CISCO SYSTEMS

VPN Client Administrator Guide

Release 3.6
August 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

CONTENTS

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 (for InstallShield installation only)
- 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. 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, local LAN access, backup servers, NAT-T. Also describes how to configure a VPN Client to work with Entrust Entelligence and smart cards.
Chapter 2	Preconfiguring the VPN Client for Remote Users	Shows how to create global and user profiles.
Chapter 3	Configuring Automatic VPN Initiation	Describes auto initiation and how to configure the vpnclient.ini file for auto initiation.
Chapter 4	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 5	Customizing the VPN Client Software	Describes how to use your own names and icons for the VPN Client applications instead of Cisco Systems names. Also describes how to install and reboot the VPN Client software without user interaction, called *silent mode*.
Chapter 6	Troubleshooting and Programmer Notes	Lists a few troubleshooting techniques. Describes how to use the SetMTU application.
Chapter 7	Windows Installer (MSI) Information	Lists the differences between InstallShield and MSI, describes alternative ways to start MSI, explains logging and upgrading.

Related Documentation

The *VPN Client User Guide for Windows* explains to Client users how to install the VPN Client for Windows software, configure connection entries, connect to Cisco VPN devices, manage VPN connections, and enroll for digital certificates. 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**.
italic font	Arguments for which you supply values are in *italics*.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font in the command-line interface (for example, **`vpnclient stat`**).
`italic screen` font	Arguments for which you supply values are in *italic screen* font.

Notes use the following conventions:

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

Cautions use the following conventions:

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

Data Formats

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

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, `192.168.12.34`); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, `255.255.255.0`). Wildcard masks use the same notation (for example, `0.0.0.255`); as the example illustrates, you can omit leading zeros in a byte position.
MAC Addresses	MAC addresses use 6-byte hexadecimal notation (for example, `00.10.5A.1F.4F.07`).
Hostnames	Hostnames use legitimate network hostname or end-system name notation (for example, `VPN01`). Spaces are not allowed. A hostname must uniquely identify a specific system on a network.

Type of Data	Format
Text Strings	Text strings use upper- and lower-case alphanumeric characters. Most text strings are case-sensitive (for example, simon and Simon represent different usernames). In most cases, the maximum length of text strings is 48 characters.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. No commas or spaces are permitted in a number.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

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

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

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

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

Configuration Information for an Administrator

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

This chapter includes the following major topics:

- VPN 3000 Series Concentrators Configuration Information
- Configuring Entrust Entelligence for the VPN Client
- Setting up the VPN Client for Authentication using Smart Cards

VPN 3000 Series Concentrators Configuration Information

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 the VPN Concentrator for Client Backup Servers
- Configuring NAT Traversal 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 complete the following tasks on 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 "Gathering Information You Need" in *VPN Client User Guide for Windows*, Chapter 2.

Step 2   Next, select a method of authentication. The Type parameter determines the group authentication method, Internal or External. Internal groups are configured on the VPN Concentrator. If you select External, you must configure an external RADIUS server to authenticate and return appropriate group attributes.

Step 3   Under the General tab | Tunneling Protocols, be sure IPSec is checked.

Step 4   Under the IPSec tab | IPSec SA, select **ESP-3DES-MD5** to require Triple-DES authentication. Alternatively, you could choose **ESP-DES-MD5**, which uses DES authentication and provides a minimum level of security. Or, to use AES, select one of the AES protocols, such as **ESP-AES128-SHA**. AES is the most secure.

> **Note**   To create or customize the Security Association (SA), see the Configuration | Policy Management | Traffic Management | Security Associations screens.

Step 5   Under IPSec > Authentication, choose the method you use for the members of the group; for example, Internal or RADIUS. If you choose an authentication method other than None or Internal, be sure to configure the external authentication server appropriately and supply users with the appropriate information for installing the VPN Client.

Step 6   To require users to enter a password each time they log in, we suggest that you *not* check Allow Password Storage on Client, which is on the Client Config tab. 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, Password, and Verify Password. VPN Client users need a user name and password to authenticate when they connect to the VPN Concentrator; see "Gathering Information You Need" in *VPN Client User Guide for Windows*, 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 and IPSec. 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 SA.
- 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:

a.   Activate one of the IKE protocols such as CiscoVPNClient-3DES-MD5-RSA-DH5, CiscoVPNClient-3DES-SHA-DSA-DH5, or CiscoVPNClient-AES128-SHA.

> **Note**   To use AES, move the AES proposal(s) to the top of the list. You must be running Release 3.6 of the VPN Client software to use AES

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."

c.   Click Security Associations, which takes you to the next step.

Step 2   Use the Configuration | Policy Management | Traffic Management | Security Associations screen to create a new SA. You can use the Security Associations link on the IKE Proposals screen.

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:

a.   To use the Organizational Unit to configure the group, under the Identity tab, enter a group name that is the same as the 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). Enter password and verify it.
or
Alternatively, you can configure a policy for certificate group matching. To use this approach, go to Configuration | Policy Management | Certificate Group Matching | Policy. For instructions on creating rules, see *VPN 3000 Series Concentrator Reference I: Configuration* for this section or refer to online help.

b.   Under the IPSec tab > IPSec SA, select the IPSec SA you created in step 2; for example, "Security association for digital certificate use."

c.   Under IPSec tab > Authentication, select the method you use for user authentication; for example, Internal. If you select an external authentication method, such as RADIUS, be sure to configure the external authentication server appropriately and supply users with the appropriate entries for the "Gathering the Information You Need" section in Chapter 2.

d.   Click **Add** or **Apply**, and save the configuration.

Step 4   Use the Configuration | User Management | Users | Add or Modify | Identity screen to configure VPN Client users for digital certificates:

a.   As the group name, enter the group you have set up in step 3 as the group parameter; continuing the example, you would enter `Finance`.

b.   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 includes the following topics:

- how firewalls work with the VPN Client
- list of the personal firewall products that the VPN Client can enforce for Internet traffic
- how to configure a stateful firewall policy on a VPN Concentrator 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 enabled 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.

> **Note**   The Always On personal firewall allows inbound access from the internal (tunneled) network to ensure that your internal applications work properly, while still providing additional protection for nontunneled traffic.

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. While the "Always On" option lets the VPN Client user choose to have basic firewall protection in effect, 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 firewall *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 though 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.)
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 three 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
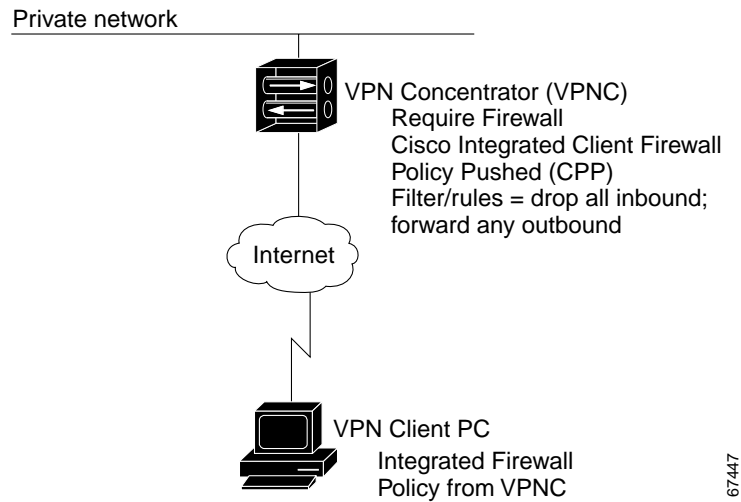
Remote Firewall

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

Private network

VPN Concentrator (VPNC)
Require firewall
Specific firewall selected
Policy set up on remote PC's firewall

Internet

VPN Client PC
ZoneAlarm, BlackICE,Custom, etc.
Firewall defines and maintains policy
VPN Client polls (AYT)

67448
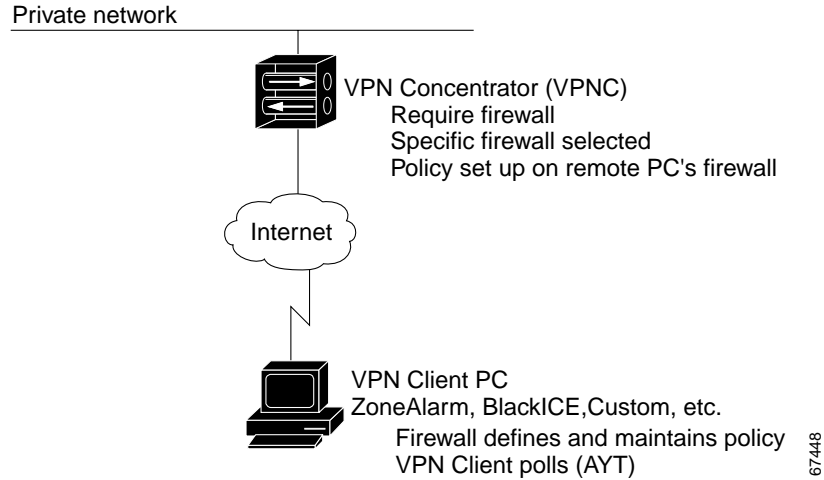
Client/Server Approach

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

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

Integrity Server (IS)
Gets User ID, Session ID, and Port from VPNC
Provides connection information to VPNC
Establishes policy; pushes policy to Integrity Agent (IA)

Private network

VPN Concentrator (VPNC)
Knows address of IS
Provides User ID/Session ID/Port to IS
Sends User ID/Session ID/Port to VPN Client

Internet

VPN Client PC
Integrity Agent (IA)

IA installed and running
VPNC and VPN Client negotiate
VPNC passes User ID/Session ID/Port to Integrity Server
VPN Client
-- initializes IA with cached info
--passes User ID/Session ID to IA
IA connects with IS; gets firewall policy from IS

IA starts enforcing policy
VPN Client polls IA every 30 seconds
If Firewall terminates, VPN connection dropped
VPN Client uninitializes IA
Caches policy

67449

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**

    a.   For the Rule Name, enter the name, such as `FW-Allow incoming HTTP`.

    b.   For Action, choose **Forward**.

    c.   For Protocol, choose **TCP**.

    d.   For TCP/UDP Destination Port, choose **HTTP(80)**.

    e.   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**.

    a.   Click the **Add Filter** box.

    b.   Enter the filter name, such as `FW-Allow Incoming HTTP`, and select the defaults for the remaining parameters.

    c.   Click **Add**, which brings up the Actions screen.

    d.   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.

    e.   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 Guide for Windows*, 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 Protection
Policy)
 •

