User Guide for VPN Monitor

CiscoWorks

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

Customer Order Number:
Text Part Number: 78-14291-01

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.

User Guide for VPN Monitor

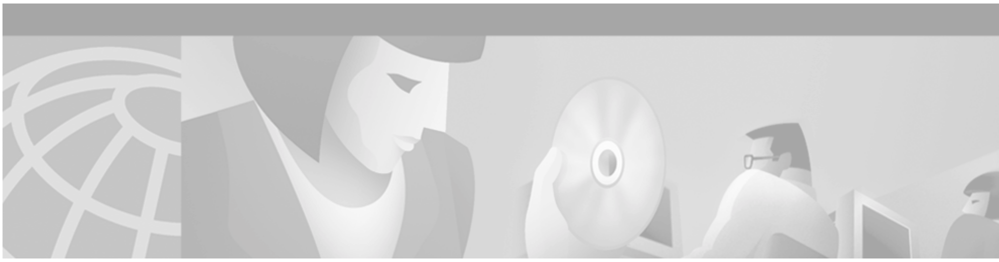
CONTENTS

CHAPTER 2

CHAPTER 3

APPENDIX A

INDEX



Preface

This manual describes VPN Monitor and provides instructions for configuring and using it. Understanding the following topics will help you get the most out of VPN Monitor and its documentation:

Audience

This guide is intended for users or prospective users of the CiscoWorks VPN Monitor product. Users should be familiar with basic and Virtual Private Network (VPN) related concepts and terminology used in internetworking. Those who are unfamiliar with VPN-related concepts should read Appendix A, "VPN Concepts."

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item	**Option** > **Network Preferences**

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

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

The following additional documentation is available:

Printed Documentation

- *Release Notes for VPN Monitor 1.2 on Windows 2000 and Solaris*

Online Documentation

- Context-sensitive online help

  You can access the help in two ways:

  - Select an option from the navigation tree, then click **Help.**
  - Click the Help button in the dialog box.

- PDF for:

  - *Installation Guide for VPN Monitor on Windows 2000 and Solaris*
  - *User Guide for VPN Monitor*

Note To read the PDF files, you must have Adobe Acrobat Reader 4.0 installed.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

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

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

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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

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

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

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

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

Overview

The CiscoWorks VPN Monitor application provides a web-based interface for monitoring and troubleshooting enterprise Virtual Private Networks (VPNs).

These topics will help you better understand VPN Monitor:

- Understanding VPN Monitor Features
- Navigating in VPN Monitor
- Locating VPN Monitor Help

Understanding VPN Monitor Features

VPN Monitor features are listed in Table 1-1.

Table 1-1 VPN Monitor Features

Feature	Description
Dashboard	
Status and Performance Monitoring	Shows the status of many aspects of your devices, including IPSec, L2TP, and PPTP tunnels, resource usage, and failures.
Threshold Events	Allows you to define warning and alert thresholds for devices on the Dashboard. When thresholds are exceeded, visual indication is shown on the Dashboard and/or events are logged in a database.

Table 1-1 VPN Monitor Features (continued)

Feature	Description
Graphing	Allows you to graph up to 10 data items for a single device, showing comparisons over time.
Protocols	
IPSec/IKE Support	Presents information about both key and data management tunnels.
Layer 2 Support on Cisco VPN concentrators	Presents information about L2TP and PPTP sessions and tunnels.
Multiple User Support	Allows multiple users to view graphs and tables from the same database records.
Secure Socket Layer (SSL) Support	Provides the capability to connect to the Cisco IOS HTTPS server securely.

Navigating in VPN Monitor

To navigate in VPN Monitor, you must first log into the CiscoWorks Server desktop. You can then select the VPN/Security Management Solution drawer to gain access to the VPN Monitor functions.

These topics help you log into the CiscoWorks Server desktop and navigate in VPN Monitor:

- Logging into the CiscoWorks Server Desktop
- Navigating in the VPN/Security Management Solution Drawer
- Navigating in the Monitoring Center Folder
- Navigating in the Administration Folder
- Understanding VPN Monitor Icons and Screen Elements

Logging into the CiscoWorks Server Desktop

The CiscoWorks Server desktop (Figure 1-1) is the interface for CiscoWorks network management applications, including VPN Monitor.

CiscoWorks Server provides secure access between the client browser and management server and also between the management server and devices. CiscoWorks Server uses Secure Socket Layer (SSL) encryption to provide secure access between the client browser and management server, and Secure Shell (SSH) to provide secure access between the management server and devices.

You can enable or disable SSL from the CiscoWorks desktop, depending on whether you want to use secure access between the client browser and the management server. To use the secure access features provided in CiscoWorks Server, you must have the security certificate files on your computer. You can either generate self-signed certificates from CiscoWorks Server desktop or obtain certificates from other agencies and use them to enable SSL in CiscoWorks Server. See *Getting Started with the CiscoWorks Server* for details.

Note You must have administrative privileges in CiscoWorks to enable and disable SSL and to manage the security certificates.

Before logging in, make sure that your browser is configured correctly for CiscoWorks. See *Installation and Setup Guide for CD One on Windows 2000* or *Installation and Setup Guide for CD One on Solaris* for details.

If you have installed the CiscoWorks package and are logging in for the first time, you can use the reserved “admin” user name and password.

Step 1 Access the CiscoWorks Server from your web browser, by entering *one* of the following:

- **http://**<*qualified domain name of the server*>**:1741**
- **http://**<*IP address of the server*>**:1741**

If you have enabled SSL in CiscoWorks, the login screen appears with a closed padlock security icon on the bottom status bar. See Figure 1-1.

If you have not enabled SSL in CiscoWorks, the login screen appears with an open padlock security icon.

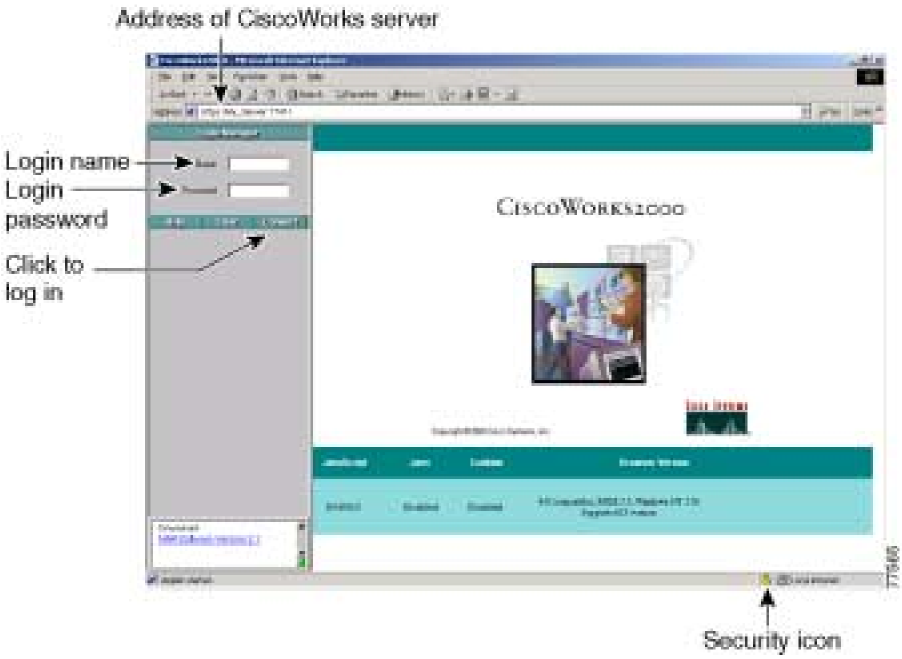
Step 2 Enter **admin** in both the Name and Password fields of the Login Manager. See Figure 1-1.

Step 3 Click **Connect** or press **Enter**. You are now logged in.

Step 4 Change the admin password using **Server Configuration** > **Setup** > **Security** > **Modify My Profile**.

For additional information about the CiscoWorks Server desktop, see *Getting Started with the CiscoWorks Server.*

Figure 1-1 CiscoWorks Login Screen



Caution When the system is installed initially, admin is the default password. To prevent all users from accessing privileged applications, change the password for admin immediately after installation.

Note Login sessions time out after two hours of inactivity. If the session is not used for two hours, you will be prompted to log in again.

