
Changing the Password on an Enrollment Request	6-6
Retrying an Enrollment Request	6-6
Importing a Certificate	6-7
Viewing a Certificate	6-7
Exporting a Certificate	6-9
Deleting a Certificate	6-10
Verifying a Certificate	6-11
Changing the Password on a Personal Certificate	6-12

CHAPTER 7

Managing the VPN Client 7-1

- Managing Connection Entries 7-1
 - Importing a Connection Entry 7-1
 - Modifying a Connection Entry 7-2
 - Deleting a Connection Entry 7-3
- Event Logging 7-4
 - Enable Logging 7-4
 - Clear Logging 7-5
 - Set Logging Options 7-5
 - Opening the Log Window 7-7
- Viewing Statistics 7-8
 - Tunnel Details 7-9
 - Route Details 7-10
 - Notifications 7-11

INDEX



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 10.2 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, “Understanding 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, “Enrolling and 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.

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.

- *Release Notes for the Cisco VPN Client, Release 4.6*
- *Cisco VPN Client Administrator Guide, Release 4.6*
- *Cisco VPN 3000 Series Concentrator Getting Started Guide, Release 4.6*
- *Cisco VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.1*
- *Cisco VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring, Release 4.1*

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
 - Cisco 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

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from 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 may have 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.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

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/en/US/partner/ordering/index.shtml>

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) 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. On the Cisco Documentation home page, click **Feedback** at the top 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: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com 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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco 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 website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- 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.

Cisco TAC Website

You can use the Cisco TAC website 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 website, 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 website. Some services on the Cisco TAC website require 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://tools.cisco.com/RPF/register/register.do>

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

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

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.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:
http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:
http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Understanding 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 10.2 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 Administration Guide*.

Connection Technologies

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

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

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

VPN Client 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 10.2 or later
Connection types	<ul style="list-style-type: none"> • async serial PPP • Internet-attached Ethernet • DSL  <p>Note The VPN Client for Mac OS X does not support Bluetooth wireless technology.</p>
Protocol	IP
Tunnel protocol	IPSec
User Authentication	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Cisco IOS devices that support Easy VPN server functionality • VPN 3000 Series Concentrators • Cisco PIX Firewall Series, Version 6.2 or later
Interfaces supported	<ul style="list-style-type: none"> • Graphical user interface • Command line interface
Online Help	<p>Complete browser-based context-sensitive Help</p> <p>Note The online help requires MS Internet Explorer.</p>
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).

Table 1-2 Program Features (continued)


Program Feature	Description
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 a 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 <i>VPN Client Administrator Guide</i> .
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.
Notifications	Software update notifications from the VPN server upon connection.
Launching from notification	Ability to launch a location site containing upgrade software from a VPN server notification.
Alerts (Delete with reason)	<p>The VPN Client provides you with a reason code or reason text when a disconnect occurs. The VPN Client supports the delete with reason function for client-initiated disconnects, concentrator-initiated disconnects, and IPSec deletes.</p> <ul style="list-style-type: none"> • If you are using a GUI VPN Client, a pop-up message appears stating the reason for the disconnect, the message is appended to the Notifications log, and is logged in the IPSec log (Log Viewer window). • If you are using a command-line client, the message appears on your terminal and is logged in the IPSec log. • For IPSec deletes, which do not tear down the connection, an event message appears in the IPSec log file, but no message pops up or appears on the terminal. <p> Note The VPN Concentrator you are connected to must be running software version 4.0 or later.</p>
Single-SA	The ability to support a single security association (SA) per VPN connection. Rather than creating a host-to-network SA pair for each split-tunneling network, this feature provides a host-to-ALL approach, creating one tunnel for all appropriate network traffic apart from whether split-tunneling is in use.

Table 1-2 Program Features (continued)

Program Feature	Description
Connect on open	This feature lets a user connect to the default user profile when starting the VPN Client. You can enable this feature on the Preferences menu under the VPN Client tab.
VPN Client API	VPN Client provides an application programming interface for performing VPN Client tasks without using the command-line or graphical interfaces that Cisco provides. This API comes with a user guide for programmers, which is in a format that can be edited.

Authentication Features

The VPN Client supports the authentication features listed in [Table 1-3](#).

Table 1-3 Authentication Features

Authentication Feature	Description
User authentication through VPN central-site device	<ul style="list-style-type: none"> • 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.

IPSec Features

The VPN Client supports the IPSec features listed in [Table 1-4](#)

Table 1-4 IPSec Features

IPSec Feature	Description
Tunnel Protocol	IPSec
Transparent tunneling	<ul style="list-style-type: none"> • IPSec over UDP for NAT and PAT • IPSec over TCP for NAT and PAT
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.

Table 1-4 IPsec Features (continued)

IPsec Feature	Description
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 1-5](#).

Table 1-5 IPsec Attributes


IPsec Attribute	Description
Main Mode and Aggressive Mode	Ways to negotiate phase one of establishing ISAKMP Security Associations (SAs)
Authentication algorithms	<ul style="list-style-type: none"> • HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function • HMAC with SHA-1 (Secure Hash Algorithm) hash function
Authentication Modes	<ul style="list-style-type: none"> • Preshared Keys • Mutual Group Authentication • X.509 Digital Certificates
Diffie-Hellman Groups	<ul style="list-style-type: none"> • Group 1 = 768-bit prime modulus • Group 2 = 1024-bit prime modulus • Group 5 = 1536 prime modulus <p> Note See the <i>Cisco VPN Client Administrator Guide</i> for more information about DH Group 5.</p>
Encryption algorithms	<ul style="list-style-type: none"> • 56-bit DES (Data Encryption Standard) • 168-bit Triple-DES • AES 128-bit and 256-bit

Table 1-5 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	<ul style="list-style-type: none">• IPsec over UDP (NAT/PAT)• IPsec over TCP (NAT/PAT)
IP compression (IPCOMP) using LZS	Data compression algorithm



Installing the VPN Client

This chapter describes how to install the VPN Client for 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 10.2 or later and 30 MB of hard disk space.

Mac OS X VPN Clients support only single interface FastEthernet network adapters. This VPN Client does not support any multiport adapters.

Gathering Information You Need

To configure and use the VPN Client, you might need the following information.

You can normally obtain this information from the system administrator of the private network you want to access. The system administrator might have preconfigured much of this data.

- Hostname or IP address of the secure gateway you are connecting to
- Your IPSec Group Name (for preshared keys)
- Your IPSec Group Password (for preshared keys)
- If authenticating with a digital certificate, the name of the certificate
- If authenticating through one of the following methods, your username and password
 - The secure gateway's internal server
 - A RADIUS server
 - An NT Domain server
- If authenticating through a token vendor, your username and PIN
- If you are configuring backup server connections, the hostnames or IP addresses of the backup servers

Obtaining the VPN Client Software

The VPN Client software is available from the Cisco website and comes as a disk image file (vpnclient-<version>-GUI.k9.dmg). Only system administrators can obtain and distribute the VPN Client software.

To obtain the installer:

-
- Step 1** Copy or download the image file to your Desktop.
 - Step 2** Double-click to extract the VPN Client installer to your Desktop.
 - Step 3** The image file remains on the 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.

- To distribute custom user profiles to the installer program, place the files in the Profiles folder of the VPN Client installer.
- To distribute custom images, place the files in the Resources folder of the VPN Client installer.
- To distribute custom global profiles, place the vpnclient.ini in the VPN Client installer directory.



Note

Refer to the *Cisco VPN Client Administrator Guide* for information on creating user profiles, global profiles, and the complete list of file parameters, keywords, and values.

To access the installer directory

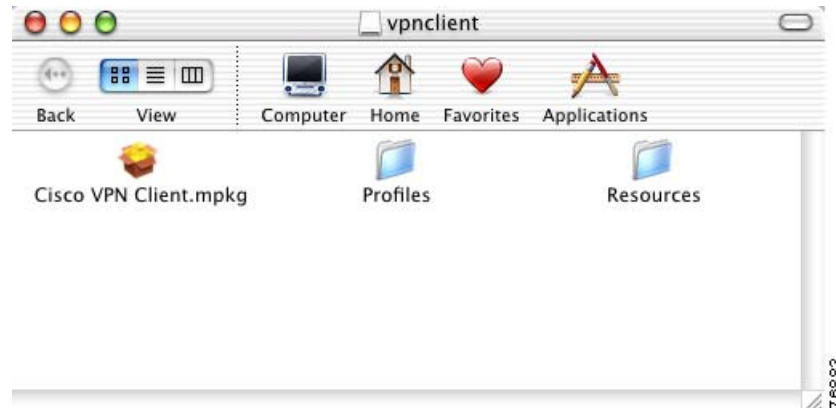
-
- Step 1** Double-click the vpnclient installer icon. (Figure 2-1).

Figure 2-1 Installer Icon



Alternately, you can right-click (control-click) the VPN Client installer icon and choose **Open** from the menu.

Figure 2-2 shows the vpnclient installer directory. This directory contains the installer package and any preconfigured files in the Profiles and Resources folders.

Figure 2-2 VPN Client Installer Directory

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).

To distribute preconfigured profiles, copy the configuration files (.pcf files) into the Profiles folder in the vpnclient installer directory.

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

Preconfiguring the Global Profile

A global profile sets rules for all remote users; it contains parameters for the VPN Client as a whole. The name of the global profile file is vpnclient.ini.

The vpnclient.ini file controls the following features:

- Control of logging services by class
- Certificate enrollment
- Missing group warning message
- VPN Client GUI preferences, such as window locations and sizes

If you do not preconfigure a global profile, the vpnclient.ini file is populated with default settings. Each time you make changes, the vpnclient.ini file is updated and stored.

Bundling a Root Certificate with the Installation Package for Darwin

To use mutual authentication, the VPN Client computer must have a root certificate installed. You can bundle a root certificate with the installation package so that the root certificate is installed automatically. The following steps place a root certificate with the installation package. The root certificate is contained in a file. The name of the file must be rootcert with no extension.

-
- Step 1** In the GUI, double-click **vpnclient-darwin-*<version>*-K9.dmg** or using the CLI, open **vpnclient-darwin-*<version>*-K9.dmg**.
- Step 2** In the GUI, drag and drop the root certificate into the CiscoVPNClient folder on the desktop, making sure the file is renamed to rootcert or using the CLI, enter the following command.
- ```
cp -f <path_to_root_cert>/<root_cert_filename> /Volumes/CiscoVPNClient
```
- Step 3** In the GUI, press **<Apple>-E** while focusing on the CiscoVPNClient folder or using the CLI, enter the following command.
- ```
umount /Volumes/CiscoVPNClient
```

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, by default, both the graphical user interface and the command-line version of the VPN Client. However, you are not required to install the GUI. See the [“Choosing the Installation Type” section on page 2-8](#) for more information.



Note

We recommend that you 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 2-12](#).

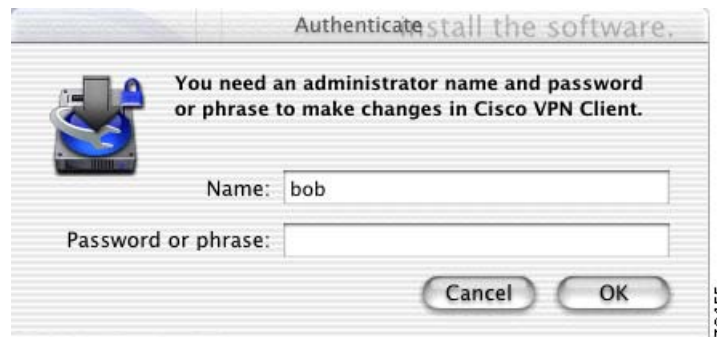
Authentication

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

-
- Step 1** Open the installer package by double-clicking the Cisco VPN Client.mpkg file that resides in the installer directory. (See [Figure 2-2](#)).
- The Authorization window appears ([Figure 2-3](#)). You must have an administrator password to install the VPN Client application.

Figure 2-3 Authorization Window

Step 2 Click the lock to authenticate your password. The Authenticate dialog box appears (Figure 2-4).

Figure 2-4 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.

The installation process includes the following steps:

- [Introduction, page 2-6](#)
- [Accepting the License Agreement, page 2-7](#)
- [Selecting the Application Destination, page 2-7](#)
- [Choosing the Installation Type, page 2-8](#)

Introduction

The first window that appears during installation is the introduction. The right pane of the Introduction window ([Figure 2-5](#)) lists system requirements. The left pane displays each of the installation steps. As you complete each step, it is highlighted with a blue bullet.

