



About This Guide

This *VPN Client Administrator Guide* tells you how to set up selected features of 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 chapters and sections in this manual apply to all platforms supported by the Cisco VPN Client unless otherwise specified.

The VPN Client is a software client that lets users:

- Connect to a Cisco VPN device
- Capture, filter, and display messages generated by the VPN Client software
- Enroll for and manage certificates
- Remove the VPN Client software from the program menu (for InstallShield installation only)
- Manually change the size of the maximum transmission unit (see “[Changing the MTU Size](#)”)

For information about how to use this application, see the *VPN Client User Guide* for your platform.

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

- Cisco VPN 3000 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 system configuration and management for the platform you are administering.

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, 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	Updating VPN Client Software	Describes how to update VPN Client software manually and automatically for all VPN Client platforms.
Chapter 4	Configuring Automatic VPN Initiation	Describes auto initiation and how to configure the vpnclient.ini file for auto initiation.
Chapter 5	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 6	Managing Digital Certificates from the Command Line	Explains how to use the command-line interface (CLI) to manage digital certificates.
Chapter 7	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 <i>silent mode</i> .
Chapter 8	Troubleshooting and Programmer Notes	Lists troubleshooting techniques. Describes how to use the SetMTU application.
Chapter 9	Windows Installer (MSI) Information	Lists the differences between InstallShield and MSI, describes alternative ways to start MSI, explains logging and upgrading.

Related Documentation

This administrator guide is a companion to the following VPN Client user guides:

- *VPN Client User Guide for Windows, Release 4.6*— explains to Windows VPN 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.
- *VPN Client User Guide for Mac OS X, Release 4.6*— explains to Mac VPN Client users how to install the VPN Client for Mac software, configure connection entries, connect to Cisco VPN devices, manage VPN connections, and enroll for digital certificates. The VPN Client on the Macintosh platform can be managed through the GUI or the command-line interface.
- *VPN Client User Guide for Linux and Solaris, Release 4.6*— explains to Linux and Solaris VPN Client users how to install the VPN Client software, configure connection entries, connect to Cisco VPN devices, manage VPN connections, and enroll for digital certificates. The VPN Client on the Linux and Solaris platforms is managed only through the command-line interface.
- 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.
- *Release Notes for the Cisco VPN Client Version 4.6*—includes information relevant to all platforms.

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 Getting Started, Release 4.1* 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 Concentrator Reference Volume I: Configuration, Release 4.1* 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 Concentrator Reference Volume II: Administration and Monitoring, Release 4.1* provides guidelines for administering and monitoring the VPN 3000 Concentrator. It explains and defines all functions available in the Administration and Monitoring screens of the VPN 3000 Concentrator Manager. Appendixes to this manual provide troubleshooting guidance and explain how to access and use the alternate command-line interface.

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

Other References

Other useful references include:

- Cisco Systems, *Dictionary of Internetworking Terms and Acronyms*. Cisco Press: 2001.
- *Virtual Private Networking: An Overview*. Microsoft Corporation: 1999. (Available from Microsoft website.)

- www.ietf.org for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).
- www.whatis.com, a web reference site with definitions for computer, networking, and data communication terms.

Conventions

This document uses the following conventions:

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

Notes use the following conventions:



Note

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

Cautions use the following conventions:



Caution

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

Data Formats

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

Type of Data	Format
IP Addresses	IP addresses use 4-byte dotted decimal notation (for example, 192.168.12.34); as the example indicates, you can omit leading zeros in a byte position.
Subnet Masks and Wildcard Masks	Subnet masks use 4-byte dotted decimal notation (for example, 255.255.255.0). Wildcard masks use the same notation (for example, 0.0.0.255); as the example illustrates, you can omit leading zeros in a byte position.

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

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

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

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOCCD-NA-12XYR or DOCCD-NA-4XYR)) through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

Cisco.com provides a broad range of features and services to help you with these tasks:

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

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

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

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

Cisco TAC Website

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

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

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

<http://tools.cisco.com/RPF/register/register.do>

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

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

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

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

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