 •

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 Protection
Policy)
```

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
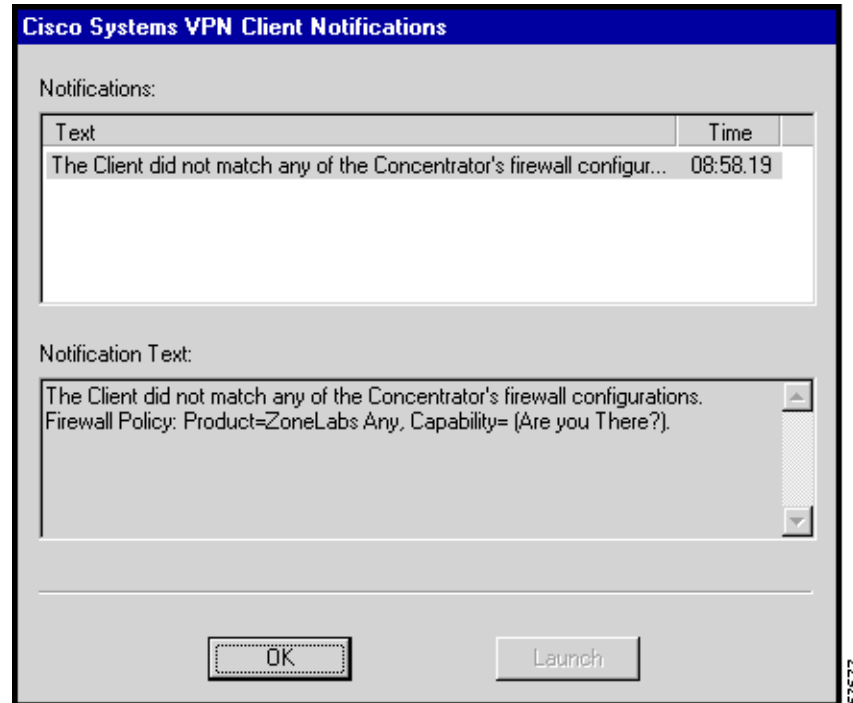
Notifying Remote Users of a Client Update

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 (the update does not happen automatically). 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. You can 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 local LAN access in specific groups 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.

   a.   Open the **Options** pull-down menu.

   b.   Choose **Properties**.

   c.   Check **Allow Local LAN Access**.

Step 2   On the VPN 3000 Concentrator, either add a new group or modify an existing group as follows:

   a.   To configure local LAN access for a specific group, go to Configuration | User Management | Groups.

   b.   Choose either **Add** to add a new group or **Modify** to enable split tunneling for an existing group.

   c.   Go to the IPSec tab.

   d.   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.

   e.   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 or print by IP Address. 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 the VPN Concentrator for Client Backup Servers

This section shows how to configure a group on the VPN Concentrator to automatically push new backup server information to a VPN Client.

Step 1	On the VPN Concentrator, go to Configuration	User Management	Group.
Step 2	To add a new group, click **Add** or to modify an existing group, highlight it in the box and click **Modify**.
Step 3	Go to the Client Config tab.
Step 4	For IPSec Backup Servers, select **Use List Below** from the drop-down menu.
Step 5	Enter a list of up to 10 IPSec backup servers in high to low priority order.
Step 6	Type each server address or name on a single line into the IPSec Backup Servers box.
Step 7	Click **Apply** and then save the configuration.

Configuring NAT Traversal for the VPN Client

NAT Traversal (NAT-T) lets the VPN Concentrator establish IPSec tunnels with a VPN Client when there is a NAT device between them. It does this by encapsulating ESP traffic in UDP datagrams, which provides ESP with the port information that NAT devices require.

You can configure NAT-T globally on the VPN Concentrator, which then activates NAT-T for all groups configured on the VPN Concentrator. Or you can configure NAT-T for specific groups only.

Global Configuration

To configure NAT-T globally, follow these steps on the VPN Concentrator:

Step 1	To enable NAT Traversal on the VPN Concentrator globally, go to Configuration	System	Tunneling Protocols| IPSec	NAT Transparency and check the **IPSec over NAT-T** check box.
Step 2	Click **Apply** and then save the configuration.

Group Configuration

To configure NAT-T by group, you can configure IPSec over UDP on a group basis as follows:

Step 1	To configure a group for IPSec over UDP, go to Configuration	User Management	Groups	Add/Modify.
Step 2	Select the **Client Config** tab.
Step 3	Click **IPSec over UDP** to enable this feature for the group.
Step 4	Enter the UDP port into the **IPSec over UDP Port** field.

Next configure the following parameters on the VPN Client.

Step 1   On the VPN Client, go to Options > Properties > General.

Step 2   Check **Enable Transparent Tunneling** check box.

Step 3   Click either the **Allow IPSec over UDP (NAT/PAT)** or the **Use IPSec over TPC (NAT/PAT/Firewall)** radio button.
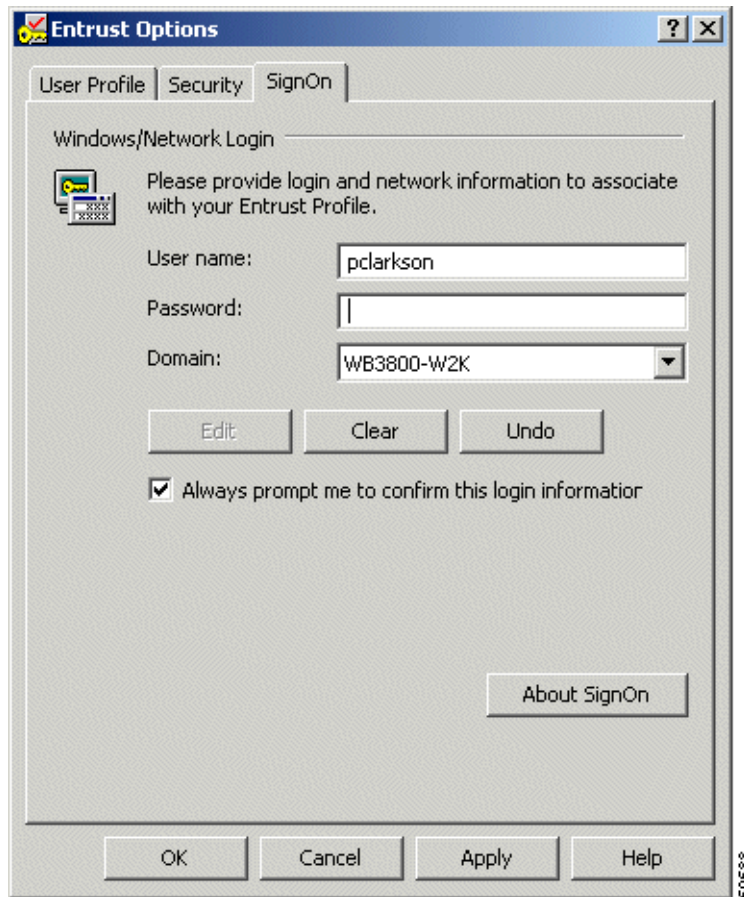
Configuring Entrust Entelligence for the VPN Client

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 for Windows*, Chapter 4.

Step 2   As part of Entust 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 to 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 see section "Configuring an Entrust Certificate for Authentication," in Chapter 3 of *VPN Client User Guide for Windows*.

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 Entrust Entelligence version 5., 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. Once the VPN Client connection is initiated, the user is prompted to enter a PIN or passcode to obtain access to the smart card. 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.

In general:

Step 1 Under Key Options, when you are performing web-based certificat enrollment, choose your smart card provider from the pull-down menu.

Step 2 For Key usage choose **Signature** and verify that **Create new key set** is selected.

Step 3 Install the certificate. The keys are generated on the smart card and a copy of the certificate is stored in the Microsoft store on your PC and listed in the VPN Client Certificate Manager screen under Personal Certificates.

Now a VPN Client user can only complete authentication when the smart card is inserted in its reader that is plugged into the proper port on the PC and when the user enters the correct PIN or passcode.

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.

■ **Setting up the VPN Client for Authentication using Smart Cards**

2

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

Groups of configuration parameters define the connection entries that remote users use to connect to a VPN device. Together these parameters form files called profiles. There are two profiles: a global profile and an individual profile. A global profile sets rules for all remote users; it contains parameters for the VPN Client as a whole. The name of the global profile file is vpnclient.ini. Individual profiles contain the parameter settings for each connection entry and are unique to that connection entry. Individual profiles have a .pcf extension.

Profiles get created in two ways: when you or a remote user creates connection entries using the VPN Dialer application (connection wizard) or when you create profiles using a text editor. In the first case, the remote user is also creating a file that can be edited through a text editor. You can start with a profile file generated through the GUI and edit it. This approach lets you control some parameters that are not available in the VPN Client GUI application.

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

This chapter explains how to create and edit the vpnclient.ini and individual 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).

Features Controlled by Global Profile

The vpnclient.ini file controls the following features:

- Start before logon

- Automatic disconnect upon log off

- Control of logging services by class

- Setting of the Stateful Firewall option

- Certificate enrollment

- Identity of a proxy server for routing HTTP traffic

- Identity of an application to launch upon connect

- Missing group warning message

- Location of the Entrust.ini file

- List of GINAs that are not compatible with the VPN Client

- Auto initiation

- Microsoft Outlook to Microsoft Exchange polling

- The method to use in adding suffixes to domain names on Windows 2000 and Windows XP platforms

Sample vpnclient.ini file

This sample file shows what you might see if you open it with a text editor

```
[main]
IncompatibleGinas=PALGina.dll,theirgina.dll
RunAtLogon=0
EnableLog=1
DialerDisconnect=1
AutoInitiationEnable=1
AutoInitiationRetryInterval=1
AutoInitiationList=techsupport,admin
[techsupport]
Network=175.55.0.0
Mask=255.255.0.0
ConnectionEntry=ITsupport
[admin]
Network=176.55.0.0
Mask=255.255.0.0
ConnectionEntry=Administration
[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
[LOG.FIREWALL]
LogLevel=1
[LOG.CLI]
LogLevel=1
[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 if it exists, 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.	Does not appear in GUI
IncompatibleGinas	Lists Graphical Identification and Authentication dynamic link libraries (GINA.DLLs) that are not compatible 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. The VPN Client goes into fallback mode only if RunAtLogon = 1. Otherwise, the Client gina is never installed. (See "Installing the VPN Client Without User Interaction".	After the keyword and equal sign, enter the name(s) of the GINAs, separated by commas. For example: IncompatibleGinas= PALgina.dll, Yourgina.dll, Theirgina.dll Do not enclose the name in quotes.	Does not appear in GUI
MissingGroupDialog	Controls the pop up window warning that occurs when a user tries to connect without setting the group name in a preshared connection.	0= Do not show the warning message. 1=Show the warning message.	Does not appear in GUI
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 entrust.ini file if it is in a location that is different from the default.ini file. The default location is the base Windows system directory.	Complete pathname of location	Does not appear in GUI

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

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
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

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%20LOGO FF&rnk=2&src=DHCS_MSPSS_gn_SRCH&SPR=NTW40

.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)
AutoInitiationEnable	Enables auto initiation, which is an automated method for establishing a wireless VPN connection in a LAN environment	0 = Disable 1 = Enable Default = 0	Dialer > Options > Automatic VPN Initiation
AutoInitiationRetry-Interval	Specifies the time to wait, in minutes, before retrying auto initiation after a connection attempt failure.	1 to 10 minutes Default = 1	Dialer > Options > Automatic VPN Initiation

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

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
AutoInitiationList	Identifies auto initiation-related section names within the vpnclient.ini file. Each section contains a Network, Mask, and ConnectionEntry. The Network and Mask values identify a subnet. The ConnectionEntry identifies a connection entry profile (.pcf) file. The vpnclient.ini file can contain a maximum of 64 entries.	A list of section names separated by commas; for example: SJWLAN, RTPWLAN, CHWLAN	Does not appear in GUI
[*section name*] (of an item in the AutoInitiationList)	Identifies the network address, subnet mask, and connection entry name for an item in the AutoInitiationList	Network = *IP address* Mask = *Subnet mask* ConnectionEntry = name of a connection entry (profile). Example: [SJWLAN] Network=110.110.110.0 Mask=255.255.0.0 ConnectionEntry=SantaJuan ita WirelessLAN	Does not appear in GUI
OutlookNotify	Controls Microsoft Outlook to Microsoft Exchange polling. In MS Outlook 2000, if Outlook is polling and synchronizing at the same time, Outlook hangs. If you prefer synchronization over new mail notifications, disable this parameter.	0 = Disable 1 = Enable Default = 1	Does not appear in GUI
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

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

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
[LOG.IPSEC]	Identifies the IPSEC class for setting the logging level.	[LOG.IPSEC] Enter exactly as shown.	Log Viewer > Options > Filter
[LOG.FIREWALL]	Identifies the FWAPI class for setting the logging level.	[LOG.FIREWALL] Enter exactly as shown	Log Viewer > Options > Filter
[LOG.CLI]	Identifies the CLI class for setting the logging level.	[LOG.CLI] Enter exactly as shown	Log Viewer > Options > Filter
LogLevel=	Determines the log level for individual classes that use logging services. By default, the log level for all classes is Low. 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.	Does not appear in GUI
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. If matching by IPSec group in 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

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

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
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
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`	Does not appear in GUI
[ApplicationLauncher]	(No VPN Client field) Required keyword to identify Application Launcher section.	`[ApplicationLauncher]` Enter exactly as shown, as first entry in the section.	Does not appear in GUI
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	*command string* Maximum 512 alphanumeric characters. Example: `c:\auth\swtoken.exe.`	Options> Application Launcher> Application

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

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
`[DNS]`	(No VPN Client field) Required keyword to identify DNS section.	`[DNS]` Enter exactly as shown, as first entry in the section.	Does not appear in GUI
`AppendOriginalSuffix=`	Determines the way the VPN Client treats suffixes to domain names. See "DNS Suffixes and the VPN Client (Windows 2000 and Windows XP Only)", following this table.	1= append the primary DNS suffix to the suffix that the VPN Concentrator supplies. 2= append the primary and connection-specific DNS suffixes to the suffix that the VPN Concentrator supplies.	Does not appear in GUI

DNS Suffixes and the VPN Client (Windows 2000 and Windows XP Only)

When a command or program such as **ping server123** passes a hostname without a suffix to a Windows 2000 or Windows XP platform, Windows 2000/XP has to convert the name into a fully-qualified domain name (FQDN). The Windows operating system has two methods for adding suffixes to domain names: Method 1 and Method 2. This section describes these two methods.