Figure 2-5 Cisco VPN Client—Introduction Window

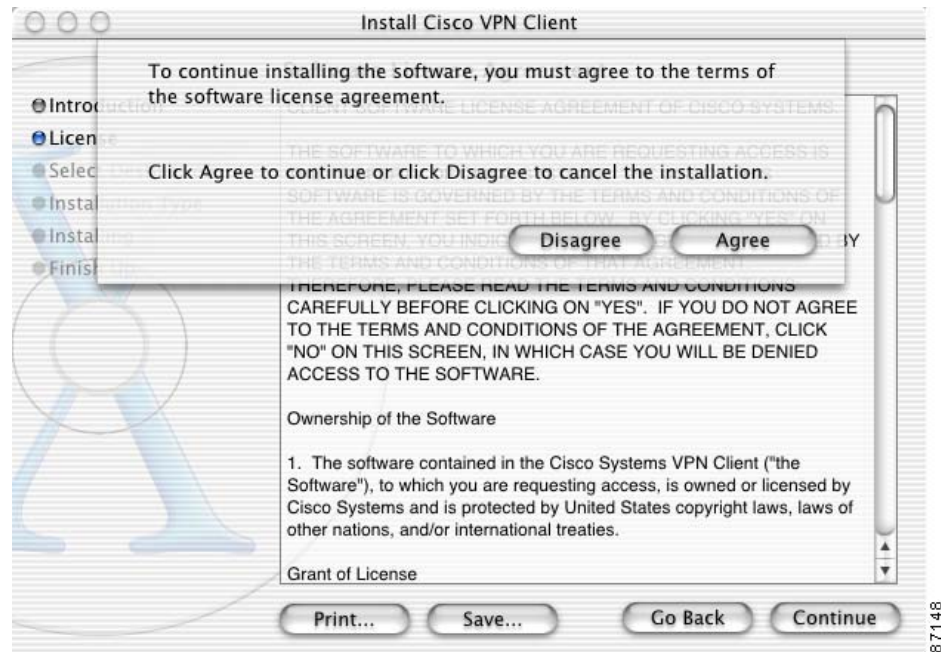


Click **Continue**.

Accepting the License Agreement

You are required to read and accept the Cisco software license agreement before you can continue with the installation process (See [Figure 2-6](#)).

Figure 2-6 Cisco Licence Agreement



Before you accept the license agreement, you can:

- **Print** the license agreement.
- **Save** the license agreement to a file.
- **Go Back** to the Introduction window.
- **Continue** and agree to the terms in the license agreement.

When you have completely read the Cisco VPN Client software license agreement, click **Continue**.

To continue with the installation, click **Agree**.

Selecting the Application Destination

If your workstation has more than one disk drive, you can select the destination volume to install the VPN Client on your workstation. [Figure 2-7](#) shows the Select Destination window.

Figure 2-7 Select Destination Window

Click **Continue**. The VPN Client is installed in the Applications directory.

Choosing the Installation Type

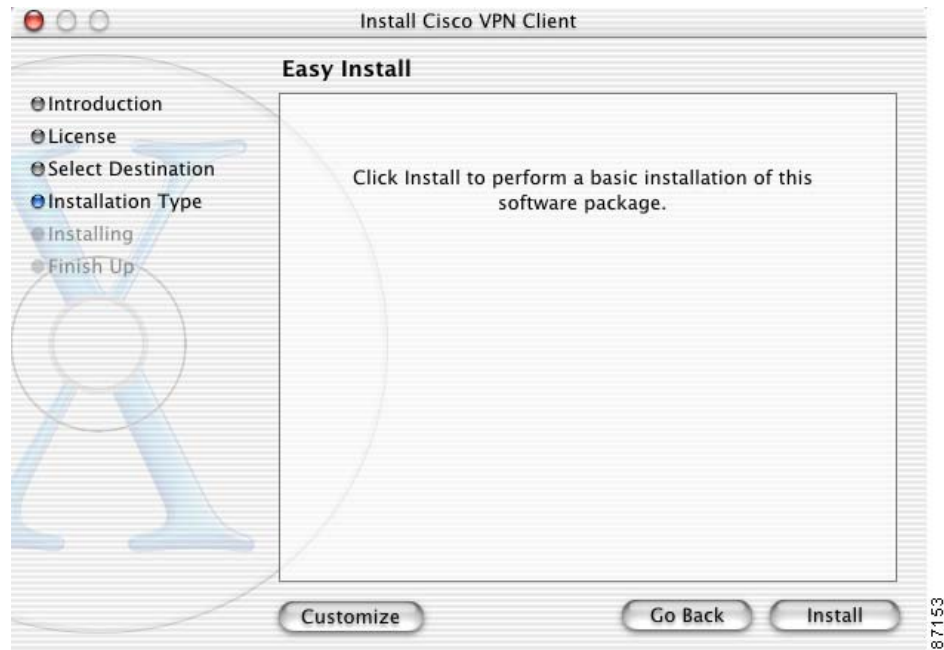
The default installation process installs the following packages with the VPN Client application:

- VPN Client application binaries (includes everything in the directory /usr/local/bin, including the ipseclog).
- VPN Client graphical user interface.
- VPN Client kernel extension
- VPN Client profiles (includes the global profile, vpnclient.ini, and any user profiles, *.pcf files).
- VPN startup (the system startup script to automatically start the client at boot time).

The VPN Client application binaries and the VPN Client kernel extension must be part of your installation. However, installing the other three packages is optional.

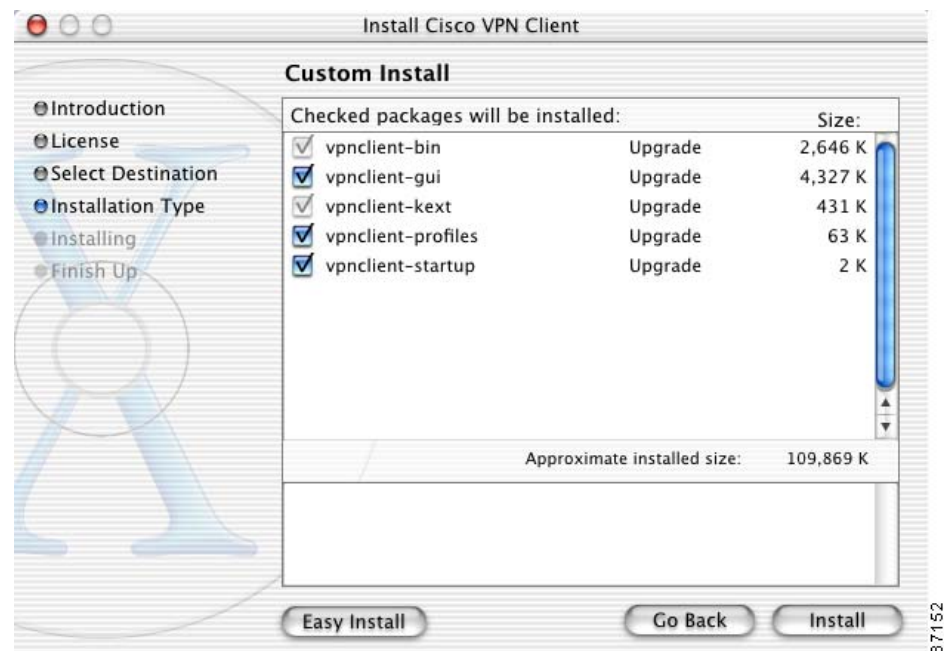
To install all packages, click Install on the Easy Install window ([Figure 2-8](#)).

Figure 2-8 Easy Install Window



To choose which packages to install, click **Customize** to open the Custom Install window (Figure 2-9).

Figure 2-9 Custom Install Window

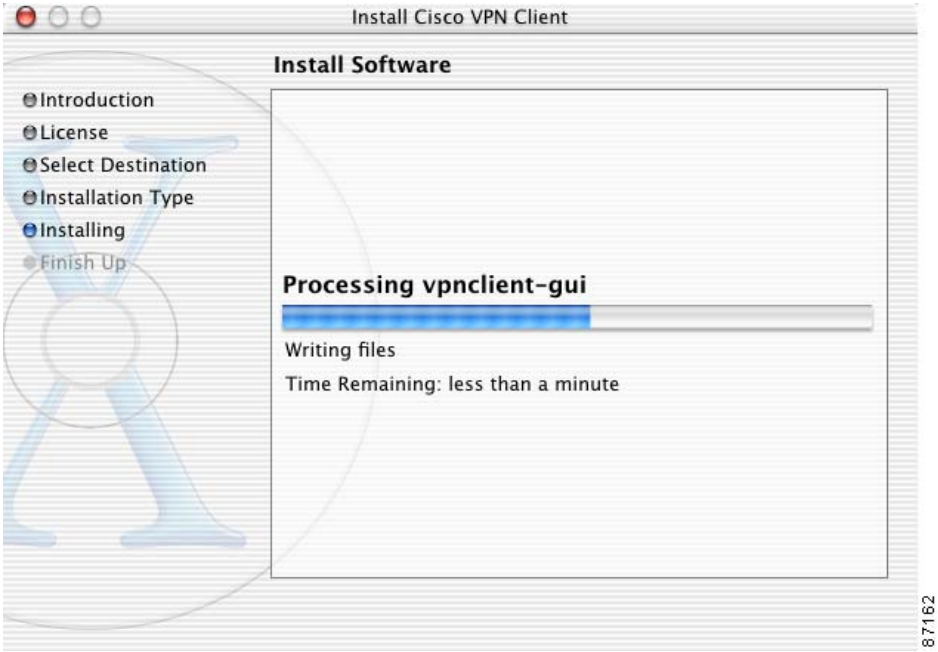


The packages with the blue check box are optional. To make a package part of your installation, check the blue box. To remove a package from your installation, uncheck the blue box.

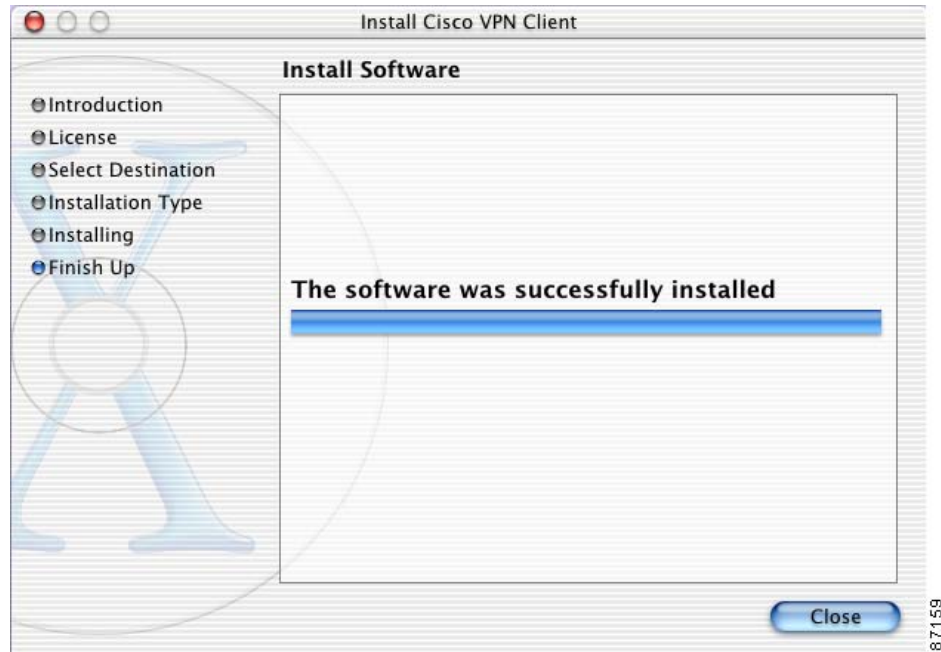
Click **Easy Install** to return to the default installation packages, or **Install** to continue with a custom installation.

A progress bar lists the installation steps as they occur (Figure 2-10).

Figure 2-10 Install Software Progress Window



When the installation is finished, a window appears to indicate whether the installation was successful (Figure 2-11).

