User Guide for
Cisco Performance Monitor 4.0

Americas 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: 408 527-0883

Text Part Number: OL-21886-01
Preface ix
Audience ix
Conventions ix
Performance Monitor Documentation x
Obtaining Documentation and Submitting a Service Request x

CHAPTER 1 Introduction 1-1
What Is Performance Monitor? 1-1
Understanding Basic Concepts 1-3
Performance Monitor and FCAPS 1-4
Supported Services and Platforms for Monitoring and Reports 1-5

CHAPTER 2 Before You Begin 2-1
Bootstrapping Devices 2-2
Setting Up SSL Services Modules 2-2
Setting Up Routers 2-3
Setting Up Catalyst 6500 Switches 2-4
Setting Up ASA Appliances, PIX Devices, and Firewall Services Modules 2-5
Setting Up VPN 3000 Concentrators 2-6
Setting Up IPSec VPN Shared Port Adapters (VPN SPA) 2-8
Using the Importing Devices Wizard to Import or Add Devices 2-8
Validating Devices 2-11
Scheduling Device Validations 2-12
Viewing Historical Validation Tasks 2-13
Validation Status 2-13
Validation Details 2-13
Setting Common Services to Use Email 2-15
Receiving SNMP Traps 2-15
Configuring the Polling Time Out 2-16

CHAPTER 3 Getting Started 3-1
Logging In to and Exiting Auto Update Server 3-1
Understanding User Permissions 3-2
Using the Performance Monitor Interface 3-3
Understanding the User Interface 3-4
  Understanding Interface Icons 3-5
  Understanding Device Icons 3-6
Using Performance Monitor Tables 3-6
Using Wizards 3-10
Using an Object Selector 3-10
Working in an Event Browser 3-12
  Event Browser Windows 3-14
MCP Process Maintenance 3-16
Sequence of Performance Monitor Operations 3-17

CHAPTER 4
Using Summaries 4-1
  Working in the Critical Problems Summary 4-2
  Working in the VPN Services Summary 4-3
  Working in the Firewall Services Summary 4-5
  Working in the Load-Balancing Summary 4-6
  Working in the SSL Services Summary 4-7

CHAPTER 5
Monitoring Remote Access VPN Services 5-1
  Understanding RAS Virtual Clusters 5-1
  Understanding Easy VPN 5-2
  Working in the RAS Clusters Table 5-2
  Working with RAS Devices 5-4
    Viewing Detail Graphs for a RAS Device 5-4
    Monitoring RAS Device Usage and Activity 5-6
    Monitoring RAS Device Failures 5-7
    Monitoring RAS Device Crypto Activity 5-8
    Viewing RAS Device Crypto Accelerator Card Data 5-10
    Viewing the Remote Access Interfaces Table 5-10
  Working with RAS Users 5-11
    Viewing RAS User Details 5-12
    Identifying the Top 10 Users of a RAS Device 5-13
    Identifying the Top 10 Users of a RAS Cluster 5-14
    Details of the Group Policy 5-16

CHAPTER 6
Monitoring Site-to-Site VPN Services 6-1
  Understanding DMVPN 6-2
Working with Site-to-Site Devices 6-3
  Monitoring Site-to-Site Device Usage and Activity 6-3
  Monitoring Site-to-Site Device Failures 6-4
  Monitoring Site-to-Site Device Crypto Activity 6-5

Working with Site-to-Site Device Details 6-6
  Displaying and Interpreting Site-to-Site Device Detail Graphs 6-6
  Displaying the Site-to-Site Device Interfaces Table 6-8

Working with Site-to-Site Tunnels 6-9
  Displaying the Site-to-Site Device Tunnels Table 6-9
  Finding a Site-to-Site VPN Tunnel 6-10

CHAPTER 7
Monitoring Firewall Services 7-1
  Working in the Firewall Devices Table 7-1
  Working With Firewall Device Details 7-2
    Displaying and Interpreting Device or Module Detail Graphs 7-3
    Displaying the Device or Module Interfaces Table 7-4
    Displaying the Device or Module Blocks Table 7-5
    Displaying the Device or Module Connections Table 7-5

CHAPTER 8
Monitoring Load-Balancing Services 8-1
  Content Switching Concepts 8-1
  Monitoring Modules Collectively 8-2
    Displaying CSM Usage and Activity Statistics 8-2
    Displaying Load Balancing Failure Statistics 8-3
    Displaying Server and Policy Reject Statistics 8-4
  Monitoring Modules Individually 8-5
    Displaying and Interpreting Module Detail Graphs 8-5
    Displaying the Virtual Servers Table 8-6
    Displaying the Real Servers Table 8-7
    Displaying the Interfaces Table 8-8

CHAPTER 9
Monitoring SSL Services 9-1
  SSL Concepts 9-1
    Purpose of SSL Modules 9-1
    Performance of SSL Modules 9-2
  Monitoring Modules Collectively 9-2
    Working with SSL Usage and Activity Statistics 9-2
    Working with SSL Statistics 9-3
## Chapter 9: Working with TCP Connection Statistics
- Monitoring Modules Individually 9-5
- Displaying and Interpreting Module Detail Graphs 9-5
- Displaying the SSL Proxy Statistics Table 9-6
- Displaying the SSL Proxy Errors Table 9-7

## Chapter 10: Using Trend Reports
- Understanding Reporting Options 10-1
- Understanding Failure Report Subcategories 10-2
- Understanding Performance Report Subcategories 10-3
- Understanding Throughput Report Subcategories 10-4
- Understanding Usage Report Subcategories 10-5
- Configuring and Generating Reports 10-6
- Understanding Historical Reports 10-8
- Viewing RAS VPN Top 10 User Reports 10-8
- Viewing RAS VPN User Session Reports 10-8
- Viewing Site-to-Site VPN Top 10 Tunnel Reports 10-10
- Working with Scheduled Email Jobs 10-11

## Chapter 11: Managing and Grouping Devices
- Managing Devices 11-2
  - Displaying Device Attributes 11-2
  - Editing a Device 11-3
  - Enabling or Disabling Device Monitoring 11-6
  - Displaying a Device Monitoring Summary 11-7
  - Deleting a Device, a Group, or a Context 11-8
- Managing Device Groups 11-9
  - Creating a Group 11-9
  - Editing a Group 11-11
  - Deleting Groups 11-12

## Chapter 12: Performance Monitor Administration
- Working with Notifications 12-1
  - Understanding Supported SNMP Traps and Syslog Messages 12-2
  - Configuring Notification Settings 12-3
  - Understanding Supported Event Types for Notifications 12-5
- Working with Event Thresholds 12-7
- Working with System Parameters 12-9
Frequently Asked Questions About Performance Monitor

Installation
- What prevents Performance Monitor from loading in my browser? A-1
- Why do I see a 500 Error when I try to run Performance Monitor? A-2
- How do I verify that Performance Monitor is running properly? A-2
- How do I change the status of Performance Monitor processes? A-3
- How do I forward SNMP traps to a different port if port 162 is already in use? A-3

Importing, Validating, and Managing Devices
- Why does import from DCR fail? A-4
- Why does the import of an SSL service module from a CSV file fail? A-4
- Why does import from a CSV file fail? A-4
- Why is a device that I imported missing from the Device Validation Tasks page? A-5
- Why do I see an error message when I try to import a PIX Firewall device? A-5
- What prevents me from adding PIX Firewall devices to Performance Monitor? A-6
- What prevents me from viewing a device under the Monitor tab? A-6
- What does the Device Not Reachable message mean? A-6
- What should I do if I see an SNMP Timeout error message/event? A-7
- Why has all device polling stopped? A-7

Administration
- What prevents me from receiving notifications? A-7
- How do I disable notifications? A-7
- How do I prevent polling information from filling the disk? A-8
- What prevents SNMP Traps from generating events? A-8
- How do I back up and restore the Performance Monitor database? A-9

Reports
- I deleted a device, then added it back. Then I ran a report and noticed that it displayed data earlier than the time I added the device. Why? A-9
- Why would the User Session Report for a VPN 3000 concentrator omit SSL VPN (WEBVPN) user login details? A-9
- Why is the User Session Report empty for a VPN 3000 concentrator? A-10
- Why are the CPU Usage% and Memory Usage% columns blank for the Cisco 800 series router? A-10

Debugging
- How do I turn on debugging? A-10
- How do I debug a problem related to importing a device? A-11
Preface

When you purchase Cisco Security Manager (Security Manager), your license grants you the right to
download, install, and use the appropriate version of Cisco Performance Monitor
(Performance Monitor).

Performance Monitor monitors and troubleshoots the health and performance of services that contribute
to network security. It enables you to isolate, analyze, and troubleshoot events in your network as they
occur, so that you can increase service availability.

This manual describes the features of the Performance Monitor application and explains how to use
those features.

SAFE is a Cisco strategy for designing, implementing, and maintaining a secure network. We
recommend that you implement the best practices in the Cisco SAFE blueprint before you install
Security Manager or any of its associated component applications. You can learn about SAFE at

Audience

This manual is intended for network and security personnel who support end users, administer network
operations, or plan network capacity.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong> font</td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><em>italic</em> font</td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><em>screen</em> font</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface screen</strong> font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td><em>italic screen</em> font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
</tbody>
</table>
Performance Monitor Documentation

For a complete list of Performance Monitor documentation, see the documentation roadmap for this version of the product at http://www.cisco.com/en/US/products/ps6498/products_documentation_roadmaps_list.html.

Also see http://www.cisco.com/go/csmanager.

Obtaining Documentation and Submitting a Service Request

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


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

Performance Monitor is a browser-based tool that monitors and troubleshoots the health and performance of services that contribute to enterprise network security. Supported service types are remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and proxied SSL.

To learn more about important security concepts, technologies, and service types, see Cisco.com.

The following topics provide an overview of Performance Monitor:

- What Is Performance Monitor?, page 1-1
- Understanding Basic Concepts, page 1-3
- Performance Monitor and FCAPS, page 1-4
- Supported Services and Platforms for Monitoring and Reports, page 1-5

What Is Performance Monitor?

Performance Monitor is a component of the Cisco Security Management Suite. It enables you to increase service availability by isolating, analyzing, and troubleshooting significant events in your network as they occur. Performance Monitor runs on top of CiscoWorks Common Services, which supplies essential server-side components and manages some functions on behalf of Performance Monitor. For more information, see the Common Services online help.

The following table describes Performance Monitor scalability.

- **Number of devices**—Supports up to 500 devices, including security contexts.
- **Number of users**—Supports up to 5 simultaneous users.
- **VPN restrictions**—We recommend that you monitor only the hubs, not the spokes, in any hub-and-spoke VPNs that you monitor. We recommend that you monitor no more than 5,000 tunnels.

See the following figure to understand the tabs from which you access all features and functions of Performance Monitor.
What Is Performance Monitor?

Summary tab options enable you to:

- Display a list of known critical problems (P1 and P2) in your network, or display graphs and charts that summarize the health and performance of any supported service in your network.
- Open a dashboard (a compact summary), or open an event browser with no set filters.

Note To understand dashboards and event browsers, see Understanding Basic Concepts, page 1-3.

Monitor tab options provide real-time monitoring for supported services on supported devices, such as:

- VPN (RAS or site-to-site) and firewall devices and services, including multi-context (virtual firewalls).
- Load-balancing services from content-switching service modules.
- SSL proxy services.

For a list of supported devices, see Supported Devices and Software Versions for Cisco Security Manager.

Options under the Reports tab enable you to:

- Configure, generate, and view reports about usage, throughput, performance, and failures.
- Schedule the automatic creation and email distribution of reports.
- Display reports for the remote-access VPN sessions of any user or all users.
- Review up to a year’s worth of report data, in which the data points occur at hourly, daily, weekly, or monthly intervals.
- Export report data in CSV, XML, or PDF formats.

Devices tab options enable you to:

- Import and validate device attributes manually or from a CSV file.
- View hardware, software, and network descriptions for devices.
- Learn when Performance Monitor most recently updated the tables and graphs under the Monitor tab, and to what extent.
- Edit device SNMP settings.
- Enable or disable device polling.
- Navigate in device groups (system-defined and user-defined) and view their properties.
- Create device groups and edit their properties.
- Delete user-defined device groups and delete references to specific devices.
Admin tab options enable you to configure event management and system parameter settings, review logs, develop customized online help content for your organization, and specify the default page.

- Event management options are:
  - Generate events based on SNMP traps, Syslog data, or crossed thresholds.
  - Use default or user-configurable thresholds.
  - Configure notification through email, SNMP traps, and Syslog.

System parameter settings control polling intervals, truncation intervals, and the intervals after which Performance Monitor deletes its records of historical data.

### Understanding Basic Concepts

The following table describes basic concepts that you must understand in order to use Performance Monitor successfully.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical problems</td>
<td>Critical problems are abnormal (P1 or P2) conditions that occur when a system component exceeds a performance threshold or functions improperly. Critical problems can cause network service disruptions and outages.</td>
</tr>
<tr>
<td>dashboard</td>
<td>The dashboard is a small browser window in which you isolate summary graphs for one or more supported services. The graphs refresh at an interval that you specify and summarize the performance of as many services as you select. If you select multiple services, the dashboard cycles through them in sequence, displaying graphs for one service at a time every time the dashboard display is refreshed. You open the dashboard when you click a detach icon (see Figure 3-2 on page 3-5) in a page under the Summary tab.</td>
</tr>
<tr>
<td>events</td>
<td>An event is a notification that a managed device or component has an abnormal condition. Multiple events can occur simultaneously on a single monitored device or service module. To display events, you open an event browser.</td>
</tr>
<tr>
<td>event browsers</td>
<td>An event browser organizes events into two event classes:</td>
</tr>
<tr>
<td></td>
<td>- Failure—Shows events in which a monitored component or service failed to operate as expected.</td>
</tr>
<tr>
<td></td>
<td>- Performance—Shows events in which a monitored component or service exceeded acceptable thresholds.</td>
</tr>
<tr>
<td></td>
<td>An event browser enables you to browse events generally or by type and to sort events by criteria that you choose. You can filter events by event class, service type, device type, severity, state, or description, and you can search for an event by its assigned event ID number. You can also accept responsibility for resolving the events that you view.</td>
</tr>
<tr>
<td></td>
<td>Each monitored service has its own dedicated event browser. The information in an event browser typically applies only to the service from which you started it. To display events for one service only, you must open the relevant event browser.</td>
</tr>
<tr>
<td>Tip</td>
<td>To open an event browser that displays unfiltered events of every type for every service, select Summary &gt; Event Browser.</td>
</tr>
</tbody>
</table>
Chapter 1      Introduction

Performance Monitor and FCAPS

In an effort to provide a clear focus and strategy for running a network safely and efficiently, the International Organization for Standardization (ISO) developed a network management model known as the FCAPS model. This model identifies five key areas of network management: Fault management, Configuration management, Accounting, Performance management, and Security.

- Fault management is concerned with detecting, diagnosing, and correcting network and system faults (outages and degradations). Fault management products typically provide for alert handling and event management functions, and can include the diagnostic tools needed to isolate faults to facilitate corrective or alternative actions.

- Configuration management is concerned with the installation, identification, inventory removal, and configuration of hardware (including components such as cards, modules, memory, and software), software, firmware, and services. Configuration management also provides for monitoring and managing the deployment status of a device. The configuration management functional area includes software management, change control, and inventory management.

- Accounting management is concerned with tracking the use of resources in a network. An example would be the allocation of billing costs for both time and services rendered by a service provider. Accounting management also addresses billing for utilization of communications and computing facilities, as well as tracking user access to networks and the resources accessed by those users. Accounting management systems typically include knowledge of tariff structures.

- Performance management is concerned with the measurement and analysis of both short-term and long-term network and system statistics related to utilization, response time, availability, and error rates. Performance management is also used to determine whether there are any outages on a network. Ideally, performance data can be used to prevent future failures by helping network planners identify trends that suggest capacity utilization or other problems before such problems affect users or services. Performance management tools are also used to assist in planning, design, and performance-tuning for improved network and systems efficiency.

- Security management is concerned with controlling access to network resources and preventing unauthorized use of or tampering with the network. Security management tools can address user access rights, data privacy, alarms and audit trails of security attacks/breaches, the management of security mechanisms, and password distribution.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summaries</td>
<td>Summary graphs and tables show the most recent 8 hours of service activity, based on polling that recurs at a configurable interval. Click hyperlinked graphs and table entries to see more detailed information.</td>
</tr>
</tbody>
</table>

Performance Monitor and FCAPS

In an effort to provide a clear focus and strategy for running a network safely and efficiently, the International Organization for Standardization (ISO) developed a network management model known as the FCAPS model. This model identifies five key areas of network management: Fault management, Configuration management, Accounting, Performance management, and Security.

- Fault management is concerned with detecting, diagnosing, and correcting network and system faults (outages and degradations). Fault management products typically provide for alert handling and event management functions, and can include the diagnostic tools needed to isolate faults to facilitate corrective or alternative actions.

- Configuration management is concerned with the installation, identification, inventory removal, and configuration of hardware (including components such as cards, modules, memory, and software), software, firmware, and services. Configuration management also provides for monitoring and managing the deployment status of a device. The configuration management functional area includes software management, change control, and inventory management.

- Accounting management is concerned with tracking the use of resources in a network. An example would be the allocation of billing costs for both time and services rendered by a service provider. Accounting management also addresses billing for utilization of communications and computing facilities, as well as tracking user access to networks and the resources accessed by those users. Accounting management systems typically include knowledge of tariff structures.

- Performance management is concerned with the measurement and analysis of both short-term and long-term network and system statistics related to utilization, response time, availability, and error rates. Performance management is also used to determine whether there are any outages on a network. Ideally, performance data can be used to prevent future failures by helping network planners identify trends that suggest capacity utilization or other problems before such problems affect users or services. Performance management tools are also used to assist in planning, design, and performance-tuning for improved network and systems efficiency.

- Security management is concerned with controlling access to network resources and preventing unauthorized use of or tampering with the network. Security management tools can address user access rights, data privacy, alarms and audit trails of security attacks/breaches, the management of security mechanisms, and password distribution.
Chapter 1  Introduction

Supported Services and Platforms for Monitoring and Reports

The capabilities of the Performance Monitor application are in the fault management and performance management categories as shown in the following table in bold text.

Table 1-2  Organization of the FCAPS Model

<table>
<thead>
<tr>
<th>Fault Management</th>
<th>Configuration Management</th>
<th>Accounting Management</th>
<th>Performance Management</th>
<th>Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handle alarms</td>
<td>System turn-up</td>
<td>Track service usage</td>
<td>Collect data</td>
<td>Control network element (NE) access</td>
</tr>
<tr>
<td>Detect trouble</td>
<td>Provisioning</td>
<td>Bill for services</td>
<td>Generate reports</td>
<td>Enable NE functions</td>
</tr>
<tr>
<td>Correct trouble</td>
<td>Autodiscovery</td>
<td>Service level agreements</td>
<td>Analyze data</td>
<td>Access logs</td>
</tr>
<tr>
<td>Test and acceptance</td>
<td>Backup and restore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network recovery</td>
<td>Database handling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward alarms</td>
<td>Manage inventory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filtering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Supported Services and Platforms for Monitoring and Reports

The following table shows which services Performance Monitor can monitor, and issue reports for, on each supported Cisco platform. Additional explanation follows the table.

Table 1-3  Supported Services and Platforms for Monitoring

<table>
<thead>
<tr>
<th>Platform</th>
<th>Monitored Service Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VPN</td>
</tr>
<tr>
<td>Adaptive Security Appliances 5500 Series</td>
<td>NA</td>
</tr>
<tr>
<td>Catalyst 6500 Series Switches</td>
<td>Content-switching Services Modules</td>
</tr>
<tr>
<td>Firewall Services Modules</td>
<td>NA</td>
</tr>
<tr>
<td>SSL Services Modules</td>
<td>NA</td>
</tr>
<tr>
<td>VPN SPAs</td>
<td>X</td>
</tr>
<tr>
<td>VSPAs</td>
<td>X</td>
</tr>
<tr>
<td>Cisco IOS Routers</td>
<td>X</td>
</tr>
<tr>
<td>PIX Firewalls</td>
<td>NA</td>
</tr>
<tr>
<td>VPN 3000 Concentrator Series</td>
<td>NA</td>
</tr>
</tbody>
</table>
When analyzing this table, keep the following in mind:

- In this table:
  - NA describes a service that the specified platform does not provide.
  - The X character describes a service that Performance Monitor supports on the specified platform.
  - The em-dash character (—) describes a service that Performance Monitor does not monitor on the specified platform.

- The following are supported services that vary for specific software or device versions:
  - PIX OS 7.0 and later support Easy VPN services, but not RAS clustering for Easy VPNs.
  - PIX OS 7.0 and later support Easy VPN, RAS VPN, site-to-site VPN, and virtual (multicontext) firewall services.
  - PIX OS 7.0 and later support RAS VPN and site-to-site VPN services in routed single context mode only.
  - FWSM versions 2.2 and later support virtual (multicontext) firewall services.
  - FWSM versions 3.1 and later support RAS VPN and site-to-site VPN services in routed single context mode only.
  - Cisco ASA Software Version 7.0 and later support Easy VPN, RAS VPN, site-to-site VPN, and virtual (multicontext) firewall services.

- Performance Monitor neither monitors nor offers reports for the load balancing of Cisco VPN 3000 concentrators or supported ASA appliances that you organize in virtual clusters. The Load Balancing column in this table refers exclusively to the web server load balancing services associated with supported content switching services modules in Catalyst 6500 series switches.
Before You Begin

Unless you configure certain options and features on your server and in your network, Performance Monitor cannot operate as designed. This chapter explains what you must do, and what we recommend that you do, so that you can use all the features Performance Monitor provides.

<table>
<thead>
<tr>
<th>Table 2-1 High-level Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
</tr>
<tr>
<td>Step 2</td>
</tr>
<tr>
<td>Step 3</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Step 4</td>
</tr>
<tr>
<td>Step 5</td>
</tr>
<tr>
<td>Step 6</td>
</tr>
</tbody>
</table>

After you complete the required high-level tasks, you can monitor your devices and perform device operations. For example, you can:

- View populated reports. See Chapter 10, “Using Trend Reports.”

Tip

We recommend that you set a firewall filter to secure your network any time you enable an insecure protocol such as SNMP.
Bootstrapping Devices

You must set up devices so Performance Monitor can validate, poll, and monitor them, as described in the following topics:

- Setting Up SSL Services Modules, page 2-2
- Setting Up Routers, page 2-3
- Setting Up Catalyst 6500 Switches, page 2-4
- Setting Up ASA Appliances, PIX Devices, and Firewall Services Modules, page 2-5
- Setting Up VPN 3000 Concentrators, page 2-6
- Setting Up IPSec VPN Shared Port Adapters (VPN SPA), page 2-8

Setting Up SSL Services Modules

The following table shows the required setup procedures for SSL services modules. For detailed documentation of Catalyst 6500 switches and SSL services modules, see Cisco.com.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td>Generate an RSA key and enable SSH on the services module.</td>
</tr>
<tr>
<td>• Confirm that an administrative user account exists on the SSL module.</td>
</tr>
<tr>
<td>• Configure the enable password on the SSL module.</td>
</tr>
<tr>
<td>• To generate an RSA key pair and enable SSH, use the following commands:</td>
</tr>
<tr>
<td>- <code>ssl-proxy(config) # ip ssh rsa keypair-name ssh-key</code></td>
</tr>
<tr>
<td>- <code>ssl-proxy(config) # crypto key generate rsa general-keys ssh-key</code></td>
</tr>
<tr>
<td>• To verify that SSH is configured correctly, enter:</td>
</tr>
<tr>
<td><code>ssl-proxy# show ip ssh</code></td>
</tr>
<tr>
<td>The following message is displayed:</td>
</tr>
<tr>
<td><code>SSH Enabled - version 1.5</code></td>
</tr>
</tbody>
</table>
Setting Up Routers

The following table shows the required setup procedures for supported Cisco routers. For detailed documentation of Cisco routers, see Cisco.com.

Table 2-3  Setup Procedures for Routers

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Enable SNMP and set up community strings. SNMP is required for validation, polling, and monitoring</td>
</tr>
<tr>
<td>Enter configuration mode, then enter snmp community community_string ro, where community_string is the read-only community string that you assign.</td>
</tr>
<tr>
<td>Caution SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic.</td>
</tr>
<tr>
<td>Step 2 (Optional) Set the system name, contact, and location variables. In Performance Monitor, these variables will be visible in the View Device Detail window. Enter configuration mode, then use the following commands:</td>
</tr>
<tr>
<td>• To set the system name, enter hostname name.</td>
</tr>
<tr>
<td>• To set the system contact, enter snmp contact contact.</td>
</tr>
<tr>
<td>• To set the location, enter snmp location location.</td>
</tr>
<tr>
<td>Step 3 Enable SNMP traps. Enter configuration mode, then use the following commands:</td>
</tr>
<tr>
<td>snmp-server host ip_address version 2c public isakmp snmp</td>
</tr>
<tr>
<td>where ip_address is the actual numeric IP address of the server on which you installed Performance Monitor.</td>
</tr>
<tr>
<td>snmp-server enable traps snmp linkdown linkup</td>
</tr>
<tr>
<td>snmp-server enable traps isakmp policy add</td>
</tr>
<tr>
<td>snmp-server enable traps isakmp policy delete</td>
</tr>
<tr>
<td>snmp-server enable traps ipsec cryptomap add</td>
</tr>
<tr>
<td>snmp-server enable traps ipsec cryptomap delete</td>
</tr>
<tr>
<td>snmp-server enable traps ipsec cryptomap attach</td>
</tr>
<tr>
<td>snmp-server enable traps ipsec cryptomap detach</td>
</tr>
<tr>
<td>snmp-server enable traps ipsec tunnel start</td>
</tr>
<tr>
<td>snmp-server enable traps ipsec tunnel stop</td>
</tr>
<tr>
<td>Step 4 Enable HTTPS. Enter configuration mode, then enter ip http secure-server.</td>
</tr>
<tr>
<td>Performance Monitor can monitor Easy VPN and DMVPN sessions only if you enable HTTPS.</td>
</tr>
</tbody>
</table>
Setting Up Catalyst 6500 Switches

The following table shows the required setup procedures for Catalyst 6500 switches in which IPSec VPN services modules or CSM services modules are running. For detailed documentation of Catalyst 6500 switches and IPSec VPN or CSM services modules, see Cisco.com.

Table 2-4  Setup Procedures for Catalyst 6500 Switches

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Enable SNMP and set up community strings.</strong> SNMP is required for polling and monitoring. Enter configuration mode, then enter <code>snmp community community_string ro</code>, where <code>community_string</code> is the read-only community string that you assign.</td>
</tr>
<tr>
<td>Caution</td>
<td>SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>(Optional) Set the system name, contact, and location variables.</strong> In Performance Monitor, these variables will be visible in the View Device Detail window. Enter configuration mode, then use the following commands.</td>
</tr>
<tr>
<td></td>
<td>• To set the system name, enter <code>hostname name</code>.</td>
</tr>
<tr>
<td></td>
<td>• To set the system contact, enter <code>snmp contact contact</code>.</td>
</tr>
<tr>
<td></td>
<td>• To set the location, enter <code>snmp location location</code>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Enable SNMP traps for CSM services modules.</strong> Enter configuration mode, then use the following commands.</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps slb real</code>.</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps snmp</code>.</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server host ip_address traps version 2 public casa slb snmp</code>, where <code>ip_address</code> is the actual numeric IP address of the server on which you installed Performance Monitor.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Enable SNMP traps for IPSec VPN services modules.</strong> Enter configuration mode, then use the following commands:</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server host ip_address version 2c community_string ipsec isakmp snmp</code> where <code>ip_address</code> is the actual numeric IP address of the server on which you installed Performance Monitor, and where <code>community_string</code> is the read-only community string you assigned.</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps snmp linkdown linkup</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps isakmp policy add</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps isakmp policy delete</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps ipsec cryptomap add</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps ipsec cryptomap delete</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps ipsec cryptomap attach</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps ipsec cryptomap detach</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps ipsec tunnel start</code></td>
</tr>
<tr>
<td></td>
<td><code>snmp-server enable traps ipsec tunnel stop</code></td>
</tr>
</tbody>
</table>
Setting Up ASA Appliances, PIX Devices, and Firewall Services Modules

The following table shows the required setup procedures for ASA appliances and PIX firewalls, and for Catalyst 6500 switches in which firewall services modules are running. For detailed documentation of these devices and technologies, see Cisco.com.

Table 2-5 Setup Procedures for Firewalls

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Specify the Performance Monitor server as the SNMP host for firewall appliances, devices, and modules. Enter this command at the firewall command line: `snmp-server host inside ip_address`, where `ip_address` is the actual numeric IP address of the server on which you installed Performance Monitor.  
  | **Caution** SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic. |
| Step 2 | Specify the Performance Monitor server as the HTTP host for polling. Enter this command at the firewall command line: `http ip_address netmask if_name`, where:  
  - `ip_address` is the numeric IP address of the server on which you installed Performance Monitor.  
  - `netmask` is the 32-bit address mask used in IP to indicate the bits of the IP address that are being used for the subnet address.  
  - `if_name` is the name of the interface—for example, `inside`.  
  You can use `netmask` to specify an entire subnet as the HTTP host. For example, to specify `171.69.74.0` as the HTTP host, you would enter: `http 171.69.74.0 255.255.255.0 inside` |
| Step 3 | Enable HTTPS polling. Enter this command at the firewall command line: `http server enable`.  
  | **Note** Although you use the `http server enable` command, the device enables its secure HTTPS server. |
| Step 4 | Configure Syslog. Messages are sent to all configured server hosts. We recommend that you log errors in production environments only. To disable Syslog logging from the firewall command line, enter this command: `no logging on`.  
  - To enable Syslog logging from the firewall command line, enter `logging on`.  
  - To set the clock on the firewall, enter `clock set hh:mm:ss (day month | month day) year`.  
  - To enable timestamps in Syslog messages, enter `logging timestamp`.  
  - To set the logging level, enter `logging trap level`, where `level` is the least significant severity level that concerns you; for example, enter `logging trap error` to log all messages with severity levels between error (level 3) and emergency (level 0). (Syslog messages have the following severity levels. 0: Emergency; 1: Alert; 2: Critical; 3: Error; 4: Warning; 5: Notification; 6: Informational; 7: Debugging.)  
  | **Note** Firewall performance might become degraded if you set the logging level too low, because a low setting triggers many messages. We recommend that you use the `error` severity level. |
|     | Set the Syslog server host as the server on which you installed Performance Monitor, enter `logging host if_name ip_address`, where `if_name` is the name of the interface (for example, `dmz`) and `ip_address` is the numeric IP address of the server on which you installed Performance Monitor, (for example, `logging host dmz 10.1.20.111`). You can configure more than one server host for Syslog. |


Setting Up VPN 3000 Concentrators

The following table shows the required setup procedures for VPN 3000 Concentrators.

For detailed documentation on VPN 3000 Concentrators, see Cisco.com. For detailed documentation on the VPN 3000 Concentrator Series Manager application, see VPN 3000 Series Concentrator Reference Volume I: Configuration and VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring.

