



VPN 3002 Hardware Client Reference, Release 4.7

February 2005

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

Text Part Number: OL-4308-02



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

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

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

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

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

Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)

VPN 3002 Hardware Client Reference, Release 4.7
Copyright © 2005, Cisco Systems, Inc.
All rights reserved.



Preface ix

Prerequisites	ix
Organization	ix
Related Documentation	xi
Documentation conventions	xii
Obtaining Documentation	xiii
Documentation Feedback	xiv
Cisco Product Security Overview	xiv
Obtaining Technical Assistance	xv
Obtaining Additional Publications and Information	xvii

CHAPTER 1

Using the VPN 3002 Hardware Client Manager	1-1
VPN 3002 Hardware Client Browser Requirements	1-1
Connecting to the VPN 3002 Using HTTP	1-2
Installing the SSL Certificate in Your Browser	1-3
Connecting to the VPN 3002 Using HTTPS	1-16
Configuring HTTP, HTTPS, and SSL Parameters	1-16
Logging into the VPN 3002 Hardware Client Manager	1-17
Interactive Hardware Client and Individual User Authentication	1-18
Logging In With Interactive Hardware Client and Individual User Authentication	1-19
Understanding the VPN 3002 Hardware Client Manager Window	1-22
Organization of the VPN 3002 Hardware Client Manager	1-25
Navigating the VPN 3002 Hardware Client Manager	1-26

CHAPTER 2

Configuration	2-1
Configuration	2-1

CHAPTER 3

Interfaces	3-1
Configuration Interfaces	3-1
Configuration Interfaces Private	3-4
Configuration Interfaces Public	3-6

CHAPTER 4

System Configuration 4-1

Configuration | System 4-1

CHAPTER 5

Servers 5-1

Configuration | System | Servers 5-1

Configuration | System | Servers | DNS 5-1

CHAPTER 6

Tunneling 6-1

Configuration | System | Tunneling Protocols 6-2

Configuration | System | Tunneling Protocols | IPSec 6-2

CHAPTER 7

IP Routing 7-1

Configuration | System | IP Routing 7-1

Configuration | System | IP Routing | Static Routes 7-2

Configuration | System | IP Routing | Static Routes | Add or Modify 7-3

Configuration | System | IP Routing | Default Gateways 7-4

Configuration | System | IP Routing | DHCP 7-6

Configuration | System | IP Routing | DHCP Options 7-7

Configuration | System | IP Routing | DHCP Options | Add or Modify 7-8

CHAPTER 8

Management Protocols 8-1

Configuration | System | Management Protocols 8-1

Configuration | System | Management Protocols | HTTP/HTTPS 8-2

About HTTP/HTTPS 8-2

Configuration | System | Management Protocols | Telnet 8-4

Configuration | System | Management Protocols | SNMP 8-6

Configuration | System | Management Protocols | SNMP Communities 8-7

Configuration | System | Management Protocols | SNMP Communities | Add or Modify 8-8

Configuration | System | Management Protocols | SSL 8-10

Configuration | System | Management Protocols | SSH 8-13

Configuration | System | Management Protocols | XML 8-15

CHAPTER 9

Events 9-1

Event Class 9-1

Event Severity Level 9-3

Event Log 9-4

Configuration System Events	9-5
Configuration System Events General	9-5
Configuration System Events Classes	9-8
Configuration System Events Classes Add or Modify	9-10
Configuration System Events Trap Destinations	9-12
Configuration System Events Trap Destinations Add or Modify	9-13
Configuration System Events Syslog Servers	9-14
Configuration System Events Syslog Servers Add or Modify	9-16

 CHAPTER 10
General 10-1

Configuration System General	10-1
Configuration System General Identification	10-2
Configuration System General Time and Date	10-3

 CHAPTER 11
Policy Management 11-1

Configuration Policy Management	11-1
Configuration Policy Management Traffic Management	11-2
Configuration Policy Management Traffic Management PAT	11-6
Configuration Policy Management Traffic Management PAT Enable	11-7
Configuration Policy Management Certificate Validation	11-8

 CHAPTER 12
Administration 12-1

Administration	12-1
Administration Software Update	12-2
Administration System Reboot	12-5
Administration Ping	12-7
Administration Traceroute	12-9
Administration Access Rights	12-10
Administration Access Rights Administrators	12-11
Administration Access Rights Access Settings	12-13
Administration File Management	12-14
Administration File Management Swap Config Files	12-15
Administration File Management Config File Upload	12-16
Certificate Management	12-18
Configuring Digital Certificates: SCEP and Manual Methods	12-18
Managing Certificates with SCEP	12-19

- Enrolling and Installing Certificates Manually 12-24
- Obtaining SSL Certificates 12-31
- Enabling Digital Certificates on the VPN 3002 12-32
- Deleting Digital Certificates 12-33
- Administration | Certificate Management 12-34
- Administration | Certificate Management | Enroll 12-40
- Administration | Certificate Management | Enroll | *Certificate Type* 12-41
- Administration | Certificate Management | Enroll | *Certificate Type* | PKCS10 12-42
- Administration | Certificate Management | *Enrollment or Renewal* | Request Generated 12-45
- Administration | Certificate Management | Enroll | Identity Certificate | SCEP 12-46
- Administration | Certificate Management | Enroll | SSL Certificate | SCEP 12-47
- Administration | Certificate Management | Install 12-49
- Administration | Certificate Management | Install | Certificate Obtained via Enrollment 12-50
- Administration | Certificate Management | Install | *Certificate Type* 12-51
- Administration | Certificate Management | Install | CA Certificate | SCEP 12-52
- Administration | Certificate Management | Install | *Certificate Type* | Cut and Paste Text 12-53
- Administration | Certificate Management | Install | *Certificate Type* | Upload File from Workstation 12-55
- Administration | Certificate Management | View 12-56
- Administration | Certificate Management | Configure CA Certificate 12-60
- Administration | Certificate Management | Renewal 12-61
- Administration | Certificate Management | *Activate or Re-Submit* | Status 12-63
- Administration | Certificate Management | Delete 12-64
- Administration | Certificate Management | Generate SSL Certificate 12-65
- Administration | Certificate Management | Export SSL Certificate 12-66
- Administration | Certificate Management | Generate SSH Host Key 12-68
- Administration | Certificate Management | View Enrollment Request 12-69
- Administration | Certificate Management | Cancel Enrollment Request 12-71
- Administration | Certificate Management | Delete Enrollment Request 12-72

CHAPTER 13

Monitoring 13-1

- Monitoring 13-1
- Monitoring | Routing Table 13-2
- Monitoring | Filterable Event Log 13-3
- Monitoring | Live Event Log 13-6
- Monitoring | System Status 13-8
- Monitoring | System Status | Memory Status 13-12

Monitoring System Status Private/Public Interface	13-14
Monitoring User Status	13-17
Monitoring Statistics	13-18
Monitoring Statistics IPsec	13-19
Monitoring Statistics HTTP	13-25
Monitoring Statistics Telnet	13-28
Monitoring Statistics DNS	13-30
Monitoring Statistics SSL	13-31
Monitoring Statistics DHCP	13-33
Monitoring Statistics SSH	13-35
Monitoring Statistics NAT	13-37
Monitoring Statistics PPPoE	13-39
Monitoring Statistics MIB-II	13-42
Monitoring Statistics MIB-II Interfaces	13-43
Monitoring Statistics MIB-II TCP/UDP	13-45
Monitoring Statistics MIB-II IP	13-48
Monitoring Statistics MIB-II ICMP	13-51
Monitoring Statistics MIB-II ARP Table	13-54
Monitoring Statistics MIB-II Ethernet	13-56
Monitoring Statistics MIB-II SNMP	13-59

 CHAPTER 14

Using the Command-Line Interface 14-1

Accessing the Command-line Interface	14-1
Starting the Command-line Interface	14-2
Using the Command-line Interface	14-3
Menu Reference	14-7

 APPENDIX A

IKE Proposals A-1

Valid IKE Proposals	A-1
---------------------	-----

 APPENDIX B

Troubleshooting and System Errors B-1

Files for Troubleshooting	B-1
LED Indicators	B-2
System Errors	B-3
Settings on the VPN Concentrator	B-5
VPN 3002 Hardware Client Manager Errors	B-5

Command-line Interface Errors **B-10**

INDEX



Preface

The *VPN 3002 Hardware Client Reference* provides guidelines for configuring the Cisco VPN 3002, details on all the functions available in the VPN 3002 Hardware Client Manager, and instructions for using the VPN 3002 Command Line Interface.

Prerequisites

We assume you have read the *VPN 3002 Hardware Client Getting Started* manual and have followed the minimal configuration steps in Quick Configuration. That section of the VPN Hardware Client Manager is not described here.

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

Organization

This manual is organized by the order in which sections appear in the VPN 3002 Hardware Client Manager table of contents (the left frame of the Manager browser window; see [Figure 1-34](#) in [Chapter 1](#), “Using the VPN 3002 Hardware Client Manager.”)

Chapter	Title	Description
Chapter 1	Using the VPN 3002 Hardware Client Manager	Explains how to log in, navigate, and use the VPN 3002 Hardware Client Manager with a browser. It explains both HTTP and HTTPS browser connections, and how to install the SSL certificate for a secure (HTTPS) connection.
Chapter 2	Configuration	Describes the main VPN 3002 Hardware Client Manager configuration screen.
Chapter 3	Interfaces	Explains how to configure the VPN 3002 private and public interfaces.
Chapter 4	System Configuration	Describes the system configuration screen of the VPN 3002 Hardware Client Manager.

Chapter	Title	Description
Chapter 5	Servers	Explains how to configure the VPN 3002 to communicate with DNS servers to convert hostnames to IP addresses.
Chapter 6	Tunneling	Explains how to configure IPSec.
Chapter 7	IP Routing	Explains how to configure static routes, default gateways, and DHCP parameters and options.
Chapter 8	Management Protocols	Explains how to configure built-in VPN 3002 servers that provide management functions: HTTP and HTTPS, Telnet, SNMP, SNMP Community Strings, SSL and SSH.
Chapter 9	Events	Explains how to configure system events such as alarms, traps, error conditions, network problems, task completion, or status changes.
Chapter 10	General	Explains how to configure the system identification, date, and time.
Chapter 11	Policy Management	Explains how to configure and use PAT and Network Extension modes.
Chapter 12	Administration	Explains how to configure and use high-level VPN 3002 administrator activities such as who is allowed to configure the system, what software runs on it, rebooting and shutting down the system, managing its configuration files, and managing X.509 digital certificates.
Chapter 13	Monitoring	Explains the many status, statistics, sessions, and event log screens that you can use to monitor the VPN 3002.
Chapter 14	Using the Command-Line Interface	Explains how to use the built-in menu- and command-line-based administrative management system via the system console or a Telnet session. With the CLI, you can access and configure all the same parameters as you can using the HTML-based VPN 3002 Hardware Client Manager.
Appendix A	IKE Proposals	Identifies and describes all valid IKE proposals for the VPN 3002.
Appendix B	Troubleshooting and System Errors	Describes common errors that may occur while configuring the system, and how to correct them. It also describes all system and module LED indicators.

Related Documentation

Refer to the following documents for further information about Cisco VPN 3000 Series applications and products.

VPN 3002 Hardware Client Documentation

The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is online only.

The *VPN 3002 Hardware Client Quick Start Card* summarizes the information for quick configuration. This quick reference card is provided with the VPN 3002 and is also available online.

The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for quick configuration. It is provided with the VPN 3002 and you can also print it from the online version; you can affix the label to the VPN 3002.

The HTML interface, called the VPN 3002 Hardware Client Manager, includes online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.

VPN 3000 Series Concentrator Documentation

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

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

VPN Client Documentation

The *VPN Client User Guide* explains how to install, configure, and use the VPN Client, which lets a remote client use the IPSec tunneling protocol for secure connection to a private network through the VPN Concentrator.

The *VPN Client Administrator Guide* tells how to configure a VPN Concentrator for remote user connections using the VPN Client, how to automate remote user profiles, how to use the VPN Client command-line interface, and how to get troubleshooting information.

Documentation on VPN Software Distribution CDs

The VPN 3000 Series Concentrator and VPN 3002 Hardware Client documentation are provided on the VPN 3000 Concentrator software distribution CD-ROM in PDF format. The VPN Client documentation is included on the VPN Client software distribution CD-ROM, also in PDF format. To view the latest

versions on the Cisco web site, click the Support icon on the toolbar at the top of the VPN Concentrator Manager, Hardware Client Manager, or Client window. To open the documentation, you need Acrobat® Reader 3.0 or later; version 4.5 is included on the Cisco VPN 3000 Concentrator software distribution CD-ROM and on the VPN Client software distribution CD-ROM.

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.

Documentation conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords 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 screen font.
boldface screen font	Information you must enter is in boldface screen font .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

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.
Filenames	Filenames on the VPN 3002 follow the DOS 8.3 naming convention: a maximum of eight characters for the name, plus a maximum of three characters for an extension. For example, LOG00007.TXT is a legitimate filename. The VPN 3002 always stores filenames in uppercase.
Port Numbers	Port numbers use decimal numbers from 0 to 65535. Commas and spaces are not permitted.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

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 Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.

- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:
<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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



Using the VPN 3002 Hardware Client Manager

The VPN 3002 Hardware Client Manager is an HTML-based interface that lets you configure, administer, monitor, and manage the VPN 3002 with a standard web browser. To use it, you connect to the VPN 3002, using a PC and browser on the same private network with the VPN 3002.

The Manager uses the standard web client / server protocol, HTTP (Hypertext Transfer Protocol), which is a cleartext protocol. However, you can also use the Manager in a secure, encrypted HTTP connection over SSL (Secure Sockets Layer) protocol, known as HTTPS.

- To use a cleartext HTTP connection, see the section, “[Connecting to the VPN 3002 Using HTTP](#).”
- To use HTTP over SSL (HTTPS) with the Manager:
 - The first time, connect to the Manager using HTTP, and
 - Install an SSL certificate in the browser; see “[Installing the SSL Certificate in Your Browser](#).”

When the SSL certificate is installed, you can connect directly using HTTPS; see “[Connecting to the VPN 3002 Using HTTPS](#).”

VPN 3002 Hardware Client Browser Requirements

The VPN 3002 Hardware Client Manager requires either Microsoft Internet Explorer version 4.0 or higher, or Netscape Navigator version 4.5–4.7. For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.



Note

You cannot use the Live Event Log feature with Netscape Navigator version 4.0

JavaScript and Cookies

Be sure JavaScript and Cookies are enabled in the browser. Refer to the documentation for your browser for instructions.

Navigation Toolbar

Do not use the *browser* navigation toolbar buttons Back, Forward, or Refresh/Reload with the VPN 3002 Hardware Client Manager unless instructed to do so. To protect access security, clicking Refresh/Reload automatically logs out the Manager session. Clicking Back or Forward might display stale Manager screens with incorrect data or settings.

We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN 3002 Hardware Client Manager.

Recommended PC Monitor/Display Settings

For optimal use, we recommend setting your monitor or display:

- Desktop area = 1024 x 768 pixels or greater. Minimum = 800 x 600 pixels.
- Color palette = 256 colors or higher.

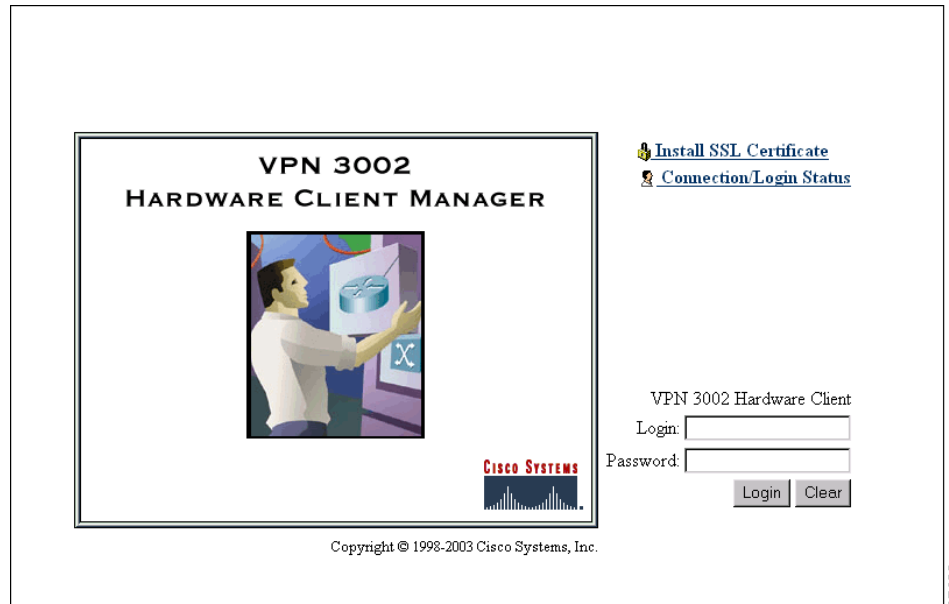
Connecting to the VPN 3002 Using HTTP

When your system administration tasks and network permit a cleartext connection between the VPN 3002 and your browser, you can use the standard HTTP protocol to connect to the system.

Even if you plan to use HTTPS, you use HTTP at first to install an SSL certificate in your browser.

-
- Step 1** Bring up the browser.
- Step 2** In the browser Address or Location field, you can just enter the VPN 3002 private interface IP address; for example, 10.10.147.2. The browser automatically assumes and supplies an http:// prefix.
- The browser displays the VPN 3002 Hardware Client Manager login screen.
-

Figure 1-1 VPN 3002 Hardware Client Manager Login Screen



To continue using HTTP for the whole session, skip to [“Logging into the VPN 3002 Hardware Client Manager.”](#)

Installing the SSL Certificate in Your Browser

The Manager provides the option of using HTTP over SSL with the browser. SSL creates a secure session between your browser (VPN 3002 hardware client) and the VPN Concentrator (server). This protocol is known as HTTPS, and uses the `https://` prefix to connect to the server. The browser first authenticates the server, then encrypts all data passed during the session.

HTTPS is often confused with a similar protocol, S-HTTP (Secure HTTP), which encrypts only HTTP application-level data. SSL encrypts *all* data between client and server at the IP socket level, and is thus more secure.

SSL uses digital certificates for authentication. The VPN 3002 creates a self-signed SSL server certificate when it boots, and this certificate must be installed in the browser. Once the certificate is installed, you can connect using HTTPS. You need to install the certificate from a given VPN 3002 only once.

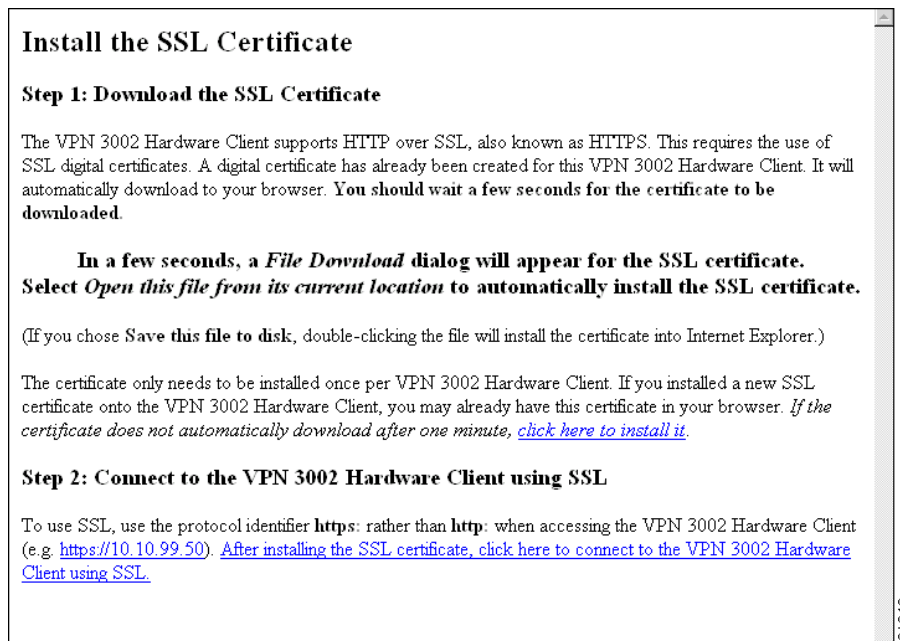
Managing the VPN 3002 is the same with or without SSL. Manager screens might take slightly longer to load with SSL because of encryption/decryption processing. When connected via SSL, the browser shows a locked-padlock icon on its status bar. Both Microsoft Internet Explorer and Netscape Navigator support SSL.

For HTTPS to work on the public interface, you must enable HTTPS on the VPN 3002 through the command-line interface or from an HTTP session on the private interface first.

Follow these steps to install and use the SSL certificate for the first time. We provide separate instructions for Internet Explorer and Netscape Navigator when they diverge.

-
- Step 1** Connect to the VPN 3002 using HTTP as above.
- Step 2** On the login screen, click the **Install SSL Certificate** link.
- The Manager displays the Install SSL Certificate screen and automatically begins to download and install its SSL certificate in your browser.
-

Figure 1-2 Install SSL Certificate Screen



The installation sequence now differs depending on the browser. Continue below for Internet Explorer, or skip to “[Installing the SSL Certificate with Netscape.](#)”

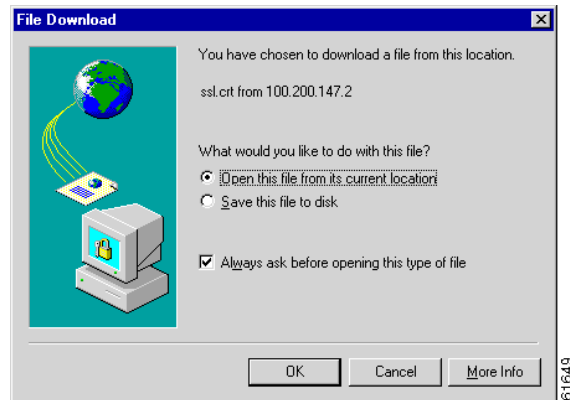
Installing the SSL certificate with Internet Explorer

This section describes SSL certificate installation using Microsoft Internet Explorer 5.0. (With Internet Explorer 4.0, some dialog boxes are different but the process is similar.)

You need to install the SSL certificate from a given VPN 3002 only once. If you do reinstall it, the browser repeats all these steps each time.

A few seconds after the VPN 3002 Hardware Client Manager SSL screen appears, Internet Explorer displays a File Download dialog box that identifies the certificate filename and source, and asks whether to Open or Save the certificate. To immediately install the certificate in the browser, select **Open**. If you **Save** the file, the browser prompts for a location; you must then double-click the file to install it.

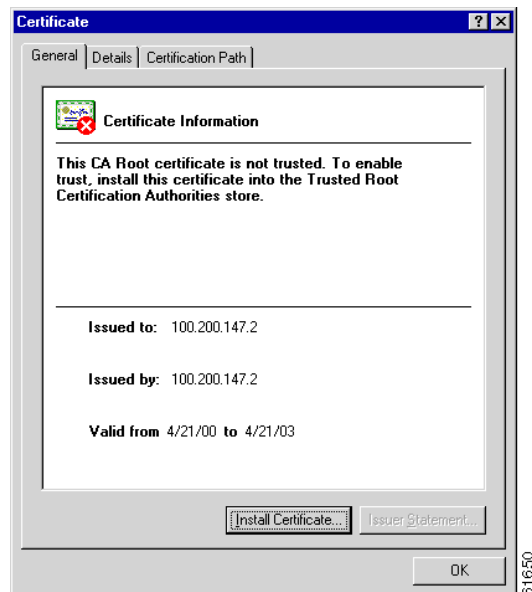
Figure 1-3 Internet Explorer File Download Dialog Box



Step 1 Click the **Open this file from its current location** radio button, then click **OK**.

The browser displays the Certificate dialog box with information about the certificate. You must now install the certificate.

Figure 1-4 Internet Explorer Certificate Dialog Box



Step 2 Click **Install Certificate**.

The browser starts a wizard to install the certificate. The certificate store is where such certificates are stored in Internet Explorer.

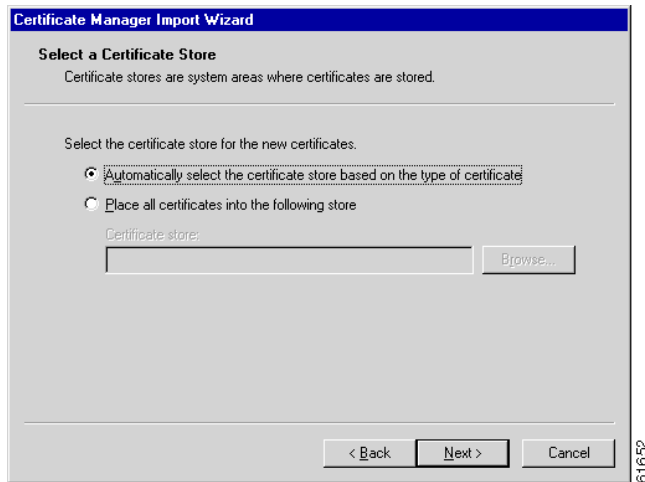
Figure 1-5 Internet Explorer Certificate Manager Import Wizard Dialog Box



Step 3 Click **Next** to continue.

The wizard opens the next dialog box asking you to select a certificate store.

Figure 1-6 Internet Explorer Certificate Manager Import Wizard Dialog Box



Step 4 Let the wizard **Automatically select the certificate store**, and click **Next**.

The wizard opens a dialog box to complete the installation.

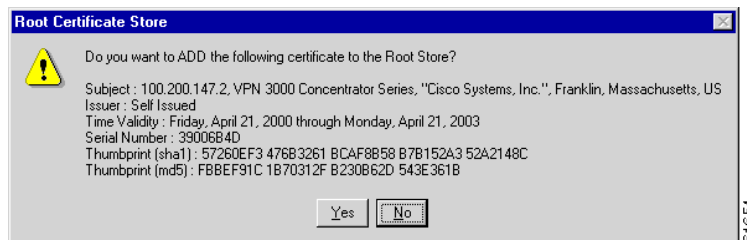
Figure 1-7 Internet Explorer Certificate Manager Import Wizard Dialog Box



Step 5 Click **Finish**.

The wizard opens the Root Certificate Store dialog box asking you to confirm the installation.

Figure 1-8 Internet Explorer Root Certificate Store Dialog Box



Step 6 To install the certificate, click **Yes**. This dialog box closes, and a final wizard confirmation dialog box opens.

Figure 1-9 Internet Explorer Certificate Manager Import Wizard Final Dialog Box



Step 7 Click **OK** to close this dialog box, and click **OK** on the Certificate dialog box (Figure 1-4) to close it. You can now connect to the VPN 3002 using HTTP over SSL (HTTPS).

Step 8 On the Manager SSL screen (Figure 1-2), click the link that says **After installing the SSL certificate, click here to connect to the VPN 3002 Hardware Client using SSL**.

Depending on how your browser is configured, you might see a Security Alert dialog box.

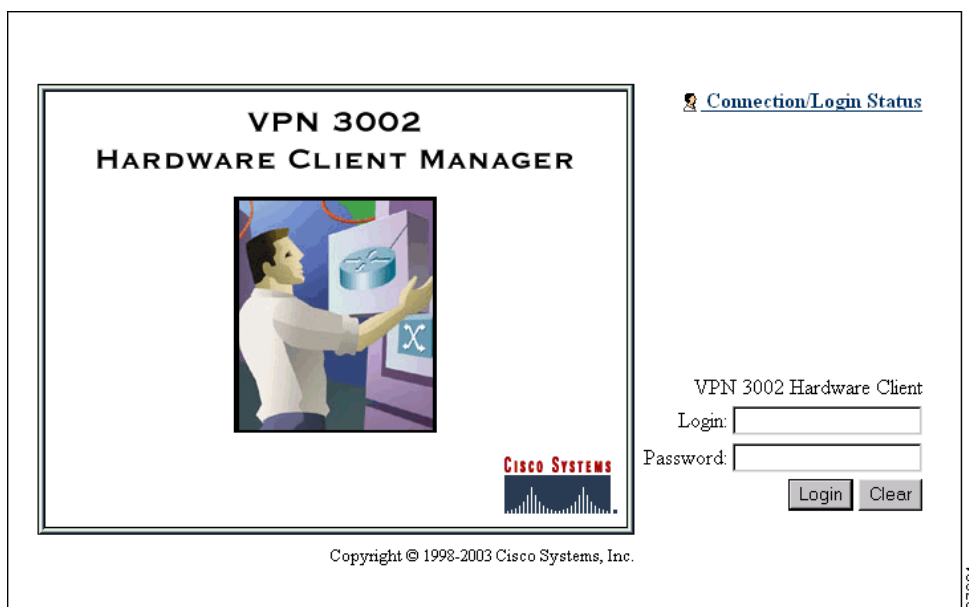
Figure 1-10 Internet Explorer Security Alert Dialog Box



Step 9 Click **OK**.

The VPN 3002 Hardware Client displays the HTTPS version of the Manager login screen.

Figure 1-11 VPN 3002 Hardware Client Manager Login Screen Using HTTPS (Internet Explorer)



The browser maintains the HTTPS state until you close it or access an unsecured site; in the latter case you might see a Security Alert screen.

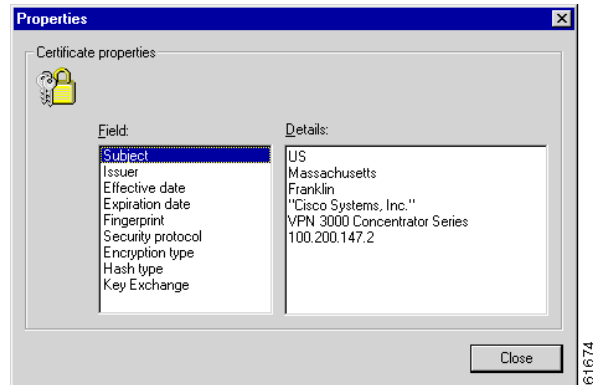
Proceed to [Logging into the VPN 3002 Hardware Client Manager](#) to log in as usual.

Viewing Certificates with Internet Explorer

There are (at least) two ways to examine certificates stored in Internet Explorer.

First, note the padlock icon on the browser status bar in [Figure 1-11](#). If you double-click the icon, the browser opens a Certificate Properties screen showing details of the specific certificate in use.

Figure 1-12 Internet Explorer 4.0 Certificate Properties Screen



Click any of the Field items to see Details. Click **Close** when finished.

Second, you can view all the certificates that are stored in Internet Explorer 4.0. Click the browser **View** menu and select **Internet Options**. Click the **Content** tab, then click **Authorities** in the Certificates section.

In Internet Explorer 5.0, click the browser **Tools** menu and select **Internet Options**. Click the **Content** tab, then click **Certificates** in the Certificates section. On the Certificate Manager, click the **Trusted Root Certification Authorities** tab.

The VPN 3002 Hardware Client SSL certificate name is its Ethernet 1 (private) IP address.

Figure 1-13 Internet Explorer 4.0 Certificate Authorities List



Select a certificate, then click **View Certificate**. The browser displays the Certificate Properties screen, as in [Figure 1-12](#) above.

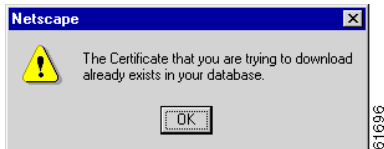
Installing the SSL Certificate with Netscape

This section describes SSL certificate installation using Netscape Navigator / Communicator 4.5.

Reinstallation

You need to install the SSL certificate from a given VPN 3002 only once. If you try to reinstall it, Netscape displays the note in [Figure 1-14](#). Click **OK** and just connect to the VPN 3002 using SSL (see Step 7 in this section).

Figure 1-14 Netscape Reinstallation Note



First-time Installation

The instructions below follow from Step 2 in “[Installing the SSL Certificate in Your Browser](#),” and describe first-time certificate installation.

A few seconds after the VPN 3002 Hardware Client Manager SSL screen appears, Netscape displays a New Certificate Authority screen.

Figure 1-15 Netscape New Certificate Authority Screen 1



Step 1 Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, which further explains the process.

Figure 1-16 Netscape New Certificate Authority Screen 2

Step 2 Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, which lets you examine details of the VPN 3002 Hardware Client SSL certificate.

Figure 1-17 Netscape New Certificate Authority Screen 3

Step 3 Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, with choices for using the certificate. No choices are checked by default.

Figure 1-18 Netscape New Certificate Authority Screen 4



- Step 4** You must check at least the first box, **Accept this Certificate Authority for Certifying network sites**. Click **Next>** to proceed.

Netscape displays the next New Certificate Authority screen, which lets you choose to have the browser warn you about sending data to the VPN 3002.

Figure 1-19 Netscape New Certificate Authority Screen 5



- Step 5** Checking the box is optional. Doing so means that you get a warning whenever you apply settings on a Manager screen, so it is probably less intrusive to manage the VPN 3002 without those warnings. Click **Next>** to proceed.

Netscape displays the final New Certificate Authority screen, which asks you to name the certificate.

Figure 1-20 Netscape New Certificate Authority Screen 6



- Step 6** In the **Nickname** field, enter a descriptive name for this certificate. “Nickname” is something of a misnomer. We suggest you use a clearly descriptive name such as `Cisco VPN 3002 10.10.147.2`. This name appears in the list of installed certificates; see “[Viewing Certificates with Netscape](#),” below.

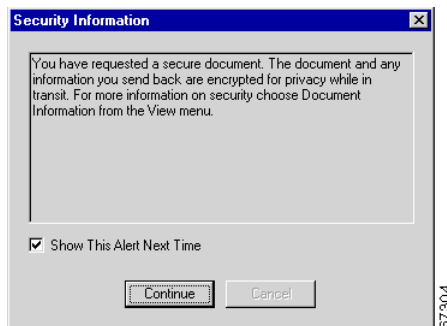
Click **Finish**.

You can now connect to the VPN 3002 using HTTP over SSL (HTTPS).

- Step 7** On the Manager SSL screen ([Figure 1-2](#)), click the link that says **After installing the SSL certificate, click here to connect to the VPN 3002 Hardware Client using SSL**.

Depending on how your browser is configured, you might see a Security Information Alert dialog box.

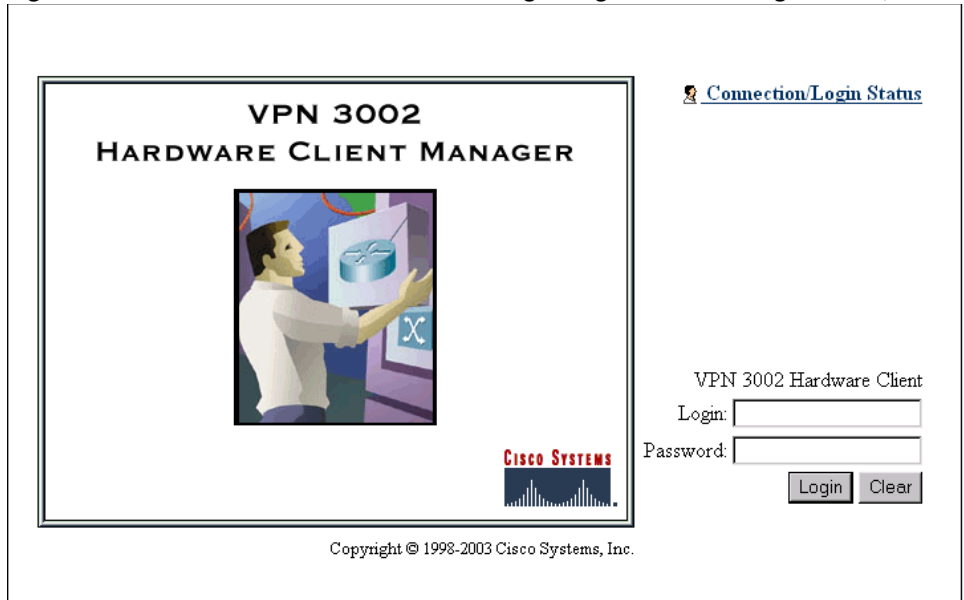
Figure 1-21 Netscape Security Information Alert Dialog Box



- Step 8** Click **Continue**.

The VPN 3002 displays the HTTPS version of the Manager login screen.

Figure 1-22 VPN 3002 Hardware Client Manager Login Screen Using HTTPS (Netscape)



The browser maintains the HTTPS state until you close it or access an unsecured site; in the latter case, you might see a Security Information Alert dialog box.

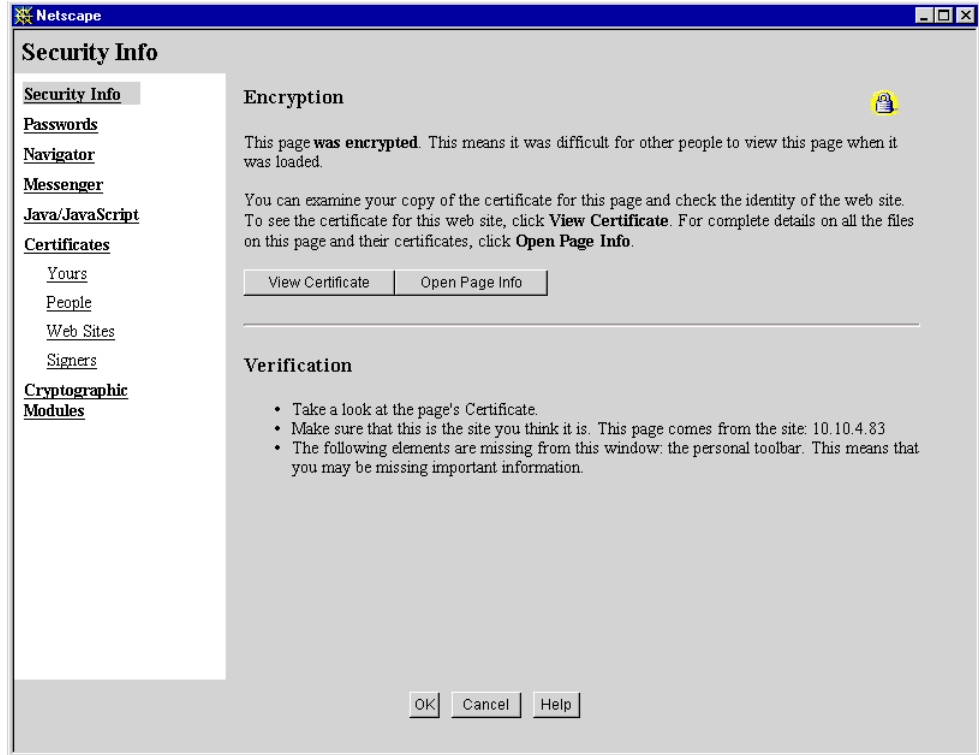
Proceed to the section, “[Logging into the VPN 3002 Hardware Client Manager](#),” to log in as usual.

Viewing Certificates with Netscape

There are (at least) two ways to examine certificates stored in Netscape Navigator / Communicator 4.5.

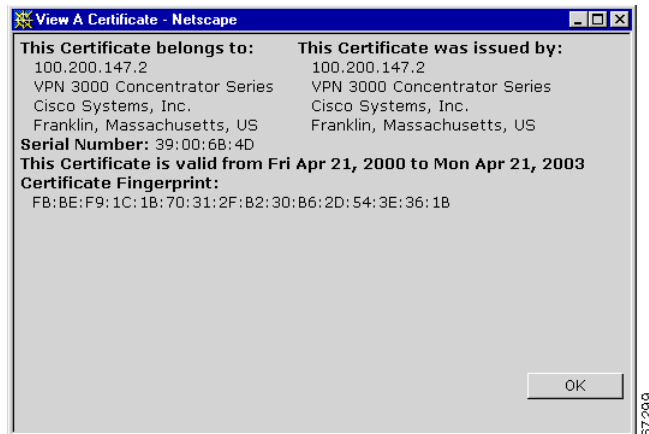
First, note the locked-padlock icon on the bottom status bar in [Figure 1-22](#). If you click the icon, Netscape opens a Security Info window. (You can also open this window by clicking Security on the Navigator Toolbar at the top of the Netscape window.)

Figure 1-23 Netscape Security Info Window



Click **View Certificate** to see details of the specific certificate in use.

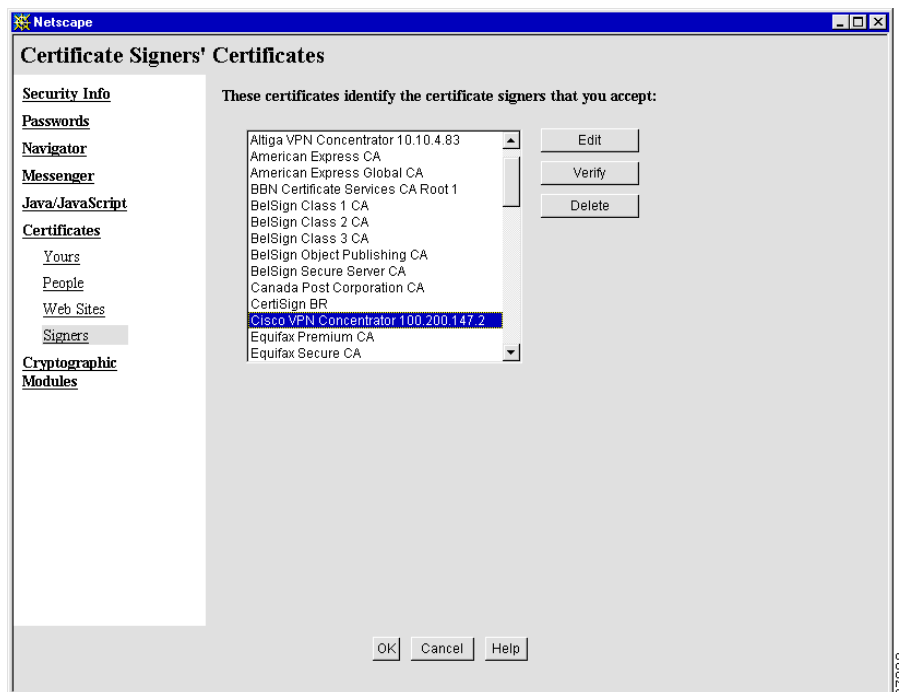
Figure 1-24 Netscape View Certificate Screen



Click **OK** when finished.

Second, you can view all the certificates that are stored in Netscape. On the Security Info window, select **Certificates**, then **Signers**. The “nickname” you entered in Step 6 in the section, “[First-time Installation](#),” identifies the VPN 3002 Hardware Client SSL certificate.

Figure 1-25 Netscape Certificates Signers List



Select a certificate, then click **Edit**, **Verify**, or **Delete**. Click **OK** when finished.

Connecting to the VPN 3002 Using HTTPS

When you have installed the SSL certificate in the browser, you can connect directly using HTTPS.

-
- Step 1** Bring up the browser.
- Step 2** In the browser **Address** or **Location** field, enter **https://** plus the VPN 3002 private interface IP address; for example, **https://10.10.147.2**.

The browser displays the VPN 3002 Hardware Client Manager HTTPS login screen.

A locked-padlock icon on the browser status bar indicates an HTTPS session. Also, this login screen does not include the Install SSL Certificate link.

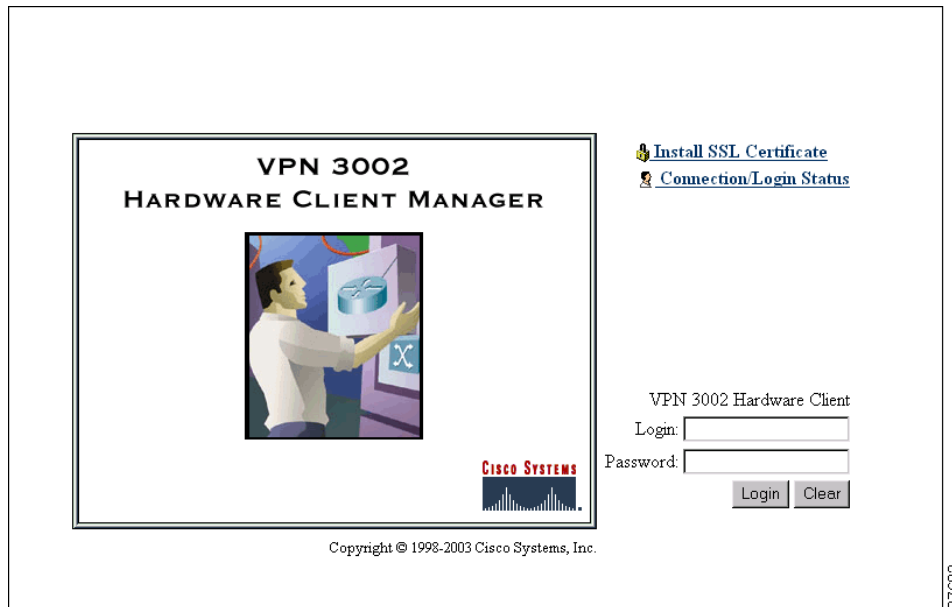
Configuring HTTP, HTTPS, and SSL Parameters

HTTP, HTTPS, and SSL are enabled by default on the VPN 3002, and they are configured with recommended parameters that should suit most administration tasks and security requirements.

To configure HTTP and HTTPS parameters, see the Configuration | System | Management Protocols | HTTP/HTTPS screen.

To configure SSL parameters, see the Configuration | System | Management Protocols | SSL screen.

Figure 1-26 VPN Hardware Client Manager HTTPS Login Screen



87692

Logging into the VPN 3002 Hardware Client Manager

Logging into the VPN 3002 Hardware Client Manager is the same for both types of connections, cleartext HTTP or secure HTTPS.

Entries are case-sensitive. With Microsoft Internet Explorer, you can select the Tab key to move from field to field; other browsers might work differently. If you make a mistake, click the Clear button and start over.

The following entries are the factory-supplied default entries. If you have changed them, use your entries.

-
- Step 1** Click in the **Login** field and type **admin**. (Do not press Enter.)
 - Step 2** Click in the **Password** field and type **admin**. (The field shows *****)
 - Step 3** Click the **Login** button.

The Manager displays the main welcome screen (Figure 1-33).

From here you can navigate the Manager using either the table of contents in the left frame, or the Manager toolbar in the top frame.

Interactive Hardware Client and Individual User Authentication

Interactive hardware client and individual user authentication provide security by requiring manual entry of usernames and passwords prior to connection. You configure these features on the VPN Concentrator to which this VPN 3002 connects, and the VPN Concentrator pushes the policies you set to the VPN 3002. You can use interactive hardware client authentication and individual user authentication in combination or separately.

For complete configuration information refer to the section on the Hardware Client tab in the *User Management* chapter of the *VPN 3000 Series Concentrator Reference Volume 1: Configuration*.

Interactive Hardware Client Authentication

When you enable interactive hardware client authentication, the VPN 3002 does not use a saved username and password. Instead, to connect you must manually enter a valid username and password for the VPN 3002 when prompted. When the VPN 3002 initiates the tunnel, it sends the username and password to the VPN Concentrator to which it connects. The VPN Concentrator facilitates authentication, on either the internal or an external server. If the username and password are valid, the tunnel is established.

Individual User Authentication

Individual user authentication protects the central site from access by unauthorized persons on the same LAN as the VPN 3002.

When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the VPN Concentrator, even though the tunnel already exists.

- If you direct the browser to a site on the remote network behind the VPN Concentrator, the VPN 3002 directs the browser to the proper pages for login. When you successfully log in, the browser displays the page you originally entered.
- You can also log in by directing the browser to the private interface of the VPN 3002 html interface. You do this by entering the IP address of the private interface in the browser Location or Address field. The browser displays the login screen for the VPN 3002. Click the Connect/ Login Status button to authenticate.

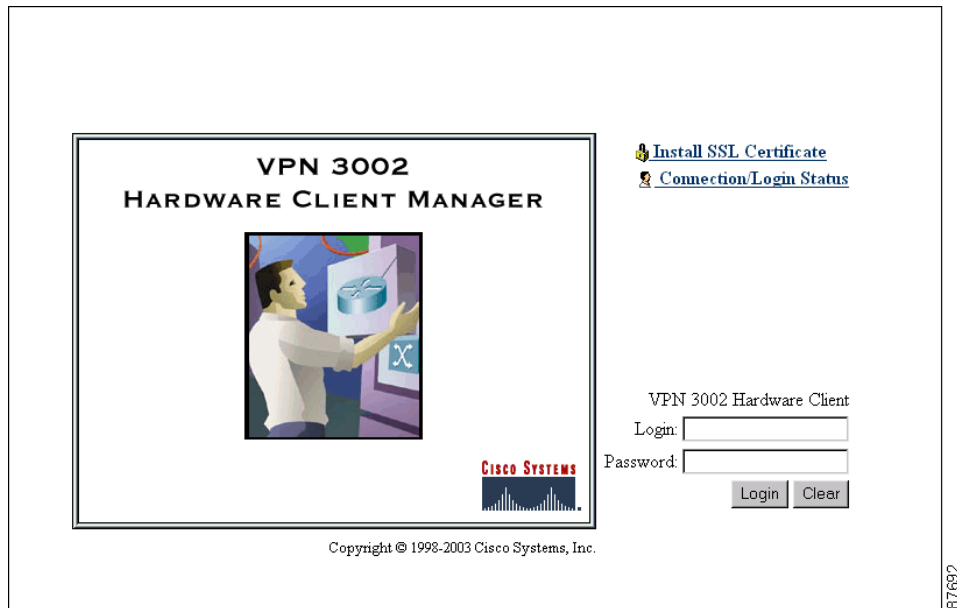
**Note**

You cannot use the command-line interface to login if user authentication is enabled. You must use a browser.

Logging In With Interactive Hardware Client and Individual User Authentication

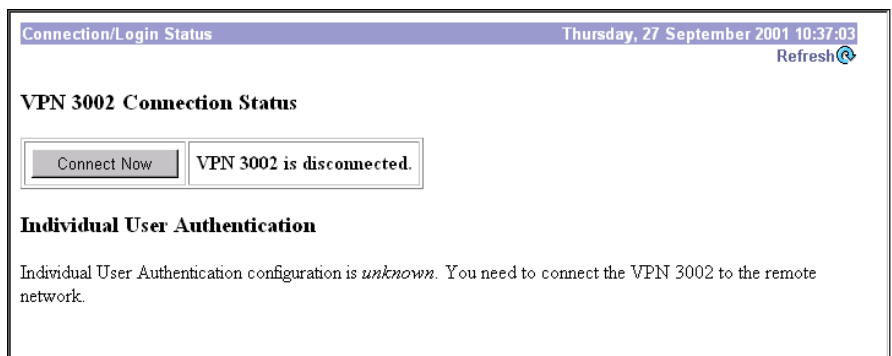
You access the interactive hardware client authentication and individual user authentication login screens from the VPN 3002 Hardware Client Manager login screen. The sequence in the login example that follows assumes that both interactive hardware client authentication and individual user authentication are required for this VPN 3002 to connect.

Figure 1-27 VPN 3002 Hardware Client Manager Login Screen



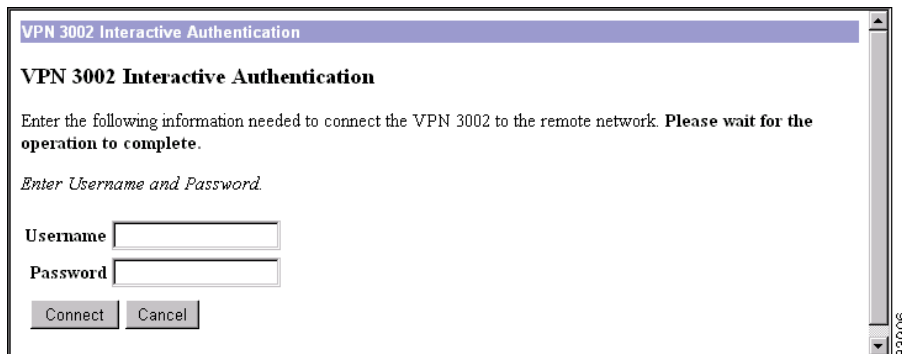
-
- Step 1** Click the **Connection Login Status** button.
The Connection/Login Status screen displays
-

Figure 1-28 Connection Login Status Screen



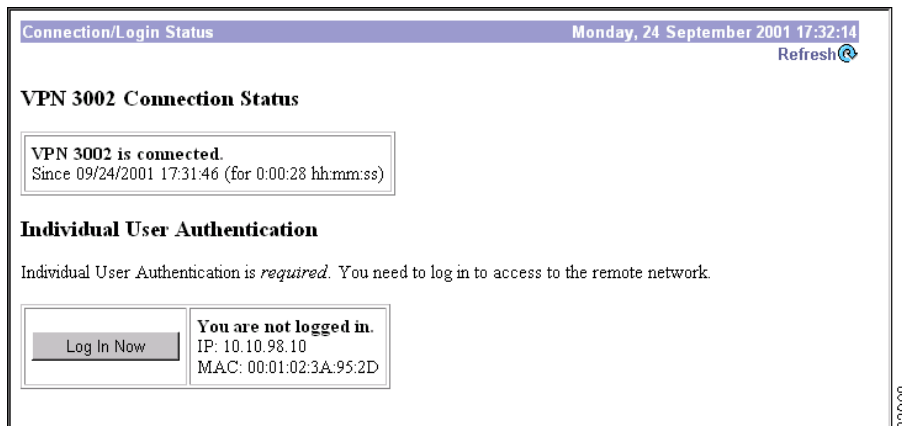
- Step 1** Click the **Connect Now** button.
The VPN 3002 Interactive Authentication screen displays.

Figure 1-29 VPN 3002 Interactive Authentication Screen



- Step 1** Enter the username and password for the VPN 3002.
- Step 2** Click **Connect**.
- If you have entered the valid username and password, the Connect Login Status screen displays the message that the VPN 3002 is connected. Next you authenticate the user.

Figure 1-30 Connection Login Status Screen



- Step 1** To authenticate an individual user, click **Log In Now**.
The Individual User Authentication screen displays.

