

VPN Client Administrator Guide

Release 3.5.1

January 2002

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

Customer Order Number: DOC-7813754=
Text Part Number: 78-13754-02

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.

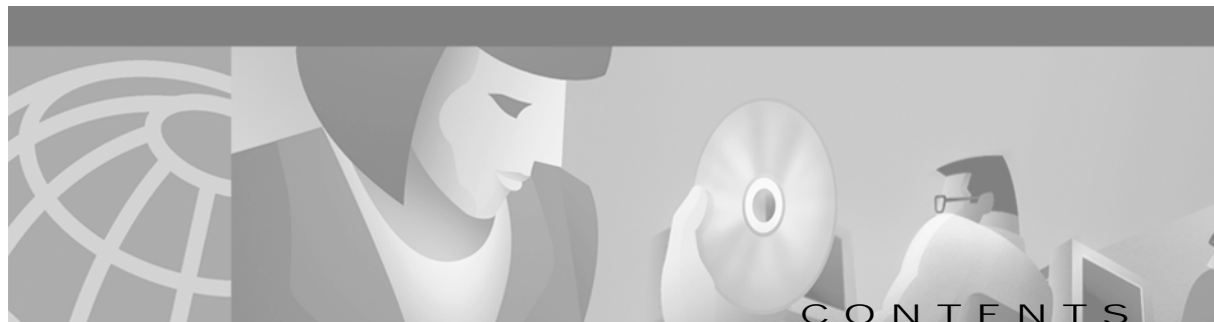
AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible 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, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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. (0110R)

VPN Client Administrator Guide

Copyright © 2001, 2002 Cisco Systems, Inc.

All rights reserved.



Preface vii

Audience vii

Organization viii

Related Documentation viii

VPN 3000 Series Concentrator Documentation ix

Other References ix

Conventions x

Data Formats xi

Obtaining Documentation xi

World Wide Web xi

Documentation CD-ROM xi

Ordering Documentation xii

Documentation Feedback xii

Obtaining Technical Assistance xii

Cisco.com xii

Technical Assistance Center xiii

 Contacting TAC by Using the Cisco TAC Website xiii

 Contacting TAC by Telephone xiii

CHAPTER 1

Configuration Information for an Administrator 1-1

VPN 3000 Series Concentrators 1-1

 Configuring a VPN 3000 Concentrator for Remote Access Users 1-1

 Completing Quick Configuration 1-1

 Creating an IPSec Group 1-2

 Creating VPN Client User Profiles 1-3

 Configuring VPN Client Users for Digital Certificate Authorization 1-3

 Configuring VPN Client Firewall Policy 1-4

 Overview 1-4

 Firewall Configuration Scenarios 1-7

 Defining a Filter and Rules to Use with Firewalls for CPP 1-9

 Configuring the VPN 3000 Concentrator to Enforce Firewall Usage on the VPN Client 1-10

 Setting up Cisco Integrated Client Firewall (CIC) for CPP 1-11

 Custom Vendor Codes 1-11

 Obtaining Firewall Troubleshooting Information 1-12

 Notifying Remote Users of a Client Update 1-13

Setting up Local LAN Access for the VPN Client	1-14
Configuring Entrust Entelligence for the VPN Client	1-16
Setting up the VPN Client for Authentication using Smart Cards	1-18

CHAPTER 2

Preconfiguring the VPN Client for Remote Users 2-1

Profiles	2-1
File format for All Profile Files	2-1
Making a Parameter Read Only	2-2
Creating a Global Profile	2-2
Global Profile Configuration Parameters	2-3
Creating Connection Profiles	2-6
Creating a .pcf file for a Connection Profile	2-7
Connection Profile Configuration Parameters	2-7
Distributing Preconfigured VPN Client Software to Users	2-12
Separate Distribution	2-12
Distribution with the VPN Client Software	2-13

CHAPTER 3

Using the VPN Client Command-Line Interface 3-1

CLI Commands	3-1
Displaying a List of VPN Client Commands	3-1
Starting a Connection—vpnclient connect	3-1
Note on Notrayicon Parameter	3-2
Displaying a Notification—vpnclient notify	3-3
Ending a Connection—vpnclient disconnect	3-4
Displaying Information About Your Connection—vpnclient stat	3-4
Return Codes	3-7
Application Example	3-9

CHAPTER 4

Rebranding the VPN Client Software 4-1

Areas Affected by Branding	4-2
Installation Bitmap	4-2
Program Menu Titles and Text	4-2
VPN Dialer	4-3
Window Titles and Text	4-3
Bitmaps	4-4
Icons	4-4
Log Viewer	4-6
Certificate Manager	4-6

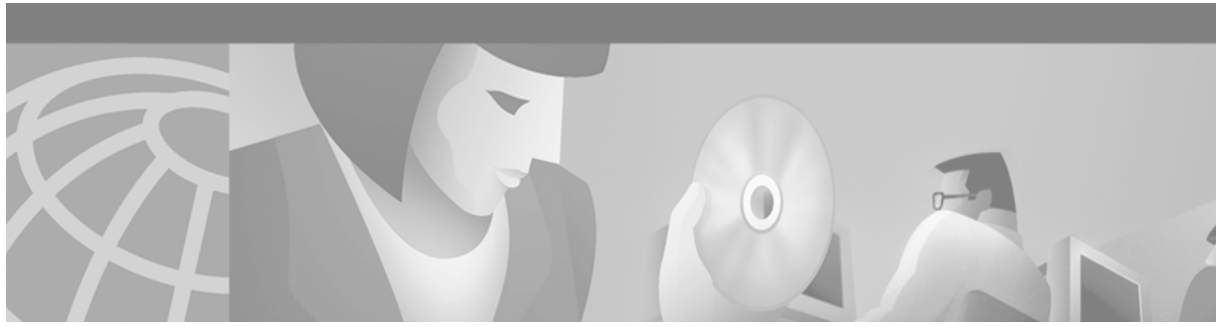
Creating the oem.ini File	4-7
Sample oem.ini File	4-7
oem.ini File Keywords and Values	4-8
Start Before Logon and GINAs	4-11
Fallback Mode	4-11
Incompatible GINAs	4-12
Installing the VPN Client in Silent Mode	4-12
Additional Bitmap—setup.bmp	4-13

CHAPTER 5

Troubleshooting and Programmer Notes 5-1

Troubleshooting the VPN Client	5-1
Gathering Information for Customer Support	5-1
If Your Operating System is Windows 98, 98 SE, ME, 2000, or XP	5-1
If Your Operating System is Windows NT or Windows 2000	5-2
Solving Common Problems	5-3
Shutting Down on Windows 98	5-3
Booting Automatically Starts up Dial-up Networking on Windows 95	5-4
Changing the MTU Size	5-4
Programmer Notes	5-6
Testing the Connection	5-6

INDEX



Preface

This *VPN Client Administrator Guide* tells you how to set up the Cisco VPN Client for users. This manual supplements the information provided in accompanying documentation for the Cisco VPN devices that work with the VPN Client.

The VPN Client comprises the following applications:

- VPN Dialer—Connects a user to a Cisco VPN device
- Log Viewer—Captures, filters, and displays messages generated by the VPN Client
- Certificate Manager—Lets you enroll for and manage certificates
- Uninstall VPN Client—Lets you remove the VPN Client software from your system
- SetMTU—Lets you manually change the size of the maximum transmission unit (see “Changing the MTU Size”)

For information about how to use these applications, see the *VPN Client User Guide*

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

- Cisco VPN 3000 Series Concentrator
- Cisco VPN 5000 Series Concentrator
- Cisco Secure PIX Firewall devices
- IOS platform devices, such as the Cisco 7100 Series Routers

Audience

We assume you are an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage internetworking systems. However, virtual private networks and VPN devices might be new to you. You should be familiar with Windows system configuration and management.

Organization

The VPN Administrator Guide is organized as follows:

Chapter	Title	Description
Chapter 1	Configuration Information for an Administrator	Explains how to configure a VPN 3000 Concentrator for remote access from a VPN Client, personal firewalls, and local LAN access. Also describes how to configure a VPN Client to work with Entrust Entelligence.
Chapter 2	Preconfiguring the VPN Client for Remote Users	Shows how to create global and user profiles.
Chapter 3	Using the VPN Client Command-Line Interface	Explains how to use the command-line interface (CLI) to connect to a VPN device, how to disconnect from a VPN device, and how to get status information from a VPN device. You can use these commands in batch mode.
Chapter 4	Rebranding the VPN Client Software	Describes how to use your own names and icons for the VPN Client applications instead of Cisco Systems names (called <i>branding</i>). This chapter also describes how to install and reboot the VPN Client software without user intervention, called <i>silent mode</i> .
Chapter 5	Troubleshooting and Programmer Notes	Lists a few troubleshooting techniques. Describes how to use the SetMTU application.

Related Documentation

The *VPN Client User Guide* explains how to install the VPN Client software, configure connection entries, connect to Cisco VPN devices, and manage VPN connections. Also the VPN Client includes an online HTML-based help system that you can access through a browser in several ways: clicking the Help icon on the Cisco Systems VPN Client programs menu (Start>Programs>Cisco Systems VPN Client>Help), pressing **F1** while using the applications, or clicking the Help button on screens that include it.

To view the latest version of the VPN Client documentation on the Cisco Web site, go to the following site and click on VPN Clients.

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

VPN 3000 Series Concentrator Documentation

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

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

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

The VPN 3000 Concentrator Manager (the Manager) also includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

Other References

Other useful references include:

- Cisco Systems, *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001.
- *Virtual Private Networking: An Overview*. Microsoft Corporation: 1999. (Available from Microsoft website.)
- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).
- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	User actions and commands are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
<code>screen font</code>	Terminal sessions and information the system displays are in <code>screen font</code> .
boldface screen font	Information you must enter is in boldface screen font in the command-line interface (for example, <code>vpnclient stat</code>).
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .

Notes use the following conventions:



Note

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

Cautions use the following conventions:



Caution

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

Data Formats

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

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

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products Marketplace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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



Configuration Information for an Administrator

This chapter provides information to a network administrator that supplements information that the *VPN Client User Guide* and the *VPN 3000 Series Concentrator Reference Volume I: Configuration* manual contain.

VPN 3000 Series Concentrators

We recommend that you carefully read the chapter on “User Management,” *VPN 3000 Series Concentrator Reference Volume I: Configuration*. The “User Management” chapter contains complete information on setting up remote users to connect through the IPSec tunnel, and also explains how to use features such as setting up a client banner, firewalls, split tunneling, and so on.

This section covers the following tasks:

- Configuring a VPN 3000 Concentrator for Remote Access Users
- Configuring VPN Client Firewall Policy
- Notifying Remote Users of a Client Update
- Setting up Local LAN Access for the VPN Client

Configuring a VPN 3000 Concentrator for Remote Access Users

Before VPN Client users can access the remote network through a VPN 3000 Concentrator, you must configure the VPN 3000 Concentrator:

- Complete all the steps in quick configuration, as a minimum.
- Create and assign attributes to an IPSec group.
- Create and assign attributes to VPN Client users as members of the IPSec group.
- Configure VPN Client users who are using digital certificates instead of pre-shared keys for authentication.

Completing Quick Configuration

For steps in quick configuration, refer to *VPN 3000 Series Concentrator Getting Started* or Quick Configuration online help.

Be sure to perform the following tasks.

- Configure and enable both Ethernet interfaces 1 and 2 (Private and Public) with appropriate IP addresses and filters.
- Configure a DNS server and default gateway.
- Enable IPSec as one of the tunneling protocols (the default).
- Enter a group name and password for an IPSec group.
- Configure at least one method for assigning user IP addresses.
- Configure authentication servers for group and user authentication. These instructions assume the internal server for both, but you can set up any of the external servers instead.
- Save the configuration.

Creating an IPSec Group

During the Quick Configuration, you can automatically create an IPSec group. If you want to add an IPSec group or modify one, follow the procedure in this section.

Refer to “User Management” in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*, or the online help, for details on configuring groups.

You may want to set base-group attributes before you create an IPSec group; see the Configuration | User Management | Base Group screen. We suggest you carefully review the General Parameters and IPSec Parameters on that screen. If you use external user authentication, base-group attributes are especially important since they govern all attributes that the external server does not return.

The VPN Client uses the IPSec protocol for creating and using secure tunnels. IPSec has two authentication phases: first for the group, then for the user. These instructions assume that you are using the VPN 3000 Concentrator internal authentication server for both group and user authentication.

Use the Configuration | User Management | Groups | Add screen to create an IPSec group:

-
- | | |
|---------------|--|
| Step 1 | Under the Identity tab, enter a Group Name and Password. VPN Client users need these to configure and connect with the VPN Client; see Table 2-1 in the <i>VPN Client User Guide</i> , Chapter 2. |
| Step 2 | Under Type, choose Internal . This parameter determines the group authentication method. If you select External, you must configure an external RADIUS server to authenticate and return appropriate group attributes. |
| Step 3 | Under the General Parameters tab Tunneling Protocols, be sure IPSec is checked. |
| Step 4 | Under the IPSec Parameters tab IPSec SA, select ESP-3DES-MD5 to require Triple-DES authentication, which is the most secure. Alternatively, you could choose ESP-DES-MD5 , which uses DES authentication and provides a minimum level of security. To create or customize the Security Association (SA), see the Configuration Policy Management Traffic Management Security Associations screens. |
| Step 5 | Under IPSec Parameters > Authentication, choose the method you use for user authentication; for example, Internal. If you choose another authentication method, be sure to configure the external authentication server appropriately and supply users with the appropriate entries for Table 2-1 in the <i>VPN Client User Guide</i> , Chapter 2. |
| Step 6 | To require users to enter a password each time they log in, we suggest that you <i>not</i> check Allow Password Storage on Client. Not checking this parameter provides greater security. |
| Step 7 | To add the group, click Add , and then save the configuration. |
-

Creating VPN Client User Profiles

For details on configuring VPN Client users within a group, see “User Management,” in the *VPN 3000 Series Concentrator Reference Volume I: Configuration*.

Use the Configuration | User Management | Users | Add or Modify screen to configure a VPN Client user:

-
- | | |
|---------------|---|
| Step 1 | Enter a User Name and Password. VPN Client users need a user name and password to authenticate when they connect to the VPN Client; see Table 2-1 in the <i>VPN Client User Guide</i> , Chapter 2. |
| Step 2 | Under Group, select the group name you configured under the section “Creating an IPSec Group.” |
| Step 3 | Carefully review and configure other attributes under General Parameters and IPSec Parameters. Note that if you are adding a user, the Inherit? checkboxes refer to base-group attributes; if you are modifying a user, the checkboxes refer to the user’s assigned-group attributes. |
| Step 4 | Click Add or Apply , and save the configuration. |
-

Configuring VPN Client Users for Digital Certificate Authorization

Use the following procedure to configure the VPN 3000 Concentrator for IPSec Client connections using digital certificates.

- Activate an IKE RSA.
- Configure a security association (SA) to use the VPN 3000 Concentrator’s identity certificate.
- Create a new group for clients connecting with certificates.
- Add VPN Client users to the new group.
- For details refer to the *VPN 3000 Series Concentrator Reference Volume I: Configuration*:
 - On configuring IKE proposals, see “Tunneling Protocols.”
 - On configuring SAs, see “Policy Management.”
 - On configuring groups and users, see “User Management.”

Follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Use the Configuration System Tunneling Protocols IPSec IKE Proposals screen to activate an IKE proposal for certificates: <ol style="list-style-type: none"> a. Activate either CiscoVPNClient-3DES-MD5-RSA or CiscoVPNClient-3DES-SHA-DSA. b. If you do not want to modify one of the standard proposals, copy an active proposal and give it a new name; for example, copy the IKE-3DES-MD5 and name it “IKE-Proposal for digital certificate use.” |
| Step 2 | Use the Configuration Policy Management Traffic Management SAs screen to create a new SA. You can use the Security Associations link on the IKE Proposals screen. <ol style="list-style-type: none"> a. Add a new SA. For example, name it “Security association for digital certificate use.” b. Change the Digital Certificates parameter to identify the VPN 3000 Concentrator’s digital certificate. This is the only field that you need to change. |

- Step 3** Use the Configuration | User Management | Groups | Add or Modify screen to configure a group for using digital certificates:
- Under Identity parameters, enter a group name that is the same as the Organizational Unit (OU) field of the certificate(s) for this group. For example, if the OU in the VPN Client certificate is Finance, you would enter Finance as the group name. The OU is a field of the ASN.1 Distinguished Name (DN).
 - Under IPsec Parameters > IPsec SA, select the IPsec SA you created in step 2; for example, "Security association for digital certificate use."
 - Under IPsec Parameters > Authentication, select the method you use for user authentication; for example, Internal. If you select another authentication method, be sure to configure the external authentication server appropriately and supply users with the appropriate entries for Table 2-1 in Chapter 2.
 - Click **Add** or **Apply**, and save the configuration.
- Step 4** Use the Configuration | User Management | User | Add or Modify | Identity screen to configure VPN Client users for digital certificates:
- As the group name, enter the name (OU) you have set up in step 3 as the group parameter; continuing the example, you would enter `Finance`.
 - Click **Add** or **Apply**, and save the configuration.
-

Configuring VPN Client Firewall Policy

To provide a higher level of security, the VPN Client can either enforce the operation of a supported firewall or receive a pushed down stateful firewall policy for Internet bound traffic. This section explains how firewalls work with the VPN Client, lists the personal firewall products that the VPN Client can enforce for Internet traffic, and shows how to configure a stateful firewall policy for the VPN Client to enforce.

Overview

This section summarizes how a network administrator can control personal firewall features from a VPN 3000 Concentrator operating as the Secure Gateway communicating policy information to the VPN Client running on a Windows platform.

