Cisco Prime Performance Manager 1.3 User Guide

November 30, 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-27430-01

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Performance Manager 1.3 User Guide
© 2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xv

CHAPTER 1 **Overview to Prime Performance Manager** 1-1

- Features and Functions 1-1
- Reports 1-3
- Dashboards 1-3
- Architecture 1-4
- Device Discovery 1-6
- Security 1-6

CHAPTER 2 **Managing Gateways and Units Using the CLI** 2-1

- Root User Login 2-1
- Starting Gateways and Units 2-1
- Stopping Gateways and Units 2-3
- Restarting Gateways and Units 2-4
- Displaying Gateway and Unit Status 2-6
- Displaying Gateway and Unit Software Versions 2-8
- Limiting Client Access to Servers 2-9

CHAPTER 3 **Managing the Web Interface** 3-1

- Launching the Web Interface 3-1
  - Information Available from the Help Menu 3-5
  - Checking Your Web Browser 3-7
- Changing User Preferences 3-7
- Changing System Configuration Settings 3-11
- Changing the GUI Polling Refresh Setting 3-13
- Adding and Removing Properties from Property Views 3-13
- Sorting Tables 3-14
- Displaying Prime Performance Manager Information 3-14

CHAPTER 4 **Prime Central Integration** 4-1

- Integrating Prime Performance Manager with Prime Central 4-1

Prime Central Integration Considerations and Next Steps 4-5

CHAPTER 5 **Discovering Network Devices** 5-1

Device Discovery Requirements 5-1
Discovering Gateways and Units 5-2
Importing Devices From Prime Network 5-2
Enabling Prime Network Cross-Launching 5-4
Prime Performance Manager Device Discovery 5-4
Managing Device Credentials 5-5
Adding SNMP Credentials 5-5
Editing SNMP Credentials 5-6
Deleting SNMP Credentials 5-6
Adding Telnet and SSH Credentials 5-7
Deleting Telnet/SSH Credentials 5-9
Telnet and SSH Credential Notes 5-9
Adding Credentials for Cisco Carrier Packet Transport Devices 5-10
Running Device Discovery from Prime Performance Manager 5-10
Data Center Device Support 5-12
Discovering Nexus Switches in VDC Mode 5-13
Hypervisor Discovery Requirements 5-14
XEN and KVM TLS Discovery Requirements 5-14

CHAPTER 6 **Managing Users and Security** 6-1

Setting Up User Access and Security 6-1
Enabling SSL on Gateways and Units 6-2
Enable SSL on a Gateway or Collocated Gateway and Unit 6-3
Enable SSL on Remote Units 6-4
Export SSL Certificates 6-5
Display SSL Status 6-5
Print SSL Certificates 6-5
Display SSL Key and Certificate 6-6
Disable SSL 6-6
User Authentication 6-7
Authentication Through PAM, TACACS+, and LDAP 6-7
Configuring User Passwords 6-9
Modifying the Password Policy 6-9
User Security Levels 6-10
Enabling Secure User Access 6-11
Disabling Secure User Access 6-12

Managing Users and User Security 6-12
Add New Users 6-12
Edit User Information 6-13
Edit User Reports 6-14
Change User Passwords 6-15
Edit User Security Settings 6-16
Manually Disable Users and Passwords 6-17
Enable User Accounts and Passwords Using the CLI 6-18
Create Messages of the Day 6-19
Display Active Sessions 6-20
List Currently Defined Users 6-20
Display the System Security Log 6-21

CHAPTER 7 **Managing Reports, Dashboards, and Views** 7-1
Displaying Reports 7-1
Reports Menu Bar 7-3
Displaying Network and Device Reports 7-6
Customizing Report Display 7-9
Creating Custom Device Star Graphs 7-12
Filtering Report Information 7-13
Changing the Master Report Settings 7-14
Enabling and Disabling Reports 7-16
Capability Polling 7-18
Exporting Reports in 3GPP XML Format 7-19
Creating Report Policies 7-20
Editing Report Policy Parameters 7-20
Creating a New Report Policy 7-21
Assigning Devices to Report Policies 7-21
Displaying Report Definitions 7-22
Displaying Data Center Reports 7-22
Setting Up Bulk Statistics Reports 7-24
Creating the Device Bulk Statistics Configuration 7-27
Removing Bulk Statistics Device Configurations 7-28
Adding New Bulk Statistics Schemas or Counters 7-28
Updating the Prime Performance Manager Bulk Statistics Schema File 7-28
Bulk Statistics Alarms 7-29
Managing Dashboards 7-31
Displaying Dashboards Status 7-31
Editing Dashboard Display 7-32

Creating and Managing Custom Report Views 7-34
Creating a Custom Report View 7-34
Adding Views to the Navigation Tree 7-35
Copying and Pasting Views 7-36
Modifying Custom Report Views 7-37
Merging View Charts 7-40
Editing Views 7-40
Creating and Managing Report Groups 7-42
Provided Groups 7-43
Creating a Report Group 7-44
Creating Algorithms Using the Algorithm Editor 7-45
Managing Report Groups 7-47
Displaying Group Reports 7-48

CHAPTER 8 **Managing Devices** 8-1
Displaying Network-Level Device Information 8-1
Displaying Network-Level Device Properties 8-2
Displaying Device Type Distributions 8-4
Displaying Alarms by Device 8-5
Displaying Alarms by Device Type 8-6
Displaying Device SNMP Time Out Alarms 8-7
Displaying Device Poll Responses 8-7
Displaying Device ICMP Ping Responses and Availability 8-8
Displaying Device Up Time 8-8
Displaying Device Software 8-9
Displaying Device Contacts and Locations 8-9
Displaying Device Vendors 8-10
Displaying Device Details in Cisco Prime Format 8-10
Managing Devices in the Network-Level View 8-11
Editing a Device Name, Web Port, and Time Zone 8-13
Editing the Device Credentials 8-13
Editing the Report Policy Assigned to a Device 8-15
Editing the Polling Group Assigned to a Device 8-15
Editing the Device SNMP IP Addresses 8-16
Relocating Devices to Units 8-16
Displaying Individual Device Information 8-17
Managing an Individual Device 8-21
Creating and Editing Device Polling Groups 8-22
Editing Polling Group Parameters 8-23

Creating a New Polling Group 8-23
Assigning Devices to Polling Groups 8-24

CHAPTER 9 **Managing Network Alarms and Events** 9-1
Displaying Active Alarms and Event History 9-1
Managing Alarms and Events 9-3
Displaying an Alarm Summary 9-4
Filtering Alarms and Events 9-4
Displaying Alarm and Event Properties 9-6
Adding Notes to Alarms or Events 9-7
Displaying Alarm or Event Details 9-8
Displaying Alarm Events 9-8
Displaying Daily Alarm and Event Archives 9-9
Displaying Device Details for an Alarm 9-9
Displaying Alarms by Device From the Alarms Window 9-11
Displaying Alarms by Device Type From the Alarms Window 9-11
Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters 9-11
Adding Upstream OSS Hosts 9-11
Editing Upstream OSS Hosts 9-12
Configuring Alarms Sent to OSS Hosts 9-13
Configuring Alarms Sent to E-mail Addresses 9-13
Forwarding Traps Directly to Hosts 9-14
Tuning Event and Alarm Parameters 9-15
Prime Performance Manager SNMP Traps 9-16
CISCO-PRIME Notification Attributes 9-16
CISCO-EPM-2 Trap Notification Attributes 9-19

CHAPTER 10 **Configuring Thresholds** 10-1
Creating Thresholds 10-1
Managing Thresholds 10-5
Editing Thresholds from the Threshold Editor 10-5
Editing Thresholds from the Alarms Window 10-6
Duplicating Thresholds 10-7
Enabling and Disabling Thresholds 10-8
Deleting Thresholds 10-9
Viewing Threshold Events 10-9

CHAPTER 11 **Displaying System Properties, Statuses, Messages, and Logs** 11-1
System Properties, Statuses, Logs, and Messages Overview 11-1

Displaying Connected Clients and System Status 11-2
Displaying System Logs 11-4
Displaying the Install Log 11-4
Displaying the Patch Log 11-4
Displaying the Console Log 11-5
Displaying the System Check Log 11-5
Displaying the Backup Log 11-5
Displaying the CLI Command Log 11-5
Displaying the Event Automation Log 11-6
Displaying the Security Log 11-6
Displaying the Application Audit Logs 11-7
Displaying the Console Log Archived Messages 11-7
Managing Log Files 11-7
Displaying System Properties and Settings 11-8
Displaying System Settings 11-8
Displaying Poller Settings 11-9
Displaying Web Settings 11-9
Displaying Reports Settings 11-10
Displaying System Messages 11-11
Displaying Information and Error Messages 11-11
Displaying User Actions 11-12
Displaying Archived Messages 11-13

CHAPTER 12 **Managing Gateways and Units** 12-1
Displaying Gateway and Unit Information 12-1
Displaying Detailed Gateway and Unit Information and Performance 12-3
Managing Gateway and Unit Connectivity 12-5
Managing Device-to-Unit Assignments 12-5
Displaying Device-to-Unit Assignments 12-6
Creating Device-to-Unit Maps 12-6
Editing Device-to-Unit Maps 12-7
Deleting Device-to-Unit Maps 12-7
Changing a Device-to-Unit Assignment 12-8
Creating Unit Protection Groups 12-8
Unit Protection Group Failover Scenarios 12-11
Managing Gateway High Availability 12-11
Managing Local High Availability 12-12
Local HA Operations Notes 12-13

Local HA Failovers and Switchovers 12-14
Freezing and Unfreezing RHCS 12-14
Switching the RHCS Cluster Server 12-15
Changing the Floating IP Address 12-15
RHCS Log Messages 12-16
Configuring the RHCS Conga Web Interface 12-17
Managing Geographical High Availability 12-18
Displaying Geographical HA Status 12-19
Switch the Primary and Secondary Geographical HA Gateways 12-20
Configure Geographical HA 12-21
Synchronizing the Geographical HA Gateways 12-21
Freezing and Unfreezing Geographical HA Gateways 12-22
Backing Up and Restoring Geographical HA Gateway Data 12-22
Accessing Geographical HA Gateways Using the GUI 12-22
Managing Devices in Geographical HA Gateways 12-23
Managing Users in Geographical HA Gateways 12-23
Managing Reports, Views, and Groups in Geographical HA Gateways 12-23
Managing Alarms and Events in Geographical HA Gateways 12-23
Managing Thresholds in and Upstream Alarm Hosts in Geographical HA Gateways 12-24
Configuring SSL on Geographical HA Gateways and Remote Units 12-24
Unit Redundancy Groups and Geographical HA 12-25
Managing Geographical and Local High Availability 12-25
Manual Disaster Recovery 12-26

CHAPTER 13 **Configuring Prime Performance Manager for Firewalls** 13-1
Gateway-to-Unit Connectivity 13-1
Configuring Gateways and Units for Firewalls 13-2
Configuring Web Client and Gateway Communication 13-3
Configuring Gateway and Unit Communication 13-3
Configuring Unit and Device Communication 13-6

CHAPTER 14 **Backing Up and Restoring Prime Performance Manager** 14-1
Prime Performance Manager Back Up and Restore Process 14-1
Backing Up Prime Performance Manager Data Files 14-2
Changing the Backup Directory 14-3
Setting the Number of Backup Days 14-3
Restoring Prime Performance Manager Data Files 14-3

APPENDIX A **Prime Performance Manager and IPv6** A-1

IPv6 Support in Prime Performance Manager A-1
Adding SNMP and Telnet/SSH Credentials A-1
Unit Configuration A-2
Device Discovery A-2
Reports A-2
Device Management Actions A-2
Alarms and Events A-2
Clients A-2
Trap Forwarding A-3
Prime Network Integration A-3
Command Line Interface A-3
IPv6 Troubleshooting A-3

APPENDIX B **Prime Performance Manager Commands** B-1

Prime Performance Manager B-5
ppm addcreds B-5
ppm addsnmpcomm B-6
ppm addunitconf B-6
ppm adduser B-7
ppm authtype B-7
ppm backup B-8
ppm backupdata B-9
ppm backupdays B-9
ppm backupdir B-10
ppm backuplog B-11
ppm backuprep B-11
ppm backupstats B-11
ppm badloginalarm B-12
ppm badlogindisable B-12
ppm bulkstatsage B-13
ppm certtool B-13
ppm changes B-14
ppm checksystem B-14
ppm clitimeout B-14
ppm cmdlog B-15
ppm compilemibs B-15
ppm console B-16

ppm consolelogsize B-16
ppm countnodes B-16
ppm crosslaunch B-16
ppm csvdrop B-17
ppm datadir B-17
ppm dbbackupdir B-18
ppm delete B-18
ppm deletecreds B-19
ppm deletesnmpcomm B-19
ppm deleteunitconf B-19
ppm deluser B-20
ppm devcachedir B-20
ppm disablepass B-20
ppm disablepwdage B-21
ppm disableuser B-21
ppm discover B-22
ppm diskcheck B-22
ppm diskmonitor B-22
ppm dumpdb B-23
ppm enablepwdage B-24
ppm enableuser B-24
ppm eventautolog B-24
ppm eventconfig B-25
ppm eventlimitsconfig B-25
ppm eventsnmpserversconfig B-26
ppm eventtool B-26
ppm evilstop B-28
ppm export B-28
ppm exportcustnames B-28
ppm exportusers B-28
ppm gatewayname B-29
ppm genkey B-29
ppm help B-29
ppm ifnameformat B-30
ppm importcustnames B-30
ppm importcw B-30
ppm inactiveuserdays B-31
ppm installlog B-32
ppm inventoryimport B-32
ppm iosreport B-32

ppm ipaccess B-33
ppm ipslaftpfilesize B-33
ppm jspport B-34
ppm keytool B-34
ppm listusers B-35
ppm localhabackupflag B-35
ppm localhacommands B-36
ppm localhappmtimeout B-36
ppm logdir B-36
ppm logger B-37
ppm logsize B-37
ppm logtimemode B-38
ppm maxasciirows B-39
ppm maxhtmlrows B-39
ppm maxpagesize B-40
ppm maxrepqueries B-40
ppm mldebug B-40
ppm modifysnmpcomm B-41
ppm modifyunitconf B-42
ppm motd B-42
ppm movenode B-43
ppm msglog B-43
ppm msglogage B-43
ppm msglogdir B-44
ppm netlog B-44
ppm netlogger B-45
ppm newlevel B-45
ppm optimizecapabilitypoll B-45
ppm osinfo B-46
ppm passwordage B-46
ppm patchlog B-47
ppm ping B-47
ppm poll B-47
ppm premotd B-48
ppm primecentralintegration B-48
ppm primeha B-49
ppm print B-50
ppm printreportstatus B-50
ppm props B-50
ppm purgedb B-51

ppm pwdchangeinterval B-51
ppm pwdchangelimit B-52
ppm pwdchangerestrict B-52
ppm readme B-53
ppm reboot B-53
ppm redistributenodes B-53
ppm redundancygroups B-54
ppm reloadbulkstats B-55
ppm reloadmibs B-55
ppm repdir B-56
ppm rephelp B-56
ppm restart B-56
ppm restore B-57
ppm restore all B-57
ppm restoreprops B-58
ppm rootvars B-58
ppm sechelp B-58
ppm seclog B-59
ppm servername B-59
ppm setpath B-60
ppm setpctrapdestination B-61
ppm showcreds B-61
ppm showsnmpcomm B-61
ppm showunitconf B-62
ppm singlesess B-62
ppm snmpcomm B-63
ppm snmpconf B-63
ppm snmpget B-63
ppm snmphelp B-66
ppm snmpmaxrows B-66
ppm snmpnext B-66
ppm snmpsetup B-68
ppm snmpwalk B-69
ppm ssl B-71
ppm sslstatus B-72
ppm starbuild B-72
ppm start B-73
ppm statreps B-73
ppm status B-75
ppm status B-75

ppm smtpport B-75
ppm syncunits B-76
ppm traprelay B-76
ppm tac B-77
ppm topxxsize B-77
ppm traceroute B-77
ppm uninstall B-78
ppm unknownage B-78
ppm updateuser B-78
ppm useraccess B-79
ppm userpass B-79
ppm version B-80
ppm who B-80
ppm xmlpoll B-81

APPENDIX C **Predefined Thresholds** C-1

GLOSSARY

INDEX

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 1.3 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, "Overview to Prime Performance Manager." For the latest Prime Performance Manager information and software updates, go to http://www.cisco.com/go/performance.

This preface includes the following topics:

- Audience, page xv
- Organization, page xvi
- Conventions, page xvii
- Product Documentation, page xvii
- Obtaining Documentation and Submitting a Service Request, page xviii

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:

- Chapter 1, "Overview to Prime Performance Manager," provides brief descriptions of Prime Performance Manager architecture, and an overview of how to use Prime Performance Manager to monitor your network performance.
- Chapter 2, "Managing Gateways and Units Using the CLI," tells you how to use Prime Performance Manager commands to manage gateways and units.
- Chapter 3, "Managing the Web Interface," describes how to access Prime Performance Manager data from the web interface.
- Chapter 4, "Prime Central Integration," provides information and procedures to integrate Cisco Prime Central with Prime Performance Manager.
- Chapter 5, "Discovering Network Devices," provides device discovery information and procedures including importing devices from Cisco Prime Network and discovering devices from Prime Performance Manager.
- Chapter 6, "Managing Users and Security," provides information about setting up and managing Prime Performance Manager users.
- Chapter 7, "Managing Reports, Dashboards, and Views," describes how to view and manage Prime Performance Manager reports, dashboards, views, and groups.
- Chapter 8, "Managing Devices," describes how to view and manage devices that have been added to Prime Performance Manager.
- Chapter 9, "Managing Network Alarms and Events," describes how to view and manage Prime Performance Manager alarms and events, including upstream OSS host creation and alarm tuning.
- Chapter 10, "Configuring Thresholds," describes how to create and manage thresholds in Prime Performance Manager.
- Chapter 11, "Displaying System Properties, Statuses, Messages, and Logs," describes Prime Performance Manager system logs and messages.
- Chapter 12, "Managing Gateways and Units," describes how to manage Prime Performance Manager units including creating of unit protection groups and gateway high availability.
- Chapter 13, "Configuring Prime Performance Manager for Firewalls," tells you how to configure Prime Performance Manager gateways and units for communication through firewalls.
- Chapter 14, "Backing Up and Restoring Prime Performance Manager," describes the Prime Performance Manager backup and restore processes.
- Appendix A, "Prime Performance Manager and IPv6," provides information about how Prime Performance Manager handles IPv6 addressing.
- Appendix B, "Prime Performance Manager Commands," describes the CLI commands that you can use to set up and operate Prime Performance Manager.
- Appendix C, "Predefined Thresholds," lists the predefined thresholds that are included in 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 1.3 User Guide* (this guide)
- *Cisco Prime Performance Manager 1.3 Release Notes*
- *Cisco Prime Performance Manager 1.3 Quick Start Guide*
- *Cisco Prime Performance Manager 1.3 Integration Developer Guide*
- *Open Source Used in Cisco Prime Performance Manager 1.3*
- *Cisco Prime Performance Manager 1.3 Documentation Overview*

Prime Performance 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

Overview to Prime Performance Manager

Cisco 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.