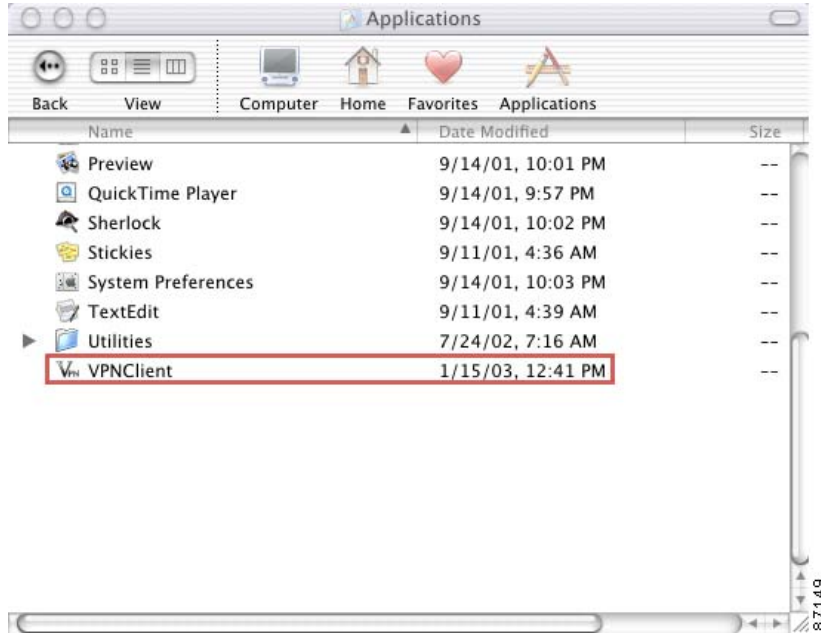
Figure 2-11 Successful Installation Confirmation Window

Click **Close**.

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.

To begin using the Client, double-click the VPN Client application icon located in the Applications directory ([Figure 2-12](#)).

Figure 2-12 Location of VPN Client Application



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
```

Alternately, you can use these commands to interact with the kernel extension:

```
sudo SystemStarter start CiscoVPN
sudo SystemStarter stop CiscoVPN
sudo SystemStarter restart CiscoVPN
```

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

Uninstalling the VPN Client

This section describes how to uninstall the VPN Client.



Note

You must have administrator privileges to uninstall the VPN Client. If you do not have administrator privileges, you must have someone with administrator privileges uninstall the product for you.

**Note**

We recommend that you uninstall any previous version of the VPN Client for Mac OS X before you install a new version.

The VPN Client uninstall script uninstalls any previous command-line or GUI version of the VPN Client from your workstation.

To uninstall the VPN Client for Mac OS X

Step 1 Open a terminal window.

Step 2 Run the following command:

```
sudo /usr/local/bin/vpn_uninstall
```

Step 3 Enter your password

Step 4 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.
-



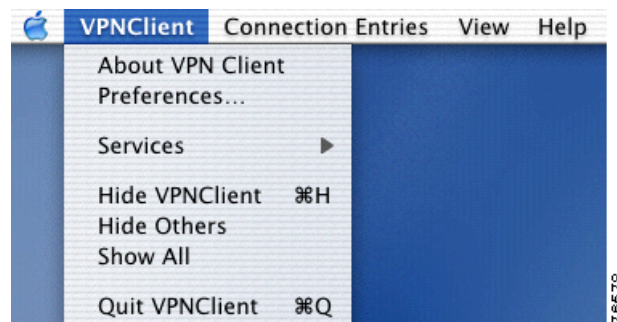
Navigating the User Interface

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

VPN Client Menu

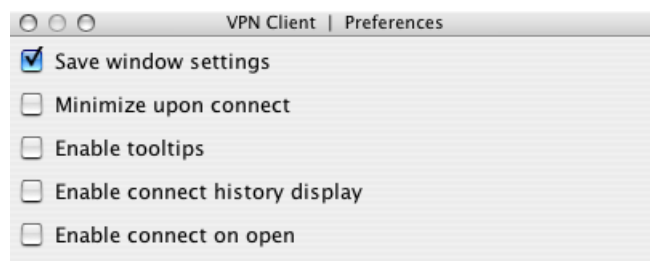
Use the VPN Client menu (Figure 3-1) to manage the VPN Client application and main window settings.

Figure 3-1 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 3-2).

Figure 3-2 VPN Client Window Preferences



- Save window settings—Saves changes to the VPN Client window. For example, you can save the window size; the window position; the selected tab; and the view (simple or advanced mode).
- 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
- Enable connect history display—Displays connection history information
- Enable connect on open—Connects to the default connection entry when you start the VPN Client.
- 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.

Choosing a Run Mode

You can run the VPN Client in simple mode or in advanced mode. The default is advanced 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-M**. Alternately, you can choose your mode from the Options menu.

Operating in Simple Mode

Use simple mode when you only need to establish a connection to a VPN device using the default connection entry.

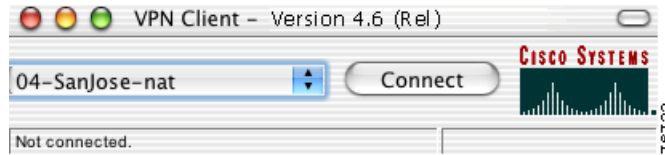


Note

You must operate in advanced mode to manage certificates and event logging or to make configuration changes to a connection entry.

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 3-3).

Figure 3-3 VPN Client Window—Simple Mode

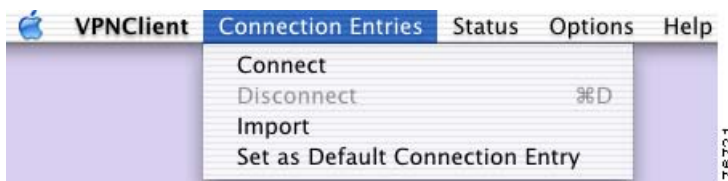
The main VPN Client window shows only the version information, the default connection entry, the connect button, and the status bar.

Main Menus—Simple Mode

This section describes the abbreviated menu choices available in simple mode. The Certificates and Log menus are only available in advanced mode.

Connection Entries Menu

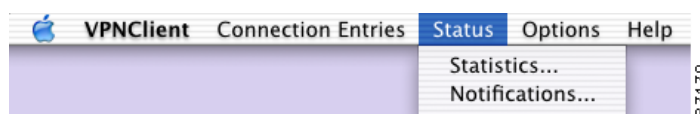
Figure 3-4 shows the Connection Entries menu options for simple mode.

Figure 3-4 Simple Mode Connection Entries Menu

- **Connect**—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.
- **Import**—Import a connection entry configuration file (a file with a .pcf extension, called a profile).
- **Set as Default Connection Entry**—Use the selected connection entry as the default. The default connection entry is used for this VPN session unless you select an alternate connection entry.

Status Menu

Figure 3-5 shows the Status Menu options for simple mode.

Figure 3-5 Simple Mode Status Menu

- **Statistics**—Open the Statistics window to view tunnel details and route details.
- **Notifications**—Open the Notifications window to view notices from the VPN device.

Operating in Advanced Mode

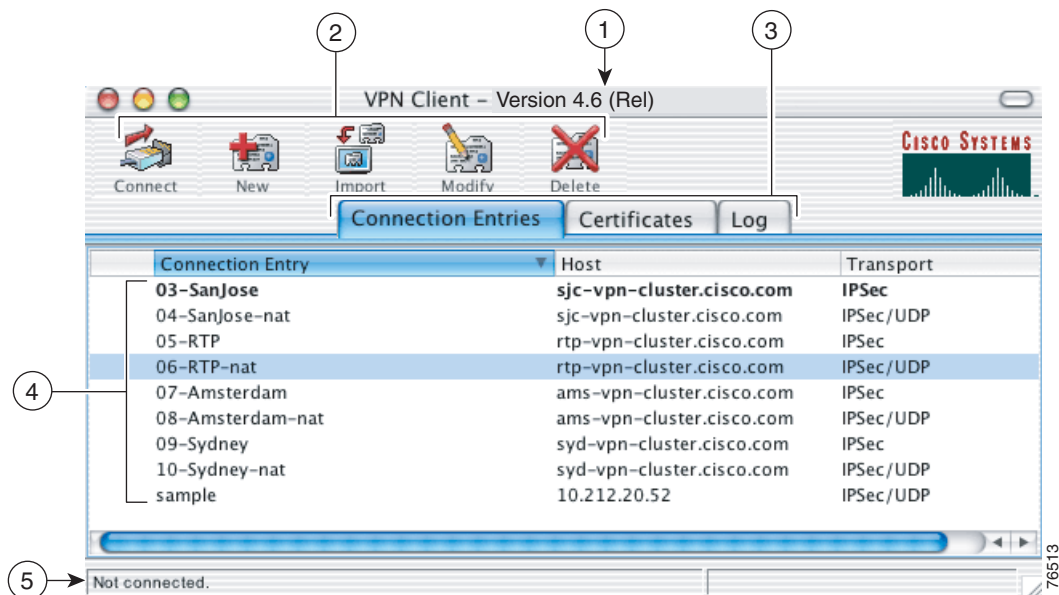
Use Advanced mode to manage the VPN Client; configure connection entries; manage certificates; view and manage event logging; and view tunnel statistics and routing data.

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 3-6 shows the VPN Client window and the primary navigation areas.

Figure 3-6 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	When connected, the status bar displays information related to the current VPN session: <ul style="list-style-type: none"> The left side indicates the connection entry name and connection status. The right side lists the amount of time for this session, the client IP address, and the number of bytes through the VPN tunnel.
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 3-6](#)). If the **Certificates** tab is forward, the View, Import, Export, Enroll, Verify, and Delete buttons control operations for the selected certificate ([Figure 3-7](#)).

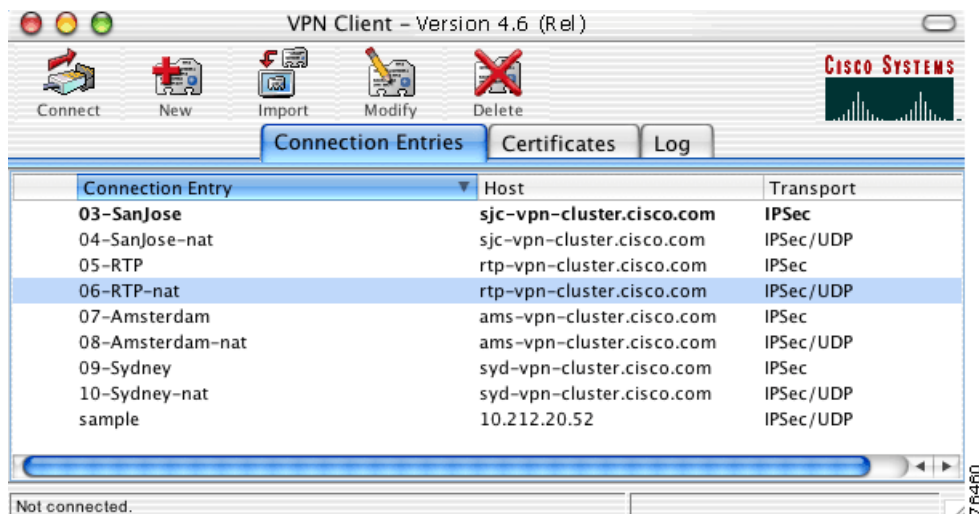
Figure 3-7 *Toolbar Buttons—Certificates Tab*



Main Tabs—Advanced Mode

This section describes the three main tabs for managing the VPN Client ([Figure 3-8](#)).

Figure 3-8 *VPN Client GUI Main Tabs*



The three 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, “Enrolling and Managing Certificates”](#) for more details on the Certificates tab.
- **Log tab**—Displays event messages from all processes that contribute to the client-peer connection, 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 running in advanced mode and active on your desktop.

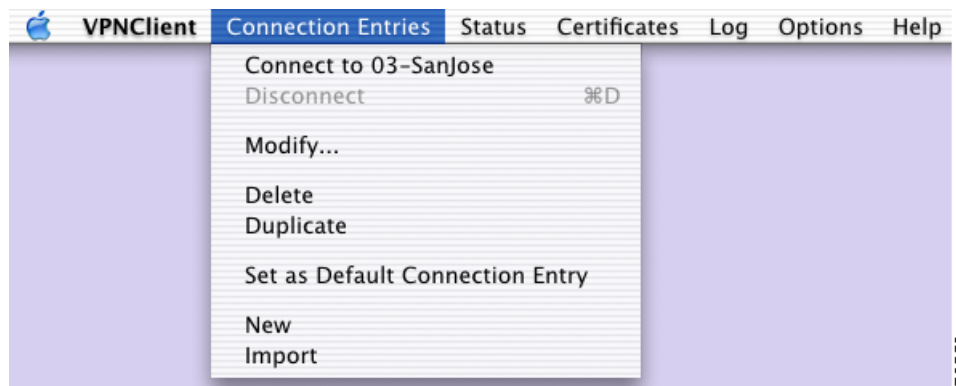
Connection Entries Menu

Use the Connection Entries menu (Figure 3-9) as a shortcut to frequently-used connection entry operations. The menu option applies to the connection entry that is currently selected on the Connection Entries tab.


Note

A connection entry must be selected to use Connection Entries menu options.

Figure 3-9 Connection Entries Menu



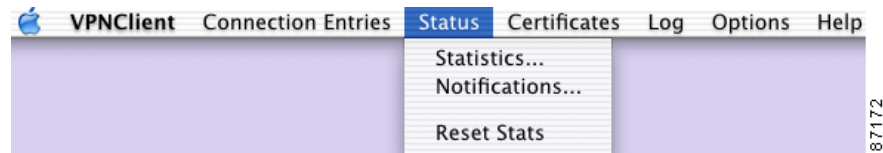
- **Connect to**—Establish a VPN connection using the selected connection entry. If the Connections tab is not selected, a submenu, which lists all available connection entries, is displayed.
- **Disconnect**—Disconnect the current VPN session.
- **Modify**—Modify the properties of the selected connection entry.
- **Delete**—Delete the selected connection entry.
- **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.
- **Set as Default Connection Entry**—Use the selected connection entry as the default. The VPN Client uses the default connection entry for this VPN session unless you select an alternate connection entry. Also, when you enable connect on open on the Preferences menu, the VPN Client opens the default connection entry when it starts up.
- **New**—Configure a new connection entry.
- **Import**—Import a connection entry from a file.

To configure a new connection entry, see [Chapter 4, “Configuring Connection Entries.”](#)

Status Menu

Use the Status menu (Figure 3-10) to display the tunnel and route statistics or to view notifications from the VPN device.

Figure 3-10 Status Menu



- Statistics—Open the Statistics window to view tunnel details and route details.
- Notifications—Open the Notifications window to view notices from the VPN device.
- Reset Stats—Reset the VPN session statistics on the Tunnel Details tab of the Statistics window.

Certificates Menu

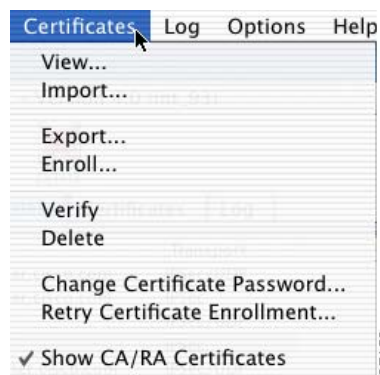
Use the Certificates menu (Figure 3-11) as a shortcut to frequently-used certificate operations. The menu option applies to the certificate that is currently selected on the Certificates tab.



Note

A certificate must be selected to use Certificates menu options.

Figure 3-11 Certificates Menu



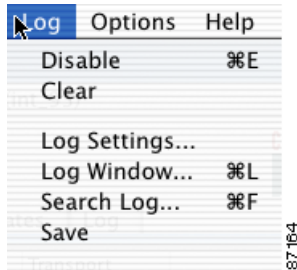
- View—View the properties of the selected certificate.
- Import—Import a certificate from a file.
- Export—Export the selected certificate to a specified file location
- Enroll—Enroll a digital certificate for user authentication.
- Verify—Verify that the selected certificate is valid.
- Delete—Delete the selected certificate.
- Change Certificate Password—Change the password used to protect the certificate while it is in the VPN Client certificate store.

- **Retry Certificate Enrollment**—Retry a previously started certificate enrollment.
- **Show or Hide CA/RA Certificates**—This menu option toggles to Show or Hide root certificates issued by either a Certificate Authority (CA) or a Registration Authority (RA).

Log Menu

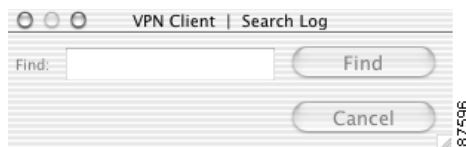
Use the Log menu (Figure 3-12) to enable, disable, view or clear the event log, or to adjust the log settings.

Figure 3-12 Log Menu



- **Enable/Disable**—Enable or disable event logging.
- **Clear**—Clear the event log.
- **Log Settings**—Open the Log Settings window to view current settings or make adjustments.
- **Log Window**—Open the Log Window, which is a separate window that displays events. From this window you can save the display, edit logging levels by event class, and clear both log displays. The Log Window shows more events than the display area of the main advanced mode window.
- **Search Log**—Open the Search Log dialog box (Figure 3-13).

Figure 3-13 Log Search Dialog Box



Enter the exact string to match in the Find entry field. The search string is not case-sensitive and wildcards are not allowed. Matched instances are highlighted on the Log tab.

- **Save**—Save the event log to a file.

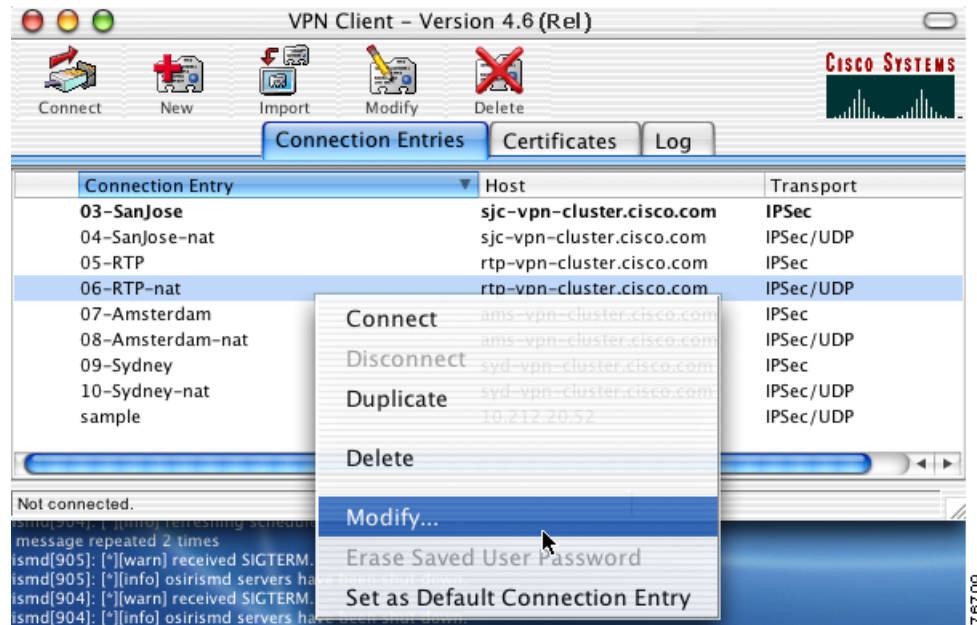
Right-Click Menus

