Cisco Prime Performance Manager 1.1 User Guide

March 2, 2012

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-24597-01

Cisco Prime Performance Manager 1.1 User Guide

CONTENTS

Preface

This guide describes the architecture, supporting hardware and software, and management procedures for Cisco Prime Performance Manager. The information in this guide helps you to complete the tasks that are necessary to use Prime Performance Manager to monitor the performance of your network.

Prime Performance Manager is a performance software product that provides key performance indicators and summarized historical statistics for managed network elements. Its core design points are ease of use, extensibility, and scalability.

This section describes the audience, organization, and conventions of the *Cisco Prime Performance Manager 1.1 User Guide*. It refers you to related publications and describes online sources of technical information.

For a more detailed description of Prime Performance Manager, see Chapter 1, "Prime Performance Manager Overview." For the latest Prime Performance Manager information and software updates, go to http://www.cisco.com/go/performance.

This preface includes the following topics:

New and Changed Information

The following table describes information that has been added or changed since the initial release of the *Cisco Prime Performance Manager 1.1 User Guide*.

Table 1 New and Changed Information in This Guide

Date Released	Revision	Location
March 2, 2012	Added the ppm genkey command (Prime Performance Manager 1.1.1 enhancement).	ppm genkey, page B-23
	Added the ppm iosreport command (Prime Performance Manager 1.1.1 enhancement).	ppm iosreport, page B-25
	Added the ppm ipslaftpfilesize command (Prime Performance Manager 1.1.1 enhancement).	ppm ipslaftpfilesize, page B-26
	Added the Disable/Enable Sending Alarms action to the list of device summary list actions (Prime Performance Manager 1.1.1 enhancement).	Editing Summary List Items, page 8-9
	Updated the dashboard categories for Prime Performance Manager 1.1.1.	Working with Dashboards, page 7-13
January 27, 2012	Revised Enabling SSL on Gateways and Units procedure.	Enabling SSL on Gateways and Units, page 5-1
	Added "Request" to the list of Category properties.	Table 9-4, "Alarms and Event Properties"
	Made corrections to the file and property used to limit the number of rows in the archived events table.	Table 9-2, "Alarms and Event History Toolbar"
	Changed CISCO-EPM and CISCO-EPM-2 table and section titles to match text in the GUI.	Table 15-1, "CISCO-EPM Trap Notification Attributes" Table 15-2, "CISCO-EPM-2 Notification Attributes"
	Added the CISCO-PRIME trap table.	Table 15-3, "CISCO-PRIME Notification Attributes"
	Changed "MWTM" instances to "PPM".	Chapter 15, "Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters"
	Created new subtopics and updated details in the gateway-to-unit firewall example.	Configuring Gateways and Units for Firewalls, page 17-2
January 10, 2012	Initial release	

Audience

This guide is for system administrators, network operators and basic users who use Prime Performance Manager for reporting on the managed network. They should have:

- Basic network management skills
- Basic Solaris system administrator skills
- Basic Linux system administrator skills

Organization

This guide is divided into the following chapters and appendices:

- Prime Performance Manager Overview provides brief descriptions of Prime Performance Manager architecture, and an overview of how to use Prime Performance Manager to monitor your network performance.
- Managing Gateways and Units Using the Command Line Interface tells you how to use Prime Performance Manager commands to manage gateways and units.
- "Using the Prime Performance Manager Web Interface" describes how to access Prime Performance Manager data from the web interface.
- "Discovering Network Devices" provides basic information and procedures for using Prime Performance Manager.
- "Setting Up and Managing Users" provides information about setting up and managing Prime Performance Manager users.
- "Working With Reports and Dashboards" describes how to view and manage Prime Performance Manager reports.
- "Using Summary Lists" describes how to view and manage Prime Performance Manager summary lists.
- "Using Alarms and Events" describes how to view and manage Prime Performance Manager alarms and events.
- "Configuring Thresholds" describes how to create and manage thresholds in Prime Performance Manager summary.
- "Reviewing Prime Performance Manager Home Page Information" describes information available from the Prime Performance Manager Home page.
- "Viewing System Properties, Statuses, Messages, and Logs" describes Prime Performance Manager system logs and messages.
- "Managing Prime Performance Manager Units" describes how to manage Prime Performance Manager units including creating of unit protection groups.
- "Creating and Editing Device Polling Groups" tells you how to create and manage Prime Performance Manager polling groups.
- "Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters" tells you how to create upstream OSS hosts and tune Prime Performance Manager alarm parameters.
- "Configuring Device Credentials for Y.1371 SLA and Ethernet Flow Point Reports" tells you how to configure device credentials for Y.1371 SLA and Ethernet Flow Point reports.
- "Configuring Prime Performance Manager for Firewalls" tells you how to configure Prime Performance Manager gateways and units for communication through firewalls.
- "Backing Up and Restoring Prime Performance Manager" describes the Prime Performance Manager backup and restore processes.
- Prime Performance Manager and IPv6 describes how IPv6 addressing is handled by Prime Performance Manager.
- "Command Reference" describes the commands used to set up and operate Prime Performance Manager.
- "Glossary" provides definitions to common industry and Prime Performance Manager terms.

Conventions

This document uses the following conventions:

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

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

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

Tip Means *the following is a useful tip*.

Product Documentation

You can access the following additional Cisco Prime Performance Manager guides on the Cisco Prime Performance Manager page on Cisco.com:

- Cisco Prime Performance Manager 1.1 User Guide (this guide)
- Cisco Prime Performance Manager 1.1 Release Notes
- Open Source Used in Cisco Prime Performance Manager 1.1
- Cisco Prime Performance Manager 1.1 Documentation Overview
- Cisco Prime Performance Manager 1.1 Quick Start Guide

Cisco License Manager data sheet can be found at http://www.cisco.com/go/performance

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Prime Performance Manager Overview

The following topics provide an overview to Cisco Prime Performance Manager user operations:

Prime Performance Manager Features and Functions

Prime Performance Manager provides performance statistics and reports for service provider and large enterprise networks including access, edge, distribution, core, mobile backhaul, Carrier Ethernet, and core MPLS networks.

Prime Performance Manager supports Cisco and non-Cisco platforms and devices. Supported Cisco devices include the Cisco 7600 Series Routers, Cisco ASR 901, 903, 1000, and 9000 Series Aggregation Services Routers, Cisco ME 3400, 3600, and 3800 Series Ethernet Access Switches, the Cisco Carrier Routing System (CRS), Cisco Mobile Wireless Routers (MWR), the Cisco uBR, and many others.

Note For a detailed list of devices supported by Prime Performance Manager, visit: http://www.cisco.com/en/US/products/ps11715/products_device_support_tables_list.html

Prime Performance Manager is packaged with more than 900 standard historical, aggregation, and summary reports. Reports can be automatically generated on a 5-minute, 15-minute, hourly, daily, weekly, or monthly basis. Prime Performance Manager allows you to define collection intervals for each supported time interval on a per-report basis. All reports are available in GUI and CSV export format. In addition, you can using an XML editor to define new reports or extend the packaged reports.

Additional Prime Performance Manager features and functions include:

- The ability to define thresholds on any Prime Performance Manager report key performance indicator (KPI). For each KPI you can define three onset and abate threshold levels and associate them with the alarms you want generated.
- The ability to create polling groups to define unique polling frequencies for devices in your network.
- The ability to create report policies that specify report sets for specific devices.

- Centralized reporting and administration through a Web 2.0 graphical user interface and a command line interface (CLI).
- A distributed architecture and embedded database that allows you to monitor and report on networks of varying sizes.
- Synchronized device inventory and credentials from Prime Network.
- Extensibility, including the ability to dynamically add new collection types, KPI definitions, GUI reports, and data exports.
- The ability to cross-launch Cisco Prime Network 3.8 and Cisco Active Network Abstraction (Cisco ANA) 3.7.2 and 3.7.3, including contextual reporting and administration integrated with Prime Performance Manager.
- Automatic device discovery and data collection based on device IP address ranges.
- Support for standard protocols as well as SNMP V2, and V3, and XML-based data collection.
- N+1 high availability protection groups for units.
- Local alarm management features and integration with upstream OSS fault management systems.
- Flexible collection schedules.
- Capability to export report data in CSV format for integration with OSS applications.
- Automatic and custom CSV file generation.
- Pull model CSV file access.

Prime Performance Manager Reports

Prime Performance Manager includes over 900 reports. All reports support table, chart, and dashboard outputs. High-level report categories include:

- Application traffic
- Availability
- IP protocol
- IP QoS
- IP SLA
- Mobile Statistics
- Resources
- Transport statistics

You can modify the provided Prime Performance Manager reports or create new reports. For information, see the *Cisco Prime Performance Manager Integration Developer Guide*.

For more information about Prime Performance Manager reports, see Chapter 7, “Working With Reports and Dashboards.”

Prime Performance Manager Dashboards

Prime Performance Manager dashboards present data from different sources on a single page. For example, the ICMP (Internet Control Message Protocol) application dashboard presents the top ten ICMP hourly packet rates, total errors, total echoes, and echo replies. The CPU/Memory dashboard presents the top ten hourly CPU average and peak utilization as well as the top ten hourly memory pool average and peak utilization. Dashboards provided with the Prime Performance Manager package include:

- Application
- IP Protocol
- IPSLA
- Resource
- Response Time
- Transport
- VPDN
- Video Monitoring Statistic

You can modify the provided Prime Performance Manager dashboards or create new ones. For information, see the *Cisco Prime Performance Manager Integration Developer Guide*.

For more information about Prime Performance Manager reports, see Chapter 7, "Working With Reports and Dashboards."

Prime Performance Manager Architecture

Prime Performance Manager software and functions are distributed across a single gateway and one or more unit servers. The units connect to a gateway through the IP network and through a Secure Sockets Layer (SSL) connection. The gateway is the connection point for users, administrators, and northbound interface (NBI) applications. It stores summarized data for network reports, and is the control point for alarm monitoring and forwarding. The gateway synchronizes administrative data with the units.

Units poll network devices and compute and store the data received from the devices. A unit can be installed with a gateway on the same physical server, or a unit can be installed on a separate physical server. The monitored devices are distributed across a single or multiple units, as directed by the gateway server.

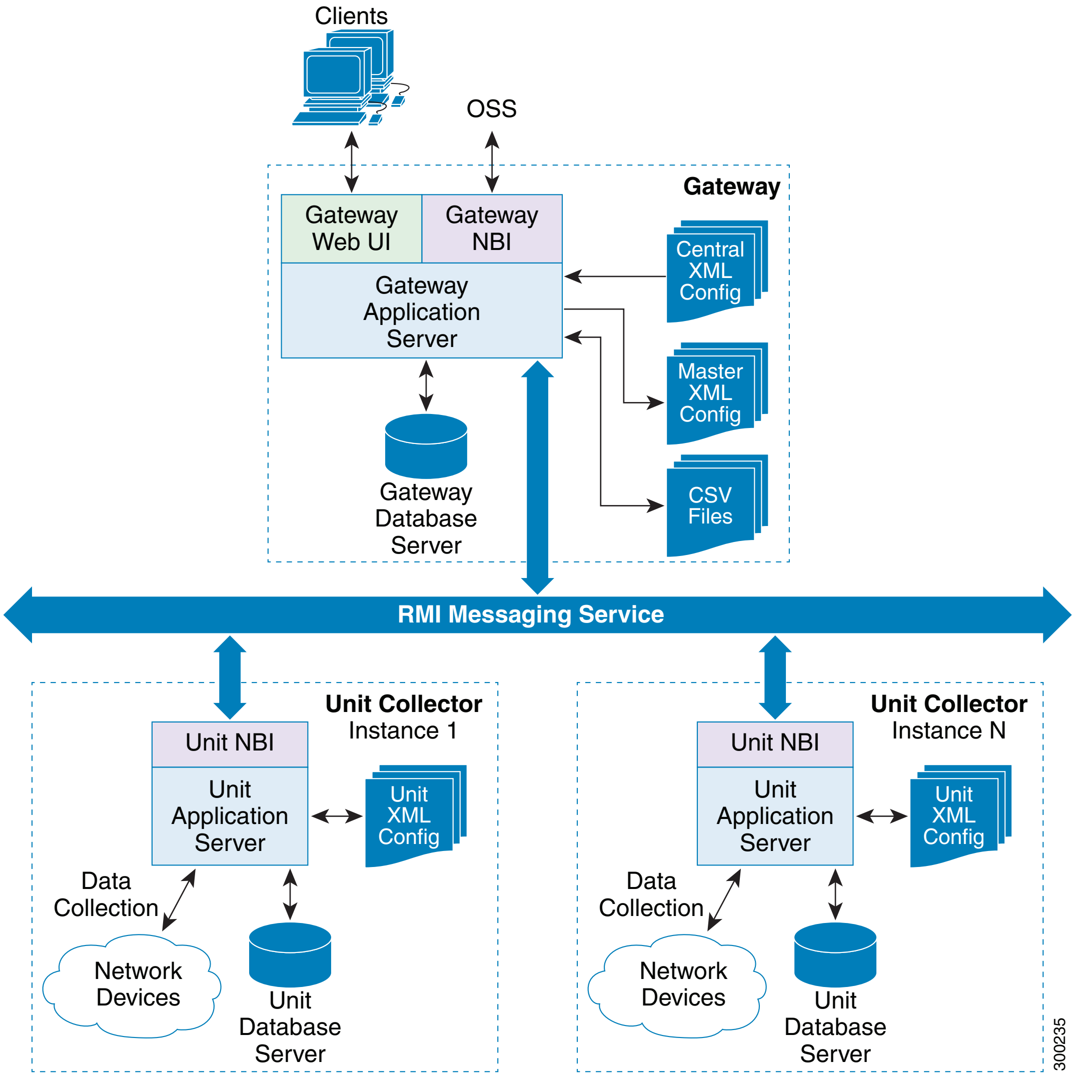
All unit monitoring and management is conducted through the gateway. Gateway-to-unit communication is conducted using Java Remote Invocation (RMI).

Figure 1-1 shows the Prime Performance Manager architecture. Architecture elements include:

- Prime Performance Manager gateways and units are software processes. Gateways and units can run on the same physical machine or on separate ones.
- The master XML configuration defines the reports and associated functions. All XML is created and managed on the gateway, and the gateway distributes the XML to the units.
- The central XML configuration is the conceptual repository used to feed to the units. The central XML configuration is backed by the master XML configuration.'
- CSV are automatically generated. They reside on the gateway and are forwarded there from the units.

- Unit XML configuration is the set of XML file that exist on the unit. These are created when Prime Performance Manager is installed and updated by the gateway.

Figure 1-1 Prime Performance Manager Architecture



Note The Prime Performance Manager database is based on Apache Derby, an open source relational database based on Java. (For information about Apache Derby, see *http://db.apache.org/derby/*). The Prime Performance Manager database resides on the units. For performance, Prime Performance Manager stores data in binary fragments that can be distributed across multiple units for performance, scale, and high availability purposes. The data fragments are reassembled for specific reports, nodes, and time frames and streamed to the gateway when users run queries. For this reason, you cannot query the Prime Performance Manager database using traditional SQL queries or DBMS applications.

Device Discovery

Devices can be added to Prime Performance Manager using one or both of the following methods:

- Import a device inventory from Cisco Prime Network or Cisco Active Network Abstraction (Cisco ANA).
- Run device discovery from Prime Performance Manager.

If devices are imported from Prime Network or Cisco ANA, the device inventory updates are automatically communicated to Prime Performance Manager, and Prime Network and Cisco ANA users can launch Prime Performance Manager reports directly from those applications.

For more information about Prime Performance Manager device discovery, see Chapter 4, "Discovering Network Devices."

Security

Prime Performance Manager security functions include:

- HTTPS web access and SSL-enabled gateway-unit communication options
- Role-based password-protected access for multiple users
- Multiple user authentication methods (PAM-based and standalone)
- Web based and CLI based user management
- Password enforcement policies (aging, minimum length, and lockouts)
- Audit trails of all user actions and all access through the web interface
- Security logs

For more information about Prime Performance Manager security functions, see Chapter 5, "Configuring SSL Between Gateways and Units," and Chapter 6, "Setting Up and Managing Users."

CHAPTER 2

Managing Gateways and Units Using the Command Line Interface

The following topics tell you how to manage Cisco Prime Performance Manager gateways and units using the command line interface.

Logging in as the Root User

To start or stop Prime Performance Manager gateways and units you must be logged in as the root user. To log in as the root user:

```
login: root
Password: root-password
```

If you are already logged in, but not as the root user, use the **su** command to change your login to root:

```
# su
# Password: root-password
```

Caution As the root user, you can harm your operating environment if you are not aware of the effects of the commands that you use. If you are an inexperienced UNIX user, limit your root user activities to the tasks described in this guide.

Starting Prime Performance Manager Gateways and Units

Before you start a Prime Performance Manager gateway or unit, verify that:

- You have IP connectivity to the Prime Performance Manager gateway and unit.
- The unit server has IP connectivity to the devices that you want to monitor.

- SNMP is enabled on each device.
- If you will run Y.1731 and Ethernet Flow Point reports, devices must have Telnet and SSH enabled.

Prime Performance Manager includes a gateway and a unit component. You must start both components. If the gateway and unit are installed on the same machine, the ppm start command will start the gateway and unit automatically.

Note During Prime Performance Manager, the installer allows you to start the gateway and unit after Prime Performance Manager is installed. These procedures only need to be performed if you did not start the gateway and unit after installation, or you stopped the gateway and unit for other reasons.

Complete the following steps to start a Prime Performance Manager gateway and unit if the unit is installed on the same machine as the gateway.

Step 1 Log in as the root user. See Logging in as the Root User, page 2-1.

Step 2 To start the gateway and unit (if installed), enter:

```
/opt/CSCOppm-gw/bin/ppm start
```

The gateway components are started:

```
Starting Prime Performance Manager Gateway App Server...
     -- Prime Performance Manager Gateway Launch         Server  IS  Started.
     -- Prime Performance Manager Gateway Database       Server  IS  Started.
     -- Prime Performance Manager Gateway Naming         Server  IS  Started.
     -- Prime Performance Manager Gateway MessageLog     Server  IS  Started.
     -- Prime Performance Manager Gateway DataServer     Server  IS  Started.
     -- Prime Performance Manager Gateway JSP            Server  IS  Started.
Prime Performance Manager Gateway App Server IS Started.
```

If a unit is installed on the same machine, the unit components are started:

```
Starting Prime Performance Manager Unit App Server...
     -- Prime Performance Manager Unit Launch         Server  IS  Started.
     -- Prime Performance Manager Unit Database       Server  IS  Started.
     -- Prime Performance Manager Unit Naming         Server  IS  Started.
     -- Prime Performance Manager Unit MessageLog     Server  IS  Started.
     -- Prime Performance Manager Unit DataServer     Server  IS  Started.
     -- Prime Performance Manager Unit JSP            Server  IS  Started.
Prime Performance Manager Unit App Server IS Started.
```

The gateway web component is started and web URL is displayed:

```
Starting Prime Performance Manager Gateway Web          Server  On  Port 4440...
     -- Prime Performance Manager Gateway Web            Server  IS  Started.
Connect Web Browser To Gateway:
    http://gatewayhostname:4440
```

If any gateway or unit component is not started, a message similar to the following appears:

```
-- Prime Performance Manager Gateway Launch         Server  NOT  Started.
```

The message can be displayed for any gateway or unit component. If it appears, review the sgmConsoleLog.txt to determine the cause and apply the appropriate fixes. sgmConsoleLog.txt is located in the /opt/CSCOppm-gw/logs/ or /opt/CSCOppm-unit/logs directories.

Complete the following steps to start a Prime Performance Manager unit installed on a machine separate from the gateway:

Step 1 log into the unit server as the root user. See Logging in as the Root User, page 2-1.

Step 2 To start the unit, enter:

```
/opt/CSCOppm-unit/bin/ppm start
```

The unit components are started:

```
Starting Prime Performance Manager Unit App Server...
     -- Prime Performance Manager Unit Launch         Server  IS  Started.
     -- Prime Performance Manager Unit Database       Server  IS  Started.
     -- Prime Performance Manager Unit Naming         Server  IS  Started.
     -- Prime Performance Manager Unit MessageLog     Server  IS  Started.
     -- Prime Performance Manager Unit DataServer     Server  IS  Started.
     -- Prime Performance Manager Unit JSP            Server  IS  Started.
Prime Performance Manager Unit App Server IS Started.
```

Note The ppm start command starts the gateway and automatically starts the unit if it is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-unit/bin/. If the gateway and unit are installed on the same machine and you want to start only the gateway, enter **ppm start gateway**. Similarly, if you want to start only the unit, enter **ppm start unit**.

Stopping Prime Performance Manager Gateways and Units

Complete the following steps to stop a Prime Performance Manager gateway and unit if the unit is installed on the same machine as the gateway:

Step 1 Log in as the root user. See Logging in as the Root User, page 2-1.

Step 2 To stop the gateway, enter:

```
/opt/CSCOppm-gw/bin/ppm stop
```

The gateway components are stopped:

```
Stopping Prime Performance Manager Gateway App     Server...
       -- Prime Performance Manager Gateway App     Server Stopped.
Stopping Prime Performance Manager Gateway Launch  Server...
       -- Prime Performance Manager Gateway Launch  Server Stopped.
Stopping Prime Performance Manager Gateway Web     Server...
       -- Prime Performance Manager Gateway Web     Server Stopped.
```

If a unit is installed on the same server as the gateway, the unit components are stopped:

```
Stopping Prime Performance Manager Unit App     Server...
-- Prime Performance Manager Unit App     Server Stopped.
Stopping Prime Performance Manager Unit Launch  Server...
       -- Prime Performance Manager Unit Launch  Server Stopped.
```

Depending on how quickly the gateway and unit can be shut down, you might see the following messages indicating additional time is needed to shut down the unit components:

```
Waiting for Prime Performance Manager Unit App Server to stop [10 more ]
Waiting for Prime Performance Manager Unit App Server to stop [9 more ]
Waiting for Prime Performance Manager Unit App Server to stop [8 more ]
Waiting for Prime Performance Manager Unit App Server to stop [7 more ]
```

Note The ppm stop command stops the gateway and automatically stops the unit if it is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-gw/bin/. If the gateway and unit are installed on the same machine and you want to stop only the gateway, enter **ppm stop gateway**. Similarly, if you want to stop only the unit, enter **ppm stop unit**.

Complete the following steps to stop a Prime Performance Manager unit installed on a machine separate from the gateway:

Step 1 log into the unit as the root user. See Logging in as the Root User, page 2-1.

Step 2 To stop the unit, enter:

```
/opt/CSCOppm-unit/bin/ppm stop
```

The unit components are stopped:

```
Stopping Prime Performance Manager Unit App     Server...
-- Prime Performance Manager Unit App     Server Stopped.
Stopping Prime Performance Manager Unit Launch  Server...
       -- Prime Performance Manager Unit Launch  Server Stopped.
```

Restarting Gateways and Units

Complete the following steps to start a Prime Performance Manager gateway:

Step 1 Log in as the root user. See Logging in as the Root User, page 2-1.

Step 2 To restart the gateway and unit (if installed), enter:

```
/opt/CSCOppm-gw/bin/ppm restart
```

First, the gateway components are stopped:

```
Stopping Prime Performance Manager Gateway App     Server...
       -- Prime Performance Manager Gateway App     Server Stopped.
Stopping Prime Performance Manager Gateway Launch  Server...
       -- Prime Performance Manager Gateway Launch  Server Stopped.
Stopping Prime Performance Manager Gateway Web     Server...
       -- Prime Performance Manager Gateway Web     Server Stopped.
```

If a unit is installed on the same server as the gateway, the unit components are stopped:

```
Stopping Prime Performance Manager Unit App     Server...
-- Prime Performance Manager Unit App     Server Stopped.
Stopping Prime Performance Manager Unit Launch  Server...
```

```
       -- Prime Performance Manager Unit Launch  Server Stopped.
```

Depending on how quickly the gateway and unit can be shut down, you might see the following messages indicating additional time is needed to shut down the unit components:

```
Waiting for Prime Performance Manager Unit App Server to stop [10 more ]
Waiting for Prime Performance Manager Unit App Server to stop [9 more ]
Waiting for Prime Performance Manager Unit App Server to stop [8 more ]
Waiting for Prime Performance Manager Unit App Server to stop [7 more ]
```

Next, the gateway components are started:

```
Starting Prime Performance Manager Gateway App Server...
     -- Prime Performance Manager Gateway Launch         Server  IS  Started.
     -- Prime Performance Manager Gateway Database       Server  IS  Started.
     -- Prime Performance Manager Gateway Naming         Server  IS  Started.
     -- Prime Performance Manager Gateway MessageLog     Server  IS  Started.
     -- Prime Performance Manager Gateway DataServer     Server  IS  Started.
     -- Prime Performance Manager Gateway JSP            Server  IS  Started.
Prime Performance Manager Gateway App Server IS Started.
```

If a unit is installed on the same machine, the unit components are started:

```
Starting Prime Performance Manager Unit App Server...
     -- Prime Performance Manager Unit Launch         Server  IS  Started.
     -- Prime Performance Manager Unit Database       Server  IS  Started.
     -- Prime Performance Manager Unit Naming         Server  IS  Started.
     -- Prime Performance Manager Unit MessageLog     Server  IS  Started.
     -- Prime Performance Manager Unit DataServer     Server  IS  Started.
     -- Prime Performance Manager Unit JSP            Server  IS  Started.
Prime Performance Manager Unit App Server IS Started.
```

The gateway web component is started and web URL is displayed:

```
Starting Prime Performance Manager Gateway Web          Server  On  Port 4440...
     -- Prime Performance Manager Gateway Web            Server  IS  Started.
Connect Web Browser To Gateway:
    http://gatewayhostname:4440
```

Note The ppm restart command restarts the gateway and automatically restarts the unit if it is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-gw/bin/. If the gateway and unit are installed on the same machine and you want to restart only the gateway, enter **ppm restart gateway**. Similarly, if you want to restart only the unit, enter **ppm restart unit**.

Complete the following steps to restart a Prime Performance Manager unit installed on a machine separate from the gateway:

Step 1 log into the unit server as the root user. See Logging in as the Root User, page 2-1.

Step 2 To restart the unit, enter:

```
/opt/CSCOppm-unit/bin/ppm restart
```

The unit components are stopped:

```
Stopping Prime Performance Manager Unit App     Server...
-- Prime Performance Manager Unit App     Server Stopped.
Stopping Prime Performance Manager Unit Launch  Server...
```

```
       -- Prime Performance Manager Unit Launch  Server Stopped.
```

Then the unit components are started:

```
Starting Prime Performance Manager Unit App Server...
     -- Prime Performance Manager Unit Launch         Server  IS  Started.
     -- Prime Performance Manager Unit Database       Server  IS  Started.
     -- Prime Performance Manager Unit Naming         Server  IS  Started.
     -- Prime Performance Manager Unit MessageLog     Server  IS  Started.
     -- Prime Performance Manager Unit DataServer     Server  IS  Started.
     -- Prime Performance Manager Unit JSP            Server  IS  Started.
Prime Performance Manager Unit App Server IS Started.
```

Viewing Gateway and Unit Status

Use the ppm status command to view the status of a Prime Performance Manager gateways and units. Gateway and unit component status will be either running or not running. Should a component have a not running status, view the sgmConsoleLog.txt to determine the cause. sgmConsoleLog.txt is located in the /opt/CSCOppm-gw/logs/ or /opt/CSCOppm-unit/logs directories.

Complete the following steps to view the gateway and unit status:

Step 1 Log in as the root user or admin user. See Logging in as the Root User, page 2-1.

Step 2 To view the status of the gateway and unit, if the unit is installed on the same machine as the gateway, enter:

`/opt/CSCOppm-gw/bin/ppm status`

The gateway status is displayed, for example:

```
==========================================================================
Prime Performance Manager Gateway Version:      1.1.0.6
Prime Performance Manager Gateway Build   Date: Tue Nov 15 02:03 EST 2011
Prime Performance Manager Gateway Install Date: Sat Nov  5 04:49 EDT 2011
Prime Performance Manager Gateway IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Gateway SSL Support:  Installed [Disabled]
==========================================================================
   sgmMsgLogServer:    1.1.0.6   Tue Nov 15 02:01 EST 2011
   sgmDataServer:      1.1.0.6   Tue Nov 15 02:01 EST 2011
==========================================================================
Prime Performance Manager Gateway Web   Server  IS  Running.
Prime Performance Manager Gateway App   Server  IS  Running.
    -- Prime Performance Manager Gateway Database       Server  IS  Running.
    -- Prime Performance Manager Gateway Naming         Server  IS  Running.
    -- Prime Performance Manager Gateway MessageLog     Server  IS  Running.
    -- Prime Performance Manager Gateway DataServer     Server  IS  Running.
    -- Prime Performance Manager Gateway JSP            Server  IS  Running.
    -- Prime Performance Manager Gateway Launch         Server  IS  Running.
Last Restart:
   Sat Nov  5 04:51:47 EDT 2011

Linux Uptime:
 16:31:23 up 329 days,  9:24,  1 user,  load average: 1.12, 1.30, 1.28

Current Time: 2011/11/06 16:31:23 EST
```

If a unit is installed on the same machine, the unit status is displayed, for example:

```
===========================================================================
Prime Performance Manager Unit Version:      1.1.0.6
Prime Performance Manager Unit Build   Date: Tue Nov 15 02:03 EST 2011
Prime Performance Manager Unit Install Date: Sat Nov  5 04:51 EDT 2011
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
===========================================================================
   sgmMsgLogServer:    1.1.0.6   Tue Nov 15 02:01 EST 2011
   sgmDataServer:      1.1.0.6   Tue Nov 15 02:01 EST 2011
===========================================================================
Prime Performance Manager Unit Web   Server  IS  Running.
Prime Performance Manager Unit App   Server  IS  Running.
    -- Prime Performance Manager Unit Database       Server  IS  Running.
    -- Prime Performance Manager Unit Naming         Server  IS  Running.
    -- Prime Performance Manager Unit MessageLog     Server  IS  Running.
    -- Prime Performance Manager Unit DataServer     Server  IS  Running.
    -- Prime Performance Manager Unit JSP            Server  IS  Running.
    -- Prime Performance Manager Unit Launch         Server  IS  Running.
Last Restart:
   Sat Nov  5 05:04:55 EDT 2011
Linux Uptime:
 16:31:30 up 329 days,  9:24,  1 user,  load average: 1.17, 1.30, 1.28

Current Time: 2011/11/06 16:31:30 EST
```

Complete the following steps to view the status of a unit installed on a machine separate from the gateway:

Step 1 log into the unit server as the root or admin user. See Logging in as the Root User, page 2-1.

Step 2 To view the status of the unit, enter:

`/opt/CSCOppm-unit/bin/ppm status`

The unit status is displayed, for example:

```
===========================================================================
Prime Performance Manager Unit Version:      1.1.0.6
Prime Performance Manager Unit Build   Date: Tue Nov 15 02:03 EST 2011
Prime Performance Manager Unit Install Date: Sat Nov  5 04:51 EDT 2011
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
===========================================================================
   sgmMsgLogServer:    1.1.0.6   Tue Nov 15 02:01 EST 2011
   sgmDataServer:      1.1.0.6   Tue Nov 15 02:01 EST 2011
===========================================================================
Prime Performance Manager Unit Web   Server  IS  Running.
Prime Performance Manager Unit App   Server  IS  Running.
    -- Prime Performance Manager Unit Database       Server  IS  Running.
    -- Prime Performance Manager Unit Naming         Server  IS  Running.
    -- Prime Performance Manager Unit MessageLog     Server  IS  Running.
    -- Prime Performance Manager Unit DataServer     Server  IS  Running.
    -- Prime Performance Manager Unit JSP            Server  IS  Running.
    -- Prime Performance Manager Unit Launch         Server  IS  Running.
Last Restart:
   Sat Nov  5 05:04:55 EDT 2011
Linux Uptime:
 16:31:30 up 329 days,  9:24,  1 user,  load average: 1.17, 1.30, 1.28

Current Time: 2011/11/06 16:31:30 EST
```

Note The ppm status command provides the gateway and unit status if the unit is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-gw/bin/. If the gateway and unit are installed on the same machine and you want to view only the gateway status, enter **ppm status gateway**. Similarly, if you want to view only the unit status, enter **ppm status unit**.

Viewing the Gateway and Unit Prime Performance Manager Version

Complete the following steps to view the gateway and unit Prime Performance Manager version:

Step 1 Log in as the root user or admin user. See Logging in as the Root User, page 2-1.

Step 2 To view the Prime Performance Manager version installed on the gateway and unit, if the unit is installed on the same machine as the gateway, enter:

```
/opt/CSCOppm-gw/bin/ppm version
```

The gateway version details are displayed, for example:

```
===========================================================================
Prime Performance Manager Gateway Version:      1.1.0.6
Prime Performance Manager Gateway Build   Date: Tue Nov 15 02:03 EST 2011
Prime Performance Manager Gateway Install Date: Sat Nov  5 04:49 EDT 2011
Prime Performance Manager Gateway IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Gateway SSL Support:  Installed [Disabled]
===========================================================================

   sgmMsgLogServer:    1.1.0.6   Tue Nov 15 02:01 EST 2011
   sgmDataServer:      1.1.0.6   Tue Nov 15 02:01 EST 2011

Current time is: 2011/11/06 17:42:57 EST
```

If the unit is installed on the same machine, the unit version details are displayed, for example:

```
===========================================================================
Prime Performance Manager Unit Version:      1.1.0.6
Prime Performance Manager Unit Build   Date: Tue Nov 15 02:03 EST 2011
Prime Performance Manager Unit Install Date: Sat Nov  5 04:51 EDT 2011
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
===========================================================================

   sgmMsgLogServer:    1.1.0.6   Tue Nov 15 02:01 EST 2011
   sgmDataServer:      1.1.0.6   Tue Nov 15 02:01 EST 2011

Current time is: 2011/11/06 17:42:58 EST
```

To view the Prime Performance Manager version on a unit installed on a machine separate from the gateway:

Step 1 log into the unit server as the root or admin user. See Logging in as the Root User, page 2-1.

Step 2 To view the Prime Performance Manager version installed on the unit, enter:

```
/opt/CSCOppm-unit/bin/ppm version
```

The unit Prime Performance Manager version is displayed, for example:

```
===========================================================================
Prime Performance Manager Unit Version:      1.1.0
Prime Performance Manager Unit Build   Date: Tue Nov 15 02:03 EST 2011
Prime Performance Manager Unit Install Date: Sat Nov  5 04:51 EDT 2011
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
===========================================================================

   sgmMsgLogServer:    1.1.0 Tue Nov 15 02:01 EST 2011
   sgmDataServer:      1.1.0 Tue Nov 15 02:01 EST 2011

Current time is: 2011/11/06 17:42:58 EST
```

Note The ppm version command provides the Prime Performance Manager gateway and unit version if the unit is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-gw/bin/. If the gateway and unit are installed on the same machine and you want to view only the Prime Performance Manager version installed on the gateway, enter **ppm version gateway**. Similarly, if you want to view only the Prime Performance Manager version installed on the unit status, enter **ppm version unit**.

Limiting Client Access to Servers

Following Prime Performance Manager installation, all client IP addresses can connect to the gateway. You can limit client access to the server by creating the ipaccess.conf file and entering the client IP addresses that want to give access to the gateway. Prime Performance Manager allows connections from only those clients and the local host.

If the file exists but is empty, Prime Performance Manager allows connections only from the local host. (Prime Performance Manager always allows connections from the local host.)

Complete the following steps to create the ipaccess.conf file and add the client IP addresses that you want to allow access to the gateway:

Step 1 Log into Prime Performance Manager server as the root user.

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Create the ipaccess.conf file:

- To create the ipaccess.conf file and add a client IP address to the list, enter:

  ```
  ./ppm ipaccess add
  ```

- To create the ipaccess.conf file and open the file to edit it directly, enter:

  ```
  ./ppm ipaccess edit
  ```

By default, the ipaccess.conf file is located in Prime Performance Manager /opt/CSCOppm-gw/etc installation directory. If you installed Prime Performance Manager in a different directory, then the default directory is located in that directory.

Step 4 Add the ipaccess.conf entries:

- Begin comment lines with a pound sign (#).
- Lines without a pound sign are Prime Performance Manager client IP addresses. Enter one address per line.
- Wildcards (*) are allowed, as are ranges (for example, 1-100). For example, if you enter the address *.*.*.*, all clients can connect to Prime Performance Manager server.

Step 5 After you create the ipaccess.conf file, you can use the full set of Prime Performance Manager ipaccess keywords to work with the file. The keywords are:

- clear—Remove all client IP addresses from the ipaccess.conf file and allow connections from any Prime Performance Manager client IP address.
- list—List all client IP addresses currently in the ipaccess.conf file. If no client IP addresses are listed (that is, the list is empty), connections from any Prime Performance Manager client IP address are allowed.
- rem—Remove the specified client IP address from the ipaccess.conf file.
- sample—Print out a sample ipaccess.conf file.

For more information, see ppm ipaccess, page B-26.

Step 6 After ipaccess.conf entries are complete, you must restart the gateway for the changes to take effect. See Restarting Gateways and Units, page 2-4.

CHAPTER 3

Using the Prime Performance Manager Web Interface

The following topics provide information about using the Cisco Prime Performance Manager web interface:

- Accessing the Prime Performance Manager Web Interface, page 3-1
- Navigating Table Columns, page 3-8
- Changing the Web Preferences, page 3-9
- Changing the GUI Polling Refresh Setting, page 3-10

Accessing the Prime Performance Manager Web Interface

The Cisco Prime Performance Manager web interface requires one of the following web browsers with JavaScript enabled:

- Microsoft Windows: Microsoft Internet Explorer version 8.0 or Mozilla Firefox 3.6.x
- Solaris: Mozilla Firefox 3.6.x
- Red Hat Linux Enterprise 5.3 or 5.5: Mozilla Firefox 3.6.x

Note If you open Cisco Prime Performance Manager in an unsupported browser, a warning is displayed. If the browser does not have JavaScript enabled, the Prime Performance Manager web interface cannot function.

To access the Cisco Prime Performance Manager web interface:

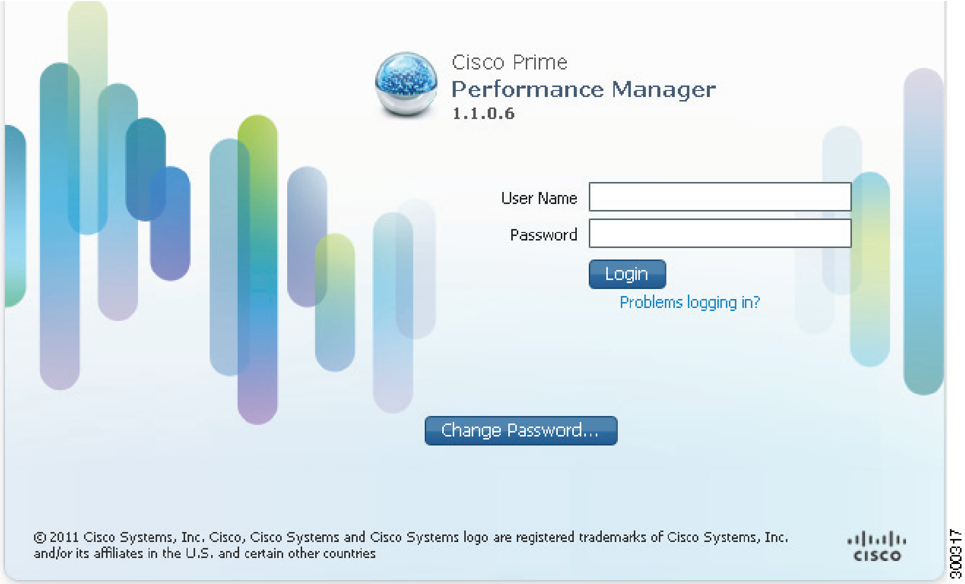
Step 1 Enter the following in the browser URL field:

```
http://ppm11-server:4440
```

Where *ppm11-server* is the name of the server where Prime Performance Manager is installed and Port 4440 is the default port.

Step 2 If user access is enabled (see Setting User Access, page 6-1), the Prime Performance Manager login screen appears (Figure 3-1). If so, enter your username and password.

Figure 3-1 Prime Performance Manager Login Window



Cisco Prime
Performance Manager
1.1.0.6

User Name
Password

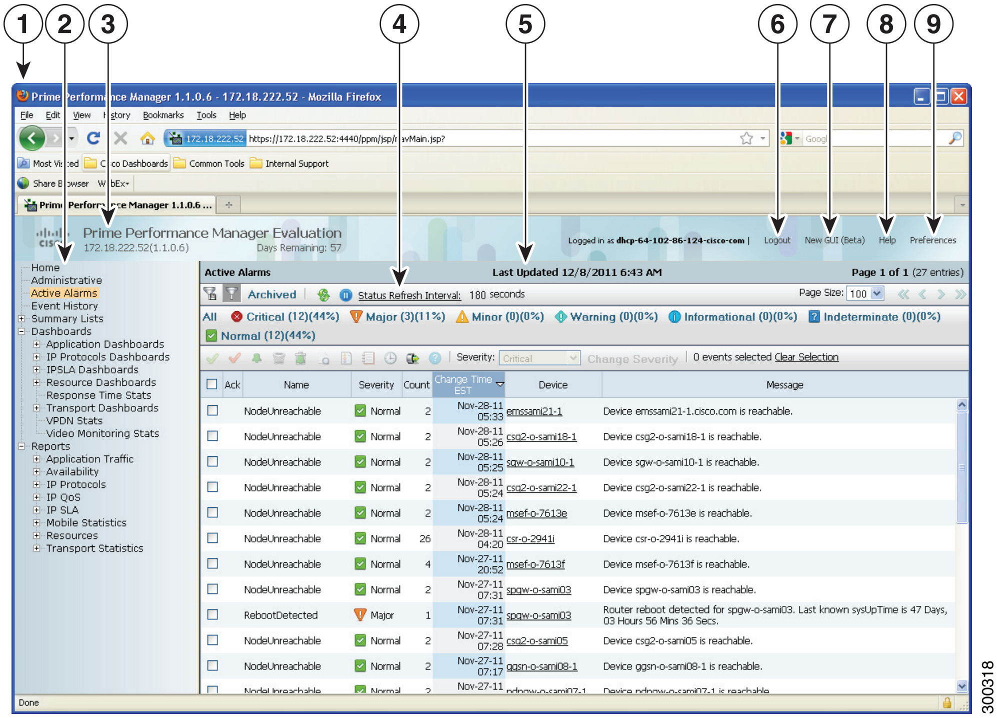
© 2011 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries

After you log in, the Cisco Prime Performance Manager GUI application launches. By default, the Active Alarms window is displayed (Figure 3-2). (For a description of the Active Alarms window and functions, see Chapter 9, "Using Alarms and Events.")

The GUI window is comprised of the following elements:

- Title bar—Shows the following information and links:
  - Prime Performance Manager version, and server name.
  - Logout (appears only if you enable user access).
  - Help—Displays Cisco Prime Performance Manager context-sensitive online help.
  - New GUI (Beta)—Displays a new GUI design currently in beta. You can try the new GUI and provide feedback to your Cisco account representative. However any errors or problems encountered with the beta GUI are not supported.
  - Preferences—Displays the options allowing you to change the Cisco Prime Performance Manager web interface display. See Changing the Web Preferences, page 3-9.
  - Status Messages—Messages include device discovery and deletion messages.
- Navigation tree—Displays all Cisco Prime Performance Manager content and functions. (See Using the Web Interface Navigation Tree, page 3-4.)
- Content pane—Displays contents for the item selected in the navigation tree.

Figure 3-2 Prime Performance Manager GUI



□	Ack	Name	Severity	Count	Change Time EST	Device	Message
□		NodeUnreachable	✓ Normal	2	Nov-28-11 05:33	emssami21-1	Device emssami21-1.cisco.com is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-28-11 05:26	csg2-o-sami18-1	Device csg2-o-sami18-1 is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-28-11 05:25	sgw-o-sami10-1	Device sgw-o-sami10-1 is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-28-11 05:24	csg2-o-sami22-1	Device csg2-o-sami22-1 is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-28-11 05:24	msef-o-7613e	Device msef-o-7613e is reachable.
□		NodeUnreachable	✓ Normal	26	Nov-28-11 04:20	csr-o-2941i	Device csr-o-2941i is reachable.
□		NodeUnreachable	✓ Normal	4	Nov-27-11 20:52	msef-o-7613f	Device msef-o-7613f is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-27-11 07:31	spgw-o-sami03	Device spgw-o-sami03 is reachable.
□		RebootDetected	Major	1	Nov-27-11 07:31	spgw-o-sami03	Router reboot detected for spgw-o-sami03. Last known sysUpTime is 47 Days, 03 Hours 56 Mins 36 Secs.
□		NodeUnreachable	✓ Normal	2	Nov-27-11 07:28	csg2-o-sami05	Device csg2-o-sami05 is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-27-11 07:17	ggsn-o-sami08-1	Device ggsn-o-sami08-1 is reachable.
□		NodeUnreachable	✓ Normal	2	Nov-27-11	pdnqw-o-sami07-1	Device pdnqw-o-sami07-1 is reachable.

1	Title bar	**6**	Logout
2	Navigation tree	**7**	Beta GUI
3	Prime Performance Manager version, and server name	**8**	Online help
4	Content area	**9**	Preferences
5	Last content update date and time		

Checking Your Browser Settings

After you display the Prime Performance Manager web interface, you can check your browser and screen settings:

Step 1 In the navigation area, click **Home**.

Step 2 Under Client Software, click **Browser Checker**.

Step 3 Review the browser information:

- Browser—The name and version of the browser you are using.
- Browser User Agent—A text string that identifies the user agent to the server. This generally includes the application name, version, host operating system, and language.
- Platform—The platform type, for example, Win32.
- Cookies Enabled—Indicates whether cookies are enabled on the browser (Yes or No).

- JavaScript Enabled—Indicates whether JavaScript is enabled (Yes or No). For Prime Performance Manager, JavaScript must be enabled.
- AJAX Component—Asynchronous JavaScript and XML (AJAX) sends asynchronous HTTP update requests. The Prime Performance Manager web application is only accessible to web browsers that have an AJAX component enabled. Typical values include XMLHttpRequest.
- Size—Indicates the resolution of the display, for example, 1600 x 1200.
- Color Depth—Indicates the depth of the color display, for example, 16.

Using the Web Interface Navigation Tree

Prime Performance Manager options appear in the navigation tree in the left pane of the GUI window (See Figure 3-2). Clicking a tree item displays the contents selected item in the content area. A plus (+) or minus (-) to the left of the item indicates whether the item has additional items under it.

Prime Performance Manager automatically updates the navigation tree when changes occur to discovered devices or the network. When any changes occur in the navigation tree, the changes are reflected in the web interface. For example, if you delete a report from the Report Status tab, the report is removed from the navigation tree.

Table 3-1 lists the navigation tree items with references to topics that describe the item in more detail.