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

- Features and Functions, page 1-1
- Reports, page 1-3
- Dashboards, page 1-3
- Architecture, page 1-4
- Device Discovery, page 1-6
- Security, page 1-6

Features and Functions

Prime Performance Manager acquires devices by importing Cisco Prime Network devices or by running device discovery (see Chapter 5, “Discovering Network Devices”). After acquiring devices, Prime Performance Manager uses SNMP polling to collect device performance statistics. Prime Performance Manager sends SNMP get, getnext, and getbulk requests to the device targeting many different SNMP MIBs. The device responds with data, and Prime Performance Manager collects the data and allows you to display it in many different ways in the Prime Performance Manager GUI.

In addition to SNMP, Prime Performance Manager supports Telnet and SSH polling for Y.1731 reports, and CSV-based (bulkstats) data collection.

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, 5000, 5500, 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, CSV-based (bulk statistics) data collectin for StarOS mobile wireless reports, and many others.

Prime Performance Manager also provides extensive data center support including reports for data center networking, computing, storage, and virtualization devices and technologies. For a list of supported data center devices and technologies, see Displaying Data Center Reports, page 7-22.

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 over 2800 standard historical, aggregation, and summary reports. Reports can be automatically generated on a 1-minute, 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 use an XML editor to define new reports or extend the packaged reports. All reports are available in graph and table view formats in the GUI, and in CSV export format.

Note For a list of all reports provided with Prime Performance Manager, from the Help menu, choose **Reports**, then click **Reports List Readme**.

Additional Prime Performance Manager features and functions include:

- The ability to add and manage users when installed as a standalone product, and integration with Cisco Prime Central user management when integrated with Cisco Prime Central.
- 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 reports based on groups of network objects, for example, a reporting group based on a particular type of interface.
- The ability to create report policies that specify report sets for specific devices.
- The ability to create custom report views so that you can watch specific report data items pulled from different reports and for different devices.
- The ability to create and display star graphs for each device separate from the custom report views.
- 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 and Cisco Prime Central, 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 CLI-based and CSV-based (bulk statistics) data collection.
- N+1 high availability protection groups for units.
- Gateway local high availability using the Red Hat Cluster Suite and geographical high availability.
- 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.
- Capability to export report data using Representation State Transfer (REST) north bound API.
- Automatic and custom CSV file generation.
- Pull model CSV file access.

- IPv6 address support.

Reports

Prime Performance Manager includes over 1900 reports. All reports support table, chart, and dashboard outputs. High-level report categories include:

- Application Traffic
- Availability
- Data Network Services
- Hypervisors
- IP Protocols
- IP QoS
- IP SLA
- Mobile IOS Statistics
- Mobile StarOS Statistics
- PPM System
- Resources
- Security
- StarOS CDMA Statistics
- Storage
- Transport Statistics
- UCS Clusters
- Video Broadcast
- Virtualization

In addition, Prime Performance Manager Data Center view provides an extensive range of data center networking, computing, storage, and virtualization device and technology reports. For more information about Prime Performance Manager reports, see Chapter 7, "Managing Reports, Dashboards, and Views."

You can modify the provided Prime Performance Manager reports or create new reports. For information, see the *Cisco Prime Performance Manager 1.3 Integration Developer Guide*.

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
- Availability

- IP Protocols
- IP QoS
- IPSLA
- Network Health
- Resource
- Response Time
- Server Health
- Transport
- VPDN
- Video Broadcast

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 dashboards, see Chapter 7, "Managing Reports, Dashboards, and Views."

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.

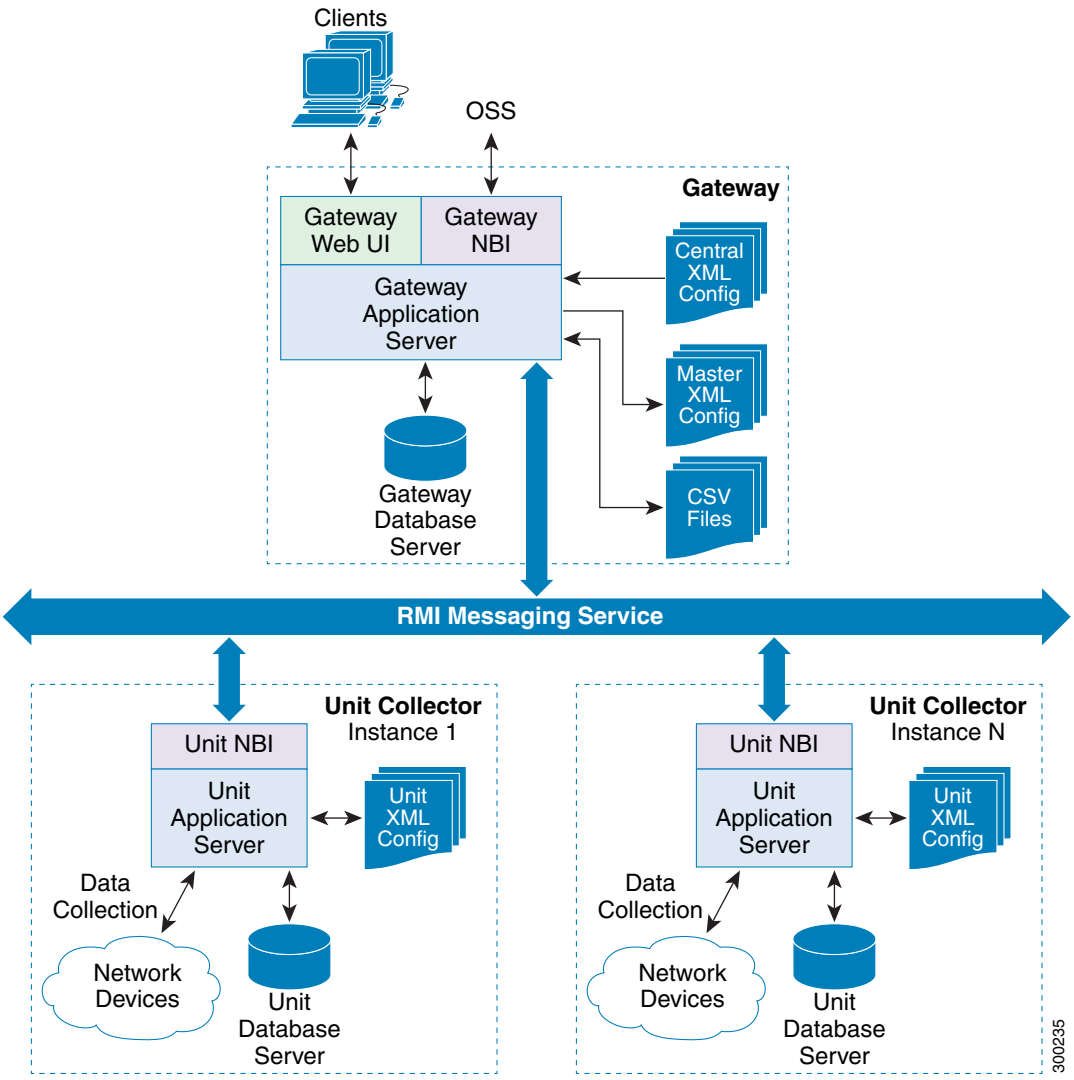
Units poll network devices and compute and store the data received from the devices. A unit can be installed with a gateway on the same physical server, or a unit can be installed on a separate physical server. The monitored devices are distributed across a single or multiple units, as directed by the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

All unit monitoring and management is conducted through the gateway. Gateway-to-unit communication is conducted using Java Remote Method 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 Prime Central.
- Run device discovery from Prime Performance Manager.

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

For more information about Prime Performance Manager device discovery, see Chapter 5, "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 6, "Managing Users and Security."

CHAPTER 2

Managing Gateways and Units Using the CLI

The following topics tell you how to start, stop, and restart Prime Performance Manager gateways and units, and how to display their status and software versions:

- Root User Login, page 2-1
- Starting Gateways and Units, page 2-1
- Stopping Gateways and Units, page 2-3
- Restarting Gateways and Units, page 2-4
- Displaying Gateway and Unit Status, page 2-6
- Displaying Gateway and Unit Software Versions, page 2-8

Root User Login

Starting, stopping, or restarting Prime Performance Manager gateways and units requires you to log in as the root user.

To log in as the root user, enter:

```
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 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.
- If you will run CSV-based reports, the device must be configured with Prime Performance Manager drop location and the same need to be updated in BulkStats.properties, which is located in /opt/CSCOppm-unit/properties/. For more information, see Setting Up Bulk Statistics Reports, page 7-24.

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 Root User Login, 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 Root User Login, 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 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 Root User Login, 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-unit/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 in to the unit as the root user. See Root User Login, 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 Root User Login, 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-unit/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 Root User Login, 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.
```

Displaying 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 Root User Login, 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:      1.3.0.6
Prime Performance Manager Gateway Build   Date: Thu Mar 22 02:03 EST 2012
Prime Performance Manager Gateway Install Date: Fri Mar 23 04:49 EDT 2012
Prime Performance Manager Gateway IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Gateway SSL Support:  Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.3.0.6Thu Mar 22 02:03 EST 2011
   sgmDataServer:      1.3.0.6Thu Mar 22 02:03 EST 2011
================================================================================
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:
    Thu Mar 22 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: 2012/03/23 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:      1.3.0.6
Prime Performance Manager Unit Build   Date: Thu Mar 22 02:03 EST 2012
Prime Performance Manager Unit Install Date: Fri Mar 23 04:51 EDT 2012
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.3.0.6 Thu Mar 22 02:03 EST 2012
   sgmDataServer:      1.3.0.6 Fri Mar 23 04:51 EDT 2012
================================================================================
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:
    Thu Mar 22 02:03:47 EDT 2012
Linux Uptime:
 16:31:30 up 329 days,  9:24,  1 user,  load average: 1.17, 1.30, 1.28

Current Time: 2012/03/23 16:31:23 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 Root User Login, 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:      1.3.0.6
Prime Performance Manager Unit Build   Date: Thu Mar 22 02:03 EST 2012
Prime Performance Manager Unit Install Date: Fri Mar 23 04:51 EDT 2012
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.3.0.6 Thu Mar 22 02:03 EST 2012
   sgmDataServer:      1.3.0.6 Fri Mar 23 04:51 EDT 2012
================================================================================
Current Time: 2012/03/23 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-unit/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**.

Displaying Gateway and Unit Software Versions

Complete the following steps to view the Prime Performance Manager software version installed on gateways and units:

Step 1 Log in as the root user or admin user. See Root User Login, 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:

The gateway status is displayed, for example:

```
================================================================================
Prime Performance Manager Gateway Version:      1.3.0.6
Prime Performance Manager Gateway Build   Date: Thu Mar 22 02:03 EST 2012
Prime Performance Manager Gateway Install Date: Fri Mar 23 04:49 EDT 2012
Prime Performance Manager Gateway IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Gateway SSL Support:  Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.3.0.6Thu Mar 22 02:03 EST 2011
   sgmDataServer:      1.3.0.6Thu Mar 22 02:03 EST 2011
================================================================================

Current time is: 2012/03/23 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:      1.3.0.6
Prime Performance Manager Unit Build   Date: Thu Mar 22 02:03 EST 2012
Prime Performance Manager Unit Install Date: Fri Mar 23 04:51 EDT 2012
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.3.0.6 Thu Mar 22 02:03 EST 2012
   sgmDataServer:      1.3.0.6 Fri Mar 23 04:51 EDT 2012
================================================================================

Current time is: 2012/03/23 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 Root User Login, 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:      1.3.0.6
Prime Performance Manager Unit Build   Date: Thu Mar 22 02:03 EST 2012
Prime Performance Manager Unit Install Date: Fri Mar 23 04:51 EDT 2012
Prime Performance Manager Unit IP Address: nnn.nnn.nnn.nnn
```

```
Prime Performance Manager Unit SSL Support:  Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.3.0.6 Thu Mar 22 02:03 EST 2012
   sgmDataServer:      1.3.0.6 Fri Mar 23 04:51 EDT 2012
================================================================================

Current time is: 2012/03/23 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-unit/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-33.

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

Managing the Web Interface

The Cisco Prime Performance Manager web interface is the primary method for displaying network reports and managing network devices and information. The following topics tell you how to launch the Prime Performance Manager web interface and customize web interface display and polling:

- Launching the Web Interface, page 3-1
- Changing User Preferences, page 3-7
- Changing the GUI Polling Refresh Setting, page 3-13
- Adding and Removing Properties from Property Views, page 3-13
- Sorting Tables, page 3-14

Launching the Web Interface

The 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 10.0.
- Solaris: Mozilla Firefox 10.0
- Red Hat Linux Enterprise 5.3, 5.5, 5.7, or 6.2: Mozilla Firefox 10.0.

Note Although Safari was not formally tested, the browser is widely used with Prime Performance Manager.

In addition, your browser must have cookies enabled. If cookies are not enabled, enable them following procedures appropriate for your browser.

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://ppm-server:4440`

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

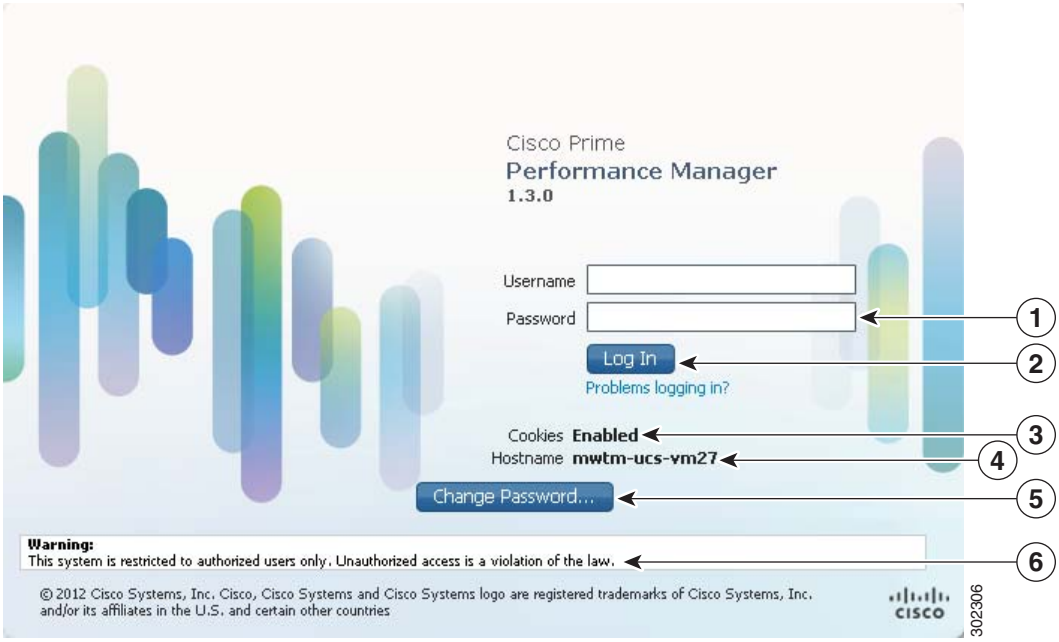
Note If user access is enabled, use https instead of http.

Note If you connect the gateway with its literal IPv6 address, enclose the address with brackets, for example, http://[2011::2:21b:78ff:febd:9e16]:4440.

Step 2 If user access is enabled (see Setting Up User Access and Security, page 6-1), the Prime Performance Manager login screen appears (Figure 3-1). The screen displays:

- Username—Enter your username.
- Password—Enter the password for the username entered.
- Log In—Starts the login.
- Cookies—Indicates whether cookies are enabled on your browser. If cookies are disabled, enable cookies following procedures for your browser before you log in.
- Hostname—The gateway hostname where you are logging in.
- Change Password—Allows you to change your password. To change your password, enter your current username and password, then click **Change Password**. Enter the new password in the Change Password dialog box.
- Authorized users message—Appears at the bottom of the login window. This message can be modified by administrators. See Create Messages of the Day, page 6-19.

Figure 3-1 Login Window



1	Login username and password fields	4	Gateway hostname
2	Login button	5	Change Password button
3	Web browser cookies setting.	6	Authorized users message

Step 3 After you enter your username and password, click **Log In**.

The Cisco Prime Performance Manager GUI application launches. By default, the Performance Reports View Editor is displayed (Figure 3-2). The View Editor allows you to create custom views with report data pulled from different reports and devices. It allows you to view the network performance areas that are of special interest. For more information, see Creating and Managing Custom Report Views, page 7-34.

The GUI window is comprised of the following elements:

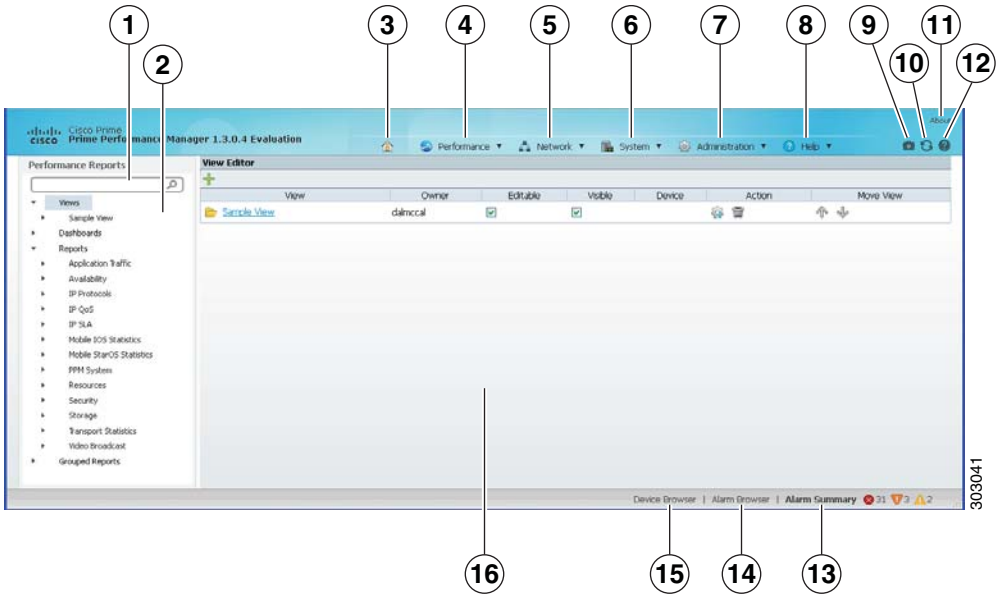
- Main menus—Prime Performance Manager provides five main menus that appear in all windows: Home, Performance, Network, System, Administration, and Help. Submenus displayed from each main menu are described in Table 3-1.

  Note The System menu is only displayed for Administrator users.

- Navigation area—The navigation area is displayed in some, but not all, Prime Performance Manager views. It appears for all performance functions (Views, Dashboards, and Reports), and includes a search field that you can use to quickly find specific reports, dashboards, or views.
- Content area—The lower right portion of the GUI displays content selected from the main menus and navigation area items.
- Popup Device Browser, Alarm Browser, and Alarm Summary—The bottom of the window contains the global toolbar, which contains:
  - Device Browser—Lists all network devices and allows you to perform actions on them. The window contains a subset of properties that are displayed when you choose **Network > Devices**. For information, see Displaying Network-Level Device Properties, page 8-2.
  - Alarm Browser—Lists all network alarms by the occurrence date and time. The browser contains the same information that is displayed when you choose Network > Alarms/Events. For information, see Displaying Alarm and Event Properties, page 9-6.
  - Alarm Summary—Shows the number of alarms by device. This window is intended as a quick reference. The number of alarms displayed corresponds to the device history limit user preference. For information, see Changing User Preferences, page 3-7.

  The Device and Alarm Browser and the Alarm Summary appear whenever you move your cursor over them. You can turn off this feature. For information, see Changing User Preferences, page 3-7.

Figure 3-2 Prime Performance Manager Window



1	Performance Reports search field	**9**	User Preferences
2	Performance Reports navigation area	**10**	Refresh tool
3	Home	**11**	Information about Prime Performance Manager
4	Performance menu	**12**	Context help tool
5	Network menu	**13**	Alarm Summary
6	System menu	**14**	Alarm Browser
7	Administration menu	**15**	Device Browser
8	Help menu	**16**	Content area

Table 3-1 lists the Prime Performance Manager navigation menus and submenus, and provides topics where more information about the menu function is provided.

Table 3-1 Navigation Menus

Menu	Submenu	For information, see...
Home	N/A	Modifying Custom Report Views, page 7-37
Performance	Views	Creating and Managing Custom Report Views, page 7-34
	Dashboards	Managing Dashboards, page 7-31
	Reports	Displaying Reports, page 7-1
Network	*Network Overview*	
	Devices	Chapter 8, “Managing Devices”
	Alarms/Events	Chapter 9, “Managing Network Alarms and Events”

Table 3-1 Navigation Menus (continued)

Menu	Submenu	For information, see...
	Network Administration	
	SNMP Editor	Adding SNMP Credentials, page 5-5
	Polling Group Editor	Creating and Editing Device Polling Groups, page 8-22
	Telnet/SSH Editor	Adding Telnet and SSH Credentials, page 5-7
	Threshold Editor	Managing Thresholds, page 10-5
	Discovery	Chapter 5, "Discovering Network Devices"
System	*System Information*	
	Gateway/Units	Chapter 12, "Managing Gateways and Units"
	Status	System Properties, Statuses, Logs, and Messages Overview, page 11-1
	Logs	Displaying System Logs, page 11-4
	Messages	Displaying Information and Error Messages, page 11-11
	Security Messages	
	User Actions	Displaying User Actions, page 11-12
Administration	*System Administration*	
	Prime Central Integration	Chapter 4, "Prime Central Integration"
	Prime Network Integration	Importing Devices From Prime Network, page 5-2
	Users/Security	Chapter 6, "Managing Users and Security"
	Unit Editor	Managing Device-to-Unit Assignments, page 12-5
	Alarms/Events Editor	Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters, page 9-11
	Group Editor	Managing Report Groups, page 7-47
	System Settings	Displaying System Properties and Settings, page 11-8
	Reports Administration	
	Report Settings	Displaying Reports Settings, page 11-10
	Report Status	Enabling and Disabling Reports, page 7-16
	Report Policies	Creating Report Policies, page 7-20

Information Available from the Help Menu

The Help menu provides in-depth information about Prime Performance Manager reports and commands, and other application details that can be useful for those seeking a deeper understanding of Prime Performance Manager. Help menu items include:

- PPM Help—Displays the Prime Performance Manager online help. The online help is based on the *Prime Performance Manager User Guide*, and covers all product operations and procedures.
- Browser Check—Checks your browser for compatibility with Prime Performance Manager. For additional information, see Checking Your Web Browser, page 3-7.

- Readmes and CLI Commands—Includes product readmes and CLI command descriptions:
  - Readme—Describes Prime Performance Manager system requirements and installation procedures.
  - Changes—Lists the changes, bug fixes, and new features in the 1.3 release.
  - Devices Info—Displays a list of devices that have been used with Prime Performance Manager by customers and in labs.
  - CLI Commands—A summary list of Prime Performance Manager commands.
  - CLI Commands Help—More detailed command information from the Prime Performance Manager online help.
  - Release Notes—Displays system release note information.
  - Quick Start—Displays quick start steps to help you get up and running quickly.
- Reports—Displays Prime Performance Manager system and report information:
  - System Reports Readme—Displays the contents of README-Reports-system.html. This file contains 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 details.
  - User Reports Readme—Displays contents of README-Reports-user.html. This file contains user-created report information including the MIB variables 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.
  - Reports List Readme—Displays an alphabetical list of all 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.
- 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.
- Supported Devices—Displays a list of devices that Prime Performance Manager officially supports on Cisco.com.
- Release Notes—Displays the Prime Performance Manager Installation Guide release notes on Cisco.com.

Checking Your Web Browser

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

Step 1 From the Help menu, choose **Browser Check**.

Step 2 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). For Prime Performance Manager, cookies must be enabled
- 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. To ensure that you can view all Prime Performance Manager GUI elements, your screen should be set to a minimum of 1280 x 1024 pixels.
- Color Depth—Indicates the depth of the color display, for example, 16.

Changing User Preferences

Prime Performance Manager provides many options that allow you to change the information that is displayed and how it is displayed in the Prime Performance Manager GUI. The options help you tailor the GUI to your individual needs and preferences.

User preferences apply only to the individual user. How they are applied depend upon whether the gateway has user security enabled:

- User security enabled—User preferences apply only to the currently logged-in user. They apply any time the user logs in, regardless of the client machine. For information about user security, see Setting Up User Access and Security, page 6-1.
- User security not enabled—Preferences apply to only the client machine, as identified by its host name or IP address. Any user logging in from that client will see the user preferences that are applied from it. If you log in from a different client, the preferences will not be applied.

To change the user preferences:

Step 1 On the right side of the main menu bar, click **Preferences**. (If user security is enabled, you can also choose User Preferences from the user ID at the top of the window.)

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

- Device Display 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 System Name—Identifies devices by their system name.
  - Show Sync Name—Identifies devices by their sync name.
  - Show Business Tag - Custom Name—For devices imported from Prime Network, identifies devices by their Custom Name business tag.
  - Show Business Tag - DNS Name—For devices imported from Prime Network, identifies devices by their DNS Name business tag.
  - Show Business Tag - System Name—For devices imported from Prime Network, identifies devices by their System Name business tag.
  - Show Business Tag - Sync Name—For devices imported from Prime Network, identifies devices by their business tag.

  Additionally, complete the following device display attributes as needed:
  - Show Device Domain Names—If checked, displays the device domain names. This option is not enabled by default.
  - Show Device Details on Hover—By default, Prime Performance Manager displays device details when you move your cursor over a device link. Use this option to turn this feature off.
  - Show Deleted Device Data—If checked, Prime Performance Manager displays deleted devices in device windows without hyperlinks, so the device data can be viewed but not accessed. This option is not enabled by default.
  - Display Device Level Data in Device Time Zone—If checked, displays device time stamps in the device time zone. These include report title time stamps, calendar popup selections, summary table maximum date strings, graph date strings, tooltip hover information, the Timestamp column in report table format, and the Timestamp values in exported CSV files.The device time zone is determined from one of the following: the time zone provisioned by the user. (see Editing a Device Name, Web Port, and Time Zone, page 8-13), the device time zone provided when the device is imported from Prime Network, or by querying the device running configuration. If this option is not enabled, device times are displayed in gateway server time zone.
  - Device History Limit—Sets the device history limit, that is, the number of devices displayed in the Network Devices window (Network > Devices > Device Summary). The default is 20. The range is 5 to 100.
- Graph Color Settings—Allows you to edit the colors used in report and group graphs including graph data, plot area, borders, and text. Twenty colors are available. To edit a color, you can edit the color hex # directly in the color sample, or click **Open Color Picker** in the right side of the color sample. In the Color Picker dialog box, edit any of the following attributes:
  - H (hue), S (saturation), and V (value) percentages (0-100).
  - R (red) G (green), or B (blue) values (0 to 255).
  - Hex value: #000000-#ffffff.

  Alternatively, you can pick colors visually from either of the color selection areas; the HSV, RGB, hex values will populate automatically. The new and existing colors are displayed side-by-side.

  Click **OK** when you complete your edits.

Note The default colors are web-safe and selected to provide the highest differentiation on report charts. If you edit them, verify that they meet web requirements and do not reduce data differentiation on reports. To return to the default colors, click **Revert to Default Colors**.

- Utilization Color Settings—Allow you to define the ascending and descending utilization ranges to assign to green, gold, orange and red colors in report charts to make utilization values in various states of criticality easier to distinguish. Default values:
  - Ascending

    Green—00.00 > 50.00

    Gold—50.01 > 70.00

    Orange—70.01 > 90.99

    Red—91.00 > 100.00
  - Descending

    Green—100.00 > 99.91

    Gold—99.90 > 99.51

    Orange—99.50 > 99.01

    Red—99.00 > 00.00

  Text Color—Defines whether the chart text color will be displayed in green, orange, and red based on the utilization values:
  - On—Turns on the utilization colors for text.
  - Off—Turns off the utilization colors for text.
  - Red/Orange/Gold Only—Turns on utilization colors for text only red, gold, and orange colors.

  Background Color—Defines whether the chart table cell background color is displayed in green, orange, and red when the utilization values are reached:
  - Reports—Turns on the utilization colors for report chart table cells.
  - Dashboards/Views—Turns on the utilization colors for dashboard and view chart table cells.
  - Both—Turns on utilization colors for reports, dashboards, and view chart table cells.
  - Off—Turns off utilization colors for chart backgrounds.
- General Display Settings—Check any of the following display options:
  - Auto Expand Reports in Tree—If checked (default), automatically expands the reports in the navigation tree.
  - Depth—If Auto Expand Reports in Tree is turned on, specifies the navigation tree depth.
  - 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. This option is not displayed by default.
  - Show Last Login Date/Time After Login—If checked (default), displays the user's last login date and the time after login in the GUI window.

  - Enable Popup Alarm Browser and Summary—If checked (default), the popup Alarm Browser and Alarm Summary (see Figure 3-2 on page 3-4) appears whenever you move your cursor over Alarm Browser or Alarm Summary at the bottom of the Prime Performance Manager window.
  - Screen Refresh Interval—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 3-13 for information.

- Report Settings—Changes report display elements.
  - Show Min Values in Graphs and Summary Tables—If checked, displays the minimum values in the graph output mode summary tables and chart legends. This option is not enabled by default.
  - Show Avg Values in Graphs and Summary Tables—If checked (default), displays the average values in the graph output mode summary tables and chart legends.
  - Show Max Values in Graphs and Summary Tables—If checked (default), displays the maximum values in the graph output mode summary tables and chart legends.
  - Show Total Values in Graphs and Summary Tables—If checked (default), displays the total values in the graph output mode summary tables and chart legends. This option is not enabled by default.
  - Show Current Values in Graphs and Summary Tables—If checked (default), displays the current values in the graph output mode summary tables and chart legends.
  - Override Report Definitions—If checked, overrides report definitions that have been set up at the individual report level and assigns the report definitions defined in the Reports Status window. For information, see Enabling and Disabling Reports.
  - Show Values with K/KB, M/MB, and G/GB—If checked (default), appends kilobyte, megabyte, and gigabyte data with one of the following: K or KB, M or MB, G or GB.
  - Display Device Alarm Severity Icon—By default, Prime Performance Manager displays the alarm severity icon for the device's highest alarm. Use this option to turn that feature off.
  - Auto Expand Report Summary Tables—If checked (default), 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.
  - Display End of Time Period in Timestamps—If selected, changes the timestamp shown in graph and table reports to the end of the report interval. By default, graph and table reports display the start time for all time intervals. For example, in an hourly report, the polling time is 6H.00M.00S to 7H.00M.00S. By default, reports display the start time, which is 6H:00M:00S. If this option is enabled, reports will display the report interval end time. In the hourly interval example, this would be 6H:59M:59S.
  - Disable Dashboards—If enabled, hides the Prime Performance Manager dashboards from the reports navigation tree. Dashboards are enabled by default. Disabling them might be useful if you do not use them.
  - Number of Digits of Precision After Decimal—Specifies the level of precision for numeric values in reports. For example, if set to 2 (default), reports will display a numeric as *...nnnnn.nn*. If set to three, the numeric is displayed as *...nnnnn.nnn*. The level of decimal precision is also controlled by the decimalPrecision report element. Prime Performance Manager displays the highest level set either in User Preferences or by the decimalPrecision element. For information about the decimalPrecision element, see the *Cisco Prime Performance Manager 1.3 Integration Developer Guide*.

  - Maximum Number of Data Series Per Report—Allows you to specify the number of items displayed in graph output mode tables and charts. This number cannot be higher than the number specified in the Maximum Top XX Entries specified on the System Configuration tab. The default is 10. For information about system configuration parameters, see Changing System Configuration Settings, page 3-11.

- Graph Settings—Change display options in report, dashboard, and view graphs:
  - Show Hover Info—Turns hover information on (default) or off. Hover information is the device details that appear when you move your cursor over a device link.
  - Show Vertical Bar Over Data Series—Turns the vertical bar displayed in charts on (default) or off. The vertical bar helps you see data points through all data items.
  - Show One Graph Column Per Report—Allows you to display one graph per screen column instead of the default two columns. This option is not enabled by default.
  - Show Vertical Graph Grid—Allows you to display vertical and horizontal lines in charts. By default, only horizontal lines are displayed in charts. This option is not enabled by default.
  - Enable Graph Time Span Bar—Displays the full screen graph adjustable time span bar (see Figure 7-5 on page 7-12) on all report graphs including graphs in views and dashboards. The time span bar allows you to bring period of time within the report period into higher focus on the chart. This option is not enabled by default.
  - Show Graph as Default Output Mode in Dashboards/Stargraphs—Makes graph output the default for dashboards and star graphs. This option is not enabled by default.
  - Enable Legends by Default—Enables legend display for all graphs.
  - Default Graph Title/Date Font Size (Pixels)—Allows you to change the graph title and font size in reports. The default is 12 pixels. The range is 12 to 18 pixels.
  - Default Graph Height (Pixels)—Allows you to change the height of graphs in reports. The default is 300 pixels. The range is 250 to 750 pixels.
  - Margins—Allows you to set the width of the graph margin: No Margins, Narrow Margins, or Wide Margins.

Step 3 After you complete your changes, return to the previous Prime Performance Manager window.

Step 4 To view the new settings, click **Reload Report** on the report toolbar (if a report is displayed), or click **Reload Page** on the main toolbar at the top of the Prime Performance Manager window.

Changing System Configuration Settings

In addition to user preferences (see Changing User Preferences, page 3-7), system administrators can change a number of system settings that control disk space monitoring and warnings, the number of days to archive message logs, maximum number of Top XX entries, as well as HTML page and table sizes. These settings apply to all users. You must be a System Administrator user to change them.

To change system configuration settings:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **System Settings**.

The System Configuration tab is displayed.

Step 3 Modify the following, as needed:

- Disk Space Monitor Checking—If enabled, the Prime Performance Manager installed directories disk space monitor script runs every ten minutes to check the disk space. Alarms are raised when disk space reaches the thresholds defined in the next to parameters.
- Warning Disk Space Remaining—Defines the disk space threshold when a warning alarm is generated, and disk cleanup begins. 30 MB is the default.
- Critical Disk Space Remaining—Defines the disk space threshold when a critical alarm is generated, and disk cleanup begins. 29 MB is the default.

Note Disk space monitoring and thresholds can also be set with the ppm diskmonitor command. For information, see ppm diskmonitor, page B-22.

- Maximum Days for Message Log Archives —Sets the maximum number of days to archive message logs. 31 days is the default. You can also set the maximum using the ppm msglogage command. For information, see ppm msglogage, page B-43.
- Maximum Entries for Top XX Output—Sets the maximum number of entries in Top XX reports. 10 is the default. The range is 5-20. You can also set the maximum using the ppm topxxsize command. For information, see ppm topxxsize, page B-77.

Note Users can set their own preference for this item in User Preferences. However, their preference cannot be greater than the value entered here. For information about user preferences, see Changing User Preferences, page 3-7.

- Maximum Rows for HTML Pages—Sets the maximum number of rows for Prime Performance Manager HTML web output; for example, statistics reports, status change messages, or SNMP trap messages. The valid range is one row to an unlimited number of rows. The default value is 100 rows. The range is 1-5000. You can also set the maximum using the ppm maxhtmlrows command. For information, see ppm maxhtmlrows, page B-39.
- Maximum Rows for Table Pages—Sets the maximum browser page size for table reports. The default value is 100 is 800. The range is 1-5000. You can also set the maximum using the ppm maxpagesize command. For information, see ppm maxpagesize, page B-40.
- Maximum Simultaneous Report Queries—Sets the maximum number of simultaneous report queries. The valid range is 1-50. 0 disables function so no maximum is set. You can also set the maximum using the ppm maxrepqueries command. For information, see ppm maxrepqueries, page B-40.
- Interface Name Format—Defines the format for displaying interface names in the Prime Performance Manager GUI:
  - Alias—The interface alias is displayed.
  - Description—The interface description is displayed.
  - Both—Both the interface alias and description are displayed.

  You can also set this parameter using the ppm ifnameformat command. For information, see ppm ifnameformat, page B-30.

Step 4 After you complete your changes, return to the previous Prime Performance Manager window.

Step 5 To view the new settings, click **Reload Report** on the report toolbar (if a report is displayed), or click **Reload Page** on the main toolbar at the top of the Prime Performance Manager window.

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.

Adding and Removing Properties from Property Views

Prime Performance Manager displays many properties and attributes in tables, including Devices, Alarms by Device, SNMP Timeout Alarms, and others. Most tables have properties that are not displayed by default. To display hidden properties, or to hide ones that are displayed:

Step 1 Right-click a property table header.

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

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

If many properties are available, for example in the Devices table, scroll the Prime Performance Manager window to display the Apply button.

Note If you do not click Apply, the change will not appear in the table.

Sorting Tables

You can easily sort any Prime Performance Manager table display, for example, Devices, Alarms by Device, and many others.

To sort a property table, 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 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).

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 user-defined device names. For more information, see Changing User Preferences, page 3-7.

Displaying Prime Performance Manager Information

You can display information about the Prime Performance Manager by clicking the **About** item at the top right corner of the Prime Performance Manager window. The following information is displayed:

- License Type—The Prime Performance Manager license type.
- Build Date—The Prime Performance Manager build date.
- Build Version, Patch Level—The build version and patch level. For example, 1.3.0.6, 0 indicates a 1.3 build with no patches installed.
- Release Notes—A link that displays the Prime Performance Manager Release Notes on Cisco.com.
- PPM on Cisco.com—A link to the Prime Performance Manager product page on Cisco.com.
- Network Management Products—A link to the Cisco Network Management product page.
- Engineering_Software_Updates—A link to the Prime Performance Manager FTP download page where software patches can be downloaded. You must be a registered user to access this site.

CHAPTER 4

Prime Central Integration

Cisco Prime Central is the presentation tier for the Cisco Prime Carrier Management suite, which includes Cisco Prime Performance Manager, Cisco Prime Network, Cisco Prime Optical, and other domain managers. Prime Central provides a number of centralized features and functions including:

- A single point of access (single sign-on) to the Prime Central domain managers.
- Central access to the experience lifecycle tasks.
- Support for LDAP, TACACS+, and RADIUS authentication plug-ins.
- Virtualization on VMware configurations.
- Common user management with role-based access control (RBAC).
- Grouping-to-domain manager mapping.
- Common adopted installation framework.
- Database and application monitoring.
- Common physical inventory management

Integrating Prime Performance Manager with Prime Central involves the following general tasks:

- Running the Prime Central integration (required)
- Creating users (required)
- Importing Prime Network credentials (optional)
- Importing trap destinations (optional)

Procedures are provided in the following topics:

- Integrating Prime Performance Manager with Prime Central, page 4-1
- Prime Central Integration Considerations and Next Steps, page 4-5

Integrating Prime Performance Manager with Prime Central

Prime Performance Manager can be integrated with Prime Central during Prime Performance Manager installation. If you did not integrate Prime Central with Prime Performance Manager during installation, you can run the integration from the Prime Performance Manager GUI or CLI.

Before You Begin

- Verify that Prime Central is installed and running on a server to which you have access.

- Verify that you have the Prime Central server database IP address or hostname, port, username, system ID, and password.
- Because you must restart the Prime Central integration layer and Prime Performance Manager after the integration, make sure you perform the procedure at a time when restarts can occur.

Note Only one Prime Performance Manager gateway can be integrated with Prime Central.

Note After you integrate Prime Performance Manager with Prime Central, all logins and user management operations are performed from Prime Central. The Prime Performance Manager User Management window is visible with reduced functionality. For information about logins and user management, see the *Cisco Prime Central 1.1 User Guide*.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Prime Central Integration**.

Step 3 In the Prime Central Integration window, enter the following:

- Database Host—Enter the Prime Central database hostname or IP address.
- Database SID—Enter the Prime Central database service name, which is primedb by default.
- Database User—Enter the Prime Central database username, which is primedba by default.
- Database Password—Enter the Prime Central database user password; for example, Test456!
- Database Port—Enter the Prime Central database port number, which is 1521 by default.

Step 4 Click the **Prime Central Integration Setup** tool on the System Prime Central Integration window toolbar.

If the integration information you entered is valid, you are prompted to restart the Prime Central integration layer. If not, an error is returned.

Step 5 Restart Prime Performance Manager gateways and unit(s) by executing the **ppm restart** command. For information, see Restarting Gateways and Units, page 2-4.

Step 6 Log into the Prime Central server and stop the Prime Central Integration Layer:

```
itgctl stop
```

Step 7 Wait two minutes, then start the Prime Central integration layer:

```
itgctl start
```

Step 8 Verify the integration,

a. Log into Prime Central. (For Prime Central login procedures, see the*Cisco Prime Central 1.1 User Guide*.)

b. From the Prime Central Administration menu, choose **Suite Monitoring**.

c. Verify that Prime Performance Manager is listed under Applications and has an Up state.

If Prime Performance Manager is not shown, complete the steps in “Prime Performance Manager Does not Appear in Prime Central” in Table 4-1 on page 4-4.

If Prime Performance Manager is shown, but its state is Down, complete the steps in“Prime Performance Manager is Displayed in Prime Central with a Down State” in Table 4-1 on page 4-4.

d. From the Prime Central Assure menu, verify that Prime Performance Manager is listed. If not, complete the steps in "Prime Performance Manager Menu Option is Missing" in Table 4-1 on page 4-4.

e. From the Prime Central Assure menu, choose Prime Performance Manager. Prime Performance Manager should be cross launched. If not, complete the steps in "Cannot Launch Prime Performance Manager from Prime Central" in Table 4-1 on page 4-4.

Step 9 If remote units are connected to the gateway, complete the "Enable SSL on Remote Units" procedure on page 6-4 to enable SSL on the remote units.

Step 10 After Prime Performance Manager is integrated with Prime Central, use the Prime Central portal to create new users, even if they already existed in Prime Performance Manager. See the *Cisco Prime Central 1.1 User Guide* for procedures.

Note When you create a user who previously existed in Prime Performance Manager, Prime Central advises you that the user already exists in Prime Performance Manager, retrieves the user properties, and applies them to the new Prime Central user. For more information, see Managing Users and User Security, page 6-12.

To integrate Prime Performance Manager with Prime Central using the Prime Performance Manager CLI:

Step 1 Log into the Prime Performance Manager gateway server as a System Administrator user.

Step 2 Enter the following command:

```
ppm primecentralintegration
```

Step 3 At the prompts, enter the Prime Central server information:

- Database Hose—Enter the Prime Central database server IP address or hostname.
- Database SID [primedb]—Enter the Prime Central database service name, which is primedb by default.
- Database User [primedba]—Enter the Prime Central database username, which is primedba by default.
- Database Password [*****]—Enter the Prime Central database user password; for example, Test456!
- Database Port [1521]—Enter the Prime Central database port number, which is 1521 by default.

Allow a few minutes for the integration layer restart to complete, then continue with the next step.

Step 4 Restart the Prime Performance Manager gateway and unit(s). See Restarting Gateways and Units, page 2-4.

Step 5 Verify the integration:

a. Log into Prime Central. (For Prime Central login procedures, see the*Cisco Prime Central 1.1 User Guide*.)

b. From the Prime Central Administration menu, choose **Suite Monitoring**.

c. Verify that Prime Performance Manager is listed under Applications and has an Up state.

If Prime Performance Manager is not shown, complete the steps in "Prime Performance Manager Does not Appear in Prime Central" in Table 4-1 on page 4-4.

If Prime Performance Manager is shown, but its state is Down, complete the steps in"Prime Performance Manager is Displayed in Prime Central with a Down State" in Table 4-1 on page 4-4.

d. From the Prime Central Assure menu, verify that Prime Performance Manager is listed. If not, complete the steps in "Prime Performance Manager Menu Option is Missing" in Table 4-1 on page 4-4.

e. From the Prime Central Assure menu, choose Prime Performance Manager. Prime Performance Manager should be cross launched. If not, complete the steps in "Cannot Launch Prime Performance Manager from Prime Central" in Table 4-1.

Step 6 If remote units are connected to the gateway, complete the "Enable SSL on Remote Units" procedure on page 6-4 to enable SSL on the remote units.

Step 7 After Prime Performance Manager is integrated with Prime Central, use the Prime Central portal to create new users, even if they already existed in Prime Performance Manager. See the *Cisco Prime Central 1.1 User Guide* for procedures.

Table 4-1 lists Prime Central integration issues and resolutions.

Table 4-1 Prime Central Integration Issues and Resolutions

Problem	Resolution
Prime Performance Manager Does not Appear in Prime Central	1. Log into the Prime Performance Manager gateway as the root user. (See Root User Login, page 2-1.) 2. Display the DMIntegrator log: `/opt/CSCOppm-gw/prime-integrator/DMIntegrator.log` 3. In the log, check to see: – Whether Prime Performance Manager registration status, either succeeded or failed. – If registration was successful, whether the Prime Central database server hostname or IP address located in the log [SERVER:] property is correct. 4. If the Prime Central Suite Monitoring table contains a Prime Performance Manager instance, select the row and press the **Delete**. 5. Wait a few minutes for Prime Central to delete the Prime Performance Manager instance, then complete the "Integrating Prime Performance Manager with Prime Central" procedure on page 4-1, making sure to enter the correct Prime Central database server information. 6. If this does not resolve the problem, call Cisco TAC.

Table 4-1 Prime Central Integration Issues and Resolutions (continued)

Problem	Resolution

Prime Performance Manager is Displayed in Prime Central with a Down State	1. Restart the Prime Performance Manager gateway and all remote units that are connected to it. See the "Restarting Gateways and Units" procedure on page 2-4.
	2. Check the Prime Performance Manager operational status. See the "Displaying Gateway and Unit Status" procedure on page 2-6.
	3. Log into the Prime Central workstation as the primeusr UNIX OS user.
	4. Stop the Prime Central Integration Layer by entering:
	`itgctl stop`
	5. Wait around two minutes, then start the integration layer:
	`itgctl start`
	6. After a few minutes, check to see if the Prime Performance Manager state changes to Up in the Suite Monitoring > Applications window.
	7. If this does not resolve the problem, call Cisco TAC.

Prime Performance Manager Menu Option is Missing	1. From the Prime Central Administration menu, choose **Users**. 2. Verify that the logged-in user has Prime Performance Manager in the domain manager access privileges. 3. If not, select the user, click **Edit** and add Prime Performance Manager to the user's domain privileges. For detailed procedures, see "Edit a User" in the *Cisco Prime Central 1.1 User Guide*. 4. Log out and then log back in
Cannot Launch Prime Performance Manager from Prime Central	1. Verify that the Prime Performance Manager gateway is up and running. See the "Displaying Gateway and Unit Status" procedure on page 2-6. All services should be running. 2. If not, restart the gateway. See the "Displaying Gateway and Unit Status" procedure on page 2-6. 3. If the problem persists, contact the Cisco TAC.

Prime Central Integration Considerations and Next Steps

After you integrate Prime Performance Manager with Prime Central, keep in mind that all user logins and management—adding, editing, removing—are performed from Prime Central. See the *Cisco Prime Central 1.1 User Guide* for login and user management procedures, as well as general information about using Prime Performance Manager in the Cisco IP NGN Suite.

When Prime Performance Manager is integrated with Prime Central, Prime Fault Management is imported as a trap destination (if it exists.) If you want to send traps to Prime Network instead, you can use the ppm setpctrapdestination command to send traps to Prime Network instead of Prime Fault Management.

After you integrate Prime Performance Manager with Prime Central, you can launch Prime Performance Manager from the Prime Central menu, selected devices and interfaces in the Prime Central inventory view, and from selected alarms in the Fault Management.

Following integration, you will likely want to perform other procedures, for example, import devices from Cisco Prime Network and begin generating reports.

Table 4-2 Post Integration Commands and Procedures

Command or Procedure	Description
ppm primecentralintegration remove	Removes Prime Performance Manager from Prime Central and returns it to a standalone domain manager.
ppm setpctrapdestination	Changes Prime Performance Manager trap destination from Prime Fault Management to Prime Network. See ppm inventoryimport, page B-32, for command options.
ppm inventoryimport	Imports the device inventory from Prime Network. See ppm inventoryimport, page B-32, for command options. To import devices using the Prime Performance Manager GUI, see Importing Devices From Prime Network, page 5-2.
ppm crosslaunch	Adds cross-launch capability to Cisco Prime Network. See ppm inventoryimport, page B-32, for command options. To install cross-launch capability on Prime Network using the Prime Performance Manager GUI, see Enabling Prime Network Cross-Launching, page 5-4.

CHAPTER 5

Discovering Network Devices

To generate reports, Prime Performance Manager must discover your network devices. This is accomplished by importing the device inventory from Cisco Prime Network, running device discovery from Prime Performance Manager, or a combination of both. Before this can occur, the SNMP credentials to allow Prime Performance Manager to connect to devices must be created. (For Y.1371 SLA and Ethernet flow point QoS reports, Telnet or SSH credentials are required.)

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

- Device Discovery Requirements, page 5-1
- Importing Devices From Prime Network, page 5-2
- Prime Performance Manager Device Discovery, page 5-4

Device Discovery Requirements

Before you begin device discovery, review the devices Prime Performance Manager supports at:

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

In addition, the Prime Performance Manager Devices Readme lists the known devices and software versions that have been used by customers and in 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 access the Devices Readme, choose **Readmes and Commands** from the Help menu, then choose **Devices Readme**.

To produce network performance reports, Prime Performance Manager accesses the devices, determines the device type and installed hardware. It checks for provisioned functions and technologies and, based on the assigned polling frequencies, 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. This can be done from the Prime Performance Manager GUI or by running the ppm inventoryimport command. (For information about this command, see ppm inventoryimport, page B-32.)
- Run device discovery from Prime Performance Manager. This can be done from the Prime Performance Manager GUI or by running the ppm discover command. (For information about this command, see ppm discover, page B-22.)

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, authentication protocol, authentication password, privacy protocol, and privacy password, depending on the device configuration.
- If Y.1731 SLA or Ethernet flow point reports are enabled, Telnet or SSH credentials are required as well. The number of credentials and their content depend on the device configuration.

Note If you are running only CSV-based reports, only the device IP address or hostname is required.

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 credentials to Prime Performance Manager before you run the device discovery.

Discovering Gateways and Units

Reports can be generated for Prime Performance Manager gateways and units to help you monitor the gateway and unit server health and performance. To enable Prime Performance Manager gateway and unit reports, you must:

- Enable SNMP on the gateway and unit servers.
- Add the gateway and unit SNMP credentials. See Adding SNMP Credentials, page 5-5.
- Run discovery from Prime Performance Manager to acquire the gateways and units. See Running Device Discovery from Prime Performance Manager, page 5-10.

If you are importing devices from Prime Network, you have two options for adding the Prime Performance Manager gateways and units:

- To import Prime Network devices with strict synchronization enabled, acquire the gateways and unit in the Prime Network inventory before you perform the import. (The strict synchronization import option restricts the devices managed by Prime Performance Manager to those imported from Prime Network.)
- When importing the devices, do not enable strict synchronization. After the devices are imported, run device discovery from Prime Performance Manager to acquire the gateways and units.

Importing Devices From Prime Network

To import a Prime Network device inventory, Prime Performance Manager connects to the Prime Network gateway and retrieves the Prime Network device IP addresses, SNMP, Telnet, or SSH credentials, and HTTP/s for vCenter.. All Prime Network devices are retrieved except those whose VNEs:

- Are in Maintenance investigation state.
- Are ICMP or cloud VNEs.
- VNEs whose admin status is down.

Prime Performance Manager then connects to the devices and probes them for supported polling parameters. 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 adds those devices. If a Prime Network device VNE goes into Maintenance state, Prime Performance Manager changes the device to unmanaged and stops polling. When the VNE state changes, Prime Performance Manager changes the device state back to managed and begins polling.

Strict Synchronization

Strict synchronization is a Prime Network import option that restricts Prime Performance Manager to Prime Network devices only. If strict synchronization is enabled, 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 using the Prime Performance Manager GUI. This procedure requires a Level 5 (administrator) user level.

Note For information on importing Prime Network devices using the CLI, see ppm inventoryimport, page B-32.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Prime Network Integration**.

Step 3 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.
- Unsecured Port—Indicates the port entered in the Port field is an unsecure port intended for BQL debugging.
- 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 have not been added to Prime Network first, and certain functionality is disabled, including the Network menu Discovery option and the ability to edit SNMP, Telnet, and SSH entries.

Step 4 From the Prime Network Integration toolbar, click the **Import Inventory** tool.

The Prime Network device inventory import proceeds.

Note If Prime Performance Manager finds duplicate device custom names, an error is issued.

Step 5 After it completes, from the Network menu, choose **Devices** to review the devices that were added. For information about the displayed device properties, see **Displaying Network-Level Device Properties, page 8-2.**

If you want to enable Prime Performance Manager cross-launches from Prime Network, complete the "Enabling Prime Network Cross-Launching" procedure on page 5-4.

Step 6 To display information about the last Prime Network inventory synchronization, on the Administration Prime Network Integration window toolbar, click **Last Inventory Import Info**.

The date and time and status of the last inventory import is displayed.

Enabling Prime Network Cross-Launching

After you import the Prime Network device inventory, you can enable cross launching so that Prime Network users can launch Prime Performance Manager from Prime Network Vision.

To enable cross-launches from Prime Network:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Prime Network Integration**.

Step 3 From the Prime Network toolbar, click the **Install Cross Launch** tool.

Note If you change the Prime Performance Manager gateway JSP port, server name, or SSL status, you must enable Prime Network cross launching again.

Prime Performance Manager Device Discovery

Importing devices from Prime Network is the most common method for adding devices to Prime Performance Manager, particularly if Prime Performance Manager is integrated with the Prime suite. (For information, see Importing Devices From Prime Network, page 5-2.)

You can also run device discovery from Prime Performance Manager. Use this discovery method when:

- You are not running Prime Network or do not wish to enable reports on Prime Network devices.
- You imported Prime Network devices but want to add devices that are not in the Prime Network inventory.

Before you run device discovery from Prime Performance Manager, you must add the device credentials. Credential management and device discovery are covered in the following topics:

- Managing Device Credentials, page 5-5.
- Running Device Discovery from Prime Performance Manager, page 5-10

Managing Device Credentials

You can run device discovery from Prime Performance Manager if you are not importing devices from Prime Network or wish to add devices that are not in the Prime Network inventory. Before you can do this, however, you must add the device credentials (or edit the credentials through the Edit Device Credentials dialog) so Prime Performance Manager can communicate with the device.

SNMP is the primary protocol used by Prime Performance Manager for device communication for nearly all Prime Performance Manager reports. For some reports, such as SLS 1731 reports, other communication methods are used, including Telnet and SSH. Adding and managing device credentials are covered in the following topics:

- Adding SNMP Credentials, page 5-5
- Editing SNMP Credentials, page 5-6
- Deleting SNMP Credentials, page 5-6
- Adding Telnet and SSH Credentials, page 5-7
- Deleting Telnet/SSH Credentials, page 5-9
- Telnet and SSH Credential Notes, page 5-9
- Adding SNMP Credentials, page 5-5

Adding SNMP Credentials

Complete the following steps to add the SNMP credentials to communicate with network devices discovered by Prime Performance Manager. This procedure is required if you run device discovery from Prime Performance Manager. You do not need to perform it if you imported devices from Prime Network and do not wish to add devices not in the Prime Network inventory.

Note To add SNMP credentials using the CLI, see ppm addsnmpcomm, page B-6.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **SNMP Editor**.

Step 3 From the SNMP Editor toolbar, click the **Add a New SNMP Entry** tool.

Step 4 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).
- Authentication Protocol (v3)—Enter the authentication protocol (SNMP v3):
  - md5—Uses the Hash-based Message Authentication Code (HMAC) MD5 algorithm for authentication
  - sha—Uses the HMAC SHA algorithm for authentication
- Authentication Password (v3)—Enter the authentication password (SNMP v3),
- Privacy Protocol (v3)—Enter the privacy protocol (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 Password (v3)—Enter the privacy password (SNMP v3).

Step 5 Click **OK**.

Step 6 Repeat Steps 3–5 until all SNMP credentials are added.

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

Editing SNMP Credentials

SNMP credentials are required for communication with devices that are discovered by Prime Performance Manager. If you need to edit the SNMP credentials:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **SNMP Editor**.

Step 3 In the SNMP table, edit any of the following SNMP parameters. See Adding SNMP Credentials, page 5-5, for parameter descriptions.

- IP Address Range or Hostname
- Read Community
- Username (v3)
- Authentication Protocol (v3):
  - md5
  - sha
- Authentication Password (v3)
- Privacy Protocol(v3):
  - 3des
  - des
  - aes128
- Privacy Password (v3)

Step 4 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 a System Administrator user.

Step 2 From the Network menu, choose **SNMP Editor**.

Step 3 Select the SNMP credential table row(s) that you want to remove by checking the box(es) on the far left column.

Step 4 On the Network SNMP Editor toolbar, click **Delete Selected SNMP Entries**.

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

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. If you plan to run Y.1731 reports, you must add the Telnet or SSH device credentials to Prime Performance Manager.

To add the Telnet or SSH credentials:

Step 1 Log into the Prime Performance Manager GUI as the administrator user.

Step 2 From the Network menu, choose **Telnet/SSH Editor**.

Step 3 In the Device Credentials Editor toolbar, click the **Add a New Device Credential for a Device** tool.

Step 4 In the Add a Credential dialog box, enter the following:

- User Name—Enter the device login username.
- Password—Enter the password for the login user.
- Enable User Name—Enter the privileged username.
- Enable Password—Enter the privileged user password.
- Connection 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.
  - vCenter_HTTPs
  - vCenter_HTTP
  - ESXi_HTTPs
  - ESXi_HTTP

  Note When you define the telnet/ssh credential for vCenter and ESXi devices, make sure the user account you use has the session privileged. For information, see Hypervisor Discovery Requirements, page 5-14.

  - XEN_TLS
  - KVM_TLS

Note XEN_TLS and KVM_TLS have discovery requirements. See XEN and KVM TLS Discovery Requirements, page 5-14

  - HyperV_HTTPs
  - HyperV_HTTP
- 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 5 Click **OK**.

The new credential is added to the Telnet/SSH credential table.

Step 6 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 7 In the Testing Credentials window, click **Close**.

Step 8 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.

Note Verify the Telnet/SSH credential has permission to execute the CLI terminal length 0 and terminal width 0, or Prime Performance Manager might not be able to collect data from the CLI.

After you add the Telnet and SSH credentials, you might want to perform the following tasks:

- Run device discovery. See Chapter 5, "Discovering Network Devices," for procedures.
- Enable the Y.1731 and Ethernet Flow Point reports: from the Performance menu, choose **Reports**, click the **Report Status** tab, enable the **IP SLA: Y.1731** and **IP QoS: Transport and Availability** reports. For more information, see Chapter 7, "Managing Reports, Dashboards, and Views."

Deleting Telnet/SSH Credentials

Complete the following steps to delete the Telnet/SSH credentials from Prime Performance Manager.

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Telnet/SSH Editor**.

Step 3 Select the Telnet/SSH credential table row(s) that you want to remove by checking the box(es) on the far left column.

Step 4 On the Network Telnet/SSH Editor toolbar, click **Delete Selected Telnet/SSH Entries**.

Step 5 When finished, on the Telnet/SSH Editor toolbar, click **Save All Telnet/SSH Entries**.

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. vCenter_HTTP/s is also imported from the Prime Network UCS cluster VNE. 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 setpctrapdestination, page B-61.
  - ppm deletecreds—Deletes the Telnet or SSH credential from the device. See ppm deletecreds, page B-19.

- ppm xmlpoll—Retrieves the device XML output. See ppm xmlpoll, page B-81.

Adding Credentials for Cisco Carrier Packet Transport Devices

Adding credentials for Cisco Carrier Packet Transport (CPT) devices requires a few additional steps because the CPT chassis has a control card and two or more line cards. One line card runs the Cisco IOS image. The CPT control card controls access to the line cards.

To Prime Performance Manager, the control card and the line card running the Cisco IOS image appear as a separate devices that use the same IP address for management. Performance statistics reside on both the control card and the line card running the Cisco IOS image. To gather both sets of statistics using the same IP address, you must complete the following steps so that Prime Performance Manager can reach the line card with the Cisco IOS image through the control card (a process called SNMP relay):

Step 1 Set up a community string for the CPT 200 chassis and card. Card discovery utilizes SNMP relay, so one community string is used for both the chassis and the card. The community string is specified as follows:

```
ppm addsnmpcomm -i [ ipaddress ]  -c public
```

Step 2 Set up Telnet credentials for the chassis and card. This is a single row specified as follows:

```
ppm addcreds -i [ ipaddress ] -u CISCO15 -r Telnet -o 23
```

The credentials database is keyed by IP address, so only a single entry can exist. Chassis access is controlled by this entry. Access to the card uses the entry credentials, but Prime Performance Manager dynamically determines the port. The port is generated internally as '2000 + slot number'.

Step 3 Run device discovery to discover the CPT chassis and card using either the GUI (see Running Device Discovery from Prime Performance Manager, page 5-10), or the command line:

```
ppm discover [ipaddress ipaddress@2
```

The '@2' tells Prime Performance Manager the card is reachable through SNMP relay using the specified IP address. The device name is suffixed with the slot#. If the IP address is resolvable to a device name, the name will have the slot number appended accordingly. For example:

```
ipaddress@2
devicename@2
```

Step 4 Verify that the CPT devices are discovered in the GUI and device details are displayed including state, IOS version, description, device type, and other details.

Step 5 Verify that reports are generated based on the device capabilities.

Running Device Discovery from Prime Performance Manager

Device discovery is accomplished either by importing devices from Prime Network (see Importing Devices From Prime Network, page 5-2), or by running device discovery from Prime Performance Manager.

To run device discovery from Prime Performance Manager you enter IP addresses, address ranges, subnets, DNS hostnames, then launch discovery. The collection of addresses used for device discovery can be saved as device seed files for future use.

Before you begin device discovery, you will need:

- A list of IP addresses, address ranges, and subnets that you want Prime Performance Manager to use for discovery.
- A device seed file containing the IP addresses, address ranges, and subnets that you want Prime Performance Manager to use for discovery. If you are running discovery for the first time, you will enter the IP addresses manually, after which you can create the seed file for later use.

To run discovery from Prime Performance Manager:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Discovery**.

The Discover Network window appears. Window areas include:

- Discovery Seeds—Displays the seed files containing the address information you want Prime Performance Manager to use for device discovery.
- SNMP Parameters—The SNMP parameters that will be used to connect to devices. See Adding SNMP Credentials, page 5-5.
- Telnet/SSH Parameters—The Telnet/SSH parameters that will be used to connect to devices if you will run Y.1731 or Ethernet flow point reports. See Adding Telnet and SSH Credentials, page 5-7.

Step 3 Load a device seed file:

To load a seed file from saved files:

a. From the Discover Network toolbar, click **Load Seeds**.

The Load File dialog box displays the following information and options:

- Folder icon—Click this icon to go up one folder in the directory structure.
- Type—Indicates whether the item in the table is a file or a folder.
- Name—Seed file or folder name.
- Last Modified—Date and time the seed file or folder was last modified.
- Size (bytes)—Size of the seed file or folder, in bytes.

b. Choose a seed file. To make it your preferred startup file, click **Make This My Preferred Startup**.

c. If needed, you can:

- Modify file names by entering the new name in the Name column
- Delete files by selecting them and clicking **Delete**.

d. Click **OK**.

Prime Performance Manager saves any changes you made, closes the dialog box, and returns to the Discovery Network window. Device address information from the seed file is displayed in the Seed Devices File pane. SNMP and Telnet/SSH parameters for each seed device is shown in the SNMP and Telnet/SSH areas.

To create a seed file:

a. Enter an IP address, IP address range, IP address/subnet, CIDR subnet, or DNS hostname in the IP address field. Example inputs include:

- IP Address: 111.222.333.555
- Address Range: 111.222.333.555-800
- CIDR: 111.222.333.555/24 or 111.222.333.555/255.255.255.0

- DNS Hostname: abc_router

b. Click **Add**. The device address or range is added to the seed file.

c. Repeat Steps a and b until you have all device address information added to the file. (Should you wish to remove the address or range, select it and click **Delete**.

Step 4 After all devices are added to the seed file, click **Save Seeds** from the Discover Network toolbar.

Step 5 In the Save File dialog box:

a. If you want to create a new directory for the file, click **New Folder**, enter the folder name, then click **OK**. Alternatively, click **Go Up One Folder** to navigate to a directory above the current one.

b. Enter the file name, then click **OK**. The new file is saved and automatically loaded into the Seed Devices File pane.

Step 6 When you are ready to start device discovery, click **Discover Network**.

- The Discover Network tool changes to Stop Discovery.
- A Discovery In Progress message appears in the title bar of all Prime Performance Manager client windows.

The Network Devices summary window appears. (For Network Devices parameter descriptions, see Table 8-2 on page 8-2.) Devices requested for discovery will display the status, Waiting and the status reason, For Unit. As the unit completes the initial device discovery, the status changes to the detected device status, which is usually Active with status reason, None.

The time required to complete device discovery depends on multiple factors including number of devices, device types, the number of enabled reports, and network latency.

Step 7 To view the devices that Prime Performance Manager discovered, from the Navigation menu, choose **Devices**. (See Displaying Network-Level Device Information, page 8-1 for information about displayed device parameters.) By default, discovered devices are 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.

Step 8 To view information about the last discovery, click **Last Discovery Info** on the Network Discovery toolbar. The date and time of the last discovery and discovery status is displayed.

Data Center Device Support

Prime Performance Manager supports the following devices used for data centers.

- Cisco ASA 5500
- Cisco Nexus 7000 Series
- Cisco Nexus 5000 Series
- Cisco Nexus 4000 Series
- Cisco Nexus 3000 Series

- Cisco Nexus 2000 Series
- Cisco ACE 20/304710
- Cisco Nexus 1000v
- Cisco Nexus 1010
- Cisco UCS FIC 6100
- Cisco UCS FIC 6200
- Cisco UCS 5100
- Cisco UCS 2100 (IO Module)
- Cisco UCS B-series
- Cisco UCS C-series
- Cisco MDS 9100
- Cisco MDS 9200
- FWSM
- HyperVisor
- VMWare

Some data center devices or device modes require you to perform special steps to enable Prime Performance Manager support. These are described in the following topics:

- Discovering Nexus Switches in VDC Mode, page 5-13

Discovering Nexus Switches in VDC Mode

The Cisco Nexus operating system, Cisco NX-OS, supports virtual device contexts (VDCs). VDCs allow Cisco Nexus 7000 data center switches to be virtualized at the device level. Each configured VDC presents itself as a unique device to connected users within the framework of that physical switch. The VDC runs as a separate logical entity within the switch, maintaining its own unique set of running software processes, having its own configuration, and being managed by a separate administrator. A Nexus can be configured with four VDCs. Each context appears as a device.

Prime Performance Manager polls the VDC separately. This means you must enter all VDC management IP adddresses and credentials, including SNMP and Telnet/SSH, into Prime Performance Manager so that Prime Performance Manager can poll the statistics and inventory data for the Data Center view.

To discover Nexus VDCs:

Step 1 Log into the Cisco Nexus switch as the administrator user. Refer to the Cisco Nexus user documentation for login procedures.

Step 2 Following instructions in the Cisco Nexus user documentation, create the VDCs under the default VDC instance, for example:

```
ppm7000a(config)# vdc ?
  <WORD>              Create a new vdc
```

Step 3 Allocate the interfaces to the VDCs under the default VDC instance, for example:

```
ppm7000a(config-vdc)# allocate interface ethernet 1/37-48
```

Step 4 Switch to the new VDC and initialize the VDC configuration following the Nexus wizard:

- admin username/password,
- snmp RO/RW credential,
- Mgmt 0 IP address (for Prime Performance Manager polling),
- Mgmt vrf route gateway, and so on

For example:

```
ppm7000a# switchto vdc ?
  ppm7000a  VDC number 1
  vdc2      VDC number 2
  vdc3      VDC number 3
  vdc4      VDC number 4
```

In the following Cisco Nexus VDC configuration example, the access VDC is managed through the 192.168.119.53 address. This address will be used as the seed during Prime Performance Manager device discovery.

```
telnet ppm70002
vdc Access id 2
  allocate interface Ethernet1/1-8
vdc Agg id 3
  allocate interface Ethernet1/9-16
vdc Core id 4
  allocate interface Ethernet1/17-24
switchto vdc access
config
vrf context management
  ip route 0.0.0.0/0 192.168.119.1
vlan 622
  name Management
username admin password 5 $1$rvdiuLA.$8j5arfEmxh1Bw7YtTNHCr/  role vdc-admin
snmp-server community SMFtest123 group vdc-operator
interface mgmt0
   ip address 192.168.119.53/25
```

Hypervisor Discovery Requirements

Prime Performance Manager can discover a variety of virtualized hypervisor devices including Hyper-V, Xen, KVM and EXSi. For VMWare hypervisors, Prime Performance Manager uses the virtualization API, libvirt. This API requires a user with a session privilege. In VMWare:

1. Create a role named "***".
2. Create a user on the Windows machine where VCenter is installed and assign that user the role, “Clone of read-only.”
3. Give the user the session privilege.

XEN and KVM TLS Discovery Requirements

XEN TLS and KVM TLS hypervisors require libvirtd 0.9.13 or above to be enabled on the hypervisor. For security, use TLS+SASL for authentication. More details can be found in libvirt website. For the Prime Performance Manager server, install library cyrus-sasl to support SASL authentication.

In addition to TLS elements, you must install some dependency libraries on the Prime Performance Manager server for hypervisor reports including libgcrypt, libintl and libiconv. For Solaris, make sure the 64 ELF libraries are used because 32 ELF is default library type.

CHAPTER 6

Managing Users and Security

Before you set up the Prime Performance Manager gateway and begin discovering and monitoring your network, you need to decide the user security levels, that is, which users will be allowed to which Prime Performance Manager functions.

Prime Performance Manager allows you to decide how users are authenticated, what actions they can perform, and which client IP addresses can access Prime Performance Manager gateways and units.

The following topics provide information about setting up user access and security, configuring user passwords, and managing Prime Performance Manager users:

- Setting Up User Access and Security, page 6-1
- Managing Users and User Security, page 6-12

Note If you integrate Prime Performance Manager with Cisco Prime Central, all user management functions are handled by Prime Central, and the user and security options are not displayed in Prime Performance Manager. After integration, users access all Cisco Prime domain managers, such as Prime Performance Manager, Prime Network, and others, using a single login. Information provided in these topics are useful, however, particularly user roles, which will be assigned in Prime Central. An understanding of user password configuration is also helpful. For more information about integrating Prime Performance Manager with Prime Central, see Chapter 4, "Prime Central Integration."

Setting Up User Access and Security

Enabling user access allows you to control what users can view and perform in Prime Performance Manager. User access provides multilevel, password-protected access to Prime Performance Manager functions. Five access roles are available, and you can assign these roles to users to allow or restrict their access to Prime Performance Manager features and functions.

Table 6-1 lists the user access task flow and topics providing the steps or additional information.

Table 6-1 Setting Up and Managing User Access and Security

User Access Task	For More Information
User and Security Setup Tasks	
Enable Secure Sockets Layer on gateways and units. This task is required.	Enabling SSL on Gateways and Units, page 6-2
Determine how users will be authenticated.	User Authentication, page 6-7

Table 6-1 Setting Up and Managing User Access and Security (continued)

User Access Task	For More Information
Configure user passwords.	Configuring User Passwords, page 6-9
Review secure password requirements.	Modifying the Password Policy, page 6-9
Review user roles.	User Security Levels, page 6-10
Enable user access.	Enabling Secure User Access, page 6-11
Disable user-based access.	Disabling Secure User Access, page 6-12
Add new users.	Add New Users, page 6-12
User and Security Management Tasks	
Edit user information.	Edit User Information, page 6-13
Define the reports users can access.	Edit User Reports, page 6-14
Change user passwords.	Change User Passwords, page 6-15
Edit user security settings.	Edit User Security Settings, page 6-16
Manually disable users and passwords.	Manually Disable Users and Passwords, page 6-17
Enable user accounts and passwords.	Enable User Accounts and Passwords Using the CLI, page 6-18
List currently defined users.	List Currently Defined Users, page 6-20
Display the system security log.	Display the System Security Log, page 6-21

Enabling SSL on Gateways and Units

To enable user access SSL must be enabled on Prime Performance Manager gateways and units. To enable SSL, you generate the SSL key and certificate for the gateway and each connected unit, then import corresponding keys and certificates to the gateway and units. In other words, 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 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:

- Enable SSL on a Gateway or Collocated Gateway and Unit, page 6-3
- Enable SSL on Remote Units, page 6-4

Enable 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.
- 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.
- 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 3 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 "Enable SSL on Remote Units" procedure on page 6-4. 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**

Note If you enabled Cisco Prime Network cross-launching before you enabled SSL, you must enable the cross launches again. For information, see Enabling Prime Network Cross-Launching, page 5-4)

Enable SSL on Remote Units

To enable SSL on remote units:

Step 1 Log into 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 Network Cross-Launching, page 5-4 procedure to ensure the cross-launch links to are updated.

Related Topics:

Export SSL Certificates, page 6-5

Display SSL Status, page 6-5

Disable SSL, page 6-6

Export 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.

Display SSL Status

To display SSL status:

- For gateways, enter:

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

- For units, enter:

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

Print SSL Certificates

To 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
  ```

Display SSL Key and Certificate

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

Disable SSL

Complete the following steps to disable and remove SSL keys and certificates from Prime Performance Manager gateways and units:

Step 1 Log into the gateway as the root or Prime Performance Manager administrator 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

User Authentication

After you implement user access for Prime Performance Manager, users must log into the system to access the Prime Performance Manager web interface and CLI commands. Security authentications include:

- Cisco Prime Central single signon (SSO) authentication. Prime Central SSO is enabled after you integrate Prime Performance Manager with Prime Network. For information, see Enabling Prime Network Cross-Launching, page 5-4.
- 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

Authentication Through PAM, TACACS+, and LDAP

Prime Performance Manager supports authentication through Pluggable Authentication Modules (PAM) for Remote Authentication Dial in User Service (RADIUS), Terminal Access Controller Access-Control System (TACACS+), and Lightweight Directory Access Protocol (LDAP) authentication.

Instructions for configuring these authentication modules are provided in the following files:

- INSTALL.pam_radius.txt
- INSTALL.pam_tacplus.txt
- INSTALL.pam_ldap.txt.

These files are located in the gateway installation directory (/opt/CSCOppm-gw/install) and in the Prime Performance Manager installation image installation directory.

To ensure the Java Virtual Machine (JVM) version and available Pluggable Authentication Modules (PAM) library match, note the following:

- If your Operating System only has a 32-bit PAM library version, use the 32-bit JVM.
- If your Operating System only has 64-bit PAM library version, use the 64-bit JVM.
- If your Operating System has both 32-bit and 64-bit PAM library versions, you can use either 32-bit or 64-bit JVM.

To check the PAM authentication module versions, complete one of the following:

- /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
  ```

- /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
  ```

- /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 the 64-bit kernel, or the 32-bit JVM if the Linux runs the 32-bit kernel.

Verify that the proper PAM library version is available on Linux to match 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 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, Solaris/Linux, or Prime).

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 Modifying the Password Policy, page 6-9.
- 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.

Modifying the Password Policy

By default, Prime Performance Manager enables password requirements that ensure the security of your system. Although not recommended, you can disable any or all of these requirements by completing the following steps:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**.

Step 3 On the Users screen, click **Password Policy**.

Step 4 By default, all password security options are enabled. Disable any that you do not want enforced:

- Password minimum length must be *n* characters.

  The default is 8. You can set a value ranging from 0 through 99.
- Password maximum length must be *n* characters.

  The default is 80. You can set a value ranging from 0 through 99.
- Password cannot be a username or the reverse of a username.
- Password cannot contain “cisco” or any variations including “ocsic”, any capitalized letter variant therein, or by substituting '1', '|', or '!' for i, '0' for 'o', or '$' for 's'.
- No character can be repeated more than three consecutive times in the password.
- Password must contain at least one character from the three character classes: upper case, lower case, digits/special characters.
- Password cannot contain ascending or descending characters.
- Password cannot be the same as the previous five passwords.

- Password cannot contain a dictionary word.

  By default, the 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:

  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.