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 3-14 shows the right-click menu options available when the Connection Entries tab is selected.

Figure 3-14 Connection Entries Right-Click Menu

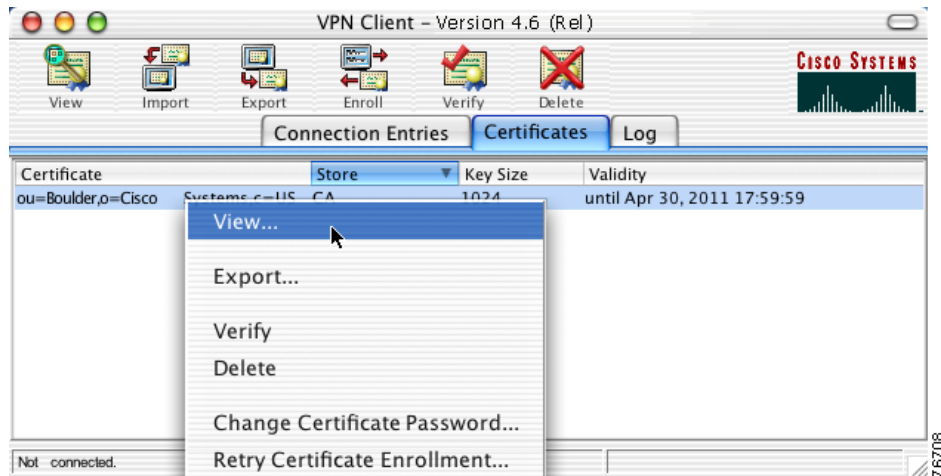


- **Connect**—Establish a VPN connection using the selected connection entry.
- **Disconnect**—Disconnect the current VPN session.
- **Duplicate**—Duplicate the selected connection entry. This action allows you to create a new connection entry using the configuration from a current connection entry as a template.
- **Delete**—Delete the selected connection entry.
- **Modify**—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.

Certificates Tab Right-Click Menu

Figure 3-15 shows the right-click menu options available when the Certificates tab is forward.

Figure 3-15 Certificates Tab Right-Click Menu



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

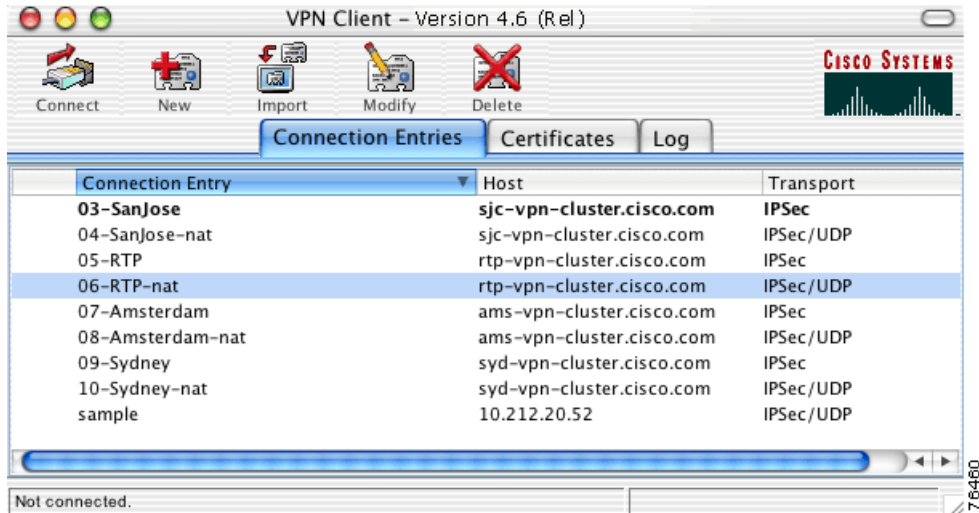
- The VPN device that is providing access to the network.
- Preshared keys—The IPSec group that you have been assigned to. Your IPSec group determines the set of privileges you have for accessing and using the private network. For example, it specifies access hours, number of simultaneous logins, user 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).

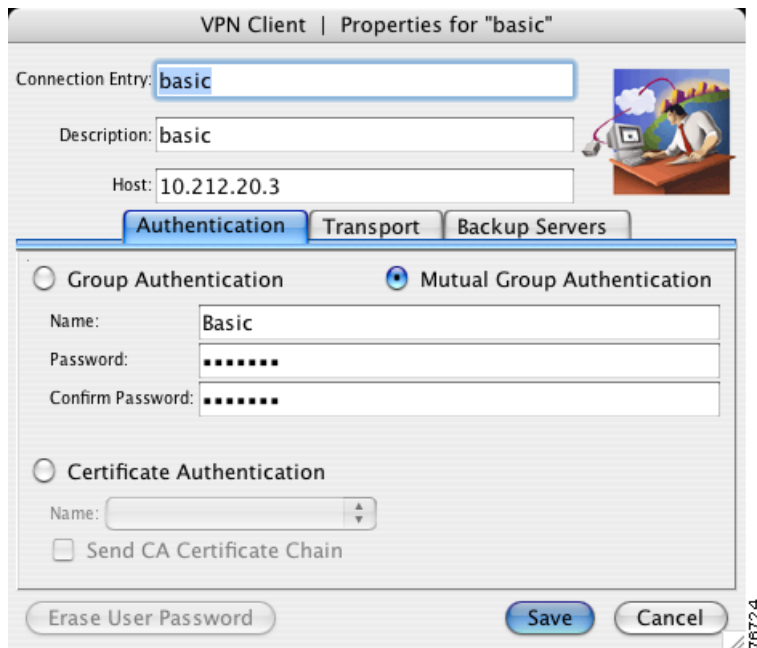
Figure 4-1 VPN Client Window



- 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 4-3](#) 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.

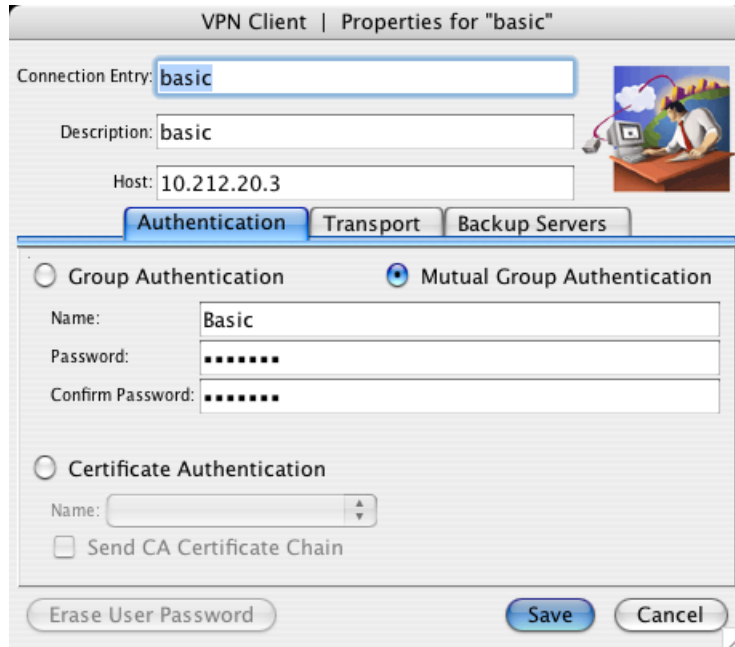
Group Authentication

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.

Mutual Group Authentication

When you select mutual group authentication, the VPN Client verifies whether you have a root certificate installed. If not, it prompts to import one. Before you continue, you must import a root certificate. For information on importing a certificate, see [Importing a Certificate](#).

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

Certificate Authentication

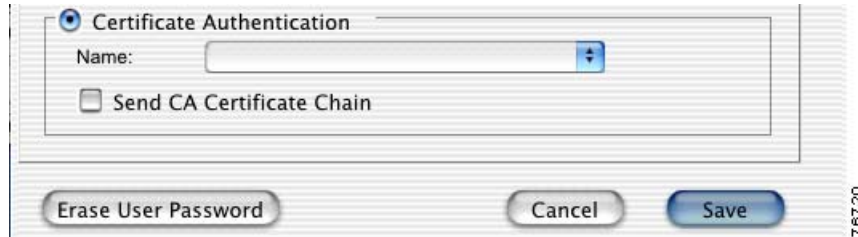
Use this procedure if you plan to use digital certificates for authenticating for this connection entry.

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 6-7 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.

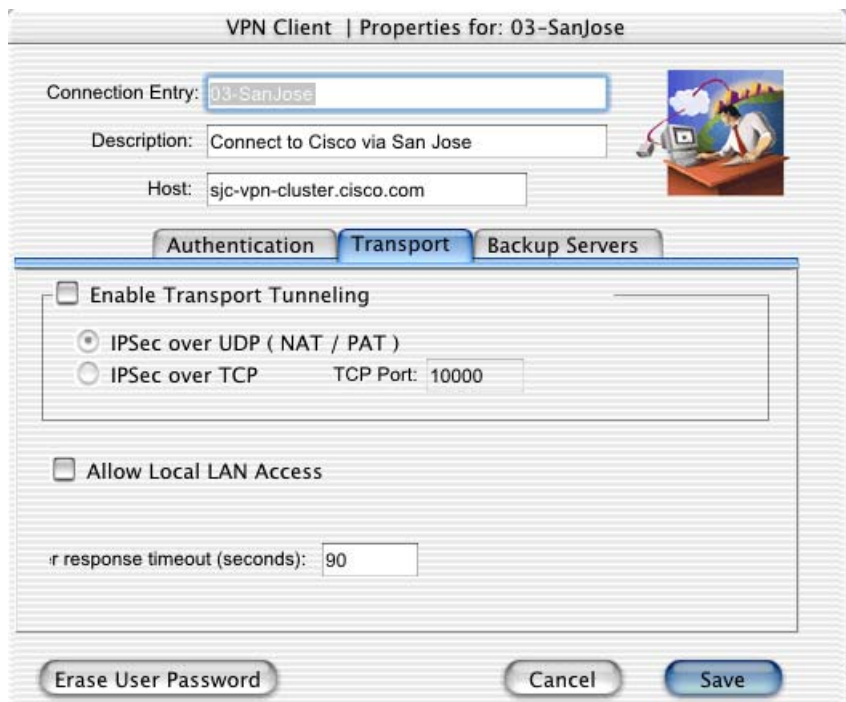
The transport parameters include:

- [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 choosing Statistics from the Status menu and clicking the **Route Details** tab. For more information, see the “[Route Details](#)” section on page 7-10.

- 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 on the VPN Client. You must also enable this feature on the VPN device you are connecting to.

Peer Response Timeout

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

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

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

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

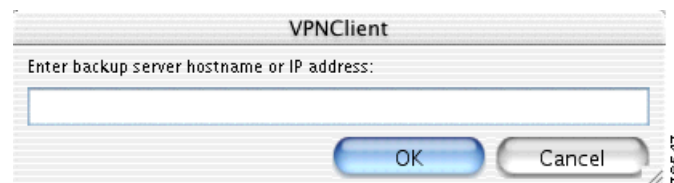


- Step 5** Check the **Enable Backup Servers** check box. This parameter is not enabled by default. The list of available backup servers is displayed. Backup servers are used in the order presented in the list.
- Step 6** To change the order in which the backup servers are used, select a backup server and use the arrow buttons to move the server up or down in the list.
- Step 7** 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**.
-



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** Open the VPN Client application by double-clicking the VPN Client icon in the Applications folder. If you created an alias, you can double-click the VPN Client icon on the Desktop or in the dock ([Figure 5-1](#)).

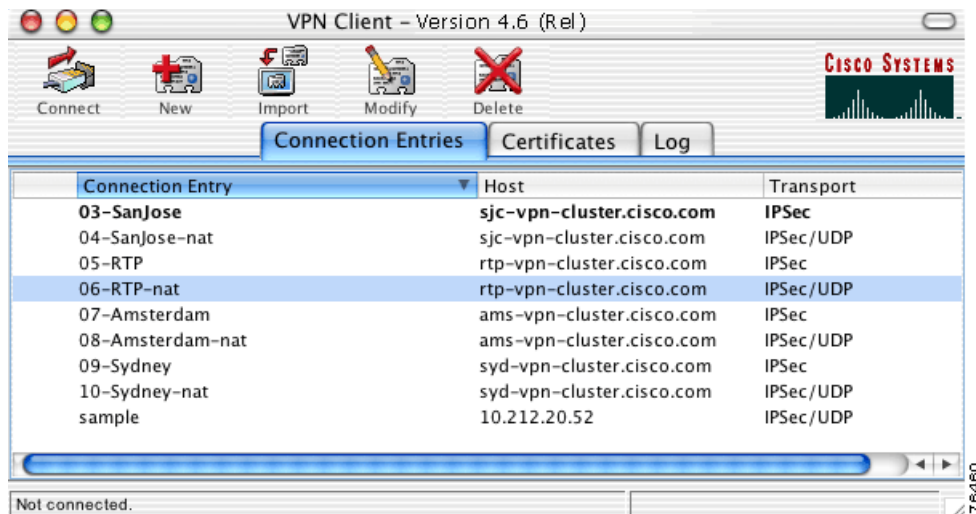
Figure 5-1 VPN Client Icon

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. For simple mode, select a connection entry from the drop-down list.
- 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.

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.

Connecting to a Default Connection Entry

If you have configured a default connection entry (sometimes called *default user* or *default profile*), the VPN Client uses this connection entry when it starts. The name of this feature is *Connect on Open*. You can enable it on the Preferences menu, see “[VPN Client Menu](#)”. An administrator configures this feature for you. For information, see the *VPN Client Administrator Guide*. For information on setting a connection entry to be the default, see “[Creating a Connection Entry](#)”.

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
- Mutual group authentication, using a root certificate generally installed by your network administrator
- 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 RSA SecurID cards and keychain fobs, and PC software called RSA SecurID for passcode generation. RSA 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 RSA SecurID passcodes for authentication:

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

In most configurations, you use RSA 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 RSA SecurID user authentication prompt follows (Figure 5-7).

Figure 5-7 User Authentication for RSA SecurID

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

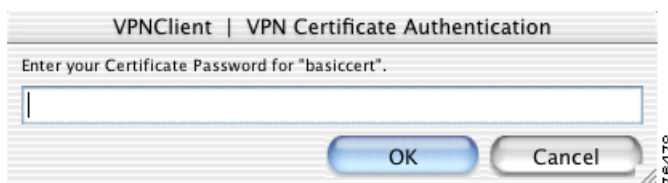
Using Digital Certificates

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, “Enrolling and Managing Certificates.”](#)



Enrolling and Managing Certificates

This chapter describes how to enroll and manage digital certificates for the VPN Client for Mac OS X, specifically how to perform the following tasks:

- Obtain personal certificates through enrollment with a certificate authority (CA), which is an organization that issues digital certificates that verify that you are who you say you are.
- Manage certificates and enrollment requests
- Import, export, view, and verify certificates

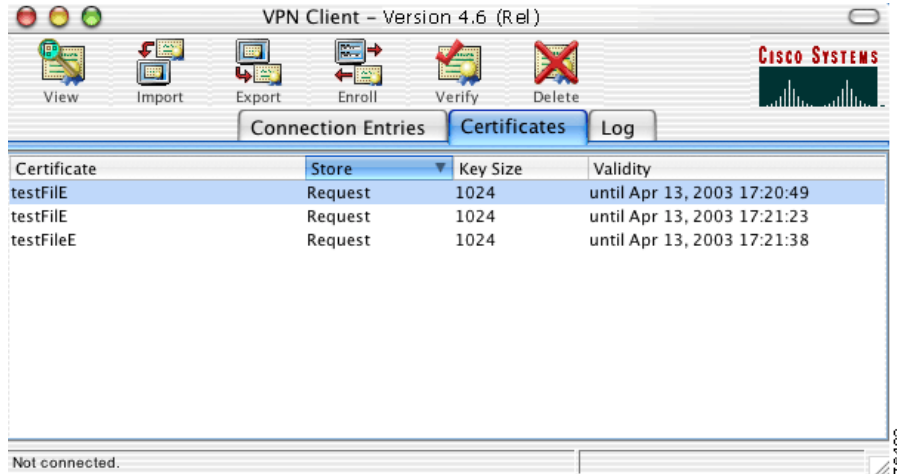
To get started with certificates, open the Certificates tab on the main VPN Client window in advanced mode. The Certificates tab lists the certificates you currently have enrolled. If there are no certificates showing, you need to enroll with a CA or contact your system administrator.

Using the Certificate Store

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

The Certificates tab on the main 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.

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.
 - Step 3** Choose a certificate enrollment type.
 - If you choose **Online**, you obtain a certificate by enrolling with a CA over the network.
 - 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.

Figure 6-2 shows the Certificate Enrollment Dialog Box.

Figure 6-2 Online Certificate Enrollment

Step 4 Enter the enrollment parameters.

- For online enrollment enter:
 - Certificate Authority—The Common name or the Subject name of the CA Certificate. This drop-down list contains a history of previously enrolled CA certificates. If you select a CA from this list, the CA URL and the CA Domain fields are pre-populated. For <New> online enrollments, you must enter the CA URL and the CA Domain manually.
 - 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`.
 - Challenge Password—Some CAs require that you enter a password to access their site. Enter this password in the Challenge Password field. Obtain the challenge password from your administrator or from the CA.
 - 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.
- For file enrollment enter:
 - File encoding type of the output file.
 - 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.
 - Binary—a base-2 PKCS10 (Public-Key Cryptography Standards) file. You cannot display a binary-encoded file
 - Filename—The full pathname for the file request. For example, `/Users/Anna/Documents/Certificates/mycert.p10`.
 - 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 **Next** to continue with certificate enrollment. The Certificate Enrollment dialog box appears (Figure 6-3).

Figure 6-3 Certificate Enrollment

- Step 6** Enter the remaining 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

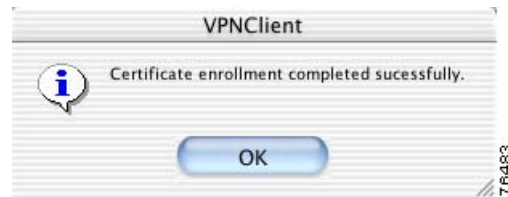
Entry Field	Description
Name (CN)	The common name for the certificate. The common name can be the name of a person, system, or other entity. It is the most specific level in the identification hierarchy. The common name becomes the name of the certificate. For example, Fred Flinstone.