Table 2-6  Setup Procedures for VPN 3000 Concentrators

<table>
<thead>
<tr>
<th>Task</th>
<th>Step 1</th>
<th>Enable HTTPS for the VPN 3000 Concentrator Series Manager (4.01 and earlier releases).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Although the VPN 3000 Concentrator Series Manager supports both HTTP and HTTPS connections, as a best practice, we recommend that you use HTTPS. An HTTPS connection requires an SSL certificate.</td>
</tr>
<tr>
<td></td>
<td>1.</td>
<td>Open a browser from a PC or workstation in the same private network as the VPN concentrator.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>In the browser Address or Location field, enter <code>https://address</code>, where <code>address</code> is the IP address of the private interface on the concentrator (for example, <code>https://10.10.147.2</code>), then press <code>Enter</code>.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
<td>If you do not see the VPN 3000 Concentrator Series Manager login prompt in your browser, telnet to the concentrator (or access it directly). From the CLI menu, select <code>Configuration &gt; System &gt; Management Protocols &gt; HTTP/HTTPS</code>. Select <code>Enable HTTPS</code>. Save and apply your changes.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable HTTPS for the VPN 3000 Concentrator Series Manager (4.1 and later releases).</td>
<td>You can enable HTTPS on the concentrator in either of two ways—using your browser or the concentrator CLI. Note that an HTTPS connection requires an SSL certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To enable HTTPS through your browser, log in to the VPN 3000 Concentrator Series Manager through a standard HTTP session, then select <code>Configuration &gt; Tunneling and Security &gt; SSL &gt; HTTPS</code>. Select the <code>Enable</code> check box and click <code>Apply</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To enable HTTPS through the CLI, telnet to the concentrator (or access it directly) and, from the CLI menu, select <code>Configuration &gt; Tunneling and Security &gt; SSL &gt; HTTPS &gt; Enable/Disable HTTPS</code>. Then select <code>Enable HTTPS</code> and save your changes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable HTTPS management sessions for the VPN 3000 Concentrator Series Manager (4.1 and later releases).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.</td>
<td>Open a browser from a PC or workstation in the same private network as the VPN concentrator.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>In the browser Address or Location field, enter <code>https://address/admin</code>, where <code>address</code> is the IP address of the concentrator, then press <code>Enter</code>.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
<td>When you see the VPN 3000 Concentrator Series Manager login prompt, enter the administrative username and the case-sensitive password (which displays as a series of asterisks), then click <code>Login</code>.</td>
</tr>
<tr>
<td></td>
<td>4.</td>
<td>Select <code>Configuration &gt; Interfaces</code>, then click the name of an interface.</td>
</tr>
<tr>
<td></td>
<td>5.</td>
<td>The interface that you select should be the one whose IP address you plan to enter in the Importing Devices wizard. See Using the Importing Devices Wizard to Import or Add Devices, page 2-8.</td>
</tr>
<tr>
<td></td>
<td>6.</td>
<td>Click the <code>WebVPN</code> tab, then select the <code>Allow Management HTTPS Sessions</code> check box.</td>
</tr>
<tr>
<td></td>
<td>7.</td>
<td>Click <code>Apply</code>.</td>
</tr>
</tbody>
</table>
Table 2-6  Setup Procedures for VPN 3000 Concentrators (continued)

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4  Enable SNMP.</td>
</tr>
<tr>
<td>1. Login to the VPN 3000 Concentrator Series Manager, as described elsewhere in this table.</td>
</tr>
<tr>
<td>2. (Optional) If no community string is configured, select Configuration &gt; System &gt; Management Protocols &gt; SNMP Communities, then click Add.</td>
</tr>
<tr>
<td>3. Enter a community string, click Add, then click Save Needed.</td>
</tr>
<tr>
<td>4. Select Configuration &gt; System &gt; Management Protocols &gt; SNMP.</td>
</tr>
<tr>
<td>5. Select the Enable check box, then click Apply.</td>
</tr>
</tbody>
</table>

⚠️ Caution  SNMP is not a secure protocol. We recommend that you create a firewall filter to secure SNMP traffic. |

| Step 5  Enable the XML interface. |
| You must enable the XML interface for at least one VPN concentrator in every remote access VPN cluster. It is not necessary to enable the XML interface on any concentrator that is not part of a cluster. |
| 1. Login to the VPN 3000 Concentrator Series Manager (as described elsewhere in this table), then select Configuration > System > Management Protocols > XML. |
| 2. Select the Enable check box, then click Apply. |

| Step 6  Configure linkup and linkdown traps. |
| 1. Login to the VPN 3000 Concentrator Series Manager (as described elsewhere in this table), select Configuration > System > Events > Classes, then click Add. |
| 2. From the Class Name list, select IP. |
| 3. From the Severity to Trap list, select 1-3, then click Add. |
| 4. Select Configuration > System > Events > Trap Destinations, then click Add. |
| 5. In the Destination field, enter the IP address of the server on which you installed Performance Monitor. |
| 6. From the SNMP Version list, select SNMPv2, then click Add. |
Step 7 Configure Syslog.

The User Session Report feature under the Reports tab can operate only if you enable Syslog on your VPN concentrators.

1. Login to the VPN 3000 Concentrator Series Manager (as described elsewhere in this table), select Configuration > System > Events > Classes, then click Add.
2. Select AUTH from the Class Name list, then select the Enable check box.
3. From the Severity to Syslog list, select 1-5, then click Add twice.
4. Select IKE from the Class Name list, then select the Enable check box.
5. From the Severity to Syslog list, select 1-5, then click Add.
6. Click Save Needed, then click OK.
7. Select Configuration > System > Events > Syslog Servers, then click Add.
8. In the Syslog Server field, enter the IP address of the server on which you installed Performance Monitor, then click Add.
9. (Optional) To improve performance in the Performance Monitor application itself if it is the only application to which the concentrator will send Syslog messages, select Configuration > System > Events > General, select None from the Severity to Syslog list, then click Apply.
10. Select the Enable check box, then click Apply.

Setting Up IPSec VPN Shared Port Adapters (VPN SPA)

The following table shows the required setup procedure for VPN SPA.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable HTTPS. Enter ip http secure server.</td>
</tr>
</tbody>
</table>

Using the Importing Devices Wizard to Import or Add Devices

Performance Monitor requires information about your devices in order to communicate with them. Use the Importing Devices wizard to import devices or to manually enter the IP addresses, hostnames, and read-only community strings for supported devices in your network. Importing is a mechanism by which you transfer a descriptive list of device attributes (and sometimes device group membership lists) from an outside inventory to Performance Monitor.

Options in the Importing Devices wizard enable you to import device attributes from a comma-separated value (CSV) file or from the Device Credentials Repository (DCR) on a Common Services-based server, or you can add device attributes manually. For general information about using wizards, see Using Wizards, page 3-10.
You cannot add, import, or validate:

- Any unsupported device type. For a list of supported devices, see Supported Devices and Software Versions for Cisco Security Manager.
- Any device when the MCP process has stopped. See MCP Process Maintenance, page 3-16.
- Any device that uses a dynamic IP address or lacks configured SNMP values.
- A VPN 3000 Series concentrator, unless you specify the correct SNMP and XML credentials, HTTPS is enabled, and the VPN 3000 Concentrator Series Manager is running.

Before You Begin
Make sure that you have the correct privileges to import or add devices. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select Devices > Importing Devices, then click Import.

Step 2 Select one of the following methods to add devices, then click Next.

- From CSV File, to use a comma-separated values file that contains the devices.
  You can import device attributes from a comma-separated value file in CSV 2.0 format only. To display a valid CSV example, click See sample CSV file in the next step. Note that Performance Monitor cannot import and validate SSL services module attributes from a CSV file.
  Before you can import devices from a CSV file, you must find or generate a CSV file of device attributes information and upload it to the server on which you installed Performance Monitor. Many element management systems enable you to export device inventory information. See your EMS software documentation to learn how to export inventory information in a CSV file. Performance Monitor has no default upload directory or configuration directory.
  - Manually Add New Devices, to enter specific device information directly.
  - From Device Credentials Repository, to import devices from the Common Services Device Credentials Repository (DCR). You must already have populated the DCR on this or another server to import the devices. Also, the DCR server must be configured as a master server. To learn how to configure a master DCR server, see the Common Services online help.

Step 3 If you selected From CSV File, complete the following procedure; otherwise, continue with the next step.

  a. Enter the complete local (on your server) pathname of the CSV file to upload, then click Next.
     For example, you might enter c:\temp\devicelist.csv. You can include or exclude any combination of devices you find in the CSV file.
  b. Select the check boxes for one or more devices to mark device attributes for import. To select all of the devices, select the check box in the column heading row.
  c. To save your selections, click Next.
  d. To review a list of the devices whose attributes you selected, click Next.

Step 4 If you selected Manually Add New Devices, complete the following procedure; otherwise, continue with the next step.

  a. From the Device Type list, select the relevant device type.
When you add multiple devices simultaneously, they must all be of the same device type. Otherwise, Performance Monitor queries during polling are inappropriate and polling results are unreliable. You must complete this step each time you manually add a different kind of device.

b. To specify the IP addresses or DNS names of the devices you plan to add, enter one or more IP addresses or DNS names in the Device Names/IP Addresses text box. Separate multiple address entries with a space or a comma.

c. Click Next.

You can specify SNMP information and Telnet login credentials (if applicable) for devices you add, but validation and polling for a device take more time to complete if the number of SNMP retries or the SNMP timeout period is greater than the default.

d. Enter the read community string in the Read Community text box.

The read community string is a password that allows read-only access to the specified devices. A single entry in the Read Community text box can apply to multiple devices, provided all of the read community strings are identical on all devices. The default entry on most devices and in Performance Monitor is public. If the community strings on your devices differ from the default, you must specify the correct community strings before validation can begin and before you can configure the devices.

e. Select a value from the SNMP Timeout list.

This is the number of seconds Performance Monitor waits for a response from the device before it asks again for a response. The minimum is 1 second and the maximum is 60 seconds. The default is 3 seconds.

f. Select a value from the SNMP Retries list.

This is the number of attempts Performance Monitor makes to communicate with the device before declaring that the device has timed out. The default is 1.

g. Do one of the following:

• If you are using the local username database on the device or an external AAA server, such as TACACS, enter the administrative username in the Username field. As you enter the username, the labels of the fields beneath it are changed to User Password, and Confirm User Password respectively. Enter the administrative password in the User Password field, then in the Confirm User Password field.

  Note  The User Password and Confirm User Password fields toggle between the Enable Password and Confirm Enable Password fields, depending on whether you are using local database or an external AAA server, or enable password authentication.

• If you are using enable password authentication, leave the username blank, enter the enable password in the Enable Password text box, and then confirm it in the Confirm Enable Password field.

  The enable password activates the privileged enable mode on a device when you access the device through a remote Telnet connection. Certain privileged operations can take place only when a device is running in enable mode.

h. Enter the HTTPS port number that the device uses for secure communication with Performance Monitor. The default port 443 is displayed in this field if you do not modify it.
The security appliance can support both SSL VPN connections and HTTPS connections for Performance Monitor sessions simultaneously on the same interface. Both HTTPS and SSL VPN use port 443 by default. Therefore, to enable both HTTPS and SSL VPN on the same interface, you must specify a different port number for either HTTPS or WebVPN. An alternative is to configure SSL VPN and HTTPS on different interfaces.

i. To save your selections and move to the next step, click Next.

Performance Monitor lists the devices whose attributes you added, so you can review your entries before validation occurs.

Step 5 If you selected From Device Credentials Repository, complete the following procedure; otherwise, continue with the next step.

a. Enter the following required information:
   - Host—The IP address or hostname of the DCR server. If you populated the DCR inventory on the same server as Performance Monitor, you can use the loopback IP address 127.0.0.1.
   - Port—The port number on which the DCR server receives HTTPS requests. The port by default is 443.
   - Username—The username of any user with authority to export and import devices.
   - Password—The password associated with the username.

b. Click Next.

c. Select the check boxes for one or more devices to mark device attributes for import. To select all of the devices, select the check box in the column heading row.

d. To save your selections and review a list of the devices whose attributes you selected, click Next.

Performance Monitor lists the devices so you can review your entries before validation occurs.

Step 6 To complete the process, click Finish. A one-time validation job starts immediately after you add or import devices. To learn about validation, see Validating Devices, page 2-11.

Tip If you imported device attributes from a CSV file, delete that file now to prevent unauthorized use of the confidential information that it contains. The unencrypted file contains important device credentials information. Its availability puts the security of your network at risk.

Validating Devices

When you validate a device of any kind, you confirm that it exists and is reachable, has the required features and interfaces enabled, has the correct credentials, uses a static (non-dynamic) IP address, and has configured SNMP values. Device validation also confirms that a VPN 3000 Series concentrator uses the correct XML credentials, has enabled HTTPS, and has enabled the VPN 3000 Concentrator Series Manager.

During device validation, Performance Monitor sets all validated devices to a managed state by default—meaning that polling is enabled. If you choose to move a device to an unmanaged state, you must revalidate it before you can monitor its health or performance.

By default, device validation occurs automatically once every day, at midnight. It occurs also at other times and intervals that you specify. You can perform an immediate, one-time validation at any time.
Validating Devices

Performance Monitor cannot validate:

- Any unsupported device type. For a list of supported devices, see Supported Devices and Software Versions for Cisco Security Manager.
- Any device when the MCP process has stopped. See MCP Process Maintenance, page 3-16.
- Any device that uses a dynamic IP address or lacks configured SNMP values.
- A VPN 3000 Series concentrator, unless you specify the correct SNMP and XML credentials, HTTPS is enabled, and the VPN 3000 Concentrator Series Manager is running.

The following topics explain how to schedule device validations, review the results of completed validation tasks, and run unscheduled validations.

- Scheduling Device Validations, page 2-12
- Viewing Historical Validation Tasks, page 2-13

Scheduling Device Validations

You can specify that device validation tasks occur at times of your choosing and recur at intervals of your choosing, or you can run an immediate, one-time validation.

Before You Begin

Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1
Select Devices > Importing Devices.

Step 2
In the Device Validation Tasks page, click Revalidate, then select options from the lists in the Start Time area.

Tip
The Start Time lists signify these values in this order from left to right: Month, calendar date, year, hour, and minute.

Step 3 (Optional)
To repeat validation at a specific interval:

a. Select the Repeat check box.

b. Enter a numeral in the Every text box.

c. Select an interval type (for example, hours) from the list.

Step 4
Do one of the following:

- To save and implement your changes, click Apply.
- To discard your changes, close the Schedule Validation Task page, and return to the Device Validation Tasks page, click Cancel.

Tip
To run an unscheduled validation once, immediately, click Run Now.
Viewing Historical Validation Tasks

You can display the results of past device validations.

**Before You Begin**

Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

**Procedure**

1. **Select Devices > Importing Devices.**
   
   Performance Monitor lists the 15 most recent validation tasks and describes their status.

2. **Click a radio button in the Device Validation Tasks list, then click Details.**
   
   The Validation Task Details window displays the historical validation results.

3. **Do one of the following:**
   - To update the Validation Task Details window if you believe that its displayed values are out-of-date, click Refresh.
   - To close the Validation Task Details window, click OK.

**Validation Status**

Historical task status messages are as follows.

<table>
<thead>
<tr>
<th>Task Status Message</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success: The task was completed in $t$ sec.</td>
<td>Variables are as follows: $t$—Count of the number of seconds that the specified validation required.</td>
</tr>
<tr>
<td>Failed: $x$ of $y$ devices were not imported. The task was completed in $t$ sec.</td>
<td>$x$—Count of the number of devices that Performance Monitor was unable to validate. This count excludes devices for which validation was partially successful. $y$—Count of the number of devices that Performance Monitor tried to validate.</td>
</tr>
<tr>
<td>Partial Success: Some of the VPN 3000 Series Concentrator clusters failed to be validated. The task was completed in $t$ sec.</td>
<td>A partially successful validation is one in which Performance Monitor is unable to gather cluster information for one or more devices. This happens when XML credentials are entered incorrectly in Performance Monitor or when the XML interface is disabled on a device.</td>
</tr>
</tbody>
</table>

**Validation Details**

There is only one kind of task detail message for a successful validation:

The device *DNS name | IP address* was imported successfully.

That message applies to any and every successful validation, regardless of service type or device type.

Historical validation task detail messages for validation failure vary by service type. Validation failure messages are as follows. (Generic messages might apply to the types of services and devices named in this table, or to other supported devices and services, such as IPSec VPN services modules or load-balancing services provided by CSM services modules.)
### Validating Devices

#### Service Type Messages

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Generic)</td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Verify that the device has a static IP address. Performance Monitor does not support dynamic IP addressing.</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Performance Monitor cannot validate a Catalyst 6500 switch unless the switch contains at least one supported services module.</td>
</tr>
<tr>
<td>SSL</td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td>Firewalls</td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td>Routers</td>
<td>The device `DNS name</td>
</tr>
<tr>
<td>RAS VPN</td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You might then see this message: An error occurred when the Router MC group was being created.</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
<tr>
<td></td>
<td>The device `DNS name</td>
</tr>
</tbody>
</table>
Setting Common Services to Use Email

You must configure Common Services to use an email server before Performance Monitor can send notifications of events or distribute scheduled reports through email.

**Before You Begin**
To complete this procedure, your user role must be either System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.

**Procedure**

**Step 1**  
From the https://<server_name>/cwhp/cwhp.applications.do page on the server where you installed Performance Monitor, select Common Services > Server > Admin.  
A new browser window opens to the Admin page in Common Services.

**Step 2**  
In the TOC, click System Preferences, then do the following:

a. In the SMTP Server field, enter localhost, or specify the IP address or fully qualified DNS name of a different mail server to use, such as: mailserver.example.com.

b. In the CiscoWorks Email ID field, enter the fully qualified email return address, such as: admin@example.com.

**Step 3**  
Click Apply.

**Receiving SNMP Traps**

**Note**  
For a list of the SNMP traps that Performance Monitor can process, see Working with Notifications, page 12-1.

If any other application on your server receives SNMP traps through UDP port 162, your installed copy of Performance Monitor will not receive any SNMP traps or display any information about events that are based on SNMP traps. In such cases, you must configure the conflicting application to forward its traps to another port and you must configure Performance Monitor to listen for traps on a different port.
**Configuring the Polling Time Out**

Performance Monitor stops polling all devices that are enabled for monitoring even if one device takes more than 30 seconds to return results. When Performance Monitor tries to retrieve the output of `show` commands from devices using HTTPS, retrieval of a single `show` command on a device might take more than 30 seconds, causing stoppage of polling. This problem might occur if Performance Monitor polls the device over a very slow WAN link.

The polling time out period for CLI commands is set by default to 30 seconds in the device.properties file available in the `NMSROOT\mcp\conf\devices` directory, where `NMSROOT` is the directory in which you installed Performance Monitor. If polling a device takes a long time, change the time out value by modifying the following line in the device.properties file:

```
Polling.CLIQuery.Timeout=timeout_value
```

where `timeout_value` is the polling time out period in seconds.
Getting Started

The following topics will help you understand and start using Performance Monitor:

- Logging In to and Exiting Auto Update Server, page 3-1
- Understanding User Permissions, page 3-2
- Using the Performance Monitor Interface, page 3-3
- Working in an Event Browser, page 3-12
- Sequence of Performance Monitor Operations, page 3-17

Logging In to and Exiting Auto Update Server

You log into Performance Monitor using the Cisco Security Management Suite home page. You can also use the home page to install the Security Manager client or to access Common Services, Auto Update Server, RME, and other software installed into Common Services.

Procedure

Step 1  In your web browser, open one of these URLs, where PMServer is the name of the computer where Performance Monitor is installed. Click Yes on any Security Alert windows.

- If you are not using SSL, open http://PMServer:1741
- If you are using SSL, open https://PMServer:443

The Cisco Security Management Suite login screen is displayed. Verify on the page that JavaScript and cookies are enabled and that you are running a supported version of the web browser. For information on configuring the browser to run Security Manager, see Installation Guide for Cisco Security Manager.

Note  We recommend that you use SSL for proper security.

Step 2  Log in to the Cisco Security Management Suite server with your username and password. When you initially install the server, you can log in using the username admin and the password defined during product installation.
Chapter 3  Getting Started

Understanding User Permissions

Your server authenticates the username and password of every user who logs in. After you start Performance Monitor, Common Services identifies the tasks and operations that you are authorized to perform based on your assigned role. Some tasks and related interface elements are hidden from unauthorized users. A user with system administrator privileges can access all features, while other users see only a subset of features. For example, a system administrator can display any scheduled email report job, regardless of who created it, while other users can display only the email jobs that they have created.

Performance Monitor user authentication and authorization come from Common Services. See the Common Services online help for details.

Note
You can configure Common Services to use Cisco ACS for the management of user accounts on your server. See “Configuring CiscoWorks Common Services to use Cisco Secure ACS Authorization and Authentication” topic in the Common Services online help.

Common Services provides seven user roles. The following table describes how those roles correspond to Performance Monitor tasks and interface elements.

<table>
<thead>
<tr>
<th>Your Common Services Role</th>
<th>Your Permitted Tasks</th>
<th>Your Visible Interface Tabs</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>All tasks (read/write).</td>
<td>All tabs and all options.</td>
</tr>
</tbody>
</table>
| Network Administrator (capacity planner)    | All privileges of a Network Operator, with the additional right to end RAS user sessions. | All tabs.  
                                                |                                                                       | However, all Admin tab options are hidden for this user role, except for the My Profile option. |
Table 3-1  Common Services User Roles and Corresponding Performance Monitor User Privileges (continued)

<table>
<thead>
<tr>
<th>Your Common Services Role</th>
<th>Your Permitted Tasks</th>
<th>Your Visible Interface Tabs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Operator</td>
<td>• Real-time monitoring.</td>
<td>All tabs.</td>
</tr>
<tr>
<td></td>
<td>• Inventory (read/write).</td>
<td>However, all Admin tab options are hidden for this user role, except for the My Profile option.</td>
</tr>
<tr>
<td></td>
<td>• Polling policy (read/write).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fault management (read/write).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Historical report scheduling (read/write).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Historical report viewing (read-only).</td>
<td></td>
</tr>
<tr>
<td>Approver</td>
<td>• Real-time monitoring.</td>
<td>Summary, Monitor, Reports, and Admin.</td>
</tr>
<tr>
<td></td>
<td>• Inventory (read/write).</td>
<td>However, all Admin tab options are hidden for this user role, except for the My Profile option.</td>
</tr>
<tr>
<td></td>
<td>• Polling policy (read/write).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fault management (read/write).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Historical report scheduling (read/write).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Historical report viewing (read-only).</td>
<td></td>
</tr>
<tr>
<td>Help Desk</td>
<td>• Real-time monitoring.</td>
<td>Summary, Monitor, and Admin.</td>
</tr>
<tr>
<td></td>
<td>• Inventory (read-only).</td>
<td>However, all Admin tab options are hidden for this user role, except for the My Profile option.</td>
</tr>
<tr>
<td></td>
<td>• Polling policy (read-only).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fault management (read-only).</td>
<td></td>
</tr>
<tr>
<td>Export Data</td>
<td>Note</td>
<td>These Common Services user roles do not correspond directly to any Performance Monitor tasks. By default, any users in these roles are considered help desk staff.</td>
</tr>
<tr>
<td>Developer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using the Performance Monitor Interface

Performance Monitor times out after 2 hours of inactivity, after which you must log in again. You cannot configure the timeout. Review the following topics to learn about recurring interface elements:

- Understanding the User Interface, page 3-4
- Using Performance Monitor Tables, page 3-6
- Using Wizards, page 3-10
- Using an Object Selector, page 3-10
Understanding the User Interface

The following figure shows and describes common elements in the Performance Monitor interface.

Figure 3-1 Common Performance Monitor Interface Elements

1. **Options bar**—Displays the options available for the selected tab.
2. **Path bar**—Says *You Are Here*, then lists the selected tab, option, and page (if relevant).
3. **Tab**—Provides access to Performance Monitor features. Click a tab to display its options.
   - **Summary**—View critical errors (P1 and P2), view summary graphs and tables for supported services, or open an event browser with no preset filters.
   - **Monitor**—Monitor the state of your remote access VPNs, site-to-site VPNs, firewall services, load-balancing services, and SSL proxy services.
   - **Reports**—Configure and generate historical reports for VPNs, firewall services, load-balancing services, and SSL proxy services.
   - **Devices**—Manage device validation and grouping.
   - **Admin**—Configure automatic notification when a monitored service fails or exceeds a threshold. Configure thresholds and intervals. View and configure log files. Set the default page.
4. **Tool bar**—Contains the Close, Help, and About links.
   - **Help**—Display context-sensitive help for the active page and access other help topics.
   - **About**—Display the Performance Monitor version and copyright.
   - **Close**—Close all Performance Monitor windows.
5. **Page**—Displays the area in which you review the information that Performance Monitor provides to you, and in which you perform application tasks.
Understanding Interface Icons

Figure 3-2 shows (and describes the purpose and correct use of) every Performance Monitor interface icon, except for the specialized icons that either:

- Indicate a specific kind of device (see Figure 3-3 on page 3-6).
- Enable you to navigate in a specific range of interrelated pages (see Figure 3-5 on page 3-8).

### Figure 3-2  Common Icons

1. Alert (active)—Appears in either of two locations. Indicates a severe problem or a failure. Click the icon to:
   - Open an event browser for the relevant service, device, or module, if the icon is in the Alert column of a descriptive table. See Working in an Event Browser, page 3-12.
   - Display the Critical Problems summary if the icon appears above a row of graphs or charts under the Summary tab. See Working in the Critical Problems Summary, page 4-2.

   **Tip** If you are unsure which result to expect when you click a particular alert icon, pause your pointer over the icon before you click. A tooltip says Critical Problems if the icon leads to the Critical Problems summary.

   **Note** After you clear an event, the alert icon is continued to be displayed in the device monitoring pages or the event browser window up to a minute or until the page is refreshed, whichever occurs first.

2. Alert (inactive)—Appears above a row of graphs or charts under the Summary tab. Indicates that there are no severe problems or failures. Click the icon to display the Critical Problems summary.

3. Detach—Appears above a row of graphs in pages under the Summary tab. Indicates that you can isolate and detach the relevant graphs as a dashboard (see Understanding Basic Concepts, page 1-3). Click the icon to open the dashboard.

4. Print Report—Appears in generated reports of historical trends or user sessions. Click the icon to print the report.

5. Report Help—Appears in generated reports of historical trends or user sessions. Click the icon to display online help.
Understanding Device Icons

In some pages, Performance Monitor uses icons to represent the validated devices in your network (Figure 3-3).

![Device Icons Diagram]

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Router.</td>
<td>5</td>
<td>SSL services module.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>VPN concentrator.</td>
<td>6</td>
<td>Unreachable device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Firewall (PIX, ASA, or services module).</td>
<td>7</td>
<td>A device for which monitoring is disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Content-switching services module.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Using Performance Monitor Tables

Tables contain items such as devices and critical problems; you can perform certain optional tasks in almost any page that contains a table. But Performance Monitor tables might differ in some ways from the tables you use in other applications, and might sometimes include unfamiliar traits like a troubleshooting function for your network devices and services. Also, some tables span multiple pages.
A single table might span multiple pages when the number of rows is insufficient to display all relevant data in a single page. In most cases, tables span multiple pages because either:

- You selected too few rows in the Rows per page list.
- Even the maximum value in the Rows per page list—40 rows—is insufficient to display the entire table in one page.

In these cases, use the navigation buttons (Figure 3-5 on page 3-8) under the table, or enter a table page number in the Go to page text box, then click Go.
Using the Performance Monitor Interface

Chapter 3  Getting Started

Figure 3-5  Table Navigation Buttons

1  Click to display the first page of a table that spans multiple pages.
2  Click to display the previous page of a table that spans multiple pages.
3  Click to display the next page of a table that spans multiple pages.
4  Click to display the last page of a table that spans multiple pages.

Table Check Boxes
A check box is present in a row when that row describes an item that you can edit or for which you can take an action. Optionally, you can select items row by row, or you can select the check box in the column heading to select all items.

Table Actions
If you plan to edit an item in a table, select its check box, then click the appropriate action button. Buttons that are not relevant to a selected item, or for which you do not have permissions, are grayed-out.

Common Elements in Tables
Table 3-2 describes elements that recur in most Performance Monitor tables.

Table 3-2  Common Elements in Performance Monitor Tables

<table>
<thead>
<tr>
<th>Element</th>
<th>Purpose or Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Data timestamp</td>
<td>Review the Current Data timestamp to learn whether the display is current. The more recent the timestamp, the greater the implied accuracy. The displayed time and the time zone abbreviation are those in your location, regardless of the location of the CiscoWorks Server.</td>
</tr>
</tbody>
</table>
| Enable Refresh Rate check box | Do either of the following:  
  • To enable automatic screen refreshes globally in Performance Monitor, select the check box.  
  • To disable automatic screen refreshes, deselect the check box. |
| minutes list | To change the repeat rate of automatic screen refreshes, if you have enabled them, select an interval from the minutes list. The fastest rate is once per minute; the slowest rate is once every 5 minutes. |
| column heading | Click a word in a column heading to sort the table by that column. For example, in a table that includes a Device column, click the Device column heading to sort the table by device names or IP addresses. Where a column heading has the image of a triangle, click the triangle to reverse the sorting order.  
  Note  Some column headings are not hyperlinked. You cannot sort a table by the values in these columns. |
| Rows per page list | Select an option from the list to change the maximum number of table rows displayed in each page. An automatic screen refresh follows your selection. |
Table 3-2 Common Elements in Performance Monitor Tables (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Purpose or Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>check boxes</td>
<td>Select the entry or entries to which an action applies. You can select entries individually, or you can select all entries simultaneously.</td>
</tr>
<tr>
<td></td>
<td>• A check box in the column heading row permits you to select or deselect all entries at once. (In a table that spans two or more pages, you select only the entries in the active page.)</td>
</tr>
<tr>
<td></td>
<td>• A check box in a row that describes one entry permits you to select that entry individually.</td>
</tr>
<tr>
<td></td>
<td>Note: You must select the entries to which an action applies before you perform the action.</td>
</tr>
<tr>
<td>Troubleshoot button</td>
<td>Troubleshooting information developed by Cisco Systems is part of the Performance Monitor application. The interactive troubleshooting tool is available online only, in these two ways:</td>
</tr>
<tr>
<td></td>
<td>• From the Troubleshoot button, where it appears in the interface. (Some pages do not include the Troubleshoot button.)</td>
</tr>
<tr>
<td></td>
<td>• From the table of contents for the Performance Monitor online help.</td>
</tr>
<tr>
<td>Refresh button</td>
<td>For a one-time, manual refresh of the active page, click Refresh.</td>
</tr>
<tr>
<td></td>
<td>Displayed values in the refreshed page are based upon data that was collected during the most recent polling cycle or from traps received from devices regarding the condition of their interfaces, real servers, or site-to-site VPN tunnels.</td>
</tr>
</tbody>
</table>

Table 3-3 Optional Tasks in Performance Monitor Tables

Table 3-3 describes optional tasks that recur in many tables pages.

<table>
<thead>
<tr>
<th>Optional Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort a table according to the values in a column.</td>
<td>Click a word in the column heading to sort a table by that column. Where a column heading has the image of a triangle, click the triangle to reverse the sorting order.</td>
</tr>
<tr>
<td></td>
<td>Note: Some column headings are not hyperlinked. You cannot sort a table by the values in these columns.</td>
</tr>
<tr>
<td>Change Performance Monitor screen refresh settings globally or refresh the active display.</td>
<td>Do any of the following:</td>
</tr>
<tr>
<td></td>
<td>• To enable automatic screen refreshes, select the Enable Refresh Rate check box.</td>
</tr>
<tr>
<td></td>
<td>• To disable automatic screen refreshes, deselect the Enable Refresh Rate check box.</td>
</tr>
<tr>
<td></td>
<td>• To change the repeat rate of automatic screen refreshes, if enabled, select an interval from the minutes list.</td>
</tr>
<tr>
<td></td>
<td>• To refresh the screen one time, even if you disabled automatic screen refreshes, click Refresh.</td>
</tr>
<tr>
<td>Assess the timeliness of the displayed values.</td>
<td>Review the Current Data timestamp to learn whether the displayed values are current. The more recent the timestamp, the greater the implied accuracy.</td>
</tr>
<tr>
<td></td>
<td>The displayed time and the time zone abbreviation are those in your location, regardless of the location of the CiscoWorks Server.</td>
</tr>
</tbody>
</table>
Using Wizards

Wizards lead you step-by-step through otherwise complicated tasks like importing or adding devices. Figure 3-6 shows a representative page from the Importing Devices wizard. The wizard elements are:

1. Table of contents (TOC) that lists the wizard steps.
2. Wizard pages.
3. Wizard action buttons.

A TOC lists the steps in the wizard, and TOC entries for steps you have completed are links that allow quick navigation back to a specific step or field. You must complete steps in a strict sequence when you work in a wizard. If you try to vary the sequence or leave the wizard too early, an error message is displayed and your action is blocked. Wizard action buttons differ according to the step that you select:

- The Back and Next buttons are grayed-out in the first and last steps, respectively.
- To exit the wizard without saving your changes, click Cancel.
- To submit your changes, then exit the wizard, click Finish.