Method 1—Primary and Connection-Specific DNS Suffixes

A primary DNS suffix is global across all adapters. A connection-specific DNS suffix is only for a specific connection (adapter), so that each connection can have a different DNS suffix.

Identifying a Primary DNS Suffix

A primary suffix comes from the computer name. To find or assign a primary DNS suffix, use the following procedure according to your operating system:

On Windows 2000

Step 1   On a Windows 2000 desktop, right click the **My Computer** icon, and select **Properties** from the menu.

The System Properties dialog displays.

Step 2   Open the **Network Identification** tab.

The entry next to `Full Computer Name` identifies the computer's name and DNS suffix on this screen, for example, `SILVER-W2KP.tango.dance.com`. The part after the first dot is the primary DNS suffix, in this example: `tango.dance.com`.

Step 3   To change the primary DNS, click **Properties** on the Network Identification tab.

The Identification Changes dialog displays.

Step 4   Click **More...**.

This action displays the DNS Suffix and Net BIOS Computer Name dialog. The `Primary DNS suffix of this computer` entry identifies the primary suffix. You can edit this entry.

On Windows XP

Step 1   Right click **My Computer**, and select **Properties** from the menu.

The System Properties dialog displays.

Step 2   Open the **Computer Name** tab.

The entry next to *Full Computer Name* identifies the computer's name and DNS suffix on this screen (for example, SILVER-W2KP.tango.dance.com). The part after the first dot is the primary DNS suffix (in this example: tango.dance.com).

Step 3   To change the primary DNS, click **Change** on the Computer Name tab.

The Computer Name Changes dialog displays.

Step 4   Click **More...**.

This action displays the DNS Suffix and Net BIOS Computer Name dialog. The Primary DNS suffix of this computer entry identifies the primary suffix. You can edit this entry.

Identifying a Connection-Specific DNS Suffix

You can identify a connection-specific DNS suffix in one of two ways.

1. The connection-specific DNS value is listed as the DNS suffix for the selected connection on the Advanced TCP/IP Settings dialog.

Note   The following instructions are for a Windows 2000 platform. There may be slight variations on a Windows XP platform.

To display the Advanced TCP/IP Settings dialog, use the following procedure:

Step 1   Right click the **My Network Places** icon to display the Properties dialog, which lists your connections.

Step 2   Double-click on a connection (for example, **local**) to display its Properties dialog. The connection uses the checked components, such as those shown in Figure 2-1, which shows components of a connection named Local Area Connection.

Figure 2-1   Displaying Properties for a Connection
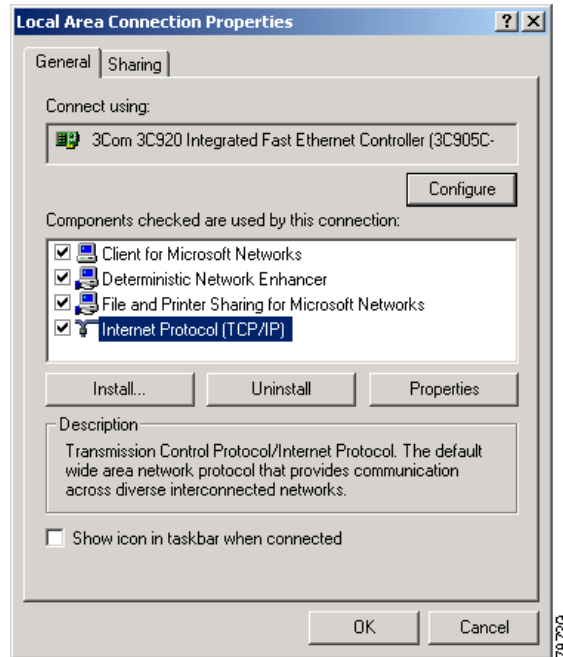
Step 3   Double-click **Internet Protocol (TCP/IP)** to reveal its properties.

Step 4   Select **Advanced**.

Step 5   Display the **DNS** tab and look at `DNS suffix for this connection` box. If the box is empty, you can have it assigned by the DHCP Server.

    a. To identify the connection-specific suffix assigned by the DHCP Server, use the **ipconfig /all** command (Alternative 2, below) and for the DNS Server address.

---

    2. The connection-specific DNS value is listed in the output from the **ipconfig /all** command, executed at the command-line prompt. Look under Windows 2000 IP Configuration for `DNS Suffix Search List`. Under Ethernet Adapter Connection Name, look for `Connection-specific DNS Suffix`.

Method 2—User Supplied DNS Suffix

For this method, you can provide specific suffixes. You can view and change suffixes in the DNS tab of the connection properties page. The Append these DNS suffixes (in order) edit box supplies the name that you can edit. The values you provide here are global to all adapters.

VPN Client Behavior

When the VPN Client establishes a VPN tunnel to the VPN central device (for example, the VPN 3000 Concentrator), the VPN Client uses Method 2 without regard for the method that the Windows platform uses. If the Windows platform is using Method 2, the VPN Client appends the suffix provided by the VPN central device. This is the default behavior and works correctly with no problem

However if Windows is using Method 1, the VPN Client does not append the primary or connection-specific suffix. To fix this problem, you can set the AppendOriginalSuffix option in the vpnclient.ini file. In Table 2-1, the [DNS] section contains this option:

[DNS]

AppendOriginalSuffix Option=1:

In this case, the VPN Client appends the primary DNS suffix to the suffix provided by the VPN Concentrator. While the tunnel is established, Windows has two suffixes: one provided by the VPN Concentrator and the primary DNS suffix.

AppendOriginalSuffix Option=2:

In this case, the VPN Client appends the primary and connection-specific DNS suffixes to the suffix provided by the VPN Concentrator. While the tunnel is established, Windows has three suffixes: one provided by the VPN Concentrator, the primary DNS suffix, and the connection-specific DNS suffix.

Note   If Windows is using Method 2, adding these values to the vpnclient.ini file has no effect.

The VPN Client sets these values every time a tunnel is established and then restores the original configuration when tearing down the tunnel.

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 2-2.

Figure 2-2   List of .pcf files
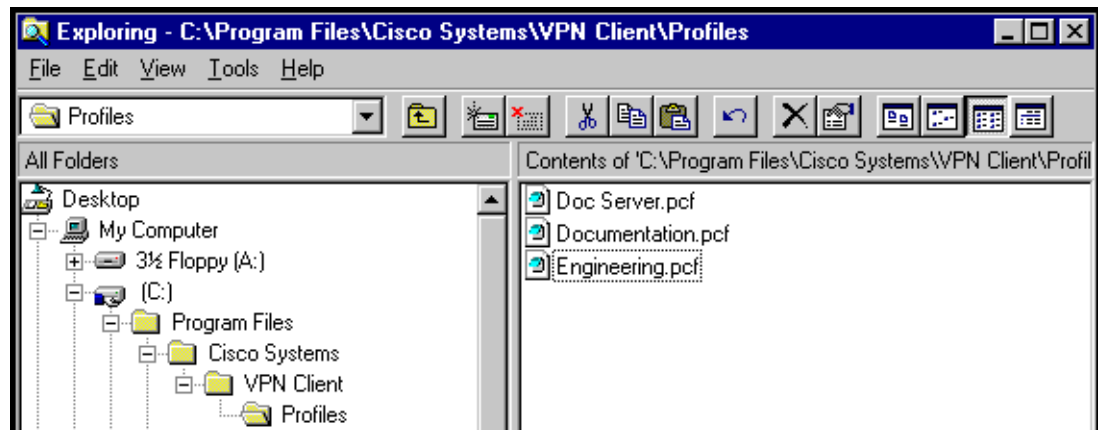
Features Controlled by Connection Profiles

A connection profile (.pcf file) controls the following features.

- Description of the connection profile
- The remote server address
- Authentication type
- Name of IPSec group containing the remote user
- Group password
- Connecting to the Internet via dial-up networking
- Type of dial-up networking connection
- Dial-Up networking phone book entry for Microsoft
- Command string for connecting through an ISP
- Name of remote user
- Remote user's password
- NT domain
- Backup servers
- Split DNS
- Logging on to Microsoft Network and credentials
- Transparent tunneling
- TCP tunneling port
- Allowing of local LAN access
- Enabling of IKE and ESP keepalives
- Setting of peer response timeout
- Certificate parameters for a certificate connection
- Setting of certificate chain
- Diffie-Hellman group
- Verification of the DN of a peer certificate

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=0
MSLogonType=0
EnableNat=1
EnableLocalLAN=0
TunnelingMode=0
TCPTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName
SendCertChain=0
VerifyCertDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSURE-OU!*"wonderland"
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 "Gathering Information You Need" in the *VPN Client User Guide for Windows*, 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 GUI.

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.	Does not appear in GUI
`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
`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 encypted 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 preshared 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

Table 2-2   .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
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.	*phonebook_name* 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.	*command string* 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
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

Table 2-2   .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
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 9x.	0 = Disable 1 = Enable Default = 1	Options > Properties > General tab
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

Table 2-2   .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
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
TCPTunnelingPort=	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 does not close.	0 = Disable 1 = Enable Default = 0	Does not appear in GUI (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, no certificate The VPN Client GUI ignores a read-only setting on this parameter.	Does not appear in VPN Dialer GUI
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

Table 2-2   .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
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.	Does not appear in VPN Dialer GUI
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.	Does not appear in VPN Dialer GUI
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.	Does not appear in VPN Dialer GUI
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.	0 = disable 1 = enable Default = 0	New > Wizard dialog box 3
VerifyCertDN	Prevents a user from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.	Include any certificate DN values of both subject and issuer: You can use all valid ASCII characters including **-_@<>().,** as well as wildcards. See example:	Does not appear in VPN Dialer GUI

Example: VerifyCertDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSURE-OU!*"wonderland"
CN="ID Cert"—Specifies an exact match on the CN.
OU"Cisco"*—Specifies any OU that contains the string "*Cisco*".
ISSUER-CN!"Entrust"—Specifies that the Issuer CN must not equal "*Entrust*".
Issuer-OU!"wonderland"*—Specifies that the Issuer OU must not contain "*wonderland*".

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
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.	Does not appear in VPN Dialer GUI

Distributing Configured VPN Client Software to Remote 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 *VPN Client User Guide for Windows*.

Step 3   Instruct users to:

a. Install the VPN Client according to the instructions in Chapter 2 of the *VPN Client User Guide for Windows*.

b. Start the VPN Client and follow the instructions in Chapter 5 of the *VPN Client User Guide for Windows*. See the section "Importing a VPN Client Configuration File."

c. Finish configuring the VPN Client according to the instructions in Chapter 3 of the *VPN Client User Guide for Windows*.

d. Connect to the private network, and enter parameters according to the instructions in Chapter 4 of the *VPN Client User Guide for Windows*.