Table 3-1 Cisco Prime Performance Manager Navigation Tree

Tree Item	Description
Home	Provides links to Prime Performance Manager user and reports documentation, commands, and other information. (See Chapter 11, "Reviewing Prime Performance Manager Home Page Information.").
Administrative	Provides the following tabs: General—Shows Prime Performance Manager system information including messages, logs, status, and properties. SNMP—Displays the SNMP Editor to edit and save SNMP settings. See Adding SNMP Credentials, page 4-4.) Polling Groups—Allows you to create device polling groups. See Chapter 14, "Creating and Editing Device Polling Groups." Telnet/SSH—Allows you to add and edit Telnet and SSH credentials for Y.1731 and Ethernet Flow Point reports. See Chapter 16, "Configuring Device Credentials for Y.1371 SLA and Ethernet Flow Point Reports." Unit Editor— Enables you to assign devices to units. See Chapter 13, "Managing Prime Performance Manager Units.") Discovery—Allows you to discover network devices using Prime Performance Manager. See Chapter 4, "Discovering Network Devices." Prime Network—Allows you to import a Prime Network device inventory. See Importing Prime Network Device Inventories, page 4-2. User Management—Displays all users in the system along with the time of their most recent login, their access level, and their account status. See Chapter 6, "Setting Up and Managing Users." Event Editor— Allows you configure event properties and also define the upstream OSS hosts. See Chapter 15, "Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters." Threshold Editor—Allows you to create and edit report thresholds. See Chapter 10, "Configuring Thresholds." If Prime Performance Manager user access is enabled, only users with Administrator (Level 5) access can see all options on the Administrative window.
Active Alarms	Displays information about Prime Performance Manager alarms. See Chapter 9, "Using Alarms and Events."
Event History	Displays information about Prime Performance Manager events. See Chapter 9, "Using Alarms and Events."
Summary Lists	Displays basic summary information about all discovered network objects. See Chapter 8, "Using Summary Lists."
Dashboards	Displays and allows you to manage Prime Performance Manager dashboards. See Chapter 7, "Working With Reports and Dashboards."
Reports	Displays and allows you to manage Prime Performance Manager reports. See Chapter 7, "Working With Reports and Dashboards."

Customizing Date and Time Ranges

Some windows require that you select date ranges for generating historical graphs. To customize the date and time range:

Step 1 Click the **Customize the date and time range** tool in the toolbar of the content area.

Step 2 In the Customize Date and Time Range dialog box, enter:

- The begin and end dates or click the Calendar tool. These dates are the dates in the gateway server time zone.
- The begin and end hour and minutes.

Note An error message appears if the end date is equal to or less than the begin date. Correct the error before proceeding.

Step 3 Click **OK**.

The Prime Performance Manager web interface accepts and applies the changes by generating a report for the chosen server time (in case of reports).

Using the Toolbar

The Prime Performance Manager web interface navigation tree toolbar displays tools and options shown in Table 3-2. However, the tools and options that appear depend upon the object you select in the navigation tree.

Table 3-2 Cisco Prime Performance Manager Web Interface Toolbar

Item	Icon	Description
Last Updated	—	The date and time Cisco Prime Performance Manager last updated the displayed information.
Page	—	Shows your location (page X of X total pages) and lists the total number of entries.
Refresh	⟳	Refreshes of the current web page.
Pause	⏸	Pauses the page refresh. Click **Pause** to disable the Page Refresh that would normally occur after the Status Refresh Interval. Click **Pause** again to re-enable the Status Refresh Interval.
Status Refresh Interval	—	Allows you change the default refresh interval. Enter a value between 180 (default) and 900 seconds. Changes only apply to the current page. Navigating away it sets the status refresh interval back to the default.
Page Size	—	Drop-down list of page sizes (the number of table rows in the display). Click the drop-down arrow to select a different value. The value that you select becomes the default page size for all pages in the web interface. The title bar displays the current page and total number of table entries.

*Table 3-2 Cisco Prime Performance Manager Web Interface Toolb*ar *(continued)*

Item	Icon	Description
Quick Search	—	Text box to filter the objects listed under the Summary List tables (Except for IP Addresses and Point Code tables). Enter the string in the text box to filter the table by and then press **Enter**. The rows under the table are filtered based on the string entered. Summary table columns used for filtered string searches include: • Devices: Internal ID, Unit, Display Name, Primary SNMP Address, Device Type, Uptime, Software Version, Ignored, Report Polling, Severity, Status and Status Reason. • Device Distributions: Type, Total, and Percentage. • Average Poll Response: Display Name, Primary SNMP Address, Device Type, Report Polling, and Average Poll Response (secs). • Uptime: Display Name, Device Type, Uptime, Reboot Reason, and Severity. • SNMP Timeout Alarms: Display Name, Primary SNMP Address, Device Type, Software Version, Uptime, Ignored, Report Polling and Severity. • Software Versions: Display Name, Device Type, Software Version and Software Description. • Gateway/Units: Display Name, Custom Name, Primary SNMP Address, Type, Connection Time, In Service, Status, and Status Reason.
Clear Filter		Clears the search filter.
>	—	Advances the display to the next page of information.
>>	—	Advances the display to the last page of information.
<	—	Moves the display to the previous page of information.
<<	—	Moves the display to the first page of information.
Critical	⊗	The number and percentage of critical alarms on the device.
Major	!	The number and percentage of major alarms on the device.
Minor	⚠	The number and percentage of minor alarms on the device.
Warning	◆	The number and percentage of warning alarms on the device.
Informational	ⓘ	The number and percentage of informational alarms on the device.
Indeterminate	?	The number and percentage of indeterminate alarms on the device.
Normal	✓	The number and percentage of normal alarms on the device.
Customize date and time range	📅	Opens the Choose a Date Range Server timezone dialog box.

Table 3-2 Cisco Prime Performance Manager Web Interface Toolbar (continued)

Item	Icon	Description
Graph Series Editor	⚙	Opens the Graph Series Editor dialog box, which provides a check box for each available data series. Check the box to display a series; uncheck it to hide a series. Clicking **OK** without selecting a series cancels the action. Prime Performance Manager displays no more than 10 series, by default.
Run	➡	Runs the report type for the chosen duration.
Export report as a CSV file	➡	Exports the data in the table to comma-separated value file (CSV file). You can save this file to disk or open it with an application that you choose (for example, Microsoft Excel).
Data Range (*timezone*)	—	Label that shows the chosen time range for the historical statistics. The label displays the data range with server time.
Type	—	Drop-down list of report types.
Duration	—	Drop-down list of default time ranges. Select one of these options, then click the **Run** tool. To specify a nondefault time range, click the **Customize Date and Time Range** tool. See Customizing Date and Time Ranges, page 3-6.
Output	—	Drop-down menu that provides these options: • Graph—Displays statistical data in graphs and tables. • Table—Presents statistical data in tabular format only. • CSV—Exports statistical data using comma-separated values.
Sort Parameter	—	Used in the graph output of certain reports to select the criteria ti include a top set of series. Also for ordering the corresponding graphs displayed.
Actions	—	The Actions menu appears for all summary lists except Device Distributions and Software Versions. Action menu items appear when you hover over the Actions link. For more information, see Editing Summary List Items, page 8-9.
Help for Reports	?	Auto-generated reports help; shows the MIB variables that are polled for generating the selected report with the calculations (if any) performed on them.

Navigating Table Columns

You can sort, show, or hide the columns in some tables in Prime Performance Manager to meet your specific needs. The web interface automatically saves your new settings and, thereafter, launches the interface with the new settings.

You can hide table columns in the Prime Performance Manager web interfaces. In the web interface, you can search for specific information and page through long tables by using its Search and Paging features.

- To view a tooltip for each column in the table, place the cursor over a column heading. If a cell is too small to show all of its text, place the cursor over the cell to see the full text of the tooltip.
- By default, Prime Performance Manager displays most of the columns in tables, but some columns may be hidden. To:
  - To display hidden columns, right-click the table heading and select the check boxes for the columns you want to display, then click **Apply** button.
  - To hide columns, right-click the table heading and clear the check boxes for the columns you want to hide, then click the **Apply** button.

- To sort a table based on the data in a column, left-click the column heading. Prime Performance Manager alpha-numerically sorts the table from top to bottom based on the data in the chosen column. To sort the table in reverse order, left-click in the column heading again.
- Icons in the column heading indicate the column on which the table is sorted and the sort direction:
  - Triangle icon—Ascending sort order (1-9, A-Z).
  - Inverted triangle—Descending (Z-A, 9-1).
- Report columns display a plus icon to indicate report key performance indicators for which thresholds can be created. For information about creating thresholds, see Chapter 10, “Configuring Thresholds.”

If you sort a table based on the Devices column, Prime Performance Manager sorts the table based on the discovered device DNS names. If you modified your web preferences to identify devices by their user-defined names, Prime Performance Manager sorts the table, based on the device user-defined names. For more information, see Changing the Web Preferences, page 3-9.

Changing the Web Preferences

You can change the device information that appears in Prime Performance Manager GUI, change report auto expand settings, optimize the GUI for slow connections and change the GUI page refresh rate. These settings are located in the Web Preferences window. To change the web preferences settings:

Step 1 In the Prime Performance Manager web interface title bar, click **Preferences**.

Step 2 In the Web Preferences window, modify the following preferences, as needed:

- Device Name Settings—Indicates how devices are identified in the Prime Performance Manager GUI. Choose one of the following:
  - Show DNS or User-Defined Names (default)—Identifies devices by their DNS or user-defined names.
  - Show IP Address in Name Field—Identifies devices by their IP addresses.
  - Show SysName—Identifies devices by their system name.
- General Display Settings—Check any of the following display options:
  - Show Device Domain Names—Displays the device domain names.
  - Auto Expand Reports in a Tree—Automatically expands the reports in the navigation tree.
  - Auto Expand Report Summary Tables—Automatically expands the report graph summary tables. Reports with Dashboard in their titles, for example in the AAA Authentication Dashboard Hourly report, collapse the summary tables by default. This preference expands the summary tables automatically.
  - Optimize GUI for Slow Connections—If you are using a low-speed connection, for example, a dial-up modem or long-distance VPN connection, check this box to turn off the row index count that is displayed in the upper right corner of a report title area. If enabled, this option displays the row number as you mouse over a table, and also displays the number of table pages and table entries. The option does not perform well in low-speed connections.

- Poller Settings—the Status Refresh Interval options specifies how frequently Prime Performance Manager refreshes the web pages. The range is 180 to 900 seconds. The default is 180 seconds. The valid range and default settings can be changed in the Server.properties file to change the settings for all users. See Changing the GUI Polling Refresh Setting, page 3-10 for information.

Changing the GUI Polling Refresh Setting

You can change the frequency Prime Performance Manager GUI page refresh setting on a system-wide level. You can change the minimum, maximum, and default refresh settings. To change the system-wide refresh settings:

Step 1 Log into the gateway as the root user.

Step 2 Navigate to the /opt/CSCOppm-gw/properties directory.

Step 3 Open the Server.properties file with a text editor and modify the following lines:

```
# Status refresh default interval in seconds
STATE_REFRESH_DEFAULT = 180

# Status refresh minimum interval in seconds
STATE_REFRESH_MIN = 180

# Status refresh maximum interval in seconds
STATE_REFRESH_MAX = 900
```

Where:

- STATE_REFRESH_DEFAULT is the default refresh setting.
- STATE_REFRESH_MIN—Is the minimum amount of time that must pass before a refresh occurs.
- STATE_REFRESH_MAX—Is the maximum amount of time allowed before a refresh must occur.

For example, to change the status refresh poller default to 300 seconds, change the STATE_REFRESH_DEFAULT line to:

```
STATE_REFRESH_DEFAULT = 300
```

The acceptable refresh range is 180 to 900 seconds.

Step 4 Save your changes and restart Prime Performance Manager gateway. See Restarting Gateways and Units, page 2-4.

CHAPTER 4

Discovering Network Devices

The following topics tell you how to add the network devices that you want to monitor to Cisco Prime Performance Manager:

- Device Discovery Requirements, page 4-1
- Importing Prime Network Device Inventories, page 4-2
- Managing Network Discovery, page 4-5

Device Discovery Requirements

Before you begin device discovery, review the devices that Prime Performance Manager officially supports. These can be found at:

http://www.cisco.com/en/US/products/ps11715/products_device_support_tables_list.html

In addition, the Devices Readme, available from the Prime Performance Manager GUI Home page, lists the known devices and software versions that have been used by customers and Cisco labs during testing and deployments. While these devices are not formally supported, informal experience indicates they can be used successfully with Prime Performance Manager.

To produce network reports, Prime Performance Manager accesses the devices, determines their capabilities, and begins the reporting process. Before this can occur, devices must be discovered and assigned to units. The units connect to the devices using the required SNMP or Telnet and SSH credentials.

Device discovery is accomplished using one or both of the following methods:

- Import the device inventory from Cisco Prime Network or Cisco Active Network Abstraction (ANA).
- Run device discovery from Prime Performance Manager. This can be done from the Administration > Discovery tab in the GUI, or by running the ppm discovery command on the CLI.

To discover a device, the following information is required:

- The device IP address or hostname.
- The SNMP credentials authorizing Prime Performance Manager to access the device SNMP engine. SNMP V2 requires a community string. SNMP V3 requires a combination of username, authorization algorithm, authorization pass phrase, privacy algorithm, and privacy pass phrase, depending on the device configuration.
- If ITU-T Y.1731 reports are enabled, Telnet or SSH credentials are required. The number of credentials and their content depend on the device configuration.

If you import the device inventory from Cisco Prime Network, Prime Performance Manager gets the device IP addresses and SNMP, Telnet, and SSH credentials from the Prime Network. If you run device discovery from Prime Performance Manager, you must add the SNMP, Telnet, or SSH credentials to Prime Performance Manager before you run the device discovery.

Importing Prime Network Device Inventories

To import a Prime Network or Cisco ANA device inventory, Prime Performance Manager connects to the Prime Network gateway and retrieves the Prime Network device IP addresses and SNMP, Telnet, or SSH credentials. All devices are retrieved except those whose VNEs are in Maintenance investigation state, or the VNE is ICMP or a cloud VNE. Prime Performance Manager then connects to the devices and probes them for supported MIBs. The MIBs are used to generate reports.

After the device connections are established and MIB profiles created, Prime Performance Manager maintains communication with the Prime Network gateway. If new Prime Network devices are added, Prime Performance Manager devices are updated with the new devices. If a Prime Network device VNE goes into Maintenance state, Prime Performance Manager changes the device to unmanaged stops polling. When the VNE state changes, Prime Performance Manager changes the device state and begins polling.

When you import Prime Network devices, you have the option to enable strict synchronization. Enabling strict synchronization restricts Prime Performance Manager to Prime Network devices; you cannot discover or manage devices that reside outside of Prime Network. Additionally, you cannot edit SNMP, Telnet, or SSH entries and you cannot edit device names. If strict synchronization is not enabled, all device discovery and SNMP, Telnet, or SSH device editing capabilities remain enabled. Strict synchronization is useful when you want a tight relationship between Prime Performance Manager and Prime Network to ensure all reports are Prime Network device reports.

To import Prime Network devices, you need the following Prime Network gateway information:

- IP address or hostname
- Port.
- Prime Network administrator or configurator username and password. The user must have a device scope set for all network elements.

Complete the following steps to import the device inventory from Cisco Prime Network or Cisco ANA using the Prime Performance Manager GUI. This procedure requires a Level 5 (administrator) user level.

Note You can use the ppm inventoryimport command to import Prime Network device information from Prime Network using the CLI. For information, see ppm inventoryimport, page B-25.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window click the **Prime Network** tab.

Step 4 In the Prime Network window, enter the following information:

- Host Name or IP Address—Enter the Prime Network gateway hostname or IP address.
- Port—Enter the Prime Network gateway port. The default Cisco Prime Network web services port is 9003. The Port field accepts values from 1 to 65535.
- User Name—Enter the Prime Network gateway administrator or configurator username.

- Password—Enter the Prime Network user password.
- Strict Sync—Check this box if you want Prime Performance Manager to monitor only Prime Network devices. If you check Strict Sync, Prime Performance Manager cannot connect to devices that haven't been added to Prime Network first, and certain functionality is disabled, including the Discovery tab and the ability to edit SNMP, Telnet, and SSH entries.

Step 5 From the Prime Network toolbar, click the **Import Inventory** tool.

The Prime Network device inventory import proceeds.

Step 6 After it completes, go to the Prime Performance Manager navigation tree and click the **Devices** summary list to review the devices that were added. For information about using the Devices summary lists, see **Using the Devices Summary List, page 8-1**.

Enabling Prime Performance Manager Cross-Launches from Prime Network

In addition to Prime Network device inventory imports, you can enable cross launching so that Prime Network users can launch Prime Performance Manager from Prime Network Vision objects.

Complete the following steps to enable Prime Performance Manager cross-launches from Prime Network:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window click the **Prime Network** tab.

Step 4 From the Prime Network toolbar, click the **Install Cross Launch** tool.

Running Device Discovery from Prime Performance Manager

You can discover network devices by running discovery from Prime Performance Manager. Use this discovery approach when:

- You are not running Prime Network or do not wish to enable reports on Prime Network devices.
- You imported Prime Network devices but did not enable strict synchronization. In this case, you can run device discovery from Prime Performance Manager to add devices not in the Prime Network inventory.

Before you run device discovery from Prime Performance Manager, you must add the SNMP credentials. See Adding SNMP Credentials, page 4-4. If you are enabling ITU-T Y.1731 reports, you must set up the Telnet and SSH credentials. See Adding Telnet and SSH Credentials, page 16-1.

Adding SNMP Credentials

Complete the following steps to add the SNMP credentials required for communication with discovered network devices.

Note You can use the ppm addsnmpcomm command to add SNMP community strings using the CLI. For information, see ppm addsnmpcomm, page B-5.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window, click the **SNMP** tab.

Step 4 From the SNMP Editor toolbar, click the **Add a New SNMP Entry** tool.

Step 5 In the Add SNMP Entry dialog box, enter the following information:

- IP Address Range or Hostname—Enter the device IP address or DNS name, or range of devices. An asterisk (*) indicates a wildcard value.
- Read Community—Enter the SNMP community name used by the device for read access to the information maintained by the SNMP agent on the device.
- Username (v3)—Enter the username (SNMP v3).
- Authorization Algorithm (v3)—Enter the authorization algorithm (SNMP v3):
  - md5—Uses the Hash-based Message Authentication Code (HMAC) MD5 algorithm for authentication
  - sha—Uses the HMAC SHA algorithm for authentication
- Authorization Passphrase (v3)—Enter the authorization passphrase (SNMP v3),
- Privacy Algorithm (v3)—Enter the privacy algorithm (SNMP v3):
  - 3des—Uses Data Encryption Standard (DES) v3.
  - des—Uses the Data Encryption Standard (DES).
  - aes128—Uses Advanced Encryption Standard (AES) 128-bit encryption.
- Privacy Passphrase (v3)—Enter the privacy algorithm (SNMP v3).

Step 6 Click **OK**.

Step 7 On the SNMP Editor toolbar, click **Save All SNMP Entries**.

Editing SNMP Credentials

Complete the following steps to edit the SNMP credentials required for communication with discovered network devices.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window, click the **SNMP** tab.

Step 4 In the SNMP table, edit any of the following SNMP parameters. See Adding SNMP Credentials, page 4-4, for parameter descriptions.

- IP Address Range or Hostname
- Read Community
- Username (v3)
- Authorization Algorithm (v3):
  - md5
  - sha
- Authorization Passphrase (v3)
- Privacy Algorithm (v3):
  - 3des
  - des
  - aes128
- Privacy Passphrase (v3)

Step 5 When finished, on the SNMP Editor toolbar, click **Save All SNMP Entries**.

Deleting SNMP Credentials

Complete the following steps to delete the SNMP credentials from Prime Performance Manager.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window, click the **SNMP** tab.

Step 4 Select the SNMP credential table row that you want to remove, then under the Action column, click Delete this Entry.

Step 5 When finished, on the SNMP Editor toolbar, click **Save All SNMP Entries**.

Managing Network Discovery

The Prime Performance Manager web interface Discovery tab allows you to discover the network. To view the Discovery tab information, click **Administrative** in the navigation tree and then click **Discovery** in the right pane. Table 4-1 lists the Discovery window options.

Table 4-1 Discovery Network Window Options

Option	Tool	Description
Load Seeds	📁	Opens Load File Dialog Window window, enabling you to load a seed file into Prime Performance Manager.
Save Seeds	💾	Saves the changes you have made to the chosen seed file.
Save As	📝	Opens the Save File Dialog Box, using which you can save the updated seed file with a new name, or overwrite an existing seed file.
Discover Network	—	Begins network discovery. If you have not defined at least one seed device in the Seed Settings tab, Prime Performance Manager prompts you to do so. When Discovery begins: • The **Discover Network** button changes to **Stop Discovery**. • The `Discovery In Progress` message appears in the title bar of all Prime Performance Manager client windows. Discovery progresses in bursts. You might see a number of updates, followed by a pause, followed by more updates. The information that Prime Performance Manager windows displays, is not fully updated until Discovery is complete. By default, Discovery times out after 600 seconds (10 minutes). To change the Discovery timeout, change the value of the DISCOVERY_TIMELIMIT entry in the Server.properties file: • If you installed Prime Performance Manager in the default directory, /opt, then the location of the Server.properties file is /opt/CSCOppm-gw/properties/Server.properties. • If you installed Prime Performance Manager in a different directory, then the Server.properties file resides in that directory. Because Prime Performance Manager is asynchronous, with the Prime Performance Manager server contacting clients one at a time, and because clients might run at different speeds, the information that Prime Performance Manager clients display during Discovery might not always be synchronized. All other Prime Performance Manager windows (Device) are also populated with the newly discovered network data.

Load File Dialog Window

Table 4-2 lists the options and information provided in the Load File window.

Table 4-2 Load File Dialog Box

Field or Button	Description
Seed File List	Seed File List pane information and options include: • Go up one Folder—Click this icon to go up one folder in the directory structure. • Type—Icon indicating whether the item in the table is a file or a folder. • Name—Name of the seed file or folder. • Last Modified—Date and time the seed file or folder was last modified. • Size (bytes)—Size of the seed file or folder, in bytes.

Table 4-2 Load File Dialog Box (continued)

Field or Button	Description
Make this my preferred startup	Specifies whether the chosen seed file should be loaded automatically whenever this Prime Performance Manager client is started or the Discovery dialog box is opened. By default, this option is not selected for all seed files. That is, no seed file is loaded automatically when Prime Performance Manager client is started or the Discovery dialog box is opened.
OK	Loads the chosen seed file, saves any changes you made to the list of files, and closes the dialog box. To load a seed file: • Double-click it in the list, select it in the list and click **OK**, Or • Enter the name of the file and click **OK**. Prime Performance Manager saves any changes you made to the list of files, closes the Load File Dialog: Seed File List dialog box, loads the seed file, and returns to the Discovery dialog box. Prime Performance Manager lists all of the seed devices in the seed file in the Seed Devices pane, and displays details of the SNMP settings for the seed devices in the Seed Details pane.
Delete	Deletes the chosen file from the seed file list. Prime Performance Manager displays an informational message containing the name and location of the deleted file.
Cancel	Closes the dialog box without loading a seed file or saving any changes to the seed file list.

Save File Dialog Box

Table 4-3 lists information and options provided in the Save File dialog box.

Table 4-3 Save File Dialog Window

Field or Button	Description
Seed File List	The Seed File List pane contains: • Go up one Folder—Click this icon to go up one folder in the directory structure. • New Folder 1. Click **New Folder** to create a new folder in the current directory. This action opens the Input dialog box. 2. Enter a folder name and click **OK**. The new folder appears in the Save File dialog box. 3. Double-click the folder to open it. You can save files in this folder or create another folder at this level. • Type—Icon indicating whether the item in the table is a file or a folder. • Name—Name of the seed file or folder. • Last Modified—Date and time the seed file or folder was last modified. • Size (bytes)—Size of the seed file or folder, in bytes.
Filename	Name by which you want to save the seed file. If you create a new seed filename, you can use any letters, numbers, or characters in the name that are allowed by your operating system. However, if you include any spaces in the new name, Prime Performance Manager converts those spaces to hyphens. For example, Prime Performance Manager saves file *a b c* as *a-b-c*.
Make this my preferred start option	Specifies whether the chosen seed file should be loaded automatically whenever this Prime Performance Manager client is started or the Discovery dialog box is opened. By default, this option is not selected. That is, a seed file is not loaded automatically when Prime Performance Manager client is started or when the Discovery dialog box is opened.
OK	Saves the seed file and any changes you made to the seed file list and closes the dialog box. To save the seed file with a new name, you can either save the file with: • A completely new name. Enter the new name and click **OK**. • An existing name, overwriting an old seed file. Select the name in the list and click **OK**. Prime Performance Manager: 1. Saves the seed file with the new name 2. Saves any changes you made to the list of files 3. Closes the Save File Dialog: Seed File List dialog box 4. Returns to the Discovery dialog box

Table 4-3 Save File Dialog Window (continued)

Field or Button	Description
Delete	Deletes the chosen file from the seed file list. Prime Performance Manager displays an informational message containing the name and location of the deleted file.
Cancel	• Closes the dialog box without saving the seed file or saving any changes to the seed file list.

Discovery Seeds Pane

The Discovery Seeds pane contains a Seed Devices File panel and a Seed Details panel. Seed Devices File options include:

- IP Address, Address Range, Subnet, CIDR, or DNS Hostname—The address or name of the chosen seed device. To create a new seed file, enter the name or address of a seed device in this field. Examples of acceptable input include:
  - IP Address: 1.2.3.4 (see the guidelines for IP addresses in).
  - Address Range: 1.2.3.2-15
  - Subnet, CIDR: 1.2.3.0/24, 1.2.3.0/255.255.255.0
  - DNS Hostname: Prime Performance Manager.cisco.com
- Add—Adds a new seed device to Prime Performance Manager.username
- Delete—Deletes the chosen seed device. A confirmation message is displayed before deleting the seed device.

The Seed Details panel lists the SNMP and Telnet/SSH parameters of discovered devices:

- SNMP Parameters:
  - IP Address Range or Hostname—IP address or DNS name of a device or range of devices. An asterisk (*) indicates a wildcard value.
  - Read Community—SNMP community name used by the device for read access to the information maintained by the SNMP agent on the device.
  - Username (v3)—Supports the SNMP v3 Username parameter. This is useful in determining whether the device will be polled using SNMPv2 or SNMPv3. SNMPv2 and SNMPv3 credentials can be provided. However, Prime Performance Manager only uses one SNMP version to communicate with devices. If both SNMPv2 and SNMPv3 are provided, Prime Performance Manager uses SNMPv3.
  - Timeout (secs)—Time, in seconds, Prime Performance Manager waits for a response from the device.
  - Retries—Number of times Prime Performance Manager attempts to connect to the device.
  - Poll Interval (mins)—Time, in minutes, between polls for the device.
- Telnet/SSH Parameters:
  - IP Address Range or Hostname—IP address or DNS name of a device or range of devices. An asterisk (*) indicates a wildcard value.
  - User Name—the device login username.
  - Password—The password for the login user.
  - Enable User Name—The privileged username.

- Enable Password—The privileged user password.
- Protocol—the transport protocol to be used to communicate with device: Telnet, SSHv1, SSHv2, or WSMA_SSH (Web Services Management Agent over SSHv2).
- Port—The device port to be used by the transport protocol chosen in the Protocol field.
- Sub System—The subsystem used by transport protocol. A blank string is the default subsystem for SSH. The default subsystem for WSMA is “wsma”.

Verifying Discovery

To view the devices that Prime Performance Manager discovered, from the navigation tree select **Summary List > Devices**. (For more information about the Devices summary list, see Using the Devices Summary List, page 8-1.) By default, the Devices table is sorted by alarm severity. If you suspect that Prime Performance Manager did not discover all of the devices, verify that:

- Prime Performance Manager server can ping the devices.
- SNMP is enabled on the devices.
- Prime Performance Manager is configured with the correct SNMP community name.

If you suspect that Prime Performance Manager did not discover all the devices, run the device discovery again.

CHAPTER 5

Configuring SSL Between Gateways and Units

The following topics tell you how to configure SSL between gateways and units:

- Enabling SSL on Gateways and Units, page 5-1
- Viewing and Exporting SSL Certificates, page 5-4
- Viewing SSL Status and Print SSL Certificates, page 5-4
- Disabling SSL, page 5-5

Enabling SSL on Gateways and Units

To enable user access (see Setting User Access, page 6-1), SSL must be enabled on Prime Performance Manager gateways and units. This process includes the generating the SSL key and certificate for the gateway and each unit connected to it, and then importing the corresponding SSL key and certificate to the gateway and units. Units must have the SSL certificate of the gateway to which it is assigned; the gateway must have the SSL certificate for each unit connected to it.

Enabling SSL on gateways and units is performed using the ppm ssl enable command. For the gateway and collocated unit, the SSL key and certificate generation and respective certificate imports are performed automatically. If you have remote units, you must copy the gateway SSL certificate to the unit and perform a number of steps manually.

Note Enabling SSL requires the gateway and unit(s) to be stopped and restarted.

To enable SSL, complete one or both of the following procedures:

- Enabling SSL on a Gateway or Collocated Gateway and Unit, page 5-1
- Enabling SSL on Remote Units, page 5-3

Enabling SSL on a Gateway or Collocated Gateway and Unit

To enable SSL on the Prime Performance Manager gateway or collocated gateway and unit:

Step 1 Log into the gateway as the root user.

Step 2 Enter the ssl enable command:

```
/opt/CSCOppm-gw/bin/ppm ssl enable
```

Prime Performance Manager:

- Stops the gateway.
- Stops the collocated unit.
- Generates RSA private key.

Step 3 When prompted, enter the SSL distinguishing information for the gateway:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager:

- Generates the following files on the gateway /opt/CSCOppm-gw/etc/ssl directory:
  - server.key—The gateway private key. Keep this key protected from unauthorized personnel.
  - server.crt—The self-signed SSL certificate.
  - server.csr—The certificate signing request (CSR). (The CSR is not used if you are using a self-signed SSL certificate.)
- Imports the gateway SSL certificate to the collocated unit.

Step 4 When prompted, enter the SSL distinguishing information for the collocated unit:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager:

- Generates the server.key, server.crt, and server.csr on the unit /opt/CSCOppm-unit/etc/ssl directory.
- Imports the collocated unit SSL certificate to the gateway.

Step 5 You are prompted to restart the gateway and unit:

```
Restart gateway and unit now (y/n)?
```

Enter **y** if you want to restart the gateway and collocated unit now, or **n** if you want to restart them later.

Note If you will enable SSL on remote units, choose **n** and continue with the "Enabling SSL on Remote Units" procedure on page 5-3. You will restart the gateway after you enable SSL on the remote units.

Note You can restart the gateway and collocated unit at any later time using the command: **/opt/CSCOppm-gw/bin/ppm restart**

Enabling SSL on Remote Units

To enable SSL on remote units:

Step 1 Log in to the remote unit.

Step 2 Enable SSL on the unit:

```
/opt/CSCOppm-unit/bin/ppm ssl enable
```

Prime Performance Manager:

- Stops the unit.
- Generates RSA private key.

Step 3 When prompted, enter the SSL distinguishing information for the unit:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Prime Performance Manager generates the server.key, server.crt, and server.csr on the unit /opt/CSCOppm-unit/etc/ssl directory:

Step 4 Import the unit certificate to the gateway:

a. Copy the **/opt/CSCOppm-unit/etc/ssl/server.crt** to a temporary location on the gateway, for example, /tmp/server.crt.

b. Enter the following command to import the unit certificate:

/opt/CSCOppm-gw/bin/ppm certtool import *myhostname*-**unit -file** *filename*

Where *alias* is a string alias for the certificate file and *filename* is the full path name for the certificate file, for example, /tmp/server.crt. Each imported certificate must have a unique alias when imported.

Step 5 Import the gateway certificate to the unit:

a. Copy the **/opt/CSCOppm-gw/etc/ssl/server.crt** to a temporary location on the unit machine, for example, /tmp/server.crt.

b. Import the gateway certificate:

/opt/CSCOppm-unit/bin/ppm certtool import *myhostname*-**gateway -file** *filename*

Where *alias* is a string that is an alias for the certificate file and *filename* is the full path name for the certificate file, for example, /tmp/server.crt.

Note The gateway imports the certificate file for each unit that connects to it. Each unit then imports the gateway certificate file for the gateway that it connects to.

Step 6 Restart the gateway:

```
/opt/CSCOppm-gw/bin/ppm restart
```

Step 7 Restart the remote unit:

```
/opt/CSCOppm-unit/bin/ppm restart unit
```

Step 8 If you previously established the Cisco Prime Network cross-launch, complete the Enabling Prime Performance Manager Cross-Launches from Prime Network, page 4-3 procedure to ensure the cross-launch links to are updated.

Related Topics:

Viewing and Exporting SSL Certificates, page 5-4

Viewing SSL Status and Print SSL Certificates, page 5-4

Disabling SSL, page 5-5

Viewing and Exporting SSL Certificates

If you implemented SSL in Prime Performance Manager, you can export SSL certificates that have been imported to Prime Performance Manager gateways or units.

To export a SSL certificate, enter the following command:

/opt/CSCOppm-gw/bin/ppm certtool export *alias* **-file** *filename*

where *alias* is the alias used when the certificate was imported and *filename* is the output file for the certificate.

To view detailed information about an SSL certificate, click the locked padlock icon in the lower-left corner of any Prime Performance Manager web interface window.

Viewing SSL Status and Print SSL Certificates

Use the following commands to view the SSL status and the SSL key and certificate pairs.

Display SSL status.

- For gateways, enter:

  ```
  /opt/CSCOppm-gw/bin/ppm ssl status
  ```

- For units, enter:

  ```
  /opt/CSCOppm-unit/bin/ppm ssl status
  ```

Print the gateway SSL certificate in X.509 format.

- For gateways, enter

```
/opt/CSCOppm-gw/bin/ppm keytool print_crt
```

- For units, enter:

```
/opt/CSCOppm-unit/bin/ppm keytool print_crt
```

List the gateway SSL key/certificate pair.

- For gateways, enter:

```
/opt/CSCOppm-gw/bin/ppm keytool list
```

- For units, enter:

```
/opt/CSCOppm-unit/bin/ppm keytool list
```

Disabling SSL

Complete the following steps to disable and remove SSL keys and certificates on a Prime Performance Manager gateway and units:

Step 1 Log into the gateway as the root or Prime Performance Manager administrator (Level 5) user.

Step 2 Stop the gateway and local unit:

```
opt/CSCOppm-gw/bin/ppm stop
```

Step 3 If remote units are connected to the gateway, log into each unit server and stop the unit:

```
opt/CSCOppm-unit/bin/ppm stop
```

Step 4 Disable SSL support on the gateway and local unit:

```
/opt/CSCOppm-gw/bin/ppm ssl disable
```

Step 5 Disable SSL on the remote units:

```
/opt/CSCOppm-unit/bin/ppm ssl disable
```

Step 6 Remove SSL keys and certificates on the gateway and local unit:

```
/opt/CSCOppm-gw/bin/ppm keytool clear
```

Step 7 Remove SSL keys and certificates on the remote units:

```
/opt/CSCOppm-unit/bin/ppm keytool clear
```

Step 8 Start the gateway and local unit:

```
opt/CSCOppm-gw/bin/ppm start
```

Step 9 Start the unit(s):

```
opt/CSCOppm-unit/bin/ppm start
```

CHAPTER 6

Setting Up and Managing Users

Before you set up your gateway for discovering, monitoring, and configuring your Cisco network, you need to make some decisions about the level of security you need in your network monitoring.

With Cisco Prime Performance Manager, you can determine how you want users to authenticate encrypted data between the application unit and the gateway, and to limit client access to specific IP addresses.

The following topics provide information about configuring Prime Performance Manager setting up and managing users:

- Setting User Access, page 6-1
- Configuring User Levels, page 6-4
- Managing Prime Performance Manager Users, page 6-14

Setting User Access

You can use user-based access to control the levels of access that users can have to the various functions in Prime Performance Manager. This is in addition to specifying root and non-root users.

User-based access provides multilevel, password-protected access to Prime Performance Manager features. Each user can have a unique username and password. There are five levels of access and you can assign these levels to users to allow or restrict their access to the features in Prime Performance Manager.

To configure Prime Performance Manager user access, perform the tasks in the following sections.

Required:

- Enabling SSL on Gateways and Units, page 5-1
- Implementing Secure User Access, page 6-2
- Creating Secure Passwords, page 6-5
- Configuring Prime Performance Manager User Account Levels, page 6-6

Optional:

- Automatically Disabling Users and Passwords, page 6-7
- Manually Disabling Users and Passwords, page 6-9
- Enabling and Changing Users and Passwords, page 6-10
- Displaying a Message of the Day, page 6-11

- Listing All Currently Defined Users, page 6-12
- Displaying the Contents of the System Security Log, page 6-13
- Disabling Prime Performance Manager User-Based Access, page 6-14

Implementing Secure User Access

Before you can access the full suite of security commands in Prime Performance Manager, you must enable Prime Performance Manager user access, configure the type of security authentication you want, and add users to your user lists.

After you implement user access for Prime Performance Manager, users must log into the system to access the:

- Prime Performance Manager web interface
- Event Editor

Two types of security authentication are possible:

- Local authentication:

  You can create user accounts and passwords that are local to Prime Performance Manager system. With this method, you can use Prime Performance Manager user access commands to manage usernames, passwords, and access levels.

- Solaris/Linux authentication:

  Uses standard Solaris- or Linux-based user accounts and passwords, as specified in the /etc/nsswitch.conf file.

  You can provide authentication using the local /etc/passwd file; a distributed Network Information Services (NIS) system. You can use all Prime Performance Manager user access commands except:

  - **`/opt/CSCOppm-gw/bin/ppm disablepass`**
  - **`/opt/CSCOppm-gw/bin/ppm passwordage`**
  - **`/opt/CSCOppm-gw/bin/ppm userpass`**

PAM Setup to Check Library Version and JVM Versions

Prime Performance Manager supports:

- Pluggable Authentication Modules (PAM) for Remote Authentication Dial in User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS+)
- Lightweight Directory Access Protocol (LDAP) authentication.

Instructions for configuring these authentication modules are provided on the gateway install directory, /opt/CSCOppm-gw/install, and on the install directory of the Prime Performance Manager installation image as INSTALL.pam_radius.txt, INSTALL.pam_tacplus.txt, and INSTALL.pam_ldap.txt.

- To ensure Java Virtual Machine (JVM) version and available Pluggable Authentication Modules (PAM) library matches, note the following:
  - If your Operating System only has 32-bit version of the PAM library, then you need to use 32-bit JVM.
  - If your Operating System only has 64-bit version of the PAM library, then you need to use 64-bit JVM.
  - If your Operating System has both 32-bit and 64-bit versions of PAM libraries, then you can use either 32-bit or 64-bit JVM.

- To check the available PAM authentication module versions based on:
  - /opt/CSCOppm-gw/install/INSTALL.pam_radius.txt, supported only in 32-bit, no 64-bit library support provided for RADIUS on Solaris, enter:

    ```
    file /usr/lib/security/pam_radius_auth.so
    ```

  - /opt/CSCOppm-gw/install/INSTALL.pam_radius.txt, supported in 32-bit and 64-bit library support provided for RADIUS on Linux, enter:

    ```
    /lib/security/pam_radius_auth.so
    /lib64/security/pam_radius_auth.so
    ```

  - Based on /opt/CSCOppm-gw/install/INSTALL.pam_tacplus.txt:

    TACACS+ on Linux, enter:

    ```
    file /lib/security/pam_tacplus_auth.so
    file /lib64/security/pam_tacplus_auth.so
    ```

    TACACS+ on Solaris, enter:

    ```
    file /usr/lib/security/pam_tacplus_auth.so
    file /usr/lib/security/sparcv9/pam_tacplus_auth.so
    ```

  - Based on /opt/CSCOppm-gw/install/INSTALL.pam_ldap.txt:

    LDAP on Linux, enter:

    ```
    file  /lib/security/pam_ldap.so
    file  /lib64/security/pam_ldap.so
    ```

    LDAP on Solaris, enter:

    ```
    file /usr/lib/security/pam_ldap.so
    file /usr/lib/security/sparcv9/pam_ldap.so
    ```

- To check JVM versions, enter:

  ```
  /opt/CSCOppm-gw/j2re/jre/bin/java -version
  ```

- For Solaris, Prime Performance Manager has both 32-bit and 64-bit JVM versions. 64-bit JVM is enabled by default. To change to 32-bit, enter:

  ```
  % cd /opt/CSCOppm-gw/j2re/jre/bin
  % mv java.sgm java.64
  % mv java.32 java.sgm
  % /opt/CSCOppm-gw/bin/ppm restart
  ```

  To check the JVM version, enter:

  ```
  /opt/CSCOppm-gw/j2re/jre/bin/java -version
  ```

- For Linux, you cannot change JVM versions. Prime Performance Manager installs the 64-bit JVM if the Linux runs 64-bit kernel, or the 32-bit JVM if the Linux runs 32-bit kernel.

  You need to ensure that the proper PAM library version is available on Linux that matches the kernel version.

Note Check the install subdirectory in /opt/CSCOppm-gw of Prime Performance Manager installation CD image for the notes - INSTALL.pam_radius.txt (for PAM RADIUS module) or INSTALL.pam_tacplus.txt (for TACPLUS module) and INSTALL.pam_ldap.txt (for LDAP module).

Configuring User Levels

You can configure one of four account levels for each user. Valid levels are:

1. Basic User (Level 1) Access
2. Network Operator (Level 3) Access
3. System Administrator (Level 5) Access
4. Custom User Level 1 (Level 11) and Custom User Level 2 (Level 12) Access

For more information about account levels, see Configuring Prime Performance Manager User Account Levels, page 6-6.

Configuring User Passwords

The method that you use for setting user passwords depends on the type of authentication that you configure on Prime Performance Manager system (local or Solaris/Linux).

Local Authentication

If the **ppm authtype** command is set to local, Prime Performance Manager prompts you to:

- Enter the user password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 6-5.
- Force the user to change the password at the next login. The default is to not force the user to change the password.

If the user needs to change a password, Prime Performance Manager displays an appropriate message, and prompts for the username and new password.

Solaris/Linux Authentication

If the **ppm authtype** command is set to Solaris or Linux, users cannot change their passwords by using Prime Performance Manager client. Instead, they must manage their passwords on the external authentication servers by using Solaris or Linux commands, such as *passwd*.

All new passwords take effect the next time Prime Performance Manager automatically synchronizes local Prime Performance Manager passwords with Solaris or Linux commands.

Enabling Secure User Access

To enable secure user access for Prime Performance Manager:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 To enable Prime Performance Manager security, the following prerequisites must be met:

- SSL must be enabled. See Enabling SSL on Gateways and Units, page 5-1.
- User access must be enabled.
- The authentication type must be set.
- Users must be added.

The **ppm useraccess** enable command takes you through all three stages, checking the status of:

1. **ppm useraccess**—Enabled or disabled.

2. **ppm authtype**—If you have not already set Prime Performance Manager authentication type, you must do so now.
3. **ppm adduser**—If you have already assigned users, Prime Performance Manager prompts you to either use the same user database, or create a new one. If you have not assigned users, you must do so now.

Tip For details on **ppm useraccess**, **ppm authtype**, and **ppm adduser** commands, see Appendix B, "Command Reference".

Run Prime Performance Manager useraccess enable command:

```
cd /opt/CSCOppm-gw/bin
./ppm useraccess enable
~text elided~
```

To activate your security changes on Prime Performance Manager client, restart Prime Performance Manager gateway using the **/opt/CSCOppm-gw/bin/ppm restart** command (see ppm restart, page B-39).

To activate your security changes on Prime Performance Manager web interface, clear the browser cache and restart the browser.

See Creating Secure Passwords, page 6-5, to further customize your Prime Performance Manager security system

Creating Secure Passwords

When setting passwords in Prime Performance Manager, the:

- Password must be at least 6 characters, and a maximum of 15 characters.
- Password cannot be identical to the username.
- New password cannot be the same as the old password.
- Prime Performance Manager does not allow users to switch back and forth between two passwords.
- Password cannot be a commonly used word. Prime Performance Manager gateway uses the system dictionary at /usr/share/lib/dict/words (Solaris) or /usr/share/dict/words (Linux) to determine whether a word is a commonly used word.

  To use your own dictionary, add a line to the System.properties file:

  - To disable Prime Performance Manager dictionary and allow common words, add:

    ```
    DICT_FILE=/dev/null
    ```

  - To use a custom dictionary, add:

    DICT_FILE=/*new-dictionary*

    where *new-dictionary* is the path and filename of the custom dictionary file, such as */users/usr11/words*. Each line in the custom dictionary must contain a single word, with no leading or trailing spaces.

Configuring Prime Performance Manager User Account Levels

This section describes the user account levels, and Prime Performance Manager client and web interface actions that are available at each level:

- Basic User (Level 1) Access, page 6-6
- Network Operator (Level 3) Access, page 6-6
- System Administrator (Level 5) Access, page 6-6
- Custom User Level 1 (Level 11) and Custom User Level 2 (Level 12) Access, page 6-7

The account level that includes an action is the lowest level with access to that action. The action is also available to all higher account levels. For example, a System Administrator also has access to all Network Operator actions.

Account levels are based on the action to be performed, not on the target network element. Therefore, if a user can perform an action on one Prime Performance Manager network element (such as deleting a node), the user can perform the same action on all similar Prime Performance Manager network elements.

Note Access to Prime Performance Manager information and downloads on Cisco.com is already protected by Cisco.com, and is not protected by Prime Performance Manager.

To configure the account level for a user, use the **ppm adduser** command, as described in Implementing Secure User Access, page 6-2, or **ppm updateuser** or **ppm newlevel** commands, as described in Enabling and Changing Users and Passwords, page 6-10.

Basic User (Level 1) Access

Basic users can view Prime Performance Manager data, load Prime Performance Manager files, and use Prime Performance Manager drill-down menus.

The following Prime Performance Manager actions in the web interfaces are available to basic users:

- View Prime Performance Manager web interface homepage
- View Reports

Network Operator (Level 3) Access

The following Prime Performance Manager actions in the web interfaces are available to network operators:

- Access all basic (Level 1) user actions
- Can view Active Alarms, Event History, Summary List
- Can access only Normal Poll node and Edit Properties option in the Actions menu

System Administrator (Level 5) Access

The following Prime Performance Manager actions in the client and web interfaces are available to system administrators:

- Accessing all basic (Level 1) user, network operator (Level 3) user access.

- Enabling and disabling reports
- Accessing all options from the Actions menu.
- Disabling, enabling and assigning temporary passwords to different user administrations.

Custom User Level 1 (Level 11) and Custom User Level 2 (Level 12) Access

The Custom User Level 1 Access and Custom User Level 2 Access by default does not have authorizations but can be customized and set permissions of all basic (Level 1) user, network operator (Level 3) and system administrator (Level 5) access.