Navigating in the VPN/Security Management Solution Drawer

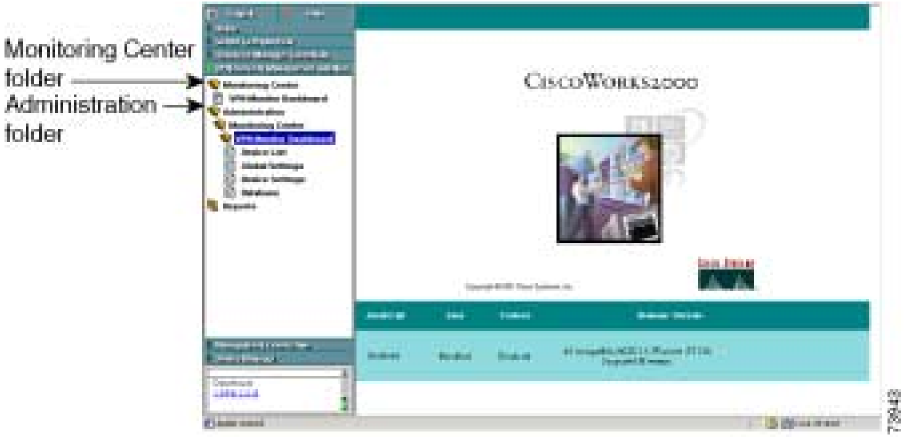
Depending on the installed applications, the CiscoWorks Server desktop contains several drawers. When the VPN/Security Management Solution bundle is installed, the VPN/Security Management Solution drawer appears in the left pane. See Figure 1-2 to view the contents of this drawer.

Step 1 Log into the CiscoWorks Server. The CiscoWorks Server desktop appears.

Step 2 From the navigation tree, select the **VPN/Security Management Solution** drawer. The Monitoring Center and Administration folders appear in the navigation tree.

The Monitoring Center folder provides access to the VPN Monitor Dashboard. The Administration folder allows users with administrative authorization to set and check settings for VPN Monitor.

Figure 1-2 VPN/Security Management Solution Drawer



Navigating in the Monitoring Center Folder

The Monitoring Center folder contains the VPN Monitor Dashboard file, which launches a dashboard for monitoring the devices you have selected. From the dashboard, you can monitor system, throughput, failure, and event log information.

Note If no devices are displayed on the dashboard, most likely it has not been configured. You must manually select devices to monitor before any information is polled and displayed on the dashboard. To do so, see the "Adding or Removing Dashboard Devices" section on page 3-1.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center**. The VPN Monitor Dashboard file is displayed.

Step 2 Click the **VPN Monitor Dashboard** file to open the dashboard. The dashboard contains System, Throughput, Failures, and Event Log tabs. See Table 1-2.

Step 3 Click a tab to display the corresponding dashboard information.

Table 1-2 Dashboard Options

Click This Tab	To Display This
System	General values polled from each device to assess device operations.
Throughput	IPSec and Layer 2 performance information. You can display this information about packets or octets by clicking the corresponding link above the Throughput table. (Packet information is displayed by default when you click the Throughput tab.)
Failures	Rates of various IPSec failures. You can display failure information about key management tunnels or data management tunnels by clicking the corresponding link above the table. (Key management tunnel information is displayed by default when you click the Failures tab.)
Event Log	Record of warnings and alerts when thresholds have been exceeded.

Navigating in the Administration Folder

If you have administrative access, you can use the Administration tasks in the Administration folder. The Administration folder allows you to set and view settings for the dashboard.

Step 1 From VPN/Security Management Solution drawer, select **Administration**. The Monitoring Center folder appears.

Step 2 Select **Monitoring Center.** The VPN Monitor Dashboard folder appears.

Step 3 Select **VPN Monitor Dashboard**. A list of files appear, as shown in Table 1-3.

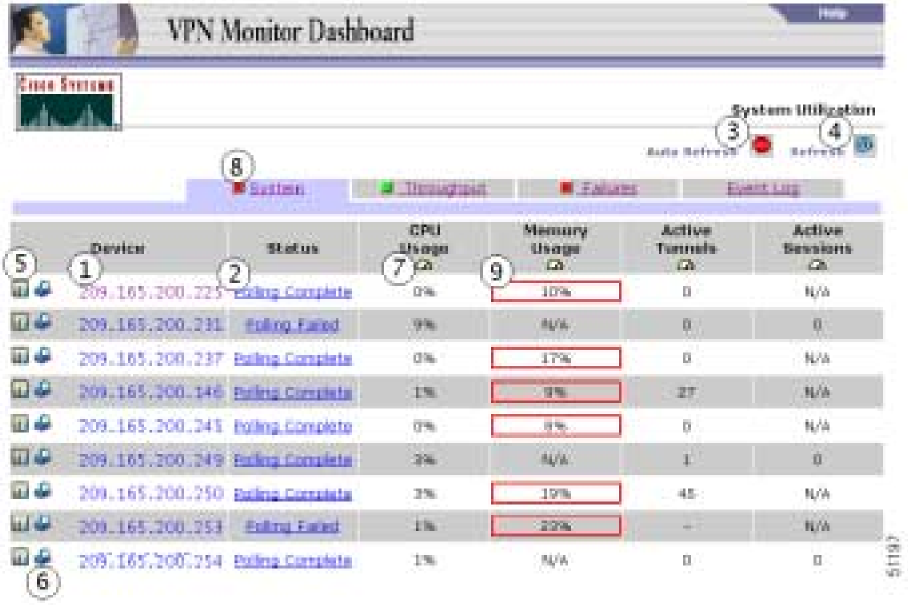
Table 1-3 Administration Files

Click This File	To Do This
Device List	Select devices to be monitored.
Global Settings	Set default polling interval and threshold values for all devices on the dashboard.
Device Settings	Set polling interval and threshold values for individual devices on the dashboard. These values override those defined in Global Settings.
Database	Configure the database data-retention policy and delete old polled data from the database.

Understanding VPN Monitor Icons and Screen Elements

Figure 1-3 shows icons and other screen elements that are used frequently in VPN Monitor. See Table 1-4 for descriptions.

Figure 1-3 Dashboard With Screen Elements



Device	Status	CPU Usage	Memory Usage	Active Tunnels	Active Sessions
209.165.200.225	Polling Complete	0%	10%	0	N/A
209.165.200.231	Polling Failed	9%	N/A	0	0
209.165.200.237	Polling Complete	0%	17%	0	N/A
209.165.200.246	Polling Complete	1%	9%	27	N/A
209.165.200.245	Polling Complete	0%	8%	0	N/A
209.165.200.249	Polling Complete	3%	N/A	1	0
209.165.200.250	Polling Complete	3%	19%	45	N/A
209.165.200.253	Polling Failed	1%	22%	--	N/A
209.165.200.254	Polling Complete	1%	N/A	0	0

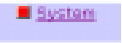
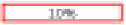
Table 1-4 VPN Monitor Icons and Screen Elements

Figure 1-3 Reference	Icons and Screen Elements	Description
1	Underlined IP address or device name (link) 172.20.99.130	Opens Device Center for the specified device, which allows you to: • Check management station-to-device connectivity. • Trace the route between the management station and the device to understand why pings fail or applications time out. • Ping the device to view packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds. • Look up a device or host to check its information via the name server. • Launch CiscoView to manage a specified device. • Display inventory information about the system, chassis, chassis cards, IOS image, flash devices, and memory pool for specified device.
2	Underlined field value (link) Polling Complete	Opens window with additional information about the item.

Table 1-4 VPN Monitor Icons and Screen Elements (continued)

Figure 1-3 Reference	Icons and Screen Elements	Description
3	⇧ ⛔	Auto Refresh (on and off). By default, device data displayed is automatically updated at an interval equal to the shortest device polling interval. Selecting the green Auto Refresh icon turns off this automatic refresh feature. Selecting the red Auto Refresh icon turns on the auto refresh feature.
4	↻	Refresh. Displays most recent polled data.
5	📊	Graph device. Opens dialog box to select items to graph and graph period and then generates the graph for a device.
6	🔍	Open tunnel list. Opens window showing the tunnel list for a device.
7	◠	View gauges. Opens window showing gauges for the corresponding column of values.

Table 1-4 VPN Monitor Icons and Screen Elements (continued)

Figure 1-3 Reference	Icons and Screen Elements	Description
8	Status box on tab  System	Threshold violation. Indicates whether any field data has reached or surpassed the thresholds set in the Global Settings and Device Settings dialog boxes in the Administration folder. The tab color represents the most significant threshold level that was exceeded. The box colors are: • Green. No Warning or Alert thresholds exceeded. • Yellow. One or more Warning thresholds exceeded. • Red. One or more Alert thresholds exceeded.
9	Field data boxed in yellow or red  10%	Threshold violation. Indicates field data that has reached or surpassed the thresholds set in the Global Settings or Device Settings dialog boxes. The box colors are: • No color. Data does not equal or exceed the Warning or Alert thresholds. • Yellow. Data equals or exceeds the Warning threshold, but does not equal the Alert threshold. • Red. Data equals or exceeds the Alert threshold.

Locating VPN Monitor Help

You can access online help from the CiscoWorks Server desktop or from the VPN Monitor dialog boxes.

Accessing Help from CiscoWorks Server Desktop

Step 1 Log into the CiscoWorks Server desktop.

Step 2 Click **Help** at the top of the navigation tree. CiscoWorks online help opens.

Step 3 Double-click **VPN/Security Management Solution** from the list of books in the Contents pane.

