



## 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 an IPsec 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
- 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 ASA 5500 Series Adaptive Security Appliance
- Cisco VPN 3000 Series Concentrator
- Cisco Secure PIX Firewall devices
- IOS platform devices, such as the Cisco xxxx 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	<a href="#">Configuration Information for an Administrator</a>	Provides administration information common across all platforms.
Chapter 2	<a href="#">Configuring the VPN Client Using ASDM</a>	Explains how to use ASDM to configure A Cisco Series 5500 Adaptive Security Appliance for VPN Client connections.
Chapter 3	<a href="#">Configuring VPN Client Parameters Using CLI</a>	Explains how to use the ASA command-line interface to configure A Cisco Series 5500 Adaptive Security Appliance for VPN Client connections.
Chapter 4	<a href="#">Configuring the VPN Client on a VPN 3000 Series Concentrator</a>	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 5	<a href="#">Preconfiguring the VPN Client for Remote Users</a>	Shows how to create global and user profiles.
Chapter 6	<a href="#">Updating VPN Client Software on a VPN 3000 Concentrator</a>	Describes how to update VPN Client software manually and automatically for all VPN Client platforms.
Chapter 7	<a href="#">Configuring Automatic VPN Initiation—Windows Only</a>	Describes auto initiation and how to configure the vpnclient.ini file for auto initiation.
Chapter 8	<a href="#">Using the VPN Client Command-Line Interface</a>	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 9	<a href="#">Managing Digital Certificates from the Command Line</a>	Explains how to use the command-line interface (CLI) to manage digital certificates.
Chapter 10	<a href="#">Customizing the VPN Client Software</a>	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> .

<b>Chapter</b>	<b>Title</b>	<b>Description</b>
Chapter 11	<a href="#">Troubleshooting and Programmer Notes</a>	Lists troubleshooting techniques. Describes how to use the SetMTU application.
Chapter 12	<a href="#">Windows Installer (MSI) Information</a>	Describes alternative ways to start MSI, explains logging and upgrading.

## Related Documentation

For the complete list of Cisco VPN Client documentation, see:

[http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html).

The VPN Client Administrator Guide is being updated at this time.

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

- *VPN Client User Guide for Windows, Release 5.0*— 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 5.0.x*—includes information relevant to all platforms.

To view the latest version of the VPN Client documentation on the Cisco Web site, see:

[http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html)

## Cisco ASA 5500 Series Adaptive Security Appliance Documentation

For the complete list of Cisco ASA 5500 Series Adaptive Security Appliance documentation, see:

<http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html>. In each instance, be sure to check the [www.cisco.com](http://www.cisco.com) documentation website for the specific software and documentation version that you are using.

### ASA Version 8.0 Documentation Set



#### Note

See also the ["Cisco ASDM Documentation" section](#).

**Getting Started (5500)**—*Cisco ASA 5500 Getting Started Guide, Software Version 8.0*

[http://www.cisco.com/en/US/docs/security/asa/asa80/getting\\_started/asa5500/quick/guide/5500gsg.html](http://www.cisco.com/en/US/docs/security/asa/asa80/getting_started/asa5500/quick/guide/5500gsg.html)

**Getting Started (5505)**—*Cisco ASA 5505 Getting Started Guide, 8.0*

[http://www.cisco.com/en/US/docs/security/asa/asa80/getting\\_started/asa5505/quick/guide/5505gsg.html](http://www.cisco.com/en/US/docs/security/asa/asa80/getting_started/asa5505/quick/guide/5505gsg.html)

**GUI Configuration**—*ASDM 6.0 User Guide*

<http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/usrguide.html>

**Selected ASDM Configuration Topics**—These documents explain how to use ASDM to configure selected VPN features.

- Clientless SSL VPN Login Screen Advanced Customization  
[http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/selected\\_topics/adv\\_custom.html](http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/selected_topics/adv_custom.html)
- Displaying Multiple Languages to SSL VPN Users  
[http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/selected\\_topics/disp\\_2lang.html](http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/selected_topics/disp_2lang.html)

**CLI Configuration**—*Cisco Security Appliance Command Line Configuration Guide, Version 8.0*  
[http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf\\_gd.html](http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html)

**Command Reference**—*Cisco Security Appliance Command Reference, Version 8.0*  
[http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/cmd\\_ref.html](http://www.cisco.com/en/US/docs/security/asa/asa80/command/reference/cmd_ref.html)

**Syslog Messages**—*Cisco Security Appliance System Log Messages, Version 8.0*  
<http://www.cisco.com/en/US/docs/security/asa/asa80/system/message/syslog.html>

**ASA 8.0 Release Notes**—Release notes for each maintenance release:  
[http://www.cisco.com/en/US/products/ps6120/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6120/prod_release_notes_list.html)

**ASDM 6.0 Release Notes**—Release notes for each maintenance release:  
[http://www.cisco.com/en/US/products/ps6121/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6121/prod_release_notes_list.html)

**Open Source Software Licenses for ASA and PIX Security Appliances, Version 8.0**  
<http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html>

### Cisco ASDM Documentation

ASDM is the graphical user interface for the Cisco ASA 5500 Series Adaptive Security Appliance.



#### Note

The documentation for a given ASDM version includes the feature set for the latest ASA platform version. For example, ASDM Version 6.1 supports ASA Version 8.0 and Version 8.1, so the ASDM guide includes all of the features for ASA Version 8.1. ASA Version 8.0 users do not have a separate guide that includes only Version 8.0 platform features.

## ASDM 6.1 Documentation Set

**Configuration**—*Cisco ASDM User Guide, 6.1*  
[http://www.cisco.com/en/US/docs/security/asdm/6\\_1/user/guide/usergd.html](http://www.cisco.com/en/US/docs/security/asdm/6_1/user/guide/usergd.html)

**Release Notes**—Release notes for each maintenance release:  
[http://www.cisco.com/en/US/products/ps6121/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6121/prod_release_notes_list.html)

## VPN 3000 Series Concentrator Documentation

For the complete list of VPN 3000 Series Concentrator documentation, see:  
[http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/tsd\\_products\\_support\\_eol\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/tsd_products_support_eol_series_home.html)



#### Note

This product is no longer being sold. For additional information, view the End-of-Sale/End-of-Life Notice at  
[http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5743/ps5749/ps2284/prod\\_end-of-life\\_notice0900aecd805cd5a0.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5743/ps5749/ps2284/prod_end-of-life_notice0900aecd805cd5a0.html)

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.

## IOS Documentation

You can find the IOS documentation set at the following URL:

[http://www.cisco.com/en/US/products/ps6350/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6350/tsd_products_support_series_home.html)

## Other References

Other useful references include:

- *Virtual Private Networking: An Overview*. Microsoft Corporation. (Available from Microsoft website.)
- [www.ietf.org](http://www.ietf.org) for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPsec).
- [www.whatis.com](http://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
<b>boldface font</b>	User actions and commands are in <b>boldface</b> .
<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 screen font.
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> in the command-line interface (for example, <b>vpnclient stat</b> ).
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .

**Notes** use the following conventions:



**Note**

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

**Cautions** use the following conventions:



**Caution**

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

## Data Formats

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

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

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

# 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.

## Notices

The following notices pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