Until you click Finish, Performance Monitor does not apply any of your selections. When you click Finish, you skip whichever steps remain undone in the wizard. Most wizards have defaults, which are applied to the steps that you skip.

Using an Object Selector

Object selectors are based on a framework of folders, subfolders, and their contents, and appear in many different pages in Performance Monitor. The elements in an object selector vary slightly, depending on its purpose. An object selector typically shows a nested tree of device groups, devices, and—sometimes—events, and lets you select devices and events as filtering criteria.
**Figure 3-7  Object Selector Elements**

1. **All tab**—Enables you to view and select:
   - Event categories, device groups, and individual devices so that you can filter the displayed results in an event browser window.
   - Device groups (system-defined or user-defined) and individual devices so that you can:
     - Restrict the scope of a report that you configure.
     - Edit SNMP settings and polling credentials.
     - Enable or disable polling.
     - View device properties.
     - Delete devices.
   - User-defined device groups and individual devices so that you can:
     - Create, modify, or delete user-defined device groups.
     - Display device group details.

2. **Selection Tab**—Enables you to isolate and display a complete list of the objects that you select under the All tab. To remove an object from the list of selections, deselect the relevant check box.

3. **Event Categories folder**—Contains events that you can select. Where it exists in the left pane of an event browser window, you can click the Event Categories folder to select all events. Alternatively, you can expand the folder and select one or both of the event categories it contains:
   - **Failure**—Also known as state events, failure events pertain to conditions for which only extreme values exist, such as *Up* and *Down*.
   - **Performance**—Also known as range events, performance events pertain to conditions for which a range of values exist, such as *OK*, *Degraded*, and *Overloaded*. 
Working in an Event Browser

An event is a notification that a monitored device or component has an abnormal condition. Multiple events can occur simultaneously on a single monitored device or service module.

An event browser window allows you to browse events and sort or filter events by criteria you choose. Performance Monitor provides filtered and unfiltered event browser options.

To open an event browser window, do any of the following:

- Under the Summary tab, select the **Event Browser** option. The event browser that opens describes all monitored events in your network, irrespective of their service type or the device on which they occur.
- Under the Summary tab, click any linked entry in the Critical Problems table. The event browser that opens describes only the events on the relevant device.
- In any TOC under the Monitor tab, click **Event Browser**. The event browser that opens describes only the events that affect the relevant service.
- Under the Monitor tab, click any hyperlinked alert icon in a table that includes an Alert column. The event browser that opens describes only the events that affect the relevant service on the relevant device.

When the event browser window opens, its left pane contains an Object Selector. See **Using an Object Selector**, page 3-10.

The following table describes some typical tasks that you can perform with an event browser. Additional tasks are explained in **Optional Tasks in Performance Monitor Tables**, page 3-9. For a general reference of event browser window elements, see **Event Browser Windows**, page 3-14.
## Table 3-4  Typical Tasks in Event Browser Windows

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use event categories to filter the events list.</td>
<td>You can view and select event types in the left pane to filter results in the right pane.</td>
</tr>
<tr>
<td></td>
<td>1. If the Event Categories folder is closed, click the + symbol to its left.</td>
</tr>
<tr>
<td></td>
<td>The folder expands. It contains event categories that you can select individually.</td>
</tr>
<tr>
<td></td>
<td>2. Select the check box to the left of an event category to select that category. Or, select the check box to the left of the folder to select all event categories.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Apply Filter</strong>. The refreshed display shows only events that match the category (or categories) you select.</td>
</tr>
<tr>
<td>Use devices or device groups to filter the events list.</td>
<td>You can view and select device groups or individual devices in the left pane to filter results in the right pane.</td>
</tr>
<tr>
<td></td>
<td>1. If the Device Groups folder is closed, click the + symbol to its left.</td>
</tr>
<tr>
<td></td>
<td>The folder expands. You can further expand the nested subfolders to view device categories and, finally, individual devices.</td>
</tr>
<tr>
<td></td>
<td>2. Select the check box to the left of a folder to select that folder and all of its descendants. Or, select the check box to the left of a device to select that device only.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Apply Filter</strong>. The refreshed display shows only the events on devices that you select.</td>
</tr>
<tr>
<td>Use severity levels to filter the events list.</td>
<td>To specify a severity level range (where P1 is the highest severity and P5 is the lowest), select the relevant option in the Select Severity list.</td>
</tr>
<tr>
<td></td>
<td>Performance Monitor applies the filter immediately and the event browser refreshes automatically to display the filtered result. The refreshed display shows only events within the specified severity range.</td>
</tr>
<tr>
<td>Use alarm states to filter the events list.</td>
<td>To specify an alarm state, select the relevant option from the Alarm Status list.</td>
</tr>
<tr>
<td></td>
<td>Performance Monitor applies the filter immediately and the event browser refreshes automatically to display the filtered result. The refreshed display shows only events within the specified alarm state (or states, if you select <strong>All</strong>).</td>
</tr>
</tbody>
</table>

**Note** Your selection in the Alarm Status list cannot be combined for filtering purposes with any selection in the Event State list. If you make selections in both lists, your second selection clears and overrides your first selection.
### Working in an Event Browser

#### Typical Tasks in Event Browser Windows (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Use event states to filter the event list. | Select a value from the Event State list in the right pane. Available options in the Event State list can vary as follows:  
- Generic—Options in the list are a superset of all possible states.  
- Service—Options in the list are only those that pertain to the specified service, such as states that can exist, for example, in a site-to-site VPN.  
- Device—Options in the list are only those that pertain to the specified device, such as states that can exist, for example, in a VPN 3000 Concentrator.  
- Combined Device and Service—Options in the list are a superset of all the states that are possible both for the specified service and for the specified device type.  
*Note* Your selection in the Event State list cannot be combined for filtering purposes with any selection in the Alarm Status list. If you make selections in both lists, your second selection clears and overrides your first selection.  
Performance Monitor applies the filter immediately and the event browser refreshes automatically to display the filtered result. |
| Use ranges of time to filter the events list. | Select a value from the Time list in the right pane.  
Performance Monitor applies the filter immediately and the event browser refreshes automatically to display the filtered result. |
| Use an Event ID to isolate and display a single event. | When Performance Monitor sends an email message to notify you about an event, it provides you with the sequential ID number it has assigned automatically to that event.  
To view the details of an event, enter its ID number in the Event ID text box, then click Find.  
*Note* An Event ID search is independent of any previous filtering. |
| Use a keyword or term to search for and display events that match a description. | You can isolate and view only the events that match a text string that Performance Monitor uses in its descriptions of events. For example, you could view only the events whose descriptions include such strings as not accessible, failure, or inbound.  
Enter a string in the Description text box. Then, to view only the events whose descriptions include that string, click Search.  
Queries are not case-sensitive.  
*Note* A description search is independent of any previous filtering. |

### Event Browser Windows

The following table describes elements in an event browser window.

#### Event Browser Window Reference

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object selector</td>
<td>The left pane contains an object selector, which is explained in <a href="#">Using an Object Selector, page 3-10</a>.</td>
</tr>
</tbody>
</table>
| Select Severity list | Enables you to select a severity level or range. The refreshed display includes only the events that match your selection, where P1 is the highest severity and P5 is the lowest.  
Select the All option to view problems from P1 to P5 and resolved problems for which the severity is now set to OK. |
### Working in an Event Browser

**Select Time list**
Enables you to restrict the display to events that occurred in a specific timeframe.

**Event State list**
Enables you to select a value. The refreshed display includes only the events triggered by a particular event state.

Event trigger values in the Event State column or in the Event State list are the same values as those that you define or modify in event-specific threshold settings under the Administration tab:

- Extreme, opposite values such as *Up* and *Down* apply to failure events.
- Values within a range, such as *OK*, *Degraded*, and *Overloaded*, apply to performance events.

**Alarm Status list**
Enables you to select an alarm state. The refreshed display includes only the events that match the alarm state you specify. The listed states are: All, Active, Cleared, and Acknowledged.

**Event ID text box**
Enables you to view detailed information about an event notification that Performance Monitor sent to you.

Enter the provided event ID number in the text box, then click **Find**.

**Description text box**
Enables you to define a query by which you can view only the events whose descriptions contain a specific text string.

Enter a keyword or term to define the parameters of your query. Acceptable parameters are limited to words or terms that match any part of any value Performance Monitor might display in the Description column.

To view only the events whose descriptions include the string you entered, click **Search**.

A description search is independent of any previous filtering.

**Device column**
Displays the DNS names of devices that provide the relevant monitored service.

The possible entries vary, according to which event browser window is open. For example, in the Firewall Event Browser, the Device column lists the DNS names of firewall devices and the DNS names of switches that contain one or more firewall service modules.

**Severity column**
Displays a severity level. The highest severity is P1; the lowest is P5.

**Type column**
Displays the type of event for which the relevant service has exceeded its threshold in this instance. Possible entries in this column are the same as the options you see when you define an event-specific threshold for the relevant monitored service.

You can display a complete list of the event types for a service if you select **Administration > Notifications**, then expand a service folder in the selection tree.

**Description column**
Describes the effect of the event on the service. For example, the description might say that bandwidth is low, or a VPN is down.

See the **Description text box** row in this table to understand how you can isolate and view only the events that match a particular description.

---

**Table 3-5  Event Browser Window Reference (continued)**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Time list</td>
<td>Enables you to restrict the display to events that occurred in a specific timeframe.</td>
</tr>
</tbody>
</table>
| Event State list   | Enables you to select a value. The refreshed display includes only the events triggered by a particular event state. Event trigger values in the Event State column or in the Event State list are the same values as those that you define or modify in event-specific threshold settings under the Administration tab:  
  - Extreme, opposite values such as *Up* and *Down* apply to failure events.  
  - Values within a range, such as *OK*, *Degraded*, and *Overloaded*, apply to performance events.  
  
**Note**  The exact values in a Event State list vary, depending on the service (or services) to which the displayed events apply. The State list includes all possible values when you select **Summary > Event Browser**. Otherwise, it displays only those states that apply to the relevant service. |
| Alarm Status list  | Enables you to select an alarm state. The refreshed display includes only the events that match the alarm state you specify. The listed states are: All, Active, Cleared, and Acknowledged. |
| Event ID text box  | Enables you to view detailed information about an event notification that Performance Monitor sent to you. Enter the provided event ID number in the text box, then click **Find**.  
  
**Note**  An Event ID search is independent of any previous filtering. |
| Description text box | Enables you to define a query by which you can view only the events whose descriptions contain a specific text string. Enter a keyword or term to define the parameters of your query. Acceptable parameters are limited to words or terms that match any part of any value Performance Monitor might display in the Description column.  
  
To view only the events whose descriptions include the string you entered, click **Search**.  
  
**Note**  A description search is independent of any previous filtering. |
| Device column      | Displays the DNS names of devices that provide the relevant monitored service.  
  
The possible entries vary, according to which event browser window is open. For example, in the Firewall Event Browser, the Device column lists the DNS names of firewall devices and the DNS names of switches that contain one or more firewall service modules. |
| Severity column    | Displays a severity level. The highest severity is P1; the lowest is P5. |
| Type column        | Displays the type of event for which the relevant service has exceeded its threshold in this instance. Possible entries in this column are the same as the options you see when you define an event-specific threshold for the relevant monitored service.  
  
You can display a complete list of the event types for a service if you select **Administration > Notifications**, then expand a service folder in the selection tree. |
| Description column | Describes the effect of the event on the service. For example, the description might say that bandwidth is low, or a VPN is down.  
  
See the **Description text box** row in this table to understand how you can isolate and view only the events that match a particular description. |
Performance Monitor polls a large number of devices frequently, for which it requires a server process called \textit{MCP}. To improve overall performance on your server, a scheduled job called \texttt{restartMCP.pl} stops and then restarts the MCP process once a week, on Sundays at 3:30 a.m. The script issues the \texttt{pdterm MCP} command and waits 1 minute, then issues the \texttt{pdeexec} MCP command.

\begin{itemize}
  \item The \texttt{restartMCP.pl} job also stops and then restarts the McpDbEngine process.
  \item The scheduled recurrence of the restartMCP.pl job is based on the local time of the server on which you installed Performance Monitor.
\end{itemize}

\begin{itemize}
  \item To display a list of scheduled jobs, go to the Windows command line and enter \texttt{at}, then press \texttt{Enter}.
  \item You can edit the entry for the \texttt{restartMCP.pl} script to modify its schedule.
\end{itemize}
Until the MCP process restarts:

- No device polling occurs.
- No new or recurring validation tasks run.
- Performance Monitor loses any SNMP traps that monitored devices send.
- You cannot add or import new devices.

The Performance Monitor interface is not affected and you can work from stored data, but some of the displayed data might not match the current condition of the devices and services in your network. Also, when you run historical reports, you might see a dip in the displayed graphs for any period of time in which the MCP process did not run.

The shutdown and restart of the MCP process generally takes less than 5 minutes.

---

### Sequence of Performance Monitor Operations

After you configure Performance Monitor and it is operating as you intend, it performs certain operations automatically, in the following sequence:

1. Runs scheduled validations to verify that devices exist and are reachable, provided device credentials are correct, required features are enabled, and required interfaces are enabled.
   
   For a VPN 3000 Series concentrator, validation also confirms that the relevant concentrator uses the correct XML credentials, has HTTPS enabled, and is running the VPN 3000 Concentrator Series Manager.

2. Updates the list of devices to poll, based on the results of scheduled validations.

3. Polls reachable devices for their current status, in order to compare device status information to performance and failure thresholds, generate performance and failure events, send event notifications, when appropriate, and update the values in tables and graphs.

   **Note**  
   If devices do not respond to the poll within the timeout period, polling to all devices stops. For more information, see Configuring the Polling Time Out, page 2-16.

4. Updates logs (continuously).

5. Performs scheduled and recurring jobs.
Using Summaries

Summary graphs and tables provide low-detail representations of performance metrics such as bandwidth consumption, connection failures, usage levels, and critical problems. Summary graphs and some table entries link to additional details about the relevant item or category.

Note

You can display certain types of summary information in a detachable dashboard, as described in Understanding Basic Concepts, page 1-3.

The following table describes the options under the Summary tab.

<table>
<thead>
<tr>
<th>Table 4-1 Performance Monitor Summary Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
</tbody>
</table>
| Critical Problems | Select the Critical Problems option to:  
  • Display a table of known critical problems.  
  • Filter problems by problem state.  
  • Acknowledge problems that Performance Monitor discovered in your network.  
  See Working in the Critical Problems Summary, page 4-2. |
| VPN | Select the VPN option to display performance summary graphs for VPN services. See Working in the VPN Services Summary, page 4-3. |
| Firewall | Select the Firewall option to display performance summary graphs for firewall services. See Working in the Firewall Services Summary, page 4-5. |
| Load Balancing | Select the Load Balancing option to display performance summary graphs for content-switching services. See Working in the Load-Balancing Summary, page 4-6. |
| SSL | Select the SSL option to display performance summary graphs for SSL proxy services. See Working in the SSL Services Summary, page 4-7. |
| Event Browser | Select the Event Browser option to open an Event Browser window with no preset filters. See Working in an Event Browser, page 3-12. |
Working in the Critical Problems Summary

A critical problem has a severity level of either P1 or P2. You can display the known critical problems for all monitored services in your network. You can acknowledge a critical problem to indicate that the problem is being addressed. The status for such problems will be changed from Active to Acknowledged. After the problem is resolved, you can clear the event from the Event Browser. An event that has been acknowledged or cleared will still be reported if the problem has not been resolved prior to the next polling cycle. If a problem has been resolved prior to the next polling cycle, the event will be cleared regardless of its status.

Procedure

Step 1 Select **Summary > Critical Problems**. For a description of the columns in the table, see Table 4-2.

Tip The table initially lists all active problems. You can change this view to see just acknowledged problems, or all problems (active or acknowledged) by selecting the desired option in the **Select Status** list. The refreshed list shows only monitored problems in the specified state. If no problems match the specified state, the refreshed list contains no records.

Step 2 For active problems, you can do the following:

- Open an Event Browser window and display a filtered list of all events on a specific device—Click a hyperlinked entry in the Description column.

  The Event Browser display is not limited to the P1 and P2 severity levels, as the Critical Problems page is. Therefore, the Event Browser might display events of any or every severity level for the device you specify.

- Acknowledge a critical problem—Select the check box in the row that describes the problem to resolve, then click **Acknowledge**. You can select multiple boxes at once, or select all problems by clicking the box in the heading row.

  You acknowledge a critical problem to indicate that the problem is being addressed. Only one user can acknowledge any specific problem. After the problem is resolved, you can clear the event from the Event Browser. Note that there is no way to undo an acknowledgement.

Reference

**Table 4-2 Critical Problems Summary**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device column</td>
<td>Identifies by DNS name or IP address the device with the monitored problem.</td>
</tr>
<tr>
<td>Family column</td>
<td>Identifies the device as a VPN router, a concentrator, or a switch with a service module.</td>
</tr>
<tr>
<td>Product column</td>
<td>Displays the relevant product model number.</td>
</tr>
<tr>
<td>Severity column</td>
<td>Displays a value between P1 and P5, where P1 is a problem of the highest severity and P5 is the lowest.</td>
</tr>
<tr>
<td>Description column</td>
<td>Displays a terse description of the critical problem.</td>
</tr>
</tbody>
</table>
Working in the VPN Services Summary

Performance Monitor provides graphs that summarize the condition of remote access and site-to-site VPN services in your network.

**Note**

All summary graphs in Performance Monitor show delta values (the differences measured between polling cycles) unless otherwise specified.

**Procedure**

**Step 1**

Select **Summary > VPN**.

The VPN page displays graphs that show the results of real-time monitoring (Table 4-3). The display is always current if you select the Enable Refresh Rate check box. Otherwise, click the **Refresh** button to refresh the view.

**Tip**

The **Critical Problems** button is colored red if at least one critical problem exists in your network. The button is otherwise gray. Click the button to display a table of all critical (P1 and P2) problems. (See **Understanding Interface Icons**, page 3-5.)

**Step 2**

Click graphs to view additional details. To isolate the graphs in the dashboard, click the detach icon.
### Types of VPN Summary Graphs

#### Table 4-3  Graphs in the VPN Summary

<table>
<thead>
<tr>
<th>Graph Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remote Access Graphs</strong></td>
<td></td>
</tr>
<tr>
<td>Top 3 Throughput (RAS)</td>
<td>Shows real-time throughput levels in Kbps for the three VPN concentrators with the highest levels of throughput. If you have fewer than three VPN concentrators in your network, there are fewer than three bars in the chart. If there is no throughput on any VPN concentrator, the chart is empty. Click to display the Remote Access Devices page, which shows performance statistics for your RAS devices individually (see Monitoring RAS Device Usage and Activity, page 5-6).</td>
</tr>
<tr>
<td>Top 3 Connection Failures % (RAS)</td>
<td>Shows real-time connection failure rates for the three VPN concentrators that are experiencing the most connection failures. If you have fewer than three VPN concentrators in your network, there are fewer than three bars in the chart. If there are no failed connections on any of your VPN concentrators, the chart is empty. Click to open an Event Browser and display severe RAS errors only (see Event Browser Windows, page 3-14).</td>
</tr>
<tr>
<td>Top 3 User Session Count (RAS)</td>
<td>Shows real-time session counts for the three devices with the most user sessions. If fewer than three devices have user sessions, there are fewer than three bars in the chart. If there are no user sessions on any of your RAS devices, the chart is empty. Click to display the Remote Access Devices page, which shows performance statistics for your RAS devices individually (see Monitoring RAS Device Usage and Activity, page 5-6).</td>
</tr>
<tr>
<td><strong>Site-to-Site Graphs</strong></td>
<td></td>
</tr>
<tr>
<td>Top 3 Throughput (Site-to-Site)</td>
<td>Shows real-time throughput levels in Kbps for the three site-to-site devices with the highest levels of throughput. If you have fewer than three site-to-site devices in your network, there are fewer than three bars in the chart. If there is no throughput on any of your site-to-site devices, the chart is empty. Click to display the Site-to-Site Devices page, which shows performance statistics for your site-to-site devices individually (see Monitoring Site-to-Site Device Usage and Activity, page 6-3).</td>
</tr>
<tr>
<td>Top 3 Connection Failures % (Site-to-Site)</td>
<td>Shows real-time connection failures of the three site-to-site devices that are experiencing the most connection failures. If you have fewer than three site-to-site devices in your network, there are fewer than three bars in the chart. If there are no failed connections on any of your site-to-site devices, the chart is empty. Click to open an Event Browser and display severe site-to-site errors only (see Event Browser Windows, page 3-14).</td>
</tr>
<tr>
<td>Top 3 Tunnel Count (Site-to-Site)</td>
<td>Shows real-time tunnel counts for the three devices with the most tunnels. If you have fewer than three site-to-site devices in your network, there are fewer than three bars in the chart. If there are no tunnels on any of your site-to-site devices, the chart is empty. Click to display the Site-to-Site Devices page, which shows performance statistics for your site-to-site devices individually (see Monitoring Site-to-Site Device Usage and Activity, page 6-3).</td>
</tr>
</tbody>
</table>
Working in the Firewall Services Summary

Performance Monitor provides graphs that summarize the current condition of firewall services in your network.

Note

All summary graphs in Performance Monitor show delta values (the differences measured between polling cycles) unless otherwise specified.

Procedure

Step 1
Select Summary > Firewall.

The Firewall page displays graphs that show the results of real-time monitoring (Table 4-4). The display is always current if you select the Enable Refresh Rate check box. Otherwise, click the refresh button to refresh the view.

Tip
The Critical Problems button is colored red if at least one critical problem exists in your network. The button is otherwise gray. Click the button to display a table of all critical (P1 and P2) problems. (See Understanding Interface Icons, page 3-5.)

Step 2
Click graphs to view additional details. To isolate the graphs in the dashboard, click the detach icon.

Types of Firewall Summary Graphs

Table 4-4  Graphs in the Firewall Summary

<table>
<thead>
<tr>
<th>Graph Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3 Interface Bandwidth Consumption %</td>
<td>Shows real-time bandwidth consumption percentages of the three PIX Firewall device interfaces that are using the most bandwidth. If there is no bandwidth consumption on any of your PIX interfaces, the chart is empty.</td>
</tr>
<tr>
<td>Note</td>
<td>Calculations of interface bandwidth consumption do not include any interfaces on firewall service modules. However, the interfaces of those IOS routers on which inspection policies are configured are used in the calculations.</td>
</tr>
<tr>
<td></td>
<td>Click to display the Firewalls page, which shows usage and activity statistics for all your firewall devices and modules (see Working in the Firewall Devices Table, page 7-1).</td>
</tr>
<tr>
<td>Top 3 Interface Errors</td>
<td>Shows real-time error counts for the three firewall device interfaces that are experiencing the most errors. If fewer than three interfaces have errors, there are fewer than three bars in the chart. If there are no errors on any of your firewall interfaces, the chart is empty.</td>
</tr>
<tr>
<td></td>
<td>Click to open an Event Browser and display severe firewall events only (see Event Browser Windows, page 3-14).</td>
</tr>
<tr>
<td>Top 3 Connections</td>
<td>Shows real-time connection counts for the three firewall devices with the most connections. If fewer than three devices have connections, there are fewer than three bars in the chart. If there are no connections on any of your firewall devices, the chart is empty.</td>
</tr>
<tr>
<td></td>
<td>Click to display the Firewalls page, which shows usage and activity statistics for all of your firewall devices (see Working in the Firewall Devices Table, page 7-1).</td>
</tr>
</tbody>
</table>
Working in the Load-Balancing Summary

Performance Monitor provides a summary of the current condition of the validated content-switching service modules (CSM) that provide web server load-balancing services in your network.

---

**Note**

All summary graphs in Performance Monitor show delta values (the differences measured between polling cycles) unless otherwise specified.

---

**Procedure**

**Step 1**

Select **Summary > Load Balancing**.

The Load Balancing page displays bar charts that show the results of real-time monitoring (Table 4-5). The display is always current if you select the Enable Refresh Rate check box. Otherwise, click the **Refresh** button to refresh the view.

---

**Tip**

The **Critical Problems** button is colored red if at least one critical problem exists in your network. The button is otherwise gray. Click the button to display a table of all critical (P1 and P2) problems. (See **Understanding Interface Icons**, page 3-5.)

**Step 2**

Click graphs to view additional details. To isolate the graphs in the dashboard, click the detach icon.

---

**Types of Load Balancing Summary Graphs**

**Table 4-5  Graphs in the Load Balancing Summary**

<table>
<thead>
<tr>
<th>Graph Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3 Current Connections</td>
<td>Shows real-time connection counts for the three CSM modules with the most connections. If fewer than three modules have connections, there are fewer than three bars in the chart. If there are no connections on any of your CSM modules, the chart is empty. Click to view the Load Balancing Modules page, which shows usage and activity statistics for all of your CSM modules (see <strong>Displaying CSM Usage and Activity Statistics</strong>, page 8-2).</td>
</tr>
<tr>
<td>Top 3 Connection Failures %</td>
<td>Shows real-time connection failure percentages for the three CSM modules with the most connection failures. If fewer than three modules have connection failures, there are fewer than three bars in the chart. If there are no connection failures on any of your CSM modules, the chart is empty. Click to open an Event Browser and display severe CSM errors only (see <strong>Event Browser Windows</strong>, page 3-14).</td>
</tr>
<tr>
<td>Top 3 Virtual Server Connections</td>
<td>Shows real-time connection counts for the three virtual servers with the most connections. If fewer than three virtual servers have connections, there are fewer than three bars in the chart. If there are no connections on any of your virtual servers, the chart is empty. Click to view the Load Balancing Modules page, which shows usage and activity statistics for all of your CSM modules individually (see <strong>Displaying CSM Usage and Activity Statistics</strong>, page 8-2).</td>
</tr>
</tbody>
</table>
Working in the SSL Services Summary

Performance Monitor provides graphs that summarize the current condition of SSL proxy services in your network.

---

**Note**

All summary graphs in Performance Monitor show delta values (the differences measured between polling cycles) unless otherwise specified.

---

**Procedure**

**Step 1**

Select `Summary > SSL`.

The SSL Summary page displays bar charts that show the results of real-time monitoring (Table 4-6). The display is always current if you select the Enable Refresh Rate check box. Otherwise, click the Refresh button to refresh the view.

---

**Tip**

The Critical Problems button is colored red if at least one critical problem exists in your network. The button is otherwise gray. Click the button to display a table of all critical (P1 and P2) problems. (See Understanding Interface Icons, page 3-5.)

---

**Step 2**

Click graphs to view additional details. To isolate the graphs in the dashboard, click the detach icon.

---

**Types of SSL Summary Graphs**

**Table 4-6**

<table>
<thead>
<tr>
<th>Graph Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 3 Connections</td>
<td>Shows real-time connection counts for the three SSL modules with the most connections. If fewer than three modules have connections, there are fewer than three bars in the chart. If there are no connections on any of your SSL modules, the chart is empty. Click to view the SSL Modules page, which shows usage and activity statistics for all of your SSL modules (see Working with SSL Usage and Activity Statistics, page 9-2).</td>
</tr>
<tr>
<td>Top 3 Error</td>
<td>Shows real-time error counts for the three SSL modules with the most errors. If fewer than three modules have errors, there are fewer than three bars in the chart. If there are no errors on any of your SSL modules, the chart is empty. Click to open an Event Browser and display severe SSL errors only (see Event Browser Windows, page 3-14).</td>
</tr>
<tr>
<td>Top 3 Module Throughput</td>
<td>Shows real-time throughput levels in bytes for the three SSL modules with the most throughput. If fewer than three modules have measurable throughput, there are fewer than three bars in the chart. If there is no measurable throughput on any of your SSL modules, the chart is empty. Click to view the SSL Modules page, which shows usage and activity statistics for all of your SSL modules individually (see Working with SSL Usage and Activity Statistics, page 9-2).</td>
</tr>
</tbody>
</table>
Working in the SSL Services Summary
Monitoring Remote Access VPN Services

A remote access service (RAS) VPN secures connections for remote users, such as mobile users or telecommuters. RAS VPN monitoring provides all of the most important indicators of cluster, concentrator, and user session performance at a glance.

Performance Monitor also enables you to determine quickly whether RAS VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users.

Optionally, you can logout one RAS user at a time.

Tip

To troubleshoot common problems with RAS VPN services, see the Troubleshooting appendix.

The following topics explain the RAS VPN monitoring features:

- Understanding RAS Virtual Clusters, page 5-1
- Understanding Easy VPN, page 5-2
- Working in the RAS Clusters Table, page 5-2
- Working with RAS Devices, page 5-4
- Working with RAS Users, page 5-11

Understanding RAS Virtual Clusters

Note

- References in Performance Monitor and documentation to load balancing services pertain only to the web server load-balancing capabilities of content switching services modules. Performance Monitor does not monitor the load balancing of concentrators or appliances that you have combined in virtual clusters.
- Although PIX OS and Easy VPN both support the use of RAS VPNs, neither technology supports the use of virtual clusters.

RAS VPNs enable remote users to participate in private networks through a shared public infrastructure, connecting through dial-up, ISDN, DSL, cable, or other technologies.
Performance Monitor monitors RAS VPN services that originate on several different kinds of devices, but special considerations apply to Cisco VPN 3000 Series concentrators and ASA 5520 or 5550 appliances because you can monitor them singly or when they are combined in a virtual cluster for load-balancing. In a virtual cluster, a collection of concentrators or a collection of appliances can function as a single entity.

The cluster is known to the outside client space by one IP address. The virtual IP address must be a routable address—meaning a valid address to which another device can send packets. Otherwise, inbound packets do not reach the cluster.

This virtual IP address is not tied to a specific device in the VPN cluster. It is serviced by the virtual cluster master. A virtual cluster master concentrator maintains the load information from all secondary concentrators or appliances in a specific cluster. Each secondary concentrator sends KeepAlive load information messages to the master.

- The VPN 3000 series includes six different concentrator models. To learn about their uses and capabilities, which can help you to assess whether the concentrators that you monitor are operating correctly, see http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/index.html.

**Understanding Easy VPN**

Cisco Easy VPN, a software enhancement for several kinds of Cisco devices, greatly simplifies VPN deployment for remote offices and teleworkers. Easy VPN centralizes VPN management across many devices, thus reducing the complexity of VPN deployments. Easy VPN implementations require that you use both a Cisco Easy VPN Server and the Cisco Easy VPN Remote feature in your supported devices.

Supported routers, appliances, firewalls, and concentrators act like remote VPN clients when you use Easy VPN. As such, these devices can receive security policies from an Easy VPN server, which minimizes the VPN configuration requirements at remote locations in your organization.

In addition, a device enabled with Cisco Easy VPN Server can terminate VPN tunnels initiated by mobile remote workers who run Cisco VPN client software on their PCs.

Performance Monitor represents all Easy VPN sessions as if they are RAS VPN sessions, even though an Easy VPN server allows supported routers, appliances, firewalls, and concentrators to act as VPN head-end devices in either site-to-site or remote-access VPNs.


- Easy VPN does not support the use of RAS clusters.
- Performance Monitor does not display Easy VPN session usernames, and does not associate usernames with specific Easy VPN sessions.
- The User Session Report feature in Performance Monitor does not support Easy VPN.

**Working in the RAS Clusters Table**

Performance Monitor provides a high-level overview that shows all of your remote access clusters. Use this overview to isolate user data and concentrator data, and display subsets of available cluster statistics.
Performance Monitor updates its record of cluster membership automatically once each day. If you add or delete VPN concentrators in a cluster or if you move a concentrator from one cluster to another, you must select Devices > Importing Devices, then click Revalidate. Otherwise, displayed information is wrong for the relevant cluster until the next automatic update.