Step 4 Click **VPN Monitor**. The VPN Monitor online help is displayed.

Accessing Help from VPN Monitor Dialog Boxes

You can access online help from a specific VPN Monitor dialog box by clicking the **Help** button located at the top right corner of the dialog box. This level of help provides details about the specific dialog box.

CHAPTER 2

Dashboard

These topics help you use the VPN Monitor Dashboard to gather and display information about VPN devices and tunnels in your network:

- Displaying System Information
- Displaying Throughput Information
- Displaying Failures
- Displaying Event Log Information
- Graphing System, Throughput, and Failure Information
- Displaying Tunnel Lists
- Using the Device Center

The Dashboard displays polled information about only those devices you previously configured to be included on the Dashboard. See "Adding or Removing Dashboard Devices" section on page 3-1 for more information.

Displaying System Information

You can display operations information for devices.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System Table displayed. See Table 2-1 for information about the table.

Table 2-1 System Table

Column	Description[1]
Device	IP address or name of device. Click IP address or name to launch Device Center for device. See "Using the Device Center" section on page 2-22 for more information.
Status	Poller state: • Polling Not Started. Poller is adding a device to the polling list. • Polling Stopped. Poller is removing a device from the polling list. • Polling Completed. Poller has accessed the device and collected all data. • Polling Failed. Poller could not retrieve all information from the device; therefore some device data might be unavailable. Click poll status to view details about: • Last Poll. Most recent date and time data was requested from the device. • Last Poll Status. Indication of whether or not all data was retrieved. • Next Poll. Date and time of next scheduled poll. • Poll Interval. Number of seconds between each poll.
CPU Usage	Percentage of CPU use compared to total capacity.
Memory Usage[2]	Percentage of memory use compared to total capacity.

Table 2-1 System Table (continued)

Column	Description[1]
Active Tunnels	Total number of existing tunnels: • Cisco VPN concentrators. Includes IPSec, L2TP, and PPTP tunnels. • Cisco VPN routers. Includes IPSec tunnels only.
Active Sessions	Total number of active sessions. See "Sessions" section on page A-6 for more information.
📊	Click to launch Graph dialog box. See "Graphing System, Throughput, and Failure Information" section on page 2-19 for information about graphs.
🔍	Click to launch Device Tunnel List dialog box. See "Displaying Tunnel Lists" section on page 2-20 for information about tunnel lists.

[1] N/A means that the information has not been polled for the device either because polling has not yet occurred or the data is not applicable to the device. A dash (-) field entry means that information for the field could not be retrieved.

[2] Applies only to Cisco VPN routers.

Tips

- The box color on the System tab indicates whether any field data has reached or surpassed the thresholds set in the Global Settings or Device Settings task in the Administration folder. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9 or "Configuring Warnings, Alerts, and Event Logging" section on page 3-2.
- Field data that has reached or surpassed the thresholds set in the Global Settings or Device Settings page in the Administration folder is highlighted with a yellow or red box, indicating the level of the exceeded threshold. See the "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Click the Gauge icon to display gauges showing information for the corresponding column of data for all devices on the Dashboard.

- Auto Refresh is enabled by default. Click the Auto Refresh icon to start or stop automatic updating of information displayed on the Dashboard. The Auto Refresh Stop icon is displayed when auto refreshing is running; clicking the icon stops automatic refreshing. The Auto Refresh Start icon is displayed when auto refreshing is not running; clicking the icon starts automatic updating.
- Click **Refresh** to update the displayed information immediately.

Displaying Throughput Information

You can display current and long-term throughput information by packets or octets for each device on the VPN Monitor Dashboard.

Displaying Packet Throughput

You can display packet throughput for all devices on the VPN Monitor Dashboard.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed.

Step 2 Click the Throughput tab. The Throughput table appears with packet information displayed.

See Table 2-2 for information about the table.

Table 2-2 Packet Throughput Table

Field	Description
Device	IP address or name of device. Click IP address or name to launch Device Center. See "Using the Device Center" section on page 2-22 for more information.
Current Packet Rate - IPSec - In	Rate per second at which IPSec packets were received during the last polling period.
Current Packet Rate - IPSec - Out	Rate per second at which IPSec packets were sent during the last polling period.
Current Packet Rate - Layer 2 - In[1]	Rate per second at which L2TP or PPTP packets were received during the last polling period.
Current Packet Rate - Layer 2 - Out[1]	Rate per second at which L2TP or PPTP packets were sent during the last polling period.
Long-term Packet Rate - IPSec - In	Rate per second at which IPSec packets were received since device started.
Long-term Packet Rate - IPSec - Out	Rate per second at which IPSec packets were sent since device started.
Long-term Packet Rate - Layer 2 - In[1]	Rate per second at which L2TP or PPTP packets were received since device started.
Long-term Packet Rate - Layer 2 - Out[1]	Rate per second at which L2TP or PPTP packets were sent since device started.
In Drops	Percentage of incoming packets that were dropped since device started.
Out Drops	Percentage of outgoing packets that were dropped since device started.

Table 2-2 Packet Throughput Table (continued)

Field	Description
📊	Click graph icon to launch Graph dialog box. See "Graphing System, Throughput, and Failure Information" section on page 2-19 for more information about graphs.
🔍	Click device monitor icon to launch Device Tunnel List dialog box. See "Displaying Tunnel Lists" section on page 2-20 for more information about tunnel lists.

[1] No data available for Cisco VPN routers (displayed as N/A).

Tips

- The color of the box on the Throughput tab indicates whether any field data has reached or surpassed the thresholds set in the Global Settings or Device Settings task in the Administration folder. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Field data that has reached or surpassed the thresholds set in the Global Settings or Device Settings task in the Administration folder is highlighted with a yellow or red box, indicating the level of the exceeded threshold. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Current rates are calculated using values obtained at the current poll and the previous poll; therefore, the first time you poll a device, the Dashboard will not show any rate data (displayed as N/A).
- Long-term rates are calculated using data that has been collected since the device started.
- Click the Gauge icon to display gauges showing information for the corresponding column of data for all devices on the Dashboard.

Displaying Octet Throughput

You can display octet throughput for all devices on the VPN Monitor Dashboard.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed.

Step 2 Click the Throughput tab. The Throughput table appears.

Step 3 Click the Octet link above the table.

See Table 2-3 for information about the table.

Table 2-3 Octet Throughput Table

Field	Description
Device	IP address or name of device. Click IP address or name to launch Device Center for device. See “Using the Device Center” section on page 2-22 for more information.
Current Octet Rate - IPSec - In	Rate per second at which IPSec octets were received during the last polling period.
Current Octet Rate - IPSec - Out	Rate per second at which IPSec octets were sent during the last polling period.
Current Octet Rate - Layer 2 - In[1]	Rate per second at which L2TP or PPTP octets were received during the last polling period.
Current Octet Rate - Layer 2 - Out[1]	Rate per second at which L2TP or PPTP octets were sent during the last polling period.
Long-term Octet Rate - IPSec - In	Rate per second at which IPSec octets were received since the device started.

Table 2-3 Octet Throughput Table (continued)

Field	Description
Long-term Octet Rate - IPSec - Out	Rate per second at which IPSec octets were sent since the device started.
Long-term Octet Rate - Layer 2 - In[1]	Rate per second at which L2TP or PPTP octets were received since the device started.
Long-term Octet Rate - Layer 2 - Out[1]	Rate per second at which L2TP or PPTP octets were sent since the device started.
📊	Click to launch Graph dialog box. See "Graphing System, Throughput, and Failure Information" section on page 2-19 for more information about graphs.
🔍	Click to launch Device Tunnel List dialog box. See "Displaying Tunnel Lists" section on page 2-20 for more information about tunnel lists.

[1] No data available for Cisco VPN routers (displayed as N/A). This counter restarts at zero when the maximum number of octets (4294967295) is reached.

Tips

- The color of the box on the Throughput tab indicates whether any field data has reached or surpassed the thresholds set in the Global Settings task in the Administration folder. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Field data that has reached or surpassed the thresholds set in the Global Settings task in the Administration folder is highlighted with a yellow or red box, indicating the level of the exceeded threshold. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Current rates are calculated using values obtained at the current poll and the previous poll; therefore, the first time you poll a device, the Dashboard does not show any rate data (displayed as N/A).

- Long-term rates are calculated using data that has been collected since the device started.
- Click the Gauge icon to display gauges showing information for the corresponding column of data for all devices on the Dashboard.

Displaying Failures

You can display IPSec failures for key management tunnels and data management tunnels.

Displaying Key Management Tunnel Failures

You can display IPSec key management tunnel failures.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed.

Step 2 Click the Failures tab. The Failures table appears with the Key Management tunnel failures displayed.

See Table 2-4 for information about the table.