To customize, these access levels, the user needs to edit the roles.conf file in the /opt/CSCOppm-gw/etc path in the gateway.

Automatically Disabling Users and Passwords

After you have implemented the basic Prime Performance Manager security system, you can customize the system to automatically disable users and passwords when certain conditions are met. For example, a series of unsuccessful login attempts or a specified period of inactivity).

Tip To view a list of current users and the status of user accounts, use **ppm listusers** command (see ppm listusers).

To automatically disable users and passwords:

Step 1 Log into the Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Enter the following command:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 (Optional) To configure Prime Performance Manager to generate an alarm after a specified number of unsuccessful login attempts by a user, enter:

```
#./ppm badloginalarm number-of-attempts
```

where *number-of-attempts* is the number of unsuccessful login attempts allowed before Prime Performance Manager generates an alarm.The number of login attempts are recorded in the security log file.

Prime Performance Manager records alarms in the system security log file. The default path and filename for the system security log file is /opt/CSCOppm-gw/logs/sgmSecurityLog.txt. If you installed Prime Performance Manager in a directory other than /opt, then the system security log file resides in that directory.

By default, there can be five unsuccessful attempts before the system generates an error.

To disable this action (that is, to prevent Prime Performance Manager from automatically generating an alarm after unsuccessful login attempts), enter:

```
#./ppm badloginalarm clear
```

Step 4 (Optional) To configure Prime Performance Manager to disable a user's account automatically after a specified number of unsuccessful login attempts, enter:

```
#ppm badlogindisable number-of-attempts
```

where *number-of-attempts* is the number of unsuccessful login attempts allowed before Prime Performance Manager disables the user's account. Prime Performance Manager does not delete the user from the user list, Prime Performance Manager only disables the user's account.

By default, there can be ten unsuccessful attempts before the system generates an error.

To re-enable the user's account, use **ppm enableuser** command.

To disable this action (that is, to prevent Prime Performance Manager from automatically disabling a user's account after unsuccessful login attempts), enter:

```
# ./ppm badlogindisable clear
```

Step 5 (Optional) Prime Performance Manager keeps track of the date and time each user last logged in. To configure Prime Performance Manager to disable a user's log in automatically after a specified number of days of inactivity, enter:

```
# ./ppm inactiveuserdays number-of-days
```

where *number-of-days* is the number of days that a user can be inactive before Prime Performance Manager disables the user's account. Prime Performance Manager does not delete the user from the user list, Prime Performance Manager only disables the user's account.

The valid range is one day to an unlimited number of days. There is no default setting.

To re-enable the user's account, use Prime Performance Manager enableuser command.

This action is disabled by default. If you do not specify the **ppm inactiveuserdays** command, user accounts are never disabled as a result of inactivity.

If you have enabled this action and you want to disable it (that is, to prevent Prime Performance Manager from automatically disabling user accounts as a result of inactivity), enter:

```
# ./ppm inactiveuserdays clear
```

Step 6 (Optional) If **ppm authtype** is set to local, you can configure Prime Performance Manager to force users to change their passwords after a specified number of days.

To configure Prime Performance Manager to force users to change their passwords after a specified number of days, enter:

```
# ./ppm passwordage number-of-days
```

where *number-of-days* is the number of days allowed before users must change their passwords.

Note You must have changed your password at least once for the **ppm passwordage** command to properly age the password.

The valid range is one day to an unlimited number of days. There is no default setting.

Prime Performance Manager starts password aging at midnight on the day that you set the value. For example, if you use the **ppm passwordage** command to set the password age to one day (24 hours), the password begins to age at midnight and expires 24 hours later.

This action is disabled by default. If you do not specify the **ppm passwordage** command, users never need to change their passwords.

If you have enabled this action and you want to disable it (that is, prevent Prime Performance Manager from forcing users to change passwords), enter:

```
# ./ppm passwordage clear
```

Note If **ppm authtype** is set to Solaris or Linux, you cannot use the **ppm passwordage** command. Instead, you must manage passwords on the external authentication servers.

Step 7 (Optional) To configure Prime Performance Manager to automatically disconnect a web interface after a specified number of minutes of inactivity, enter:

```
# ./ppm clitimeout number-of-minutes
```

where *number-of-minutes* is the number of minutes a client can be inactive before Prime Performance Manager disconnects the client.

The valid range is one minute to an unlimited number of minutes. There is no default value.

This action is disabled by default. If you do not specify the **ppm clitimeout** command, clients are never disconnected as a result of inactivity.

If you have enabled this action and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the following command:

```
# ./ppm clitimeout clear
```

Manually Disabling Users and Passwords

As described in the Automatically Disabling Users and Passwords, page 6-7, you can customize Prime Performance Manager to automatically disable users and passwords when certain conditions are met. However, you can also manually disable Prime Performance Manager users and passwords whenever you suspect that a security breech has occurred.

Note You can add new user and password from Prime Performance Manager web interface, see Managing Prime Performance Manager Users, page 6-14 for more details.

To disable Prime Performance Manager users and passwords:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Enter:

```
# cd /opt/CSCOppm-gw/bin
```

Step 3 (Optional) To delete a user entirely from Prime Performance Manager user access account list, enter:

```
# ./ppm deluser username
```

where *username* is the name of the user.

If you later decide to add the user back to the account list, you must use **ppm adduser** command.

Step 4 (Optional) If **ppm authtype** is set to local, you can disable a user’s password. To disable a user’s password, enter:

```
# ./ppm disablepass username
```

where *username* is the name of the user. Prime Performance Manager does not delete the user from the account list, Prime Performance Manager only disables the user's password.

Note If **ppm authtype** is set to Solaris or Linux, you cannot use the **ppm disablepass** command. Instead, you must manage passwords on the external authentication servers.

The user must change the password the next time they log in.

You can also re-enable the user's account with the same password, or with a new password:

- To re-enable the user's account with the same password as before, use the **ppm enableuser** command.
- To re-enable the user's account with a new password, use the **ppm userpass** command.

Step 5 (Optional) To disable a user's account, but not the user's password, enter:

```
# ./ppm disableuser username
```

where *username* is the name of the user.

Note If **ppm authtype** is set to Solaris or Linux, you must be logged in as the root user, to enter this command.

Prime Performance Manager does not delete the user from the account list; Prime Performance Manager only disables the user's account. The user cannot log in until you re-enable the user's account:

- To re-enable the user's account with the same password as before, use the **ppm enableuser** command.
- To re-enable the user's account with a new password, use the **ppm userpass** command.

Enabling and Changing Users and Passwords

Prime Performance Manager also enables you to re-enable users and passwords, and change user accounts.

To enable and change users and passwords:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Enter the following command:

```
# cd /opt/CSCOppm-gw/bin
```

Step 3 (Optional) To re-enable a user's account, which had been disabled either automatically by Prime Performance Manager, enter the following command:

```
# ./ppm enableuser username
```

where *username* is the name of the user. Prime Performance Manager re-enables the user's account with the same password as before.

Note If **ppm authtype** is set to Solaris or Linux, you must be logged in as the root user, to enter this command.

Step 4 (Optional) If **ppm authtype** is set to local, you can change a user's password, or re-enable the user's account with a new password, if the user's account had been disabled automatically by Prime Performance Manager. To change a password or to re-enable a user's account with a new password, enter:

```
# ./ppm userpass username
```

where *username* is the name of the user.

Prime Performance Manager prompts you for the new password. When setting the password, follow the rules and considerations in the Creating Secure Passwords, page 6-5.

If the user's account has also been disabled, Prime Performance Manager re-enables the user's account with the new password.

Note If **ppm authtype** is set to Solaris or Linux, you cannot use the **ppm userpass** command. Instead, you must manage passwords on the external authentication servers.

Step 5 (Optional) To change a user's account level and password, enter the following command:

```
# ppm updateuser username
```

where *username* is the name of the user.

Note If **ppm authtype** is set to Solaris or Linux, you must be logged in as the root user, to enter this command.

Prime Performance Manager prompts you for the new account level.

If **ppm authtype** is set to local, Prime Performance Manager also prompts you for the user's new password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 6-5.

Step 6 (Optional) To change a user's account level, but not the user's password, enter the following command:

```
# ./ppm newlevel username
```

where *username* is the name of the user.

Prime Performance Manager prompts you for the new account level.

Displaying a Message of the Day

You can use Prime Performance Manager to display a user-specified Prime Performance Manager system notice called the Message of the Day. You can use the Message of the Day to inform users of important changes or events in Prime Performance Manager system.

If you enable the Message of the Day, it appears whenever a user attempts to launch a client.

The Message of the Day also allows you to exit Prime Performance Manager Web User Interface before starting it in certain scenarios. If the user accepts the message, the client launches. If the user declines the message, the client does not launch.

To display the Message of the Day dialog box:

- Launch a web interface. If there is a message, the Message of the Day dialog box appears.

To configure Prime Performance Manager to display the Message of the Day:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Enter the following commands:

```
cd /opt/CSCOppm-gw/bin
./ppm motd enable
```

Prime Performance Manager displays:

```
Enter location of the message of the day file: [/opt/CSCOppm-gw/etc/motd]
```

Step 3 Press **Enter to accept the default value**; or type a different location and press **Enter**.

when a user login to Prime Performance Manager web interface, Prime Performance Manager displays:

```
Last Updated: MM:DD:YYYY Hrs:Sec AM
Message of the day
```

Step 4 **Accept** or **Decline** the Message of the day. If you accept the message, you are logged into Prime Performance Manager Web Interface.

To create the message text (the first time) or edit the existing text, enter:

```
./ppm motd edit
```

To display the contents of the Message of the Day file, enter:

```
./ppm motd cat
```

To disable the Message of the Day file, enter:

```
./ppm motd disable
```

Listing All Currently Defined Users

To list all currently defined users in Prime Performance Manager User-Based Access account list:

Note You can also view user account information on Prime Performance Manager User Accounts web page, refer Managing Prime Performance Manager Users, page 6-14 for more details.

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 List all users:

```
./ppm listusers
```

Prime Performance Manager displays the following information for each user:

- Username
- Last time the user logged in
- User’s account access level
- User’s current account status, such as Account Enabled or Password Disabled

To list information for a specific user, enter:

```
./ppm listusers username
```

where *username* is the name of the user.

Displaying the Contents of the System Security Log

To display the contents of the system security log with PAGER:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Display the security log contents:

```
./ppm seclog
```

The following security events are recorded in the log:

- All changes to system security, including adding users
- Login attempts, whether successful or unsuccessful, and logoffs
- Attempts to switch to another user's account, whether successful or unsuccessful
- Attempts to access files or resources of higher account level
- Access to all privileged files and processes
- Operating system configuration changes and program changes, at the Solaris level
- Prime Performance Manager restarts
- Failures of computers, programs, communications, and operations, at the Solaris level

Step 4 Clear the log, by entering:

```
/opt/CSCOppm-gw/bin/ppm seclog clear
```

The default path and filename for the system security log file is */opt/CSCOppm-gw/logs/sgmSecurityLog.txt*. If you installed Prime Performance Manager in a directory other than */opt*, then the system security log file is located in that directory.

Note You can also view the system security log on Prime Performance Manager System Security Log web page. For more information, see Viewing the Security Log, page 12-11.

Disabling Prime Performance Manager User-Based Access

To completely disable Prime Performance Manager User-Based Access:

Step 1 Log into Prime Performance Manager gateway as the root user. See Logging in as the Root User, page 2-1.

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Disable user-based access:

```
./ppm useraccess disable
```

Prime Performance Manager user access is disabled the next time you restart Prime Performance Manager gateway (using the ppm restart command).

Managing Prime Performance Manager Users

Prime Performance Manager allows you to manage users through the web interface. User access must be enabled. A Level 5 user must be created during installation or post-installation, using Prime Performance Manager CLI as root.

A web user with user management permissions with Prime Performance Manager access Level 5, can add or delete users and modify user passwords and roles/access levels.

To manage users, click **Administrative** in the navigation tree and then click **User Management**. All Prime Performance Manager users are displayed with the time of their most recent logins, their access levels, and their account statuses. Table 6-1 lists the User Management tab information and options.

Table 6-1 User Management Tab

Option	Tool	Description
Create a new user account	➕	Creates a new user account.
Delete an existing user account	➖	Deletes one or more users. The user interface asks for confirmation and deletes the user. To delete multiple users, check the check box in the user row and then click the **Delete an existing user account** button in the toolbar.
Users selected		The number of currently selected users.
Clear Selection		Deselects the selected list of users.

To add a new user:

Step 1 Click **Administrative** in the navigation tree and then click **User Management.**

Step 2 In the User Management window, click the **Create a New User Account** tool.

Step 3 Complete the new user information. The options that appear depend on whether you enabled local authentication or rely on Solaris or Linux user authentication.

- Name—Enter the user name.
- Level—Enter the user authentication level for the user. The valid values are:
  - Basic User, Level 1
  - Network Operator, Level 3
  - System Administrator, Level 5
  - Custom Level 1
  - Custom Level 2
- Password (local authentication only)—Enter the user password.
- Confirm Password (local authentication only)—Retype the password to confirm the new password.
- Force user to reset password at login? (local authentication only)—If selected, the user will be required to change the password the next time they log in.
- Add users not known to system? (Solaris or Unix authentication only)—If selected, allows users who are not known to the system to be added.

Step 4 Click **OK**.

After you add users, the User Management table contains the following information:

Action—Allows you to change the user’s password.

- User—The Prime Performance Manager user for whom a user-based access account is set up.
- Last Login—The date and time the user last logged into Prime Performance Manager.
- Access Level—Authentication level and number for the user. Valid access levels and numbers include:
  - Basic User, Level 1
  - Network Operator, Level 3
  - System Administrator, Level 5
  - Custom Level 1, 11
  - Custom Level 2, 12
- Account Status—The current user’s account status: Enabled (the account is functioning normally), or Disabled. A user account can be disabled for the following reasons:
  - A System Administrator disabled the account. See the “ppm disablepass” section on page B-17 and the “ppm disableuser” section on page B-17 for more information.
  - Prime Performance Manager disabled the account because of too many failed attempts to log in using the account. See the “ppm badlogindisable” section on page B-11 for more information.
  - Prime Performance Manager disabled the account because it was inactive for too many days. See the “ppm inactiveuserdays” section on page B-24 for more information.

- Expired Password
- Temporary Password

To update a user:

Step 1 Click the **Change a User's Password** icon under the Action column.

Step 2 In the Update User window, complete the following information.

- Password—Enter the password.
- Confirm Password—Retype the password to confirm the new password.
- Force user to reset password at login?—Select if you want the user to change their password at their next log in.

Step 3 Click **OK**.

CHAPTER 7

Working With Reports and Dashboards

The following topics describe how to use Prime Performance Manager reports and dashboards. Topics include:

Using Reports

The Reports navigation tree item in the Prime Performance Manager web interface allows you view all reports that are globally available. Selecting a report in the navigation tree displays the report information in the content area.

You can configure Prime Performance Manager to gather critical information at scheduled intervals from network objects. Prime Performance Manager uses the information to calculate statistics, such as Ethernet, peer flap, performance, device availability, and other statistics. Prime Performance Manager generates reports based on these statistics.

Prime Performance Manager supports predefined system reports. These reports are listed in the Report XML Definitions page (Home > Reports Documentation) page. The XML and the property files describe the MIB tables and the fields that are polled for data from the device. It also describes the fields that are mapped to the report columns.

To generate new reports for the devices, refer to the predefined system reports as examples, and add new report XML files to the etc/pollers/user directory in the Prime Performance Manager gateway installation directory, by default it is /opt/CSCOppm-gw.

The new user-defined report XML files must have a unique filename from the predefined system report files. For additional details on how to define new reports, see the *Cisco Prime Network 1.1 Integration Developer Guide*.

To view all reports:

Step 1 Log into the Prime Performance Manager GUI application.

Step 2 In the navigation area, select **Reports**.

Step 3 Expand the Reports navigation tree to the report you want to view, then click the report. For example, if you want to view current TCP reports, select **Reports > Application Traffic > TCP**.

All TCP reports appear. See Viewing Reports, page 7-4 for more information.

To view the report for a single device of a specified report type:

Step 1 Select a device using the Device Summary List. (See Using the Devices Summary List, page 8-1.)

Step 2 Click the type of report you want to view.

Reports for the active devices appear in the right content pane.

Step 3 Select a device.

The reports for that specific device are displayed. See Viewing Device Level Reports, page 7-3 for more information

Viewing Report Status

The Reports Status table in the Prime Performance Manager web interface content pane allows you to globally enable and disable reports that are displayed in the left navigation tree.

Note Only reports that run on a regularly scheduled interval are displayed in the Hourly and Daily data. Reports that run continuously are not displayed.

To access the main Reports page:

Step 1 In a web browser, launch the Prime Performance Manager web interface (see Accessing the Prime Performance Manager Web Interface, page 3-1).

Step 2 In the navigation tree, click **Reports**.

The Reports Status table in the content area displays the report type and the status (enabled or disabled).

Step 3 Select the report that you wish to disable and click **Save**.

The reports in the left navigation tree refreshes to display the status of the report disabled.

To enable a report in Prime Performance Manager web interface, check the check box in the Status column.

Related Topics

Viewing Network Level Reports, page 7-3

Viewing Device Level Reports, page 7-3

Viewing Network Level Reports

The Network Level Reports display a summary of the top level graph view summary that is available for a particular report, in the left navigation pane. At Network Level, Table/CSV/Graph views are available to all devices in the network. To view a Network Level Report, select **Reports > Availability > Interfaces**.

The right content pane displays the network level graph view summary of devices available.

To view the different types of reports in the right content pane, click the **Reports** drop-down arrow and select the reports you want to view.

Related Topic

Viewing Graph Series Editor Details, page 7-8

Viewing Device Level Reports

The Device Level Reports display details on reports that are available for a particular device. If you select a device from the top level graph view summary in the right content pane (see Viewing Network Level Reports, page 7-3 for details) it displays the reports detail for that device with the device name in the left navigation pane.

See Working With Reports and Dashboards, page 7-1 for more information.

After you select a device, the Report Status tab appears. This tab displays the devices that are specific to that device. See Viewing Report Status, page 7-2 for more information

Related Topics

- Viewing Device, Gateway, or Unit Details, page 7-6
- Displaying Active Alarms and Event History, page 9-1
- Active Alarms and Event History Toolbar, page 9-4

Enabling Reports Using the CLI

Using CLI commands, you can generate reports that can be run at specified intervals. You can enable and disable automatic generation of these reports, using the ppm statreps commands (see ppm statreps, page B-55).

After you enable generation of a report, it will run at the specified intervals until you disable it with the appropriate CLI command.

Enabling reports using the CLI, is the same as enabling and disabling reports from the Reports page. To enable or disable report aging settings, select **Report** in the left navigation pane and enter the aging value in the Aging Settings.

The database report aging occurs once every day before the backup starts. It is triggered by the cron job ppmCron.sh backup

To enable reports using the CLI:

Step 1 Log in as the root user.

Step 2 Enter:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Enter the following CLI command to enable all report types:

```
./ppm statreps all
```

To see a list of all report-related CLI commands, enter the following command:

```
./ppm rephelp
```

Viewing Reports

After you generate reports, you can view them using the Prime Performance Manager web interface. You can view historical reports for all objects of a specific type. For example, all link reports for all links.

You can also view reports for a specific object. For example, all link reports for a specific link.

For the reports whose output type is Graph, the Graph Series Editor window is displayed when you click the Custom series icon. See Viewing Graph Series Editor Details, page 7-8 for details.

For these reports, you can use the Sort Parameter option to select the criteria to include a top set of series. You can also use this option to sort the graphs that are displayed.

You can access reports in the Prime Performance Manager web interface through these categories. Prime Performance Manager provides over 900 reports divided into the following categories:

- Application Traffic
- Availability
- IP Protocols
- IP QoS
- IP SLA
- Mobile Statistics
- Resources
- Transport Statistics

The best way to view the individual reports is to drill down the Reports navigation tree. Another way to view the reports provided with Prime Performance Manager is viewing the Report Status tab. See Viewing Report Status, page 7-2.

Note Prime Performance Manager reports are based on the MIBs supported on the devices. For a list of MIBs supported in Prime Performance Manager, in the navigation area, click **Home**, then under Reports Documentation click **SNMP MIBs**.

Yo can view a web report either for all objects of a specified type or for a single object of a specified type.

To view a web report for all objects of a specified type:

Step 1 Select **Reports** in the Prime Performance Manager web navigation tree and click the type of report you want to view

For example, if you want to view hourly TCP Segments report, select **Reports > Application Traffic > TCP> TCP Segments > 15 Minutes/Hourly/Daily**.

All link reports appear.

Step 2 Click the **Reports** drop-down arrow and navigate to the type of report you need. (You need to select the various drop-down menus)

Step 3 Select **Duration** from the drop-down lists. For example, if you wanted to view hourly link reports for the last 12 hours, choose **Last 12 Hours** from the **Duration** drop-down.

For most Statistics and Accounting reports, to customize the date, time range, or both, click the **Customize the date and time range** icon. Note that these dates are the dates with server time zone.

Step 4 Click the **Output Mode** drop-down to view the corresponding report in Graph/Table/CSV mode.

CSV reports for all devices are generated in /opt/CSCOppm-gw/reports and prefixed with the report type for additional context.

For example, B20110308.0945-0500-20110308.1000-0500_ppm-xxx-vm38.csv report is prefixed with CPU.B20110308.0945-0500-20110308.1000-0500_ppm-xxx-vm38.csv.

Step 5 Click the green arrow to run the report

To view a web report for a single object of a specified type:

Step 1 Click a device in the web navigation tree to select an object in a device.

Step 2 In the content area in the right pane, click the **Reports** tab.

Reports appear for the active object only.

Step 3 Click the **Reports** drop-down arrow and navigate to the type of report you need. (You need to select the various drop-down menus)

Step 4 Select **Duration** from the drop-down lists. For example, if you wanted to view hourly link reports for the last 12 hours, choose **Last 12 Hours** from the **Duration** drop-down.

For most Statistics and Accounting reports, to customize the date, time range, or both click the Customize the date and time range icon. Note that these dates are the dates with server time zone.

Step 5 Click the **Output Mode** drop-down to view the corresponding report in Graph/Table/CSV mode.

CSV reports for all devices are generated in /opt/CSCOppm-gw/reports and prefixed with the report type for additional context.

For example, B20110308.0945-0500-20110308.1000-0500_ppm-xxx-yy38.csv report is prefixed with CPU.B20110308.0945-0500-20110308.1000-0500_ppm-xxx-yy38.csv. All the CSV reports are available only after they are compressed in .zip format.

Step 6 Click the green arrow to run the report

Tip For details on web toolbars and icons, see Using the Toolbar, page 3-6.

Related Topics

Viewing Device Level Reports, page 7-3

Viewing Graph Series Editor Details, page 7-8

Enabling and Disabling Reports, page 7-8

Enabling Reports Using the CLI, page 7-3

Viewing Device, Gateway, or Unit Details

The Details tab displays information such as naming and status details for the chosen device, gateway, or unit.

To view the details of a selected device, gateway, or unit:

Step 1 From the Reports menu, choose a report.

Step 2 Select an object from the reports and then click a device from the top level graph view summary in the right content pane.

Step 3 The Reports, Details, Events, Alarms and Report Status tab displays. See Table 7-1 for more details.

Table 7-1 Gateway and Unit Details

Section	Field	Description
Naming Information	Display Name	The device display name.
	Custom Name	The custom device name, if one is defined. If not, this field displays, Unknown.
	Sync Name	The device synchronization name.
	IP Address or Host Name	The device IP address or DNS name, as discovered by Prime Performance Manager.
	SysName	The name set on the router and returned, using the SNMP variable sysName.
	Device Type	Type of the device.
	Location	The device physical location. If the device location details are not available, this field displays Unknown.
	Unit	The name of the unit to which the device belongs.

Table 7-1 Gateway and Unit Details (continued)

Section	Field	Description
Status Information	Is Ignored	Indicates whether the device is Ignored (that is, whether to include the device when aggregating and displaying Prime Performance Manager status information).
	Alarm Severity	Indicates the alarm severity of the object.
	Status	The device's current status: • Active • Discovering • Polling • Unknown • Unmanaged • Waiting • Warning
	Last Status Change	Date and time when the device status was last changed.
	Status Reason	Status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears.
Polling Information	Report Polling	Indicates whether report polling is enabled for this device.
	First Discovered	The date and time when Prime Performance Manager first discovered the device.
	Last Poll IP Address	The last IP address that was polled for this device.
	Last Full Poll Time	The date and time of the last full poll of the device for device-related MIBs
	Last Poll Response (secs)	The time, in seconds, taken by this device to respond to the last poll request.
	Avg. Poll Response (secs)	The average time, in seconds, taken by this device to respond to Prime Performance Manager poll requests.
Descriptive Information	Contact	The contact person for the managed device and contact information, if available. If the contact details are not available, this field displays Unknown.
	Software Version	The software version (for example, the ONS package or IOS version) that is installed on the device.
	Software Description	Comprehensive information about the software that is installed on the device.
Uptime Information	Uptime	The time the device has been up, in days, hours, minutes, and seconds.
	Reboot Time	The date and time of the last device reboot.
	Reboot Reason	The reason for the last reboot of the device.

Table 7-1 Gateway and Unit Details (continued)

Section	Field	Description
IP Address	IP Address	IP addresses associated with this device, including the primary SNMP address and all backup IP addresses, that are intended for SNMP.
	Last Regular Poll Time	The date and time of the last full poll of the device. If the IP address has never been polled, Prime Performance Manager displays, Never Polled.
	SNMP Pollable	Indicates whether the IP address is used for SNMP polling.

To view the details of a gateway or unit:

Step 1 In the navigation tree Summary List, choose **Gateway/Units**.

Step 2 Choose a gateway or unit from the Gateway/Units table in the content pane.

The Details, Events and Alarms tab provides detailed information about the gateway or unit. See Table 7-1 for information.

Enabling and Disabling Reports

To enable/disable specific reports, select the **Setting** tab (see Viewing Historical Statistics Report Settings, page 7-9) in the Reports page. All reports (5 Minute, 15 Minute, Hourly Report, Daily Report) can be enabled or disabled. By default, all the reports are run every 15 minutes, hourly and daily.

You can see the device appearing at the bottom on the left navigation tree, after a specific device is selected from the right pane.

Note Administrator (Level 5) and operator (Level 3) users can enable 5-minute reports. However, the SNMP polling interval for the devices that require a 5-minute report, can only be set by administrator users.

The XML report definition are located on the gateway in the /opt/CSCOppm-gw/etc/pollers/system or /opt/CSCOppm-gw/etc/pollers/user directories. Administrator (Level 5) access is required to edit the report definitions.

Enabling a 5-minute report increases disk space utilization required for the units and decreases the performance of the units because of the increase in disk activity.

Viewing Graph Series Editor Details

The Graph Series Editor window allows you to show or hide a selected data series.This window appears if you select the report output as Graph. Most network-level reports contain the top 10 series of data.

See Table 7-2 for more details.

Table 7-2 Graph Series Editor

Column or Buttons	Descriptions
Selected Series	Displays the domain name IDs for the data that is used to create the report.
Available Series	Displays the list of available objects for this report. If there are many objects in the report, the objects in the Available Series column span multiple pages and all objects are not shown on one page. See Using the Toolbar, page 3-6 for more information on using the paging features. To view all selected objects, sort the table by the Display column.
Display Depending on the report type you select, other columns displayed will differ.	Column of check boxes that allow you to display (by checking) or hide (by unchecking) the data series associated with the chosen backhaul. The Prime Performance Manager displays only 10 series, by default.
Clear Selection	Deselects the selected list of series and the **OK** button is grayed out. This is a simple way to deselect all the display check boxes.
OK	Applies the selections you made. If you deselect all items in the dialog box, the **OK** and **Clear Selection** buttons are grayed out.
Cancel	Cancels your selections and closes the Graph Series Editor window.

Viewing Historical Statistics Report Settings

To view the Prime Performance Manager historical statistics:

Step 1 In Prime Performance Manager web interface, in the navigation tree, click **Reports**.

The Report Status window appears as described in Viewing Reports, page 7-4.

Step 2 Click **Report Settings**.

The Historical Stats Report Settings information (Table 7-3) is displayed.

- Click **Disabled** or **Enabled** to change the state of any of the reports.

  Enabling/Disabling reports flag allows you to view the reports (5 minute, 15 minute hourly and daily) at different intervals at the device level.

- Click any field, except the Reports Directory field, to modify its value.

Table 7-3 Historical Statistics Report Settings

Area	Field	Description
General Settings	Reports Directory	Specifies the directory in which Prime Performance Manager reports are stored. You must use the CLI to change the directory in which the reports are stored; you cannot click on this field to modify it.
	Time Mode	Specifies the time mode, either 12-hour or 24-hour, for the reports.
	Master Report Flag	If this option is enabled, the individual report settings are used. If this is option is disabled, all reports are turned off.
	5 Min Report Flag	If this option is enabled/flagged, a 5-minute report is generated.To enable a 5-minute report, you should edit the corresponding XML definition of the report. See Enabling and Disabling Reports, page 7-8 for mode details.
	15 Min Report Flag	If this option is enabled/flagged, a 15-minute report is generated.
	Hourly Report Flag	If this option is enabled/flagged, a hourly report is generated.
	Daily Report Flag	If this option is enabled/flagged, a daily report is generated.
	Weekly Report Flag	If this option is enabled/flagged, a weekly report is generated.
	Monthly Report Flag	If this option is enabled/flagged, a monthly report is generated.
	Export CSV Reports	Specifies whether to automatically generate reports in CSV format.
	Perform Disk Space Checking	Specifies whether disk space checking is enabled or disabled. Usage of disk space increases after each report is enabled. The increase in disk space is specific to each report, number of devices and device configuration. Monitor the usage of disk space and disable the reports for specific devices or decrease the aging value to delete old reports frequently.

Table 7-3 Historical Statistics Report Settings (continued)

Area	Field	Description
Aging Settings	5 Min Stats Aging (Days)	Specifies the database aging value for 5-minute statistics. When records exceed the specified value, they are aged out of the database.
	15 Min Stats Aging (Days)	Specifies the database aging value for 15-minute statistics. When records exceed the specified value, they are aged out of the database.
	Hourly Stats Aging (Days)	Specifies the database aging value for hourly statistics. When records exceed the specified value, they are aged out of the database.
	Daily Stats Aging (Days)	Specifies the database aging value for daily statistics. When records exceed the specified value, they are aged out of the database.
	Weekly Stats Aging (Days)	Specifies the database aging value for week statistics. When records exceed the specified value, they are aged out of the database.
	Monthly Stats Aging (Days)	Specifies the database aging value for monthly statistics. When records exceed the specified value, they are aged out of the database.
	5 Min CSV Aging (Days)	Specifies the database aging value for 5-minute CSV statistics. When records exceed the specified value, they are aged out of the database.
	15 Min CSV Aging (Days)	Specifies the database aging value for 15-minute CSV statistics. When records exceed the specified value, they are aged out of the database.
	Hourly CSV Aging (Days)	Specifies the database aging value for hourly CSV statistics. When records exceed the specified value, they are aged out of the database.
	Daily CSV Aging (Days)	Specifies the database aging value for daily CSV statistics. When records exceed the specified value, they are aged out of the database.
	Weekly CSV Aging (Days)	Specifies the database aging value for weekly CSV statistics. When records exceed the specified value, they are aged out of the database.
	Monthly CSV Aging (Days)	Specifies the database aging value for monthly CSV statistics. When records exceed the specified value, they are aged out of the database.

Managing Report Policies

You can create report policies to customize report attributes for certain device types or individual devices. For example, you might decide if you want to enable or disable reports based on the device type, or set custom report intervals to a device type or specific devices. Devices discovered during device discovery are assigned the standard report policies. However, you can:

- Change the report policy based on the device type. For example, to change the reports generated for all Cisco 7606 routers, you would modify the Cisco7606s report policy.
- Create a new report policy and assign devices to it. For example, if you want to assign the same report policy to a group of devices with different device types, you create the report policy and assign each device to it.

Related Topics

- Editing Report Policy Parameters, page 7-12
- Creating a New Report Policy, page 7-12
- Assigning Devices to Report Policies, page 7-13

Editing Report Policy Parameters

To edit the parameters of an existing report policy:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, click **Reports**.

Step 3 In the Report Policy Editor window, click the **Report Policies** tab.

Step 4 Scroll to the device type group you want to modify and click the **Edit Policy** tool in the Edit Policies column.

The Edit Report Policy: *devicegroup* window appears. This is the same window that is displayed when you click the Report Status tab. However, changes that you make here only apply to the device group that you selected, whereas changes made in the Report Status tab apply to all devices.

Step 5 Modify any of the following:

- Check the reports that you want enabled for this device type.
- Check the report intervals that you want applied to this device group:
  - 5 Minute
  - 15 Minute
  - Hourly
  - Daily
  - Weekly
  - Monthly
  - CSV Only

Note You cannot edit the report policy name of policies created by Prime Performance Manager. These are based on the device types discovered during device discovery.

Step 6 On the Report Policy toolbar, click the **Save Report Policy** tool.

Creating a New Report Policy

To create a new polling group:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, click **Reports**.

Step 3 In the Reports window, click the **Report Policies** tab.

Step 4 On the Report Policy Editor toolbar, click the **Add Report Policy** tool.

Step 5 In the Save Report Policy dialog box, enter the report policy name.

Step 6 Click **OK**.

Step 7 On the Report Policy Editor toolbar, click the **Save Polling Group** tool.

Step 8 Complete the "Editing Report Policy Parameters" procedure on page 7-12 to edit the reports and report intervals that you want for the new report policy.

Assigning Devices to Report Policies

By default, Prime Performance Manager creates device type report policies and assigns devices to them based on their device type. You can create custom report policies and reassign the devices to them.

To assign a device to a custom report policy:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, expand the **Summary Lists** and click **Devices**.

Step 3 In the device table, select the row of the device whose report policy you want to change. To select more than one device, press **Shift** and highlight the device table row.

Step 4 From the Devices window toolbar Actions menu, choose **Edit Report Policy**.

Step 5 In the Edit Report Policy dialog box, choose the report policy that you want to assign. The following options appear:

- The device type report policy. This option is not displayed if you choose multiple devices with different device types.
- This Device Only—If selected, allows you to edit the report policy parameters and assign it to the selected devices.
- Default—Assigns the device(s) to the default report policy.
- Custom groups—If you created report policies, they are displayed.

Step 6 Click **OK**.

Working with Dashboards

Prime Performance Manager dashboards present data from different sources on a single page. For example, the ICMP (Internet Control Message Protocol) application dashboard presents the top ten ICMP hourly packet rates, total errors, total echoes, and echo replies. The CPU/Memory dashboard presents the top ten hourly CPU average and peak utilization as well as the top ten hourly memory pool average and peak utilization. Many dashboards are provided with the Prime Performance Manager package. High-level dashboard categories include:

- Application
- Availablity
- Health
- IP Protocol
- IP QoS
- IPSLA
- Resource

- Response Time
- Transport
- VPDN Statistics
- Video Monitoring Statistics

Note Prime Performance Manager 1.1 includes only some of the dashboard categories listed above.

You can modify the provided Prime Performance Manager dashboards or create new ones. For information, see the *Cisco Prime Performance Manager Integration Developer Guide*.

Editing Dashboard Status

To change the Prime Performance Manager dashboard status, that is, to change the data displayed in the dashboards:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 In the navigation area, click **Dashboards**.

Step 3 In the Dashboard Status Table, check the dashboard item that you do want enabled; uncheck items that you do not want enabled. (By default, all dashboard items are enabled.)

Step 4 On the Dashboard Status Table toolbar, click **Save All Dashboard Entries**.

Items that you enabled are displayed in the navigation tree; items that you disabled are removed.

Editing Dashboard Display

You can change the information displayed in a dashboard at the dashboard level or at the individual data display level.

To change a dashboard display:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 In the navigation area, click **Dashboards**.

Step 3 In the Dashboard tree, click the dashboard item that you want to modify. You can either choose the dashboard, to modify the entire dashboard, or you can choose a dashboard item.

Step 4 From the dashboard toolbar, choose any of the following items to modify the dashboard display:

- Interval—Modifies the dashboard interval:
  - Hourly
  - Daily
  - Weekly
  - Monthly
- Duration—You change the dashboard duration:

  - 12 hours
  - 24 hours
  - 3 days
  - 7 days
- Duration—You change the dashboard duration:
  - 12 hours
  - 24 hours
  - 3 days
  - 7 days

Step 5 To change the date and time range, click the **Change Date and Time Range** tool. (See Customizing Date and Time Ranges, page 3-6.)

Step 6 To change the information display, click **View Chart** or **View Table**, respectively. You can change the display for the entire dashboard, or for individual dashboard elements by clicking the tools within each element.

Step 7 When finished, click the **Run Selected Report for Selected Report Duration** tool.

CHAPTER 8

Using Summary Lists

Prime Performance Manager summary lists provide summary information for areas described in the following topics:

- Using the Devices Summary List, page 8-1
- Using the Device Distributions Summary List, page 8-3
- Using the Alarms Summary List, page 8-3
- Using the Average Poll Response Summary List, page 8-4,
- Using the Uptime Summary List, page 8-5
- Using the SNMP Timeout Alarms Summary List, page 8-7
- Using the Software Versions Summary List, page 8-7
- Using the Gateways and Units Summary List, page 8-7
- Adding and Removing Summary List Table Columns, page 8-9
- Editing Summary List Items, page 8-9

Using the Devices Summary List

The Devices summary list displays information about devices that Cisco Prime Performance Manager has discovered. To display the Devices table, choose **Summary Lists > Devices**. See Table 8-1 to see details of the Devices table.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Table 8-1 Devices Table

Column	Description
Internal ID	Internal ID of the device. The internal ID is a unique ID for every object, which the Prime Performance Manager assigns for its own internal use.
Unit	Name of the unit.
Display Name	Name of the device. This column is displayed by default.
Custom Name	Custom name of the device.

Table 8-1 Devices Table (continued)

Column	Description
IP Address or DNS Hostname	IP address or DNS name of the device, as Prime Performance Manager discovered it.
SysName	System name of the device.
Primary SNMP Address	IP address of the device, which SNMP uses to poll the device. This column is displayed by default.
Device Type	Description of the hardware platform that supports a feature. This column is displayed by default.
Software Version	Version of device's software. This column is displayed by default.
Avg. Poll Response (secs)	Average response time for the device to respond to poll from the Prime Performance Manager server.
Uptime	Time the device has been up, in days, hours, minutes, and seconds. This column is displayed by default.
Reboot Reason	Reason for the last reboot of the device.
Discovery Source	Indicates the source of the device discovery, either PPM (Prime Performance Manager) or Prime Network.
Ignored	Users with authentication level Network Operator (level 3) and higher can edit this field. Users with authentication level Power User (level 2) and higher can edit the Unignore field.
Report Polling	Indicates whether or not report polling is enabled for this device. This column is displayed by default.
Severity	Indicates the alarm severity for the chosen device. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. This column is displayed by default.
Last Status Change	Date and time that the status of the device last changed.
Status	Current status of the device. Possible values are: • Active • Discovering • Polling • Unknown • Unmanaged • Waiting • Warning This column is displayed by default.

Table 8-1 Devices Table (continued)

Column	Description
Status Reason	Reason for the current status of the device. For a full list of possible reasons, see the *stateReasons.html* file. • If you installed Prime Performance Manager Gateway in the default directory, /opt, then the file is located at /opt/CSCOppm-gw/apache/share/htdocs/eventHelp directory. • If you installed the Prime Performance Manager unit in the default directory, /opt, then the file is located at /opt/CSCOppm-gw/apache/share/htdocs/eventHelp directory If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. This column is displayed by default.
Contact	The name of the device contact, if added.
Location	The device location, if added.
Polling Group	The polling group to which the device is assigned. See Chapter 14, “Creating and Editing Device Polling Groups.”
Report Policy	The report policy to which the device is assigned. See Managing Report Policies, page 7-11.

Using the Device Distributions Summary List

The Device Distributions link displays the percentage distribution summary lists. It displays information about device type, total number of devices and their percentage distribution. To display the Device Distributions table, choose **Summary Lists > Device Distributions**. Device Distribution fields include:

- Type—Description of the hardware platform that supports a feature. See the description of Device Type in Using the Devices Summary List, page 8-1 for more information.
- Total (*total number of devices*)—Total number of devices of a particular type.
- Percentage—Percentage of devices of this type out of all the discovered devices.

Using the Alarms Summary List

The Alarms table displays a count of alarms by device and severity. To display the Alarms table, choose **Summary Lists > Alarms**. See Table 8-2 for more details.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Table 8-2 Alarm Descriptions

Column	Tool	Description
Internal ID	—	Internal ID of the device. The internal ID is a unique ID for every object, which Prime Performance Manager assigns for its own internal use. This ID can also be useful when TAC needs to debug problems.
Device	—	Name of the device. When you click any of the device names, the Alarms tab of that device is displayed. This column is displayed by default.
Ignored	—	Users with authentication level Network Operator (level 3) and higher can edit this field. Users with authentication level Power User (level 2) and higher can edit the Unignore field.
Last Status Change	—	Date and time that the status of the device alarms last changed.
Total	—	Total number of alarms for the device. This column is displayed by default.
Critical (*alarm count*) (*alarm percentage*)	⊗	Total number of critical alarms for the device. Click the severity name to sort the page by Critical severity.This column is displayed by default.
Major (*alarm count*) (*alarm percentage*)	▼	Total number of major alarms for the device. Click the severity name to sort the page by Major severity. This column is displayed by default.
Minor (*alarm count*) (*alarm percentage*)	⚠	Total number of minor alarms for the device. Click the severity name to sort the page by Minor severity. This column is displayed by default.
Warning (*alarm count*) (*alarm percentage*)	◆	Total number of warning alarms for the device. Click the severity name to sort the page by Warning severity. This column is displayed by default.
Informational (*alarm count*) (*alarm percentage*)	ⓘ	Total number of informational alarms for the device. Click the severity name to sort the page by Informational severity. This column is displayed by default.
Indeterminate (*alarm count*) (*alarm percentage*)	?	Total number of indeterminate alarms for the device. Click the severity name to sort the page by Indeterminate severity. This column is displayed by default.
Normal (*alarm count*) (*alarm percentage*)	✓	Total number of normal alarms for the device. Click the severity name to sort the page by Normal severity. This column is displayed by default.

Using the Average Poll Response Summary List

The Average Poll Response table display the average time taken (in secs) by a device to respond to the Prime Performance Manager server poll requests. To display the Average Poll Response table, choose **Summary Lists > Average Poll Response**. See Table 8-2 for more details.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Table 8-3 Average Poll Response

Column	Description
Internal ID	Internal ID of the device. The internal ID is a unique ID for every object, which Prime Performance Manager assigns for its own internal use. This ID can also be useful when TAC needs to debug problems.
Unit	Name of the unit.
Display Name	Name of the device.
Primary SNMP Address	IP address of the device, which SNMP uses to poll the device. This column is displayed by default.
Device Type	Description of the hardware platform that supports a feature. See the description of Device Type in Using the Devices Summary List, page 8-1 for more information.
Report Polling	Indicates whether or not report polling is enabled for this device. This column is displayed by default.
Avg. Poll Response (secs)	Average response time for the device to respond to poll from the Prime Performance Manager server.

Using the Uptime Summary List

The Uptime link displays the uptime for managed devices. To display the Uptime for Managed Devices table, choose **Summary Lists > Uptime**. See Table 8-4 for more details.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Table 8-4 Uptime Summary List

Column	Description
Internal ID	Internal ID of the device. The internal ID is a unique ID for every object, which the Prime Performance Manager assigns for its own internal use.
Unit	Name of the unit.
Display Name	The device display name.
Device Type	Description of the hardware platform that supports a feature. See the description of Device Type in Using the Devices Summary List, page 8-1 for more information. This column is displayed by default.
Uptime	Time the device has been up, in days, hours, minutes, and seconds. This column is displayed by default.

Table 8-4 Uptime Summary List (continued)

Column	Description
Reboot Reason	Reason for the last reboot of the device. This column is displayed by default.
Severity	Indicates the alarm severity for the chosen device. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. This column is displayed by default.

Using the Contacts/Locations Summary List

The Contacts/Locations link displays the contacts and locations for managed devices if that information was entered. To display the Contacts/Locations table, choose **Summary Lists > Contacts/Locations**. See Table 8-5 for more details.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Table 8-5 Contacts/Locations Summary List

Column	Description
Internal ID	Internal ID of the device. The internal ID is a unique ID for every object, which the Prime Performance Manager assigns for its own internal use.
Display Name	The device display name.
IP Address or DNS Hostname	IP address or DNS name of the device, as the Prime Performance Manager discovered it.
SysName	System name of the device.
Primary SNMP Address	IP address of the device, which SNMP uses to poll the device. This column is displayed by default.
Device Type	Description of the hardware platform that supports a feature. See the description of Device Type in Using the Devices Summary List, page 8-1 for more information. This column is displayed by default.
Contact	The device contact name. This column is displayed by default.
Location	The device location. This column is displayed by default.

Using the SNMP Timeout Alarms Summary List

The SNMP Timeout Alarms link displays the Devices for Alarm NodeUnreachable table. To display this table, choose **Summary Lists > SNMP Timeout Alarms**. The table displays the same columns as that of Devices Table. See Using the Devices Summary List, page 8-1.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Using the Software Versions Summary List

The Software Versions table lists the software versions for each device Cisco Prime Performance Manager manages.

To access the Software Versions page from the Web interface navigation tree, choose **Summary Lists > Software Versions**. Table 8-6 shows the Software Versions summary table columns.

Note Some table columns are hidden by default. To display a hidden column, see Adding and Removing Summary List Table Columns, page 8-9.

Table 8-6 Software Versions Summary List

Column	Description
Display Name	Name of the device.
Device Type	Description of the hardware platform that supports a feature. See the description of Device Type in Using the Devices Summary List, page 8-1 for more information. This column is displayed by default.
Software Version	Software version used by the device. This column is displayed by default.
Software Description	Full software version information. This column is displayed by default.

Using the Gateways and Units Summary List

The Gateway/Units table lists the number of gateway and unit that are configured on Prime Performance Manager web interface. To view the Gateway/Units table, choose **Summary Lists > Gateway/Units**. Table 8-7 shows the Gateways and Units summary list table columns.

To access a unit or gateway, select a gateway or unit from the table. The unit or gateway details appear on the right content pane.

In the details page, the same number of tabs that is displayed for a unit or gateway, with the exception of the Devices for Unit tab, which appears only for the unit. The Devices for Unit table details are the same as the Device table details. See Using the Devices Summary List, page 8-1 for more information.