Figure 1-31 Individual User Authentication Screen

-
- Step 1** Enter the username and password for this VPN 3002 user.
- Step 2** Click **Login**. If the username and password you entered are valid, the Connection/Login Status window displays information about the connection.
-

Figure 1-32 Connection/Login Status Screen

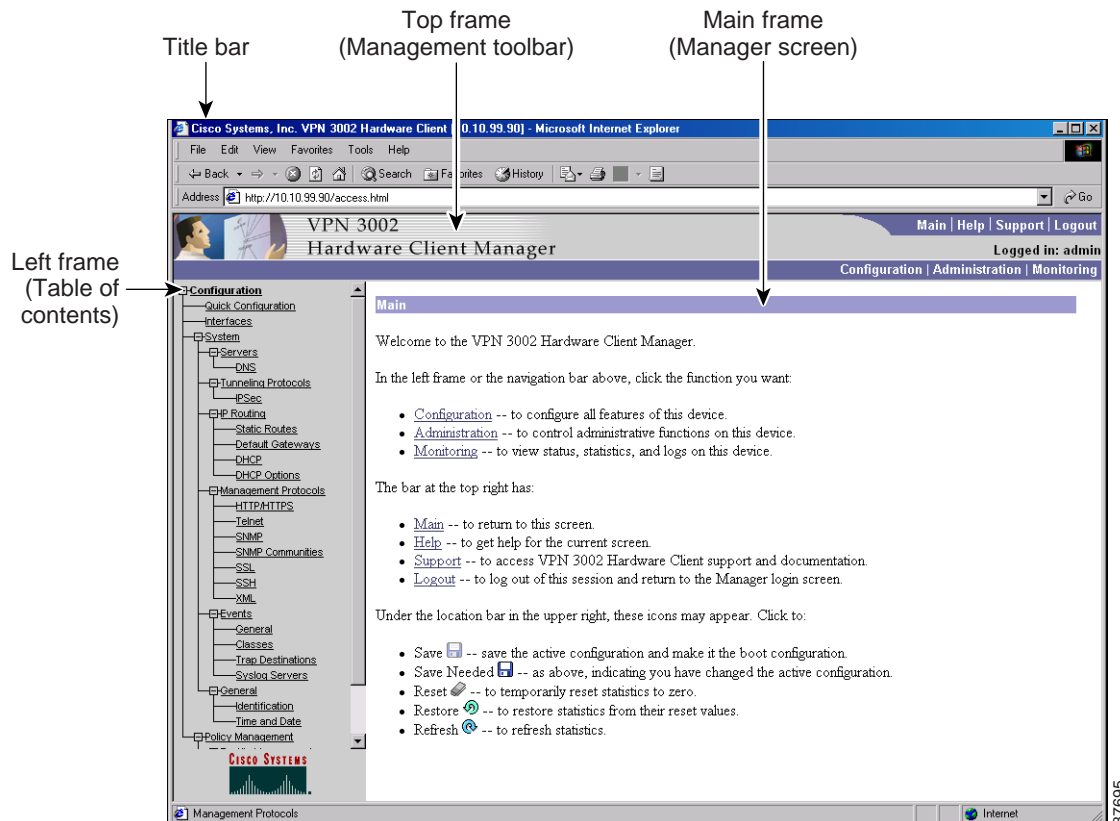
The user behind the VPN 3002 is connected to the VPN Concentrator at the central site.

Click **Go back to the VPN 3002 administrative login page** to return to the VPN 3002 Hardware Client Manager login screen and access other features and functions of the VPN 3002.

Understanding the VPN 3002 Hardware Client Manager Window

The VPN 3002 Hardware Client Manager window on your browser consists of three frames—top, left, and main—and it provides helpful messages and tips as you move the mouse pointer over window items. The title bar and status bar also provide useful information.

Figure 1-33 VPN 3002 Hardware Client Manager Window.



Title bar

The title bar at the top of the browser window includes the VPN 3002 device name or IP address in brackets, for example, [10.10.4.6].

Status bar

The status bar at the bottom of the browser window displays Manager activity and explanatory messages for some items.

Mouse pointer and tips

As you move the mouse pointer over an active area, the pointer changes shape and icons change color. A description also appears in the status bar area. If you momentarily rest the pointer on an icon, a descriptive tip appears for that icon.

**Top frame
(Manager toolbar)**

The Manager toolbar in the top frame provides quick access to Manager features. These include the following icons:

Main

Click on the **Main** tab to go to the main Manager screen, and to close all subordinate sections and titles in the left frame.

Help

Click on the **Help** tab to open context-sensitive online help. Help opens in a separate browser window that you can move or resize as you want. Close the help window when you are finished.

Support

Click on the **Support** tab to open a Manager screen with links to Cisco support and documentation resources.

Logout

Click on the **Logout** tab to log out of the Manager and return to the login screen.

Logged in: [username]

The administrator username you used to log in to this Manager session.

Configuration

Click on the **Configuration** tab to go to the main Configuration screen, to open the first level of subordinate Configuration pages in the left frame if they are not already open, and to close any open Administration or Monitoring pages in the left frame.

Administration

Click on the **Administration** tab to go to the main Administration screen, to open the first level of subordinate Administration pages in the left frame if they are not already open, and to close any open Configuration or Monitoring pages in the left frame.

Monitoring

Click on the **Monitoring** tab to go to the main Monitoring screen, to open the first level of subordinate Monitoring pages in the left frame if they are not already open, and to close any open Configuration or Administration pages in the left frame.

Save 

Click on the **Save** icon to save the active configuration and make it the boot configuration. In this state, the reminder indicates that the active configuration is the same as the boot configuration, but you can save it anyway. When you change the configuration, the reminder changes to Save Needed.

Save Needed 

This reminder indicates that you have changed the active configuration. Click on the **Save Needed** icon to save the active configuration and make it the boot configuration. As you make configuration entries, they take effect immediately and are included in the active, or running, configuration. However, if you reboot the VPN 3002 without saving the active configuration, and configuration changes are lost. Clicking on this reminder saves the active configuration as the boot configuration and restores the Save reminder.

Refresh 

Click on the **Refresh** icon to refresh (update) the screen contents on screens where it appears (mostly in the Monitoring section). The date and time above this reminder indicate when the screen was last updated.

Reset 

Click on the **Reset** icon to reset, or start anew, the screen contents on screens where it appears (mostly in the Monitoring section).

Restore 

Click on the **Restore** icon to restore the screen contents to their status prior to when you last clicked the Reset icon.




Click on the **Cisco Systems logo** to open a browser and go to the Cisco.com web site, www.cisco.com

**Left frame
(Table of Contents)**

On Manager screens, the left frame provides a table of contents. The table of contents uses the familiar Windows Explorer metaphor of collapsed and expanded entries.

**Main section titles
(Configuration,
Administration, Monitoring)**

Click on a title to open subordinate sections and titles, and to go to that Manager screen in the main frame.

Closed or collapsed 

Click on the **closed/collapsed** icon to open subordinate sections and titles. Clicking on this icon does not change the screen in the main frame.

Open or expanded 

Click on the **open/expanded** icon to close subordinate sections and titles. Clicking on this icon does not change the screen in the main frame.

**Main frame
(Manager screen)**

The main frame displays the current VPN 3002 Manager screen.

Many screens include a bullet list of links and descriptions of subordinate sections and titles. You can click on a link to go to that Manager screen, and open subordinate sections and titles in the table of contents.

Organization of the VPN 3002 Hardware Client Manager

The VPN 3002 Hardware Client Manager consists of three major sections and many subsections:

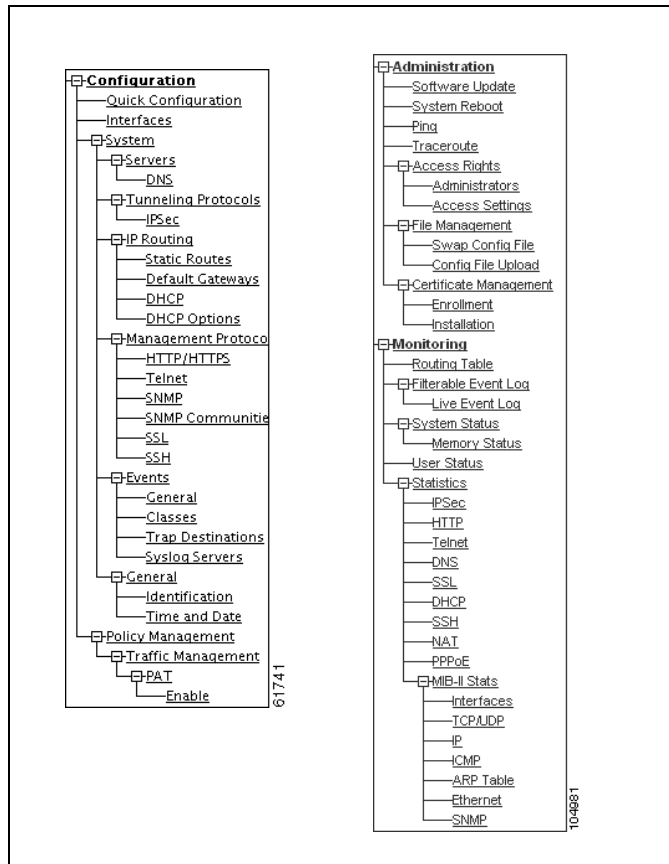
- Configuration: setting all the parameters for the VPN 3002 that govern its use and functionality as a VPN device:
 - Quick Configuration: supplying the minimal parameters needed to make the VPN 3002 operational.
 - Interfaces: Ethernet parameters.
 - System: parameters for system-wide functions such as server access, IPSec tunneling protocol, built-in management servers, event handling, and system identification.
 - Policy Management: enabling PAT (Port Address Translation).
- Administration: managing higher level functions that keep the VPN3002 operational and secure, such as who is allowed to configure the system, what software runs on it, and managing its configuration files and digital certificates.
- Monitoring: viewing routing tables, event logs, system LEDs and status, and data on user sessions.

This manual covers all these topics. For Quick Configuration, refer to the *VPN 3002 Hardware Client Getting Started* guide.

Navigating the VPN 3002 Hardware Client Manager

Your primary tool for navigating the VPN 3002 Hardware Client Manager is the table of contents in the left frame. [Figure 1-34](#) shows all its entries, completely expanded. (The figure shows the frame in multiple columns, but the actual frame is a single column. Use the scroll controls to move up and down the frame.)

Figure 1-34 Manager Table of Contents





Configuration

Configuring the VPN 3002 means setting all the parameters that govern its use and functionality as a VPN device.

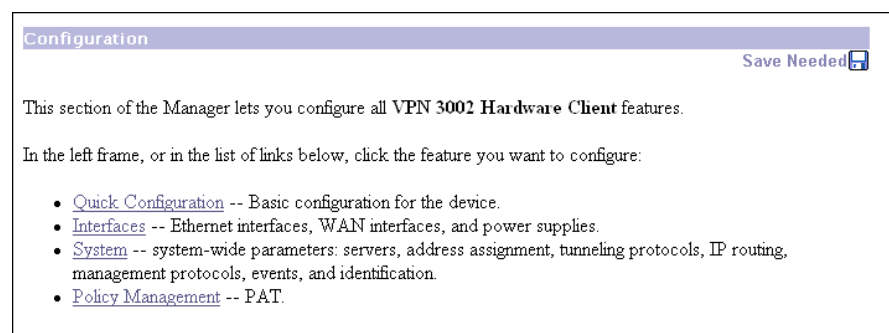
Cisco supplies default parameters that cover typical installations and uses; after you supply minimal parameters in Quick Configuration, the system is operational. But to tailor the system to your needs, and to provide an appropriate level of system security, you can configure the system in detail.

Configuration

This section of the Manager lets you configure all VPN 3002 features and functions.

- **Quick Configuration:** the minimal parameters needed to make the VPN 3002 operational. For more information, use online Help, or see the *VPN 3002 Hardware Client Getting Started* manual, available only online.
- **Interfaces:** parameters specific to the private and public interfaces.
- **System:** parameters for system-wide functions: server access, IPSec, IP routing, built-in management servers, system events, and system identification.
- **Policy Management:** enabling or disabling Protocol Address Translation (PAT).

Figure 2-1 Configuration Screen



See the appropriate chapter in this manual for each section of the Manager. Online help is available for all sections.



Interfaces

This section of the VPN 3002 Hardware Client Manager applies functions that are interface-specific, rather than system-wide.

Configuration | Interfaces

You configure two network interfaces for the VPN 3002 to operate as a VPN device: the private interface and the public interface. If you used Quick Configuration as described in the *VPN 3002 Hardware Client Getting Started* manual, the system supplied many default parameters for the interfaces. Here you can configure them explicitly.

- Private is the interface to your private network (internal LAN).
- Public is the interface to the public network.

Configuring an Ethernet interface includes supplying an IP address and subnet mask, and setting speed and transmission mode.

The VPN 3002 includes some IP routing functions: static routes, DHCP, and PPPoE. You configure static routes, the default gateway, and DHCP in the IP Routing section; see the Configuration | System | IP Routing screens. PPPoE requires no further configuration than supplying a username and password in the Public Interface parameter.





Note

Interface settings take effect as soon as you apply them. If the system is in active use, changes might affect tunnel traffic.

The table on the Configuration | Interfaces screen shows all installed interfaces and their status.


Figure 3-1 VPN 3002 Configuration | Interfaces Screen

Configuration | Interfaces Tuesday, 18 September 2001 15:18:58
Save Needed  Refresh 

This section lets you configure the VPN 3002 Hardware Client's network interfaces.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	10.10.99.50	255.255.0.0	00.90.A4.00.25.A8	
Ethernet 2 (Public)	Waiting for PPPoE	0.0.0.0	0.0.0.0	00.90.A4.00.25.A9	
DNS Server(s)	10.10.99.60				
DNS Domain Name	ispdomain.com				



18978

To configure a module, either click the appropriate link in the status table; or use the mouse pointer to select the module on the back-panel image, and click anywhere in the highlighted area.

Interface

The VPN 3002 interface installed in the system. To configure an interface, click the appropriate link.

Ethernet 1 (Private), Ethernet 2 (Public)

To configure Ethernet interface parameters, click the appropriate highlighted link in the table or click in a highlighted module on the back-panel image. See Configuration | Interfaces | Private/Public.

DNS Server(s)

To configure DNS Server(s), click the highlighted link in the table. See Configuration | System | Servers | DNS.

DNS Domain Name

To configure DNS Server(s), click the highlighted link in the table. See Configuration | System | Servers | DNS.

Status

The operational status of this interface:

- **UP** (green) = Configured, enabled, and operational; ready to pass data traffic.
- **DOWN** (red) Configured but disabled or disconnected.
- **Testing** = In test mode; no regular data traffic can pass.
- **Dormant** (red) = Configured and enabled but waiting for an external action, such as an incoming connection.
- **Not Present** (red) = Missing hardware components.
- **Lower Layer Down** (red) = Not operational because a lower-layer interface is down.
- **Unknown** (red) = Not configured or not able to determine status.
- **Not Configured** = Present but not configured.
- **Waiting for DHCP/PPPoE** = Waiting for DHCP or PPPoE to assign an IP address.

IP Address

The IP address configured on this interface.

Subnet Mask

The subnet mask configured on this interface.

MAC Address

This is the unique hardware MAC (Media Access Control) address for this interface, displayed in 6-byte hexadecimal notation. You cannot change this address.

Default Gateway

The IP routing subsystem routes data packets first using static routes, then the default gateway. If you do not specify a default gateway, the system drops packets it cannot otherwise route.


To configure a default gateway, click the appropriate highlighted link in the table or click in a highlighted module on the back-panel image. See [Configuration | System | IP Routing | Default Gateways](#).

Configuration | Interfaces | Private

This screen lets you configure parameters for the private interface. It displays the current parameters, if any.

Figure 3-2 Configuration | Interfaces | Private Screen

Configuration | Interfaces | Private

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring the Private Interface.

<input type="radio"/>	Disabled	Select to disable this interface.
<input checked="" type="radio"/>	Static IP Addressing	Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	10.10.99.90
	Subnet Mask	255.255.0.0
	MAC Address	00.90.A4.04.01.AC
	Speed	10/100 auto
	Duplex	Auto
	MTU	1500

Apply Cancel

79369



Caution

If you modify any parameters of the private interface that you are currently using to connect to the VPN 3002, you will break the connection, and you will have to restart the Manager from the login screen.

Disabled

To make the interface offline, click **Disabled**. This state lets you retain or change its configuration parameters.

If the interface is configured but disabled (offline), the appropriate Ethernet Link Status LED blinks green on the VPN 3002 front panel.

Static IP Addressing

To change the IP address of the private interface, click **Static IP Addressing**.

IP Address

Enter the IP address for this interface, using dotted decimal notation (for example, 192.168.12.34). Note that 0.0.0.0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

Enter the subnet mask for this interface, using dotted decimal notation (for example 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

MAC Address

This is the unique hardware MAC (Media Access Control) address for this interface, displayed in 6-byte hexadecimal notation. You cannot change this address.

Speed

click the drop-down menu button and select the interface speed:

- **10 Mbps** = Fix the speed at 10 megabits per second (10Base-T networks).
- **100 Mbps** = Fix the speed at 100 megabits per second (100Base-T networks).
- **10/100 auto** = Let the VPN 3002 automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

Duplex

Click the drop-down menu button and select the interface transmission mode:

- **Auto** = Let the VPN 3002 automatically detect and set the appropriate transmission mode, either full or half duplex (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.
- **Full-Duplex** = Fix the transmission mode as full duplex: transmits and receives at the same time.
- **Half-Duplex** = Fix the transmission mode as half duplex: transmits or receives, but not at the same time.

MTU

Accept the default value, 1500 bytes per packet.

Apply/Cancel

To apply your settings to the system and include them in the active configuration, click **Apply**. The Manager returns to the Configuration | Interfaces screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Interfaces screen.

Configuration | Interfaces | Public

This screen lets you select a connection method—DHCP, PPPoE, or static IP addressing—for the public interface. It also allows you to disable the public interface.

Figure 3-3 Configuration | Interfaces | Public Screen

Configuration | Interfaces | Public

Configuring the Public Interface.

<input type="radio"/>	Disabled	Select to disable this interface.
<input checked="" type="radio"/>	DHCP Client Lease Info: 161.44.128.136 expires in 15:46:28 (hh:mm:ss)	Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input type="radio"/>	PPPoE Client	Select to connect to a public network via PPPoE. Enter the PPPoE User Name and Password/Verify.
	PPPoE User Name <input type="text"/>	
	PPPoE Password <input type="text"/>	
	Verify PPPoE Password <input type="text"/>	
<input type="radio"/>	Static IP Addressing	Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address <input type="text" value="161.44.128.136"/>	
	Subnet Mask <input type="text" value="255.255.255.0"/>	
	MAC Address <input type="text" value="00.90.A4.04.01.AD"/>	The MAC address for this interface.
	Speed <input type="text" value="10/100 auto"/>	Select the speed for this interface.
	Duplex <input type="text" value="Auto"/>	Select the duplex mode for this interface.
	MTU <input type="text" value="1500"/>	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	IPSec Fragmentation Policy	<input type="radio"/> Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission
		<input checked="" type="radio"/> Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)
		<input type="radio"/> Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)

Apply Cancel

Disabled

To make the interface offline, click **Disabled**. This state lets you retain or change its configuration parameters.

DHCP Client

Click this radio button if you want to obtain the IP address and subnet mask for this interface via DHCP. If you click this button, you do not make entries in the IP address and subnet mask parameters that follow.

PPPoE Client

click this radio button if you want to connect using PPPoE. If you select PPPoE, you do not make entries in the static IP addressing parameters that follow.

PPPoE User Name

If you have selected PPPoE, enter a valid PPPoE username.

PPPoE Password

If you have selected PPPoE, enter the PPPoE password for the username you entered above.

Verify PPPoE Password

If you have selected PPPoE, enter the PPPoE password again to verify it.

Static IP Addressing

click this radio button if you want to use a static IP address.

IP Address

If you are using static IP addressing, enter the IP address for this interface, using dotted decimal notation (for example, 192.168.12.34). Note that 0.0.0.0 is not allowed. Be sure no other device is using this address on the network.

Subnet Mask

If you are using static IP addressing, enter the subnet mask for this interface, using dotted decimal notation (for example, 255.255.255.0). The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.34 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed.

MAC Address

This is the unique hardware MAC (Media Access Control) address for this interface, displayed in 6-byte hexadecimal notation. You cannot change this address.

Speed

If you are using static IP addressing, click the drop-down menu button and select the interface speed:

- **10 Mbps** = Fix the speed at 10 megabits per second (10Base-T networks).
- **100 Mbps** = Fix the speed at 100 megabits per second (100Base-T networks).
- **10/100 auto** = Let the VPN 3002 automatically detect and set the appropriate speed, either 10 or 100 Mbps (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the speed. Otherwise, select the appropriate fixed speed.

Duplex

If you are using static IP addressing, click the drop-down menu button and select the interface transmission mode:

- **Auto** = Let the VPN 3002 automatically detect and set the appropriate transmission mode, either full or half duplex (default). Be sure that the port on the active network device (hub, switch, router, etc.) to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode.
- **Full-Duplex** = Fix the transmission mode as full duplex: transmits and receives at the same time.
- **Half-Duplex** = Fix the transmission mode as half duplex: transmits or receives, but not at the same time.

MTU

The MTU value specifies the maximum transmission unit (packet size) in bytes for the interface. Valid values range from 68 through 1500. The default value, 1500, is the MTU for IP.

Change this value only when the VPN 3002 is dropping large packets because of the additional 8 bytes that a PPPoE header adds, or when other intermediate devices drop large, fragmentable packets without issuing an ICMP message. In such cases, determine the largest packet size that can pass without being dropped, and set the MTU to that value. The object is to reduce overhead on the system by sending packets that are as large as possible, but that are not so large as to require fragmentation and reassembly.

A good way to find out the largest packet size that can be passed is to use the Ping utility as follows:

```
ping -f -l <packet size in bytes> <destination IP address>, where
```

f = do not fragment

l = frame length.

For example: ping -f -l 1400 10.10.32.4



Note

The value you use when pinging does not include IP, ICMP, or Ethernet headers, which total 42 bytes. You need to include these 42 bytes when you set the MTU value for the interface.

If the interface is receiving large packets that require fragmentation, and the DF (Don't Fragment) bit is set, use the third option in the IPSec Fragmentation Policy field (see below). You can find out if the DF bit is set by using a traffic analyzer, or you may receive this ICMP message: "Fragmentation required but the DF bit is set."



Note

Changing the MTU or the fragmentation option on *any* interface tears down *all* existing connections. For example, if 100 active tunnels terminate on the public interface, and you change the MTU on the private interface, all of the active tunnels on the public interface are dropped.

IPSec Fragmentation Policy

The IPSec fragmentation policy specifies how to treat packets that exceed the MTU setting when tunneling traffic through the public interface. This feature provides a way to handle cases where a router or NAT device between the VPN 3002 and the VPN Concentrator rejects or drops IP fragments. For

example, suppose a PC behind a VPN 3002 wants to FTP put a large file to an FTP server behind a VPN Concentrator. The PC transmits packets that when encapsulated would exceed the VPN 3002's MTU size on the public interface. The following options determine how the VPN 3002 processes these packets.

The fragmentation policy you set here applies to all traffic travelling out the VPN 3002 public interface to VPN Concentrators. The second and third options described below may affect performance rates.

Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission

The VPN 3002 encapsulates all tunneled packets. After encapsulation, the VPN 3002 fragments packets that exceed the MTU setting before transmitting them through the public interface. This option works for situations where fragmented packets are allowed through the tunnel without hindrance. For the FTP example, large packets are encapsulated and then fragmented at the IP layer. Intermediate devices may drop fragments or just out-of-order fragments. Load-balancing devices can introduce out-of-order fragments.

Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)

The VPN 3002 fragments tunneled packets that would exceed the MTU setting during encapsulation. For this option, the VPN 3002 drops large packets that have the Don't Fragment (DF) bit set, and sends an ICMP message "Packet needs to be fragmented but DF is set" to the packet's initiator. The ICMP message includes the maximum MTU size allowed. Path MTU Discovery means that an intermediate device (in this case the VPN 3002) informs the source of the MTU permitted to reach the destination.

If a large packet does not have the DF bit set, the VPN 3002 fragments prior to encapsulating, thus creating two independent non-fragmented IP packets, and transmits them out the public interface. This is the default policy for the VPN 3002 hardware client.

For this example, the PC that is the FTP client may use Path MTU Discovery to adjust the size of the packets it transmits to this destination.

Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)

The VPN 3002 fragments tunneled packets that exceed the MTU setting before encapsulating them. If the DF bit on these packets is set, the VPN 3002 clears the DF bit, fragments the packets, and then encapsulates them. This action creates two independent non-fragmented IP packets leaving the public interface and successfully transmits these packets to the peer site by turning the fragments into complete packets to be reassembled at the peer site.

In our example, the VPN 3002 overrides the MTU and allows fragmentation by clearing the DF bit.

Apply / Cancel

To apply your settings to this interface and include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | Interfaces screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Interfaces screen.



System Configuration

System configuration means configuring parameters for system-wide functions in the VPN 3002.


Configuration | System

This section of the Manager lets you configure parameters for:

- **Servers:** identifying servers for DNS information for the VPN 3002.
- **Tunneling Protocols:** configuring IPsec connections.
- **IP Routing:** configuring static routes, default gateways, and DHCP.
- **Management Protocols:** configuring and enabling built-in servers for HTTP/HTTPS, Telnet, SNMP, SSL, SSH, and XML.
- **Events:** handling system events via logs, SNMP traps, and syslog.
- **General:** identifying the system and setting the time and date.

See the appropriate chapter in this manual or the online help for each section.

Figure 4-1 Configuration | System screen

Configuration | System Save Needed 

This section of the VPN 3000 Concentrator Manager lets you configure system-wide parameters.

In the left frame, or in the list of links below, click the parameters you want to configure:

- [Servers](#) -- authentication, accounting, DNS, DHCP, and NTP.
- [Address Management](#) -- address assignment options and address pools.
- [Tunneling Protocols](#) -- PPTP, L2TP, IPsec LAN-to-LAN, IPsec IKE proposals, and IPsec over TCP.
- [IP Routing](#) -- static routes, default gateways, OSPF, global DHCP, and redundancy (VRRP).
- [Management Protocols](#) -- FTP, HTTP/HTTPS, TFTP, Telnet, SNMP, SSL, SSH and XML.
- [Events](#) -- defaults, classes, trap destinations, syslog and SMTP servers, and email.
- [General](#) -- system name, contact, location, time and date, maximum sessions, global authentication.
- [Client Update](#) -- enable, clients, URLs, revisions.
- [Load Balancing](#) -- cluster configuration, priority, enable, etc.

67598



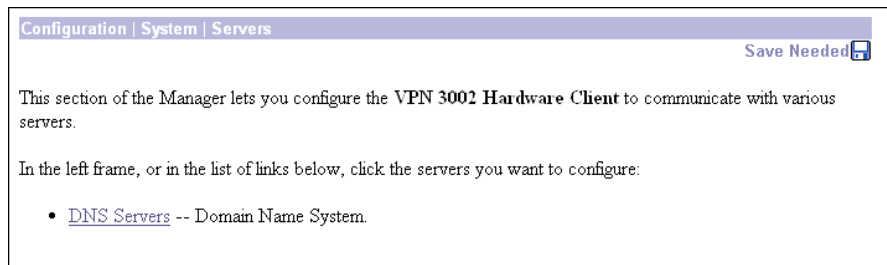
Servers

Configuring servers means identifying DNS servers to the VPN 3002 so it can communicate with them correctly. DNS servers convert hostnames to IP addresses. The VPN 3002 functions as a client of these servers.

Configuration | System | Servers

This section of the Manager lets you configure the VPN 3002 to communicate with DNS servers.

Figure 5-1 Configuration | System | Servers Screen



Configuration | System | Servers | DNS

This screen lets you configure the Domain Name System (DNS) servers for the VPN 3002. DNS servers convert domain names to IP addresses. Configuring DNS servers here lets you enter hostnames (for example, mail01) rather than IP addresses as you configure and manage the VPN 3002.

You can configure up to three DNS servers that the system queries in order.



Note

DNS information that you add here is for the VPN 3002 only. PCs located behind the VPN 3002 on the private network get DNS information that is configured on the central-site VPN Concentrator in the Group settings for the VPN 3002.

Figure 5-2 Configuration | System | Servers | DNS Screen

Configuration | System | Servers | DNS

Configure system-wide DNS (Domain Name System) servers.

i Configuring DNS is optional, but it lets you use hostnames rather than IP addresses.

Enabled

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Timeout Period seconds

Timeout Retries

Apply Cancel

61749

Enabled

To use DNS functions, check **Enabled** (the default). To disable DNS, clear the box.

Domain

Enter the name of the registered domain of the ISP for the VPN 3002; for example, `yourisp.com`. Maximum 48 characters. This entry is sometimes called the domain name suffix or sub-domain. The DNS system within the VPN 3002 automatically appends this domain name to hostnames before sending them to a DNS server for resolution.

Primary DNS Server

Enter the IP address of the primary DNS server, using dotted decimal notation; for example, `192.168.12.34`. Be sure this entry is correct to avoid DNS resolution delays.

Secondary DNS Server

Enter the IP address of the secondary (first backup) DNS server, using dotted decimal notation. If the primary DNS server does not respond to a query within the Timeout Period specified below, the system queries this server.

Tertiary DNS Server

Enter the IP address of the tertiary (second backup) DNS server, using dotted decimal notation. If the secondary DNS server does not respond to a query within the Timeout Period specified below, the system queries this server.

Timeout Period

Enter the initial time in seconds to wait for a response to a DNS query before sending the query to the next server. Minimum is 1, default is 2, maximum is 30 seconds. This time doubles with each retry cycle through the list of servers.

Timeout Retries

Enter the number of times to retry sending a DNS query to the configured servers, in order. In other words, this is the number of times to cycle through the list of servers before returning an error. Minimum is 0, default is 2, maximum is 10 retries.

Apply / Cancel

To apply your settings for DNS servers and include the settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Servers screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Servers screen.



Tunneling

Tunneling is the heart of virtual private networking. Tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network.

The secure connection is called a tunnel, and the VPN 3002 uses the IPSec tunneling protocol to:

- Negotiate tunnel parameters.
- Establish tunnels.
- Authenticate users and data.
- Manage security keys.
- Encrypt and decrypt data.
- Manage data transfer across the tunnel.
- Manage data transfer inbound and outbound as a tunnel endpoint.

The VPN 3002 functions as a bidirectional tunnel endpoint:

- It can receive plain packets from the private network, encapsulate them, create a tunnel, and send them to the other end of the tunnel where they are unencapsulated and sent to their final destination
- It can receive encapsulated packets from the public network, unencapsulate them, and send them to their final destination on the private network.

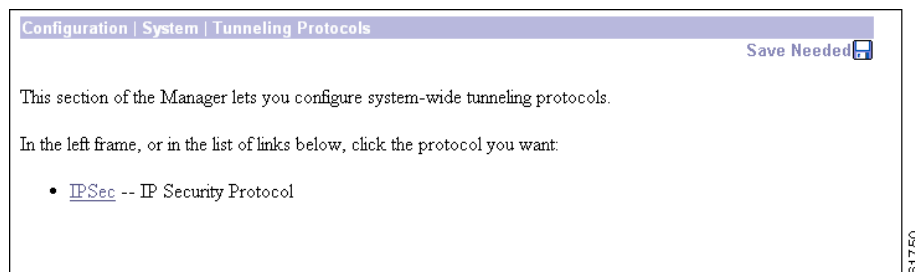
This section explains how to configure the IPSec tunneling protocol.

Configuration | System | Tunneling Protocols

This section lets you configure the IPsec tunneling protocol.

Click **IPsec** on the Tunneling Protocols screen.

Figure 6-1 Configuration | System | Tunneling Protocols Screen



Configuration | System | Tunneling Protocols | IPsec

The VPN 3002 complies with the IPsec protocol and is specifically designed to work with the VPN Concentrator. It can also establish IPsec tunnels to other IPsec security gateways, including the Cisco PIX firewall, and Cisco IOS routers. IPsec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol.

In IPsec terminology, a “peer” is a remote-access client or another secure gateway. During tunnel establishment under IPsec, the two peers negotiate Security Associations (SAs) that govern authentication, encryption, encapsulation, key management, etc. These negotiations involve two phases: the first phase establishes the tunnel (the IKE SA); the second phase governs traffic within the tunnel (the IPsec SA).

The VPN 3002 initiates all tunnels with the VPN Concentrator; the VPN Concentrator functions only as responder. The VPN 3002 as initiator proposes SAs; the responder accepts, rejects, or makes counter-proposals—all in accordance with configured SA parameters. To establish a connection, both entities must agree on the SAs.

The Cisco VPN 3002 supports these IPsec attributes, but they are configurable on the central-site VPN Concentrator, not on the VPN 3002:

- Main mode for negotiating phase one of establishing ISAKMP Secure Associations (SAs) (automatic if you are using certificates)
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs
- Authentication Algorithms:
 - ESP-MD5-HMAC-128
 - ESP-SHA1-HMAC-160
- Authentication Modes:
 - Preshared Keys
 - X.509 Digital Certificates
- Diffie-Hellman Groups 1 and 2

- Encryption Algorithms:
 - DES-56 = Data Encryption Standard (DES) with a 56-bit key.
 - 3DES-168 = Triple-DES with a 168-bit key.
 - AES-128 = Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
 - AES-192 = AES encryption with a 192-bit key.
 - AES-256 = AES encryption with a 256-bit key.
- Extended Authentication (XAuth)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode

Figure 6-2 Configuration | System | Tunneling Protocols | IPSec Screen

Configuration | System | Tunneling Protocols | IPSec

Enter the information needed to connect to the central-site VPN Concentrator server.

Remote Easy VPN Server: 161.44.246.15
Enter remote server address/host name.

Backup Easy VPN Servers: [List]
 • Enter up to 10 backup server addresses/host names from high priority to low.
 • Enter each backup server address/host name on a single line.

Alert when disconnecting

Inform VPN Concentrator server before the system shuts down or reboots.

IPSec over TCP
Check to enable IPSec over TCP.

IPSec over TCP Port: 10000
Enter IPSec over TCP port (1-65535).

Use Certificate
Click to use the installed certificate.

Certificate Transmission:

- Entire certificate chain
- Identity certificate only

 Choose how to send the digital certificate to the server.

Group: 3002Group
Name

User: 3002user

Password: [Masked]
Verify: [Masked]

Apply Cancel

113009

Remote Easy VPN Server

Enter the IP address or hostname of the remote server. This is the IP address or hostname of the public interface on the VPN Concentrator to which this VPN 3002 connects. Use dotted decimal notation; for example, 192.168.34.56. To enter a hostname, a DNS server must be configured.

Backup Easy VPN Servers

To configure IPSec backup servers on the VPN 3002, enter up to 10 backup servers, using either IP address or hostname. Enter each backup server on a separate line. To enter a hostname, a DNS server must be configured. Further, if you use hostnames and the DNS server is unavailable, significant delays can occur.



Note

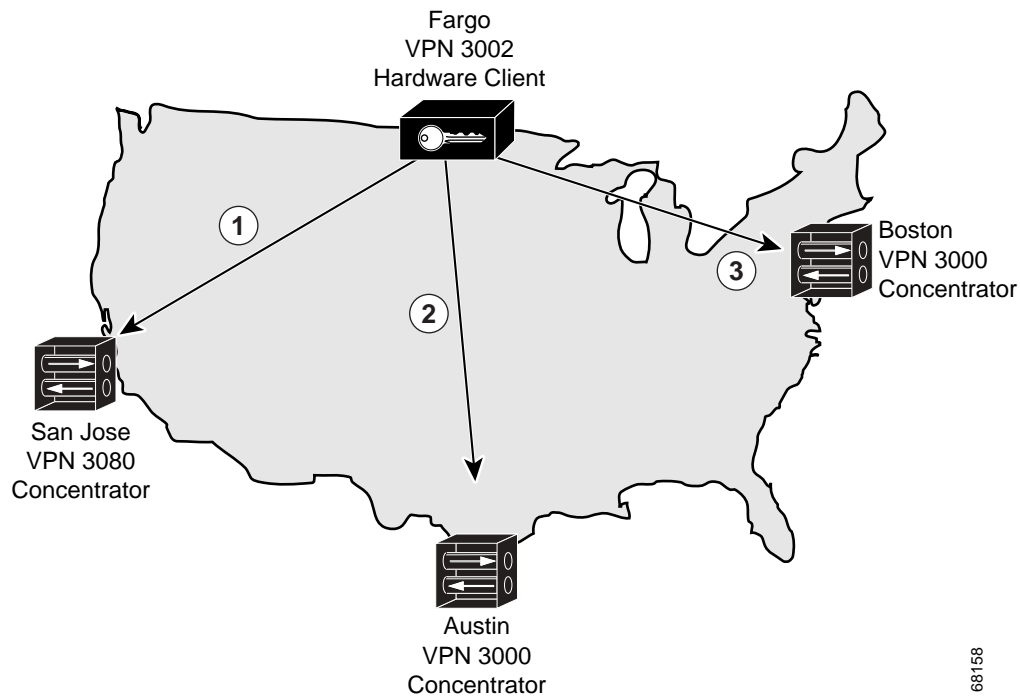
If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind the VPN 3002 obtain DNS and WINS information from the VPN 3002 through DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires.

About Backup Servers

IPSec backup servers let a VPN 3002 connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002, or on a group basis at the central-site VPN Concentrator. If you configure backup servers on the primary central-site VPN Concentrator, that VPN Concentrator pushes the backup server policy to the VPN 3002 hardware clients in the group. By default, the policy is to use the backup server list configured on the VPN 3002. Alternatively, the VPN Concentrator can push a policy that supplies a list of backup servers in order of priority, replacing the backup server list on the VPN 3002 if one is configured. It can also disable the feature and clear the backup server list on the VPN 3002 if one is configured.

Figure 6-3 illustrates how the backup server feature works.

Figure 6-3 Backup Server Implementation



68158

XYZ corporation has large sites in three cities: San Jose, California; Austin, Texas; and Boston, Massachusetts. They just opened a regional sales office in Fargo, North Dakota. To provide access to the corporate network from Fargo, they use a VPN 3002 that connects to a VPN 3080 in San Jose (1). If the VPN 3002 is unable to contact the corporate network, Fargo cannot place orders. The IPSec backup server feature lets the VPN 3002 connect to one of several sites, in this case using Austin (2) and Boston (3) as backup servers, in that order.

The VPN 3002 in Fargo first tries to reach San Jose. If the initial IKE packet for that connection (1) times out (8 seconds), it tries to connect to Austin (2). Should this negotiation also time out, it tries to connect to Boston (3). These attempts continue until the VPN 3002 has tried all servers on its backup server list, to a maximum of 10.

Be aware of the following characteristics of the backup server feature:

- If the VPN 3002 cannot connect after trying all backup servers on the list, it does not automatically retry.
 - In Network Extension mode, the VPN 3002 attempts a new connection after 4 seconds.
 - In Client mode, the VPN 3002 attempts a new connection when the user clicks the Connect Now button on the Monitoring | System Status screen, or when data passes from the VPN 3002 to the VPN Concentrator.
- A VPN 3002 must connect to the primary VPN Concentrator to download a backup server list configured on the primary VPN Concentrator. If that VPN Concentrator is unavailable, and if the VPN 3002 has a previously configured backup server list, it can connect to the servers on that list.
- It can download a backup server list only from the primary VPN Concentrator. The VPN 3002 cannot download a backup server list from a backup server.
- The VPN Concentrators that you configure as backup servers do not have to be aware of each other.
- If you change the configuration of backup servers, or delete a backup server during an active session between a VPN 3002 and a backup server, the session continues without adopting that change. New settings take effect the next time the VPN 3002 connects to its primary VPN Concentrator.

You can configure the backup server feature from the primary VPN Concentrator or the VPN 3002.

- From the VPN Concentrator configure backup servers on either of the Configuration | User Management | Base Group or Groups | Mode Configuration screens.
- On the VPN 3002, configure backup servers on the Configuration | System | Tunneling Protocols | IPSec screen.

The list you configure on the VPN 3002 applies only if the option, Use Client Configured List, is set in the IPSec Backup Servers parameter. To set this option, go to the Mode Configuration tab on the Configuration | User Management | Groups | Add/Modify screen of the primary VPN Concentrator to which the VPN 3002 connects.

**Note**

The group name, username, and passwords that you configure for the VPN 3002 must be identical for the primary VPN Concentrator and all backup servers. Also, if you require interactive hardware client authentication and/or individual user authentication for the VPN 3002 on the primary VPN Concentrator, be sure to configure it on backup servers as well.

Alert when disconnecting

The VPN 3002 notifies the VPN Concentrator at the central site of sessions that are about to be disconnected from its side of the connection, and conveys the reason. The VPN Concentrator decodes the reason, and displays it in the event log or in a pop-up screen. The feature is enabled by default. This screen lets you disable the feature so that the VPN 3002 does not send or receive alerts.

Uncheck the box to disable alerts.

- The VPN 3002 no longer sends alerts when it disconnects sessions.
- The VPN 3002 does not receive alerts when the VPN Concentrator at the central site disconnects sessions.



Note

To send and receive alerts, the VPN 3002 and the VPN Concentrator to which the VPN 3002 connects must be running software version 4.0 or greater, and must have the feature enabled.

IPSec over TCP

Check IPSec over TCP if you want to connect using IPSec over TCP. This feature must also be enabled on the VPN Concentrator to which this VPN 3002 connects. See the explanation that follows.

IPSec over TCP Port

Enter the IPSec over TCP port number. You can enter one port. The port that you configure on the VPN 3002 must also match that configured on the VPN Concentrator to which this VPN 3002 connects.

About IPSec over TCP

IPSec over TCP encapsulates encrypted data traffic within TCP packets. This feature enables the VPN 3002 to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls.



Note

This feature does not work with proxy-based firewalls.

The VPN 3002 Hardware Client, which supports one tunnel at a time, can connect using either standard IPSec, IPSec over TCP, or IPSec over UDP or IPSec over NAT-T.

To use IPSec over TCP, both the VPN 3002 and the VPN Concentrator to which it connects must be running version 3.5 software.

Use Certificate

This parameter specifies whether to use preshared keys or a PKI (Public Key Infrastructure) digital identity certificate to authenticate the peer during Phase 1 IKE negotiations. See the discussion under Administration | Certificate Management, which is where you install digital certificates on the VPN 3002.

Check the box to use digital certificates.

Certificate Transmission

If you configured authentication using digital certificates, choose the type of certificate transmission.

- Entire certificate chain = Send the peer the identity certificate and all issuing certificates. Issuing certificates include the root certificate and any subordinate CA certificates.
- Identity certificate only = Send the peer only the identity certificate.

Group

The VPN 3002 connects to the VPN Concentrator using this Group name and password, which must be configured on the central-site VPN Concentrator. Group and usernames and passwords must be identical on the VPN 3002 and on the VPN Concentrator to which it connects.

Name

In the Group Name field, enter a unique name for the group to which this VPN 3002 belongs. This is the group name configured on the central-site VPN Concentrator to which this VPN 3002 connects. Maximum is 32 characters, case-sensitive.

Password

In the Group Password field, enter a unique password for this group. This is the group password configured on the VPN Concentrator to which this VPN 3002 connects. Minimum is 4, maximum is 32 characters, case-sensitive. The field displays only asterisks.

Verify

In the Group Verify field, re-enter the group password to verify it. The field displays only asterisks.

User

You must also enter a username and password, and they must match the username and password configured on the central-site VPN Concentrator to which this VPN 3002 connects.

Name

In the User Name field, enter a unique name for the user in this group. Maximum is 32 characters, case-sensitive. This is the username configured on the central-site VPN Concentrator to which this VPN 3002 connects. Maximum is 32 characters, case-sensitive.

Password

In the User Password field, enter the password for this user. This is the user password configured on the central-site VPN Concentrator to which this VPN 3002 connects. Minimum is 4, maximum is 32 characters, case-sensitive.

Verify

In the User Verify field, re-enter the user password to verify it. The field displays only asterisks.



IP Routing

The VPN 3002 includes an IP routing subsystem with static routing, default gateways, and DHCP.

To route packets, the subsystem uses static routes and the default gateway. If you do not configure the default gateway, the subsystem drops packets that it can not otherwise route.

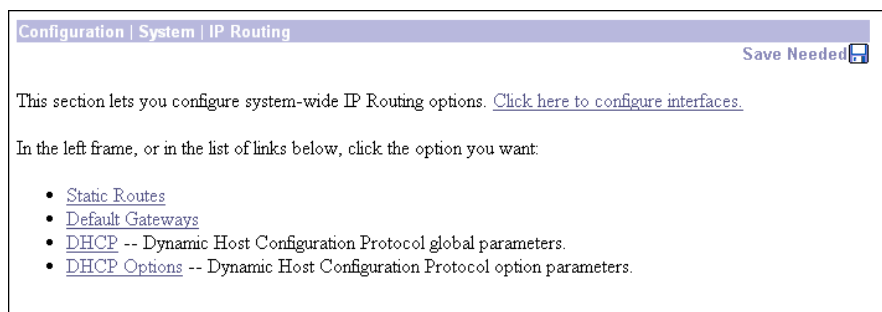
You configure static routes and default gateways in this section. This section also includes the system-wide DHCP (Dynamic Host Configuration Protocol) server parameters.

Configuration | System | IP Routing

This section of the Manager lets you configure system-wide IP routing parameters.

- **Static Routes:** manually configured routing tables.
- **Default Gateways:** routes for otherwise unrouted traffic.
- **DHCP:** Dynamic Host Configuration Protocol global parameters.
- **DHCP Options:** facilities that allow the VPN 3002 DHCP server to respond with configurable parameters for specific kinds of devices such as PCs, IP telephones, print servers, etc., as well as an IP address.

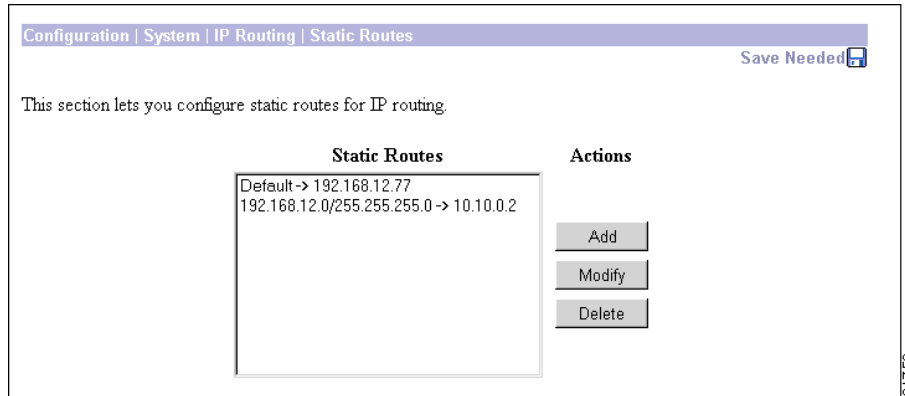
Figure 7-1 Configuration | System | IP Routing Screen



Configuration | System | IP Routing | Static Routes

This section of the Manager lets you configure static routes for IP routing.

Figure 7-2 Configuration | System | IP Routing | Static Routes Screen



Static Routes

The Static Routes list shows manual IP routes that have been configured. The format is [destination network address/subnet mask -> outbound destination]; for example, 192.168.12.0/255.255.255.0 -> 10.10.0.2. If you have configured the default gateway, it appears first in the list as [Default -> default router address]. If no static routes have been configured, the list shows --Empty--.

Add / Modify / Delete

To configure and add a new static route, click **Add**. The Manager opens the Configuration | System | IP Routing | Static Routes | Add screen.

To modify a configured static route, select the route from the list and click **Modify**. The Manager opens the Configuration | System | IP Routing | Static Routes | Modify screen. If you select the default gateway, the Manager opens the Configuration | System | IP Routing | Default Gateways screen.

To delete a configured static route, select the route from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining static routes in the list. You cannot delete the default gateways here; to do so, see the Configuration | System | IP Routing | Default Gateways screen.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | IP Routing | Static Routes | Add or Modify

These Manager screens let you:

- **Add:** Configure and add a new static, or manual, route to the IP routing table.
- **Modify:** Modify the parameters for a configured static route.

Figure 7-3 Configuration | System | IP Routing | Static Routes | Add Screen

Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address Enter the network address.

Subnet Mask Enter the subnet mask.

Metric Enter the numeric metric for this route (1 through 16).

Destination

Router Address Enter the router/gateway IP address.

Interface Ethernet 1 (Private) (10.10.147.2) Select the interface to route to.

Add Cancel

61755

Network Address

Enter the destination network IP address that this static route applies to. Packets with this destination address will be sent to the Destination below. Used dotted decimal notation; for example, 192.168.12.0.

Subnet Mask

Enter the subnet mask for the destination network IP address, using dotted decimal notation (for example, 255.255.255.0). The subnet mask indicates which part of the IP address represents the network and which part represents hosts. The router subsystem looks at only the network part.

The Manager automatically supplies a standard subnet mask appropriate for the IP address you just entered. For example, the IP address 192.168.12.0 is a Class C address, and the standard subnet mask is 255.255.255.0. You can accept this entry or change it. Note that 0.0.0.0 is not allowed here, since that would resolve to the equivalent of a default gateway.

Metric

Enter the metric, or cost, for this route. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if a route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Destination

Click a radio button to select the outbound destination for these packets. You can select only one destination: either a specific router/gateway, or a VPN 3002 interface.

Destination Router Address

Enter the IP address of the specific router or gateway to which to route these packets; that is, the IP address of the next hop between the VPN 3002 and the packet's ultimate destination. Use dotted decimal notation; for example, 10.10.0.2. We recommend that you select this option.

Interface

Click the drop-down menu button and select a configured VPN 3002 interface as the outbound destination. We do not recommend this option; enter a destination router address above.

Add or Apply / Cancel

To add a new static route to the list of configured routes, click **Add**. Or to apply your changes to a static route, click **Apply**. Both actions include your entries in the active configuration. The Manager returns to the Configuration | System | IP Routing | Static Routes screen. Any new route appears at the bottom of the Static Routes list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing | Static Routes screen, and the Static Routes list is unchanged.

Configuration | System | IP Routing | Default Gateways

This screen lets you configure the default gateway for IP routing. You use this same screen both to initially configure and to change default gateways. You can also configure the default gateway on the Configuration | Quick | System Info screen.

The IP routing subsystem routes data packets first using static routes, then the default gateway. If you do not specify a default gateway, the system drops packets it can not otherwise route.

Figure 7-4 Configuration | System | IP Routing | Default Gateways Screen

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

61756

Default Gateway

Enter the IP address of the default gateway or router. Use dotted decimal notation; for example, 192.168.12.77. This address must not be the same as the IP address configured on any VPN 3002 interface. If you do not use a default gateway, enter 0.0.0.0 (the default entry).

To delete a configured default gateway, enter 0.0.0.0.

The default gateway must be reachable from a VPN 3002 interface, and it is usually on the public network. The Manager displays a warning screen if you enter an IP address that is not on one of its interface networks, and it displays a dialog box if you enter an IP address that is not on the public network.

Metric

Enter the metric, or cost, for the route to the default gateway. Use a number from 1 to 16, where 1 is the lowest cost. The routing subsystem always tries to use the least costly route. For example, if this route uses a low-speed line, you might assign a high metric so the system will use it only if all high-speed routes are unavailable.

Apply / Cancel

To apply the settings for default gateways, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen. If you configure a Default Gateway, it also appears in the Static Routes list on the Configuration | System | IP Routing | Static Routes screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Configuration | System | IP Routing | DHCP

This screen lets you configure DHCP (Dynamic Host Configuration Protocol) server parameters that apply to DHCP server functions within the VPN 3002.

The DHCP server for the private interface lets IP hosts in its network automatically obtain IP addresses from a limited pool of addresses for a fixed length of time, or *lease period*. Before the lease period expires, the VPN 3002 displays a message offering to renew it. If the lease is not renewed, the connection terminates when the lease expires, and the IP address becomes available for reuse. Using DHCP simplifies configuration since you do not need to know what IP addresses are considered valid on a particular network.

Figure 7-5 Configuration | System | IP Routing | DHCP Screen

Enabled

Check the box to enable the DHCP server functions on the VPN 3002. The box is checked by default. To use DHCP address assignment, you must enable DHCP functions here.

Lease Timeout

Enter the timeout in minutes for addresses that are obtained from the DHCP server. Minimum is 5, default is 120, maximum is 500000 minutes. DHCP servers “lease” IP addresses to clients on the VPN 3002 private network for this period of time.

The Lease Timeout period you configure applies only when the tunnel to the VPN Concentrator is established. When the tunnel is not established, the Lease Timeout period is 5 minutes.

Address Pool Start/End

Enter the range of IP addresses that the DHCP server can assign. Use dotted decimal notation. The default is 127 successive addresses, with the first address being the address immediately after that of the private interface. The maximum number of addresses you can configure is 127.

Apply/Cancel

To apply the settings for DHCP parameters, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | IP Routing screen.

Reminder:

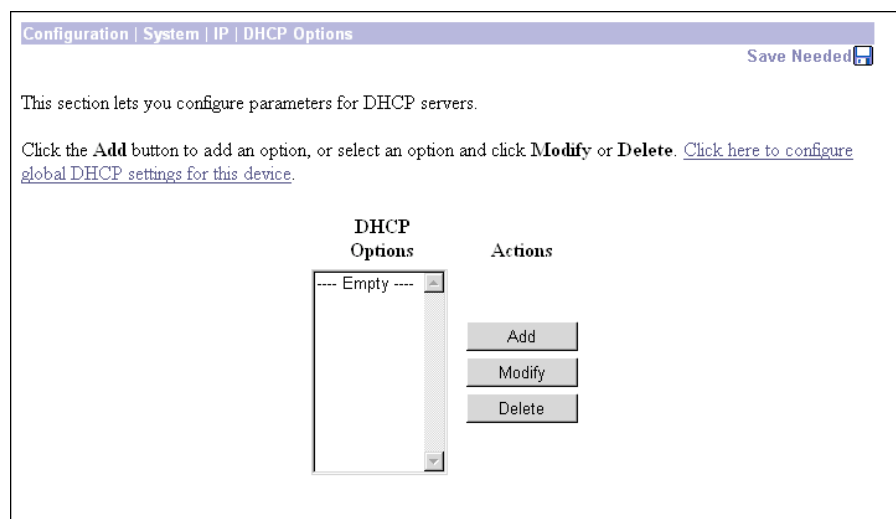
To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | IP Routing screen.

Configuration | System | IP Routing | DHCP Options

This section lets you configure DHCP options.

Figure 7-6 Configuration | System | IP Routing | DHCP Options Screen



DHCP Option

DHCP Options are facilities that allow the VPN 3002 DHCP server to respond to configurable parameters for specific kinds of devices such as PCs, IP telephones, print servers, etc., as well as an IP address.

Add/Modify/Delete

To configure and add DHCP options, click **Add**. The Manager opens the Configuration | System | IP | DHCP Options | Add screen. To modify a configured DHCP option, select the option from the list and click **Modify**. The Manager opens the Configuration | System | IP | DHCP Options | Modify screen.

To remove a configured DHCP option, select the option from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining DHCP options in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | IP Routing | DHCP Options | Add or Modify

These screens let you:

Add a new DHCP option to the list of DHCP options this VPN 3002 uses.

Modify a configured DHCP option.

Figure 7-7 Configuration | System | IP Routing | DHCP Options | Add Screen

DHCP Option

Use the pull-down menu to the DHCP Options field to select the option you want to add or modify. You can add or modify only one option at a time.



Note

Configured VPN 3002 DHCP server options are sent to DHCP client only if those options are specified in the Parameters Request List of the DHCPDISCOVER and DHCPREQUEST messages.

Option Value

Enter the value you want this option to use, for example, the IP address for the TFTP server option, the number of seconds for the ARP Cache Timeout option, 1 or 0 to enable or disable IP forwarding, etc.

Nonconfigurable DHCP Options

You cannot configure the following DHCP Options:

- Subnet Mask (option 1)
- Router (option 3)
- Domain Name Server (option 6)
- Domain Name (option 15)
- NetBios Name Server/WINS (option 44).

You configure these values on the central-site VPN Concentrator for the group to which the VPN 3002 Hardware Client belongs. As is the case for all group configuration parameters, the central-site VPN Concentrator pushes these values to the VPN 3002 over the tunnel.