Table 2-4 Key Management Tunnel Failures Table

Field	Description
Device	IP address or name of device. Click IP address or name to launch Device Center for device. See "Using the Device Center" section on page 2-22 for more information.
IKE Failures	Percentage of times connection attempts to the device have failed because an IKE Security Association (SA) does not activate. These failures could occur due to: • Misconfiguration • Mistyping of the password • Attempted intrusion Investigate this issue using Syslog Analysis reports. If the Syslog Analysis reports do not indicate any of the above reasons, then most likely the failure is due to a known bug, CSCdw71601, with the VPN Concentrator. To resolve this, increase the IKE Failures threshold.
IKE Auth Failures	Percentage of IKE authentication failures. These packet level failures impact the speed with which VPN connection between two devices is established. These failures could occur due to: • Malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator. • Large number of corrupted IKE packets due to errors on the communication link. To resolve this, contact your system administrator.

Table 2-4 Key Management Tunnel Failures Table (continued)

Field	Description
IKE Decrypt Failures	Percentage of IKE decryption failures. These packet level failures impact the speed with which VPN connection between two devices is established. When this threshold reaches or surpasses the set values (box turns yellow or red), it might indicate a malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator.
Hash Failures	Percentage of hash failures. These packet level failures impact the speed with which VPN connection between two devices is established. When this threshold reaches or surpasses the set values (box turns yellow or red), it might indicate a malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator.
IKE No SA	Percentage of IKE No Security Association (SA) failures. When a monitored device reboots, the IPSec No SAs and IKE No SAs threshold for that device reaches or surpasses the set values (box turns yellow or red). This is because a remote device continues to try to communicate with the rebooted device using the previously agreed upon parameters, which the rebooted device no longer recognizes. If the monitored device has *not* been rebooted, and the IPSec No SAs and IKE No SAs threshold for that device have exceeded, then it indicates a potential security violation. Investigate the issue using Syslog Analysis reports.

Table 2-4 Key Management Tunnel Failures Table (continued)

Field	Description
📊	Click to launch Graph dialog box. See "Graphing System, Throughput, and Failure Information" section on page 2-19 for more information about graphs.
🔍	Click to launch Device Tunnel List dialog box. See "Displaying Tunnel Lists" section on page 2-20 for more information about tunnel lists.

Tips

- The color of the box on the Failures tab indicates whether any field data has reached or surpassed the thresholds set in the Global Settings or Device Settings page in the Administration folder. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Field data that has reached or surpassed the thresholds set in the Global Settings or Device Settings page in the Administration folder is highlighted with a yellow or red box, indicating the level of the exceeded threshold. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Click the Gauge icon to display gauges showing information for the corresponding column of data for all devices on the Dashboard.

Displaying Data Management Tunnel Failures

You can display IPSec data management tunnel failures.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed by default.

Step 2 Click the Failures tab. The Failures table appears with the Key Management tunnel failures displayed by default.

Step 3 Click the Data Management link above the Failures table.

See Table 2-5 for information about the table.

Table 2-5 Data Management Tunnel Failures Table

Field	Description
Device	IP address or name of device. Click IP address or name to launch Device Center for device. See "Using the Device Center" section on page 2-22 for more information.
IPSec Auth Failures - In	Percentage of inbound packets that were dropped due to IPSec authentication failures. These packet level failures impact the effective data throughput experienced by the user after connection to the device has been established. When this threshold reaches or surpasses the set values (box turns yellow or red), it might indicate a malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator.
IPSec Auth Failures - Out	Percentage of outbound packets that were dropped due to a failure in creating the message authentication code (MAC). These packet level failures impact the effective data throughput experienced by the user after connection to the device has been established. When this threshold reaches or surpasses the set values (box turns yellow or red), it might indicate a malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator.

Table 2-5 Data Management Tunnel Failures Table (continued)

Field	Description
IPSec Decrypt Failures	Percentage of packets that were dropped due to IPSec decryption failures. These packet level failures impact the effective data throughput experienced by the user after connection to the device has been established. When this threshold reaches or surpasses the set values (box turns yellow or red), it might indicate a malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator.
IPSec Encrypt Failures	Percentage of packets that were dropped due to IPSec encryption failures. These packet level failures impact the effective data throughput experienced by the user after connection to the device has been established. When this threshold reaches or surpasses the set values (box turns yellow or red), it might indicate a malfunctioning in the crypto accelerator. To resolve this, replace or upgrade the crypto accelerator.
IPSec Proposals - Invalid	Percentage of invalid IPSec proposals. When this threshold reaches or surpasses the set values (box turns yellow or red), it indicates either the hub or the remote device has been misconfigured, which results in connectivity failure. To resolve this, using IPsec Flow Monitor MIB or Syslog Analysis reports, identify which remote device is failing to connect and fix the configuration.

Table 2-5 Data Management Tunnel Failures Table (continued)

Field	Description
IPSec Proposals - Rejects	Percentage of rejected IPSec proposals. When this threshold reaches or surpasses the set values (box turns yellow or red), it indicates either the hub or the remote device has been misconfigured, which results in connectivity failure. To resolve this, using IPsec Flow Monitor MIB or Syslog Analysis reports, identify which remote device is failing to connect and fix the configuration.
Replay - All	Total number of packets replayed since device started. When this threshold reaches or surpasses the set values (box turns yellow or red), it indicates a potential security violation. To resolve this, investigate the issue using Syslog Analysis reports. For more information see the Essentials user guide.
Replay - 24hrs	Total number of packets replayed that occurred over approximately the past 24 hours. This field shows N/A if the device started *more* than 24 hours ago, but polling of the device started *less* than 24 hours ago. When this threshold reaches or surpasses the set values (box turns yellow or red), it indicates a potential security violation. To resolve this, investigate the issue using Syslog Analysis reports. For more information see the Essentials user guide.

Table 2-5 Data Management Tunnel Failures Table (continued)

Field	Description
IPSec No SA	Percentage of IPSec No Security Association (SA) failures. When a monitored device reboots, the IPSec No SAs and IKE No SAs threshold for that device reaches or surpasses the set values (box turns yellow or red). This is because a remote device continues to try to communicate with the rebooted device using the previously agreed upon parameters, which the rebooted device no longer recognizes. If the monitored device has *not* been rebooted, and the IPSec No SAs and IKE No SAs values for that device have exceeded, then it indicates a potential security violation. Investigate the issue using Syslog Analysis reports.
📊	Click to launch Graph dialog box. See "Graphing System, Throughput, and Failure Information" section on page 2-19 for more information about graphs.
🔍	Click to launch Device Tunnel List dialog box. See "Displaying Tunnel Lists" section on page 2-20 for more information about tunnel lists.

Tips

- The color of the box on the Failures tab indicates whether any field data has reached or surpassed the thresholds set in the Global Settings or Device Settings page in the Administration folder. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
- Field data that has reached or surpassed the thresholds set in the Global Settings or Device Settings page in the Administration folder is highlighted with a yellow or red box, indicating the level of the exceeded threshold. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.

- Click the Gauge icon to display gauges showing information for the corresponding column of data for all devices on the Dashboard.

Displaying Event Log Information

You can display information about threshold violations in the event log. Thresholds for these events are set in the Global Settings or Device Settings page in the Administration folder. See "Configuring Warnings, Alerts, and Event Logging" section on page 3-2.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center** > **VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed by default.

Step 2 Click the **Event Log** tab. The Event Log table appears.

See Table 2-6 for information about the table.

Step 3 To sort the Event Log table, click the **Configure Filter** tab. The Event Log Filter Settings dialog box appears.

Step 4 Fill in the appropriate fields and click **Submit**. The Event Log table re-appears, sorted according to the provided specifications.

Table 2-6 Event Log Table

Field	Description
Device	IP address or name of device. Click IP address or name to launch Device Center for device. See "Using the Device Center" section on page 2-22 for more information.
Severity	Severity of event: • Warning (yellow) or Alert (red) indicates thresholds that were reached or exceeded. • Normal (green) indicates warning and alert thresholds are no longer being exceeded. See "Understanding VPN Monitor Icons and Screen Elements" section on page 1-9.
Description	Short description of event: • Severity. Normal, Warning, or Alert. • Device. IP address or name of device on which event occurred. • Event detail. Description of event, threshold setting, and value of threshold violation.
Time	Date and time event occurred.
📊	Click to launch Graph dialog box. See "Graphing System, Throughput, and Failure Information" section on page 2-19 for more information about graphs.
🔍	Click to launch Device Tunnel List dialog box. See "Displaying Tunnel Lists" section on page 2-20 for more information about tunnel lists.

Tips

- Click **Next** to display additional events.
- Click **Previous** to display preceding events.

Graphing System, Throughput, and Failure Information

You can graph any combination of the following types of data:

- System operations statistics
- Packet and octet throughput
- Key management and data management failures

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed by default.

Step 2 From any dashboard table accessible from the System, Throughput, Failures, and Event Log tabs, click the graph icon. The VPN Monitor Dashboard - Graph Data and Time Period Selection dialog box opens.