Optional versus Required Configuration Option

The VPN Concentrator can require that a VPN Client use a designated firewall configuration or make this configuration optional. Making a designated firewall configuration optional gives a VPN Client user a chance to install the desired firewall on the client PC. When the VPN Client tries to connect, it notifies the VPN Concentrator about any firewalls installed on the client PC. The VPN Concentrator sends back information about what firewall the VPN Client must use. If the firewall configuration is optional, the VPN Concentrator can notify the VPN Client that there is a mismatch but still allow the VPN Client to establish a tunnel. The optional feature thus lets the network administrator of the VPN Client maintain the tunneled connection while obtaining and installing the required firewall.

Stateful Firewall (Always On)

The VPN Client configuration option Stateful Firewall (Always On) is activated on the VPN Client. This configuration option is not negotiated. The policy is not controlled from the VPN Concentrator. The VPN Client user enables this option on the VPN Client under the Options menu or while the VPN Client is active by right-clicking on the VPN Client icon and selecting the option.

When enabled, this feature allows no inbound sessions from all networks, whether or not a VPN connection is in effect. Also, the firewall is active for both tunneled and nontunneled traffic. Users who enable this feature cannot have a server running on their PC and their system can no longer respond to PING requests. There are two exceptions to allowing no inbound traffic. The first is DHCP, which sends requests to the DHCP server out one port but receives responses from DHCP through a different port. For DHCP, the stateful firewall allows inbound traffic. The second is ESP (VPN data). The stateful firewall allows ESP traffic from the secure gateway, because ESP rules are packet filters and not session-based filters.

Stateful Firewall (Always On) is the most basic VPN Client firewall and provides the highest level of security. However, it is also the least flexible, since it blocks almost all incoming traffic and does not allow outbound traffic to be limited.

Cisco Integrated Client

The VPN Client on the Windows platform includes a stateful firewall that incorporates Zone Labs technology. This firewall is used for both the Stateful Firewall (Always On) feature and the Centralized Protection Policy (see “Centralized Protection Policy (CPP)”). This firewall is transparent to the VPN Client user, and is called “Cisco Integrated Client Firewall” or CIC. The “Always On” option lets the VPN Client user choose to have basic firewall protection always on; CPP lets an administrator define rules to enforce for inbound/outbound Internet traffic during split tunneling operation. Since tunnel everything already forces all traffic back through the tunnel, CPP is not used for tunnel everything.

Centralized Protection Policy (CPP)

Centralized Protection Policy (CPP) also known as *push policy*, lets a network administrator define a set of rules for allowing or dropping Internet traffic while the VPN Client is tunneled in to the VPN Concentrator. A network administrator defines this policy on the VPN Concentrator, and the policy is sent to the VPN Client during connection negotiation. The VPN Client passes the policy to the Cisco Integrated Client, which then enforces the policy. If the client user has already selected the “Always On” option, any more restrictive rules are enforced for Internet traffic while the tunnel is established. Since CIC includes a stateful firewall module, most configurations block all inbound traffic and permit either all outbound traffic or traffic through specific TCP and UDP ports outbound. CIC, Zone Alarm, and Zone Alarm Pro firewalls can assign firewall rules. CPP rules are in effect during split tunneling and help protect the VPN Client PC from Internet attacks by preventing servers from running and by blocking any inbound connections unless they are associated with outbound connections.

CPP provides more flexibility than the Stateful Firewall (Always On) feature, since with CPP, you can refine the ports and protocols that you want to permit.

Policy Configured on the Remote PC—Personal Firewall Enforcement

As an alternative to CPP, a network manager can define policy on the personal firewall that is installed on the same PC as the VPN Client. This approach accommodates situations where there is already a firewall set up and in use on the PC. The VPN Client then polls the personal firewall every 30 seconds to make sure it is running and if it is not, terminates the secure connection to the VPN Concentrator. In this case, the VPN Concentrator does not define the firewall policy. The only contact the VPN Client has with the firewall is polling it to ascertain that it is running, a capability known as Are You There (AYT). ZoneAlarm, ZoneAlarm Pro, and BlackIce can all use AYT.

Zone Labs Integrity Agent and Integrity Server (IA/IS)

The Zone Labs Integrity solution secures remote PCs on Windows platforms. This feature is a client/server solution that comprises four components:

Integrity Server (IS)—located on a central organization's network, IS maintains policies for the firewall on the remote VPN Client PCs. A network manager defines the policy on the IS, the IS downloads the policy to the Integrity Agent (IA) on the remote PC through a secure tunnel activated through the VPN Concentrator. The IS monitors the PC to ensure enforcement of the policy. The IS also communicates with the VPN Concentrator to establish/terminate connections, exchange session and user information, and report status information.

Integrity Agent (IA)—on the remote PC enforces the protection policies it receives from IS and communicates with IS to exchange policy and status information. The IA also communicates with the VPN Client on the remote PC to obtain server addresses and to exchange status information with the VPN Concentrator.

VPN Concentrator—provides the means for configuring firewall functionality by group. It reports the IS's IP address and other VPN session-related information to the VPN Client, which passes it on to the IA. The VPN Concentrator also communicates with the IS to establish and terminate sessions, exchange session and user information, and request and acquire authentication status.

VPN Client—on the remote PC gets the IS addresses and information from the VPN Concentrator and passes it to the IA. The VPN Client also gets and reports status information from the IA and terminates sessions.

Once the connection is up and IS has communicated the firewall policy to IA, then IS and IA keep in touch through a heartbeat mechanism.

Table 1-1 Summary and Comparison of Firewall Configurations

Product/Policy	Where Defined	Security/Flexibility	What it Does/When Used
Stateful Firewall (Always on)	VPN Client Option	Blocks all unauthorized inbound traffic; least flexible (no application awareness)	Blocks all inbound traffic, all networks with few exceptions.
Centralized Protection Policy (CPP) with Cisco Integrated Client (CIC)	Policy pushed; central control	Centrally controlled. Determined by traffic filters and rules defined on VPN Concentrator	Used with split tunneling to protect VPN Client PC and private network from incoming traffic from the Internet. (Tunnel everything already blocks all nontunneled traffic.)

Table 1-1 Summary and Comparison of Firewall Configurations

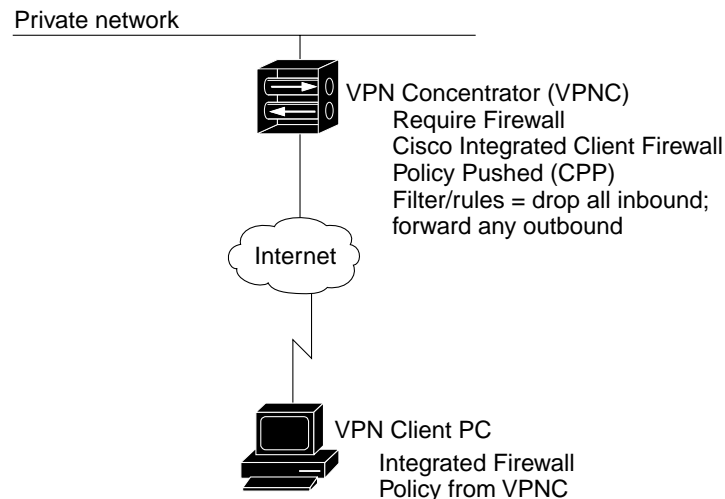
Product/Policy	Where Defined	Security/Flexibility	What it Does/When Used
ZoneAlarm and ZoneAlarm Pro with CPP	Policy pushed; central control	Centrally controlled. Determined by traffic filters and rules defined on VPN Concentrator	Used with split tunneling to protect VPN Client PC and private network from unauthorized incoming and outbound traffic from/to the Internet when a tunnel is active.
ZoneAlarm and ZoneAlarm Pro BlackIce Agent/Defender	Policy defined on VPN Client PC (AYT)	Determined by traffic filters and rules defined on VPN Client PC	Used when personal firewall is installed on the VPN Client and policy is not pushed. No specific policy is enforced.
Client/Server Firewall—Zone Labs Integrity	Policy pushed from Integrity Server (IS)	Most secure and flexible central control of firewall policies.	Enforces centralized corporate role-based policies on the VPN Client PC. Lets administrator monitor and enforce application control and prevent unauthorized inbound/outbound traffic.

Firewall Configuration Scenarios

This section shows two sample firewall configurations. Each diagram shows the parameter settings in effect on the VPN Concentrator as well as the firewall product and policy in effect on the VPN Client.

Cisco Integrated Client

Figure 1-1 shows a typical configuration for Cisco Integrated Client, in which the policy (CPP) is pushed to the VPN Client. This policy blocks inbound traffic from the Internet while split tunneling is in use. Traffic from the private network is not blocked, however.

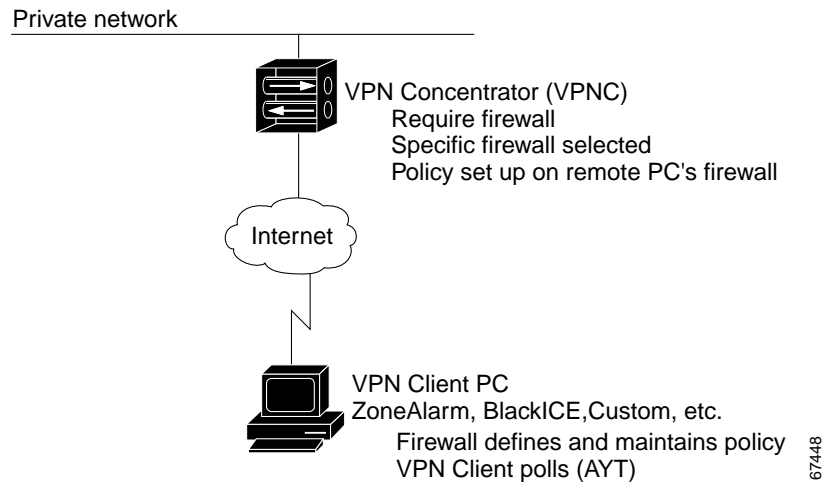
Figure 1-1 Cisco Integrated Client

67447

Remote Firewall

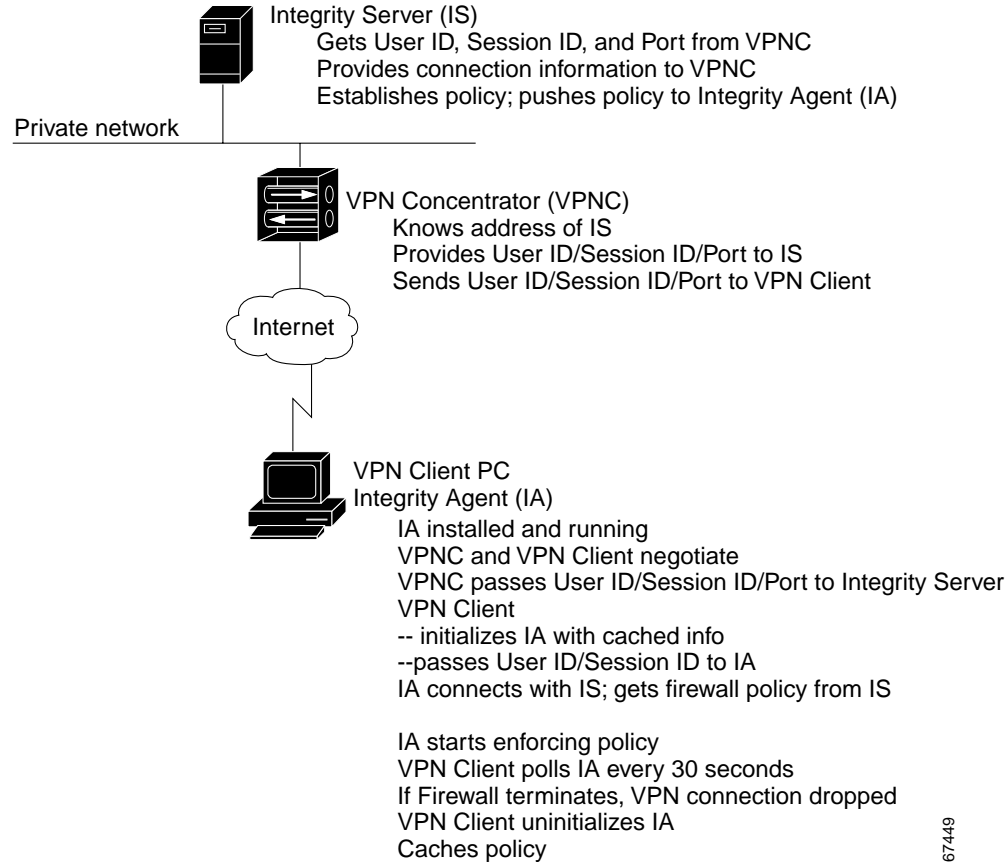
Figure 1-2 shows a configuration in which the policy is set up on a personal firewall on the PC. In this case, Are You There (AYT) is the policy. The VPN Client polls the firewall every 30 seconds to ensure that it is still running and if it is not, the VPN Client terminates the session.

Figure 1-2 Remote Firewall Determines Policy—ZoneAlarm Pro



Client/Server Approach

Figure 1-3 shows a sample configuration for Zone Labs Integrity.

Figure 1-3 Client/Server—Integration With Zone Labs Integrity Server

Defining a Filter and Rules to Use with Firewalls for CPP

When you want the VPN Concentrator to push the firewall policy to the VPN Client, you must first define the policy on the VPN Concentrator. To do this you need to create a filter and add rules to the filter on the public network. The VPN 3000 Concentrator provides a default filter you can use for CPP by selecting it from the menu. The name of this filter is “Firewall Filter for VPN Client (Default)”. This filter allows all outbound traffic and drops all inbound traffic.

Firewall filters are session filters, rather than packet filters. This means that for an “allow all outbound/drop all inbound” rule, the CPP policy lets inbound responses come from outbound sessions *only* from IP protocols TCP, UDP, and ICMP. These protocols are the only protocols that are “stateful.” Most administrators will want to use a rule that blocks all inbound traffic and either permits all outbound traffic or limits outbound traffic to specific TCP and UDP ports. For complete information on creating filters and adding rules in general, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, Configuration | Policy Management | Traffic Management.

Example 1-1 Creating a Filter for a Firewall Policy allowing the VPN Client to Act as a Web Server

This example shows step-by-step how to add a filter that allows outbound traffic to any protocol and to allow inbound traffic from HTTP but none of the other protocols. In this way, you can enable your VPN Client to become a Web server.

-
- Step 1** First, create a rule that allows inbound traffic only from HTTP. To do this, go to Configuration | Policy Management | Traffic Management | Rules.
- Step 2** Click **Add**
- For the Rule Name, enter the name, such as **FW-Allow incoming HTTP**.
 - For Action, choose **Forward**.
 - For Protocol, choose **TCP**.
 - For TCP/UDP Destination Port, choose **HTTP(80)**.
 - Click **Add**.
- Step 3** Next add a filter that drops all inbound traffic except from HTTP but forwards any outbound traffic while connected through a tunnel. To do this, under Traffic Management, click **Filters**.
- Click the **Add Filter** box.
 - Enter the filter name, such as **FW-Allow Incoming HTTP**, and select the defaults for the remaining parameters.
 - Click **Add**, which brings up the Actions screen.
 - On this screen, highlight the rule you made in Step 2 and click **Add** to move it to the Current Rules in Filter column. Do the same for the Any Out (forward/out) rule.
 - Click **Done**.
- Step 4** Save the configuration.
- This filter now is available under Base Group and Groups for you to select for the CPP policy.
-

Configuring the VPN 3000 Concentrator to Enforce Firewall Usage on the VPN Client

This section shows how to configure the VPN Concentrator to require the VPN Client to enforce the use of a personal firewall on the VPN Client PC. On the VPN 3000 Concentrator side, you configure the Base Group or a specific group of users to enforce a personal firewall policy on the VPN Client side. Use the following general procedure.

-
- Step 1** To configure firewalls for the Base Group, choose **Configuration | User Management | Base Group** or to configure firewalls for a specific group, choose **Configuration | User Management | Groups**.
- Step 2** To add a firewall, do one of the following:
- For the Base Group, choose the **Client FW** tab.
 - To create a new group for a firewall configuration, click **Add Group** and then click the **Client FW** tab.
 - To add a firewall to an existing group, highlight the group name, click **Modify Group**, and click the **Client FW** tab.
- Step 3** To require a firewall, under the Firewall Setting attribute, choose **Firewall Required**.
- Step 4** Under the Firewall attribute, choose a firewall from the Firewall pull-down menu. If the firewall you are using is not on the list, you must use **Custom**.

- Step 5** Choose the **Firewall Policy**: Policy defined by the remote firewall (AYT) or Policy pushed (CPP). (See the next section.)

For complete information, refer to *VPN 3000 Series Concentrator Reference Volume I: Configuration*, the section “User Management” or the VPN 3000 Concentrator Network Manager’s online help.

Setting up Cisco Integrated Client Firewall (CIC) for CPP

- Step 1** Under Client FW tab on Firewall Setting, choose **Firewall Required**.
- Step 2** On the Firewall pull-down menu, choose **Cisco Integrated Client Firewall**.
- Step 3** On Firewall Policy, click **Policy Pushed** and select a filter that contains firewall policy rules. You can choose the default firewall filter or one that you have configured for a special purpose (see “Defining a Filter and Rules to Use with Firewalls for CPP”).