**Procedure**

**Step 1** Select Monitor > Remote Access VPN > Clusters. For an explanation of the columns in the table, see Table 5-1.

Performance Monitor averages its measurements of VPN concentrator health and performance to arrive at the high-level statistics it displays for the clusters in your network.

**Step 2** You can do any of the following to further refine the list or to obtain more detailed information:

- To find a device in the list, enter the IP address or DNS name of the device in the Find Device field and click Find. If the device can be found, the Remote Access Device Graphs page displays information about the specified concentrator. For information on the types of graphs, see Viewing Detail Graphs for a RAS Device, page 5-4.

- To display a graph of dropped packets for a RAS cluster, click the relevant entry in the Packet Drop % column.

- To display a throughput graph for a RAS cluster, click the relevant entry in the Throughput (kbps) column.

- To display a graph of bandwidth usage for a RAS cluster, click the relevant entry in the Bandwidth Usage % column.

**Table 5-1  Remote Access Clusters Page**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster column</td>
<td>Displays the DNS name of the virtual cluster master.</td>
</tr>
<tr>
<td>Devices column</td>
<td>Displays the total number of devices in the cluster.</td>
</tr>
<tr>
<td>Master Device column</td>
<td>Displays the IP address of the master device on the specified cluster.</td>
</tr>
<tr>
<td></td>
<td>The virtual cluster master concentrator maintains the load information from all secondary concentrators in the cluster. Each secondary sends load information in the KeepAlive message exchange to the master.</td>
</tr>
<tr>
<td># of Users column</td>
<td>Displays the aggregate total number of active sessions on all RAS devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you or one of your colleagues log out a RAS user, this value might differ the next time the display is refreshed.</td>
</tr>
<tr>
<td>Load Variance column</td>
<td>Indicates skew, calculated by measuring the difference between the device with the highest load and the device with the lowest load.</td>
</tr>
<tr>
<td></td>
<td>Device load is calculated as a percentage of current active sessions divided by the configured maximum-allowed connections.</td>
</tr>
</tbody>
</table>
Working with RAS Devices

See the following topics to learn how to isolate and monitor information that describes the status of any validated VPN concentrator:

- Viewing Detail Graphs for a RAS Device, page 5-4
- Monitoring RAS Device Usage and Activity, page 5-6
- Monitoring RAS Device Failures, page 5-7
- Monitoring RAS Device Crypto Activity, page 5-8
- Viewing RAS Device Crypto Accelerator Card Data, page 5-10
- Viewing the Remote Access Interfaces Table, page 5-10

Viewing Detail Graphs for a RAS Device

You can isolate information about a validated Cisco VPN 3000 Series concentrator in your network and display detailed graphs that describe its health and performance.

Procedure

**Step 1** Select Monitor > Remote Access VPN > Device Details.

By default, the Remote Access Device Graphs page displays graphs that describe the health and performance of whichever device uses the lowest number as its IP address. For a description of the graphs, see Table 5-2.

Table 5-1 Remote Access Clusters Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Drop % column</td>
<td>Displays the computation of dropped packets in IPSec Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all inbound and outbound packets on all RAS devices. Click any hyperlinked entry in the Packets Drop column to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Throughput (kbps) column</td>
<td>Displays the sum of outbound and inbound octets across public interfaces on all RAS devices. Click any hyperlinked entry in the Throughput (kbps) column to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Bandwidth Usage % column</td>
<td>Displays an averaged percentage that shows bandwidth used by all RAS devices, divided by bandwidth available to all RAS devices. Click any hyperlinked entry in the Bandwidth Usage % column to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Inbound Connection Failure % column</td>
<td>Displays an averaged percentage that shows the inbound Phase-1 (IKE) and Phase-2 (IPSec) connections that were initiated remotely and failed, over all inbound connection attempts.</td>
</tr>
</tbody>
</table>

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
A known problem might interfere with your ability to interpret a graph that uses two vertical (Y) axes. The first Y axis always begins at zero, but the second Y axis begins at the lowest value for the specified time range—even when that value is greater than zero. Thus, the two Y axes might not be directly comparable.

**Step 2** Select the device whose graphs you want to view from the **Select Device** list.

## Types of RAS Graphs

<table>
<thead>
<tr>
<th>Table 5-2</th>
<th>Types of RAS Graphs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graph Type</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Bandwidth Utilization | Illustrates percentages of device bandwidth capacity used on the public interface:  
  - The vertical axis shows the average percentage of bandwidth capacity used in a specific polling cycle.  
  - The horizontal axis shows the time of day for the polling cycle. |
| CPU Usage | Illustrates used percentages of device CPU capacity:  
  - The vertical axis shows the average percentage of CPU capacity used in a specific polling cycle.  
  - The horizontal axis shows time of day for the polling cycle. |
| Inbound Connect Failures | Illustrates the trend of inbound connection failures over time:  
  - The vertical axis shows the average number of failures in a specific polling cycle.  
  - The horizontal axis shows time of day for the polling cycle. |
| Throughput vs. Session | Displays a line graph that helps you compare throughput trends to the trend of the number of VPN sessions over time:  
  - Because it shows two kinds of information, it has two vertical axes:  
    - The vertical axis on the left (orange) shows the average throughput in a specific polling cycle, in bytes.  
    - The vertical axis on the right (blue) shows the average number of sessions in a specific polling cycle.  
  - The horizontal axis shows the time of day at which Performance Monitor calculated the trends in each vertical axis. |
| IKE Phase 1 Connection Failures | Illustrates the percentage of failures in Phase-1 (IKE) connections:  
  - The vertical axis shows the average percentage of failed connections in a specific polling cycle.  
  - The horizontal axis shows time of day for the polling cycle. |
| IPSec Phase 2 Connection Failures | Illustrates the percentage of failures in Phase-2 (IPSec) connections:  
  - The vertical axis shows the average percentage of failed connections in a specific polling cycle.  
  - The horizontal axis shows time of day for the polling cycle. |
Monitoring RAS Device Usage and Activity

Performance Monitor provides a high-level overview that shows all of the validated Cisco VPN 3000 Series concentrators that are providing RAS VPN services in any cluster in your network. Use this overview to:

- Isolate data that describe VPN concentrator usage and activity, concentrator failures, and concentrator cryptographic activity.
- View tables and graphs that summarize the condition of any VPN concentrator.

Procedure

Step 1

Select **Monitor > Remote Access VPN > Devices**. For an explanation of the columns in the table, see Table 5-3.

The Remote Access Devices page displays a table of concentrator usage and activity statistics. All measured values on the page are computed as *deltas* (meaning they indicate the scope of difference from one polling cycle to the next)—except for the whole number count of current users.

**Note**

If you or one of your colleagues log out a RAS user, the whole number count of current users might differ the next time the display is refreshed.

Step 2

You can do any of the following to further refine the list or to obtain more detailed information:

- To limit the list to only those devices in a specific cluster, select the cluster in the **Select Cluster** list. Note that Easy VPN does not support the use of RAS clusters.
- To display detailed graphs for one concentrator, click the IP address or DNS name in the Device column.
- To display a graph of dropped packets for one concentrator, click the relevant entry in the Packet Drop % column.
- To display a throughput graph for one concentrator, click the relevant entry in the Throughput (kbps) column.
- To display a graph of bandwidth usage for one concentrator, click the relevant entry in the Bandwidth Usage % column.

Reference

**Table 5-3 Remote Access Devices**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe RAS errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14. <strong>Note</strong> After you clear an event, the alert icon continues to be displayed in the device monitoring pages for up to a minute or until the page is refreshed, whichever occurs first.</td>
</tr>
</tbody>
</table>
## Table 5-3  Remote Access Devices (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device column</td>
<td>Displays the device IP address or DNS name. Click any hyperlinked Device column entry to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Cluster column</td>
<td>Displays the DNS name of the virtual cluster master.</td>
</tr>
<tr>
<td>Model column</td>
<td>Displays the Cisco device model name and number.</td>
</tr>
<tr>
<td># Of Users column</td>
<td>Displays the number of active sessions.</td>
</tr>
<tr>
<td>Note</td>
<td>If you or one of your colleagues log out a RAS user, this value might differ the next time the display is refreshed.</td>
</tr>
<tr>
<td>Packet Drop % column</td>
<td>Displays a computation of the dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all inbound and outbound packets. Click any hyperlinked Packet Drop % column entry to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Packets In column</td>
<td>Displays the number of inbound packets.</td>
</tr>
<tr>
<td>Packets Out column</td>
<td>Displays the number of outbound packets.</td>
</tr>
<tr>
<td>Throughput (kbps) column</td>
<td>Displays the sum of outbound and inbound octets through the public interface on the specified RAS device. Click any hyperlinked Throughput (kbps) column entry to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Bandwidth Usage % column</td>
<td>Displays the percentage of bandwidth used by the specified RAS device, divided by the bandwidth available to it. Click any hyperlinked Bandwidth Usage column entry to open a new browser that displays your selection as a graph.</td>
</tr>
<tr>
<td>Last Updated column</td>
<td>Displays the most recent date and time at which Performance Monitor polled the device.</td>
</tr>
</tbody>
</table>

### Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

## Monitoring RAS Device Failures

You can display and work from a table that describes the operational failures of your validated VPN concentrators.

### Procedure

**Step 1**  Select **Monitor > Remote Access VPN > Devices > Failures**. For an explanation of the columns in the table, see Table 5-4.

All measured values on the Remote Access Failures page are computed as deltas.
Step 2  You can refine the list and also get more detail:

- To limit the list to only those devices in a specific cluster, select the cluster in the Select Cluster list. Note that Easy VPN does not support the use of RAS clusters.
- To display detailed statistics for one VPN concentrator, click the IP address or DNS name in the Device column. See Working with RAS Devices, page 5-4.

### Table 5-4  Remote Access Failures

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe RAS errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
<tr>
<td>Device column</td>
<td>Displays the device DNS name or IP address. Click any Device column entry to display performance summary graphs for the selected device.</td>
</tr>
<tr>
<td>Inbound Connect Failure % column</td>
<td>Displays the percentage of all inbound connection attempts that failed during Phase-1 (IKE) or Phase-2 (IPSec) and were initiated remotely.</td>
</tr>
<tr>
<td>IKE Phase 1 Failure % column</td>
<td>Displays the percentage of Phase-1 (IKE) tunnels that were initiated locally and failed to activate.</td>
</tr>
<tr>
<td>IPSec Phase 2 Failure % column</td>
<td>Displays the percentage of received Phase-2 (IPSec) exchanges that were invalid and rejected.</td>
</tr>
<tr>
<td>Replays column</td>
<td>Displays the total number of inbound packets dropped (because of anti-replay processing) by all current and previous Phase-2 (IPSec) tunnels.</td>
</tr>
</tbody>
</table>

### Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

### Monitoring RAS Device Crypto Activity

You can display and work from a high-level table of cryptographic activity data for validated VPN concentrators.

**Note**  Displayed results do not include the VPN 3005 Concentrator or the VPN 3015 Concentrator. These devices use software encryption instead of scalable encryption processor (SEP) cards.
## Procedure

**Step 1** Select Monitor > Remote Access VPN > Devices > Cryptos. For an explanation of the columns in the table, see Table 5-5. All measured values on the Remote Access Cryptos page are computed as deltas, except for the whole number count of SEP cards.

**Step 2** You can refine the list and also get more detail:
- To limit the list to only those devices in a specific cluster, select the cluster in the Select Cluster list. Note that Easy VPN does not support the use of RAS clusters.
- To display detailed statistics for one VPN concentrator, click the IP address or DNS name in the Device column. See Working with RAS Devices, page 5-4.

## Reference

### Table 5-5 Remote Access Device Cryptos

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe RAS errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
<tr>
<td>Device column</td>
<td>Displays the device IP address or DNS name. Click any Device column entry to display performance graphs for the selected device.</td>
</tr>
<tr>
<td>No. Cards column</td>
<td>Displays the total number of installed scalable encryption processor (SEP) cards in the monitored device.</td>
</tr>
<tr>
<td>Encryption Failure % column</td>
<td>Displays the percentage of outbound encryptions that ended in failure in all currently active Phase-2 (IPSec) tunnels, across all SEP cards.</td>
</tr>
<tr>
<td>Decryption Failure % column</td>
<td>Displays the percentage of inbound decryptions that ended in failure in all currently active Phase-2 (IPSec) tunnels, across all SEP cards.</td>
</tr>
<tr>
<td>Packet Drop % column</td>
<td>Displays the percentage of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels across all SEP cards.</td>
</tr>
<tr>
<td>Encrypted Packets column</td>
<td>Displays the aggregate number of encrypted, outbound packets across all SEP cards.</td>
</tr>
<tr>
<td>Decrypted Packets column</td>
<td>Displays the aggregate number of decrypted, inbound packets across all SEP cards.</td>
</tr>
<tr>
<td>Throughput (Kbps) column</td>
<td>Displays the aggregate number of outbound (encrypted) and inbound (decrypted) octets across all SEP cards, in Kbps.</td>
</tr>
</tbody>
</table>

### Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Chapter 5  Monitoring Remote Access VPN Services

Viewing RAS Device Crypto Accelerator Card Data

You can display and work from a table of cryptographic accelerator card data for one validated VPN concentrator.

Note

Displayed results do not include the VPN 3005 Concentrator or the VPN 3015 Concentrator. These devices use software encryption instead of SEP cards.

Procedure

Step 1
Select Monitor > Remote Access VPN > Device Details > Crypto Status. For an explanation of the columns in the table, see Table 5-6.

All measured values on the Remote Access Cryptos page are computed as deltas.

Step 2
Select the device you want to view from the Select Device list.

Reference

Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Table 5-6  Remote Access Cryptos

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot column</td>
<td>Identifies the number of the slot in the VPN concentrator where the SEP card is installed.</td>
</tr>
<tr>
<td>Status column</td>
<td>Displays a message that describes the functional status of the SEP card.</td>
</tr>
<tr>
<td>Packets In column</td>
<td>Displays the number of decrypted inbound packets on the SEP card.</td>
</tr>
<tr>
<td>Packets Out column</td>
<td>Displays the number of encrypted outbound packets on the SEP card.</td>
</tr>
<tr>
<td>Packet Drop % column</td>
<td>Displays the number of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all decrypted inbound and encrypted outbound packets.</td>
</tr>
<tr>
<td>Throughput (Kbps)</td>
<td>Displays the total number of encrypted outbound and decrypted inbound octets over time on the SEP card.</td>
</tr>
</tbody>
</table>

Viewing the Remote Access Interfaces Table

You can display and work from a table of interface status data for one validated VPN concentrator.
Working with RAS Users

The following topics describe the features with which you monitor RAS users.

- Viewing RAS User Details, page 5-12
- Identifying the Top 10 Users of a RAS Device, page 5-13
- Identifying the Top 10 Users of a RAS Cluster, page 5-14
Viewing RAS User Details

You can isolate and display detailed recent connection information for a single current RAS VPN user. Optionally, you can log out the user you find.

---

**Note**

Finding a user session might take longer than 1 minute if the relevant VPN concentrator has many active sessions.

---

**Tip**

You can also display reports that:

- Rank the top 10 RAS VPN users over a range of time that you specify, according to a trending type that you select. See Viewing RAS VPN Top 10 User Reports, page 10-8.
- Describe the VPN sessions of one or more RAS VPN users over a range of time that you specify. See Viewing RAS VPN User Session Reports, page 10-8.

---

**Before You Begin**

The user logout feature is available to you only if:

- Your CiscoWorks user role is System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.
- The VPN 3000 Concentrator Series Manager is enabled on the relevant VPN concentrator, and Performance Monitor has a record of the correct authentication credentials for that concentrator.

**Procedure**

**Step 1** Select **Monitor > Remote Access VPN > User Lookup**.

**Step 2** Enter the user details:

- **Find User**—Enter the user’s IP address or username.
- **Search In**—If desired, you can restrict your search to either one device or one cluster, and identify the search target by selecting its name or IP address. Select Devices All to not restrict the search to a specific device or cluster.

**Step 3** Click **Go**. If the user is found, the following user session details are shown:

- **User Name**—The user’s login name.
- **Group Name**—The user group to which the user belongs.
- **Cluster Name**—Identifies the cluster by name or IP address, if the VPN concentrator is a cluster member.
- **Device Name**—Identifies the VPN concentrator by name or IP address.
- **Client IP Address**—The user’s IP address.
- **Protocol**—The user’s connection protocol, such as IPSec over UDP.
- **Throughput (Kbps)**—The user’s average throughput per second.
- **Connection Duration**—Measured in days, hours, minutes, and seconds.
Chapter 5  Monitoring Remote Access VPN Services

Working with RAS Users

- Octet In—The total number of inbound octets since tunnel inception.
- Octet Out—The total number of outbound octets since tunnel inception.

**Step 4** *(Optional)* To end the user session, click **Logout**.

If the logout is successful, the specified user is logged out and his or her IP address no longer appears in any table that describes active RAS sessions. A system message tells you “The user <username> was logged out successfully.”

**Related Topics**
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

### Identifying the Top 10 Users of a RAS Device

Performance Monitor can rank the top 10 users who are connected to all validated VPN concentrators or to the validated concentrators in one cluster. The ranking values are determined by throughput, connection duration, or total traffic per user.

**Note**
Performance Monitor ranks the top 10 users on each VPN concentrator. It then ranks only those users against one another when it calculates the top 10 users overall. A user who ranks outside the top 10 for a specific concentrator is excluded from the overall ranking even when the top users for a different concentrator have lower throughput or bandwidth requirements than the excluded user. The top 10 ranking is therefore approximate.

**Before You Begin**
The user logout feature is available to you only if:
- Your CiscoWorks user role is System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.
- The VPN 3000 Concentrator Series Manager is enabled on the relevant VPN concentrator, and Performance Monitor has a record of the correct authentication credentials for that concentrator.

**Procedure**

**Step 1** Select **Monitor > Remote Access VPN > Device Details > Top 10 Device Users**.

All measured values on the Top 10 Device Users page are whole numbers, rather than deltas. For a description of the table columns, see Table 5-8.

**Step 2** Select the device you want to view from the **Select Device** list.

**Step 3** Select the ranking criterion for the calculation of top users from the **Compute Using** list. Your options are:
- Throughput—Ranks users according to their throughput, measured in kbps.
- Connect Duration—Ranks users according to the duration of their current session (in days, hours, minutes, and seconds).
- Total Traffic—Ranks users according to the sum of their inbound and outbound packets.
Working with RAS Users

Step 4  If desired, you can disconnect a user. Ending a user session might take longer than 1 minute if the VPN concentrator has many active sessions.

To log out a user, click the radio button for the user, then click **Logout**. If the logout is successful, the user is logged out and his or her IP address no longer appears in any table that describes active RAS sessions.

Reference

Table 5-8  Top 10 Device Users

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User column</td>
<td>Displays the username that is associated with the current session.</td>
</tr>
<tr>
<td>Note</td>
<td>EzVPN sessions do not support this feature.</td>
</tr>
<tr>
<td>Group column</td>
<td>Displays the user group name that is associated with the username.</td>
</tr>
<tr>
<td></td>
<td>The group name is hyperlinked if the user session is associated with a router that is configured as an Easy VPN server. In this case, you can click the link to open the Details of the Group Policy window. See Details of the Group Policy, page 5-16.</td>
</tr>
<tr>
<td>Public IP Address column</td>
<td>Displays the user IP address.</td>
</tr>
<tr>
<td>Protocol column</td>
<td>Identifies the protocol in use for the described VPN session.</td>
</tr>
<tr>
<td>Traffic In column</td>
<td>Displays the total number of inbound packets.</td>
</tr>
<tr>
<td>Traffic Out column</td>
<td>Displays the total number of outbound packets.</td>
</tr>
<tr>
<td>Total Traffic column</td>
<td>Displays the combined number of inbound and outbound octets.</td>
</tr>
<tr>
<td>Connect Duration column</td>
<td>Displays the number of days, hours, minutes, and seconds since the user established the current session.</td>
</tr>
<tr>
<td>Throughput (Kbps) column</td>
<td>Displays the total number of encrypted outbound and decrypted inbound octets over time per user session.</td>
</tr>
</tbody>
</table>

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Identifying the Top 10 Users of a RAS Cluster

You can rank all users that are connected to a cluster, or rank users across all clusters, excluding any Easy VPN users. Easy VPN does not support the use of RAS clusters.

You can also logout one user at a time, excluding any Easy VPN users.

Before You Begin

The user logout feature is available to you only if:

- Your CiscoWorks user role is System Administrator or Network Administrator. See Understanding User Permissions, page 3-2.
The VPN 3000 Concentrator Series Manager is enabled on the relevant VPN concentrator, and Performance Monitor has a record of the correct authentication credentials for that concentrator.

**Procedure**

**Step 1** Select **Monitor > Remote Access VPN > Top 10 Cluster Users**.

All measured values on the Top 10 Cluster Users page are whole numbers, rather than deltas.

**Step 2** Select the cluster you want to view from the **Select Cluster** list. Select All to not restrict the report to a specific cluster.

**Step 3** Select the ranking criterion for the calculation of top users from the **Compute Using** list. Your options are:

- Throughput—Ranks users according to their throughput, measured in kbps.
- Connect Duration—Ranks users according to the duration of their current session (in days, hours, minutes, and seconds).
- Total Traffic—Ranks users according to the sum of their inbound and outbound packets.

**Step 4** If desired, you can disconnect a user. Ending a user session might take longer than 1 minute if the VPN concentrator has many active sessions.

To log out a user, click the radio button for the user, then click **Logout**. If the logout is successful, the user is logged out and his or her IP address no longer appears in any table that describes active RAS sessions.

**Reference**

**Table 5-9** **Top 10 Cluster Users**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User column</td>
<td>Displays the authenticated username for the current session.</td>
</tr>
<tr>
<td>Group column</td>
<td>Displays the user group name entry that is associated with the named user.</td>
</tr>
<tr>
<td>Public IP column</td>
<td>Displays the user’s public IP address.</td>
</tr>
<tr>
<td>Protocol column</td>
<td>Identifies which Layer 2 protocol type is used for this VPN session: IPSec, L2TP, or PPTP.</td>
</tr>
<tr>
<td>Traffic In column</td>
<td>Displays the number of inbound packets.</td>
</tr>
<tr>
<td>Traffic Out column</td>
<td>Displays the number of outbound packets.</td>
</tr>
<tr>
<td>Total Traffic column</td>
<td>Displays the combined number of inbound and outbound octets.</td>
</tr>
<tr>
<td>Connect Duration column</td>
<td>Displays the number of seconds since the active session began.</td>
</tr>
<tr>
<td>Throughput (kbps) column</td>
<td>Displays the number of outbound octets, added to the number of inbound octets, per user session.</td>
</tr>
</tbody>
</table>
Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Details of the Group Policy

The following table describes the fields for the group policy that is assigned to a user session when the session is associated with a router that is configured as an Easy VPN server. For information on opening this window, see Identifying the Top 10 Users of a RAS Device, page 5-13 or Identifying the Top 10 Users of a RAS Cluster, page 5-14.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name row</td>
<td>Displays the user group name that is associated with the username in the relevant session.</td>
</tr>
<tr>
<td>Pool Name row</td>
<td>Displays the name of the IP local pool address, which defines a range of addresses from which to allocate an internal IP address to a client. Although a user must define at least one pool name, a separate pool may be defined for each group policy. This attribute must be defined and must refer to a valid IP local pool address, or the client connection will fail.</td>
</tr>
<tr>
<td>DNS Servers row</td>
<td>Displays a comma-separated list of the IP addresses for all of the DNS servers that the specified group uses.</td>
</tr>
<tr>
<td>WINS Servers row</td>
<td>Displays a comma-separated list of the IP addresses for all of the WINS servers that the specified group uses.</td>
</tr>
<tr>
<td>Domain Name row</td>
<td>Displays the DNS-resolvable domain name that the group uses, such as cisco.com.</td>
</tr>
<tr>
<td>ACL row</td>
<td>Sometimes displays the name of an ACL that defines which traffic is to be encrypted. The ACL name is shown only when you configure split-tunneling for the relevant group.</td>
</tr>
<tr>
<td>Backup Gateway row</td>
<td>Displays the IP address or hostname of the backup gateway that the router is configured to try first if the connection to the primary Easy VPN server fails.</td>
</tr>
<tr>
<td>Firewall Are-U-There row</td>
<td>Shows whether any clients have sent a signal to the server group to indicate that their VPN sessions pass through the Black Ice or Zone Alarm personal firewalls.</td>
</tr>
<tr>
<td>Include-local-lan row</td>
<td>Indicates whether an attribute is set for the group that (without the use of split-tunneling) supports simultaneous connections to the client and to a local network—sometimes called a “stub” network—that sends all non-local traffic on the default route 0.0.0.0/0.</td>
</tr>
<tr>
<td>Group Lock row</td>
<td>Indicates whether an attribute is set for the server group so that its users can supply Xauth usernames, including a group name, when preshared key authentication uses IKE. <strong>Note</strong> We recommend that clients who use RSA signature authentication mechanisms such as certificates not use the Group-Lock attribute. Instead, such clients should use the User-VPN-Group attribute.</td>
</tr>
<tr>
<td>Save Password row</td>
<td>Indicates whether an option is enabled for the server group that allows users to save their XAuth credentials locally on their client PCs.</td>
</tr>
</tbody>
</table>

**Note** No equivalent information is available for Easy VPN sessions that originate from PIX Security Appliances.
Monitoring Site-to-Site VPN Services

Site-to-site VPN monitoring provides all the most important indicators of device and tunnel performance at a glance. Performance Monitor also enables you to determine quickly whether site-to-site problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users.

Site-to-site VPNs permit connections between:

- An organization’s headquarters, remote offices, and branch offices.
- An organization’s intranet and its trusted partners, suppliers, customers, or communities of interest.

Performance Monitor monitors site-to-site VPN services in:

- Cisco IOS VPN routers.
- Cisco Catalyst 6500 series switches in which one or more supported services modules are installed.
- Cisco VPN 3000 Series concentrators.
- Adaptive Security Appliances.
- PIX Security Appliances (also known as PIX firewalls).

---

**Note**
Performance Monitor represents all Easy VPN sessions as if they are RAS VPN sessions, even though an Easy VPN server allows supported routers, appliances, firewalls, and concentrators to act as VPN head-end devices in *either* site-to-site or remote-access VPNs. See Understanding Easy VPN, page 5-2.

---

**Tip**
To troubleshoot common problems with site-to-site VPN services, see the Troubleshooting appendix.

The following topics explain the site-to-site VPN monitoring features:

- Understanding DMVPN, page 6-2
- Working with Site-to-Site Devices, page 6-3
- Working with Site-to-Site Device Details, page 6-6
- Working with Site-to-Site Tunnels, page 6-9
Understanding DMVPN

The Dynamic Multipoint VPN (DMVPN) feature on Cisco IOS routers provides a simple and scalable way to create large and small IPsec VPNs by combining GRE tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP). In NHRP, the hub maintains a database of public IP addresses for all spokes. Spokes in a DMVPN network register their public IP addresses with the hub during every boot session. Source spokes query the NHRP database on the hub to obtain the public IP address of destination spokes. A multipoint GRE tunnel interface enables a single GRE tunnel to support multiple IPSec tunnels. This method reduces complexity.

DMVPN supports two configurations, hub-to-spoke and spoke-to-spoke.

- The benefits of a hub-to-spoke deployment include:
  - Simplified and smaller configurations for hub and spoke.
  - Zero-touch provisioning for adding new spokes to the VPN.
  - Support for dynamically addressed spokes.
  - Support for multicast traffic from hub to spokes.

- The benefits of a spoke-to-spoke deployment include all of the benefits from a hub and spoke deployment, plus:
  - Direct dynamic spoke-to-spoke tunnels.
  - Support for participation by smaller spokes in the virtual full mesh.

In addition, Performance Monitor enables you to select a third option, spoke-to-hub. Spoke-to-hub is not actually a configuration that you can deploy. Instead, it is a convenience in Performance Monitor that enables you to select a spoke and quickly identify its associated hub.

In Performance Monitor, DMVPN usage is represented in the Tunnels page, where any displayed results are constrained by your selections from the Select Tunnel Type list. See Displaying the Site-to-Site Device Tunnels Table, page 6-9.

Note
You might receive a flood of email messages about your DMVPN spoke-to-spoke tunnels if you do all of the following:

- Configure DMVPN to use a full mesh topology that supports spoke-to-spoke sessions.
- Configure a threshold for site-to-site VPN tunnel down events.
- Schedule automatic email notification for those events.

Site-to-site tunnels are dynamic and have short lives by design, which include many tunnel down events. If this email flood problem affects you, we recommend that you either disable email notification or configure Performance Monitor to monitor hubs only.

DMVPN and Easy VPN Comparison

The following table describes major differences between DMVPN and Easy VPN. To learn more about Easy VPN and how it is represented in Performance Monitor, see Understanding Easy VPN, page 5-2.
Chapter 6  Monitoring Site-to-Site VPN Services

Working with Site-to-Site Devices

The following topics explain how you can monitor the status of individual devices and modules that provide site-to-site VPN services.

- Monitoring Site-to-Site Device Usage and Activity, page 6-3
- Monitoring Site-to-Site Device Failures, page 6-4
- Monitoring Site-to-Site Device Crypto Activity, page 6-5

Table 6-1  Comparison of DMVPN and Easy VPN

<table>
<thead>
<tr>
<th>Service/Feature Name</th>
<th>DMVPN</th>
<th>Easy VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for multicast traffic</td>
<td>Yes.</td>
<td>—</td>
</tr>
<tr>
<td>Spoke-to-spoke communication</td>
<td>Yes.</td>
<td>—</td>
</tr>
<tr>
<td>Support for GRE/Quality of Service</td>
<td>Yes.</td>
<td>—</td>
</tr>
<tr>
<td>Support for routing protocols</td>
<td>Yes.</td>
<td>—</td>
</tr>
<tr>
<td>Support for certificates</td>
<td>Yes.</td>
<td>—</td>
</tr>
<tr>
<td>Stateful failover</td>
<td>Depends on routing protocol for recovery.</td>
<td>Yes.</td>
</tr>
<tr>
<td>Scalability per hub</td>
<td>Because of routing protocols, DMVPN hubs</td>
<td>Supports many spokes per hub.</td>
</tr>
<tr>
<td></td>
<td>support fewer spokes per hub.</td>
<td></td>
</tr>
<tr>
<td>Identical configuration for all spokes</td>
<td>—</td>
<td>Yes.</td>
</tr>
<tr>
<td>Cross-platform support</td>
<td>—</td>
<td>Yes.</td>
</tr>
<tr>
<td>Support for software or hardware clients</td>
<td>Hardware client only.</td>
<td>Yes.</td>
</tr>
<tr>
<td>Always up tunnel to hub</td>
<td>Yes.</td>
<td>Not required.</td>
</tr>
</tbody>
</table>

Working with Site-to-Site Devices

You can display and work from a table of usage and activity statistics for any of the validated site-to-site devices or service modules in your network. You can view all of your devices or only those in specific groups. You can use this overview to:

- Isolate descriptions of device usage and activity, device failures, and device crypto activity.
- Display charts and graphs that summarize the condition of any device or module that provides site-to-site VPN services.

To view the site-to-site device table, select Monitor > Site-to-Site VPN > Devices. For an explanation of the columns in this table, see Table 6-2.

Following are some of the things you can do using this table:

- Display only the devices in one user-defined device group, or display all devices—Select a group name from the Select Group list. The refreshed page lists only the devices in the specified group. The default is to display all devices. Note that some of your monitored devices might not belong to any user-defined device groups.
- Open an Event Browser that displays only the critical errors (P1 or P2) for a specific device or service module—Click the alert icon in the Alert column for the device.
Chapter 6  Monitoring Site-to-Site VPN Services

Working with Site-to-Site Devices

Note  The Alert column is empty for a device or module without any critical errors.