Step 3 Select the check box next to the data items to include in the graph. You can include up to 10 data items from any or all categories.

The selections correspond to the data available in the System, Throughput, and Failures Dashboard tables:

- For System, see Table 2-1 on page 2-2.
- For Throughput Packets, see Table 2-2 on page 2-5.
- For Throughput Octets, see Table 2-3 on page 2-7.
- For Failures Key Mgmt, see Table 2-4 on page 2-10.
- For Failures Data Mgmt, see Table 2-5 on page 2-13.

Step 4 In the **Graph the last** field, enter a number from 1-721 (hours), 1-31 (days), or 1-4 (weeks) then click the next field to select hours, days, or weeks from the drop-down list. For example, if you enter 12 and select Hours, VPN Monitor generates a graph containing data collected during the last 12 hours.

Step 5 Click **Submit**. VPN Monitor generates the graph.

Tips

- From the Graph dialog box, click **Print** to print the generated graph.
- From the Graph dialog box, click **Close** to exit the dialog box without generating a graph.
- From the Graph dialog box, click **Back** to return to the VPN Monitor Dashboard - Graph Data and Time Period Selection dialog box.
- When multiple data items are displayed on the same graph and at least one item has a very large value, data items with smaller values might be difficult to discern. To see the detail for the smaller value data items, generate the graph for only those items.

Displaying Tunnel Lists

You can display tunnel details for particular devices.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected and the System table displayed by default.

Step 2 From any Dashboard table accessible from the System, Throughput, Failures, and Event Log tabs, click the Tunnel List icon. The Tunnel List dialog box opens.

See Table 2-7 for information about the table.

Table 2-7 Tunnel List Table

Field	Description
Tunnel Type	Tunnel type, either LAN-to-LAN or Remote Access.
Remote Endpoint	IP address of device at remote end.
Local Network[1]	Network identifier of local end.
Remote Network[1]	Network identifier of remote end.
User Name[2]	Name of session user.
Connect Time	Number of days, hours, and minutes that tunnel has been connected and running.
Packets In[1]	Number of IPSec packets received.
Packets Out[1]	Number of IPSec packets sent.
Octets In[3]	Number of IPSec or Layer 2 octets received.
Octets Out[3]	Number of IPSec or Layer 2 octets sent.

[1] Applies only to IPSec.

[2] Applies only to remote access VPNs terminating on Cisco VPN concentrators.

[3] The Layer 2 counter restarts at zero when the maximum number of octets (4294967295) is reached.

Tips

- Click a column heading to sort the table in ascending or descending order according to the data in the column. For example, to sort the table by IP addresses in the local network, click the Local Network column heading. The entries are sorted and displayed in ascending order. Click the Local Network column again, and the entries are sorted and displayed in descending order.
- Click **Refresh** to display the most recently polled data.

- In some concentrator configurations, a single remote-access session might be set up using two distinct tunnels:
  - one from the public interface of the concentrator to the remote client
  - another from the private interface of the concentrator to the remote client

  In these cases, VPN Monitor displays two distinct tunnels corresponding to each remote-access session.

Using the Device Center

You can access the Device Center to view information for a particular device.

Step 1 From the VPN/Security Management Solution drawer, select **Monitoring Center > VPN Monitor Dashboard**. The VPN Monitor Dashboard opens with the System tab selected by default and the System table displayed.

Step 2 From any Dashboard table accessible from the System, Throughput, Failures, and Event Log tabs, click the IP address link in the Device column. The Device Center dialog box opens.

For information about using and understanding the Device Center, start the applications in the Device Center, then click **Help** for the online help.

Tips

- Click **Back** to return to VPN Monitor.
- Click **Close** to close the dialog box.

CHAPTER 3

Dashboard Settings

These topics help you can add and remove devices from the Dashboard, specify warning and alert thresholds, and manage polled data:

- Adding or Removing Dashboard Devices
- Configuring Warnings, Alerts, and Event Logging
- Configuring Database Settings

Adding or Removing Dashboard Devices

Cisco-supported VPN devices within your VPN network are listed in the Available Devices column. You need to configure VPN Monitor to poll and display information about specific devices on the Dashboard.

Before you can use VPN Monitor, you must select the devices to monitor and add them to the device dashboard.

Note You can monitor a maximum of 30 devices at once.

Step 1 Select **VPN/Security Management Solution** > **Administration** > **Monitoring Center** > **VPN Monitor Dashboard** > **Device List**.

The Device List window opens.

Step 2 Select a device from Available Devices, then click **Add**.

The device is added to Dashboard Devices. Monitoring of the device starts immediately.

Step 3 To remove a device from the dashboard, select the device from Dashboard Devices, then click **Remove**. The device is removed from Dashboard Devices and returned to Available Devices.

Tip

- You can add devices that do not appear in the Available Devices column. See Appendix B, "Why doesn't my device appear in the Available Devices List?"

Configuring Warnings, Alerts, and Event Logging

You can configure warnings, alerts, event logging, and polling for all devices using Global Settings and for individual devices using Device Settings.

Configuring Global Settings

You can set polling intervals, thresholds, and event logging for all devices.

Step 1 From the VPN/Security Management Solution drawer, select **Administration** > **Monitoring Center** > **VPN Monitor Dashboard** > **Global Settings**. The Global Threshold Settings dialog box opens.

Step 2 In the **Polling Interval** field, click the drop-down list box to select the time interval between polls.

Step 3 For each item to monitor for threshold violations, enter a number in the Threshold field for Warnings or Alerts. The items correspond to the data displayed in the System, Throughput, and Failures Dashboard tables. See "Understanding Threshold Settings" section on page 3-4 for descriptions of the items in the table.

Step 4 To record the occurrence of a threshold violation in the Event log, select the check box in the Log column corresponding to the desired item.

Step 5 Click **Save**.

Tips

- You can set as many (all) or as few thresholds as would be helpful to you.
- Click **Defaults** to replace the current threshold settings with the factory default settings. Click **Save** to save the default settings.
- Click **Refresh** to replace the displayed threshold settings with the settings last saved.
- Modified settings are not saved and used until you click **Save**.

Configuring Device Settings

You can set specific polling intervals, thresholds, and event logging for individual devices.

Step 1 From the VPN/Security Management Solution drawer, select **Administration** > **Monitoring Center** > **VPN Monitor Dashboard** > **Device Settings**. The Device Settings dialog box opens. For descriptions of the fields, see Table 3-1.

Step 2 In the Select Device column, click the device settings icon corresponding to the desired device. The Device Polling and Threshold Settings dialog box for that device opens.

Step 3 In the **Polling Interval** field, click the drop-down list box to select the time interval between polls. This field defines how often new data is retrieved from the device. To use the polling interval from the global settings, select the **Use Global Polling Interval** check box.

Step 4 To use the same thresholds as those set for the global settings, select the **Use All Global Threshold Settings** check box. To use threshold settings you have configured for the specific device, leave the **Use All Global Threshold Settings** check box blank.

Step 5 For each item you want to monitor threshold violations, enter a number in the Threshold field for Warnings or Alerts. The items correspond to the data displayed in the System, Throughput, and Failures Dashboard tables. See "Understanding Threshold Settings" section on page 3-4 for descriptions of the items in the table.

Step 6 To record the occurrence of the threshold violation in the Event log, click the box in the Log column corresponding to the desired item.

Step 7 Click **Save**.

Table 3-1 Device Settings Selection Dialog Box

Field	Description
Select Device	Click to set thresholds for a specific device.
Device Name	IP address or name of device. Click to launch Device Center.
Device Type	Type of device. Valid types are: • Unknown (could not be determined) • Router (Cisco VPN router) • Concentrator (Cisco VPN concentrator)

Understanding Threshold Settings

The Global Polling and Threshold Settings dialog box and the Device Polling and Threshold Settings dialog box are similar. Both allow you to configure warning and alarm thresholds, logging of specific threshold violations in the event log, and polling intervals. However, the Global Polling and Threshold Settings dialog box applies to *all* devices, whereas the Device Polling and Threshold dialog box applies to a *single* device. See "Configuring Global Settings" section on page 3-2 for the steps to configure these settings. See "Configuring Device Settings" section on page 3-3 for the steps to configure these settings.

See Table 3-2 for descriptions of the items in the dialog box.

Table 3-2 Device Polling and Threshold Settings

Field	Description
Device[1]	IP address or name of device.
Polling Interval	Click drop-down list box to select interval between polls.
Use Global Polling Interval[1]	Select check box to use the same polling interval as the one set for global settings.
Use All Global Threshold Settings[1]	Select check box to use same thresholds as those set for global settings.
System	
CPU Usage	Percentage of CPU in use compared to total capacity.
Memory Usage[2]	Percentage of memory in use compared to total capacity.
Active Tunnels	Total number of existing tunnels: • Cisco VPN concentrators. Includes IPSec, L2TP, and PPTP tunnels. • Cisco VPN routers. Includes IPSec tunnels only.
Active Sessions[3]	Total number of active sessions. See "Sessions" section on page A-6 for more information.
Throughput	
Current IPSec Packet Rate (In)	Rate per second at which IPSec packets were received during the last polling period.
Current IPSec Packet Rate (Out)	Rate per second at which IPSec packets were sent during the last polling period.