Setting up a Client/Server Firewall —Zone Labs Integrity

- Step 1** Configure firewall policy on the Integrity Server (IS), following Zone Labs documentation.
- Step 2** On the VPN Concentrator, go to Configuration | System | Servers | Firewall Server. For the Zone Labs Integrity Server, enter the host name or IP address and the port number.
- Step 3** Under Configuration | User Management | Base Group or Groups | Client FW tab (see “Defining a Filter and Rules to Use with Firewalls for CPP”), configure the following:
- a. Firewall Setting = **Firewall Required**
 - b. Firewall = **Zone Labs Integrity**
 - c. Firewall Policy = **Policy from Server**
- Step 4** Save the configuration.

Custom Vendor Codes

On the VPN 3000 Concentrator, you can configure a custom firewall. Currently there are no supported firewall configurations that you cannot choose from the menu on the VPN Concentrator. This feature is mainly for future use. Nevertheless, the following table lists the vendor codes and products that are currently supported.

Table 1-2 Custom Vendor and Product codes

Vendor	Vendor Code	Products	Product Code
Cisco Systems	1	Cisco Integrated Client (CIC)	1
Zone Labs	2	Zone Alarm	1
		ZoneAlarm Pro	2
		Zone Labs Integrity	3
NetworkICE	3	BlackIce Defender	1

Obtaining Firewall Troubleshooting Information

This section describes two ways to obtain information about firewall negotiations: through the IPSec Log or a notification from the VPN Concentrator.

Examining the IPSec Log

One way to see what is happening during tunnel negotiation between the VPN Client and the VPN Concentrator is to examine messages in the IPSec Log. You can use the Log Viewer application to do this (for information on using Log Viewer, refer to the *VPN Client User Manual*, Chapter 5). During tunnel negotiation, the VPN Client initiates the firewall exchange by sending the VPN Concentrator a list of firewalls installed and running on the PC, if any. The VPN Concentrator then sends messages indicating its firewall requirements to the VPN Client.

Following is an example of this exchange.

```

8      14:33:08.911  09/14/01  Sev=Info/5      IKE/0x6300005D
Client sending a firewall request to concentrator

9      14:33:08.911  09/14/01  Sev=Info/5      IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized Policy Push).
.
.

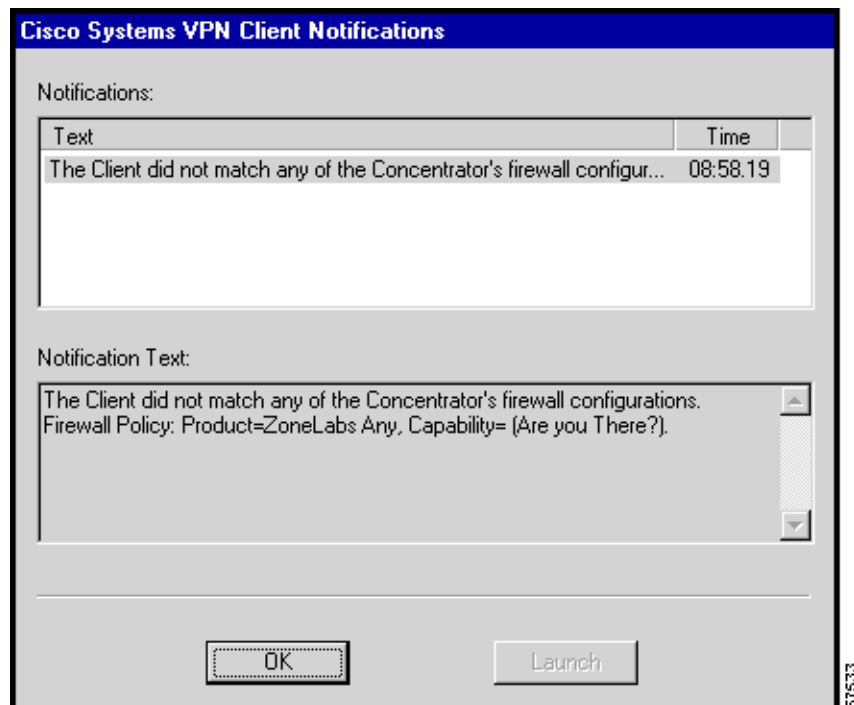
20     14:33:09.873  09/14/01  Sev=Info/5      IKE/0x6300005E
Client received a firewall reply from concentrator

21     14:33:09.873  09/14/01  Sev=Info/5      IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized Policy Push).
```

Notifications

If the VPN Client and VPN Concentrator firewall configurations do not match, the VPN Concentrator notifies the VPN Client when the VPN Client user attempts to connect. If the firewall configuration is required, the connection attempt fails; if the firewall configuration is optional, the tunnel comes up.

Figure 1-4 Firewall Mismatch Notification



Notifying Remote Users of a Client Update

You can notify VPN Client users when it is time to update the VPN Client software on their remote systems. The notification can include a location containing the client update. Use the Client Update procedure at the VPN 3000 Concentrator to configure a client notification:

- Step 1** To enable Client Update, go to Configuration | System | Client Update and click **Enable**.
- Step 2** At the Configuration | System | Client Update | Enable screen, check **Enabled** (the default) and then click **Apply**.
- Step 3** On the Configuration | System | Client Update | screen, click **Entries**.
- Step 4** On the Entries screen, click **Add**.
- Step 5** For Client Type, enter the windows operating systems to notify:
 - Windows includes all Windows based platforms
 - Win9X includes Windows 95, Windows 98, and Windows ME platforms
 - WinNT includes Windows NT 4.0, Windows 2000, and Windows XP platforms

**Note**

The VPN 3000 Concentrator sends a separate notification message for each entry in a Client Update list. Therefore your client update entries must not overlap. For example, the value `Windows` includes all Windows platforms, and the value `WinNT` includes Windows NT 4.0, Windows 2000 and Windows XP platforms. So you would not include both `Windows` and `WinNT`. To find out the client types and version information, click on the lock icon at the top left corner of the Cisco Systems VPN Client main window and choose **About VPN Client**.

Step 6 In the URL field, enter the URL that contains the notification.

To activate the Launch button on the VPN Client Notification, the message must include the protocol HTTP or HTTPS and the server address of the site that contains the update. The message can also include the directory and filename of the update, for example, `http://www.oz.org/upgrades/clientupdate`. If you do not want to activate the Launch button for the remote user, you do not need to include a protocol in the message.

In the Revisions field, enter a comma separated list of client revisions that do not need the update because they are already using the latest software. For example, the value `3.0.2 (Rel) , 3.1 (Rel)` identifies the releases that are compliant; all other VPN Clients need to upgrade.

Step 7 Click **Add**.

The Notification dialog box appears when the remote user first connects to the VPN device or when the user clicks the Notifications button on the Connection Status dialog box. When the notification pops up, on the VPN Client, click **Launch** on the Notification dialog box to open a default browser and access the URL containing the update.

Setting up Local LAN Access for the VPN Client

Remote users with Cable or DSL access from home might have home networks for sharing files and printers. With releases prior to Release 3.1, when remote users connected to a central site from their home PC, they could no longer access printers and files on other PCs in their LAN because all traffic was encrypted and sent through the IPsec tunnel. With Release 3.1 of both the VPN Client and the VPN 3000 Concentrator, you may configure local LAN access for remote users so that they can access resources on the LAN at the client side and still maintain the secure connection to the central site (through the IPsec tunnel).

Before you begin, you should carefully read the section on split tunneling in the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*. See the section explaining Configuration | User Management | Groups | Add or Modify | IPsec tab.

Configuring local LAN access involves the following general steps:

- Enabling local LAN access on the VPN Client
- Enabling split tunneling on the VPN 3000 Concentrator
- Adding the accessible networks to a network list (or using the default network address).

Use the following procedure:

-
- Step 1** On the VPN Client, enable the Allow Local LAN Access parameter.
- Open the **Options** pull-down menu.
 - Choose **Properties**.
 - Check **Allow Local LAN Access**.
- Step 2** On the VPN 3000 Concentrator, either add a new group or modify an existing group as follows:
- To configure local LAN access for a specific group, go to Configuration | User Management | Groups.
 - Choose either **Add** to add a new group or **Modify** to enable split tunneling for an existing group.
 - Go to the IPSec tab.
 - At the Split Tunneling Policy attribute, under Value, click the **Tunnel everything** radio button and then click **Allow the networks in list to bypass the tunnel**. This enables local LAN access on the VPN Client.
 - At the Split Tunneling Network List, under Value, choose the network list you have created for local LAN access, if any.
- VPN Client Local LAN is the default and is assigned the address 0.0.0.0/0.0.0.0. This IP address allows access to all hosts on the client side LAN without regard to the network addressing configured on that network. Since this local LAN access is limited to only one local network, if you have multiple network cards in the client PC, you can access only the network in which the VPN Client has established the VPN connection.

For information on creating a network list, see *VPN 3000 Series Concentrator Reference Volume I: Configuration*, “Configuration | Policy Management | Traffic Management | Network Lists”.



Note

When the VPN Client is connected and configured for local LAN access, you cannot print or browse by name on the local LAN. When the VPN Client is disconnected, you can print or browse by name.

You can browse by IP Address or to print, you can change the properties for the network printer to use the IP Address instead of names. For example instead of the syntax \\sharename\printername, use \\x.x.x.x\printername, where x.x.x.x is an IP address.

To print and browse by name, you can use an LMHOSTS file. To do this, add the IP addresses and local hostnames to a text file named LMHOSTS and place it on all your local PCs in the \Windows directory. The PC's TCP/IP stack then uses the IP address to hostname mapping in the LMHOSTS file to resolve the name when printing or browsing. This approach requires that all local hosts have a static IP address; or if you are using DHCP, you must configure local hosts to always get the same IP address.

Example LMHOSTS file:

```
192.168.1.100 MKPC
192.168.1.101 SBPC
192.168.1.101 LHPC
```

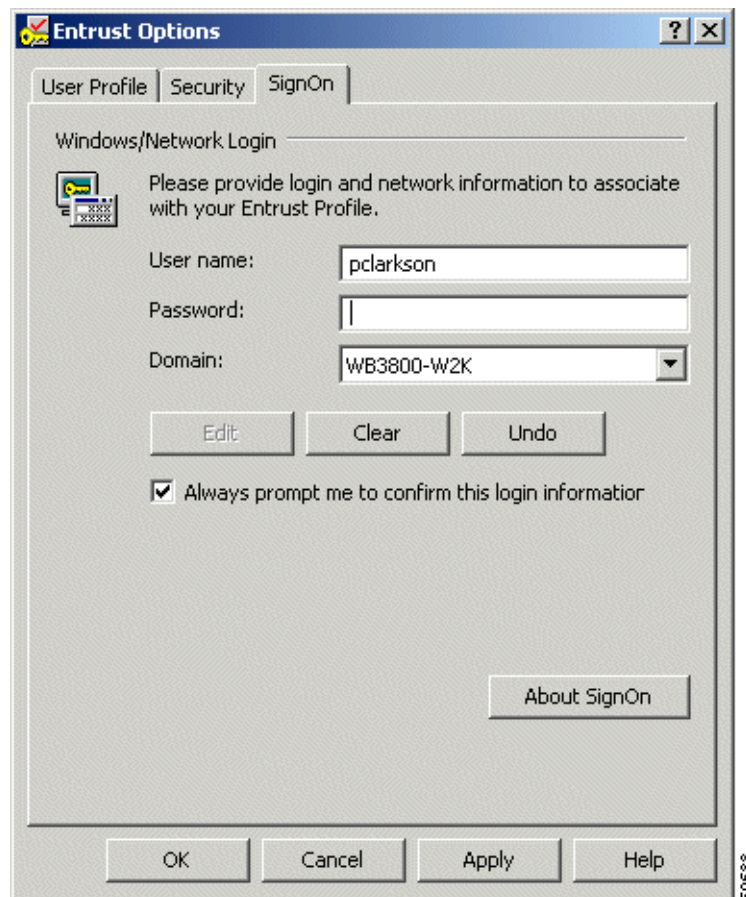
Configuring Entrust Entelligence for the VPN Client

This section explains how to set up a VPN Client to access Entrust Entelligence to obtain an Entrust identity certificate. It also provides information for using the VPN Client software with Entrust. For Entrust installation and configuration information, see your Entrust documentation—*Entrust Entelligence Quick Start Guide* or Entrust Entelligence online help.

Use the following procedure:

-
- Step 1** Install Entrust Entelligence software on the remote user's PC.
- You should install the Entrust Entelligence software before you install the VPN Client. The order is important when the VPN Client is using Start before Logon and Entrust SignOn at the same time. For information about what happens when both of these features are configured on the VPN Client, refer to *VPN Client User Guide*, Chapter 4.
- Step 2** As part of Entrust Entelligence installation, create a new Entrust profile, using the Create Entrust Profile Wizard.
- To create an Entrust Entelligence profile, you need the following information:
- The Entrust Entelligence reference number
 - The Entrust Entelligence authorization code
 - The name of a directory for storing the profile
 - A name for the profile
 - A password, following the rules set by the Entrust administrator
- Step 3** Optionally install Entrust SignOn, following the instructions in the Entrust documentation.
- a. As part of Entrust SignOn installation, you see the Entrust Options dialog box. (See Figure 1-5.)
 - b. Make sure that you check **Always prompt me to confirm this login information**. Checking this box causes the Entrust SignOn login dialog box to pause and allow the VPN connection come up before the remote user enters the NT logon information.

Figure 1-5 Entrust Options SignOn Tab



- Step 4** After creating a profile, log out of Entrust Entelligence.
- Step 5** Install the VPN Client software.
- Step 6** Create a new connection entry that includes authenticating using an Entrust certificate. For instructions refer to section “Configuring an Entrust Certificate for Authentication,” in Chapter 3 of *VPN Client User Guide*.

**Note**

The VPN Client relies on an up-to-date Entrust DLL file. The name of this file is `kmpapi32.dll`. If you are using version of Entrust Entelligence 5.1, the DLL file is up to date. If you have version 4.0 or 5.0 installed on the VPN Client system, then the DLL file is not up to date.

If “Entelligence Certificate (Entrust)” does not appear in the Certificate menu in the New Connection Entry Wizard, you probably do not have the latest version of the DLL file, which ships with the VPN Client software. To update the `kmpapi32.dll` file, copy it to the VPN Client system from the Release medium you are using and place it in the Windows system directory. For Windows NT and Windows 2000 systems, this directory is `\WinNT\System`. For a new installation of Windows 2000, the directory is `\Windows\System`. For Windows 9x and Windows ME, the directory is `\Windows\System32`.

Setting up the VPN Client for Authentication using Smart Cards

The VPN Client supports authentication via a certificate stored on a smart card. Once you create a connection entry and choose the certificate for authentication, the VPN Client user needs to insert the smart card into its reader (in general) and enter a PIN or passcode to authenticate a connection request. The private key stays on the smart card and is never accessible without entering the PIN or passcode. Also, in most cases, there is a limit to how many times someone can try to enter the PIN or passcode after which there is a lock on the card.

Explaining how to configure VPN Client authentication for every smart card vendor is beyond the scope of this documentation. You must follow documentation from your smart card vendor to obtain this information.

**Note**

With most vendors, when the smart card is not plugged in, the Certificate Manager still displays the certificate in the Personal Certificates list. However when disconnected, e-token by Aladdin removes the certificate from the list. The certificate appears in the list only when the e-token is inserted and active.



Preconfiguring the VPN Client for Remote Users

This chapter explains how to prepare configurations for remote users and how to distribute them. This chapter includes the following sections:

- Profiles
- Creating a Global Profile
- Creating Connection Profiles

Profiles

A series of configuration parameters determine the connection entries that remote users choose to connect to a VPN device. Together these parameters form files called profiles. There are two profiles: an individual profile and a global profile. Individual profiles contain the parameter settings for each connection entry and are unique to that connection entry. A global profile sets certain standards for all profiles. The name of the global profile file is `vpnclient.ini`.

Profiles get created in two ways: when a remote user creates connection entries using the Dialer application (connection wizard) and when the administrator creates profiles using a text editor and places them in the remote user's local file system to be used with the Dialer application. In the first case, the remote user is also creating a file that can be edited through a text editor. The individual profiles have a `.pcf` extension.

The default location for individual profiles is `C:\Program Files\Cisco Systems\VPN Client\Profiles`.

This chapter explains how to create and edit both types of profiles. Both files use the same conventions.



Note

The easiest way to create a profile is to run the VPN Client and use the VPN Dialer application to configure the parameters. When you have created a profile in this way, you can copy the `.pcf` file to a distribution disk for your remote users. This approach eliminates errors you might introduce by typing the parameters and the group password gets automatically converted to an encrypted format.

File Format for All Profile Files

The vpnclient.ini and .pcf files follow normal Windows.ini file format:

- Use a semicolon (;) to begin a comment.
- Place section names within brackets [section name]; they are not case sensitive.
- Use key names to set values for parameters; *keyword = value*. Keywords without values, or unspecified keywords, use VPN Client defaults. Keywords can be in any order and are not case sensitive, although using lower and uppercase makes them more readable.

Making a Parameter Read Only

To make a parameter read-only so that the client user cannot change it within the VPN Client applications, precede the parameter name with an exclamation mark (!). This controls what the user can do within the VPN Client applications only. You cannot prevent someone from editing the global or .pcf file and removing the read-only designator.

Creating a Global Profile

The name of the global profile is vpnclient.ini. You can locate it in the C:\Program Files\Cisco Systems\VPN Client directory (default location created during installation). If you open it with a text editor, you might see the following.

Sample vpnclient.ini file

```
[main]
RunAtLogon=0
EnableLog=1
DialerDisconnect=1
[LOG.IKE]
LogLevel=1
[LOG.CM]
LogLevel=1
[LOG.PPP]
LogLevel=2
[LOG.DIALER]
LogLevel=2
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=0
[LOG.IPSEC]
LogLevel=3
[CertEnrollment]
SubjectName=Alice Wonderland
Company=University of OZ
Department=International Relations
State=Massachusetts
Country=US
Email=AliceW@UOZ.com
CADomainName=CertsAreUs
```

```
CAHostAddress=10.10.10.10
CACertificate=CAU
[Application Launcher]
Enable=1
Command=c:\apps\apname.exe
```

The rest of this section explains the parameters that can appear in the `vpnclient.ini` file, what they mean, and how to use them.