Management Protocols

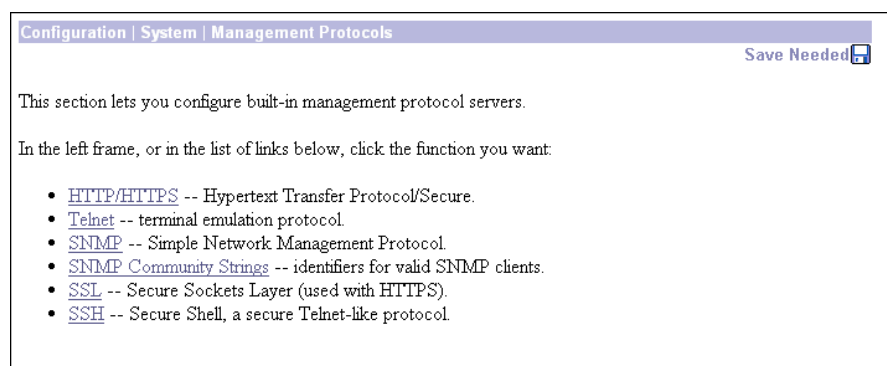
The VPN 3002 Hardware Client includes various built-in servers, using various protocols, that let you perform typical network and system management functions. This section explains how you configure and enable those servers.

Configuration | System | Management Protocols

This section of the Manager lets you configure and enable built-in VPN 3002 servers that provide management functions using:

- **HTTP/HTTPS:** Hypertext Transfer Protocol, and HTTP over SSL (Secure Sockets Layer) protocol.
- **Telnet:** terminal emulation protocol, and Telnet over SSL.
- **SNMP:** Simple Network Management Protocol.
- **SNMP Community Strings:** identifiers for valid SNMP clients.
- **SSL:** Secure Sockets Layer protocol.
- **SSH:** Secure Shell.
- **XML:** Extensible Markup Language

Figure 8-1 Configuration | System | Management Protocols Screen



Configuration | System | Management Protocols | HTTP/HTTPS

This screen lets you configure and enable the VPN 3002 HTTP/HTTPS server: Hypertext Transfer Protocol and HTTP over SSL (Secure Sockets Layer) protocol. When the server is enabled, you can use a Web browser to communicate with the VPN 3002. HTTPS lets you use a Web browser over a secure, encrypted connection.

About HTTP/HTTPS

The Manager requires the HTTP/HTTPS server. *If you click **Apply**, even if you have made no changes on this screen, you break your HTTP/HTTPS connection and you must restart the Manager session from the login screen.*

If you disable *either* HTTP or HTTPS, and that is the protocol you are currently using, you can reconnect with the other protocol if it is enabled and configured.

If you disable *both* HTTP and HTTPS, you cannot use a Web browser to connect to the VPN 3002. Use the Cisco command-line interface from the console or a Telnet session.

Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see Chapter 1.
- To configure SSL parameters, see the Configuration | System | Management Protocols | SSL screen.
- To install, generate, view, or delete the SSL certificate on the VPN 3002, see the Administration | Certificate Management screens.

Figure 8-2 Configuration | System | Management Protocols | HTTP/HTTPS Screen

Configuration | System | Management Protocols | HTTP/HTTPS

Configure the HTTP/HTTPS server.

Warning: If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Enable HTTP Disabling will provide additional security.

Enable HTTPS HTTPS uses SSL encryption to provide security.

Enable HTTPS on Public Check to enable HTTPS on the Public interface.

HTTP Port The default port is 80. Changing the port will provide additional security.

HTTPS Port The default port is 443. Changing the port will provide additional security.

Maximum Sessions Enter the maximum number of concurrent HTTP/HTTPS server users.

61760

Enable HTTP

Check the box to enable the HTTP server. The box is checked by default. HTTP must be enabled to install the SSL certificate in the browser initially, so you can thereafter use HTTPS. Disabling the HTTP server provides additional security, but makes system management less convenient. See the notes above.

Enable HTTPS

Check the box to enable the HTTPS server. The box is checked by default. HTTPS, also known as HTTP over SSL, lets you use the Manager over an encrypted connection.

Enable HTTPS on Public

Check the box to enable HTTPS on the Public interface.

HTTP Port

Enter the port number that the HTTP server uses. The default is 80, which is the well-known port.

HTTPS Port

Enter the port number that the HTTPS server uses. The default is 443, which is the well-known port.

Maximum Sessions

Enter the maximum number of concurrent, combined HTTP and HTTPS sessions (users) that the server allows. Minimum is 1, default is 4, maximum is 10.

Apply/Cancel

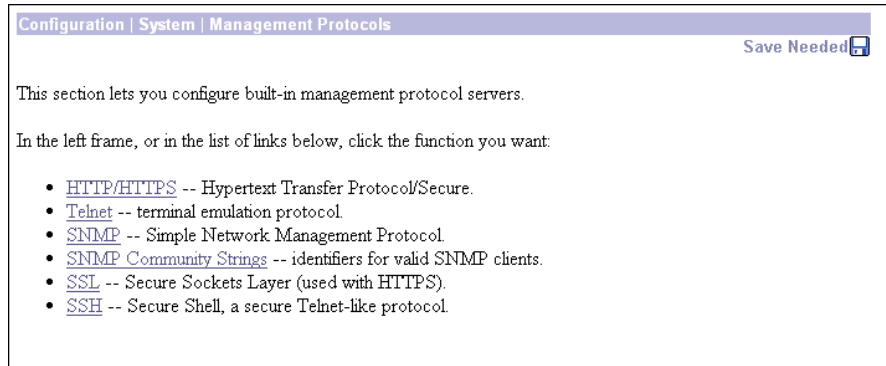
To apply your HTTP/HTTPS server settings, to include your settings in the active configuration, *and to break the current HTTP/HTTPS connection*, click **Apply**. If HTTP or HTTPS is still enabled, the Manager returns to the main login screen. If both HTTP and HTTPS are disabled, you can no longer use the Manager, and you will have to gain access through the console other configured connection.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Figure 8-3 Configuration | System | Management Protocols Screen



Configuration | System | Management Protocols | Telnet

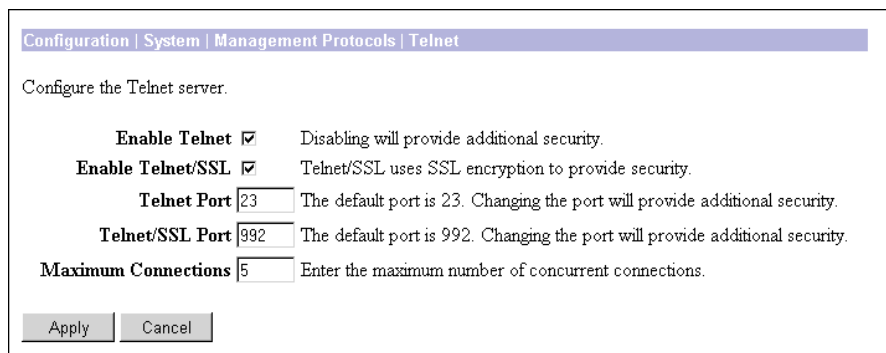
This screen lets you configure and enable the VPN 3002 Telnet terminal emulation server, and Telnet over SSL (Secure Sockets Layer protocol). When the server is enabled, you can use a Telnet client to communicate with the VPN 3002. You can fully manage and administer the VPN 3002 using the Cisco Command Line Interface (CLI) via Telnet.

Telnet server login usernames and passwords are the same as those enabled and configured on the Administration | Access Rights | Administrators screens.

Telnet/SSL uses a secure, encrypted connection. This enabled by default for Telnet/SSL clients.

See the Configuration | System | Management Protocols | SSL screen to configure SSL parameters. See the Administration | Certificate Management | Certificates screen to manage the SSL digital certificate.

Figure 8-4 Configuration | System | Management Protocols | Telnet Screen



Enable Telnet

Check the box to enable the Telnet server. The box is checked by default. Disabling the Telnet server provides additional security, but doing so prevents using the Cisco CLI via Telnet.

Enable Telnet/SSL

Check the box to enable Telnet over SSL. The box is checked by default. Telnet/SSL uses Telnet over a secure, encrypted connection.

Telnet Port

Enter the port number that the Telnet server uses. The default is 23, which is the well-known port number.

Telnet/SSL Port

Enter the port number that Telnet over SSL uses. The default is 992, which is the well-known port number.

Maximum Connections

Enter the maximum number of concurrent, combined Telnet and Telnet/SSL connections that the server allows. Minimum is 1, default is 5, maximum is 10.

Apply / Cancel

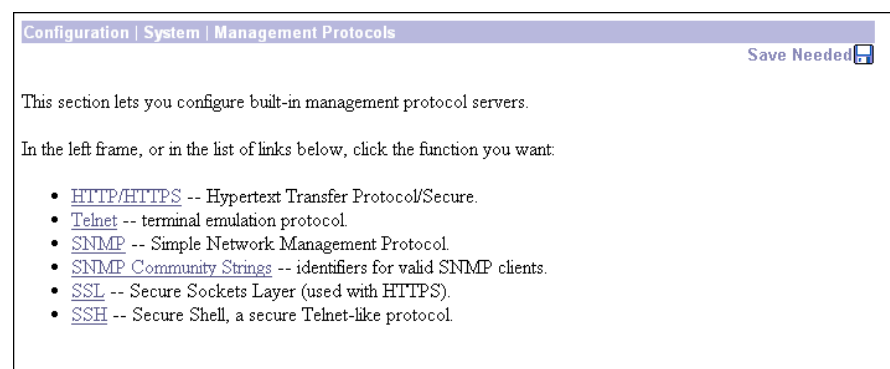
To apply your Telnet settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click Cancel. The Manager returns to the Configuration | System | Management Protocols screen.

Figure 8-5 Configuration | System | Management Protocols Screen



Configuration | System | Management Protocols | SNMP

This screen lets you configure and enable the SNMP (Simple Network Management Protocol) agent. When enabled, you can use an SNMP manager to collect information from the VPN 3002 but not to configure it.

To use SNMP, you must also configure an SNMP Community on the Configuration | System | Management Protocols | SNMP Communities screen.

The settings on this screen have no effect on sending system events to SNMP trap destinations (see Configuration | System | Events | General and Trap Destinations). For those functions, the VPN 3002 acts as an SNMP client.

Figure 8-6 Configuration | System | Management Protocols | SNMP Screen

Enable SNMP

Check the box to enable SNMP. The box is checked by default. Disabling SNMP provides additional security.

SNMP Port

Enter the port number that SNMP uses. The default is 161, which is the well-known port number. Changing the port number provides additional security.

Maximum Queued Requests

Enter the maximum number of outstanding queued requests that the SNMP agent allows. Minimum is 1, default is 4, maximum is 200.

Apply / Cancel

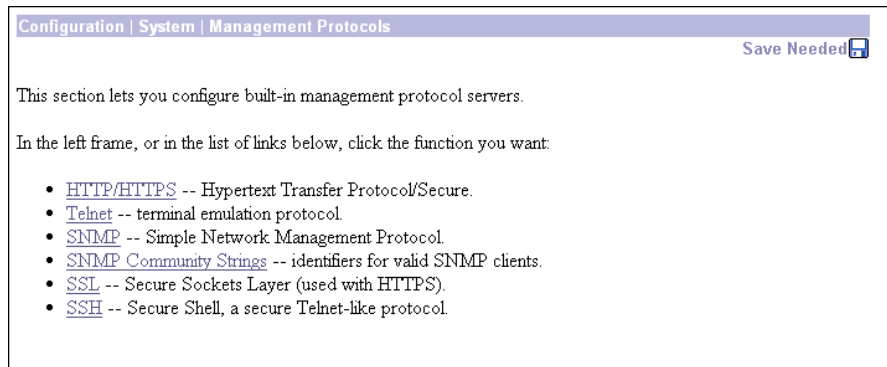
To apply your SNMP settings, and to include the settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Figure 8-7 Configuration | System | Management Protocols Screen

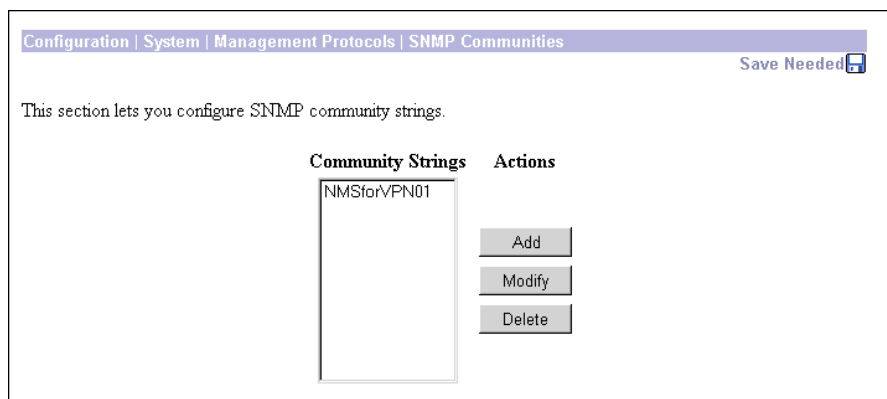


Configuration | System | Management Protocols | SNMP Communities

This section of the Manager lets you configure and manage SNMP community strings, which identify valid communities from which the SNMP agent accepts requests. A community string is like a password: it validates messages between an SNMP manager and the agent.

To use the VPN 3002 SNMP agent, you must configure and add at least one community string. You can configure a maximum of 10 community strings. To protect security, the SNMP agent does *not* include the usual default public community string, and we recommend that you not configure it.

Figure 8-8 Configuration | System | Management Protocols | SNMP Communities screen



Community Strings

The Community Strings list shows SNMP community strings that have been configured. If no strings have been configured, the list shows **--Empty--**.

Add/Modify/Delete

To configure and add a new community string, click **Add**. The Manager opens the Configuration | System | Management Protocols | SNMP Communities | Add screen.

To modify a configured community string, select the string from the list and click **Modify**. The Manager opens the Configuration | System | Management Protocols | SNMP Communities | Modify screen.

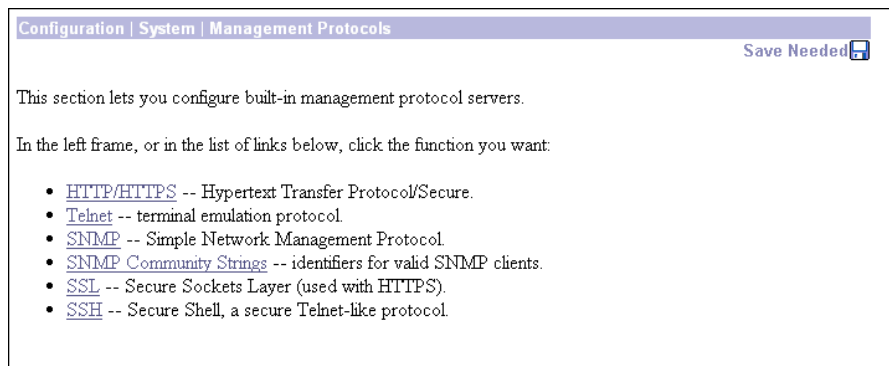
To delete a configured community string, select the string from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Figure 8-9 Configuration | System | Management Protocols Screen



Configuration | System | Management Protocols | SNMP Communities | Add or Modify

These Manager screens let you:

- **Add:** Configure and add a new SNMP community string.
- **Modify:** Modify a configured SNMP community string.

Figure 8-10 Configuration | System | Management Protocols | SNMP Communities | Add Screen

Configuration | System | Management Protocols | SNMP Communities | Add

Add an SNMP Community string.

Community String Enter the community string.

Add Cancel

61765

Community String

Enter the SNMP community string. Maximum 31 characters, case-sensitive.

Add or Apply / Cancel

To add this entry to the list of configured community strings, click **Add**. Or to apply your changes to this community string, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Management Protocols | SNMP Communities screen; a new entry appears at the bottom of the Community Strings list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your entry or changes, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols | SNMP Communities screen, and the Community Strings list is unchanged.

Figure 8-11 Configuration | System | Management Protocols Screen

Configuration | System | Management Protocols

Save Needed

This section lets you configure built-in management protocol servers.

In the left frame, or in the list of links below, click the function you want:

- [HTTP/HTTPS](#) -- Hypertext Transfer Protocol/Secure.
- [Telnet](#) -- terminal emulation protocol.
- [SNMP](#) -- Simple Network Management Protocol.
- [SNMP Community Strings](#) -- identifiers for valid SNMP clients.
- [SSL](#) -- Secure Sockets Layer (used with HTTPS).
- [SSH](#) -- Secure Shell, a secure Telnet-like protocol.

61699

Configuration | System | Management Protocols | SSL

This screen lets you configure the VPN 3002 SSL (Secure Sockets Layer) protocol server. These settings apply to both HTTPS and Telnet over SSL. HTTPS lets you use a web browser over a secure, encrypted connection to manage the VPN 3002.

SSL creates a secure session between the client and the VPN 3002 server. The client first authenticates the server, they negotiate session security parameters, and then they encrypt all data passed during the session. If, during negotiation, the server and client cannot agree on security parameters, the session terminates.

SSL uses digital certificates for authentication. The VPN 3002 creates a self-signed SSL server certificate when it boots; or you can install in the VPN 3002 an SSL certificate that has been issued in a PKI context. This certificate must then be installed in the client (for HTTPS; Telnet does not usually require it). You need to install the certificate from a given VPN 3002 only once.

The default SSL settings should suit most administration tasks and network security requirements. *We recommend that you not change them without good reason.*

**Note**

To ensure the security of your connection to the Manager, if you click **Apply** on this screen, *even if you have made no changes*, you break your connection to the Manager and you must restart the Manager session from the login screen.

Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see Chapter 1.
- To configure HTTPS parameters, see the Configuration | System | Management Protocols | HTTP/HTTPS screen.
- To configure Telnet/SSL parameters, see the Configuration | System | Management Protocols | Telnet screen.
- To manage SSL digital certificates, see the Administration | Certificate Management screens.

Figure 8-12 Configuration | System | Management Protocols | SSL Screen

Configuration | System | Management Protocols | SSL

Configure SSL.

If you click **Apply**, you will break your HTTP/HTTPS connection to this device, and you will have to restart from the login screen.

Encryption Protocols

- RC4-128/MD5
- 3DES-168/SHA
- DES-56/SHA
- RC4-40/MD5 Export
- DES-40/SHA Export

Check the encryption algorithms to enable. Unchecking them all disables SSL.

Client Authentication

Check to enable client authentication. Client authentication requires an installed Certificate Authority and a personal certificate installed in your browser.

SSL Version

Select the SSL version to use. Using a SSL V2 Hello provides compatibility with most browsers.

Generated Certificate Key Size

Select the key size used in the generated certificate.

61766

Encryption Protocols

Check the boxes for the encryption algorithms that the VPN 3002 SSL server can negotiate with a client and use for session encryption. All are checked by default. You must check at least one algorithm to enable SSL. *Unchecking all algorithms disables SSL.*

The algorithms are negotiated in the following order (you cannot change the order, but you can enable or disable selected algorithms):

- **RRC4-128/MD5** = RC4 encryption with a 128-bit key and the MD5 hash function. This option is available in most SSL clients.
- **3DES-168/SHA** = Triple-DES encryption with a 168-bit key and the SHA-1 hash function. This is the strongest (most secure) option.
- **DES-56/SHA** = DES encryption with a 56-bit key and the SHA-1 hash function.
- **RC4-40/MD5 Export** = RC4 encryption with a 128-bit key, 40 bits of which are private, and the MD5 hash function. This option is available in the non-U.S. versions of many SSL clients.
- **DES-40/SHA Export** = DES encryption with a 56-bit key, 40 bits of which are private, and the SHA-1 hash function. This option is available in the non-U.S. versions of many SSL clients.

Client Authentication

This parameter applies to HTTPS only; it is ignored for Telnet/SSL.

Check the box to enable SSL client authentication. The box is not checked by default. In the most common SSL connection, the client authenticates the server, not vice-versa. Client authentication requires personal certificates installed in the browser, and trusted certificates installed in the server. Specifically, the VPN 3002 must have a root CA certificate installed; and a certificate signed by one of the VPN 3002 trusted CAs must be installed in the Web browser. See Administration | Certificate Management.

SSL Version

Click the drop-down menu button and select the SSL version to use. SSL Version 3 has more security options than Version 2, and TLS (Transport Layer Security) Version 1 has more security options than SSL Version 3. Some clients that send an SSL Version 2 “Hello” (initial negotiation), can actually use a more secure version during the session. Telnet/SSL clients usually can use only SSL Version 2.

Choices are:

- **Negotiate SSL V2/V3** = The server tries to use SSL Version 3 but accepts Version 2 if the client can not use Version 3. This is the default selection. This selection works with most browsers and Telnet/SSL clients.
- **SSL V3 with SSL V2 Hello** = The server insists on SSL Version 3 but accepts an initial Version 2 “Hello.”
- **SSL V3 Only** = The server insists on SSL Version 3 only.
- **SSL V2 Only** = The server insists on SSL Version 2 only. This selection works with most Telnet/SSL clients.
- **TLS V1 Only** = The server insists on TLS Version 1 only. At present, only Microsoft Internet Explorer 5.0 supports this option.
- **TLS V1 with SSL V2 Hello** = The server insists on TLS Version 1 but accepts an initial SSL Version 2 “Hello.” At present, only Microsoft Internet Explorer 5.0 supports this option.

Generated Certificate Key Size

Click the drop-down menu button and select the size of the RSA key that the VPN 3002 uses in its self-signed (generated) SSL server certificate. A larger key size increases security, but it also increases the processing necessary in all transactions over SSL. The increases vary depending on the type of transaction (encryption or decryption).

Choices are:

- **512-bit RSA Key** = This key size provides sufficient security. It is the most common, and requires the least processing.
- **768-bit RSA Key** = This key size provides normal security and is the default selection. It requires approximately 2 to 4 times more processing than the 512-bit key.
- **1024-bit RSA Key** = This key size provides high security. It requires approximately 4 to 8 times more processing than the 512-bit key.

Apply/Cancel

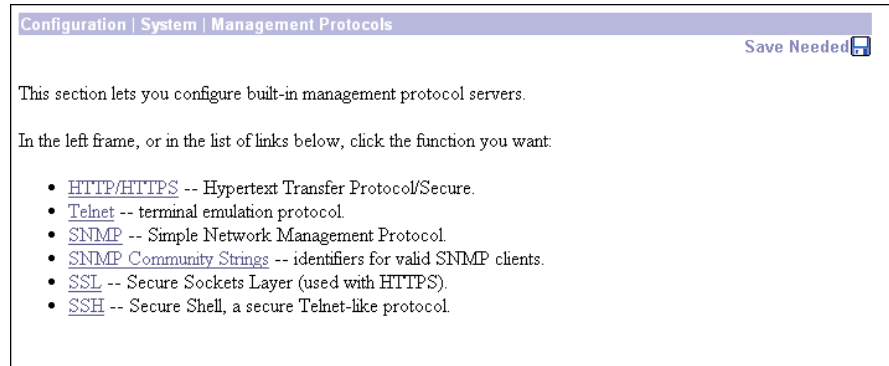
To apply your SSL settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the initial Login screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Figure 8-13 Configuration | System | Management Protocols Screen



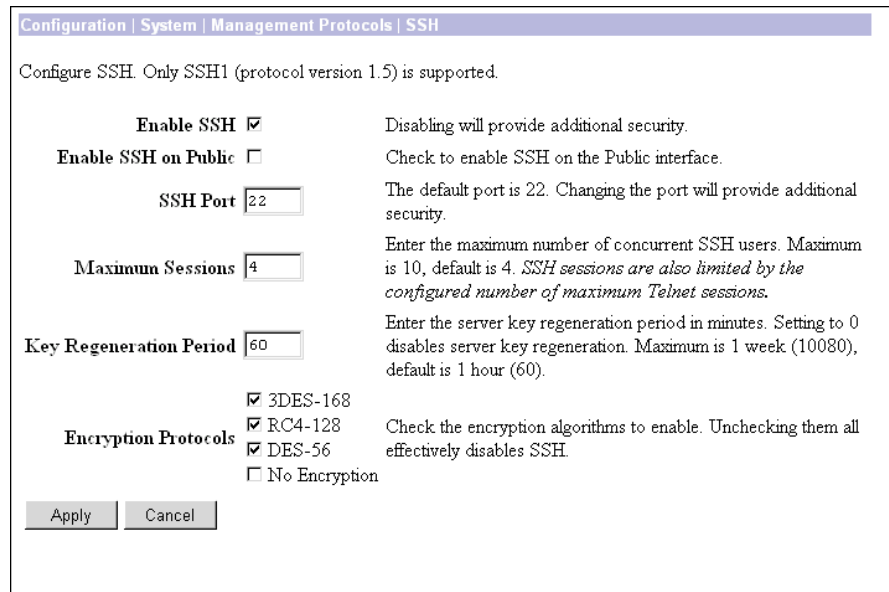
Configuration | System | Management Protocols | SSH

This screen lets you configure the VPN 3002 SSH (Secure Shell) protocol server. SSH is a secure Telnet-like terminal emulator protocol that you can use to manage the VPN 3002, using the Command Line Interface, over a remote connection.

The SSH server supports SSH1 (protocol version 1.5), which uses two RSA keys for security. All communication over the connection is encrypted. To provide additional security, the remote client authenticates the server and the server authenticates the client.

At the start of an SSH session, the VPN 3002 sends both a host key and a server key to the client, which responds with a session key that it generates and encrypts using the host and server keys. The RSA key of the SSL certificate is used as the host key, which uniquely identifies the VPN 3002. See Configuration | System | Management Protocols | SSL.

Figure 8-14 Configuration | System | Management Protocols | SSH screen



Enable SSH

Check the box to enable the SSH server. The box is checked by default. Disabling the SSH server provides additional security by preventing SSH access.

Enable SSH on Public

Check the box to enable SSH on the Public interface.

SSH Port

Enter the port number that the SSH server uses. The default is 22, which is the well-known port.

Maximum Sessions

Enter the maximum number of concurrent SSH sessions allowed. Minimum is 1, default is 4, and maximum is 10.

Key Regeneration Period

Enter the server key regeneration period in minutes. If the server key has been used for an SSH session, the VPN 3002 regenerates the key at the end of this period. Minimum is 0 (which disables key regeneration, default is 60 minutes, and maximum is 10080 minutes (1 week).



Note

Use 0 (disable key regeneration) only for testing, since it lessens security.

Encryption Protocols

Check the boxes for the encryption algorithms that the VPN 3002 SSH server can negotiate with a client and use for session encryption. All algorithms are checked by default. You must check at least one algorithm to enable a secure session. *Unchecking all algorithms disables SSH.*

- **3DES-168** = Triple-DES encryption with a 168-bit key. This option is the most secure but requires the greatest processing overhead.
- **RC4-128** = RC4 encryption with a 128-bit key. This option provides adequate security and performance.
- **DES-56** = DES encryption with a 56-bit key. This option is least secure but provides the greatest export flexibility.
- **No Encryption** = Connect without encryption. This option provides no security and is for testing purposes only. It is not checked by default.

Enable SCP

Check the Enable SCP check box to enable file transfers using secure copy (SCP) over SSH.

Apply / Cancel

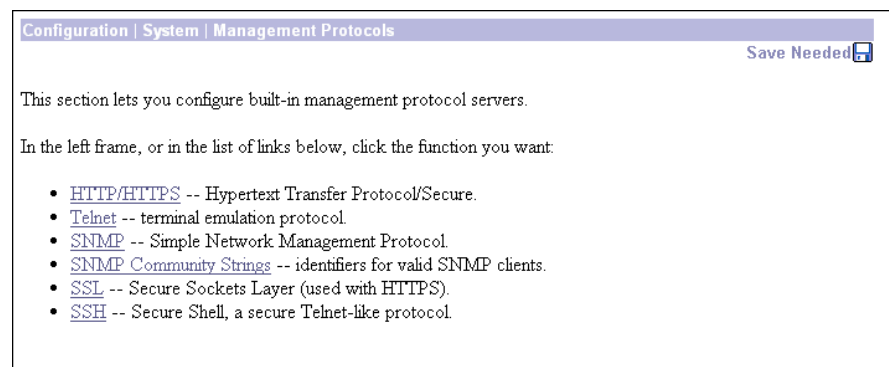
To apply your SSH settings, and to include your settings in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Management Protocols screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Management Protocols screen.

Figure 8-15 Configuration | System | Management Protocols Screen



Configuration | System | Management Protocols | XML

This screen lets you configure the VPN 3002 to support an XML-based interface. Enabling XML management (the default condition) allows the VPN 3002 to be more easily managed by a centralized management system. XML is enabled by default. To disable the XML option, clear the check box. To reenble the XML option, click the check box.

On this screen, you can also configure the VPN 3002 to enable HTTPS or SSH (or both) on the public interface and to lock the XML interface to a specific HTTPS or SSH IP address.

Figure 8-16 Configuration | System | Management Protocols | XML Screen

Configuration | System | Management Protocols | XML

Configure XML management.

Enable Check to enable XML management. Note that HTTPS or SSH must be enabled.

Enable HTTPS on Public Check to enable HTTPS on the Public interface. This will allow XML over HTTPS through the Public interface.

HTTPS IP Address Enter the IP address and wildcard from which to allow HTTPS access on on the Public interface. **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. Entering 0.0.0.0 will match the specified address; entering 255.255.255.255 will match *all* addresses.

HTTPS Wildcard-mask

Enable SSH on Public Check to enable SSH on the Public interface. This will allow XML over SSH through the Public interface.

SSH IP Address Enter the IP address and wildcard from which to allow SSH access on on the Public interface. **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. Entering 0.0.0.0 will match the specified address; entering 255.255.255.255 will match *all* addresses.

SSH Wildcard-mask

68224

Enable

Check the **Enable** check box, the default, to enable the XML management capability. You must also enable HTTPS or SSH on the VPN 3002 public interface. Disabling the XML management capability is not recommended.

Enable HTTPS on Public

Check the **Enable HTTPS on Public** check box to allow XML management over HTTPS on the VPN 3002 public interface.

Enable SSH on Public

Check the **Enable SSH on Public** check box to allow XML management over Secure Shell (SSH) on the VPN 3002 public interface.



Events

An *event* is any significant occurrence within or affecting the VPN 3002 such as an alarm, trap, error condition, network problem, task completion, threshold breach, or status change. The VPN 3002 records events in an event log, which is stored in nonvolatile memory. You can also specify that certain events trigger a console message, a UNIX syslog record, or an SNMP management system trap.

Event attributes include *class* and *severity level*. For detailed information about event classes and severity levels, see the *VPN 3002 Hardware Client Reference*, available online only.

Event Class

Event class denotes the source of the event and refers to a specific hardware or software subsystem within the VPN 3002. The following table describes the event classes.

Table 9-1 *Event Classes*

Class Name	Class Description (Event Source) (*Cisco-specific Event Class)
AUTH	Authentication*
AUTHDBG	Authentication debugging*
AUTHDECODE	Authentication protocol decoding*
AUTOUPDATE	Autoupdate subsystem*
CAPI	Cryptography subsystem*
CERT	Digital certificates subsystem
CONFIG	Configuration subsystem*
DHCP	DHCP subsystem
DHCPDBG	DHCP debugging*
DHCPDECODE	DHCP decoding*
DM	Data Movement subsystem*
DNS	DNS subsystem
DNSDBG	DNS debugging*
DNSDECODE	DNS decoding*
EVENT	Event subsystem*

Class Name	Class Description (Event Source) (*Cisco-specific Event Class)
EVENTDBG	Event subsystem debugging*
EVENTMIB	Event MIB changes*
FSM	Finite State Machine subsystem (for debugging)*
FTPD	FTP daemon subsystem
GENERAL	NTP subsystem and other general events
HARDWAREMON	Hardware monitoring (fans, temperature, voltages, etc.)
HTTP	HTTP subsystem
HWDIAG	Hardware diagnostics for WAN module*
IKE	ISAKMP/Oakley (IKE) subsystem
IKEDBG	ISAKMP/Oakley (IKE) debugging*
IKEDECODE	ISAKMP/Oakley (IKE) decoding*
IP	IP router subsystem
IPDBG	IP router debugging*
IPDECODE	IP packet decoding*
IPSEC	IP Security subsystem
IPSECDBG	IP Security debugging*
IPSECDECODE	IP Security decoding*
LBSSF	Load Balancing/Secure Session Failover subsystem*
MIB2TRAP	MIB-II trap subsystem: SNMP MIB-II traps*
PPP	PPP subsystem
PPPDBG	PPP debugging*
PPPDECODE	PPP decoding*
PPPoE	PPPoE subsystem
PSH	Operating system command shell*
PSOS	Embedded real-time operating system*
QUEUE	System queue*
REBOOT	System rebooting
RM	Resource Manager subsystem*
SNMP	SNMP trap subsystem
SSH	SSH subsystem
SSL	SSL subsystem
SYSTEM	Buffer, heap, and other system utilities*
TCP	TCP subsystem
TELNET	Telnet subsystem
TELNETDBG	Telnet debugging*
TELNETDECODE	Telnet decoding*
TIME	System time (clock)



Note The Cisco-specific event classes provide information that is meaningful only to Cisco engineering or support personnel. Also, the DBG and DECODE events require significant system resources and might seriously degrade performance. We recommend that you avoid logging these events unless Cisco requests it.

Event Severity Level

Severity level indicates how serious or significant the event is; that is, how likely it is to cause unstable operation of the VPN 3002, whether it represents a high-level or low-level operation, or whether it returns little or great detail. Level 1 is most significant. [Table 9-2](#) describes the severity levels.

Table 9-2 Event Severity Levels

Level	Category	Description
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that may require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.
6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding.
11	Packet Decode	Low-level packet header decoding.
12	Packet Decode	Hex dump of header.
13	Packet Decode	Hex dump of packet.

Within a severity level category, higher-numbered events provide more details than lower-numbered events, without necessarily duplicating the lower-level details. For example, within the Information category, Level 6 provides greater detail than Level 4 but does not necessarily include the same information as Level 4.

Logging higher-numbered severity levels degrades performance, since more system resources are used to log and handle these events.



Note The Debug (7–9) and Packet Decode (10–13) severity levels are intended for use by Cisco engineering and support personnel. We recommend that you avoid logging these events unless Cisco requests it.

The VPN 3002, by default, displays all events of severity level 1 through 3 on the console. It writes all events of severity level 1 through 5 to the event log. You can change these defaults on the Configuration | System | Events | General screen, and you can configure specific events for special handling on the Configuration | System | Events | Classes screens.

Event Log

The VPN 3002 records events in an event log, which is stored in nonvolatile memory. Thus the event log persists even if the system is powered off. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The VPN 3002 holds 256 events. The log wraps when it is full; that is, newer events overwrite older events when the log is full.

For the event log, you can configure which event classes and severity levels to log.



NoteThe VPN 3002 automatically saves the log file if it crashes, and when it is rebooted. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging.

Event Log Data

Each entry (record) in the event log consists of several fields including:

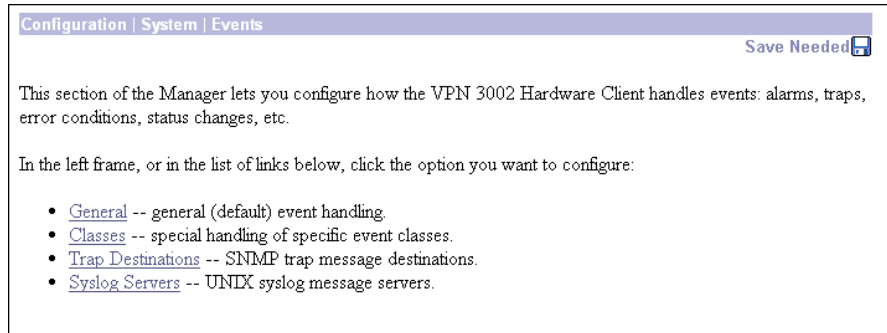
- A sequence number.
- Date and time.
- Event severity level.
- Event class and number.
- Event repetition count.
- Event IP address (only for certain events).
- Description string.

For more information, see the [Monitoring | Filterable Event Log](#) screen.

Configuration | System | Events

This section of the Manager lets you configure how the VPN 3002 handles events. Events provide information for system monitoring, auditing, management, accounting, and troubleshooting.

Figure 9-1 Configuration | System | Events Screen



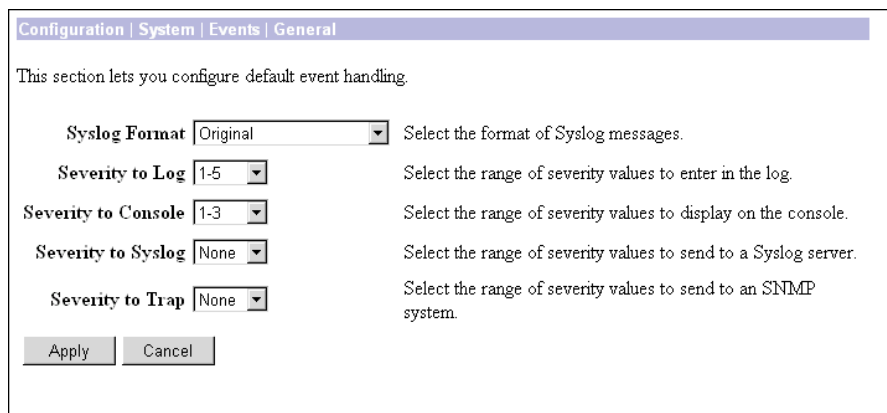
61768

Configuration | System | Events | General

This Manager screen lets you configure the general, or default, handling of all events. These defaults apply to all event classes.

You can override these default settings by configuring specific events for special handling on the Configuration | System | Events | Classes screens.

Figure 9-2 Configuration | System | Events | General Screen



61769

Syslog Format

Click the Syslog Format drop-down menu button and choose the format for all events sent to UNIX syslog servers. Choices are:

- Original = Original VPN 3002 event format with information on one line. Each entry in the event log consists of the following fields:

Sequence Date Time SEV=Severity Class/Number RPT=RepeatCount String

- *Sequence*: The sequence number of the event.
- *Date*: The date the event occurred. The date is in the following format: MM/DD/YYYY.
- *Time*: The time the event occurred. The time is in the following format: hh:mm:ss.ttt.
- *Severity*: The severity of the event (1-13). To see how this original severity level maps to Cisco IOS severity levels, see the “Cisco IOS Severities” table.
- *Class/Number*: The event class and event number. For a list of event classes, see the “Events” chapter.
- *RepeatCount*: The number of times this particular event has occurred since the VPN 3002 was last booted.
- *String*: The description of the event. The string sometimes includes the IP address of the user whose session generated the event.

For example:

```
3 12/06/1999 14:37:06.680 SEV=4 HTTP/47 RPT=17 10.10.1.35 New administrator login:
admin.
```

- Cisco IOS Compatible = Event format that is compatible with Cisco syslog management applications. Each entry in the event log is one line consisting of the following fields:

Sequence: Date Time TimeZone TimeZoneOffset %Class-Severity-Number: RPT=RepeatCount: String

- *Sequence*: The sequence number of the event.
- *Date*: The date the event occurred. The date is in the following format: YYYY MMM DD.
- *Time*: The time the event occurred. The time is in the following format: hh:mm:ss.ttt.
- *TimeZone*: The time zone in which the event occurred.
- *TimeZoneOffset*: The offset of the time zone from GMT.
- *Class*: The event class. For a list of event classes, see the “Events” chapter.
- *Severity*: The Cisco IOS severity of the event (0-7). The “Cisco IOS Severities” table shows the mapping between Cisco IOS format severity levels and Original format severity levels.
- *Number*: The event number.
- *RepeatCount*: The number of times this particular event has occurred since the VPN Concentrator was last booted.
- *String*: The description of the event. The string sometimes includes the IP address of the user whose session generated the event.

For example:

```
3 1999 Dec 06 14:37:06.680 EDT -4:00 %HTTP-5-47:RPT=17 10.10.1.35: New
administrator login: admin.
```

The Original severities and the Cisco IOS severities differ. Original severities number from 1-13. (For the meaning of each Original severity, see Table 8-1.) Cisco IOS severities number from 0–7. The “[Cisco IOS Severities](#)” table that follows shows the meaning of Cisco IOS severities and how they map to Original severities.

Table 9-3 Cisco IOS Severities

Cisco IOS Severity	Meaning	Original Severity
0	Emergencies	1
1	Alerts	Not used
2	Critical	2
3	Errors	Not used
4	Warning	3
5	Notification	4
6	Informational	5, 6
7	Debugging	7-13

Severity to Log

Click the drop-down menu button and select the range of event severity levels to enter in the event log by default. The choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is 1-5; if you choose this range, all events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the drop-down menu button and select the range of event severity levels to display on the console by default. The choices are: None, 1, 1-2, 1-3, ..., 1-13. The default is 1-3; if you choose this range, all events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the drop-down menu button and select the range of event severity levels to send to a UNIX syslog server by default. The choices are: None, 1, 1-2, 1-3, ..., 1-6. The default is None; if you choose this range, no events are sent to a syslog server.

If you select any severity levels to send, you must also configure the syslog server(s) on the Configuration | System | Events | Syslog Servers screens.

Severity to Trap

Click the drop-down menu button and select the range of event severity levels to send to an SNMP network management system (NMS) by default. Event messages sent to SNMP systems are called “traps.” The choices are: None, 1, 1-2, 1-3. The default is None; if you choose this range, no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the Configuration | System | Events | Trap Destinations screens.

The VPN 3002 can send the standard, or “well-known,” SNMP traps listed in [Table 9-4](#). To have an SNMP NMS receive them, you must configure the events as in the table, and configure a trap destination.

Table 9-4 Configuring “Well-Known” SNMP Traps

To send this “well-known” SNMP trap	Configure either General event handling or this Event Class	With this Severity to Trap
coldStart	EVENT	1 or higher
linkDown	IP	1-3 or higher
linkUp	IP	1-3 or higher
authFailure ¹	SNMP	1-3 or higher

1. This trap is SNMP authentication failure, not tunnel authentication failure.

Apply/Cancel

To include your settings for default event handling in the active configuration, click **Apply**. The Manager returns to the Configuration | System | Events screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

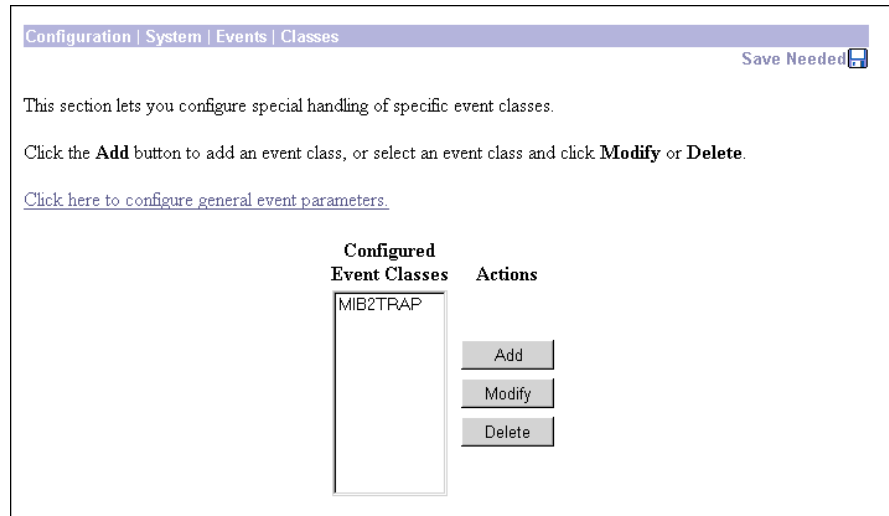
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events screen.

Configuration | System | Events | Classes

This section of the Manager lets you add, configure, modify, and delete specific event classes for special handling. You can thus override the general, or default, handling of event classes. For example, you might want to send email for HARDWAREMON events of severity 1-2, whereas default event handling does not send any email.

Event classes denote the source of an event and refer to a specific hardware or software subsystem within the VPN 3002. Table 8-1 describes the event classes.

Figure 9-3 Configuration | System | Events | Classes Screen



To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*”

Configured Event Classes

The Configured Event Classes list shows the event classes that have been configured for special handling. The initial default entry is MIB2TRAP, which are SNMP MIB-II events, or “traps,” that you might want to monitor with an SNMP network management system. Other configured event classes are listed in order by class number and name. If no classes have been configured for special handling, the list shows --Empty--.

Add/Modify/Delete

To configure and add a new event class for special handling, click **Add**. See Configuration | System | Events | Classes | Add.

To modify an event class that has been configured for special handling, select the event class from the list and click **Modify**. See Configuration | System | Events | Classes | Modify.

To remove an event class that has been configured for special handling, select the event class from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Classes | Add or Modify

These screens let you:

Add: Configure and add the special handling of a specific event class.

Modify: Modify the special handling of a specific event class.

Figure 9-4 Configuration | System | Events | Classes | Add Screen

Class Name

Add screen:

Click the drop-down menu button and select the event class you want to add and configure for special handling. (Please note that **Select Class** is an instruction reminder, not a class.) Table 8-1 describes the event classes.

Modify screen:

The field shows the configured event class you are modifying. You cannot change this field.

All subsequent parameters on this screen apply to this event class only.

Enable

Check this box to enable the special handling of this event class. (The box is checked by default.)

Clearing this box lets you set up the parameters for the event class but activate it later, or temporarily disable special handling without deleting the entry. The Configured Event Classes list on the Configuration | System | Events | Classes screen indicates disabled event classes. Disabled event classes are handled according to the default parameters for all event classes.

Severity to Log

Click the drop-down menu button and select the range of event severity levels to enter in the event log. The choices are: None, 1, 1-2, 1-3,..., 1-13. The default is 1-5; if you choose this range, events of severity level 1 through severity level 5 are entered in the event log.

Severity to Console

Click the drop-down menu button and select the range of event severity levels to display on the console. The choices are: None, 1, 1-2, 1-3,..., 1-13. The default is 1-3; if you choose this range, events of severity level 1 through severity level 3 are displayed on the console.

Severity to Syslog

Click the drop-down menu button and select the range of event severity levels to send to a UNIX syslog server. The choices are: None, 1, 1-2, 1-3,..., 1-13. The default is None; if you choose this range, no events are sent to a syslog server.



Note

Sending events to a syslog server generates IP packets, which can generate new events if this setting is above level 9. We strongly recommend that you keep this setting at or below level 6. Avoid setting this parameter above level 9.

If you select any severity levels to send, you must also configure the syslog server(s) on the Configuration | System | Events | Syslog Servers screens, and you should configure the Syslog Format on the Configuration | System | Events | General screen.

Severity to Trap

Click the drop-down menu button and select the range of event severity levels to send to an SNMP network management system. Event messages sent to SNMP systems are called “traps.” The choices are: None, 1, 1-2, 1-3, 1-4, 1-5. The default is None; if you choose this range, no events are sent as SNMP traps.

If you select any severity levels to send, you must also configure SNMP destination system parameters on the Configuration | System | Events | Trap Destinations screens.

To configure “well-known” SNMP traps, see [Table 9-4](#) under Severity to Trap for Configuration | System | Events | General.

Add or Apply/Cancel

To add this event class to the list of those with special handling, click **Add**. Or to apply your changes to this configured event class, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Classes screen. Any new event class appears in the Configured Event Classes list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events | Classes screen.

Configuration | System | Events | Trap Destinations

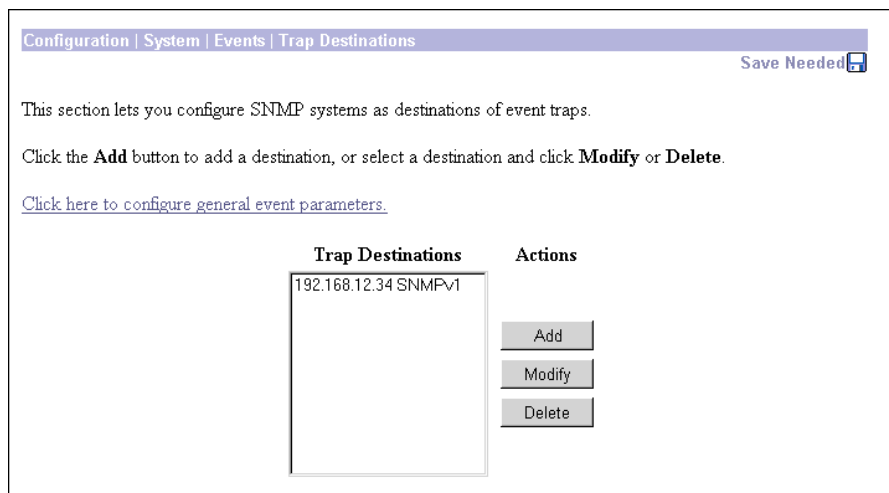
This section of the Manager lets you configure SNMP network management systems as destinations of event traps. Event messages sent to SNMP systems are called “traps.” If you configure any event handling, default or special, with values in Severity to Trap fields, you must configure trap destinations in this section.

To configure default event handling, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the Configuration | System | Events | Classes screens.

To configure “well-known” SNMP traps, see [Table 9-4](#) under Severity to Trap for Configuration | System | Events | General.

To have an SNMP-based network management system (NMS) receive any events, you must also configure the NMS to “see” the VPN 3002 as a managed device or “agent” in the NMS domain.

Figure 9-5 Configuration | System | Events | Trap Destinations Screen



Trap Destinations

The Trap Destinations list shows the SNMP network management systems that have been configured as destinations for event trap messages, and the SNMP protocol version associated with each destination. If no trap destinations have been configured, the list shows --Empty--.

Add/Modify/Delete

To configure a new SNMP trap destination, click **Add**. See Configuration | System | Events | Trap Destinations | Add.

To modify an SNMP trap destination that has been configured, select the destination from the list and click **Modify**. See Configuration | System | Events | Trap Destinations | Modify.

To remove an SNMP trap destination that has been configured, select the destination from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Trap Destinations | Add or Modify

These screens let you:

Add: Configure and add an SNMP destination system for event trap messages.

Modify: Modify a configured SNMP destination system for event trap messages.

Figure 9-6 Configuration | System | Events | Trap Destinations | Add Screen

Destination

Enter the IP address or hostname of the SNMP network management system that is a destination for event trap messages. (If you have configured a DNS server, you can enter a hostname; otherwise enter an IP address.)

SNMP Version

Click the drop-down menu button and select the SNMP protocol version to use when formatting traps to this destination. Choices are SNMPv1 (version 1; the default) and SNMPv2 (version 2).

Community

Enter the community string to use in identifying traps from the VPN 3002 to this destination. The community string is like a password: it validates messages between the VPN 3002 and this NMS destination. If you leave this field blank, the default community string is `public`.

Port

Enter the UDP port number by which you access the destination SNMP server. Use a decimal number from 0 to 65535. The default is 162, which is the well-known port number for SNMP traps.

Add or Apply/Cancel

To add this system to the list of SNMP trap destinations, click **Add**. Or to apply your changes to this trap destination, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Trap Destinations screen. Any new destination system appears in the Trap Destinations list.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

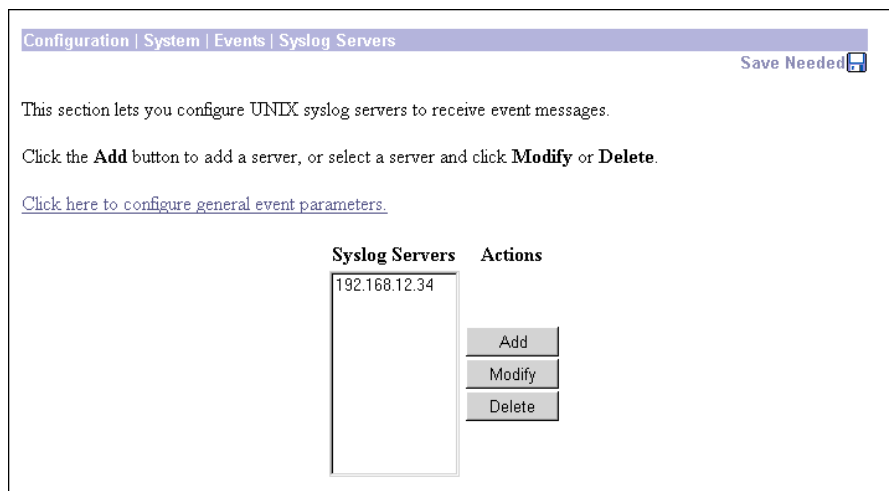
To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | Events | Trap Destinations screen, and the Trap Destinations list is unchanged.

Configuration | System | Events | Syslog Servers

This section of the Manager lets you configure UNIX syslog servers as recipients of event messages. Syslog is a UNIX daemon, or background process, that records events. The VPN 3002 can send event messages in two syslog formats to configured syslog systems. If you configure any event handling, default or special, with values in Severity to Syslog fields, you must configure syslog servers in this section.

To configure default event handling and syslog formats, click the highlighted link that says “*Click here to configure general event parameters.*” To configure special event handling, see the Configuration | System | Events | Classes screens.

Figure 9-7 Configuration | System | Events | Syslog Servers Screen



Syslog Servers

The Syslog Servers list shows the UNIX syslog servers that have been configured as recipients of event messages. You can configure a maximum of five syslog servers. If no syslog servers have been configured, the list shows --Empty--.

Add/Modify/Delete

To configure a new syslog server, click **Add**. See Configuration | System | Events | Syslog Servers | Add.

To modify a syslog server that has been configured, select the server from the list and click **Modify**. See Configuration | System | Events | Syslog Servers | Modify.

To remove a syslog server that has been configured, select the server from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

Reminder:

*The Manager immediately includes your changes in the active configuration. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

Configuration | System | Events | Syslog Servers | Add or Modify

These Manager screens let you:

Add: Configure and add a UNIX syslog server as a recipient of event messages. You can configure a maximum of five syslog servers.

Modify: Modify a configured UNIX syslog server that is a recipient of event messages.

Figure 9-8 Configuration | System | Events | Syslog Servers | Add Screen

Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

Syslog Server Enter the IP address or hostname of the syslog server.

Port Enter the port used by the syslog server.

Facility Select the syslog facility tag for events sent to this server.

61778

Syslog Server

Enter the IP address or hostname of the UNIX syslog server to receive event messages. (If you have configured a DNS server, you can enter a hostname; otherwise, enter an IP address.)

Port

Enter the UDP port number by which you access the syslog server. Use a decimal number from 0 to 65535. The default is 514, which is the well-known port number.

Facility

Click the drop-down menu button and select the syslog facility tag for events sent to this server. The facility tag lets the syslog server sort messages into different files or destinations. The choices are:

- **User** = Random user-process messages.
- **Mail** = Mail system.
- **Daemon** = System daemons.
- **Auth** = Security or authorization messages.
- **Syslog** = Internal syslogd-generated messages.
- **LPR** = Line printer subsystem.
- **News** = Network news subsystem.
- **UUCP** = UUCP (UNIX-to-UNIX Copy Program) subsystem.
- **Reserved (9) through Reserved (14)** = Outside the Local range, with no name or assignment yet, but usable.
- **CRON** = Clock daemon.
- **Local 0 through Local 7** (default) = User defined.