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   Copy the VPN Client software files from the distribution CD-ROM into each directory where you created an vpnclient.ini (global) file and separate connection profiles for a set of users.

Step 2   Prepare and distribute the bundled software.

CD-ROM or network distribution: Be sure the vpnclient.ini 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.

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

Configuring Automatic VPN Initiation

Note   Before you begin, we highly recommend that you read the document "SAFE: Wireless LAN Security in Depth," which you can access at http://www.cisco.com/go/safe. This document analyzes the best practices of implementing security for wireless LANs using VPNs.

Automatic VPN initiation (auto initiation) provides secure connections within an on-site wireless LAN (WLAN) environment through a VPN Concentrator. When auto initiation is configured on the VPN Client, the VPN Client:

- Becomes active immediately when a user starts his/her PC or when the PC becomes active after being on standby or hibernating

- Detects that it is in an on-site wireless LAN environment (has a wireless network card installed, is associated with an access point, and has an IP address defined as requiring auto initiation)

- Establishes a VPN tunnel to the VPN Concentrator defined for its network, prompts the user to authenticate, and allows that user network access

Figure 3-1 depicts a simple network configuration that employs VPN for securing on-site WLANs. The VPN 3000 Concentrators, which may or may not be using load balancing, provide the gateway between the untrusted and the trusted networks. The DHCP Server can be on either side of the VPN 3000 Concentrator. VPN Client users with laptops that have wireless NIC cards can connect through access points (AP) throughout the campus or building and tunnel to the trusted 30.30.30.x network from the untrusted 10.10.10.x network. The network administrator can set this type of scenario up to be largely transparent to the VPN Client user.

Figure 3-1   Auto Initiation Scenario
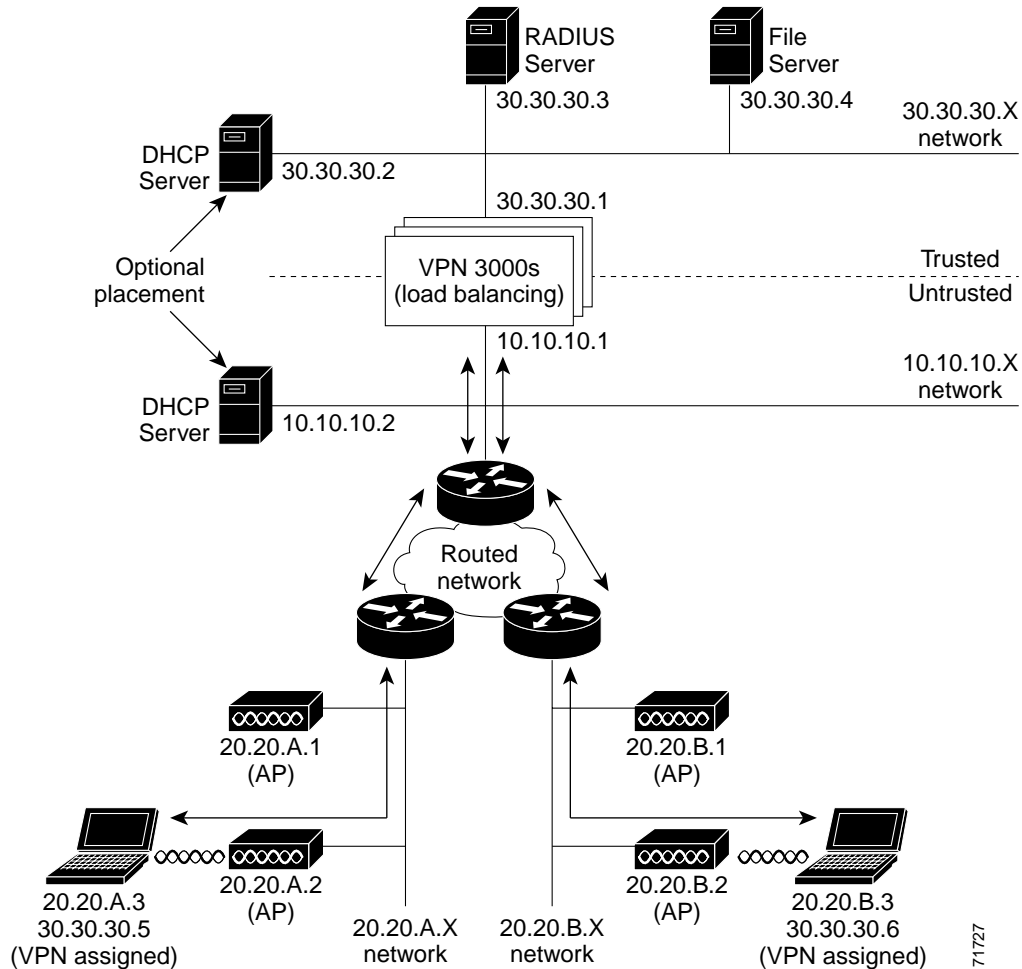
To configure auto initiation for users on the network, you add parameters to the VPN Client's global profile (vpnclient.ini). For information on how to create or use a global profile, see "Creating a Global Profile."

The only configurable features available to the user through the VPN Client GUI application are the ability to disable auto initiation and the ability to change the retry interval. These features are available through the Options menu when auto initiation has been configured through the global profile. If auto initiation is not configured, these options do not appear in the Options menu. When auto initiation is configured, some VPN Client status displays and dialog boxes differ slightly from standard connection dialog boxes to indicate to the user that auto initiation is occurring. For a complete explanation of how auto initiation appears to the VPN Client user, see *Cisco VPN Client User Guide for Windows*, "Using Automatic VPN Initiation."

The auto initiation feature can be used in WLAN environments containing NIC cards and access points from any vendor.

Creating Entries in the vpnclient.ini File

This section shows how to create or edit the vpnclient.ini file to activate auto initiation on a VPN Client.

Preparation

Before you begin, you should gather the information you need to configure auto initiation:

- The network IP addresses for the client network
- The subnet mask for the client network
- The names for all connection entries that users are using for their connections.

What You Have to Do

To configure auto initiation, you must add the following keywords and values in the [Main] section of the vpnclient.ini global profile file:

- AutoInitiationEnable—enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.

- AutoInitiationRetryInterval—specifies the number of minutes to wait before retrying an auto initiation connection. The range is one to ten minutes. If you don't include this parameter in the file, the default retry interval is one minute.

- AutoInitiationList—provides a series of section names, each of which contains a network address, subnet mask, and a connection entry name. The network and subnet mask identify a subnet. The connection entry specifies a connection entry profile (.pcf file). You can include a maximum of 64 section (network) entries.

For example, suppose a sales manager travels among three locations (Chicago, Denver, and Laramie) within a corporation, attending sales meetings, and wants to securely and easily initiate a wireless connection at these locations. The vpnclient.ini contains the entries shown in this example. The connection entry named in each network section points to the individual's profile (.pcf) for that on-site wireless LAN network.

Example 3-1   Section of vpnclient.ini File for Auto Initiation

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=ChicagoWLAN,DenverWLAN,LaramieWLAN
[ChicagoWLAN]
Network=110.110.110.0
Mask=255.255.255.0
ConnectionEntry=Chicago (points to a connection profile named chicago.pcf)
[DenverWLAN]
Network=220.220.220.0
Mask=255.255.255.0
ConnectionEntry=Denver (points to a connection profile named denver.pcf)
[LaramieWLAN]
Network=221.221.221.0
Mask=255.255.255.0
ConnectionEntry=Laramie (points to a connection profile named laramie.pcf)
```

C H A P T E R 4

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 3.6
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows
Running on WinNT

Usage:
vpnclient connect <profile> [user <username>][eraseuserpwd | pwd <password>]
                            [nocertpwd] [notrayicon | sd]
vpnclient disconnect
vpnclient stat [reset] [traffic] [tunnel] [route] [firewall] [repeat]
vpnclient notify
vpnclient verify [autoinitconfig]
```

Starting a Connection—vpnclient connect

To start a connection, enter the following command:

```
vpnclient connect <profile> [user <username>][eraseuserpwd | pwd <password>]
                            [nocertpwd] [notrayicon | sd]
```

Table 4-1 lists the command options you can use with the vpnclient connect command, includes the task that each option performs, and gives an example of each option.

Table 4-1   Command Line Options

option	Definition	Notes and Examples
profile	Name of the connection entry (.pcf file), that you have previously configured. Required.	If the filename contains spaces, enclose it in double quotes on the command line. Example: **vpnclient connect "to work"**
user	Specifies a username for authentication; with the pwd option, suppresses the username prompt in authentication dialog. Optional.	Updates the username in the .pcf file with this name. However, if the name supplied is not valid, the VPN Client displays the authentication dialog on a subsequent request. Example: **vpnclient connect user robron pwd siltango toVPN**
eraseuserpwd	Erases the user password saved on the Client PC thereby forcing the VPN Client to prompt for a password. Optional.	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. Example: **vpnclient connect eraseuserpwd toVPN**
pwd	Specifies a password for authentication; with the user option on the command line, suppresses the password prompt in authentication dialog. Optional.	If the password supplied is not valid, the VPN Client displays the authentication dialog on a subsequent request. After encrypting and using the password for the connection, the VPN Dialer clears the password in the .pcf file. Using this option on the command line compromises security and is not recommended. Example: **vpnclient connect user robron pwd siltango toVPN**
nocertpwd	Suppresses prompting for a certificate password. Optional.	Example: **vpnclient connect nocertpwd toVPN**
notrayicon	Suppresses display of the dialer icon in the Windows system tray (lower right corner of your screen). Optional.	This parameter lets you suppress prompting when the connection is disconnected using the `vpnclient disconnect` command (see "Note on Notrayicon Parameter"). If you use this parameter, you cannot use the sd parameter. Example: **vpnclient connect notrayicon toVPN**
sd	Silent disconnect. Suppresses connection terminating messages, such as "Your IPSec connection has been terminated." Optional.	You can use this parameter to improve the automatic connection process. If you use this parameter, you cannot use the notrayicon parameter. Unlike the notrayicon, the sd option adds the lock icon to the system tray, which provides access to statistics and connection parameters. Example: **vpnclient connect sd towork**

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 first 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.

> **Note**   If you click on the VPN Dialer option in the Cisco System VPN Client list of applications, after you have used the notrayicon on the command line, the lock icon appears on the system tray.

Example 4-1   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 3.6
Copyright <C> 1998-2002 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 4-1   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.
```

Example 4-2   vpnclient connect Command Using Parameters

The following command connects to the remote network without user interaction. Notice that the password appears on the command line in clear text.

```
C:\Program Files\Cisco Systems\VPN Client\vpnclient connect Docserver user ronrob pwd
silvertango
Cisco Systems VPN Client Version 3.6
Copyright <C> 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows, WinNT
Running on: 4.0.1381

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.
```

Displaying a Notification—vpnclient notify

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

```
vpnclient notify
```

Example 4-3   vpnclient notify Command

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 3.6
Copyright <C> 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on:  4.0.1381

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 3.6
Copyright <C> 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on:  4.0.1381

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

Displaying an Automatic VPN Initiation Configuration

To display your configuration for auto initiation, enter the following command:

vpnclient verify autoinitconfig

Note   If the mask in the output display does not match the value in the profile, then the mask is invalid. An invalid mask is displayed as 255.255.255.255

Example 4-4   vpnclient verify Command

The following command shows your auto initiation configuration for three access points.

```
c:\Program Files\Cisco Systems\VPN Client>vpnclient verify autoinitconfig
Cisco Systems VPN Client Version 3.6
Copyright <C> 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows, WinNT
Running on: 4.0.1381

Auto-initiation Configuration Information.
Enable:1
Retry Interval:2
List Entry 0:Network:10.10.10.10
    Mask:255.0.0.0
    Connection Entry:"SalesA"
List Entry 1:Network:20.20.20.20
    Mask:255.0.0.0
    Connection Entry:"SalesB"
List Entry 2:Network:30.30.30.30
    Mask:255.0.0.0
    Connection Entry:"SalesC"
```

Ending a Connection—vpnclient disconnect

To disconnect from your session, enter the following command:

```
vpnclient disconnect
```

Example 4-5   vpnclient disconnect Command

The following command disconnects you from your secure connection.