- Display charts and graphs that summarize the overall condition of one device or service module—Click the DNS name or IP address in the Device column.
- Display a throughput graph for one device or service module—Click a hyperlinked entry in the Throughput (Kbps) column.
- Display a graph of dropped packets for one device or service module—Click a hyperlinked entry in the Packet Drop % column.

Table 6-2  Site-to-Site Devices Table

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe site-to-site VPN errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
<tr>
<td>Note</td>
<td>After you clear an event, the alert icon continues to be displayed in the device monitoring pages for up to a minute or until the page is refreshed, whichever occurs first.</td>
</tr>
<tr>
<td>Device column</td>
<td>Displays the device IP address or DNS name.</td>
</tr>
<tr>
<td>Model column</td>
<td>Displays the Cisco device model name.</td>
</tr>
<tr>
<td>CPU Usage % column</td>
<td>Displays the average used percentage of total CPU capacity.</td>
</tr>
<tr>
<td>Memory Usage % column</td>
<td>Displays the average used percentage of total processor memory capacity since the previous polling cycle.</td>
</tr>
<tr>
<td>Throughput (Bps) column</td>
<td>Displays the sum of inbound and outbound octets through the public interface since the previous polling cycle, in bytes.</td>
</tr>
<tr>
<td>No. Tunnels column</td>
<td>Displays the combined number of active and inactive tunnels since the previous polling cycle.</td>
</tr>
<tr>
<td>Packets In column</td>
<td>Displays the number of packets received through all active Phase-1 (IKE) and Phase-2 (IPSec) tunnels since the previous polling cycle.</td>
</tr>
<tr>
<td>Packets Out column</td>
<td>Displays the number of packets sent through all active Phase-1 (IKE) and Phase-2 (IPSec) tunnels since the previous polling cycle.</td>
</tr>
<tr>
<td>Packet Drop % column</td>
<td>Displays the number of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels since the previous polling cycle as a percentage of all such inbound and outbound packets.</td>
</tr>
<tr>
<td>Last Updated column</td>
<td>Displays the most recent date and time at which Performance Monitor polled the device.</td>
</tr>
</tbody>
</table>

Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Monitoring Site-to-Site Device Failures

To display and work from a table that describes the operational failures of validated site-to-site devices and service modules, select Monitor > Site-to-Site VPN > Devices > Failures.
All measured values on the Site-to-Site Failures page are computed as deltas. For a description of the columns, see Table 6-3.

To display charts and graphs that summarize the overall condition of one device or service module in the Failures table, click the relevant DNS name or IP address in the Device column.

**Table 6-3**  
**Site-to-Site Device Failures**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe site-to-site VPN errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
<tr>
<td>Device column</td>
<td>Displays the device DNS name or IP address.</td>
</tr>
<tr>
<td>Inbound Connection</td>
<td>Displays the inbound Phase-1 (IKE) and Phase-2 (IPSec) connections that were initiated remotely and failed, as a percentage of all connection attempts (inbound and outbound).</td>
</tr>
<tr>
<td>Failure % column</td>
<td>Displays the outbound Phase-1 (IKE) and Phase-2 (IPSec) connections that were initiated locally and failed, as a percentage of all outbound connection attempts.</td>
</tr>
<tr>
<td>Outbound Connection</td>
<td>Displays the total number of inbound packets dropped (because of anti-replay processing) by all current and previous IPSec Phase-2 tunnels.</td>
</tr>
<tr>
<td>Failure % column</td>
<td>Displays the sum of inbound and outbound connection failures over all exchanges.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

**Monitoring Site-to-Site Device Crypto Activity**

To display and work from a table of cryptographic activity on any validated site-to-site device, select Monitor > Site-to-Site VPN > Devices > Cryptos.

The Site-to-Site Cryptos page describes the encryption and decryption activities of your VPN routers and IPSec VPN service modules. All measured values on the Site-to-Site Cryptos page are computed as deltas. For a description of the columns, see Table 6-4.

To display charts and graphs that summarize the overall condition of one device or service module in the Crypto Activity table, click the relevant DNS name or IP address in the Device column.

**Table 6-4**  
**Site-to-Site Cryptos Page**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe site-to-site VPN errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
</tbody>
</table>
### Displaying and Interpreting Site-to-Site Device Detail Graphs

You can display a graphical representation of the status of any validated device in any of your site-to-site VPNs.

**Procedure**

1. **Step 1**
   Select *Monitor > Site-to-Site VPN > Device Details.*

   Initially, Performance Monitor displays graphs that describe the health and performance of whichever device uses the lowest number as its IP address. For a description of the graphs, see Table 6-5.

   **Note**
   A known problem might interfere with your ability to interpret a graph that uses two vertical (Y) axes. The first Y axis always begins at zero, but the second Y axis begins at the lowest value for the specified time range—even when that value is greater than zero. Thus, the two Y axes might not be directly comparable.

2. **Step 2**
   Select the device whose graphs you want to view from the *Select Device* list.
## Types of Site-to-Site Graphs

**Table 6-5**  
**Types of Site-to-Site Device Graphs**

<table>
<thead>
<tr>
<th>Graph Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CPU Usage**               | Illustrates the used percentage of device CPU capacity:  
|                             | • The vertical axis shows the average percentage of CPU capacity used in a specific polling cycle.  
|                             | • The horizontal axis shows the time of day for the polling cycle.                                                                                                                                         |
| **Memory Usage**            | Illustrates the used percentage of device memory capacity:  
|                             | • The vertical axis shows the average percentage of memory capacity used in a specific polling cycle.  
|                             | • The horizontal axis shows the time of day for the polling cycle.                                                                                                                                         |
| **Packet Drops**            | Illustrates the percentage of dropped packets in site-to-site VPN tunnels:  
|                             | • The vertical axis shows the average percentage of dropped packets in a specific polling cycle.  
|                             | • The horizontal axis shows time of day for the polling cycle.                                                                                                                                             |
| **Throughput vs. No. Tunnels** | Displays a line graph that helps you compare throughput trends to the trend of the number of tunnels in use over time:  
|                             | • Because it shows two kinds of information, it has two vertical axes:  
|                             |   • The vertical axis on the left (orange) shows the average throughput for a specific polling cycle, in bytes per second.   
|                             |   • The vertical axis on the right (blue) shows the average number of tunnels in a specific polling cycle.  
|                             | • The horizontal axis shows the time of day at which Performance Monitor calculated the trends in each vertical axis.                                                                                     |
| **Inbound Connection Failures** | Illustrates the trend of inbound connection failures over time:  
|                             | • The vertical axis shows the average number of failures in a specific polling cycle.  
|                             | • The horizontal axis shows the time of day for the polling cycle.                                                                                                                                         |
| **Outbound Connection Failures** | Illustrates the trend of outbound connection failures over time:  
|                             | • The vertical axis shows the average number of failures in a specific polling cycle.  
|                             | • The horizontal axis shows the time of day for the polling cycle.                                                                                                                                         |

**Related Topics**

- [Optional Tasks in Performance Monitor Tables, page 3-9](#)
- [Common Elements in Tables, page 3-8](#)
Displaying the Site-to-Site Device Interfaces Table

You can display and work from a table of site-to-site device interface performance and activity statistics.

**Procedure**

**Step 1** Select Monitor > Site-to-Site VPN > Device Details > Interfaces. For an explanation of the columns in the table, see Table 6-6.

The Site-to-Site Interfaces page describes device interfaces that are either bound to a crypto map or that are of Internet Assigned Number Authority (IANA) interface type 131—tunnel.

All measured values on the Site-to-Site Interfaces page are computed as deltas.

**Step 2** Select the device you want to view from the Select Device list.

By default, only the VPN interfaces are listed in the table. However, you can select All Interfaces from the Select Interfaces list to see all of the interfaces for the device.

**Reference**

**Table 6-6** Site-to-Site Interfaces Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descr column</td>
<td>Provides a specific description of the physical interface. For example, DEC 21143A PCI Fast Ethernet.</td>
</tr>
<tr>
<td>Address column</td>
<td>Displays the interface MAC address.</td>
</tr>
<tr>
<td>Admin Status column</td>
<td>Displays either Up or Down.</td>
</tr>
<tr>
<td>Operation Status column</td>
<td>Displays either Up or Down.</td>
</tr>
<tr>
<td>Type column</td>
<td>Displays the frame type to which TCP/IP is bound. For example, a displayed type of iso88023-csmacd indicates a frame type of 100 MBits/s FastEthernet that applies CSMACD (carrier sense multiple access/collision detection).</td>
</tr>
<tr>
<td>Speed (Kbps) column</td>
<td>Displays the interface speed in Kbps.</td>
</tr>
<tr>
<td>Packet In column</td>
<td>Displays the total number of packets received on the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Packet Out column</td>
<td>Displays the total number of packets sent from the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Packet Drop % column</td>
<td>Displays the total percentage of packets dropped since the previous polling cycle.</td>
</tr>
<tr>
<td>Throughput (Bps) column</td>
<td>Displays the average interface throughput rate in bytes.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Working with Site-to-Site Tunnels

The following topics describe ways to work with tunnels in site-to-site VPNs.

- Displaying the Site-to-Site Device Tunnels Table, page 6-9
- Finding a Site-to-Site VPN Tunnel, page 6-10

Displaying the Site-to-Site Device Tunnels Table

You can display and work from a table of VPN tunnels on all of your validated site-to-site devices, or display the tunnels on one device.

To display the list of tunnels, select Monitor > Site-to-Site VPN > Device Details > Tunnels.

By default, the Tunnels page describes tunnels on all of your validated site-to-site devices. The displayed values are whole numbers, computed since tunnel inception.

You can filter the list using the drop-down lists above the table:

- Select Device—Select the IP address of a device to display information about VPN tunnels on that device.
- Select Tunnel Type—Select a DMVPN tunnel type for viewing, or view all site-to-site tunnels, or learn which hub a device uses.
  - All — View all DMVPN tunnels for the selected device.
  - DMVPN Hub-Spoke — View only the hub-to-spoke DMVPN tunnels for the selected device.
  - DMVPN Spoke-Hub — This option is a convenience in Performance Monitor that enables you to quickly identify which hub is associated with a spoke that you select from the Select Device list.
  - DMVPN Spoke-Spoke — View only the spoke-to-spoke DMVPN tunnels. These tunnels are dynamic and can have very short lifetimes that generate many tunnel up and tunnel down events.

The following table describes the columns in the tunnels table.

<table>
<thead>
<tr>
<th>Table 6-7 Tunnels Page</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Endpoint column</td>
<td>Displays the IP address of the local endpoint device interface at which the tunnel terminates.</td>
</tr>
<tr>
<td></td>
<td>In the case of a DMVPN tunnel, you can click the hyperlinked IP address to see the remote IP address and the time at which the tunnel is scheduled to expire.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The identity of the “local” endpoint device might vary in Performance Monitor, because its definition is always relative to the device that you monitor.</td>
</tr>
<tr>
<td>Remote Endpoint column</td>
<td>Displays the IP address of the remote endpoint device interface at which the tunnel terminates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The identity of the “remote” endpoint device might vary in Performance Monitor, because its definition is always relative to the device that you monitor.</td>
</tr>
</tbody>
</table>
Chapter 6  Monitoring Site-to-Site VPN Services

Working with Site-to-Site Tunnels

You can locate, isolate, and display the properties of a single tunnel.

Procedure

Step 1  Select Monitor > Site-to-Site VPN > Tunnel Lookup.
The Site-to-Site Tunnel Lookup page appears.

Step 2  To identify one tunnel, enter:
• The IP address of the endpoint device interface at which one end of the tunnel terminates.
• The IP address of the endpoint device interface at which the opposite end of the same tunnel terminates.

Step 3  Click Go. If the tunnel is found, the page displays the details for the tunnel. For an explanation of the columns, see Displaying the Site-to-Site Device Tunnels Table, page 6-9.

Related Topics
• Optional Tasks in Performance Monitor Tables, page 3-9
• Common Elements in Tables, page 3-8

Table 6-7 Tunnels Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Subnet column</td>
<td>Taken together, the values in these three columns define the access list for one tunnel:</td>
</tr>
<tr>
<td>Remote Subnet column</td>
<td>• Local Subnet—Displays the tunnel subnet and mask on the local endpoint device.</td>
</tr>
<tr>
<td>Protocol column</td>
<td>• Remote Subnet—Displays the tunnel subnet and mask on the remote endpoint device.</td>
</tr>
<tr>
<td></td>
<td>• Protocol—Displays the tunnel protocol and the port used, such as TCP 80.</td>
</tr>
<tr>
<td>Status column</td>
<td>Displays either Up or Down.</td>
</tr>
<tr>
<td>Active Time column</td>
<td>Displays the tunnel lifetime in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Auth Fail In column</td>
<td>Displays the number of authentication failures for inbound packets since tunnel inception.</td>
</tr>
<tr>
<td>Auth Fail Out column</td>
<td>Displays the number of authentication failures for outbound packets since tunnel inception.</td>
</tr>
<tr>
<td>Packets In column</td>
<td>Displays the number of inbound packets since tunnel inception.</td>
</tr>
<tr>
<td>Packets Out column</td>
<td>Displays the number of outbound packets since tunnel inception.</td>
</tr>
<tr>
<td>Packet Drop % column</td>
<td>Displays dropped packets as a percentage of all inbound and outbound packets since tunnel inception.</td>
</tr>
<tr>
<td>Throughput (Bps) column</td>
<td>Displays the sum of inbound and outbound octets through the tunnel since tunnel inception, in bytes.</td>
</tr>
<tr>
<td>Last Update column</td>
<td>Displays the most recent date and time at which Performance Monitor polled the device.</td>
</tr>
</tbody>
</table>

Related Topics
• Optional Tasks in Performance Monitor Tables, page 3-9
• Common Elements in Tables, page 3-8
Monitoring Firewall Services

Performance Monitor determines the condition of firewall services provided through Cisco Adaptive Security appliances, Cisco Secure PIX Firewall devices and through firewall services modules (FWSM) in Cisco Catalyst 6500 switches.

The following topics explain the firewall monitoring features:

- Working in the Firewall Devices Table, page 7-1
- Working With Firewall Device Details, page 7-2

Tip
To troubleshoot common problems with firewall services, see the Troubleshooting appendix.

Working in the Firewall Devices Table

Performance Monitor provides a high-level overview that shows all of your validated firewall devices, modules, and security contexts in a table. You can use this table to isolate descriptions of their status, usage, and errors.

Procedure

Step 1
Select Monitor > Firewall > Devices. For an explanation of the columns in the table, see Table 7-1.

Step 2
You can do any of the following to further refine the list or to obtain more detailed information:

- To limit the list to show only the virtual contexts of a single device, select the admin context of the device from the Select Admin Context list. The default setting is to show all, which lists all firewalls, including all virtual contexts.
- To open an event browser and display severe firewall errors only, click the alert icon when it is in the Alert column.
- To display graphs that summarize the condition of a single device, module, or context, click the IP address or DNS name of a device, module, or context where it appears in the Device column.
Working With Firewall Device Details

The following topics explain the monitoring features for a single firewall device or module:

- Displaying and Interpreting Device or Module Detail Graphs, page 7-3
- Displaying the Device or Module Interfaces Table, page 7-4
- Displaying the Device or Module Blocks Table, page 7-5
- Displaying the Device or Module Connections Table, page 7-5

Reference

Table 7-1  Firewall Devices Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe firewall errors only. See Understanding Interface Icons, page 3-5.</td>
</tr>
<tr>
<td></td>
<td>For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
<tr>
<td></td>
<td>Note After you clear an event, the alert icon continues to be displayed in the device monitoring pages for up to a minute or until the page is refreshed, whichever occurs first.</td>
</tr>
<tr>
<td>Device column</td>
<td>Displays the DNS name or IP address of the relevant firewall.</td>
</tr>
<tr>
<td></td>
<td>Note A router is displayed in the Firewall Devices page only if at least one interface is configured with an inspection policy.</td>
</tr>
<tr>
<td>Model column</td>
<td>Describes the hardware model of the relevant appliance, device, or services module.</td>
</tr>
<tr>
<td>Version column</td>
<td>Indicates the Cisco firewall software release version that is installed on the relevant firewall.</td>
</tr>
<tr>
<td>Memory Usage % column</td>
<td>Displays the percentage of bytes from memory that the relevant firewall is using.</td>
</tr>
<tr>
<td>CPU Usage % column</td>
<td>Displays the current percentage of CPU capacity in use, averaged over the most recent 5 seconds.</td>
</tr>
<tr>
<td>No. Connections column</td>
<td>Displays the total number of active connections on the relevant firewall.</td>
</tr>
<tr>
<td>Xlates column</td>
<td>Displays the number of active translations on the relevant firewall.</td>
</tr>
<tr>
<td>Packet Rate In column</td>
<td>Displays the sum of the current rate of inbound packets across all interfaces.</td>
</tr>
<tr>
<td>Packet Rate Out column</td>
<td>Displays the sum of the current rate of outbound packets across all interfaces.</td>
</tr>
<tr>
<td>No. Errors column</td>
<td>Displays the number of inbound packet errors since the previous polling cycle, aggregated over all firewall interfaces.</td>
</tr>
<tr>
<td>Throughput (Kbps) column</td>
<td>Displays average throughput speed per second on the relevant firewall, aggregated across all its interfaces, since the previous polling cycle.</td>
</tr>
<tr>
<td>Last Updated column</td>
<td>Displays the time at which polling or traps provided the displayed values.</td>
</tr>
</tbody>
</table>

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Working With Firewall Device Details

The following topics explain the monitoring features for a single firewall device or module:
Displaying and Interpreting Device or Module Detail Graphs

You can display and work from graphs that illustrate CPU usage, memory usage, interface errors, throughput, and connections for one validated firewall device or module.

Step 1

Select **Monitor > Firewall > Device Details.**

By default, Performance Monitor displays graphs that describe the health and performance of whichever device or module uses the lowest number as its IP address. For a description of the graphs, see Table 7-2.

*Note* A known problem might interfere with your ability to interpret a graph that uses two vertical (Y) axes. The first Y axis always begins at zero, but the second Y axis begins at the lowest value for the specified time range—even when that value is greater than zero. Thus, the two Y axes might not be directly comparable.

Step 2

Select the device whose graphs you want to view from the Select Device list.

Types of Firewall Graphs

<table>
<thead>
<tr>
<th>Graph Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
<td>Illustrates used percentages of device or module CPU capacity:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the average percentage of CPU capacity used in the relevant polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>Illustrates used percentages of device or module memory capacity:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the average percentage of memory capacity used in the relevant polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
<tr>
<td>Throughput vs. Connection</td>
<td>Displays a line graph that helps you compare throughput trends to connection trends over time:</td>
</tr>
<tr>
<td></td>
<td>• Because it shows two kinds of information, it has two vertical axes.</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis on the left (orange) shows the average throughput in bytes in the relevant polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis on the right (blue) shows the average number of firewall connections in the relevant polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day at which Performance Monitor calculated the trends in each vertical axis.</td>
</tr>
<tr>
<td>Interface Error</td>
<td>Illustrates the trend of device or module interface errors over time:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the average number of errors in the relevant polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
</tbody>
</table>
Displaying the Device or Module Interfaces Table

You can display and work from a table of interface performance statistics for one validated firewall device or module.

Note

The interfaces of those routers on which an inspection policy is configured are displayed in the Firewall Interfaces page. However, for PIX, ASA, and FWSM devices, all interfaces are displayed.

Procedure

Step 1

Select Monitor > Firewall > Device Details > Interfaces. For an explanation of the columns in the table, see Table 7-3.

All measured values on the Firewall Interfaces page are computed as *deltas*—meaning they indicate the scope of difference from one polling cycle to the next.

Step 2

Select the device whose details you want to view from the Select Device list.

Reference

Table 7-3  Firewall Interfaces Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>Displays the device DNS name or IP address.</td>
</tr>
<tr>
<td>Speed (Kbps) column</td>
<td>Displays the average speed (in kilobits) of traffic flow through the relevant interface.</td>
</tr>
<tr>
<td>Bytes In column</td>
<td>Displays the total number of inbound bytes on the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Bytes Out column</td>
<td>Displays the total number of outbound bytes on the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Packets In column</td>
<td>Displays the total number of inbound packets on the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Packets Out column</td>
<td>Displays the total number of outbound packets on the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Packet Errors column</td>
<td>Displays the total number of packet errors on the interface since the previous polling cycle.</td>
</tr>
<tr>
<td>Bandwidth Utilization %</td>
<td>Displayed values vary by device type:</td>
</tr>
<tr>
<td>column</td>
<td>• PIX—Displays the percentage of bandwidth capacity that is in use.</td>
</tr>
<tr>
<td></td>
<td>• Firewall service module—Displays “N/A.”</td>
</tr>
</tbody>
</table>

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Displaying the Device or Module Blocks Table

A block is an internal buffer that processes packets. Values displayed in the Firewall Blocks table describe the state of the blocks on one validated firewall device or module. You can display and work from a table of firewall block statistics.

Procedure

**Step 1** Select **Monitor > Firewall > Device Details > Blocks**.

By default, the Firewall Blocks page displays information for the blocks of whichever device or module uses the lowest number as its IP address.

**Step 2** Select the device whose details you want to view from the **Select Device** list. The columns show the following information:

- **Block Size**—Displays block size in bytes.
- **No. Available**—Displays the number of available blocks (in the relevant block size).
- **No. In Use**—Displays the number of blocks in use (in the relevant block size).

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Displaying the Device or Module Connections Table

A firewall permits or denies a connection after it examines the purpose and protocol of a connection request. You can display and work from a table of connection statistics for one validated firewall device or module.

Procedure

**Step 1** Select **Monitor > Firewall > Device Details > Connections**.

Each row displays a rate of change that is calculated per second for the described value. (The type of rate is specified in every instance of a measured value.)

Because Performance Monitor recalculates each value constantly, any row might display a value of zero (0) at any time if there are no relevant changes during a specific second.

The displayed values are not cumulative. Values might increase or decrease when the display is refreshed.

**Note** An unconfigured firewall feature displays a value of zero at all times.

**Step 2** Select the device whose details you want to view from the **Select Device** list.
Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Monitoring Load-Balancing Services

Load-balancing is a technology that enables network traffic to follow multiple paths to a specific destination. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users.

Content switching is a type of server load-balancing. It balances the load of traffic across web servers based on server load and content availability.

Performance Monitor supports the monitoring of validated content-switching service modules (CSM) that are installed in Cisco Catalyst 6500 Series switches.

---

**Note**

Performance Monitor does not monitor the cluster load balancing capabilities or cluster load balancing performance of Cisco VPN 3000 concentrators.

The following topics describe the features with which you monitor web server load balancing services in your network:

- Content Switching Concepts, page 8-1
- Monitoring Modules Collectively, page 8-2
- Monitoring Modules Individually, page 8-5

---

**Tip**

To troubleshoot common problems with load-balancing services, see the Troubleshooting appendix.

Content Switching Concepts

A content switch analyzes the availability of web content and the load on web servers. Using the results of this analysis, the content switch balances the load of traffic across servers and accelerates the delivery of web content in a way that is transparent to the website end-user.

Properly-configured content switches:

- Improve the responsiveness of websites.
- Help guarantee efficient delivery of high-bandwidth files.
- Decrease network congestion.
- Optimize resource utilization in networks and servers.
- Improve the performance and scalability of web application platforms.
Purpose of Content-Switching Service Modules

A content-switching service module (CSM) provides high-performance connections between network devices and server farms based on Layer 4 through Layer 7 packet information. Clients connect to the CSM by supplying the virtual IP address (VIP) associated with the virtual server. When a client initiates a connection to the virtual server, the CSM selects a real server for the connection based on configured load-balancing algorithms and policies.

<table>
<thead>
<tr>
<th>Virtual Servers</th>
<th>Virtual servers use real server farms through policies you configure on the CSM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Servers</td>
<td>Real servers are physical or virtual devices assigned to a server farm. Real servers provide the services that are load balanced. When the server receives a client request, it pulls matching information from a disk and sends it to the CSM for forwarding to the client.</td>
</tr>
<tr>
<td>Server Farms</td>
<td>A server farm or server pool is a collection of real servers that contain the same content. You specify the server farm name when you configure the server farm and add servers to it, and when you bind the server farm to a virtual server.</td>
</tr>
</tbody>
</table>

Performance Monitor enables you to monitor the CSM as it tracks network sessions and server load conditions in real time and directs sessions to the most appropriate servers.

Monitoring Modules Collectively

The following topics explain how you can monitor CSM modules collectively:

- Displaying CSM Usage and Activity Statistics, page 8-2
- Displaying Load Balancing Failure Statistics, page 8-3
- Displaying Server and Policy Reject Statistics, page 8-4

Displaying CSM Usage and Activity Statistics

You can display usage and activity statistics for all of the validated CSM modules in your network.

Procedure

**Step 1** Select Monitor > Load Balancing > Modules. For an explanation of the columns in the table, see Table 8-1.

All measured values on the Load Balancing Modules page are computed as *deltas* (meaning they indicate the scope of difference from one polling cycle to the next)—except for the whole number count of current connections.

**Step 2** To display detail graphs for one CSM module, click the relevant entry in the Chassis:Module column.
Displaying Load Balancing Failure Statistics

You can display and work from a table that describes the operational failures of your validated CSM modules.

Procedure

**Step 1**  Select **Monitor > Load Balancing > Failures**. For an explanation of the columns in the table, see **Table 8-2**.

All measured values on the Load Balancing Failures page are computed as deltas.

**Step 2**  To display summary graphs for one CSM module, click the relevant entry in the Chassis:Module column.
Displaying Server and Policy Reject Statistics

You can display and work from a table of rejection statistics for your validated CSM modules.

Procedure

Step 1  Select Monitor > Load Balancing > Rejects. For an explanation of the columns in the table, see Table 8-3.

All measured values on the Load Balancing Rejects page are computed as deltas.

Step 2  To display summary graphs for one CSM module, click the relevant entry in the Chassis:Module column.

Reference

Table 8-3  Load Balancing Rejects Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe CSM errors only. See Understanding Interface Icons, page 3-5. For reference information on the Event Browser elements, see Event Browser Windows, page 3-14.</td>
</tr>
</tbody>
</table>

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Monitoring Modules Individually

The following topics explain how you can monitor CSM modules individually:

- Displaying and Interpreting Module Detail Graphs, page 8-5
- Displaying the Virtual Servers Table, page 8-6
- Displaying the Real Servers Table, page 8-7
- Displaying the Interfaces Table, page 8-8

Displaying and Interpreting Module Detail Graphs

You can display and work from a page of detail graphs for one validated CSM module.

Procedure

Step 1  Select Monitor > Load Balancing > Module Details.

By default, Performance Monitor displays graphs that describe the health and performance of whichever module uses the lowest number as its IP address. For a description of the graphs, see Table 8-4.

Step 2  Select the IP address and slot number of the CSM module you want to view from the Select Chassis:Module list.

Table 8-3  Load Balancing Rejects Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis:Module column</td>
<td>Displays the IP address of the relevant Catalyst 6500 switch and the numbered slot in which the CSM module is installed.</td>
</tr>
<tr>
<td>No. of No Active Server Rejects column</td>
<td>Displays the number of connections that were rejected because the relevant server farm had no active servers.</td>
</tr>
<tr>
<td>No. of No Match Policy Rejects column</td>
<td>Displays the number of connections that were rejected because they failed to match any configured policy.</td>
</tr>
<tr>
<td>No. of No Config Policy Rejects column</td>
<td>Displays the number of connections that were rejected because the matching virtual server was not configured with any policy.</td>
</tr>
</tbody>
</table>

Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Chapter 8  Monitoring Load-Balancing Services

Monitoring Modules Individually

Types of Load Balancing Graphs

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Failures</td>
<td>Illustrates the trend of module connection failures over time:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the percentage of failures in a specific polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
<tr>
<td>Dropped Connection</td>
<td>Illustrates the trend of dropped connections over time:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the average number of dropped connections in a specific polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
<tr>
<td>Current Connections</td>
<td>Illustrates the trend of successful connections over time:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the average number of successful connections in a specific polling cycle.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
<tr>
<td>Total Rejects</td>
<td>Illustrates the trend of rejected connections over time:</td>
</tr>
<tr>
<td></td>
<td>• The vertical axis shows the average sum of these values over time:</td>
</tr>
<tr>
<td></td>
<td>• The number of connections that were rejected because the relevant server farm had no active</td>
</tr>
<tr>
<td></td>
<td>servers.</td>
</tr>
<tr>
<td></td>
<td>• The number of connections that were rejected because they failed to match any configured policy.</td>
</tr>
<tr>
<td></td>
<td>• The number of connections that were rejected because the matching virtual server was not</td>
</tr>
<tr>
<td></td>
<td>configured with any policy.</td>
</tr>
<tr>
<td></td>
<td>• The horizontal axis shows the time of day for the polling cycle.</td>
</tr>
</tbody>
</table>

Displaying the Virtual Servers Table

You can display and work from a table of virtual server statistics for one validated CSM module.

Procedure

Step 1  Select Monitor > Load Balancing > Virtual Servers. For an explanation of the columns in the table, see Table 8-5.

The Load Balancing Virtual Servers page displays information about all of the virtual servers associated with a specific CSM module.

Step 2  Select the IP address and slot number of the CSM module you want to view from the Select Chassis:Module list.

Reference

Table 8-5  Load Balancing Virtual Servers Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>Displays the name of the virtual server that is configured on the CSM.</td>
</tr>
</tbody>
</table>
Displaying the Real Servers Table

You can display and work from a table of real server statistics for one validated CSM service module.

Procedure

**Step 1** Select Monitor > Load Balancing > Real Servers. For an explanation of the columns in the table, see Table 8-6.

The Load Balancing Real Servers page displays information about all of the real servers associated with a specific CSM module.

**Step 2** Select the IP address and slot number of the CSM module you want to view from the Select Chassis:Module list.

Reference

### Table 8-5 Load Balancing Virtual Servers Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address column</td>
<td>Displays the IP address of the relevant virtual server.</td>
</tr>
<tr>
<td>Port column</td>
<td>Displays the logical port from which the virtual server manages the relevant content type.</td>
</tr>
<tr>
<td>State column</td>
<td>Displays the functional state of the virtual server.</td>
</tr>
<tr>
<td>No. Current Connections column</td>
<td>Displays the number of active connections.</td>
</tr>
<tr>
<td>No. Total Connections column</td>
<td>Displays the total number of connections since the previous polling cycle.</td>
</tr>
</tbody>
</table>

### Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

### Table 8-6 Load Balancing Real Servers

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Farm column</td>
<td>Displays the name of the server farm.</td>
</tr>
<tr>
<td>Address column</td>
<td>Displays the IP address of the real server.</td>
</tr>
<tr>
<td>Port column</td>
<td>Displays the port number of the real server.</td>
</tr>
<tr>
<td>State column</td>
<td>Displays the state of the real server.</td>
</tr>
<tr>
<td>No. Current Connections column</td>
<td>Displays the number of active connections.</td>
</tr>
<tr>
<td>No. Total Connections column</td>
<td>Displays the total number of connections since the previous polling cycle.</td>
</tr>
<tr>
<td>No. Total Failed Connections column</td>
<td>Displays the total number of connections that failed since the previous polling cycle.</td>
</tr>
<tr>
<td>Connection Failed % column</td>
<td>Displays the percentage of connections that failed since the previous polling cycle.</td>
</tr>
</tbody>
</table>
Displaying the Interfaces Table

You can display and work from a table of interface statistics for one validated CSM module.

**Procedure**

**Step 1**
Select `Monitor > Load Balancing > Interfaces`. For an explanation of the columns in the table, see Table 8-7.

Statistics on the Load Balancing Interfaces page describe routed VLANs that are associated with a CSM module interface.

All measured values on the Load Balancing Interfaces page are computed as deltas.