Global Profile Configuration Parameters

Table 2-1 lists all parameters, keywords, and values. It also includes the parameter name as used in the VPN Client GUI application (such as Dialer and Log Viewer) and where to configure it in the application.

Table 2-1 *vpnclient.ini file parameters*

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
[main]	Required keyword to identify main section.	[main] Enter exactly as shown, as first entry in the file.	N/A
RunAtLogon	Specifies whether to start the VPN Client connection before users log on to their Microsoft network. Available only for the Windows NT platform (Windows NT 4.0, Windows 2000 and Windows XP). This feature is sometimes known as the NT Logon feature.	0 = Disable 1 = Enable Default = 0	Dialer > Options > Windows Logon Properties > Enable start before logon
EntrustIni=	Locates the <code>entrust.ini</code> file if it is in a location that is different from the default <code>.ini</code> file. The default location is the base Windows system directory.	complete pathname of location	N/A
DialerDisconnect=	Determines whether to automatically disconnect upon logging off a Windows NT platform (Windows NT 4.0, Windows 2000 and Windows XP). Disabling this parameter lets the VPN connection remain when the user logs off, allowing that user to log back in without having to establish another connection.	0 = Disable 1 = Enable Default = 1 (disconnect on logoff)	Dialer > Options > Windows Logon Properties > Disconnect VPN connection when logging off

Note There are limitations to `DialerDisconnect`. For example, in the case of MS DUN, the RAS (PPP) connection might go down when the user logs off. For more information about this specific case, see the following URL:
http://support.microsoft.com/support/kb/articles/Q158/9/09.asp?LN=EN-US&SD=gn&FR=0&qry=RAS%20AND%20LOGOFF&rnk=2&src=DHCS_MSPSS_gn_SRCH&SPR=NTW40

Table 2-1 *vpnclient.ini file parameters (continued)*

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
EnableLog=	Determines whether to override log settings for the classes that use the logging services. By default, logging is turned on. This parameter lets a user disable logging without having to set the log levels to zero for each of the classes. By disabling logging you can improve the performance of the client system.	0 = Disable 1 = Enable Default = 1	Log Viewer > Options > Capture
StatefulFirewall=	Determines whether the stateful firewall is always on. When enabled, the stateful firewall always on feature allows no inbound sessions from all networks, whether a VPN connection is in effect or not. Also, the firewall is active for both tunneled and nontunneled traffic.	0 = Disable 1 = Enable Default = 0	Dialer > Options > Stateful Firewall (Always On)

Note For each class that follows, use the LogLevel= parameter to set the logging level

[LOG.IKE]	Identifies the IKE class for setting the logging level.	[LOG.IKE] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.CM]	Identifies the CM class for setting the logging level.	[LOG.CM] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.PPP]	Identifies the PPP class for setting the logging level.	[LOG.PPP] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.DIALER]	Identifies the DIALER class for setting the logging level.	[LOG.DIALER] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.CVPND]	Identifies the CVPND class for setting the logging level.	[LOG.CVPND] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.CERT]	Identifies the CERT class for setting the logging level.	[LOG.CERT] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.IPSEC]	Identifies the IPSEC class for setting the logging level.	[LOG.IPSEC] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.FWAPI]	Identifies the FWAPI class for setting the logging level.	[LOG.FWAPI] Enter exactly as shown	Log Viewer > Options > Filter
[LOG.FIREWALL]	Identifies the FIREWALL class for setting the logging level.	[LOG.FIREWALL] Enter exactly as shown	Log Viewer > Options > Filter

Table 2-1 *vpnclient.ini file parameters (continued)*

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
LogLevel=	Determines the log level for individual classes that use logging services. By default, the log level for all classes is <code>Low</code> . You can use this parameter to override the default setting for the preceding [LOG] parameters.	0 = Disable 1 = Low - only critical and warning events 2 = Medium - critical, warning, and informational events 3 = High - all events Default = 1	Log Viewer > Options > Filter
[CertEnrollment]	Required keyword to identify the Certificate Enrollment section.	[CertEnrollment] Enter exactly as shown.	N/A
SubjectName=	Identifies the username associated with this certificate.	Maximum of 519 alphanumeric characters.	Certificate Manager > Enrollment form
Company=	Identifies the company or organization of the certificate owner.	Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
Department=	Identifies the department or organizational unit of the certificate owner. When used with a VPN 3000 Concentrator, must match the group name in the configuration.	Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
State=	Identifies the state or province of the certificate owner	Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
Country=	Identifies the two-letter code identifying the country of this certificate owner.	Maximum of 2 alphanumeric characters.	Certificate Manager > Enrollment form
Email=	Identifies the certificate owner's email address.	Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
IPAddress	Identifies the IP address of the system of the certificate owner.	Internet address in dotted decimal notation.	Certificate Manager > Enrollment form
Domain	Identifies the fully qualified domain name of the host that is serving the certificate owner.	Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
CADomainName=	Identifies the domain name that the certificate authority belongs to; for network enrollment.	Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
CAHostAddress=	Identifies the IP address or hostname of the certificate authority.	Internet hostname or IP address in dotted decimal notation. Maximum of 129 alphanumeric characters.	Certificate Manager > Enrollment form
CACertificate=	Identifies the name of the self-signed certificate issued by the certificate authority.	Maximum of 519 alphanumeric characters. Note: The VPNClient GUI ignores a read-only setting on this parameter.	Certificate Manager > Enrollment form

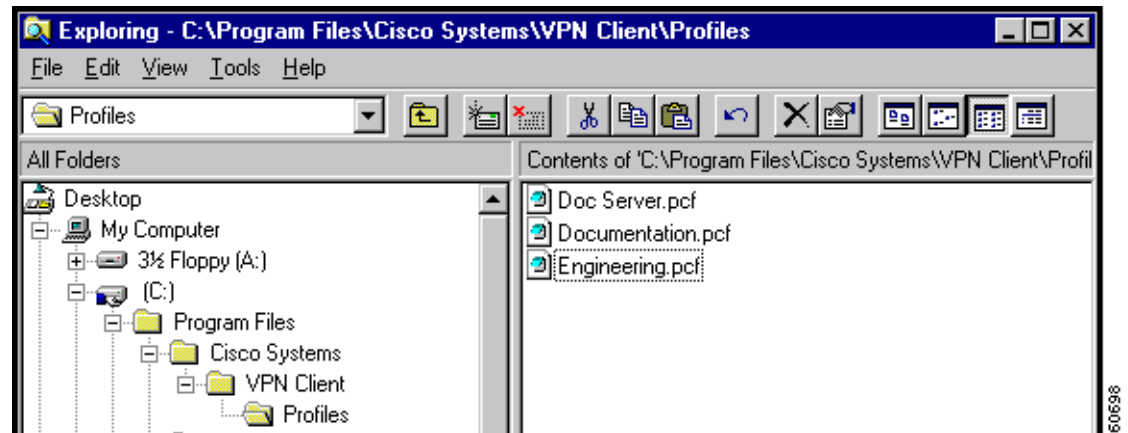
Table 2-1 *vpnclient.ini file parameters (continued)*

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
NetworkProxy=	Identifies a proxy server you can use to route HTTP traffic. Using a network proxy can help prevent intrusions into your private network.	IP address in dotted decimal notation or domain name. Maximum of 519 alphanumeric characters. The proxy setting sometimes has a port associated with it. Example: 10.10.10.10:8080	N/A
[ApplicationLauncher]	(No VPN Client field) Required keyword to identify Application Launcher section.	[ApplicationLauncher] Enter exactly as shown, as first entry in the section.	N/A
Enable=	Use this parameter to allow VPN Client users to launch an application when connecting to the private network.	0 = Disabled (default) 1 = Enabled Disabled means no launching.	Options> Application Launcher
Command=	The name of the application to be launched. This variable includes the pathname to the command, and the name of the command complete with arguments, for example, <code>c:\auth\swtoken.exe</code> .	<i>command string</i> Maximum 512 alphanumeric characters.	Options> Application Launcher> Application

Creating Connection Profiles

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) in the Program Files\Cisco Systems\VPN Client\Profiles directory (if the software installed in the default location) in the VPN Client user's local file system. These parameters include the remote server address, IPsec group name and password, use of a log file, use of backup servers, and automatic Internet connection via Dial-Up Networking. Each connection entry has its own .pcf file. For example, if you have three connection entries, named Doc Server, Documentation, and Engineering, the Profiles directory shows the list of .pcf files shown in Figure 2-1.

Figure 2-1 List of .pcf files



Sample .pcf file

When you open the Doc Server.pcf file, it looks like the example below. This is a connection entry that uses preshared keys. Note that the `enc_` prefix (for example, `enc_GroupPwd`) indicates that the value for that parameter is encrypted.

```
[main]
Description=connection to TechPubs server
Host=10.10.99.30
AuthType=1
GroupName=docusers
GroupPwd=
enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C851ECF2DCC8BD488857EFA
FDE1397A95E01910CABECCE4E040B7A77BF
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=alice
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=1
BackupServer=Engineering1, Engineering2, Engineering 3, Engineering4
EnableMSLogon=1
MSLogonType=0
EnableNat=1
EnableLocalLAN=0
TunnelingMode=0
TCPTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName
SendCertChain=0
DHGroup=2
ForceKeepAlives=0
PeerTimeOut=90
```

You can configure the VPN Client for remote users by creating a profile configuration file for each connection entry and distribute the .pcf files with the VPN Client software. These configuration files can include all, or only some, of the parameter settings. Users must configure those settings not already configured.

You can also distribute the VPN Client to users without a configuration file and let them configure it on their own. In this case, when they complete their configuration using the VPN Client program, they are in effect creating a .pcf file for each connection entry, which they can edit and share.

To protect system security you should *not* include key security parameters such as the IPSec group password, authentication username, or authentication password in .pcf files for remote users.

**Note**

Whatever preconfiguring you provide, you must supply users with the information they need to configure the VPN Client. See Table 2-1 in the *VPN Client User Guide*, Chapter 2 for information users need.

Creating a .pcf file for a Connection Profile

Each user requires a unique configuration file. Use Notepad or another ASCII text editor to create and edit each file. Save as a text-only file with no formatting.

Connection Profile Configuration Parameters

Table 2-2 lists all parameters, keywords, and values. It also includes the VPN Client parameter name (if it exists) that corresponds to the keyword and where it is configured on the VPN Client.

Table 2-2 .pcf file parameters

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
[main]	(No VPN Client field) Required keyword to identify main section.	[main] As the first entry in the file, enter exactly as shown.	N/A
Description=	Description A line of text that describes this connection entry. Optional.	Any text. Maximum 246 alphanumeric characters.	New > Wizard dialog box 1 Options > Properties > General tab
Host=	Remote server address The hostname or IP address of the Cisco remote access server (a VPN device) to which remote users connect.	Legitimate Internet hostname, or IP address in dotted decimal notation. Maximum 255 alphanumeric characters.	New > Wizard dialog box 2 VPN Client main dialog box
AuthType=	Authentication type	The authentication type of this user: 1 = Pre-shared keys 3 = Digital Certificate using an RSA signature. Default = 1	New > Wizard dialog box 3

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
GroupName=	Group Name The name of the IPsec group that contains this user. Used with pre-shared keys.	The exact name of the IPsec group configured on the VPN device. Maximum 32 alphanumeric characters. Case-sensitive.	New > Wizard dialog box 3 Options > Properties > Authentication tab
GroupPwd=	Group Password The password for the IPsec group that contains this user. Used with pre-shared keys. The first time the VPN Client reads this password, it replaces it with an encrypted one (enc_GroupPwd).	The exact password for the IPsec group configured on the VPN device. Minimum of 4, maximum 32 alphanumeric characters. Case-sensitive clear text.	New > Wizard dialog box 3 Options > Properties > Authentication tab
encGroupPwd=	The password for the IPsec group that contains the user. Used with pre-shared keys. This is the scrambled version of the GroupPwd.	Binary data represented as alphanumeric text.	Does not appear in GUI.
EnableISPConnect=	Connect to the Internet via Dial-Up Networking Specifies whether the VPN Client automatically connects to an ISP before initiating the IPsec connection; determines whether to use PppType parameter.	0 = Disable (default) 1 = Enable Default = 0 The VPN Client GUI ignores a read-only setting on this parameter.	Options > Properties > Connections tab > Connect to the Internet via dial-up
ISPConnectType=	Dial-Up Networking connection entry type Identifies the type to use: ISPConnect or ISPCommand.	0 = ISPConnect 1 = ISPCommand The VPN Client GUI ignores a read-only setting on this parameter.	Options > Properties > Connections tab (choosing either DUN or Third Party (command))
ISPConnect=	Dial-Up Networking Phonebook Entry (Microsoft) Use this parameter to dial into the Microsoft network; dials the specified dial-up networking phone book entry for the user's connection. Applies only if EnableISPConnect=1 and ISPConnectType=0.	<i>phonebook_name</i> This variable is the name of the phone book entry for DUN – maximum of 256 alphanumeric characters. The VPN Client GUI ignores a read-only setting on this parameter.	Options > Properties > Connections tab > <Microsoft Dial-Up Networking
ISPCommand=	Dial-Up Networking Phonebook Entry (command) Use this parameter to specify a command to dial the user's ISP dialer. Applies only if EnableISPConnect=1 and ISPConnectType=1.	<i>command string</i> This variable includes the pathname to the command and the name of the command complete with arguments; for example: c:\isp\ispdialer.exe dialEngineering Maximum 512 alphanumeric characters.	Options > Properties > Connections tab > Third party dialup program

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
Username=	User Authentication: Username The name that authenticates a user as a valid member of the IPSec group specified in GroupName.	The exact username. Case-sensitive, clear text, maximum of 32 characters. The VPN Client prompts the user for this value during user authentication.	Connect > User Authentication dialog box
UserPassword=	User Authentication: Password The password used during extended authentication. The first time the VPN Client reads this password, it saves it in the file as the enc_UserPassword and deletes the clear-text version. If SaveUserPassword is disabled, then the VPN Client deletes the UserPassword and does not create an encrypted version. You should only modify this parameter manually if there is no GUI interface to manage profiles.	Maximum of 32 alphanumeric characters, case sensitive.	Connect > User Authentication dialog box
encUserPassword	Scrambled version of the user's password.	Binary data represented as alphanumeric text.	Does not appear in GUI.
SaveUserPassword	Determines whether or not the user password or its encrypted version are valid in the profile. This value is set in the VPN device, not the VPN Client.	0 = do not allow user to save password information locally. 1 = allow user to save password locally. Default = 0.	Does not appear in GUI.
NTDomain=	User Authentication: Domain The NT Domain name configured for the user's IPSec group. Applies only to user authentication via a Windows NT Domain server.	NT Domain name. Maximum 14 alphanumeric characters. Underbars are not allowed.	Connect > User Authentication dialog box
EnableBackup=	Enable backup server(s) Specifies whether to use backup servers if the primary server is not available.	0 = Disable 1 = Enable Default = 0	Options > Properties > Connections tab
BackupServer=	(Backup server list) List of hostnames or IP addresses of backup servers. Applies only if EnableBackup=1.	Legitimate Internet hostnames, or IP addresses in dotted decimal notation. Separate multiple entries by commas. Maximum of 255 characters in length.	Options > Properties > Connections tab
EnableMSLogon=	Logon to Microsoft Network Specifies that users log on to a Microsoft network. Applies only to systems running Windows operating systems.	0 = Disable 1 = Enable Default = 1	Options > Properties > General tab

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
MSLogonType=	Use default system logon credentials Prompt for network logon credentials Specifies whether the Microsoft network accepts the user's Windows username and password for logon, or whether the Microsoft network prompts for a username and password. Applies only if EnableMSLogon=1.	0 = Use default system logon credentials (default); i.e., use the Windows logon username and password. 1 = Prompt for network logon username and password.	Options > Properties > General tab
EnableNat=	Enable Transparent Tunneling Allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing NAT or PAT.	0 = Disable 1 = Enable Default = 1	Options > Properties > General tab
TunnelingMode=	Specifies the mode of transparent tunneling, over UDP or over TCP; must match that used by the secure gateway with which you are connecting.	0 = UDP 1 = TCP Default = 0	Options > Properties > General tab
TCP TunnelingPort=	Specifies the TCP port number, which must match the port number configured on the secure gateway.	Port number from 1 through 65545 Default = 10000	Options > Properties > General tab
EnableLocalLAN=	Allow Local LAN Access Specifies whether to enable access to resources on a local LAN at the Client site while connected through a secure gateway to a VPN device at a central site.	0 = Disable 1 = Enable Default = 0	Options> Properties > General tab
ForceKeepAlives=	Enable IKE and ESP keepalives Allows the VPN Client to keep sending IKE and ESP keepalives for a connection at approximately 20 second intervals so the port on an ESP-aware NAT/Firewall doesn't close.	0 = Disable 1 = Enable Default = 0	N/A (hidden)
PeerTimeout=	Peer response timeout The number of seconds to wait before terminating a connection because the VPN device on the other end of the tunnel is not responding.	Number of seconds Minimum = 30 seconds Maximum = 480 seconds Default = 90 seconds	Options> Properties> General tab
CertStore=	Certificate Store Identifies the type of store containing the configured certificate.	1 = Cisco 2 = Microsoft Default = 0 The VPN Client GUI ignores a read-only setting on this parameter.	N/A

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
CertName=	Certificate Name Identifies the certificate used to connect to a VPN device.	Maximum 129 alphanumeric characters The VPN Client GUI ignores a read-only setting on this parameter.	New > Wizard dialog box 3
CertPath=	The complete pathname of the directory containing the certificate file.	Maximum 259 alphanumeric characters The VPN Client GUI ignores a read-only setting on this parameter.	N/A
CertSubjectName	The fully qualified distinguished name (DN) of certificate's owner. If present, the VPN Dialer enters the value for this parameter.	Either do not include this parameter or leave it blank. The VPN Client GUI ignores a read-only setting on this parameter.	N/A
CertSerialHash	A hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. If present, the VPN Dialer enters the value for this parameter.	Either do not include this parameter or leave it blank. The VPN Client GUI ignores a read-only setting on this parameter.	N/A
SendCertChain	Sends the chain of CA certificates between the root certificate and the identity certificate plus the identity certificate to the peer for validation of the identity certificate.	1 = enabled 0 = disabled Default = 0	New > Wizard dialog box 3
DHGroup=	Allows a network administrator to override the default group value on a VPN device used to generate Diffie-Hellman key pairs.	1 = modp group 1 2 = modp group 2 5 = modp group 5 Default = 2 Note: This value is preset only for pre-shared keys; for a certificate-authenticated connection, the DHGroup number is negotiated.	N/A

Distributing Preconfigured VPN Client Software to Users

When you have created the VPN Client profile configuration file, you can distribute it to users separately or as part of the VPN Client software.