Add or Apply/Cancel

To add this server to the list of syslog servers, click **Add**. Or to apply your changes to this syslog server, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the Configuration | System | Events | Syslog Servers screen. Any new server appears in the Syslog Servers list.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entries, click **Cancel**. The Manager returns to the Configuration | System | Events | Syslog Servers screen, and the Syslog Servers list is unchanged.



General

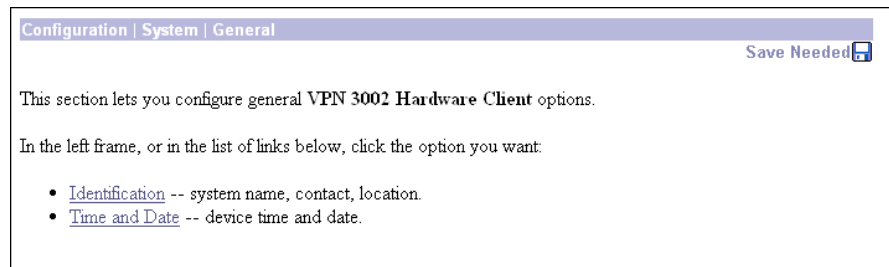
General configuration parameters include VPN 3002 environment items: system identification, time, and date.

Configuration | System | General

This section of the Manager lets you configure general VPN 3002 parameters.

- **Identification:** system name, contact person, system location.
- **Time and Date:** system time and date.

Figure 10-1 Configuration | System | General Screen



Configuration | System | General | Identification

This screen lets you configure system identification parameters that are stored in the standard MIB-II system object. Network management systems using SNMP can retrieve this object and identify the system. Configuring this information is optional.

Figure 10-2 Configuration | System | General | Identification Screen

Configuration | System | General | Identification

Configure system identification (optional). These entries are stored in the MIB-II *system* object.

System Name Enter a system name for the device; e.g., vpn01

Contact Enter the name of the contact person

Location Enter the device location; e.g., Computer Lab 3

Apply Cancel

61780

System Name

Enter a system name that uniquely identifies this VPN 3002 on your network; for example, VPN01. Maximum 255 characters.

Contact

Enter the name of the contact person who is responsible for this VPN 3002. Maximum 255 characters.

Location

Enter the location of this VPN 3002. Maximum 255 characters.

Apply / Cancel

To apply your system identification settings and include them in the active configuration, click **Apply**. The Manager returns to the Configuration | System | General screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | General screen.

Configuration | System | General | Time and Date

This screen lets you set the time and date on the VPN 3002. Setting the correct time is very important so that logging information is accurate.

Figure 10-3 Configuration | System | General | Time and Date Screen

Configuration | System | General | Time and Date

Configure the time and date.

i Setting the time on your VPN 3002 Hardware Client is very important, so that logging information is correct.

The current time on the device is Friday, 23 February 2001 15:12:14.

New Time 15 : 12 : 10 February / 23 / 2001 (GMT-05:00) EST

Enable DST Support

Apply Cancel

61781

Current Time

The screen shows the current date and time on the VPN 3002 at the time the screen displays. You can refresh this by redisplaying the screen.

New Time

The values in the New Time fields are the time and date on the *browser PC* at the time the screen displays. Any entries you make apply to the *VPN 3002*, however.

In the appropriate fields, make any changes. The fields are, in order: Hour : Minute : Second Month / Day / Year Time Zone. Click the drop-down menu buttons to select Month, and Time Zone. The time zone selections are offsets in hours relative to GMT (Greenwich Mean Time), which is the basis for Internet time synchronization. Enter the Year as a four-digit number.

Enable DST Support

To enable DST support, check the box. During DST (Daylight-Saving Time), clocks are set one hour ahead of standard time. Enabling DST support means that the VPN 3002 automatically adjusts the time zone for DST or standard time. If your system is in a time zone that uses DST, you must enable DST support.

Apply/Cancel

To apply your time and date settings, and to include your settings in the active configuration, click Apply. The Manager returns to the Configuration | System | General screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your settings, click **Cancel**. The Manager returns to the Configuration | System | General screen.



Policy Management

The VPN 3002 works in either of two modes: Client mode or Network Extension mode. To view a brief interactive multimedia piece that explains the differences between the two modes, go to this url:

http://www.cisco.com/mm/techsnap/VPN3002_techsnap.html

Your web browser must be equipped with a current version of the Macromedia Flash Player to view the content. If you are unsure whether your browser has the most recent version, you may want to download and install a free copy from:

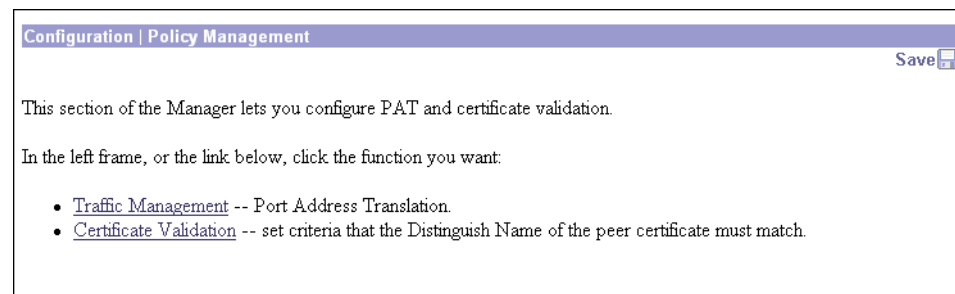
http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash

Policy management on the VPN 3002 includes deciding whether you want the VPN 3002 to use Client Mode or Network Extension mode. This section lets you enable or disable PAT.

Configuration | Policy Management

The Configuration | Policy Management screen introduces this section of the Manager.

Figure 11-1 Configuration | Policy Management Screen



Traffic Management

To enable or disable PAT, click **Traffic Management**.

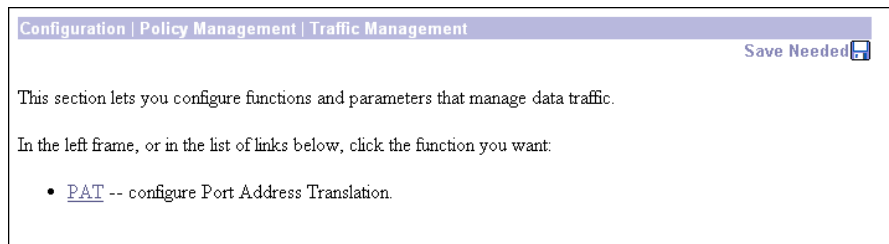
Certificate Validation

To enable and set criteria that must match for the VPN 3002 to verify a certificate from the Concentrator to which it connects, click **Certificate Validation**.

Configuration | Policy Management | Traffic Management

When you click Traffic Management on the Configuration | Policy Management screen, the Manager displays the Configuration | Policy Management | Traffic Management screen.

Figure 11-2 Configuration | Policy Management | Traffic Management Screen



PAT

To configure PAT (Port Address Translation) click **PAT**.

About PAT (Client Mode)

Client mode, also called Port Address Translation (PAT) mode, isolates all devices on the VPN 3002 private network from those on the corporate network. In PAT mode:

- IPsec encapsulates all traffic going from the private network of the VPN 3002 to the network(s) behind the Internet Key Exchange (IKE) peer, that is, the central-site VPN Concentrator.
- PAT mode uses NAT (Network Address Translation). NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the IP address of the VPN 3002 public interface. The VPN Concentrator assigns this address. NAT also keeps track of these mappings so that it can forward replies to the correct device.

All traffic from the private network appears on the network behind the IKE peer with a single source IP address. This IP address is the one the central-site VPN Concentrator assigns to the VPN 3002. The IP addresses of the computers on the VPN 3002 private network are hidden. You cannot ping or access a device on the VPN 3002 private network from outside of that private network, or directly from a device on the private network at the central site.

In client mode, the tunnel establishes when data passes to the VPN Concentrator, or when you click Connect Now in the Monitoring | System Status screen.

Client Mode with Split Tunneling

You assign the VPN 3002 to a client group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec and PAT are applied to all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator.

Traffic from the VPN 3002 to any destination other than those within the network list for that group on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices connected to the VPN 3002 private interface to the assigned IP address of the public interface and also keeps track of these mappings so that it can forward replies to the correct device.

The network and addresses on the private side of the VPN 3002 are hidden, and cannot be accessed directly.

VPN 3000 Series VPN Concentrator Settings Required for PAT

For the VPN 3002 to use PAT, these are the requirements for the central-site VPN Concentrator.

1. The VPN Concentrator at the central site must be running Software version 3.x or later.
2. Address assignment must be enabled, by whatever method you choose to assign addresses (for example, DHCP, address pools, per user, or client-specified). If the VPN Concentrator uses address pools for address assignment, make sure to configure the address pools your network requires. See Chapter 6, *Address Management*, in the *VPN 3000 Series Concentrator Reference Volume I*.
3. Configure a group to which you assign this VPN 3002. This includes assigning a group name and Password. See Chapter 14, *User Management*, in the *VPN 3000 Series Concentrator Reference Volume I*.
4. Configure one or more users for the group, including usernames and passwords.

About Network Extension Mode

Network Extension mode allows the VPN 3002 to present a single, routable network to the remote private network over the VPN tunnel. IPSec encapsulates all traffic from the VPN 3002 private network to networks behind the central-site VPN Concentrator. PAT does not apply. Therefore, devices behind the VPN Concentrator have direct access to devices on the VPN 3002 private network over the tunnel, and only over the tunnel, and vice versa. The VPN 3002 must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

In this mode, the central-site VPN Concentrator does not assign an IP address for tunneled traffic (as it does in Client/PAT mode). The tunnel is terminated with the VPN 3002 private IP address (the assigned IP address). To use Network Extension mode, you must configure an IP address other than the default of 192.168.10.1 and disable PAT.

In Network Extension mode, the VPN 3002 automatically attempts to establish a tunnel to the VPN Concentrator. However, if you enable interactive hardware client authentication, the tunnel establishes when you perform the following steps.

-
- Step 1 Click the **Connection/Login Status** button on the VPN 3002 Hardware Client login screen. The Connection/Login screen displays.
 - Step 2 Click **Connect Now** in the Connection/Login screen.

Step 3 Enter the username and password for the VPN 3002.

Alternatively, you can initiate a tunnel by clicking **Connect Now** on the in the Monitoring | System Status screen.

Network Extension Mode with Split Tunneling

You always assign the VPN 3002 to a client group on the central-site VPN Concentrator. If you enable split tunneling for that group, IPSec operates on all traffic that travels through the VPN 3002 to networks within the network list for that group behind the central-site VPN Concentrator. PAT does not apply.

Traffic from the VPN 3002 to any other destination than those within the network list on the central-site VPN Concentrator travels in the clear without applying IPSec. NAT translates the network addresses of the devices on the VPN 3002 private network to the address of the VPN 3002 public interface. Thus the network and addresses on the private side of the VPN 3002 are accessible over the tunnel, but are protected from the Internet, that is, they cannot be accessed directly.

VPN 3000 Series Concentrator Settings Required for Network Extension Mode

For the VPN 3002 to use Network Extension mode, these are the requirements for the central-site VPN Concentrator.

1. The VPN Concentrator at the central site must be running Software version 3.0 or later.
2. Configure a group to which you assign this VPN 3002. This includes assigning a group name and password. See Chapter 14, *User Management*, in the *VPN 3000 Series Concentrator Reference Volume I*.
3. Configure one or more users for the group, including usernames and passwords.
4. Configure either a default gateway or a static route to the VPN 3002 private network. See Chapter 8, “IP Routing” in the *VPN 3000 Series Concentrator Reference Volume I*.
5. If you want the VPN 3002 to be able to reach devices on other networks that connect to this VPN Concentrator, review your Network Lists. See Chapter 15, “Policy Management” in the *VPN 3000 Series Concentrator Reference Volume I*.
6. Enable Network Extension Mode. See the section that follows for details.

Network Extension Mode per Group

A network administrator can now restrict the use of network extension mode. VPN 3002 hardware clients can use network extension mode only if, on the VPN Concentrator, you enable network extension mode on a group basis for VPN 3002 hardware clients.



Note

If you disallow network extension mode, which is the default setting on the VPN Concentrator, the VPN 3002 can connect to that VPN Concentrator in PAT mode only. In this case, be careful that all VPN 3002s in the group are configured for PAT mode. If a VPN 3002 is configured to use network extension mode and the VPN Concentrator to which it connects disallows network extension mode, the VPN 3002 will attempt to connect every 4 seconds, and every attempt will be rejected; this is the equivalent of denial of service attack.

Tunnel Initiation

The VPN 3002 always initiates the tunnel to the central-site VPN Concentrator. The central-site VPN Concentrator cannot initiate a tunnel to a VPN 3002. The VPN 3002 creates only one IPSec tunnel to the central-site VPN Concentrator, in either PAT or Network Extension mode. The tunnel can support multiple encrypted data streams between users behind the VPN 3002 and the central site. With split tunneling enabled, it can also support multiple unencrypted data streams to the internet.

In PAT mode, the tunnel establishes when data passes to the VPN Concentrator, or when you click **Connect Now** in the Monitoring | System Status screen.

In Network Extension mode, the VPN 3002 automatically attempts to establish a tunnel to the VPN Concentrator.

Tunnel Initiation with Interactive Hardware Client Authentication

In either Client or Network Extension mode, when you enable interactive hardware client authentication, the tunnel establishes when you perform the following steps.

-
- Step 1** In the VPN 3002 Hardware Client login screen, click the **Connection/Login Status** button. The Connection/Login screen displays.
 - Step 2** Click **Connect Now**.
 - Step 3** Enter the username and password for the VPN 3002.
- See the section, “Logging in With Interactive Hardware Client and Individual User Authentication” in Chapter 1 for detailed instructions.
-

Alternatively, you can click **Connect Now** on the in the Monitoring | System Status screen, after which the system prompts you to enter the username and password for the VPN 3002. See the section, “Monitoring | System Status” in the Monitoring chapter.

Data Initiation

After the tunnel is established between the VPN 3002 and the central-site VPN Concentrator, the VPN Concentrator can initiate data exchange only in Network Extension mode with all traffic travelling through the tunnel. If you want the tunnel to remain up indefinitely, configure the VPN 3002 for Network Extension mode and do not use split tunneling.

Table 11-1 summarizes instances in which the VPN 3002 and the central-site VPN Concentrator can initiate data exchange.

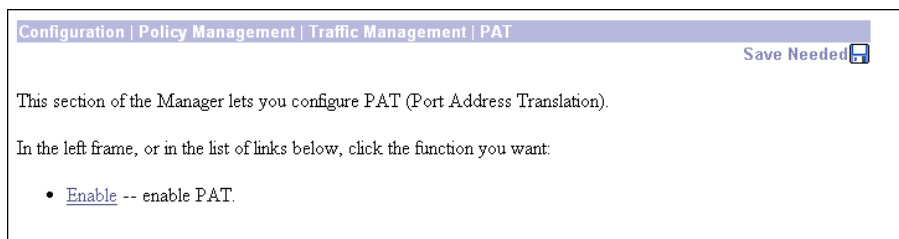
Table 11-1 Data Initiation: VPN 3002 and Central-Site VPN Concentrator

Mode	Tunneling Policy	VPN 3002 Can Send Data First	Central-Site VPN Concentrator Can Send Data First (after VPN 3002 initiates the tunnel)
PAT	All traffic tunneled	Yes	No
PAT	Split tunneling enabled	Yes	No
Network Extension	All traffic tunneled	Yes	Yes
Network Extension	Split tunneling enabled	Yes	No

Configuration | Policy Management | Traffic Management | PAT

When you click **PAT** in the Configuration | Policy Management | Traffic Management screen, the Configuration | Policy Management | Traffic Management | PAT screen displays.

Figure 11-3 Configuration | Policy Management | Traffic Management | PAT Screen



PAT mode provides many-to-one translation; that is, it translates many private network addresses to the single address configured on the public network interface.

Enable

To enable PAT, click **Enable**.

Configuration | Policy Management | Traffic Management | PAT | Enable

This screen lets you enable or disable PAT, which applies PAT to all configured traffic traveling from the private interface to the public interface.

Figure 11-4 Configuration | Policy Management | Traffic Management | PAT | Enable Screen

Configuration | Policy Management | Traffic Management | PAT | Enable

Check the box to enable PAT over the tunnel. Uncheck the box to disable PAT over the tunnel (LAN Extension mode).

PAT Enabled

Apply Cancel

61785

PAT Enabled

Check the box to enable Client Mode (PAT), or clear it to enable Network Extension Mode.



Note

Remember that to use Network Extension Mode, you must configure an IP address other than the default for the private interface. If you do not change the IP address of the private interface, you can not disable PAT.

Apply/Cancel

To enable or disable PAT, and include your setting in the active configuration, click **Apply**. The Manager returns to the Configuration | Policy Management | Traffic Management | PAT screen.

Reminder:

*To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.*

To discard your entry and leave the active configuration unchanged, click **Cancel**. The Manager returns to the Configuration | Policy Management | Traffic Management | PAT screen.

Configuration | Policy Management | Certificate Validation

When you click Certificate Validation on the Configuration | Policy Management screen, the Manager displays the Configuration | Policy Management | Certificate Validation screen.

Figure 11-5 Configuration | Policy Management | Certificate Validation Screen

Configuration | Policy Management | Certificate Validation

Set criteria that must match to verify a certificate. Use the **Distinguished Name**, **Operator**, and **Value** fields, or enter text directly in the **Matching Criteria** box.

The matching criteria may contain multiple DN Components. A DN Component is defined as <DN> <Operator> <Value>. An example of the matching criteria is: *OU="Engineering",ISSUER-O="Cisco"*.

- Enclose Value strings in double quotes.
 - If you use the **Value** box, the Manager adds the double quotes automatically.
 - If the value itself has double quotes, replace them with two sets of double quotes. For example, enter the value *Tech Eng* as *""Tech"" Eng*.
- Use commas with no spaces to separate components.

Enable Check to enable the matching criteria.

Distinguished Name	Operator	Value
Subject ▼ CommonName (CN) ▼	Equal (=) ▼	

Append

Matching Criteria

Apply Cancel

87689

To provide additional security, you can set criteria that a certificate from the VPN Concentrator to which the VPN 3002 connects must match. The criteria are based on fields in either the subject or issuer distinguished name (DN). If the criteria do not match, the connection fails.

This feature prevents a user from connecting with a stolen but valid certificate and a hijacked IP address.

Enable

Check the box to enable certificate validation based on matching criteria you configure in this screen.

Distinguished Name Component

Select the type of distinguished name (Subject or Issuer) and the fields you want to use in the matching criteria.

A distinguished name can contain a selection from the following fields:

Field	Content
-------	---------

Subject and Issuer consist of a specific-to-general identification hierarchy: CN, OU, O, L, SP, and C. These labels and acronyms conform to X.520 terminology.

Subject	The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
---------	---

Issuer	The CA or other entity (jurisdiction) that issued the certificate.
--------	--

Field	Content
-------	---------

Common Name (CN)	The name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.
------------------	--

Surname (SN)	The family name or last name of the certificate owner.
--------------	--

Country (C)	The two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
-------------	---

Locality (L)	The city or town where the organization is located.
--------------	---

State/Province (S/P)	The state or province where the organization is located.
----------------------	--

Organization (O)	The name of the company, institution, agency, association, or other entity.
------------------	---

Organizational Unit (OU)	The subgroup within the organization.
--------------------------	---------------------------------------

Title (T)	The title of the certificate owner, such as Dr.
-----------	---

Name (N)	The name of the certificate owner.
----------	------------------------------------

Given Name (GN)	The first name of the certificate owner.
-----------------	--

Initials (I)	The first letters of each part of the certificate owner's name.
--------------	---

E-mail Address (EA)	The e-mail address of the person, system or entity that owns the certificate
---------------------	--

Generational Qualifier (GENQ)	A generational qualifier such as Jr, Sr, or III.
-------------------------------	--

DN Qualifier (DNQ)	A specific DN attribute.
--------------------	--------------------------

Operator

The Operators are =, !=, * or !*. This section defines each of the operators, and explains how they are used in a sample Matching Criteria set at
 CN="IDCert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland"

Field	Content	Example
Equals (=)	The distinguished name field must exactly match the value.	<i>CN="ID Cert"</i> specifies an exact match on the CN.
Contains (*)	The distinguished name field must contain the value within it.	<i>OU*"Cisco"</i> specifies any OU that contains the string "Cisco".
Not Equals (!=)	The distinguished name field must not match the value.	<i>ISSUER-CN! "Entrust"</i> specifies that the Issuer CN must not equal "Entrust".
Does Not Contain (!*)	The distinguished name field must not contain the value within it.	<i>ISSUER-OU!*</i> specifies that the Issuer OU must not contain "wonderland".

Value

The value to be matched against. The VPN 3002 automatically places text values within double quotes. To enter values manually, follow the rules on the screen. Values are not case-sensitive.

Append

To enter the next part of a rule, click **Append**. When you click Append, the VPN Concentrator adds on the part you have defined to the rule that appears under Matching Criteria. In this way, you can build a complex rule testing on multiple components. The VPN Concentrator checks the information in the certificate against all parts of the rule. All parts must test true for the rule to match for this group.

Matching Criteria

The matching criteria text box displays the rule. You can create or edit the rule directly in this box. If you create a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value "Tech" Eng as: ""Tech" Eng" .

Apply/Cancel

After entering all parts of the rule for this group, click **Apply** to complete or **Cancel** to cancel it.

Reminder:

To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

To discard your settings, click **Cancel**. The Manager returns to the Configuration | Policy Management | Certificate Group Matching | Rules screen, and the Rules list is unchanged.



Administration

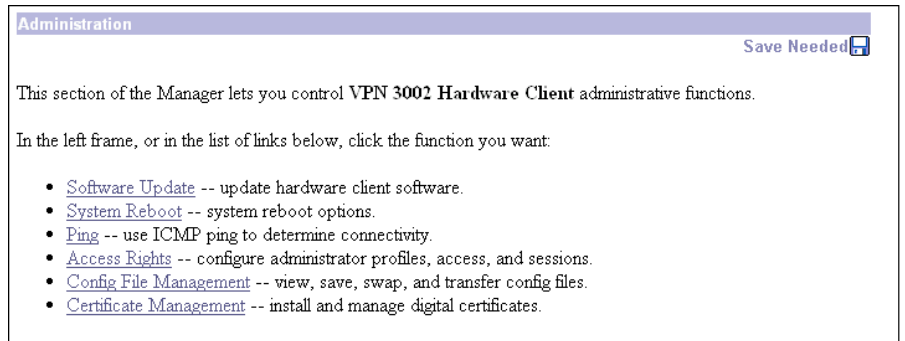
Administering the VPN 3002 involves activities that keep the system operational and secure. Configuring the system sets the parameters that govern its use and functionality as a VPN device, but administration involves higher level activities such as who is allowed to configure the system, and what software runs on it.

Administration

This section of the Manager lets you control administrative functions on the VPN 3002.

- **Software Update:** upload and update the VPN 3002 software image.
- **System Reboot:** set options for VPN 3002 shutdown and reboot.
- **Ping:** use ICMP ping to determine connectivity.
- **Access Rights:** configure administrator profiles, access, and sessions.
 - **Administrators:** configure administrator usernames, passwords, and rights.
 - **Access Settings:** set administrative session idle timeout and limits.
- **Config File Management:** manage configuration files.
 - **View Configuration Files:** view the configuration file currently on the VPN 3002.
 - **Swap Configuration Files:** swap backup and boot configuration files.
 - **Upload Configuration Files:** upload a new configuration file to the VPN 3002.
- **Certificate Management:** install and manage digital certificates.
 - **Enrollment:** create a certificate request to send to a Certificate Authority.
 - **Installation:** install digital certificates.
 - **Certificates:** view, modify, and delete digital certificates.

Figure 12-1 Administration Screen



Administration | Software Update

This section of the Manager lets you update the VPN 3002 executable system software. This process uploads the file to the VPN 3002, which then verifies the integrity of the file.

The new image file must be accessible by the workstation you are using to manage the VPN 3002. Software image files ship on the Cisco VPN 3002 CD-ROM. Updated or patched versions are available from the Cisco Website, www.cisco.com, under Service & Support > Software Center.

It takes a few minutes to upload and verify the software, and the system displays the progress. Please wait for the operation to finish.

To run the new software image, you must reboot the VPN 3002. The system prompts you to reboot when the update is finished.

We also recommend that you clear your browser cache after you update the software image: delete all the temporary internet files, history files, and location bar references.



Note

The VPN 3002 has two locations for storing image files: the active location, which stores the image currently running on the system; and the backup location. Updating the image overwrites the stored image file in the backup location and makes it the active location for the next reboot. Updating *twice*, therefore, overwrites the image file in the active location; and the current image file is lost. The Manager displays a warning on this screen if you have already updated the image without rebooting.



Caution

You can *update* the software image while the system is still operating as a VPN device. *Rebooting* the system, however, terminates all active sessions.

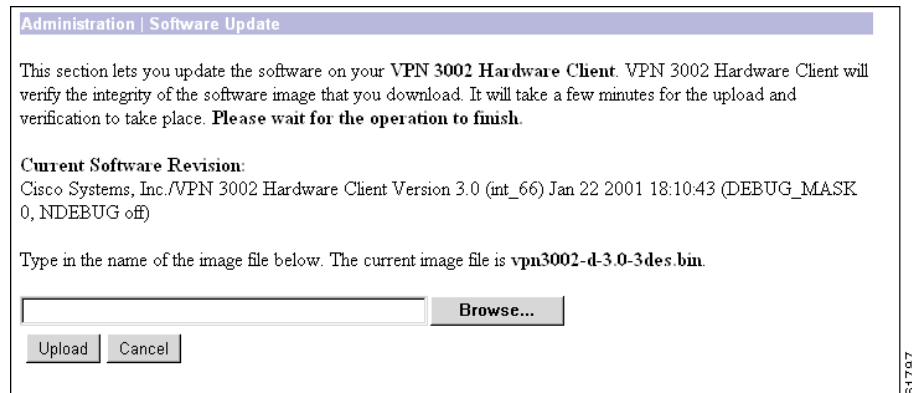


Caution

While the system is updating the image, do not perform any other operations that affect Flash memory (listing, viewing, copying, deleting, or writing files.) Doing so might corrupt memory.

Updating the software image also makes available any new Cisco-supplied configurable selections. When you reboot with the new image, the system updates the active configuration in memory with these new selections, but it does not write them to the CONFIG file until you click the **Save Needed** icon in the Manager window.

Figure 12-2 Administration | Software Update Screen



61787

Current Software Revision

The name, version number, and date of the software image currently running on the system.

Browse...

Enter the complete pathname of the new image file, or click **Browse...** to find and select the file from your workstation or network. Cisco-supplied VPN 3002 software image files are named:

vpn3002 <Major Version> .<Minor Version>.<Patch Version>.bin; for example,
vpn3002-3.5.Rel-k9.bin.

The Major and Minor Version numbers are always present; the Sustaining and Patch Version numbers are present only if needed.

Be sure you select the correct file for your VPN 3002; otherwise the update will fail.

Upload/Cancel

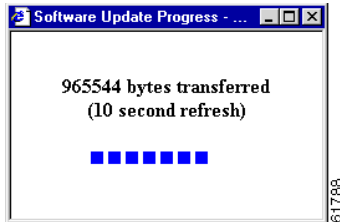
To upload the new image file to the VPN3002, click **Upload**.

To cancel your entries on this screen, *or to stop a file upload that is in progress*, click **Cancel**. The Manager returns to the main Administration screen. If you then return to the Administration | Software Update screen, you might see a message that a file upload is in progress. Click the highlighted link to stop it and clear the message.

Software Update Progress

This window shows the progress of the software upload. It refreshes the number of bytes transferred at 10-second intervals.

Figure 12-3 Administration | Software Update Progress Window



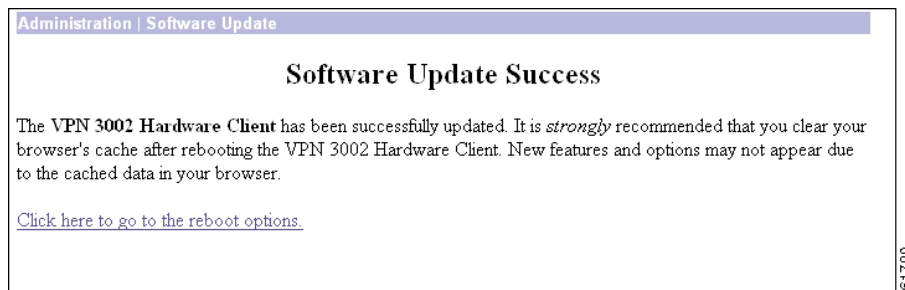
When the upload is finished, or if the upload is cancelled, the progress window closes.

Software Update Success

The Manager displays this screen when it completes the software upload and verifies the integrity of the software. To go to the Administration | System Reboot screen, click the highlighted link.

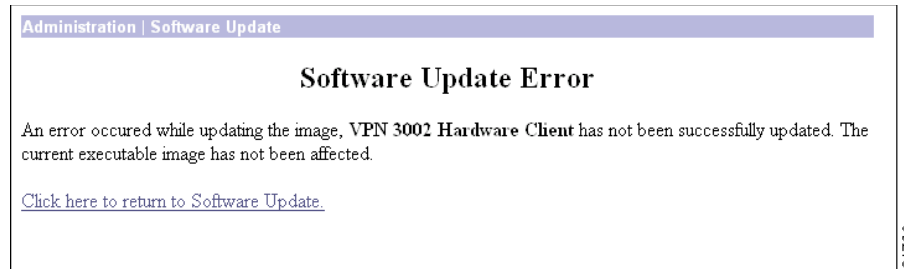
We strongly recommend that you clear your browser cache after you update the software image: delete all the temporary internet files, history files, and location bar references.

Figure 12-4 Administration | Software Update Success Screen



Software Update Error

This screen appears if there was an error in uploading or verifying the image file. You might have selected the wrong file. Click the highlighted link to return to the Administration | Software Update screen and try the update again, or contact Cisco support.

Figure 12-5 Administration | Software Update Error Screen

Administration | System Reboot

This screen lets you reboot or shutdown (halt) the VPN 3002 with various options.

We strongly recommend that you shut down the VPN 3002 before you turn power off. If you just turn power off without shutting down, you might corrupt Flash memory and affect subsequent operation of the system.

If you are logged in the Manager when the system reboots or halts, it automatically logs you out and displays the main login screen. The browser might appear to hang during a reboot; that is, you cannot log in and you must wait for the reboot to finish. You can log back in while the VPN 3002 is in a shutdown state, before you turn power off.

If a delayed reboot or shutdown is pending, the Manager also displays a message that describes when the action is scheduled to occur.



Note

Reboot or shutdown that does not wait for sessions to terminate, terminates all active sessions without warning and prevents new user sessions.

The VPN 3002 automatically saves the current event log file as SAVELOG.TXT when it reboots, and it overwrites any existing file with that name. See Configuration | System | Events | General, Administration | Config File Management, and Monitoring | Filterable Event Log for more information on the event log file.

Figure 12-6 Administration | System Reboot Screen

Administration | System Reboot Save

This section presents reboot options.

If you reboot, the browser may appear to hang as the device is rebooted.

Action

Reboot

Shutdown without automatic reboot

Cancel a scheduled reboot/shutdown

Configuration

Save the active configuration at time of reboot

Reboot without saving the active configuration

Reboot ignoring the configuration file

When to Reboot/Shutdown

Now

Delayed by minutes

At time (24 hour clock)

Wait for sessions to terminate (don't allow new sessions)

61791

Action

Click a radio button to select the desired action. You can select only one action.

- **Reboot** = Reboot the VPN 3002. Rebooting terminates all sessions, resets the hardware, loads and verifies the software image, executes system diagnostics, and initializes the system. A reboot takes about 60-75 seconds. (This is the default selection.)
- **Shutdown without automatic reboot** = Shut down the VPN 3002; that is, bring the system to a halt so you can turn off the power. Shutdown terminates all sessions and prevents new user sessions (but not administrator sessions). While the system is in a shutdown state, the **SYS** LEDs blink on the front panel.
- **Cancel a scheduled reboot/shutdown** = Cancel a reboot or shutdown that is waiting for a certain time or for sessions to terminate. (This is the default selection if a reboot or shutdown is pending.)

Configuration

Click a radio button to select the configuration file handling at reboot. These selections apply to reboot only. You can select only one option.

- **Save the active configuration at time of reboot** = Save the active configuration to the `CONFIG` file, and reboot using that new file.
- **Reboot without saving the active configuration** = Reboot using the existing `CONFIG` file and without saving the active configuration. (This is the default selection.)

- **Reboot ignoring the Configuration file** = Reboot using all the factory defaults; that is, start the system as if it had no `CONFIG` file. You will need to go through all the Quick Configuration steps described in the *VPN 3002 Getting Started* manual, including setting the system date and time and supplying an IP address for the Ethernet 1 (private) interface, using the system console. This option *does not* destroy any existing `CONFIG` file, and it *does not* reset Administrator parameter settings.

When to Reboot/Shutdown

Click a radio button to select when to reboot or shutdown. You can select only one option.

- **Now** = Reboot or shutdown as soon as you click Apply. (This is the default selection.)
- **Delayed by [NN] minutes** = Reboot or shutdown `NN` minutes from when you click Apply, based on system time. Enter the desired number in the field; the default is 10 minutes. (FYI: 1440 minutes = 24 hours.)
- **At time [HH:MM]** = Reboot or shutdown at the specified system time, based on a 24-hour clock. Enter the desired time in the field. Use 24-hour notation and enter numbers in all positions. The default is 10 minutes after the current system time.
- **Wait for sessions to terminate (do not allow new sessions)** = Reboot or shutdown as soon as the last session terminates, and do not allow any new sessions in the meantime. If you (the administrator) are the last session, you must log out for the system to reboot or shutdown.

Apply/Cancel

To take action with the selected options, click **Apply**. The Manager returns to the main Administration screen if you do not reboot or shutdown now.

To cancel your settings on this screen, click **Cancel**. The Manager returns to the main Administration screen. (Note that this **Cancel** button does not cancel a scheduled reboot or shutdown.)

Administration | Ping

This screen lets you use the ICMP ping (Packet Internet Groper) utility to test network connectivity. Specifically, the VPN 3002 sends an ICMP Echo Request message to a designated host. If the host is reachable, it returns an Echo Reply message, and the Manager displays a Success screen. If the host is not reachable, the Manager displays an Error screen.

You can also Ping hosts from the Administration | Sessions screen.

Figure 12-7 Administration | Ping Screen

Administration | Ping

This screen lets you test network connectivity. Please wait for the operation to complete.

Address/Hostname to Ping

Ping Cancel

61792

Address/Hostname to Ping

Enter the IP address or hostname of the system you want to test. (If you configured a DNS server, you can enter a hostname; otherwise, enter an IP address.) Maximum is 64 characters.

Ping/Cancel

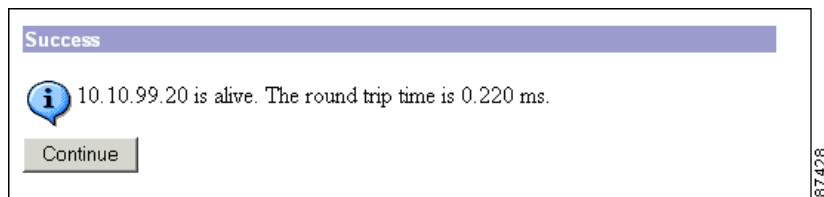
To send the ping message, click **Ping**. The Manager pauses during the test, which might take a few moments; *please wait for the operation to finish*. The Manager then displays either a Success or Error screen; see below.

To cancel your entry on this screen, click **Cancel**. The Manager returns to the main Administration screen.

Success (Ping)

If the system is reachable, the Manager displays a Success screen with the name of the tested host, as well as the amount of time, in milliseconds, between when the VPN 3002 sent the ping message, and when it received a response.

Figure 12-8 Administration | Ping | Success Screen



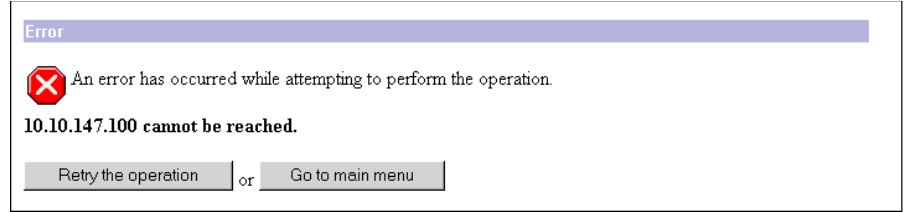
Continue

To return to the Administration | Ping screen, click **Continue**.

Error (Ping)

If the system is unreachable for any reason, host down, ICMP not running on host, route not configured, intermediate router down, network down or congested, etc., the Manager displays an Error screen with the name of the tested host. To troubleshoot the connection, try to Ping other hosts that you know are working.

Figure 12-9 Administration | Ping | Error Screen



To return to the Administration | Ping screen, click **Retry the operation**.

To go to the main Manager screen, click **Go to main menu**.

61794

Administration | Traceroute

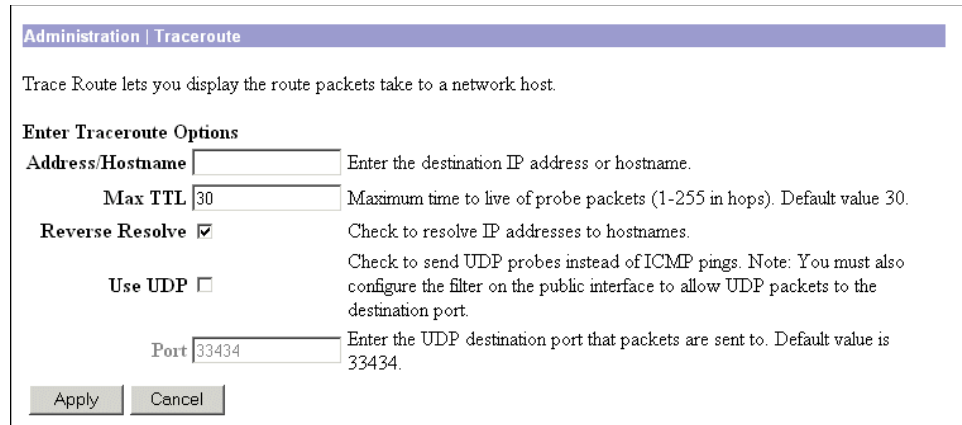


Caution

Traceroute requires Sun Microsystems Java™ Runtime Environment (JRE)1.4.1. If you do not have JRE installed, do not attempt to run this feature. Running Traceroute without JRE causes the VPN 3002 Manager to fail.

Traceroute is a helpful tool for troubleshooting connectivity problems. The Traceroute feature lets you trace the path a data packet takes through the Internet between the VPN 3002 and a destination device. The VPN 3002 sends an ICMP or UDP probe to the destination device, then reports the probe's route, the number of hops, and the time between hops.

Figure 12-10 Administration | Traceroute Screen



104077

Address/Hostname

Enter the IP address or hostname of the destination device. If you enter an IP address, use dotted decimal notation (for example, 192. 168.12.34).

Max TTL

Enter the maximum number of hops for probe packets. Traceroute stops after this many hops. Valid entries are 1 to 255 hops. The default is 30 hops.

Reverse Resolve

Check the **Reverse Resolve** check box to resolve the hostnames of intermediate hops to their IP addresses. The default is checked.

Use UDP

Check the **Use UDP** check box to send UDP packets rather than ICMP pings, the default.

Port

If you checked Use UDP, enter the UDP destination port number. The default port number is 33434.

Apply/Cancel

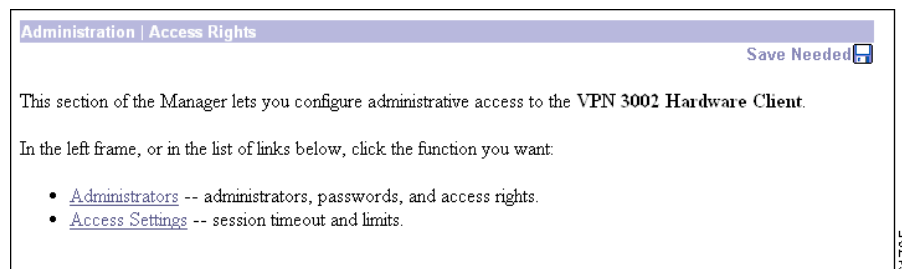
To run the Traceroute command with these settings, click **Apply**. To discard your settings, click **Cancel**. The Manager returns to the Administration screen.

Administration | Access Rights

This section of the Manager lets you configure and control administrative access to the VPN 3002.

- **Administrators:** configure administrator usernames, passwords, and rights.
- **Access Settings:** set administrative session timeout and limits.

Figure 12-11 Administration | Access Rights Screen



Administration | Access Rights | Administrators

Administrators are special users who can access and change the configuration, administration, and monitoring functions on the VPN 3002. Only administrators can use the VPN 3002 Hardware Client Manager.

This section of the Manager lets you change administrator properties and rights. Any changes take effect as soon as you click **Apply**.

Figure 12-12 Administration | Access Rights | Administrators Screen

Administrator

The VPN 3002 has three predefined administrators:

- **admin** = System administrator with access to, and rights to change, all areas. This is the only administrator enabled by default; in other words, this is the only administrator who can log in to, and use, the VPN 3002 Hardware Client Manager as supplied by Cisco.
- **config** = Configuration administrator with access rights to Quick Configuration and monitoring management options only.
- **monitor** = Monitor administrator with rights to monitoring management options only.



Note

The VPN 3002 saves Administrator parameter settings from this screen in nonvolatile memory, not in the active configuration (CONFIG) file. Thus, these settings are retained even if the system loses power. These settings are also retained even if you reboot the system with the factory configuration file.

Password

Enter or edit the unique password for this administrator. Maximum is 31 characters. The field displays only asterisks.

**Note**

The default password that Cisco supplies is the same as the username. We strongly recommend that you change this password.

Verify

Re-enter the password to verify it. The field displays only asterisks.

Enabled

Check the box to enable, or clear the box to disable, an administrator. Only enabled administrators can log in to, and use, the VPN 3002 Hardware Client Manager. You must enable at least one administrator, and you can enable all administrators. By default, only admin is enabled.

Apply/Cancel

To save this screen settings in nonvolatile memory, click **Apply**. The settings immediately affect new sessions. The Manager returns to the Administration | Access Rights screen.

To discard your settings or changes, click **Cancel**. The Manager returns to the Administration | Access Rights screen.

Administration | Access Rights | Access Settings

This screen lets you configure general options for administrator access to the Manager.

Figure 12-13 Administration | Access Rights | Access Settings Screen

Session Idle Timeout

Enter the idle timeout period in seconds for administrative sessions. If there is no activity for the period, the Manager session terminates. Minimum is 1, default is 600, and maximum is 1800 seconds (30 minutes).

The Manager resets the inactivity timer only when you click an action button (Apply, Add, Cancel, etc.) or a link on a screen—that is, when you invoke a different screen. Entering values or setting parameters on a given screen *does not* reset the timer.

Session Limit

Enter the maximum number of simultaneous administrative sessions allowed. Minimum is 1, default is 10, and maximum is 50 sessions.

Config File Encryption

To encrypt sensitive entries in the CONFIG file, check the box (default). The CONFIG file is in ASCII text format (.INI format). Check this box to encrypt entries such as passwords, keys, and user information.

To use clear text for all CONFIG file entries, clear the box. For maximum security, we do *not* recommend this option.

Apply/Cancel

To save your settings in the active configuration, click **Apply**. The Manager returns to the Administration | Access Rights screen.

To cancel your settings, click **Cancel**. The Manager returns to the Administration | Access Rights screen.

Administration | File Management

This section of the Manager lets you manage files in VPN 3002 Flash memory. (Flash memory acts like a disk.) These files include CONFIG, CONFIG.BAK, saved log files, memory reports, and copies of any of these files that you have saved under different names.

Figure 12-14 Administration | File Management | View Screen

Administration | File Management

This section of the Manager lets you view files on the **VPN 3002 Hardware Client**.

- Config File [[View](#) | [Delete](#) | [Swap with Back-up Config File](#) | [Upload via HTTP](#)]
- Back-up Config File [[View](#) | [Delete](#) | [Swap with Config File](#)]
- Crash Dump File [[View](#) | [Delete](#)]
- Saved Log File [[View](#) | [Delete](#)]
- Memory Report [[View](#) | [Delete](#)]

87387

View (Save)

View Files lets you view configuration and saved log files. You can also save these files to the PC on which you are viewing them.

To view a file, click **View** next to the type of file you want to see. The Manager opens a new browser window to display the file, and the browser address bar shows the filename.

You can also save a copy of the file on the PC that is running the browser. Click the **File** menu on the *new* browser window and select **Save As...** The browser opens a dialog box that lets you save the file. The default filename is the same as on the VPN 3002.



Note

Be sure to save a configuration file as a .TXT file, not a .HTM file. Some browser versions default to saving the file as an .HTM file, so you may need to change the file type. Saving the file as an .HTM file causes some data to be added to the top of the configuration file that is not valid configuration data. If you subsequently upload the file containing the invalid data to the VPN Concentrator or VPN 3002, it may cause unpredictable results.

Alternatively, you can use the secondary mouse button to click **View** on this Manager screen. A pop-up menu presents choices whose exact wording depends on your browser, but among them are:

- **Open Link, Open Link in New Window, Open in New Window** = Open and view the file in a new browser window, as above.
- **Save Target As..., Save Link As...** = Save a copy of the file on your PC. Your system will prompt for a filename and location. The default filename is the same as on the VPN 3002.

When you are finished viewing or saving the file, close the new browser window.

Delete

Delete lets you delete configuration files, saved log files, crash dump files, and memory reports. To delete a file, click **Delete** next to the type of file you want to delete. When you select this option, a pop-up window displays asking you to confirm or cancel. If you confirm, the file is deleted; the Manager refreshes the screen and shows the revised list of files. There is no undo.

Swap Config Files

Swap Config Files lets you swap the boot configuration file with the backup configuration file. When you select this option, the Administration | File Management | Swap Config Files window displays.

Config File Upload via HTTP

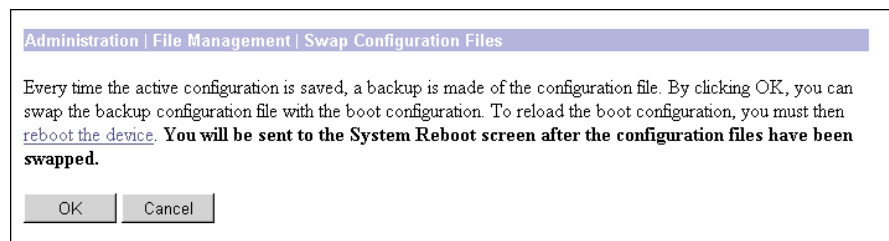
Config File Upload allows you to upload a configuration file. When you select this option, the Administration | File Management | Config File Upload window displays.

Administration | File Management | Swap Config Files

This screen lets you swap the boot configuration file with the backup configuration file. Every time you save the active configuration, the system writes it to the `CONFIG` file, which is the boot configuration file; and it saves the previous `CONFIG` file as `CONFIG.BAK`, the backup configuration file.

To reload the boot configuration file and make it the active configuration, you must reboot the system. When you click **OK**, the system automatically goes to the Administration | System Reboot screen, where you can reboot the system. You can also click the highlighted link to go to that screen.

Figure 12-15 Administration | File Management | Swap Config Files Screen



OK/Cancel

To swap `CONFIG` and `CONFIG.BAK` files, click **OK**. The Manager goes to the Administration | System Reboot screen.

To leave the files unchanged, click **Cancel**. The Manager returns to the Administration | File Management | View screen.

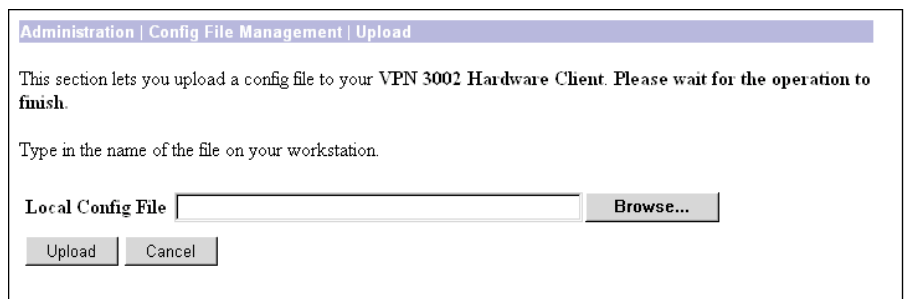
Administration | File Management | Config File Upload

This screen lets you use HTTP (Hypertext Transfer Protocol) to transfer a configuration file from your PC, or a system accessible from your PC, to the VPN 3002 Flash memory.

This function provides special handling for configuration (`config`) files. If the uploaded file has the VPN 3002 filename `config`, the system deletes any existing `config.bak` file, renames the existing `config` file as `config.bak`, then writes the new `config` file. However, these actions occur only if the file transfer is successful, so existing files are not corrupted.

To use these functions, you must have Administrator or Configuration Access Rights. See the Administration | Access Rights | Administrators screen.

Figure 12-16 Administration | File Management | Config File Upload Screen



Local Config File/Browse...

Enter the name of the file on your PC. In a Windows environment, enter the complete pathname using MS-DOS syntax; for example, `c:\vpn3002\config0077`. You can also click the Browse button to open a file navigation window, find the file, and select it.

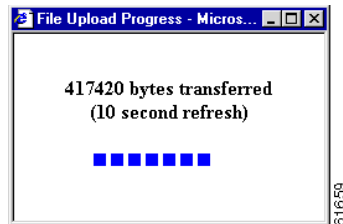
Upload/Cancel

To upload the file to the VPN 3002, click **Upload**. The Manager opens the File Upload Progress window.

To cancel your entries on this screen, *or to stop a file upload that is in progress*, click **Cancel**. The Manager returns to the Administration | File Management | View screen. Stopping an upload might leave a temporary file in VPN 3002 Flash memory. Such files are named `TnnnF.nnn` (for example, `T003F.002`). You can delete them on the Administration | File Management | View Config Files screen.

File Upload Progress

This window shows the progress of the file upload. It refreshes the number of bytes transferred at 10-second intervals.

Figure 12-17 Administration | File Management | File Upload Progress Window

When the upload is finished, or if the upload is cancelled, the progress window closes.

File Upload Success

The Manager displays this screen to confirm that the file upload was successful.

Figure 12-18 Administration | Config File Management | Upload Success Screen

To go to the Administration | Config File Management | View screen and examine files in flash memory, click the highlighted link.

File Upload Error

The Manager displays this screen if there was an error during the file upload and the transfer was not successful. Flash memory might be full, or the file transfer might have been interrupted or cancelled.

Figure 12-19 Administration | Config File Management | Upload Error Screen

Click the link, **Click here to see the list of files**, to go to the Administration | File Management | View screen and examine space and files in Flash memory.

Click the link, **Click here to return to File Upload**, to return to the Administration | File Management | File Upload screen.

Certificate Management

Digital certificates are a form of digital identification used for authentication. A digital certificate contains information that identifies a device or user, such as the name, serial number, company, department, or IP address. Certificate Authorities (CAs) issue digital certificates in the context of a Public Key Infrastructure (PKI), which uses public-key/private-key encryption to ensure security. CAs are trusted authorities that “sign” certificates to verify their authenticity, thus guaranteeing the identity of the device or user.

A *CA certificate* is one used to sign other certificates. A CA certificate that is self-signed is called a *root certificate*; one issued by another CA certificate is called a *subordinate certificate*. CAs also issue *identity certificates*, which are the certificates for specific systems or hosts. There can be up to six root or subordinate CA certificates (including supporting RA certificates) but only one identity certificate on a VPN 3002.

The VPN 3002 supports X.509 digital certificates (International Telecommunications Union Recommendation X.509), including SSL (Secure Sockets Layer) certificates that are self-signed or issued in a PKI context.

The VPN 3002 stores digital certificates and private keys in Flash memory. You do not need to click **Save Needed** to store them, and they are not visible under Administration | File Management. All stored private keys are encrypted.

The VPN 3002 can have only one SSL certificate installed per interface. If you generate a self-signed SSL certificate, it replaces any installed PKI-context SSL certificate; and vice-versa.

For information on using SSL certificates, see the “Installing the SSL Certificate in your Browser” section in Chapter 1 of the *VPN 3002 Hardware Client Reference Volume*. See also Configuration | System | Management Protocols | HTTP/HTTPS and Telnet, and Configuration | System | Management Protocols | SSL.

The Role of Time

Digital certificates are time-sensitive in the following ways:

- Digital certificates indicate the time frame during which they are valid. Therefore, it is essential that the time on the VPN Concentrator is correct and synchronized with network time.
- You must complete the enrollment and certificate installation process within one week of generating the request. If you do not, the pending request is deleted.

Configuring Digital Certificates: SCEP and Manual Methods

To use digital certificates for authentication, you first enroll with a Certificate Authority (CA), and obtain and install a CA certificate on the VPN 3002. Then you enroll and install an identity certificate from the same CA.

You can enroll and install digital certificates on the VPN 3002 in either of two ways:

- Using Cisco's Simple Certificate Enrollment Protocol (SCEP).

SCEP is a secure messaging protocol that requires minimal user intervention. SCEP is the quicker method, and it lets you to enroll and install certificates using only the VPN 3002 Manager. To use SCEP, you must enroll with a CA that supports SCEP, and you must enroll via the Internet.

- Manually, exchanging information with the CA directly.

The manual method involves more steps. You can do some of the steps using the Manager. Other steps require that you exchange information with the CA directly. You deliver your enrollment request and receive the certificate from the CA via the Internet, email, or a floppy disk.



Note

If you install a CA certificate using the manual method, you must also use the manual method to request identity or SSL certificates from that CA. Conversely, to request identity and SSL certificates using SCEP, you must first use SCEP to obtain the CA certificate.

Tasks Summary

Whether you use SCEP or the manual method, you perform the following tasks to obtain and install certificates:

1. Obtain and install one or more CA certificate(s).
2. Create an enrollment request for an identity certificate.
3. Request an identity certificate from the same CA that issued the CA certificate(s).
4. Install the identity certificate on the VPN 3002.
5. Enable certificates.

About the Documentation

The print version of this guide provides step-by-step examples of configuring digital certificates using SCEP and manually, beginning with the next section, "[Managing Certificates with SCEP](#)."

The online Help and the print version both provide detailed information on the parameters for each of the Manager screens that you use to configure digital certificates.

Managing Certificates with SCEP

The following sections provide step-by-step instructions for using SCEP to enroll and install digital certificates.

Obtaining and Installing CA Certificates Automatically Using SCEP

To use SCEP to enroll for identity or SSL certificates, you must also use SCEP to obtain the associated CA certificate. The Manager does not let you enroll for a certificate from a CA unless that CA certificate was installed using SCEP. A certificate that is obtained via SCEP and therefore capable of issuing other SCEP certificates, is called *SCEP-enabled*.

**Tip**

To obtain CA certificates using SCEP, you need to know the URL of your CA. Find out your CA's SCEP URL before beginning the following steps.