Domain	The Fully Qualified Domain Name (FQDN) of the host for your system. For example, Dialin_Server.
Email (E)	The user e-mail address for the certificate. For example, email@company.com
IP Address	The IP address of the user's system. For example, 192.168.23.9
Department (OU)	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 (O)	The company name for the certificate.
State (ST)	The state for the certificate.
Country (C)	The 2-letter country code for your country. For example, US. This two-letter country code must conform to ISO 3166 country abbreviations.

- Step 7** Click **Enroll** to enroll a certificate from a CA, **Go Back** to review previous certificate enrollment parameters, or **Cancel**.

The certificate enrollment is listed in the certificate store as a *request*. To resume a certificate enrollment request, right-click and choose **Resume Certificate Enrollment**. Alternately, you can resume an enrollment from the Certificates menu.

A prompt indicates whether the certificate enrollment is successful (Figure 6-4).

Figure 6-4 Enrollment Complete



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

Managing Enrollment Requests

While a request is pending approval by the CA administration, the VPN Client places the enrollment request in the list on the Certificates tab. You can view, delete, or change the password for any request in the list; or you can retry a network enrollment request. To perform any of these actions, select the pending enrollment request and click on the Certificate menu.

Viewing the Enrollment Request

To display the enrollment request

-
- Step 1** Select the enrollment request in the certificate store
 - Step 2** Choose **View** from the Certificates menu.
 - Step 3** The VPN Client displays the pending request. The *Issuer* field shows the subject name and not the name of the CA, since the CA has not yet issued the certificate.



Tip You can also change the certificate request password from the **View** dialog box.

Deleting an Enrollment Request

To delete an enrollment request

-
- Step 1** Select the enrollment request from the certificate store.
 - Step 2** Choose **Delete** from the Certificates menu.
The VPN Client prompts you for a password.

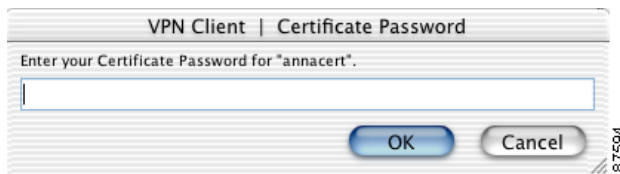
- Step 3** Enter the password in the Password field (if there is one) and click **OK**.
The VPN Client verifies the password. If the password is correct, the VPN Client deletes the request.
-

Changing the Password on an Enrollment Request

To change the certificate password on an enrollment request

- Step 1** Select the certificate request from the certificate store.
Step 2 Choose **Change Certificate Password** from the Certificates menu.
The VPN Client displays the Certificate Password dialog box (Figure 6-5).

Figure 6-5 *Changing a Certificate Password*



- Step 3** Enter the current password and click **OK**.
Step 4 At the prompt, enter the new password and click **OK**.
Step 5 At the next prompt, enter the new password again to verify it and click **OK**.
The VPN Client responds with a success message.



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

Retrying an Enrollment Request

To retry a pending online enrollment request

- Step 1** Select the enrollment request in the certificate store.
Step 2 Choose **Retry Client Enrollment** from the Certificates menu.
The VPN Client prompts you to enter a password. This password must match the password you are using to protect the certificate's private key, if any.
Step 3 Enter the password and click **OK** to resume the enrollment request.
-

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 6-6).

Figure 6-6 Import Certificate



- Step 3** Enter the import path.
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.
 - Step 4** Enter the import password—This is the password used to protect the certificate file, called the import password, and is assigned by the system administrator.
 - Step 5** Enter the New Password—This is the password 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 6** Verify the New Password again.
 - 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 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 6-7).

Figure 6-7 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—The MD5 and SHA-1 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

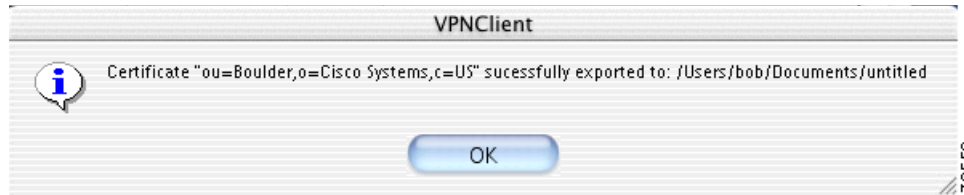
To export a certificate from the certificate store to a specified file

- Step 1** Click the Certificates tab.
- Step 2** Select the certificate to export.
- Step 3** Click **Export** at the top of the VPN Client window. The Export Certificate dialog box appears (Figure 6-8).

Figure 6-8 Export Certificate



- Step 4** Enter the export path.
- 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 5** To export the entire certificate chain, check the box next to this parameter.
- Step 6** Enter a password to protect the exported certificate file. We recommend that you always enter a password to protect your certificates.
- Step 7** Verify the exported certificate file password.
- Step 8** Click **Export**. The certificate is copied to the selected directory and a prompt (Figure 6-9) indicates whether the export is successful.

Figure 6-9 Successful Export Prompt

Step 9 Click **OK** to return to the VPN Client window.

Deleting a Certificate

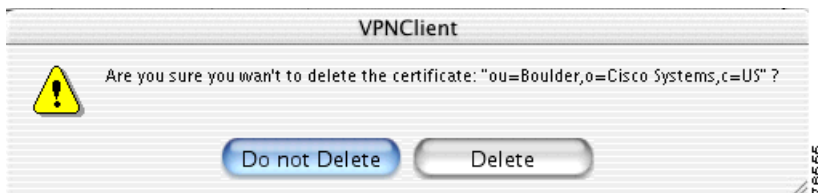
You can delete any certificate from your certificate store. You must provide a password to delete an enrollment certificate.



Caution You cannot retrieve a certificate that has been deleted.

To delete a user or root certificate

- Step 1** Click the Certificates tab.
- Step 2** Select the certificate to delete.
- Step 3** Click **Delete** at the top of the VPN Client window. A warning prompt appears (Figure 6-10).

Figure 6-10 Delete Certificate Warning

Step 4 Verify the name of the certificate and click **Delete**. The selected certificate is deleted from the certificate store.

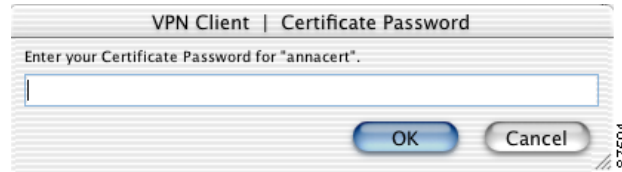
Click **Do not Delete** to return to the VPN Client window without deleting the selected certificate.

To delete an enrollment certificate

- Step 1** Click the Certificates tab.
- Step 2** Select the enrollment certificate to delete.

- Step 3** Click **Delete** at the top of the VPN Client window. The Certificate Password dialog box appears (Figure 6-11).

Figure 6-11 Password Prompt for Deleting Enrollment Certificates.



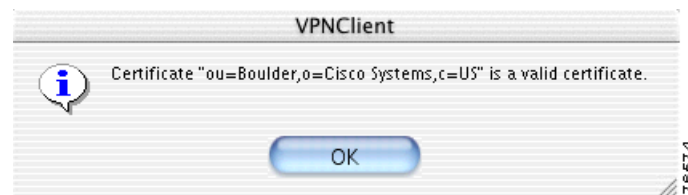
- Step 4** Enter the Certificate Password for the selected certificate to delete.
- The Certificate Password is the password assigned by you to protect the certificate while it is in your certificate store. This is the password set in the New Password field when you enrolled this certificate. See the “[Enrolling Certificates](#)” section on page 6-2.
- Step 5** Click **OK**. The certificate is deleted from the certificate store.

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 6-12) to indicate the validity of the certificate.

Figure 6-12 Verify Certificate



- Step 3** Click **OK** to return to the VPN Client window.
- If your certificate is invalid, contact the network administrator for instructions.

Changing the Password on a Personal Certificate

To view personal (root) certificates issued by either a Certificate Authority (CA) or a Registration Authority (RA), use the **Show/Hide CA/RA Certificates** option from the Certificates menu.

To change the password on a personal certificate

-
- Step 1** Select a certificate from the certificate store under the Certificates tab.
 - Step 2** Display the Certificates menu and choose **Change Certificate Password**
The VPN Client displays the Change Certificate Password dialog box. In the Current field, type the password you are currently using to protect your private key.
 - Step 3** In the New field, type the new password.
 - Step 4** In the Confirm field, type the same password again.
 - Step 5** Click **OK**.
-



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.

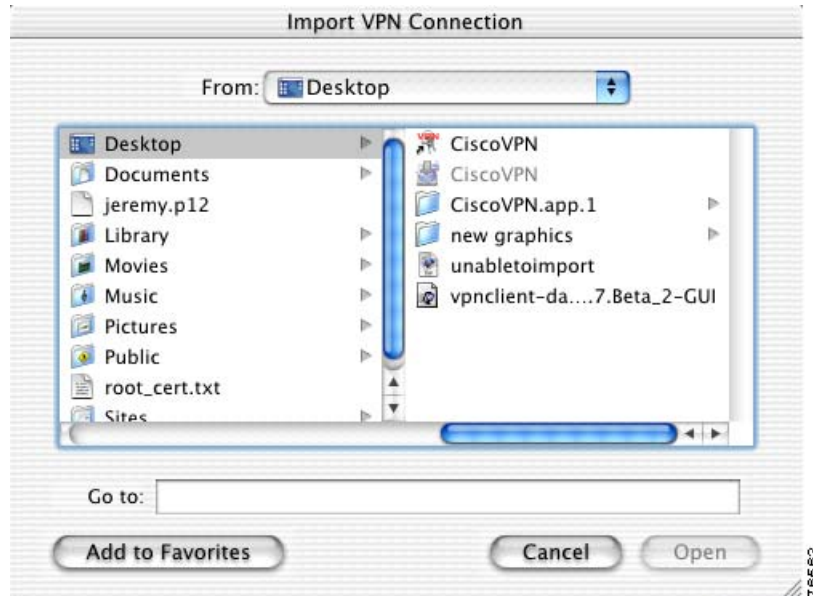
Importing a Connection Entry

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.

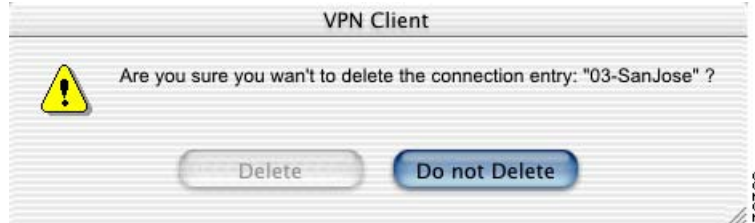
Deleting a Connection Entry

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.

Event Logging

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

The event log can help 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