**Step 2**
Select the IP address and slot number of the CSM module you want to view from the Select Chassis:Module list.

---

**Reference**

<table>
<thead>
<tr>
<th>Table 8-7 Load Balancing Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
</tr>
<tr>
<td>Descr column</td>
</tr>
<tr>
<td>Address column</td>
</tr>
<tr>
<td>Admin Status column</td>
</tr>
<tr>
<td>Operation Status column</td>
</tr>
<tr>
<td>Type column</td>
</tr>
<tr>
<td>Speed (Kbps) column</td>
</tr>
<tr>
<td>Packets In column</td>
</tr>
<tr>
<td>Packets Out column</td>
</tr>
<tr>
<td>Packet Drop % column</td>
</tr>
<tr>
<td>Throughput (Kbps) column</td>
</tr>
</tbody>
</table>

**Related Topics**

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Monitoring SSL Services

Performance Monitor features enable you to monitor and interpret important aspects of Secure Socket Layer (SSL) module operations and performance in real time.

The following topics explain the SSL module monitoring features:

- SSL Concepts, page 9-1
- Monitoring Modules Collectively, page 9-2
- Monitoring Modules Individually, page 9-5

SSL Concepts

Secure Socket Layer (SSL) is a protocol that enables secure transfers of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys.

The following topics provide information that you might require in order to understand SSL monitoring:

- Purpose of SSL Modules, page 9-1
- Performance of SSL Modules, page 9-2

Purpose of SSL Modules

The SSL service module is an integrated module for Cisco Catalyst 6500 Series switches. Any port on a Series 6500 switch can offload resource-intensive SSL functions from web servers in your network when it is the proxy SSL port for those servers. One SSL module can act as the proxy for several web servers.

SSL modules accelerate the delivery of encrypted web traffic and perform all SSL-related tasks (including delivery of web-enabled applications). Thus, your web servers deliver cleartext web content faster and in greater quantities than they can when they perform their own SSL functions.

Properly configured SSL modules:

- Increase the number of secure connections a website supports.
- Permit a web server to process more requests for content.
- Provide server load balancing.
Performance of SSL Modules

The chassis of a Catalyst 6500 switch can hold as many as four SSL modules. Under optimal conditions, each SSL module provides:

- As many as 2,500 connection setups per second—or 10,000 per chassis when four modules are installed.
- As much as 300-Mbps bulk-encrypted throughput—or 12.2-Gbps per chassis when four modules are installed.
- As many as 60,000 concurrent connections—or 240,000 per chassis when four modules are installed.

Every SSL module has its own CPU and its own IP address.

If an SSL module is not configured correctly or is not functioning correctly, encrypted and cleartext web services in your network might become degraded.

If you determine that an SSL module in your network is providing service levels below its designed capacity, you can isolate the cause, and then take corrective action with your network management tools.

Monitoring Modules Collectively

The following topics explain how you can monitor SSL modules collectively:

- Working with SSL Usage and Activity Statistics, page 9-2
- Working with SSL Statistics, page 9-3
- Working with TCP Connection Statistics, page 9-4

Working with SSL Usage and Activity Statistics

You can display usage and activity statistics for all of the validated SSL modules in your network.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Monitor &gt; SSL &gt; Modules. For an explanation of the columns in the table, see Table 9-1.</td>
</tr>
<tr>
<td>Step 2</td>
<td>To display detail graphs for one SSL module, click the relevant IP address in the Module column.</td>
</tr>
</tbody>
</table>
You can display and work from a table of SSL activity statistics for all of your validated SSL modules.

**Step 1** Select Monitor > SSL > Statistics. For an explanation of the columns in the table, see Table 9-2. All measured values on the SSL Statistics page are computed as deltas (meaning they indicate the scope of difference from one polling cycle to the next)—except for the whole number counts of active sessions and active connections.

**Step 2** To display summary graphs for one SSL module, click the relevant IP address or DNS name in the Module column.
You can display and work from a table of TCP connection statistics for all of your validated SSL modules.

**Step 1**  
Select **Monitor > SSL > TCP Connections**. For an explanation of the columns in the table, see **Table 9-3**.

All measured values on the SSL TCP Statistics page are computed as deltas.

**Step 2**  
To display summary graphs for one SSL module, click the relevant IP address or DNS name in the Module column.

### Working with TCP Connection Statistics

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert column</td>
<td>Displays an alert icon in cases of high-severity problems or failures. Click the icon to open an event browser and view a filtered display of severe SSL errors only. See <strong>Understanding Interface Icons, page 3-5</strong>. For reference information on the Event Browser elements, see <strong>Event Browser Windows, page 3-14</strong>.</td>
</tr>
<tr>
<td>Module column</td>
<td>Displays the module IP address.</td>
</tr>
<tr>
<td>Connects Attempted</td>
<td>Displays the total number of attempted SSL connections since the previous polling cycle.</td>
</tr>
<tr>
<td>Connects Completed</td>
<td>Displays the total number of SSL connections that were completed successfully since the previous polling cycle.</td>
</tr>
<tr>
<td>Connects Active</td>
<td>Displays the number of active SSL connections.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>Displays the total number of active SSL sessions.</td>
</tr>
<tr>
<td>Handshake Failures</td>
<td>Displays the number of handshake failures that occurred since the previous polling cycle.</td>
</tr>
<tr>
<td>Data Failures</td>
<td>Displays the number of data failures that occurred since the previous polling cycle.</td>
</tr>
</tbody>
</table>
Monitoring Modules Individually

The following topics explain how you can monitor validated SSL modules individually:

- Displaying and Interpreting Module Detail Graphs, page 9-5
- Displaying the SSL Proxy Statistics Table, page 9-6
- Displaying the SSL Proxy Errors Table, page 9-7

Displaying and Interpreting Module Detail Graphs

You can display and work from a page of detail graphs for one validated SSL module.

Procedure

1. Select **Monitor > SSL > Module Details**.

   By default, Performance Monitor displays graphs that describe the health and performance of whichever module uses the lowest number as its IP address. For a description of the graphs, see Table 9-4.

   **Note** A known problem might interfere with your ability to interpret a graph that uses two vertical (Y) axes. The first Y axis always begins at zero, but the second Y axis begins at the lowest value for the specified time range—even when that value is greater than zero. Thus, the two Y axes might not be directly comparable.

2. Select the device whose graphs you want to view from the **Select Device** list.
Types of SSL Module Graphs

<table>
<thead>
<tr>
<th>Table 9-4</th>
<th>Interpreting SSL Module Graphs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| CPU Usage | Illustrates used percentages of module CPU capacity:  
• The vertical axis shows the average percentage of CPU capacity used in the relevant polling cycle.  
• The horizontal axis shows the time of day for the polling cycle. |
| Memory Usage | Illustrates used percentages of module memory capacity:  
• The vertical axis shows the average percentage of memory capacity used in the relevant polling cycle.  
• The horizontal axis shows the time of day for the polling cycle. |
| Error Rate | Illustrates the trend of module interface errors over time:  
• The vertical axis shows the average number of errors in the relevant polling cycle.  
• The horizontal axis shows the time of day for the polling cycle. |
| Throughput vs. Connections | Displays a line chart that helps you compare throughput trends to connection trends over time:  
• Because it shows two kinds of information, it has two vertical axes.  
  – The vertical axis on the left (blue) shows the average throughput in bytes in the relevant polling cycle.  
  – The vertical axis on the right (red) shows the average number of SSL connections in the relevant hour.  
• The horizontal axis shows the time of day at which Performance Monitor calculated the trends in each vertical axis. |

Displaying the SSL Proxy Statistics Table

You can display and work from a table of proxy statistics for one validated SSL module.

**Procedure**

**Step 1** Select Monitor > SSL > Proxy Statistics. For an explanation of the columns in the table, see Table 9-5.

All measured values on the SSL Proxy Statistics page are computed as deltas.

**Step 2** Select the device you want to view from the Select Device list.

**Reference**

<table>
<thead>
<tr>
<th>Table 9-5</th>
<th>SSL Proxy Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Proxy column</td>
<td>Displays the proxy service name.</td>
</tr>
<tr>
<td>Connects Attempted column</td>
<td>Displays the total number of attempted connections for the relevant proxy service since the previous polling cycle.</td>
</tr>
</tbody>
</table>
Displaying the SSL Proxy Errors Table

You can display and work from a table of proxy errors for one validated SSL module.

**Procedure**

1. **Step 1** Select Monitor > SSL > Proxy Errors. For an explanation of the columns in the table, see Table 9-6. All measured values on the SSL Proxy Errors page are computed as deltas.

2. **Step 2** Select the device you want to view from the Select Device list.

**Reference**

**Table 9-6 SSL Proxy Errors**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy column</td>
<td>Displays the proxy service name.</td>
</tr>
<tr>
<td>Handshake Failures column</td>
<td>Displays the number of SSL failures for the relevant proxy service that occurred during the Handshake state.</td>
</tr>
<tr>
<td>Data Failures column</td>
<td>Displays the number of SSL failures for the relevant proxy service that occurred during the Data state.</td>
</tr>
<tr>
<td>MAC Errors column</td>
<td>Displays the number of Machine Authentication Code (MAC) verification errors for the relevant proxy service since the previous polling cycle.</td>
</tr>
<tr>
<td>Version Mismatch column</td>
<td>Displays the number of SSL version mismatch errors for the relevant proxy service since the previous polling cycle.</td>
</tr>
</tbody>
</table>
### Table 9-6  
**SSL Proxy Errors (continued)**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Compress column</td>
<td>Displays the number of errors for the relevant proxy service since the previous polling cycle in which compression algorithms were unsupported.</td>
</tr>
<tr>
<td>No Cipher column</td>
<td>Displays the number of errors for the relevant proxy service since the previous polling cycle in which SSL ciphers were incompatible.</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Optional Tasks in Performance Monitor Tables, page 3-9](#)
- [Common Elements in Tables, page 3-8](#)
Using Trend Reports

Note
To learn about supported services and platforms, see Supported Services and Platforms for Monitoring and Reports, page 1-5.

The following topics describe the reporting features available in Performance Monitor and explain how to use and save the historical trend reports that you generate.

- Understanding Reporting Options, page 10-1
- Configuring and Generating Reports, page 10-6
- Working with Scheduled Email Jobs, page 10-11

Understanding Reporting Options

You can configure and generate reports for all supported service types. Reports are organized in four broad categories and more than 30 narrow subcategories.

Note
Only RAS VPN and site-to-site VPN services support all four of the high-level report categories. Subcategories are service-specific in most cases.

A subcategory measures trends over time for one narrow condition on a validated device or in a supported service. Subcategories are specific to categories; for example, subcategories in the Failure category are specific kinds of failures. The number of subcategories that you can select for a report ranges from one to four, depending on the subcategories you select.

The report categories are:

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Reference</th>
</tr>
</thead>
</table>
Understanding Failure Report Subcategories

Each generated line graph in a Failure report displays results for one device or service module or virtual server, depending on the service type and subcategory you select—as described in Table 10-1, which:

- Lists all subcategories for configuring Failure reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Failure reports.

Note
When you run historical reports, you might see a dip in the graph for any period of time during which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

<table>
<thead>
<tr>
<th>Failure Report Subcategory</th>
<th>Relevant Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of Inbound Conn Failures</td>
<td>Remote Access VPN</td>
<td>Graph shows the trend of failed inbound connections over time as a percentage of all inbound connections for all remote access VPN devices.</td>
</tr>
<tr>
<td>% of Phase 1 Conn Failures</td>
<td>Remote Access VPN</td>
<td>Graph shows the trend of failed Phase-1 (IKE) connections over time as a percentage of all Phase-1 connections.</td>
</tr>
<tr>
<td>% of Phase 2 Conn Failures</td>
<td>Remote Access VPN</td>
<td>Graph shows the trend of failed Phase-2 (IPSec) connections over time as a percentage of all Phase-2 connections.</td>
</tr>
<tr>
<td>% Of Conns Dropped By All Virtual Servers</td>
<td>Load Balancing</td>
<td>Graph shows the trend of dropped virtual server connections over time as a percentage of all connections.</td>
</tr>
<tr>
<td>% Of Failed Conns Per Module</td>
<td>Load Balancing</td>
<td>Graph shows the trend of failed load-balancing connections over time as a percentage of all CSM service module connections.</td>
</tr>
<tr>
<td>% Of Inbound Conn Failures</td>
<td>Site-to-Site VPN</td>
<td>Graph shows the trend of failed inbound Phase-1 (IKE) and Phase-2 (IPSec) tunnels over time as a percentage of all inbound exchanges.</td>
</tr>
<tr>
<td>% Of Outbound Conn Failures</td>
<td>Site-to-Site VPN</td>
<td>Graph shows the trend of failed outbound Phase-1 (IKE) and Phase-2 (IPSec) tunnels over time as a percentage of all outbound exchanges.</td>
</tr>
<tr>
<td>% of Total Conn Failures</td>
<td>Site-to-Site VPN</td>
<td>Graph shows the trend of failed Phase-1 (IKE) and Phase-2 (IPSec) connections over time as a percentage of all inbound and outbound exchanges.</td>
</tr>
</tbody>
</table>

Note
Trend reports are not usually useful when they are based on a small number of data points. The date range and trending type determine the number of data points. For example, there is only one data point if you apply the Daily trending type to less than 2 days’ worth of data. It is not possible to graph a trend from only one data point.
Understanding Performance Report Subcategories

Each generated line graph in a Performance report displays results for one device or service module or virtual server, depending on the service type and subcategory you select—as described in Table 10-2, which:

- Lists all subcategories for configuring Performance reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Performance reports.

**Note** When you run historical reports, you might see a dip in the graph for any period of time during which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

<table>
<thead>
<tr>
<th>Performance Report Subcategory</th>
<th>Relevant Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth Usage</strong></td>
<td>Remote Access VPN</td>
<td>Graph shows trends for the average percentage of total bandwidth capacity used over time, calculated as the sum of inbound and outbound packets, factored against the interface speed.</td>
</tr>
</tbody>
</table>
| **CPU Usage** | • Firewall  
• Remote Access VPN  
• Site-to-Site VPN  
• SSL | Graph shows trends for the average percentage of total CPU capacity used over time. |
| **CPU Usage Rev** | Site-to-Site VPN | Graph shows trends for the average percentage of total CPU capacity used over time.  
**Note** If the displayed report is empty when you select the CPU Usage Rev subcategory, use the CPU Usage subcategory instead. |
| **FTP Fixup** | Firewall | Graph shows trends for the average per-second activity and change rate over time for FTP Fixup—the PIX OS inspection function, as applied to FTP traffic. |
| **HTTP Fixup** | Firewall | Graph shows trends for the average per-second activity and change rate over time for HTTP Fixup—the PIX OS inspection function, as applied to HTTP traffic. |
| **Memory Usage** | • Firewall  
• Site-to-Site VPN  
• SSL | Graph shows trends for the average percentage of processor memory capacity used over time. |
| **SSL Connections** | SSL | Graph shows trends for the total number of active SSL connections over time. |
| **TCP Fixup** | Firewall | Graph shows trends for the average per-second activity and change rate over time for TCP Fixup—the PIX OS inspection function, as applied to TCP traffic. |
Understanding Reporting Options

Understanding Throughput Report Subcategories

Each generated line graph in a Throughput report displays results for one device, service module, or virtual server, depending on the service type and subcategory you select—as described in Table 10-3, which:

- Lists all subcategories for configuring Throughput reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Throughput reports.

Note

When you run historical reports, you might see a dip in the graph for any period of time in which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.
### Understanding Reporting Options

#### Understanding Usage Report Subcategories

Each generated line graph in a Usage report displays results for one device, service module, or virtual server, depending on the service type and subcategory you select—as described in Table 10-4, which:

- Lists all subcategories for configuring Usage reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Usage reports.

**Note** When you run historical reports, you might see a dip in the graph for any period of time in which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

### Table 10-3 Throughput Report Configuration Subcategories

<table>
<thead>
<tr>
<th>Throughput Report Subcategory</th>
<th>Relevant Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>Remote Access VPN • Site-to-Site VPN</td>
<td>Graph shows trends for the sum in kbps of inbound and outbound octets through all public interfaces over time, factored against interface speed.</td>
</tr>
<tr>
<td>Throughput Per Accelerator</td>
<td>Remote Access VPN</td>
<td>Graph shows trends for the sum, in kbps, of inbound and outbound octets across scalable encryption processor (SEP) accelerator cards over time, factored against SEP card speed. <strong>Note</strong> Each line in the graph represents a separate SEP card. There are no SEP cards in a VPN 3005 Concentrator or a VPN 3015 Concentrator, so these devices are excluded from the report. You cannot select any other report subcategory when you select Throughput Per Accelerator.</td>
</tr>
<tr>
<td>Throughput Per Interface</td>
<td>Remote Access VPN • Site-to-Site VPN</td>
<td>Graph shows trends for the sum, in kbps, of inbound and outbound octets through the public interfaces of one device over time, factored against interface speed. <strong>Note</strong> Each line in the graph represents a separate interface. You cannot select any other report subcategory when you select Throughput Per Interface.</td>
</tr>
<tr>
<td>% Of Crypto Packet Drop</td>
<td>Site-to-Site VPN</td>
<td>Graph shows the trend of dropped crypto packets as a percentage of all encrypted and decrypted packets over time.</td>
</tr>
<tr>
<td>% Of Crypto Packet Errors</td>
<td>Remote Access VPN</td>
<td>Graph shows the trend of encrypted packets with errors in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all encrypted packets over time.</td>
</tr>
<tr>
<td>% Of Packets Dropped</td>
<td>Remote Access VPN • Site-to-Site VPN</td>
<td>Graph shows the trend of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all inbound and outbound packets over time.</td>
</tr>
</tbody>
</table>
You can configure and generate historical reports for any supported service in your network.

**Procedure**

1. **Step 1** Select **Reports > Service Type > Configure Report**, where **Service Type** is the service you select in the options bar.

   The Configure Report page displays an Object Selector, action buttons, lists, and reporting categories that apply to the service you select. See Using an Object Selector, page 3-10.

2. **Step 2** If the All tab is not active, click it to display a list of device groups and individual devices in the selection tree. Select the devices whose information you want to include in the report; select a device group to select all devices in the group and its descendants in the hierarchy.

   You must select at least one device from the tree before you can configure a report. The following reporting subcategories require that you select *no more than* one device:
   - Site-To-Site: Throughput: Throughput Per Interface.

---

**Table 10-4 Usage Report Configuration Subcategories**

<table>
<thead>
<tr>
<th>Usage Report Subcategory</th>
<th>Relevant Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Tunnels</td>
<td>Site-to-Site VPN</td>
<td>Graph shows trends for the combined number of Phase-1 (IKE) and Phase-2 (IPSec) tunnels for site-to-site VPNs over time.</td>
</tr>
<tr>
<td>Number of Users</td>
<td>Remote Access VPN</td>
<td>Graph shows trends for the aggregate number of active sessions on all RAS devices over time.</td>
</tr>
<tr>
<td># Of Conns Per Module</td>
<td>Load Balancing</td>
<td>Graph shows trends for the average number of connections over time for each CSM module in a specific chassis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Each line in the graph represents a separate service module. You cannot select any other report subcategory when you select # Of Conns Per Module.</td>
</tr>
<tr>
<td># Of Conns Per Virtual Server</td>
<td>Load Balancing</td>
<td>Graph shows trends for the number of connections over time for each virtual server associated with a specific chassis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Each line in the graph represents a separate virtual server. You cannot select any other report subcategory when you select # Of Conns Per Virtual Server.</td>
</tr>
</tbody>
</table>

**Note** Trend reports are not usually useful when they are based on a small number of data points. The date range and trending type determine the number of data points. For example, there is only one data point if you apply the Daily trending type to less than 2 days’ worth of data. It is not possible to graph a trend from only one data point.
• Load Balancing: Failure: % Of Conns Dropped By All Virtual Servers.
• Load Balancing: Failure: % Of Failed Conns Per Module.

**Step 3**
Select a report category, then select a subcategory, and click >> (Add) to move it to the Selected List. Click << (Remove) if you selected the wrong subcategory.

You can select more than one type of report, following these rules:

- You cannot select more than four subcategories for any report.
- You cannot select more than two subcategories for a report unless all of the subcategories you select measure units in percentages. In such cases, you can select as many as four subcategories.
- You cannot select more than two subcategories if either one of your selections measures units in percentages.
- In some cases, as specified in Understanding Reporting Options, page 10-1 and its subtopics, sometimes you can select only one subcategory.

There are more than 30 subcategories of reports. For a description of the report types, see:

- Understanding Performance Report Subcategories, page 10-3.

**Step 4**
Select an interval from the Trending Type list. Trending options are:

- Hourly—The report shows monitored values at intervals of 1 hour for the range of calendar dates that you specify.
- Daily—The report shows monitored values at intervals of 1 day for the range of calendar dates that you specify.
- Weekly—The report shows monitored values at intervals of 1 week for the range of calendar dates that you specify.
- Monthly—The report shows monitored values at intervals of 1 month for the range of calendar dates that you specify.

**Step 5**
Select the start (From) and end (To) dates for data to include in the report.

**Step 6**
Do one of the following:

- To generate the report and view it in a new browser window, click **View**.
- To generate the report and configure one-time or recurring email distribution options for it, click **Email**. When configuring a recurring email job, you can specify how many hours of data to include in the report.
- To generate the report and save it to a file, select a file format and click **Export**. The following formats are available:
  - CSV—Exports data in an ASCII list of comma-separated values that you can display in tabular form in most spreadsheet applications.
  - XML—Exports data in extensible markup language that you can review in a web browser or word processor or other application that displays XML files.
  - PDF—Exports data in portable document format, which you can review with the Adobe Acrobat Reader application or any other application that displays PDF files.
Understanding Historical Reports

A generated report displays graphs that show historical trends for the subcategories you select, to which Performance Monitor applies the trending type and date range you specify. To understand a specific graph, see Understanding Reporting Options, page 10-1 and its subtopics.

The Details area in the Performance Monitor Report page lists your username, the trending type, and the range of dates for the relevant report.

Related Topic
- Configuring and Generating Reports, page 10-6

Viewing RAS VPN Top 10 User Reports

You can view an historical report of the top 10 RAS VPN users in your network across all RAS devices.

**Note**
Performance Monitor does not display this information for Easy VPN RAS sessions.

**Procedure**

**Step 1** Select Reports > Remote Access > Top 10 Users.

By default, the Top 10 Users page displays the 10 RAS users whose throughput levels are highest, with hourly data points for the last 24 hours. If fewer than 10 users have connected to your RAS VPN in the last 24 hours, there are fewer than 10 results displayed.

Information in the report is based on user activity rankings from every device.

**Step 2** If desired, modify the report criteria and click Go to see the results. You can:

- Change the trending type. Select one of the following:
  - Hourly—Shows monitored values at 1-hour intervals.
  - Daily—Shows monitored values at 1-day intervals.
  - Weekly—Shows monitored values at 1-week intervals.
  - Monthly—Shows monitored values at 1-month intervals.

- Specify a different range of reporting dates by entering different dates in the From and To fields.

Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Viewing RAS VPN User Session Reports

You can view reports that describe the remote access VPN sessions over time of multiple users or of one user whom you specify.
Some multi-user session queries return a high number of results. In cases where a query returns more than 10,000 results, the User Session Report page takes several minutes to load in your browser. If such a delay is unacceptable to you, we recommend that you select a specific device and adjust the Start and End times before you submit your query.

### Before You Begin

This feature requires that your VPN 3000 concentrators, ASA and PIX devices are configured to send Syslog messages to Performance Monitor.

- See Setting Up ASA Appliances, PIX Devices, and Firewall Services Modules, page 2-5, for help configuring your appliances and firewalls.
- See Setting Up VPN 3000 Concentrators, page 2-6, for help configuring your VPN concentrators.
- See Working with Notifications, page 12-1, for a list of the Syslog messages that Performance Monitor can process.

### Procedure

**Step 1** Select Reports > Remote Access > User Session Report.

The User Session Report page includes an Object Selector. See Using an Object Selector, page 3-10.

**Step 2** Decide whether to display session reports for multiple users or one user, then do one of the following:

- To display information that includes every user session, select Search All Users.
- To limit your search to the user sessions in a single cluster, select the cluster parent in the tree.
- To limit your search to the user sessions on a single device, select the device in the tree.
- To limit your search to the sessions of one user, enter the username in the User Name text box.

**Step 3** To define the interval in which Performance Monitor searches for sessions, do both of the following:

- In the Start Time area, select a calendar date and enter a time of day in HH:MM:SS format. The values in the Start Time area define the beginning of the interval in which Performance Monitor searches for session information.
- In the End Time area, select a calendar date and enter a time of day in HH:MM:SS format. The values in the End Time area define the end of the interval in which Performance Monitor searches for session information.

**Step 4** Do either or both of the following:

- To display the report in a new browser window, click View.
- To export the report, select a file format (CSV or XML), then click Export.

If you select CSV, Performance Monitor might prompt you to accept a CiscoWorks Server certificate if you did not previously specify the server as a trusted source. If you accept the certificate, Performance Monitor displays the exported CSV data in your default spreadsheet application. If you decline the certificate, Performance Monitor prompts you for a filename and path to save the CSV file locally.

If you select XML, an XML export opens a new browser window from which you can save the displayed result. Select File > Save As to save a local copy of the exported report.

The content of the report is explained in Table 10-5.
Configuring and Generating Reports

Chapter 10      Using Trend Reports

User Session Report Format

Table 10-5   User Session Report Format

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username column</td>
<td>Displays the authenticated username you entered as a search query, provided that you searched for one user and that a matching username was found. If you searched for the sessions of all users in a specific timeframe, the Username column might contain all of the authenticated usernames associated with all of the sessions in that timeframe.</td>
</tr>
<tr>
<td>IP Address column</td>
<td>Displays the user IP address associated with the described session. The IP address for a specific user might vary between sessions, particularly in networks that use dynamic addressing.</td>
</tr>
<tr>
<td>State column</td>
<td>Displays the most recent status of the described user session—Active or Completed.</td>
</tr>
<tr>
<td>VPN Device Name column</td>
<td>Displays the DNS name of the VPN concentrator through which the described session took place (or is taking place, in the case of an active session).</td>
</tr>
<tr>
<td>Start Time column</td>
<td>Displays the date and time at which the described session began, in MM/DD/YYYY HH:MM:SS format.</td>
</tr>
<tr>
<td>End Time column</td>
<td>Displays the date and time at which the described session ended, in MM/DD/YYYY HH:MM:SS format. If End Time values are red, the exact end time is unknown. The displayed value in such cases is the time at which Performance Monitor polling determined that the session was no longer active.</td>
</tr>
<tr>
<td>Duration column</td>
<td>Displays the duration of the session in days, hours, minutes, and seconds. If the exact end time is unknown, values in the Duration column are red. The displayed value in such cases is the duration at which Performance Monitor polling determined that the session was no longer active.</td>
</tr>
<tr>
<td>Last Verified column</td>
<td>Displays the most recent time (in MM/DD/YYYY HH:MM:SS format) at which device polling provided information for the described session.</td>
</tr>
<tr>
<td>Bytes In column</td>
<td>Displays the total number of tunneled bytes that the user received through your network during the described session.</td>
</tr>
<tr>
<td>Bytes Out column</td>
<td>Displays the total number of tunneled bytes that the user sent through your network during the described session.</td>
</tr>
</tbody>
</table>

Viewing Site-to-Site VPN Top 10 Tunnel Reports

You can view an historical report of the top 10 site-to-site VPN tunnels in your network across all devices.

Procedure

Step 1   Select Reports > Site-to-Site > Top 10 Tunnels.

By default, the Top 10 Tunnels page displays the 10 tunnels with the highest throughput levels, applying hourly data points to the last 24 hours. If fewer than 10 tunnels have had measurable throughput in the last 24 hours, fewer than 10 results are displayed.

For an explanation of the columns in the table, see Table 10-6.
Step 2 If desired, modify the report criteria and click Go to see the results. You can:

- Change the trending type. Select one of the following:
  - Hourly—Shows monitored values at 1-hour intervals.
  - Daily—Shows monitored values at 1-day intervals.
  - Weekly—Shows monitored values at 1-week intervals.
  - Monthly—Shows monitored values at 1-month intervals.
- Specify a different range of reporting dates by entering different dates in the From and To fields.

Reference

Table 10-6 Top 10 Tunnels Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name column</td>
<td>Displays the DNS name or IP address of the described device.</td>
</tr>
<tr>
<td>Local Endpoint column</td>
<td>Displays the IP address of the local endpoint device interface at which the tunnel terminates.</td>
</tr>
<tr>
<td>Note</td>
<td>The identity of the “local” endpoint device might vary in Performance Monitor because its definition is always relative to the device that you monitor.</td>
</tr>
<tr>
<td>Remote Endpoint column</td>
<td>Displays the IP address of the remote endpoint device interface at which the tunnel terminates.</td>
</tr>
<tr>
<td>Note</td>
<td>The identity of the “remote” endpoint device might vary in Performance Monitor because its definition is always relative to the device that you monitor.</td>
</tr>
<tr>
<td>Local Subnet column</td>
<td>Taken together, the values in these three columns define the access list for one tunnel:</td>
</tr>
<tr>
<td>Remote Subnet column</td>
<td>• Local Subnet—Displays the tunnel subnet and mask on the local endpoint device.</td>
</tr>
<tr>
<td>Protocol column</td>
<td>• Remote Subnet—Displays the tunnel subnet and mask on the remote endpoint device.</td>
</tr>
<tr>
<td>Throughput (Kbps) column</td>
<td>• Protocol—Displays the tunnel protocol and the port used, such as TCP 80.</td>
</tr>
<tr>
<td></td>
<td>Displays the sum of inbound and outbound octets through the tunnel since tunnel inception, in Kbps.</td>
</tr>
</tbody>
</table>

Related Topics
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

Working with Scheduled Email Jobs

You can view and delete the scheduled email jobs through which Performance Monitor distributes historical reports.

Procedure

Step 1 Select Reports > Service Type > Scheduled Email Jobs, where Service Type is the service that you select in the options bar.

Step 2 Select one job from the list.
Step 3  
Do one of the following:

- To display the job in the Email Job Details window, click View.
- To delete the job, click Delete. You cannot undo a job deletion.

Reference

Table 10-7  Email Jobs

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name column</td>
<td>Displays the name of the job, which consists of:</td>
</tr>
<tr>
<td></td>
<td>- Your CiscoWorks username—for example, Admin.</td>
</tr>
<tr>
<td></td>
<td>- The specified service type—for example, RAS.</td>
</tr>
<tr>
<td></td>
<td>- The value that you entered in the Job Name field in the Schedule Email Report window.</td>
</tr>
<tr>
<td>Recurring column</td>
<td>Displays either:</td>
</tr>
<tr>
<td></td>
<td>- Yes—the job is scheduled to recur.</td>
</tr>
<tr>
<td></td>
<td>- No—the job is scheduled to occur only once.</td>
</tr>
<tr>
<td>Next Schedule column</td>
<td>For recurring jobs only, displays the next date and time at which the job recurs.</td>
</tr>
<tr>
<td>Last Run Status column</td>
<td>Displays a message to indicate whether the email was sent successfully or if delivery failed.</td>
</tr>
<tr>
<td>Last Run Time column</td>
<td>Displays the most recent time (in MM/DD/YYYY HH:MM:SS format) at which this scheduled email job ran.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring and Generating Reports, page 10-6
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8
Managing and Grouping Devices

In Performance Monitor, a device is either a physical node in the network or it is a virtual node that is defined by a physical node. In either case, whether physical or virtual, a device must be IP-addressable.

For example, you can use multicontext mode to partition a single firewall into multiple virtual devices, known as security contexts. A firewall that runs in multicontext mode has a configuration for each context to define its security policy, interfaces, and other options—just as you might expect to configure equivalent options on a physical device.

System administrators add and manage contexts in the system configuration. The system configuration identifies basic firewall settings, but does not include any network interfaces or network settings for itself; rather, it uses a context that is designated as the admin context.

The admin context is just like any other security context, except that a user who logs in to the admin context has administrative rights over the system and all of the other contexts. In Performance Monitor, you import only the admin context from a device when you want to monitor every configured context on a physical device. Similarly, when you delete an admin context in Performance Monitor, you simultaneously delete the record that Performance Monitor maintains for every context on the relevant physical device.