Separate Distribution

To distribute the configuration file separately and have users import it to the VPN Client after they have installed it on their PCs, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Distribute the appropriate profile files to users on whatever media you prefer. |
| Step 2 | Supply users with necessary configuration information for Table 2-1 in Chapter 2 of the <i>VPN Client User Guide</i> . |
| Step 3 | Instruct users to: <ul style="list-style-type: none">a. Install the VPN Client according to the instructions in Chapter 2 of the <i>VPN Client User Guide</i>.b. Start the VPN Client and follow the instructions in Chapter 5 of the <i>VPN Client User Guide</i>. See the section “Importing a VPN Client Configuration File.”c. Finish configuring the VPN Client according to the instructions in Chapter 3 of the <i>VPN Client User Guide</i>.d. Connect to the private network, and enter parameters according to the instructions in Chapter 4 of the <i>VPN Client User Guide</i>. |
-

Distribution with the VPN Client Software

If the `vpnclient.ini` file is bundled with the VPN Client software when it is first installed, it automatically configures the VPN Client during installation. You can also distribute the profile files (one `.pcf` file for each connection entry) as preconfigured connection profiles for automatic configuration.

To distribute preconfigured copies of the VPN Client software to users for installation, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | <p>Copy the VPN Client software files from the distribution CD-ROM into each directory where you created an <code>vpnclient.ini</code> (global) file and separate connection profiles for a set of users.</p> <p>Cisco Systems provides two images of the VPN Client software files on the distribution CD-ROM:</p> <ul style="list-style-type: none">• <i>CD-ROM image</i>: Directory <code>\VPN Client\CD-ROM</code>. Use these files if users are installing the VPN Client through a direct network connection.• <i>Diskette image</i>: Directories <code>\VPN Client\Floppy\Disk1</code>, <code>..\Disk2</code>, and <code>..\Disk3</code>. Use these files if users are installing the VPN Client from diskettes. Copy the complete subdirectories to your system. |
| Step 2 | <p>Prepare and distribute the bundled software.</p> <p><i>CD-ROM or network distribution</i>: Be sure the <code>vpnclient.ini</code> file and profile files are in the same directory with all the CD-ROM image files. You can have users install from this directory through a network connection; or you can copy all files to a new CD-ROM for distribution; or you can create a self-extracting ZIP file that contains all the files from this directory, and have users download it, and then install the software.</p> |

Diskette distribution:

- a. Move the vpnclient.ini and profile files to the ..\Disk1 subdirectory.
- b. Copy the files from the subdirectories onto three separate diskettes labelled Disk1, Disk2, and Disk3 for distribution to users.

Step 3 Supply users with any other necessary configuration information and instructions. See Chapter 2 of the *VPN Client User Guide*.



Using the VPN Client Command-Line Interface

This chapter explains how to use the VPN Client command-line interface (CLI) to connect to a Cisco VPN device, generate statistical reports, and disconnect from the device. You can create your own script files that use the CLI commands to perform routine tasks, such as connect to a corporate server, run reports, and then disconnect from the server.

CLI Commands

This section lists each command, its syntax, and gives an example. It is organized by task.

Displaying a List of VPN Client Commands

To get a list of all VPN Client commands, go to the directory that contains the VPN Client software, and enter the `vpnclient` command at the command-line prompt:

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient
Cisco Systems VPN Client Version 3.5
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows
Running on WinNT

Usage:
vpnclient connection profilename [nocertpwd] [notrayicon] [eraseuserpwd]
vpnclient disconnect
vpnclient stat [reset] [traffic] [tunnel] [route] [firewall] [repeat]
vpnclient notify
```

Starting a Connection—`vpnclient connect`

To start a connection, enter the following command:

```
vpnclient connect profilename [nocertpwd] [notrayicon] [eraseuserpwd]
where
```

profilename is the name of the connection entry you have previously configured (`.pcf` file). This parameter is required. Enter the profile name without the `.pcf` extension. If the filename contains spaces, enclose it in double quotes on the command line.

`notrayicon` is an optional parameter that suppresses the displaying of the dialer icon in the Windows system tray (lower right corner of your screen). This parameter lets you suppress prompting when the connection is disconnected using the `vpnclient disconnect` command (see “Note on Notrayicon Parameter”).

`eraseuserpwd` is an optional parameter that erases the user password saved on the Client PC thereby forcing the VPN Client to prompt for a password. You might have configured a connection with Saved Password to suppress a password prompt when connecting using a batch file. You can then use the `Eraseuserpwd` to return to the more secure state of requiring password input from the console when connecting.

`nocertpwd` is an optional parameter that suppresses prompting for a certificate password.

Note on Notrayicon Parameter

When you connect using the `vpnclient connect` command, the connection icon (lock) displays in the system tray in the lower right corner of your screen. In this case, when you then use the `vpnclient disconnect` command to disconnect from the VPN device, the VPN Client displays the message:

```
Your IPsec connection has been terminated [OK].
```

You must then click OK to continue.

However, if you include the `notrayicon` argument in your command-line string, no icon appears in the system tray. When you disconnect, the above message does not occur. Also the “Disconnect VPN connection when logging off” feature is not in effect (see Note).



Note

When you use the `notrayicon` option either directly on the command line or in a batch file, make sure that you issue a `vpnclient disconnect` command before logging off or your VPN connection remains active.

Example of vpnclient connect command

This section shows an example of the `vpnclient connect` command that connects you to the Documentation Server using the profile name “Docserver.”

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient connect Docserver
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on WinNT
```

```
Initializing the IPsec link.
Contacting the security gateway at 10.10.10.1
Authenticating user.
```

At this point, the VPN Client displays an authentication dialog box that prompts for your username and password:

Figure 3-1 *Authenticating a User*

After you enter your name and password, authentication succeeds, and the command continues executing.

```
Contacting the security gateway at 10.10.10.1
Negotiating security policies.
Securing communication channel.
Your link is secure.
```

Displaying a Notification—`vpnclient notify`

When you connect using the `notrayicon` option, you can display a notification using the `vpnclient notify` command:

```
vpnclient notify
```

For example, the following session shows how to use the `vpnclient notify` command to display a notification from a network administrator.

```
C:\Program Files\Cisco Systems\VPN Client\vpnclient connect notrayicon Docserver
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT
```

```
Initializing the IPsec link.
Contacting the security gateway at 10.10.10.1
Authenticating user.
Contacting the security gateway at 10.10.10.1
Negotiating security policies.
Securing communication channel.
Your link is secure.
```

```
C:\Program Files\Cisco Systems\Vpn Client\vpnclient notify
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT
```

```
Notification:
Your network administrator has placed an update of the Cisco Systems VPN Client at the
following location:
http://www.mycompany.com/clientupdate
```

Ending a Connection—`vpnclient disconnect`

To disconnect from your session, enter the following command:

```
vpnclient disconnect
```

For example, the following command disconnects you from your secure connection.

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient disconnect
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT
```

```
Disconnecting the IPSEC link.
Your IPSec link has been disconnected.
```

Displaying Information About Your Connection—`vpnclient stat`

To generate status information about your connection, enter the following command:

```
vpnclient stat [reset] [traffic] [tunnel] [route] [firewall] [repeat]
```

When entered without any of the optional parameters, the `vpnclient stat` command displays all status information. The following parameters are optional:

<code>reset</code>	Restarts all connection counts from zero. SA stats are not reset.
<code>traffic</code>	Displays a summary of bytes in and out, packets encrypted and decrypted, packets bypassed, and packets discarded.
<code>tunnel</code>	Displays IPSec tunneling information.
<code>route</code>	Displays configured routes.
<code>Firewall</code>	Identifies the type of firewall in use and displays information generated by the firewall configuration.
<code>repeat</code>	Provides a continuous display, refreshing it every few seconds. To end the display, press <ctrl-C>.

The following examples show sample output from the `vpnclient stat` command.

Following is a example of the information that the `vpnclient stat` command displays.

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient stat
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT
```

```
IPSec tunnel information.
Client address: 209.154.64.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
Local LAN Access is enabled.
Personal Firewall: Cisco Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)
```

VPN traffic summary.

Time connected: 0 day<s>, 00:18.32

Bytes out: 3420

Bytes in: 3538

Packets encrypted: 23

Packets decrypted: 57

Packets bypassed: 102

Packets discarded: 988

Configured routes

Secured	Network	Destination	Netmask	Bytes
*	10.10.32.32		255.255.255.255	0
*	0.0.0.0		0.0.0.0	1899

Local	Network	Destination	Netmask
	209.154.64.0		255.255.255.255
	209.154.65.0		255.255.255.255
	209.154.66.0		255.255.255.255
	209.154.67.0		255.255.255.255
	209.154.68.0		255.255.255.255
	209.154.69.0		255.255.255.255

Firewall Rules.

Act	Dir	Src Address	Dst Address	Pro	Src Port	Dst Port
Fwd	In	Any	Local	Any	N/A	N/A
Fwd	Out	Local	Any	Any	N/A	N/A
Drp	In	Any	Local	Any	N/A	N/A
Fwd	Out	Local	Any	Any	N/A	N/A
Drp	In	Any	Local	Any	N/A	N/A
Drp	Out	Local	Any	Any	N/A	N/A

The `vpnclient stat reset` command resets all connection counters.

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient stat reset
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT
```

Tunnel statistics have been reset.

Here is a sample of the information that the `vpnclient stat traffic` command generates.

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient stat traffic
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT
```

VPN traffic summary

Time connected: 0 day<s>, 00:10:39

Bytes in: 0

Bytes out: 2974

Packets encrypted: 21

Packets decrypted: 0

Packets bypassed: 138

Packets discarded: 118

To display only tunneling information, use the `vpnclient stat tunnel` command. Here is a sample.

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient stat tunnel
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
```

```

Client Type<s>: Windows
Running on: WinNT

IPSec tunnel information.
Client address: 220.111.22.30
Server address: 10.10.10.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
Local LAN Access is enabled.
Personal Firewall: Cisco Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)

```

The `vpnclient stat route` command displays information similar to the following display.

```

C:\Program Files\Cisco Systems\VPN Client>vpnclient stat route
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT

Configured routes
Secured  Network DestinationNetmask          Bytes
*        10.10.32.32          255.255.255.255          0
*        0.0.0.0              0.0.0.0                  1899

Local    Network DestinationNetmask
209.154.64.0      255.255.255.255
209.154.65.0      255.255.255.255
209.154.66.0      255.255.255.255
209.154.67.0      255.255.255.255
209.154.68.0      255.255.255.255
209.154.69.0      255.255.255.255

```

The `vpnclient stat firewall` command displays information similar to the following display.

```

C:\Program Files\Cisco Systems\VPN Client>vpnclient stat firewall
Cisco Systems VPN Client Version 3.5
Copyright <C> 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on: WinNT

Personal Firewall: Cisco Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)

Firewall Rules
Act  Dir  Src Address  Dst Address  Pro  Src Port  Dst Port
Fwd  In   Any         Local        Any  N/A       N/A
Fwd  Out  Local       Any          Any  N/A       N/A
Drp  In   Any         Local        Any  N/A       N/A
Fwd  Out  Local       Any          Any  N/A       N/A
Drp  In   Any         Local        Any  N/A       N/A
Drp  Out  Local       Any          Any  N/A       N/A

```

Return Codes

This section lists the error levels (return codes) that you can receive when using the VPN Client command-line interface.

Return Code	Message	Meaning
200	SUCCESS_START	The VPN Client connection started successfully.
201	SUCCESS_STOP	The VPN Client connection has ended.
202	SUCCESS_STAT	The VPN Client has generated statistical information successfully.
203	SUCCESS_ENUMPPP	The enumppp command has succeeded. This command lists phone book entries when connecting to the Internet via dial-up.
1	ERR_UNKNOWN	An unidentifiable error has occurred during command-line parsing.
2	ERR_MISSING_COMMAND	Command is missing from command-line input.
3	ERR_BAD_COMMAND	There is an error in the command entered; check spelling.
4	ERR_MISSING_PARAMS	The command-line input is missing required parameter(s).
5	ERR_BAD_PARAMS	The parameter(s) in the command input are incorrect; check spelling.
6	ERR_TOO_MANY_PARAMS	The command-line input contains too many parameters.
7	ERR_NO_PARAMS_NEEDED	The command entered does not require parameters.
8	ERR_ATTACH_FAILED	Interprocess communication error occurred attaching to the generic interface.
9	ERR_DETACH_FAILED	Interprocess communication error occurred detaching from the generic interface.
10	ERR_NO_PROFILE	The VPN Client failed to read the profile.
11	ERR_PWD_MISMATCHED	Reserved
12	ERR_PWD_TOO_LONG	The password contains too many characters. The group password limit is 32 characters; the certificate password limit is 255 characters.
13	ERR_TOO_MANY_TRIES	Attempts to enter a valid password have exceed the amount allowed. The limit is three times.
14	ERR_START_FAILED	The connection attempt has failed; unable to connect.
15	ERR_STOP_FAILED	The disconnect action has failed; unable to disconnect.
16	ERR_STAT_FAILED	The attempt to display connection status has failed.
17	ERR_ENUM_FAILED	Unable to list phonebook entries.
18	ERR_COMMUNICATION_FAILED	A serious interprocess communication error has occurred.
19	ERR_SET_HANDLER_FAILED	Set console control handler failed.
20	ERR_CLEAR_HANDLER_FAILED	Attempt to clean up after a user break failed.
21	ERR_OUT_OF_MEMORY	Out of memory. Memory allocation failed.

Return Code	Message	Meaning
22	ERR_BAD_INTERFACE	Internal display error.
23	ERR_UNEXPECTED_CALLBACK	In communicating with the Connection Manager, an unexpected callback (response) occurred.
24	ERR_DO_NOT_CONTINUE	User quit at a banner requesting “continue?”
25	ERR_GUI_RUNNING	Cannot use the command-line interface when connected through the graphical interface dialer application.
26	ERR_SET_WORK_DIR_FAILED	The attempt to set the working directory has failed. This is the directory where the program files reside.
27	ERR_NOT_CONNECTED	Attempt to display status has failed because there is no connection in effect.
28	ERR_BAD_GROUP_NAME	The group name configured for the connection is too long. The limit is 128 characters.
29	ERR_BAD_GROUP_PWD	The group password configured for the connection is too long. The limit is 32 characters.
30	ERR_BAD_AUTHTYPE	The authentication type configured for the connection is invalid.
31	RESERVED_01	Reserved.
32	RESERVED_02	Reserved.
33	ERR_COMMUNICATION_TIMED_OUT	Interprocess communication timed out.
34	ERR_BAD_3RD_PARTY_DIAL	Failed to launch a third-party dialer.
35	ERR_DAEMON_NOT_RUNNING (CVPND.EXE)–Non-Windows only	Connection needs to be established for command to execute.
36	ERR_DAEMON_ALREADY_RUNNING (CVPND.EXE)–Non-Windows only	Command cannot work because connection is already established.

Application Example

Here is an example of a DOS batch file (.bat) that uses CLI commands to connect to the corporate office from a branch office, run an application, and then disconnect from the corporate site.