Step 5 When finished, click **Save**.

User Security Levels

Prime Performance Manager provides three default user roles and two user roles that you can customize. 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 user also has access to all Network Operator user 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 User Authentication, page 6-7, or **ppm updateuser** or **ppm newlevel** commands, as described in Enable User Accounts and Passwords Using the CLI, page 6-18.

Table 6-2 Prime Performance Manager User Levels

Role	Access
Basic User	• View Prime Performance Manager data, load Prime Performance Manager files, and use Prime Performance Manager drill-down menus. • View Prime Performance Manager web interface homepage. • View Reports.
Network Operator	• Access all basic user actions. • View active alarms and event history. • Access only the Normal Poll and Edit Properties options in the device Actions menu.

Table 6-2 Prime Performance Manager User Levels (continued)

Role	Access
System Administrator	• Access all basic user and network operator user functions. • Enable and disable reports • Access all options from the device Actions menu. • Disable, enable, and assign temporary passwords to different user administrations.
Custom Level 1 Custom Level 2	The Custom Level 1 and Custom Level 2 by default do not have authorizations. However, they can be customized and set permissions from basic user, network operator, and system administrator roles. To customize, these access levels, edit the roles.conf file in the /opt/CSCOppm-gw/etc.

Enabling Secure User Access

Secure user access to Prime Performance Manager can be enabled by integrating with Prime Central and managing users through Prime Central, or by enabling secure user access from Prime Performance Manager. For information about integrating Prime Performance Manager with Prime Central, see Chapter 4, "Prime Central Integration."

To enable secure user access for Prime Performance Manager that is not integrated with Prime Central:

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

Step 2 If SSL is not enabled, complete the "Enabling SSL on Gateways and Units" procedure on page 6-2.

Step 3 Run the ppm useraccess enable command:

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

After enabling user access, the ppm useraccess command calls up the authentication type and add user commands:

- ppm authtype—If you have not set Prime Performance Manager authentication type, you must set it now.
- ppm adduser—If you have created users, Prime Performance Manager prompts you to use the same user database or create a new one.

Step 4 To activate your security changes on the client, restart the Prime Performance Manager gateway:

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

Step 5 To activate the security changes on Prime Performance Manager web interface, clear the browser cache and restart the browser.

Step 6 See Modifying the Password Policy, page 6-9, to further customize your Prime Performance Manager security.

Disabling Secure User Access

Should you wish to disable Prime Performance Manager secure user access, complete the following steps:

Step 1 Log into Prime Performance Manager gateway as the root user. See Root User Login, 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 Users and User Security

Prime Performance Manager allows you to add and manage users through the web interface. Before you can do this, however, user access must be enabled. A System Administrator user must be created during installation or post-installation, using Prime Performance Manager CLI as root.

A web user with System Administrator permissions can add or delete users, modify user passwords and roles and access levels. In addition, report policies can be assigned to users specifying what reports they are allowed to see.

These actions are covered in the following topics:

- Add New Users, page 6-12
- Edit User Information, page 6-13
- Change User Passwords, page 6-15
- Edit User Security Settings, page 6-16
- Manually Disable Users and Passwords, page 6-17
- Enable User Accounts and Passwords Using the CLI, page 6-18
- Create Messages of the Day, page 6-19
- List Currently Defined Users, page 6-20
- Display the System Security Log, page 6-21
- Disabling Secure User Access, page 6-12

Add New Users

Administrator users can add new users to Prime Performance Manager. To add a new user:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**.

Step 3 In the Users window, click the **Create a New User Account** tool.

Step 4 Complete the new user information. The options that appear depend on whether you enabled local authentication or use another type of user authentication. (See User Authentication, page 6-7.)

- User Name—Enter the new username.
- First Name—Enter the user first name.
- Last Name—Enter the user's last name.
- Role—Enter the user authentication role for the user. The valid values are:
  - Basic User
  - Network Operator
  - System Administrator
  - Custom Level 1
  - Custom Level 2

Note For a description of security levels, see User Security Levels, page 6-10.

- Password (local authentication only)—Enter the user password.
- Confirm Password (local authentication only)—Retype the password to confirm the new password.
- Email—(optional) Enter the user's email address.
- Phone—(optional) Enter the user's phone number.
- Customer—(optional) Enter the user's customer name.
- Account Number—(optional) Enter the user's account number.
- 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.

Step 5 Click **OK**.

Edit User Information

After you add users, you can change the user information at any later point, for example, you might want to change their user level.

To edit user information:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**.

The Users table displays the following information:

- User Name—The Prime Performance Manager user for whom a user-based access account is set up.
- First Name—The user's first name.
- Last Name—The user's last name.
- Login Time—The date and time the user last logged into Prime Performance Manager.

- Role—Authentication level and number for the user. You can modify the user access level. Valid access levels and numbers include:
  - Basic User
  - Network Operator
  - System Administrator
  - Custom Level 1
  - Custom Level 2

  See Table 6-2 on page 6-10, for a description of actions each user can perform.
- Active—The current user's account status: Yes (the account is functioning normally), or No. A user account can be disabled for the following reasons:
  - A System Administrator disabled the account. See "Manually Disable Users and Passwords" section on page 6-17 for more information.
  - Prime Performance Manager disabled the account because of too many failed attempts to log in. See the "Edit User Security Settings" section on page 6-16 for more information.
  - Prime Performance Manager disabled the account because it was inactive for too many days. See the "Edit User Security Settings" section on page 6-16 for more information.
  - Expired Password—Indicates the user's password has expired.
  - Temporary Password—Indicates the user has a temporary password.
- Details—Allows you to display and/or edit the following optional user details by clicking the circle icon in the Details cell:
  - Email
  - Phone
  - Customer
  - Account Number

Edit User Reports

By default, all users can access all reports available on the gateway. To limit the reports that a user can access:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**.

Step 3 Select the user, then click **Edit Reports**.

Step 4 In the Edit User Reports dialog box, expand the report trees and deselect the reports you do not want the user to access.

Step 5 If you want to provide additional reporting filtering:

a. Expand the report tree to the end report view. In this view, report names have a Filter icon next to the report name.

b. Click the **Filter** icon next to the report you want to filter,.

c. In the Filter [report name] dialog box, enter the following:
   - Column Name—Choose the report data item that you want to base the filter on. The items displayed depend on the report.
   - Operator—Enter the operator value: equals, not equal, greater than, and others.
   - Filter Value—Enter the filter value. For example, filter the parameter to listed in Column Name by the operation in the Operator field to the number entered here.

d. Click **Save**.

Change User Passwords

Administrators can change any user password; individual users can change their own passwords. If you want to change your own password:

Step 1 Log into Prime Performance Manager.

Step 2 From the user ID on the top right corner of the Prime Performance Manager window, choose **Change Password**.

Step 3 In the Change Password dialog box, enter the new password, then enter it again in the Confirm Password field.

Step 4 Click **OK**.

If you are an administrator and want to change a user password:

Step 1 Log into Prime Performance Manager as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**.

Step 3 Select a user whose password you want to change, then click the **Reset Password** tool.

Step 4 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 5 Click **OK**.

Note You can also change user passwords using the ppm userpass command. See ppm userpass, page B-79.

Edit User Security Settings

You can edit user security settings that to automatically disable users and passwords when certain conditions are met, for example, control the number of failed logins before an alarm is issued, the number of failed logins before a user disabled, and other security parameters.

To edit user security settings:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**

Step 3 On the Users screen, click **Security Settings**.

Step 4 In the Security Settings window, edit any of the following:

- Number of Failed Logins Before Alarm—Sets the number of failed logins before an alarm is raised. The default is 5. The range is 1-10. Entering 0 disables this setting. (To provision this parameter using the CLI, see ppm badloginalarm, page B-12.)
- Number of Failed Logins Before Account Disabled—Sets the number of failed logins before the user's account is disabled. The default is 10. The range is 1-10. Entering 0 disables this setting. (To provision this parameter using the CLI, see ppm badlogindisable, page B-12.)
- Number of Days Before Disabling Inactive Users—Sets the number of days of inactivity before a user is disabled. The valid range is 1-365. The default is 0; inactive users will never be disabled. (To provision this parameter using the CLI, see ppm inactiveuserdays, page B-31.)
- Number of Days Before Forcing a Password Change—Sets the number of days before the user must change their password. The valid range is 1-365. The default is 0; users will never be forced to change their password. (To provision this parameter using the CLI, see ppm passwordage, page B-46.)
- Password Notification Early Notification Days—Sets the number of days before password expiration when a notification is sent to the user. The default is 15 days. The range is 0-30.
- Number of Minutes Before Disabling Inactive Clients—Sets the number of minutes before disabling an inactive client. The valid range is 1-120. The default is 0; inactive clients are never disabled. (To provision this parameter using the CLI, see ppm clitimeout, page B-14.)
- Single Session—Defines the number of active sessions a user can create:
  - Enable—Only a single session is allowed per user. If a user logs into a second web interface session, the first session is ended.
  - Disable—(Default) Disables the single session per user restriction. The user can log in as the same user from multiple web interfaces.
  - Block—Only a single session is allowed per user. If a user attempts to log into a second web interface session, they are blocked until they close the first session.
- Restrict Password Changes—Provides restrictions on the password change frequency:
  - Password Change Interval—Specifies with time interval, between 1 and 745 hours, within which the password change restriction applies. 48 hours is the default.
  - Number of Password Changes per Interval—Specifies the permissible number of password changes, between 1 and 10, allowed within the time interval specified in Password Change Interval. Two is the default.

Manually Disable Users and Passwords

As described in the Edit User Security Settings, page 6-16, 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 Users and User Security, page 6-12 for more details.

To disable Prime Performance Manager users and passwords:

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

Step 2 Enter:

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

Step 3 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 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. This also applies to authentication performed by Prime Central single signon.

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 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.

Enable User Accounts and Passwords Using the CLI

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 Root User Login, page 2-1.

Step 2 Enter the following command:

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

Step 3 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 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 Modifying the Password Policy, page 6-9.

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 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 Modifying the Password Policy, page 6-9.

Step 6 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.

Create Messages of the Day

You can provision Prime Performance Manager to display a user-defined system message of the day to appear before and after users log in. User s must accept the message before they are allowed to proceed. You can use the message of the day to communicate important system changes or events to users.

To display the message of the day, launch Prime Performance Manager. If a pre-login message of the day is enabled, it is displayed and requires you to accept the message before the login window is displayed. If a post-login message is enabled, it appears right after you log in and requires you to accept it before the Prime Performance Manager window is displayed.

To create or edit the message of the day:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**

Step 3 On the Users screen, click **Security Settings**.

Step 4 Complete one or both of the following messages:

- To create a pre-login message, check the Pre-Login Message box, enter the message, then click **Save**.
- To create a post-login message, check the Post-Login Message box, enter the message, then click **Save**.

The messages will appear at the next user login.

Note Messages of the day can also be configured using the ppm motd and ppm premotd commands. For information, see ppm motd, page B-42 and ppm premotd, page B-48.

Display Active Sessions

To see a list of users who are actively logged into the server:

Step 1 Log into the Prime Performance Manager gateway as a System Administrator user.

Step 2 From the Administration menu, choose **Users/Security**

Step 3 On the Users screen, click **Active Sessions**.

Step 4 On the Active Sessions as of [current date] screen, the following user information is displayed:

- Client ID
- Username
- IP/Host Name
- Login Time
- Last Access Time
- Login Method

List Currently Defined Users

To list all currently defined users in Prime Performance Manager user-based access account list using the CLI:

Note You can also view user account information on Prime Performance Manager User Management page, see Managing Users and User Security, page 6-12 for more details.

Step 1 Log into Prime Performance Manager gateway as the root user. See Root User Login, 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
- Password Aging—Whether password aging is enabled for the user.

To list information for a specific user, enter:

`./ppm listusers` *username*

where *username* is the name of the user.

Display 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 Root User Login, 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 Displaying the Security Log, page 11-6.

CHAPTER 7

Managing Reports, Dashboards, and Views

Prime Performance Manager provides over 2800 reports and dashboards covering many different network device hardware and software elements. You can change how report data is displayed, enable and disable reports, and create customized report policies for specific devices or groups of devices. In addition, you create your own custom report views and groups. These and other report features and functions are described in the following topics:

- Displaying Reports, page 7-1
- Changing the Master Report Settings, page 7-14
- Enabling and Disabling Reports, page 7-16
- Creating Report Policies, page 7-20
- Displaying Report Definitions, page 7-22
- Displaying Data Center Reports, page 7-22
- Setting Up Bulk Statistics Reports, page 7-24
- Managing Dashboards, page 7-31
- Creating and Managing Custom Report Views, page 7-34
- Creating and Managing Report Groups, page 7-42

Displaying Reports

After Prime Performance Manager device discovery is completed (see Chapter 5, "Discovering Network Devices"), you can display reports by either choosing **Reports** from the Performance menu to display network reports or drill down to a device and display the device reports.

Tip To display a list of all provided reports, from the Help menu, choose **Reports**, then click **Reports List Readme**.

At the network report level, the following report categories are displayed in the navigation area:

- Application Traffic
- Availability
- Data Network Services
- Hypervisors

- IP Protocols
- IP QoS
- IP SLA
- Mobile IOS Statistics
- Mobile StarOS Statistics
- PPM System
- Resources
- Security
- StarOS CDMA Statistics
- Storage
- Transport Statistics
- UCS Clusters
- Video Broadcast
- Virtualization

At the device report level, only the report categories containing reports generated for the device are displayed. As you navigate through Prime Performance Manager reports, keep the following in mind:

- Prime Performance Manager presents reports in a context-sensitive hierarchy. The navigation area is the highest report category level. As you drill down to lower levels, the focus turns to the content area, where you can display detailed reports at specific time intervals. The number of report levels depend on the report category.
- The reports available at any given point depend entirely on the focus. At the network level, the largest number of reports are available because many devices are in focus. As you shift the focus to individual devices, device elements, or to specific report categories, the number of available reports shrinks.
- Report availability ultimately depends upon the hardware and technologies provisioned on the devices. A report will not be displayed for a technology not provisioned on a device.

The device time zone displayed in reports is obtained from one of the following:

1. The time zone entered in the device Time Zone field. See Editing a Device Name, Web Port, and Time Zone, page 8-13.
2. The device time zone when the device was imported from Prime Network.
3. The time zone retrieved from the device.
4. The time zone of the Prime Performance Manager server where the device is connected.

For bulk statistics reports (Moble StarOS Statistics), the following notes apply:

- The time zone displayed for Cisco ASR 5000 and Cisco ASR 5500 devices depends on the bulk statistics file name and header sections. If devices are not configured to send files in the correct formats, the time zone will not display properly.
- The time zone name (EDT, UTC, etc.) is taken from bulk statistics file name. For example: RTPZ5SVCGW02_bulkstats_20120912_113502_EDT_5_5.csv.
- The time zone offset [(+/-)HHMM offset] is taken from the bulk statistics header. For example:

  Version-1.4.0,172.18.20.168,20120912-153526,20120912-113526,EDT,-0400,120912-11:35, private

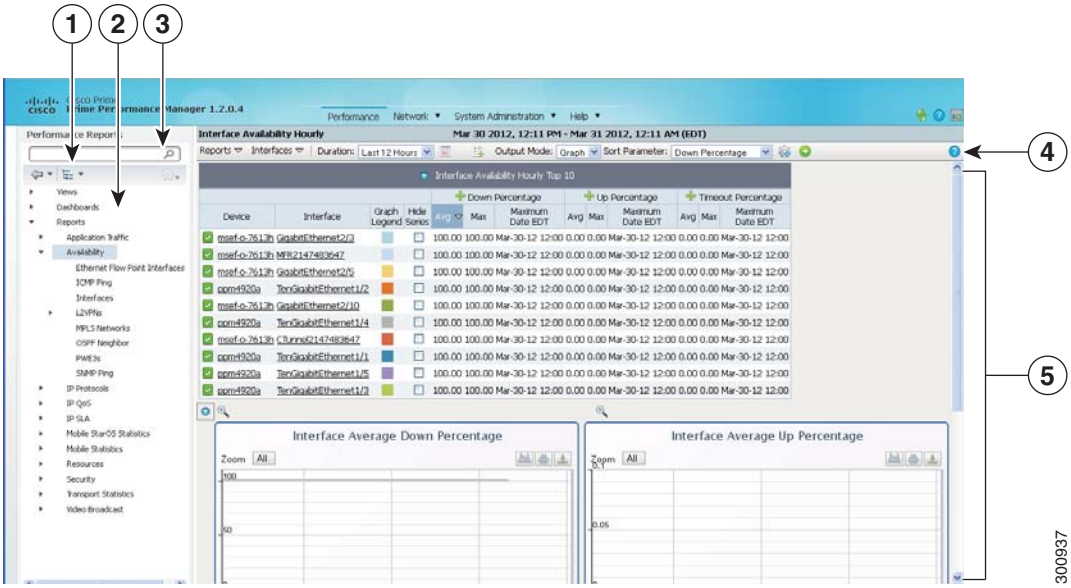
Figure 7-1 shows the Prime Performance Manager reports window with the Interface Availability report displayed in graph output format. Window elements include:

- Navigation tree—Allows you to select high-level report categories and subcategories. You can switch between tree or list views by selecting **Tree View** or **List View** respectively at the top of the navigation area.
- Search—Allows you to search for reports containing key words. For example, entering “Ethernet” will display all reports with Ethernet in their titles.

Note The Search field is also available from the Views and Dashboards windows.

- Content area—Displays report information. You can switch between graph and table formats by selecting **Graph** or **Table** in the reports toolbar Output Mode.

Figure 7-1 Reports Window



1	Navigation tree display tools	**4**	Menu bar
2	Navigation tree	**5**	Content area (graph view)
3	Search field		

Reports Menu Bar

The reports window and menu bar (Figure 7-2) provide many tools and functions that allow you to display individual reports specific to your needs and interests. The window title bar displays the report name and report period. The report time period shows the time zone in *TTT* format (where *TTT* is the time zone, for example, EDT) for all network-level reports when the Display Device Level Data in Device Time Zone user preference is disabled. When the preferences is enabled and the report or

dashboard is device level, the time zone is shown in GMT + *hh:mm* format. The duration is relative to the server or device time zone. For information about setting user preferences, see Changing User Preferences, page 3-7.

The Reports menu bar allows you change the report presentation in many different ways to meet your personal preferences or to highlight data that is of special interest. The menu bar is context sensitive; items that appear depend on the report category and selected report. Menu bar report options include:

- Reports—Allows you to choose the next level report beneath the report level currently in focus. For example, if you choose Availability > MPLS Networks, MPLS availability reports are displayed along with report intervals, for example, hourly, daily, weekly, or monthly.
- *Report Subcategory*—For report categories with multiple levels, a report subcategory menu is displayed with the subcategory name. The navigation tree, Reports menu, and subcategory menu operate hierarchically; selections vary depending on the depth of the report view in focus.
- Duration—Allows you to choose the report duration. The duration options that appear depend on the report intervals that are enabled:
  - 5 Minute—Last 6 hours, 24 hours, 3 days, 7 days.
  - 15 Minute—Last 12 hours, 24 hours, 3 days, 7 days, 14 days.
  - Hourly reports—Last 12 hours, 24 hours, 3 days, 7 days, 14 days, 21 days, 30 days, current month, previous month.
  - Daily reports—Last 7 days, 14 days, 21 Days, 30 days 6 months.
  - Weekly reports—Last 30 days, 60 days, 90 days, 6 months, 1 year.
  - Monthly reports—Last 90 days, 6 months, 1 year, 5 years.