- Step 1** Using the VPN 3002 Manager, display the Administration | Certificate Management screen. (See [Figure 12-20](#).)

Figure 12-20 Administration | Certificate Management Screen

Administration | Certificate Management
Thursday, 15 January 2004 11:18:57
Refresh

This section lets you view and manage certificates on the VPN 3002 Hardware Client.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
ms-root-sha-06-2001 at cisco	ms-root-sha-06-2001 at cisco	06/04/2022	No	View Delete

Identity Certificates (current: 1, maximum: 1)

Subject	Issuer	Expiration	Actions
Gateway A at Cisco Systems	ms-root-sha-06-2001 at cisco	04/02/2004	View Renew Delete

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.86.194.176 at Cisco Systems, Inc.	10.86.194.176 at Cisco Systems, Inc.	01/14/2007	View Renew Delete Export Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
1024 bits	RSA	09/28/2001	Generate

Enrollment Status [[Remove All](#): [Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 1)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

104903

- Step 2** Click **Click here to install a CA certificate**.

**Note**

The Click here to install a CA certificate option is available from this window only when no CA certificates are installed on the VPN 3002. If you do not see this option, click **Click here to install a certificate**. The Manager displays the Administration | Certificate Management | Install screen. Then click **Install CA Certificate**.

The Manager displays the Administration | Certificate Management | Install | CA Certificate screen. (See [Figure 12-21](#).)

Figure 12-21 Administration | Certificate Management | Install | CA Certificate

Administration | Certificate Management | Install | CA Certificate

Choose the method of installation:

- [SCEP \(Simple Certificate Enrollment Protocol\)](#)
- [Cut & Paste Text](#)
- [Upload File from Workstation](#)

[<< Go back to and choose a different type of certificate](#)

68172

- Step 3** Click **SCEP (Simple Certificate Enrollment Protocol)**. The Manager displays the Administration | Certificate Management | Install | CA Certificate | SCEP screen. (See [Figure 12-22](#).)

Figure 12-22 The Administration | Certificate Management | Install | CA Certificate | SCEP Screen

Administration | Certificate Management | Install | CA Certificate | SCEP

Enter the information needed to retrieve the CA certificate via SCEP. **Please wait for the operation to complete.**

URL

CA Descriptor Required for some PKI configurations.

68173

- Step 4** Fill in the fields and click Retrieve.
- **URL:** Enter the URL of the CA's SCEP interface.
 - **CA Descriptor:** Some CAs use descriptors to further identify the certificate. If your CA gave you a descriptor, enter it here. Otherwise enter a descriptor of your own. You must enter something in this field.
 - **Retrieve / Cancel:**
 - To retrieve a CA certificate from the CA and install it on the VPN 3002, click **Retrieve**.
 - To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See [Figure 12-20](#).)

The Manager installs the CA certificate on the VPN 3002 and displays the Administration | Certificate Management screen. Your new CA certificate appears in the Certificate Authorities table.

**Note**

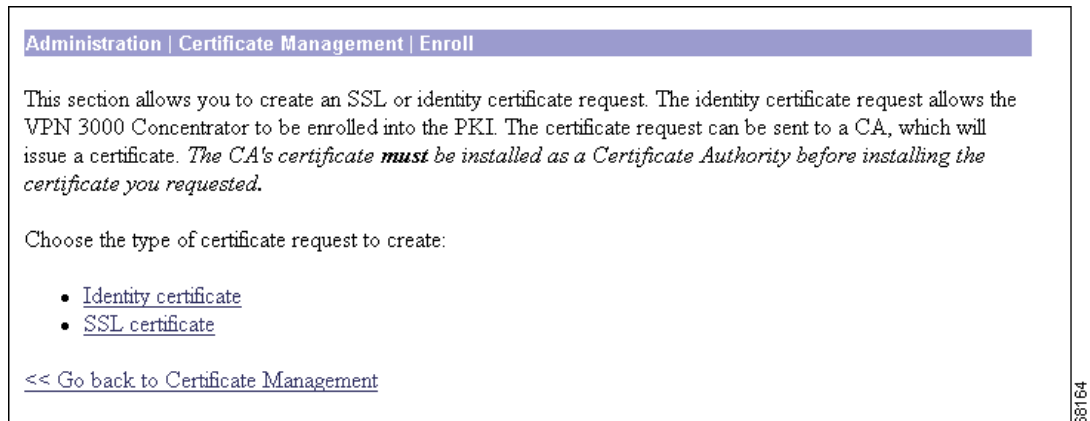
If you have trouble enrolling or installing digital certificates via SCEP, enable both the CLIENT and CERT event classes to assist in troubleshooting.

Enrolling and Installing Identity Certificates Automatically Using SCEP

Follow these steps for each identity certificate you want to obtain:

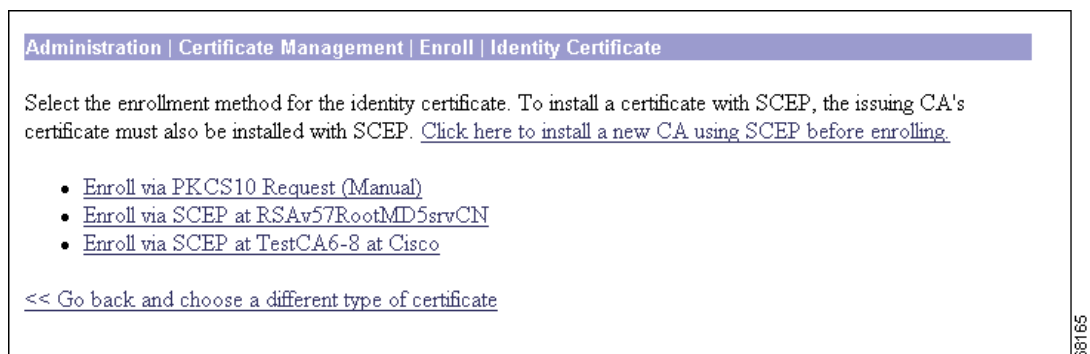
- Step 1** Display the Administration | Certificate Management screen. (See [Figure 12-20](#).)
- Step 2** Click **Click here to enroll with a Certificate Authority**. The Manager displays the Administration | Certificate Management | Enroll screen. ([Figure 12-23](#).)

Figure 12-23 Administration | Certificate Management | Enroll Screen



- Step 3** Click **Identity Certificate**. The Manager displays the Administration | Certificate Management | Enroll | Identity Certificate screen. (See [Figure 12-24](#).)

Figure 12-24 Administration | Certificate Management | Enroll | Identity Certificate Screen



Notice that a link appears corresponding to each SCEP-enabled CA certificate on the VPN 3002. The title of the link depends on the name of the CA certificate: Enroll via SCEP at *Certificate Name*. For example, if you have a CA certificate on your VPN 3002 named “TestCA6-8,” the following link appears: Enroll via SCEP at TestCA6-8.

If you do not see any Enroll via SCEP options, there are no SCEP-enabled CA certificates on the VPN 3002. Follow the steps in the [“Obtaining and Installing CA Certificates Automatically Using SCEP”](#) section to obtain a CA certificate via SCEP before you proceed.

- Step 4 Click **Enroll via SCEP at Certificate Name**. The Administration | Certificate Management | Enroll | Identity Certificate | SCEP screen displays. (See [Figure 12-25](#).)

Figure 12-25 Administration | Certificate Management | Enroll | Identity Certificate | SCEP Screen

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

Enter the information to be included in the certificate request. **Please wait for the operation to finish.**

Common Name (CN)	<input type="text"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text"/>	Enter the department.
Organization (O)	<input type="text"/>	Enter the Organization or company.
Locality (L)	<input type="text"/>	Enter the city or town.
State/Province (SP)	<input type="text"/>	Enter the State or Province.
Country (C)	<input type="text"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Challenge Password	<input type="text"/>	Enter and verify the challenge password for this certificate request.
Verify Challenge Password	<input type="text"/>	
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA key pair.

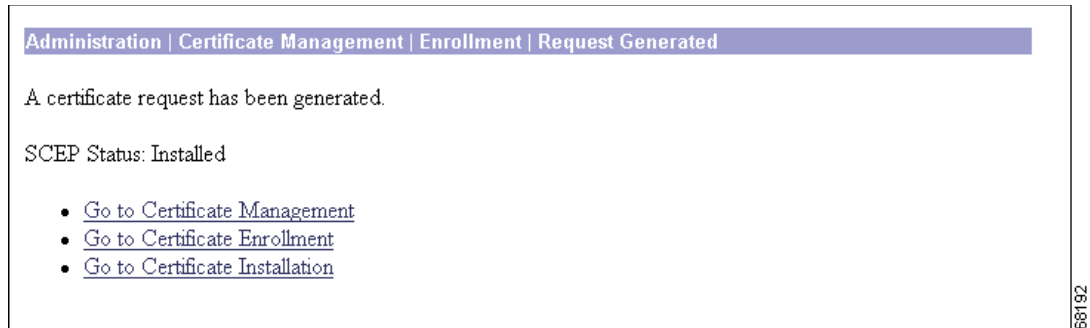
89188

- Step 5 Fill in the fields and click **Enroll**. (For information on the fields on this screen, see [Table 12-1](#).) The VPN 3002 sends the certificate request to the CA.

If the CA does not issue the certificate immediately (some CAs require manual verification of credentials and this can take time), the certificate request could enter polling mode. In polling mode, the VPN 3002 re-sends the certificate request to the CA a specified number of times at regular intervals until the CA responds or the process times out. (For information on configuring the polling limit and interval, see the Administration | Certificate Management | Configure CA Certificate screen.) The certificate request appears in the Enrollment Status table on the Administration | Certificate Management screen until the CA responds. Once the CA responds and issues the certificate, the VPN 3002 installs it automatically.

If the CA responds immediately, the Manager installs the identity certificate on the VPN 3002 and displays the Administration | Certificate Management | Enrollment | Request Generated screen. (See [Figure 12-26](#).)

Figure 12-26 Administration | Certificate Management | Enrollment | Request Generated Screen



Click **Go to Certificate Management**. The Manager displays the Administration | Certificate Management screen. Your new identity certificate appears in the Identity Certificates table.

Enrolling and Installing Certificates Manually

The following sections provide step-by-step instructions for enrolling and installing digital certificates manually.

Obtaining and Installing CA Certificates Manually

Certificate authorities are trusted entities that “sign” certificates to verify their authenticity. A CA certificate is one used to sign other certificates. You obtain CA certificates according to the procedures of individual CAs.

-
- Step 1** You can obtain a CA certificate via email, floppy disk, or over the Internet. Retrieve a CA certificate according to the policies and procedures of your CA, and download it to your management work station.
- Step 2** To install the CA certificate, begin at the VPN 3002 Manager **Administration | Certificate Management** screen. When you begin, there are no entries in the Certificate Authorities, Identity Certificates, SSL Certificates, or Enrollment Status fields.

Figure 12-27 Administration | Certificate Management Screen

Administration | Certificate Management Friday, 21 June 2002 13:42:53
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- [Click here to install a CA certificate](#)
- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 0, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
No Certificate Authorities				

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificate [[Generate](#)] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
10.10.99.50 at Cisco Systems, Inc.	10.10.99.50 at Cisco Systems, Inc.	10/18/2004	View Renew Delete

Enrollment Status [[Remove All](#): [Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

78409

- Step 3 Click **[Click here to install a CA certificate](#)**. The Administration | Certificate Management | Install screen displays.



Note The [Click here to install a CA certificate](#) option is available from this screen only when no CA certificates are installed on the VPN 3002. If you do not see this option, click **[Click here to install a certificate](#)**. The Manager displays the Administration | Certificate Management | Install screen. Then click **[Install CA certificate](#)**.

Figure 12-28 Administration | Certificate Management | Install Screen

Administration | Certificate Management | Install

Choose the type of certificate to install:

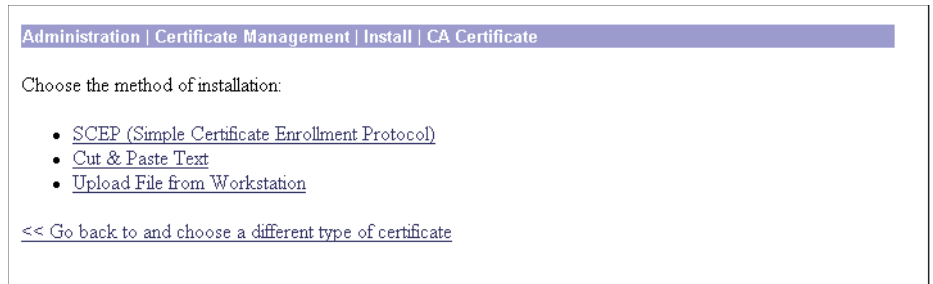
- [Install CA certificate](#)
- [Install SSL certificate with private key](#)
- [Install certificate obtained via enrollment](#)

[<< Go back to Certificate Management](#)

68171

- Step 4 Click **[Install CA Certificate](#)**. The Administration | Certificate Management | Install | CA Certificate screen displays.

Figure 12-29 Administration | Certificate Management | Install | CA Certificate Screen



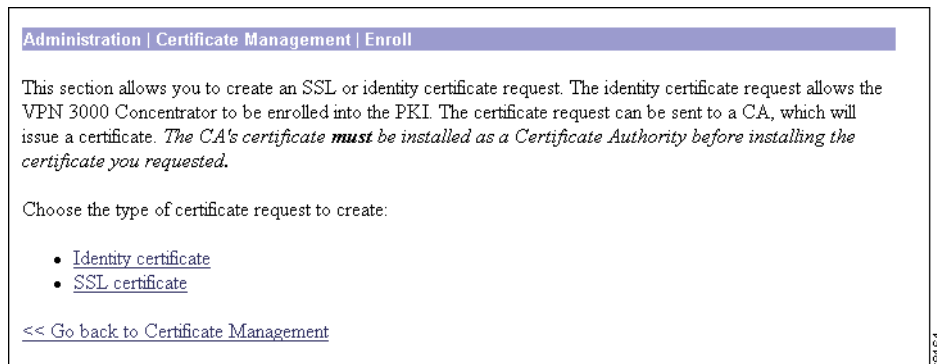
- Step 5** Click **Upload File from Workstation** or **Cut and Paste Text**, depending on how you have retrieved the CA certificate. The Manager displays a screen appropriate to your choice.
- Step 6** Include certificate information according to your chosen method.
- Step 7** Click **Install**. The Manager installs the CA certificate on the VPN 3002. You return to the Administration | Certificate Management screen, which now displays the newly installed CA certificate.

Creating an Enrollment Request for an Identity Certificate Manually

An enrollment request for an identity certificate consists of a base 64 encoded PKCS#10 file that the VPN 3002 generates based on information you provide in the steps that follow.

- Step 1** In the Administration | Certificate Management screen (Figure 12-20), click **Click here to enroll with a Certificate Authority**. The Administration | Certificate Management | Enroll screen displays.

Figure 12-30 Administration | Certificate Management | Enroll Screen



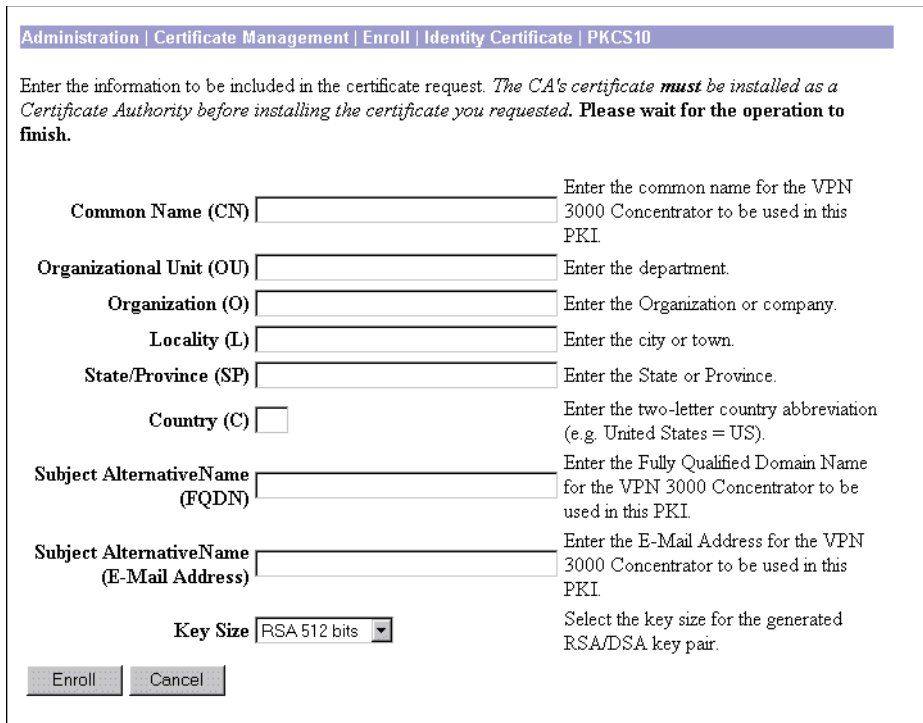
- Step 2** Click **Identity certificate**. The Administration | Certificate Management | Enroll | Identity Certificate screen displays.

Figure 12-31 Administration | Certificate Management | Enroll | Identity Certificate Screen



Step 3 Click **Enroll via PKCS10 Request (Manual)**. The Administration | Certificate Management | Enroll | Identity Certificate | PKCS10 Screen displays.

Figure 12-32 Administration | Certificate Management | Enroll | Identity Certificate | PKCS10 Screen

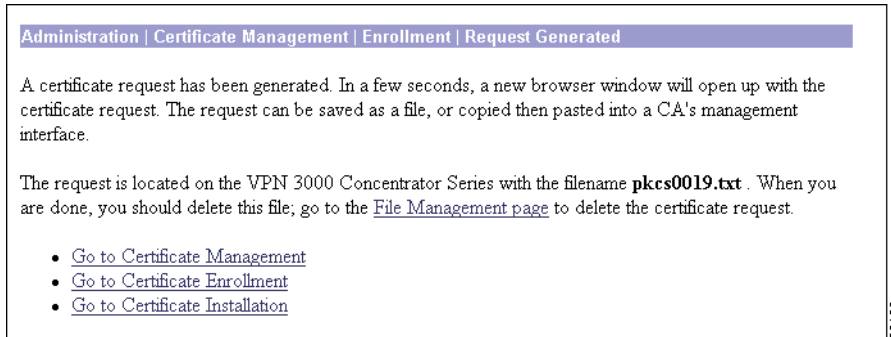


Step 4 Enter values in each of the fields on this screen. Table 12-1 defines these fields.

Step 5 When you have finished, click **Enroll**.

The Administration | Certificate Management | Enroll | Request Generated screen displays (Figure 12-33).

Figure 12-33 Administration | Certificate Management | Enroll | Request Generated Screen



The Manager displays this screen when the system has successfully generated a certificate request.

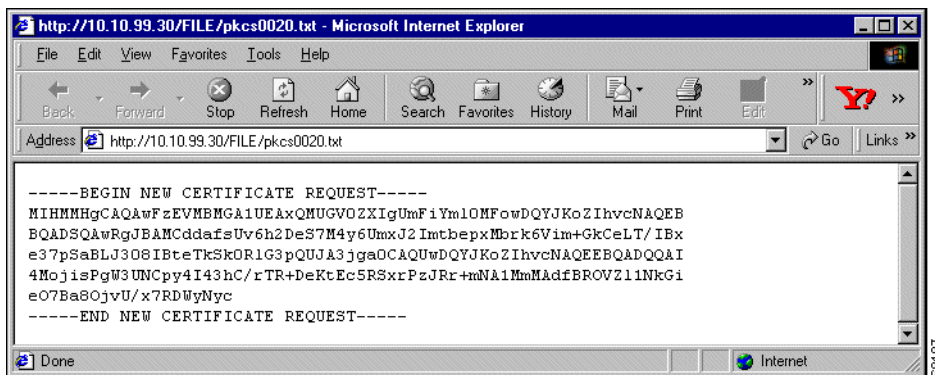


Note

You must complete the enrollment and certificate installation process within one week of generating the request. If you do not, the pending request is deleted.

As the screen text indicates, within a few seconds, a browser window opens with the certificate request.

Figure 12-34 Example of a Certificate Request



You have generated a base 64 encoded PKCS#10 file (Public Key Certificate Syntax-10), which most CAs recognize or require. The system automatically saves this file in Flash memory with the filename shown in the browser (pkcsNNNN.txt).

In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN 3002 in encrypted form.

Step 6 Save the request in one of the following ways:

- Save the request to a file (to transmit the file to the CA via email or floppy disk).
- Select and copy the request to the clipboard, and then paste the request into an email to the CA.
- Copy and paste the request into the CA's management interface via the Internet.

Some CAs let you paste the request in a web interface, some ask you to send a file; use the method your CA requires.

Step 7 Close this browser window when you have finished.

Requesting an Identity Certificate from a CA Manually

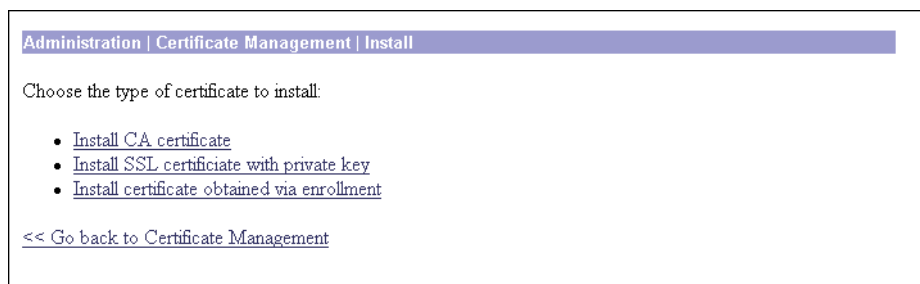
Next you submit the identity request to a CA. This must be the same CA that issued the CA certificate for this connection. Submit the request and retrieve an identity certificate according to the procedures of your CA.

Installing the Identity Certificate on the VPN 3002 Manually

The following steps provide instructions on installing an Identity certificate on the VPN 3002.

Step 1 From the Administration | Certificate Management screen, click **Click here to install a certificate** to navigate to the Administration | Certificate Management | Install screen.

Figure 12-35 Administration | Certificate Management | Install Screen



Step 2 Click **Install certificate obtained via enrollment**. The Administration | Certificate Management | Install certificate obtained via enrollment screen displays.

Figure 12-36 Administration | Certificate Management | Install certificate obtained via enrollment Screen

Administration | Certificate Management | Install certificate obtained via enrollment

Select a enrollment request to install.

Enrollment Status

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
snoopy	N/A	09/05/2001	ID	Re-enroll	Manual	In Progress	[View Install Delete]
10.10.99.30	RSAv57RootMD5srvCN	09/07/2001	SSL	Re-enroll	SCEP	Complete	[View Activate Delete]
Linda 3	RSAv57RootMD5srvCN	09/07/2001	ID	Initial	SCEP	Error	[View Re-submit Delete]

<< Go back and choose a different type of certificate

- Step 3** In the **Actions** column of the Enrollment Status table, click **Install**. The Administration | Certificate Management | Install Identity Certificate screen displays.

Figure 12-37 Administration | Certificate Management | Install Identity Certificate Screen

Administration | Certificate Management | Install | Identity Certificate

Choose the method of installation:

- [Cut & Paste Text](#)
- [Upload File from Workstation](#)

<< Go back to and choose a different type of certificate

- Step 4** Choose either installation method: **Cut & Paste Text** or **Upload File from Workstation**.
- Step 5** The Manager displays a screen appropriate to your choice. Include the certificate information according to your chosen method. Click **Install**. The Manager installs the identity certificate on the VPN 3002 and displays the Administration | Certificate Management screen. Your new identity Certificate appears in the Identity Certificates table.
- Step 6** Confirm that the Issuer fields for Certificate Authorities and Identity Certificates match for this connection. You must get the Identity certificate and the CA certificate from the same CA.

Obtaining SSL Certificates

If you use a secure connection between your browser and the VPN 3002, the VPN 3002 requires an SSL certificate. You only need one SSL certificate on your VPN 3002.

When you initially boot the VPN 3002, a self-signed SSL certificate is automatically generated. Because a self-signed certificate is self-generated, this certificate is not verifiable. No CA has guaranteed its identity. But this certificate allows you to make initial contact with the VPN 3002 using the browser. If you want to replace it with another self-signed SSL certificate, follow these steps:

-
- Step 1** Display the Administration | Certificate Management screen. (See [Figure 12-20](#).)
 - Step 2** Click **Generate** above the SSL Certificate table. The new certificate appears in the SSL Certificate table, replacing the existing one.
-

If you want to obtain a *verifiable* SSL certificate (that is, one issued by a CA), follow the same procedure you used to obtain identity certificates. (See the “[Enrolling and Installing Identity Certificates Automatically Using SCEP](#)” section.) But this time, on the Administration | Certificate Management | Enroll screen, click **SSL certificate** (instead of Identity certificate).

Some web servers export their SSL certificates with the private key attached. If you have a PEM-encoded certificate with a corresponding private key that you want to install, follow the same procedure you used to obtain identity certificates. (See the “[Enrolling and Installing Identity Certificates Automatically Using SCEP](#)” section.) But this time, on the Administration | Certificate Management | Installation screen, click **Install SSL certificate with private key** (instead of Install certificate obtained via enrollment).

Enabling Digital Certificates on the VPN 3002



Note

Before you enable digital certificates on the VPN 3002, you must obtain at least one CA and one identity certificate. If you do not have a CA and an identity certificate installed on your VPN 3002, follow the steps in the previous section before beginning this section.

For the VPN 3002 to use the digital certificates you obtained, you must enable authentication using digital certificates.

Step 1 Display the Configuration | System | Tunneling Protocols | IPsec screen.

Figure 12-38 Configuration | System | Tunneling Protocols | IPsec Screen

Configuration | System | Tunneling Protocols | IPsec

Enter the information needed to connect to the central-site VPN Concentrator server.

Remote Server Enter remote server address/host name.

Backup Servers

- Enter up to 10 backup server addresses/host names from high priority to low.
- Enter each backup server address/host name on a single line.

IPsec over TCP Check to enable IPsec over TCP.

IPsec over TCP Port Enter IPsec over TCP port (1-65535).

Use Certificate Click to use the installed certificate.

Certificate Transmission
 Entire certificate chain Choose how to send the digital certificate to the server.
 Identity certificate only

Group **Name**

User **Password**

Verify

67599

Step 2 Check the **Use Certificate** check box.

Step 3 Select a Certificate Transmission option. If you want the VPN 3002 to send the peer the identity certificate and all issuing certificates (including the root certificate and any subordinate CA certificates), click **Entire certificate chain**. If you want to send the peer only the identity certificate, click **Identity certificate only**.

Step 4 Click **Apply**. The Manager returns to the Configuration | System | Tunneling Protocols screen.

Step 5 Click the **Save Needed** icon.

Deleting Digital Certificates

Delete digital certificates in the following order:

1. Identity or SSL certificates
2. Subordinate certificates
3. Root certificates



Note

You cannot delete a certificate if it is in use by an SA, if it is the issuer of another installed certificate, or if it is referenced in an active certificate request.

Follow these steps to delete certificates:

- Step 1** Display the Administration | Certificate Management screen. (See [Figure 12-20](#).)
- Step 2** Find the certificate you want to delete and click **Delete**. The Administration | Certificate Management | Delete screen appears.

Figure 12-39 Administration | Certificate Management | Delete Screen

Administration | Certificate Management | Delete

Subject	Issuer
CN=10.10.99.30	CN=10.10.99.30
OU=VPN 3000 Concentrator	OU=VPN 3000 Concentrator
O=Cisco Systems, Inc.	O=Cisco Systems, Inc.
L=Franklin	L=Franklin
SP=Massachusetts	SP=Massachusetts
C=US	C=US

Serial Number 3B8D11D6

Signing Algorithm MD5WithRSA

Public Key Type RSA (1024 bits)

MD5 Thumbprint FD:AD:40:68:2D:A4:F5:DD:43:0A:F5:4D:99:A8:D6:2E

SHA1 Thumbprint 6E:39:6B:AE:AF:18:A9:19:CE:9F:F1:4D:59:D9:1F:26:0B:FB:C1:13

Validity 8/29/2001 at 12:01:26 to 8/28/2004 at 12:01:26

Are you **sure** you want to delete this certificate?

- Step 3** Click **Yes**. The Manager returns to the Administration | Certificate Management window.

Administration | Certificate Management

This section of the Manager shows outstanding enrollment requests and all the certificates installed on the VPN 3002, and it lets you manage them.

The links at the top of this screen guide you step-by-step through the process of enrolling and installing certificates. For more information on the certificate management process, see the “[Enrolling and Installing Digital Certificates](#)” section.

- To install a CA certificate (via SCEP or manually), click on **Click Here to Install a CA Certificate**.



Note The Click here to install a CA certificate option is only available from this window when no CA certificates are installed on the VPN 3002. If you do not see this option, click **Click here to install a certificate**. The Manager displays the Administration | Certificate Management | Install. Then click **Install CA Certificate**.

- To create an SSL or identity certificate enrollment request, click on **Click Here to Enroll with a Certificate Authority**.
- To install the certificate obtained via enrollment, click on **Click Here to Install a Certificate**.

The VPN 3002 notifies you (by issuing a severity 3 CERT class event) if any of the installed certificates are within one month of expiration.

The Manager displays this screen each time you install a digital certificate.

Figure 12-40 Administration | Certificate Management Screen

Administration | Certificate Management
Thursday, 15 January 2004 11:18:57
Refresh

This section lets you view and manage certificates on the VPN 3002 Hardware Client.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
ms-root-sha-06-2001 at cisco	ms-root-sha-06-2001 at cisco	06/04/2022	No	View Delete

Identity Certificates (current: 1, maximum: 1)

Subject	Issuer	Expiration	Actions
Gateway A at Cisco Systems	ms-root-sha-06-2001 at cisco	04/02/2004	View Renew Delete

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.86.194.176 at Cisco Systems, Inc.	10.86.194.176 at Cisco Systems, Inc.	01/14/2007	View Renew Delete Export Generate Enroll Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
1024 bits	RSA	09/28/2001	Generate

Enrollment Status [[Remove All: Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#)] (current: 0 available: 1)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

104903

Certificate Authorities Table

This table shows root and subordinate CA certificates installed on the VPN 3002.

Current


The actual number of CA certificates installed on this VPN 3002.

Maximum

The maximum possible number of CA certificates allowed on this VPN 3002.

Fields

These fields appear in the Certificate Authorities table:

Field	Content
Subject/Issuer	The Common Name (CN) or Organizational Unit (OU) (if present), plus the Organization (O) in the Subject and Issuer fields of the certificate. The format is CN at O, OU at O, or just O; for example, Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See Administration Certificate Management Certificates View.
Expiration	The expiration date of the certificate. The date format is MM/DD/YYYY.
SCEP Issuer	In order for a certificate to be available for SCEP enrollment, it must be installed via SCEP. This field indicates if the certificate is SCEP-enabled. <ul style="list-style-type: none"> • Yes = This certificate can issue identity and SSL certificates via SCEP. • No = This certificate cannot issue certificates via SCEP.
	 <hr/> <p>Note If you want to use a certificate for SCEP enrollment, but that certificate is not SCEP-enabled, reinstall it using SCEP.</p> <hr/>
Actions	This column allows you to manage particular certificates. The actions available vary with type and status of the certificate. <ul style="list-style-type: none"> • View = View details of this certificate. • Delete = Delete this certificate from the VPN 3002.

Identity Certificates Table

This table shows installed server identity certificates.

Fields

These fields appear in the Identity Certificates table:

Field	Content
Subject/Issuer	The Common Name (CN) or Organizational Unit (OU) (if present), plus the Organization (O) in the Subject and Issuer fields of the certificate. The format is CN at O, OU at O, or just O; for example, Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See Administration Certificate Management Certificates View.
Expiration	The expiration date of the certificate. The date format is MM/DD/YYYY.
Actions	This column allows you to manage particular certificates. The actions available vary with type and status of the certificate. <ul style="list-style-type: none">• View = View details of this certificate.• Delete = Delete this certificate from the VPN 3002.• Renew = Generate a new enrollment request based on the content of this certificate.

SSL Certificate Table

This table shows the SSL server certificate installed on the VPN 3002. The system can have only one SSL server certificate installed per (public or private) interface: either a self-signed certificate or one issued in a PKI context.

Fields

These fields appear in the SSL Certificates table:

Field	Content
Interface	The interface on which this SSL certificate is installed.
Subject/Issuer	The Common Name (CN) or Organizational Unit (OU) (if present), plus the Organization (O) in the Subject and Issuer fields of the certificate. The format is CN at O, OU at O, or just O; for example, Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See Administration Certificate Management Certificates View.
Expiration	The expiration date of the certificate. The date format is MM/DD/YYYY.
Actions	This column allows you to manage particular certificates. The actions available vary with type and status of the certificate. <ul style="list-style-type: none">• View = View details of this certificate.• Renew = Generate a new enrollment request based on the content of this certificate.• Delete = Delete this certificate from the VPN 3002.• Export = Copy this certificate to another interface on this VPN 3002 or to another VPN 3002.• Generate = Generate a new SSL certificate, with a new key.• Enroll = Enroll this certificate with a CA.• Import = Copy a certificate to this interface from another interface on this VPN 3002 or from another VPN 3002.

SSH Host Key Table

Fields

These fields appear in the SSH Host Key table:

Field	Content
Key Size	This size (in bits) of the SSH host key.
Key Type	The type of encryption of the SSH host key. (Only RSA is currently supported.)
Date Generated	The generation date of the certificate.
Actions	Generate = Generate a new SSH host key.

Enrollment Status Table

This table tracks the status of active enrollment requests.

The VPN 3002 supports one (installed) identity certificate and one (outstanding) enrollment request. If you currently have an identity certificate on your VPN 3002 and you want to change it, you can request a second certificate, but the VPN 3002 does not install this certificate immediately. The new certificate appears in the Enrollment Status table; you must activate it manually.

The VPN 3002 automatically deletes entries that have the status “Timedout,” “Failed,” “Cancelled,” or “Error” and are older than one week.

[Remove All:]

Click a **Remove All** option to delete all enrollment requests of a particular status.

- Errored = Delete all enrollment requests with the status “Error.”
- Timed-out = Delete all enrollment requests with the status “Timed-out.”
- Rejected = Delete all enrollment requests with the status “Rejected.”
- Cancelled = Delete all enrollment requests with the status “Cancelled.”
- In Progress = Delete all enrollment requests with the status “In Progress.”

Current

The number of enrollment requests currently outstanding.

Available

The number of enrollment requests still available.

Fields

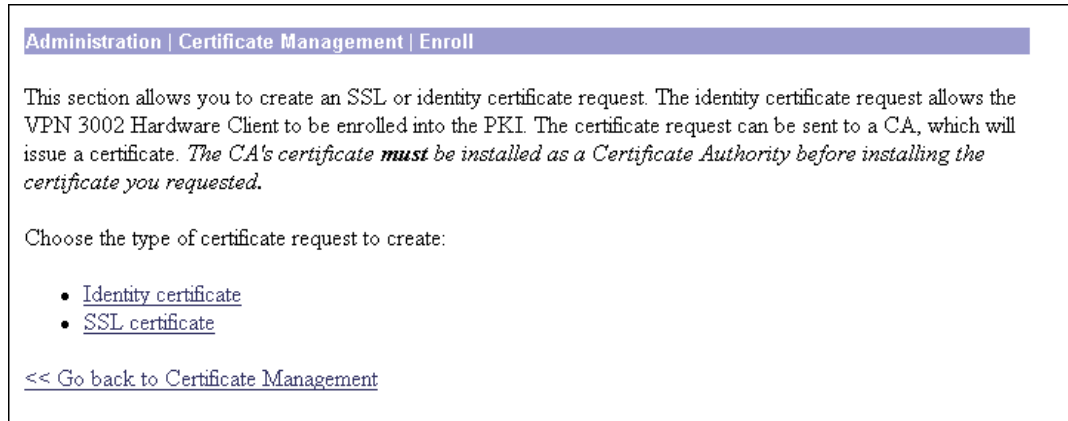
These fields appear in the Enrollment Status table:

Field	Content
Subject/Issuer	The Common Name (CN) or Organizational Unit (OU) (if present), plus the Organization (O) in the Subject and Issuer fields of the certificate. The format is CN at O, OU at O, or just O; for example, Root 2 at CyberTrust. The CN, OU, and O fields display a maximum of 33 characters each. See Administration Certificate Management Certificates View.
Date	The original date of enrollment.
Use	The type of certificate: identity or SSL.
Reason	The type of enrollment: initial, re-enrollment, or re-key.
Method	The method of enrollment: SCEP or manual.
Status	<ul style="list-style-type: none"> • In Progress = The request has been created, but the requested certificate has not yet been installed. This value is used only for PKCS10 (manual) enrollment requests. • Timedout = The SCEP polling cycle has ended after reaching the configured maximum number of retries. This value is used only for enrollment request created using SCEP. • Rejected = The CA refused to issue the certificate. This value is used only for enrollment request created using SCEP. • Cancelled = The certificate request was cancelled while the VPN 3002 was in polling mode. • Error = An error occurred during the enrollment process. Enrollment was stopped.
Actions	<p>This column allows you to manage enrollments requests. The actions available vary with the type and status of the enrollment request.</p> <ul style="list-style-type: none"> • View = View details of this enrollment request. • Install = Install the enrollment request. This action is available only for PKCS10 (manual) enrollment requests. • Cancel = Cancel a request that is pending. This action is available only for SCEP enrollment requests with “Polling” status. • Re-submit = Re-initiate SCEP communications with the CA or RA using the previously entered request information. This action is available only for SCEP enrollment requests. • Activate = Bring this certificate into service. • Delete = Delete an enrollment request from the VPN 3002.

Administration | Certificate Management | Enroll

Choose whether you are creating an enrollment request for an identity certificate or an SSL certificate.

Figure 12-41 Administration | Certificate Management | Enroll Screen



Identity Certificate

Click **Identity Certificate** to create a certificate request for an identity certificate. The Manager displays the Administration | Certificate Management | Enroll | Identity Certificate screen.

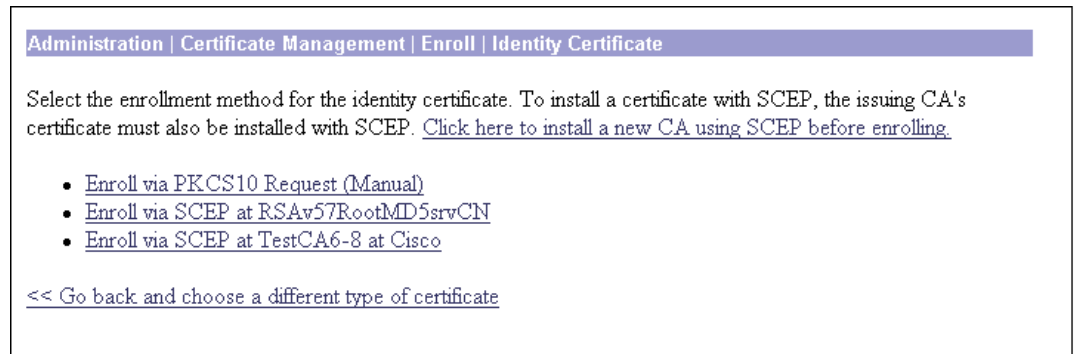
SSL Certificate

Click **SSL Certificate** to create a certificate request for an SSL certificate. The Manager displays the Administration | Certificate Management | Enroll | SSL Certificate screen.

Administration | Certificate Management | Enroll | *Certificate Type*

Choose the method for enrolling the (identity or SSL) certificate.

Figure 12-42 Administration | Certificate Management | Enroll | Identity Certificate Screen



Enroll via PKCS10 Request (Manual)

Click **Enroll via PKCS10 Request (Manual)** to enroll the certificate manually.

Enroll via SCEP at *[Name of SCEP CA]*

You can enroll certificates using SCEP only if you installed the CA certificate using SCEP. One Enroll via SCEP at *[Name of SCEP CA]* link appears on this screen for each CA certificate on the VPN 3002 that was installed using SCEP. To see which CA certificates on your VPN 3002 were installed using SCEP, see the Certificate Authorities table on the Administration | Certificate Management screen. “Yes” in the SCEP Issuer column indicates that the CA certificate was installed using SCEP; “No” indicates it was installed manually.

If no CA certificate on the VPN 3002 was installed using SCEP, then no Enroll via SCEP at *[Name of SCEP CA]* link appears on this screen. You do not have the option of using SCEP to enroll the certificate.

Click **Enroll via SCEP at *[Name of SCEP CA]*** to enroll the certificate automatically using SCEP.

Install a New SA Using SCEP before Enrolling

If you want to install a certificate using SCEP, but no Enroll via SCEP at *[Name of SCEP CA]* link appears here, click **Install a new SA Using SCEP before Enrolling**. Install a CA certificate using SCEP, then return to this screen to install the certificate. A SCEP link now appears.

<< Go back and choose a different type of certificate

Click << **Go back and choose a different type of certificate** to return to the Administration | Certificate Management | Enroll screen. (See [Figure 12-41](#).)

Administration | Certificate Management | Enroll | *Certificate Type* | PKCS10

To generate an enrollment request for an SSL or identity certificate, you need to provide information about the VPN 3002.

Figure 12-43 Administration | Certificate Management | Enroll | Identity Certificate via PKCS10 Screen

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.*

Common Name (CN) <input style="width: 90%;" type="text"/>	Enter the common name for the VPN 3002 Hardware Client to be used in this PKI.
Organizational Unit (OU) <input style="width: 90%;" type="text"/>	Enter the department.
Organization (O) <input style="width: 90%;" type="text"/>	Enter the Organization or company.
Locality (L) <input style="width: 90%;" type="text"/>	Enter the city or town.
State/Province (SP) <input style="width: 90%;" type="text"/>	Enter the State or Province.
Country (C) <input style="width: 20px;" type="text"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN) <input style="width: 90%;" type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3002 Hardware Client to be used in this PKI.
Subject AlternativeName (E-Mail Address) <input style="width: 90%;" type="text"/>	Enter the E-Mail Address for the VPN 3002 Hardware Client to be used in this PKI.
Key Size <input style="width: 80px;" type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA/DSA key pair.

67601

Fields

For an explanation of each of the fields on this screen, see [Table 12-1](#).

Table 12-1 Fields in a Certificate Request


Field Name	Manual	SCEP	Content
Common Name (CN)	Yes	Yes	The primary identity of the entity associated with the certificate, for example, Gateway A. Spaces are allowed. You must enter a name in this field.
Organizational Unit (OU)	Yes	Yes	The name of the department or other organizational unit to which this VPN 3002 belongs, for example: VPNC. Spaces are allowed.  Caution The value you enter in this field must match on both ends of the connection.
Organization (O)	Yes	Yes	The name of the company or organization to which this VPN 3002 belongs, for example: Cisco Systems. Spaces are allowed.
Locality (L)	Yes	Yes	The city or town where this VPN 3002 is located, for example: Franklin. Spaces are allowed.
State/Province (SP)	Yes	Yes	The state or province where this VPN 3002 is located, for example: Massachusetts. Spell the name out completely; do not abbreviate. Spaces are allowed.
Country (C)	Yes	Yes	The country where this VPN 3002 is located, for example: US. Use two characters, no spaces, and no periods. This two-character code must conform to ISO 3166 country codes.
Subject Alternative Name (Fully Qualified Domain Name) (FQDN)	Yes	Yes	The fully qualified domain name that identifies this VPN 3002 in this PKI, for example: Cisco.com. This field is optional. The alternative name is an additional data field in the certificate that provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections.
Subject Alternative Name (E-mail Address) (E-mail)	Yes	Yes	The e-mail address of the VPN 3002 administrator, for example: gatewaya@cisco.com.
Challenge Password	No	Yes	This field displays if you are requesting a certificate using SCEP. Use this field according to the policy of your CA: Your CA might have given you a password. If so, enter it here for authentication. Your CA might allow you to provide your own password to identify yourself to the CA in the future. If so, create your password here. Your CA might not require a password. If not, leave this field blank.

Table 12-1 Fields in a Certificate Request

Field Name	Manual	SCEP	Content
Verify Challenge Password	Mp	Yes	Re-enter the password.
Key Size	Yes	Yes	<p>The algorithm for generating the public-key/private-key pair, and the key size. If you are requesting an SSL certificate, or if you are requesting an identity certificate using SCEP, only the RSA options are available.</p> <ul style="list-style-type: none"> • RSA 512 bits = Generate 512-bit keys using the RSA (Rivest, Shamir, Adelman) algorithm. This key size provides sufficient security and is the default selection. It is the most common, and requires the least processing. • RSA 768 bits = Generate 768-bit keys using the RSA algorithm. This key size provides normal security. It requires approximately 2 to 4 times more processing than the 512-bit key. • RSA 1024 bits = Generate 1024-bit keys using the RSA algorithm. This key size provides high security, and it requires approximately 4 to 8 times more processing than the 512-bit key. • RSA 2048 = Generate 2048-bit keys using the RSA algorithm. This key size provides very high security. It requires 8-16 times more processing than the 512-bit key.
	Yes	No	<ul style="list-style-type: none"> • DSA 512 bits = Generate 512-bit keys using DSA (Digital Signature Algorithm). • DSA 768 bits = Generate 768-bit keys using the DSA algorithm. • DSA 1024 bits = Generate 1024-bit keys using the DSA algorithm.

Enroll / Cancel

To generate the certificate request, click **Enroll**. The Manager displays the Administration | Certificate Management | Enrollment | Request Generated screen (See [Figure 12-44](#).) with the text of your certificate.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen.

Administration | Certificate Management | *Enrollment or Renewal* | Request Generated

The Manager displays this screen when the system has successfully generated a certificate request. The request is a Base-64 encoded file in PKCS-10 format (Public Key Certificate Syntax-10), which most CAs recognize or require. The system automatically saves this file in Flash memory with the filename shown in the screen (pkcsNNNN.txt). You can select and copy the request to the clipboard, or you can save it as a file on your PC or a network host. Some CAs let you paste the request in a web interface, some ask you to send a file; use the method your CA requires.

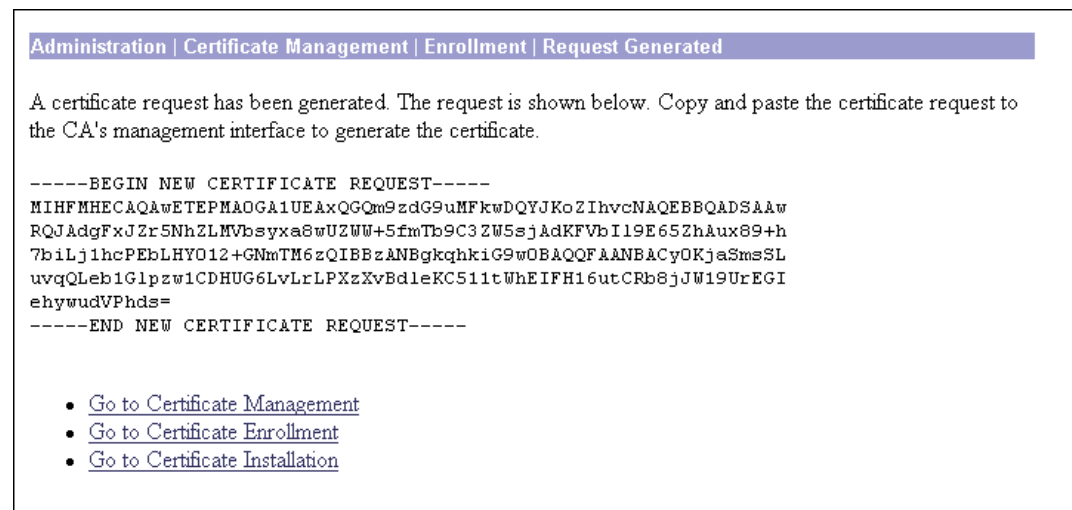
In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN 3002, and it is not visible.



Note

You must complete the enrollment and certificate installation process within one week of generating the request.

Figure 12-44 Administration | Certificate Management | Enrollment | Request Generated Screen



To go to the Administration | File Management | Files screen, click the highlighted **File Management** page link. From there you can view, copy, or delete the file in Flash memory.

Go to Certificate Management

If you want to view the certificate request, click **Go to Certificate Management**. The Manager displays the Administration | Certificate Management screen. (See [Figure 12-20](#).)

Go to Certificate Enrollment

If you want to enroll another certificate, click **Go to Certificate Enrollment**. The Manager displays the Administration | Certificate Management | Enroll screen.

Go to Certificate Installation

If you want to install the certificate you have just enrolled, click **Go to Certificate Installation**. The Manager displays the Administration | Certificate Management | Install screen.

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

To generate an enrollment request for an identity certificate, you need to provide information about the VPN 3002.

Figure 12-45 Administration | Certificate Management | Enroll | Identity Certificate | SCEP Screen

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

Enter the information to be included in the certificate request. **Please wait for the operation to finish.**

<p>Common Name (CN) <input style="width: 90%;" type="text"/></p> <p>Organizational Unit (OU) <input style="width: 90%;" type="text"/></p> <p>Organization (O) <input style="width: 90%;" type="text"/></p> <p>Locality (L) <input style="width: 90%;" type="text"/></p> <p>State/Province (SP) <input style="width: 90%;" type="text"/></p> <p>Country (C) <input style="width: 90%;" type="text"/></p> <p>Subject AlternativeName (FQDN) <input style="width: 90%;" type="text"/></p> <p>Subject AlternativeName (E-Mail Address) <input style="width: 90%;" type="text"/></p> <p>Challenge Password <input style="width: 90%;" type="text"/></p> <p>Verify Challenge Password <input style="width: 90%;" type="text"/></p> <p>Key Size <input style="width: 80%;" type="text" value="RSA 512 bits"/> <input style="width: 20%;" type="button" value="v"/></p>	<p>Enter the common name for the VPN 3002 Hardware Client to be used in this PKI.</p> <p>Enter the department.</p> <p>Enter the Organization or company.</p> <p>Enter the city or town.</p> <p>Enter the State or Province.</p> <p>Enter the two-letter country abbreviation (e.g. United States = US).</p> <p>Enter the Fully Qualified Domain Name for the VPN 3002 Hardware Client to be used in this PKI.</p> <p>Enter the E-Mail Address for the VPN 3002 Hardware Client to be used in this PKI.</p> <p>Enter and verify the challenge password for this certificate request.</p> <p>Select the key size for the generated RSA key pair.</p>
---	--

67597

Fields

For an explanation of each of the fields on this screen, see [Table 12-1](#).

Enroll / Cancel

To generate the certificate request and install the identity certificate on the VPN 3002, click **Enroll**. The Manager displays the Administration | Certificate Management | Enrollment | Request Generated screen. (See [Figure 12-44](#).)

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See [Figure 12-20](#).)

Administration | Certificate Management | Enroll | SSL Certificate | SCEP

To generate an enrollment request for an SSL certificate, you need to provide information about the VPN 3002.

Figure 12-46 Administration | Certificate Management | Enroll | SSL Certificate | SCEP Screen

Administration | Certificate Management | Enroll | SSL Certificate | SCEP

Enter the information to be included in the certificate request. **Please wait for the operation to finish.**

Type in the name of the certificate file below.

Common Name (CN)	<input type="text" value="vpn02.cisco.com"/>	Enter the common name for the VPN 3002 Hardware Client to be used in this PKI. Use the domain name or IP address you will use to connect to this VPN 3002 Hardware Client.
Organizational Unit (OU)	<input type="text"/>	Enter the department.
Organization (O)	<input type="text"/>	Enter the Organization or company.
Locality (L)	<input type="text"/>	Enter the city or town.
State/Province (SP)	<input type="text"/>	Enter the State or Province.
Country (C)	<input type="text"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3002 Hardware Client to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3002 Hardware Client to be used in this PKI.
Challenge Password	<input type="text"/>	Enter and verify the challenge password for this certificate request.
Verify Challenge Password	<input type="text"/>	
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA key pair.

67603

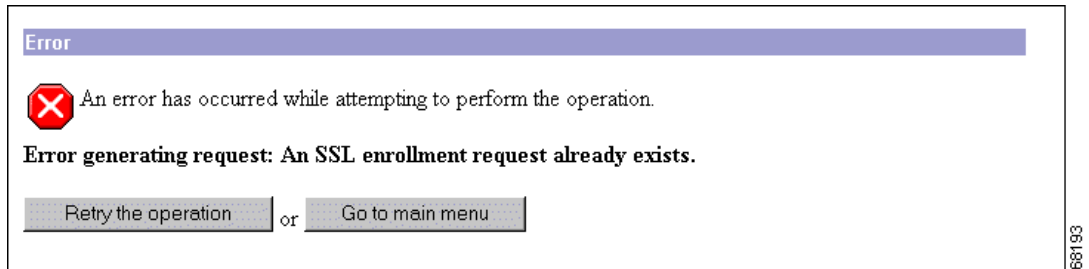
Fields

For an explanation of each of the fields on this screen, see [Table 12-1](#).

Enroll

To generate the certificate request and install the SSL certificate on the VPN 3002, click **Enroll**. The Manager displays the Administration | Certificate Management | Enrollment | Request Generated screen.

If there is already an active request for an SSL certificate, this error message appears.



To return to the Administration | Certificate Management | Enroll | SSL Certificate | SCEP screen, click **Retry the operation**.

To return to the Main screen, click **Return to main menu**.

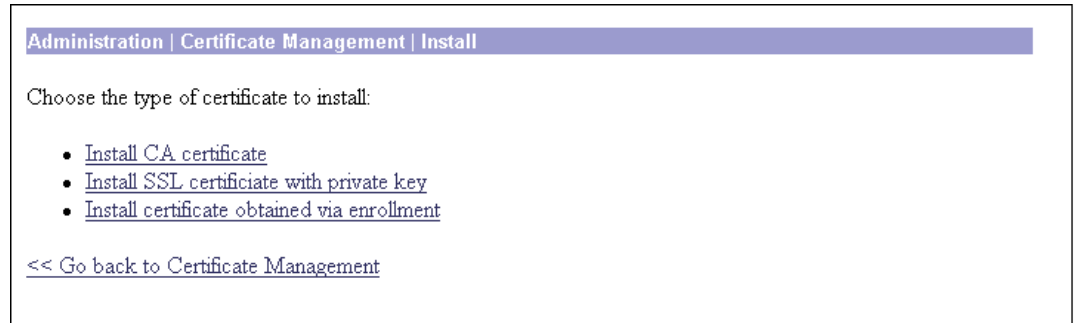
Cancel

To discard your entries and cancel the request, click **Cancel**. The Manager displays the Administration | Certificate Management screen.

Administration | Certificate Management | Install

Choose the type of certificate you want to install.

Figure 12-47 Administration | Certificate Management | Install Screen



Install CA Certificate

If you want to install a CA certificate, click **Install CA Certificate**. The Manager displays the Administration | Certificate Management | Install | CA Certificate screen.

Install SSL Certificate with Private Key

Some web servers export their SSL certificates with the private key attached. If you have a PEM-encoded certificate with a corresponding private key that you want to install, click **Install SSL Certificate with Private Key**. The Manager displays the Administration | Certificate Management | Install | SSL Certificate with Private Key screen.