```
runxls.bat
rem assume you have generated a report in the middle of the night that needs
rem to be sent to the corporate office.

rem .. generate report.xls . .

rem connect to the home office
vpnclient connect notrayicon myprofile

rem check return code from vpnclient call....
if %errorlevel% neq 200 goto failed
rem if okay continue and copy report

copy report.xls \\mycorpserver\directory\overnight_reports /v

rem now disconnect the VPN connection
vpnclient disconnect
echo Spreadsheet uploaded
goto end
:failed
echo failed to connect with error = %errorlevel%
:end
```

■ Application Example



Rebranding the VPN Client Software

This chapter explains how to replace the Cisco Systems brand with your own organization's brand. When you install and launch the VPN Client software, you see your own organization name, program name, and application names on menus, windows, dialogs, and icons. It also explains how to set up the software so that your users can install it automatically without being prompted. This feature is called *silent install*.

To rebrand the VPN Client software, you create your own distribution image combining the following elements, which this chapter describes:

- Cisco Systems image that you receive on the Cisco Systems software distribution CD.
- An oem.ini file that you create.
- Your own bitmap and icon files to replace the Cisco Systems brand.
- A vpnclient.ini file for configuring the VPN Client software globally (see Chapter 2, "Preconfiguring the VPN Client for Remote Users").
- Individual profile (.pcf) files for each connection entry (see Chapter 2, "Preconfiguring the VPN Client for Remote Users").
- setup.bmp—a bitmap file that displays on the first InstallShield® window when you install the VPN Client.
- wizard.bmp—a bitmap that displays Connection Wizard.

These elements should all be in the same directory and folder. Because some of the files may be too large to distribute the oem software on diskettes, we recommend that you make a CD ROM distribution image.

Rebranding takes place when the VPN Client and installation program see a text file called oem.ini on your distribution image. The oem.ini file is patterned after Microsoft standard initialization files. You create the oem.ini file and supply your own text, bitmap files, and icon files. When present, the oem.ini, bitmap, and icon files are read when you first start the VPN Client. Since the VPN Client software reads these files when it first starts, the changes to them take effect only *after* you restart the VPN Client applications.

This chapter contains the following sections:

- Areas Affected by Branding
- Creating the oem.ini File
- Additional Bitmap—setup.bmp

Areas Affected by Branding

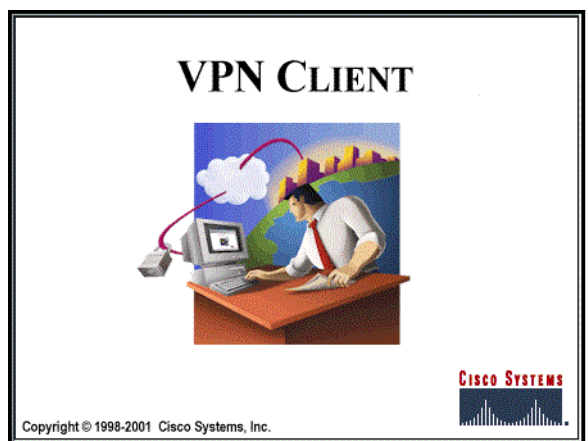
Branding replaces the following screen text, bitmaps, and icons.

- Brand names on windows and dialog boxes
- Product names on windows and dialog boxes
- Organization logo on all wizard windows
- Icons on the user authentication dialog boxes, the system tray (at the bottom right of the screen), desktop (shortcut), status messages, Log View windows, and Certificate Manager windows

Installation Bitmap

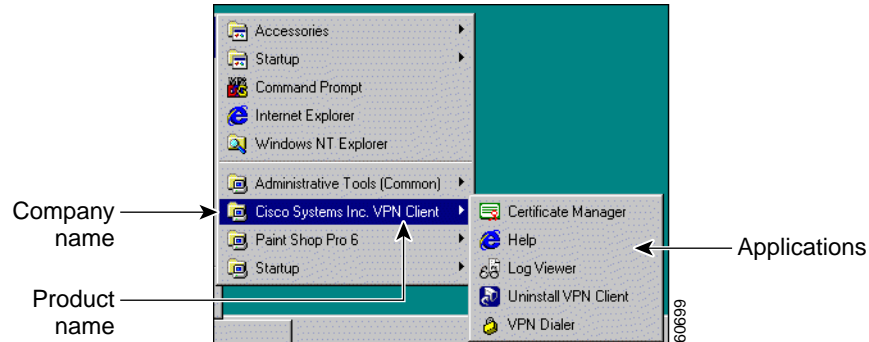
The InstallShield uses a bitmap when installing the VPN Client software: the setup bitmap (setup.bmp). Figure 4-1 shows the setup bitmap that displays as the first screen during installation.

Figure 4-1 Setup Bitmap



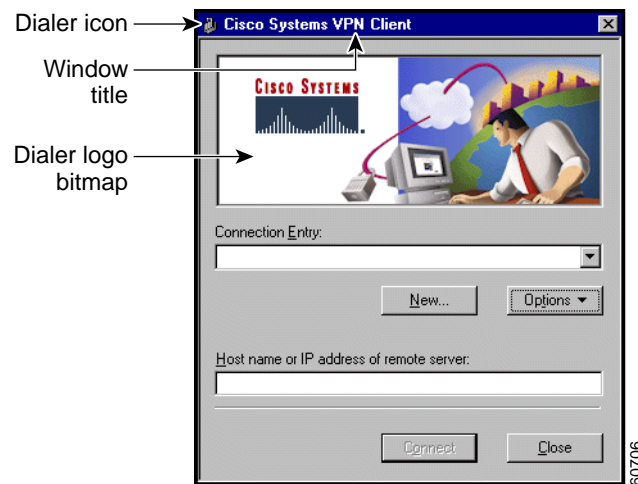
Program Menu Titles and Text

After installation, your organization or company, product, and application names appear in the Cisco Systems VPN Client applications menu. (See Figure 4-2.)

Figure 4-2 Applications menu

VPN Dialer

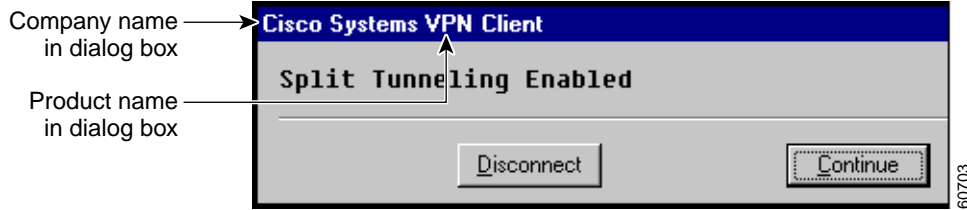
Figure 4-3 shows a dialer icon, window title, and dialer logo bitmap that the oem.ini file replaces in the VPN dialer software.

Figure 4-3 Three Types of Branding Changes

When you click the icon in the title line and select **About Cisco Systems VPN Client**, you see information about the copyright and version number of the VPN Client. The oem.ini file replaces the window title and the icon. Also the window displays (OEM) when you are using the OEM version of the client software.

Window Titles and Text

Figure 4-4 is typical of dialog boxes showing status messages. You can replace “Cisco Systems” with your organization’s name and “VPN Client” with a different name for the client application.

Figure 4-4 Window Titles in a Dialog Box

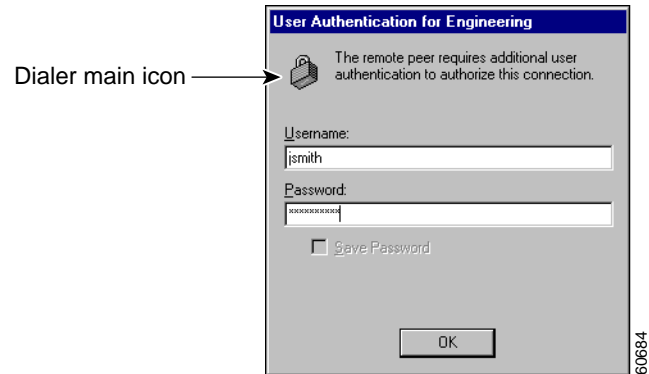
Bitmaps

The VPN Dialer application displays the wizard bitmap on windows while connecting to a VPN device. Figure 4-5 shows the wizard bitmap as used in the connection wizard.

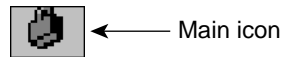
Figure 4-5 Connection Wizard Dialog Box

Icons

The next set of figures show the icons used in the VPN Dialer application. You can use the oem.ini file to replace all icons with icons you design for your organization. The interface uses several icon (.ico) files. The basic size is 32x32 pixels (the User Authentication window in Figure 4-6). The operating system automatically condenses the 32x32 icon to fit the 16x16 size displayed on window titles and the system tray. (See Figure 4-3 and Figure 4-7.)

Figure 4-6 *Dialer Icon on User Authentication Window*

The smaller icon on the system tray appears at the bottom right section of your screen.

Figure 4-7 *Icon on System Tray*

Four icons display while the VPN Dialer is connecting to VPN device. (See Figure 4-8 to Figure 4-11.)

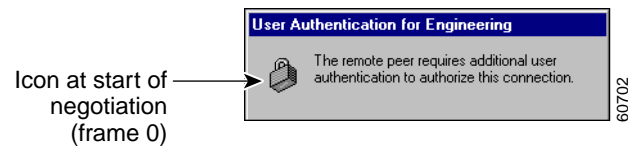
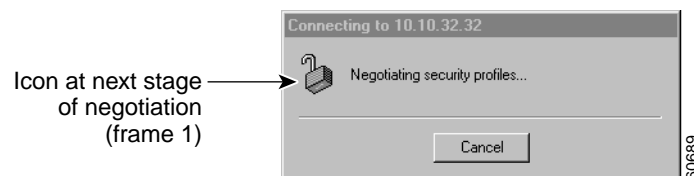
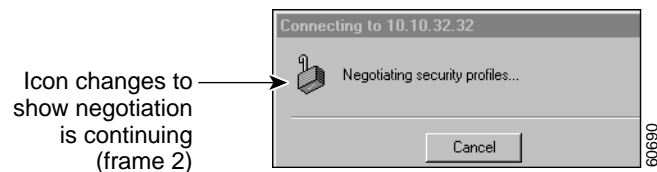
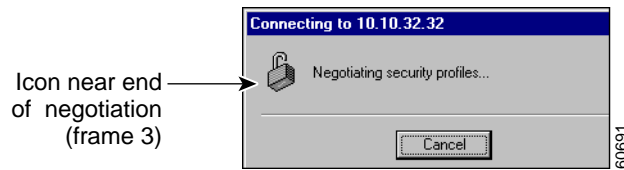
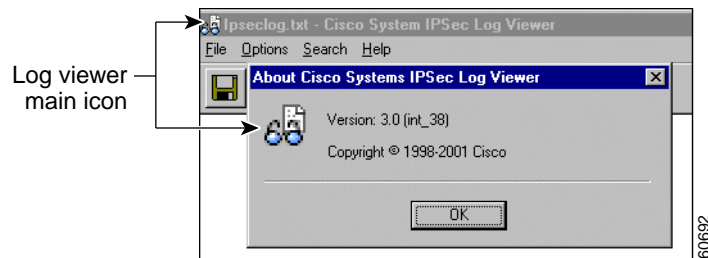
Figure 4-8 *Start of Negotiation***Figure 4-9** *First Change***Figure 4-10** *Second Change*

Figure 4-11 Third Change

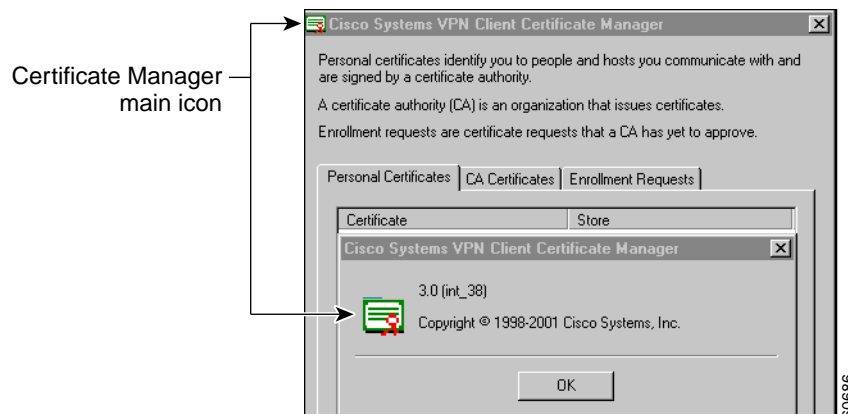
Log Viewer

The Log Viewer section of the oem.ini file replaces the icon used in the Log Viewer application (Figure 4-12). You can also replace the name of the application.

Figure 4-12 Log Viewer Icon

Certificate Manager

The Certificate Manager section of the oem.ini file replaces the icon used in the Certificate Manager application. (See Figure 4-13.) You can also replace the name of the application.

Figure 4-13 Certificate Manager Icon

Creating the oem.ini File

Your distribution CD must contain the oem.ini file to execute the branding changes. The oem.ini file contains the locations and names of bitmaps, icons, window titles, and screen text needed for OEM branding, all of which need to be in the same directory. When you install or start the VPN Client, the software checks to see if there is an oem.ini file. If so, the software scans it for bitmaps, icons, and text. If the oem.ini file lacks an element (for example, text for the product name), then the software uses whatever you have specified in the default section of the file. If no oem.ini file exists, the software defaults to Cisco Systems bitmaps, icons, and text.

Use Notepad or another ASCII text editor to create the oem.ini file and enter brand text and the names of your bitmap and icon files. See Table 4-1.

The format of the oem.ini file is the same as a standard Windows `ini` file:

- Use a semicolon (;) to begin a comment.
- Set values by entering `keyword=value`.
- If you don't specify a value for a keyword, the application uses the default.
- Keywords are not case-sensitive, but using upper and lowercase makes them more readable.

Sample oem.ini File

```
; This is a sample oem.ini file that you can use to overwrite Cisco Systems
; brand name on windows, bitmaps, and icons with your organization's brand
; name.
;
; This file has six sections: [Main],[Brand], [Default], [Dialer],
; [Log viewer], and [Configuration Manager]. Each section has keywords
; designating parts of the interface that the file replaces.
;
; The [Main] section specifies incompatible GINAs.

[Main]
IncompatibleGinas=PALGina.dll

; The [Brand] section controls window titles during installation and in the
; destination folder for the product and applications.
;
[Brand]

CompanyText = Wonderland University
ProductText = Wonderland Client

;
; The default section establishes the default bitmap and icon to use if
; assignments are left blank. WizardBitMap appears in installation and
; connection wizards. This section also sets up silent installation.
; Silent mode installation proceeds without user intervention.
;
[Default]
WizardBitMap = wuwiz.bmp
MainIcon = wudial.ico
SilentMode = 1
InstallPath = C:\Program Files\Wonderland University\Wonderland Client
DefGroup = Wonderland Client
Reboot = 1
;
; The [Dialer] section controls the text and icons for the dialer software.
```

```

; AppNameText appears on the application selection menu. DialerBitMap
; appears on connection windows. AllowSBLLaunches controls whether a remote user can
; launch an application before connecting and logging on to a Windows NT platform
;
[Dialer]