There are two possible behaviors when Performance Monitor represents a specific security context in lists, menus, graphs, reports, logs, or other places:

- The IP address of the admin context appears as a prefix for the context name, as follows: `<IP_address_of_admin_context>:<context_name>`. This happens when Performance Monitor has, by default, used the admin context IP address and credentials to poll and monitor the security contexts on a validated device.

  **Note**  
  Performance Monitor automatically discovers all of the security contexts on a device when you import the admin context and—as a convenience to you—uses the IP address and credentials information for the admin context to poll and monitor the other contexts on the device. However, when Performance Monitor uses the admin context IP address to poll and monitor security contexts on a device, no more than five contexts can be monitored. If your device includes more than five contexts, you can manually enter the IP address and credentials for any or every context at any time after discovery.

- The IP address of the security context appears without any prefix. This happens after you manually edit the credentials of a context that was previously represented in the default way, `<IP_address_of_admin_context>:<context_name>`.
A device group in Performance Monitor is similar to a folder. Some device groups are system-defined, where others are user-defined:

- System-defined device groups automatically sort your physical devices and security contexts by device or service type. System-defined device groups are consistent and logical.
- User-defined device groups in Performance Monitor are an organizational convenience in which you can collect any combination of devices, security contexts, and other device groups. Among the devices in a user-defined group, no physical, logical, or topological relationship is assumed unless you organize devices in a consistent way.

**Note**
Topics in Chapter 2, “Before You Begin,” describe the device import and device validation features under the Devices tab.

Topics in this section describe the following options under the Devices tab:
- Managing Devices, page 11-2
- Managing Device Groups, page 11-9

## Managing Devices

When you select Devices > Managing Devices, Performance Monitor displays an object selector and action buttons that enable you to manage your devices. See Using an Object Selector, page 3-10.

**Tip**
If you have recently imported or added a device and it is not yet visible, click Refresh to update the device list in the Managing Devices object selector. To understand device icons, see Understanding Device Icons, page 3-6.

The following topics explain the device management options.
- To understand device attributes and the View button, see Displaying Device Attributes, page 11-2.
- To understand configurable device properties and the Edit button, see Editing a Device, page 11-3.
- To understand the Enable Monitoring button and the Disable Monitoring button, see Enabling or Disabling Device Monitoring, page 11-6.
- To understand the device monitoring operations summary and the Report button, see Displaying a Device Monitoring Summary, page 11-7.
- To understand the use and effect of the Delete button, see Deleting a Device, a Group, or a Context, page 11-8.

## Displaying Device Attributes

You can display attributes for any validated device.

**Before You Begin**
Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.
Procedure

Step 1  Select Devices > Managing Devices.

The Managing Devices page displays an Object Selector and action buttons. See Using an Object Selector, page 3-10.

Step 2  Select a device or a device group from the selection tree, then click View.

The View Device Detail window displays device attributes (Table 11-1).

Note  The View Device Detail window displays no details for a parameter in cases where the corresponding parameter is not set on the device.

Reference

Table 11-1  View Device Detail Window

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Displayed Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Enabled</td>
<td>Yes or No.</td>
</tr>
<tr>
<td>Name</td>
<td>Hostname, IP address, or SNMP sysname.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Device IP address</td>
</tr>
<tr>
<td>SysName</td>
<td>System name.</td>
</tr>
<tr>
<td>SysOid</td>
<td>Unique identifier for the device type.</td>
</tr>
<tr>
<td>Product</td>
<td>Specific product revision.</td>
</tr>
<tr>
<td>Family</td>
<td>Device type.</td>
</tr>
<tr>
<td>Version</td>
<td>Software version installed on the device.</td>
</tr>
<tr>
<td>Description</td>
<td>Detailed device description.</td>
</tr>
<tr>
<td>Contact</td>
<td>Person to contact if this device is malfunctioning or misconfigured.</td>
</tr>
<tr>
<td>Location</td>
<td>Physical location of the device.</td>
</tr>
</tbody>
</table>

Editing a Device

You can edit the SNMP settings and device credentials that Performance Monitor uses when it communicates with a device for validation or polling.

If you select a security context to edit, special considerations apply because you can change the way Performance Monitor represents that context in lists, menus, graphs, reports, logs, or other places if you change the IP address that Performance Monitor associates with the context.
Note

- Validation and polling for a device take more time to complete if the number of SNMP retries or the SNMP timeout period is greater than the default.
- If you manually edit the credentials of a security context that Performance Monitor represented previously in the default way, `<IP_address_of_admin_context>:<context_name>`, the security context is represented by its own IP address.

Before You Begin
Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1
Select Devices > Managing Devices.
The Managing Devices page displays an object selector and action buttons. See Using an Object Selector, page 3-10.

Step 2
Select a device or a device group from the selection tree, then click Edit.

Tip
You can select more than one device at a time. However, your selections are limited to devices of the same type.

Step 3
In the Edit Devices window, complete the optional tasks that meet your requirements (Table 11-2).
The refreshed display shows the result of any optional task that you complete.

Step 4
(Optional) If you plan to save your changes and implement them, you can select the Validate edited devices check box to revalidate the edited device or device group automatically after you click Apply.

Step 5
Do one of the following:
- To discard your changes and close the Edit Devices window, click Cancel.
- To save your changes and implement them, click Apply.
## Table 11-2  Tasks in the Edit Devices Window

<table>
<thead>
<tr>
<th>Optional Task</th>
<th>Procedure</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a different SNMP read community string.</td>
<td>Overwrite the string in the Read Community (or the Chassis Read Community) text box.</td>
<td>The read community string is a password that allows read-only access to the specified device or security context. The default is public. If the community string on your device (or devices, if you selected more than one) differs from the default, you must specify the correct community string before validation can begin and before you can monitor the device. A single Read Community entry can apply to all of the devices that you select, provided that all devices use the identical string. In the case of a security context, the correct read community string to use is the one associated with the IP address that Performance Monitor uses to poll and monitor the context.</td>
</tr>
<tr>
<td>Specify a different SNMP timeout setting.</td>
<td>Select a value from the SNMP Timeout list.</td>
<td>This value is the number of seconds Performance Monitor waits for a response from the device before it asks for a response again. The minimum duration is 1 second and the maximum is 60 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td>Specify a different number of SNMP retry attempts.</td>
<td>Select a value from the SNMP Retries list.</td>
<td>This value is the number of tries Performance Monitor makes to communicate with the device before declaring that the device has timed out. The default is 1 try.</td>
</tr>
<tr>
<td>Use a different administrative username.</td>
<td>Overwrite the existing username if Performance Monitor displays the Username text box.</td>
<td>Performance Monitor displays the Username text box for devices and security contexts that support Telnet connections. In the case of a security context, the correct username to use is the one associated with the IP address that Performance Monitor uses to poll and monitor the context.</td>
</tr>
<tr>
<td>Use a different administrative password.</td>
<td>Overwrite the existing password if Performance Monitor displays the Password text box and the Confirm Password text box.</td>
<td>Performance Monitor displays the Password text box and the Confirm Password text box for devices that support Telnet connections.</td>
</tr>
</tbody>
</table>
Enabling or Disabling Device Monitoring

Tables, graphs, and reports contain information about only those validated devices for which monitoring is enabled. Performance Monitor automatically enables monitoring after a successful device validation; thus it automatically polls the device in following polling cycles.

If you decide to exclude a device from polling, you can disable monitoring for it. Later, at your discretion, you can reenable monitoring manually.

Before You Begin
Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.
Procedure

Step 1 Select Devices > Managing Devices.

The Managing Devices page displays an object selector and action buttons. See Using an Object Selector, page 3-10.

Step 2 Select a device or a device group from the selection tree, then do one of the following:

- Click Enable Monitoring to poll the selected device in every polling cycle.
- Click Disable Monitoring to stop polling the device.

Step 3 (Optional) Select a device from the selection tree, then click View to verify whether monitoring is enabled or disabled for the device.

The Info window displays text that describes the device (Table 11-1). The first line of text says Polling Enabled is either Yes or No.

Related Topics

- Managing Devices, page 11-2
- Displaying Device Attributes, page 11-2

Displaying a Device Monitoring Summary

You can display an operations summary that tells you when Performance Monitor most recently updated the information it uses for tables and graphs under the Monitor tab, and to what extent it updated that information.

Procedure

Step 1 Select Devices > Managing Devices.

Note If you plan to display the monitoring summary, it is not necessary to select anything from the Managing Devices selection tree. If you make selections, they will have no effect on the displayed result.

Step 2 Click Report. For a description of the summary report, see Table 11-3.

Reference

Table 11-3 Monitoring Summary Report

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Unit</td>
<td>Identifies the category of information for which monitored values were updated.</td>
</tr>
<tr>
<td>Last Polling Update</td>
<td>Displays the time and date at which polling occurred most recently, in this format: HH:MM:SS CiscoWorks_Server_timezone YYYY/MM/DD.</td>
</tr>
</tbody>
</table>
Deleting a Device, a Group, or a Context

Performance Monitor enables you to delete its record of a validated device or all devices in a device group. You can also delete the record of a validated admin context. When you delete an admin context, you also delete every virtual context that is associated with that admin context. You cannot directly delete a virtual context.

Before You Begin
Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1
Select Devices > Managing Devices.

The Managing Devices page displays an object selector and action buttons. See Using an Object Selector, page 3-10.

Step 2
Select at least one object from the selection tree, then click Delete.

- If your selection includes a device, that device is removed from system-defined groups and user-defined groups. Performance Monitor no longer polls the device.
- If your selection includes a virtual context, Performance Monitor deletes its record of, and stops polling, that virtual context.
- If your selection includes a device group, all of its member devices are removed from system-defined groups and user-defined groups. Performance Monitor no longer polls any of the devices.
- If your selection includes an admin context, Performance Monitor deletes its record of that admin context as well as its records of all of the virtual contexts on the same physical device. Performance Monitor no longer polls any context on the relevant device.

Information about your selected devices, virtual contexts, device groups, or admin contexts no longer appears in Performance Monitor tables, graphs, or reports.

Related Topic
- Managing Devices, page 11-2
Managing Device Groups

Device groups enable you to interact with multiple devices in a single operation. A device group is a named entity that can contain devices, other groups, or a combination of devices and groups. A group is the conceptual equivalent of a folder.

If you select **Devices > Managing Groups**, you can display existing device groups and place devices into new or existing groups.

Tip
Click **Refresh** to update the device groups list in the selection tree.

The Managing Groups page displays an Object Selector and action buttons. See Using an Object Selector, page 3-10.

Every device known to Performance Monitor appears in one or more of the **system-defined groups** and might also appear in **user-defined groups**.

### System-Defined Groups
System-defined groups exist by default as soon as you install Performance Monitor:

- The **Device Types** folder organizes all devices by device type, and lists even those validated devices for which you have temporarily disabled monitoring.
- The **Monitored Devices** folder organizes monitored devices by device type. It lists only those validated devices for which monitoring is enabled.

You cannot edit or delete a system-defined group. Performance Monitor populates system-defined groups automatically, based on the information it reads from devices during polling. For information about enabling or disabling monitoring for a device, see Enabling or Disabling Device Monitoring, page 11-6.

Note
A system-defined group reflects device or network changes only after Performance Monitor completes the next polling cycle. See Working with System Parameters, page 12-9 for help with configuring polling intervals.

### User-Defined Groups
User-defined groups are groups that you create to meet a requirement that the system-defined groups cannot meet. For example, you might create groups that divide your network assets by geographic regions or corporate divisions.

You can define any number of groups. All groups can contain any combination of subgroups and devices in an organizational hierarchy that you specify.

### Related Topics
- Creating a Group, page 11-9
- Editing a Group, page 11-11
- Deleting Groups, page 11-12

### Creating a Group
You can create user-defined device groups.

Note
To understand the requirements for valid group names and valid group descriptions, see Naming Guidelines, page 11-10.
Managing Device Groups

Before You Begin
Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1  Select Devices > Managing Groups.
The Managing Groups page displays an Object Selector and action buttons. See Using an Object Selector, page 3-10.

Step 2  Click either the Device Groups folder or a user-defined group.
Your selection defines the parent of the group you create.

Step 3  To configure a new device group, click Add.

Note  You can create a new group only if you select its parent first. You cannot add subgroups to any system-defined group.

The Add Group page displays an Object Selector, text boxes, and action buttons.

Step 4  Enter a valid name for the new group in the Name text box.

Step 5  (Optional) Enter a valid description of the new group in the Description text box.

Step 6  In the selection tree, select one or more devices or device groups (to select all of the subgroups and devices that they contain).

Step 7  To add the selected devices to the new group, click Add.
Added devices appear in the Devices in Group list.

Step 8  (Optional) To remove devices from the group, select them from the Devices in Group list, then click Remove.

Step 9  Save or discard your changes and return to the Managing Groups page:
• To save the new group, click Save.
The new group is displayed and added to the Object Selector.
• To discard your changes, click Cancel.

Related Topics
• Managing Device Groups, page 11-9

Naming Guidelines
Performance Monitor imposes these restrictions on the names and descriptions of user-defined device groups:
• No more than 64 characters are permitted in a device group name.
• No more than 256 characters are permitted in a device group description.
• In addition to spaces and alphanumeric characters (upper case and lower case) such as a123b or A123B, Performance Monitor permits only these characters in device group names and descriptions:
  ! # $ % ^ * + / : ; = ? _ ` \ ( ) { } ~ ,
• These characters are forbidden in group names and descriptions:
  * & ^ @ < > |

### Editing a Group

You can edit the names, descriptions, and structure of user-defined device groups.

**Before You Begin**

Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

**Procedure**

**Step 1**

Select **Devices > Managing Groups**.

The Managing Groups page displays an Object Selector and action buttons. See Using an Object Selector, page 3-10.

**Step 2**

Click a user-defined device group.

**Step 3**

To change the device group, click **Edit**.

___________

**Note**

You cannot edit a system-defined group.

The Edit Group page displays an Object Selector, text boxes, and action buttons.

**Step 4**

Complete the tasks that meet your requirements (**Table 11-4**).

The refreshed display shows the result of any task that you complete.

**Step 5**

Save or discard your changes and return to the Managing Groups page:

- To save the new group, click **Save**.
  
  The new group is displayed and added to the Object Selector.

- To discard your changes, click **Cancel**.

---

**Reference**

**Table 11-4 Tasks in the Edit Group Page**

<table>
<thead>
<tr>
<th>Optional Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the device group name.</td>
<td>Change the device group name in the Name text box. See Naming Guidelines, page 11-10.</td>
</tr>
<tr>
<td>Provide or change the device group description.</td>
<td>Enter the new or changed device group description in the Description text box. See Naming Guidelines, page 11-10.</td>
</tr>
</tbody>
</table>
| Add devices individually to the edited group. | 1. Select one or more devices from the selection tree.  
                                             2. To add the selected devices to the edited group, click **Add**.  
                                             Added devices appear in the Devices in Group list. |
Deleted Groups

You can delete user-defined device groups.

**Before You Begin**

Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

**Procedure**

2. Click a user-defined device group.
3. To delete the device group, click Delete.

**Note**

You cannot delete a system-defined group.

4. Click OK.

Although you delete the user-defined group, the devices in that group are not deleted. You can continue to access the relevant devices from the system-defined device groups in which they are listed.

**Related Topic**

- Managing Device Groups, page 11-9
Effective network management requires the fastest possible identification and resolution of events that occur on mission-critical systems.

Performance Monitor administrative options enable you to configure event detection that identifies, displays, and logs events proactively, according to formula-based and user-configurable thresholds.

The following table describes the administrative options that you access from within Performance Monitor.

<table>
<thead>
<tr>
<th>Table 12-1 Performance Monitor Administrative Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Notifications</td>
</tr>
<tr>
<td>Events</td>
</tr>
<tr>
<td>System Parameters</td>
</tr>
<tr>
<td>Logs</td>
</tr>
<tr>
<td>My Profile</td>
</tr>
</tbody>
</table>

**Working with Notifications**

Performance Monitor can notify you automatically when important conditions meet or exceed the performance parameters that you define globally or for a specific service. Performance Monitor sends separate notifications for each notification type that you configure.

The following topics explain notifications and how to configure them:

- Understanding Supported SNMP Traps and Syslog Messages, page 12-2
- Configuring Notification Settings, page 12-3
- Understanding Supported Event Types for Notifications, page 12-5
Understanding Supported SNMP Traps and Syslog Messages

Notifications require that Performance Monitor receive essential information from monitored devices, which provide that information by means of SNMP traps, Syslog messages, and device polling. For additional information, see Receiving SNMP Traps, page 2-15.

Performance Monitor can process the following kinds of SNMP traps:

<table>
<thead>
<tr>
<th>Source Device</th>
<th>Supported SNMP Traps and Syslog Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA devices</td>
<td>• ASA-4-113019</td>
</tr>
<tr>
<td></td>
<td>• ASA-7-713052</td>
</tr>
<tr>
<td>CSM service module</td>
<td>• Real server state transition</td>
</tr>
<tr>
<td></td>
<td>• Interface operation status</td>
</tr>
<tr>
<td>VPN service module</td>
<td>• Policy added</td>
</tr>
<tr>
<td></td>
<td>• Policy deleted</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap added</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap deleted</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap attached</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap detached</td>
</tr>
<tr>
<td></td>
<td>• Tunnel start</td>
</tr>
<tr>
<td></td>
<td>• Tunnel stop</td>
</tr>
<tr>
<td></td>
<td>• Interface operational status</td>
</tr>
<tr>
<td>VPN router</td>
<td>• Policy added</td>
</tr>
<tr>
<td></td>
<td>• Policy deleted</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap added</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap deleted</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap attached</td>
</tr>
<tr>
<td></td>
<td>• Cryptomap detached</td>
</tr>
<tr>
<td></td>
<td>• Tunnel start</td>
</tr>
<tr>
<td></td>
<td>• Tunnel stop</td>
</tr>
<tr>
<td></td>
<td>• Interface operational status</td>
</tr>
</tbody>
</table>
Performance Monitor can process the following kinds of Syslog messages:

<table>
<thead>
<tr>
<th>Source Device</th>
<th>Supported Syslog Message Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN 3000 concentrator</td>
<td>• IKE-5-120</td>
</tr>
<tr>
<td></td>
<td>• AUTH-5-28</td>
</tr>
<tr>
<td>PIX firewalls</td>
<td>• PIX-1-104001</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-105006</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-105007</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-101001</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-1011002</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-101004</td>
</tr>
<tr>
<td></td>
<td>• PIX-2-709007</td>
</tr>
<tr>
<td></td>
<td>• PIX-3-201008</td>
</tr>
<tr>
<td></td>
<td>• PIX-3-202001</td>
</tr>
<tr>
<td></td>
<td>• PIX-4-113019</td>
</tr>
<tr>
<td></td>
<td>• PIX-7-713052</td>
</tr>
<tr>
<td>Firewall service modules</td>
<td>• PIX-1-105006</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-105007</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-101001</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-1011002</td>
</tr>
<tr>
<td></td>
<td>• PIX-1-101004</td>
</tr>
<tr>
<td></td>
<td>• PIX-2-709007</td>
</tr>
<tr>
<td></td>
<td>• PIX-3-201008</td>
</tr>
<tr>
<td></td>
<td>• PIX-3-202001</td>
</tr>
<tr>
<td></td>
<td>• FWSM-4-113019</td>
</tr>
<tr>
<td></td>
<td>• FWSM-7-713052</td>
</tr>
</tbody>
</table>

### Configuring Notification Settings

Performance Monitor can notify you automatically when important conditions meet or exceed the performance parameters that you define globally or for a specific service. Performance Monitor sends separate notifications for each notification type that you configure.

Three notification levels exist:

- **Global**—all events for all service types.
- **Service**—all events for one service type.
- **Event**—a specific event for a specific service type.
Working with Notifications

Note
If you configure a notification setting globally and duplicate it at either the service level or the event level, you will receive duplicate notifications. You will also receive duplicate notifications if you configure notification settings at the event level that overlap with notification settings you configure at the service level.

Before You Begin
- Make sure that you have configured CiscoWorks Common Services to use an email server. See Setting Common Services to Use Email, page 2-15.
- Make sure that you have the correct privileges to configure notification settings. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select Admin > Notifications.
Step 2 Select the type of notification you want to configure in the tree:
- Global—To configure Global notifications.
- A service type (Firewall, Load Balancing, Remote Access VPN, SSL, Site-to-Site VPN)—To configure notifications for all event types for that service.
- An event type within a service type (the lowest nodes in the tree, for example, CPU Usage)—To configure notifications only for that event type. See Understanding Supported Event Types for Notifications, page 12-5.

Tip Your selection in the tree refreshes the screen, but your selection is not retained in the tree. To see what kind of notification you are configuring, you must look at the title in the right pane above the Email Recipients list. This title will say “Global Notifications,” “Service Notifications: Service Type,” or “Event Notifications: Event Type.”

Step 3 Perform any of the tasks explained in Table 12-2.

Table 12-2 Notification Configuration Procedures

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an email recipient.</td>
<td>1. In the Email Recipients area, click Add.</td>
</tr>
<tr>
<td></td>
<td>2. In the Edit Email Recipients window, enter one email address in the Email Address text box.</td>
</tr>
<tr>
<td></td>
<td>3. Define the severity range of events for which to send email messages: Select options in the From Priority list and the To Priority list, where P1 is a problem of high severity, P5 is a problem of low severity, and OK is a resolved problem. The severity level selection in the From area must be lower than the level selection in the To area.</td>
</tr>
<tr>
<td></td>
<td>4. Click Apply. The Edit Email Recipients window closes. The Notifications page is refreshed and the recipient that you define appears in the Email Recipients list.</td>
</tr>
</tbody>
</table>
Working with Notifications

Understanding Supported Event Types for Notifications

Notifications support more than 40 different event types, categorized by service type (see Table 12-3).

Table 12-2 Notification Configuration Procedures (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an SNMP trap recipient.</td>
<td>1. In the Trap Recipients area, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Edit Trap Recipients window, enter the monitored device IP address or DNS hostname in the Host text box.</td>
</tr>
<tr>
<td></td>
<td>3. Enter the device SNMP port number in the Port text box.</td>
</tr>
<tr>
<td></td>
<td>4. Enter the device read community string in the Community text box.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Apply</strong>. The Edit Trap Recipients window closes. The Notifications page is refreshed and the recipient that you define</td>
</tr>
<tr>
<td></td>
<td>appears in the Trap Recipients list.</td>
</tr>
</tbody>
</table>

Add a Syslog recipient.

1. In the Syslog Recipients area, click **Add**.
2. In the Edit Syslog Recipients window, enter one Syslog hostname or IP address in the Host text box.
3. Enter the device port number in the Port text box.
4. Click **Apply**. The Edit Syslog Recipients window closes. The Notifications page is refreshed and the recipient that you define appears in the Syslog Recipients list.

Edit a recipient.

1. Select the recipient to edit and click the Edit button for that area.
2. Change settings as appropriate, then click **Apply**.

Delete a recipient (disable notification).

Select the recipient to delete and click the Delete button for that area.

**Note** Deletions take effect immediately. There is no undo function.

Configure thresholds for an event type

If you select a specific event type, you can configure the threshold settings for that event notifications by clicking the Threshold button below the recipients lists. For more information on configuring thresholds, see Working with Event Thresholds, page 12-7.
Table 12-3  Notification Event Types

<table>
<thead>
<tr>
<th>Monitored Service</th>
<th>Supported Event Types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall</strong></td>
<td>CPU Usage</td>
</tr>
<tr>
<td></td>
<td>Command Replication</td>
</tr>
<tr>
<td></td>
<td>Device Accessible via Https</td>
</tr>
<tr>
<td></td>
<td>Device Accessible via Snmp</td>
</tr>
<tr>
<td></td>
<td>Failover</td>
</tr>
<tr>
<td></td>
<td>Failover Cable</td>
</tr>
<tr>
<td></td>
<td>Fragment Size</td>
</tr>
<tr>
<td></td>
<td>HA Other</td>
</tr>
<tr>
<td></td>
<td>Interface State</td>
</tr>
<tr>
<td></td>
<td>Memory Usage</td>
</tr>
<tr>
<td></td>
<td>New Connections</td>
</tr>
<tr>
<td></td>
<td>Regular Translation</td>
</tr>
<tr>
<td></td>
<td>Translation Slot</td>
</tr>
<tr>
<td><strong>Load Balancing</strong></td>
<td>Connection Failure</td>
</tr>
<tr>
<td></td>
<td>Created Connection Rate</td>
</tr>
<tr>
<td></td>
<td>Dropped Connection</td>
</tr>
<tr>
<td></td>
<td>Interface Status</td>
</tr>
<tr>
<td></td>
<td>Real Server Status</td>
</tr>
<tr>
<td><strong>Remote Access VPN</strong></td>
<td>Bandwidth Usage</td>
</tr>
<tr>
<td></td>
<td>CPU Usage</td>
</tr>
<tr>
<td></td>
<td>Device Accessible via Snmp</td>
</tr>
<tr>
<td></td>
<td>Device Load</td>
</tr>
<tr>
<td></td>
<td>Inbound Connection Failures</td>
</tr>
<tr>
<td></td>
<td>Interface Status</td>
</tr>
<tr>
<td></td>
<td>Packet Drop</td>
</tr>
<tr>
<td></td>
<td>SEP Module Packet Drop</td>
</tr>
<tr>
<td></td>
<td>SEP Module Status</td>
</tr>
<tr>
<td><strong>SSL</strong></td>
<td>CPU Usage</td>
</tr>
<tr>
<td></td>
<td>Device Accessible via Https</td>
</tr>
<tr>
<td></td>
<td>Memory Usage</td>
</tr>
<tr>
<td></td>
<td>SSL Errors</td>
</tr>
</tbody>
</table>
When you create a threshold, you:

- Define the boundaries of operational states (such as OK, Degraded, and Overloaded) for a performance metric or failure metric in a specific service.
- Specify the number of consecutive polling cycles during which an operational state must recur before records are updated.
- Associate a priority level with each possible operational state for a specific metric (for display and user notification purposes).

Although the thresholds that you define use different services, metrics, and states, every threshold definition follows the same basic workflow.

### Table 12-3 Notification Event Types

<table>
<thead>
<tr>
<th>Monitored Service</th>
<th>Supported Event Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-Site VPN</td>
<td>CPU Usage</td>
</tr>
<tr>
<td></td>
<td>Connection Failures</td>
</tr>
<tr>
<td></td>
<td>Crypto Map Binding</td>
</tr>
<tr>
<td></td>
<td>Crypto Map Change</td>
</tr>
<tr>
<td></td>
<td>Crypto Packet Drops</td>
</tr>
<tr>
<td></td>
<td>Device Accessible via Https</td>
</tr>
<tr>
<td></td>
<td>Device Accessible via Snmp</td>
</tr>
<tr>
<td></td>
<td>ISAKMP Policy Change</td>
</tr>
<tr>
<td></td>
<td>Interface Status</td>
</tr>
<tr>
<td></td>
<td>Memory Usage</td>
</tr>
<tr>
<td></td>
<td>Packet Drop</td>
</tr>
<tr>
<td></td>
<td>Tunnel Status</td>
</tr>
</tbody>
</table>

You might receive a flood of email messages about your DMVPN spoke-to-spoke tunnels if you do all of the following:

- Configure DMVPN to use a full mesh topology that supports spoke-to-spoke sessions.
- Configure a threshold for site-to-site VPN tunnel down events.
- Schedule automatic email notification for those events.

Site-to-site tunnels are dynamic and have short lives by design, which include many tunnel down events. If this email flood problem affects you, we recommend that you either disable email notification or configure Performance Monitor to monitor hubs only.
When conditions exceed or fall below the thresholds that you define, Performance Monitor records an alarm that you can display and interpret in the relevant Event Browser. If applicable, you can also display critical problems in the Critical Problems summary. See Working in an Event Browser, page 3-12 and Working in the Critical Problems Summary, page 4-2.

Before You Begin
Make sure that you have the correct privileges to use this option. See Understanding User Permissions, page 3-2.

Procedure

Step 1 Select Admin > Events.

Step 2 Select a service from the TOC.

Note Although IOS routers are displayed in the Firewall Devices page if they are configured with inspection policies, you must set event thresholds for routers by selecting the site-to-site VPN service from Admin > Events. Setting event thresholds for the firewall service from the Threshold Configuration page does not apply to routers.

Step 3 Scan the entries in the Events list until you locate the performance metric or failure metric for which you plan to configure thresholds, then select the radio button in the relevant row.

Step 4 Click Threshold.

Tip You can also configure thresholds for an event if you select Admin > Notifications, then select an event and click Threshold.

A Threshold Configuration page appears.

- If you select a failure metric, two opposite State Name values (such as Up and Down) appear in the Threshold Configuration page. Or, one extreme state value (such as OK) precedes multiple intermediate state values.
- If you select a performance metric, a range of State Name values (such as OK, Medium, and High) appears in the Threshold Configuration page; each value is associated with an upper and lower percentage in a range.

Step 5 Select the Enable check box.
You must select the Enable check box, or you cannot define values in a Threshold Configuration page.

Step 6 Do one of the following:

- If you see two opposite values (such as the benign Up and the problematic Down) in the State Name area, specify:
  - The event priority level for the problematic state.
  - The number of polling cycle failures that trigger, and the number of successes that clear, the event associated with the problematic state in the Repetitions before State Change field.
• If you see a range of three values in the State Name area, specify the upper and lower threshold percentages, polling cycle repetitions, and priority levels for each of the three values in the range. For example, you could select 10% as the lower threshold boundary for the intermediate state. (Your selection would, in such a case, be applied automatically as the upper threshold percentage for the benign state.)

Note
When you configure thresholds for a performance metric, the lower threshold percentage for a benign state is always zero (0%), and the priority is always \textit{OK}. The upper threshold percentage for a problematic state is always 100%. You cannot change these values.

Step 7
Do one of the following:

- To discard your selections and return to the Events page, click \texttt{Cancel}.
- To save and implement your selections, click \texttt{Apply}.
- To reset all values to their default settings and remain in the Threshold Configuration page, click \texttt{Default}.

---

## Working with System Parameters

You can configure polling intervals, truncation intervals, and user session data storage settings.

**Before You Begin**

Make sure that you have the correct privileges to use this option. See \textit{Understanding User Permissions}, page 3-2.

**Procedure**

**Step 1** Select \texttt{Admin \textgreater{} System Parameters}.

**Step 2** Configure the desired settings as explained in Table 12-4. The table shows the minimum and maximum values allowed for each setting, and the default for the setting. To return all values to their defaults, click the \texttt{Default} button.

---

### System Parameters

#### Table 12-4 System Parameter Settings

<table>
<thead>
<tr>
<th>Row Name</th>
<th>Optional Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Interval (min)</td>
<td>Configure polling intervals.</td>
<td>Select an option from the list to specify the number of minutes between polls, then click \texttt{Apply}.</td>
</tr>
<tr>
<td>Hourly aggregated data is kept for (days)</td>
<td>Configure the truncation interval for hourly data.</td>
<td>Select an option from the list to specify the number of days for which hourly data is retained, then click \texttt{Apply}.</td>
</tr>
</tbody>
</table>
Working with Logs

In the unlikely event that you have problems with Performance Monitor itself, you can display or download Performance Monitor debugging log files to assist TAC in resolving the problems.

You can also display an audit trail that describes the VPN sessions of every RAS user whom you (or your colleagues) have logged out.

Before You Begin

Make sure that you have the correct privileges to use this option. You must be either a System Administrator or a Network Administrator to terminate a user session. See Understanding User Permissions, page 3-2.