  Note Intervals greater than the reporting aging intervals will not be displayed. For information, see Changing the Master Report Settings, page 7-14.

- Columns—Allows you to change the display from 1 to 3 columns.

Tip You can enable the Show One Graph Column Per Report user preference to display all reports as one column per graph. This can be useful if you have device configurations with long index component names that result in long titles and legends, or if you prefer viewing one stacked list of graphs. This preference sets the default. You always change it using the Columns parameter.

- Customize Date and Time Range—Allows you to create a report with a custom date and time range. The maximum time periods you can specify depend on the report interval:
  - Hourly reports—Seven days.
  - Daily reports—31 days.
  - Weekly reports—One year.
  - Monthly reports—Five years.

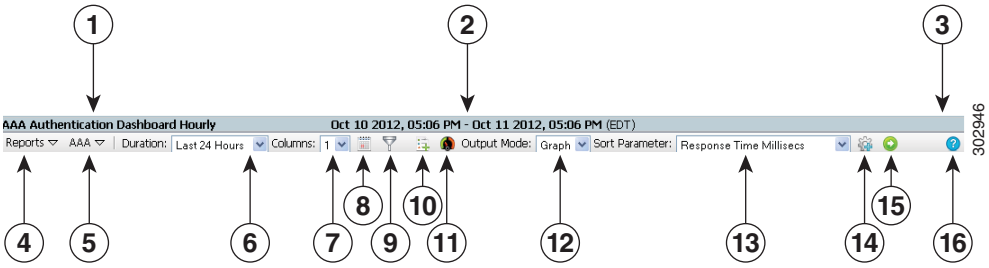
  Note Intervals greater than the reporting aging intervals will not be displayed.

- Report Object Filter—Allows you to filter report information based on different criteria. See Filtering Report Information, page 7-13 for information.

- Toggle Legends—For reports displayed in graph output, turns the chart legend on and off. If turned on, the chart legend appears under each chart displaying the color-coded report items. and the average and maximum data values for each item.
- Go Live—Initiates 15-second polling for device-level reports. (This tool is not displayed for network-level reports.) For more information, see Displaying Network and Device Reports, page 7-6.
- Output Mode—Allows you to change the report output format:
  - Graph—(Default) Displays the top *nn* report items in table and chart formats. By default, ten report items are displayed. (You can change the number of data items that are displayed in User Preferences. For information, see Changing User Preferences, page 3-7. Graph output provides many other customization options. For information, see Customizing Report Display, page 7-9.)
  - Table—Displays all report data in table format. While graph format displays only the top *nn* report items, the table output format displays all items. Page controls in the top right control the number of table rows to display. By default, 200 rows per page are displayed. To see all of the data, use the control to page through it, or use the **Page Size** control to adjust the page size.

    In table output, you can click the **Export report page as CSV file** button to export the current page in comma separated values format.
- Sort Parameter—Allows you to choose a parameter to sort the report information. The parameters displayed depend on the report. For example, in the Figure 7-1 Interface Availability report, the sort parameters are Down Percentage, Up Percentage, and Timeout Percentage.
- Graph Series Editor—Opens the Graph Series Editor dialog box where you can add and remove report items, or "series" from the report display. Report items are often, but not always, devices. For performance, select no more than ten items. (This option is only available in graph output mode.)
- Run Report—Runs the report after you modify any report parameters in the menu bar.
- Help for Report—Displays a text file with the MIB variables that are polled for generating the report, including any calculations that are performed. This text file also has links to the associated report XML files.

Figure 7-2 Reports Menu Bar



1	Report title	**9**	Report Object Filter
2	Report time period	**10**	Toggle Legends
3	Report table row currently in focus	**11**	Go Live
4	Reports selection menu	**12**	Output Mode
5	Report subcategory menu (Interfaces in this example)	**13**	Sort Parameter

6	Duration	**14**	Graph Series Editor
7	Columns	**15**	Run Selected Report
8	Customize Report Date and Time	**16**	Help for Report

Displaying Network and Device Reports

Displaying network and device reports is accomplished using very similar procedures. Prime Performance Manager allows you to easily navigate up and down the report hierarchy, from network-wide views to individual device and device element reports.

Note Network reports include only the devices with report information for the selected report category.

Network-Wide Device Reports

To view a network-wide report:

Step 1 From the Performance menu, choose **Reports**.

Step 2 In the navigation area, expand the **Reports** item and choose the report category that you want to view, for example, Application Traffic, Availability, IP Protocols, or other category.

The content area displays the default network report for the report category you selected. The default report is based on the sort weight Prime Performance Manager assigns to the report. For example, if you choose **Availability > MPLS Networks**, the MPLS Interface Availability hourly network report is displayed. If you choose **Resources > CPU**, the network CPU Utilization report is displayed.

Reports are displayed in graph format by default. For practicality, only ten devices are displayed in graph views. (The number can be changed using the ppm topxxsize command. For information, see ppm topxxsize, page B-77.) If more are available, the report includes a "Top N" in its title. To view the other devices, switch to table view, or use the Graph Series Editor described in Step 4 to add and remove devices.

Step 3 After you select a report category from the navigation tree, you can:

- Modify the parameters of the default report and run the report again, or
- Choose a different report from the content area Reports menu and/or the next level report menu, if it is displayed, or
- Drill down to the device report by clicking a device link.

Note You can change the number of devices displayed in graph view and report summary table using the Maximum Number of Data Series per Report user preference. For information, see Changing User Preferences, page 3-7.

Step 4 As needed, perform any or all of the following report modifications by choosing items on the report menu bar (Figure 7-2):

- Click **Duration** and choose a different report duration. The duration options depend on the report interval:
  - 5 Minute—Last 6 hours, 24 hours, 3 days, 7 days.
  - 15 Minute—Last 12 hours, 24 hours, 3 days, 7 days, 14 days.

  - Hourly reports—Last 12 hours, 24 hours, 3 days, 7 days, 14 days, 21 days, 30 days, current month, previous month.
  - Daily reports—Last 7 days, 14 days, 21 Days, 30 days, 6 months.
  - Weekly reports—Last 30 days, 60 days, 90 days, 6 months, 1 year.
  - Monthly reports—Last 90 days, 6 months, 1 year, 5 years.
- Click **Customize Date and Time** and choose a custom report start and end date and time. Use this option if the default Duration time periods do not meet your needs. The custom time period can be no longer than seven days.
- Click **Report Object Filter** to filter report information. For information, see Filtering Report Information, page 7-13.
- For reports in graph output:
  - Click **Toggle Legends** to turn the graph legend on and off. For reports displayed in graph output, Toggle Legends turns the chart legend on and off. If turned on, the chart legend appears under each chart displaying the color-coded report items and the average and maximum data values for each item.
  - Click **Graph Series Editor** and add or remove devices to and from the report.

Note Graph output provides many other customization options. For information, see Customizing Report Display, page 7-9.)

- Click **Output Mode** and choose a different report output:
  - Graph (default)—Displays the top N (10 is the default) devices for the selected report in graphical format.
  - Table—Displays all the devices for the selected report in table format. Click the **Export report page as CSV file** button to export the current page in comma separated values format.
- Click **Sort Parameter** and choose a different report parameter to sort the report information. The parameters are based on the report.

Step 5 When finished, click **Run Report** (green arrow) to run the report with the modified parameters.

Individual Device Reports

Displaying device reports is similar to network device reports, with some navigation and option differences. To display a report for an individual device:

Step 1 From the Network menu, choose **Devices**.

All the devices polled by Prime Performance Manager are displayed.

Step 2 Click the link of the device that you want to view.

The content area displays the default report for the device you selected. The default is based on the sort weight Prime Performance Manager assigns to the report.

Reports are displayed in graph format by default.

Step 3 After you display the default device report, you can:

- Modify the parameters of the default report and run the report again, or

- Choose a different report from the content area Reports menu and/or the next level report menu, if it is displayed.

Step 4 As needed, perform any or all of the following report modifications by choosing items on the report menu bar (Figure 7-2):

- Click **Duration** and choose the report duration. The duration options depend on the report interval:
  - 5 Minute—Last 6 hours, 24 hours, 3 days, 7 days.
  - 15 Minute—Last 12 hours, 24 hours, 3 days, 7 days, 14 days.
  - Hourly reports—Last 12 hours, 24 hours, 3 days, 7 days, 14 days, 14 days, 21 days, 30 days, current month, previous month.
  - Daily reports—Last 7 days, 14 days, 21 Days, 30 days, 60 days, 6 months.
  - Weekly reports—Last 30 days, 60 days, 90 days, 6 months, 1 year.
  - Monthly reports—Last 90 days, 6 months, 1 year, 5 years.
- Click **Customize Date and Time** and choose a custom report start and end date and time. Use this option if the default Duration time periods do not meet your needs. The maximum custom time periods are:
  - 5 Minute—Three days.
  - 15 Minute—Seven days.
  - Hourly reports—Seven days.
  - Daily reports—31 days.
  - Weekly reports—One year.
  - Monthly reports—Five years.
- Click Report Object Filter to filter report information. See Filtering Report Information, page 7-13.
- For reports in graph output,
  - Click **Toggle Legends** to turn the graph legend on and off.
  - Click **Graph Series Editor** and add or remove devices to and from the report.
- Click **Go Live** to start 15-second updates for device-level reports. After you click Go Live:
  - The summary table, tools left of the report chart, and all toolbar functions that do not apply to live mode are removed.
  - End Live Mode appears at the top of the report window.
  - Reports are updated continuously every 15 seconds.

  Live mode continues as long as you remain on the device page, or until you click End Live Mode. If you move away from the device window to another window, Live Mode stops. To start it, return to the device report and click Live Mode.

Note Some reports, such as ICMP Ping, do not support 15-second polling. If so, an alert will tell you that Go Live is not supported.

Note Some devices take longer than 15 seconds to poll. If so, Prime Performance Manager sends a series of messages, initially stating the device is not responsive. Prime Performance Manager then increases the polling interval until it finds an interval that is successful. It will attempt each interval two times. If data is not recovered at 1-minute polling, Go Live mode will exit.

- Click **Output Mode** and choose a different report output:
  - Graph (default)—Displays the top ten devices for the selected report in graphical format.

    Note Graph output provides many other customization options. For information, see Customizing Report Display, page 7-9.)

  - Table—Displays all the devices for the selected report in table format.
  - CSV—Saves the report in CSV format to your client computer.
- Click **Sort Parameter** and choose a different report parameter to sort the report information. The parameters are based on the report.

Step 5 When finished, click **Run the Selected Report** (green arrow) to run the report with the modified parameters.

Related Topics

Changing the Master Report Settings, page 7-14

Customizing Report Display

Prime Performance Manager provides many options to control the report information and how it is presented. The Graph report output provides options that allow you to customize the display to highlight report data or to suit your personal preferences. For example:

- Click **Hide Row** in a table item—Hides the item from the chart. In addition to Hide Series,
  - Click colored boxes in the Graph Legend—Highlights the associated series in the graph.
- Click a data series name in the legend—Hides/displays the series. (It also grays out the text when the series is hidden.)
- Click **Show Graph in Full Screen**—Display the chart in full-screen size.
- Click **Show Related TCAs**—If thresholds are created, displays the threshold in graphical format. If a threshold is not provisioned, the tool is inactive. For information about creating thresholds, see Creating Thresholds, page 10-1.
- Click different report time intervals on the **Zoom** tool
- Click **Copy to Clipboard**—Copies the chart to a clipboard that is unique for each user on the server. You can copy multiple charts to the clipboard. The clipboard retains graphs copied to it until you paste the clipboard contents to a custom view page. See Creating a Custom Report View, page 7-34.

Tip Perform the copy and paste operations in two tabs. In one tab, drill through the reports and click the graphs you want. In the other tab, you can paste the items directly into the view you want.

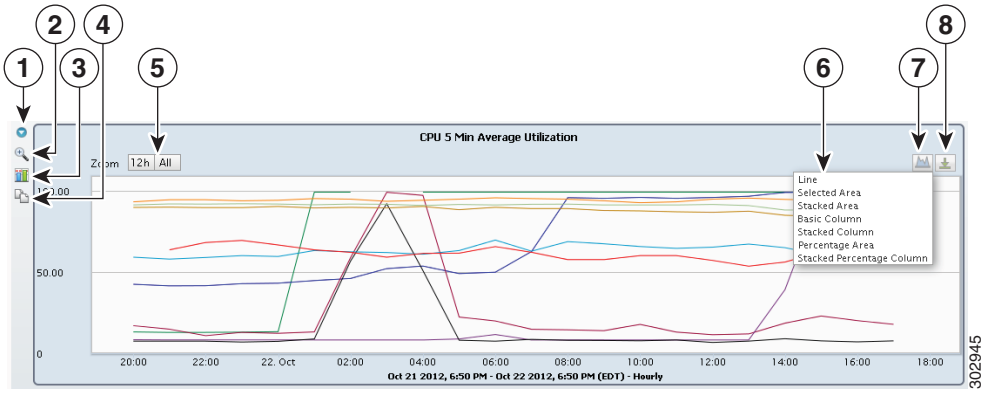
- Click **Add to Star Graphs** to add the report chart to the Star Graphs tab. See Creating Custom Device Star Graphs, page 7-12 for information.

Note

Inside the chart images:

- Click **Graph Style**—Allows you to change how data is presented in the graph:
  - Line—Displays data in lines.
  - Selected Area—Highlights one series.
  - Stacked Area—Shades and stacks all series.
  - Basic Column—For leaf graphs, displays basic bar graphs. Not available for other level graphs.
  - Stacked Column—Similar to the Stacked Area option, but displayed in columns.
  - Percentage Area—Displays the percentage contribution of each series.
  - Stacked Percentage Column—Similar to the Percentage Area option, but displayed in columns.
- **Export to Image**—Downloads the chart to your computer as a PNG or JPG image, or as a PDF.

Figure 7-3 Graph Display Options



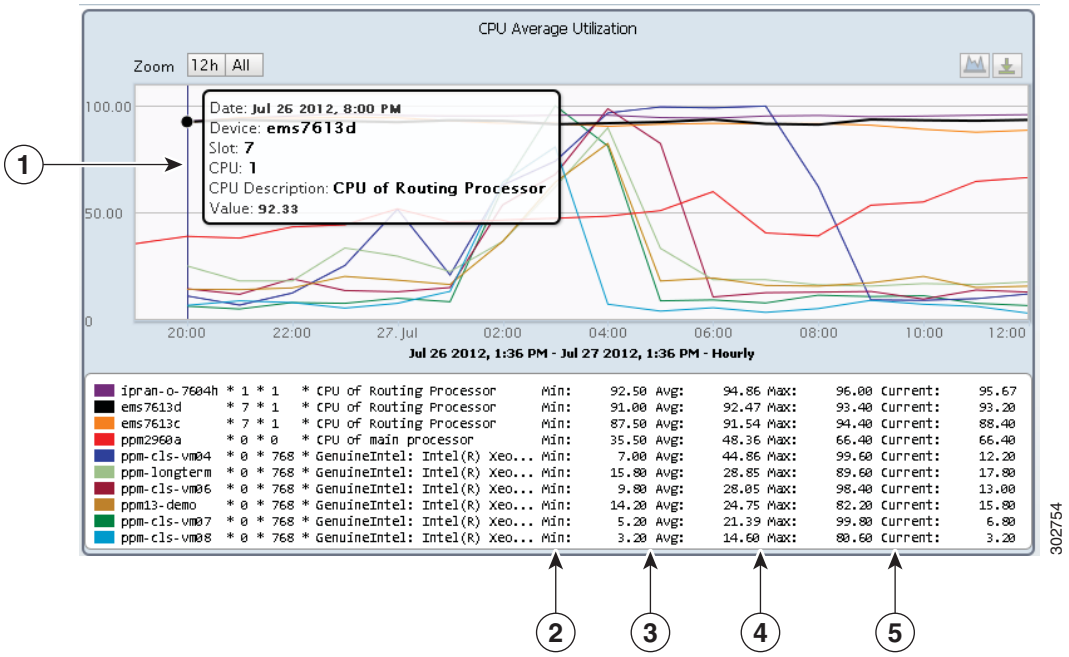
1	Hide Row	**5**	Zoom
2	Show Graph in Fullscreen	**6**	Graph style options
3	Toggle Related Threshold	**7**	Graph Style
4	Copy to Clipboard	**8**	Export Graph

For example, you can choose whether you want the minimum, maximum, average, total, and current data values displayed in graphs and summary tables. In other words, for any data item, the minimum value for the report period, maximum value, average, total, and current values can be displayed. Figure 7-4

shows the minimum, maximum, average and current data for a CPU utilization report. In addition, you can enable or disable the graph vertical data point bar, change the graph height, or display only one graph column per report.

Tip Click the legend color swatches to highlight or not highlight the corresponding series in the chart. Click the legend text to show or hide that series.

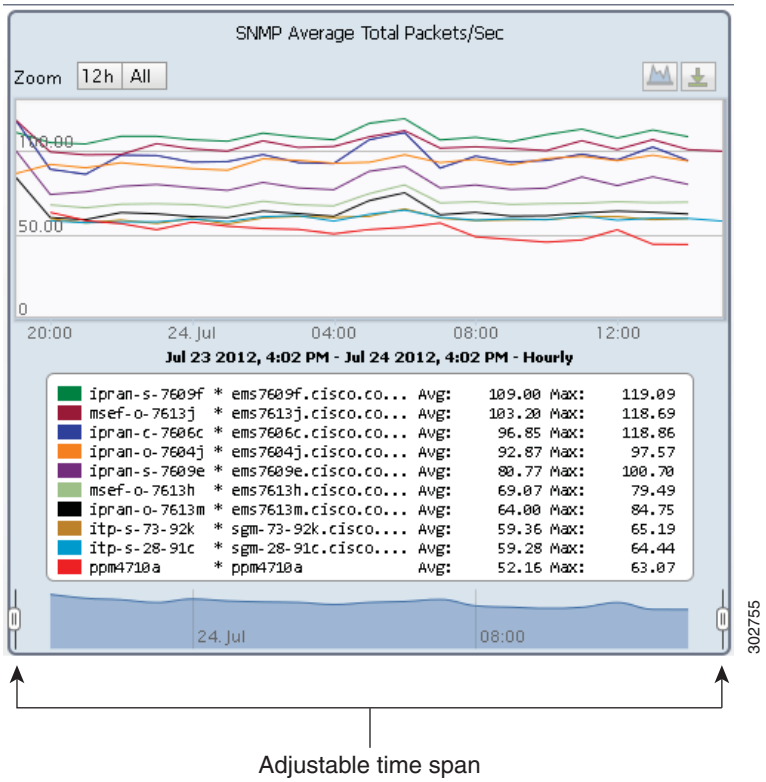
Figure 7-4 Graph Bar and Data Display Options



1	Vertical data point bar	**4**	Maximum data
2	Minimum data	**5**	Current data
3	Average data		

The time span bar (Figure 7-5) is another option you can use to reduce the time span within a chart so you can view intervals of interest in greater detail. By default, the time span bar is displayed in all full screen charts. However, it can be enabled so that it appears on all report charts.