Table 3-2 Device Polling and Threshold Settings (continued)

Current IPSec Octet Rate (In)	Rate per second at which IPSec octets were received during the last polling period.
Current IPSec Octet Rate (Out)	Rate per second at which IPSec octets were sent during the last polling period.
Long-Term IPSec Packet Rate (In)	Rate per second at which IPSec packets were received since device started.
Long-Term IPSec Packet Rate (Out)	Rate per second at which IPSec packets were sent since device started.
Long-Term IPSec Octet Rate (In)	Rate per second at which IPSec octets were received since device started.
Long-Term IPSec Octet Rate (Out)	Rate per second at which IPSec octets were sent since device started.
Current Layer 2 Packet Rate (In)[4]	Rate per second at which Layer 2 packets were received during the last polling period.
Current Layer 2 Packet Rate (Out)[4]	Rate per second at which Layer 2 packets were sent during the last polling period.
Current Layer 2 Octet Rate (In)[4]	Rate per second at which Layer 2 octets were received during the last polling period.
Current Layer 2 Octet Rate (Out)[4]	Rate per second at which Layer 2 octets were sent during the last polling period.
Long-Term Layer 2 Packet Rate (In)[4]	Rate per second at which Layer 2 packets were received since device started.
Long-Term Layer 2 Packet Rate (Out)[4]	Rate per second at which Layer 2 packets were sent since device started.
Long-Term Layer 2 Octet Rate (In)[4]	Rate per second at which Layer 2 octets were received since device started.
Long-Term Layer 2 Octet Rate (Out)[4]	Rate per second at which Layer 2 octets were sent since device started.

Table 3-2 Device Polling and Threshold Settings (continued)

IPSec Packets Dropped (In)	Percentage of incoming packets that were dropped since device started. This does not include packets dropped because replay was detected.
IPSec Packets Dropped (Out)	Percentage of outgoing packets that were dropped since device started.
Failures	
IKE Failures	Percentage of IKE phase 1 tunnels that failed to activate.
IKE Authorization Fails	Percentage of IKE authorization failures.
IKE Decryption Failures	Percentage of IKE decryption failures.
IKE Hash Failures	Percentage of hash failures.
IKE No Security Association	Percentage of IKE No SA failures.
IPSec Authorization Failures (In)	Percentage of inbound packets that were dropped due to IPSec authentication failures.
IPSec Authorization Failures (Out)	Percentage of outbound data management packets that were dropped because the message authentication code (MAC) could not be computed.
IPSec Decryption Failures	Percentage of packets that were dropped due to IPSec decryption failures.
IPSec Encryption Failures	Percentage of packets that were dropped due to IPSec encryption failures.
IPSec Invalid Proposals	Percentage of invalid IPSec proposals.
IPSec Rejected Proposals	Percentage of rejected IPSec proposals.
IPSec Replay Drops	Total number of replayed data management packets since device started.
IPSec Replay Drops Last 24 Hours	Total number of replayed data management packets that occurred during the last 24 hours.
IPSec No Security Association	Percentage of IPSec No SA failures.

[1] Applies to Device Settings dialog box only. Field is not present in Global Settings dialog box.

[2] Applies only to Cisco VPN routers.

[3] Applies only to Cisco VPN concentrators.

[4] Does not apply to Cisco VPN routers.

Tips

- Current rates are calculated using values obtained at the current poll and the previous poll; therefore, the first time you poll a device, the Dashboard will not show any rate data (displayed as N/A).
- Long-term rates are calculated using the device system up time.
- Setting a highly infrequent polling interval might not capture threshold violations that occurred between polls. You might need to adjust your polling interval to suit the current condition of your network.

Configuring Database Settings

You can manually delete polled and event log data from the database, or you can limit the number of days VPN Manager stores this data before automatically deleting it.

Step 1 From the VPN/Security Management Solution drawer, select **Administration** > **Monitoring Center** > **VPN Monitor Dashboard** > **Database**. The Delete Polling Data dialog box opens.

The **Starting date of polling data** field contains the date and time when polling started.

Step 2 You can manually or automatically delete polled and event log data:

- For manual deletion, enter a month, date, and year in the **Remove all polled and event data prior to** field, then click **Remove Entries**. Polled and event log data stored on or before the specified date is deleted.
- For automatic deletion, select a value (*n*) from the drop-down list in the **Automatically remove polled and event data more than *n* day(s) old** field, where *n* represents the age at which polled and event data is deleted, then click **Set Limit**.

Note You cannot change the value for automatic removal if that process is running.

After polling data is manually deleted, a new start date for the polling data appears in the **Starting date of polling data** field.

Tips

- Depending on the global or per device polling interval you set, polling and storing data can affect:
  - Memory and CPU usage on the devices being polled
  - Traffic throughput on the devices being polled
  - Disk space and memory use on the CiscoWorks Server

  The more frequent the polling rate, the greater the impact on the devices being polled, their ability to process network traffic, and the performance of the CiscoWorks Server. If you notice performance degradation, you can decrease the polling rates, reduce the number of days for which polled and event log data is stored, or both.
- You can delete entries manually at any time regardless of whether you have set a limit to store (and automatically delete) polled and event log data.

APPENDIX A

VPN Concepts

This appendix introduces Virtual Private Network (VPN) concepts as they apply to monitoring with VPN Monitor:

- Key Terms
- VPN Types
- VPN Components
- VPN Services
- IPSec Framework
- Layer 2 Protocols

Key Terms

Acronym	Term	Definition
3DES	Triple Data Encryption Standard	Provides strong data encryption. US only.
AH	Authentication Header	Provides basic data authentication.
CA	Certification Authority	Provides verification of device identity using digital certificates.
CBC	Cipher Block Chaining	Provides data encryption and authentication using AH and ESP.
DES	Data Encryption Standard	Provides a scheme to increase the strength of encryption.

Acronym	Term	Definition
DH	Diffie-Hellman Key Exchange	Provides a method that enables two devices to exchange keys securely over an insecure medium.
ESP	Encapsulating Security Protocol	Provides tunneling services for encryption and/or authentication.
HMAC	Keyed-Hashing for Message Authentication	Provides message authentication using hashes for encryption.
IETF	Internet Engineering Task Force	Task force responsible for developing Internet standards.
IKE	Internet Key Exchange	Provides device authentication by negotiating matching security policies.
IPSec	IP Security Protocol	Creates network layer tunnels with data encryption, authentication, and integrity services.
ISAKMP	Internet Security Association and Key Management Protocol	Provides a generic protocol that enables two devices to exchange security parameters.
L2F	Layer 2 Forwarding	Creates network access server (NAS)-initiated tunnels for forwarding PPP sessions.
L2TP	Layer 2 Tunneling Protocol	Provides data link layer user authentication, tunnel IP address assignment, and multiprotocol support.
LAC	L2TP Access Concentrator	Device terminating calls to remote systems and tunneling PPP sessions between remote systems and the LNS.
LNS	L2TP Network Server	Device able to terminate L2TP tunnels from a LAC and terminate PPP sessions to remote systems through L2TP data sessions.
MAC	Message Authentication Code	The cryptographic checksum of the message used to verify its (the message's) authenticity.
MD5	Message Digest 5	Provides basic message authentication.
NAS	Network Access Server	Gateway that connects asynchronous devices to a LAN or WAN through network and terminal emulation software. Performs both synchronous and asynchronous routing of supported protocols.

Acronym	Term	Definition
PNS	PPTP Network Server	Device able to terminate PPTP tunnels from a PAC and terminate PPP sessions to remote systems through PPTP data sessions.
PPP	Point-to-Point Protocol	Tunnels multiple network-layer protocols.
PPTP	Point-to-Point Tunneling Protocol	Creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over the Internet or other TCP/IP-based networks. PPTP is a Microsoft-proprietary protocol.
PAC	PPTP Access Concentrator	Device terminating calls to remote systems and tunnelling PPP sessions between remote systems and the PNS.
PSTN	Public Switched Telephone Network	Refers to the variety of telephone networks and services in place worldwide. Also called Plain Old Telephone System (POTS).
SA	Security Association	Defines a set of security parameters for a particular tunnel. Key management tunnels employ one SA, while data management tunnels employ several.
SHA	Secure Hash Algorithm	Provides strong message authentication.
SPI	Security Parameter Index	Number assigned to an SA for identification.
VPN	Virtual Private Network	Provides same network connectivity for users over a public infrastructure as they would have over a private network.

VPN Types

A Virtual Private Network (VPN) provides the same network connectivity for remote users over a public infrastructure as they would have over a private network. VPN services for network connectivity include authentication, data integrity, and encryption.