---

Table 12-4  System Parameter Settings (continued)

<table>
<thead>
<tr>
<th>Row Name</th>
<th>Optional Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily aggregated data is kept for (days)</td>
<td>Configure the truncation interval for daily data.</td>
<td>Select an option from the list to specify the number of days for which daily data is retained, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Weekly aggregated data is kept for (days)</td>
<td>Configure the truncation interval for weekly data.</td>
<td>Select an option from the list to specify the number of days for which weekly data is retained, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Monthly aggregated data is kept for (days)</td>
<td>Configure the truncation interval for monthly data.</td>
<td>Select an option from the list to specify the number of days for which monthly data is retained, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Event data is kept for (days)</td>
<td>Configure the truncation interval for event history data.</td>
<td>Select an option from the list to specify the number of days after which the event history truncates, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Task data is kept for (days)</td>
<td>Configure the truncation interval for task history data.</td>
<td>Select an option from the list to specify the number of days after which the task history truncates, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>User Session Polling Interval (hours)</td>
<td>Configure the user session polling interval.</td>
<td>Select an option from the list to specify the number of hours between polls, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>User Session Report data is kept for (days)</td>
<td>Configure the truncation interval for user session data.</td>
<td>Select an option from the list to specify the number of days after which the user session report truncates, then click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Logout User Audit Trail data is kept for (months)</td>
<td>Configure the truncation interval for user audit trail data.</td>
<td>Select an option from the list to specify the number of months after which the user audit trail truncates, then click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>
Procedure

Step 1  Select Admin > Logs.

Step 2  Select an option from the TOC:

- Click Debugging Log Files to display a list of the logs used in troubleshooting Performance Monitor, including their location on the server and current size. The following debugging logs are available:
  - faults.log—The Faults Log describes historical fault data.
  - job.log—The Job Log describes historical Performance Monitor jobs.
  - polling.log—The Polling Log displays historical device polling data.
  - validation.log—The Validation Log displays historical device validation data.
  - mcpui.log—The Monitoring Center for Performance User Interface Log describes recent user interface operations.
- Click Logout User Audit Trail to display statistics about the RAS VPN users whom you (or your colleagues) have logged out. Table 12-5 describes terminated user sessions.

Note  The user logout feature is described in Chapter 5, “Monitoring Remote Access VPN Services.”

Step 3  (Optional) If you selected Debugging Log Files from the TOC, click a radio button to select a log, then do one of the following:

- To view an HTML version of the log, click View.
- To save a local copy of the log, click Download and then in the window that appears, select File > Save As to save the log as a text file or an HTML file.

You can click Refresh while displaying a log to display information from the most recent polling cycle.

Reference

Table 12-5    Logout User Audit Trail

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Name</td>
<td>Displays the CiscoWorks username of the user who ended (or tried to end)</td>
</tr>
<tr>
<td>Name column</td>
<td>the described VPN session.</td>
</tr>
<tr>
<td>Status column</td>
<td>States either that the forced logout succeeded or failed.</td>
</tr>
<tr>
<td>Error Message column</td>
<td>In cases of failure, displays the relevant error message.</td>
</tr>
<tr>
<td>Time column</td>
<td>Displays a timestamp that indicates when the described VPN session ended.</td>
</tr>
<tr>
<td>Logged Out User</td>
<td>Displays the username for the terminated VPN session.</td>
</tr>
<tr>
<td>column</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 12      Performance Monitor Administration

Selecting a Default Page

You can select a page to display by default when you start Performance Monitor. The default is Summary > Critical Problems.

Procedure

**Step 1**  Select Admin > My Profile.

**Step 2**  Click the name of a page in the selection tree to select that page, then click Apply.

The page that you select is displayed first the next time you start Performance Monitor.

### Table 12-5  Logout User Audit Trail (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Group column</td>
<td>States the name of the VPN 3000 user group associated with the RAS user whose session was terminated.</td>
</tr>
<tr>
<td>Client IP Addr column</td>
<td>Displays the IP address from which the described RAS user connected to the VPN.</td>
</tr>
<tr>
<td>Protocol column</td>
<td>Identifies the protocol of the described VPN session.</td>
</tr>
<tr>
<td>VPN3K Device column</td>
<td>Displays the DNS name or IP address of the VPN 3000 concentrator from which the RAS user was disconnected.</td>
</tr>
<tr>
<td>Traffic In column</td>
<td>Displays the number of inbound bytes.</td>
</tr>
<tr>
<td>Traffic Out column</td>
<td>Displays the number of outbound bytes.</td>
</tr>
<tr>
<td>Connection Duration column</td>
<td>Displays the total duration (in seconds) of the VPN tunnel, before its disconnection.</td>
</tr>
<tr>
<td>Throughput (kbps) column</td>
<td>Displays the averaged throughput speed in the VPN tunnel, before its disconnection.</td>
</tr>
</tbody>
</table>
Frequently Asked Questions About Performance Monitor

The following topics answer common questions about Performance monitor and contain troubleshooting tips:

- Installation, page A-1
- Importing, Validating, and Managing Devices, page A-4
- Administration, page A-7
- Reports, page A-9
- Debugging, page A-10

Installation

- What prevents Performance Monitor from loading in my browser?
- Why do I see a 500 Error when I try to run Performance Monitor?
- How do I verify that Performance Monitor is running properly?
- How do I change the status of Performance Monitor processes?

What prevents Performance Monitor from loading in my browser?

When you start or restart your server, required processes take about 5 minutes to initialize. If you try to load Performance Monitor in your browser while those processes are initializing, you might see an error message like one of these:

- Could not connect to JRun Connector Proxy
- Internal Server Error
  The server encountered an internal error or misconfiguration and was unable to complete your request.

If you see a message of this kind, wait a few minutes, then try again to start Performance Monitor. If you still cannot start it, contact the system administrator.
Why do I see a 500 Error when I try to run Performance Monitor?

If you see the following error message when you try to start Performance Monitor, you are probably using the Cisco Secure ACS Server (ACS) for authentication and authorization (AAA):

```
Error: 500
Location: /mcp/goHome.do
Internal Servlet Error:
java.lang.ArrayIndexOutOfBoundsException: 0 >= 0
```

If you use ACS for AAA, do the following to verify that ACS and Performance Monitor are configured correctly to work together:

**Step 1** Make sure that your Performance Monitor server is configured to use your ACS Server for AAA:

a. From a browser, log in to your Performance Monitor server.

b. Change the URL to `https://server_name/cwhp/loginModule.do`, where `server_name` is the DNS name or IP address of your Performance Monitor server.

   The ACS radio button should be selected in the AAA Server Information page and the required credentials should be present.

**Step 2** Make sure that your ACS server is configured to work with Performance Monitor. A corresponding ACS username must exist for every Performance Monitor username.

a. Verify that every ACS user who will access Performance Monitor belongs to a group that is authorized to access Performance Monitor. See the Cisco Secure ACS user guide for details.

b. Edit the ACS group to which the Performance Monitor users belong. Verify that the MCP check box and the Assign Performance Monitor for Any Network Device radio button are selected. See the Cisco Secure ACS user guide for details.

How do I verify that Performance Monitor is running properly?

Performance Monitor runs properly only when its required server processes are also running.

**Step 1** From a browser, log in to your Performance Monitor server.

**Step 2** In Common Services, select **Server > Admin > Processes**.

**Step 3** Make sure these processes are running:

- Apache
- Tomcat
- MCP
- McpDbEngine

**Step 4** If a required process is not running, you can start the process. See How do I change the status of Performance Monitor processes?
How do I change the status of Performance Monitor processes?

If any process is not running, you can either start the process, or stop all processes and then restart them (to ensure all processes are started in the appropriate order).

**Step 1**  
To restart a specific process, do one of the following:

- From a Performance Monitor browser session—In Common Services, select Server > Admin > Processes, then select a process and click either Start or Stop.

- From the server—From NMSROOT\bin in a Windows command window, enter `pexec <Process Name>` at the prompt. (The process name is case-sensitive.)

**Note**  
If you select specific processes, the process dependencies do not start automatically.

Wait 5 minutes for the processes to start.

**Step 2**  
If the problem persists, restart all processes from the server. Log out of any browser sessions, then log into the server and open a Windows command line. Change directories to NMSROOT\bin, and enter the following commands in order to stop and then restart all processes.

a. To stop processes, enter `net stop crmdmgtd`.

b. To start processes, enter `net start crmdmgtd`.

How do I forward SNMP traps to a different port if port 162 is already in use?

If another application on your server uses UDP port 162 to receive SNMP traps, you must use the `modifyTrapReceiverPort.pl` script to specify a different port number in the Fault.properties file for Performance Monitor.

**Tip**  
If you do not know which specific application uses UDP port 162 on your server (or even know whether any application uses that port), you can use the Windows command `netstat -o -p udp` to associate a process ID number (PID) with that port, then use the Task Manager (Ctrl-Shift-Esc) to associate the PID with a named application.

**Step 1**  
To stop the CiscoWorks Server daemon manager, enter `net stop crmdmgtd` at the Windows command line.

**Step 2**  
Configure the application that forwards SNMP traps to forward them to your Performance Monitor server on a UDP port that you choose. The UDP port number must be above 1024.

**Step 3**  
Enter the following at the command line to configure Performance Monitor to receive SNMP traps on that UDP port:

```
NMSROOT\mcp\bin\modifyTrapReceiverPort.pl disable port_number
```

where NMSROOT is the full pathname of the subdirectory where you installed Common Services and `port_number` is the actual UDP port number on which your Performance Monitor server will receive SNMP traps.
Appendix A  Frequently Asked Questions About Performance Monitor

Importing, Validating, and Managing Devices

- Why does import from DCR fail?
- Why does the import of an SSL service module from a CSV file fail?
- Why does import from a CSV file fail?
- Why is a device that I imported missing from the Device Validation Tasks page?
- Why do I see an error message when I try to import a PIX Firewall device?
- What prevents me from adding PIX Firewall devices to Performance Monitor?
- What prevents me from viewing a device under the Monitor tab?
- What does the Device Not Reachable message mean?
- What should I do if I see an SNMP Timeout error message/event?
- Why has all device polling stopped?

Why does import from DCR fail?

There are two possible explanations:

- If SSL is not enabled on the DCR server from which you failed to import device credentials, enable SSL on that DCR server, then try again to import.
- If the DCR server has an incorrect record for the SNMP configuration and login credentials that a device uses, correct that record on the DCR server, then try again to import.

Why does the import of an SSL service module from a CSV file fail?

You cannot import an SSL service module from a CSV file, but you can add one to Performance Monitor manually. If the SSL service module has a DNS name, make sure a DNS server is configured on Performance Monitor. This enables Performance Monitor to convert the DNS name to an IP address.

To learn how to add an SSL service module manually, see Using the Importing Devices Wizard to Import or Add Devices, page 2-8.

Why does import from a CSV file fail?

This can be because you are using an incorrect CSV file format. To see a sample CSV file that uses the supported format, go to https://<server_name>/mcp/device_CSV_sample.htm, where server_name is the DNS name or IP address of your Performance Monitor server:

You can generate a CSV file from the Device Credentials Repository (DCR) in Common Services or from RME. Performance Monitor supports only CSV version 3.0, not any earlier versions.
Why is a device that I imported missing from the Device Validation Tasks page?

If no new tasks are displayed in the Device Validation Tasks page (Devices > Importing Devices) after you complete all of the required steps in the import devices wizard, or if devices that are being imported are not visible in other interface pages, ensure that the MCP process is running. The MCP process is responsible for validating and polling devices. If this process is not running, the Device Validation Tasks page does not display the new validation tasks and the Import Devices page does not display any relevant error message.

Step 1  To determine whether the MCP process is running:
  a. Log in to your Performance Monitor server.
  b. Do one of the following:
     • From a browser — Select Common Services > Server > Admin > Processes.
     • From the server — From NMSROOT\bin in the CLI, enter pdshow MCP at the prompt. (MCP must be capitalized.)

Step 2  If the MCP process is not running, do one of the following:
  • From a browser — Select Common Services > Server > Admin > Processes and, from the Start Process page, select the MCP process, then click Start.
  • From the server — From NMSROOT\bin in the CLI, enter pdeexec MCP at the prompt. (MCP must be capitalized.)

Wait 2-3 minutes for the MCP process to start.

Step 3  From the Performance Monitor interface, select Devices > Importing Devices.

Step 4  Click Refresh.

Why do I see an error message when I try to import a PIX Firewall device?

You see the following error message because you are using the enable password instead of the user password while importing a PIX Firewall device:

The Device <device name> could not be imported. Either the firewall HTTPS interface was not enabled or the credentials are not correct. One device failed to be imported. To monitor this device, you must import it again.

To resolve this problem, use the user password instead of the enable password.
What prevents me from adding PIX Firewall devices to Performance Monitor?

If Microsoft Windows Certificate Services generated the certificates on your PIX Firewalls, any malformed URLs in the certificates—or malformed Microsoft universal naming convention (UNC) names—might cause problems in Performance Monitor.

In the following example, a UNC in the last line of text is incorrectly represented as a file:// URL. This kind of error can cause problems in Performance Monitor:

```
[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://yourtest01/CertEnroll/TestConnect.crl
URL=file://\yourtest01\CertEnroll\TestConnect.crl
```

To work around problems of this kind, check your PIX Firewall certificates. If they contain any malformed URLs or misrepresented UNCs, generate a new certificate that contains no errors, then add the device to Performance Monitor.

What prevents me from viewing a device under the Monitor tab?

Verify that the device is being monitored and check the Validation Task Details page for error messages.

**Step 1** Select Devices > Managing Devices.
Verify that the device is present in the Managing Devices page and that it is being monitored.

**Step 2** Select Devices > Importing Devices.

**Step 3** Click the radio button for the device in the Device Validation Tasks list, then click Details.
The Validation Task Details window displays the historical validation results. See Viewing Historical Validation Tasks, page 2-13.

**Step 4** To update the Validation Task Details window, click Refresh.

What does the Device Not Reachable message mean?

The poller could not retrieve all information from the device; therefore, some device data might be unavailable. This happens when:

- **IP connectivity to the device is lost.** Look for and fix network problems that might affect IP connectivity. If the device is too busy to respond to SNMP requests, see its documentation to learn how to analyze the problem and to tune the device.

- **Community strings on the device have changed.** Correct the relevant entries in Performance Monitor, then try again to poll the device.

- **MIB variables on the device have restricted access.** Confirm whether the installed OS version supports the MIBs that Performance Monitor uses. If any newer OS versions are available for the device, consider upgrading to the latest OS version.
What should I do if I see an SNMP Timeout error message/event?

To increase the SNMP Timeout parameters, do one of the following:

- Change the parameters when you import the device under Devices > Importing Devices. See Using the Importing Devices Wizard to Import or Add Devices, page 2-8.
- Edit the device under Devices > Managing Devices. See Editing a Device, page 11-3.

**SNMP Retries** refers to the maximum number of retries. A retry means that there is a failure to talk to the device SNMP agent; therefore, Performance Monitor makes the request again.

**SNMP Timeout** refers to the interval that the device waits between requests. Subsequent retry intervals are computed using the following logic: The retry policy is to double the previous timeout value. For example, if the initial timeout is 3 seconds and the retry count is 3, the timeout values between each retry are 3, 6, 12—a total of 21 seconds.

Why has all device polling stopped?

If a single device does not respond to Performance Monitor polling within the timeout period, polling to all devices stops. You might want to increase the polling timeout period. For more information, see Configuring the Polling Time Out, page 2-16.

Administration

- What prevents me from receiving notifications?
- How do I disable notifications?
- How do I prevent polling information from filling the disk?
- What prevents SNMP Traps from generating events?
- How do I back up and restore the Performance Monitor database?

What prevents me from receiving notifications?

The notifications are probably not configured.

**Step 1** Select Admin > Notifications.
**Step 2** From the selection tree, select Site-to-Site VPN.
**Step 3** Verify that the Email Recipients, Trap Recipients, and Syslog Recipients notifications are configured. If they are not configured, configure them. See Configuring Notification Settings, page 12-3.

How do I disable notifications?

**Step 1** Select Admin > Notifications.
**Step 2** Click the relevant service folder in the selection tree.
The Service Notifications page displays Email Recipients, Trap Recipients, and Syslog Recipients notifications. Notifications are disabled immediately. There is no undo function.

Step 3  Select the notification to disable, click Delete for that type of notification.

**How do I prevent polling information from filling the disk?**

To prevent information from gathering at a high polling rate and filling the disk, configure the number of days that polled data is stored. Select Admin > System Parameters, reduce the values, then click Apply. See Working with System Parameters, page 12-9.

**What prevents SNMP Traps from generating events?**

When SNMP traps do not generate events, the cause can be one or both of the following:

- Another application in addition to Performance Monitor uses UDP port 162 on your server.
- The device might not be configured to send SNMP traps.

Step 1  If another application on your server uses UDP port 162 to receive SNMP traps, you must reconfigure Performance Monitor to receive traps on a different port. From the Windows command line, enter:

```
NMSROOT\bin\perl.exe NMSROOT\mcp\bin\modifyTrapReceiverPort.pl port
```

where *NMSROOT* is the full pathname of the subdirectory in which you installed Common Services and *port* is the numeric value of the port that you will use. (This command edits the Fault.properties file for Performance Monitor.)

Step 2  Restart Performance Monitor.

After you restart it, Performance Monitor listens for traps on the new port number.

Step 3  Make sure that the device is configured to send SNMP traps. To learn what steps are required, see Bootstrapping Devices, page 2-2. You can:

- Set up SNMP traps to generate the Real Server Status load balancing event.
- Set up SNMP traps to generate the following site-to-site VPN events:
  - Crypto Map Binding
  - Crypto Map Change
  - ISAKMP Policy Change
  - Tunnel Status
  - Interface Status
How do I back up and restore the Performance Monitor database?

Performance Monitor uses Common Services to back up and restore the database. When you perform backup and restore, the database for all applications that use Common Services are backed up or restored (for example, if Performance Monitor and Security Manager are installed on the same server, the backup/restore covers both applications).

To create backups or a regular backup schedule, open Common Services and select Server > Admin > Backup. Click the Help button to learn more about backup and restore.

Reports

- I deleted a device, then added it back. Then I ran a report and noticed that it displayed data earlier than the time I added the device. Why?
- Why would the User Session Report for a VPN 3000 concentrator omit SSL VPN (WEBVPN) user login details?
- Why is the User Session Report empty for a VPN 3000 concentrator?
- Why are the CPU Usage% and Memory Usage% columns blank for the Cisco 800 series router?

I deleted a device, then added it back. Then I ran a report and noticed that it displayed data earlier than the time I added the device. Why?

When you delete a device, it is marked as Deleted in the database, but the data related to that device is removed only after 2 hours. Every 2 hours, a background process updates the database and removes data for deleted devices. If you add the device back sooner than 2 hours (before the database removes the related data) and run a report the next day, you have information for that day as well as for the previous days of the week (except for the less-than-2-hour span when the device was deleted).

Why would the User Session Report for a VPN 3000 concentrator omit SSL VPN (WEBVPN) user login details?

You must enable the WEBVPN syslog classname on the concentrator:

Step 1 Log in to the VPN 3000 Concentrator Series Manager.
Step 2 Select Configuration > System > Events > Classes.
Step 3 Click Add.
Step 4 From the Class Name list, select WEBVPN, then select the Enable check box.
Step 5 From the Events to Syslog list, select 1-5, then click Add.
Step 6 Click Save Needed—located in the upper right corner.
Step 7 Click OK.
Step 8 Enable syslog. See Why is the User Session Report empty for a VPN 3000 concentrator? for instructions.
Why is the User Session Report empty for a VPN 3000 concentrator?

This could be because syslog is not enabled on the VPN 3000 concentrator. To enable syslog:

Step 1 Log in to the VPN 3000 Concentrator Series Manager.
Step 2 Select Configuration > System > Events > Classes, then click Add.
Step 3 From the Class Name list, select AUTH, then select the Enable check box.
Step 4 From the Severity to Syslog list, select 1-5, then click Add twice.
Step 5 From the Class Name list, select IKE, then select the Enable check box.
Step 6 From the Severity to Syslog list, select 1-5, then click Add.
Step 7 Click Save Needed, in the upper right corner, then click OK.
Step 8 Select Configuration > System > Events > Syslog Servers., then click Add.
Step 9 In the Syslog Server field, enter the IP address of your Performance Monitor server, then click Add.
Step 10 (Optional) To improve performance in the Performance Monitor application itself if it is the only application to which the concentrator will send syslog messages:
   a. Select Configuration > System > Events > General.
   b. Select None from the Severity to Syslog list.
   c. Click Apply.

Why are the CPU Usage% and Memory Usage% columns blank for the Cisco 800 series router?

This is a known problem. The management information base (MIB) for Cisco 800 Series routers does not provide CPU usage information and, in some cases (when certain IOS images are installed), does not provide Memory usage information.

Debugging

- How do I turn on debugging?
- How do I debug a problem related to importing a device?

How do I turn on debugging?

Step 1 Start Performance Monitor.
Step 2 Change the URL to https://server_name/mcp/debuglog.do, where server_name is the DNS name or IP address of your Performance Monitor server.
   The Enable Debug Log window opens.
Step 3 For each log file that matters to you, select on from the list in the debug column.
Step 4  Click Submit, then close the window.

Step 5  To turn debugging off when you are done.
   b. Select off from the list in the debug column.
   c. Click Submit, then close the window.

How do I debug a problem related to importing a device?

Step 1  Turn debugging on for the following log files:
   • validation.log
   • mcpui.log
   See How do I turn on debugging? for instructions.

Step 2  Restart Performance Monitor, then try again to import the device.

Step 3  Select Admin > Logs > Debugging Log Files.

Step 4  Select the validation.log and mcpui.log files, then click Download.

Step 5  Send the downloaded files to the TAC support engineer who is handling your case.

Step 6  Turn debugging off after you are done.
   a. Go to https://server_name/mcp/debuglog.do, where server_name is the DNS name or IP address of your Performance Monitor server.
   b. Select off from the list in the debug column.
Numerics

500 error message A-2

A

ACS
  troubleshooting 500 error message A-2
adding
  device groups (see under device groups, managing) 11-9
  devices 2-8
e-mail targets for global 12-4
SNMP traps for notifications 12-5
Syslog targets for notifications 12-5
administering Performance Monitor 12-1
default page, selecting 12-12
event thresholds, working with 12-7
logs, working with 12-10
notifications, working with 12-1
notification settings, configuring 12-3
system parameters, working with aggregated data, settings for deleting 12-9
approver user role 3-3
authentication, user 3-2
authorization, user 3-2

B

bandwidth
  consumption graphs 4-5
  utilization graphs 5-6

C

categories
  events 3-11
  reports 10-1
Cisco Catalyst 6500 Series switches
  low performance in SSL modules 9-2
Cisco Security Management Suite server, logging into or exiting 3-1
CiscoWorks Common Services 1-1
  logging into or exiting 3-1
  roles, user 3-2
cluster RAS data, isolating and viewing 5-2
cluster RAS device data, isolating and viewing
  details for a device, viewing 5-4
  device crypto accelerator card data, viewing 5-10
  device crypto activity, monitoring 5-8
  device failures, monitoring 5-7
  interface status for a single device 5-10
  usage and activity, monitoring 5-6
cluster RAS users, working with 5-11
  identifying top 10 users of a device 5-13
  of a RAS cluster 5-14
community strings
  adding devices 2-8
concepts
  content switching 8-1
  critical problems 1-3
dashboard 1-3
event browser 1-3
events 1-3
firewall services 7-1
graphs and tables 1-4
remote access VPN services 5-1
site-to-site VPN 6-1
SSL services 9-1
user roles and permissions
  approver 3-3
  developer 3-3
  export data 3-3
  help desk 3-3
  network administrator (capacity planner) 3-2
  network operator 3-3
  system administrator 3-2
connection failure graphs
  top three remote access devices 4-4
  top three site-to-site devices 4-4
connection graphs, top three firewall devices 4-5
core view (see dashboard) 1-3
content-switching services, monitoring 8-1
collective modules 8-2
  activity statistics, displaying 8-2
  CSM usage, displaying 8-2
  load balancing failure statistics, displaying 8-3
  server and policy reject statistics, displaying 8-4
concepts in 8-1
CSM Services summary, working in 4-6
individual modules 8-5
  interfaces table, displaying 8-8
  module detail graphs, displaying and interpreting 8-5
  real servers table, dislpaying 8-7
  virtual servers table, displaying 8-6
service modules, purpose of 8-2
CPU usage graphs
  firewall devices 7-3
  site-to-site devices 6-7
Critical Problems summary, working in 4-2
CSV file format 2-9
dashboard, working with 1-3
default startup page, selecting 12-12
deleting
  aggregated data 12-9
  device groups 11-12
  devices 11-8
  targets for notification 12-5
developer user role 3-3
device groups, managing 11-9
  deleting 11-12
  editing 11-11
  naming guidelines for 11-10
  user-defined, creating 11-9
devices
  about 11-1
    adding 2-8
    attributes, displaying 11-2
    CSV file format 2-9
    device monitoring, enabling or disabling 11-6
    importing 2-8
    managing 11-2
      deleting 11-8
      editing 11-3
      maximum number you can monitor 1-1
      validating 2-11
        historical validation tasks, viewing 2-13
        scheduling device validations 2-12
disabling TrapForwarder A-3
displaying
current network condition of
  CSM load balancing services 4-6
  firewall services 4-5
  SSL load balancing services 4-7
  VPN services 4-3
  known critical problems in network 4-2
dropped packet graphs for site-to-site devices 6-7
E

eediting
device groups 11-11
devices 11-3
e-mail
jobs, and reporting 10-11
targets, adding for notifications 12-4
event
categories 3-11
thresholds, working with 12-7
export data user role 3-3

F

faults.log, description 12-11
FCAPS, and Performance Monitor 1-4
features of Performance Monitor
event management 1-3
historical reports 1-2
real-time monitoring 1-2
summary views 1-2
system parameter settings 1-3
firewall services, monitoring 7-1
concepts in 7-1
detail 7-2
connection statistics, displaying 7-5
current interface state, displaying 7-4
current state of blocks on firewall devices, displaying 7-5
summary graphs, interpreting 7-3
high-level overview, displaying 7-1
tables and pages useful in
Firewall Device Blocks Details table 7-5
Firewall Device Connections table 7-5
Firewall Device Interface Status table 7-4
Firewall Devices table 7-1
Firewall Services summary 4-5
summary graphs 7-3

frequently asked questions A-1

G

ggetting started 3-1
Event Browsers 3-12
Object Selector, using 3-10
routers and switches, setting up 2-2
sequence of operations 3-17
tables 3-6
actions on tables 3-8
check boxes 3-8
common elements in 3-8
multipage tables 3-7
optional tasks in 3-9
rows and columns 3-6
user interface 3-3
icons and symbols 3-5
understanding 3-4
wizards, using 3-10

H

help desk user role 3-3

I

importing devices 2-8
Importing Devices wizard 2-8
inbound connection failure graphs for site-to-site devices 6-7
installation troubleshooting
error messages, understanding A-1
process status, changing A-3
TrapForwarder, disabling A-3
interface error graphs
firewall devices 7-3
top three errors 4-5
Index

J
job.log, description 12-11

L
log files
descriptions 12-11
working with 12-10

M
MCP process maintenance 3-16
mcpui.log, description 12-11
memory usage graphs
  firewall devices 7-3
  site-to-site devices 6-7
monitoring features, matrix of 1-5

N
naming guidelines for device groups 11-10
network administrator (capacity planner) user role 3-2
network operator user role 3-3
notifications
  settings for, configuring 12-3
  SNMP traps supported 12-2
  syslog messages supported 12-2
  working with 12-1

P
packet drop
  remote access devices graph 5-6
  site-to-site devices graph 6-7
Performance Monitor
  logging into or exiting 3-1
  overview 1-1
  user authentication and authorization 3-2
  verifying processes A-2
permissions 3-2
polling.log, description 12-11
polling timeout, configuring 2-16
processes, verifying A-2

R
RAS cluster device data, isolating and viewing
detail 5-4
  device crypto accelerator card data, viewing 5-10
  device crypto activity, monitoring 5-8
  device failures, monitoring 5-7
  usage and activity, monitoring 5-6
tables and pages useful in
  RAS Clusters table 5-2
RAS device data, isolating and viewing
status display, tabular format 5-10
tables and pages useful in 5-10
read community strings
adding devices 2-8
remote access VPN services, monitoring 5-1
  cluster users, working with 5-11
  details, displaying 5-12
  top 10 users of a cluster, identifying 5-14
  top 10 users of a device, identifying 5-13
RAS cluster device data, isolating and viewing 5-6
  detail 5-4
  remote access clusters, displaying 5-2
RAS cluster device details, working with 5-4
  device crypto accelerator card data, displaying 5-10
  device crypto activity, monitoring 5-8
  device failures, monitoring 5-7
  interface status data for a device, displaying 5-10
  summary graphs, interpreting 5-4
  viewing 5-4
reports (see trend reports) 10-1
roles 3-2
routers and switches, setting up 2-2

SNMP (Simple Network Management Protocol)
  traps, receiving 2-15
  traps supported for notifications 12-2
  trap target, adding notifications 12-5
SSL services, monitoring 9-1
  all modules collectively 9-2
    activity statistics, displaying 9-2
    SSL statistics, working with 9-3
    SSL usage, displaying 9-2
    TCP connection statistics, working with 9-4
  concepts in 9-1
  individual modules 9-5
    module detail graphs, displaying and interpreting 9-5
    proxy errors, working with 9-7
    proxy statistics 9-6
  modules
    low performance in, troubleshooting 9-2
    purpose of 9-1
SSL Services summary, working in 4-7
  tables and pages useful in 4-7
  summaries, using 4-1
  Critical Problems summary 4-2
  CSM Services summary 4-6
  Firewall Services summary 4-5
  options (table) 4-1
    Critical Problems 4-1
    Event Browser 4-1
    Firewall 4-1
    Load Balancing 4-1
    SSL 4-1
    VPN 4-1
  SSL Services summary 4-7
  VPN Services summary 4-3
syslog messages supported for notifications 12-2
Syslog target, adding for notifications 12-5
system administrator user role 3-2
system parameters, working with 12-9
throughput graphs

for remote access devices, displaying 5-6

top 10, displaying 6-9
top 10, displaying

throughput versus connection graphs for firewall devices 7-3

throughput versus tunnels graphs for site-to-site devices 6-7

top 10, displaying

top three

in RAS VPNs 4-4
in site-to-site VPNs 4-4
top three

timeout, configuring polling 2-16

TrapForwarder, disabling A-3
trend reports, using 10-1
categories 10-1
configuring reports 10-6
e-mail jobs, working with 10-11
historical reports, understanding 10-8
RAS VPN user session reports, viewing 10-8
reporting options, understanding 10-1
failure report subcategories 10-2

performance report subcategories 10-3
throughput report subcategories 10-4
usage report subcategories 10-5
top 10 site-to-site VPN tunnel reports, viewing 10-10

top 10 user reports, viewing 10-8
top 10 user reports, viewing 10-8
top 10 user reports, viewing

troubleshooting

500 error message A-2
cannot open Performance Monitor in browser A-1
frequently asked questions A-1
installation error messages, understanding A-1
polling ceases for all devices 2-16
process status, changing A-3
SSL modules, low performance in 9-2
SSL service module, cannot import using CSV file A-4
TrapForwarder, disabling A-3

verifying processes A-2
tunnels

tunnels

locating 6-10
top 10, displaying 6-9
tunnel count graphs, top three site-to-site devices 4-4

working with 6-9

working with 6-9

user

roles and permissions 3-2
approver 3-3
developer 3-3
export data 3-3
help desk 3-3
network administrator (capacity planner) 3-2
network operator 3-3
system administrator 3-2

session count graphs, top three remote access devices 4-4

supported simultaneously 1-1

validation.log, description 12-11

VPN restrictions 1-1

VPN services, monitoring

remote access 5-1

remote access

cluster device details, displaying 5-4
cluster users, monitoring 5-11

concentrators providing services, displaying all 5-6

concepts in 6-1

remote access clusters, displaying 5-1

remote access clusters, displaying 5-1

service status, displaying 4-3

site-to-site 6-1

site-to-site

concepts in 6-1
device details, displaying 6-6
devices, displaying all 6-3
device status, displaying 6-3
tunnels, working with 6-9