AppNameText = Wonderland Dialer

DialerBitMap = wudial.bmp

MainIcon = wudial.ico

Frame0Icon = wudial.ico

Frame1Icon = wudial1.ico

Frame2Icon = wudial2.ico

Frame3Icon = wudial3.ico

AllowSBLLaunches = 0

;
; The [Log viewer] section controls the text and icons for the Log Viewer
; application. AppNameText appears on the application selection menu and
; the title screen. MainIcon appears on the window title bar and About
; dialog.
;
[Log viewer]
AppNameText = Wonderland LogViewer
MainIcon = log.ico
;
; The [Certificate Manager] section controls the text and icon for the
; Certificate Manager application. AppNameText appears on the application
; selection menu and the title screen. MainIcon appears on the window title
; bar.
;
[Certificate Manager]
AppNameText = Wonderland Certificate Manager
MainIcon = cm.ico

```

oem.ini File Keywords and Values

Table 4-1 describes each part of the oem.ini file.

Table 4-1 oem.ini File Parameters

Keyword	Description	Value
[Main]	Optional field to identify a section of the OEM.ini file to address special circumstances.	Keep exactly as shown.
IncompatibleGinas=	Lists Graphical Identification and Authentication dynamic link libraries (GINA.DLLs) that are incompatible with Cisco's GINA. Adding a GINA to the list causes the VPN Client to leave the GINA alone during installation and use fallback mode. (See section "Start Before Logon and GINAs".)	After the keyword and equal sign, enter the name(s) of the GINAs, separated by commas. For example: IncompatibleGinas= PALGina.dll, Ourgina.dll Do not enclose the name in quotes.
[Brand]	Required field to identify the branding text that appears on window titles and descriptions throughout the client application.	Keep exactly as shown, as the first branding section of the file.
CompanyText=	Keyword that identifies the name of your organization. If not present, the default is "Cisco Systems."	After the keyword and equal sign, enter the organization's name. The name can contain spaces and is not case sensitive.

Table 4-1 oem.ini File Parameters (continued)

Keyword	Description	Value
ProductText=	Keyword that identifies the name of the application. If not present, the default is “VPN Client.”	After the keyword and equal sign, enter the product name. The name can contain spaces and is not case sensitive.
[Default]	Required field to identify the section that contains names of default bitmap and icon to use if values are blank.	Enter exactly as shown, as the second section of the file.
WizardBitMap=	Keyword that identifies the vertical graphic that appears on the side of some VPN Client windows, the Connection Wizard dialog box. (See Figure 4-5.) The Cisco Systems vertical graphic is 104x249 pixels; 256 colors.	After the keyword and equal sign, enter the name of the wizard bitmap file.
MainIcon=	Keyword that identifies the main icon to use as a default. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the default icon file. You need to create only the 32x32 size.
SilentMode=	Keyword that identifies whether or not to activate silent installation.	After the keyword and equal sign, enter either 0 or 1. 1 activates silent installation: 0 = prompt the user during installation. 1 = do not prompt the user during installation.
InstallPath=	Keyword that identifies the directory into which to install the client software.	After the keyword and equal sign, enter the name of the directory in the suggested format: <i>root: \programs\company\product</i>
DefGroup=	Keyword that identifies the name of the folder to contain the client software.	After the keyword and equal sign, enter the name of the destination folder in the suggested format: <i>foldername</i>
Reboot=	Keyword that identifies whether to restart the system after the silent installation. If SilentMode is on (1) and Reboot is 1, the system automatically reboots after installation finishes.	After the keyword and equal sign, enter 0, 1, or 2: 0 = display the reboot dialog. 1 (and SilentMode = 1) = automatically reboot the system when installation finishes. 2 (and SilentMode = 1) = do not reboot after installation finishes.
[Dialer]	Required field to identify the section that contains the name of the Dialer application, the bitmap to use on the connections window, and the connection icons.	Enter exactly as shown, as the third section of the file.
AppNameText=	Keyword that identifies the name of the dialer application.	After the keyword and equal sign, enter the name of the dialer application. The name can contain spaces and is not case sensitive.
DialerBitMap=	Keyword that identifies the dialer bitmap (shown in Figure 4-3.) The dimensions of this bitmap are 298x116 pixels; 256 colors.	After the keyword and equal sign, enter the name of the dialer bitmap file.

Table 4-1 oem.ini File Parameters (continued)

Keyword	Description	Value
MainIcon=	Keyword that identifies the primary icon file for the connection and authentication windows. This icon appears in the User Authentication window and the system tray, for example. (See Figure 4-6 and Figure 4-7.) You can rotate or flip the lock image to fit with the brand graphic. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the primary icon file. The User Authentication window uses the 32x32 size and the system tray uses the 16x16 size. You need to create only the 32x32 size.
Frame0Icon=	Keyword that identifies the Frame 0 icon file, which is based on the main icon. (See Figure 4-8.) This icon shows at the start of the connection negotiation. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame0 icon file.
Frame1Icon=	Keyword that identifies the Frame 1 icon file, which is based on the main icon. (See Figure 4-9.) This icon shows further progress of the connection. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame1 icon file.
Frame2Icon=	Keyword that identifies the Frame 2 icon file, which is based on the main icon. (See Figure 4-10.) This icon shows further progress of connection establishment. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame2 icon file.
Frame3Icon=	Keyword that identifies the Frame 3 icon file, which is based on the main icon. (See Figure 4-11.) This icon shows the end of connection establishment. The dimensions are 32x32 pixels; 256 colors.	After the keyword and equal sign, enter the name of the Frame3 icon file.
AllowSBLLaunches	Keyword that identifies whether a VPN Client user is allowed to launch a third party application before logging on to a Windows NT platform.	After the keyword and equal sign, enter 1 to enable or 0 to disable this feature. The default is 0 (to disable). (See Note after table.)
[Log viewer]	Required field to identify the application name and icon for the Log Viewer application.	Keep exactly as shown, as the fourth section of the file.
AppNameText=	Keyword that identifies the name of the Log Viewer application.	After the keyword and equal sign, enter the name you want to give to the Log Viewer application. The name can contain spaces and is not case sensitive.
MainIcon=	Keyword that identifies the icon for the Log Viewer title bar, About window and applications menu. There are two sizes used: dimensions are 32x32 and 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the icon (.ico) file for this icon. You need to create only the 32x32 size.
[Certificate Manager]	Required field to identify the application name and icon for the Certificate Manager application.	Keep exactly as shown, as the sixth section of the file.
AppNameText=	Keyword that identifies the name of the Certificate Manager application.	After the keyword and equal sign, enter the name you want to give to the Certificate Manager application. The name can contain spaces and is not case sensitive.
MainIcon=	Keyword that identifies the icon for the Configuration Manager title bar and the applications menu. The dimensions are 16x16 pixels; 256 colors.	After the keyword and equal sign, enter the name of the icon (.ico) file for this icon.

**Note**

When AllowSBLLaunches is 0, “Allow launching of third party applications before logon” under Windows Logon Properties is unavailable. There might be cases when you need to launch an application before starting your connection, for example, to authenticate your access credentials. In this case you can use the following procedure:

In the VPN Dialer program, choose **Options > Windows Logon Properties**.

Uncheck **Disconnect VPN connection when logging off**.

Log out.

Log in with cached credentials.

Make your VPN Dialer connection.

Log out.

Log in again while already connected.

Start Before Logon and GINAs

The VPN Client can load prior to logging in to a Windows NT platform (Windows NT 4.0, Windows 2000, and Windows XP). This feature lets remote users establish a VPN connection to a private network where they can successfully log in to a domain. When installed on a Windows NT platform, the VPN Client tries to replace the standard Microsoft logon dialog box (the same one that appears after you press Ctrl+Alt+Del when booting your PC, called a GINA). The name of the Microsoft GINA is msgina.dll and you can find it in the registry at the location:

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
GinaDLL = msgina.dll
```

The VPN Client replaces the msgina.dll with the VPN Client’s GINA (csgina.dll), and then points to it so that you can still see and use the MS GINA. When you start your PC and press Ctrl+Alt+Del, you are launching the VPN Client Dialer application and the MS logon dialog box. The VPN Client detects whether the necessary Windows services are running and if not, displays a message asking you to wait. If you look in the VPN Client registry, you see the following parameters and values:

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 1
PreviousGinaPath = msgina.dll
```

Fallback Mode

In some cases a third-party program replaces the MS GINA, and in some of these cases the VPN Client works with the third-party program, while in other cases, it does not. The VPN Client maintains a list of incompatible GINAs that it does not work with, and does not replace the GINA file in use. This is called *fallback* mode. The list of incompatible GINAs resides in the registry, and the VPN Client refers to the list only during installation. The following registry entry is an example.

```
HKLM\Software\Cisco Systmes\VPN Client\
IncompatibleGinas=PALgina.dll,nwgina.dll,logonrem.dll,ngina.dll
```

In fallback mode, the VPN Client performs differently when Start Before Logon is in use. Instead of loading when you press Ctrl+Alt+Del, the VPN Dialer loads as soon as the VPN service starts. When operating in fallback mode, the VPN Client does not check to see if the necessary Windows services have started. As a result, the VPN connection could fail if initiated too quickly. In fallback mode, when the VPN connection succeeds, you then press Ctrl+Alt+Del to get to the Microsoft logon dialog box. In this mode, you see the following VPN Client registry parameters and values:

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 0
PreviousGinaPath = msgina.dll
```

**Note**

You can change the VPN Client to fallback mode by changing the GinaInstalled registry entry from 1 to 0 and restarting Windows.

Incompatible GINAs

If a new problem GINA is discovered after the VPN Client is released, you can add the GINA to the incompatible GINA list in the oem.ini file. Adding the GINA to this list places it in the IncompatibleGinas list in the registry when you install the VPN Client and puts the VPN Client into fallback mode, thus avoiding possible conflicts (see section “oem.ini File Keywords and Values”).

Installing the VPN Client in Silent Mode

To install the VPN Client software without user intervention, you can use the *silent mode*. To implement silent mode with or without rebranding, you can create an oem.ini file containing only the part that configures silent mode. In this file, you turn Silent Mode on, identify the pathname and folder to contain the VPN Client software, and reboot the system, all without user interaction.

During silent mode installation, the installation program does not display error messages. The program stores error messages in a log file named VPNLog.txt located in the windows system directory (WINSYSDIR).

**Note**

If the installation program detects a 2.x version of the VPN Client, the program still prompts the user for input when converting the connection entry profiles.

A sample oem.ini file for implementing silent mode follows:

```
[Default]
SilentMode = 1
InstallPath = C:\Program Files\Engineering\IPSec Connections
DefGroup = IPSec remote users
Reboot = 1
```

Table 4-2 oem.ini File Silent Mode Parameters

.ini parameter (keyword)	Parameter Description	Values
SilentMode=	Keyword that identifies whether or not to activate noninteractive installation.	After the keyword and equal sign, enter either 0 or 1. 1 activates silent installation: 0 = prompt the user during installation. 1= do not prompt the user during installation.
InstallPath=	Keyword that identifies the directory for the client software installation.	After the keyword and equal sign, enter the name of the directory in the suggested format: <i>root:\programs\organization\product</i>

Table 4-2 *oem.ini File Silent Mode Parameters (continued)*

.ini parameter (keyword)	Parameter Description	Values
DefGroup=	Keyword that identifies the name of the folder to contain the client software.	After the keyword and equal sign, enter the name of the destination folder in the suggested format: <i>foldername</i>
Reboot=	Keyword that identifies whether to restart the system after the silent installation. If SilentMode is on (1) and Reboot is 1, the system automatically reboots after installation finishes.	After the keyword and equal sign, enter 0, 1, or 2: 0 = display the reboot dialog. 1 (and SilentMode = 1) = automatically reboot the system when installation finishes. 2 (and SilentMode = 1) = do not reboot after installation finishes.

Additional Bitmap—setup.bmp

The oem version of VPN Client includes a bitmap on the distribution CD that is not in the oem.ini file: `setup.bmp`. You can substitute your own image for this .bmp file, as long as you keep the current filename (`setup.bmp`) and make sure that the file is in the same directory and folder as the oem.ini file.

`setup.bmp` displays a logo on the window when you start the installation program. The size of the Cisco Systems setup bitmap is 330x330 pixels and it uses 256 colors.



Troubleshooting and Programmer Notes

This chapter contains information to help you resolve problems installing or running the VPN Client. It also contains notes helpful to writing programs for special needs.

Troubleshooting the VPN Client

This section describes how to perform the following tasks:

- Gathering Information for Customer Support
- Solving Common Problems
- Changing the MTU Size

Gathering Information for Customer Support

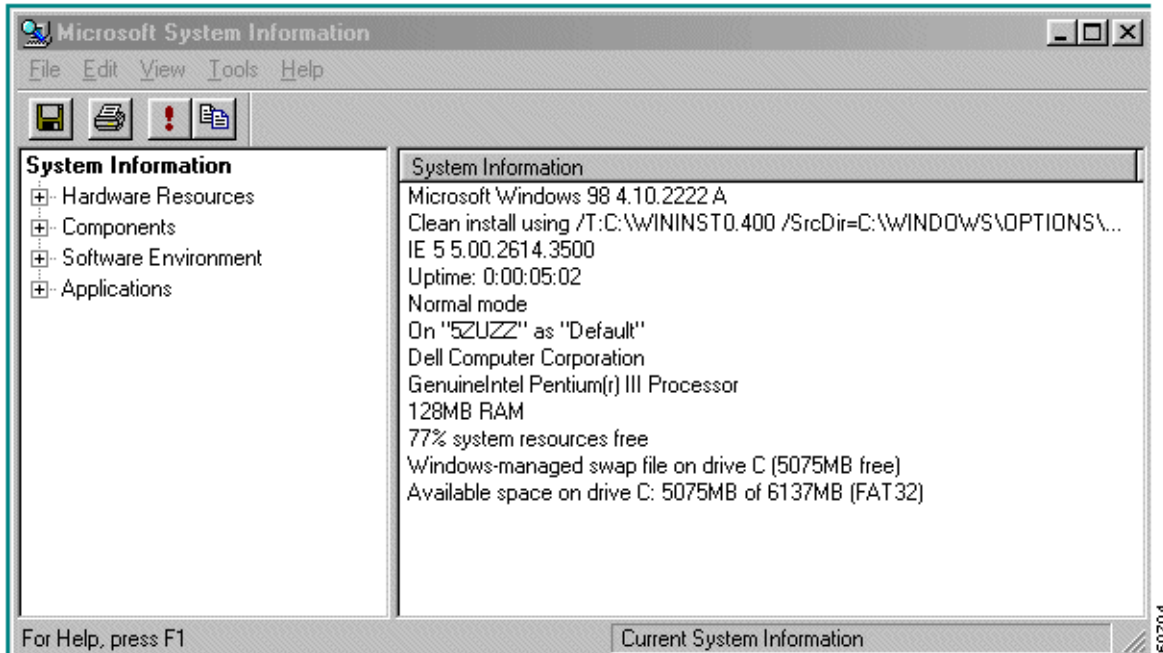
If you are having problems running the VPN Client on your PC, you can gather system information that is helpful to a customer support representative and e-mail it to us. We recommend that you do the following *before* you contact us.

If Your Operating System is Windows 98, 98 SE, ME, 2000, or XP

Go to the **Start** menu and select **Programs > Accessories > System Tools > System Information**.

Windows displays the Microsoft System Information screen, such as the one in Figure 5-1.

Figure 5-1 System Information Screen on Windows 98



Select a category and the screen displays details for that category. You can then execute the **Export** command and choose a name and destination. Windows creates a text file, which you can attach to an e-mail message and send to the support center.

If Your Operating System is Windows NT or Windows 2000

On the Windows NT or Windows 2000 operating system, you can run a utility named `WINMSD` from a command-line prompt. `WINMSD` generates a file containing information about your system configuration, and the software and drivers installed.

To use this utility, perform the following steps:

-
- Step 1** Go to the **Start** menu and select **Programs > Command Prompt**.

This action displays a window with a DOS prompt, such as `c:\`.

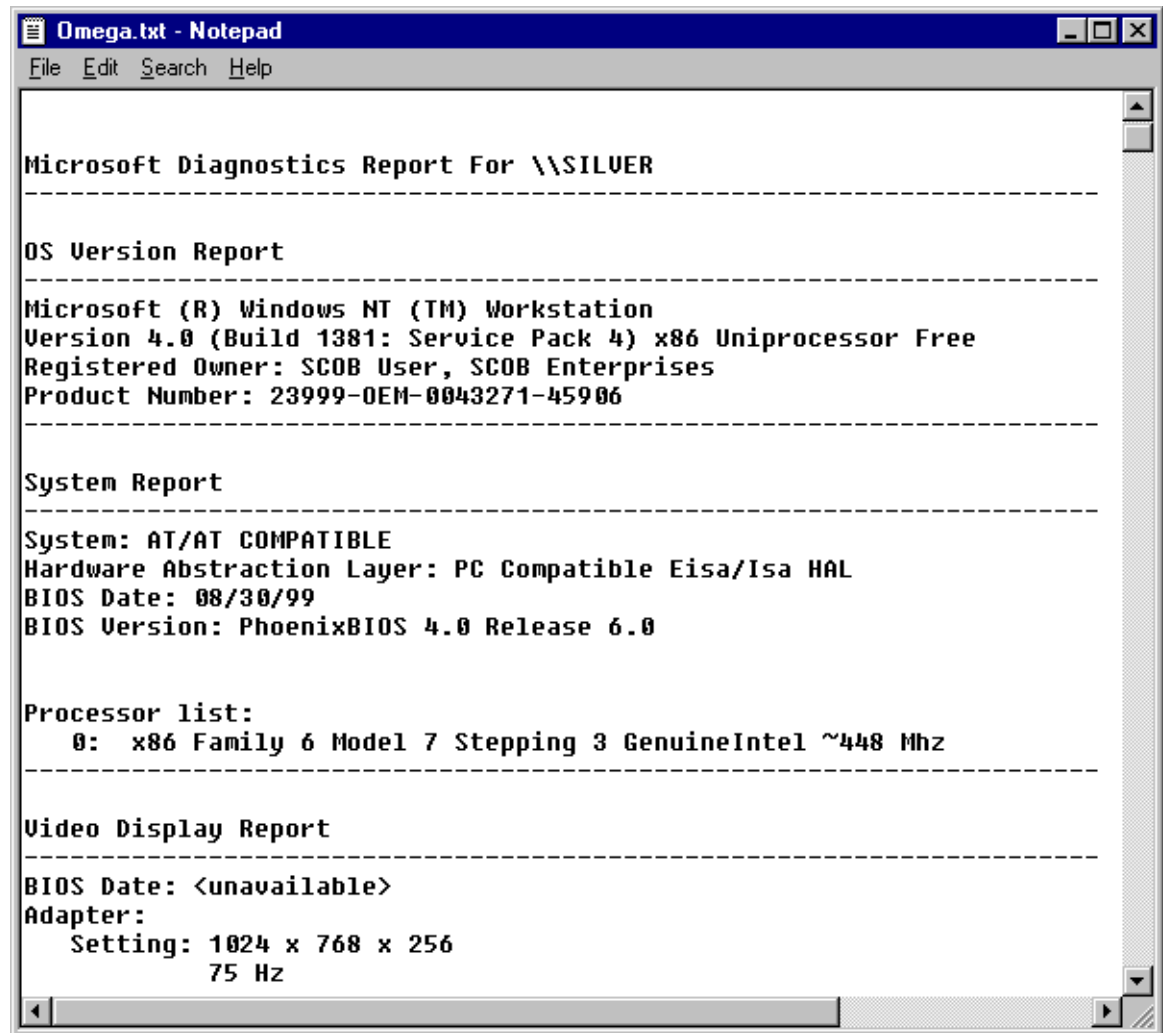
- Step 2** Type the following command at the DOS prompt:

```
c:\>winmsd /a /f
where /a = all and /f = write to file.
```

This command generates a text (.txt) file with the name of your computer and places the file in the directory from which you run the command. For example, if the name of your machine is **SILVER** and you execute the command from the `c:` drive (as shown above), the text file name is `silver.txt`.

If you open the file with a text editor, such as Notepad, you see a file such as the one shown in Figure 5-2, which was from a Windows NT system.

Figure 5-2 System Text File



You can attach this file to an e-mail message and send it to the support center.

Solving Common Problems

This section describes some common problems and what to do about them.

Shutting Down on Windows 98

You may experience a problem with your Windows 98 system shutting down when the VPN Client software is installed. If so, you need to disable the fast shutdown feature, as follows:

- Step 1 At the Microsoft System Information screen (shown in Figure 5-1), select **Tools> System Configuration**. Microsoft displays a **Properties** page.
- Step 2 From the **General** page, select the **Advanced** button.

Step 3 Choose the **Disable Fast Shutdown** option.

Booting Automatically Starts up Dial-up Networking on Windows 95

Some versions of Internet Explorer silently control startup options in Windows 95 so that every time you start your system, Dial-Up Networking launches. If this occurs, as it does in Internet Explorer 3.0, go to View > Options > Connections and uncheck the option `Connect to the Internet as needed`.

Changing the MTU Size

The Set MTU option is used primarily for troubleshooting connectivity problems.



Note

The VPN Client automatically adjusts the MTU size to suit your environment, so running this application should not be necessary.