The two basic VPN types are:

- Remote Access VPNs. Securely connects remote users, such as mobile users and telecommuters, to the enterprise.
- LAN-to-LAN VPNs. Securely connects remote and branch offices to the enterprise (intranet VPNs). Securely connects third-parties, such as customers, suppliers, and business partners, to the enterprise (extranet VPNs).

Remote Access VPNs

Remote access VPNs secure connections for remote users, such as mobile users or telecommuters, to corporate LANs over shared service provider networks.

There are two types of remote access VPNs:

- Client-Initiated. Remote users use clients to establish a secure tunnel across an ISP's shared network to the enterprise.
- NAS-Initiated. Remote users dial in to an ISP Network Access Server (NAS). The NAS establishes a secure tunnel to the enterprise private network that might support multiple remote user-initiated sessions.

LAN-to-LAN VPNs

There are two common types of LAN-to-LAN VPNs (also known as site-to-site VPNs): intranet and extranet. Intranet VPNs connect corporate headquarters, remote offices, and branch offices over a public infrastructure. Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a public infrastructure.

VPN Components

Three main components of VPNs are:

- Tunnels
- Endpoints
- Sessions

Tunnels

A tunnel is an encapsulated traffic flow. VPN Monitor supports three types of tunnels:

- L2TP
- PPTP
- IPSec

Endpoints

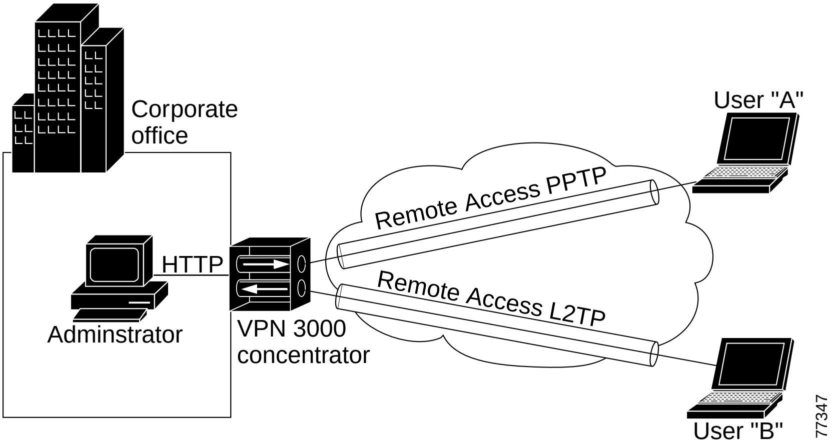
An endpoint is a network device on which a tunnel terminates. Any of the following networking devices can serve as an endpoint: a computer running a VPN client, a router, a gateway, or a network access server. The two ends of a tunnel are commonly referred to as the source and the destination endpoints.

- A source endpoint initiates the tunnel.
- A destination endpoint terminates the tunnel.

Sessions

A remote access tunnel can contain one or more PPP connections. Each PPP connection represents one specific user. VPN Monitor refers to these PPP connections as sessions. However, the VPN 3000 Concentrator Manager refers to *any* user connection to a device as a session, see Figure A-1.

Figure A-1 Simplified Session Scenario



VPN Monitor refers to the following *two* connections as sessions:

- User “A” (remote access session)
- User “B” (remote access session)

VPN Concentrator refers to the following *three* connections as sessions:

- User “A” (remote access session)
- User “B” (remote access session)
- Administrator (management session)

VPN Services

VPNs provide the following types of services:

- Peer Authentication
- Data Confidentiality
- Data Integrity
- Data Origin Authentication

Peer Authentication

Before a VPN is established, each endpoint verifies the other’s identity.

Data Confidentiality

Data confidentiality prevents unauthorized viewing of data between endpoints. Encryption is one method used to ensure data confidentiality. Data confidentiality is facilitated when a source endpoint encrypts or encodes data before sending it across a network. The designated destination endpoint can then decrypt or decode and read the data.

Data Integrity

Data integrity validates that data received by the destination endpoint is identical to the data sent by the source.

Data Origin Authentication

Data origin authentication verifies that data originated from the specified endpoint. Data origin authentication requires data integrity and device authentication. Data origin authentication allows non-repudiation (the ability of a third-party to trace and prove communication occurred between two endpoints).

IPSec Framework

The IPSec framework is a set of open standards developed by the Internet Engineering Task Force (IETF). This framework provides security services at Layer 3, the Network layer of the OSI model.

The IPSec framework provides these features:

- Peer Authentication
- Data Integrity
- Data Origin Authentication

The IPSec framework facilitates these features using two types of tunnels:

- Key Management Tunnels (also known as IKE tunnels)
- Data Management Tunnels (also known as IPSec tunnels)

Both key management and data management tunnels comprise Security Associations.

Key Management Tunnels

Key management tunnels (also known as IKE tunnels) are used to set up and maintain data management tunnels. Key management tunnels use the IKE protocol to perform their functions. The IKE protocol authenticates the peer and then negotiates a compatible security policy before establishing the data tunnel.

The key management tunnel facilitates:

- IPSec Key Negotiation
- IPSec Key Renegotiation
- The exchange of control messages for maintaining data management tunnels

Data Management Tunnels

Data management tunnels (also known as IPSec tunnels) are used to secure data traffic. Data management tunnels use the Authentication Header (AH) protocol and the Encapsulated Security Protocol (ESP) to perform their operations.

Data management tunnels facilitate:

- Data integrity
- Data confidentiality

Data management tunnels can be set up automatically using key management tunnels or manually by the operator.

There are two modes of operation for a data management tunnel:

- Tunnel mode, where the tunnel protects both the data and the identities of the endpoints.
- Transport mode, where the tunnel protects only the data.

Security Associations

A security association (SA) is a set of security parameters for authentication and encryption used by a tunnel. Key management tunnels use one SA for both directions of traffic; data management tunnels use at least one SA for each direction of traffic. Each endpoint assigns a unique identifier, called a security parameter index (SPI), to each SA.

Layer 2 Protocols

There are three types of Layer 2 protocols:

- PPTP
- L2F
- L2TP

VPN Monitor supports PPTP and L2TP on Cisco VPN concentrators.

PPTP

Point-to-Point Tunneling Protocol (PPTP) creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over the Internet or other TCP/IP-based networks. PPTP is a Microsoft-proprietary protocol.

L2F

Layer 2 Forwarding (L2F) creates NAS-initiated tunnels by forwarding Point-to-Point (PPP) sessions from one endpoint to another across a shared network infrastructure. L2F is a Cisco-proprietary protocol. VPN Monitor does not support L2F.

L2TP

Layer 2 Tunneling Protocol (L2TP) was developed to address the limitations of IPSec for client-to-gateway and gateway-to-gateway configuration, without limiting multivendor interoperability. An extension of Point-to-Point Protocol (PPP), L2TP is based on the Layer 2 Forwarding protocol (L2F) and the Microsoft-proprietary Point-to-Point Tunneling Protocol (PPTP).

APPENDIX B

Frequently Asked Questions (FAQs)

Use the information in these topics to answer some of your common questions:

- What is the impact of using VPN Monitor to monitor my network?
- Why doesn’t my device appear in the Available Devices List?
- What should I do if I am experiencing difficulty adding or importing devices?
- How can I keep the information gathered at a high polling rate from filling my disk?
- How can I find the minimized panel for a particular device?
- Why isn’t Layer 2 tunnel information shown for Cisco VPN routers?
- Why are IPSec No SAs and IKE No SAs warnings and alerts generated when a device on the Dashboard reboots?
- Why are large percentage of IKE Failures displayed on the Dashboard for VPN concentrators?
- Why does the VPN Monitor Dashboard display Polling Failed status?
- What security monitoring features does VPN Monitor provide?
- Why is the Dashboard inconsistent with the Tunnel List and Graphs?

What is the impact of using VPN Monitor to monitor my network?

Monitoring is accomplished by polling the devices listed in your VPN Monitor Dashboard. Depending on the global and per device polling intervals you have set, monitoring can affect:

- Memory and CPU usage on the devices being polled
- Traffic throughput on the devices being polled
- Disk space and memory capacity on the CiscoWorks Server

The more frequent the polling rate, the greater the impact on the devices being polled, their ability to process network traffic, and the performance of the CiscoWorks Server.

Default polling rates are set at the factory. However, you can modify them based on your particular needs and the capacity of your network. If you notice degradation of your network performance, you can lessen the affect of polling on your network by decreasing the polling rates.

Why doesn’t my device appear in the Available Devices List?

There are many reasons why your device might not appear in the Available Devices list. Use the steps in Table B-1 to troubleshoot and solve this problem.