```
C:\Program Files\Cisco Systems\VPN Client\vpnclient disconnect
Cisco Systems VPN Client Version 3.6
Copyright <C> 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type<s>: Windows
Running on:  4.0.1381

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:

reset	Restarts all connection counts from zero. SA stats are not reset.
traffic	Displays a summary of bytes in and out, packets encrypted and decrypted, packets bypassed, and packets discarded.
tunnel	Displays IPSec tunneling information.
route	Displays configured routes.
firewall	Identifies the type of filewall in use and displays information generated by the firewall configuration.
repeat	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. For more information on statistical output, see *VPN Client User Guide for Windows*.

Example 4-6   vpnclient stat Command

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

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient stat
Cisco Systems VPN Client Version 3.6 (int_67)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 4.0.1381

IPSec tunnel information.
Connection Entry: Engineering
Client address: 200.200.100.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled
Personal Firewall: Cisco Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)

VPN traffic summary.
Time connected: 0 day(s), 00:00.37
Bytes in: 480
Bytes out: 1008
Packets encrypted: 8
Packets decrypted: 8
Packets bypassed: 22
Packets discarded: 0

Configured routes.
Secured      Network Destination    Netmask                    Bytes
   *         10.10.32.32            255.255.255.255            1072
   *         0.0.0.0               0.0.0.0                     0

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
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
```

Example 4-7   vpnclient stat reset Command

The vpnclient stat reset command resets all connection counters.

```
C:\Program Files\Cisco Systems\VPN Client>vpnclient stat reset
Cisco Systems VPN Client Version 3.6 (int_67)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 4.0.1381
```

Example 4-8   vpnclient stat traffic Command

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 3.6 (int_67)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 4.0.1381

VPN traffic summary.
Time connected: 0 day(s), 00:01.17
Bytes in: 720
Bytes out: 1512
Packets encrypted: 12
Packets decrypted: 12
Packets bypassed: 24
Packets discarded: 0
```

Example 4-9   vpnclient stat tunnel Command

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

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient stat tunnel
Cisco Systems UPN Client Version 3.6 (int_67)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 4.0.1381

IPSec tunnel information.
Connection Entry: Engineering
Client address: 200.200.100.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled
Personal Firewall: Cisco Integrated Client
Firewall Policy: Centralized Protection Policy (CPP)
```

Example 4-10   vpnclient stat route Command

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

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient stat route
Cisco Systems UPN Client Version 3.6 (int_67)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 4.0.1381

Configured routes.
Secured     Network Destination     Netmask                 Bytes
    *       10.10.32.32             255.255.255.255          1904
    *       0.0.0.0                 0.0.0.0                  3279

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
```

Example 4-11   vpnclient stat firewall Command

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

```
C:\Program Files\Cisco Systems\UPN Client>vpnclient stat firewall
Cisco Systems UPN Client Version 3.6 (int_67)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 4.0.1381

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
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.

Return Code	Message	Meaning
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.
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 sd 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
```

5

Customizing 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 customize 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. Cisco supplies an oem.ini template for you to customize.

- 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. (InstallShield only)

- wizard.bmp—a bitmap that displays Connection Wizard. Applicable only to InstallShield installation.

- For Microsoft Windows Installer (MSI), a transform that you supply. Cisco supplies a transform template (oem.mst) for you to customize.

$\begin{smallmatrix}&&\\&&\end{smallmatrix}$

Note The VPN Client comes with a zip file containing all of the elements required for customizing the VPN Client for an MSI installation. For instructions for customizing and using the transform, see "Customizing the VPN Client Using an MSI Transform" in this chapter.

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.

Customizing the VPN Client occurs 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 Customizing the VPN Client
- Creating the oem.ini File
- Installing the VPN Client Without User Interaction
- Customizing the VPN Client Using an MSI Transform

Areas Affected by Customizing the VPN Client

Customizing 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 5-1 shows the setup bitmap that displays as the first screen during installation via InstallShield.

Figure 5-1   Setup Bitmap
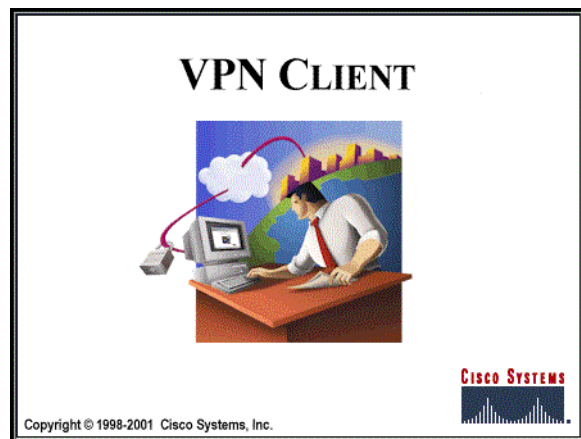
Program Menu Titles and Text

After installation, your organization or company, product, and application names appear in the Cisco Systems VPN Client applications menu. (See Figure 5-2.)

Figure 5-2   Applications menu

Company name — Cisco Systems Inc. VPN Client
Product name
Applications
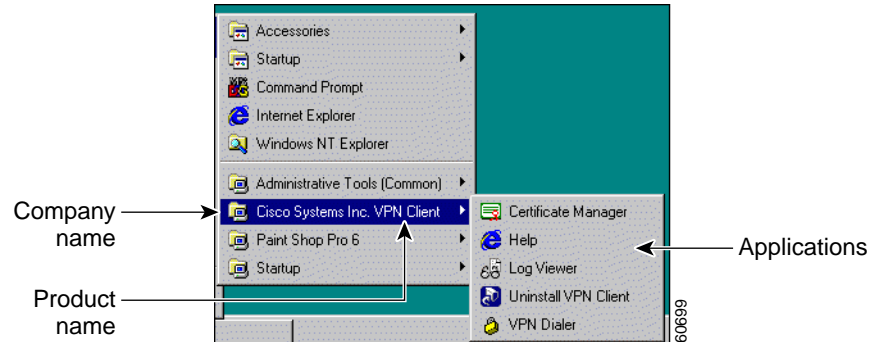
VPN Dialer

Figure 5-3 shows a dialer icon, window title, and dialer logo bitmap that the oem.ini file replaces in the VPN dialer software.

Figure 5-3   Three Types of Branding Changes

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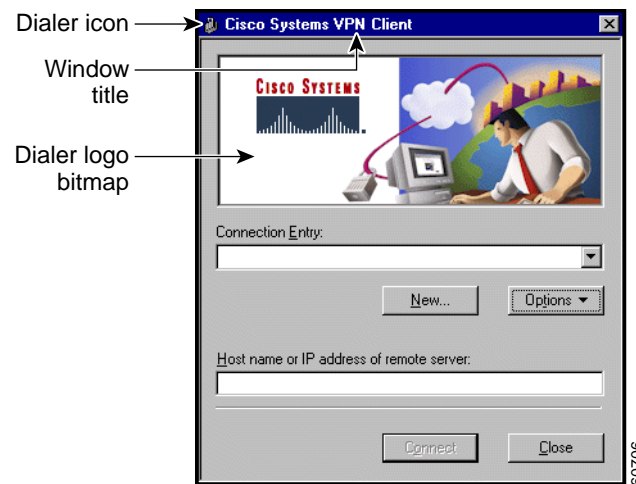
When you click the icon in the title line and select **About Cisco Systems VPN Client**, you see information about the copyright and version number of the VPN Client. The oem.ini file replaces the window title and the icon. Also the window displays (OEM) when you are using the OEM version of the client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

Window Titles and Text

Figure 5-4 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 5-4   Window Titles in a Dialog Box

Company name in dialog box → **Cisco Systems VPN Client**

Product name in dialog box → **Split Tunneling Enabled**

Disconnect   Continue

60703
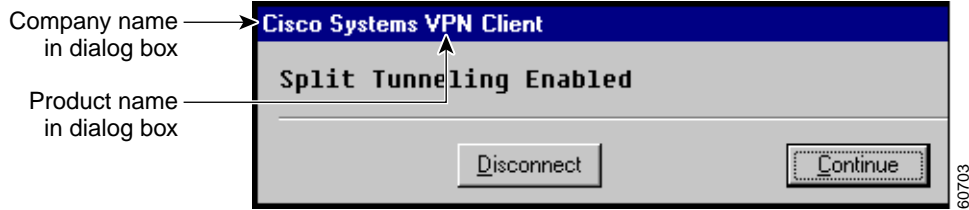
Bitmaps

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

Figure 5-5   Connection Wizard Dialog Box

New Connection Entry Wizard   ✕

CISCO SYSTEMS

Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .

Wizard bitmap →

◉ Group Access Information
Name:
Password:
Confirm Password:

○ Certificate
Name: Aliice (Cisco)
Validate Certificate...

< Back   Next >   Cancel   Help

60697

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 5-6). The operating system automatically condenses the 32x32 icon to fit the 16x16 size displayed on window titles and the system tray. (See Figure 5-3 and Figure 5-7.)

Figure 5-6   Dialer Icon on User Authentication Window

Dialer main icon ———→

User Authentication for Engineering

The remote peer requires additional user authentication to authorize this connection.

Username:
jsmith

Password:
****

☐ Save Password

OK

60684
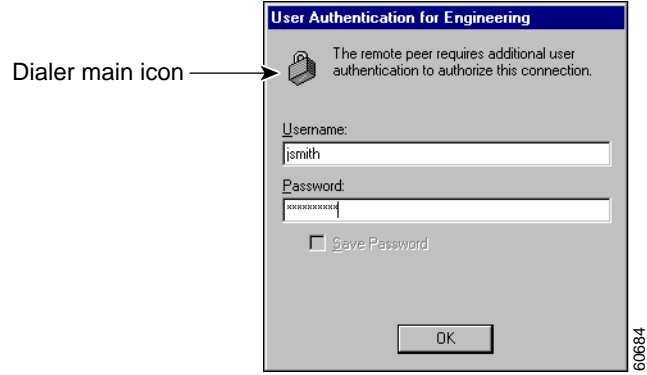
The smaller icon on the system tray appears at the bottom right section of your screen.

Figure 5-7   Icon on System Tray

←——— Main icon

Four icons display while the VPN Dialer is connecting to VPN device. (See Figure 5-8 to Figure 5-11.)

Figure 5-8   Start of Negotiation

Icon at start of ———→
negotiation
(frame 0)

User Authentication for Engineering

The remote peer requires additional user authentication to authorize this connection.

60702

Figure 5-9   First Change

Icon at next stage ———→
of negotiation
(frame 1)

Connecting to 10.10.32.32

Negotiating security profiles...

Cancel

60689
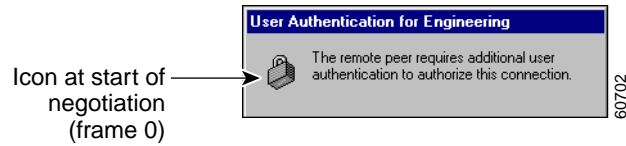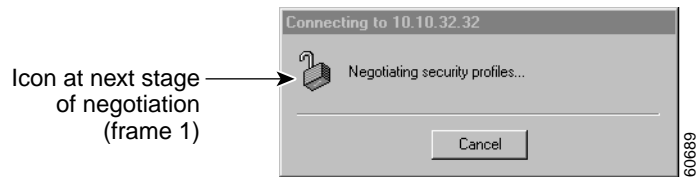
Figure 5-10   Second Change

Icon changes to ———→
show negotiation
is continuing
(frame 2)

Connecting to 10.10.32.32

Negotiating security profiles...