Table 8-7 Gateways and Units Summary List

Column	Description
Internal ID	Internal ID of the device. The internal ID is a unique ID for every object, which the Prime Performance Manager assigns for its own internal use.
Display Name	Name of the device.
Custom Name	Custom name of the device.
IP Address or DNS Hostname	IP address or DNS name of the device, as the Prime Performance Manager discovered it.
Primary SNMP Address	IP address of the device, which SNMP uses to poll the device. (There might be other IP addresses on the device that are not the primary SNMP address). This column is displayed by default.
Redundancy Group	If the unit belongs to a redundancy group, the redundancy group name. See Creating Unit Protection Groups, page 13-4.
Primary/Redundant	If the unit belongs to a redundancy group, the unit roll, either primary or redundant.
Type	Description of the type of device (gateway or unit).
Connection Time	Connection time with the server to a unit or gateway.
In Service	Total time the server is in service.
Last Status Change	Date and time that the status of the device last changed.
Status	Current status of the unit or gateway. Possible values are: • Active • Discovering • Polling • Unknown • Unmanaged • Waiting • Warning This column is displayed by default.
Status Reason	Reason for the current status of the device. For a full list of possible reasons, see the *stateReasons.html* file. • If you installed Prime Performance Manager Gateway in the default directory, /opt, the file is located at /opt/CSCOppm-gw/apache/share/htdocs/eventHelp directory. • If you installed Prime Performance Manager unit in the default directory, /opt, then the file is located at /opt/CSCOppm-gw/apache/share/htdocs/eventHelp directory If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip.

Note Only one unit (local unit) at any time can be mapped to a gateway and the other units are distributed and managed by the gateway.

Adding and Removing Summary List Table Columns

Summary list tables contain many columns that are hidden by default. To display hidden columns, and to hide columns that are displayed:

Step 1 Right-click a summary table header.

Step 2 In the list of columns, check the columns that you want display; uncheck columns that you want to hide.

Step 3 At the bottom of the column list, click **Apply**.

Editing Summary List Items

The following actions can be performed by Level 3 or higher users on devices displayed in the Devices, Average Poll Response, Uptime, Contact/Locations, SNMP Timeout Alarms, and Gateway/Units (Edit Properties and Delete only) summary list tables:

- Normal Poll Device—Polls the devices selected in the summary list.
- Edit Properties—Allows you to edit the device display name and default web port. See Using Edit Properties, page 8-10.
- Edit Report Policy—Allows you to change the report policy assigned to the device. See Using Edit Report Policy, page 8-10
- Edit Polling Policy—Allows you to change the polling policy assigned to the device. See Using Edit Report Policy, page 8-10.
- Edit SNMP IP Addresses—Allows you to edit a device SNMP IP addresses. See Using Edit SNMP IP Addresses, page 8-11.
- Relocate Device—Allows you to relocate a device from one unit to another. See Using Relocate Device, page 8-11.
- Disable/Enable Sending Alarms (Release 1.1.1 only)—Disables or enables sending alarms from the selected device.
- Manage/Unmanage—Allows you to change unmanaged devices to managed, and managed devices to managed.
- Delete—Deletes the chosen object.

Using Edit Properties

Actions > Edit Properties opens the Edit Properties window. Options include:

- Name—Name of the device. The name is green for valid inputs and red for invalid inputs. The name may include up to 100 alphanumeric and the special characters hyphen (-), underscore (_), period (.), and colon (:). If you enter an invalid name, the Save option is disabled. After saving, the new name is displayed in the navigation tree and in the Details panel. The character '.' is allowed only when the resulting name is a valid hostname.
- Default Web Port—The default port for web connections.
- Save—Saves the changes you have made.
- Restore—Restores the changes that you make to the fields of the Edit Properties dialog box.
- Cancel—Closes the window without saving the changes you have made.

Using Edit Report Policy

Actions > Edit Report Policy opens the Edit Report Policy dialog box. Options include:

- Report Policy—Allows you to assign a different report policy to the device. For information about creating report policies, see Managing Report Policies, page 7-11.
- Save—Saves the changes you have made.
- Cancel—Closes the dialog box without saving the changes you have made.

Using Edit Polling Group

Actions > Edit Polling Group opens the Polling Group Details dialog box. Options include:

- Polling Policy—Allows you to assign a different polling policy to the device. For information about creating and editing polling policies, see Chapter 14, "Creating and Editing Device Polling Groups."
- Polling Interval—The polling interval configured in the polling policy. If you choose This Device Only, the field is editable.
- Polling Interval—The polling interval in minutes configured in the polling policy. Polling Interval is not editable unless you choose This Device Only in the Polling Policy field.
- Timeout—The timeout duration in seconds configured in the polling policy. Timeout is not editable unless you choose This Device Only in the Polling Policy field.
- Retries—The number of times Prime Performance Manager will retry a connection after a timeout configured in the polling policy. Retries is not editable unless you choose This Device Only in the Polling Policy field.
- Save—Saves the changes you have made.
- Cancel—Closes the dialog box without saving the changes you have made.

Using Edit SNMP IP Addresses

Note The Actions menu Edit SNMP IP Addresses option opens Cisco Prime Performance Manager: Edit SNMP IP Addresses window. Edit SNMP IP Addresses properties are shown in Table 8-8.

Note The Edit SNMP IP Addresses option is available only for the users with authentication Level 5.

Table 8-8 Edit SNMP Address Window

Field or Button	Description
Available IP Addresses	List of all IP addresses not associated with SNMP for polling.
IP Addresses for SNMP	Lists the IP addresses associated with the device, including the primary SNMP address and all backup IP addresses, that are intended for SNMP.
Add	Adds the IP Addresses from the Available IP Address box to the IP Addresses for SNMP box. This option is disabled if there is no IP address in the Available IP Address box.
Remove	Removes the IP Addresses from the IP Addresses for SNMP box and adds them to the Available IP Addresses box. This option is disabled if there is no IP address in the IP Addresses for SNMP box.
Raise	Moves the selected IP address up one level in the IP Addresses for SNMP box. This option is disabled if there is only one IP address in the IP Addresses for SNMP box.
Lower	Moves the selected IP address down one level in the IP Addresses for SNMP box. This option is disabled if there is only one IP address in the IP Addresses for SNMP box.
Save	Saves the changes you have made.
Cancel	Closes the window without applying any changes you have made.

Using Relocate Device

The Relocate Device action opens Cisco Prime Performance Manager: Relocate Device window. Relocate Device options are shown in Table 8-9.

Table 8-9 Relocate Device Window

Field	Description
Unit	Drop-down that lists the configured unit that can be used by a device to relocate.
Save	Saves the changes that you have made.
Cancel	Closes the window without applying any changes that you have made.

CHAPTER 9

Using Alarms and Events

The following topics provide information about using the Cisco Prime Performance Manager alarms and events:

- Displaying Active Alarms and Event History, page 9-1
- Active Alarms and Event History Toolbar, page 9-4
- Filtering Alarms and Events, page 9-7
- Viewing Alarms and Events Properties, page 9-9
- Attaching Notes to Alarms or Events, page 9-12

Displaying Active Alarms and Event History

Active Alarms and Event History allows to view a network summary of active alarms and historical events. The contents of the Active Alarms window and the Event History window are very similar in appearance. However, the Active Alarms table shows fewer entries than the Event History table because multiple events are associated with a single alarm.

Note The appearance and the contents displayed in the Events and Alarms tab are not the same while viewing reports at the device level. For more information see Working With Reports and Dashboards, page 7-1

To see a summary of all active alarms, in the Prime Performance Manager web interface, in the navigation tree click **Active Alarms**. Active alarms are displayed in the right pane and includes basic information for each active alarm. Prime Performance Manager updates the alarm information at least once a minute. For information about the Active Alarms display, see Active Alarms and Event History Toolbar, page 9-4

To see a summary of recent events, in the navigation tree click **Event History**. Events are displayed in the right pane. For more information about the Event History display, see Active Alarms and Event History Toolbar, page 9-4

If you select a device in the navigation tree and click the Alarms or Events tab, the Prime Performance Manager displays alarms or events information for only that device.

The select multiple alarms or events in the table, check the check box for the alarm or event in the far left column. To clear the selection, from the toolbar, click **Clear Selection**. You can use the Shift key to select multiple rows. To clear the selection, left-click anywhere in the table. For more information about sorting, displaying, or hiding columns, see Navigating Table Columns, page 3-8.

Table 9-1shows the Active Alarms, Alarms tab, Event History, and Events tabs details.

Table 9-1 Active Alarms and Event History

Column	Description
Internal ID	Internal ID of the alarm or event. The internal ID is a unique ID that Prime Performance Manager assigns for its own internal use. This ID can also be useful when the Cisco Technical Assistance Center (TAC) needs to debug problems.
Ack	Indicates whether the alarm or event is acknowledged. To acknowledge an unacknowledged alarm or event, click the Acknowledge toolbar tool. To make a previously acknowledged event unacknowledged, click the Unacknowledged toolbar tool. This column is displayed by default.
Name	The name of the alarm or event. This column is displayed by default under Active Alarms and Alarms tab.
Alarm Nature	The alarm nature. The alarm nature is determined when the alarm is created. The valid values are: • ADAC—Automatically detected and automatically cleared • ADMC—Automatically detected and manually cleared • Undefined—Undefined This column is under Active Alarms and Alarms tab.
Alarm Type	The alarm type. Valid values are: • Communications • Processing Error • Environmental • QOS • Equipment • Undefined
Element Name	The network element name associated with the event.

Table 9-1 Active Alarms and Event History (continued)

Column	Description
Category	The event category. Default values include: • Create—Creation event, such as the creation of a seed file. • Delete—Deletion event, such as the deletion of an object or file. • Discover—Discovery event, such as Discovery beginning. • Edit—Edit event. A user has edited an object. • Ignore—Ignore event. A user has ignored a link or linkset. • Login—Login event. A user has logged into Prime Performance Manager. • LoginDisable—LoginDisable event. The Prime Performance Manager has disabled a user’s User-Based Access authentication because of too many failed attempts to log into Prime Performance Manager. • LoginFail—LoginFail event. An attempt by a user to log into Prime Performance Manager has failed. • Logout—Logout event. A user has logged out of Prime Performance Manager. • OverWrite—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • Poll—Poll event, such as an SNMP poll. • Purge—Purge event. A user has requested Discovery with Delete Existing Data selected, and Prime Performance Manager has deleted the existing Prime Performance Manager database. • Status—Status change message generated. • Request—A request is created for every user-initiated action that generates a request from the gateway to a unit.
Severity	The alarm or event severity. Severities include: Critical Major Minor Warning Normal Indeterminate Informational **Note** You cannot change the severity of an event.
Original Severity	The original severity of the event.
Count	The number of events in the sequence of events for an alarm.
Note	Indicates whether a note is associated with the event.
Create Time CST	Central Standard Time (CST) at which this event was received. This column is displayed by default in the Event History window and the Events tab.

Table 9-1 Active Alarms and Event History (continued)

Column	Description
Create Time (Device Time Zone)	Device time zone at which the event was received.
Change Time CST	Central Standard Time (CST) at which this event was last updated.
Change Time (Device Time Zone)	Device time zone at which the event was updated.
Ack By	• If you did not implement the Prime Performance Manager User-Based Access, the name of the device that last acknowledged the event. • If you implemented the Prime Performance Manager User-Based Access, the name of the user who last acknowledged the event. • If no one acknowledged the event, this field is blank.
Ack Time CST	Time at which the event was acknowledged.
Ack Time (Device Time Zone)	Device time zone at which the event was acknowledged.
Clear By	User who cleared the event. This column is in Active Alarms and Alarms tab and is hidden by default.
Clear Time	Time at which the event was cleared. This column is in Active Alarms and Alarms tab.
Clear Time (Device Time Zone)	Device time zone at which the event was cleared. This column is in Active Alarms and Alarms tab and is hidden by default.
Device	Name of the device associated with the alarm or event. If no device is associated with the alarm or event, None appears.
Device type	The device type.
Message	Message associated with the alarm or event.

Active Alarms and Event History Toolbar

The Active Alarms and Event History displays include a toolbar that you can use to manage the alarms or events display. Table 9-2 lists the tools and their functions.

Table 9-2 Alarms and Event History Toolbar

Tool	Name	Description
▽	Modify Event Filter	Opens the Prime Performance Manager Alarm and Event Filter dialog box.
▽	Remove Filter	Activates and deactivates the event filter specified in the Event Filter dialog box. If: • The filter is activated, Prime Performance Manager shows only those alarms or events that pass the filter. • The filter is deactivated, Prime Performance Manager shows all alarms or events. If you activate a filter in an object’s Recent Events table in the Prime Performance Manager main window, the filter is activated in all Recent Events tables in the Prime Performance Manager main window for all other objects.
—	Archived (web interface only)	Appears in the tool bar when you view the Event History table or the Active Alarms table. Click the Archived button to display a table of archived events or alarms. This button works as a toggle, so you can use it to switch back and forth. ⚠ **Caution** You can limit the number of rows in the archived events table by editing the MaxArchivedRecords property in the etc/SgmEventLimits.conf file. The default value is 200,000. Increasing it can significantly impact server performance.
⟳	Refresh	Forces a refresh of the current web page. Click this icon to refresh the current page.
⏸	Pause or Resume	Pauses or resumes the table. While the table is paused, Prime Performance Manager does not display new alarms or events (unless you apply a filter or edit your preferences). When the table is resumed, all new alarms or events that occurred after the table was paused are added to the display. If alarms or events are deleted while the table is paused, they are not removed from the table. Instead, they are dimmed and cannot be acknowledged or edited. Deleted alarms or events are removed from the table when you resume the table.
N/A	All	Filters the page by all severities.
✖	Critical (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Critical severity. This opens the Active Alarms filtered by Critical Severity page. The alarm count and the alarm percentage are not displayed in the Event History table.
!	Major (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Major severity. This opens the Active Alarms filtered by Major Severity page. The alarm count and the alarm percentage are not displayed in the Event History table.
⚠	Minor (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Minor severity. This opens the Active Alarms filtered by Minor Severity page. The alarm count and the alarm percentage are not displayed in the Event History table.
◆	Warning (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Warning severity. This opens the Active Alarms filtered by Critical Severity page. The alarm count and the alarm percentage are not displayed in the Event History table.

Table 9-2 Alarms and Event History Toolbar (continued)

Tool	Name	Description
ℹ	Informational (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Informational severity. This opens the Active Alarms filtered by Critical Severity page. Filtering the page by alarm informational severity, allows the user to determine the status of a device. The alarm count and the alarm percentage are not displayed in the Event History table.
?	Indeterminate (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Indeterminate severity. This opens the Active Alarms filtered by Indeterminate Severity page. The alarm count and the alarm percentage are not displayed in the Event History table.
☑	Normal (*alarm count*) (*alarm percentage*)	Filters the page to include only the alarms with Normal severity. This opens the Active Alarms filtered by Normal Severity page. The alarm count and the alarm percentage are not displayed in the Event History table.
✓	Acknowledge	Acknowledges the selected alarms or events.
✓	Unacknowledge	Unacknowledges the selected alarms or events.
🔔	Clear	Clears the chosen alarms in the Active Alarms table. When you clear an alarm, the alarm no longer affects the severity of the object (its severity changes to normal), but the alarm remains visible in the Active Alarms table. This option is not available for events.
🗑	Delete	Deletes the chosen alarms or events. When you delete an alarm or event, you remove it from the table, and Prime Performance Manager archives the alarm or event in its database. Also, the alarm or event, no longer affects the severity of the object.
🗑	Clear and Delete	Clears the chosen alarms and also deletes them from the Active Alarms table. Use the **Clear** and **Delete** button if you need to designate an alarm as Manually Cleared before deleting it. When you use the **Clear** and **Delete** button, Prime Performance Manager changes the alarm severity of the object to normal, sends an alarm log message to /opt/CSCOppm-gw/logs/messageLog.txt, and sends a trap to a northbound host to indicate that the alarm cleared. This option is not available for events.
🔍	Event Properties	Opens the Alarm and Event Properties window, Properties tab.
📄	Events for Alarm	Launches a dialog box that shows a table of events that are associated with the selected alarm. (This button is only available in alarm tables.)
📒	Edit Notes	Opens the Alarm and Event Properties window, Notes tab.

Table 9-2 Alarms and Event History Toolbar (continued)

Tool	Name	Description
🕒	Time Difference	Shows the time difference in days, minutes, hours, and seconds between two alarms or events. • In the client interface, use the Ctrl key to select two alarms or events. • In the web interface, check the check boxes of two alarms or events. Then click the Time Difference button.
➡	Export the report as a CSV file	Exports the alarms and events related table data to a report with comma-separated values (CSV file). You can save this file to disk or open it with an application that you choose (for example, Microsoft Excel).
?	Help for Event	Shows context-sensitive help for the chosen alarm or event in a separate browser window. For TCAs, displays the View Threshold dialog box.
	Report for Event	If a TCA is selected, launches the associated report.

Filtering Alarms and Events

You can use the Modify Event Filter to change the alarm or event information appears.

To change the alarms or events display, in the navigation tree, choose **Active Alarms** or **Event History**, then click the Modify event filter tool. The Prime Performance Manager Alarm and Event Filter dialog box appears. The dialog box allows you to set filtering options based on three areas:

- Categories
- Severities
- Other

Use the Categories pane to specify the alarm or event categories you want to display. The following categories are available:

- Status
- Create
- Delete
- Discover
- Edit
- Ignore
- Login
- LoginDisable
- LoginFail
- Logout
- OverWrite
- Poll
- Purge
- Request

All categories are checked by default. You can click **Deselect All**, or **Select All** to select or deselect all categories.

Note These are the default categories; additional categories might be defined by the Prime Performance Manager system administrator.

The Severities pane allows you to specify which alarm/event severities you want to display. Severities include:

- Informational
- Normal
- Indeterminate
- Warning
- Critical
- Minor
- Major

The Alarm and Event Filter dialog box Other pane allows you to further define the alarms and events filter. These settings are applied to all alarms/events displays in the current view. Table 9-3 describes the options in the Other pane.

Table 9-3 Alarm and Event Filter Dialog Box Other Pane

Field	Description
Acknowledged	Check box indicating whether only acknowledged alarms/events appear in the Active Alarms/Event History window. This check box is checked by default.
Unacknowledged	Check box indicating whether only unacknowledged alarms/events appear in the Active Alarms/Event History window. This check box is checked by default.
Time Before	Check box indicating whether only alarms/events that Prime Performance Manager logs before a specified date and time, appear in the Active Alarms/Event History window. This check box is unchecked by default.
Time Before	Specifies the date and time prior to which alarms/events that Prime Performance Manager logs appear in the Active Alarms/Event History window. This field is dimmed unless the Time Before check box is checked.
Time After	Check box indicating whether only alarms/events that Prime Performance Manager logs after a specified date and time, appear in the Active Alarms/Event History window. This check box is unchecked by default.
Time After	Specifies the date and time after which alarms/events that Prime Performance Manager logs appear in the Active Alarms/Event History window. This field is dimmed unless the Time After check box is checked.
Name or Message Matches	Check box indicating whether only alarms/events that contain the specified message text appear in the Active Alarms/Event History window. This check box is unchecked by default. The Name or Message Matches field value is retained after a message filter is set.

Table 9-3 Alarm and Event Filter Dialog Box Other Pane (continued)

Field	Description
Match Case	Indicates whether only alarms/events that match the case of the text in the Name or Message Matches field should appear in the Active Alarms/Event History window. This field is dimmed unless Name or Message Matches is selected. Match Case default is not selected by default if Name or Message Matches is selected. Match Case is disabled if Match Regex is selected. The Active Alarms/Event History table is filtered properly, based on the text entered in the Name or Message Matches text box (case sensitive), if Match Case is selected. The Match Case selection is retained after a message filter is set.
Match Regex	Check box indicating whether only alarms/events that match the regular expression of the text in the Name or Message Matches field should appear in the Active Alarms/Event History window. This field is dimmed unless the Name or Message Matches check box is checked. Match Regex is unchecked by default, if the Name or Message Matches check box is checked. Match Regex is disabled if the Match Case check box is checked. The Active Alarms/Event History table is filtered properly, based on the regular expression entered in the Name or Message Matches text box (case-sensitive), if the Match Regex check box is selected. The check box Match Regex is selected after a message filter is checked. **Note** If invalid regex is provided, then Active Alarms/Event History table does not contain any rows.
Suppress for unmanaged devices	Check box to suppress alarms/events for any objects that have been set to the unmanaged state. To suppress alarms/events for unmanaged objects, check the check box. To retain alarms/events for unmanaged objects, uncheck the check box. **Note** If you are viewing alarms/events for a specific object in the navigation tree of Prime Performance Manager main window, this button is not available.

Viewing Alarms and Events Properties

You can use Prime Performance Manager to view detailed information about a chosen alarm or event, including its associated object, status, and other information. To view detailed information about an alarm or event, in the Web interface, check the alarm or event check box, then in the toolbar, click the **Event Properties** 🔍. The Event Properties dialog box appears. Table 9-4 lists the alarms and event properties.

Table 9-4 Alarms and Event Properties

Tab, Field, or Button	Description
Message	Message text for the alarm or event.
Properties	Shows detailed information about the chosen alarm or event.

Table 9-4 Alarms and Event Properties (continued)

Tab, Field, or Button	Description
Notes	Shows notes associated with this alarm or event. If no note is currently associated with the alarm or event, this field displays No Notes. In the Notes tab, the date and time the Notes field for this alarm or event was last updated is displayed. If no note is currently associated with the alarm or event, this field displays Not Set.
Details	Shows specific alarm or event attributes.
Events for Alarm	Shows a table of events associated with the selected alarm. (This tab does not appear in the Event Properties dialog box if it is selected through the Event History link.)
Category	Type of the alarm or event. Default values are: • **Create—**Creation event, such as the creation of a seed file. • **Delete**—Deletion event, such as the deletion of an object or file. • **Discover**—Discovery event, such as Discovery beginning. • **Edit—**Edit event. A user has edited an object. • **Ignore**—Ignore event. A user has ignored a link or linkset. • **Login**—Login event. A user has logged into Prime Performance Manager. • **LoginDisable**—LoginDisable event. The Prime Performance Manager has disabled a user’s User-Based Access authentication as a result of too many failed attempts to log into Prime Performance Manager. • **LoginFail**—LoginFail event. A user’s attempt to log into Prime Performance Manager has failed. • **Logout**—Logout event. A user has logged out of Prime Performance Manager. • **OverWrite**—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • **Poll**—Poll event, such as an SNMP poll. • **Purge—**Purge event. A user has requested Discovery with Delete Existing Data selected, and the Prime Performance Manager has deleted the existing Prime Performance Manager database. • **Request**—Request event. A user has initiated an action that generates a request from the gateway to a unit. • **Status**—Status change message generated.

Table 9-4 Alarms and Event Properties (continued)

Tab, Field, or Button	Description
Severity	Severity of the alarm or event. Possible severities are: ✖ Critical ! Major ! Minor ! Warning ✓ Normal ? Indeterminate i Informational
Original Severity	Original severity of the alarm or event.
Create Time	Date and time the event was logged.
Change Time	Date and time the alarm last changed. This field is important only for alarms.
Acknowledged	Indicates whether the alarm or event has been acknowledged.
Acknowledged By	Name of the device that last acknowledged the alarm or event. If no one has acknowledged the alarm or event, this field is not shown.
Acknowledge Time	Time at which the event was acknowledged.
Cleared By	User who cleared the event.
Clear Time	Time at which the event was cleared.
Internal ID	Internal identification that the Prime Performance Manager uses for the alarm or event.
Name	Name for the alarm or event, for example, InterfaceState.
Alarm Nature	Nature of the alarm.
Alarm Type	Type of the alarm.
Count	Number of events in the sequence of events for an alarm. This field is important only for alarms because an event count will always be 1.
Element Name	Name of the managed element, for example, the device name.
Device	Name of the device associated with the alarm or event.
Create Time (Device Time Zone)	Device time zone at which the event was received.
Change Time (Device Time Zone)	Device time zone at which the event was updated.
Acknowledge Time (Device Time Zone)	Device time zone at which the event was acknowledged.
Clear Time (Device Time Zone)	Device time zone at which the event was cleared.

Attaching Notes to Alarms or Events

You can use Prime Performance Manager to add notes to alarms and events. To add a note to an alarm or event, in the Web interface, select an alarm or event checking its check box, then click **Edit Notes**. The Event Properties dialog box appears with the Notes tab selected. See Table 9-5 for more detail.

Note You can add a note to an alarm or event by using either the Prime Performance Manager web interface. You can also view the note from either interface.

Table 9-5 Alarms/Events Notes Attachment

Field or Button	Description
Name	Message text of the alarm or event.
Last Update	Date and time the Notes field for this alarm or event was last updated. If no note is currently associated with this alarm or event, this field shows the value Not Set. You cannot edit this field.
Notes	Notes to associate with this alarm or event. In this field, you can enter any important information about the alarm or event, such as its associated object, what triggered the alarm or event, how often it has occurred, and so on.
Edit Note	Enables you to edit or add a note.
Save	Saves changes you have made to the alarm or event information.
Cancel	Cancels the operation without saving any changes.
Help	Shows Online help for the current window.

Related Topic

Viewing Alarms and Events Properties, page 9-9

CHAPTER 10

Configuring Thresholds

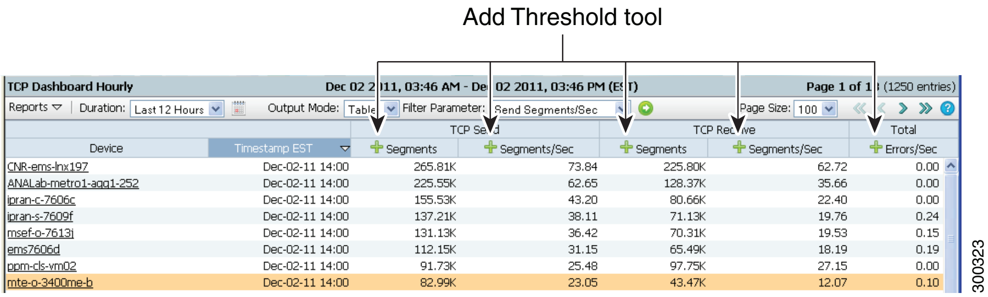
The following topics provide information about configuring thresholds in Cisco Prime Performance Manager:

- Creating Thresholds in Prime Performance Manager, page 10-1
- Managing Thresholds, page 10-4

Creating Thresholds in Prime Performance Manager

Prime Performance Manager allows you to create thresholds to generate alarms when a given report key performance indicator (KPI) rises or falls to a specified point. Threshold-eligible report KPIs are identified by Add Threshold tools in the report KPI column header. Figure 10-1 shows an example.

Figure 10-1 Add Threshold Tools



TCP Dashboard Hourly — Dec 02 2011, 03:46 AM - Dec 02 2011, 03:46 PM (EST) — Page 1 of 13 (1250 entries)

Reports | Duration: Last 12 Hours | Output Mode: Table | Filter Parameter: Send Segments/Sec | Page Size: 100

		TCP Send		TCP Receive		Total
Device	Timestamp EST	Segments	Segments/Sec	Segments	Segments/Sec	Errors/Sec
CNR-ems-lnx197	Dec-02-11 14:00	265.81K	73.84	225.80K	62.72	0.00
ANALab-metro1-agg1-252	Dec-02-11 14:00	225.55K	62.65	128.37K	35.66	0.00
ipran-c-7606c	Dec-02-11 14:00	155.53K	43.20	80.66K	22.40	0.00
ipran-s-7609f	Dec-02-11 14:00	137.21K	38.11	71.13K	19.76	0.24
msef-o-7613j	Dec-02-11 14:00	131.13K	36.42	70.31K	19.53	0.15
ems7606d	Dec-02-11 14:00	112.15K	31.15	65.49K	18.19	0.19
ppm-cls-vm02	Dec-02-11 14:00	91.73K	25.48	97.75K	27.15	0.00
mte-o-3400me-b	Dec-02-11 14:00	82.99K	23.05	43.47K	12.07	0.10

To create a threshold, you provide the KPI onset and abate points. Onset is the rising or falling KPI value that, when reached, generates an alarm. Abate is he rising or falling KPI value that, when reached, clears the alarm. Additionally, you can specify the type of alarm you want raised, the days and times you want the threshold to run, and the number of required threshold-crossing occurrences before the alarm is raised or cleared.

As you prepare to create thresholds in Prime Performance Manager, keep the following in mind:

- Prime Performance Manager validates your threshold entries based on the KPI type, either rising or falling. For a rising threshold, for example interface availability up percentage, the higher alarm threshold value must be greater than the lower alarm. For a falling threshold, for example, interface availability up percentage, the higher alarm threshold must be lower than the one entered for the lower alarm.

- To avoid flooding the system with alarms, testing thresholds on a small group of devices before rolling them out to the full network is recommended.
- To avoid alarm flapping, set the abate value at a reasonable distance from the onset value. The distance depends on the expected KPI fluctuation. KPIs with larger fluctuations should have a wider onset-to-abate gap than KPIs with smaller fluctuations.
- Prime Performance Manager displays Add Threshold tools for any threshold-capable KPI, and excludes report data that cannot have thresholds created, such as name and description.

To create a Prime Performance Manager threshold.

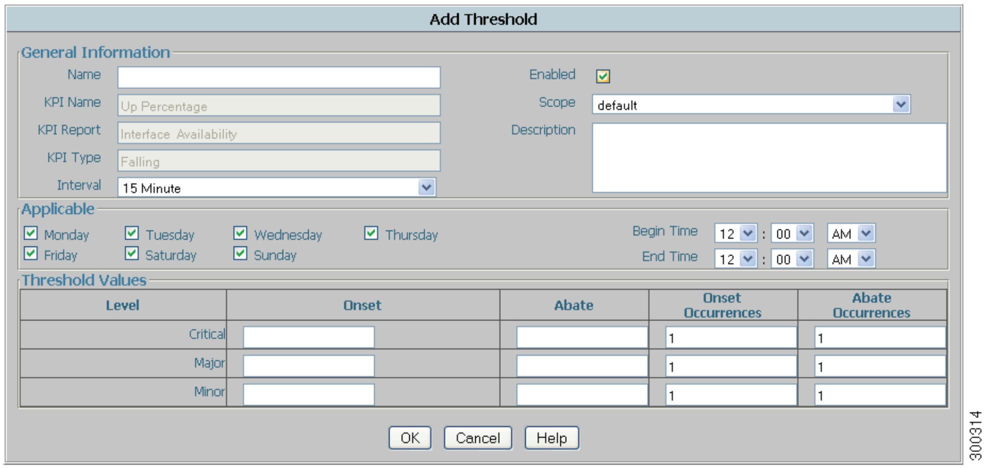
Step 1 Log into Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the Reports navigation area, display the report containing the KPI for which you want to create a threshold.

Step 3 After the report is displayed, click the Add Threshold tool in the KPI column header.

The Add Threshold dialog box appears (Figure 10-2).

Figure 10-2 Add Threshold Dialog Box



Add Threshold

General Information

Name:

KPI Name: Up Percentage

KPI Report: Interface Availability

KPI Type: Falling

Interval: 15 Minute

Enabled ☑

Scope: default

Description:

Applicable

☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday

☑ Friday ☑ Saturday ☑ Sunday

Begin Time 12 : 00 AM

End Time 12 : 00 AM

Threshold Values

Level	Onset	Abate	Onset Occurrences	Abate Occurrences
Critical			1	1
Major			1	1
Minor			1	1

Step 4 Enter the threshold parameters:

- Name—Enter a unique name for the threshold.
- KPI Name—Is automatically generated from the report attribute name. It cannot be edited.
- KPI Report—Is automatically generated from the report name. It cannot be edited.
- KPI Type—Indicates the KPI type, either rising or falling. It cannot be edited. For a rising threshold, the critical alarm threshold must be higher than the major alarm threshold, and the major alarm threshold must be higher than the minor alarm. For falling KPI thresholds, the critical alarm entry must be lower than the major alarm, and the major alarm must be lower than the minor alarm.
- Interval—Choose the time interval. The time interval is the frequency at which Prime Performance Manager will check the data point value identified by the threshold. Threshold intervals include:
  - 5 Minute
  - 15 Minute (default)
  - Hourly

- Daily
- Weekly
- Monthly

Note Verify that the report has these intervals enabled. Be default, Prime Performance Manager 15-minute, hourly, daily, weekly, and monthly intervals are enabled. To run a threshold every 5 minutes, you must enable 5-minute report interval. For information about configuring reports, see Chapter 7, "Working With Reports and Dashboards."

- Enabled—The threshold is enabled by default. If you want to create the threshold but do not want to enable it, uncheck this box. You can enable the threshold later on the Threshold Editor window. For example, you might want to create all the thresholds first, review them in the Thresholds Editor window, then enable them at one time. For information about Thresholds Editor, see **Managing Thresholds, page 10-4.**
- Scope—Set the threshold scope. The scope indicates the devices for which you want the threshold reported. The "default" value means report the threshold for any reportable device. You can set the scope for a subset of devices, for example, you can choose Cisco7606s to report the threshold only for Cisco 7606 routers, and so on. The device groups that appear come from the Polling Groups tab. Device groups are based on the device types that are found during device discovery.
- Description—Add any notes, as needed, to help describe the threshold. The field accepts any alphanumeric text.
- Days—Enter the days for which you want the threshold applied. For example, you might only want to check some thresholds once a week, in which case, you would pick the day of the week when you want the threshold to apply.
- Hours—Enter the time period (hours and minutes) for which you want the threshold applied. If you enter the same value, the threshold is always applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical:
  - Onset—Enter the onset threshold value(s) in the alarm box(es) that you want raised. You can set values for any or all alarm types. However, alarm entries must match the KPI type. For a rising KPI, the critical alarm threshold entry must be higher than the major alarm, and the major alarm threshold must be higher than the minor alarm. For a falling KPI type, the critical alarm threshold must be lower than the major alarm, and the major alarm must be lower than the minor alarm.
  - Abate—Enter the threshold value in the box of the alarm(s) when you want the alarm cleared. For a rising KPI type, the abate value must always be lower than the onset value. For a falling KPI type, the abate value must be lower than the onset.
  - Onset Occurrences—Enter the number of onset threshold crossings that must occur before the alarm is raised.
  - Abate Occurrences—Enter the number of abate occurrences that must occur before the alarm is cleared.

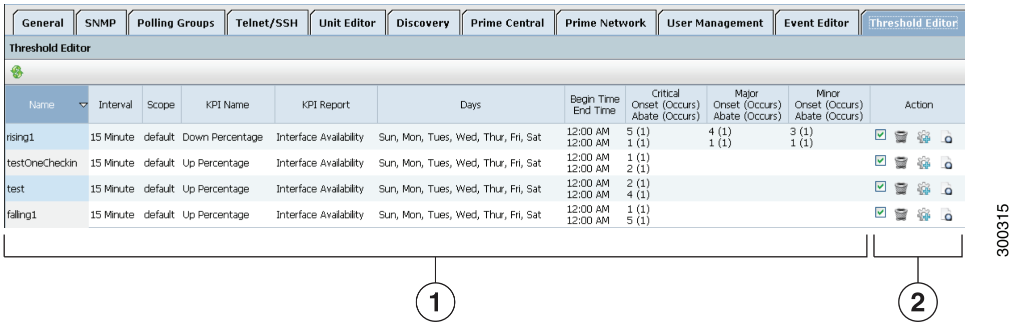
Step 5 Click **OK**.

The TCA is added to the gateway thresholds. To view and edit the thresholds, click **Administrative** > **Threshold Editor**. For more information, see Chapter 10, "Managing Thresholds."

Managing Thresholds

Prime Performance Manager thresholds can be viewed, edited, disabled, enabled, and deleted from the Administrative > Thresholds Editor tab, shown in Figure 10-3. The editor displays thresholds added from the Prime Performance Manager reports GUI (see To create a Prime Performance Manager threshold., page 10-2), and ones created using an XML editor and added directly to the gateway.

Figure 10-3 Edit Thresholds Tab



Name	Interval	Scope	KPI Name	KPI Report	Days	Begin Time End Time	Critical Onset (Occurs) Abate (Occurs)	Major Onset (Occurs) Abate (Occurs)	Minor Onset (Occurs) Abate (Occurs)	Action
rising1	15 Minute	default	Down Percentage	Interface Availability	Sun, Mon, Tues, Wed, Thur, Fri, Sat	12:00 AM 12:00 AM	5 (1) 1 (1)	4 (1) 1 (1)	3 (1) 1 (1)	☑
testOneCheckin	15 Minute	default	Up Percentage	Interface Availability	Sun, Mon, Tues, Wed, Thur, Fri, Sat	12:00 AM 12:00 AM	1 (1) 2 (1)			☑
test	15 Minute	default	Up Percentage	Interface Availability	Sun, Mon, Tues, Wed, Thur, Fri, Sat	12:00 AM 12:00 AM	2 (1) 4 (1)			☑
falling1	15 Minute	default	Up Percentage	Interface Availability	Sun, Mon, Tues, Wed, Thur, Fri, Sat	12:00 AM 12:00 AM	1 (1) 5 (1)			☑

1	Threshold values	**2**	Threshold actions: Enable/Disable, Delete, Edit

Related Topics

Editing Thresholds, page 10-4

Enabling and Disabling Thresholds, page 10-5

Deleting Thresholds, page 10-5

Viewing Thresholds Parameters and Reports from the Alarms Window, page 10-6

Viewing Threshold Events, page 10-7

Editing Thresholds

To edit a threshold.

Step 1 Log into Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click **Threshold Editor**.

Step 4 In the Actions column of the threshold you want to edit, click **Edit This [*Rising/Falling*] Threshold**.

Step 5 In the Edit Thresholds dialog box, edit any of the following values. For detailed descriptions, see Creating Thresholds in Prime Performance Manager, page 10-1.

- Name—The threshold name.
- KPI Name—Cannot be edited.
- KPI Report—Cannot be edited.
- KPI Type—Cannot be edited.

- Interval—The threshold time interval:
- Scope—The threshold scope.
- Enabled—Enables the threshold.
- Description—Threshold text description.
- Days—The days when the threshold is applied.
- Hours—The time period (hours and minutes) when the threshold is applied.
- Threshold Values—The threshold onset, abate, and number of occurrence values for the alarms that are raised.

Step 6 When finished, click **OK**.

The edits are displayed in the Thresholds Editor.

Enabling and Disabling Thresholds

To enable or disable a threshold:

Step 1 Log into Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click **Threshold Editor**.

Step 4 In the Actions column of the threshold you want to enable or disable, check (enable) or uncheck (disable) the **Enable This Threshold** check box.

Prime Performance Manager will update the threshold information.

Note You can also enable and disable thresholds using the "Editing Thresholds" procedure on page 10-4.

Deleting Thresholds

To delete a threshold:

Step 1 Log into Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click **Threshold Editor**.

Step 4 In the Actions column of the threshold you want to delete, click the **Delete This Threshold** tool.

Step 5 On the confirmation, click **OK**.

Prime Performance Manager will remove the threshold from the table.

Viewing Thresholds Parameters and Reports from the Alarms Window

From the Prime Performance Manager Alarms window can perform the following perform the following actions from a threshold crossing alarm:

- View threshold parameters (all users).
- Edit threshold parameters (administrator users only).
- View a report for the threshold crossing (all users).

When threshold crossing alarms occur, you can view the threshold parameters from the Alarms window:

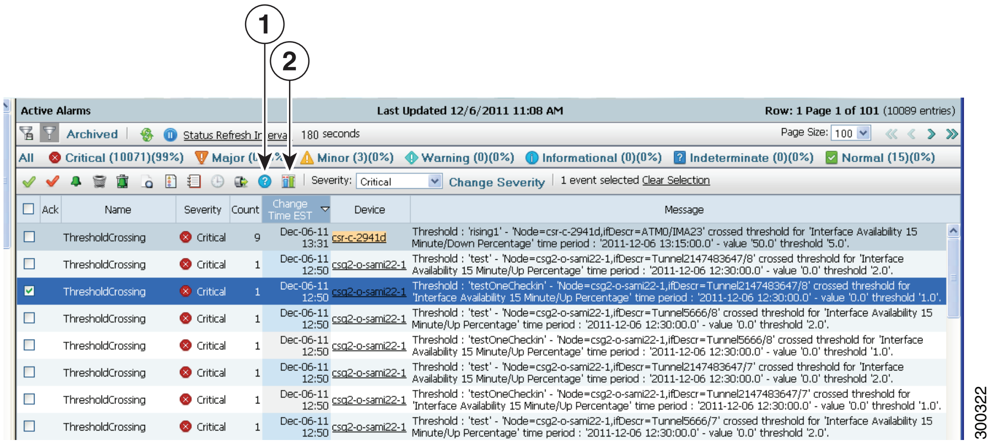
Step 1 Log into the Prime Performance Manager GUI.

Step 2 Click **Active Alarms**.

Step 3 Select a Threshold Crossing alarm.

Step 4 In the Alarms window toolbar, click **Help for Event**.

Figure 10-4 Displaying Threshold Parameters from the Alarms Window



☐	Ack	Name	Severity	Count	Change Time EST	Device	Message
☐		ThresholdCrossing	Critical	9	Dec-06-11 13:31	csr-c-2941d	Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' crossed threshold for 'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06 13:15:00.0' - value '50.0' threshold '5.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.
☑		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'testOneCheckin' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '1.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel5666/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'testOneCheckin' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel5666/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '1.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/7' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'testOneCheckin' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/7' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '1.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel5666/7' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.

1	Help for Event tool	**2**	Report for Event tool

Step 5 The View Thresholds dialog box or the Edit Threshold dialog box (administrator users) displays the following threshold values. For detailed descriptions, see Creating Thresholds in Prime Performance Manager, page 10-1.

- Name—The threshold name.
- KPI Name—The key performance indicator name.
- KPI Type—The KPI type (not editable).
- KPI Report—The KPI report.
- Interval—The threshold time interval (not editable).
- Scope—The threshold scope.
- Enabled—Indicates whether the threshold is enabled (checked) or disabled (not checked).
- Description—Threshold text description.

- Days—The days when the threshold is applied.
- Hours—The time period (hours and minutes) when the threshold is applied.
- Threshold Values—The threshold onset, abate, and number of occurrence values for the alarms that are raised.

Step 6 When finished, click **OK**.

Step 7 To view a report for the threshold crossing, in the Alarms window toolbar, click **Report for Event**.

The threshold crossing report window appears.

Step 8 When finished, click **OK**.

Viewing Threshold Events

To view threshold events, in the navigation area, click the **Event History**. The types of threshold events that appear include:

- All threshold crossing events, for example:

```
Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' crossed threshold for
'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06
10:30:00.0' - value '50.0' threshold '5.0'.
```

and

```
Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' is below threshold for
'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06
10:15:00.0'
```

- All threshold user creation or edition activities, for example:

```
Gateway: node123- Threshold rising1 - Threshold2811 - 15 Minute was overwritten by
user123.
```

CHAPTER 11

Reviewing Prime Performance Manager Home Page Information

The following topic describes the information provided on the Cisco Prime Performance Manager Home page:

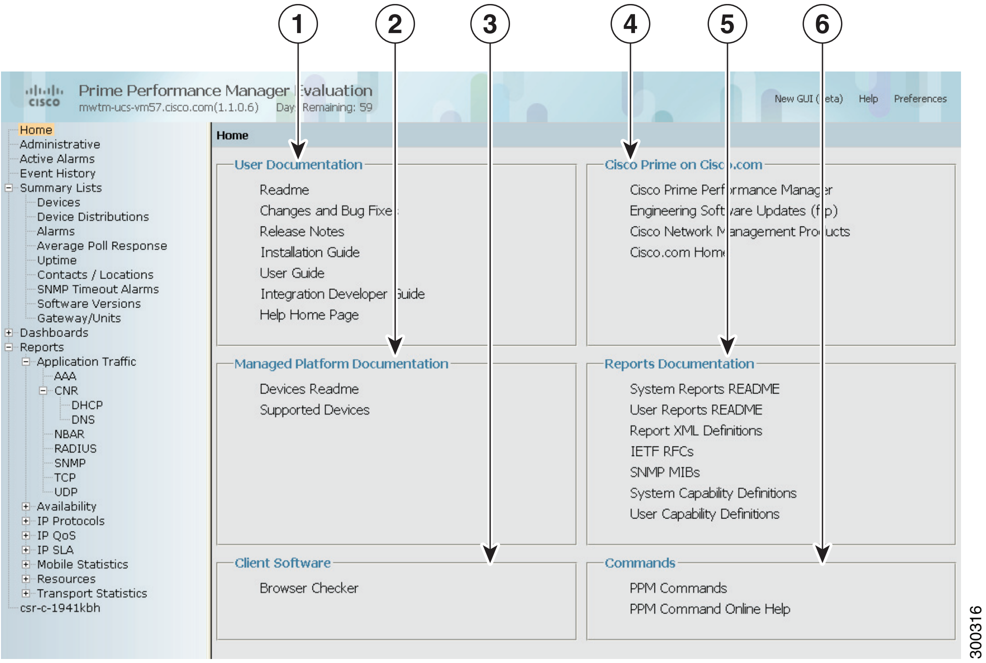
- Displaying the Home Page, page 11-1

Displaying the Home Page

Prime Performance Manager web interface Home page (see Figure 11-1) provides access to Prime Performance Manager client software, Cisco documentation, and information about Prime Performance Manager. The Home page content area contains the following areas:

- User Documentation
- Managed Platform Documentation
- Client Software
- Prime on Cisco.com
- Reports Documentation
- Commands

Figure 11-1 Prime Performance Manager Home Page



1	User Documentation	**4**	Cisco Prime on Cisco.com
2	Managed Platform Documentation	**5**	Reports Documentation
3	Client Software	**6**	Commands

To access the Home page, in the navigation area, click **Home**. Table 11-1 shows the information provided on the Home page.

Table 11-1 Prime Performance Manager Home Page Information

Pane	GUI Element	Description
User Documentation	Readme	Describes Prime Performance Manager system requirements, Linux and Solaris requirements, and installation procedures.
	Changes and Bug Fixes	Lists the changes, bug fixes, and new release features.
	Release Notes	Displays the Prime Performance Manager Release Notes on Cisco.com.
	Installation Guide	Displays the Prime Performance Manager Installation Guide on Cisco.com.
	User Guide	Displays the Prime Performance Manager User Guide on Cisco.com.
	Integration Developer Guide	Displays the Prime Performance Manager Integration Developer Guide on Cisco.com.
	Help Home Page	Displays the Prime Performance Manager online help.