Install Certificate Obtained via Enrollment

If you want to install a certificate manually that you have obtained by enrolling a certificate request with a CA, click **Install Certificate Obtained via Enrollment**. The Manager displays the Administration | Certificate Management | Install Certificate Obtained via Enrollment screen.

Administration | Certificate Management | Install | Certificate Obtained via Enrollment

Once you have enrolled a certificate, you can install it. This screen allows you to install an enrolled certificate.

Figure 12-48 Administration | Certificate Management | Install | Certificate Obtained via Enrollment Screen

Administration | Certificate Management | Install certificate obtained via enrollment

Select an enrollment request to install.

Enrollment Status

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
snoopy	N/A	09/05/2001	ID	Re-enroll	Manual	In Progress	[View Install Delete]
10.10.99.30	RSAAv57RootMD5srvCN	09/07/2001	SSL	Re-enroll	SCEP	Complete	[View Activate Delete]
Linda 3	RSAAv57RootMD5srvCN	09/07/2001	ID	Initial	SCEP	Error	[View Re-submit Delete]

[<< Go back and choose a different type of certificate](#)

98189

Enrollment Status Table

For a description of the fields in this table, see the “[Enrollment Status Table](#)” section.

<< Go back and choose a different type of certificate

If you do not want to install a certificate that you have obtained via filing an enrollment request with your CA, click << **Go back and choose a different type of certificate**. The Manager returns to the Administration | Certificate Management | Install screen.

Administration | Certificate Management | Install | *Certificate Type*

Choose the method you want to use to install the certificate.

Figure 12-49 Administration | Certificate Management | Install | CA Certificate



SCEP (Simple Certificate Enrollment Protocol)



Note

This option is available only for CA certificates.

If you want to install the CA certificate automatically using SCEP, click **SCEP (Simple Certificate Enrollment Protocol)**. The Manager displays the Administration | Certificate Management | Install | CA Certificate | SCEP screen. (See [Figure 12-50](#).)

Cut & Paste Text

If you want to cut and paste the certificate using a browser window, click **Cut & Paste Text**. The Manager displays the Administration | Certificate Management | Install | *Certificate Type* | Cut & Paste Text screen. (See [Figure 12-51](#).)

Upload File from Workstation

If your CA certificate is stored in a file, click **Upload File from Workstation**. The Manager displays the Administration | Certificate Management | Install | *Certificate Type* | Upload File from Workstation screen. (See [Figure 12-54](#).)

<< Go back and choose a different type of certificate

If you do not want to install a CA certificate, click **<< Go back and choose a different type of certificate** to display the Administration | Certificate Management | Install screen. (See [Figure 12-47](#).)

Administration | Certificate Management | Install | CA Certificate | SCEP

In this screen, provide information about the certificate authority in order to retrieve and install a CA certificate automatically using SCEP.

Figure 12-50 Administration | Certificate Management | Install | CA Certificate | SCEP Screen

Administration | Certificate Management | Install | CA Certificate | SCEP

Enter the information needed to retrieve the CA certificate via SCEP. **Please wait for the operation to complete.**

URL

CA Descriptor Required for some PKI configurations.

68173

URL

Enter the URL of the SCEP interface of the CA.

CA Descriptor

Some CAs use descriptors to further identify the certificate. If your CA gave you a descriptor, enter it here. Otherwise enter a descriptor of your own. You must enter something in this field.

Retrieve / Cancel

To retrieve a CA certificate from the CA and install it on the VPN 3002, click **Retrieve**.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See [Figure 12-20](#).)

Administration | Certificate Management | Install | *Certificate Type* | Cut and Paste Text

To install the certificate using the manual method, cut and paste the certificate text into the Certificate Text window.

Figure 12-51 Administration | Certificate Management | Install | CA Certificate | Cut and Paste Text Screen

The screenshot shows a window titled "Administration | Certificate Management | Install | CA Certificate | Cut & Paste Text". The window contains the instruction "Paste the CA certificate text into the box below." Below this instruction is a large, empty text area labeled "Certificate Text". At the bottom of the window are two buttons: "Install" and "Cancel".

68174

Figure 12-52 Administration | Certificate Management | Install | SSL Certificate | Cut and Paste Text Screen

The screenshot shows a window titled "Administration | Certificate Management | Install | SSL Certificate | Cut & Paste Text". The window contains the instruction "Paste the SSL certificate text into the box below." Below this instruction is a large, empty text area labeled "Certificate Text". Below the text area is a dropdown menu labeled "Interface" with "Private" selected. At the bottom of the window are two buttons: "Install" and "Cancel".

104802

Figure 12-53 Administration | Certificate Management | Install | SSL Certificate with Private Key/ Cut and Paste Text Screen

Certificate Text

Paste the PEM or base-64 encoded certificate text from the clipboard into this window. If you are installing an SSL certificate with a private key, include the encrypted private key.

Password



Note

This field appears only if you are installing an SSL certificate with a private key.

Enter a password for decrypting the private key. Use the same password you used to encrypt the private key when you exported it. (See Administration | Certificate Management | Export SSL Certificate.)

Interface



Note

This field appears only if you are installing an SSL certificate.

Choose the interface on which to install the certificate.

Install / Cancel

To install the certificate on the VPN 3002, click **Install**.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See [Figure 12-20](#).)

Administration | Certificate Management | Install | *Certificate Type* | Upload File from Workstation

If you want to install a certificate stored on your PC, use this screen to upload the certificate file to the VPN 3002.

Figure 12-54 Administration | Certificate Management | Install | CA Certificate | Upload File from Workstation Screen

Administration | Certificate Management | Install | CA Certificate | Upload File from Workstation

Enter the name of the CA certificate file.

Filename Browse...

Install Cancel

68175

Figure 12-55 Administration | Certificate Management | Install | SSL Certificate | Upload File from Workstation Screen

Administration | Certificate Management | Install | SSL Certificate | Upload File from Workstation

Enter the name of the SSL certificate file.

Filename Browse...

Interface Private ▾

Install Cancel

104805

Figure 12-56 Administration | Certificate Management | Install | SSL Certificate with Private Key | Upload File from Workstation Screen

Administration | Certificate Management | Install | SSL Certificate with Private Key | Upload File from Workstation

Enter the name of the SSL certificate with private key file and the password to decrypt the private key.

Filename Browse...

Password

Interface Private ▾

Import Cancel

104804

Filename / Browse

Enter the name of the certificate file that is on your PC. In a Windows environment, enter the complete pathname using MS-DOS syntax, for example: c:\Temp\certnew.cer. You can also click the **Browse** button to open a file navigation window, find the file, and select it.

Password

**Note**

This field appears only if you are installing an SSL certificate with a private key.

Enter a password for decrypting the private key. Use the same password you used to encrypt the private key when you exported it. (See Administration | Certificate Management | Export SSL Certificate.)

Interface

**Note**

This field appears only if you are installing an SSL certificate.

Choose the interface on which to install the certificate.

Install / Cancel

To install the certificate on the VPN 3002, click **Install**.

To discard your entries and cancel the request, click **Cancel**. The Manager returns to the Administration | Certificate Management screen. (See [Figure 12-20](#).)

Administration | Certificate Management | View

The Manager displays this screen of certificate details when you click **View** for a certificate on the Administration | Certificate Management | Certificates screen. The details vary depending on the certificate content.

The content and format for certificate details are governed by ITU (International Telecommunication Union) X.509 standards, specifically RFC 2459. The Subject and Issuer fields conform to ITU X.520.

This screen is read-only; you cannot change any information here.

Figure 12-57 Administration | Certificate Management | View Screen

Administration | Certificate Management | View

Subject	Issuer
CN=TestCA6-8 RA	CN=TestCA6-8
OU=Devtest	OU=QA
O=Cisco Systems	O=Cisco
L=Franklin	L=Franklin
SP=MA	SP=MA
C=US	C=US

Serial Number 61136DCA000100000370

Signing Algorithm MD5WithRSA

Public Key Type RSA (1024 bits)

Certificate Usage Digital Signature, Non Repudiation

MD5 Thumbprint 22:12:65:2E:2B:12:05:B4:49:16:F0:6B:BA:45:A1:7B

SHA1 Thumbprint 46:3C:E2:0B:0F:AA:0A:41:05:56:8A:FA:B5:5D:C1:15:04:D1:25:1E

Validity 6/22/2001 at 11:28:38 to 6/22/2002 at 11:38:38

CRL Distribution Point /CN=TestCA6-8,CN=2KPDC,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=qa2000,DC=com/objectclass=cRLDistributionPoint

68179

Certificate Fields

A certificate contains some or all of the following fields:

Field	Content
Subject	The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
Issuer	The CA or other entity (jurisdiction) that issued the certificate. Subject and Issuer consist of a specific-to-general identification hierarchy: CN, OU, O, L, SP, and C. These labels and acronyms conform to X.520 terminology, and they echo the fields on the Administration Certificate Management Enrollment screen.
CN	Common Name: the name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy. For the VPN 3002 self-signed SSL certificate, the CN is the IP address on the Ethernet 1 (Private) interface at the time the certificate is generated. SSL compares this CN with the address you use to connect to the VPN 3002 via HTTPS, as part of its validation.
OU	Organizational Unit: the subgroup within the organization (O).
O	Organization: the name of the company, institution, agency, association, or other entity.
L	Locality: the city or town where the organization is located.
SP	State/Province: the state or province where the organization is located.
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Serial Number	The serial number of the certificate. Each certificate issued by a CA must be unique among all certificates issued by that CA. CRL checking uses this serial number.
Signing Algorithm	The cryptographic algorithm that the CA or other issuer used to sign this certificate.
Public Key Type	The algorithm and size of the certified public key.
Certificate Usage	The purpose of the key contained in the certificate, for example: digital signature, certificate signing, nonrepudiation, key or data encipherment, etc.
MD5 Thumbprint	A 128-bit MD5 hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a root certificate's authenticity, you can check this value with the issuer.

Field	Content
SHA1 Thumbprint	A 160-bit SHA-1 hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.
Validity	<p>The time period during which this certificate is valid.</p> <p>Format is MM/DD/YYYY at HH:MM:SS to MM/DD/YYYY at HH:MM:SS. Time uses 24-hour notation, and is local system time.</p> <p>The Manager checks the validity against the VPN 3002 system clock, and it flags expired certificates in event log entries.</p>
Subject Alternative Name (Fully Qualified Domain Name)	The fully qualified domain name for this VPN 3002 that identifies it in this PKI. The alternative name is an optional additional data field in the certificate, and it provides inter operability with many Cisco IOS and PIX systems in LAN-to-LAN connections.
CRL Distribution Point	The distribution point for CRLs from the issuer of this certificate. If this information is included in the certificate in the proper format, and you enable CRL checking, you do not have to provide it on the Administration Certificate Management Configure CA Certificate screen.

Back

To return to the Administration | Certificate Management screen, click **Back**.

Administration | Certificate Management | Configure CA Certificate

This screen lets you configure this CA certificate to be able to issue identity certificates via SCEP.

Figure 12-58 Administration | Certificate Management | Configure CA Certificate Screen

The screenshot shows a web interface for configuring a CA certificate. At the top, a breadcrumb trail reads 'Administration | Certificate Management | Configure CA Certificate'. Below this, the certificate name is 'Certificate.RSAv57RootMD5srvCN'. The main section is titled 'SCEP Configuration' and contains three input fields with labels and instructions:

- Enrollment URL:** A text box containing 'http://100.220.0.110:446/p'. To its right, the text reads 'Enter the URL for enrollment.'
- Polling Interval:** A text box containing '1'. To its right, the text reads 'Enter the polling interval in minutes.'
- Polling Limit:** A text box containing 'none'. To its right, the text reads 'Enter the maximum number of polling attempts to reach the SCEP PKI. Enter "none" to set no limit on the number of attempts.'

At the bottom left of the form area, there are two buttons: 'Apply' and 'Cancel'. On the right side of the screenshot, there is a vertical text label '68261'.

Certificate

The certificate for which you are configuring SCEP parameters. This is the name in the Subject field of the Certificate Authorities table on the Administration | Certificate Management screen.

SCEP Configuration

Enrollment URL

Enter the URL where the VPN 3002 should send SCEP enrollment requests made to this CA certificate. The default value of this field is the URL used to download this CA certificate.

Polling Interval

If the CA does not issue the certificate immediately (some CAs require manual verification of credentials and this can take time), the certificate request could enter polling mode. In polling mode, the VPN 3002 re-sends the certificate request to the CA over a specified period until the CA responds or the process times out.

Enter the number of minutes the VPN 3002 should wait between re-sends. The minimum number of minutes is 1; the maximum number of minutes is 60. The default value is 1.

Polling Limit

Enter the number of times the VPN 3002 should re-send an enrollment request if the CA does not issue the certificate immediately. The minimum number of re-sends is 0; the maximum number is 100. If you do not want any polling limit (in other words you want infinite re-sends), enter *none*.

Apply / Cancel

To configure CRL checking for this certificate, click **Apply**. The Manager returns to the Administration | Certificate Management screen.

To discard your settings, click **Cancel**. The Manager returns to the Administration | Certificate Management screen.

Administration | Certificate Management | Renewal

Certificate renewal is a shortcut that allows you to generate an enrollment request based on the content of an existing certificate.

When you renew a certificate via SCEP, the new certificate does not automatically overwrite the original certificate. It remains in the Enrollment Request table until the administrator manually activates it. For more information on activating certificates, see the “[Administration | Certificate Management | Activate or Re-Submit | Status](#)” section.

Use this screen to re-enroll or re-key a certificate. If you *re-enroll* the certificate, the new certificate uses the same key pair as the expiring certificate. If you *re-key* the certificate, it uses a new key pair.

Figure 12-59 Administration | Certificate Management | Renewal

Administration | Certificate Management | Renewal

This section allows you to re-enroll or re-key a certificate, so that the VPN 3002 Hardware Client updates its certificate. The certificate request can be sent to a CA, which in turn, sends back a certificate. **Please wait for the operation to finish.**

Certificate SSL Certificate

Renewal Type Re-enrollment Select the type of renewal. A *re-enrollment* uses the same key for the certificate. A *re-key* generates a new key for the certificate.
 Re-key

Enrollment Method Select the renewal method for this certificate.

Challenge Password

Verify Challenge Password Enter and verify the challenge password for this certificate request.

682789

Certificate

This field displays the type of certificate that you are re-enrolling or re-keying.

Renewal Type

Specify the type of request:

- Re-enrollment = Use the same key pair as the expiring certificate.
- Re-key = Use a new key pair.

Enrollment Method

Choose an enrollment method:

- PKCS10 Request (Manual) = Enroll using the manual process.
- *Certificate Name* via SCEP = Enroll automatically using this SCEP CA.

Challenge Password

Your CA might have given you a password as a means of verifying your identity. If you have a password from your CA, enter it here.

If you did not receive a password from your CA, choose a password now. You can use this password in the future to identify yourself to your CA.

Verify Challenge Password

Re-type the challenge password you just entered.

Renew / Cancel

To renew the certificate, click **Renew**.

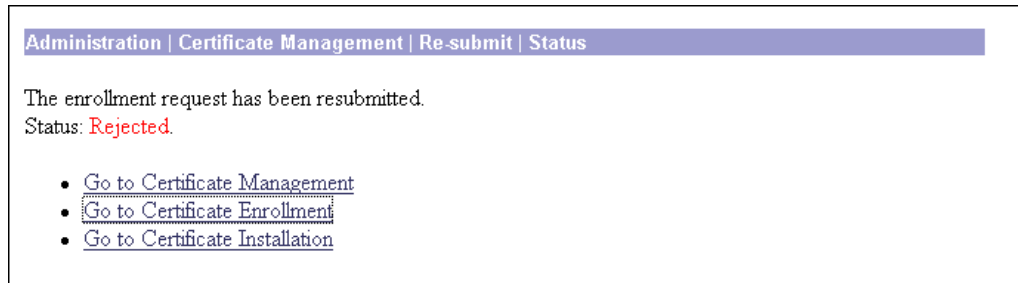
To discard your settings, click **Cancel**. The Manager returns to the Administration | Certificate Management screen.

Administration | Certificate Management | *Activate or Re-Submit* | Status

This status screen appears after you activate or re-submit an enrollment request. It displays the status of the request.

If you are installing an SSL certificate with a private key, include the encrypted private key.

Figure 12-60 Administration | Certificate Management | Re-submit | Status screen



Status

- Installed = The CA returned the certificate and it has been added to the certificate store.
- Rejected = The CA refused to issue a certificate.
- Polling = The CA has pended the approval request; or, CA is unavailable.
- Error = There has been an error processing the enrollment request.

Go to Certificate Management

If you want to view the certificate request, click **Go to Certificate Management**. The Manager displays the Administration | Certificate Management screen.

Go to Certificate Enrollment

If you want to enroll another certificate, click **Go to Certificate Enrollment**. The Manager displays the Administration | Certificate Management | Enroll screen. (See [Figure 12-41](#).)

Go to Certificate Installation

If you want to install the certificate you have just enrolled, click **Go to Certificate Installation**. The Manager displays the Administration | Certificate Management | Install screen. (See [Figure 12-47](#).)

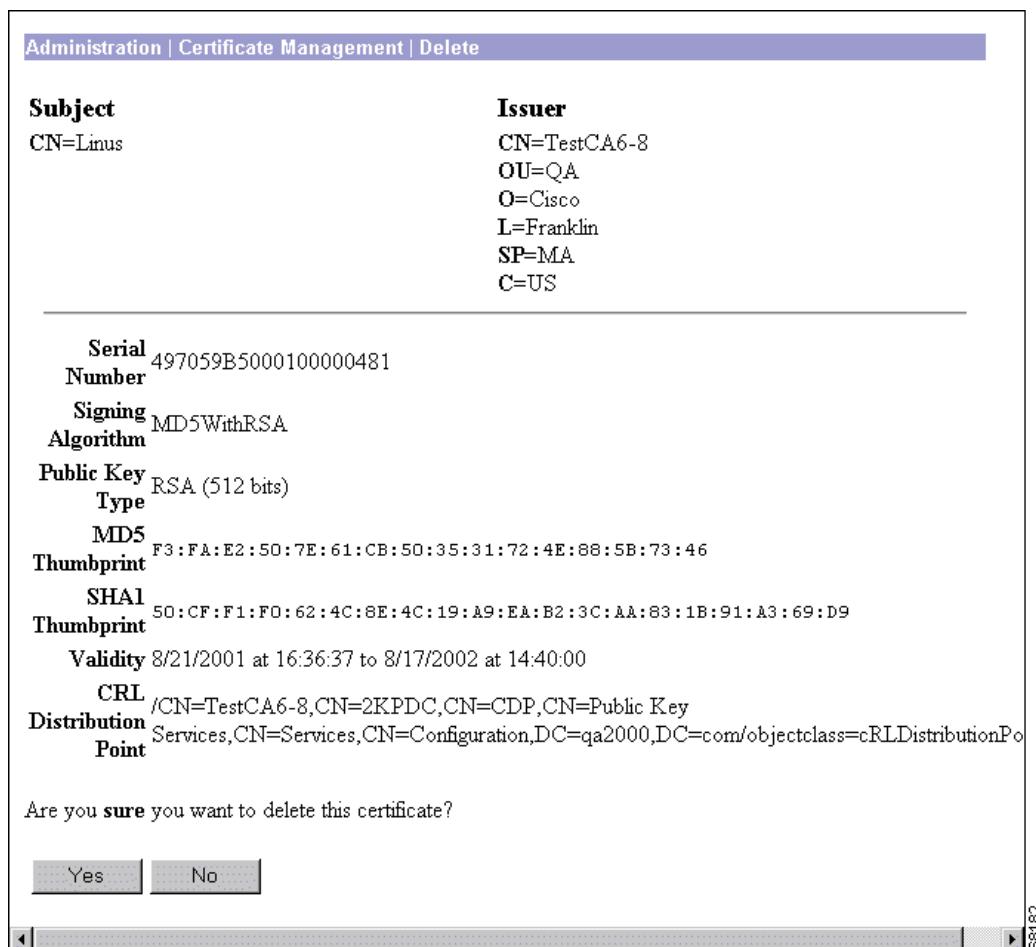
Administration | Certificate Management | Delete

The Manager displays this confirmation screen when you click **Delete** for a certificate on the Administration | Certificate Management screen. The screen shows the same certificate details as on the Administration | Certificate Management | View screen.

Please note:

- You must delete CA certificates from the bottom up: server identity first, then subordinate CA, then root CA certificates last. Otherwise, the Manager displays an error message.
- If the certificate is in use by an SA or referenced in an active enrollment request, the Manager displays an error message.

Figure 12-61 Administration | Certificate Management | Delete Screen



Fields

For a description of the fields in this certificate, see the “[Certificate Fields](#)” section.

Yes / No

To delete this certificate, click **Yes**.



Note

There is no undo.

The Manager returns to the Administration | Certificate Management screen and shows the remaining certificates.

To retain this certificate, click **No**. The Manager returns to the Administration | Certificate Management screen, and the certificates are unchanged.

Administration | Certificate Management | Generate SSL Certificate

Figure 12-62 Administration | Certificate Management | Generate SSL Certificate Screen

Administration | Certificate Management | Generate SSL Certificate

You are about to generate a certificate for the Private Interface . The certificate will have the following DN for both Subject and Issuer.

CN=10.86.194.173
 OU=VPN 3000 Concentrator
 O=Cisco Systems, Inc.
 L=Franklin
 SP=Massachusetts
 C=US

The certificate will be valid for 3 years from yesterday.

Choose the RSA Keysize. 1024-bits

Generate Cancel

104799

Choose the RSA Keysize

Choose the RSA key size according what your CA supports and the level of security you desire. The choices are: 2048-bits, 1024-bits, 768-bits, and 512-bits. The larger the key size, the more secure it is.

Generate/Cancel

Click Generate to generate a new SSL certificate for this interface.

Click Cancel to cancel the operation and return to the Administration | Certificate Management screen.

Administration | Certificate Management | Export SSL Certificate

This screen allows you to copy an SSL certificate from this interface to another or from this VPN 3002 to another.

Figure 12-63 Administration | Certificate Management | Export SSL Certificate Screen

Administration | Certificate Management | Export SSL Certificate

You are about to export the certificate for the Private Interface. Please enter a password that is used to encrypt the private key. Click export to open the certificate in a new window.

Enter Password

Verify Password

104797

Enter Password

Enter a password for encrypting the private key.

Verify Password

Retype the password to verify it.

Export/Cancel

Click **Cancel** to cancel the operation and return to the Administration | Certificate Management screen. Click **Export** to view the certificate. A new browser window appears, displaying the certificate. (See [Figure 12-64](#).)

Figure 12-64 Sample SSL Certificate Export

```

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICoDAaBgkqhkiG9w0BBQMwDQIQ1OnVf7287gCAQUEggKAHVEKFG2x0/FqM1BO
ccn9TAcVRVPjReYmB/5IIXU/ITeOWznRDxb1ODrGZPnsOemRFgrvNrVxAPcORY/v
SdIgfsnJXEBOS8Uuj0aSTozSTNfZurFQ+NLrBH8ZhNS/gUy2etKQZ5b/fIXJjN+
cGfGRjQWn02qZ6UgfjzAYMdvh8BIQL370S02y57VXEGVxf0iFGg6e8zQydzmVlaL
41pj+kULApRdZ6qic/MZnwAS8DAfotEJqLsIEtSDk637vm5Hk40NRW2DuuUApBPG
ytWdltMoRLH8DxU1TFi+OLz9tfSs1bGT+1ZovV8ZxG89b7TYcbXo7ZoC4Cbhd1tP
GCv+LLtPA8btZT13v3p/mUqOobA3wcGagR7qjoqSBMrB6AoRWb028aQh8vEImN8x
pnj7Zo5ubkvuXcZ5+5YRdc+AdrziPrUN8cXziXdx77xsIkxgh+53adbaGjQj06qB
5SgrfJH8eWnkP7zENseyy9XbQS2h8d2peUzJ022LZQAbnjamUYkR10aP80Aowe8BT
Q4C814QrvL26cK1heZvhUBcJ1WFyLWLeTpY9juagZ9OudAtpkA7kj5HAc1PeX2Qy
ateMz/eVf1ukGgyJuigRPq/zPpo8MjZh5o15WHAhOn9fk+cIwiKRD61QHaKQQuzh
LkupIRs/xrC1b/P/OXuxowYmp/aCfuoSUqUhu9NJicOLEzE60TGMvQ+0w7MP1/vh
XH1sP/fqBkogMRVigkrTKODjSsQtvoc4nG/b58TqNH7oSyk17rS4E3AnAphPN/TM
Usq6tLmn2fMjM3Exc4BN04RI7iK6LVpg6t/1/nBw8oe37gK4LYBkp/AR3CXaETi3
m1S8ew==
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICijCCAfMCD/9ko4wDQYJKoZIhvcNAQEEBQAwYsxCzAJBgNVBAYTA1VTMRYw
FAYDVQQIEW1NYXNzYWNoeXN1dHRzMREwDwYDVQQHEWhGcmFua2xpbjEcmBoGA1UE
ChQ2Q21zY28gU31zdGVtcywgSW5jLjEeMBwGA1UECxQVV1BOIDMwMDAgQ29uY2Vu
dHJhdG9yMRMwEQYDVQQDFAo5MC4xNDguMS41MB4XDTA0MDEwODE3MjUzNFoXDTE3
MDEwNzE3MjUzNFoYsxCzAJBgNVBAYTA1VTMRYwFAYDVQQIEW1NYXNzYWNoeXN1
dHRzMREwDwYDVQQHEWhGcmFua2xpbjEcmBoGA1UEChQ2Q21zY28gU31zdGVtcywg
SW5jLjEeMBwGA1UECxQVV1BOIDMwMDAgQ29uY2VuZDhJhdG9yMRMwEQYDVQQDFAo5
MC4xNDguMS41MIGfMAOGCSqGSIb3DQEBAQUAA4GNADCB1QKgQCui5oG3C1/8/P1
1PNTkM5SV1zXdXNDEn/LPFYm2nr0r1Jy2R9oTTYn2qs81DXtScXRQSNRbNur+5Q
C8YCPINzMcvAHEkwZ87mG7xOB1BEa93w0AL7Nt3PcdtbAzaHOF1bTO11pDC6eE5o
3+sgVJ1eaVuAGDYegPFWhhdaOzOrKwIDAQABMAOGCSqGSIb3DQEBAUAA4GBADUg
08RqCDBDA8gNueON0Sp3tmFVnxY2c8zbpJdgrSz/O+Jy54Tc5fU/xEib8MIO7j
zgprruv/wcUPNi+jMU5f8oIbiWKJcR6eK23O/S+u8fcQnKZ031YNQXS/YEZF3mE
GjW5nYPELB7XShKijmIWzD1+cuNwe38mF6X1aVYT
-----END CERTIFICATE-----

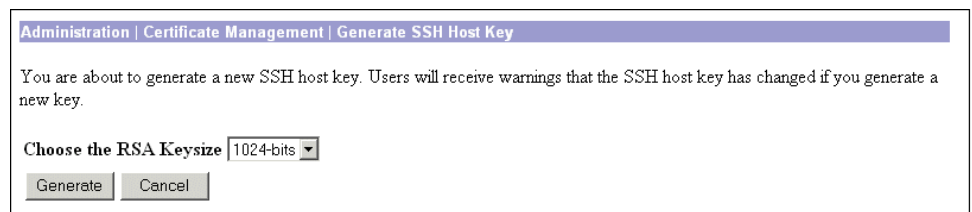
```

You can now copy the certificate text, or save it to a file; then, install the certificate on the appropriate interface or VPN 3002.

Administration | Certificate Management | Generate SSH Host Key

This screen allows you to generate a new SSH Host key. In order to access the VPN 3002 via SSH, the VPN 3002 must have a host key. Only one key is required. The VPN 3002 generates a host key automatically during reboot or upgrade, by taking the public/private key pair from the SSL certificate. If you want a stronger key, or if the original key has been in any way compromised, use this screen to generate a new one.

Figure 12-65 Administration | Certificate Management | Generate SSH Host Key Screen



Choose the RSA Keysize

Choose the RSA key size according what your CA supports and the level of security you desire. The choices are: 2048-bits, 1024-bits, 768-bits, and 512-bits. The larger the key size, the more secure it is.

Generate/Cancel

Click **Generate** to create a new SSH Host key.

Click **Cancel** to cancel the operation and return to the Administration | Certificate Management screen

Administration | Certificate Management | View Enrollment Request

This screen allows you to view the details of an enrollment request.

Figure 12-66 Administration | Certificate Management | View Enrollment Request Screen

Subject	Issuer
CN=Snoopy OU=Eng O=Cisco L=Franklin SP=Ma C=US	N/A

Public Key Type RSA (512 bits)
Request Usage Identity
MD5 Thumbprint 20:32:24:A3:46:D2:CE:1C:E9:C1:27:32:9B:AB:50:06
Generated 08/21/2001 17:25:56
Enrollment Type Initial
Enrollment Method Manual/OOB
Enrollment Status In Progress

Back

Enrollment Request Fields

An enrollment request contains some or all of the following fields:

Field	Content
Subject	The person or system that uses the certificate.
Issuer	The CA or other entity (jurisdiction) from whom the certificate is being requested. Subject and Issuer consist of a specific-to-general identification hierarchy: CN, OU, O, L, SP, and C. These labels and acronyms conform to X.520 terminology, and they echo the fields on the Administration Certificate Management Enrollment screen.

Field	Content
CN	<p>Common Name: the name of a person, system, or other entity. This is the lowest (most specific) level in the identification hierarchy.</p> <p>For the VPN 3002 self-signed SSL certificate, the CN is the IP address on the Ethernet 1 (Private) interface at the time the certificate is generated. SSL compares this CN with the address you use to connect to the VPN 3002 via HTTPS, as part of its validation.</p>
OU	Organizational Unit: the subgroup within the organization (O).
O	Organization: the name of the company, institution, agency, association, or other entity.
L	Locality: the city or town where the organization is located.
SP	State/Province: the state or province where the organization is located.
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Public Key Type	The algorithm and size of the public key that the CA or other issuer used in generating this certificate.
Request Usage	The type of certificate: Identity or SSL.
MD5 Thumbprint	A 128-bit MD5 hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.
SHA1 Thumbprint	A 160-bit SHA-1 hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.
Generated	The date the request was initiated.
Enrollment Type	The type of enrollment: initial, re-enroll, or re-key.
Enrollment Method	The method of enrollment: SCEP or manual.
Enrollment Status	The current status of the enrollment: complete, rejected, error, and so on.

Back

Click **Back** to display the Administration | Certificate Management screen.

Administration | Certificate Management | Cancel Enrollment Request

This screen shows you the details of the enrollment request and allows you to cancel it.

You can cancel only a SCEP enrollment request, and you can do so only when the request is in polling mode. Once a request is cancelled, you can then remove it, re-submit it, or view its details.

Figure 12-67 Administration | Certificate Management | Cancel Enrollment Request Screen

Administration | Certificate Management | Cancel Enrollment Request

Subject	Issuer
CN=Linda 3	CN=RSAv57RootMD5srvCN
OU=	
O=	
L=	
SP=	
C=	

Public Key Type RSA (512 bits)

Request Usage Identity

MD5 Thumbprint A9:92:F9:6F:EB:23:CF:F2:9D:5B:54:7B:79:27:18:74

Generated 09/07/2001 11:44:00

Enrollment Type Initial

Enrollment Method SCEP

Enrollment Status Polling: 1 attempts

Are you **sure** you want to cancel this enrollment request?

36198

Fields

For a description of the fields in this enrollment request, see the “[Enrollment Request Fields](#)” section.

Yes / No

To cancel this enrollment request, click **Yes**.



Note

There is no undo.

The Manager returns to the Administration | Certificate Management screen.

To retain this enrollment request, click **No**. The Manager returns to the Administration | Certificate Management screen, and the enrollment requests are unchanged.

Administration | Certificate Management | Delete Enrollment Request

This screen shows you details of the enrollment request and allows you to delete it. Deleting an enrollment request removes it from the Enrollment Request table (on the Administration | Certificate Management page) and destroys all record of it.

Figure 12-68 Administration | Certificate Management | Delete Enrollment Request

Administration | Certificate Management | Delete Enrollment Request

Subject	Issuer
CN=Snoopy	N/A
OU=Eng	
O=Cisco	
L=Franklin	
SP=Ma	
C=US	

Public Key Type RSA (512 bits)
Request Usage Identity
MD5 Thumbprint 20:32:24:A3:46:D2:CE:1C:E9:C1:27:32:9B:AB:50:06
Generated 08/21/2001 17:25:56

Enrollment Type Initial
Enrollment Method Manual/OOB
Enrollment Status In Progress

Are you **sure** you want to delete this enrollment request?

Fields

For a description of the fields in this enrollment request, see the [“Enrollment Request Fields”](#) section.

Yes / No

To delete this enrollment request, click **Yes**.



Note

There is no undo.

The Manager returns to the Administration | Certificate Management screen and shows the remaining enrollment requests.

To retain this enrollment request, click **No**. The Manager returns to the Administration | Certificate Management screen, and the enrollment requests are unchanged.



Monitoring

Monitoring

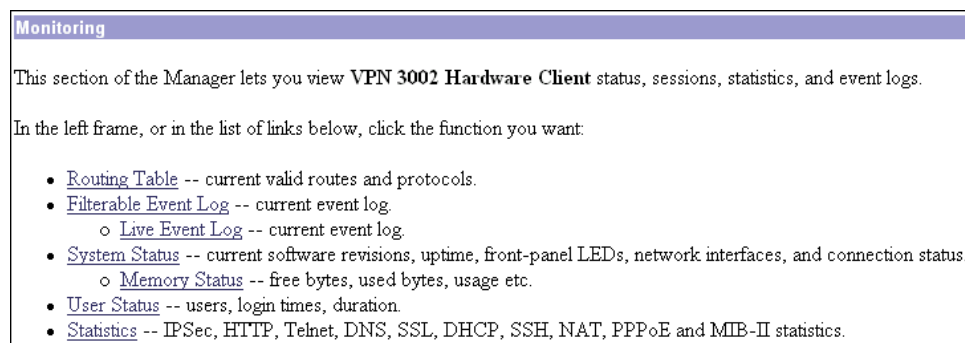
The VPN 3002 tracks many statistics and the status of many items essential to system administration and management. This section of the Manager lets you view all those status items and statistics. You can even see the state of LEDs that show the status of hardware subsystems in the device. You can also see statistics that are stored and available in standard MIB-II data objects.

This section of the Manager lets you view VPN 3002 status, sessions, statistics, and event logs.

- **Routing Table:** current valid routes, protocols, and metrics.
- **Filterable Event Log:** current event log in memory, filterable by event class, severity, IP address, etc.
 - **Live Event Log:** current event log, continuously updated.
- **System Status:** current software revisions, uptime, network interfaces, and connection status.
 - **Memory Status:** Current status of the VPN 3002 memory use, measured in block size, free blocks and used blocks.
- **User Status:** current users, login times, uptime
- **General Statistics:** IPSec, HTTP, Telnet, DNS, SSL, DHCP, SSH, PPPoE, NAT, and MIB-II statistics for interfaces, TCP/UDP, IP, ICMP, the ARP table, Ethernet traffic, and SNMP.

These Manager screens are read-only “snapshots” of data or status at the time the screen displays. Most screens have a Refresh button that you can click to get a fresh snapshot and update the screen, but you cannot modify the data on the screen.

Figure 13-1 Monitoring Screen



Monitoring | Routing Table

This screen shows the VPN 3002 routing table at the time the screen displays.

Figure 13-2 Monitoring | Routing Table Screen

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
0.0.0.0	0.0.0.0	130.0.0.1	Public Interface	Default	0	1
130.0.0.0	255.255.0.0	0.0.0.0	Public Interface	Local	0	1
192.168.10.0	255.255.255.0	0.0.0.0	Private Interface	Local	0	1

Refresh	To update the screen and its data, click Refresh . The date and time indicate when the screen was last updated.
Valid Routes	The total number of current valid routes that the VPN 3002 knows about. This number includes <i>all</i> valid routes, and it might be greater than the number of rows in the routing table, which shows only the best routes with duplicates removed.
Address	The packet destination IP address that this route applies to. This address is combined with the subnet mask to determine the destination route. 0.0.0.0 indicates the default gateway.
Mask	The subnet mask for the destination IP address in the Address field. 0.0.0.0 indicates the default gateway.
Next Hop	For remote routes, the IP address of the next system in the path to the destination. 0.0.0.0 indicates a local route; that is, there is no next hop.
Interface	The VPN 3002 network interface through which traffic moves on this route: <ul style="list-style-type: none"> • Private interface • Public interface
Protocol	The protocol or source of this routing table entry: <ul style="list-style-type: none"> • Static = configured static route. • Local = local VPN 3002 interface address. • ICMP = learned from an ICMP (Internet Control Message Protocol) redirect message. • Default = the default gateway.
Age	The number of seconds since this route was last updated or otherwise validated. The age is relative to the screen display time; for example, 25 means the route was last validated 25 seconds before the screen was displayed. 0 indicates a static, local, or default route.
Metric	The metric, or cost, of this route. 1 is lowest, 16 is highest.

Monitoring | Filterable Event Log

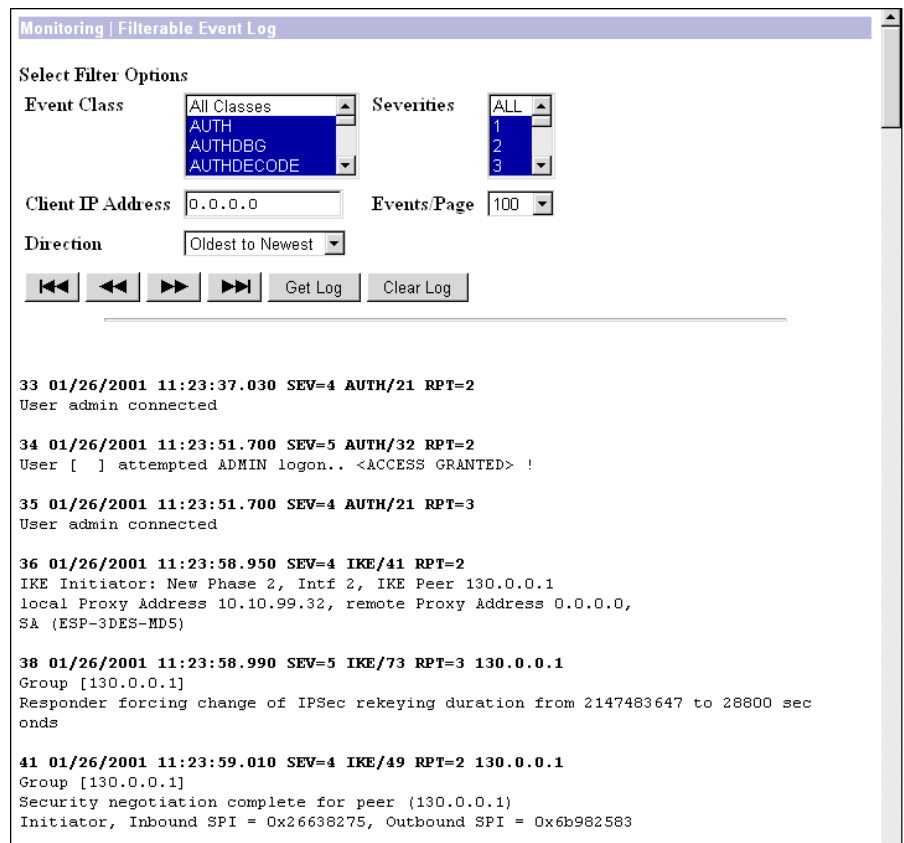
This screen shows the events in the current event log, lets you filter and display events by various criteria, and lets you manage the event log file. For troubleshooting any system difficulty, or just to examine details of system activity, consult the event log first.

The VPN 3002 records events in nonvolatile memory, thus the event log persists even if the system is powered off. It holds 256 events, and it wraps when it is full (that is, entry 257 overwrites entry 1, etc.). Use the scroll controls (if present) to display more events in the log.

To configure event handling, see the Configuration | System | Events screens.

To Get, Save, or Clear the event log file, you must have Access Rights to Read/Write Files. See the Administration | Administrators | Modify Properties screen.

Figure 13-3 Monitoring | Filterable Event Log Screen







61672

Select Filter Options

You can select any or all of the following options for filtering and displaying the event log. After selecting the option(s), click any one of the four Page buttons. The Manager refreshes the screen and displays the event log according to your selections.

Your filter options remain in effect as long as you continue working within and viewing Monitoring | Filterable Event Log screens. The Manager resets all options to their defaults if you leave and return, or if you click Filterable Event Log in the left frame of the Manager window (the table of contents). You cannot save filter options.

Event Class	To display all the events in a single event class, click the drop-down menu button and select the event class. To select a contiguous range of event classes, select the first class in the range, hold down the keyboard Shift key, and select the last class in the range. To select multiple event classes, select the first class, hold down the keyboard Ctrl key, and select the other classes. By default, the Manager displays All Classes of events. Table 9-3 under Configuration System Events describes the event classes.
Severities	To display all events of a single severity level, click the drop-down menu button and select the severity level. To select a contiguous range of severity levels, select the first severity level in the range, hold down the keyboard Shift key, and select the last severity level in the range. To select multiple severity levels, select the first severity level, hold down the keyboard Ctrl key, and select the other severity levels. By default, the Manager displays All severity levels. See Table 9-3 under Configuration System Events for an explanation of severity levels.
Client IP Address	To display all events relating to a single IP address, enter the IP address in the field using dotted decimal notation; for example, 10.10.1.35. By default, the Manager displays all IP addresses. To restore the default, enter 0.0.0.0.
Events/Page	To display a given number of events per Manager screen (page), click the drop-down menu button and select the number. Choices are 10 , 25 , 50 , 100 , 250 , and ALL . By default, the Manager displays 100 events per screen.
Direction	To display events in a different chronological order, click the drop-down menu button and select the order. Choices are: <ul style="list-style-type: none"> • Oldest to Newest = Display events in actual chronological order, with oldest events at the top of the screen. This is the default selection. • Newest to Oldest = Display events in reverse chronological order, with newest events at the top of the screen.
First Page 	To display the first page (screen) of the event log, click this button. By default, the Manager displays the first page of the event log when you first open this screen.
Previous Page 	To display the previous page (screen) of the event log, click this button.
Next Page 	To display the next page (screen) of the event log, click this button.
Last Page 	To display the last page (screen) of the event log, click this button.

All four Page buttons are also present at the bottom of the screen.

Get Log

To download the event log from VPN 3002 memory to your PC and view it or save it as a text file, click **Get Log**. The Manager opens a new browser window to display the file. The browser address bar shows the VPN 3002 address and log file default filename; for example,

```
http://10.10.4.6/LOG/vpn3002log.txt.
```

To save a copy of the log file on your PC, click the **File** menu on the *new* browser window and select **Save As...** The browser opens a dialog box that lets you save the file. The default filename is `vpn3002log.txt`.

Alternatively, you can use the *secondary* mouse button to click **Get Log** on this Monitoring | Filterable Event Log screen. A pop-up menu presents choices whose exact wording depends on your browser, but among them are:

- **Open Link, Open Link in New Window, Open in New Window** = Open and view the file in a new browser window, as above.
- **Save Target As..., Save Link As...** = Save a copy of the log file on your PC. Your system will prompt for a filename and location. The default filename is `vpn3002log.txt`.

When you are finished viewing or saving the file, close the new browser window.

Clear Log

To clear the current event log from memory, click this button. The Manager then refreshes the screen and shows the empty log.

**Caution**

The Manager immediately erases the event log from memory without asking for confirmation. *There is no undo.*

Event Log Format

Each entry (record) in the event log consists of eight or nine fields:

```
Sequence Date Time Severity Class/Number Repeat (IPAddress)
String
```

(The IPAddress field only appears in certain events.)

For example:

```
3 12/06/2001 14:37:06.680 SEV=4 HTTP/47 RPT=17 10.10.1.35
New administrator login: admin.
```

Event Sequence

The sequential number of the logged entry. Numbering starts or restarts from 1 when the system powers up, when you save the event log, or when you clear the event log. When the log file wraps after 256 entries, numbering continues with event 257 overwriting event 1.

Although numbering restarts at 1 when the system powers up, it does *not* overwrite existing entries in the event log; it appends them. Assuming the log does not wrap, it could contain several sequences of events starting at 1. Thus you can examine events preceding and following reboot or reset cycles.

Event Date

The date of the event: MM/DD/YYYY. For example, 12/06/2001 identifies an event that occurred on December 6, 2001.

Event Time	The time of the event: hour:minute:second.millisecond. The hour is based on a 24-hour clock. For example, 14:37:06.680 identifies an event that occurred at 2:37:06.680 PM.
Event Severity	The severity level of the event; for example: SEV=4 identifies an event of severity level 4. See Table 9-3 under Configuration System Events for an explanation of severity levels.
Event Class/Number	The class—or source—of the event, and the internal reference number associated with the specific event within the event class. For example: HTTP/47 indicates that an administrator logged in to the VPN 3002 using HTTP to connect to the Manager. Table 9-3 under Configuration System Events describes the event classes. The internal reference number assists Cisco support personnel if they need to examine a log file.
Event Repeat	The number of times that this specific event has occurred since the VPN 3002 was last booted or reset. For example, RPT=17 indicates that this is the seventeenth occurrence of this specific event.
Event IP address	The IP address of the client or host associated with this event. Only certain events have this field. For tunnel-related events, this is typically the “outer” or tunnel endpoint address. In the Event log format example above, 10.10.1.35 is the IP address of the host PC from which admin logged in using the Manager.
Event String	The string, or message, that describes the specific event. Each event class comprises many possible events, and the string gives a brief description. Event strings usually do not exceed 80 characters. In the Event log format example above, “New administrator login: admin” describes the event.

Monitoring | Live Event Log

This screen shows events in the current event log and automatically updates the display every 5 seconds. The events might take a few seconds to load when you first open the screen.

Note for Netscape users:

The live event log requires Netscape version 4.5 or higher. It does not run on other versions of Netscape.

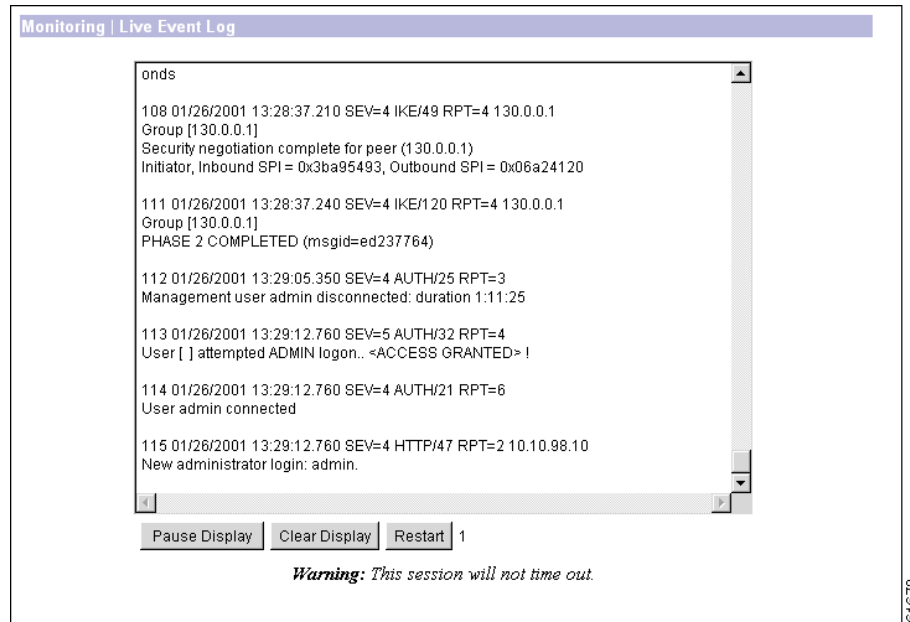
The screen always displays the most recent event at the bottom. Use the scroll bar to view earlier events. To filter and display events by various criteria, see the [Monitoring | Filterable Event Log](#) section above.



Note

If you keep this Manager screen open, your administrative session does not time out. Each automatic screen update resets the inactivity timer. See Session Idle Timeout on the Administration | Access Rights | Access Settings screen.

Figure 13-4 Monitoring | Live Event Log Screen



Pause Display/Resume Display

To pause the display, click **Pause Display**. While paused, the screen does not display new events, the button changes to Resume Display, and the timer counts down to 0 and stops. You can still scroll through the event log. Click the button to resume the display of new events and restart the timer.

Clear Display

To clear the event display, click **Clear Display**. This action does *not* clear the event log, only the display of events on this screen.

Restart

To clear the event display and reload the entire event log in the display, click **Restart**.

Timer

The timer counts 5 – 4 – 3 – 2 – 1 to show where it is in the 5-second refresh cycle. A momentary Rx indicates receipt of new events. A steady 0 indicates the display has been paused.

Monitoring | System Status

This screen shows the status of several software and hardware variables at the time the screen displays. From this screen you can also display the status of the IPsec tunnel SAs, tunnel duration, plus front and rear panel displays of the VPN 3002.

Figure 13-5 Monitoring | System Status Screen



Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

VPN Client Type

The type, or model number, of this VPN 3002 hardware client.

Bootcode Rev

The version name, number, and date of the VPN 3002 bootcode software file. When you boot or reset the system, the bootcode software runs system diagnostics, and it loads and executes the system software image. The bootcode is installed at the factory, and there is no need to upgrade it. If an engineering change requires a bootcode upgrade, only Cisco support personnel can do so.

Software Rev

The version name, number, and date of the VPN 3002 Hardware Client system software image file. You can update this image file from the Administration | Software Update screen.

Up Since

The date and time that the VPN 3002 was last booted or reset.

RAM Size

The total amount of SDRAM memory installed in the VPN 3002. *Memory Status* is a link to a table that displays information about memory use on the VPN 3002; it includes information about block size, with data about used and free blocks, bytes, and percentages.

Disconnect Now

Disconnects the tunnel.

Connect Now

Connects the tunnel.

Assigned IP Address

The IP address assigned to the VPN 3002 by the central-site VPN Concentrator when PAT mode is enabled. This field is not displayed when the VPN 3002 is running in Network Extension mode, because the central-site VPN Concentrator does not assign an IP address to the VPN 3002 in Network Extension mode.

Tunnel Established to

The IP address of the VPN Concentrator to which this VPN 3002 connects.

Duration

The length of time that this tunnel has been up.

Tunnel Type

The type of tunnel and port. Possible types are IPSec, IPSec over TCP, IPSec over UDP, or IPSec over NAT-T.

Security Associations

This table describes the following attributes of the SAs for this VPN 3002.

Type

The type of tunnel for this SA, either IPSec or IKE (the control tunnel).

Remote Address

Network/subnet mask for this split-tunneled SA.

Encryption

The encryption method this SA uses.

Authentication

The authentication method this SA uses.

Octets In

The number of octets (bytes) this SA has received since the tunnel has been up.

Octets Out

The number of octets (bytes) this SA has sent since the tunnel has been up.

Packets In

The number of packets this SA has received since the tunnel has been up.

Packets Out

The number of packets this SA has sent since the tunnel has been up.

Other

Additional information about this SA, including mode.

Front Panel

The front panel image is an inactive link.

Back Panel

The back panel image includes active links for the VPN 3002 private and public interfaces. Use the mouse pointer to select either the private or public module on the back-panel image and click anywhere in the highlighted area. The Manager displays the appropriate Monitoring | System Status | Interface screen.

Monitoring | System Status | Memory Status

This screen displays status and data for the VPN 3002 system memory.

Figure 13-6 Monitoring | System Status | Memory Status Screen

Monitoring | System Status | Memory Status Thursday, 30 January 2003 11:58:40 Refresh

System Memory Summary

Total Memory	Memory Status	Total Block Usage
16 MB	Green	38%

Memory resources are sufficient for normal operation.

Block Usage List

Block Size (Bytes)	Used		Free		Usage
	Blocks	Bytes	Blocks	Bytes	
64	1122	71808	3878	248192	22%
128	69	8832	2431	311168	2%
256	51	13056	949	242944	5%
512	42	21504	1458	746496	2%
1024	38	38912	462	473088	7%
2048	17	34816	233	477184	6%
4096	11	45056	39	159744	22%
8192	6	49152	23	188416	20%
> 8192	27	2152436	0	1089536	66%
Total	1383	2435572	9473	3936768	38%

[Detailed Memory Report](#)

The remaining system memory is used for the executable image and is not included in this table.

87384

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

System Memory Summary

This section summarizes memory use on the VPN 3002.

Total Memory

Total amount of system memory, in megabytes, on the VPN 3002.

Memory Status

Green: sufficient memory resources are available for normal VPN 3002 operations.

Yellow: Memory resources are running low; approaching maximum number of connections.

Red: Memory resources are critically low; new IPsec connections are prevented.

**Note**

It is possible for Memory Status to be Red, preventing new connections, even while total memory usage is significantly less than 100%. This is because some VPN 3002 functions and features require specific block sizes to operate, and those block sizes are critically low. If this occurs, follow the instructions in the section, “[Memory Detail Report](#)” that follows.

Total Block Usage

Memory use in total percent of blocks currently in use.

Block Usage List

Provides a list of blocks by size and number, both used and free.

Block Size (Bytes)

The number of blocks by size of block in bytes.

Used/Free Blocks

The number of used blocks and free blocks.

Used/Free Bytes

The number of used bytes and free bytes.

Usage

The percentage of blocks in use.

Memory Detail Report

Click this button to generate a text file that displays details of memory usage in a new window.

Memory Detail Report

This screen displays a text file that summarizes memory use on the VPN 3002. You can view, copy, save, or delete "Memory.txt." If necessary, you can send this file to the Cisco TAC by email to help with trouble-shooting.

Monitoring | System Status | Private/Public Interface

This screen displays status and statistics for a VPN 3002 Ethernet interface. To configure an interface, see Configuration | Interfaces.

Figure 13-7 Monitoring | System Status | Public Interface Screen

Interface	Public Interface
IP Address	130.0.0.2
Status	UP
Rx Unicast	3031
Tx Unicast	3397
Rx Multicast	0
Tx Multicast	0
Rx Broadcast	0
Tx Broadcast	8

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Back

To return to the Monitoring | System Status screen, click **Back**.

Interface

The VPN 3002 Ethernet interface number:

- Private interface
- Public interface

IP Address

The IP address configured on this interface.

Status

The operational status of this interface:

- UP (UP/DHCP, UP/PPPoE) = configured and enabled, ready to pass data traffic.
- Waiting for DHCP/PPPoE = configured and enabled, waiting for negotiations to complete.
- Disabled = configured but disabled.
- DOWN (DOWN/DHCP, DOWN/PPPoE) = configured but
- Testing = in test mode; no regular data traffic can pass.
- Dormant = configured and enabled but waiting for an external action, such as an incoming connection.
- Not Present = missing hardware components.
- Lower Layer Down = not operational because a lower-layer interface is down.
- Unknown = not configured.

Rx Unicast

The number of unicast packets that were received by this interface since the VPN 3002 was last booted or reset. Unicast packets are those addressed to a single host.