Cancel

60690

Figure 5-11   Third Change

Icon near end
of negotiation
(frame 3)
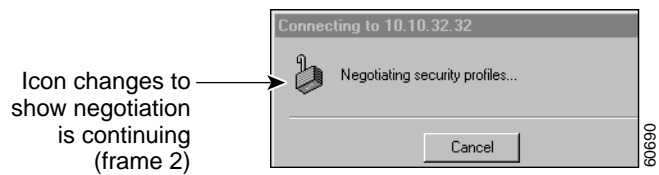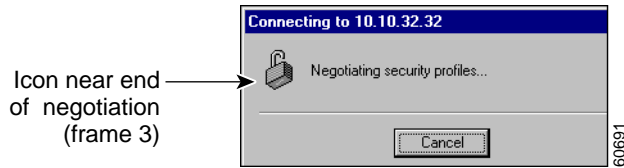
Log Viewer

The Log Viewer section of the oem.ini file replaces the icon used in the Log Viewer application (Figure 5-12). You can also replace the name of the application.

Figure 5-12   Log Viewer Icon

Log viewer
main icon

Certificate Manager

The Certificate Manager section of the oem.ini file replaces the icon used in the Certificate Manager application. (See Figure 5-13.) You can also replace the name of the application.

Figure 5-13   Certificate Manager Icon

Certificate Manager
main icon
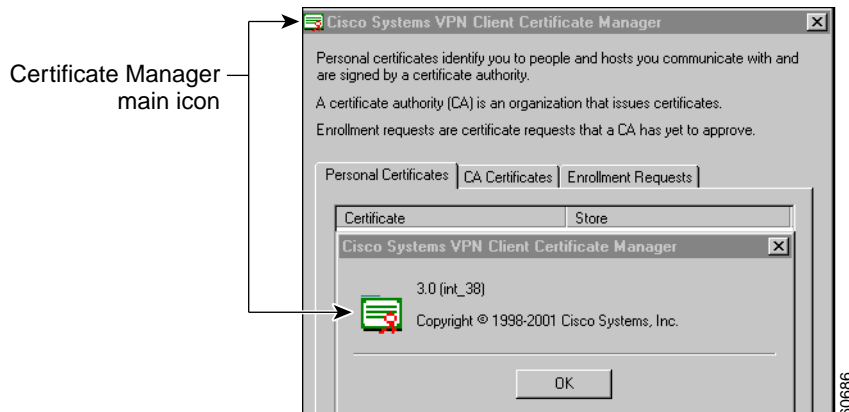
Additional Bitmap—setup.bmp

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.

Creating the oem.ini File

Your distribution CD must contain the oem.ini file for customizing. The oem.ini file contains the locations and names of bitmaps, icons, window titles, and screen text needed for customizing, 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 5-1.

> **Note**   You can edit the oem.ini file that Cisco Systems supplies.

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 determines whether kerberos uses TCP or UDP (the default).

[Main]
DisableKerberosOverTCP = 1

; 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 = wumainicon.ico
MainIconX = RedXLocked.ico
MainIconU = YellowUnlocked.ico
MainIconUB = BlueUnlocked.ico
MainIconUG = GreenUnlocked.ico
MainIconUR = RedUnlocked.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
;
; The [Set MTU] section controls the text and icon for the
; Set MTU applications. AppNameText appears on the application
; selection menu and the title screen. MainIcon appears on the window title
; bar.
;
```