Table 11-1 Prime Performance Manager Home Page Information (continued)

Pane	GUI Element	Description
Managed Platform Documentation	Devices Readme	Displays a list of devices that have been used with Prime Performance Manager by customers and in labs.
	Supported Devices	Displays a list of devices that Prime Performance Manager officially supports on Cisco.com.
Client Software	Browser Checker	Runs a check on your web browser. For information, see Checking Your Browser Settings, page 3-3.
Cisco Prime on Cisco.com	Cisco Prime Performance Manager Home Page	Displays the Prime Performance Manager Cisco.com product information page.
	Engineering Software Updates (FTP)	Provides a link to Prime Performance Manager software updates provided by Cisco Engineering.
	Cisco Network Management Products	Displays the Network Management and Automation product information page.
	Cisco.com Home	Displays the Cisco.com website.
Reports Documentation	System Reports README	Displays README-Reports-system.html which provides Prime Performance Manager report information including the MIB variables Prime Performance Manager polls, the formulas used in metric calculations, the format of CSV export files and other report information.
	User Reports README	Displays README-Reports-user.html which provides information about user-created reports including the MIB variables Prime Performance Manager polls, the formulas used in metric calculations, the format of CSV export files and other report information.
	Report XML Definitions	Provides the XML, properties, and notes for Prime Performance Manager reports.
	IETF RFCS	Provides links to industry-standard RFCs supported by Prime Performance Manager.
	SNMP MIBs	Provides the SNMP MIBs supported by Prime Performance Manager.
	System Capability Definitions	Displays the SystemCapability.xml file (located in /opt/CSCOppm-gw/etc/), which defines the Prime Performance Manager system capabilities used for enabling and disabling reports.
	User Capability Definitions	Displays the UserCapability.xml file (located in /opt/CSCOppm-gw/etc/), which defines any user-created report functions.
Commands	PPM Commands	Displays a list of all Prime Performance Manager commands. This output appears entering the CLI help command.
	PPM Command Online Help	Provides a link to the Prime Performance Manager command documentation in online help.

CHAPTER 12

Viewing System Properties, Statuses, Messages, and Logs

To access the Administrative page of Prime Performance Manager web interface, click **Administrative** in the navigation tree in the left pane. The tabs on the Administration page appear in the right pane.

This chapter contains descriptions of these tabs and instructions on:

Note If Prime Performance Manager User-Based Access is enabled, only users with authentication level 5 (Administrator) can see all options. The Administrative page is not visible to Operator and lower users.

System Properties, Statuses, Messages, and Logs Overview

The Prime Performance Manager web interface General tab provides access to Prime Performance Manager system information, including messages, logs, status, and properties.

To view general system information, click **Administrative** in the navigation tree and then click the **General** tab in the right pane. This tab displays the information indicated in Table 12-1.

Table 12-1 General Tab Details

Pane	GUI Elements	Description	Reference
System Status	• System Status • System Versions • System Check • Connected Clients	Displays the output of these system commands: • ppm status • ppm version • ppmCheckSystemLog.txt • ppm who	For details, see Viewing System Statuses, page 12-8.
System Messages	• Info Messages • Error Messages • User Actions • Message Archives • Console Log Archives	Displays tabular information on system messages.	For details, see Viewing System Messages, page 12-2.
Properties	• System • Server • WebConfig • Reports	Displays the contents of these system property files: • System.properties • Server.properties • WebConfig.properties • Reports.properties	For details, see Viewing System Properties, page 12-12.
System Logs	• Install Log • Console Log • Backup Log • Command Log • Event Automation Log • Security Log • Web Access Log • Web Error Log	Displays the contents of these system logs: • cisco_primepm_gw_install.log • sgmConsoleLog.txt • ppmBackupLog.txt • Command Log • eventAutomationLog.txt • sgmSecurityLog.txt • Web Access Logs • Web Error Logs	For details, see Viewing System Logs, page 12-9.

Viewing System Messages

To view the following Prime Performance Manager system messages from Prime Performance Manager web interface, click **Administrative** in the navigation tree in the left pane and then click the **General** tab in the right pane:

Note These messages are related to Prime Performance Manager system itself, not to your network.

- Viewing Information Messages, page 12-3

- Viewing Error Messages, page 12-3
- Viewing Prime Performance Manager User Action Messages, page 12-4
- Viewing All Archived Prime Performance Manager Messages, page 12-6
- Viewing Console Log Archived Messages, page 12-7

Viewing Information Messages

To view information messages, click the **Administrative > General** tab. In the right pane, select the **Info Messages** link from System Messages section.

The System Messages: Last *number* Info Messages page displays informational messages in the Prime Performance Manager system log. These messages help you to diagnose and correct Prime Performance Manager operational problems. See Table 12-2 for more details.

Table 12-2 Info Messages

Column	Description
Period (in heading)	Collection period of the table, such as *Since Server Restart*.
Timestamp (in heading)	Date and time that Prime Performance Manager last updated the information on the page.
Row	Unique number identifying each entry in the table. You cannot edit this field.
Time	Date and time the message was logged. To sort the messages by time, click the **Time** heading.
Source	Source for the message, with the format *process.host.id*, where: • *process* is the process that logged the message. • *host* is the hostname of the process that logged the message. • *id* is a Prime Performance Manager ID that uniquely identifies the process that logged the message. This is when two or more clients are running on the same node and are connected to the same Prime Performance Manager server.
Task	Task, or thread, that logged the message.
Message	Text of the message. To sort the messages alphabetically by message text, click the **Message** heading.

Viewing Error Messages

The System Messages: Last *number* Error Messages page displays error messages that are stored in Prime Performance Manager system log. These messages help you to diagnose and correct Prime Performance Manager operational problems.

To access this page, click **Administrative > General > Error Messages** below the System Messages section, See Table 12-3 for more details

Table 12-3 Error Messages

Column	Description
Period (in heading)	Collection period of the table, such as *Since Server Restart*.
Timestamp (in heading)	Date and time that Prime Performance Manager last updated the information on the page.
Row	Unique number identifying each entry in the table. You cannot edit this field.
Time	Date and time the message was logged. To sort the messages by time, click the **Time** heading.
Source	Source for the message, with the format *process.host.id*, where: • *process* is the process that logged the message. • *host* is the hostname of the process that logged the message. • *id* is a Prime Performance Manager ID that uniquely identifies the process that logged the message. This is when two or more clients are running on the same node and are connected to the same Prime Performance Manager server.
Task	Task, or thread, that logged the message.
Message	Text of the message. To sort the messages alphabetically by message text, click the **Message** heading.

Viewing Prime Performance Manager User Action Messages

The System Messages: Last *number* Action Messages page displays user action messages stored in the Prime Performance Manager system log. These messages help you to diagnose and correct Prime Performance Manager operational problems, and to monitor audit trails of user actions.

To access this page select **Administrative > General> User Actions** below the System Messages section.

Prime Performance Manager displays the System Messages: Last *number* Action Messages page. The System Messages: Last *number* Action Messages page has these sections:

- Last Action Messages Menu, page 12-4
- Last Action Messages Table, page 12-5

Last Action Messages Menu

By default, Prime Performance Manager displays action messages of all classes on the System Messages: Last *number* Action Messages page. However, Prime Performance Manager provides menu options that enable you to display messages that pertain only to a specific class on the page. See Table 12-4 for more details.

Table 12-4 Last Action Messages Menu

Column	Description
Create	Opens the System Messages: Last *number* Action: specified web page:
Delete	Opens the Delete Messages web page, displaying only Delete action messages.
Discover	Opens the Discover Messages web page, displaying only Discover action messages.
Edit	Opens the Edit Messages web page, displaying only Edit action messages.
Ignore	Opens the Ignore Messages web page, displaying only Ignore action messages.
OverWrite	Opens the OverWrite Messages web page, displaying only OverWrite action messages.
Poll	Opens the Poll Messages web page, displaying only Poll action messages.
Purge	Opens the Purge Messages web page, displaying only Purge action messages.
LogInOut	Opens the LogInOut Messages web page, displaying only Log in and Log out action messages.
All	Opens a web page that displays all action messages.
Request	Opens the Request web page, displaying every user-initiated action messages from the gateway to a unit.

Last Action Messages Table

The Last Action Messages table contains the following items. See Table 12-5 for more details.

Table 12-5 Last Action Messages Table

Column	Description
Period	Collection period of the table, such as Since Server Restart.
Timestamp	Date and time that the information on the page was last updated by Prime Performance Manager.
Row	Unique number identifying each entry in the table. You cannot edit this field.
Time	Date and time the message was logged. To sort the messages by time, click the **Time** heading.

Table 12-5 Last Action Messages Table (continued)

Column	Description
Class	Class of the message. Possible classes are: • **Create**—Creation event, such as the creation of a seed file. • **Delete**—Deletion event, such as the deletion of an object or file. • **Discover**—Discovery event, such as Discovery beginning. • **Edit**—Edit event. A user has edited an object. • **Ignore**—Ignore event. A user has flagged a link or linkset as Ignored. • **LogInOut**—Login event. A user has logged into Prime Performance Manager. **OverWrite**—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • **Poll**—Poll event, such as an SNMP poll. • **Purge**—Purge event. A user has requested Discovery with Delete Existing Data chosen, and Prime Performance Manager has deleted the existing Prime Performance Manager database. • **Request**—User-initiated action messages from the gateway to a unit. To sort the messages by class, click the **Class** heading.
Message	Text of the message. To sort the messages alphabetically by message text, click the **Message** heading.

Viewing All Archived Prime Performance Manager Messages

The System Message Archives: All Messages page displays all archived messages in Prime Performance Manager system logs, including:

- error
- informational
- trace
- debug
- dump
- action
- SNMP

To access the System Message Archives, select **Administrative > Message Archives** on the All Messages page.

On the System Message Archives: All Messages page, messages are archived by timestamp.

Each archived file contains all Prime Performance Manager system messages for a single session for the server to which you are connected, and which is currently running on the Prime Performance Manager server. If you restart the server, Prime Performance Manager creates a new file.

To view archived messages, click a timestamp. The System Messages Archive: Last *number* All Messages page appears that displays all messages that were in the system log at the time specified in the timestamp.

You may see an entry labeled, *messageLog-old* among a list of files that have timestamps in the filenames. A daily **cron** job creates the files with the timestamps. The **cron** job that runs at midnight, searches through the *messageLog.txt* and *messageLog-old.txt* files for all entries from the past day.

The *messageLog-old.txt* file exists only if the size of *messageLog.txt* exceeds the limit set by the ppm logsize command. Prime Performance Manager lists the contents of *messageLog-old.txt* because it could contain important data from the day the message log file rolled over. See Table 12-6 for more details.

The Last All Messages table contains this information (without column headers).

Table 12-6 Archived Messages

Description	Information
Index	Message number that Prime Performance Manager assigns to the message.
Time	Date and time the message was logged.
Type	Type of message. Possible types are: • Action • Debug • Dump • Error • Info • SNMP • Trace
Source	Source for the message, with the format *process.host.id*, where: • *process* is the process that logged the message. • *host* is the hostname of the process that logged the message. • *id* is a Prime Performance Manager ID that uniquely identifies the process that logged the message. This is when two or more clients are running on the same node and are connected to the same Prime Performance Manager server.
Task	Task, or thread, that logged the message.
Message	Text of the message.

Viewing Console Log Archived Messages

The System Console Archives: All Messages page displays all archived system console messages.

To access the System Console Archives: All Messages page, choose **Administrative > Console Log Archives**.

On the System Console Archives: All Messages page, messages are archived by timestamps. Each archived file contains all Prime Performance Manager system console messages for a single session for the server to which you are connected, and which is currently running on the Prime Performance Manager server. If you restart the server, Prime Performance Manager creates a new file.

To view these archived messages, click a timestamp. The Console Archive: Last *number* All Messages page appears that displays all console messages that were in the system log at the time specified by the timestamp.

Viewing Network Status Archives

The Network Status Archives page displays all archived network status messages.

To access the System Console Archives: All Messages page, choose **Administrative > Network Status Archives**.

On the Network Status Archives: All Messages page, messages are archived by timestamps. Each archived file contains all Prime Performance Manager network status messages for a single session for the server to which you are connected, and which is currently running on the Prime Performance Manager server. If you restart the server, Prime Performance Manager creates a new file.

To view these archived messages, click a timestamp. The Network Status Archive: Last *number* All Messages page appears that displays all network status messages that were in the system log at the time specified by the timestamp.

Viewing System Statuses

You can view Prime Performance Manager system status information from Prime Performance Manager web interface by clicking **Administrative** in the navigation tree in the left pane and then clicking **General** tab in the right pane:

- Viewing System Status, page 12-8
- Viewing System Versions, page 12-8
- Viewing System Check, page 12-8
- Viewing Connected Clients, page 12-9

Viewing System Status

To access system status information, choose **Administrative > System Status** (Prime Performance Manager might take a few seconds to display this page). This page displays the status of all Prime Performance Manager servers, local clients, and processes.

Viewing System Versions

To access version information, choose **Administrative > System Versions** (Prime Performance Manager might take a few seconds to display this page). This page displays version information for all Prime Performance Manager servers, clients, and processes.

Viewing System Check

To access system information, choose **Administrative > System Check**. Prime Performance Manager displays the output from the following command:

```
/opt/CSCOppm-gw/logs/sgmCheckSystemLog.txt
```

Viewing Connected Clients

To access connected client information, choose **Administrative > Connected Clients**. This page lists all Prime Performance Manager clients that are currently connected to the Prime Performance Manager server. It also lists all Solaris and Linux users that are logged into the Prime Performance Manager server.

Viewing System Logs

You can view Prime Performance Manager system logs information from Prime Performance Manager web interface by clicking **Administrative** in the navigation tree in the left pane and then clicking **General** tab in the right pane:

- Viewing the Install Log, page 12-9
- Viewing the Console Log, page 12-9
- Viewing the Backup Log, page 12-9
- Viewing the Command Log, page 12-10
- Viewing the Event Automation Log, page 12-10
- Viewing the Security Log, page 12-11
- Viewing the Web Access Logs, page 12-11
- Viewing the Web Error Logs, page 12-12

Viewing the Install Log

The Install Log displays the contents of Prime Performance Manager installation log file for the server to which you are connected, and which is currently running Prime Performance Manager.

To access the Install Log, choose **Administrative > Install Log**. You can also view the Console Log with the **ppm installlog** command.

Viewing the Console Log

The Console Log displays the contents of Prime Performance Manager system console log file for the server to which you are connected, and which is currently running Prime Performance Manager.

The console log file contains error and warning messages from the Prime Performance Manager server, such as those that might occur if the Prime Performance Manager server cannot start. It also provides a history of start-up messages for server processes and the time each message appeared.

To access the Console Log, choose **Administrative > Console Log**. You can also view the Console Log with the **ppm console** command.

Viewing the Backup Log

The Backup Log displays the contents of Prime Performance Manager backup log file for the server to which you are connected, and which is currently running Prime Performance Manager.

The default path and filename for the backup log file is /opt/CSCOppm-gw/logs/ppmBackupLog.txt. If you installed Prime Performance Manager in a directory other than /opt, then the backup log file is in that directory.

To access the Backup Log, choose **Administrative > Backup Log**. You can also view the Backup Log with the **ppm backuplog** command.

Viewing the Command Log

The Command Log displays the contents of the Prime Performance Manager system command log file for the server to which you are connected, and which is currently running on the Prime Performance Manager server.

The system command log lists all Prime Performance Manager commands that have been entered for the Prime Performance Manager server, the time each command was entered, and the user who entered the command.

To access the Command Log, choose **Administrative > Command Log**. You can also view the Command Log with the **ppm cmdlog** command.

The Prime Performance Manager Command Log, shown in Table 12-7page appears.

Table 12-7 Command Log

Column	Description
Timestamp	Date and time the command was logged. To sort the messages by time, click the **Timestamp** heading.
User Name	User who entered the command. To sort the commands by user, click the **User** heading.
Command	Text of the command. To sort the messages alphabetically by command text, click the **Command** heading.

Viewing the Event Automation Log

The Event Automation Log displays the contents of the system event automation log file for the server to which you are connected, and which is currently running on the Prime Performance Manager server. The system event automation log lists all messages that event automation scripts generate.

The default path and filename for the system event automation log file is /opt/CSCOppm-gw/logs/eventAutomationLog.txt. If you installed Prime Performance Manager in a directory other than /opt, then the system event automation log file is in that directory.

To access the Event Automation Log, choose **Administrative > Event Automation Log**. You can also view the Event Automation Log with the **ppm eventautolog** command.

Related Topics

Viewing the Security Log, page 12-11

Viewing the Web Access Logs, page 12-11

Viewing the Web Error Logs, page 12-12

Viewing the Security Log

The Security Log displays the contents of Prime Performance Manager system security log file for the server to which you are connected, and which is currently running Prime Performance Manager server. The system security log lists:

- All security events that have occurred for the Prime Performance Manager server.
- The time each event occurred.
- The user and command that triggered the event.
- The text of any associated message.

The default path and filename for the system security log file is /opt/CSCOppm-gw/logs/sgmSecurityLog.txt. If you installed Prime Performance Manager in a directory other than /opt, the system security log file is in that directory.

To access the Security Log, choose **Administrative > Security Log in the System Logs section**. You must be an System Administrator to access Security Log. You can also view the Security Log with the **ppm seclog** command. Table 12-8 shows the Security Log columns.

Table 12-8 Security Log

Column	Description
Timestamp	Date and time the security event occurred. To sort the entries by time, click the **Time** heading.
User	User who triggered the security event. To sort the entries by user, click the **User** heading.
Message	Text of the security event message. To sort the entries alphabetically by message text, click the **Message** heading.
Command	Text of the command that triggered the security event. To sort the entries alphabetically by command text, click the **Command** heading.

Viewing the Web Access Logs

The Web Access Logs page displays a list of web access log files for the server to which you are connected, and which is currently running the Prime Performance Manager server.

The web access log lists all system web access messages that have been logged for the Prime Performance Manager server, providing an audit trail of all access to the Prime Performance Manager server through the Prime Performance Manager web interface.

The default path and filename for the web access log file is /opt/CSCOppm-gw/apache/logs/access_log. If you installed Prime Performance Manager in a directory other than /opt, then the web access log file is in that directory.

To access the Web Access Logs page, choose **Administrative > Web Access Logs**. You can also view the Web Access Logs page using the **ppm webport** command.

Viewing the Web Error Logs

The Web Error Logs page displays a list of web error log files for the server to which you are connected, and which is currently running on the Prime Performance Manager server. The web server error log lists all system web error messages that have been logged for the Prime Performance Manager web server.

You can use the web error log to troubleshoot the source of problems that users may have encountered while navigating Prime Performance Manager web interface.

The default path and filename for the web error log file is /opt/CSCOppm-gw/apache/logs/error_log. If you installed Prime Performance Manager in a directory other than /opt, then the web error log file is in that directory.

To access the Web Error Logs page, choose **Administrative > Web Error Logs**. You can also view the Web Error Logs page using the **ppm webport** command.

Viewing Properties

Property files for Prime Performance Manager are in the /opt/CSCOppm-gw/properties directory. You can view the Prime Performance Manager properties from the Prime Performance Manager web interface by clicking **Administrative** in the navigation tree in the left pane and then clicking the **General** tab in the right pane:

- Viewing System Properties, page 12-12
- Viewing Server Properties, page 12-13
- Viewing Web Configuration Properties, page 12-13
- Managing Units Overview, page 13-1

Viewing System Properties

To access the System Properties file, choose **Administrative > System** in the Properties pane.

Prime Performance Manager displays the contents of the /opt/CSCOppm-gw/properties/System.properties file.

The System Properties file contains Prime Performance Manager server and client properties that control various Prime Performance Manager configuration parameters. Table 12-9 shows commands that you can use to change system properties.

Table 12-9 System Properties

To change this system property	Use this Prime Performance Manager command
BACKUP_RMIPORT	ppm serverlist delete, page B-42
BACKUP_SERVER	
BACKUP_WEBPORT	
BADLOGIN_TRIES_ALARM	ppm badloginalarm, page B-10
BADLOGIN_TRIES_DISABLE	ppm badlogindisable, page B-11
CHART_MAX_WINDOW	ppm checksystem, page B-12
CONSOLE_ARCHIVE_DIR_MAX_SIZE	ppm authtype, page B-7

Table 12-9 System Properties (continued)

To change this system property	Use this Prime Performance Manager command
CONSOLE_LOG_MAX_SIZE	ppm consolelogsize, page B-14
CSV_STRING_DELIMITER	
CW2K_SERVER	ppm datadir, page B-14
CW2K_WEB_PORT	
CW2K_SECURE_WEB_PORT	
JSP_PORT	ppm ipslaftpfilesize, page B-26
LOGAGE	ppm msglogage, page B-33
LOGDIR	ppm msglogdir, page B-33
LOGSIZE	ppm logsize, page B-28
LOGTIMEMODE	ppm logtimemode, page B-30
LOG_TROUBLESHOOTING	ppm uninstall, page B-59
PERSISTENCEDIR	ppm datadir, page B-14
PROMPT_CREDS	ppm logsize, page B-28
SBACKUPDIR	ppm backupdir, page B-9
SERVER_NAME	ppm servername, page B-42
SNMPCONFFILE	ppm snmpconf, page B-45
SSL_ENABLE	ppm ssl, page B-53
TRAP_LIST_ENABLE	ppm uninstall, page B-59
WEB_PORT	ppm webport, page B-62

Viewing Server Properties

To access the Server Properties file, choose **Administrative > Server** in the Properties pane. Prime Performance Manager displays the contents of the /opt/CSCOppm-gw/properties/Server.properties file.

The Server Properties file contains various properties that control the Prime Performance Manager server.

You can change the SNMP_MAX_ROWS property using the ppm snmpmaxrows command (See ppm snmpmaxrows, page B-48.) To change poller parameters in the Server Properties file, see the "Changing the GUI Polling Refresh Setting" section on page 3-10.

Viewing Web Configuration Properties

To access the Web Configuration Properties file, choose **Administrative > WebConfig** in the Properties pane. Prime Performance Manager displays the contents of the /opt/CSCOppm-gw/properties/WebConfig.properties file.

The Web Configuration Properties file contains properties that control the configuration of Prime Performance Manager web interface. For example:

```
MAX_ASCII_ROWS       = 6000
MAX_HTML_ROWS        = 100
```

```
# The selectable page sizes start at MIN_SELECTABLE_PAGE_SIZE and doubles until
# the MAX_SELECTABLE_PAGE_SIZE value is reached
# (e.g. 25, 50, 100, 200, 400, 800)
MIN_SELECTABLE_PAGE_SIZE = 25
MAX_SELECTABLE_PAGE_SIZE = 800
LOG_UPDATE_INTERVAL = 300
WEB_UTIL            = percent
WEB_NAMES           = display
MAX_EV_HIST         = 15000
```

You can use Prime Performance Manager to change the web configuration properties. See Table 12-10 for more details.

Table 12-10   Web Configuration Properties

Web Configuration Property	Changing Default Setting
LOG_UPDATE_INTERVAL	To control how often, in seconds, Prime Performance Manager updates certain web output, use the **ppm webport** command. The valid range is 1 second to an unlimited number of seconds. The default value is 300 seconds (5 minutes).
MAX_EV_HIST	To set the maximum number of rows for Prime Performance Manager to search in the event history logs, use the **ppm maxhtmlrows** command. The event history logs are the current and archived Prime Performance Manager network status logs for status change and SNMP trap messages. Prime Performance Manager sends the results of the search to the web browser, where the results are further limited by the setting of ppm maxhtmlrows command. The valid range is one row to an unlimited number of rows. The default value is 15,000 rows.
MAX_HTML_ROWS	To set the maximum number of rows for Prime Performance Manager HTML web output, such as displays of statistics reports, status change messages, or SNMP trap messages, use the **ppm maxhtmlrows** command. This lets you select a page size (if you have not explicitly chosen a page size). After you select a page size from any page, Prime Performance Manager remembers your preference until you delete your browser cookies. The default value is 100 rows.
MIN_SELECTABLE_PAGE_SIZE	This setting determines the minimum page size that you can select from the Page Size drop-down menu. The page size values start with the MIN_SELECTABLE_PAGE_SIZE and double until they reach the MAX_SELECTABLE_PAGE_SIZE.
MAX_SELECTABLE_PAGE_SIZE	This setting determines the maximum page size that you can select from the Page Size drop-down menu. The page size values start with the MIN_SELECTABLE_PAGE_SIZE and double until they reach the MAX_SELECTABLE_PAGE_SIZE.

Table 12-10 Web Configuration Properties (continued)

Web Configuration Property	Changing Default Setting
WEB_NAMES	To specify whether Prime Performance Manager should show real DNS names or display names in web pages, enter the **ppm webport** command. To show: - The real DNS names of nodes, as discovered by Prime Performance Manager, enter **Prime Performance Manager webnames real**. - Display names, enter **Prime Performance Manager webnames display**. Display names are new names that you specify for nodes. This is the default setting. For more information about display names.
WEB_UTIL	To specify whether Prime Performance Manager should display send and receive as percentages or in Erlangs in web pages, enter the **ppm who** command. To display: - As a percentage, enter **Prime Performance Manager webutil percent**. This is the default setting. - In Erlangs (E), enter **Prime Performance Manager webutil erlangs**.

Each of the web configuration commands requires you to be logged in as the root user, as described in the "Before you begin device discovery, review the devices that Prime Performance Manager officially supports. These can be found at:" section on page 4-1, as described in the "Managing Prime Performance Manager Users" section on page 6-14.

Viewing System Reports Property

To access the Report Properties file, choose **Administrative > Reports** in the Properties pane. Prime Performance Manager displays the contents of the /opt/CSCOppm-gw/properties/Reports.properties file.

The Report Properties file contains various properties that can be enabled/disabled in the Prime Performance Manager server. For example:

```
STATS_REPORTS       = enable

RPT_5MIN_AGE        = 3
RPT_15MIN_AGE       = 3
RPT_HOURLY_AGE      = 7
RPT_DAILY_AGE       = 31
RPT_WEEKLY_AGE      = 365
RPT_MONTHLY_AGE = 1825

RPT_5MIN_CSV_AGE    = 3
RPT_15MIN_CSV_AGE   = 3
RPT_HOURLY_CSV_AGE  = 7
RPT_DAILY_CSV_AGE   = 31
RPT_WEEKLY_CSV_AGE = 365
RPT_MONTHLY_CSV_AGE = 1825

RPT_TIMEMODE        = 24
NODE_NAME_TYPE      = dnsname
```

```
RPT_5MIN_ENABLED     = true
RPT_15MIN_ENABLED    = true
RPT_HOURLY_ENABLED   = true
RPT_DAILY_ENABLED    = true
```

Managing Log Files

You can use the following commands to change the Prime Performance Manager log file location, file size, time mode, and maximum number of archive days:

- **ppm msglogdir**—Changes the location of the system message log directory. By default, all Prime Performance Manager system message log files are located on the gateway at /opt/CSCOppm-gw/logs, and on the unit at /opt/CSCOppm-unit/logs. The command is specific to the each gateway and unit instance. For more information, see ppm msglogdir, page B-33.
- **ppm logsize**— Changes the message log file size. The command is specific to the each gateway and unit instance. For more information, see ppm logsize, page B-28.
- **ppm logtimemode**—Sets the log file time mode for dates. For more information, see ppm logtimemode, page B-30.
- **msglogage**—Sets the maximum number of days to archive all types of log files before deleting them from the server. For more information, see ppm msglogage, page B-33.

CHAPTER 13

Managing Prime Performance Manager Units

The following topics tell you how to manage Cisco Prime Performance Manager units:

Managing Units Overview

Prime Performance Manager allows you to create multiple units, assign them to a gateway and distribute the network devices among them. During device discovery, whether performed from Prime Performance Manager or by importing the Prime Network device inventory, Prime Performance Manager assigns devices to units based upon the device-to-unit mappings that you must create in the Unit Editor administrative tab. You can create these mappings before or after device discovery. If you create the mappings before device discovery, Prime Performance Manager assigns the devices to the units based on the information in the maps. If device-to-unit maps are not present when device discovery is run, Prime Performance Manager assigns all discovered devices to the unit installed with the gateway, if present, or to another unit if a collocated unit is not installed.

Note Determining the best allocation of devices among multiple units will take time. Many factors are involved including the unit server size, the number of enabled reports, the number of reportable objects, and many other factors.

The following topics tell you how to create and manage the device-to-unit maps:

Creating Device-to-Unit Maps

The following procedure tells you how to create a device-to-unit map to distribute devices across multiple units. Before you complete the procedure, you will need the IP addresses or address ranges of all discovered devices, and a plan on how you want to distribute them across the units.

To create the map:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click **Unit Editor**.

Step 4 On the Unit Editor toolbar, click **Add a Device to Unit Mapping**.

Step 5 In the Add Device to Unit Map dialog box, enter the following:

- IP Address Range or Hostname—Enter the device IP address, device IP address range, or host name of the device(s) you want to assign to the unit for this map.
- Unit—Choose the unit where you want to assign the devices. The field is populated with units that are assigned to the gateway.

Step 6 Click **OK**.

The map is added to the Unit Editor table.

Step 7 Repeat Steps 4 through 6 until you've completed the device maps that you want.

Step 8 In the Unit Editor toolbar, click **Save all Unit Entries**.

Step 9 Choose one of the following:

- If device discovery has been completed and you want to redistribute the devices now, on the Unit Editor toolbar, click **Redistribute Devices to Units**. Click **OK** on the confirmation dialog.
- If device discovery is not completed, you can run it at any time. During device discovery, devices are assigned to units based on the maps in the Unit Editor table. For device discovery procedures, see Chapter 4, "Discovering Network Devices."

Editing Device-to-Unit Maps

To edit a device-to-unit map, complete the following steps:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click **Unit Editor**.

Step 4 In the Unit Editor device-to-unit entries, edit the following:

- IP Address Range or Hostname—In the table cell, you can edit the device IP address, device IP address range, or host name.
- Unit—If you want to assign the IP address or address range to a different unit, choose the unit from the drop-down list, which displays units connected to the gateway.

Step 5 When you are finished, in the Unit Editor toolbar, click **Save all Unit Entries**.

Step 6 Choose one of the following:

- If device discovery is completed and you want to redistribute the devices based on the edits, on the Unit Editor toolbar, click **Redistribute Devices to Units**. Click **OK** on the confirmation dialog.

- If device discovery is not completed, you can run it at any time, and the edited device-to-unit maps will be applied at that time.

Deleting Device-to-Unit Maps

To delete a device-to-unit map:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click **Unit Editor**.

Step 4 In the Unit Editor device-to-unit entries, click the map table row(s) that you want to delete. To select more than one map, press Shift.

Step 5 When you are finished, in the Unit Editor toolbar, click **Save all Unit Entries**.

Step 6 Choose one of the following:

- If device discovery is completed and you want to redistribute the devices based on the edits, on the Unit Editor toolbar, click **Redistribute Devices to Units**. Click **OK** on the confirmation dialog.
- If device discovery is not completed, you can run it at any time, and the edited device-to-unit maps will be applied at that time.

Changing a Device Unit Assignment

You can change the device unit assignment by editing the device-to-unit map. (See Editing Device-to-Unit Maps, page 13-2.) You can also change the device unit assignment by individual device in the Devices summary list. To do this:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Summary Lists > Devices**.

Step 3 In the device table, choose the device(s) whose unit assignment you want to change. To choose more than one device, press **Shift**.

Step 4 From the Actions menu, choose **Relocate Device**.

Step 5 In the Relocate Device dialog box, choose the unit to which you want to assign the device(s), then click **Relocate**.

The new device-to-unit assignments will occur immediately.

- IP Address Range or Hostname—In the table cell, you can edit the device IP address, device IP address range, or host name.
- Unit—If you want to assign the IP address or address range to a different unit, choose the unit from the drop-down list, which displays units connected to the gateway.

Step 6 When you are finished, in the Unit Editor toolbar, click **Save all Unit Entries**.

Creating Unit Protection Groups

Prime Performance Manager protection groups provide protection for units on a 1:1 or N:1 basis, where N = any number of primary units. Prime Performance Manager unit protection groups include the following key points:

- Redundancy groups are created after Prime Performance Manager installation using the ppm redundancygroups command; they cannot be created or managed using the Prime Performance Manager GUI.
- Multiple redundancy groups can be created. However a unit can only belong to one redundancy group.
- A unit added to a protection group as a redundant unit cannot have devices attached to it. If a failure occurs to a primary unit, the devices attached to the primary unit are switched to the redundant unit.
- Devices cannot be added to units in standby status, regardless of whether the unit is designated as a primary or standby unit. If a redundant unit become active due to a switchover, the following occurs:
  - When you request a new device discovery, the device is directed to the active redundant unit for processing. After the failback to the primary unit, the primary unit processes the discovered device(s).
  - When you move a device to the active redundant unit, the device is moved to the active redundant unit. After the failback, the primary unit processes the moved device.
  - If you move a device from an active redundant unit to another unit, the move is completed. After the failback, the primary unit does not process the moved node.
  - Moving a device to a failed primary unit is not allowed.
- To prevent units from engaging in down/up flapping, a switchover delay is provided. The delay is the amount of time the gateway waits after a unit becomes unavailable before it initiates a failover to the redundant unit. You specify the length of the delay when you create the redundancy group. The gateway determines the unit unavailability based on a unit connection that is lost. The connection can be lost for many reasons, for example, the unit is shut down or it crashes, or the network connectivity between the gateway and unit is lost.
- After the problem that caused a switchover is resolved, you must manually initiate the return to the primary unit using the ppm redundancygroups failback command.
- Following a switchover, redundant units service devices in the same manner as the primary unit. State changes are communicated to the gateway. After a failback, the primary unit picks up where the redundant unit left off.

To create a unit redundancy group, use the ppm redundancy command:

ppm redundancygroups [**list** | **detail** | **create** | **add** | **remove** | **delete** | **redundant** | **delay** | **enable** | **disable** | **failover** | **failback** | **import** | **export**]

- **list**—Lists the redundancy groups defined on the gateway, similar to the following:

```
ppm redundancygroups list
groupA, Enabled, Number of Units: 2
groupB, Enabled, Number of Units: 4
```

- **detail** [*group name*]—Lists the redundancy group details, similar to the following:

```
ppm redundancygroups detail groupA
ID: 54001
Name: groupA
Enabled
Created: Wed Sep 21 11:44:36 EDT 2011
Create User: localhost
Last Modified: Wed Sep 21 11:44:36 EDT 2011
Last Modified User: localhost
Enabled
Fail over delay: 60
Units: [
        unit1,     Primary,
         unit2,  Redundant
        unit3,  Primary
        unit4,  Primary
```

- **create** [*group name* | *delay* | *unit(s)...*]—Creates a redundancy group with the provided group name, switchover delay (in seconds), and unit(s).
- **add** [*group name* | *unit(s)* ...]—Adds unit(s) to a redundancy group.
- **remove** [*group name* | *unit(s)* ...]—Removes a unit(s) from a redundancy group.

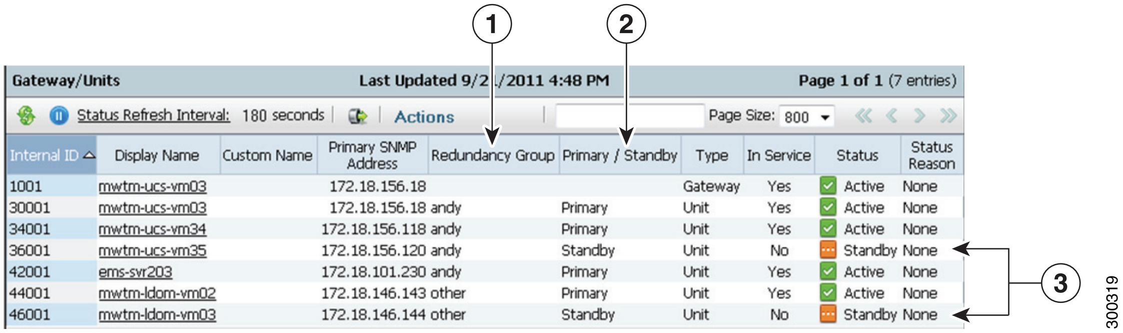
  Note A redundant unit cannot be removed from a redundancy group. To remove a redundant unit, you must change the redundant unit for the group, then you can remove the old redundant unit. Another option is to delete and recreate the redundancy group.

- **delete** [*group name*]—Deletes a redundancy group. The unit redundancy mode is not checked.
- **redundant** [*group name* | *unit*]—Changes the redundant unit of a redundancy group. No devices can be attached to the new redundant node.
- **delay** [*group name* | *delay*]—Changes the redundancy group failover delay. The delay is the number of seconds the gateway waits after detecting a unit unavailability before it initiates a failover to the redundant unit.
- **enable** [*group name*]—Enables a redundancy group.
- **disable** [*group name*]—Disables a redundancy group. If a group is disabled, automatic failovers do not occur. However, you can perform manual failovers and failbacks.
- **failover** [*unit*]—Forces the failover of a unit to the redundant unit.
- **failback** [*unit*]—Initiates a return of control from the redundant unit to the specified unit.
- **import** [*/directory/filename*]—Imports redundancy group definitions from the provided file name.
- **export** [*/directory/filename*]—Exports redundancy group definitions to the provided file name.

Note Unit protection groups cannot be created or managed using the Prime Performance Manager GUI.

After protection groups are created, you can view them in the Gateway/Units summary list, as shown in Figure 13-1. The Redundancy Group column shows whether the unit belongs to a redundancy group, and if so, the name of the group to which the unit is assigned. The Primary/Redundant column shows the role of the unit in the redundancy group, either primary or redundant, The Status column indicates the unit status, either active or standby.

Figure 13-1 Protection Groups



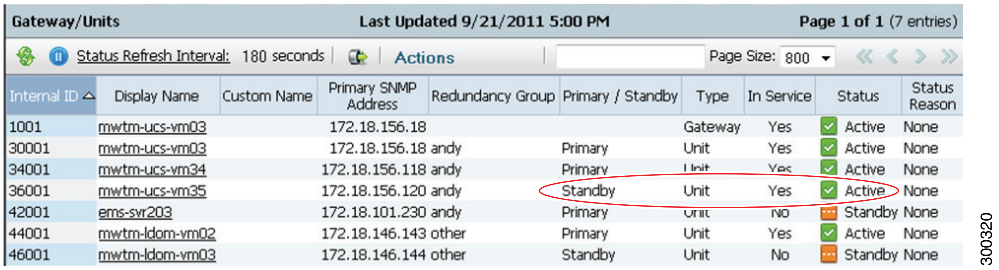
1
2
3
300319
Gateway/Units
Last Updated 9/21/2011 4:48 PM
Page 1 of 1 (7 entries)
Status Refresh Interval: 180 seconds
Actions
Page Size: 800

Internal ID	Display Name	Custom Name	Primary SNMP Address	Redundancy Group	Primary / Standby	Type	In Service	Status	Status Reason
1001	mwtm-ucs-vm03		172.18.156.18			Gateway	Yes	✓ Active	None
30001	mwtm-ucs-vm03		172.18.156.18	andy	Primary	Unit	Yes	✓ Active	None
34001	mwtm-ucs-vm34		172.18.156.118	andy	Primary	Unit	Yes	✓ Active	None
36001	mwtm-ucs-vm35		172.18.156.120	andy	Standby	Unit	No	Standby	None
42001	ems-svr203		172.18.101.230	andy	Primary	Unit	Yes	✓ Active	None
44001	mwtm-ldom-vm02		172.18.146.143	other	Primary	Unit	Yes	✓ Active	None
46001	mwtm-ldom-vm03		172.18.146.144	other	Standby	Unit	No	Standby	None

1	Redundancy Group column.	**2**	Status column.
2	Primary/Redundant column.		

Figure 13-1 shows a redundant unit that has been switched to active status.

Figure 13-2 Redundant Units in Active Status



300320
Gateway/Units
Last Updated 9/21/2011 5:00 PM
Page 1 of 1 (7 entries)
Status Refresh Interval: 180 seconds
Actions
Page Size: 800

Internal ID	Display Name	Custom Name	Primary SNMP Address	Redundancy Group	Primary / Standby	Type	In Service	Status	Status Reason
1001	mwtm-ucs-vm03		172.18.156.18			Gateway	Yes	✓ Active	None
30001	mwtm-ucs-vm03		172.18.156.18	andy	Primary	Unit	Yes	✓ Active	None
34001	mwtm-ucs-vm34		172.18.156.118	andy	Primary	Unit	Yes	✓ Active	None
36001	mwtm-ucs-vm35		172.18.156.120	andy	Standby	Unit	Yes	✓ Active	None
42001	ems-svr203		172.18.101.230	andy	Primary	Unit	No	Standby	None
44001	mwtm-ldom-vm02		172.18.146.143	other	Primary	Unit	Yes	✓ Active	None
46001	mwtm-ldom-vm03		172.18.146.144	other	Standby	Unit	No	Standby	None

Unit Protection Group Failover Scenarios

The following sections describe unit protection group and failover behavior after different network circumstances occur.

Unit Shut Down or Failure

After a unit is shut down or stops functioning, the gateway waits for the delay time configured for the protection group. After that, the gateway determines the unit is down and forces a failover of its devices to the redundant server. The redundant server starts collecting statistics for the devices. The redundant unit now owns the devices and forwards CSV data to the gateway. The gateway accesses the redundant server for interactive reports. The unit that is down does not collect statistics. After it recovers and reconnects to the server, a handshake occurs and the gateway informs the unit that it is being covered for by a redundant unit. The failed unit is placed in a standby state and remains idle. It does not poll any devices; however, it can provide historical data to the gateway for interactive reporting.

To return the failed unit to its primary role, you must issue a failback. After the failback is requested, the devices on the redundant unit return to the primary unit and processing continues on the primary unit. The redundant unit returns to standby state and stops device polling, although it can participate in interactive reports. The primary unit returns to normal state and begins forwarding CSV data to the gateway.

Gateway-to-Unit Connectivity Failure

In the event connectivity between a gateway and primary unit is lost, the redundant unit picks up for the “failed” unit and takes ownership of the devices. During the network connectivity unavailability, the redundant unit and the primary unit both poll the devices. The primary unit does not forward data to the gateway it has no connectivity to the gateway. After connectivity is restored and the unit reconnects to the gateway, during the handshake the unit recognizes that a redundant unit is processing for it and at this time it drops any data queued for the gateway. This includes CSV and event data. The “failed” unit is placed in a standby state and is idle. It does not poll any devices; however it can provide historical data to the gateway for interactive reporting. To return the primary unit to its original role, you must issue a failback command.

Gateway Failure

If a gateway is brought down either by the ppm shutdown command or because of a failure, the unit continues to process devices and queue data for the gateway. After the gateway is restored, the unit forwards the queued data to the gateway. Because the gateway contains the unit protection group configuration information, a gateway failure causes a loss to the unit redundancy. If a gateway is down and a unit that is part of a redundancy group fails, the redundant unit will not take over for the failed unit.

CHAPTER 14

Creating and Editing Device Polling Groups

The following topics tell you how to configure polling groups:

- Device Polling Groups, page 14-1
- Editing Polling Group Parameters, page 14-2
- Creating a New Polling Group, page 14-2
- Assigning Devices to Polling Groups, page 14-3

Device Polling Groups

Device polling is the frequency at which Prime Performance Manager retrieves updated information from devices. When you complete device discovery (see Chapter 4, "Discovering Network Devices"), Prime Performance Manager assigns devices to polling groups based on the device type. For example, all discovered Cisco 7606 Series Routers are assigned to a Cisco7606s polling group, all Cisco MWR 1941-DC Mobile Wireless Routers are placed in a CiscoMWR-1941-DC polling group, and so on. The number of polling groups created during device discovery depend on the number of unique device types Prime Performance Manager discovers. If all devices belong to the same device type, then only one polling group is created.

Polling groups are defined by the attributes listed in Table 14-1. All polling groups created during device discovery are assigned the default values. However, you can:

- Change the polling based on the device type. For example, to change the polling for all Cisco 7606 routers, you would modify the Cisco7606s polling group.
- Create a new polling group and assign devices to it. For example, if you want to assign the same polling parameters to a group of devices with different device types, you create the polling group and assign each device to it.

Table 14-1 Polling Group Parameters

Parameter	Default	Description
Poll Interval	15 minutes	The interval of time at which Prime Performance Manager polls the device.
Time Out	30 seconds	If Prime Performance Manager cannot connect to the device initially, the amount of time it will continue to try to connect before it times out.
Retries	2	If Prime Performance Manager cannot connect to the device, the number of times it will retry the connection after the time out interval is reached.

Editing Polling Group Parameters

Complete the following steps to edit the parameters of an existing polling group:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click the **Polling Groups** tab.

Step 4 Scroll to the polling group you want to modify and edit the values in the following table cells:

- Poll Interval
- Time Out
- Retries

See Table 14-1 on page 14-1, for polling group parameter descriptions and default values.

Note You cannot edit the polling group name.

Step 5 On the Polling Group toolbar, click the **Save Polling Group** tool.

Creating a New Polling Group

Complete the following steps to create a new polling group:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click the **Polling Groups** tab.

Step 4 On the Polling Group toolbar, click the **Add Polling Group** tool.

Step 5 Scroll to the polling group you want to modify and edit the values in the following table cells:

- Poll Interval
- Time Out
- Retries

See Table 14-1 on page 14-1, for polling group parameter descriptions and default values.

Note You cannot edit the polling group name.

Step 6 On the Polling Group toolbar, click the **Save Polling Group** tool.

Assigning Devices to Polling Groups

By default, Prime Performance Manager creates device type polling groups and assigns devices to them based on their device type. You can create custom polling groups and reassign the devices to them. To assign a device to a custom polling group:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, expand the **Summary Lists** and click **Devices**.

Step 3 In the device table, select the row of the device whose polling group you want to change. To select more than one device, press **Shift** and highlight the device table row.

Step 4 From the Devices window toolbar Actions menu, choose **Edit Polling Group**.

Step 5 In the Edit Polling Group dialog box, choose the polling group you want to assign. The following options appear:

- The device type polling group. This option is not displayed if you choose multiple devices with different device types.
- This Device Only—If selected, allows you to edit the polling group parameters and assign it to the selected devices.
- Default—Assigns the device(s) to the default polling group.
- Custom groups—If you created polling groups, they are displayed.

Step 6 Click OK.

CHAPTER 15

Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters

The following topics tell you how to add upstream OSS hosts for Prime Performance Manager alarm SNMP traps. It also tells you how to tune Prime Performance Manager alarms and events:

Adding Upstream OSS Hosts

To add OSS hosts for Prime Performance Manager SNMP traps:

Step 1 log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click the **Event Editor** tab.

Step 4 On the Event Editor toolbar, click the **Add a New Host** tool.

Step 5 In the Add Upstream OSS Host dialog box, enter the host parameters:

- Host—Enter the hostname or IP address
- Port—Enter the port Prime Performance Manager should use to connect to the host.
- Community—Enter the SNMP community string.
- SNMP Version—Enter the SNMP version, either Version 1 or 2c.

Note Prime Performance Manager supports SNMP v3 for device SNMP credentials. However, only SNMP v1 and 2c are supports for upstream OSS hosts.

- Trap Type—Enter the SNMP trap type:
  - CISCO-PRIME—The Cisco Prime trap type.
  - CISCO-SYSLOG—The Cisco Syslog trap type. See CISCO-PRIME Notification Attributes, page 15-8.

  - CISCO-EPM—The Cisco EPM trap type. See CISCO-EPM Trap Notification Attributes, page 15-4.
  - CISCO-EPM-2—The Cisco EPM 2 trap type. See CISCO-EPM-2 Trap Notification Attributes, page 15-5

Step 6 Click **OK**.