The maximum transmission unit (MTU) parameter determines the largest packet size in bytes that the client application can transmit through the network. If the MTU size is too large, the packets may not reach their destination. Adjusting the size of the MTU affects all applications that use the network adapter. Therefore the MTU setting you use can affect your PC's performance on the network.

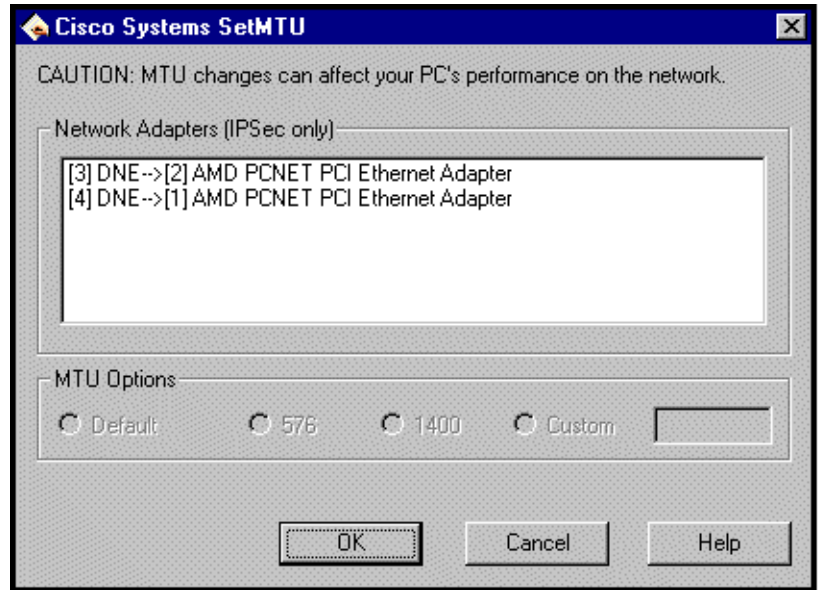
MTU sizing affects fragmentation of IPsec and IPsec through NAT mode packets to your connection destination. A large size (for example, over 1400) can increase fragmentation. Using 1400 or smaller usually prevents fragmentation. Fragmentation and reassembly of packets at the destination causes slower tunnel performance. Also, many firewalls do not let fragments through.

To change the size of the MTU, use the following procedure:

Step 1 Select **Start > Programs > Cisco Systems VPN Client > SetMTU**.

The Set MTU window appears.

Figure 5-3 Setting MTU Size on Windows NT



Step 2 Click a network adapter on the list of network adapters.

Step 3 Click one of the following choices under MTU Options:

Default	The factory setting for this adapter type.
576 (in bytes)	The standard size for dial-up adapters.
1400 (in bytes)	The choice recommended for both straight IPSec and IPSec through NAT. Using this value guarantees that the client does not fragment packets under normal circumstances.
Custom	Enter a value in the box. The minimum value for MTU size is 68 bytes.

Step 4 Click OK.

You must restart your system for your change to take effect

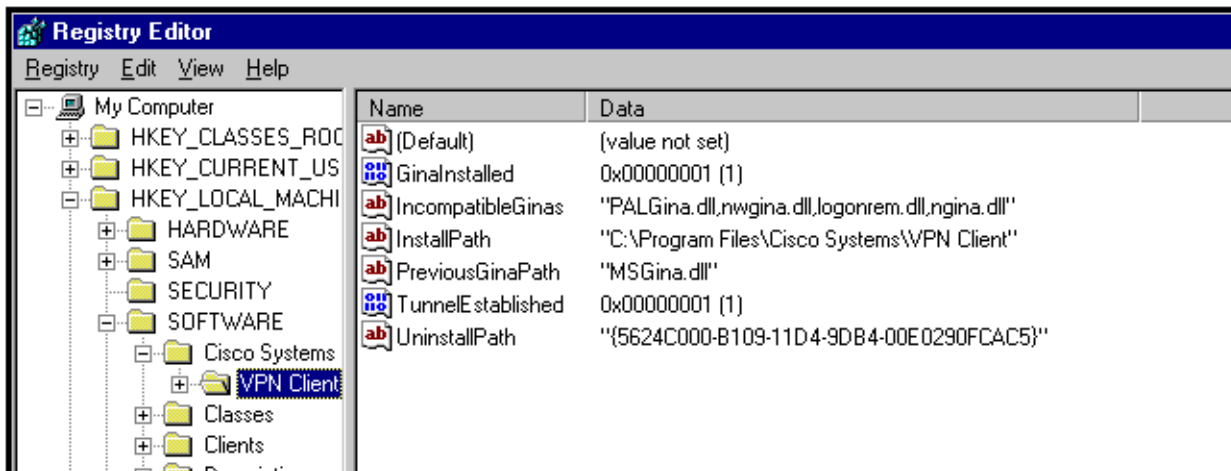
Programmer Notes

This section contains information to aid a programmer in writing programs that perform routine tasks.

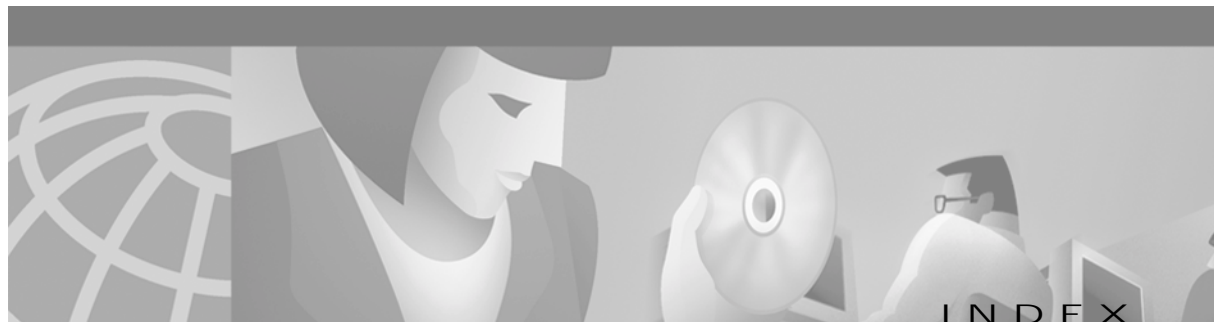
Testing the Connection

As part of a program, you might want to test a connection to see if it is active before performing the tasks that are the purpose of the program. To test the connection, you can poll the TunnelEstablished entry in the HKEY_LOCAL_MACHINE registry. To see this entry, bring up the Registry Editor and go to SOFTWARE > Cisco Systems > VPN Client. (See Figure 5-4.) In the list of entries, you see TunnelEstablished. This entry can have only two values: 1 or 0. If the connection is working, the value is 1; if not, the value is 0.

Figure 5-4 Cisco Systems VPN Client Registry Entries



60700



A

activating an IKE proposal 1-3
adding an SA 1-3
ApplicationLauncher parameters 2-5
authentication parameters (.pcf file) 2-9
AuthType parameter (.pcf file) 2-8
AYT firewall policy 1-6

B

BackupServer parameter (.pcf file) 2-10
batch files
 erasing saved password 3-2
 suppressing termination prompt 3-2
bitmaps
 dialer 4-3
 setup.bmp 4-2, 4-13
BlackIce Defender
 firewall on remote PC 1-6
bmp files 4-13
 for installation 4-2
brand parameters (oem.ini file) 4-8

C

CD-ROM
 image for VPN Client software 2-13
Centralized Protection Policy (CPP) 1-5
certificate enrollment
 IP address 2-5
 parameters (vpnclient.ini file) 2-4
Certificate Manager

 parameters (oem.ini file) 4-10
 rebranding 4-6
certificate parameters (.pcf files) 2-11
certificates
 Entrust 1-16
 group name requirement 1-4
 organization unit field 1-4
 VPN Client connections
 configuring VPN concentrator 1-3
changing the MTU size 5-4
Cisco, contacting
 technical support xii
 telephone xiii
 Web page xii
Cisco.com Web page xii
Cisco Integrated Client
 scenario 1-7
 VPN Client software 1-5
Cisco TAC
 phone numbers xiii
 Web page xiii
client/server firewall 1-6
command-line interface
 error messages 3-7
commands
 displaying a list 3-1
 vpnclient
 connect 3-1
 disconnect 3-4
 notify 3-3
 stat 3-4
configuration parameters
 global profile 2-2

- individual profiles 2-7
- configurations
 - client/server 1-11
- configuring
 - Entrust certificate 1-16
 - local LAN access for VPN Client 1-14
 - personal firewalls 1-4
- connection
 - ending 3-4
 - getting status 3-4
 - profiles 2-6
 - starting 3-1
 - testing 5-6
- connection entry
 - file 2-6
 - preconfigured
 - distributing 2-12
- contacting Cisco with questions xii
- continuous display 3-4
- CPP
 - defining filters and rules 1-9
- creating
 - connection profiles 2-6
 - Entrust profile 1-16
 - global profile 2-2
 - IPSec group in VPN Concentrator 1-2
 - oem.ini file 4-7
 - user profiles in VPN Concentrator 1-3

D

- data formats xi
- DefGroup parameter (oem.ini file) 4-9
- Description parameter (.pcf file) 2-7
- DHCP inbound traffic
 - stateful firewall 1-5
- DHGroup parameter (.pcf files) 2-12
- DialerDisconnect parameter (vpnclient.ini file) 2-3
- dialer icon

- main dialog box 4-3
- suppressing 3-2
- dialer parameters (oem.ini file) 4-9
- directory
 - profiles 2-2, 2-6
- Disable Fast Shutdown option 5-4
- diskette image
 - VPN Client software 2-13
- displaying
 - information continuously 3-4
 - notifications 3-3
- distributing preconfigured software 2-12
- documentation
 - additional viii
 - cautions x
 - notes x
 - on CD-ROM xi
 - ordering xii

E

- EnableBackup parameter (.pcf file) 2-10
- EnableISPCConnect parameter (.pcf file) 2-8
- EnableLocalLAN parameter (.pcf file) 2-10
- EnableLog parameter (vpnclient.ini file) 2-3
- EnableMSLogon parameter (.pcf file) 2-10
- EnableNat parameter (.pcf file) 2-10
- encGroupPwd parameter (.pcf file) 2-8
- ending a connection 3-4
- Entrust certificates
 - enabling VPN Client 1-16
- EntrustIni parameter (vpnclient.ini file) 2-3
- eraseuserpwd parameter 3-2
- error messages 3-7
- ESP inbound traffic
 - stateful firewall 1-5

F

files

- .bmp 4-2
- .pcf 2-6
- oem.ini 4-7
- vpnclient.ini 2-1
 - sample 2-2

filters

- defining for CPP 1-9

firewalls

- AYT 1-6
- BlackIce Defender 1-6
- Cisco Integrated Client 1-5
- client/server

- configuring 1-11

configurations

- comparisons 1-6
 - group 1-10
 - matching 1-4
 - scenarios 1-7

CPP 1-5

custom 1-11

defining filters and rules 1-9

Integrity Server 1-6

notifications during negotiations 1-12

personal firewall

- enforcement on remote PC 1-6

requiring 1-4

stateful on VPN Client 1-5

ForceKeepAlives parameter (.pcf file) 2-11

formats

- data xi
- IP addresses xi

fragmentation

- preventing 5-4

G

GINA.DLL files 4-8

global profile

- creating 2-2

GroupName parameter (.pcf file) 2-8

GroupPwd parameter (.pcf file) 2-8

H

HKEY_LOCAL_MACHINE 5-6

Host parameter (.pcf file) 2-8

I

icons

- Certificate Manager 4-6

- dialer 4-3

- Log Viewer 4-6

- rebranding 4-4

IKE proposal

- activating 1-3

incompatible ginas

- start before logon feature 4-11

IncompatibleGinas parameter (oem.ini file) 4-8

installation

- automatic 4-1

InstallPath parameter (oem.ini file) 4-9

Integrity Server firewall

- configuring 1-11
 - feature description 1-6

IP addresses

- certificate enrollment 2-5
 - format xi

IPSec group

- creating on VPN Concentrator 1-2

IPSec log file

- troubleshooting firewall configurations 1-12

ISPCCommand parameter (.pcf file) 2-9
 ISPCConnect parameter (.pcf file) 2-9
 ISPCConnectType parameter (.pcf file) 2-8

L

local LAN access
 configuring 1-14
 LogLevel parameter 2-4
 log parameters (vpnclient.ini file) 2-4
 Log Viewer
 icon 4-6
 parameters (oem.ini file) 4-10
 rebranding 4-6

M

MainIcon parameter (oem.ini file) 4-9
 making a parameter read only 2-2
 matching firewall configurations 1-4
 maximum transmission unit
 see MTU setting
 MSLogonType parameter (.pcf file) 2-10
 MTU setting 5-4
 changing 5-4

N

notifications
 displaying 3-3
 firewalls 1-12
 upgrade 1-13
 notify command 3-3
 notrayicon parameter 3-2

O

obtaining documentation xi

oem.ini file
 creating 4-7
 keywords and values 4-8
 rebranding VPN Client 4-7
 sample 4-7
 organizational unit field in certificate 1-4
 overriding password 3-2

P

parameters
 Certificate Manager (oem.ini) 4-10
 DefGroup (oem.ini) 4-9
 eraseuserpwd 3-2
 IncompatibleGinas (oem.ini) 4-8
 InstallPath (oem.ini) 4-9
 Log viewer (oem.ini) 4-10
 MainIcon (oem.ini) 4-9
 peer timeout (.pcf file) 2-11
 profile (.pcf)
 authentication 2-9
 AuthType 2-8
 BackupServer 2-10
 certificate parameters 2-11
 Description 2-7
 DHGroup 2-12
 EnableISPCConnect 2-8
 EnableLocalLAN 2-10
 EnableMSLogon 2-10
 EnableNat 2-10
 encGroupPwd 2-8
 ForceKeepAlives 2-11
 GroupName 2-8
 GroupPwd 2-8
 Host 2-8
 ISPCCommand 2-9
 ISPCConnect 2-9
 ISPCConnectType 2-8
 MSLogonType 2-10

- PeerTimeout 2-11
- SendCertChain 2-12
- TCPTunnelingPort 2-10
- TunnelingMode 2-10
- read only 2-2
- reboot (oem.ini) 4-9
- repeat 3-4
- reset 3-4
- route 3-4
- SilentMode (oem.ini) 4-9
- traffic 3-4
- tunnel 3-4
- vpnclient.ini
 - ApplicationLauncher 2-5
 - certificate enrollment 2-4
 - DialerDisconnect 2-3
 - EnableLog 2-3
 - EntrustIni 2-3
 - log class 2-4
 - LogLevel 2-4
 - RunAtLogon 2-3
 - StatefulFirewall 2-3
- WizardBitMap (oem.ini) 4-9
- pcf files
 - creating 2-6
 - distributing with VPN Client software 2-13
 - parameters 2-7
 - sample 2-6
- PeerTimeout parameter (.pcf file) 2-11
- personal firewalls
 - configuring for VPN Client
 - VPN Concentrator 1-4
- preconfigured connection entry
 - distributing 2-12
- preconfiguring VPN Clients for remote users 2-1
- profile
 - connection entry 2-6
 - creating user 1-3
 - directory 2-2

- Entrust 1-16
- file format 2-1
- global 2-1
- programmer notes
 - testing a connection 5-6

R

- read-only parameters 2-2
- Reboot parameter (oem.ini) file 4-9
- rebranding VPN Client software
 - areas affected by 4-2
 - bitmaps 4-4
 - Certificate Manager application 4-6
 - icons 4-4
 - Log Viewer application 4-6
 - menu titles and text 4-2
 - oem.ini file 4-7
 - setup bitmap 4-2
 - VPN Dialer application 4-3
- registry
 - testing a connection 5-6
- related documentation viii
- Remote Firewall
 - scenario 1-8
- resetting counts 3-4
- routing information 3-4
- rules
 - defining for CPP 1-9
- RunAtLogon parameter (vpnclient.ini file) 2-3

S

- SA
 - adding 1-3
- sample files
 - .pcf file 2-6
 - oem.ini file 4-7

- vpnclient.ini 2-2
- SendCertChain parameter 2-12
- Set MTU program 5-4
- setup.bmp 4-2, 4-13
- silent install 4-1
- SilentMode parameter
 - oem.ini file 4-12
- SilentMode parameter (oem.ini file) 4-9
- software image
 - CD-ROM 2-13
 - diskette 2-13
- start before logon
 - gina files 4-11
- starting a connection 3-1
- stateful firewall
 - always on 1-5
- StatefulFirewall parameter (vpnclient.ini file) 2-3
- status information
 - generating 3-4
- support, Cisco xii
- system information
 - Windows 98 5-1
 - Windows NT 5-2
- system security
 - protecting 2-7

T

- TAC
 - phone numbers xiii
- TCPTunnelingPort parameter (.pcf file) 2-10
- testing a connection 5-6
- traffic information 3-4
- troubleshooting
 - connectivity application 5-4
 - generating information 5-1
- TunnelEstablished parameter in registry 5-6
- tunneling information 3-4
- TunnelingMode parameter (.pcf file) 2-10

U

- upgrade notifications
 - configured on VPN Concentrator 1-13
- user profiles
 - creating for distribution 2-6
 - creating in VPN Concentrator 1-3

V

- VPN Client
 - applications vii
 - configuring 2-1
- vpnclient.ini file
 - file format 2-1
 - sample 2-2
- VPN Concentrator
 - configuring personal firewalls for VPN Client 1-4
 - creating user profiles 1-3
- VPN Dialer
 - rebranding 4-3

W

- Windows 98
 - generating system information 5-2
 - shut down problem 5-3
- Windows NT or Windows 2000
 - generating system information 5-2
- WINMSD utility
 - Windows NT or Windows 2000 5-2
- WizardBitMap parameter (oem.ini file) 4-9