Table B-1 Troubleshooting the Available Devices List

Steps	Troubleshooting Task	Resolution
1	Determine whether the device is in Inventory. Select **Resource Manager Essentials > Administration > Inventory > List Devices**.[1]	If the device is present, go to step 2. If the device is not present, add it to Inventory. Select **Resource Manager Essentials > Administration > Inventory > Add Devices**.[1]
2	Determine whether the device is running the correct software version: • Use CiscoView. Select **Device Manager > CiscoView**.[2] or • Telnet to the device and use the CLI.	Cisco VPN concentrators should be running 2.5.2f or later. Cisco VPN routers should be running 12.1(5a)E or later. If the device is running the correct software version, go to step 3. If the device is not running the correct software version, upgrade to the correct software version.

Table B-1 Troubleshooting the Available Devices List (continued)

Steps	Troubleshooting Task	Resolution
3	Determine whether Inventory has the correct software version for the device: 1. Select **Resource Manager Essentials** > **Inventory** > **Software Report** > **System Views** > **All Devices**. 2. In the Devices field, select the device that you want to add to the Dashboard. 3. Click **Add**. 4. Click **Finish**. 5. If the device is a Cisco 3000 VPN concentrator, check at the Version String column. If the device is a Cisco 7100, 7200, or 7400 router, check the Software Version column.	If the software version is correct, go to step 4. If the software version is incorrect, upgrade Inventory: 1. Select **Resource Manager Essentials** > **Administration** > **Inventory** > **Update Inventory**. The Collect Device Inventory dialog box appears. 2. Select the devices you want polled for new information, then click **Finish**.[1]

Table B-1 Troubleshooting the Available Devices List (continued)

Steps	Troubleshooting Task	Resolution
4	If the device is not Cisco VPN 3000 concentrator, or a Cisco 1700, 2600, 3600, 7100, 7200, or 7400 series router, determine whether it has IPSec MIB support. VPN Monitor supports only devices running software versions with the appropriate IPSec MIB support. To determine if the device has IPSec MIB support, enter: **`show crypto mib ipsec flowmib version`**	If the device has the appropriate IPSec MIB support, add the device to the *VPN Monitor* static view. If you have not already created a VPN Monitor static view, create one and add the device to it: 1. Select **Resource Manager Essentials** > **Administration** > **Device Views** > **Add Static Views**. The Add Static Views dialog box appears. 2. For the view name, enter **`VPN Monitor`**. 3. Enter the optional description, and select a type of view (custom or private). Only users with the system administrator role can create custom views. 4. Select the view that has the devices you want to add from Views. 5. Select the names of the devices you want from Devices and move them into Selected Devices. 6. Click **Finish**. The new view will be created.

1. See the Essentials online help for more information.
2. See the CiscoView online help for more information.

What should I do if I am experiencing difficulty adding or importing devices?

If you have difficulty adding or importing devices, do the following:

Step 1 Verify that the device is available in the *VPN Devices* dynamic view or the *VPN Monitor* static view.

Step 2 Ping the device using the same name you entered in the Inventory to identify the device.

If you used the IP address to identify the device, ping the device using the IP address. Otherwise, ping the device using <*hostname*>.<*domain name*>

where *hostname* is the name of the device entered in the Inventory and *domain name* is the name of the domain.

Use the default settings for packet size, packet count, and timeout interval.

Step 3 Verify that you have entered the correct read community string. Open a Telnet session to the device to check its SNMP configuration.

If the device does not respond to the SNMP Get request packets from your server, make sure it has an SNMP agent that is enabled and accessible using the community string you specified.

Step 4 Increase the SNMP timeout setting to 60 seconds. See the Inventory online help.

Note For VPN Monitor to function correctly, you must increase the SNMP timeout setting to a maximum of 60 seconds. This applies only to devices running Cisco IOS release 12.1(7)E.

How can I keep the information gathered at a high polling rate from filling my disk?

You can configure the number of days that polled data is stored. From the VPN Management Solution drawer, select **Administration > Monitoring Center** > **VPN Monitor Dashboard > Database** and select a value (*n*) from the drop-down menu in the **Automatically remove polled and event data more than *n* day(s) old** field, where *n* represents the age at which polled and event data is deleted.

How can I find the minimized panel for a particular device?

Move the pointer over the minimized dialog boxes. The full dialog box name, including the device name or IP address, is displayed in a pop-up window.

Why isn’t Layer 2 tunnel information shown for Cisco VPN routers?

VPN Monitor does not support monitoring of Layer 2 VPNs on Cisco VPN routers. Layer 2 is supported only on Cisco VPN concentrators.

Why are IPSec No SAs and IKE No SAs warnings and alerts generated when a device on the Dashboard reboots?

When a monitored device reboots, the IPSec No SAs and IKE No SAs thresholds for that device reaches or surpasses the set values (box turns yellow or red). This is because a remote device continues to try to communicate with the rebooted device using the previously agreed upon parameters, which the rebooted device no longer recognizes.

If the monitored device has *not* been rebooted, and the IPSec No SAs and IKE No SAs values for that device have exceeded, then it indicates a security violation. Investigate the problem using Syslog Analysis reports.

Why are large percentage of IKE Failures displayed on the Dashboard for VPN concentrators?

Cisco VPN concentrators running image versions 2.5.2F to 3.5, occasionally, display a large percentage of IKE Failures on the Dashboard due to a known bug, CSCdw7160, within the concentrator image. To resolve this, increase/adjust the IKE Failures threshold.

Step 1 From the VPN/Security Management Solution drawer, select **Administration** > **Monitoring Center** > **VPN Monitor Dashboard** > **Global Settings**. The Global Threshold Settings dialog box opens.

Step 2 In the **Failures > IKE Failures > Warning and Alert** fields, increase the threshold values.

Step 3 To record the occurrence of a threshold violation in the Event log, select the check box in the Log column corresponding to the desired item.

Step 4 Click **Save**.

Why does the VPN Monitor Dashboard display Polling Failed status?

Polling Failed status indicates that the poller could not retrieve all information from the device; therefore some device data might be unavailable.

The poller is unable to retrieve all information due to the following reasons:

- Loss of IP connectivity to the device.
- Change in the community strings on the device.
- Access restrictions on some of the MIB variables on the device.

What security monitoring features does VPN Monitor provide?

VPN monitor displays the following occurrences, which might indicate potential security breaches:

- A high occurrence of replayed packet counts. See the following values in the Data Management Failures table:
  - Replay - All
  - Replay - 24hrs
  - IPSec - Auth Fails - In
  - IPSec - Decrypt Fails
  - IPSec No SAs values

  See “Displaying Data Management Tunnel Failures” section on page 2-12 for more information.
- A frequent occurrence of decryption and validation failures. See the following values in the Key Management Failures table:
  - IKE Auth Fails
  - IKE Decrypt Fails
  - Hash Fails

See “Displaying Key Management Tunnel Failures” section on page 2-9 for more information.

- IKE No SAs or IPsec No SAs warnings or alerts under normal operations. See “Why are IPSec No SAs and IKE No SAs warnings and alerts generated when a device on the Dashboard reboots?” section on page B-8 for the exception to this rule. See “Displaying Data Management Tunnel Failures” section on page 2-12 and “Displaying Key Management Tunnel Failures” section on page 2-9, respectively for more information.

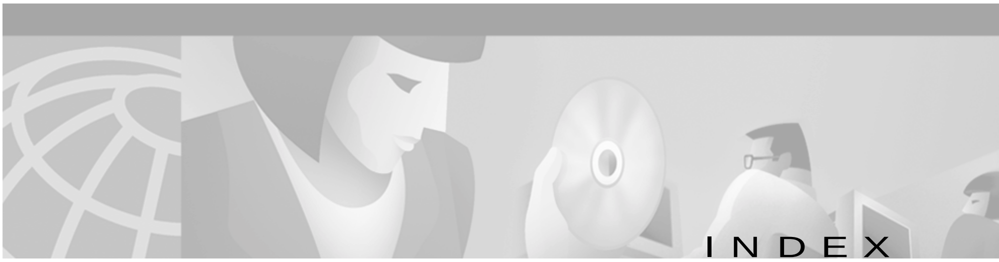
Why is the Dashboard inconsistent with the Tunnel List and Graphs?

If Auto Refresh is enabled, the Dashboard automatically refreshes with updated data at an interval equal to the shortest device polling interval. The Tunnel List displays data polled at the time the you open the Tunnel List. Given the differences in the way the data is polled and updated on these dialog boxes, the data on one dialog box might be more current than the data on the other dialog box.

For example, assume the shortest device polling interval is five minutes. You open the Dashboard and it displays data from the last poll (which just occurred). After five minutes, the devices are polled again, and the Dashboard is updated, showing two tunnels for a particular device.

After three minutes, you open the Tunnel List for the device and notice that it shows “No tunnels on this device.” There appears to be a discrepancy because the Dashboard shows two tunnels from the last poll, and the Tunnel List shows no tunnels from the instant poll. In this case, the Tunnel List is displaying the *most current data*.

After two minutes, the devices are polled again, and the Dashboard is updated with the data it obtained. For example, it shows three tunnels for the device. In this case, the Dashboard is now displaying the *most current data*.



INDEX