Step 7 On the Event Editor toolbar, click **Save Configuration**.

The new host is added to the Upstream OSS Hosts table.

Editing Upstream OSS Hosts

To edit OSS hosts for Prime Performance Manager SNMP traps:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click the **Event Editor** tab.

Step 4 In the Upstream OSS Host table, select the host entry you want to edit, then modify the following as needed. For field descriptions, see Adding Upstream OSS Hosts, page 15-1.

- Host
- Port
- Community
- SNMP Version
- Trap Type:
  - CISCO-PRIME
  - CISCO-SYSLOG
  - CISCO-EPM
  - CISCO-EPM-2

Step 5 Click **OK**.

Step 6 On the Event Editor toolbar, click **Save Configuration**.

Tuning Event and Alarm Parameters

To modify Prime Performance Manager event and alarm parameters:

Step 1 log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 In the Administrative window, click the **Event Editor** tab.

Step 4 Under properties, edit the following parameters:

- Maximum Events—Edit the maximum number of events that Prime Performance Manager should retain in the events database. The default is 50,000.
- Maximum Alarms—Edit the maximum number of alarms that Prime Performance Manager should retain in the alarms database. The default is 25,000.
- Maximum Database Size—Edit the maximum database size, in MB, that Prime Performance Manager should allow the database to reach. The default is 200,000 MB.
- Event Age—Edit the number of days Prime Performance Manager should retain events. The default is 7 days.
- Alarm Age—Edit the number of days Prime Performance Manager should retain alarms. The default is 14 days.
- Cleared Alarm Age—Edit the number of seconds Prime Performance Manager should retain cleared alarms. The default is 1440 minutes (24 hours).
- Archive Active Alarms—Indicate whether active alarms should be archived, True (default) or False.
- Send Events—Indicates whether traps are sent to the OSS upstream host for events, True or False (default).
- Send Alarms—Indicates whether traps are sent to the OSS upstream host for alarms, True (default) or False.
- Send Updates—Indicates whether traps are sent to the OSS upstream host for updates, True (default) or False.

Note The Send Event, Alarms, Updates control the traps sent to the OSS. For example, if Send Updates is false, Prime Performance Manager only sends traps when the alarm is raised.

- Trap Throttle—Slows down the rate that Prime Performance Manager sends traps to the OSS so that the OSS is not overwhelmed. The default is 10 milliseconds.
- Heartbeat Interval—Sets the rate at which Prime Performance Manager sends a heartbeat trap to the OSS to indicate that Prime Performance Manager is still running. The default is 0.
- Node Display Name—Sets the device display name in the Prime Performance Manager Alarms and Events window:
  - CustomName—Uses the custom name.
  - NodeName—Uses the device hostname.
  - SysName—Uses the device system name.

Step 5 When finished, on the Event Editor toolbar, click **Save Configuration**.

Prime Performance Manager SNMP Traps

The following sections describe the OSS host traps used by Prime Performance Manager.

- CISCO-EPM Trap Notification Attributes, page 15-4
- CISCO-EPM-2 Trap Notification Attributes, page 15-5
- CISCO-PRIME Notification Attributes, page 15-8

CISCO-EPM Trap Notification Attributes

The CISCO-EPM trap (CISCO-EPM-NOTIFICATION-MIB::ciscoEpmNotificationAlarmRev1) supports new, update, and delete events. This trap is the first EPM trap version. Compare it with CISCO-EPM-2 trap and use the one with the data that meets your Prime Performance Manager northbound OSS integration needs.

Table 15-1 describes the CISCO-EPM notification attributes.

Table 15-1 CISCO-EPM Trap Notification Attributes

Attribute Name	OID	Value
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	Unused
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Unused
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Unused
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	Unique event ID
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	0, 1, or 2 Corresponds to New, Update, or Delete
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	0, 1, or 2 Corresponds to New, Update, or Delete
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Unused
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer corresponding to user-defined event category.
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	String representation of user-defined event category.
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	Always ipv4
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager Server IP address.
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	The classification of the modeled NE. For example, MWRdevice, ITPdevice, ONSdevice, SP, Linkset, Link, AS, ASPA, SGMP, and Interface.
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	Always ipv4.
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	The IP address of the managed object, either the router IP address or the Prime Performance Manager server IP address.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	Event message text.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer corresponding to user-defined event severity.

Table 15-1 CISCO-EPM Trap Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	String representation of user-defined event severity. The set of alarm severity values are: • 0—Normal • 1—Indeterminate • 2—Informational • 3—Warning • 4—Minor • 5—Major • 6—Critical A separate OID indicating a clear alarm is not provided. A clear alarm is indicated by this OID when the severity is 0 (Normal).
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Unused (always 0).
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	Communication.
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	The event/alarm name.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	The UNIX time when the event occurred. Example: 2030-04-14, 16:05:05.369,0400
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	The UNIX time when the event changed, for example: 2030-04-14, 16:05:05.369,0400
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	Either 2 for alert or 3 for event.
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Number of times this event or alert has occurred.
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	Correlation key.
cenCustomerIdentification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	Network element name.
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	Acknowledged by username.
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	Unique event ID.

CISCO-EPM-2 Trap Notification Attributes

The CISCO-EPM-2 trap (CISCO-EPM-NOTIFICATION-MIB::ciscoEpmNotificationAlarmRev2) supports new, update, and delete events. This is the second EPM trap version. Compare it with the CISCO-EPM trap and use the one that meets your Prime Performance Manager northbound OSS integration needs.

Table 15-2 describes the CISCO-EPM-2 notification attributes.

Table 15-2 CISCO-EPM-2 Notification Attributes

Attribute Name	OID	Value
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	EPM version number: EPM(1), EPM-2(2).
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	Unused.

Table 15-2 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Unused.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	Unique event ID.
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	The alarm status: 0—New 1—Update 2—Delete
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	The alarm status definition: 0—New 1—Update 2—Delete
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	AlarmNature (Undefined(0), ADAC(1), ADMC(2))
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer corresponding to user-defined event category.
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	String representation of user-defined event category.
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	Always ipv4.
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager server IP address.
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	The classification of the modeled NE. For example, MWRdevice, ITPdevice, ONSdevice, SP, Linkset, Link, AS, ASPA, SGMP, and Interface.
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	Always ipv4.
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	The IP address of the managed object. Values are either the IP address of the router or the IP address of the Prime Performance Manager 1.1 server.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	Event message text.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Integer corresponding to user-defined event severity.

Table 15-2 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	String representation of user-defined event severity. Alarm severity values are: 0—Normal 1—Indeterminate 2—Informational 3—Warning 4—Minor 5—Major 6—Critical A separate OID indicating a clear alarm is not provided. A clear alarm is indicated by this OID when the severity is 0 (Normal).
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Unused (Always 0).

cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	List of key/value pairs to accommodate alarm attributes not included in other EPM notification varbinds. Includes timestamps in the managed device time zone.
		NodeCreateTime=2010-06-17,23:25:44.65,-2202
		NodeChangeTime=2010-06-17,23:31:41.517,-2202
		NodeClearTime=2010-06-17,23:31:41.516,-2202
		NodeAckTime=2010-06-17,23:28:38.337,-2202

cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	The event/alarm name.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	UNIX time when event occurred. See cenAlarmTimestamp. Example: 2030-04-14, 16:05:05.369,0400
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	UNIX time when event changed. See cenAlarmUpdatedTimestamp. Example: 2030-04-14, 16:05:05.369,0400
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	Either 2 for alert or 3 for event.
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Number of times this event or alert has occurred.
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	Correlation key
cenCustomerIdentification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	Network element name

Table 15-2 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	Format: AckUserName;Timestamp AckUserName is one of: • < *PPM Client Name* > - the Prime Performance Manager client name if user access is disabled • < *PPM username* > - the Prime Performance Manager username if user access is enabled
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	Format: ClearUserName;Timestamp ClearUserName is one of: • < *PPM Client Name* > - manual clear: the Prime Performance Manager client name if user access is disabled • < *PPM username* > - manual clear: the Prime Performance Manager username if user access is enabled • < AutoClear > - auto clear: the string value "AutoClear"

CISCO-PRIME Notification Attributes

The CISCO-PRIME trap (CISCO-EPM-NOTIFICATION-MIB::ciscoEpmNotification) supports new, update, and delete events. Information was removed from it to correspond to the Cisco Prime Network trap.

Table 15-3 describes the CISCO-PRIME notification attributes.

Table 15-3 CISCO-PRIME Notification Attributes

Attribute Name	OID	Value
cenAlarmVersion	1.3.6.1.4.1.9.9.311.1.1.2.1.2	The version of this MIB. The version string format is: major version.minor version. **Note** Always set to 3.
cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	The time when the alarm was raised. The cenAlarmTimestamp value is contained in the SNMP TimeTicks Variable Binding type, which represents the time in hundredths of a second. The event creation time (long) value in Cisco Prime Network is divided by 10 and modulo by (2^32)-1 before it is packaged. For example: Cisco PPM Event Creation time = X cenAlarmTimestamp = (X / 10)%((2^32) - 1)

Table 15-3 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Alarms persist over time and their fields can change values. The last time a field changed, this alarm was updated. The updated time denotes this time.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	The unique alarm instance ID.
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Unused varbind.
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	Alarm name (short description).
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Unused varbind.
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer corresponding to a user-defined event category.
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	String representation of user-defined event category.
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	The Internet address type where the server generating this trap is reached. This value is set to 1 for IPv4 management.
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager gateway IP address.

cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	Fordevice and TCA events, this is a string that identifies the source of the event. For example:
		Node=1.2.3.4
		Node=1.2.3.4,ifDescr=Ethernet0/0
		For PPM system events, this is an empty string ("").

cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	The type of internet address at which the managed object is reachable. This value is set to 1 for IPV4 management.
cenAlarmManagedObjectAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.15	IP Address of the managed object: • Node and TCA events - IP Address of the network element • System event-Cisco PPM gateway IP address.
cenAlarmDescription	1.3.6.1.4.1.9.9.311.1.1.2.1.16	Event message text.
cenAlarmSeverity	1.3.6.1.4.1.9.9.311.1.1.2.1.17	Indicates the severity of the alarm using an integer value.

Table 15-3 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
cenAlarmSeverityDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.18	String representation of the alarm severity. Alarm severity values are: • 0—Normal • 1—Indeterminate • 2—Informational • 3—Warning • 4—Minor • 5—Major • 6—Critical A separate OID indicating a clear alarm is not provided. A clear alarm is indicated by this OID when the severity is 0 (Normal).
cenAlarmTriageValue	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Unused varbind.
cenEventIDList	1.3.6.1.4.1.9.9.311.1.1.2.1.20	Unused varbind.
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	User input message.
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	User input message.
cenUserMessage3	1.3.6.1.4.1.9.9.311.1.1.2.1.23	User input message.
cenAlarmMode	1.3.6.1.4.1.9.9.311.1.1.2.1.24	The possible values are: • 2—Alarm • 3—Event
cenPartitionNumber	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unused varbind.
cenPartitionName	1.3.6.1.4.1.9.9.311.1.1.2.1.26	Unused varbind.
cenCustomerIdentification	1.3.6.1.4.1.9.9.311.1.1.2.1.27	Unused varbind.
cenCustomerRevision	1.3.6.1.4.1.9.9.311.1.1.2.1.28	Unused varbind.
cenAlertID	1.3.6.1.4.1.9.9.311.1.1.2.1.29	Unused varbind.

CHAPTER 16

Configuring Device Credentials for Y.1371 SLA and Ethernet Flow Point Reports

The following topics show you how configure the Telnet and SSH access credentials which are required if you plan to enable ITU-T Y.1371 SLA and Ethernet flow point QoS reports on devices running IOS-XR:

- Adding Telnet and SSH Credentials, page 16-1
- Telnet and SSH Credential Notes, page 16-2

Adding Telnet and SSH Credentials

Y.1731 reports can be enabled on devices running IOS and IOS-XR, and Ethernet flow point QoS reports can be enabled on devices running IOS-XR. Before you enable these reports, you must add the device Telnet or SSH credentials to Prime Performance Manager. To add the Telnet or SSH credentials:

Step 1 Log into the Prime Performance Manager GUI as the administrative (Level 5) user.

Step 2 In the navigation area, click **Administrative**.

Step 3 Click the **Telnet/SSH** tab.

Step 4 In the Device Credentials Editor toolbar, click the **Add a New Device Credential for a Device** tool.

Step 5 In the Add a Credential dialog box, enter the following:

- User Name—Enter the device login user name.
- Password—Enter the password for the login user.
- Enable User Name—Enter the privileged user name.
- Enable Password—Enter the privileged user password.
- Protocol—Choose the transport protocol to be used to communicate with device:
  - Telnet—Telnet
  - SSHv1—SSH Version 1
  - SSHv2—SSH Version 2
  - WSMA_SSH—Web Services Management Agent over SSHv2. WSMA is an infrastructure framework that allows external applications to monitor and control Cisco devices. WSMA uses transports such as SSH, HTTP, and HTTPS to access a set of Web Services agents residing on the Cisco device.

- Port—The device port to be used by the transport protocol chosen in the Protocol field.
- Sub System—The subsystem used by transport protocol. If the subsystem is defined on the device, enter it here. A blank string is the default subsystem for SSH. The default subsystem for WSMA is "wsma".

Step 6 Click **OK**.

The new credential is added to the Telnet/SSH credential table.

Step 7 Test the credential:

a. In the new credential table row Actions column, click the **Test the Credential** tool.

A Testing Credentials for [*device name*] window appears. If Prime Performance Manager succeeded in connecting to the device with the credentials you entered, the following is displayed:

```
****Starting Credentials Test****
Connection test successfully!
****Test Completed****
```

If Prime Performance Manager could not connect to the device, an error is displayed, for example:

```
****Starting Credentials Test****
Exception while connecting to device!
****Test Completed****
```

Step 8 In the Testing Credentials window, click **Close**.

Step 9 If the credentials test succeeded, on the Device Credentials Editor toolbar, click the **Save All Credentials** tool to save the new credential.

If the credentials test failed, verify the credentials with your network administrator and check network connectivity. You can update the credential and run the test again until it succeeds. Additionally, you can:

- From the Actions column, click the **Clear the Row** tool to clear the row contents or click the **Delete this Credential** tool to delete the entire credential.
- From the Device Credentials Editor toolbar, click the **Reload Credentials from the Server** tool to reload all the Telnet and SSH credentials.

After you add the Telnet and SSH credentials, you might want to perform the following tasks:

- Run device discovery. See Chapter 4, "Discovering Network Devices,"for procedures.
- Enable the Y.1731 and Ethernet Flow Point reports: click **Reports** in the navigation tree, click the **Report Status** tab, enable the **IP SLA: Y.1731** and **IP QoS: Transport and Availability** reports. For more information, see Chapter 7, "Working With Reports and Dashboards."

Telnet and SSH Credential Notes

After adding the Telnet and SSH credentials, running device discovery, and enabling the Y.1731 and Ethernet Flow Point reports, review the following information:

- Default Credential—Prime Performance Manager includes a default *.*.*.* Telnet credential. The default values are from XMP_PAL.properties file. You can edit XMP_PAL.properties to set new initial default credential. If you change the default credentials in the web GUI and save it, your new default credentials will be saved to credential file instead of property file, which means now the default credentials are from credential file.

- Device Discovery—During device discovery, the Telnet and SSH credentials of discovered devices are displayed in a table beneath the SNMP credentials. The Telnet and SSH search algorithm seeks an exact match first. If no exact match is found, the default entry is used for device Telnet/SSH access credential.
- Events—If a Telnet or SSH credential issue arises, a Credential Problem state event is displayed in the device summary indicating an issue accessing the device by its Telnet or SSH credential exists.
- Reports—Only the Y.1731 SLA and Ethernet Flow Point reports require Telnet or SSH credentials. All other reports use SNMP polling.
- Prime Network Integration—When you import device credentials from Prime Network, the protocol credential, including Telnet, SSH_v1 and SSH_v2, are imported with the SNMP credentials. For protocols not supported by Prime Performance Manager, the default protocol, Telnet, is used and relevant information is logged.

Tip To view detailed information about a device inventory import, click the question mark icon in Prime Performance Manager toolbar.

- Commands—Telnet and SSH credentials can be managed using the following commands:
  - ppm addcreds—Adds the Telnet and SSH credentials to access the device. See ppm addcreds, page B-5.
  - ppm showcreds—Shows the Telnet or SSH credential configured for a device. See ppm showcreds, page B-44.
  - ppm deletecreds—Deletes the Telnet or SSH credential from the device. See ppm deletecreds, page B-16.
  - ppm xmlpoll—Retrieves the device XML output. See ppm xmlpoll, page B-63.

CHAPTER 17

Configuring Prime Performance Manager for Firewalls

The following topics tell you how to configure Prime Performance Manager for firewalls:

- Gateway-to-Unit Connectivity, page 17-1
- Configuring Gateways and Units for Firewalls, page 17-2

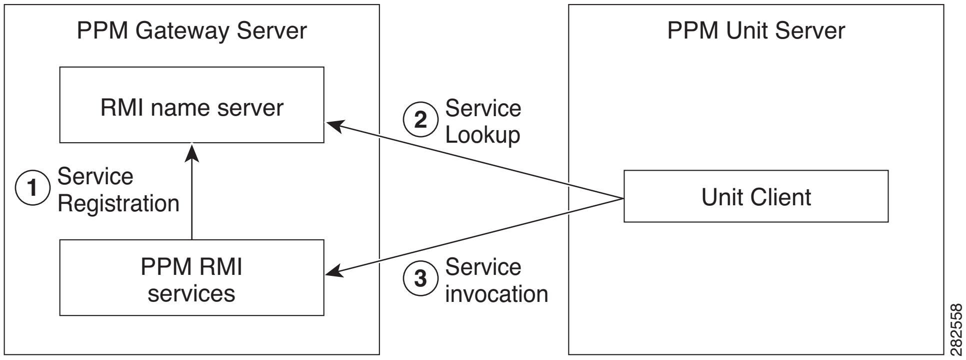
Gateway-to-Unit Connectivity

Prime Performance Manager runs on standard IP-connected networks and has the flexibility to adapt to different network environments including firewalls and Secure Sockets Layer (SSL) connectivity. Prime Performance Manager can run in each of these environments individually, or in any combination of networking environments.

Figure 17-1 shows the communication elements between the Prime Performance Manager gateway and units. Communication elements include:

- Two-way Remote Method Invocation (RMI) between gateway and unit processes. The gateway and unit send requests and receive responses to and from each other. Each can send unsolicited notifications. For example, if a unit detects a change in a device state, it sends a notification to the gateway, and the gateway updates its database.
- One-way HTTP communication between a web browser and the gateway embedded web server, using the request/response model.

Figure 17-1 Prime Performance Manager Communication



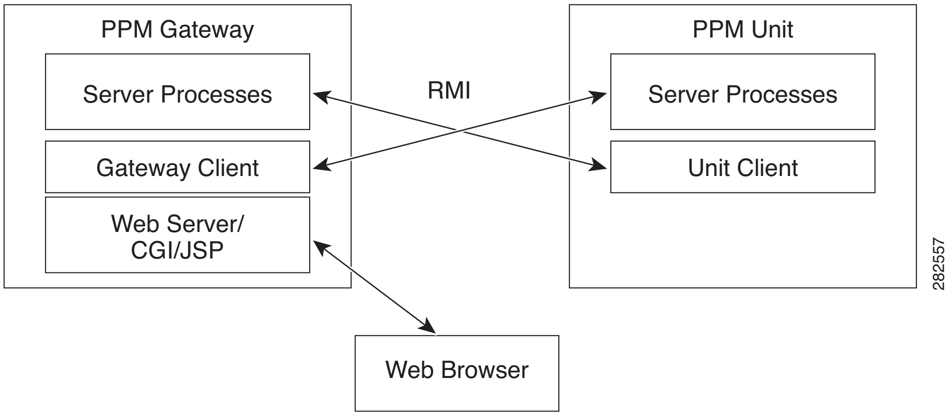
1	Service registration	**3**	Service invocation
2	Service lookup		

RMI is a Java-based technology that allows one Java application to communicate with another Java application (usually residing on different hosts) using remote method invocation. RMI manages method parameters and return values using Java object serialization. RMI uses TCP as the default communication mechanism.

The following RMI components run on Prime Performance Manager gateways and units:

- RMI name server
- Prime Performance Manager RMI services
- Prime Performance Manager client process

Figure 17-2 RMI Components



When the Prime Performance Manager gateway starts, the RMI services register with the RMI name server. These registered RMI services have one single published IP address.

When the Prime Performance Manager unit starts, it establishes a TCP connection to the RMI name server and performs a service lookup. The RMI name server returns the published IP address for the Prime Performance Manager RMI services. The unit then establishes another TCP connection to the published IP address of Prime Performance Manager RMI services for unit client and server communication.

Configuring Gateways and Units for Firewalls

Configuring Prime Performance Manager for firewalls includes communication through firewalls between:

- Web clients and a gateway/collocated unit.
- Gateways and remote unit(s).
- Unit(s) and devices.

Configurations for each are provided in the following topics:'

- Configuring Web Client and Gateway Communication, page 17-3
- Configuring Gateway and Unit Communication, page 17-3
- Configuring Unit and Device Communication, page 17-6

Configuring Web Client and Gateway Communication

If a gateway and unit are installed on the same server and you only want to enable communication from web clients to the gateway, open the firewall WEB_PORT port. No additional changes are needed. By default, WEB_PORT is 4440. If you need to change it to a different port, you can use the ppm webport command. See ppm webport, page B-62, for more information.

Configuring Gateway and Unit Communication

To enable the Prime Performance Manager gateway to communicate with units through a firewall, provision the firewall to allow Prime Performance Manager packets to pass through it. Ports used by Prime Performance Manager are configured in the System.properties file. System.properties is located in /opt/CSCOppm-gw/properties or /opt/CSCOppm-unit/properties. If you installed Prime Performance Manager in a different directory, the file resides in that directory.

Table 17-1 lists the Prime Performance Manager ports and firewall requirements.

Table 17-1 Prime Performance Manager Ports

Port	Description
RMIREGISTRY_PORT	The port on which the RMI naming server listens. You must specify a port number; 0 is not allowed.
DATASERVER_PORT	The port on which the data service listens. If you specify 0, Prime Performance Manager uses a random available port, 1024 and above. Prime Performance Manager maintains the chosen port until the next server restart. 45751 and 55751 are good alternate ports for gateways and units respectively.
LOGINSERVER_PORT	The port on which the log in service listens. If you specify 0, Prime Performance Manager uses a random available port, 1024 and above. Prime Performance Manager maintains the chosen port until the next server restart. 45752 and 55752 are good alternate ports for gateways and units respectively.
WEB_PORT	The port on which the Prime Performance Manager gateway listens. You must specify a port number; 0 is not allowed. To change the WEB_PORT number, use the ppm webport command. See ppm webport, page B-62.

Table 17-1 Prime Performance Manager Ports (continued)

Port	Description
CLIENT_PORT	The port on which the Prime Performance Manager server listens for RMI callbacks (unsolicited notifications): • If you specify CLIENT_PORT = 0, Prime Performance Manager uses any available port, 1024 and above. • If you specify CLIENT_PORT with a single value other than 0, such as CLIENT_PORT = 33459, Prime Performance Manager uses that port, and you can run only one Prime Performance Manager unit process at a time. • If you specify CLIENT_PORT with a range of values other than 0, such as CLIENT_PORT = 33459-33479, Prime Performance Manager can use any of the ports in the range, including the beginning and ending ports, and you can run more than one Prime Performance Manager unit process at a time. Because a gateway server can connect to multiple units, specify a range if more than one unit is defined in the deployment. Because a unit connects to only one gateway, you only need to specify a single port.

To provision the firewall for gateway and unit communications:

Step 1 Identify the TCP ports that you want to use for two-way TCP connections between the gateway and unit and gateway and web client. See Table 17-1.

Step 2 Log into the gateway.

Step 3 Navigate to the directory containing the System.properties file.

If you installed Prime Performance Manager in the default directory, System.properties is located in the /opt/CSCOppm-gw/properties or /opt/CSCOppm-unit/properties directory.

If you installed Prime Performance Manager in a different location, specify the path where you installed Prime Performance Manager in place of the default (/opt) path.

Step 4 Back up the System.properties file.

Caution Always back up of the System.properties file before you edit it.

Step 5 Use a text editor to specify the appropriate port number where indicated. See Table 17-1 for port descriptions and values. For example:

For the gateway:

```
SERVER_NAME       = gateway123
RMIREGISTRY_PORT = 45742
DATASERVER_PORT  = 45751
LOGINSERVER_PORT = 45752
CLIENT_PORT       = 33459-33479
WEB_PORT          = 4440
```

For the unit:

```
SERVER_NAME      = unit123
RMIREGISTRY_PORT = 55742
DATASERVER_PORT  = 45751
LOGINSERVER_PORT = 45752
CLIENT_PORT      = 33459
GATEWAY_RMIREGISTRY_PORT = 45742
```

Step 6 Modify the device configuration files with the selected port numbers.

On Cisco devices, you can use extended access lists to allow the chosen TCP port numbers to pass between the appropriate interface(s). Assuming a single device separates the Prime Performance Manager gateway and unit servers, you can use the following extended access list:

Unit interface:

```
Interface FastEthernet 1/1
ip address 192.168.1.100 255.255.255.0
ip access-group unit-to-gateway in
```

Gateway interface:

```
interface FastEthernet 2/1
ip address 192.168.2.100 255.255.255.0
ip access-group gateway-to-unit in
```

These entries allow data to flow between the gateway and unit that initiated the session. Without these entries, units cannot access the gateway server.

Here is an access list entry to allow the unit and web browser connections to the gateway:

```
ip access-list extended unit-to-gateway
10 permit tcp any established
20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 45742
30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 45751
40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 45752
50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 33459
60 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 4440
```

Here is an access list to allow gateway connections to the unit:

```
ip access list extended gateway-to-unit
20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 55742
30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 55751
40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 55752
50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 33459
```

Step 7 Restart the gateway to use the new TCP ports. As the root user, enter:

```
#cd /opt/CSCOppm-gw/bin/ppm restart
```

The gateway and collocated unit processes restart using the new ports.

Step 8 If the unit properties changed, restart the units:

```
#cd /opt/CSCOppm-unit/bin/ppm restart
```

Both access list examples allow established TCP connections. When a unit or gateway establishes a TCP connection to the other end, it uses a fixed destination port. However, the source port from the initiating party is random. The established keyword allows a returning TCP packet to go back to the random initiating source port.

Configuring Unit and Device Communication

For units to communicate to devices through a firewall, SNMP Port 161 must be open. If you use reports that require SSH or Telnet, such as Y.1731 or EVC reports, the SSH or Telnet ports must be open between the units and devices as specified in the Telnet/SSH tab under Adminstration. The default port for Telnet is 23 and the default port for SSH is 22. The SNMP Trap port 162 does not need to be opened between devices and the units since PPM does not process SNMP traps from devices.

CHAPTER 18

Backing Up and Restoring Prime Performance Manager

The following topics tell you how to back up and restore Prime Performance Manager:

Prime Performance Manager Back Up and Restore Process

The Prime Performance Manager backup and restore function allows you to retrieve user accounts, logs, reports, and security-related parts of Prime Performance Manager data files from the previous night's backup. You should perform backup and restore in sets at the same clock time. Sets consists of a gateway and its units.

Note If backups are not performed in sets, data might become unsynchronized between the gateway and its units.

The backup and restore steps on a gateway and colocated unit include:

1. Backup is normally performed on the gateway at 3:30 AM and the unit at 2:30 AM. This spreads the load so they are both not backing up at exactly the same time.
2. Backup is restored to the gateway first.
3. Backup is restored to the unit.
4. The gateway is started.
5. The unit is started.

The backup and restore steps on a gateway and multiple units include:

1. Backup is normally performed on the gateway at 2:30 AM and all units at at 3:30 AM.
2. Backup is restored to the gateway first.
3. Backup is restored to each unit. These can be done in parallel.

4. The gateway is started
5. The units are started, either serially or in parallel.

Prime Performance Manager supports backup and restore on the same machine. Prime Performance Manager does not support:

- Taking a backup on one unit and restoring to another unit.
- Taking a backup on a gateway with one IP address and restoring to a gateway with a different IP address.

Note For very large networks, system responsiveness may temporarily degrade during backups.

Prime Performance Manager automatically backs up all Prime Performance Manager data files to Prime Performance Manager installation directory daily at same clock time.

To change the time at which Prime Performance Manager automatically backs up files, log in as the root user and change the *root crontab* file:

- **crontab -l** lists cron jobs.
- **crontab -e** opens up an editor so you can make changes and save them.

Related topics:

- Backing Up Prime Performance Manager Data Files, page 18-2
- Changing the Backup Directory, page 18-3
- Setting the Number of Backup Days, page 18-3
- Restoring Prime Performance Manager Data Files, page 18-3

Backing Up Prime Performance Manager Data Files

To manually back up Prime Performance Manager data files at any time on a Solaris or Linux server:

Step 1 Log in as the root user.

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Back up Prime Performance Manager files:

```
./ppm backup
```

Prime Performance Manager backs up the data files in the installation directory.

If you installed Prime Performance Manager in the default directory, */opt*, then the default backup directory is also */opt*. If you installed Prime Performance Manager in a different directory, then the default backup directory is that directory.

Changing the Backup Directory

To change the directory in which Prime Performance Manager stores its nightly backup files:

Step 1 Log in as the root user.

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Change the backup directory location:

./ppm backupdir *directory*

where *directory* is the new backup directory.

If the new directory does not exist, Prime Performance Manager does not change the directory, but issues an appropriate warning message.

Setting the Number of Backup Days

To set the number of days that Prime Performance Manager saves backup files:

Step 1 Log in as the root user.

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Change the number of backup days (default is 1):

```
./ppm backupdays
```

Step 4 Enter a value for the number of days from 1 to 30.

Prime Performance Manager will save backup files for the number of days that you entered. In this example, Prime Performance Manager saves backup files for the last five days, and deletes backup files that are older than five days.

Note Backups can take large amounts of data storage, so plan accordingly.

Restoring Prime Performance Manager Data Files

Prime Performance Manager supports backup and restore on the same machine. Prime Performance Manager does not support taking a backup on one unit and restoring to another, nor can you take a backup on a gateway with one IP address and restore it to a gateway with a different IP address.

To restore Prime Performance Manager, you can choose to restore all files, or only log files, reports, or security files.

To restore Prime Performance Manager from a previous backup:

Step 1 Log in as the root user.

Step 2 Change to the bin directory:

```
cd /opt/CSCOppm-gw/bin
```

Step 3 Restore Prime Performance Manager data files:

```
./ppm restore
```

To restore only parts of Prime Performance Manager, use the following keywords:

- **logs**—Restores only Prime Performance Manager log files.
- **reports**—Restores only Prime Performance Manager report files.
- **security**—Restores only the security-related parts of Prime Performance Manager data files. This option is useful if you inadvertently delete your user accounts or make other unwanted changes to your Prime Performance Manager security information.
- data—Restores only the database.
- etc—Restores only the configuration files and report definitions. This is useful if you removed or accidently edited the report definition files.

Step 4 To view statistics on the backup process, enter:

```
./ppm backupstats
```

Note If the number of backup days has been set to more than one day (see Setting the Number of Backup Days, page 18-3), Prime Performance Manager will prompt you for a server backup file restore from as there is no client backups.

Warning **Do not interrupt this command. Doing so can corrupt your Prime Performance Manager data files.**

APPENDIX A

Prime Performance Manager and IPv6

The following topics describe Prime Performance Manager IPv6 behavior and configuration practices:

IPv6 Support in Prime Performance Manager

You cannot use an IPv6 address for the Prime Performance Manager server name or gateway address. This means you cannot install the gateway with the IPv6 address and the web browser can't access the Prime Performance Manager web GUI using an IPv6 address. However, you can configure an IPv6 address in the gateway interface for communication with an IPv6 unit or between the Prime Performance Manager gateway and an IPv6 Prime Network gateway.

When integrating with Prime Network, Prime Network can't be IPv6 only because an IPv4 address is needed to do the cross-launches and send notification from Prime Network to Prime Performance Manager gateway.

Adding SNMP and Telnet/SSH Credentials

Prime Performance Manager can manage both IPv4 and IPv6 devices. The address format complies with the RFC 2732 and RFC 4291. To configure the credentials with wildcard matching, the IPv6 prefix can be used.

Unit Configuration

To allocate the devices to a different unit, you can configure the unit using either an IPv4 or an IPv6 address. The IPv4 CIDR or IPv6 prefix is supported for both IPv4 and IPv6. Always verify that the device is reachable from the Prime Performance Manager unit regardless of whether the device is IPv4 or IPv6.

Device Discovery

Unlike IPv4 device discovery, the IPv6 prefix can’t be used for device discovery. To match the IPv6 device for getting the credential used for discovery, the algorithm of longest match is used to find the SNMP or Telnet/SSH credential. If none is found, the default entry,::/0, is used.

For some software versions, the SNMP isn't supported over IPv6. Before applying your IPv6 settings to the device, verify that the software versions support SNMP over IPv6.

Reports

IPv4 and IPv6 devices can be polled by Prime Performance Manager units to generate stats reports. There is no difference in report itself regardless of whether the data is polled by an IPv4 or IPv6 address. For reports related to IP addresses, there is limitation on the device because most of the MIBs required for these reports don't support IPv6 addresses, for example, pseudowires, MPLS TE and VidMon. For reports with MIB data that supports IPv6, only IPSLA reports support the IPv6 in Prime Performance Manager in the current release. More are planned for the future.

Device Management Actions

For device management, you can perform the same actions on IPv6 devices as you can for IPv4 devices. For information about summary list actions, see Editing Summary List Items, page 8-9.

Alarms and Events

Similar as IPv4 device, the alarms or events generated for IPv6 device are also available in Alarm and Event GUI.

Clients

Only IPv4 address can be accessed by web browser to connect Prime Performance Manager gateway even if there is IPv6 address is configured in Prime Performance Manager gateway. This is the same as previous release. The IPv6 access to Prime Performance Manager gateway will be enhanced in next release.

Trap Forwarding

Trap forwarding can be configured in the Prime Performance Manager web GUI. Both IPv4 and IPv6 addresses are supported.

Prime Network Integration

Both IPv4 and IPv6 address can be used for Prime Network integration, including inventory import and cross-launch Installation. After installing the cross-launch with a Prime Network IPv6 address, the Prime Performance Manager gateway IPv4 address is used to navigate to the Prime Performance Manager web report from Prime Network. If notifications are sent out from Prime Network to Prime Performance Manager, the IPv4 address is used to connect to the Prime Performance Manager gateway.

Command Line Interface

IPv6 is supported by Prime Performance Manager that have an IP address as a parameter, such as snmpget/snmpwalk and addsnmpcomm, and others.

If you are using ipaccess to control the login access in a Prime Performance Manager gateway, verify that the addresses used by the Prime Performance Manager unit are in this access list. The access list must include both IPv4 and IPv6 addresses.

APPENDIX B

Command Reference

This appendix provides the format and a brief description of Cisco Prime Performance Manager commands, listed alphabetically. Each command is available on the:

- Server and Solaris or Linux both gateway and unit.
- Server and Solaris or Linux gateway only
- Server and Solaris or Linux unit only

You can run commands from:

- *install_directory*/bin

  where *install_directory* is the directory where Prime Performance Manager server is installed (by default, /opt/CSCOppm-gw or /opt/CSCOppm-unit)
- Alternatively, if you have the *install_directory*/bin in your path, you can run commands from your path.

This appendix contains:

- General Commands, page B-1

General Commands

General commands for Prime Performance Manager include:

- Prime Performance Manager, page B-5
- ppm addcreds, page B-5
- ppm addsnmpcomm, page B-5
- ppm addunitconf, page B-6
- ppm adduser, page B-6
- ppm authtype, page B-7
- ppm backup, page B-8
- ppm backupdays, page B-8
- ppm backupdir, page B-9
- ppm backuplog, page B-10
- ppm backupstats, page B-10
- ppm badloginalarm, page B-10

Prime Performance Manager

Command Description

Displays the command syntax for the Prime Performance Manager command and all of its options. The function of this command is identical to **/opt/CSCOppm-gw/bin/ppm help**.

Prime Performance Manager help is network specific, so only the commands pertaining to each network type appear. If you set all network types, you can see all the commands.

Related Topic

Chapter 3, "Using the Prime Performance Manager Web Interface"

ppm addcreds

Syntax

/opt/CSCOppm-gw/bin/ppm addcreds -i *ipaddress/hostname* [**-u** *user name* **-n** *enable_username*] [**-r** *protocoltype*] [**-o** *port*] [**-s** *sub_system*]

Command Description

Adds the Telnet and SSH credentials to access the device with the given IP address or host name.

- **-i** *ipaddress*—The device IP address or host name.
- **-u** *username*—The user name to log into the device.
- **-n** *enable_username*—Enables the privileged user name.
- **-r** *protocoltype*—Indicates the protocol type: Telnet, SSHv1, SSHv2, or WSMA over SSHv2.
- [**-o** *port*] —The port number used to access the device.
- [**-s** *sub_system*]—The subsystem used by transport protocol if a subsystem is defined on the device

ppm addsnmpcomm

Syntax

/opt/CSCOppm-gw/bin/ppm addsnmpcomm -i *ipaddress* [**-r** *retry* | **-t** *timeout* | **-p** *poll*] **-c** *community*

Command Description

Adds an SNMP configuration to Prime Performance Manager server.

- **-i** *ipaddress*—The IP address of the device (required)
- **-r** *retry*—The number of times to retry connecting to the device (optional)
- **-t** *timeout*—The timeout value, in seconds (optional)
- **-p** *poll*—The poll interval, in minutes (optional)
- **-c** *community*—The read community string of the device (required)

You do not need to restart Prime Performance Manager server.

Related Topic

- ppm deletesnmpcomm, page B-16
- ppm modifysnmpcomm, page B-31
- ppm showsnmpcomm, page B-44
- ppm snmpsetup, page B-50

ppm addunitconf

Syntax

/opt/CSCOppm-gw/bin/ppm addunitconf {**-i** *ipaddress* **|** **-u** *unitname* }

Command Description

Command uses the option -i (*ipaddress*) and -u (*unitname*) to add a unit configuration.

ppm adduser

Syntax

/opt/CSCOppm-gw/bin/ppm adduser [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access, adds the specified user to the authentication list.

When you add a user, Prime Performance Manager prompts you for this information:

- User's password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 6-5.
- Whether to force the user to change the password at the next log in. The default is not to force the user to change the password.
- Authentication level for the user. Valid levels are:
  - **1**—Basic User
  - **3**—Network Operator
  - **5**—System Administrator
  - **11**—Custom Level 1
  - **12**—Custom Level 2

You must log in as the root user to use this command.

Note If you enable Solaris authentication, you must log in as the root user, to use this command (see Implementing Secure User Access, page 6-2).

Related Topic

- Setting User Access, page 6-1
- Implementing Secure User Access, page 6-2

ppm authtype

Syntax

/opt/CSCOppm-gw/bin/ppm authtype [**local** | **solaris** | **linux**]

Command Description

Configures Prime Performance Manager security authentication:

- **local**—Allows you to create user accounts and passwords that are local to the Prime Performance Manager system. When using this method, you manage usernames, passwords, and access levels by using Prime Performance Manager commands.
- **solaris**—Uses standard Solaris-based user accounts and passwords, as the /etc/nsswitch.conf file specifies. You can provide authentication with the local /etc/passwd file. You can do this:
  - From a distributed Network Information Services (NIS) system

  Or

  - With any other authentication tool, such as RADIUS or TACACS+.
- **linux**—Uses standard Linux-based user accounts and passwords, as the */etc/nsswitch.conf* file specifies. You can provide authentication with the local */etc/passwd* file; from a distributed NIS system; or with any other authentication tool, such as RADIUS or TACACS+.

Note When using the Solaris or Linux options, if you have enabled user access, you must enable SSL (see Managing Prime Performance Manager Users, page 6-14 to ensure secure passwords between Prime Performance Manager client and server.)

You must log in as the root user to use this command.

Related Topic

- Setting User Access, page 6-1
- Implementing Secure User Access, page 6-2

ppm backup

Syntax

/opt/CSCOppm-gw/bin/ppm backup

Command Description

Note Because backups can be large, verify that your file system has enough space to handle the backups.

Backs up Prime Performance Manager data files to Prime Performance Manager installation directory. Prime Performance Manager automatically backs up all data files nightly at 1:30 AM. However, you can use this command to back up the files at any other time. If you installed Prime Performance Manager in:

- The default directory, /opt, then the locations of the backup files are /ppm10-$SERVERTYPE-$SERVERNAME-backup.tar, where $SERVERTYPE = gateway or unit as appropriate and $SERVERNAME = the name of the server as specified during installation.
- A different directory, then the backup files reside in that directory.

To restore Prime Performance Manager data files from the previous night's backup, use **/opt/CSCOppm-gw/bin/ppm restore** command. Do not try to extract the backup files manually.

You must log in as the root user to use this command.

Note Prime Performance Manager performs a database integrity check during the backup. If the check fails, the previous backup is not overwritten. Instead, Prime Performance Manager creates a new failed file (for example: ppm10-gateway-ems-lnx001-backup-failed.tar).

Related Topics

- ppm backupdays, page B-8
- ppm backupdir, page B-9
- ppm restore, page B-40

ppm backupdays

Syntax

/opt/CSCOppm-gw/bin/ppm backupdays [*days*]

Command Description

This command sets the number of days to save backup files on Prime Performance Manager server and client. The default value is one day, but you can configure Prime Performance Manager to save multiple days of backup files.

This command accepts values from 1 to 30 days. If you attempt to set a value outside of this range, Prime Performance Manager responds with this message:

```
Value out of range of 1-30.
```

Prime Performance Manager stores backup files in the backup directory (see ppm backupdir, page B-9). Prime Performance Manager uses this file naming convention when there are multiple backup files:

ppm<*releasenumber*>- [gateway|unit]-backup.tar.[*date*]

For example:

ppm10-gateway-ems-lnx001-backup.tar[*date*]

ppm10-unit-ems-lnx001-backup.tar[*date*]

If the number of backup days is more than one, and you run the **/opt/CSCOppm-gw/bin/ppm restore** command, Prime Performance Manager prompts you for a server or client backup file to restore from. This is because there would be more than one backup file to choose from). See ppm restore, page B-40.

The following is an example of setting the number of backup days to five days:

```
# ./ppm backupdays

Current value is: 1

Enter number of days to save backup files <1-30>: [1] 5

Setting number of days to save backup files to 5 days.
```

In this example, Prime Performance Manager saves backup files for the last five days. Prime Performance Manager deletes backup files that are older than five days.

Note If you notice multiple backups, ensure that there is enough free space in the backupdir file system (see ppm backupdir, page B-9).

Related Topic

- Backing Up Prime Performance Manager Data Files, page 18-2
- ppm backupdir, page B-9
- ppm restore, page B-40

ppm backupdir

Syntax

/opt/CSCOppm-gw/bin/ppm backupdir [*directory*]

Command Description

Note You must stop Prime Performance Manager server before performing this command. You are prompted whether you want to continue.

You can change the directory in which Prime Performance Manager stores its nightly backup files. The default backup directory is the directory in which Prime Performance Manager is installed. If you installed Prime Performance Manager in:

- The default directory, /opt, then the default backup directory is also /opt.
- A different directory, then the default backup directory is that directory.

If you specify a new directory that does not exist, Prime Performance Manager does not change the directory and issues an appropriate message.

You must log in as the root user to use this command.

Related Topic

- ppm backupdays, page B-8

ppm backuplog

Syntax

/opt/CSCOppm-gw/bin/ppm backuplog [*clear* | *-r*]

Command Description

Uses PAGER to display the contents of the system backup log.

To clear the log, enter **/opt/CSCOppm-gw/bin/ppm backuplog clear**.

To display the contents of the log in reverse order, with the most recent commands at the beginning of the log, enter **/opt/CSCOppm-gw/bin/ppm backuplog -r**.

You must log in as the root user to use this command.

ppm backupstats

Syntax

/opt/CSCOppm-gw/bin/ppm backupstats

Command Description

This command displays statistics on backup process. You must log in as the root user to use this command.

ppm badloginalarm

Syntax

/opt/CSCOppm-gw/bin/ppm badloginalarm [*tries* | *clear*]

Command Description

Number of unsuccessful log-in attempts allowed before Prime Performance Manager generates an alarm.

There can be an unlimited number of unsuccessful attempts. The default value is five unsuccessful attempts.

Prime Performance Manager records alarms in the system security log file. The default path and filename for the system security log file is /opt/CSCOppm-gw/logs/sgmSecurityLog.txt. If you installed Prime Performance Manager in a directory other than /opt, then the system security log file resides in that directory.

To view the system security log file, enter **/opt/CSCOppm-gw/bin/ppm seclog**. You can also view the system security log on Prime Performance Manager System Security Log web page (see Displaying the Contents of the System Security Log, page 6-13).

To disable this function (that is, to prevent Prime Performance Manager from automatically generating an alarm after unsuccessful log-in attempts), enter **/opt/CSCOppm-gw/bin/ppm badloginalarm clear**.

You must log in as the root user to use this command.

Related Topic

Automatically Disabling Users and Passwords, page 6-7

ppm badlogindisable

Syntax

/opt/CSCOppm-gw/bin/ppm badlogindisable [*tries* | *clear*]

Command Description

Number of unsuccessful log-in attempts by a user allowed before Prime Performance Manager disables the user's authentication. To re-enable the user's authentication, use **/opt/CSCOppm-gw/bin/ppm enableuser** command.

There can be an unlimited number of unsuccessful attempts. The default value is 10 unsuccessful attempts.

To disable this function (that is, to prevent Prime Performance Manager from automatically disabling a user's authentication after unsuccessful log-in attempts), enter **/opt/CSCOppm-gw/bin/ppm badlogindisable clear**.

You must log in as the root user to use this command.

Related Topic

Automatically Disabling Users and Passwords, page 6-7

ppm certtool

Syntax

/opt/CSCOppm-gw/bin/ppm certtool [**clear** | **delete** *alias* | **export** *alias* [**-file** *filename*] | **import** *alias* [**-file** *filename*] | **list**]

Command Description

If you enable the Secure Sockets Layer (SSL) icon your Prime Performance Manager system, you can use this command to manage SSL certificates on Prime Performance Manager web interface from the command line.

Note If you installed Prime Performance Manager server gateway and unit on the same workstation, running this command is not necessary. Instead, when you use the **/opt/CSCOppm-gw/bin/ppm keytool** command to manage SSL certificates on the server, Prime Performance Manager automatically manages the certificates on the web interface.

Use these keywords and arguments with this command:

- **import** *alias* [**-file** *filename*]—Imports a signed SSL certificate in X.509 format. This is the most common use for this command.

  The *alias* argument can be any character string; the hostname of the server from which you are importing the certificate is a good choice.