Tx Unicast

The number of unicast packets that were routed to this interface for transmission since the VPN 3002 was last booted or reset, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Rx Multicast

The number of multicast packets that were received by this interface since the VPN 3002 was last booted or reset. Multicast packets are those addressed to a specific group of hosts.

Tx Multicast

The number of multicast packets that were routed to this interface for transmission since the VPN 3002 was last booted or reset, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Rx Broadcast

The number of broadcast packets that were received by this interface since the VPN 3002 was last booted or reset. Broadcast packets are those addressed to all hosts on a network.

Tx Broadcast

The number of broadcast packets that were routed to this interface for transmission since the VPN 3002 was last booted or reset, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

Monitoring | User Status

This section displays statistics for devices behind the VPN 3002 Hardware Client.

Figure 13-8 Monitoring | User Status screen

Username	IP Address	MAC Address	Login Time	Duration (hh:mm:ss)	Actions
3002user	10.10.98.10	00.01.02.3A.95.2D	Oct 11 16:40:44	1:24:00	[Logout]

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Cisco IP Phone Bypass Enabled/Disabled

Indicates whether the Cisco IP Phone Bypass feature is enabled or disabled for the VPN 3002. This feature is enabled or disabled for the group on the VPN Concentrator to which the VPN 3002 belongs. For more information, see Configuration | User Management | Base Group/Groups, Hardware Client tab for the VPN Concentrator.

Username

The username for the session.

IP Address

The IP address of the device logged in behind the VPN 3002.

MAC Address

The MAC address for the device logged in behind the VPN 3002.

Login Time

The date and time of day when the user logged in to the VPN 3002.

Duration

The length of time that the user has been logged in; the format is hh:mm:ss.

Actions

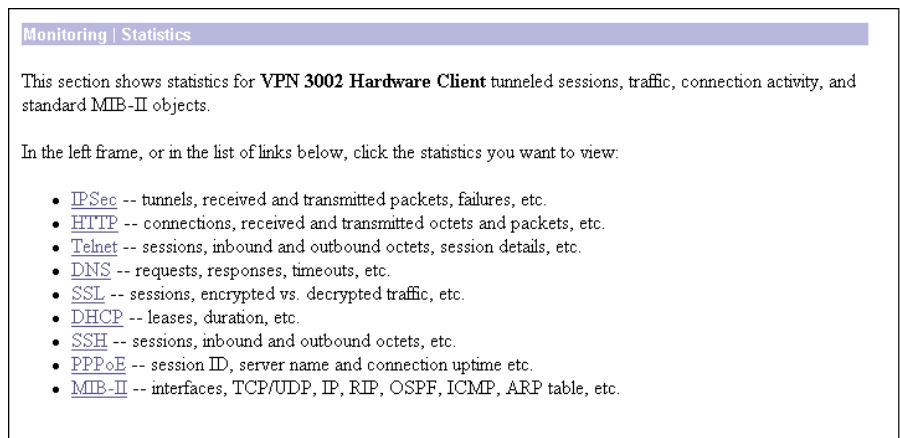
Possible actions: Ping and Logout.

Monitoring | Statistics

This section of the Manager shows statistics for traffic and activity on the VPN 3002 since it was last booted or reset, and for current tunneled sessions, plus statistics in standard MIB-II objects for interfaces, TCP/UDP, IP, ICMP, the ARP table, and SNMP.

- **IPSec:** total Phase 1 and Phase 2 tunnels, received and transmitted packets, failures, drops, etc.
- **HTTP:** total data traffic and connection statistics.
- **Telnet:** total sessions, and current session inbound and outbound traffic.
- **DNS:** total requests, responses, timeouts, etc.
- **SSL:** total sessions, encrypted vs. unencrypted traffic, etc.
- **DHCP:** leased addresses, duration, etc.
- **SSH:** total and active sessions, bytes and packets sent and received, etc.
- **PPPoE:** session ID, server name, duration, etc.
- **NAT:** sessions; inbound and outbound packets; source, destination and translated IP addresses and ports; sessiontype
- **MIB-II Stats:** interfaces, TCP/UDP, IP, ICMP, the ARP table, Ethernet, and SNMP.

Figure 13-9 Monitoring | Statistics Screen



Monitoring | Statistics | IPsec

This screen shows statistics for IPsec activity, including the current IPsec tunnel, on the VPN 3002 since it was last booted or reset. These statistics conform to the IETF draft for the IPsec Flow Monitoring MIB.

Figure 13-10 Monitoring | Statistics | IPsec Screen

IKE (Phase 1) Statistics		IPsec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	1
Total Tunnels	2	Total Tunnels	4
Received Bytes	61358	Received Bytes	6536
Sent Bytes	7980	Sent Bytes	2104
Received Packets	775	Received Packets	44
Sent Packets	83	Sent Packets	13
Received Packets Dropped	1	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notices	755	Sent Packets Dropped	0
Sent Notices	132	Inbound Authentications	44
Received Phase-2 Exchanges	4	Failed Inbound Authentications	0
Sent Phase-2 Exchanges	0	Outbound Authentications	13
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	44
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	13
Phase-2 SA Delete Requests Received	0	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	3	System Capability Failures	0
Initiated Tunnels	0	No-SA Failures	0
Failed Initiated Tunnels	0	Protocol Use Failures	0
Failed Remote Tunnels	0		
Authentication Failures	0		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
No-SA Failures	0		

68295

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

IKE (Phase 1) Statistics

This table provides IPSec Phase 1 (IKE: Internet Key Exchange) global statistics. During IPSec Phase 1 (IKE), the two peers establish control tunnels through which they negotiate Security Associations.

Active Tunnels

The number of currently active IKE control tunnels.

Total Tunnels

The cumulative total of all currently and previously active IKE control tunnels.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IKE tunnels.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IKE tunnels.

Received Packets

The cumulative total of packets received by all currently and previously active IKE tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IKE tunnels.

Received Packets Dropped

The cumulative total of packets that were dropped during receive processing by all currently and previously active IKE tunnels. If there is a problem with the content of a packet, such as hash failure, parsing error, or encryption failure, received in Phase 1 or the negotiation of Phase 2, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Sent Packets Dropped

The cumulative total of packets that were dropped during send processing by all currently and previously active IKE tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Received Notifies

The cumulative total of notify packets received by all currently and previously active IKE tunnels. A notify packet is an informational packet that is sent in response to a bad packet or to indicate status; for example, error packets, keepalive packets, etc.

Sent Notifies

The cumulative total of notify packets sent by all currently and previously active IKE tunnels. See comments for Received Notifies above.

Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges received by all currently and previously active IKE tunnels; that is, the total of Phase-2 negotiations received that were initiated by a remote peer. A complete exchange consists of three packets.

Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were sent by all currently and previously active and IKE tunnels; that is, the total of Phase-2 negotiations initiated by this VPN 3002.

Invalid Phase-2 Exchanges Received

The cumulative total of IPSec Phase-2 exchanges that were received, found to be invalid because of protocol errors, and dropped, by all currently and previously active IKE tunnels. In other words, the total of Phase-2 negotiations that were initiated by a remote peer but that this VPN 3002 dropped because of protocol errors.

Invalid Phase-2 Exchanges Sent

The cumulative total of IPSec Phase-2 exchanges that were sent and were found to be invalid, by all currently and previously active IKE tunnels.

Rejected Received Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by a remote peer, received, and rejected by all currently and previously active IKE tunnels. Rejected exchanges indicate policy-related failures, such as configuration problems.

Rejected Sent Phase-2 Exchanges

The cumulative total of IPSec Phase-2 exchanges that were initiated by this VPN 3002, sent, and rejected, by all currently and previously active IKE tunnels. See comment above.

Phase-2 SA Delete Requests Received

The cumulative total of requests to delete IPSec Phase-2 Security Associations received by all currently and previously active IKE tunnels.

Phase-2 SA Delete Requests Sent

The cumulative total of requests to delete IPSec Phase-2 Security Associations sent by all currently and previously active IKE tunnels.

Initiated Tunnels

The cumulative total of IKE tunnels that this VPN 3002 initiated.

Failed Initiated Tunnels

The cumulative total of IKE tunnels that this VPN 3002 initiated and that failed to activate.

Failed Remote Tunnels

The cumulative total of IKE tunnels that remote peers initiated and that failed to activate.

Authentication Failures

The cumulative total of authentication attempts that failed, by all currently and previously active IKE tunnels. Authentication failures indicate problems with preshared keys, digital certificates, or user-level authentication.

Decryption Failures

The cumulative total of decryptions that failed, by all currently and previously active IKE tunnels.

Hash Validation Failures

The cumulative total of hash validations that failed, by all currently and previously active IKE tunnels. Hash validation failures usually indicate misconfiguration or mismatched preshared keys or digital certificates.

System Capability Failures

The cumulative total of system capacity failures that occurred during processing of all currently and previously active IKE tunnels. These failures indicate that the system has run out of memory, or that the tunnel count exceeds the system maximum.

No-SA Failures

The cumulative total of nonexistent-Security Association failures that occurred during processing of all currently and previously active IKE tunnels. These failures occur when the system receives a packet for which it has no Security Association, and might indicate synchronization problems.

IPSec (Phase 2) Statistics

This table provides IPSec Phase 2 global statistics. During IPSec Phase 2, the two peers negotiate Security Associations that govern traffic within the tunnel.

Active Tunnels

The number of currently active IPSec Phase-2 tunnels.

Total Tunnels

The cumulative total of all currently and previously active IPSec Phase-2 tunnels.

Received Bytes

The cumulative total of bytes (octets) received by all currently and previously active IPSec Phase-2 tunnels, before decompression. In other words, total bytes of IPSec-only data received by the IPSec subsystem, before decompressing the IPSec payload.

Sent Bytes

The cumulative total of bytes (octets) sent by all currently and previously active IPSec Phase-2 tunnels, after compression. In other words, total bytes of IPSec-only data sent by the IPSec subsystem, after compressing the IPSec payload.

Received Packets

The cumulative total of packets received by all currently and previously active IPSec Phase-2 tunnels.

Sent Packets

The cumulative total of packets sent by all currently and previously active IPSec Phase-2 tunnels.

Received Packets Dropped

The cumulative total of packets dropped during receive processing by all currently and previously active IPSec Phase-2 tunnels, excluding packets dropped due to anti-replay processing. If there is a problem with the content of a packet, the system drops the packet. This number should be zero or very small; if not, check for misconfiguration.

Received Packets Dropped (Anti-Replay)

The cumulative total of packets dropped during receive processing due to anti-replay errors, by all currently and previously active IPSec Phase-2 tunnels. If the sequence number of a packet is a duplicate or out of bounds, there might be a faulty network or a security breach, and the system drops the packet.

Sent Packets Dropped

The cumulative total of packets dropped during send processing by all currently and previously active IPSec Phase-2 tunnels. This number should be zero; if not, check for a network problem, check the event log for an internal subsystem failure, or contact Cisco support.

Inbound Authentications

The cumulative total number of inbound individual packet authentications performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Inbound Authentications

The cumulative total of inbound packet authentications that failed, by all currently and previously active IPSec Phase-2 tunnels. Failed authentications could indicate corrupted packets or a potential security attack (“man in the middle”).

Outbound Authentications

The cumulative total of outbound individual packet authentications performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Outbound Authentications

The cumulative total of outbound packet authentications that failed, by all currently and previously active IPSec Phase-2 tunnels. This number should be zero or very small; if not, check the event log for an internal IPSec subsystem problem.

Decryptions

The cumulative total of inbound decryptions performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Decryptions

The cumulative total of inbound decryptions that failed, by all currently and previously active IPSec Phase-2 tunnels. This number should be zero or very small; if not, check for misconfiguration.

Encryptions

The cumulative total of outbound encryptions performed by all currently and previously active IPSec Phase-2 tunnels.

Failed Encryptions

The cumulative total of outbound encryptions that failed, by all currently and previously active IPSec Phase-2 tunnels. This number should be zero or very small; if not, check the event log for an internal IPSec subsystem problem.

System Capacity Failures

The total number of system capacity failures that occurred during processing of all currently and previously active IPSec Phase-2 tunnels. These failures indicate that the system has run out of memory or some other critical resource; check the event log.

No-SA Failures

The cumulative total of nonexistent-Security Association failures which occurred during processing of all currently and previously active IPSec Phase-2 tunnels. These failures occur when the system receives an IPSec packet for which it has no Security Association, and might indicate synchronization problems.

Protocol Use Failures

The cumulative total of protocol use failures that occurred during processing of all currently and previously active IPSec Phase-2 tunnels. These failures indicate errors parsing IPSec packets.

Monitoring | Statistics | HTTP

This screen shows statistics for HTTP activity on the VPN 3002 since it was last booted or reset.

To configure system-wide HTTP server parameters, see the Configuration | System | Management | Protocols | HTTP screen.

Figure 13-11 Monitoring | Statistics | HTTP Screen

			Sent	Received
Octets	1475558	240902		
Packets	1666	502		
			Sockets	Sessions
Active	1	1		
Peak	5	1		
Total	177	7		

HTTP Sessions				Octets		Packets		Sockets		
Login Name	IP Address	Login Time	Encryption	Sent	Received	Sent	Received	Active	Peak	Total
admin	161.44.246.135	Oct 11 17:15:46	None	374135	33033	412	65	1	4	44

Max Connections: 5

902389

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Octets Sent/Received

The total number of HTTP octets (bytes) sent or received since the VPN 3002 was last booted or reset.

Packets Sent/Received

The total number of HTTP packets sent or received since the VPN 3002 was last booted or reset.

Packets Sent Sockets/Sessions

The number of HTTP connections for the VPN 3002.

Active

The number of currently active HTTP connections on the VPN 3002.

Peak

The maximum number of HTTP connections that were simultaneously active on the VPN 3002 since it was last booted or reset.

Total

The total number of HTTP connections on the VPN 3002 since it was last booted or reset.

HTTP Sessions

This section provides information about HTTP sessions on the VPN 3002 since it was last booted or reset.

Login Name

The name of the administrative user for the HTTP session.

IP Address

The IP address of administrative user for the HTTP session.

Login Time

The time when the HTTP session began.

Encryption

The encryption method used in the HTTP session.

Octets Sent/Received

Number of octets sent or received during the HTTP session.

Packets Sent/Received

Number of packets sent or received during the HTTP session.

Sockets Active

The number of currently active sockets for the HTTP session.

Sockets Peak

The maximum number of sockets simultaneously active during the HTTP session.

Sockets Total

The total number of sockets active during the HTTP session.

Max Connections

The maximum number of concurrent HTTP connections for the VPN 3002 since it was last rebooted or reset.

Monitoring | Statistics | Telnet

This screen shows statistics for Telnet activity on the VPN 3002 since it was last booted or reset, and for current Telnet sessions.

To configure the VPN 3002 Telnet server, see the Configuration | System | Management Protocols | Telnet screen.

Figure 13-12 Monitoring | Statistics | Telnet Screen

The screenshot shows a web interface for monitoring Telnet statistics. At the top, it displays the page title 'Monitoring | Statistics | Telnet' and the date/time 'Thursday, 01 November 2001 10:49:00'. There are 'Reset' and 'Refresh' buttons. Below this, three summary statistics are shown: Active Sessions: 1, Attempted Sessions: 1, and Successful Sessions: 1. A table titled 'Telnet Sessions' provides detailed data for a client with IP address 10.10.98.10:4474. The table has columns for Client IP Address:Port, Inbound Octets (Total, Command, Discarded), and Outbound Octets (Total, Dropped).

Client IP Address:Port	Inbound Octets			Outbound Octets	
	Total	Command	Discarded	Total	Dropped
10.10.98.10:4474	100	6	0	3563	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Sessions

The number of active Telnet sessions. The Telnet Sessions table shows statistics for these sessions.

Attempted Sessions

The total number of attempts to establish Telnet sessions on the VPN 3002 since it was last booted or reset.

Successful Sessions

The total number of Telnet sessions successfully established on the VPN 3002 since it was last booted or reset.

Telnet Sessions

This table shows statistics for active Telnet sessions on the VPN 3002. Each active session is a row.

Client IP Address:Port

The IP address and TCP source port number of the remote Telnet client for this session.

Inbound Octets Total

The total number of Telnet octets (bytes) received by this session.

Inbound Octets Command

The number of octets (bytes) containing Telnet commands or options, received by this session.

Inbound Octets Discarded

The number of Telnet octets (bytes) received and dropped during input processing by this session.

Outbound Octets Total

The total number of Telnet octets (bytes) transmitted by this session.

Outbound Octets Dropped

The number of outbound Telnet octets dropped during output processing by this session.

Monitoring | Statistics | DNS

This screen shows statistics for DNS (Domain Name System) activity on the VPN 3002 since it was last booted or reset.

To configure the VPN 3002 to communicate with DNS servers, see the Configuration | System | Servers | DNS screen.

Figure 13-13 Monitoring | Statistics | DNS Screen

The screenshot shows a web interface for monitoring DNS statistics. At the top, there is a navigation bar with 'Monitoring | Statistics | DNS' on the left and 'Thursday, 01 November 2001 11:57:18' on the right. Below the navigation bar, there are two buttons: 'Reset' with a trash icon and 'Refresh' with a circular arrow icon. In the center, there is a table with the following data:

Requests	6
Responses	1
Timeouts	3
Server Unreachable	0
Other Failures	0

On the right side of the screenshot, there is a vertical label '67684'.

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests

The total number of DNS queries the VPN 3002 made since it was last booted or reset. This number equals the sum of the numbers in the Responses, Timeouts, Server Unreachable and Other Failures fields (the four fields that follow).

Responses

The number of DNS queries that were successfully resolved.

Timeouts

The number of DNS queries that failed because there was no response from the server.

Server Unreachable

The number of DNS queries that failed because, according to the VPN 3002 routing table, the address of the server is not reachable.

Other Failures

The number of DNS queries that failed for an unspecified reason.

Monitoring | Statistics | SSL

This screen shows statistics for SSL (Secure Sockets Layer) protocol traffic on the VPN 3002 since it was last booted or reset.

To configure SSL, see Configuration | System | Management Protocols | SSL.

Figure 13-14 Monitoring | Statistics | SSL Screen

	Inbound Octets	Outbound Octets
Unencrypted	35	414
Encrypted	778	1903
Total Sessions	1	
Active Sessions	0	
Max Active Sessions	1	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Unencrypted Inbound Octets

The number of octets (bytes) of inbound traffic output by the decryption engine.

Encrypted Inbound Octets

The number of octets (bytes) of encrypted inbound traffic sent to the decryption engine. This number includes negotiation traffic.

Unencrypted Outbound Octets

The number of unencrypted outbound octets (bytes) sent to the encryption engine.

Encrypted Outbound Octets

The number of octets (bytes) of outbound traffic output by the encryption engine. This number includes negotiation traffic.

Total Sessions

The total number of SSL sessions.

Active Sessions

The number of currently active SSL sessions.

Max Active Sessions

The maximum number of SSL sessions simultaneously active at any one time.

Monitoring | Statistics | DHCP

This screen shows statistics for DHCP (Dynamic Host Configuration Protocol) server activity on the VPN 3002 since it was last booted or reset. Each row of the table shows data for each IP address handed out to a DHCP client (PC) on the VPN 3002 private network.

To configure the DHCP server, see Configuration | System | IP Routing | DHCP.

Figure 13-15 Monitoring | Statistics | DHCP Screen

The screenshot shows a web interface for monitoring DHCP statistics. At the top, it displays 'Monitoring | Statistics | DHCP' and the date/time 'Thursday, 01 November 2001 11:10:14' with a 'Refresh' button. The statistics are as follows:

Active Leases	1
Maximum Active Leases	1
Timeouts	985
Pool Start	Pool End
10.10.99.91	10.10.99.217

Below the statistics is a table of leased IP addresses:

Leased IP Address	Time Left	MAC Address	Host Name
10.10.99.91	1:38:40	00.01.03.CF.9E.79	mkrupp-w2k1

A vertical label '67883' is visible on the right side of the screenshot.

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Active Leases

The number of DHCP leases currently active.

Maximum Active Leases

The maximum number of DHCP leases simultaneously active at any one time.

Timeouts

The number of DHCP queries that failed because there was no response from the server.

Pool Start

The IP address at the start of the DHCP IP address pool.

Pool End

The IP address at the end of the DHCP IP address pool.

Leased IP Address

The IP address leased from the DHCP server by the remote client.

Time Left

The time remaining until the current IP address lease expires, shown as HH:MM:SS.

MAC Address

The hardwired MAC (Medium Access Control) address of the interface, in 6-byte hexadecimal notation, that maps to the IP Address.

Host Name

The name of the DHCP client (PC) on this interface.

Monitoring | Statistics | SSH

This screen shows statistics for SSH (Secure Shell) protocol traffic on the VPN 3002 since it was last booted or reset.

To configure SSH, see Configuration | System | Management Protocols | SSH.

Figure 13-16 Monitoring | Statistics | SSH Screen

The screenshot shows the 'Monitoring | Statistics | SSH' interface. At the top right, it displays the date and time: 'Thursday, 01 November 2001 12:06:39'. Below this are 'Reset' and 'Refresh' buttons. The main content area contains two tables. The first table shows overall statistics for Octets and Packets sent and received, and a sub-table for Sessions (Active, Maximum, Total). The second table, titled 'SSH Sessions', lists individual sessions with columns for Login Name, Remote IP Address:Port, Login Time, Encryption, and Octets/Packets sent and received.

	Sent	Received
Octets	1872	564
Packets	44	13

Sessions	
Active	1
Maximum	1
Total	2

SSH Sessions							
Login Name	Remote IP Address:Port	Login Time	Encryption	Octets		Packets	
				Sent	Received	Sent	Received
admin	83.0.0.4:4309	Nov 01 11:54:39	3DES-168	896	272	20	6

67704

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Octets Sent/Received

The total number of SSH octets (bytes) sent/received since the VPN 3002 was last booted or reset.

Packets Sent/Received

The total number of SSH packets sent/received since the VPN 3002 was last booted or reset.

Active Sessions

The number of currently active SSH sessions.

Maximum Sessions

The maximum number of simultaneously active SSH sessions on the VPN 3002.

Total Sessions

The total number of SSH sessions since the VPN 3002 was last booted or reset.

SSH Sessions

Presents details on SSH sessions.

Login Name

The name of the administrator using the session.

Remote IP Address:Port

The remote IP address for the session.

Login Time

The time of day when the login for the session occurred.

Encryption

The type of encryption algorithm used for the session.

Octets Sent/Received

The number of octets sent and received during the session.

Packets Sent/Received

The number of packets sent and received during the session.

Monitoring | Statistics | NAT

This screen shows statistics for NAT (Network Address Translation) activity on the VPN 3002 since it was last booted or reset.

Figure 13-17 Monitoring | Statistics | NAT screen

The screenshot shows the 'Monitoring | Statistics | NAT' screen. At the top right, it displays the date and time 'Thursday, 11 October 2001 18:05:49' and buttons for 'Reset' and 'Refresh'. The main content area contains two tables. The first table shows summary statistics for NAT activity. The second table, titled 'NAT Sessions', shows a list of active sessions with columns for Source, Destination, Translated, and Translated details.

Packets	
In	16
Out	199
Translations	
Active	1
Peak	6
Total	93

NAT Sessions											
Source		Destination		Translated				Translated			
IP Address	Port	IP Address	Port	IP Address	Port	Direction	Age	Type	Bytes	Packets	
10.10.98.10	137	192.168.255.255	137	192.168.10.1	49233	Outbound	5713	Net BIOS UDP Prozy	1638	21	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Packets In/Out

The total of NAT packets inbound and outbound since the last time the VPN 3002 was rebooted or reset.

Translations Active

The number of currently active NAT sessions.

Translations Peak

The maximum number of NAT sessions that were simultaneously active on the VPN 3002 since it was last booted or reset.

Translations Total

The total number of NAT sessions on the VPN 3002 since it was last booted or reset.

NAT Sessions

The following sections provide detailed information about active NAT sessions on the VPN 3002.

Source IP Address/Port

The source IP address and port for the NAT session.

Destination IP Address/Port

The destination IP address and port for the NAT session.

Translated IP Address/Port

The translated IP address and port for the NAT session. The VPN3002 uses this port number to keep track of which devices initiate data transfer; by keeping this record, the VPN 3002 is able to correctly route responses.

Direction

The direction, inbound or outbound, of the data transferred for the NAT session.

Age

The number of half seconds remaining until the NAT session times out.

Type

The type of packets for the NAT session. The possible types are:

- TCP NAT session
- UDP NAT session
- FTP session
- TFTP session

- NetBIOS over TCP Proxy
- NetBIOS over UDP Proxy
- NetBIOS Datagram Service
- No Port Mapping (ICMP)
- H.323 Proxies
 - RAS (Registration, Admission and Status) Proxy for a GateKeeper
 - ILS Proxy (Internet Locator Services) Proxy for an ILS server
 - H.225 (H.225 signalling protocol) Proxy
 - H.245 (H.245 control protocol) Proxy

Translated Bytes/Packets

The total number of translated bytes and packets for the NAT session.

Monitoring | Statistics | PPPoE

This screen shows statistics for PPPoE (PPP over Ethernet) activity on the VPN 3002 since it was last booted or reset.

Figure 13-18 Monitoring | Statistics | PPPoE Screen

The screenshot shows a web interface for monitoring PPPoE statistics. At the top, it displays 'Monitoring | Statistics | PPPoE' and the date/time 'Thursday, 01 November 2001 16:28:11'. There are 'Reset' and 'Refresh' buttons. The main content is titled 'PPPoE Statistics' and contains two tables. The first table lists active sessions with columns for User Name, Session ID, MAC Address, Server Name, and Duration. The second table shows various error and timeout counts with columns for PADI Timeouts, PADR Timeouts, Multiple PADO Rx, PADT Rx, PADT Tx, Generic Errors Rx, and Malformed Packets Rx.

PPPoE Statistics						
		PPPoE Access Concentrator				
User Name	Session ID	MAC Address	Server Name	Duration		
test2	2	00.02.4A.5A.C0.70	7200_Mercury	0:26:55		

PADI Timeouts	PADR Timeouts	Multiple PADO Rx	PADT Rx	PADT Tx	Generic Errors Rx	Malformed Packets Rx
1	0	0	1	0	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

User Name

The username for the PPPoE session.

Session ID

The ID for the session assigned by the ISP. The Session ID combined with the Access Concentrator MAC Address (see below) uniquely identifies the PPPoE session.

PPPoE Access Concentrator

The device your Internet Service Provider (ISP) uses to manage PPPoE traffic. Fields include Session ID, MAC Address, and Server Name. These fields have entries only if a PPPoE session is established.

MAC Address

The MAC (Medium Access Control) address of the PPPoE Access Concentrator, in 6-byte hexadecimal notations.

Server Name

The name of the server for the PPPoE Access Concentrator.

Duration

The amount of time that this PPPoE session has been up, in the format hh:mm:ss.

PADI Timeouts

The number of PPPoE Active Discovery Initiation packets for which the VPN 3002 received no response.

PADR Timeouts

The number of PPPoE Active Discovery Request packets for which the VPN 3002 received no response.

Multiple PADO Rx

The number of multiple PPPoE Active Discovery Offer packets received, that is, the number of times more than one PPPoE access concentrator responded to the PADI the VPN 3002 sent.

PADT Rx

The number of PPPoE Active Discovery Terminate packets received.

PADT Tx

The number of PPPoE Active Discovery Terminate packets sent.

Generic Errors Rx

The number of errors received during the PPPoE session.

Malformed Packets Rx

The number of malformed packets received during the PPPoE session.

Monitoring | Statistics | MIB-II

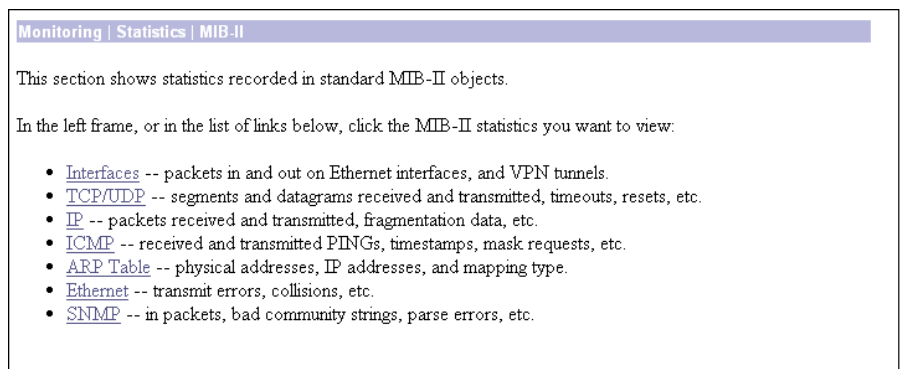
This section of the Manager lets you view statistics that are recorded in standard MIB-II objects on the VPN 3002. MIB-II (Management Information Base, version 2) objects are variables that contain data about the system. They are defined as part of the Simple Network Management Protocol (SNMP); and SNMP-based network management systems can query the VPN 3002 to gather the data.

Each subsequent screen displays the data for a standard MIB-II group of objects:

- **Interfaces:** packets sent and received on network interfaces and VPN tunnels.
- **TCP/UDP:** Transmission Control Protocol and User Datagram Protocol segments and datagrams sent and received, etc.
- **IP:** Internet Protocol packets sent and received, fragmentation and reassembly data, etc.
- **ICMP:** Internet Control Message Protocol ping, timestamp, and address mask requests and replies, etc.
- **ARP Table:** Address Resolution Protocol physical (MAC) addresses, IP addresses, and mapping types.
- **Ethernet:** errors and collisions, MAC errors, etc.
- **SNMP:** Simple Network Management Protocol requests, bad community strings, parsing errors, etc.

To configure and enable the VPN 3002 SNMP server, see the Configuration | System | Management Protocols | SNMP screen.

Figure 13-19 Monitoring | Statistics | MIB-II Screen



Monitoring | Statistics | MIB-II | Interfaces

This screen shows statistics in MIB-II objects for VPN 3002 interfaces since the system was last booted or reset.

Figure 13-20 Monitoring | Statistics | MIB-II | Interfaces Screen

		Unicast		Multicast		Broadcast	
Interface	Status	In	Out	In	Out	In	Out
Private Interface	UP	1060	1071	101899	0	89086	139
Public Interface	UP/DHCP	147	2173	114224	0	175082	11

68311

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN 3002 interface:

- Private
- Public

Status

The operational status of this interface:

- UP (UP/DHCP, UP/PPPoE)= configured and enabled, ready to pass data traffic.
- Waiting for DHCP/PPPoE = configured and enabled, ready to pass data traffic.

- Disabled = configured by disabled.
- DOWN(DOWN/DHCP, DOWN/PPPoE) = configured but down.
- Testing = in test mode; no regular data traffic can pass.
- Dormant = configured and enabled but waiting for an external action, such as an incoming connection.
- Not Present = missing hardware components.
- Lower Layer Down = not operational because a lower-layer interface is down.
- Unknown = not configured.

Unicast In

The number of unicast packets that were received by this interface. Unicast packets are those addressed to a single host.

Unicast Out

The number of unicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Unicast packets are those addressed to a single host.

Multicast In

The number of multicast packets that were received by this interface. Multicast packets are those addressed to a specific group of hosts.

Multicast Out

The number of multicast packets that were routed to this interface for transmission, including those that were discarded or not sent. Multicast packets are those addressed to a specific group of hosts.

Broadcast In

The number of broadcast packets that were received by this interface. Broadcast packets are those addressed to all hosts on a network.

Broadcast Out

The number of broadcast packets that were routed to this interface for transmission, including those that were discarded or not sent. Broadcast packets are those addressed to all hosts on a network.

Monitoring | Statistics | MIB-II | TCP/UDP

This screen shows statistics in MIB-II objects for TCP and UDP traffic on the VPN 3002 since it was last booted or reset. RFC 2012 defines TCP MIB objects, and RFC 2013 defines UDP MIB objects.

Figure 13-21 Monitoring | Statistics | MIB-II | TCP/UDP Screen

TCP			UDP	
Segments Received	2061		Datagrams Received	846
Segments Transmitted	1921		Datagrams Transmitted	94
Segments Retransmitted	0		Errored Datagrams	0
Timeout Min	1000	msec	No Port	0
Timeout Max	32000	msec		
Connection Limit	-1			
Active Opens	0			
Passive Opens	194			
Attempt Failures	0			
Established Resets	2			
Current Established	1			

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

TCP Segments Received

The total number of segments received, including those received in error and those received on currently established connections. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Transmitted

The total number of segments sent, including those on currently established connections but excluding those containing only retransmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Segments Retransmitted

The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted bytes. Segment is the official TCP name for what is casually called a data packet.

TCP Timeout Min

The minimum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Timeout Max

The maximum value permitted for TCP retransmission timeout, measured in milliseconds.

TCP Connection Limit

The limit on the total number of TCP connections that the system can support. A value of -1 means there is no limit.

TCP Active Opens

The number of TCP connections that went directly from an unconnected state to a connection-synchronizing state, bypassing the listening state. These connections are allowed, but they are usually in the minority.

TCP Passive Opens

The number of TCP connections that went from a listening state to a connection-synchronizing state. These connections are usually in the majority.

TCP Attempt Failures

The number of TCP connection attempts that failed. Technically this is the number of TCP connections that went to an unconnected state, plus the number that went to a listening state, from a connection-synchronizing state.

TCP Established Resets

The number of established TCP connections that abruptly closed, bypassing graceful termination.

TCP Current Established

The number of TCP connections that are currently established or are gracefully terminating.

UDP Datagrams Received

The total number of UDP datagrams received. Datagram is the official UDP name for what is casually called a data packet.

UDP Datagrams Transmitted

The total number of UDP datagrams sent. Datagram is the official UDP name for what is casually called a data packet.

UDP Errored Datagrams

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port (UDP No Port). Datagram is the official UDP name for what is casually called a data packet.

UDP No Port

The total number of received UDP datagrams that could not be delivered because there was no application at the destination port. Datagram is the official UDP name for what is casually called a data packet.

Monitoring | Statistics | MIB-II | IP

This screen shows statistics in MIB-II objects for IP traffic on the VPN 3002 since it was last booted or reset. RFC 2011 defines IP MIB objects.

Figure 13-22 Monitoring | Statistics | MIB-II | IP Screen

Monitoring Statistics MIB-II IP		Thursday, 11 October 2001 17:45:12
Packets Received (Total)	3396	Reset Refresh
Packets Received (Header Errors)	0	
Packets Received (Address Errors)	0	
Packets Received (Unknown Protocols)	0	
Packets Received (Discarded)	0	
Packets Received (Delivered)	2931	
Packets Forwarded	2	
Outbound Packets Discarded	0	
Outbound Packets with No Route	2	
Packets Transmitted (Requests)	2026	
Fragments Needing Reassembly	0	
Reassembly Successes	0	
Reassembly Failures	0	
Fragmentation Successes	0	
Fragmentation Failures	0	
Fragments Created	0	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Packets Received (Total)

The total number of IP data packets received by the VPN 3002, including those received with errors.

Packets Received (Header Errors)

The number of IP data packets received and discarded due to errors in IP headers, including bad checksums, version number mismatches, other format errors, etc.

Packets Received (Address Errors)

The number of IP data packets received and discarded because the IP address in the destination field was not a valid address for the VPN 3002. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (such as Class E).

Packets Received (Unknown Protocols)

The number of IP data packets received and discarded because of an unknown or unsupported protocol.

Packets Received (Discarded)

The number of IP data packets received that had no problems preventing continued processing, but that were discarded (for example, for lack of buffer space). This number does not include any packets discarded while awaiting reassembly.

Packets Received (Delivered)

The number of IP data packets received and successfully delivered to IP user protocols (including ICMP) on the VPN 3002; that is, the VPN 3002 was the final destination.

Packets Forwarded

The number of IP data packets received and forwarded to destinations other than the VPN 3002.

Outbound Packets Discarded

The number of outbound IP data packets that had no problems preventing their transmission to a destination, but that were discarded (for example, for lack of buffer space).

Outbound Packets with No Route

The number of outbound IP data packets discarded because no route could be found to transmit them to their destination. This number includes any packets that the VPN 3002 could not route because all of its default routers were down.

Packets Transmitted (Requests)

The number of IP data packets that local IP user protocols (including ICMP) supplied to transmission requests. This number does not include any packets counted in Packets Forwarded.

Fragments Needing Reassembly

The number of IP fragments received by the VPN 3002 that needed to be reassembled.

Reassembly Successes

The number of IP data packets successfully reassembled.

Reassembly Failures

The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). This number is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.

Fragmentation Successes

The number of IP data packets that have been successfully fragmented by the VPN 3002.

Fragmentation Failures

The number of IP data packets that have been discarded because they needed to be fragmented but could not be (because the Don't Fragment flag was set).

Fragments Created

The number of IP data packet fragments that have been generated by the VPN 3002.

Monitoring | Statistics | MIB-II | ICMP

This screen shows statistics in MIB-II objects for ICMP traffic on the VPN 3002 since it was last booted or reset. RFC 2011 defines ICMP MIB objects.

Figure 13-23 Monitoring | Statistics | MIB-II | ICMP screen

	Received	Transmitted
Total	804	14319
Errors	0	0
Destination Unreachable	64	96
Time Exceeded	0	11404
Parameter Problems	0	0
Source Quench	0	0
Redirects	0	2079
Echo Requests (PINGs)	10	730
Echo Replies (PINGs)	730	10
Timestamp Requests	0	0
Timestamp Replies	0	0
Address Mask Requests	0	0
Address Mask Replies	0	0

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Total Received/Transmitted

The total number of ICMP messages that the VPN 3002 received/sent. This number includes messages counted as Errors Received/Transmitted. ICMP messages solicit and provide information about the network environment.

Errors Received/Transmitted

The number of ICMP messages that the VPN 3002 received but determined to have ICMP-specific errors (bad ICMP checksums, bad length, etc.).

The number of ICMP messages that the VPN 3002 did not send due to problems within ICMP such as a lack of buffers.

Destination Unreachable Received/Transmitted

The number of ICMP Destination Unreachable messages received/sent. Destination Unreachable messages apply to many network situations, including inability to determine a route, an unusable source route specified, and the Don't Fragment flag set for a packet that must be fragmented.

Time Exceeded Received/Transmitted

The number of ICMP Time Exceeded messages received/sent. Time Exceeded messages indicate that the lifetime of the packet has expired, or that a router cannot reassemble a packet within a time limit.

Parameter Problems Received/Transmitted

The number of ICMP Parameter Problem messages received/sent. Parameter Problem messages indicate a syntactic or semantic error in an IP header.

Source Quench Received/Transmitted

The number of ICMP Source Quench messages received/sent. Source Quench messages provide rudimentary flow control; they request a reduction in the rate of sending traffic on the network.

Redirects Received/Transmitted

The number of ICMP Redirect messages received/sent. Redirect messages advise that there is a better route to a particular destination.

Echo Requests (PINGs) Received/Transmitted

The number of ICMP Echo (request) messages received/sent. Echo messages are probably the most visible ICMP messages. They test the communication path between network entities by asking for Echo Reply response messages.

Echo Replies (PINGs) Received/Transmitted

The number of ICMP Echo Reply messages received/sent. Echo Reply messages are sent in response to Echo messages, to test the communication path between network entities.

Timestamp Requests Received/Transmitted

The number of ICMP Timestamp (request) messages received/sent. Timestamp messages measure the propagation delay between network entities by including the originating time in the message, and asking for the receipt time in a Timestamp Reply message.

Timestamp Replies Received/Transmitted

The number of ICMP Timestamp Reply messages received/sent. Timestamp Reply messages are sent in response to Timestamp messages, to measure propagation delay in the network.

Address Mask Requests Received/Transmitted

The number of ICMP Address Mask Request messages received/sent. Address Mask Request messages ask for the address (subnet) mask for the LAN to which a router connects.

Address Mask Replies Received/Transmitted

The number of ICMP Address Mask Reply messages received/sent. Address Mask Reply messages respond to Address Mask Request messages by supplying the address (subnet) mask for the LAN to which a router connects.

Monitoring | Statistics | MIB-II | ARP Table

This screen shows entries in the Address Resolution Protocol mapping table since the VPN 3002 was last booted or reset. ARP matches IP addresses with physical MAC addresses, so the system can forward traffic to computers on its network. RFC 2011 defines MIB entries in the ARP table.

The entries are sorted first by Interface, then by IP Address. To speed display, the Manager might construct multiple 64-row tables. Use the scroll controls (if present) to view the entire series of tables.

You can also delete dynamic, or learned, entries in the mapping table.

Figure 13-24 Monitoring | Statistics | MIB-II | ARP Table Screen

Interface	Physical Address	IP Address	Mapping Type	Action
1	FF.FF.FF.FF.FF.FF	192.168.0.0	Static	
1	00.90.A4.00.00.A2	192.168.10.1	Static	
1	00.90.A4.00.00.A2	192.168.10.100	Static	
1	FF.FF.FF.FF.FF.FF	192.168.255.255	Static	
2	00.10.5A.12.EF.78	10.10.23.2	Dynamic	[Delete]
2	FF.FF.FF.FF.FF.FF	161.44.246.0	Static	
2	00.D0.BC.F3.ED.A8	161.44.246.2	Dynamic	[Delete]
2	00.D0.D3.35.21.A4	161.44.246.3	Dynamic	[Delete]
2	00.D0.00.AF.FB.FF	161.44.246.4	Dynamic	[Delete]
2	00.01.02.5F.9C.9F	161.44.246.6	Dynamic	[Delete]
2	00.A0.C9.E5.84.0E	161.44.246.7	Dynamic	[Delete]
2	00.90.27.B1.07.36	161.44.246.8	Dynamic	[Delete]
2	00.50.DA.D7.2E.0B	161.44.246.9	Dynamic	[Delete]
2	00.01.E6.00.88.48	161.44.246.10	Dynamic	[Delete]
2	00.60.B0.9C.12.44	161.44.246.11	Dynamic	[Delete]
2	00.90.A4.00.0E.7C	161.44.246.20	Dynamic	[Delete]
2	00.40.96.37.C9.8A	161.44.246.45	Dynamic	[Delete]
2	08.00.20.F8.CE.22	161.44.246.46	Dynamic	[Delete]
2	00.01.03.22.15.0C	161.44.246.47	Dynamic	[Delete]
2	08.00.20.C1.D8.28	161.44.246.51	Dynamic	[Delete]
2	08.00.20.FD.67.4C	161.44.246.54	Dynamic	[Delete]
2	00.40.96.38.F3.20	161.44.246.55	Dynamic	[Delete]
2	00.B0.D0.68.9D.3E	161.44.246.56	Dynamic	[Delete]
2	00.50.04.D4.64.EF	161.44.246.57	Dynamic	[Delete]
2	00.01.02.3A.C4.2D	161.44.246.65	Dynamic	[Delete]
2	00.40.96.48.55.3F	161.44.246.66	Dynamic	[Delete]
2	00.50.DA.E7.C2.70	161.44.246.67	Dynamic	[Delete]

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The VPN 3002 network interface on which this mapping applies:

- Private Interface
- Public Interface

Physical Address

The hardwired MAC (Media Access Control) address of a physical network interface card, in 6-byte hexadecimal notation, that maps to the IP Address. Exceptions are:

- 00 = a virtual address for a tunnel.
- FF.FF.FF.FF.FF.FF = a network broadcast address.

IP Address

The IP address that maps to the Physical Address.

Mapping Type

The type of mapping:

- Other = none of the following.
- Invalid = an invalid mapping.
- Dynamic = a learned mapping.
- Static = a static mapping on the VPN 3002.

Action/Delete

To remove a dynamic, or learned, mapping from the table, click **Delete**. *There is no confirmation or undo.* The Manager deletes the entry and refreshes the screen.

To delete an entry, you must have the administrator privilege to Modify Config under General Access Rights. See Administration | Access Rights | Administrators.

You cannot delete static mappings.

Monitoring | Statistics | MIB-II | Ethernet

This screen shows statistics in MIB-II objects for Ethernet interface traffic on the VPN 3002 since it was last booted or reset. IEEE standard 802.3 describes Ethernet networks, and RFC 1650 defines Ethernet interface MIB objects.

To configure Ethernet interfaces, see Configuration | Interfaces.

Figure 13-25 Monitoring | Statistics | MIB-II | Ethernet Screen

Monitoring Statistics MIB-II Ethernet														Monday, 05 November 2001 14:21:21	
														Reset Refresh	
Interface	Errors					Deferred Transmits	Collisions				MAC Errors		Speed (Mbps)	Duplex	
	Alignment	FCS	Carrier Sense	SQE Test	Frame Too Long		Single	Multiple	Late	Excessive	Transmit	Receive			
Ethernet 1 (Private)	1	1	0	0	0	0	0	1	1	125	0	0	100	Half	
Ethernet 2 (Public)	0	0	0	0	0	0	0	0	0	0	0	0	100	Half	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Interface

The private or public interface to which the data in this row applies.

Alignment Errors

The number of frames received on this interface that are not an integral number of bytes in length and do not pass the FCS (Frame Check Sequence; used for error detection) check.

FCS Errors

The number of frames received on this interface that are an integral number of bytes in length but do not pass the FCS (Frame Check Sequence) check.

Carrier Sense Errors

The number of times that the carrier sense signal was lost or missing when trying to transmit a frame on this interface.

SQE Test Errors

The number of times that the SQE (Signal Quality Error) Test Error message was generated for this interface. The SQE message tests the collision circuits on an interface.

Frame Too Long Errors

The number of frames received on this interface that exceed the maximum permitted frame size.

Deferred Transmits

The number of frames for which the first transmission attempt on this interface is delayed because the medium is busy. This number does not include frames involved in collisions.

Single Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by exactly one collision. This number is not included in the Multiple Collisions number.

Multiple Collisions

The number of successfully transmitted frames on this interface for which transmission is inhibited by more than one collision. This number does not include the Single Collisions number.

Late Collisions

The number of times that a collision is detected on this interface later than 512 bit-times into the transmission of a packet. 512 bit-times = 51.2 microseconds on a 10-Mbps system.

Excessive Collisions

The number of frames for which transmission on this interface failed due to excessive collisions.

MAC Errors: Transmit

The number of frames for which transmission on this interface failed due to an internal MAC sublayer transmit error. This number does not include Carrier Sense Errors, Late Collisions, or Excessive Collisions.

MAC Errors: Receive

The number of frames for which reception on this interface failed due to an internal MAC sublayer receive error. This number does not include Alignment Errors, FCS Errors, or Frame Too Long Errors.

Speed (Mbps)

The nominal bandwidth of the interface in megabits per second.

Duplex

The current LAN duplex transmission mode for this interface:

- Full = Full-Duplex: transmission in both directions at the same time.
- Half = Half-Duplex: transmission in only one direction at a time.

Monitoring | Statistics | MIB-II | SNMP

This screen shows statistics in MIB-II objects for SNMP traffic on the VPN 3002 since it was last booted or reset. RFC 1907 defines SNMP version 2 MIB objects.

To configure the VPN 3002 SNMP server, see [Configuration | System | Management Protocols | SNMP](#).

Figure 13-26 Monitoring | Statistics | MIB-II | SNMP Screen

Monitoring Statistics MIB-II SNMP		Thursday, 01 November 2001 12:07:39
Requests Received	10	Reset Refresh
Bad Version	0	
Bad Community String	0	
Pasing Errors	0	
Silent Drops	0	
Proxy Drops	0	

Reset

To reset, or start anew, the screen contents, click **Reset**. The system temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle's trip odometer, versus the regular odometer.

Restore

To restore the screen contents to their actual statistical values, click **Restore**. This icon displays only if you previously clicked the Reset icon.

Refresh

To update the screen and its data, click **Refresh**. The date and time indicate when the screen was last updated.

Requests Received

The total number of SNMP messages received by the VPN 3002.

Bad Version

The total number of SNMP messages received that were for an unsupported SNMP version. The VPN 3002 supports SNMP version 2.

Bad Community String

The total number of SNMP messages received that used an SNMP community string the VPN 3002 did not recognize. See [Configuration | System | Management Protocols | SNMP Communities](#) to configure permitted community strings. To protect security, the VPN 3002 *does not* include the usual default public community string.

Parsing Errors

The total number of syntax or transmission errors encountered by the VPN 3002 when decoding received SNMP messages.

Silent Drops

The total number of SNMP request messages that were silently dropped because the reply exceeded the maximum allowable message size.

Proxy Drops

The total number of SNMP request messages that were silently dropped because the transmission of the reply message to a proxy target failed for some reason (other than a timeout).



Using the Command-Line Interface

The VPN 3002 Hardware Client command-line interface (CLI) is a menu- and command-line-based configuration, administration, and monitoring system built into the VPN 3002. You use it via the system console or a Telnet or SSH session.

You can use the command-line interface to completely manage the system. You can access and configure the same parameters as the HTML-based VPN 3002 Hardware Client Manager.

This chapter describes general features of the command-line interface and how to access and use it. It *does not* describe the individual menu items and parameter entries. For information on specific parameters and options, see the corresponding section of the Manager in this manual. For example, to understand Ethernet interface configuration parameters and choices, see Configuration | Interfaces | Private/Public in [Chapter 2, “Interfaces”](#).

Accessing the Command-line Interface

You can access the command-line interface via the system console or via a Telnet or SSH client.

Console Access

To use the console:

1. Connect a PC to the VPN 3002 via an RJ-45 serial cable (which Cisco supplies with the system) between the console port on the VPN 3002 and the COM1 or serial port on the PC. For more information, see the *VPN 3002 Hardware Client Getting Started* guide.
2. Start a terminal emulator (e.g., HyperTerminal) on the PC. Configure a connection to COM1 with port settings of:

9600 bits per second.

8 data bits.

No parity.

1 stop bit.

Set the emulator for VT100 emulation, or let it auto-detect the emulation type.

3. Press **Enter** on the PC keyboard until you see the login prompt. (You might see a password prompt and error messages as you press Enter; ignore them and stop at the login prompt.)

Login: _

Telnet or SSH Access

To access the command-line interface via a Telnet or SSH client:

1. Enable the Telnet or SSH server on the VPN 3002. (They are both enabled by default on the private network.) See the Configuration | System | Management Protocols | Telnet screen on the Manager.
2. Start the Telnet or SSH client, and connect to the VPN 3002 using these parameters:
 - Host Name or Session Name** = The IP address on the VPN 3002 private interface; e.g., 10.10.147.2
 - Port** = Telnet (default Telnet port is 23, SSH port is 22)
 - Terminal Type** = VT100 or ANSI
3. The VPN 3002 displays a login prompt.

Login: _

Starting the Command-line Interface

You start the command-line interface by logging in.

Login usernames and passwords for both console and Telnet access are the same as those configured and enabled for administrators. See the Administration | Access Rights | Administrators screen. By default, only `admin` is enabled.

This example uses the factory-supplied default admin login and password. If you have changed them, use your entries.

At the prompts, enter the administrator login name and password. Entries are case-sensitive.

Login: admin

Password: admin (The CLI does not show your entry.)

The CLI displays the opening welcome message, the main menu, and the `Main ->` prompt.

```

                Welcome to
                Cisco Systems
                VPN 3002 Hardware Client
                Command Line Interface
    Copyright (C) 1998-2001 Cisco Systems, Inc.
```

- ```

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

Main -> \_

# Using the Command-line Interface

This section explains how to:

- Choose menu items.
- Enter values for parameters and options.
- Specify configured items by number or name.
- Navigate quickly, using shortcuts, through the menus.
- Display a brief help message.
- Save entries to the system configuration file.
- Stop the command-line interface.
- Understand administrator access rights.

The command-line interface displays menus or prompts at every level to guide you in choosing configurable options and setting parameters. The prompt always shows the menu context.

## Choosing Menu Items

To use the command-line interface, enter a number at the prompt that corresponds to the desired menu item, and press **Enter**.

For example, this is the Configuration > System > General > System Identification menu:

```
1) Set System Name
2) Set Contact
3) Set Location
4) Back
```

```
General -> _
```

Enter 1 to set the system name.

## Entering Values

The command-line interface shows any current or default value for a parameter in brackets [ ]. To change the value, enter a new value at the prompt. To leave the value unchanged, just press **Enter**.

Continuing the example above, this is the prompt to enter a value for the system name:

```
> Host Name
```

```
General -> [Lab VPN] _
```

You can enter a new name at the prompt, or just press **Enter** to keep the current name.

## Navigating Quickly

There are two ways to move quickly through the command-line interface: shortcut numbers, and the Back/Home options. Both ways work only when you are at a menu, not when you are at a value entry.

### Using Shortcut Numbers

When you become familiar with the structure of the interface, which parallels the HTML-based VPN 3002 Hardware Client Manager, you can quickly access any level by entering a series of numbers separated by periods. For example, suppose you want to change the Access Rights for Administrators. The series of menus that gets to that level from the main menu is:

```
Main -> _
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

```
Main -> 2 (Administration)
```

```
1) Software Update
2) System Reboot
3) Ping
4) Traceroute
5) Access Rights
6) File Management
7) Certificate Management
8) Back
```

```
Config -> 5 (Access Rights)
```

```
1) Administrators
2) Access Settings
3) Back
```

```
Admin -> 1
```

```
Administrative Users

Username Enabled

admin Yes
config No
isp No

```

```
1) Modify Administrator
2) Back
```

```
Admin -> 1
> Which Administrator to Modify
```

```
Admin ->
```



As a shortcut, you can just enter 2.5.1.1 at the Main-> prompt, and move directly to the Modify Administrators menu:

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

```
Main -> 2.5.1.1
```

```
> Which Administrator to Modify
```

```
Admin ->
```



#### Note

At this last prompt, you cannot use a number shortcut. At this prompt, you must type in the name of the administrator you want to modify, for example, `config`.

```
Admin -> config
```

The prompt always shows the current context in the menu structure.

## Using Back and Home

Most menus include a numbered Back choice. Instead of entering a number, you can just enter `b` or `B` to move back to the previous menu.

Also, at any menu level, you can just enter `h` or `H` to move home to the main menu.

## Getting Help Information

To display a brief help message, enter `5` at the main menu prompt. The command-line interface explains how to navigate through menus and enter values. This help message is available only at the main menu.

```
Cisco Systems. Help information for the Command Line Interface
```

```
From any menu except the Main menu.
-- 'B' or 'b' for Back to previous menu.
-- 'H' or 'h' for Home back to the main menu.
```

```
For Data entry
-- Current values are in '[']'s. Just hit 'Enter' to accept value.
```

```
1) View Help Again
2) Back
```

```
Help -> _
```

To return to the main menu from this help menu, enter `h` or `H` (for home), or `2` or `b` or `B` (for back) at the prompt.

## Saving the Configuration File

Configuration and administration entries take effect immediately and are included in the active, or running, configuration. However, if you reboot the VPN 3002 without *saving* the active configuration, you lose any changes.

To save changes to the system configuration (CONFIG) file, navigate to the main menu. At the prompt, enter **4** for **Save changes to Config file**.

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 4

The system writes the active configuration to the CONFIG file and redisplay the main menu.

## Stopping the Command-line Interface

To stop the command-line interface, navigate to the main menu and enter **6** for **Exit** at the prompt:

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 6

Done

Make sure you save any configuration changes before you exit from the CLI.