**Note**

To search the log, choose Search Log from the Log menu. Matched instances are highlighted on the Log tab.

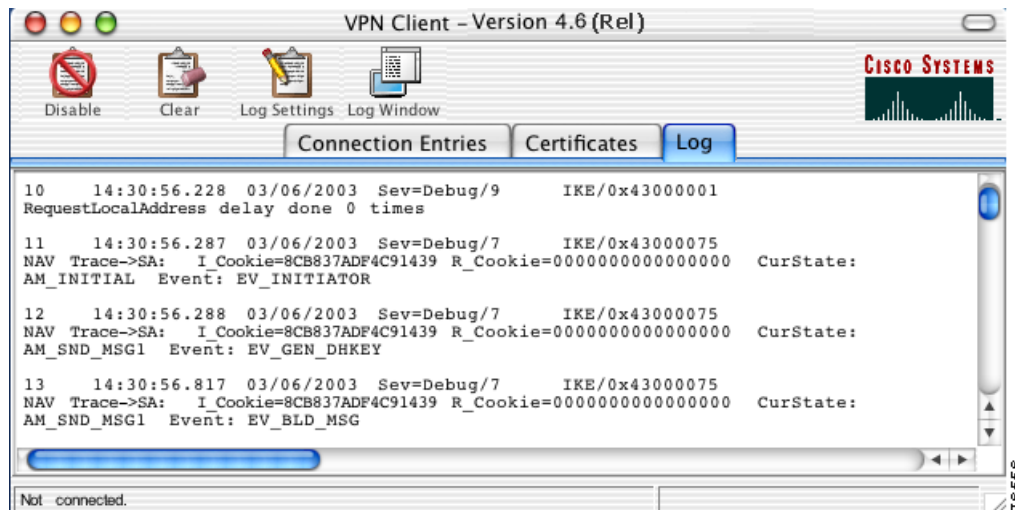
Enable Logging

**Note**

If you enable logging during normal use of the VPN Client, it might affect the performance of the application. We recommend that you only enable logging when troubleshooting.

To enable logging, click **Enable** at the top of the VPN Client window. Alternately, you can choose **Enable** from the Log menu. The event logging window displays (Figure 7-4).

Figure 7-4 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

To store the event messages before you clear the log, choose Save from the Log menu.

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 Log Settings dialog box appears (Figure 7-5).

Figure 7-5 Log Settings

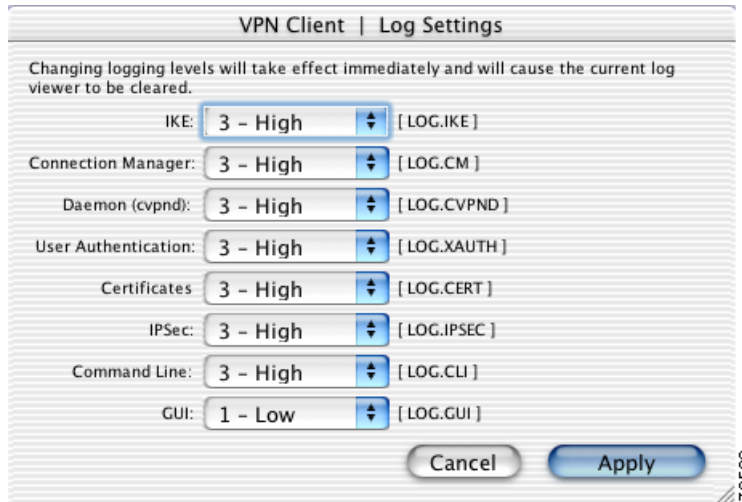


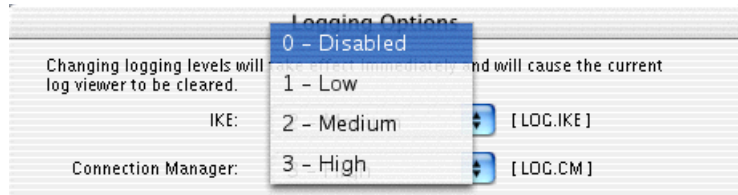
Table 7-1 describes the log classes that generate events in the VPN Client log viewer.

Table 7-1 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
[LOG.GUI]	The VPN Client for Mac OS X user interface.	Graphical User Interface

- 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 7-6](#) shows the logging levels.

Figure 7-6 Logging Levels



There are four logging levels:

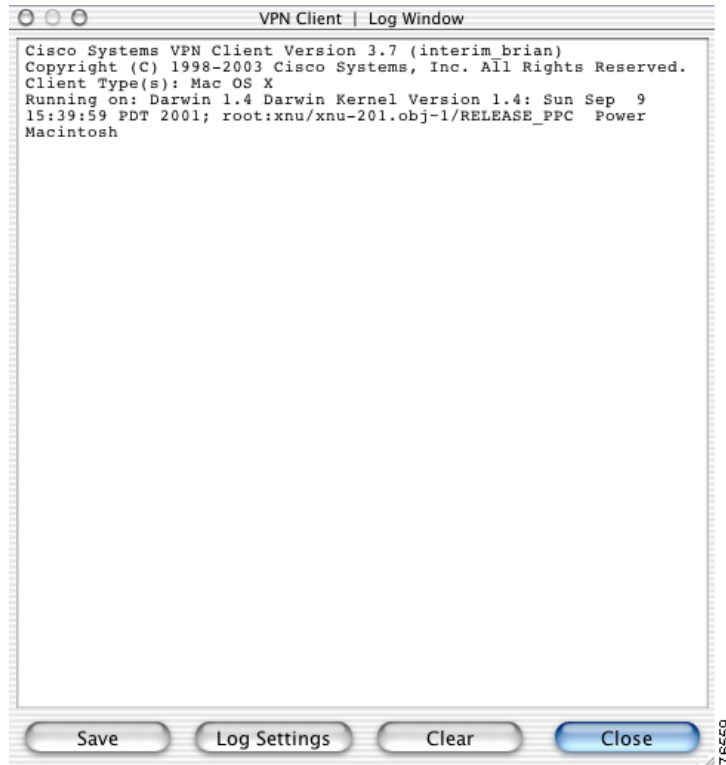
- **0**—Disables logging services for the specified [LOG] class.
- **1**—Low, displays only critical and warning events. This is the default.
- **2**—Medium, displays critical, warning, and informational events.
- **3**—High, displays all events.

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

Opening the Log Window

To display the events log in a separate window, click **Log Window** at the top of the VPN Client window. The VPN Client Log Window appears ([Figure 7-7](#)).

Figure 7-7 Log Window



The following buttons allow you to manage the information in the Log Window:

- **Save** the data in the event log to a file.



Note The VPN Client saves the information to the Client install directory. The default file name is based on the date and time (in 24-hour format) that the log file was created; for example, LOG-2003-03-13-52-56.text. You can save what is in the present log to a different directory and filename, but you cannot change the default log directory and filename.

- Open the **Log Settings** window.
- **Clear** the information listed in the log window.
- **Close** the Log Window.

Viewing Statistics

View VPN session information on the Statistics window. The Statistics window lists tunnel details, route details, and other 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

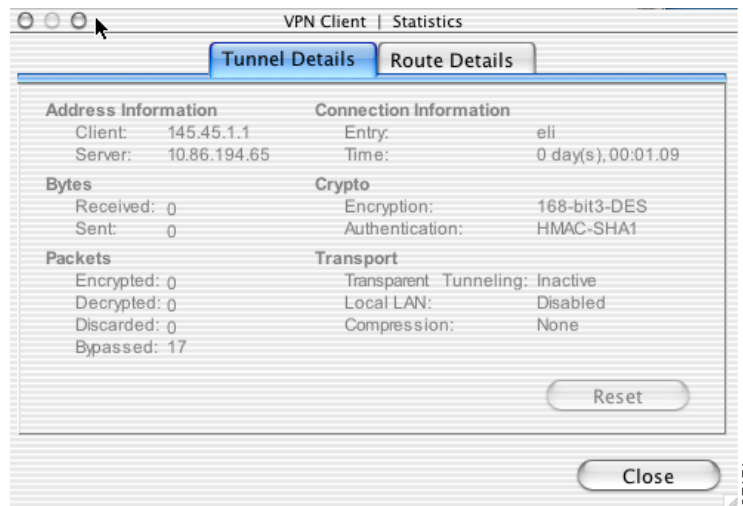
To view VPN session statistics, choose **Statistics** from the Status menu.

The Statistics window has two tabs, Tunnel Details and Route Details. The Tunnel Details tab lists information about the VPN tunnel. The Route Details tab lists information about excluded and secured routes.

Tunnel Details

The Tunnel Details tab (Figure 7-8) displays the IP addresses assigned for this session and byte and packet statistics.

Figure 7-8 Statistics Window—Tunnel Details



Use the **Reset** button to clear the fields in the tunnel details display. Alternately, you can reset the statistics by choosing **Reset Stats** from the Status menu.

Table 7-2 describes the statistics fields on the Tunnel Details tab.

Table 7-2 Tunnel Details

Field	Description
Client Address Information	IP address assigned to the client for this VPN session
Server Address Information	IP address of the VPN device you are connected to.
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.
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.

Table 7-2 Tunnel Details (continued)

Field	Description
Connection Entry Name	The name of the connection entry for this VPN session.
Connection Time	The connection time for this VPN session.
Encryption	<p>Encryption algorithm used for this VPN session. The VPN Client supports:</p> <ul style="list-style-type: none"> • 56-bit DES (Data Encryption Standard) • 168-bit Triple-DES • AES 128-bit and 256-bit <p>Note The VPN Client continues to support DES/MD5. However, support for DES/SHA is no longer available, and Release 3.7 and later 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 <i>Cisco VPN Client Administrator Guide</i> lists all supported encryption configurations.</p>
Authentication	<p>Authentication algorithm used for this VPN session. The VPN Client supports:</p> <ul style="list-style-type: none"> • HMAC-MD 5 (Hashed Message Authentication Coding with Message Digest 5 hash function) • HMAC-SHA-1 (Secure Hash Algorithm hash function)
Transparent tunneling	Displays whether transparent tunneling 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.

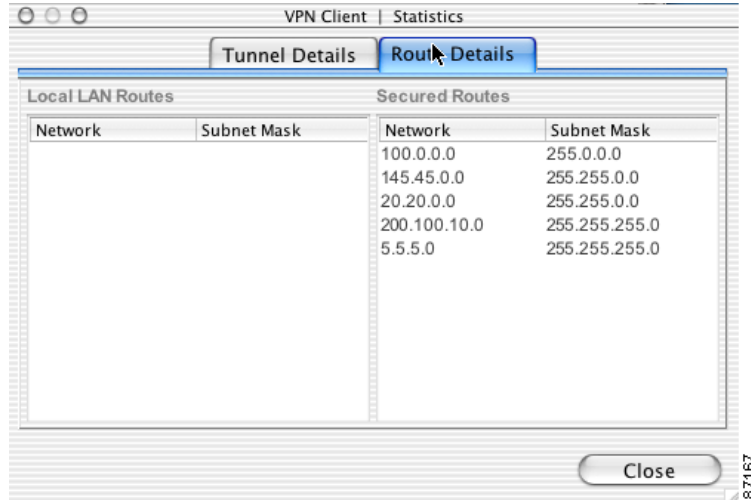
Route Details

The Route Details tab displays the routes that VPN traffic takes into the network, which can be either Local LAN routes or secured routes.

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

To display route data during an active VPN session, open the Statistics window and click the Route Details tab (Figure 7-9).

Figure 7-9 Statistics Window—Route Details



For each local LAN or secured route, the following information is listed:

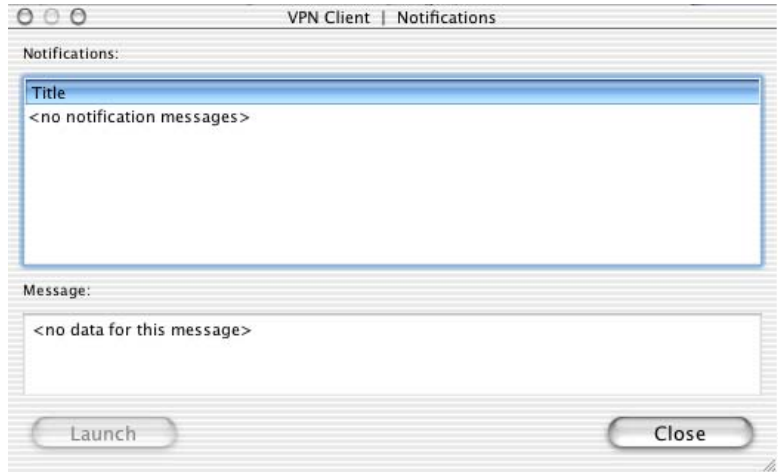
- Network—The IP address of the VPN device providing the route to the network.
- Subnet Mask—The subnet mask applied to the route.

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 7-10), choose **Notifications** from the Status menu.

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 7-10 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.

Some notifications contain a URL which directs you to the location of more current versions of the VPN Client. If the URL exists, the Launch button becomes active. If you click the **Launch** button, a browser open on your workstation.



A

- administrator password [2-4](#)
- advanced mode
 - buttons [3-5](#)
 - menus [3-6](#)
 - tabs [3-5](#)
 - window [3-4](#)
- AES (Advanced Encryption Standard) [1-6](#)
- aggressive mode [1-6](#)
- algorithms
 - data compression [1-7](#)
 - encryption [1-6](#)
 - in VPN client [1-2](#)
- application binaries [2-8](#)
- applications directory [2-8](#)
- authentication
 - algorithms [1-6](#)
 - certificate [4-4](#)
 - extended [1-7](#)
 - features [1-5](#)
 - installation [2-4](#)
 - methods [4-3](#)
 - mode [1-6](#)
- authentication methods [5-3](#)
 - digital certificate [5-6](#)
 - RADIUS [5-4](#)
 - SecurID [5-5](#)
 - shared key [5-3](#)
 - VPN group name [5-4](#)
- authenticity [6-8](#)

B

- backup servers
 - change order [4-9](#)
 - list [4-8](#)
 - tab [4-3](#)
- base-64 encoding type [6-3](#)
- binaries, application [2-8](#)
- binary encoding type [6-3](#)
- bytes received [7-9](#)

C

- CA (Certificate Authority) [6-2](#)
- cable modem [1-1](#)
- CA URL [6-3](#)
- certificate
 - at login [5-6](#)
 - authentication [4-4](#)
 - chain [4-5](#)
 - challenge password [6-3](#)
 - change password [3-7](#)
 - changing password [6-12](#)
 - contents [6-2](#)
 - deleting [6-10](#)
 - digital [1-6](#)
 - enrollment [3-10](#)
 - expiration [6-2](#)
 - exporting [6-9](#)
 - file enrollment [6-2](#)
 - identity [4-3](#)
 - importing [6-7](#)
 - import password [6-7](#)

- management [6-1](#)
- new password [6-3](#)
- online enrollment [6-2](#)
- password [5-6, 6-7](#)
- peer [1-5](#)
- properties [6-8](#)
- resume enrollment [3-8](#)
- store [6-1](#)
- validity [3-7](#)
- verifying [6-11](#)
- viewing [6-7](#)
- view properties [3-7](#)
- X.509 [1-6](#)
- certificate chain [6-9](#)
- certificates menu [3-7](#)
- certificates tab [3-5](#)
- challenge password, certificate [6-3](#)
- challenge phrase [2-5](#)
- changing
 - certificate password [6-12](#)
 - password on an enrollment request [6-6](#)
- classes for logging [7-6](#)
- clear log file [7-5](#)
- client type (platform) [3-1](#)
- client upgrades [7-12](#)
- coding, HMAC [1-6](#)
- command-line interface, logging [7-6](#)
- common name, certificate [6-4](#)
- configuration file [7-1](#)
- connecting
 - default connection entry [5-3](#)
- connecting to default connection entry [5-3](#)
- connection
 - prerequisites [5-1](#)
 - status [5-3](#)
- connection entries tab [3-5](#)
- connection entry
 - creating [4-2](#)
 - default [5-3](#)

- defined [4-1](#)
- delete [3-6](#)
- deleting [7-3](#)
- importing [7-1](#)
- menu [3-3](#)
- modifying [7-2](#)
- saving [7-3](#)
- setting default [3-3, 3-6](#)