  To import the certificate from a file, specify the optional **-file** keyword and a filename.

- **export** *alias* [**-file** *filename*]—Exports the specified SSL certificate in X.509 format.

  To export the certificate to a file, specify the optional **-file** keyword and a filename.
- **list**—Lists all SSL certificates on Prime Performance Manager.
- **delete** *alias*—Removes the specified SSL certificate from Prime Performance Manager.
- **clear**—Removes all SSL certificates from Prime Performance Manager.

Solaris Only: You must log in as the root user to use this command in Solaris.

Related Topic

Viewing and Exporting SSL Certificates, page 5-4

ppm crosslaunch

Syntax

/opt/CSCOppm-gw/bin/ppmcrosslaunch [*install* | *uninstall*]

Command Description

Manages the cross launch points for Prime Network (Cisco ANA) through Prime Performance Manager.

install—Creates the cross-launch menu items in Prime Network (Cisco ANA) Network Vision , so Prime Performance Manager reports can be launched from Prime Network.

uninstall— Removes the cross-launch menu items from Prime Network (Cisco ANA) Network Vision.

ppm changes

Command Description

Displays the contents of the Prime Performance Manager CHANGES file. The CHANGES file lists all bugs that have been resolved in Prime Performance Manager, sorted by release. If you installed Prime Performance Manager in:

- The default directory, /opt, then Prime Performance Manager CHANGES file resides in the /opt/CSCOppm-gw/install directory.
- A different directory, then the file resides in that directory.

ppm checksystem

Command Description

Checks the system for a server installation and reviews the:

- System requirements
- TCP/IP address and port usage checks
- Disk space usage check
- Server summary
- Error summary

You must log in as the root user to use all features of this command. The logs/troubleshooting folder has limited permissions to read when the user is not a root user.

ppm clitimeout

Syntax

/opt/CSCOppm-gw/bin/ppm clitimeout [*mins* | *clear*]

Command Description

Specifies how long, in minutes, an Prime Performance Manager client can be inactive before Prime Performance Manager automatically disconnects it.

This function is disabled by default. If you do not specify this command, clients are never disconnected as a result of inactivity.

If you enter **/opt/CSCOppm-gw/bin/ppm clitimeout** command, the valid range is one minute to an unlimited number of minutes. No default value exists.

If you enable this function and you want to disable it (that is, never disconnect a client as a result of inactivity), enter **/opt/CSCOppm-gw/bin/ppm clitimeout clear** command.

You must log in as the root user to use this command.

Related Topic

Automatically Disabling Users and Passwords, page 6-7

ppm cmdlog

Syntax

/opt/CSCOppm-gw/bin/ppm cmdlog [**clear** | **-r**]

Command Description

Uses PAGER to display the contents of the system command log. The system command log lists:

- All **ppm** commands that were entered for the Prime Performance Manager server.
- The time each command was entered.
- The user who entered the command.

To clear the log, enter **ppm cmdlog clear**.

To display the contents of the log in reverse order, with the most recent commands at the beginning of the log, enter **ppm cmdlog -r**.

You must log in as the root user to use this command.

ppm compilemibs

Syntax

/opt/CSCOppm-gw/bin/ppm compilemibs

Command Description

Compiles MIB files in the /opt/CSCOppm-gw/etc/mibs folder and generates a compiled output file. During execution the system reports inconsistencies like duplicate varaibles names, duplicate OIDs and missing dependant MIBs. After it has completed, you are prompted to reload the compiled output to the Prime Performance Manager server.

This command is available only on the gateway.

ppm console

Command Description

Displays the contents of the console log file, sgmConsoleLog.latest.

The console log file contains unexpected error and warning messages from Prime Performance Manager server, such as those that might occur if Prime Performance Manager server cannot start.

You must log in as the root user to use this command.

ppm consolelogsize

Syntax

/opt/CSCOppm-gw/bin/ppm consolelogsize [*megs*]

Command Description

Sets the maximum size (in megabytes) of the console log file.

To view help for this command, include the following parameter: **-h**.

ppm countnodes

Command Description

Displays the number of nodes in the current Prime Performance Manager database.

You must log in as the root user to use this command.

ppm datadir

Syntax

/opt/CSCOppm-gw/bin/ppm datadir [*directory* | *nostart*]

Command Description

Note You must stop Prime Performance Manager server before performing this command. You are prompted whether to continue.

Sets the directory in which Prime Performance Manager stores data files. Use this command when you want to move the data directory to a larger filing system to accommodate the increasing size of the directory.

The default directory for data files resides in the Prime Performance Manager installation directory. If you installed Prime Performance Manager in:

- The default directory, /opt, then the default directory is /opt/CSCOppm-gw/data.
- A different directory, then the default directory resides in that directory.

Use this command if you want to store data files in a different directory; for example, in a Network File System location on another server.

After you change the directory, Prime Performance Manager prompts to confirm whether you want to restart Prime Performance Manager server. The new directory takes effect when you restart Prime Performance Manager server.

You must log in as the root user to use this command.

ppm delete

Syntax

/opt/CSCOppm-gw/bin/ppm delete [**all** | **node** [**all** | *node* [*node*]...] | **sp** [**all** | *point-code*:*net* [*point-code*:*net*]...] | **linkset** [**all** | *node*/*linkset* [*node*/*linkset*]...]

Command Description

Deletes objects from Prime Performance Manager database.

- **all**—Deletes all objects from Prime Performance Manager database.
- **node all**—Deletes all nodes from Prime Performance Manager database.
- **node** *node* [*node*]...—Deletes one or more nodes from Prime Performance Manager database. Use the *node* arguments to specify one or more nodes.
- **sp all**—Deletes all nodes from Prime Performance Manager database.
- **sp** *point-code*:*net* [*point-code*:*net*]...—Deletes one or more signaling points from Prime Performance Manager database. Use the *point-code*:*net* arguments to specify one or more signaling points, which the point code and network name identify; for example, 1.22.0:net0.
- **linkset all**—Deletes all linksets from Prime Performance Manager database.
- **linkset** *node*/*linkset* [*node*/*linkset*]...—Deletes one or more linksets from Prime Performance Manager database. Use the *node*/*linkset* arguments to specify one or more linksets associated with specific nodes.

You must log in as the root user to use this command.

ppm deletecreds

Syntax

/opt/CSCOppm-gw/bin/ppm deletecreds -i [*ipaddress/hostname*] **-a**

Command Description

Deletes the Telnet and SSH device credentials for the specified device or all credentials on the Prime Performance Manager gateway.

-i *ipaddress/hostname*—Deletes the Telnet and SSH device credentials for the specified IP address or host name.

-a—Deletes all Telnet and SSH device credentials on the gateway.

ppm deletesnmpcomm

Syntax

/opt/CSCOppm-gw/bin/ppm deletesnmpcomm -i *ipaddress*

Command Description

Deletes an SNMP configuration from Prime Performance Manager server.

-i *ipaddress*—The IP address of the device (required)

You do not need to restart Prime Performance Manager server.

Related Topic

- ppm addsnmpcomm, page B-5
- ppm modifysnmpcomm, page B-31
- ppm showsnmpcomm, page B-44
- ppm snmpsetup, page B-50

ppm deluser

Syntax

/opt/CSCOppm-gw/bin/ppm deluser [*username*]

Command Description

If you enable Prime Performance Manager user-based access, deletes the specified user from the authentication list. To add the user back to the list, use **/opt/CSCOppm-gw/bin/ppm adduser** command.

You must log in as the root user to use this command.

Related Topic

Manually Disabling Users and Passwords, page 6-9

ppm deleteunitconf

Syntax

/opt/CSCOppm-gw/bin/ppm deleteunitconf [-i (*ipaddress*)]

Command Description

This command deletes the existing configuration that specifies the relationship between nodes and their managed units.

ppm disablepass

Syntax

/opt/CSCOppm-gw/bin/ppm disablepass [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access, and set **ppm authtype** to **local**, disables the specified user's authentication and password. Prime Performance Manager does not delete the user from the authentication list.

Prime Performance Manager only disables the user's authentication and password. To re-enable the user's authentication with:

- The same password as before, use **/opt/CSCOppm-gw/bin/ppm enableuser** command.
- A new password, use **/opt/CSCOppm-gw/bin/ppm userpass** command.

Note The user can re-enable authentication with a new password by attempting to log in by using the old password; Prime Performance Manager then prompts the user for a new password.

If you set **/opt/CSCOppm-gw/bin/ppm authtype** to **Solaris** or **Linux**, you cannot use this command; instead, you must manage passwords on the external authentication servers.

You must log in as the root user to use this command. You must also set **/opt/CSCOppm-gw/bin/ppm authtype** to **local**.

Related Topic

Manually Disabling Users and Passwords, page 6-9

ppm disableuser

Syntax

/opt/CSCOppm-gw/bin/ppm disableuser [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access, this disables the specified user's authentication. Prime Performance Manager does not delete the user from the authentication list, Prime Performance Manager only disables the user's authentication. To re-enable the user's authentication with:

- The same password as before, use the **/opt/CSCOppm-gw/bin/ppm enableuser** command.
- A new password, use the **/opt/CSCOppm-gw/bin/ppm userpass** command.

You must log in as the root user to use this command.

Related Topic

Manually Disabling Users and Passwords, page 6-9

ppm discover

Syntax

/opt/CSCOppm-gw/bin/ppm discover [*seed-node*] [*seed-node*]...

Command Description

You use this command to discover the network from the command line. Use the *seed-node* arguments to specify the DNS names or IP addresses of one or more seed nodes.

You must log in as the root user to use this command.

Related Topic

Managing Network Discovery, page 4-5

ppm diskmonitor

Syntax

/opt/CSCOppm-gw/bin/ppm diskmonitor [**enable** | **disable** | **status**] | **warning** [*megs]* | **shutdown** [*megs]* | ***stopscript*** *[path]*

Command Description

Monitors the disk space usage of Prime Performance Manager installed directories. When enabled, a script (*diskWatcher.sh*) runs every hour to check two thresholds:

- Warning—Warns Prime Performance Manager operator when the disk space usage exceeds the threshold value. Prime Performance Manager logs the warning in the sgmConsoleLog.txt file. For example:

```
WARNING: The following partition is getting low on free disk space:
                              /opt
                              Space left = 905 MB
```

- Shutdown—Shuts down Prime Performance Manager server when the disk space usage exceeds the threshold value.

The parameters of Prime Performance Manager **diskmonitor** command are:

- **enable**—Enables the hourly check of disk space usage of Prime Performance Manager installed directories.
- **disable**—Disables the hourly check of disk space usage of Prime Performance Manager installed directories.
- **status**—Displays the current status of the disk monitor feature (whether enabled or disabled).
- **warning** [*megs]*—Sets the warning threshold in MBs. The default setting is 1000 MB.

- **shutdown** [*megs]*—Sets the shutdown threshold in MBs. The default setting is 100 MB.
- **stopscript** [*path*]—Sets the custom script to call for stop.

You must log in as the root user to use this command.

ppm enableuser

Syntax

/opt/CSCOppm-gw/bin/ppm enableuser [*username*]

Command Description

If you enable Prime Performance Manager user-based access, re-enables the specified user's authentication, which had been disabled either automatically by Prime Performance Manager root user.

The user's authentication is re-enabled with the same password as before.

You must log in as the root user to use this command.

Related Topic

Enabling and Changing Users and Passwords, page 6-10

ppm eventautolog

Syntax

/opt/CSCOppm-gw/bin/ppm eventautolog [**clear** | **-r**]

Command Description

Uses PAGER to display the contents of Prime Performance Manager event automation log. The event automation log lists all messages generated by scripts launched by event automation.

To clear the log and restart the server, enter **/opt/CSCOppm-gw/bin/ppm eventautolog clear**.

To display the contents of the log in reverse order, with the most recent events at the beginning of the log, enter **/opt/CSCOppm-gw/bin/ppm eventautolog -r**.

You must log in as the root user to use this command.

ppm eventconfig

Syntax

/opt/CSCOppm-gw/bin/ppm eventconfig [**view** | **edit** |**restore** | **master**]

Command Description

Allows you to manage the event configuration:

- To view the event configuration file, use the **ppm eventconfig view** command.
- To edit the event configuration file in your environment with a text editor, use **/opt/CSCOppm-gw/bin/ppm eventconfig edit** command. (The default text editor is 'vi'.)

- To restore the event configuration file to the last active copy, use the **/opt/CSCOppm-gw/bin/ppm eventconfig restore** command.
- To restore the event configuration file to the master copy (the default copy shipped with Prime Performance Manager), use the **/opt/CSCOppm-gw/bin/ppm eventconfig master** command.

You must log in as the root user to use this command.

ppm eventtool

Syntax

/opt/CSCOppm-gw/bin/ppm eventtool {**-a** *actionName*} {*parameters*}

Command Description

Invokes Prime Performance Manager event API operations.

These action names (and any corresponding required parameters) can be specified with the **-a** option:

Option	Action Names	Required Parameters
-a	acknowledgeEvents	**-l** or **-L** **-u** **-n**
	appendNote	**-e** **-n** **-u**
	changeSeverities	**-s** **-l** or **-L** **-u** **-n**
	clearEvents	**-l** or **-L** **-u** **-n**
	deleteEvents	**-l** or **-L** **-u** **-n**
	getAllEventsAsTraps	**-t**
	getFilteredEventsAsTraps	**-t** **-f**
	getNote	**-e**
	setNote	**-e** **-n** **-u**

These parameters can be used:

Parameter	Description
-e	Specifies an event ID parameter.
-f	Specifies a file name for EventFilter, which is an XML element defined in Prime Performance Manager WSDL definitions.
-l	Specifies a file name for EventIDList, which is an XML element defined in Prime Performance Manager WSDL definitions.
-n	Specifies an event note string.
-s	Specifies an event severity.
-t	Specifies a file name for TrapTarget, which is an XML element defined in Prime Performance Manager WSDL definitions.
-u	Specifies a user ID for event operation.
-H	Specifies a hostname to connect to. If unspecified, the default value is obtained from the Prime Performance Manager server System.properties file, SERVER_NAME property.
-p	Specifies a port to connect to. If unspecified, the default value is obtained from the Prime Performance Manager server *System.properties* file, WEB_PORT property.
-L	Specifies a list of event IDs, separated by '|'.
-S	Specifies whether to use SSL (https) for NBAPI access. Default is no SSL.
-h	Prints help information.

You must log in as the root user to use this command.

Related Documentation

See http://www.cisco.com/go/performance

ppm evilstop

Command Description

Forcefully stops all Prime Performance Manager servers on the local host.

You must log in as the root user to use this command.

ppm export

Syntax

/opt/CSCOppm-gw/bin/ppm export

Command Description

Exports current Prime Performance Manager data.

You must log in as the root user to use this command.

ppm exportcustnames

Syntax

/opt/CSCOppm-gw/bin/ppm exportcustnames

Command Description

Allows to export custom names for import to another server.

ppm export cw

Syntax

/opt/CSCOppm-gw/bin/ppm export cw

Command Description

Exports current Prime Performance Manager node names, and read and write SNMP community names, in CiscoWorks v2 import format, with fields separated by commas (,). You can export this data to a file, then use the file to import the nodes into the CiscoWorks database.

You must log in as the root user to use this command.

ppm export cwv3

Syntax

/opt/CSCOppm-gw/bin/ppm export cwv3

Command Description

Exports current Prime Performance Manager node names, and read and write SNMP community names, in CiscoWorks v3 import format, with fields separated by commas (,). You can export this data to a file, then use the file to import the nodes into the CiscoWorks database.

You must log in as the root user to use this command.

ppm exportusers

Syntax

/opt/CSCOppm-gw/bin/ppm exportusers

Command Description

Allows to export users for import to another server.

ppm genkey

Syntax

/opt/CSCOppm-gw/bin/ppm genkey[**gw**|**unit**|**both**|]

Command Description

Creates SSL keys and certificates. The command provides an easy way to regenerate SSL keys and certificates after the Prime Performance Manager has been running for a while with SSL enabled. This might be needed if a certificate expires or if you have a policy to regenerate the certificates after a period of time. The command is normally used as:

```
ppm genkey both
```

The **both** option generates new keys and certificates, then exchanges them between gateway and unit automatically so you can regenerate the set of keys and certifications at one time. If you use only the gw or unit option, you must import the certificates to the other side.

Note To run this command, you must have Prime Performance Manager 1.1.1 installed.

ppm help

Syntax

/opt/CSCOppm-gw/bin/ppm help [*keyword*]

Command Description

Displays the command syntax for the Prime Performance Manager command and all of its options. The function of this command is identical to **Prime Performance Manager.**

Prime Performance Manager help is network specific, so only the commands pertaining to each network type appear. If you set all network types, you can see all the commands.

To see the syntax for a specific command, enter **/opt/CSCOppm-gw/bin/ppm help** and that command. For example, if you enter **/opt/CSCOppm-gw/bin/ppm help restart**, Prime Performance Manager displays:

```
ppm restart     - Restarts all ppm Servers on the local host.
ppm restart web - Restarts Web servers on the local host.
ppm restart jsp - Restarts JSP servers on the local host.
ppm restart pm  - Restarts Process Manager on the local host.
```

Related Topic

Chapter 3, "Using the Prime Performance Manager Web Interface"

ppm importcustnames

Syntax

/opt/CSCOppm-gw/bin/ppm importcustnames [*inputfile*]

Command Description

Allows to import custom names from another server.

ppm importcw

Syntax

/opt/CSCOppm-gw/bin/ppm importcw [*cwfile*]

Command Description

Imports node hostname and read-community strings from the CiscoWorks server to Prime Performance Manager.

cwfile—File name of the CiscoWorks export file (export format must be in CSV file format).

You must log in as the root user to use this command. You do not need to restart the server to activate this command. After running this command, Prime Performance Manager discovers the imported nodes.

ppm inactiveuserdays

Syntax

/opt/CSCOppm-gw/bin/ppm inactiveuserdays [*days* | *clear*]

Command Description

If you enable Prime Performance Manager user-based access, number of days a user can be inactive before disabling that user account.

This function is disabled by default. If you do not specify this command, user accounts are never disabled as a result of inactivity.

If you enter the **ppm inactiveuserdays** command, the valid range is one day to an unlimited number of days. There is no default setting.

If you have enabled this function and you want to disable it (that is, prevent Prime Performance Manager from automatically disabling user accounts as a result of inactivity), enter **/opt/CSCOppm-gw/bin/ppm inactiveuserdays clear**.

To re-enable the user's authentication, use **/opt/CSCOppm-gw/bin/ppm enableuser** command.

You must log in as the root user to use this command.

Related Topics

- Chapter 6, "Setting Up and Managing Users"
- Automatically Disabling Users and Passwords, page 6-7

ppm installlog

Syntax

/opt/CSCOppm-gw/bin/ppm installlog [*server* | *client*]

Command Description

Displays the latest install log for the **server** or **client**. If you do not specify **server** or **client**, displays the latest install log for both the server and client.

You must log in as the root user to use this command.

ppm inventoryimport

Syntax

/opt/CSCOppm-gw/bin/ppm inventoryimport [- *strictSync* | - *looseSync*]

Command Description

Imports device information from Prime Network (Cisco ANA) device inventory.

strictSync — In Strict Synchronization mode, only Prime Network type of devices are discovered.

looseSync — In Loose Synchronization mode, beside the devices imported from Prime Network, Prime Performance Manager can manage devices that are not in Prime Network inventory.

ppm iosreport

Syntax

/opt/CSCOppm-gw/bin/ppm iosreport

Command Description

Lists the IOS versions of all devices that are managed by Prime Performance Manager. The command's CSV output format is:

node name, custom name, node type, IOS version, serial number, system name, system location. IP address

Note To run this command, you must log in as the root user and have Prime Performance Manager 1.1.1 installed.

ppm ipaccess

Syntax

ppm ipaccess [**add** [*ip-addr*] | **clear** | **edit** | **list** | **rem** [*ip-addr*] | **sample**]

Command Description

You use this command to create and manage a list of client IP addresses that can connect to the Prime Performance Manager server.

The list of allowed client IP addresses resides in the ipaccess.conf file. By default, when you first install Prime Performance Manager, the ipaccess.conf file does not exist and all client IP addresses can connect to Prime Performance Manager server.

To create the ipaccess.conf file and specify the list of allowed client IP addresses, use one of these keywords:

- **add**—Add the specified client IP address to the ipaccess.conf file. If the ipaccess.conf file does not already exist, this command creates a file with the first entry.
- **clear**—Remove all client IP addresses from the ipaccess.conf file and allow connections from any Prime Performance Manager client IP address.
- **edit**—Open and edit the ipaccess.conf file directly. If the ipaccess.conf file does not already exist, this command creates an empty file.
- **list**—List all client IP addresses currently in the ipaccess.conf file. If no client IP addresses appear (that is, the list is empty), connections from any Prime Performance Manager client IP address are allowed.
- **rem**—Remove the specified client IP address from the ipaccess.conf file.
- **sample**—Print out a sample ipaccess.conf file.

Any changes you make take effect when you restart Prime Performance Manager server.

See Implementing Secure User Access, page 6-2 for more information about using this command.

You must log in as the root user to use this command.

ppm ipslaftpfilesize

Syntax

/opt/CSCOppm-gw/bin/ppm ipslaftpfilesize [*file size in bytes*]

Command Description

When an IP SLA probe sends FTP transfer requests to a remote server, it retrieves a file with a specified size from the FTP server. This command tells Prime Performance Manager the size of the file, so it can compute the transfer rate. Unless you use this command to specify otherwise, Prime Performance Manager assumes the FTP file size is 1 MB.

Note To run this command, you must have Prime Performance Manager 1.1.1 installed.

ppm jspport

Syntax

/opt/CSCOppm-gw/bin/ppm jspport [*port-number*]

Command Description

Sets a new port number for the JSP server, where *port-number* is the new, numeric port number. Prime Performance Manager verifies that the new port number is not already in use.

This command is needed only if you change the port number after you install Prime Performance Manager. This is because another application must use the current port number.

The new port number must contain only numbers. If you enter a port number that contains nonnumeric characters, such as **ppm13**, an error message appears, and Prime Performance Manager returns to the command prompt without changing the port number.

You must log in as the root user to use this command.

ppm keytool

Syntax

/opt/CSCOppm-gw/bin/ppm keytool [**clear** | **genkey** | **import_cert** *cert_filename* | **import_key** *key_filename cert_filename* | **list** | **print_csr** | **print_crt**]

Command Description

If you implement SSL in your Prime Performance Manager system, manages SSL keys and certificates on Prime Performance Manager server.

Use these keywords and arguments with this command:

- **clear**—Stops Prime Performance Manager server, if necessary, and removes all SSL keys and certificates from the server. Before restarting the server, you must either generate new SSL keys by using the **ppm keytool genkey** command; or, you must completely disable SSL by using the **ppm ssl disable** command.
- **genkey**—Stops Prime Performance Manager server, if necessary, and generates a new self-signed public or private SSL key pair on Prime Performance Manager server. The new keys take effect when you restart the server.
- **import_cert** *cert_filename*—Imports the specified signed SSL certificate in X.509 format.
- **import_key** *key_filename cert_filename*—Imports the specified SSL key in OpenSSL format and the specified signed SSL certificate in X.509 format.
- **list**—Lists all SSL key-certificate pairs on Prime Performance Manager server.
- **print_csr**—Prints a certificate signing request (CSR) in X.509 format.
- **print_crt**—Prints Prime Performance Manager server's SSL certificate in X.509 format.

You must log in as the root user to use this command.

Related Topic

Managing Prime Performance Manager Users, page 6-14

ppm listusers

Syntax

/opt/CSCOppm-gw/bin/ppm listusers [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access, lists all currently defined users in the authentication list, including this information for each user:

- Username.
- Last time the user logged in.
- User's authentication access level.
- User's current authentication status, such as Account Enabled or Password Disabled.

To list information for a specific user, use the *username* argument to specify the user.

You must log in as the root user to use this command.

Related Topic

Listing All Currently Defined Users, page 6-12

ppm logger

Command Description

Displays the system messages *messageLog.txt* file with tail -f.

To stop the display, press **Ctrl-C**.

ppm logsize

Syntax

/opt/CSCOppm-gw/bin/ppm logsize [*number-of-lines*]

Command Description

Sets the maximum size for truncating and rolling log files.

- Message log files are in *$LOGDIR/*messageLog-archives (typically, /opt/CSCOppm-gw/logs/messageLog-archives).
- Network log files are in *$LOGDIR*/netStatus/archive

If you enter this command without the *number-of-lines* argument, Prime Performance Manager displays the current maximum number of lines. You can change this value.

The message and network log process archives the log file when the maximum number of lines is reached. The filename format of archived log files is:

- messageLog.*YYYY*:*MMDD*:*hhmm*:*y*.txt.Z or

- networkLog.*YYYY*:*MMDD*:*hhmm*:*y*.txt.Z

where:

- *YYYY* is the year
- *MM* is the month in a two-digit format
- *DD* is the day of the month
- *hh* is the hour of the day in 24-hour notation
- *mm* is the minute within the hour
- *y* is one of these variables:

Variable	Meaning	Example
r	The log file was created because Prime Performance Manager server restarted.	messageLog.2008:0328:1427:r.txt.Z networkLog.2008:0328:1427:r.txt.Z
c	The log file was created because a user ran **/opt/CSCOppm-gw/bin/ppm msglog clear** command.	messageLog.2008:0328:1433:c.txt.Z networkLog.2008:0328:1433:c.txt.Z
o	The log file was created from a pre-existing messageLog-old.txt file (used in previous Prime Performance Manager releases).	messageLog.2008:0328:1413:o.txt.Z networkLog.2008:0328:1413:o.txt.Z
0 (or higher number)	A counter that starts at 0 and increments sequentially. The number resets to 0 when the server restarts.	messageLog.2008:0328:1427:3.txt.Z networkLog.2008:0328:1427:3.txt.Z

When messageLog.txt or networkLog.txt reaches the number of lines specified by **/opt/CSCOppm-gw/bin/ppm logsize** command, Prime Performance Manager creates a new log archive file by using the filename format above.

When the maximum number of lines is reached, the log filename contains a counter value to differentiate itself from other archived files (for example, messageLog.2011:0328:1427:1.txt.Z and messageLog.2011:0328:1427:2.txt.Z).

The default value for *number-of-lines* is 500,000 lines.

The valid range is 1,000 lines to an unlimited number of lines. The default value is 500,000 lines. If you specify a larger file size for the log file, the log file and its copy require proportionally more disk space.

When changing the number of lines to display, remember that every 5,000 lines require approximately 1 MB of disk space. You need to balance your need to refer to old messages against the amount of disk space they occupy.

Note All log files are aged out by a timing mechanism (**/opt/CSCOppm-gw/bin/ppm msglogage**). You can estimate a size for the *$LOGDIR/*messageLog-archives directory based on the number of lines, the amount of data that is logged (**/opt/CSCOppm-gw/bin/ppm mldebug**), and the log age.

You must log in as the root user to use this command. If you change the *number-of-lines* value, you must restart the server (**/opt/CSCOppm-gw/bin/ppm restart**).

ppm logtimemode

Syntax

/opt/CSCOppm-gw/bin/ppm logtimemode [**12** | **24**]

Command Description

Sets the time mode for dates in log files:

- **12**—Use 12-hour time, with AM and PM so that 1:00 in the afternoon is 1:00 PM.
- **24**—Use 24-hour time, also called military time so that 1:00 in the afternoon is 13:00. This is the default setting.

You must log in as the root user to use this command.

ppm maxhtmlrows

Syntax

/opt/CSCOppm-gw/bin/ppm maxhtmlrows [*number-of-rows*]

Command Description

Sets the maximum number of rows for Prime Performance Manager HTML web output; for example, statistics reports, status change messages, or SNMP trap messages.

Note If you have set the Page Size on Prime Performance Manager web interface, this command does not override that setting. When you set the Page Size feature on the Prime Performance Manager web interface, browser cookies store the setting until the cookie expires or Prime Performance Manager deletes it.

If you enter this command without the *number-of-rows* argument, Prime Performance Manager displays the current maximum number of rows. You can then change that value or leave it. The valid range is one row to an unlimited number of rows. The default value is 100 rows.

You must log in as the root user to use this command.

Related Topic

Chapter 3, "Using the Prime Performance Manager Web Interface"

ppm mldebug

Syntax

/opt/CSCOppm-gw/bin/ppm mldebug [*mode*]

Command Description

Sets the mode for logging Prime Performance Manager debug messages:

- **normal**—Logs all action, error, and info messages. Use **ppm mldebug normal** to revert to the default settings if you accidentally enter **ppm mldebug** command.
- **list**—Displays the current settings for **ppm mldebug** command.

- **all**—Logs all messages, of any type.
- **none**—Logs no messages at all.
- **minimal**—Logs all error messages.
- **action**—Logs all action messages.
- **debug**—Logs all debug messages.
- **dump**—Logs all dump messages.
- **error**—Logs all error messages.
- **info**—Logs all info messages.
- **NBAPI-SOAP**—Logs all northbound SOAP messages.
- **snmp**—Logs all SNMP messages.
- **trace**—Logs all trace messages.
- **trapsIn**—Logs all incoming trap messages.
- **trapsOut**—Logs all outgoing trap messages.

This command can adversely affect Prime Performance Manager performance. Use this command **only** under guidance from the Cisco Technical Assistance Center (TAC).

You must log in as the root user to use this command.

ppm modifysnmpcomm

Syntax

/opt/CSCOppm-gw/bin/ppm modifysnmpcomm -i *ipaddress* {**-r** *retry* | **-t** *timeout* | **-p** *poll* **-c** *community*}

Command Description

Modifies an existing SNMP configuration on Prime Performance Manager server.

- **-i** *ipaddress*—the IP address of the device (required)
- At least one of the following:
  - **-r** *retry*—the number of times to retry connecting to the device
  - **-t** *timeout*—the timeout value, in seconds
  - **-p** *poll*—the poll interval, in minutes
  - **-c** *community*—the read community string of the device

You do not need to restart Prime Performance Manager server.

Related Topic

- ppm addsnmpcomm, page B-5
- ppm deletesnmpcomm, page B-16
- ppm showsnmpcomm, page B-44
- ppm snmpsetup, page B-50

ppm modifyunitconf

Syntax

/opt/CSCOppm-gw/bin/ppm modifyunitconf {**-i** *ipaddress* | **-u** *unitname* }

Command Description

Command uses the option **-i** (*ipaddress*) and **-u** (*unitname*) to modify a unit configuration.

ppm motd

Syntax

/opt/CSCOppm-gw/bin/ppm motd [**cat** | **disable** | **edit** | **enable**]

Command Description

Manages Prime Performance Manager Message of the Day file, which is a user-specified Prime Performance Manager system notice. You can set the Message of the Day to inform users of important changes or events in Prime Performance Manager system.

The Message of the Day also provides users with the chance to exit Prime Performance Manager or GTT client before launching.

If you enable the Message of the Day, it appears whenever a user attempts to launch an Prime Performance Manager or GTT client. If the user:

- Accepts the message, the client launches.
- Declines the message, the client does not launch.

Use these keywords with this command:

- **enable**—Enables the Message of the Day function. Initially, the message of the day file is blank; use **ppm motd edit** command to specify the message text.
- **edit**—Edits the Message of the Day.
- **cat**—Displays the contents of the Message of the Day file.
- **disable**—Disables this function (that is, stops displaying the Message of the Day whenever a user attempts to launch an Prime Performance Manager or GTT client).

You must log in as the root user to use this command.

Related Topic

Displaying a Message of the Day, page 6-11

ppm msglog

Syntax

/opt/CSCOppm-gw/bin/ppm msglog [**clear** | **-r**]

Command Description

Uses PAGER to display the contents of the system message log.

To save the current contents of the log, clear the log, and restart the server, enter **/opt/CSCOppm-gw/bin/ppm msglog clear**.

To display the contents of the log in reverse order, with the most recent messages at the beginning of the log, enter **/opt/CSCOppm-gw/bin/ppm msglog -r**.

You must log in as the root user to use this command.

ppm msglogage

Syntax

/opt/CSCOppm-gw/bin/ppm msglogage [*number-of-days*]

Command Description

Sets the maximum number of days to archive all types of log files before deleting them from Prime Performance Manager server.

If you enter this command without the *number-of-days* argument, Prime Performance Manager displays the current maximum number of days. You can then change that value or leave it. The valid range is one day to an unlimited number of days. The default value is 31 days.

The start date for aging out and deleting files is always yesterday at 12 AM. For example, say that you set the value to one day and you run the **ppm msglogage** command at 3 PM on January 10th.

To find files that will be deleted by the aging process, count back to 12 AM on January 10th, then add the number of days set in the command. In this example, we added one more day, so any file with an earlier timestamp than January 9th at 12 AM will be removed.

You must log in as the root user to use this command.

ppm msglogdir

Syntax

/opt/CSCOppm-gw/bin/ppm msglogdir [*directory*]

Command Description

Note You must stop Prime Performance Manager server before performing this command. You are prompted whether to continue.

Changes the default location of all Prime Performance Manager system message log files. By default, the system message log files reside on Prime Performance Manager server at /opt/CSCOppm-*xxx*/logs. Where *xxx* denotes a unit or gateway.

Note Do not set the new directory to any of these: */usr*, */var*, */opt*, or */tmp*. Also, do not set the new directory to the same directory in which you are storing GTT files (**ppm gttdir**), report files (**ppm repdir**), route table files (**ppm routedir**), or address table files (**ppm atbldir**).

After you change the directory, Prime Performance Manager asks if you want to restart Prime Performance Manager server. The new directory takes effect when you restart Prime Performance Manager server.

You must log in as the root user to use this command. If you change to a default location outside Prime Performance Manager, you must have appropriate permissions for that location.

ppm netlog

Syntax

/opt/CSCOppm-gw/bin/ppm netlog [clear | -r]

Command Description

Uses PAGER to display the contents of the network status log. To:

- Save the current contents of the log, clear the log, and restart the server, enter **/opt/CSCOppm-gw/bin/ppm netlog clear**.
- Display the contents of the log in reverse order, with the most recent network status messages at the beginning of the log, enter **/opt/CSCOppm-gw/bin/ppm netlog -r**.

You must log in as the root user to use this command.

ppm netlogger

Server Only

Command Description

Displays the current contents of the network status log file with tail -f command.

To stop the display, enter **Ctrl-c**.

ppm newlevel

Syntax

/opt/CSCOppm-gw/bin/ppm newlevel [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access, changes the authentication level for the specified user. Valid levels are:

- **1**—Basic User
- **3**—Network Operator
- **5**—System Administrator
- **11** & **12** — Custom Level

You must log in as the root user to use this command.

Related Topic

Enabling and Changing Users and Passwords, page 6-10

ppm osinfo

Command Description

Depending on the networks that you have set, displays the operating system versions of software that Prime Performance Manager supports.

ppm passwordage

Note You should have already changed your password at least once for this command to properly age the password.

Syntax

/opt/CSCOppm-gw/bin/ppm passwordage [*days* | *clear*]

Command Description

If you enable Prime Performance Manager User-Based Access and you set **/opt/CSCOppm-gw/bin/ppm authtype** to **local**, number of days allowed before forcing users to change passwords. The number of days start to accrue beginning yesterday at 12 AM.

Note For more details on how this works, see ppm msglogage, page B-33.

This function is disabled by default. If you do not specify this command, users will never need to change their passwords.

If you enter **/opt/CSCOppm-gw/bin/ppm passwordage** command, the valid range is one day to an unlimited number of days. No default setting exists.

If you enabled this function and you want to disable it (that is, prevent Prime Performance Manager from forcing users to change passwords), enter **/opt/CSCOppm-gw/bin/ppm passwordage clear**.

Note If **/opt/CSCOppm-gw/bin/ppm authtype** is set to **solaris**, you cannot use this command. Instead, you must manage passwords on the external authentication servers.

You must log in as the root user to use this command.

Related Topic

Automatically Disabling Users and Passwords, page 6-7

ppm patchlog

Syntax

/opt/CSCOppm-gw/bin/ppm patchlog

Command Description

Uses PAGER to display the contents of the patch log, which lists the patches that you installed on Prime Performance Manager server.

The default path and filename for the patch log file is /opt/CSCOppm-gw/install/sgmPatch.log. If you installed Prime Performance Manager in a directory other than */opt*, then the patch log file resides in that directory.

You must log in as the root user to use this command.

ppm poll

Syntax

/opt/CSCOppm-gw/bin/ppm poll [*node*] [*node*]...

Command Description

You use this command to poll one or more known nodes from the command line. Use the *node* arguments to specify the DNS names or IP addresses of one or more known nodes.

You must log in as the root user to use this command.

ppm print

Syntax

/opt/CSCOppm-gw/bin/ppm print {**all** | **device** | **snmp** | **task** | **alarmsummary** [*severity*] **[quiet]**}

Command Description

Displays information about device versions, SNMP settings, running tasks, summary of alarms, or all of this information.

Use these keywords with this command:

- **device**—Prints name, state, and system description of all nodes in the network.
- **snmp**—Prints SNMP information such as read and write community strings.
- **task**—Prints a list of task IDs and related information.
- **alarmsummary**—Prints a list of alarms sorted by severity types (critical, major, minor, and so on).
  - *severity*—Prints a list of alarms of a specified severity type. The *severity* takes one of these values: critical, major, minor, warning, informational, or indeterminate.
  - **quiet**—Use this keyword to print only the alarm counts (without the severity label)
- **all**—Prints the information available in all of the keywords of this command.

You must log in as the root user to use this command.

ppm props

Command Description

Displays the contents of the *System.properties* files for both Prime Performance Manager server and client installs.

You must log in as the root user to use this command.

ppm purgedb

Command Description

Permanently deletes all components in Prime Performance Manager database marked for deletion.

Prime Performance Manager retains information about older objects in its database even after they have been deleted. This is considered a logically deleted state.

Prime Performance Manager retains this information to maintain any user customized data associated with an object (for instance, a customized name) in case the object is rediscovered in the future. Logically deleted data is physically deleted after seven days if it is not reused by then.

You can use the **ppm purgedb** command to immediately remove this logically deleted data from Prime Performance Manager database.

Unfortunately, this benefit may have a side effect. In certain cases, rediscovery of a deleted object may cause Prime Performance Manager to use obsolete information in the database, rather than the new information. Ultimately, some configuration changes are not detected, and the viewable data from the client application is incorrect.

Note **/opt/CSCOppm-gw/bin/ppm purgedb** command does not cause the loss of any collected statistical data.

You must log in as the root user to use this command.

ppm readme

Command Description

Displays the contents of the README file for Prime Performance Manager.

Related Topic

Chapter 3, "Using the Prime Performance Manager Web Interface"

ppm reboot

Command Description

Reboots the Solaris Prime Performance Manager system.

You must log in as the root user to use this command.

ppm redundancygroup

Syntax

/opt/CSCOppm-gw/bin/ppm redundancygroups [**list** | **detail** | **create** | **add** | **remove** | **delete** | **redundant** | **delay** | **enable** | **disable** | **failover** | **failback** | **import** | **export**]

Command Description

Creates and manages unit protection groups. Use the following keywords with this command:

- **list**—Lists the redundancy groups defined on the gateway, similar to the following:

```
ppm redundancygroups list
groupA, Enabled, Number of Units: 2
groupB, Enabled, Number of Units: 4
```

- **detail** [*group name*]—Lists the redundancy group details, similar to the following:

```
ppm redundancygroups detail groupA
ID: 54001
Name: groupA
Enabled
Created: Wed Sep 21 11:44:36 EDT 2011
Create User: localhost
Last Modified: Wed Sep 21 11:44:36 EDT 2011
Last Modified User: localhost
Enabled
Fail over delay: 60
Units: [
        unit1,     Primary,
         unit2,  Redundant
        unit3,  Primary
        unit4,  Primary
```

- **create** [*group name* | *delay* | *unit(s)...*]—Creates a redundancy group with the provided group name, switchover delay (in seconds), and unit(s).
- **add** [*group name* | *unit(s) ...*]—Adds unit(s) to a redundancy group.
- **remove** [*group name* | *unit(s) ...*]—Removes a unit(s) from a redundancy group.

Note A redundant unit cannot be removed from a redundancy group. To remove a redundant unit, you must change the redundant unit for the group, then you can remove the old redundant unit. Another option is to delete and recreate the redundance group.

- **delete** [*group name*]—Deletes a redundancy group. The unit redundancy mode is not checked.
- **redundant** [*group name* | *unit*]—Changes the redundant unit of a redundancy group. No devices can be attached to the new redundant node.
- **delay** [*group name* | *delay*]—Changes the failover delay of a redundancy group. The delay, specified in seconds, is the amount of time the gateway waits after detecting a unit is unavailable before initiating a failover to the redundant unit
- **enable** [*group name*]—Enables a redundancy group.
- **disable** [*group name*]—Disables a redundancy group. When a group is disabled automatic failovers will not occur. However, you can perform manual failovers and failbacks.
- **failover** [*unit*]—Forces the failover of a unit to the redundant unit of the redundancy group. The

- **failback** [*unit*]—Initiates a return of control from the redundant unit to the specified unit.
- **import** [*/directory/filename*]—Imports a redundancy group definitions from the provided file name.
- **export** [*/directory/filename*]—Exports redundancy group definitions to the provided file name.

Related Topic

Creating Unit Protection Groups, page 13-4

ppm reloadmibs

Syntax

/opt/CSCOppm-gw/bin/ppm reloadmibs

Command Description

Command to reload the snmpinfo.dat file

ppm repdir

Syntax

/opt/CSCOppm-gw/bin/ppm repdir [*dir*] [nostart]

Command Description

Command to set directory used for reports. You must log in as the root user to use this command.

ppm rephelp

Command Description

Displays Help for all commands that are related to Prime Performance Manager reports.

You must log in as the root user to use this command.

ppm restart

Syntax

/opt/CSCOppm-gw/bin/ppm restart [**jsp** | **pm** | **web**]

Command Description

Restarts Prime Performance Manager servers on the local host:

- **jsp**—Restarts Prime Performance Manager JSP Server.
- **pm**—Restarts Prime Performance Manager Application Server and all managed processes.
- **web**—Restarts Prime Performance Manager web Server.

If you do not specify a keyword, **/opt/CSCOppm-gw/bin/ppm restart** restarts all Prime Performance Manager servers.

You must log in as the root user to use this command.

ppm restore

Syntax

/opt/CSCOppm-gw/bin/ppm restore [**logs** | **reports** | **security**]

Command Description

Restores Prime Performance Manager data files from a previous backup, stored in Prime Performance Manager installation directory. If you installed Prime Performance Manager in:

- The default directory, /opt, then the locations of the backup files are /opt/ppm10-Unit-ems-lnx001-backup.tar and /opt/ppm10-gateway-ems-lnx001-backup.tar.
- A different directory, then the backup files reside in that directory.

You can restore data files on the same Solaris or Linux server; or, on a different Solaris or Linux server that is running Prime Performance Manager 1.*x*.

To restore only specific parts of Prime Performance Manager data files, use these keywords:

- **logs**—Restores only Prime Performance Manager log files, such as the message log files.
- **reports**—Restores only Prime Performance Manager report files, such as the statistics report files.
- **security**—Restores only the security-related parts of Prime Performance Manager data files. This command is useful if you inadvertently delete your user accounts or make other unwanted changes to your Prime Performance Manager security information.

Note If **/opt/CSCOppm-gw/bin/ppm backupdays** was previously used to set the number of backup days to more than one day, **/opt/CSCOppm-gw/bin/ppm restore** command prompts you for a server or client backup file to restore from. This is because there would be more than one backup file to choose from).

To change the directory in which Prime Performance Manager stores these backup files, use **/opt/CSCOppm-gw/bin/ppm backupdir** command.

The server is restarted automatically after running **/opt/CSCOppm-gw/bin/ppm restore** command.

You must log in as the root user to use this command.

Related Topic

- Backing Up Prime Performance Manager Data Files, page 18-2
- ppm backupdays, page B-8
- ppm backupdir, page B-9

ppm restore all

Syntax

/opt/CSCOppm-gw/bin/ppm restore all [**nostart**]

Command Description

Restores all system files.

The server is restarted automatically after running **/opt/CSCOppm-gw/bin/ppm restore all** command.

The server is not restarted automatically after running **/opt/CSCOppm-gw/bin/ppm restore all nostart** command.

You must log in as the root user to use this command.

ppm restoreprops

Command Description

Restores Prime Performance Manager server and client *System.properties* files and other important configuration files to the backup versions of the files.

You must log in as the root user to use this command.

ppm rootvars

Command Description

Displays the contents of the */etc/CSCOppm.sh* file, which determines the root location of Prime Performance Manager server and client installation.

ppm sechelp

Command Description

Displays help for all commands that are related to Prime Performance Manager security.

You must log in as the root user to use this command.

Related Topic

Chapter 6, "Setting Up and Managing Users"

ppm seclog

Syntax

/opt/CSCOppm-gw/bin/ppm seclog [**clear** | **-r**]

Command Description

Uses PAGER to display the contents of the system security log.

These security events are recorded in the log:

- All changes to system security, including adding users.
- Log-in attempts, whether successful or unsuccessful, and logoffs.
- Attempts to switch to another user's account, whether successful or unsuccessful.
- Attempts to access files or resources of higher authentication level.
- Access to all privileged files and processes.
- Operating system configuration changes and program changes, at the Solaris level.
- Prime Performance Manager restarts.

- Failures of computers, programs, communications, and operations, at the Solaris level.

To clear the log, enter **/opt/CSCOppm-gw/bin/ppm seclog clear**.

To display the contents of the log in reverse order, with the most recent security events at the beginning of the log, enter **/opt/CSCOppm-gw/bin/ppm seclog -r**.

The default path and filename for the system security log file is */opt/CSCOppm-gw/logs/sgmSecurityLog.txt*. If you installed Prime Performance Manager in a directory other than */opt*, then the system security log file resides in that directory.

You must log in as the root user to use this command.

Related Topic

Displaying the Contents of the System Security Log, page 6-13

ppm serverlist delete

Syntax

ppm serverlist delete [*servername* | *all*]

Command Description

Deletes Prime Performance Manager server from the list, where *servername* is the name of the server deleted.

You must log in as the root user to use this command.

ppm serverlist list

Syntax

/opt/CSCOppm-gw/bin/ppm serverlist list

Command Description

Lists all Prime Performance Manager servers configured.

- Add—Adds new Prime Performance Manager server to the list, where ***servername* is the name of the new server added and *port number* is the port number of the corresponding client.**
- Delete—Deletes Prime Performance Manager server from the list, where *servername* is the name of the server deleted.

You must log in as the root user to use this command.

ppm servername

Syntax

/opt/CSCOppm-gw/bin/ppm servername [*hostname*] [nostopstart]

Command Description

Command resets Prime Performance Manager server default hostname, where hostname is the new default hostname.

- Ensure that the new default hostname is valid and defined in your /etc/hosts file. If not, you might not be able to start Prime Performance Manager server.
- User should be logged in as root user to run this command.
- nostopstart - The server is not stopped and started automatically while running this command.