## Understanding Access Rights

What you see and can configure depends on administrator access rights. If you do not have permission to configure an option, you see **-)**, rather than a number, in menus. For example, here is the main menu for the default Monitor administrator:

- ) Configuration
- ) Administration
- 3) Monitoring
- ) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> \_

The default Monitor administrator can only monitor the VPN 3002, not configure system parameters or administer the system.

See Administration | Access Rights | Administrators in [Chapter 11, “Administration”](#), for more information.

# Menu Reference

This section shows all the menus in the first three levels below the main menu. (There are many additional menus below the third level; and within the first three levels, there are some non-menu parameter settings. To keep this chapter at a reasonable size, we show only the *menus* here.)

The numbers in each heading are the keyboard shortcut to reach that menu from the main menu. For example, entering 1.3.1 at the main menu prompt takes you to the Configuration > System Management> IP Routing menu.



## Note

The menus and options, and thus the keyboard shortcuts, might change with new software versions. Please check familiar shortcuts carefully when using a new release.

## Main Menu

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> \_

## 1 Configuration

- 1) Quick Configuration
- 2) Interface Configuration
- 3) System Management
- 4) Policy Management
- 5) Back

Config -> \_

### 1.1 Configuration > Quick Configuration

See the *VPN 3002 Hardware Client Getting Started* guide for complete information about Quick Configuration.

### 1.2 Configuration > Interface Configuration

This table shows current IP addresses.

..

- 1) Configure the Private Interface
- 2) Configure the Public Interface
- 3) Back

Interfaces -> \_

## 1.2.1 or 1.2.2 Configuration > Interface Configuration > Configure the Private/Public Interface

- 1) Interface Setting (Disable or Static IP)
- 2) Select Internet Speed
- 3) Select Duplex
- 4) Set MTU
- 5) Back

Private/Public Interface -> \_

## 1.3 Configuration > System Management

- 1) Servers (DNS)
- 2) Tunneling Protocols (IPSec Parameters)
- 3) IP Routing (static routes, etc.)
- 4) Management Protocols (Telnet, HTTP, etc.)
- 5) Event Configuration
- 6) General Config (system name, time, etc.)
- 7) Back

System -> \_

### 1.3.1 Configuration > System Management > Servers

- 1) DNS Servers
- 2) Back

Servers -> \_

### 1.3.2 Configuration > System Management > Tunneling Protocols

- 1) IPSec
- 2) Back

Tunnel -> \_

### 1.3.3 Configuration > System Management > IP Routing

- 1) Static Routes
- 2) Default Gateway
- 3) DHCP
- 4) DHCP Options
- 5) Back

Routing -> \_

### 1.3.4 Configuration > System Management > Management Protocols

- 1) Configure HTTP/HTTPS
- 2) Configure Telnet
- 3) Configure SNMP
- 4) Configure SNMP Community Strings
- 5) Configure SSL
- 6) Configure SSH
- 7) Configure XML
- 8) Back

Network -> \_

### 1.3.5 Configuration > System Management > Event Configuration

- 1) General
- 2) Classes
- 3) Trap Destinations
- 4) Syslog Servers
- 5) Back

Event -> \_

### 1.3.6 Configuration > System Management > General Config

- 1) System Identification
- 2) System Time and Date
- 3) Back

General -> \_

### 1.4 Configuration > Policy Management

- 1) Traffic Management
- 2) Certificate Validation
- 3) Back

Policy -> \_

### 1.4.1 Configuration > Policy Management > Traffic Management

- 1) Port Address Translation (PAT)
- 2) Back

Traffic ->

### 1.4.2 Configuration > Policy Management > Certificate Validation

- 1) Enable/disable the matching criteria
- 2) Modify the matching criteria
- 3) Back

Certificate Validation ->

## 2 Administration

- 1) Software Update
- 2) System Reboot
- 3) Ping
- 4) Traceroute
- 5) Access Rights
- 6) File Management
- 7) Certificate Management
- 8) Back

Admin -> \_

### 2.1 Administration > Software Update

```
Name of the file for main code upgrade? [vpn3002c.bin]
IP address of the host where the file resides? [10.10.66.10]

(M)odify any of the above (C)ontinue or (E)xit? [M]
```

### 2.2 Administration > System Reboot

- 1) Cancel Scheduled Reboot/Shutdown
- 2) Schedule Reboot
- 3) Schedule Shutdown
- 4) Back

Admin -> \_

#### 2.2.2 Administration > System Reboot > Schedule Reboot

- 1) Save active Configuration and use it at Reboot
- 2) Reboot without saving active Configuration file
- 3) Reboot ignoring the Configuration file
- 4) Back

Admin -> \_

#### 2.2.3 Administration > System Reboot > Schedule Shutdown

- 1) Save active configuration and use it at next reboot
- 2) Shutdown without saving active Configuration file
- 3) Shutdown, ignoring the Configuration file at next reboot
- 4) Back

Admin -> \_

### 2.3 Administration > Ping

> Ping host

Admin -> \_

## 2.4 Administration > Traceroute

```
> Destination Address/Hostname
```

```
Admin -> _
```

## 2.5 Administration > Access Rights

- 1) Administrators
- 2) Access Settings
- 3) Back

```
Admin -> _
```

### 2.5.1 Administration > Access Rights > Administrators

```
Admin -> 1
```

```
Administrative Users

Username Enabled

admin Yes
config No
isp No

```

- 1) Modify Administrator
- 2) Back

```
Admin ->
```

### 2.5.2 Administration > Access Rights > Access Settings

- 1) Set Session Timeout
- 2) Set Session Limit
- 3) Set Config File Encryption
- 4) Zeroize/Regenerate DES Config File Encryption Key
- 5) Back

```
Admin -> _
```

## 2.6 Administration > File Management

```
List of Files

CONFIG CONFIG.BAK

1) View Config File
2) Delete Config File
3) View Backup Config File
4) Delete Backup Config File
5) View Crashdump File
6) Delete Crashdump File
7) View Savelog File
8) Delete Savelog File
9) View Memory Report
10) Delete Memory Report
11) Swap Config Files
12) Back

File -> _
```

### 2.6.11 Administration > File Management > Swap Configuration Files

```
Every time the active configuration is saved,...
.
.
.

1) Swap
2) Back

Admin -> _
```

## 2.7 Administration > Certificate Management

```
1) Enrollment
2) Installation
3) Certificate Authorities
4) Identity Certificates
5) SSL Certificates
6) Enrollment Status
7) SSH Host Key
8) Back

Certificates -> _
```

### 2.7.2 Administration > Certificate Management > Installation

```
1) Install Certificate Authority
2) Install Certificate obtained via enrollment
3) Back

Certificates -> _
```



## 2.7.3 Administration > Certificate Management > Certificate Authorities

```
Certificate Authorities
.
.
.
1) View Certificate
2) Delete Certificate
3) Configure Certificate
4) Back

Certificates -> _
```

## 2.7.4 Administration > Certificate Management > Identity Certificates

```
Identity Certificates
.
.
.
1) View Certificate
2) Delete Certificate
3) Renew Certificate
3) Back

Certificates -> _
```

## 2.7.5 Administration > Certificate Management > SSL Certificates

```
1) Private SSL Certificate
2) Public SSL Certificate
3) Back

SSL Certificates -> _
```

## 2.7.6 Administration > Certificate Management > Enrollment Status

```
1) View Enrollment Request
2) Install/Activate Enrollment Request
3) Resubmit Enrollment Request
4) Delete/Cancel Enrollment Request
5) Back

Certificates -> _
```

## 2.7.7 Administration > Certificate Management > SSH Host Key

```
1) Generate SSH Host Key
2) Back

SSH Certificate -> _
```

## 3 Monitoring

- 1) Routing Table
- 2) Event Log
- 3) System Status
- 4) User Status
- 5) General Statistics
- 6) Back

Monitor -> \_

### 3.1 Monitoring > Routing Table

```
Routing Table
.
.
'q' to Quit, '<SPACE>' to Continue ->
.
.
1) Refresh Routing Table
2) Back
```

Routing -> \_

### 3.2 Monitoring > Event Log

- 1) Configure Log viewing parameters
- 2) View Event Log
- 3) Clear Log
- 4) Back

Log -> \_

#### 3.2.2 Monitoring > Event Log > View Event Log

```
[Event Log entries]
.
.
.
1) First Page
2) Previous Page
3) Next Page
4) Last Page
5) Back
```

Log -> \_

### 3.3 Monitoring > System Status

```
System Status
.
.
.
1) Refresh System Status
2) Reset System Status
3) Restore System Status
4) Connect Now
5) Disconnect Now
6) View Memory Status
7) Back

Status -> _
```

### 3.4 Monitoring > User Status

```
Authenticated Users

 Username IP Address MAC Address Login Time Duration

1) Refresh User Status
2) Log out User
3) Back

Sessions ->
```

### 3.5 Monitoring > General Statistics

```
1) Protocol Statistics
2) Server Statistics
3) MIB II Statistics
4) Back

General -> _
```

#### 3.4.1 Monitoring > General Statistics > Protocol Statistics

```
1) IPSec Statistics
2) HTTP Statistics
3) Telnet Statistics
4) DNS Statistics
5) SSL Statistics
6) SSH Statistics
7) PPPoE Statistics
8) NAT Statistics
9) Back

General -> _
```

#### 3.4.2 Monitoring > General Statistics > Server Statistics

```
1) DHCP Statistics
2) Back

General -> _
```

#### 3.4.3 Monitoring > General Statistics > MIB II Statistics

```
1) Interface-based
2) System-level
3) Back

MIB2 -> _
```



## IKE Proposals

IKE proposals are sets of parameters for Phase I IPSec negotiations. During Phase 1, the two peers establish a secure tunnel within which they then negotiate the Phase 2 parameters.

You configure IKE proposals on the VPN Concentrator, not on the VPN 3002. The VPN Concentrator software includes a set of preconfigured IKE proposals active by default, and a second preconfigured set inactive by default. You can configure additional IKE proposals to a maximum of 150. On the VPN Concentrator, see Configuration | System | Tunneling Protocols | IPSec | IKE Proposals.

## Valid IKE Proposals

[Table A-1](#) describes IKE proposals that are valid for the VPN 3002 Hardware Client. Use this information to configure IKE proposals for the VPN 3002. For instructions about configuring IKE proposals, see the section, “Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add, Modify, or Copy” in the *Tunneling* chapter of the *VPN 3000 Series Concentrator Reference Volume I*.

**Table A-1** Valid VPN 3002 Hardware 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)   |

| Proposal Name                     | Authentication Mode             | Authentication Algorithm | Encryption Algorithm | Diffie- Hellman Group |
|-----------------------------------|---------------------------------|--------------------------|----------------------|-----------------------|
| 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)   |
| 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)   |

| Proposal Name                     | Authentication Mode             | Authentication Algorithm | Encryption Algorithm | Diffie- Hellman Group |
|-----------------------------------|---------------------------------|--------------------------|----------------------|-----------------------|
| 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)    |
| 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)   |
| CiscoVPNClient-3DES-SHA-DSA       | DSA Digital Certificate (XAUTH) | SHA/HMAC-160             | 3DES-168             | Group 2 (1024 bits)   |

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





## Troubleshooting and System Errors

---

Appendix A describes files for troubleshooting the VPN 3002 and LED indicators on the system. It also describes common errors that might occur while configuring and using the system, and how to correct them.

### Files for Troubleshooting

The VPN 3002 Hardware Client creates several files that you can examine and that can assist Cisco support engineers when troubleshooting errors and problems:

- Event log.
- SAVELOG.TXT—Event log that is automatically saved when the system crashes and when it is rebooted.
- CRSHDUMP.TXT—Internal system data file that is written when the system crashes.
- CONFIG—Normal configuration file used to boot the system.
- CONFIG.BAK—Backup configuration file.

### Event Logs

The VPN 3002 records system events in the event log, which is stored in nonvolatile memory (NVRAM). To troubleshoot operational problems, we recommend that you start by examining the event log. To view the event log, see [Administration | File Management | View](#), and click on **View Saved Log File**. To configure events, and to choose the events you want to view, see [Configuration | System | Events and Monitoring | Filterable Event Log](#).

The VPN 3002 automatically saves the event log to a file in flash memory if it crashes, and when it is rebooted. This log file is named SAVELOG.TXT, and it overwrites any existing file with that name. The SAVELOG.TXT file is useful for debugging. To view SAVELOG.TXT, see [Administration | File Management | View](#), and click on **View Saved Log File**.

## Crash Dump File

If the VPN 3002 crashes during operation, it saves internal system data in nonvolatile memory (NVRAM), and then automatically writes this data to a CRSHDUMP.TXT file in flash memory when it is rebooted. This file contains the crash date and time, software version, tasks, stack, registers, memory, buffers, and timers which help Cisco support engineers diagnose the problem. In case of a crash, we ask that you send this file when you contact TAC for assistance. To view the CRSHDUMP.TXT file, see Administration | File Management | View, and click on **View Saved Log Crash Dump File**.

## Configuration Files

The VPN 3002 saves the current boot configuration file (CONFIG) and its predecessor (CONFIG.BAK) as files in flash memory. These files may be useful for troubleshooting. See Administration | File Management for information on managing files in flash memory.

## LED Indicators

LED indicators on the VPN 3002 are normally green or flashing amber. LEDs that are solid amber or off may indicate an error condition.

Contact Cisco TAC if any LED indicates an error condition.

## VPN 3002 Front LEDs

The LEDs on the front of the VPN 3002 are:

| LED | Status         | Explanation                        |
|-----|----------------|------------------------------------|
| PWR | Green          | Unit is on and has power.          |
|     | Off            | Unit is powered off.               |
| SYS | Flashing amber | Unit is performing diagnostics.    |
|     | Solid amber    | Unit has failed diagnostics.       |
|     | Flashing green | Unit is negotiating DHCP or PPPoE. |
|     | Green          | Unit is operational.               |
| VPN | Off            | No VPN tunnel exists.              |
|     | Amber          | Tunnel has failed.                 |
|     | Green          | Tunnel is established.             |

## VPN 3002 Rear LEDs

The LEDs on the rear of the VPN 3002 indicate the status of the private and public interfaces.

| LED            | Explanation                                |
|----------------|--------------------------------------------|
| Green          | Interface is connected to the network.     |
| OFF            | Interface is not connected to the network. |
| Flashing amber | Traffic is traveling across the interface. |

## System Errors

If you have configured the VPN 3002, and you are unable to connect to or pass data to the central-site VPN Concentrator, use [Table B-1](#) to analyze the problem. Also, use the following section of this appendix to check the settings on the VPN Concentrator to which this VPN 3002 connects.

**Table B-1 Analyzing System Errors**

| Problem or Symptom                                                                                                 | Possible Solution                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel is not up or not passing data.                                                                              |                                                                                                                                                                                                                                            |
| PWR LED is off.                                                                                                    | Make sure that the power cable is plugged into the VPN 3002 and a power outlet.                                                                                                                                                            |
| SYS LED is solid amber.                                                                                            | Unit has failed diagnostics. Contact Cisco Support immediately.                                                                                                                                                                            |
| You see this LED display:<br>PWR = green<br>SYS LED = green<br>VPN LED = off.                                      | <ol style="list-style-type: none"> <li>1. Verify that the VPN Concentrator to which this VPN 3002 connects is running version 3.0 software.</li> <li>2. Navigate to Monitoring &gt; System Status. Click on <b>Connect Now</b>.</li> </ol> |
| <b>Connect Now</b> did not bring up the tunnel, and the public interface LED (rear of unit) is off.                | <ol style="list-style-type: none"> <li>1. Check that a LAN cable is properly attached to the public interface of the VPN 3002.</li> <li>2. Make sure the IP address for the public interface is properly configured.</li> </ol>            |
| Public interface LED is on, but attempting to ping the default gateway (Administration > Ping) yields no response. | <ol style="list-style-type: none"> <li>1. Make sure the default gateway is properly configured.</li> <li>2. Contact your ISP.</li> </ol>                                                                                                   |

Table B-1 Analyzing System Errors (continued)

| Problem or Symptom                                                                    | Possible Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VPN LED is solid amber (tunnel failed to establish to central-site VPN Concentrator). | <ol style="list-style-type: none"> <li>1. Make sure the IPSec parameters are properly configured. Verify: <ul style="list-style-type: none"> <li>– Public IP Address of the IKE peer (central-site VPN Concentrator) is correct.</li> <li>– Group name and password are correct.</li> <li>– User name and password are correct.</li> </ul> </li> <li>2. Make sure the group and user names and passwords match those set for the VPN 3002 on the central-site VPN Concentrator.</li> <li>3. After you make any changes, navigate to Monitoring &gt; System Status and click on <b>Connect Now</b>.</li> <li>4. Study the event log files. To capture more events, and to interpret events, see Chapter 9, “Events,” in the <i>VPN 3002 Hardware Client User Reference</i>.</li> </ol> |
| My PC cannot communicate with the remote network.                                     | <ol style="list-style-type: none"> <li>1. Verify that the VPN Concentrator to which this VPN 3002 connects is running version 3.0 software.</li> <li>2. Navigate to Monitoring &gt; System Status and click on <b>Connect Now</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Connect Now</b> worked.                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LED(s) for the private interface/switch port are off.                                 | Make sure that a LAN cable is properly attached to the private interface of the VPN 3002 and the PC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| LED(s) for the private interface/switch port are on.                                  | <ol style="list-style-type: none"> <li>1. Is this PC configured as a DHCP client? If so, verify that the DHCP server on the VPN 3002 is enabled.</li> <li>2. With any method of address assignment, verify that the PC has an IP address and subnet mask.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Attempting to ping the default gateway (Administration > Ping) yields no response.    | <ol style="list-style-type: none"> <li>1. Make sure your PC has an appropriate IP address, reachable on this network.</li> <li>2. Contact your network administrator.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

# Settings on the VPN Concentrator

If your VPN 3002 experiences connectivity problems, check the configuration of the VPN Concentrator.

- 
- Step 1** Configure the connection as a Client, *not* LAN-to-LAN.
  - Step 2** Assign this VPN 3002 to a group. Configure group and user names and passwords. These must match the group and user names and passwords that you set on the VPN 3002. Refer to Chapter 14, “User Management,” in the *VPN 3000 Series Concentrator Reference Volume I*.
  - Step 3** If the VPN 3002 uses PAT mode, enable a method of address assignment for the VPN 3002: DHCP, address pools, per user, or client specified. Refer to Chapter 6, “Address Management,” in the *VPN 3000 Series Concentrator Reference Volume I*.
  - Step 4** If you are using Network Extension mode, configure a default gateway or a static route to the private network of the VPN 3002. Refer to Chapter 8, “IP Routing,” in the *VPN 3000 Series Concentrator Reference Volume I*.
  - Step 5** Check the Event log. Refer to Chapter 10, “Events,” in the *VPN 3000 Series Concentrator Reference Volume I*.

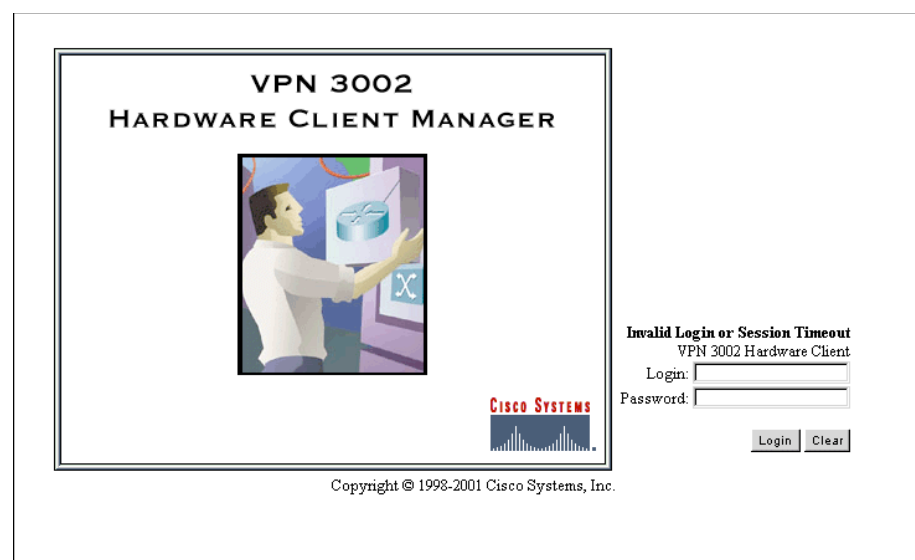
## VPN 3002 Hardware Client Manager Errors

The following sections describe errors that might occur while using the HTML-based VPN 3002 Hardware Client Manager with a browser.

### Invalid Login or Session Timeout

The Manager displays the Invalid Login or Session Timeout screen (see [Figure B-1](#)).

**Figure B-1** Invalid Login or Session Timeout Screen



61694

**Table B-2** *Invalid Login or Session Timeout Screen*

| Problem                                                                                                                                                | Possible Cause                                                                                                                                                                                                                                                                                                                                                                                                                              | Solution                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You entered an invalid administrator login-name and password combination                                                                               | <ul style="list-style-type: none"> <li>Typing error.</li> <li>Invalid (unrecognized) login name or password.</li> </ul>                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>Reenter the login name and password, and click on <b>Login</b>.</li> <li>Use a valid login name and password.</li> <li>Verify your typing before clicking on <b>Login</b>.</li> </ul> |
| The Manager session has been idle longer than the configured timeout interval. (The default timeout interval is 600 seconds, which equals 10 minutes). | <ul style="list-style-type: none"> <li>No activity has occurred for (interval) seconds. The Manager resets the inactivity time only when you click on an action button such as <b>Apply</b>, <b>Add</b>, or <b>Cancel</b>, or a link on a screen that invokes a different screen. Entering values or setting parameters on a given screen does not reset the timer.</li> <li>The timeout interval is set too low for normal use.</li> </ul> | On the Administration   Access Rights   Access Settings screen, change the Session Timeout interval to a larger value and click on <b>Apply</b> .                                                                            |

## Manager Logs Out

The Manager unexpectedly logs out.

**Table B-3** *Browser Refresh or Reload Button Logs Out the Manager.*

| Problem                                                                                                                                                  | Possible Cause                                                                                                                             | Solution                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You clicked on the <b>Refresh</b> or <b>Reload</b> button on the browser navigation toolbar, and the Manager logged out. The main login screen displays. | To protect access security, clicking on <b>Refresh</b> or <b>Reload</b> on the browser toolbar automatically logs out the Manager session. | <p>Do not use the browser navigation toolbar buttons with the VPN 3002 Hardware Client Manager.</p> <p>Use only the Manager Refresh button where it appears on a screen.</p> <p>We recommend that you hide the browser navigation toolbar to prevent mistakes.</p> |

## Incorrect Display

The Manager displays an incorrect screen or data when you click on the browser back or forward button.

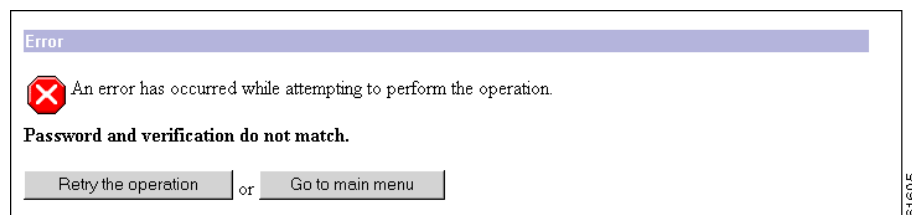
**Table B-4 Browser Back or Forward Button Displays an Incorrect Screen or Incorrect Data**

| Problem                                                                                                                                                         | Possible Cause                                                                                                                                                          | Solution                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You clicked on the <b>Back</b> or <b>Forward</b> button on the <i>browser</i> navigation toolbar, and the Manager displayed the wrong screen or incorrect data. | To protect security and the integrity of data entries, clicking on <b>Back</b> or <b>Forward</b> on the browser toolbar deletes pointers and values within the Manager. | Do not use the browser navigation toolbar buttons with the VPN 3002 Hardware Client Manager.<br><br>Navigate using the location bar at the top of the Manager window, the table of contents in the left frame, or links on Manager screens.<br><br>We recommend that you hide the browser navigation toolbar to prevent mistakes. |

## Error Message

The Manager displays a screen with the message: “Error/An error has occurred while attempting to perform the operation.” An additional error message describes the erroneous operation (see [Figure B-2](#)).

**Figure B-2 Error Screen**



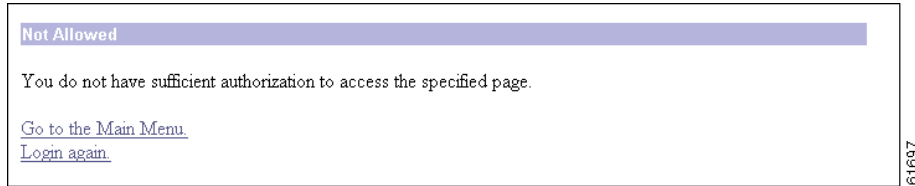
**Table B-5 Error Message Displays**

| Problem                                                  | Possible cause                                          | Solution                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You tried to perform some operation that is not allowed. | The screen displays a message that describes the cause. | <ul style="list-style-type: none"> <li>Click on <b>Retry the operation</b> to return to the screen where you were working and correct the mistake. Carefully check all your previous entries on that screen. The Manager attempts to retain valid entries, but invalid entries are lost.</li> <li>Click on <b>Go to main menu</b> to go to the main Manager screen.</li> </ul> |

## Not Allowed Message

The Manager displays a screen with the message: “Not Allowed / You do not have sufficient authorization to access the specified page.” (see [Figure B-3](#)).

**Figure B-3** Not Allowed Screen



**Table B-6** Not Allowed Message Displays

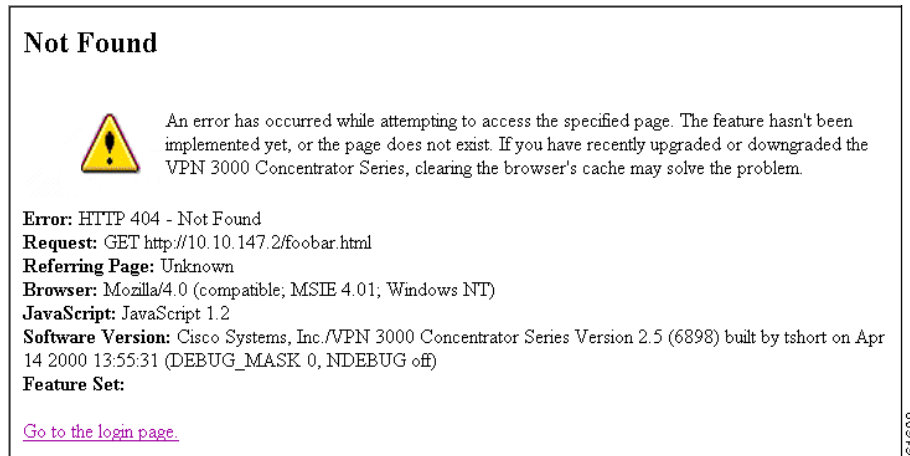
| Problem                                                                                  | Possible cause                                                                                                                                                                                               | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| You tried to access an area of the Manager that you do not have authorization to access. | <ul style="list-style-type: none"> <li>You logged in using an administrator login name that has limited privileges.</li> <li>You logged in from a workstation that has limited access privileges.</li> </ul> | <ul style="list-style-type: none"> <li>Log in using the system administrator login name and password. (Defaults are admin / admin.)</li> <li>Log in from a workstation with greater access privileges.</li> <li>Have the system administrator change your privileges on the Administration   Access Rights   Administrators screen.</li> <li>Have the system administrator change the privileges of your workstation on the Administration   Access Rights   Access Control List screen.</li> </ul> |



## Not Found

The Manager displays a screen with the message: “Not Found/An error has occurred while attempting to access the specified page.” The screen includes additional information that identifies system activity and parameters.

**Figure B-4 Not Found Screen**



**Table B-7 Not Found Message Displays**

| Problem                              | Possible cause                                                                                                                                                       | Solution                                                                                                                                                                                                                                       |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Manager could not find a screen. | <ul style="list-style-type: none"> <li>You updated the software image and did not clear the browser's cache.</li> <li>There is an internal Manager error.</li> </ul> | <p>Clear the browser's cache: delete its temporary internet files, history files, and location bar references. Then try again.</p> <p>Please note the system information on the screen and contact Cisco support personnel for assistance.</p> |

## Microsoft Internet Explorer Script Error: No such interface supported

Microsoft Internet Explorer displays a Script Error dialog box that includes the error message: **No such interface supported.**

**Table B-8 Microsoft Internet Explorer Script Error**

| Problem                                                                                                                                                                                          | Possible cause                                         | Solution                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| While using a Manager function that opens another browser window (such as Save Needed, Help, Software Update, etc.), Internet Explorer cannot open the window and displays the error dialog box. | A bug in the Internet Explorer JavaScript interpreter. | <ol style="list-style-type: none"> <li>Click on <b>No</b> on the error dialog box.</li> <li>Log out of the Manager.</li> <li>Close Internet Explorer.</li> <li>Reinstall Internet Explorer.</li> </ol> |

## Command-line Interface Errors

These errors may occur while using the menu-based command-line interface from a console or Telnet session.

*Table B-9 Command-Line Interface Errors*

| Error                                                     | Problem                                                                                        | Possible Cause                                                                                                                                                                                                                                                                      | Solution                                                                                                                                                                 |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERROR:-- Bad IP Address/Subnet Mask/Wildcard Mask/Area ID | The system expected a valid 4-byte dotted decimal entry, and the entry was not in that format. | <ul style="list-style-type: none"> <li>You entered something other than a 4-byte dotted decimal number. You might have omitted a byte position, or entered a number greater than 255 in a byte position.</li> <li>You entered 0.0.0.0 instead of an appropriate address.</li> </ul> | At the prompt, reenter a valid 4-byte dotted decimal number.                                                                                                             |
| ERROR:-- Out of Range value entered. Try again.           | The system expected a number within a certain range, and the entry was outside that range.     | <ul style="list-style-type: none"> <li>You entered a letter instead of a number.</li> <li>You entered a number greater than the possible menu numbers.</li> </ul>                                                                                                                   | At the prompt, reenter a number in the appropriate range.                                                                                                                |
| ERROR:-- The Passwords do not match. Please try again.    | The entry for a password and the entry to verify the password do not match.                    | <ul style="list-style-type: none"> <li>You mistyped an entry.</li> <li>You entered either a password or verify entry, but not the other.</li> </ul>                                                                                                                                 | At the Verify prompt, reenter the password. If the original password is incorrect, press <b>Enter</b> and reenter both the password and the verification at the prompts. |



---

## Numerics

3DES-168/SHA SSL encryption algorithm [8-11](#)

3DES-168 SSH encryption algorithm [8-14](#)

---

## A

accessing the CLI [14-1](#)

access rights

- administration [12-10](#)

- default Monitor administrator (CLI) [14-6](#)

access settings, general, for administrators [12-13](#)

add

- event class [9-10](#)

- SNMP community [8-8](#)

- SNMP event destination [9-13](#)

- static route for IP routing [7-3](#)

- syslog server to receive events [9-16](#)

Address Resolution Protocol (ARP) mapping table [13-54](#)

administering the VPN 3002 [12-1](#)

administration\_file\_management [12-13](#)

administrators

- access rights [12-10](#)

- access settings, general [12-13](#)

- configuring [12-11](#)

- parameters saved in nonvolatile memory [12-11](#)

- password [12-11](#)

- predefined [12-11](#)

- properties and rights, changing [12-11](#)

- session idle timeout [12-13](#)

ARP table [13-54](#)

authentication

- client, SSL (HTTPS only) [8-11](#)

- using digital certificates [12-18](#)

---

## B

Back and Home CLI choices [14-5](#)

back panel display (monitoring) [13-11](#)

backup configuration file

- swapping [12-15](#)

- use in troubleshooting [B-2](#)

backup server list [6-4](#)

backup servers

- configuring [6-4](#)

- DNS and WINS servers [6-4](#)

- overview [6-4](#)

Bad IP Address (error) [B-10](#)

bidirectional tunnel endpoint [6-1](#)

bootcode

- version and filename [13-9](#)

boot configuration file, swapping [12-15](#)

browser

- Back or Forward button displays incorrect screen or incorrect data [B-7](#)

- clear cache after software update [12-4](#)

- installing SSL certificate [1-3](#)

- navigation toolbar, don't use with Manager [1-2](#)

- requirements [1-1](#)

built-in servers, configuring *See* management protocols [8-1](#)

---

## C

CA, *See also* Certificate Authority

CA certificates

- definition [12-18](#)

- installing [12-49](#)
- cancelling an enrollment request [12-71](#)
- certificate
  - PEM-encoded [12-31](#)
- certificate, *See also* digital certificates
- Certificate Authority
  - definition [12-18](#)
- certificate management [12-18](#)
- changing administrator properties and rights [12-11](#)
- clear event log [13-5](#)
- CLI
  - accessing [14-1](#)
    - via console [14-1](#)
    - via Telnet [14-2](#)
  - Back and Home choices [14-5](#)
  - choosing a menu item [14-3](#)
  - configuration menu [14-7](#)
  - entering values [14-3](#)
  - errors [B-10](#)
  - help command [14-5](#)
  - main menu [14-2, 14-7](#)
  - menu reference [14-7](#)
  - navigating with shortcut numbers [14-4](#)
  - prompt contains menu context [14-3](#)
  - saving configuration file [14-6](#)
  - shortcut numbers [14-4](#)
  - starting [14-2](#)
  - stopping [14-6](#)
  - using [14-1, 14-3](#)
- client authentication, SSL (HTTPS only) [8-11](#)
- client mode
  - definition [11-2](#)
  - effect on backup server connection [6-5](#)
  - See also* PAT mode
- Command Line Interface
  - See* CLI
- concentrator settings
  - required for Network Extension mode [11-4](#)
  - required for PAT [11-3](#)
- CONFIG.BAK file
  - See* backup configuration file
  - use in troubleshooting [B-2](#)
- configuration
  - quick [2-1](#)
  - system [4-1](#)
  - VPN 3002 Hardware Client Manager [2-1](#)
- configuration files
  - automatic backup with file upload [12-16](#)
  - changes with software update [12-2](#)
  - handling at reboot or shutdown [12-6](#)
  - handling during file upload [12-16](#)
  - managing and viewing [12-14](#)
  - saving with CLI [14-6](#)
  - swap [12-15](#)
  - useful for troubleshooting [B-2](#)
- configuration menu, CLI [14-7](#)
- configuring
  - administrative access to the VPN 3002 [12-10](#)
  - backup servers [6-4](#)
  - default gateways for IP routing [7-4](#)
  - interfaces [3-1](#)
  - private interface [3-4](#)
  - public interface [3-6](#)
  - remote server [6-3](#)
  - static routes for IP routing [7-2](#)
  - VPN Concentrator with CLI [14-1](#)
- connecting to VPN Concentrator
  - using HTTP [1-2](#)
  - using HTTPS [1-16](#)
- console, accessing CLI via [14-1](#)
- crash
  - dump file [B-2](#)
- crash, system
  - saves log file [B-1](#)
- CRSHDUMP.TXT file [B-2](#)

---

**D**

data formats [xiii](#)

data initiation

VPN 3002 and central-site concentrator [11-6](#)

date and time, configuring [10-3](#)

Daylight-Saving Time (DST), enabling [10-3](#)

default

event handling, configuring [9-5](#)

gateways, configuring for IP routing [7-4](#)

Monitor administrator access rights (CLI) [14-6](#)

delete

digital certificate [12-33, 12-64](#)

enrollment request [12-72](#)

DES-40/SHA Export SSL encryption algorithm [8-11](#)

DES-56/SHA SSL encryption algorithm [8-11](#)

DES-56 SSH encryption algorithm [8-14](#)

DHCP [7-9](#)

configuring parameters on VPN 3002 [7-6](#)

statistics [13-33](#)

digital certificates

CA [12-18](#)

definition [12-18](#)

deleting [12-33, 12-64](#)

enabling on the VPN 3002 [12-32](#)

enrolling [12-22, 12-40](#)

fields [12-58](#)

identity [12-18, 12-36](#)

installing [12-22, 12-50](#)

installing automatically via SCEP [12-19](#)

IPSec LAN-to-LAN [6-7](#)

managing [12-18](#)

PKCS-10 request [12-45](#)

renewal [12-61](#)

root [12-18](#)

saving in Flash memory [12-18](#)

SCEP-enabled [12-19](#)

SSL [1-3, 12-18](#)

troubleshooting [12-21](#)

viewing and managing on VPN 3002 [12-34](#)

viewing details [12-56](#)

X.509 [12-18](#)

disabling the public interface [3-6](#)

display/PC monitor, recommended settings [1-2](#)

DNS

backup server, configuring [6-4](#)

servers, configuring [5-1](#)

statistics [13-30](#)

documentation

additional [xi](#)

cautions [xii](#)

notes [xii](#)

Domain Name Servers *See* DNS

downloading

backup server list from a VPN Concentrator [6-5](#)

event log to PC [13-5](#)

Dynamic Host Configuration Protocol *See* DHCP

---

**E**

encryption algorithms

SSH [8-14](#)

SSL [8-11](#)

enrolling

certificates [12-40](#)

identity certificate via SCEP [12-46](#)

enrollment request

cancelling [12-71](#)

creating [12-40](#)

deleting [12-72](#)

PKCS-10 [12-45](#)

removing according to status [12-38](#)

status table [12-38](#)

viewing details [12-69](#)

entering values with CLI [14-3](#)

erasing the event log [13-5](#)

error

an error has occurred ... [B-7](#)

- bad IP address [B-10](#)
- CLI [B-10](#)
- insufficient authorization [B-8](#)
- invalid login [B-5](#)
- Manager unexpectedly logs out [B-6](#)
- message displays [B-7](#)
- no such interface supported (IE) [B-9](#)
- not allowed [B-8](#)
- not found [B-9](#)
- out of range value [B-10](#)
- passwords do not match [B-10](#)
- session timeout [B-5](#)
- VPN 3002 Hardware Client Manager [B-5](#)
- Ethernet
  - interface
    - status and statistics [13-14](#)
  - MIB-II statistics [13-56](#)
- event
  - class [9-1](#)
  - configuring [9-5](#)
  - configuring default handling [9-5](#)
  - configuring for special handling
    - modify [9-10](#)
  - configuring special handling [9-8](#)
    - add [9-10](#)
  - definition [9-1](#)
  - severity level [9-3](#)
  - trap destinations, configuring [9-12](#)
- event log
  - clear (erase) [13-5](#)
  - definition [9-4](#)
  - download to PC [13-5](#)
  - format [9-6, 13-5](#)
  - get [13-5](#)
  - live [13-6](#)
  - monitoring [13-3, 13-6](#)
  - save [13-5](#)
  - saved on system crash or reboot [B-1](#)
  - saved on system failure or reboot [9-4](#)

- stored in nonvolatile memory [13-3](#)
- view [13-5](#)
- viewing [13-6](#)
- exiting from CLI [14-6](#)
- exporting an SSL certificate [12-66](#)

---

## F

- file management on VPN 3002 [12-14](#)
- file upload to VPN 3002 [12-2, 12-16](#)
  - stopping [12-3, 12-16](#)
- filterable event log, monitoring [13-3](#)
- flash memory
  - corrupting [12-2, 12-5](#)
  - managing files [12-14](#)
  - temporary files in [12-16](#)
- format
  - data [xiii](#)
  - event log [13-5](#)
  - syslog [9-6](#)
- fragmentation policy
  - IPSec [3-8](#)
- front panel display (monitoring) [13-11](#)

---

## G

- gateways, default [7-4](#)
- general (default) event handling [9-5](#)
- general parameters, configuring [10-1](#)
- generating
  - SSH host key [12-68](#)
  - SSL certificate [12-65](#)
- get event log [13-5](#)

---

## H

- halting the VPN 3002 [12-5](#)
- help, CLI [14-5](#)

- Home and Back CLI choices [14-5](#)
  - host key
    - SSH [8-13](#)
  - HTTP
    - configuring internal server [8-2](#)
    - enabling [8-2](#)
    - port number [8-3](#)
    - statistics [13-25](#)
    - using with Manager [1-2](#)
  - HTTPS
    - configuring internal server [8-2](#)
    - connecting using [1-16](#)
    - definition [1-3](#)
    - enabling [8-3](#)
    - enabling on public interface for XML support [8-16](#)
    - login screen [1-17](#)
    - port number [8-3](#)
- 
- ICMP
    - MIB-II statistics [13-51](#)
    - PING [12-7](#)
  - identification, configuring [10-2](#)
  - identifying servers to the VPN 3002 [5-1](#)
  - identity certificates
    - definition [12-18](#)
    - enrolling [12-40](#)
    - installed on the VPN 3002 [12-36](#)
    - maximum allowed [12-18](#)
  - idle timeout
    - administrator sessions [12-13](#)
    - live event log overrides [13-6](#)
  - IEEE standard 802.3, Ethernet networks [13-56](#)
  - IKE proposals, valid for VPN3002 [A-1](#)
  - image, software
    - filenames [12-3](#)
  - indicators, LED [B-2](#)
  - individual user authentication
    - login screen [1-19](#)
  - installing
    - CA certificates [12-49](#)
    - CA certificates, automatic method (using SCEP) [12-19](#)
    - enrolled certificates [12-50](#)
    - identity certificates, automatic method [12-22](#)
    - SSL certificate
      - with Internet Explorer [1-4](#)
      - with Netscape [1-9](#)
  - Install SSL Certificate (screen) [1-4](#)
  - interactive hardware client authentication
    - login screen [1-19](#)
  - interfaces
    - configuring [3-1](#)
    - Ethernet, configuring
      - transmission mode [3-5, 3-8](#)
    - MIB-II statistics [13-43](#)
    - private, configuring [3-4](#)
    - public, configuring [3-6](#)
    - status [3-3](#)
  - Internet Explorer, requirements [1-1](#)
  - Invalid Login or Session Timeout (error) [B-5](#)
  - IP MIB-II statistics [13-48](#)
  - IP routing
    - configuring [7-1](#)
  - IPSec
    - attributes configurable on the central-site concentrator [6-2](#)
    - configuring [6-2](#)
    - statistics [13-19](#)
  - IPSec fragmentation [3-8](#)
  - IPSec over TCP [6-6](#)
    - requirements [6-6](#)
  - ITU (International Telecommunication Union)
    - standards [12-56](#)
- 
- J
    - JavaScript, requirements [1-2](#)

## L

- lease period, DHCP [7-6](#)
- LED indicators
  - table [B-2](#)
- live event log [13-6](#)
  - Netscape requirements [13-6](#)
- log file
  - live event log [13-6](#)
  - saving on system reboot [12-5](#)
  - See also* event log
- logging in to the VPN Concentrator Manager [1-17](#)
- login
  - name, factory default (Manager) [1-17](#)
  - password, factory default (Manager) [1-17](#)
  - screen [1-3](#)
    - HTTPS [1-17](#)
    - HTTPS using Internet Explorer [1-8](#)
    - HTTPS using Netscape [1-14](#)
  - using CLI [14-2](#)
  - using interactive hardware client authentication and individual user authentication [1-19](#)

## M

- main menu, CLI [14-2, 14-7](#)
- management protocols, configuring [8-1](#)
- Manager table of contents [1-26](#)
- Manager unexpectedly logs out (error) [B-6](#)
- managing digital certificates on VPN 3002 [12-34](#)
- managing VPN Concentrator with CLI [14-1](#)
- memory, SDRAM [13-9](#)
- menu
  - choosing a menu item in CLI [14-3](#)
  - context in CLI prompt [14-3](#)
- menu reference, CLI [14-7](#)
- MIB-II
  - statistics [13-42](#)
    - ARP table [13-54](#)

- Ethernet traffic [13-56](#)
  - interfaces [13-43](#)
  - IP traffic [13-48](#)
  - SNMP [13-59](#)
  - TCP/UDP [13-45](#)
- system object [10-2](#)
- Microsoft Internet Explorer script error message [B-9](#)
- model number, system [13-9](#)
- modifying
  - event class [9-10](#)
  - SNMP community [8-8](#)
  - SNMP event trap destination [9-13](#)
  - static route, for IP routing [7-3](#)
  - syslog server to receive events [9-16](#)
- monitoring statistics [13-1](#)
- MTU [3-8](#)

## N

- NAT (Network Address Translation)
  - definition [11-2](#)
- navigating
  - the VPN 3002 Hardware Client Manager [1-26](#)
- Netscape Navigator, requirements [1-1](#)
- Network Address Translation *See* NAT
- Network Extension mode [11-3](#)
  - effect on backup server connection [6-5](#)
  - required settings on VPN Concentrator [11-4](#)
- nonvolatile memory [12-11](#)
  - event log stored in [13-3](#)
- No such interface supported (error) [B-9](#)
- Not Allowed (error) [B-8](#)
- Not Found (error) [B-9](#)

## O

- options configurable only on central-site Concentrator [7-9](#)
- Out of Range value (error) [B-10](#)



---

**P**

## password

- administrator [12-11](#)
- factory default (Manager) [1-17](#)

Passwords do not match (error) [B-10](#)

## PAT mode

- configuring [11-6](#)
- definition [11-2](#)
- enabling [11-7](#)
- many-to-one translation [11-6](#)
- required settings on VPN Concentrator [11-3](#)

PC monitor/display, recommended settings [1-2](#)

peer [6-2](#)

PEM-encoded certificate [12-31](#)

ping a host [12-7](#)

## PKCS-10

- enrollment request [12-45](#)

policy management [11-1](#)

Port Address Translation mode *See* PAT mode

## port number

- HTTP [8-3](#)
- HTTPS [8-3](#)
- SNMP [8-6](#)
- SSH [8-14](#)
- syslog server [9-16](#)
- Telnet [8-5](#)
- Telnet over SSL [8-5](#)

power, turning off [12-5](#)

PPPoE [3-6](#)

- statistics [13-39](#)

PPP over Ethernet *See* PPPoE

prerequisites, system administrator [ix](#)

preshaed keys [6-7](#)

## private interface

- configuring [3-4](#)

private keys, saving in Flash memory [12-18](#)

## public interface

- configuring [3-6](#)

Public Key Certificate Syntax-10 *See* PKCS-10

Public Key Infrastructure (PKI) [6-7, 12-18](#)

---

**Q**

Quick Configuration [2-1](#)

---

**R**

RC4-128 SSH encryption algorithm [8-14](#)

RC4-40/MD5 Export SSL encryption algorithm [8-11](#)

## reboot

- handling configuration files [12-6](#)
- reloads the boot configuration file [12-15](#)
- saving log file [12-5, B-1](#)
- system [12-5](#)

re-enrolling a certificate [12-61](#)

re-keying a certificate [12-61](#)

## remote server

- configuring [6-3](#)

renewing a DHCP lease [7-6](#)

renewing digital certificates [12-61](#)

## requirements

- browser [1-1](#)
- Internet Explorer [1-1](#)
- IPSec over TCP [6-6](#)
- JavaScript [1-2](#)
- Netscape Navigator [1-1](#)

RFC 1650, Ethernet interface MIB objects [13-56](#)

RFC 1907, SNMP version 2 MIB objects [13-59](#)

RFC 2011, ARP table entries [13-54](#)

RFC 2011, IP and ICMP MIB objects [13-48, 13-51](#)

RFC 2012, TCP MIB objects [13-45](#)

RFC 2013, UDP MIB objects [13-45](#)

RFC 2459 [12-56](#)

root CA certificate [12-18](#)

routing table (monitoring) [13-2](#)

RRC4-128/MD5 SSL encryption algorithm [8-11](#)

RSA key, SSH [8-13](#)

## S

SAVELOG.TXT file [9-4, 12-5, B-1](#)

saving

configuration file with CLI [14-6](#)

event log [13-5](#)

log file on system reboot [9-4, 12-5](#)

SCEP

enrolling an identity certificate [12-46](#)

enrolling SSL certificate [12-47](#)

installing CA certificates [12-19](#)

installing identity certificates [12-22](#)

SCEP-enabled certificate [12-19](#)

troubleshooting [12-21](#)

screen

login, using HTTPS [1-17](#)

SDRAM memory [13-9](#)

secure connection

*See also* tunnel

tunnel [6-1](#)

Secure Shell protocol *See* SSH

Secure Sockets Layer *See* SSL [12-18](#)

Security Associations (SAs) [6-2](#)

self-signed certificates

CA certificates [12-18](#)

SSL [12-18](#)

server identity certificates [12-36](#)

server key, SSH [8-13](#)

servers

backup, configuring [6-4](#)

backup, overview [6-4](#)

configuring system access [5-1](#)

remote, configuring [6-3](#)

session idle timeout

live event log overrides [13-6](#)

session key

SSH [8-13](#)

Session Timeout (error) [B-5](#)

severity level, events [9-3](#)

shutdown system [12-5](#)

Simple Network Management Protocol *See* SNMP

SNMP

configuring internal server [8-6](#)

enabling [8-6](#)

event trap destinations, configuring [9-12](#)

add [9-13](#)

modify [9-13](#)

MIB-II statistics [13-59](#)

port number [8-6](#)

traps, configuring "well-known" [9-8](#)

traps, configuring for specific events [9-11](#)

SNMP communities

adding [8-8](#)

configuring [8-7](#)

modifying [8-8](#)

software image

filenames [12-3, 13-9](#)

updating on VPN 3002

procedure [12-2](#)

stopping an image update [12-3](#)

version info [12-3, 13-9](#)

split tunneling

client (PAT) mode [11-3](#)

Network Extension mode [11-4](#)

SSH

configuring internal server [8-13](#)

enable [8-14](#)

enabling on public interface for XML support [8-16](#)

encryption algorithms [8-14](#)

host key [8-13](#)

port number [8-14](#)

RSA key [8-13](#)

server key [8-13](#)

server key regeneration [8-14](#)

session key [8-13](#)

statistics [13-35](#)

- SSH Host Key, generating [12-68](#)
- SSL
  - client authentication (HTTPS only) [8-11](#)
  - configuring internal server [8-10](#)
  - encryption algorithms [8-11](#)
  - statistics [13-31](#)
- SSL certificate [8-10, 12-18](#)
  - enrolling [12-40](#)
  - enrolling via SCEP [12-47](#)
  - exporting [12-66](#)
  - installing in browser [1-3](#)
  - installing with Internet Explorer [1-4](#)
  - installing with Netscape [1-9](#)
  - obtaining [12-31](#)
  - viewing with Internet Explorer [1-8](#)
  - viewing with Netscape [1-14](#)
  - VPN Concentrator [1-3](#)
- standards
  - IEEE standard 802.3, Ethernet networks [13-56](#)
  - ITU [12-56](#)
  - RFC 1650, Ethernet interface MIB objects [13-56](#)
  - RFC 1907, SNMP version 2 MIB objects [13-59](#)
  - RFC 2011, ARP table entries [13-54](#)
  - RFC 2011, IP and ICMP MIB objects [13-48, 13-51](#)
  - RFC 2012, TCP MIB objects [13-45](#)
  - RFC 2013, UDP MIB objects [13-45](#)
  - RFC 2459 [12-56](#)
  - X.509 [12-56](#)
  - X.520 [12-56](#)
- starting the CLI [14-2](#)
- static IP address [3-7](#)
- static routes
  - adding [7-3](#)
  - configuring for IP routing [7-2](#)
  - modifying [7-3](#)
- statistics
  - devices behind the VPN 3002 Hardware Client [13-17](#)
  - DHCP [13-33](#)
  - DNS [13-30](#)
  - HTTP [13-25](#)
  - IPSec [13-19](#)
  - MIB-II [13-42](#)
    - ARP table [13-54](#)
    - Ethernet [13-56](#)
    - ICMP [13-51](#)
    - interfaces [13-43](#)
    - IP traffic [13-48](#)
    - SNMP [13-59](#)
    - TCP/UDP [13-45](#)
  - monitoring [13-1, 13-18](#)
  - PPPoE [13-39](#)
  - public/private Ethernet interface [13-14](#)
  - SSH [13-35](#)
  - SSL [13-31](#)
  - Telnet [13-28](#)
  - user status [13-17](#)
- stopping
  - CLI [14-6](#)
  - file upload to VPN 3002 [12-3, 12-16](#)
  - the VPN 3002 [12-5](#)
- subordinate CA certificate [12-18](#)
- superuser *See* administrators
- swap configuration files [12-15](#)
- syslog format, events [9-6](#)
- syslog server
  - configuring for events
    - add [9-16](#)
    - modify [9-16](#)
    - port number [9-16](#)
- syslog servers, configuring for events [9-14](#)
- system configuration [4-1](#)
- system identification, configuring [10-2](#)
- system reboot [12-5](#)
  - reloads the boot configuration file [12-15](#)
  - saving the log file [12-5](#)
- system shutdown [12-5](#)
  - handling configuration files [12-6](#)
- system status

monitoring [13-8](#)  
 private/public interface [13-14](#)

---

## T

table of contents, Manager [1-26](#)  
 TCP/UDP MIB-II statistics [13-45](#)  
 Telnet  
   accessing CLI [14-2](#)  
   configuring internal server [8-4](#)  
   enabling [8-4](#)  
   port number [8-5](#)  
   statistics [13-28](#)  
 Telnet over SSL  
   configuring internal server [8-4](#)  
   port number [8-5](#)  
 time and date, configuring [10-3](#)  
 timeout, administrator [12-13](#)  
   live event log overrides [13-6](#)  
 time zone, configuring [10-3](#)  
 traceroute [12-9](#)  
 traffic management, configuring [11-1](#)  
 transmission mode, configuring Ethernet interface [3-5, 3-8](#)  
 traps, configuring  
   "well-known" [9-8](#)  
   destination systems [9-12, 9-13](#)  
   general events [9-8](#)  
   specific events [9-11](#)  
 troubleshooting  
   crash dump file [B-2](#)  
   event log [B-1](#)  
   files created for [B-1](#)  
   information in event log [9-4](#)  
   information in the event log [13-3](#)  
   using configuration files [B-2](#)  
 tunnel  
   configuring protocols [6-2](#)  
   endpoint [6-1](#)  
   functional description [6-1](#)

initiation [11-5](#)  
 protocols [6-1](#)  
 type (model number), system [13-9](#)

---

## U

UDP MIB-II traffic statistics [13-45](#)  
 updating software on VPN 3002 [12-2](#)  
 upload files to VPN 3002 [12-16](#)  
 user status [13-17](#)  
 using the CLI [14-3](#)  
 using the VPN Concentrator Manager [1-1](#)

---

## V

valid IKE proposals [A-1](#)  
 viewing  
   digital certificate details [12-56](#)  
   digital certificates on VPN 3002 [12-34](#)  
   enrollment request [12-69](#)  
   event log [13-5](#)  
   SSL certificates  
     with Internet Explorer [1-8](#)  
     with Netscape [1-14](#)  
   VPN 3002 status, sessions, statistics, and event logs [13-1](#)  
 VPN 3002 Hardware Client Manager  
   errors [B-5](#)  
   navigating [1-26](#)  
   organization [1-25](#)  
   window [1-22](#)  
 VPN Concentrator Manager  
   logging in [1-17](#)  
   using [1-1](#)

---

## W

WINS  
 backup server, configuring [6-4](#)

---

## X

### X.509

digital certificates [12-18](#)

standards [12-56](#)

### X.520 standards [12-56](#)

### XML

configuring [8-15](#)

enabling [8-16](#)