```
[Set MTU]
AppNameText = MTU Setter Application
MainIcon = MtuIcon.ico
AutoSetMtu = 1
SetMtuValue = 1300
MTUAdjustmentOverride = 144
```

oem.ini File Keywords and Values

Table 5-1 describes each part of the oem.ini file.

Table 5-1   oem.ini File Parameters

Keyword	Description	Value
`[Main]`	Optional field that identifies a section of the OEM.ini file to address special circumstances.	Keep exactly as shown.
`DisableKerberosOverTCP=`	InstallShield only When installing the VPN Client on Windows, the installation program sets a registry value that forces windows to use Kerberos over TCP instead of UDP, the default. Some NAT devices, such as Linksys, do not support out-of-order IP fragments, which breaks Kerberos. With TCP, fragmentation is not required.	After the keyword and equal sign, enter either 1 or 0. 0 = keep the default, which is to force Kerberos to use TCP. 1 = prevent Kerberos from using TCP.
`[Brand]`	Required field that identifies 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=`	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.
`ProductText=`	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 that identifies 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=`	Identifies the vertical graphic that appears on the side of some VPN Client windows, the Connection Wizard dialog box. (See Figure 5-5.) 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=`	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.

Table 5-1   oem.ini File Parameters (continued)

Keyword	Description	Value
SilentMode=	InstallShield only Specifies whether 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=	InstallShield only 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: *root:\programs\company\product*
DefGroup=	InstallShield only 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: *foldername*
Reboot=	InstallShield only Specifies 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 that identifies 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=	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=	Identifies the dialer bitmap (shown in Figure 5-3.) The dimensions of this bitmap are 298x116 pixels; 256 colors.	After the keyword and equal sign, enter the name of the dialer bitmap file.
MainIcon=	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 5-6 and Figure 5-7.) 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 system tray uses the 16x16 size. You need to create only the 32x32 size.

For examples of following five icons, see *Cisco VPN Client User Guide for Windows*, Chapter 4, "Using Automatic VPN Initiation."

Table 5-1   oem.ini File Parameters (continued)

Keyword	Description	Value
MainIconX=	Identifies the yellow, locked padlock with a red X over it, representing the disconnecting of an existing connection.	After the keyword and equal sign, enter the name of the icon file. The system tray uses the 16x16 size.
MainIconU=	Identifies the unlocked yellow padlock, representing suspended auto initiation.	After the keyword and equal sign, enter the name of the icon file. The system tray uses the 16x16 size.
MainIconUB=	Identifies the unlocked blue padlock, representing suspended auto initiation but with the dialer window showing.	After the keyword and equal sign, enter the name of the icon file. The system tray uses the 16x16 size.
MainIconUG=	Identifies the unlocked green padlock, representing that auto initiation is in process.	After the keyword and equal sign, enter the name of the icon file. The system tray uses the 16x16 size.
MainIconUR=	Identifies the unlocked red padlock, representing that the dialer is disabling auto initiation from the suspended mode.	After the keyword and equal sign, enter the name of the icon file. The system tray uses the 16x16 size.
Frame0Icon=	Identifies the Frame 0 icon file, which is based on the main icon. (See Figure 5-8.) 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=	Identifies the Frame 1 icon file, which is based on the main icon. (See Figure 5-9.) 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=	Identifies the Frame 2 icon file, which is based on the main icon. (See Figure 5-10.) 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=	Identifies the Frame 3 icon file, which is based on the main icon. (See Figure 5-11.) 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	InstallShield only Specifies 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 that identifies the application name and icon for the Log Viewer application.	Keep exactly as shown, as the fourth section of the file.
AppNameText=	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.

Table 5-1   oem.ini File Parameters (continued)

Keyword	Description	Value
MainIcon=	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.
[Certificate Manager]	Required field that identifies the application name and icon for the Certificate Manager application.	Keep exactly as shown, as the sixth section of the file.
AppNameText=	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=	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.
[Set Mtu]	Required field that identifies the section that contains the name of the Set MTU application, the name of the Set MTU icon, and other settings.	Enter exactly as shown.
AppNameText=	Identifies the name of the Set MTU application.	After the keyword and equal sign, enter the name you want to give to this application. The name can contain spaces and is not case sensitive.
MainIcon=	Identifies the icon for the Set MTU 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.
AutoSetMtu=	InstallShield only Identifies whether to automatically set the MTU for all adaptors during installation using the SetMTU- Value.	After the keyword and equal sign, enter a value 0 or 1: 0 = do not set MTU; do not launch. 1 = set MTU and silently launch during installation. This is the default
SetMTUValue=	InstallShield only Identifies the value to be used for all adapters bound to TCP/IP	After the keyword and equal sign, enter a value between 64 and 1500, inclusive. The default = 1300.
MTUAdjustOverride=	InstallShield only; Windows NT-based only. Identifies the DNE MtuAdjustment parameter. This value identifies the amount the NIC's MTU will be reduced.	After the keyword and equal sign, set to a value between 0 and 1300, inclusive. To use the SetMTU application to set the MTU for the TCP/IP protocol, set this parameter to 0.

> **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.

Customizing the VPN Client Using an MSI Transform

This section describes how to customize VPN Client installation using a transform for the MSI. To customize the applications, you need *both* a transform and an oem.ini file.

> ⚠️ **Caution** Do not modify the MSI file. To customize MSI, use a transform. Failure to follow recommended procedure will limit the level of support you can expect from Cisco.

Creating the Transform

To create the transform, you edit the vpnclient_en.msi file. You can create the transform with any commercially available MSI installation package, such as Wise or InstallShield. The procedure in this section uses the Microsoft ORCA editor available from the Microsoft Windows Installer SDK. The version used here is from Microsoft Platform SDK November 2001. So before you begin, make sure that ORCA is installed on your system. If you need information on transforms and ORCA, refer to the ORCA documentation.

Here is the procedure:

Step 1   Start ORCA.

Step 2   Select **File > Open** and enter **vpnclient_en.msi**.

Step 3   Select **Transform > Apply Transform** and select **oem.mst**, the transform template.

To customize oem.mst, you modify some of the information you see in the tables. The parts to modify have green change bars on the left side of the row. Figure 5-14 shows a partial oem.mst file.

Figure 5-14   Editing the Tables in a Transform File

Table 5-2 outlines the changes to make in the tables in the oem.mst file. The columns in the table are defined as follows:

- Table Name—the name of the table to edit
- Changes Needed—a list of the changes to make to the table
- Install Requirement—the entries that modify the installation software
- Client Requirement—the entries that modify the way the VPN Client operates at runtime

Table 5-2   Oem.mst Tables

Table Name	Changes Needed	Modifies Install Parameters	Modifies VPN Client Runtime Parameters
Binary	top16—Add your own 500x63 bitmap for the MSI Install side16—Add you own 501x314 bitmap for the MSI Install	Yes for both	No for both
Component	CsCoFile_OemFiles—needed to install icons, bitmaps, and oem.ini file for custom VPN Clients	No	Yes
Directory	INSTALLDIR—Change to your own directory INSTALLDIR2—Change to your own directory Cisco_Systems_VPN_Client—Change to your own folder name	Yes for all	No for all

Table 5-2   Oem.mst Tables (continued)

Table Name	Changes Needed	Modifies Install Parameters	Modifies VPN Client Runtime Parameters
Feature Components	Complete | CsCoFile_OemFiles—needed to install icons, bitmaps, and oem.ini file for custom VPN Clients	No	Yes
File	Add the following files for customizing the VPN Client. For examples, see the oem.mst transform and the oem.ini files. oem.ini Wizard.bmp Dialer.bmp MainIcon.ico frame0.ico frame1.ico frame2.ico frame3.ico logview.ico certmgr.ico setmtu.ico MainIconX.ico MainIconU.ico MainIconUB.ico MainIconUG.ico MainIconUR.ico	No	Yes
Icon	Add the following icon files for customizing the VPN Client. These icons are for shortcuts on the Program Group. For examples, see the oem.mst transform and the oem.ini files. MainIcon.ico logview.ico certmgr.ico setmtu.ico	No	Yes

Table 5-2   Oem.mst Tables (continued)

Table Name	Changes Needed	Modifies Install Parameters	Modifies VPN Client Runtime Parameters
Media	Add the following icon files for customizing the VPN Client. For examples, see the oem.mst transform and the oem.ini files. oem.ini Wizard.bmp Dialer.bmp MainIcon.ico frame0.ico frame1.ico frame2.ico frame3.ico logview.ico certmgr.ico setmtu.ico MainIconX.ico MainIconU.ico MainIconUB.ico MainIconUG.ico MainIconUR.ico	No	Yes
Property	ProductName—Supply company and product names for installation.	Yes	No
	Manufacturer—Change *publisher* in the support information screen under Control Panel > Add/Remove Programs.	No	Yes
	ARPURLINFOABOUT—Change the web page in the support information screen under Control Panel > Add/Remove Programs.	No	Yes
Shortcut	LOG_VIEWER—Change the name and the icon for the Log Viewer application.	No for all	Yes for all
	Certificate_Manager—Change the name and the icon for the Certificate Manager application.		
	Dialer—Change the name and the icon for the VPN Dialer application.		
	SET_MTU—Change the name and the icon for the Set MTU application.		

OEM.INI File and MSI

At run-time, you need an oem.ini file to tell the VPN Client to use custom bitmaps and icons.

Copy your oem.ini file, the custom bitmaps, and the custom icons to your distribution media, for example a CD, placing them in the same directory as the vpnclient_en.msi file. If you use the transform to install the VPN Client, the oem.ini file, bitmaps, and icons, are copied along with the VPN Client files during installation. For a sample oem.ini file, see "Sample oem.ini File." For more information on the oem.ini file, see Table 5-1.

Table 5-3 lists InstallShield-specific control parameters and how to achieve similar results in MSI. The oem.ini file modifies both InstallShield installation parameters and VPN Client runtime parameters. For MSI all oem.ini parameters are required except the installation-time parameters.

Table 5-3   Oem.ini File Keywords and MSI Equivalents

Keyword	MSI Equivalent
DisableKerberosOverTCP=	Transform Table: Property DISABLEKERBEROSOVERTCP
SilentMode=	Executing MSI installation using the /q switch For example: **msiexec /I vpnclient_en.msi /q**
InstallPath=	Transform Table: Directory INSTALLDIR INSTALLDIR2
DefGroup=	Transform Table: Directory Cisco_Systems_VPN_Client
AllowSBLLaunches	Transform Table: Registry registry6 Software\Cisco Systems\VPN Client\Secure | AllowsSBLLaunches
AutoSetMtu=	Transform Table: Property LAUNCHSETMTU
SetMTUValue=	Transform Table: Property SETMTUVALUE
MTUAdjustOverride=	Transform Table: Property DNEMTUADJUSTMENT Windows NT-based only.

Installing the VPN Client using the Edited Transform

To install the VPN Client with the transform oem.mst that you have prepared, execute the following command at the command-line prompt.

msiexec /i vpnclient_en_msi TRANSFORMS=oem.mst

If you want to record errors that might occur during the installation, you can create a log file as follows:

msiexec /i vpnclient_en_msi /l*v! c:oeminstall.log TRANSFORMS=oem.mst

Installing the VPN Client Without User Interaction

This section describes how to produce installation without user interaction for both InstallShield installations and MSI installations. Installing the VPN Client without user interaction is called *silent mode*. In silent mode, no messages or prompts appear on the screen.

Silent Installation Using InstallShield

To implement silent mode with or without customizing the VPN Client applications, 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 5-4   oem.ini File Silent Mode Parameters

.ini parameter (keyword)	Parameter Description	Values
SilentMode=	Identifies whether 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=	Identifies the directory for the client software installation.	After the keyword and equal sign, enter the name of the directory in the suggested format: *root:\programs\organization\product*
DefGroup=	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: *foldername*
Reboot=	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.

Silent Installation Using MSI

To install the VPN Client without dialogs and messages (user interface) displaying on the screen, you can use either of the two following commands on the command line.

msiexec.exe /q [n|b|r|f] /i vpnclient_en.msi

or

vpnclient_en.exe /q [n|b|r|f]

Option	What it Displays
q or **qn**	No user interface. It is advisable to enable logging to determine whether the installation succeeded, since this option eliminates all information including fatal error messages.
qb	The basic user interface, which is a limited progress dialog that Windows Installer generates. It is advisable to enable logging with this option as well.
qr	Reduced user interface, similar to the full user interface option, but includes only a subset of all dialogs. For example, this option displays the welcome, license agreement, destination folder, and start dialogs, but does not let the user change the destination folder.
qf	Full or complete user interface including all dialogs. This is the default setting.

Launching SetMTU with Silent Installation

The SetMTU utility is automatically launched in silent mode with the value of 1300 for all installed adapters. To disable the SetMTU utility during installation, set the LAUNCHSETMTU property on the command-line to 0. To modify the MTU value, set SETMTUVALUE to *value*. To override the DNE MtuAdjuistment parameter, which is set to 0, set DNEMTUADJUSTMENT to *value*.

For example, to disable SetMTU and set the DNE Mtuadjustment to 144, execute the following command:

vpnclient_en.msi LAUNCHSETMTU=0 DNEMTUADJUSTMENT=144

For information on the SetMTU utility, see "Changing the MTU Size."

Installing the VPN Client Without User Interaction

C H A P T E R **6**

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.

This chapter includes the following main topics:

Troubleshooting the VPN Client

Start Before Logon and GINAs

Programmer Notes

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 6-1.

Figure 6-1   System Information Screen on Windows 98
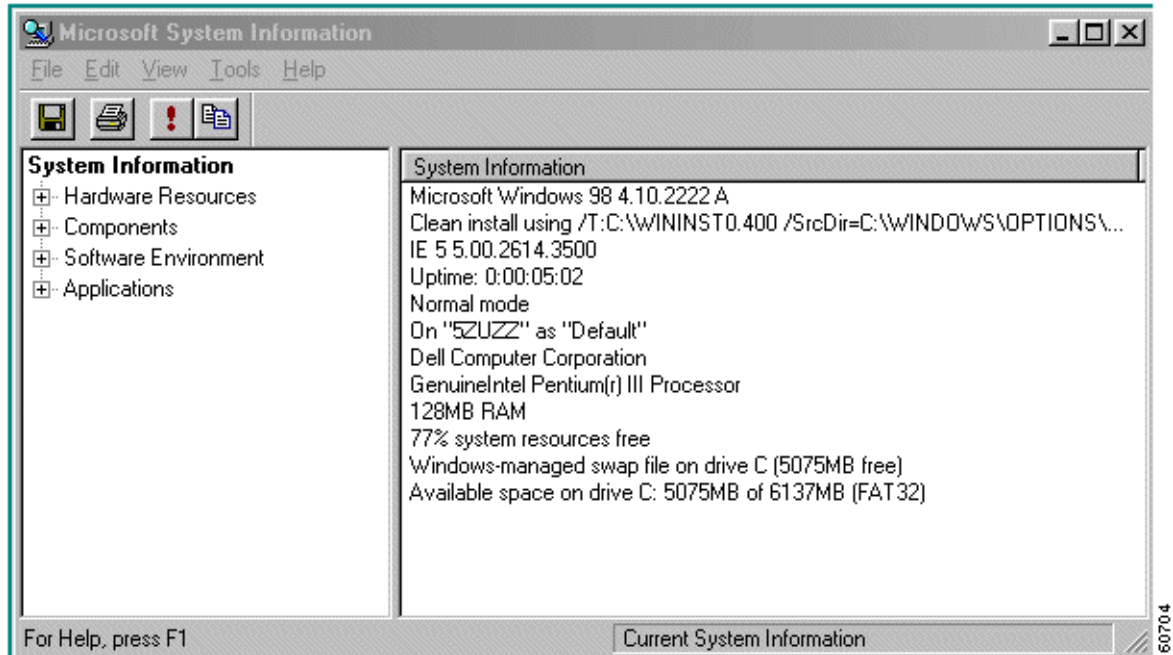
Select a category and the screen displays details for that category. You can then execute the **Export** command and choose a name and destination. Windows creates a text file, which you can attach to an e-mail message and send to the support center.

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:\.
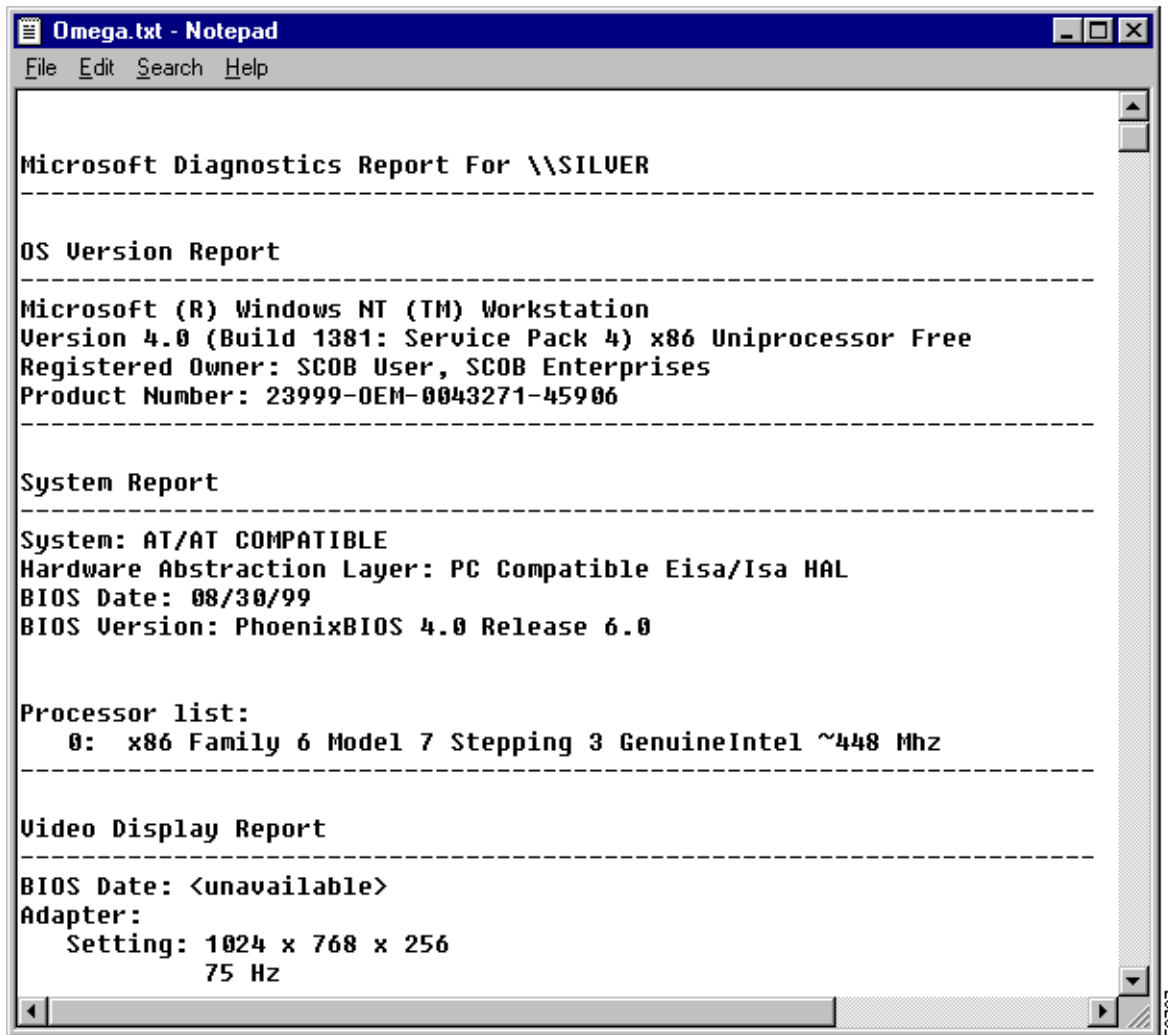
Step 2   Type the following command at the DOS prompt:

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 6-2, which was from a Windows NT system.

Figure 6-2   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 6-1), 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 1300) can increase fragmentation. Using 1300 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 6-3   Setting MTU Size on Windows NT
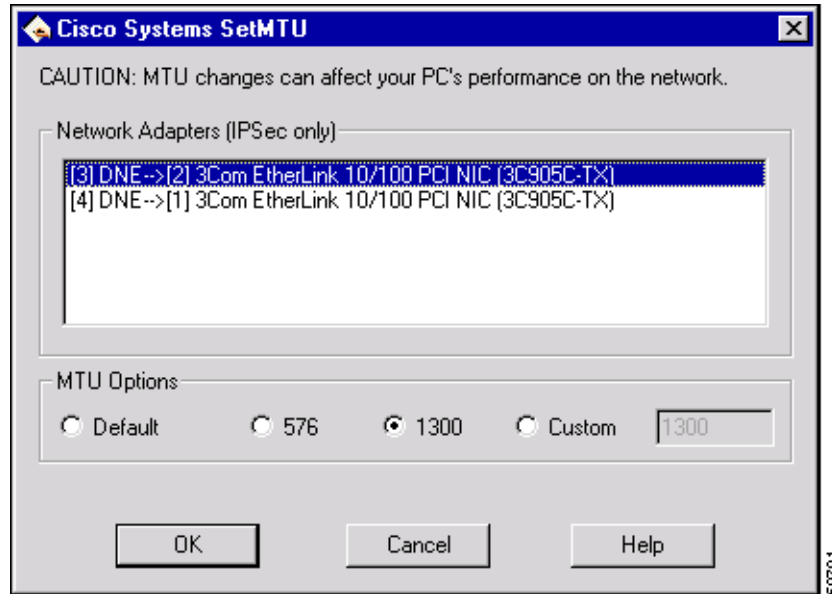
Step 2   Click a network adapter on the list of network adapters.

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.
1300 (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

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 start before logon (SBL) is enabled 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
```

> **Note**   When you enable start before logon for the first time, you must reboot for the system to load csgina.