Related Topic

- Chapter 2, "Managing Gateways and Units Using the Command Line Interface"

ppm setpath

Syntax

/opt/CSCOppm-gw/bin/ppm setpath [*username*]

Command Description

Appends binary (*bin*) directories to the path for a user. Users can then append the proper Prime Performance Manager binary directories to their paths without manually editing the *.profile* and *.cshrc* files.

This command appends lines such as these to the user's *.profile* file:

PATH=$PATH:/opt/CSCOppm-gw/bin:/opt/CSCOppm-gw Client/bin # CiscoPPM

and appends lines such as these to the user's *.cshrc* file:

set path=($path /opt/CSCOppm-gw/bin /opt/CSCOppm-gw Client/bin) # CiscoPPM

Thereafter, you can enter Prime Performance Manager commands as:

/opt/CSCOppm-gw/bin/ppm help

When entering this command, remember that:

- If you enter this command and you do not specify a *username*, Prime Performance Manager appends the *bin* directories to your path (that is, to the path for the user who is currently logged in and entering **/opt/CSCOppm-gw/bin/ppm setpath** command).
- If you enter this command and you specify a *username*, Prime Performance Manager appends the *bin* directories to the path for the specified user. To specify a *username*, follow these conditions:
  - You must log in as the root user.
  - The specified *username* must exist in the local */etc/passwd* file.
  - You cannot specify a *username* that is defined in a distributed Network Information Services (NIS) system or in an Network File System-mounted (NFS-mounted) home directory.
- If you enter this command more than once for the same user, each command overwrites the previous command. Prime Performance Manager does not append multiple *bin* directories to the same path.

ppm showcreds

Syntax

/opt/CSCOppm-gw/bin/ppm showcreds -i *ipaddress/hostname*

Command Description

Displays the Telnet and SSH device credentials on the Prime Performance Manager gateway.

-i *ipaddress/hostname*—The IP address or host name of the device (required)

ppm showsnmpcomm

Syntax

/opt/CSCOppm-gw/bin/ppm showsnmpcomm [**-i** *ipaddress*]

Command Description

Shows the specified SNMP configuration, or all SNMP configurations, on Prime Performance Manager server.

-i *ipaddress*—the IP address of the device (optional). If not specified, displays all SNMP configurations on the server.

Related Topic

- ppm addsnmpcomm, page B-5
- ppm deletesnmpcomm, page B-16
- ppm modifysnmpcomm, page B-31
- ppm snmpsetup, page B-50

ppm showunitconf

Syntax

/opt/CSCOppm-gw/bin/ppm showunitconf [-i (*ipaddress*)**]**

Command Description

Shows the configuration that specifies the relationship between nodes and their managed units.

-i *ipaddress* - IP address of the node is optional. If not specified, displays all configured entries on the server.

Note If a node is not specified in the configuration, it means the node will be managed by the default unit. The default unit is the unit which connects to the gateway first.

ppm singlesess

Syntax

/opt/CSCOppm-gw/bin/ppm singlesess [*enable* | *disable* | *status*]

Command Description

This command manages single session per user..

- **enable**—Enables the single session per user.

  Logging into a web interface as a user ends all the existing web interface sessions for that user.
- **disable**—Disables the single session per user.

  This command allows logging in as the same user from multiple web interfaces.
- **status**—Shows the status of the single session per user.

You must log in as the root user to use this command.

ppm snmpcomm

Syntax

/opt/CSCOppm-gw/bin/ppm snmpcomm [*name*]

Command Description

You use this command to set a new default SNMP read community name. Prime Performance Manager automatically updates the name in the SNMP parameters file. The default path and filename for the SNMP parameters file is /opt/CSCOppm-gw/etc/communities.conf.

You must log in as the root user to use this command.

ppm snmpconf

Syntax

/opt/CSCOppm-gw/bin/ppm snmpconf [*filename*]

Command Description

Sets the file used for SNMP parameters, such as community names, timeouts, and retries.

The default path and filename for the SNMP parameters file is /opt/CSCOppm-gw/etc/communities.conf. If you installed Prime Performance Manager in a directory other than /opt, then the file resides in that directory.

When you specify a new path or filename, Prime Performance Manager restarts the servers.

Note The SNMP parameters file uses the HP OpenView format; therefore, you can set this path and filename to point to the HP OpenView *ovsnmp.conf* file in an existing OpenView system. For information about exporting SNMP community names from CiscoWorks Resource Manager Essentials (RME).

You must log in as the root user to use this command.

ppm snmpget

Syntax

/opt/CSCOppm-gw/bin/ppm snmpget [**-J***JVM_ARG1* [**-J***JVM_ARG2*]...] [**-v** *snmp_version*] [**-c** *community_string*] [**-r** *retry*] [**-t** *timeout*] [**-d** *output_delimiter*] [**--header|--no-header**] [**--raw-octets|--no-raw-octets**] [**--str-octets|--no-str-octets**] [**--raw-timeticks|--no-raw-timeticks**] [**--resolve-integer|--no-resolve-integer**] [**--resolve-bits|--no-resolve-bits**] [**--get-sysuptime|--no-get-sysuptime**] [**--detect-mib-error**] [**--instance** *oids*] [**--int-instance** *integer*] [**--str-instance** *string*] [*hostname*] [*oid*] [*oid*]...

Command Description

Queries the specified *hostname* by using SNMP **GetRequests**. Use these optional keywords and arguments with this command:

- **-J***JVM_ARG1*—JVM options. You must specify the **-J** keyword and arguments before any other keywords and arguments.

  For example, by default JVM uses a maximum of 64 MB of memory. However, if you are working in a large table, JVM might require more memory. To enable JVM to use a maximum of 256 MB of memory, use this syntax:

  -J-Xmx256m

- **-v** *snmp_version*—SNMP protocol version. Valid versions are **1** or **2c**. The default version is **2c**.
- **-c** *community_string*—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-r** *retry*—SNMP retry count. You specify the default retry count in the SNMP parameters file, *communities.conf*.
- **-t** *timeout*—SNMP timeout, in seconds. You specify the default timeout in the SNMP parameters file, *communities.conf*.
- **-d** *output_delimiter*—Output delimiter. The default output delimiter is a colon (**:**).
- **--header|--no-header**—Specifies whether to display variable names as table headers:
  - Specify **--header** to display variable names as table headers for tabular output, or to display MIB variable OIDs with the value for nontabular output. This is the default setting.
  - Specify **--no-header** if you do not want to display variable names as table headers for tabular output, or MIB variable OIDs with the value for nontabular output.
- **--raw-octets|--no-raw-octets**—Specifies whether to display octets as raw octets:
  - Specify **--raw-octets** to display raw octets, such as **6c 69 6e 6b**, for octet strings.
  - Specify **--no-raw-octets** if you do not want to display raw octets for octet strings. This is the default setting.

  The other option for displaying octets is **--str-octets|--no-str-octets**.
- **--str-octets|--no-str-octets**—Specifies whether to display octets as strings:
  - Specify **--str-octets** to display octets as strings, such as **link**. This is the default setting.
  - Specify **--no-str-octets** if you do not want to display octets as strings.

  The other option for displaying octets is **--raw-octets|--no-raw-octets**.
- **--raw-timeticks|--no-raw-timeticks**—Specifies the time format:

- Specify **--raw-timeticks** to specify raw timeticks, such as **2313894**.
- Specify **--no-raw-timeticks** to specify formatted timeticks, such as **6 Hours 26 Mins 12 Secs**. This is the default setting.

- **--resolve-integer|--no-resolve-integer**—Specifies the time format. Use:
  - **--resolve-integer** to display integers using the string description in the MIB, such as **available** or **unavailable**.
  - **--no-resolve-integer** to display integers as numbers. This is the default setting.
- **--resolve-bits|--no-resolve-bits**—Specifies the time format. Use:
  - **--resolve-bits** to display bits using the string description in the MIB, such as **continue** or **ruleset**.
  - **--no-resolve-bits** to display bits as numbers, such as **1** or **14**. This is the default setting.
- **--get-sysuptime|--no-get-sysuptime**—Specifies whether to retrieve the **sysuptime**. Use:
  - **--get-sysuptime** to retrieve the sysuptime in the same packet as each SNMP operation.
  - **--no-get-sysuptime** if you do not want to retrieve the sysuptime in the same packet. This s the default setting.
- **--detect-mib-error**—Detects errors in returned MIB variables, such as **noSuchInstance**, **noSuchObject**, and **endOfMibView**. If the system detects any such errors, an error message and error code appear.

  Sometimes multiple MIB variables are returned at the same time, some of which are in error; others are not. If this occurs and you:
  - Specified **--detect-mib-error**, none of the correct values appear, only the error message, and it returns an error code.
  - Did not specify **--detect-mib-error**, a return code of 0 is returned and all MIB variables appear. (Even noSuchInstance appears as a returned value.) This is the default setting, with **--detect-mib-error** not specified.
- **--instance** *oids*—Appends instance OIDs to each polling MIB variable. For example, these commands perform the same function:

  ppm snmpget --instance 172.18.16.10 node_1 ipAdEntIfIndex ipAdEntNetMask

  ppm snmpget node_1 ipAdEntIfIndex.172.18.16.10 ipAdEntNetMask.172.18.16.10
- **--int-instance** *integer*—Appends the specified integer instance OID to each polling MIB variable.
- **--str-instance** *string*—Appends string instance OIDs to each polling MIB variable; for example, these commands perform the same function:

  ppm snmpget --str-instance link_1 node_1 cItpSpLinksetState

  ppm snmpget node_1 cItpSpLinksetState.6.108.115.110.97.109.101
- *hostname*—Name of the host to query.
- *oid*—One or more OIDs or variable names.

The default path for the SNMP parameters file, communities.conf, is /opt/CSCOppm-gw/etc/communities.conf. If you installed Prime Performance Manager in a directory other than /opt, then the file resides in that directory. You can edit the file manually or using Prime Performance Manager web interface.

You must log in as the root user to use this command.

ppm snmphelp

Command Description

Displays help for all commands that are related to SNMP queries.

You must log in as the root user to use this command.

ppm snmpmaxrows

Syntax

/opt/CSCOppm-gw/bin/ppm snmpmaxrows [*number-of-rows*]

Command Description

Sets the value of maximum rows for SNMP walk.

Prime Performance Manager collects network information from device MIBs using SNMP protocol. In certain ITP networks, some MIB tables can be very large (such as GTT tables, MTP3 accounting statistics tables, etc.)

The default value of 100,000 rows is usually sufficient even for large networks. However, for very large networks, if the limit needs to be increased, you can customize the this parameter. It is not recommended to exceed 300,000 rows.

If you enter this command without the *number-of-rows* argument, Prime Performance Manager displays the current maximum number of rows. You can then change that value or leave it. The valid range is 1 row to an unlimited number of rows. However, it is not recommended to set this number at less than 10,000. The default value is 100,000 rows.

You must log in as the root user to use this command.

ppm snmpnext

Syntax

ppm snmpnext [**-J***JVM_ARG1* [**-J***JVM_ARG2*]...] [**-v** *snmp_version*] [**-c** *community_string*] [**-r** *retry*] [**-t** *timeout*] [**-d** *output_delimiter*] [**--header|--no-header**] [**--raw-octets|--no-raw-octets**] [**--str-octets|--no-str-octets**] [**--raw-timeticks|--no-raw-timeticks**] [**--resolve-integer|--no-resolve-integer**] [**--resolve-bits|--no-resolve-bits**] [**--get-sysuptime|--no-get-sysuptime**] [**--detect-mib-error**] [**--instance** *oids*] [**--int-instance** *integer*] [**--str-instance** *string*] [*hostname*] [*oid*] [*oid*]...

Command Description

Queries the specified *hostname* by using SNMP **GetNextRequests**. Use these optional keywords and arguments with this command:

- **-J***JVM_ARG1*—JVM options. You must specify the **-J** keyword and arguments before any other keywords and arguments.

For example, by default JVM uses a maximum of 64 MB of memory; however, if you explore a large table, JVM might require more memory. To enable JVM to use a maximum of 256 MB of memory, use this option:

-J-Xmx256m

- **-v** *snmp_version*—SNMP protocol version. Valid versions are **1** or **2c**. The default version is **2c**.
- **-c** *community_string*—SNMP community string. You specify the default community string in the SNMP parameters file, communities.conf.
- **-r** *retry*—SNMP retry count. You specify the default retry count in the SNMP parameters file, *communities.conf*.
- **-t** *timeout*—SNMP timeout, in seconds. You specify the default timeout in the SNMP parameters file, *communities.conf*.
- **-d** *output_delimiter*—Output delimiter. The default output delimiter is a colon (**:**).
- **--header|--no-header**—Specifies whether to display variable names as table headers:
  - Specify **--header** to display variable names as table headers for tabular output or MIB variable OIDs with the value for nontabular output. This is the default setting.
  - Specify **--no-header** if you do not want to display variable names as table headers for tabular output or MIB variable OIDs with the value for nontabular output.
- **--raw-octets|--no-raw-octets**—Specifies whether to display octets as raw octets. Use:
  - **--raw-octets** to display raw octets, such as **6c 69 6e 6b**, for octet strings.
  - **--no-raw-octets** if you do not want to display raw octets for octet strings. This is the default setting.

  The other option for displaying octets is **--str-octets|--no-str-octets**.
- **--str-octets|--no-str-octets**—Specifies whether to display octets as strings. Use:
  - **--str-octets** to display octets as strings, such as **link**. This is the default setting.
  - **--no-str-octets** if you do not want to display octets as strings.

  The other option for displaying octets is **--raw-octets|--no-raw-octets**.
- **--raw-timeticks|--no-raw-timeticks**—Specifies the time format:
  - Specify **--raw-timeticks** to specify raw timeticks, such as **2313894**.
  - Specify **--no-raw-timeticks** to specify formatted timeticks, such as **6 Hours 26 Mins 12 Secs**. This is the default setting.
- **--resolve-integer|--no-resolve-integer**—Specifies the time format. Use:
  - **--resolve-integer** to display integers using the string description in the MIB, such as **available** or **unavailable**.
  - **--no-resolve-integer** to display integers as numbers. This is the default setting.
- **--resolve-bits|--no-resolve-bits**—Specifies the time format:
  - Specify **--resolve-bits** to display bits using the string description in the MIB, such as **continue** or **ruleset**.
  - Specify **--no-resolve-bits** to display bits as numbers, such as **1** or **14**. This is the default setting.
- **--get-sysuptime|--no-get-sysuptime**—Specifies whether to retrieve the **sysuptime**. Use:
  - **--get-sysuptime** to retrieve the sysuptime in the same packet as each SNMP operation.

  - **--no-get-sysuptime** if you do not want to retrieve the sysuptime in the same packet. This is the default setting.

- **--detect-mib-error**—Detects errors in returned MIB variables, such as **noSuchInstance**, **noSuchObject**, and **endOfMibView**. If the system detects any such errors, an error message appears and an error code is returned.

  Sometimes multiple MIB variables are returned at the same time, some of which are in error; others are not. If this occurs and you:

  - Specified **--detect-mib-error**, none of the correct values appear, only the error message and it returns an error code.
  - Did not specify **--detect-mib-error**, a return code of 0 is returned and all MIB variables appear (even noSuchInstance appears as a returned value). This is the default setting, with **--detect-mib-error** not specified.

- **--instance** *oids*—Appends instance OIDs to each polling MIB variable. For example, these commands perform the same function:

  ppm snmpget --instance 172.18.16.10 node_1 ipAdEntIfIndex ipAdEntNetMask

  ppm snmpget node_1 ipAdEntIfIndex.172.18.16.10 ipAdEntNetMask.172.18.16.10

- **--int-instance** *integer*—Appends the specified integer instance OID to each polling MIB variable.
- **--str-instance** *string*—Appends string instance OIDs to each polling MIB variable. For example, these commands perform the same function:

  ppm snmpget --str-instance link_1 node_1 cItpSpLinksetState

  ppm snmpget node_1 cItpSpLinksetState.6.108.115.110.97.109.101

- *hostname*—Name of the host to be queried.
- *oid*—One or more OIDs or variable names.

The default path for the SNMP parameters file, *c*ommunities.conf, is /opt/CSCOppm-gw/etc/communities.conf. If you installed Prime Performance Manager in a directory other than /opt, then the file resides in that directory. You can edit the file manually or by using Prime Performance Manager client.

You must log in as the root user to use this command.

ppm snmpsetup

Syntax

/opt/CSCOppm-gw/bin/ppm snmpsetup

Command Description

Set SNMP community strings for multiple devices and discover. You do not need to restart the server when using this command.

Related Topic

- ppm addsnmpcomm, page B-5
- ppm deletesnmpcomm, page B-16

- ppm modifysnmpcomm, page B-31
- ppm showsnmpcomm, page B-44

ppm snmpwalk

Syntax

/opt/CSCOppm-gw/bin/ppm snmpwalk [**-J***JVM_ARG1* [**-J***JVM_ARG2*]...] [**-v** *snmp_version*] [**-c** *community_string*] [**-r** *retry*] [**-t** *timeout*] [**-x** *maximum_rows*] [**-d** *output_delimiter*] [**--tabular**|**--no-tabular**] [**--getbulk**|**--no-getbulk**] [**--header**|**--no-header**] [**--raw-octets**|**--no-raw-octets**] [**--str-octets**|**--no-str-octets**] [**--raw-timeticks**|**--no-raw-timeticks**] [**--resolve-integer**|**--no-resolve-integer**] [**--resolve-bits**|**--no-resolve-bits**] [**--get-sysuptime**|**--no-get-sysuptime**] [**--detect-mib-error**] [**--instance** *oids*] [**--int-instance** *integer*] [**--str-instance** *string*] [*hostname*] [*oid*] [*oid*]...

Command Description

Queries the specified *hostname* by using SNMP **GetNextRequests** to go through the MIB. Use these optional keywords and arguments with this command:

- **-J***JVM_ARG1*—JVM options. You must specify the **-J** keyword and arguments before any other keywords and arguments.

  For example, by default JVM uses a maximum of 64 MB of memory; however, if you are going through a large table, JVM might require more memory. To enable JVM to use a maximum of 256 MB of memory, use this option:

  -J-Xmx256m

- **-v** *snmp_version*—SNMP protocol version. Valid versions are **1** or **2c**. The default version is **2c**.
- **-c** *community_string*—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-r** *retry*—SNMP retry count. You specify the default retry count in the SNMP parameters file, *communities.conf*.
- **-t** *timeout*—SNMP timeout, in seconds. You specify the default timeout in the SNMP parameters file, *communities.conf*.
- **-x** *maximum_rows*—Maximum number of rows to go through. If a table has more than the maximum number of rows, ppm **snmpwalk** command fails. You can use the **-m** keyword and argument to increase the maximum number of rows to go through. The default setting is 10,000 rows.

  However, for every 10,000 rows gone through, JVM requires an additional 10 MB of memory. You can use the **-J** keyword and argument to increase the memory available to JVM.

- **-d** *output_delimiter*—Output delimiter. The default output delimiter is a colon (**:**).
- **--tabular**|**--no-tabular**—Specifies whether to print the result of the query in tabular format. Use:
  - **--tabular** to print the result in tabular format. This is the default setting.
  - **--no-tabular** if you do not want to print the result in tabular format.
- **--getbulk**|**--no-getbulk**—(SNMP version 2c only) Specifies whether to use the **getbulk** command to go through the table. Use:
  - **--getbulk** to use the **getbulk** command. This is the default setting.
  - **--no-getbulk** if you do not want to use the **getbulk** command.

- **--header|--no-header**—Specifies whether to display variable names as table headers. Use:
  - **--header** to display variable names as table headers for tabular output or to display MIB variable OIDs with the value for nontabular output. This is the default setting.
  - **--no-header** if you do not want to display variable names as table headers for tabular output or MIB variable OIDs with the value for nontabular output.
- **--raw-octets|--no-raw-octets**—Specifies whether to display octets as raw octets. Use:
  - **--raw-octets** to display raw octets, such as **6c 69 6e 6b**, for octet strings.
  - **--no-raw-octets** if you do not want to display raw octets for octet strings. This is the default setting.

  The other option for displaying octets is **--str-octets|--no-str-octets**.
- **--str-octets|--no-str-octets**—Specifies whether to display octets as strings. Use:
  - **--str-octets** to display octets as strings, such as **link**. This is the default setting.
  - **--no-str-octets** if you do not want to display octets as strings.

  The other option for displaying octets is **--raw-octets|--no-raw-octets**.
- **--raw-timeticks|--no-raw-timeticks**—Specifies the time format. Use:
  - **--raw-timeticks** to specify raw timeticks, such as **2313894**.
  - **--no-raw-timeticks** to specify formatted timeticks, such as **6 Hours 26 Mins 12 Secs**. This is the default setting.
- **--resolve-integer|--no-resolve-integer**—Specifies the time format. Use:
  - **--resolve-integer** to display integers using the string description in the MIB, such as **available** or **unavailable**.
  - **--no-resolve-integer** to display integers as numbers. This is the default setting.
- **--resolve-bits|--no-resolve-bits**—Specifies the time format. Use:
  - **--resolve-bits** to display bits using the string description in the MIB, such as **continue** or **ruleset**.
  - **--no-resolve-bits** to display bits as numbers, such as **1** or **14**. This is the default setting.
- **--get-sysuptime|--no-get-sysuptime**—Specifies whether to retrieve the sysuptime. Use:
  - **--get-sysuptime** to retrieve the sysuptime in the same packet as each SNMP operation.
  - **--no-get-sysuptime** if you do not want to retrieve the **sysuptime** in the same packet. This is the default setting.
- **--detect-mib-error**—Detects errors in returned MIB variables, such as **noSuchInstance**, **noSuchObject**, and **endOfMibView**. If the system detects any such errors, an error message and error code appear.

  Sometimes multiple MIB variables are returned at the same time, some of which are in error; others are not. If this occurs and you:
  - Specified **--detect-mib-error**, none of the correct values appear, only the error message and an error code is returned.
  - Did not specify **--detect-mib-error**, a return code of 0 and all MIB variables appear; even noSuchInstance appears as a returned value. This is the default setting, with **--detect-mib-error** not specified.
- **--instance** *oids*—Appends instance OIDs to each polling MIB variable. For example, these commands perform the same function:

ppm snmpget --instance 172.18.16.10 node_1 ipAdEntIfIndex ipAdEntNetMask

ppm snmpget node_1 ipAdEntIfIndex.172.18.16.10 ipAdEntNetMask.172.18.16.10

- **--int-instance** *integer*—Appends the specified integer instance OID to each polling MIB variable.
- **--str-instance** *string*—Appends string instance OIDs to each polling MIB variable. For example, these commands perform the same function:

  ppm snmpget --str-instance link_1 node_1 cItpSpLinksetState

  ppm snmpget node_1 cItpSpLinksetState.6.108.115.110.97.109.101

- *hostname*—Name of the host to query.
- *oid*—One or more OIDs or variable names.

The default path for the SNMP parameters file, communities.conf, is /opt/CSCOppm-gw/etc/communities.conf. If you installed Prime Performance Manager in a directory other than */opt*, then the file resides in that directory. You can edit the file manually or using Prime Performance Manager client.

You must log in as the root user to use this command.

ppm ssl

Syntax

/opt/CSCOppm-gw/bin/ppm ssl [**enable** | **disable** | **status**]

Command Description

If you enable the SSL on Prime Performance Manager and you have an SSL key-certificate pair on Prime Performance Manager, you can use this command to manage SSL support in Prime Performance Manager:

- **enable**—Enables SSL support.
- **disable**—Disables SSL support.
- **status**—Displays the current status of SSL support in Prime Performance Manager, including whether you enabled or disabled SSL support, and which SSL keys and certificates exist.

You must log in as the root user to use this command. See Managing Prime Performance Manager Users, page 6-14 for more information.

ppm sslstatus

Syntax

/opt/CSCOppm-gw/bin/ppm sslstatus

Command Description

Displays the current status for SSL that Prime Performance Manager supports, including whether you enabled or disabled SSL support; and, which SSL keys and certificates exist.

You must log in as the root user to use this command.

Related Topic

Managing Prime Performance Manager Users, page 6-14

ppm start

Syntax

```
/opt/CSCOppm-gw/bin/ppm start
```

Command Description

Starts the Prime Performance Manager gateway and unit (if installed on the same machine).

You must log in as the root user to use this command.

Note If the database has an exception during start up, the gateway and unit (if installed) will not start.

Related Topic

Managing Gateways and Units Using the Command Line Interface, page 2-1

ppm start jsp

Syntax

```
/opt/CSCOppm-gw/bin/ppm startjsp
```

Command Description

Starts Prime Performance Manager JSP Server on the local host.

You must log in as the root user to use this command.

ppm start pm

Syntax

```
/opt/CSCOppm-gw/bin/ppm startpm
```

Command Description

Starts Prime Performance Manager Application Server and all managed processes on the local host.

You must log in as the root user to use this command.

ppm start web

Syntax

/opt/CSCOppm-gw/bin/ppm startweb

Command Description

Starts Prime Performance Manager web server on the local host.

You must log in as the root user to use this command.

ppm statreps

Full Syntax

/opt/CSCOppm-gw/bin/ppm statreps [**none**] [**default**] [**all**] [*enable* | *disable*] [*noexport* | *export*] **status,** [**status** [*node*]] **status config**, **status reps**, **config**, **reps**, [**setstatus**[*category*] [*enable* | *disable*]], [**setstatus**[*category*] [*enable* | *disable*] [*node*]], [**5min** [*enable*|*disable*]], [**15min** [*enable*|*disable*]], [**hourly** [*enable*|*disable*]], [**hourly** [*enable*|*disable*]], [**daily** [*enable* |*disable*]], [**5mincsvage** [*days*]], [**15mincsvage** [*days*]], [**hourlycsvage** [*days*]], [**dailycsvage** [*days*]], [**5minage** [*days*]], [**15minage** [*days*]], [**hourlyage** [*days*]], [**dailyage** [*days*]] , [*nodiskcheck* | *diskcheck*], [**timemode** [*12* | *24*]], [**csvnames** [*ppm* | *3gpp*]], [**nametype**[*dnsname*] [*customname* | *sysname*]], [**csvtype** [*allnodes* | *pernodeuniq*]], [**zipcsvdelay** [*mins*]]

Optionally, you can specify a hostname or IP address to enable or disable the specified report for a specific device. For example the following command enables CPU reports for the device *name*

```
ppm statreps cpu <ip address>
```

If you specify a command in which the hostname or IP address is not applicable, the host parameter is ignored and does not cause an error.

Command Description

[*enable* | *disable*] - Enable/Disable master report.

[*all*] - Enable all report types.

[*default*] - Enable all default report types.

[*none*] - Disable all report types.

[*noexport* | *export*] - Enable/Disable all csv files.

[*nodiskcheck* | *diskcheck*] - Checks for available disk space.

status - Display network report settings.

status [*node*] - Display node report settings.

status config - Display master report config settings.

status reps - Display individual report enable status.

config - Display master report config settings.

reps - Display individual report enable status.

setstatus [[*category*] [*enable* | *disable*]] - Enable/Disable Network report settings.

setstatus [[*category*] [enable | disable] [node]] - Enable/Disable Node report settings.

5min [*enable* | *disable*] - Enable/Disable 5 minute master report.

15min [*enable* | *disable*] - Enable/Disable 15 minute master report.

hourly [*enable* | *disable*] - Enable/Disable hourly master report.

daily [*enable* | *disable*] - Enable/Disable daily master report.

5mincsvage [*days*] - Specifies the days to keep 5 min csv files.

15mincsvage [*days*] - Specifies the days to keep 15 min csv files.

hourlycsvage [*days*] - Specifies the days to keep hourly csv files.

dailycsvage [*days*] - Specifies the days to keep daily csv files.

5minage [*days*] - Specifies the days to keep 5min data.

15minage [*days*] - Specifies the days to keep 15min data.

hourlyage [*days*] - Specifies the days to keep hourly data.

dailyage [*days*] - Specifies the days to keep daily data.

timemode [*12* | *24*] - Display in 12 or 24 hour time.

csvnames [*ppm* | *3gpp*] - Specifies the format for csv filenames.

nametype [*dnsname* | *customname* | *sysname*] - Specifies the nodename type for csv files.

csvtype [*allnodes* | *pernodeuniq*] - Specifies the combined or pernode csv Files.

zipcsvdelay [*mins*] - Specifies the minutes to wait before zipping csv Files.

ppm syncunits

Syntax

/opt/CSCOppm-gw/bin/ppm syncunits [enable | disable| status]

Command Description

Command manages file synchronization between the gateway and units.

ppm status

Syntax

/opt/CSCOppm-gw/bin/ppm status

Command Description

Displays the status of all Prime Performance Manager servers on the local host.

Related Topic

Chapter 3, "Using the Prime Performance Manager Web Interface"

ppm stop

Syntax

/opt/CSCOppm-gw/bin/ppm stop

Command Description

Stops all Prime Performance Manager servers on the local host.

You must log in as the root user to use this command.

ppm stop jsp

Syntax

/opt/CSCOppm-gw/bin/ppm stopjsp

Command Description

Stops Prime Performance Manager JSP Server on the local host.

You must log in as the root user to use this command.

ppm stop pm

Syntax

/opt/CSCOppm-gw/bin/ppm stoppm

Command Description

Stops Prime Performance Manager Application Server and all managed processes on the local host.

You must log in as the root user to use this command.

ppm stop web

Syntax

/opt/CSCOppm-gw/bin/ppm stopweb

Command Description

Stops Prime Performance Manager web server on the local host.

You must log in as the root user to use this command.

ppm tac

Syntax

/opt/CSCOppm-gw/bin/ppm tac [*short*]

Command Description

Collects important troubleshooting information for the Cisco Technical Assistance Center and writes the information to the /opt/CSCOppm-gw/tmp/cisco_ppm_tshoot.log file.

short—Collects the basic information required for diagnosis of the problem.

You must log in as the root user to use this command.

ppm trapratelimit abate

Syntax

/opt/CSCOppm-gw/bin/ppm trapratelimit abate [*offset*]

Command Description

This option configures the trap abate offset.

By default, a node generating 2,000 or more traps (major limiting count) in the last 30 minutes (limiting interval) is considered to generate too many traps.

Prime Performance Manager raises a TrapRateStatus major alarm and stops trap processing for this node. If the node no longer experiences a trap storm in the next cycle (limiting interval), Prime Performance Manager will automatically reset the ProcessTrap flag and begin processing traps again.

The abate offset is the offset value from the trap major limit count. The abate threshold limit is the limiting count minus the offset value. By default, the offset value is 200.

For example, if a node generates 2,000 traps (major limiting count) minus 200 traps (the default offset value), which equals 1,800 or more traps, it is considered to be faulty and Prime Performance Manager stops trap processing for this node.

You must log in as the root user to use this command.

ppm trapratelimit major

Syntax

/opt/CSCOppm-gw/bin/ppm trapratelimit major [*count*]

Command Decription

This option configures the trap major limiting count or the major threshold limit.

By default, a node generating 2,000 or more traps (major limiting count) in the last 30 minutes (limiting interval) is considered to generate too many traps.

Prime Performance Manager raises a TrapRateStatus major alarm and stops trap processing for this node. If the node no longer experiences a trap storm in the next cycle (limiting interval), Prime Performance Manager will automatically reset the ProcessTrap flag and begin processing traps again.

You must log in as the root user to use this command.

ppm trapratelimit interval

Syntax

/opt/CSCOppm-gw/bin/ppm trapratelimit interval [*min*]

Command Decription

This option configures the interval at which nodes are checked for a trap storm.

By default, a node generating 2,000 or more traps (major limiting count) in the last 30 minutes (limiting interval) is considered to generate too many traps.

Prime Performance Manager raises a TrapRateStatus major alarm and stops trap processing for this node. If the node no longer experiences a trap storm in the next cycle (limiting interval), Prime Performance Manager will automatically reset the ProcessTrap flag and begin processing traps again.

You must log in as the root user to use this command.

ppm trapratelimit minor

Syntax

/opt/CSCOppm-gw/bin/ppm trapratelimit minor [*count*]

Command Description

This option configures the trap minor limiting count or the minor threshold limit.

By default, if a node generates 1,000 or more traps (minor limiting count) in the last 30 minutes (limiting interval) Prime Performance Manager raises a TrapRateStatus minor alarm. Prime Performance Manager will continue to process traps from the node.

- If the node no longer experiences a trap storm in the next cycle (limiting interval), Prime Performance Manager will automatically clear the minor alarm.
- If the node continues to receive 2,000 or more traps (major limiting count) Prime Performance Manager raises TrapRateStatus major alarm and stop trap processing for this node.

You must log in as the root user to use this command.

ppm uninstall

Syntax

/opt/CSCOppm-gw/bin/ppm uninstall

Command Description

Uninstalls Prime Performance Manager.

You must log in as the root user to use this command.

ppm unknownage

Syntax

/opt/CSCOppm-gw/bin/ppm unknownage [*number-of-days*]

Command Description

Sets the maximum number of days to retain **Unknown** objects before deleting them from Prime Performance Manager database.

If you enter this command without the *number-of-days* argument, Prime Performance Manager displays the current maximum number of days. You can then change that value or leave it. The valid range is one day to an unlimited number of days. The default value is seven days. Setting this value to 0 days means that, after one hour, the system deletes **Unknown**.

You must log in as the root user to use this command.

ppm updateuser

Syntax

/opt/CSCOppm-gw/bin/ppm updateuser [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access, changes the authentication level for the specified user. Valid levels are:

- **1**—Basic User
- **3**—Network Operator
- **5**—System Administrator
- **11** & **12** — Custom Level

If you set **ppm authtype** to **local**, you also use this command to change the user's password. When setting the password, follow the rules and considerations in Creating Secure Passwords, page 6-5.

See Enabling and Changing Users and Passwords, page 6-10 for more information on authentication levels and the use of this command.

You must log in as the root user to use this command.

Note If you have enabled Solaris authentication, you must log in as the root user, to use this command (see Setting User Access, page 6-1).

ppm useraccess

Syntax

/opt/CSCOppm-gw/bin/ppm useraccess [**disable** | **enable**]

Command Description

Enables or disables Prime Performance Manager User-Based Access. User-Based Access provides multilevel password-protected access to Prime Performance Manager features. Each user can have a unique username and password. You can also assign each user to one of five levels of access, which control the list of Prime Performance Manager features accessible by that user.

Note You must enable Prime Performance Manager User-Based Access to use the associated Prime Performance Manager security commands (see Setting User Access, page 6-1).

The **ppm useraccess** command goes through the following stages, checking the status of:

- **ppm useraccess**—Enabled or disabled.
- **ppm authtype**—If you have not already set Prime Performance Manager authentication type, you must do so now.
- **ppm adduser**—If you have already assigned users, Prime Performance Manager asks if you want to use the same user database, or create a new one. If you have not assigned users, you must do so now.

You must log in as the root user to use this command.

Related Topic

Setting User Access, page 6-1

ppm userpass

Syntax

/opt/CSCOppm-gw/bin/ppm userpass [*username*]

Command Description

If you enable Prime Performance Manager User-Based Access and **/opt/CSCOppm-gw/bin/ppm authtype** is set to **local**, changes the specified user's Prime Performance Manager security authentication password.

If Prime Performance Manager automatically disables the user's authentication, this command re-enables the user's authentication with a new password.

If **/opt/CSCOppm-gw/bin/ppm authtype** is set to Solaris or Linux, you cannot use this command; instead, you must manage passwords on the external authentication servers.

You must log in as the root user to use this command.

Related Topic

Enabling and Changing Users and Passwords, page 6-10

ppm version

Syntax

/opt/CSCOppm-gw/bin/ppm version

Command Description

Displays version information for Prime Performance Manager servers and clients on the local host.

Related Topic

Chapter 3, "Using the Prime Performance Manager Web Interface"

ppm webport

Syntax

/opt/CSCOppm-gw/bin/ppm webport [*port-number*]

Command Description

Sets a new port number for the web server, where *port-number* is the new, numeric port number. Prime Performance Manager verifies that the new port number is not already in use.

The new port number must contain only numbers. If you enter a port number that contains nonnumeric characters, such as **ppm13**, Prime Performance Manager displays an error message and returns to the command prompt without changing the port number.

You must log in as the root user to use this command.

ppm who

Syntax

/opt/CSCOppm-gw/bin/ppm who

Command Description

Displays a list of all client usernames and processes connected to the server.

ppm xmlpoll

Syntax

/opt/CSCOppm-gw/bin/ppm xmlpoll -i *ipaddress/hostname* **-p -a** [**-d** *parameters*]

Command Description

Runs the XML poller to get the device XML output.

-i *ipaddress/hostname*—The IP address or host name of the device (required)

-p—Package

-a—Action

-d—Parameters

GLOSSARY

This glossary contains Cisco Prime Performance Manager specific terms. For an online listing of other internetworking terms and acronyms, see this URL:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

A

access list A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

alarm An alarm is a sequence of events, each representing a specific occurrence in the alarm lifecycle. The lifecycle of an alarm can include any number of related events that are triggered by changes in severity, updates to services, and so on. See event.

ANSI American National Standards Institute.

API Application Programming Interface. A source code interface that a computer system or program library provides to support requests for services by a computer program.

auto start Setting that enables Prime Performance Manager to start a process automatically when the Process Manager is started. See Message Log Server, Process Manager.

B

browser GUI-based hypertext client application, such as Internet Explorer or Mozilla, used to access hypertext documents and other services located on innumerable remote servers throughout the World Wide Web (WWW) and Internet.

C

Cisco IOS software Cisco Internetwork Operating System software. Cisco system software that provides common functionality, scalability, and security for many Cisco products. The Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms.

CLI Command line interface. An interface that allows the user to interact with the Cisco IOS software operating system by entering commands and optional arguments.

client Node or software program that requests services from a server. Prime Performance Manager user interface is an example of a client. See also server.

command line interface See CLI.

community name See community string.

community string Text string that acts as a password and is used to authenticate messages sent between a management station and a node containing an SNMP agent. The community string is sent in every packet between the manager and the agent. Also called community name, read community.

console log Log containing unexpected error and warning messages from Prime Performance Manager server, such as those that might occur if Prime Performance Manager server cannot start.

CSV Comma-separated values. A widely-used file format for storing tabular data.

D

demand polling User-initiated poll of selected nodes. Contrast with status polling.

device See node.

device type In Prime Performance Manager, the type of a discovered device. Also called system object ID.

discovered Object that has been discovered by Prime Performance Manager. Also called *known*. Contrast with unknown.

Discovery Process by which Prime Performance Manager discovers objects in your network. See also recursive Discovery.

display name User-specified name for a node. Contrast with DNS name. See also node name.

domain name The style of identifier—a sequence of case-insensitive ASCII labels separated by dots ("bbn.com.")—defined for subtrees in the Internet Domain Name System [R1034] and used in other Internet identifiers, such as host names, mailbox names, and URLs.

Domain Name System See DNS.

DNS Domain Name System. System used on the Internet for translating names of network nodes into addresses.

DNS name Initial name of a node, as discovered by Prime Performance Manager. Contrast with display name. See also node name.

E

Erlang (E) The international (dimensionless) unit of the average traffic intensity (occupancy) of a facility during a period of time, normally, a busy hour. The number of Erlangs is the ratio of the time during which a facility is occupied (continuously or cumulatively) to the time this facility is available for occupancy. Another definition is the ratio of the average call arrival rate into the system, to the average call duration. One Erlang is equivalent to 36 ccs (completed call seconds), which is another traffic intensity unit.

event An event is a singular occurrence in time. Events are derived from incoming traps and notifications, and from detected status changes.

Prime Performance Manager can detect events that are triggered by SNMP traps or notifications, status changes, and user actions. See alarm.

exclude Removing a network object from a view, while retaining the object in Prime Performance Manager database.

F

Field Replaceable Units See FRU.

FRU Assemblies such as power supplies, fans, processor modules, interface modules, and so forth.

G

graphical user interface See GUI.

GUI Graphical user interface. User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms utilizing a GUI.

H

host Computer system on a network. Similar to the term node except that host usually implies a computer system, whereas node generally applies to any network system.

host address See host number.

host number Part of an IP address that designates which node on the subnetwork is being addressed. Also called a host address.

HTML Hypertext Markup Language. Simple hypertext document formatting language that uses tags to indicate how a given part of a document should be interpreted by a viewing application, such as a web browser. See also hypertext and browser.

hypertext Electronically-stored text that allows direct access to other texts by way of encoded links. Hypertext documents can be created using HTML, and often integrate images, sound, and other media that are commonly viewed using a browser. See also HTML and browser.

Hypertext Markup Language See HTML.

I

ignore Exclude an object when aggregating and displaying Prime Performance Manager status information. See also unignore.

installation log Log containing messages and other information recorded during installation.

interface Connection between two systems or devices.

internal ID Unique identifier assigned by Prime Performance Manager, for its own internal use.

Internet Protocol See IP.

IP Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791.

IP address 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. See also IP.

IPC Inter Processor Communication.

ITU International Telecommunication Union.

K

known See discovered.

L

LAN Local Area Network.

local authentication Type of Prime Performance Manager security authentication that allows the creation of user accounts and passwords local to Prime Performance Manager system. When using this method, usernames, passwords, and access levels are managed using Prime Performance Manager commands.

For more information on Solaris authentication, see the "Implementing Secure User Access" section on page 2.

local IP address IP address used by Prime Performance Manager client to connect to Prime Performance Manager server.

M

Management Information Base See MIB.

mask Bit combination used in Prime Performance Manager to indicate the significant bits of the point code.

For ANSI and China standard networks using the default 24-bit point code format, the default mask is **255.255.255**.

For ITU networks using the default 14-bit point code format, the default mask is **7.255.7**.

For NTT and TTC networks using the default 16-bit point code format, the default mask is **31.15.127**.

Message Log Server Multi-threaded processes that logs messages from the Process Manager and Prime Performance Manager client. See also Process Manager.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

N

name server Server connected to a network that resolves network names into network addresses.

NAT Network Address Translation. Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

Network Address Translation See NAT.

network management system See NMS.

Network Time Protocol See NTP.

new node Node that Prime Performance Manager has newly discovered, and that has not yet been added to the current view.

NMS Network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer such as an engineering workstation. NMSes communicate with agents to help keep track of network statistics and resources.

node Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations.

node name Name of a node. This is either the DNS name of the node, or a user-specified name. See display name, DNS name.

note User-defined descriptive string attached to an object.

NTP Network Time Protocol. Timing protocol that maintains a common time among Internet hosts in a network.

P

PDU Protocol Data Unit. OSI term for packet.

ping Packet internet groper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

polling Access method in which a primary network device inquires, in an orderly fashion, whether secondaries have data to transmit. The inquiry occurs in the form of a message to each secondary that gives the secondary the right to transmit.

poll interval Time between polls.

poll response Time taken by a node to respond to Prime Performance Manager poll requests.

port In IP terminology, an upper-layer process that receives information from lower layers. Ports are numbered, and each numbered port is associated with a specific process. For example, SMTP is associated with port 25. A port number is also called a well-known address.

preferences Settings that enable a user to change the way Prime Performance Manager presents information.

primary SNMP address IP address used by SNMP to poll the node. (There might be other IP addresses on the node that are not the primary SNMP address.) Contrast with secondary IP address.

process Internal execution component of Prime Performance Manager. See Message Log Server, Process Manager.

Process Manager Multi-threaded process that handles the management of registered Prime Performance Manager processes.

Q

QoS Quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

Quality of Service See QoS.

R

RAN Radio Access Network.

RAN backhaul The end-to-end RAN connections between the BTS or Node B at the cell site and the BSC or RNC.

RAN shorthaul An interface that transports GSM or UMTS voice and data traffic between the BTS or Node-B and the RAN-O node at the cell site. At the aggregation site, RAN shorthauls exist between the RAN-O node and the BSC or RNC.

RAN-O RAN optimization. Standard-based, end-to-end, IP connectivity for GSM and UMTS RAN transport. The Cisco solution puts RAN voice and data frames into IP packets at the cell-site, and transports them seamlessly over an optimized backhaul network. At the central site, the RAN frames are extracted from IP packets, and the GSM or UMTS data streams are rebuilt.

read community See community string.

recursive Discovery Discovery of the entire network. Prime Performance Manager discovers all seed nodes and attempts to manage them; then attempts to discover and manage all ITP nodes that are adjacent to those seed nodes (unless the nodes are connected by serial links only); then attempts to discover and manage all ITP nodes that are adjacent to *those* nodes; and so on, until Prime Performance Manager has discovered the entire network.

route Path through an internetwork.

S

secondary IP address Alternate or backup IP address used by a node. Contrast with primary SNMP address.

seed file List of seed nodes. See seed node.

seed node Node used by Prime Performance Manager to discover the other objects in your network.

server Node or software program that provides services to clients. See client.

Simple Network Management Protocol See SNMP.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SOAP Simple Object Access Protocol. A protocol for exchanging XML-based messages over computer networks. See XML.

SSL Secure Sockets Layer. A protocol for transmitting private documents via the Internet.

status Current condition, such as Active or Unknown, of a network object.

status polling Regularly scheduled polling of nodes performed by Prime Performance Manager. Contrast with demand polling.

system object ID See device type.

T

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. See also TCP/IP.

TCP/IP Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite. See also IP and TCP.

TFTP Trivial File Transfer Protocol. A protocol that is used to transfer small files between hosts of a network. See also host.

thread name Task name.

timeout Event that occurs when one network device expects to hear from another network device within a specified period of time, but does not. The resulting timeout usually results in a retransmission of information or the dissolving of the session between the two devices.

tooltip Popups that display information about objects and table entries.

Transmission Control Protocol See TCP.

Transmission Control Protocol/Internet Protocol See TCP/IP.

Trivial File Transfer Protocol See TFTP.

U

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

unignore Stop ignoring the selected object at the next polling cycle. See also ignore.

unknown Device type for which Prime Performance Manager is unable to determine the device type. If a node, the node failed to respond to an SNMP request. If a linkset or link, either the associated node failed to respond to an SNMP request, or Prime Performance Manager found that the linkset or link no longer exists. Contrast with discovered.

unmanaged Node status in which the node is known indirectly by Prime Performance Manager (Prime Performance Manager knows the device exists but no known SNMP stack exists on the device for Prime Performance Manager to query), or a user has set the node to this status to prevent Prime Performance Manager from polling the node.

User-Based Access Prime Performance Manager security scheme that provides multi-level password-protected access to Prime Performance Manager features. Each user can have a unique username and password. Each user can also be assigned to one of five levels of access, which control the list of Prime Performance Manager features accessible by that user.

For more information, see the "Setting User Access" section in Chapter 6, "Setting Up and Managing Users."

User Datagram Protocol See UDP.

Amount of an object's send or receive capacity that is being used, expressed as a percentage or in Erlangs.

W

World Wide Web See WWW.

WWW World Wide Web. Large network of Internet servers providing hypertext and other services to terminals running client applications such as a browser. See also *browser*.

X

XML Extended Markup Language. A general-purpose markup language for to facilitating the sharing of data across different information systems connected through the Internet. See SOAP.

INDEX