- template [3-6](#)
- connection manager [7-6](#)
- connection technologies [1-1](#)
- connection types [1-3](#)
- connect on open [5-3](#)
- copyright information [3-1](#)
- country code [6-8](#)
- CRL (Certificate Revocation List) [6-9](#)
- custom installation [2-9](#)

D

- data compression [1-7, 7-10](#)
- data formats [ix](#)
- DDNS (Dynamic Domain Name System) [1-4](#)
- Dead Peer Detection
 - see DPD
- default connection entry [3-3](#)
 - connecting [5-3](#)
- default installation [2-9](#)
- delete
 - certificate [6-10](#)
 - connection entry [3-6, 7-3](#)
- delete with reason [1-4](#)
- deleting
 - enrollment request [6-5](#)
- department, certificate [6-4](#)
- DES (Data Encryption Standard) [7-10](#)
- destination volume [2-7](#)
- DHCP request [1-4](#)
- Diffie-Hellman groups [1-6](#)

directory, applications [2-8](#)
 disable logging [3-8](#)
 disconnect client [3-3, 3-9](#)
 disk drive [2-7](#)
 disk space [2-1](#)
 DNS, split [1-6](#)
 documentation
 conventions [viii](#)
 obtaining [ix](#)
 related [viii](#)
 domains [1-6](#)
 DPD
 adjusting peer time out [4-8](#)
 keep alive mechanism
 DSL [1-1](#)
 duplicate function [3-9](#)

E

easy install [2-9](#)
 Easy VPN [1-1](#)
 enable logging [3-8](#)
 enable transport [4-7](#)
 encoding types [6-3](#)
 encryption algorithm [1-6](#)
 enrolling certificates [6-2](#)
 enrollment, resume [3-10](#)
 enrollment parameters [6-4](#)
 enrollment request
 changing password [6-6](#)
 deleting [6-5](#)
 resuming [6-6](#)
 viewing [6-5](#)
 enrollment type, certificate [6-2](#)
 erase user password [3-9](#)
 ESP (protocol 50) [4-7](#)
 event logging [3-2](#)
 event messages [3-5](#)
 export certificate [6-9](#)

export path, certificate [6-9](#)
 extended authentication [1-7, 7-6](#)

F

features
 authentication [1-5](#)
 IPSec [1-5](#)
 program [1-3](#)
 VPN Client [1-3](#)
 firewall, see PIX firewall
 firewalls [4-7](#)
 FQDN (Fully Qualified Distinguished Name) [6-8](#)

G

graphical user interface, logging [7-6](#)
 group
 authentication [5-4](#)
 names [1-2](#)
 passwords [1-2](#)
 group authentication [4-3](#)
 GUI
 installing [2-8](#)
 logging [7-6](#)
 supported [1-1](#)

H

hard disk space [2-1](#)
 hash [6-8, 7-10](#)
 hash function, MD5 [1-6](#)
 hiding client window [3-2](#)
 hijacked IP address [1-5](#)
 HMAC (Hashed Message Authentication Coding) [1-6](#)
 host name [4-3](#)
 host name population [1-4](#)
 hybrid authentication on Darwin [2-4](#)

I

- icon for installer [2-2](#)
- identity certificate [4-3](#)
- IKE (Internet Key Exchange) [1-2, 7-6](#)
- IKE keepalives [1-5](#)
- image file [2-2](#)
- import
 - certificate [6-7](#)
 - connection entry [7-1](#)
 - password [6-7](#)
- installation
 - authentication [2-4](#)
 - customize [2-9](#)
 - default [2-9](#)
 - process [2-6](#)
 - requirements [2-1](#)
 - successful [2-11](#)
- installation packages [2-8](#)
- installer
 - directory [2-3](#)
 - extracting [2-2](#)
 - icon [2-2](#)
 - package [2-2](#)
- installing the GUI [2-4, 2-8](#)
- interfaces, supported [1-1](#)
- invalid certificate [6-11](#)
- IP address [7-9](#)
- IPCOMP (IP compression) [1-7](#)
- IPSec
 - attributes [1-6](#)
 - features [1-5](#)
 - group [4-4](#)
 - module [7-6](#)
 - with VPN [1-2](#)
- ISDN [1-1](#)

K

- keepalives [1-5](#)
- kernel extension [2-8](#)
- key
 - pair [6-8](#)
 - preshared [1-6, 4-1](#)
 - size [6-2, 6-8](#)
- keywords [2-2](#)

L

- LAN connection [1-1](#)
- launch, from notification [1-4](#)
- launch browser [7-12](#)
- license agreement [2-7](#)
- local LAN access [1-3, 4-7, 7-10](#)
- log
 - menu [3-8](#)
 - settings [3-8](#)
 - tab [3-5](#)
 - window [3-8, 7-8](#)
- log file, saving [3-8, 7-8](#)
- logging
 - classes [7-6](#)
 - clear [7-5](#)
 - levels [7-7](#)
 - options [7-5](#)
 - view in external window [7-7](#)
- login, simultaneous [4-1](#)

M

- Macintosh OS
 - services [3-2](#)
- main mode [1-6](#)

- main tabs
 - certificates [3-5](#)
 - connection entries [3-5](#)
 - log [3-5](#)
- main VPN Client window [3-4, 5-2](#)
- managing
 - certificates [6-1](#)
 - connection entries [7-1](#)
- MD5 (Message Digest 5) [1-6](#)
- menus
 - certificates [3-7](#)
 - connection entries [3-6](#)
 - log [3-8](#)
 - main [3-6](#)
 - right-click [3-8](#)
 - status [3-7](#)
- minimize client window [3-2](#)
- mode
 - advanced [3-4](#)
 - aggressive [1-6](#)
 - authentication [1-6](#)
 - configuration [1-7](#)
 - main [1-6](#)
 - simple [3-2](#)
 - transparent tunneling [4-7](#)
 - tunnel encapsulation [1-7](#)
- modify connection entry [7-2](#)
- MTU size [1-4](#)

N

- NAT Transparency [1-4, 7-10](#)
- new password, certificate [6-3](#)
- notifications [7-11](#)
- notifications, from VPN device [1-4](#)
- notifications, viewing [3-7](#)

O

- obtaining
 - documentation [ix](#)
 - installer [2-2](#)
 - software [2-2](#)
- operating system [1-3](#)

P

- packages
 - installation [2-8](#)
 - remove [2-9](#)
- packets
 - querying [1-6](#)
 - tunneling [1-6](#)
- packets encrypted [7-9](#)
- parameters
 - defining [2-3](#)
 - transport [4-6](#)
- passcodes [5-5](#)
- password
 - administrator [2-4](#)
 - certificate [6-7](#)
 - challenge [6-3](#)
 - changing [3-7](#)
 - import [6-7](#)
 - new [6-3](#)
- passwords
 - enrollment request
 - changing [6-6](#)
 - personal certificate [6-12](#)
- PAT (Port Address Translation) [1-4, 4-7](#)
- pcf file [2-3, 7-1](#)
- peer certificate [1-5](#)
- peer response timeout [4-8](#)
 - adjusting [4-8](#)
- peer VPN concentrator [4-5](#)
- PIX firewall [1-1](#)

PKI (Public Key Infrastructure) [1-3, 4-4](#)
 platform [3-1](#)
 POTS [1-1](#)
 preconfiguration tasks [2-2](#)
 preconfigured files [2-2](#)
 preconfigured keys [2-1](#)
 preferences, client window [3-1](#)
 prerequisites
 installation [2-1, 2-6](#)
 passwords [2-1](#)
 RSA PIN [5-1](#)
 VPN connection [5-1](#)
 preshared keys [4-1](#)
 private network [2-3](#)
 profile, user [2-3, 7-1](#)
 program features [1-3](#)
 progress bar, installation [2-10](#)
 protocol [1-3](#)
 protocols
 DPD

Q

quitting client [3-2](#)

R

RADIUS authentication [5-4](#)
 reset statistics [3-7, 7-9](#)
 resume enrollment [3-10](#)
 resuming an enrollment request [6-6](#)
 right-click menus [3-8](#)
 root certificate
 installing automatically on Darwin [2-4](#)
 routing data [3-2](#)
 RSA [5-5](#)
 run mode [3-2](#)

S

SA (security association) [1-4](#)
 save log file [3-8](#)
 SCEP (Simple Certificate Enrollment Protocol) [6-1](#)
 SecurID authentication [5-5](#)
 session time [3-4](#)
 SHA-1 (Secure Hash Algorithm) [1-6](#)
 shared key authentication [5-3](#)
 show/hide window [3-2](#)
 signing key pair [6-8](#)
 simple mode
 menu [3-3](#)
 window [3-2](#)
 single SA [1-4](#)
 software upgrades [1-4, 7-11](#)
 split DNS [1-6](#)
 split tunneling [1-4, 1-6](#)
 stateful firewalls [4-7](#)
 statistics
 tunnel [3-7](#)
 viewing [7-8](#)
 status bar [3-4, 5-3](#)
 status menu [3-3, 3-7](#)
 subnet mask [7-11](#)
 supported VPN devices [1-1](#)
 system administrator [2-1](#)
 system requirements [2-1](#)

T

tab
 certificates [3-5](#)
 connection entries [3-5](#)
 log [3-5](#)
 TCP port [4-7](#)
 technical support [x](#)
 template [3-6](#)
 terminate connections [1-1](#)

terms, license agreement [2-7](#)

toggle command [3-2](#)

tooltips, enabling [3-2](#)

transparent tunneling [1-5, 4-7](#)

transport

parameters [4-6](#)

tunneling [4-7](#)

Triple-DES (Data Encryption Standard) [1-6](#)

tunneling

encapsulation mode [1-7](#)

protocol [1-3](#)

split [1-6](#)

transparent [4-7](#)

tunnel routing data [3-2](#)

tunnel statistics [3-7](#)

U

UDP packets [4-7](#)

uninstalling the VPN client [2-4](#)

upgrades [7-11](#)

user

access [1-2](#)

password [3-9](#)

profiles [2-3](#)

user authentication

methods [5-3](#)

supported types [1-3](#)

VPN device [1-5](#)

user profiles, installing [2-8](#)

V

verify certificate [3-7, 6-11](#)

version information [3-4](#)

view

certificate properties [3-7](#)

certificates [6-7](#)

logging [7-7](#)

notifications [3-7](#)

statistics [7-8](#)

viewing

enrollment request [6-5](#)

VPN Client

defined [1-2](#)

features [1-3](#)

icon [5-2](#)

menus [3-6](#)

quitting [3-2](#)

window [3-4, 5-2](#)

VPN Daemon [7-6](#)

VPN device

DPD [4-8](#)

VPN devices [1-1](#)

VPN Group [4-3](#)

VPN server notification [1-4](#)

VPN startup [2-8](#)

W

warnings [6-10](#)

window, log [3-8](#)

window settings [3-2](#)

X

X.509 [1-2](#)

XAUTH (extended authentication) [1-7](#)