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 vpnclient.ini file, and the VPN Client refers to the list only during installation. The following entry is an example.

```
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
```

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 vpnclient.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").

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 6-4.) 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 6-4   Cisco Systems VPN Client Registry Entries
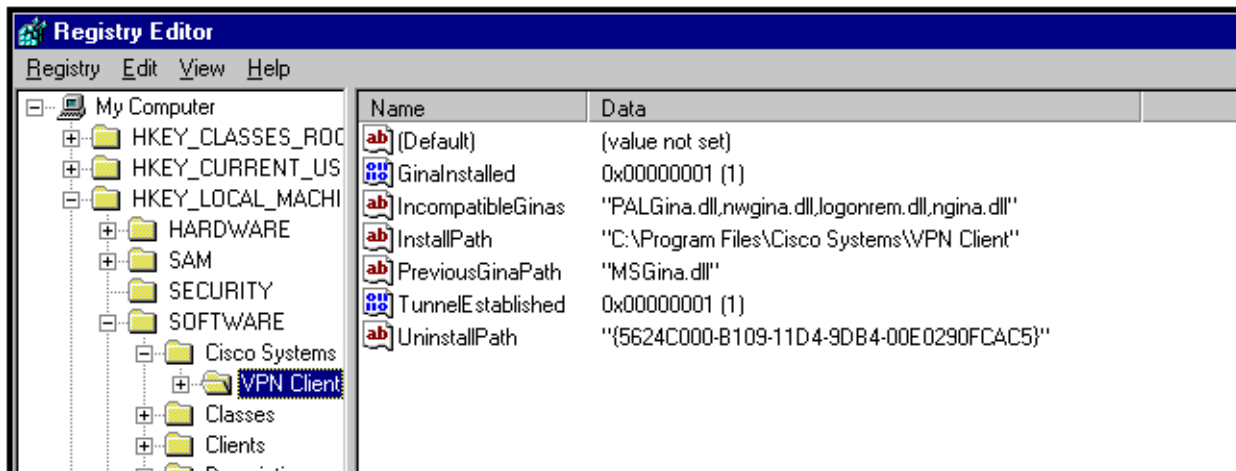
Command Line Switches for ipsecdialer Command

The ipsecdialer command starts a connect from the command line by bringing up the VPN Client GUI application. You can use switches to specify parameters with this command. Table 6-1 lists the switches you can include in the ipsecdialer command and describes the task that each switch performs.

Table 6-1   Command Line Switches

Switch	Parameter	Description
/c	Auto-connect	Starts the VPN Dialer application for the specified connection entry and displays the authentication dialog. Example: **ipesedialer /c towork**
/eraseuserpwd	Erase User Password	Erases the user password saved on the Client PC thereby forcing the VPN Client to prompt for a password. Example:**ipsecdialer /c /eraseuserpwd towork**
/user	Username	Specifies a username for authentication. Suppresses the username prompt in authentication dialog. Updates the username in the .pcf file. You can use this parameter only with the /c switch. Example: **ipsecdialer /c /user robron /pwd siltango towork**
/pwd	Password	Specifies a password for authentication. Suppresses the password prompt in authentication dialog. Updates the password in the .pcf file during authentication and then clears the password from the pcf file. Example: **ipsecdialer /c /user robron /pwd siltango towork**
/sd	Silent disconnect	Suppresses connection terminating messages, such as "Your IPSec connection has been terminated." You can use this parameter to improve the automatic connection process. Example: **ipsecdialer /sd towork**

IKE Proposals

Table 6-2 lists the IKE proposals that the VPN Client supports.

Table 6-2   Valid VPN Client IKE Proposals

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
CiscoVPNClient-3DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-3DES-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	DES-56	Group 2 (1024 bits)
CiscoVPNClient-AES128-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES128-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES192-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-192	Group 2 (1024 bits)
CiscoVPNClient-AES192-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-192	Group 2 (1024 bits)
CiscoVPNClient-AES256-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
CiscoVPNClient-AES256-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
IKE-3DES-MD5	Preshared Keys	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
IKE-3DES-SHA	Preshared Keys	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
IKE-DES-MD5	Preshared Keys	MD5/HMAC-128	DES-56	Group 2 (1024 bits)
IKE-AES128-MD5	Preshared Keys	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
IKE-AES128-SHA	Preshared Keys	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
IKE-AES192-MD5	Preshared Keys	MD5/HMAC-128	AES-192	Group 2 (1024 bits)
IKE-AES192-SHA	Preshared Keys	SHA/HMAC-160	AES-192	Group 2 (1024 bits)
IKE-AES256-MD5	Preshared Keys	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
IKE-AES256-SHA	Preshared Keys	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
CiscoVPNClient-3DES-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-DES-MD5-RSA-DH1	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	DES-56	Group 1 (768 bits)
CiscoVPNClient-AES128-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES128-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES256-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
CiscoVPNClient-AES256-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
CiscoVPNClient-3DES-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
CiscoVPNClient-3DES-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
CiscoVPNClient-AES128-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
CiscoVPNClient-AES128-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
CiscoVPNClient-AES192-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-192	Group 5 (1536 bits)
CiscoVPNClient-AES192-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-192	Group 5 (1536 bits)
CiscoVPNClient-AES256-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-256	Group 5 (1536 bits)
CiscoVPNClient-AES256-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-256	Group 5 (1536 bits)
IKE-3DES-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
IKE-3DES-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
IKE-AES128-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
IKE-AES128-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
IKE-AES256-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
IKE-AES256-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
IKE-DES-MD5-RSA-DH1	RSA Digital Certificate	MD5/HMAC-128	DES-56	Group 1 (768 bits)

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
IKE-3DES-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
IKE-3DES-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
IKE-AES128-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
IKE-AES128-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
IKE-AES192-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-192	Group 5 (1536 bits)
IKE-AES192-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-192	Group 5 (1536 bits)
IKE-AES256-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-256	Group 5 (1536 bits)
IKE-AES256-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-256	Group 5 (1536 bits)

Table 6-3 lists phase 2 proposals that the VPN Client sends.

Table 6-3   Phase 2 Proposals

AES256	MD5	IPCOMPRESSION
AES256	SHA	IPCOMPRESSION
AES128	MD5	IPCOMPRESSION
AES128	SHA	IPCOMPRESSION
AES256	MD5	
AES256	SHA	
AES128	MD5	
AES128	SHA	
3DES	MD5	IPCOMPRESSION
3DES	SHA	IPCOMPRESSION
3DES	MD5	
3DES	SHA	
DES	MD5	IPCOMPRESSION
DES	MD5	
NULL	MD5	
NULL	SHA	

Windows Installer (MSI) Information

This chapter describes how to use the Microsoft Windows Installer for the network administrator. For end user instructions, see *Cisco VPN Client for Windows User Guide*, Chapter 2. For information on customizing the VPN Client applications, see "Customizing the VPN Client Using an MSI Transform." For installing MSI without user interaction, see "Installing the VPN Client Without User Interaction."

This chapter includes the following main topics:

Differences Between InstallShield and MSI

Starting the VPN Client MSI

Logging During Installation

Differences Between InstallShield and MSI

Table 7-1 describes the differences between InstallShield and MSI installation.

Table 7-1   InstallShield and MSI Features Compared

InstallShield	MSI
Usable on all platforms including Windows 9.x	Usable only on Windows NT SP6, Windows 2000, and Windows XP for Release 3.6
Detects and uninstalls an older VPN Client.	Detects but does not automatically uninstall an older VPN Client. Remove previous versions via Add/Remove programs.
Provides a proprietary installation package and customizing process.	Provides a standard installation package and customizing process.
Silent installation suppresses all dialogs and messages, including errors.	Silent installation can be customized to include error reporting.
Provides no automatic rollback when installation fails.	Provides automatic rollback in case of installation failure; undoes changes to the system made during attempted installation.
No automatic replacement of deleted or corrupted files upon first use	Automatic replacement of deleted or corrupted files upon first use. Replaces registry keys associated with shortcuts under Start	Program Files.

Starting the VPN Client MSI

Installing the VPN Client 3.6 via MSI requires Windows Installer version 2.0, which is standard with Windows XP but not with Windows NT 4.0 (SP6) or Windows 2000. When using MSI to install the VPN Client on Windows NT and Windows 2000, the installation application installs or upgrades Windows Installer to version 2.0. This occurs only once.

To install the VPN Client, you must be an administrator.

Alternative Ways to Launch MSI

There are various ways to launch MSI. *Cisco VPN Client User Guide for Windows* explains how to install the VPN Client using an executable that runs a wizard (vpnclient_en.exe). This method automatically installs or upgrades the Windows Installer to version 2.0 if necessary. However, this is only one way to install the application.

Launching MSI via Command Line

If Windows Installer 2.0 is already installed, you can install the VPN Client using the msiexec.exe command on the command line as follows.

msiexec.exe /i vpnclient_en.msi *[options]*

where

/i is the installation switch.

vpnclient_en.msi is the application to be installed.

> **Note** For complete documentation on the msiexec.exe command, see *Windows Installer version 2.0*, Microsoft Platform SDK, August 2001.

Launching MSI via the MSI Icon

If Windows Installer is already installed, you can launch the installation package by double-clicking the MSI icon.

Figure 7-1   MSI icon
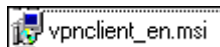
Logging During Installation

To better understand what is happening while MSI is installing the VPN Client, you should initiate logging on the command line by executing the msiexec.exe command with the following options:

msiexec.exe /l [i|w|e|a|r|u|c|m|o|p|v|+|!|*] *logfile*

where:

/l is the switch that turns on logging.

logfile is the name of the file to receive the logging information.

Option	Information Provided
i	Status messages
w	Non-fatal warnings
e	All error messages
a	Start up actions
r	Action-specific records
u	User requests
c	Initial user interface parameters
m	Out-of-memory or fatal exit information
o	Out-of-disk-space messages
p	Terminal properties
v	Verbose output
+	Append to existing file
!	Send each line to the log
*	Log all information except for what the verbose option generates.

Example 7-1   Installing with Logging

The following command installs the VPN Client and includes a log of all information (*v). It also specifies sending each line to the log file (!).

```
msiexec /i vpnclient_en.msi /l*v! vpnclient_msi.log
```

Example 7-2   Installing via the Executable from the Command Line with Logging

The following command installs the VPN Client and logs all information to a log file.

```
vpnclient_en.exe /l*v! vpnclient_msi.log
```

Note   You should always include the ! option for logging, since many of the installer events are not recorded if you do not include this option.

A

B

C