Figure 7-5 Graph Time Span Bar



These and many other options are provisioned in the User Preferences window. For information, see Changing User Preferences, page 3-7.

Creating Custom Device Star Graphs

At the device report level, you can pick individual report charts and add them to the Star Graphs tab to create a customized, device-level report view.

To create a custom device hot chart:

Step 1 From the Network menu, choose **Devices**.

Step 2 Click the link of the device for which you want to create a custom view.

Step 3 From the device Reports menu, display the report containing the data you want to add to the custom view.

The report is displayed in chart output format by default.

Step 4 Navigate to the chart that you want to add, and click the **Add to Star Graphs** tool inside the graph.

The graph is automatically added to the Star Graphs tab.

Note Prime Performance Manager copies the device-level equivalent of the item you copied. For example, if you drilled into an individual CPU and add it to a star graph, the star graph page will show a report for all device CPUs, not just the one you copied.

Step 5 Repeat Step 4 until you have added the charts that you want to the Star Graphs tab. You can navigate to different reports and select charts from them as well.

Note For performance, you should add no more than ten graphs to the Star Graphs tab.

Step 6 When finished, click the **Star Graphs** tab to view your custom report view for the device. The tab displays the selected charts in normal report view. Most of the report menu bar (see Figure 7-2 on page 7-5) actions are available including Interval, Duration, Custom Date Range, and the ability to toggle between graph and table output formats at the global and individual report item level.

Report items in the Star Graphs view remain until you delete them.

Step 7 To remove a report item, click the **Remove this Graph** toolbar item inside the chart you want to delete. You can also remove a star chart report by unchecking the star of the report on the page where it was first starred.

Filtering Report Information

You can filter report information to display data within certain numeric or alphabetic parameters, for example, to display a down percentage 80 and higher.

Note If you filter reports so that only one report object remains, Prime Performance Manager combines the object data into one graph and displays it without requiring you to drill down.

To filter report information:

Step 1 Display the report following the "Displaying Reports" procedure on page 7-1.

Step 2 On the report toolbar, click the **Report Object Filter** tool.

Step 3 In the Set Report Object Filter dialog box, complete the following:

- Column Name—Choose the report column that you want to use to filter the report information. The columns will vary, depending on the report.

  Note Non-editable fields to the right of Column Name provide database name and data type for the displayed report item. For example, Device has the database name, node, and data type, string. This data is provided for informational purposes and can be useful when customizing reports. (For information about customizing Prime Performance Manager reports, see the *Cisco Prime Performance Manager 1.3 Integration Developer Guide*.

- Operator—Enter the operator:
  - equals
  - not equals
  - contains
  - not contains
  - greater than

  - less than
- Filter Value—Enter the value to be used with the column and operator to filter the report, for example, if you want to display only GigabitEthernet interfaces, you would enter the following values:
  - Column Name: **Interface**
  - Operator: **contains**
  - Filter Value: **GigabitEthernet**

Note When filtering on columns that are percentages, enter filter values in decimal format with a leading 0. For example, to filter everything below 93.25%, enter 0.9325. Entering 93.25 or .9325 will generate the desired results.

Step 4 Click **OK**.

Step 5 On the report toolbar, click **Run the Report**.

The report displays the filtered information.

Step 6 To remove the filter:

a. On the report toolbar, click the **Report Object Filter** tool.

b. In the Set Report Object Filter dialog box, remove the entry in the Filter Value field.

c. Click **OK**.

d. On the report toolbar, click **Run the Report**.

The report displays the full report information.

Changing the Master Report Settings

You can provision report intervals and report aging parameters and apply them to all Prime Performance Manager reports from the Performance > Reports > Administration Report Settings window. The master report settings allows you to set up the broad rules for report generation and management. These rules can be overridden at the individual report level, for example, you might decide not to enable 1-minute reports as a global setting, but enable 1-minute reports for certain critical areas.

To provision the master report general and aging settings:

Step 1 From the Administration menu, click **Report/Group Settings**.

The Administration Report Settings window displays the general and aging report settings.

Step 2 In the General Settings area, click **Time Mode** if you want to change the report time mode, either 12 or 24-hour (default). For the other settings, click **Disabled** or **Enabled** to disable or enable the setting. See Table 7-1 for general setting descriptions.

Step 3 In the Aging Settings area, click a field and edit the aging value for the report, as needed. See Table 7-1 for aging setting descriptions.

Step 4 When finished, return to the previous Prime Performance Manager window.

Step 5 To display the report setting changes, click Run Report click **Reload Report** on the report toolbar (if a report is displayed), or click **Reload Page** on the main toolbar at the top of the Prime Performance Manager window.

Table 7-1 Historical Statistics Report Settings

Area	Field	Description
General Settings	Reports Directory	Directory where Prime Performance Manager stores reports. The default is /opt/CSCOppm-gw/reports. You cannot edit this field. To change the reports directory, use the ppm repdir command. See ppm repdir, page B-56.
	Time Mode	The report time mode, either 12-hour or 24-hour (default).
	Master Report Flag	Enables or disables report generation for all reports: • Enabled—(default) Report generation is on, pending provisioning set at the individual report time interval. • Disabled—Stops all report generation regardless of the provisioning at the individual report time interval.
	1 Min Report Flag	If enabled, 1-minute reports are generated. If you enable 1-minute reports, you must: • Enable 1-minute reports at the individual report level. (See Enabling and Disabling Reports, page 7-16.) One-minute reports are not enabled automatically across all reports. This field is disabled by default.
	5 Min Report Flag	If enabled, 5-minute reports are generated. This field is disabled by default.
	15 Min Report Flag	If enabled (default), 15-minute reports are generated.
	Hourly Report Flag	If enabled (default), hourly reports are generated.
	Daily Report Flag	If enabled (default), daily reports are generated.
	Weekly Report Flag	If enabled (default), weekly reports are generated.
	Monthly Report Flag	If enabled (default), monthly reports are generated.
	Export Reports	If enabled, automatically generate reports in CSV and 3GPP XML format and stores them in the /opt/CSCOppm-gw/reports directory. This field is disabled by default. **Note** If you enable this field, enable report backups. For information, see ppm backuprep, page B-11.
	Generate DB Reports	If enabled (default), automatically generate reports and stores report data in the report database.
	Export Hourly 5 Minute CSV Reports	If enabled, automatically generates hourly 5-minute reports in CSV format and stores them in the /opt/CSCOppm-gw/reports directory. This field is disabled by default.
	Export Hourly 15 Minute CSV Reports	If enabled, automatically generate hourly 15-minute reports in CSV format and stores them in the /opt/CSCOppm-gw/reports directory. This field is disabled by default.
	Perform Disk Space Checking	Enables or disables disk space checking. Disk space usage increases with every enabled report. The increase depends on the report, the number of devices, and their configurations. Monitor disk space usage and disable the reports for specific devices or decrease the aging value to delete old reports frequently.

Table 7-1 Historical Statistics Report Settings (continued)

Area	Field	Description
Aging Settings[1]	1 Min Stats Aging (Days)	Database aging value for 1-minute statistics. The default is 2 days.
	5 Min Stats Aging (Days)	Database aging value for 5-minute statistics. The default is 3 days.
	15 Min Stats Aging (Days)	Database aging value for 15-minute statistics. The default is 7 days.
	Hourly Stats Aging (Days)	Database aging value for hourly statistics. The default is 14 days.
	Daily Stats Aging (Days)	Database aging value for daily statistics. The default is 94 days.
	Weekly Stats Aging (Days)	Database aging value for week statistics. The default is 730 days.
	Monthly Stats Aging (Days)	Database aging value for monthly statistics. The default is 1825 days.
	1 Min CSV Aging (Days)	Database aging value for 1-minute CSV statistics. The default is 2 days.
	5 Min CSV Aging (Days)	Database aging value for 5-minute CSV statistics. The default is 3 days.
	15 Min CSV Aging (Days)	Database aging value for 15-minute CSV statistics. The default is 7 days.
	Hourly CSV Aging (Days)	Database aging value for hourly CSV statistics. The default is 14 days.
	Daily CSV Aging (Days)	Database aging value for daily CSV statistics. The default is 94 days.
	Weekly CSV Aging (Days)	Database aging value for weekly CSV statistics. The default is 730 days.
	Monthly CSV Aging (Days)	Database aging value for monthly CSV statistics. The default is 1825 days.
	Bulk Stats Aging (Days)	Specifies the aging value for bulk statistic files in the drop directory. The age is the age of files received, not a database age. The default is 14 days.

1. When records exceed the specified value, they are aged out of the database.

Enabling and Disabling Reports

While you can apply report settings to all Prime Performance Manager reports (see Changing the Master Report Settings, page 7-14), you can also apply many of the same settings to the report categories and individual reports. For example, you might want to enable and disable all Application Traffic reports or all Availability reports. Within a report category, you can enable or disable reports at specific intervals. Report intervals include 1-minute, 5-minute, 15-minute, hourly, daily, weekly, and monthly intervals. All reports and report intervals are enabled by default except for 1-minute and 5-minute reports, which are disabled by default.

Report data options include the ability to generate report data in CSV format, and the ability to indicate whether report data should be storied in the database.

When modifying reports and report intervals, keep the following in mind:

- Although administrator and operator users can enable 1-minute and 5-minute reports, only system administrator users can enable the SNMP device polling interval required for these intervals.
- Enabling a 1-minute and 5-minute reports increases the Prime Performance Manager unit disk space utilization and decreases unit performance because of the increased disk activity.
- Only reports that run on a regularly scheduled intervals are displayed in the hourly and daily data. Reports that run continuously are not displayed.

To enable or disable reports or change report intervals:

Step 1 From the Administration menu, click **Report Status**.

The Administration Reports Status table (Figure 7-6) displays the high-level report categories and their status: enabled (check box left of the report category is checked) or disabled (check box is not checked).

Step 2 Under Report Name, click the show reports tool to display the reports within a category.

Step 3 As needed, modify any of the following report settings:

- Report intervals—Select the report intervals that you want to enable for the report: 1 Minute, 5 Minute, 15 Minute, Hourly, Daily, Weekly, Monthly.

Note One-minute and five-minute reports require substantial storage and can impact device performance. Enable these intervals with care.

Note Prime Performance Manager automatically adjusts the polling frequency to match the most frequent provisioned report frequency.

- Report data—Two options are provided for report data:
  - CSV—If enabled, reports are generated automatically as CSV files for the selected report intervals and stored in /opt/CSCOppm-gw/reports.
  - DB—If enabled, report statistics are collected and stored in the Prime Performance Manager database. Reports are visible in the Prime Performance Manager Reports window.

  Table 7-2 lists the report data options.

Table 7-2 Report Data Options

CSV	DB	Results
No	Yes	• Report statistics are collected and stored in the Prime Performance Manager database. Reports are visible in the Prime Performance Manager Reports window. • CSV files are not generated.
Yes	Yes	• Report statistics are collected and stored in the Prime Performance Manager database. Reports are visible in the Prime Performance Manager Reports window. • CSV files are generated.
Yes	No	• No report statistics are collected or stored in the Prime Performance Manager database. Reports are not visible in the Prime Performance Manager Reports window. • CSV files are generated.
No	No	• No report statistics are collected or stored in the Prime Performance Manager database. Reports are not visible in the Prime Performance Manager Reports window. • CSV files are not generated.

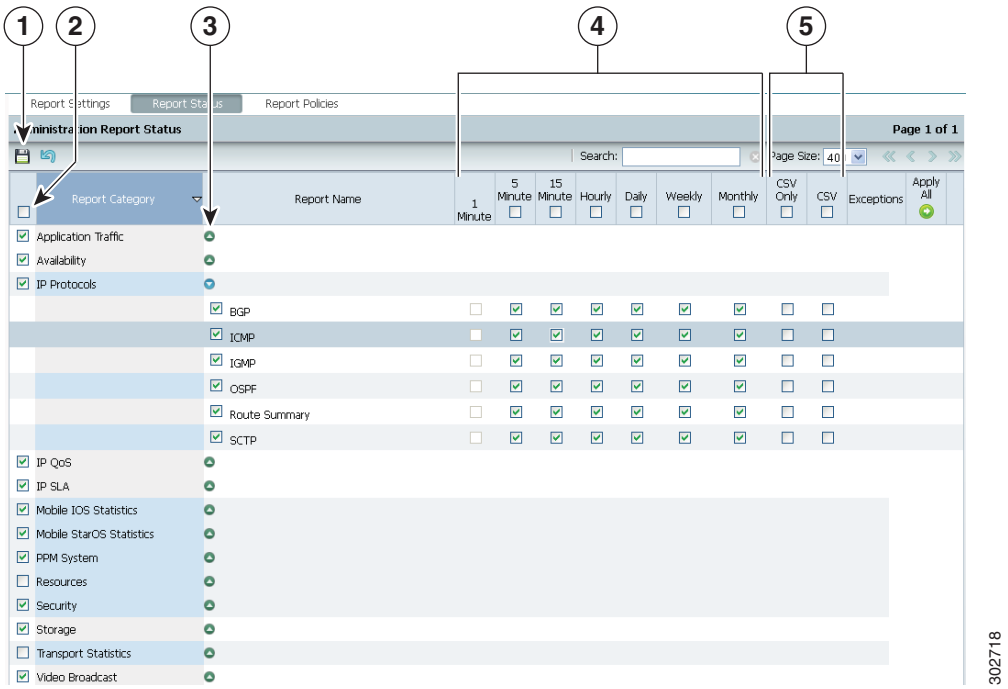
- Exceptions—Report settings can be set at the device level different from the ones set here. If so, an icon appears in this column. Clicking it displays the devices where report settings differ.

- Apply All—Applies the report category settings to all devices, overriding any report settings that might be set at the device level.

Step 4 Choose the report categories and intervals you want to enable or disable by clicking the check box to the left of each category, subcategory, or time interval. Checking or unchecking a report category automatically selects or deselects categories under it.

Step 5 When finished, click **Save Report Settings** in the Report Status toolbar.

Figure 7-6 Enabling Reports and Report Intervals



1	Save report settings	**4**	Report interval settings
2	Enable or disable report category	**5**	Database storage options
3	Display or hide subreports		

Note You can use the ppm statreps command to modify the report status from the CLI. For information, see ppm statreps, page B-73).

Capability Polling

The Prime Performance Manager capability polling feature polls devices to see what MIBs the device supports, then determines the reports the device is capable of supporting. Capability polling occurs once a day. It also occurs when users request a poll, or when a device is rebooted or has a configuration change, such as a new card installation.

By default, capability polling is enabled in optimized mode. This means capability polling is only conducted for device reports that are enabled at the master or individual device report levels. This means when you display individual device reports, only the reports that are enabled at the master or individual device report levels are displayed.

For performance, leaving capability polling optimization enabled is recommended. However, in certain scenarios, for example, in a lab environment where device configurations and capabilities change frequently for testing, you can use the ppm optimizecapabilitypoll command to disable capability polling optimization. This would allow users to see what set of reports could be enabled for a given device as well as the reports that are enabled. For information, see ppm optimizecapabilitypoll, page B-45.

Exporting Reports in 3GPP XML Format

CSV is the default format for exported Prime Performance Manager reports. You can change the format to 3rd Generation Partnership Project (3GPP) XML format. To change CSV to 3GPP XML:

Step 1 log into the Prime Performance Manager gateway server as the root user. See Root User Login, page 2-1.

Step 2 Enter the following commands:

```
/opt/CSCOppm-gw/bin/ppm statreps csvnames 3gpp
/opt/CSCOppm-gw/bin/ppm statreps expformat xml
```

Step 3 Open a Prime Performance Manager browser session.

Step 4 From the Performance menu, choose **Reports**, then click **Report/Group Settings**.

Step 5 Enable **Export Reports**.

Step 6 Click **Report/Group Status**.

Step 7 Verify that one or more report intervals and CSV are enabled.

Step 8 Allow time for reports to be generated, then display the 3GPP XML reports. Reports will have the following characteristics:

- All XML report files have an xml.zip extension.
- Each report has an XML header, file header and file footer. The file header and footer have the start and end time stamps for the reporting interval.
- Each device is enclosed in the <measData> </measData> tags and has a <granPeriod> tag.
- The <measTypes> tag encloses column names, excluding the key fields.
- The <measValue> tag encloses key names and values.
- The <measResults> tag encloses the column values in the same order as the column names enclosed within <measTypes>.
- The column names containing any of the following special characters, ' " & < >, are encoded in XML format. For example, "ppm5550a" and "ppm5580a" contain apostrophes that are encoded in the column/key values.

Creating 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 7-20
- Creating a New Report Policy, page 7-21
- Assigning Devices to Report Policies, page 7-21

Editing Report Policy Parameters

By default, all devices are assigned to a report policy created for the device type. To edit the parameters of an existing report policy:

Step 1 Log into the Prime Performance Manager GUI as the system administrator user.

Step 2 From the Administration menu, click **Report Policies**.

Step 3 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 4 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 5 On the Report Policy toolbar, click the **Save Report Policy** tool.

Creating a New Report Policy

To create a new report policy:

Step 1 Log into the Prime Performance Manager GUI as the administrative user.

Step 2 From the Administration menu, click **Report Policies**.

Step 3 On the Report Policy Editor toolbar, click the **Add Report Policy** tool.

Step 4 In the Save Report Policy dialog box, enter the report policy name.

Step 5 Click **OK**.

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

Step 7 Complete the "Editing Report Policy Parameters" procedure on page 7-20 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 system administrator user.

Step 2 From the Network menu, choose **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**.

Displaying Report Definitions

Prime Performance Manager cover many networking devices and technologies. To view the underlying XML definitions for a report, from the Help menu, choose **Reports**, then click **Report XML Definitions**. The README-Reports-system.html file is displayed. It provides the MIB tables and the fields that are polled to retrieve data from the device. It also describes the fields that are mapped to the report columns.

README-Reports-system.html is located in the /opt/CSCOppm-gw/etc/pollers/system or /opt/CSCOppm-gw/etc/pollers/user directories. Administrator access is required to edit the report definitions.

Should the provided Prime Performance Manager reports not meet all of your needs, you can create new ones using the provided reports as examples. For information about creating new reports, see the *Cisco Prime Network 1.3 Integration Developer Guide*.

Note In instances where a user file and a system file for the same report exist, the user file has priority.

Displaying Data Center Reports

Prime Performance Manager supports many data center networking, computing, storage, virtualization, and management devices and technologies. To display data center reports, from the Performance menu, choose **Views**. Supported data center devices and technologies are displayed in a Data Center view. Table 7-3 lists the data center devices and technologies that Prime Performance Manager supports.

Table 7-3 Supported Data Center Devices and Technologies

Category	Device/Technology	Chassis Components	Card/Interface Components
Network	Cisco ASR 9000	Supervisor card, line cards, routes, and neighbors	interfaces, ports
	Cisco ASR 1000	Same as Cisco ASR 9000	
	Cisco Nexus 7000 VDC	Supervisor card, line cards, VLAN, Interfaces, ports channels, vPC peer members	interfaces, subinterfaces, VLANs
	Cisco Nexus 5000	Same as Cisco Nexus 7000	
	Cisco Nexus 3000	+ route table size. ECMP variance and LPM statistics	
	Cisco Nexus 1000	Supervisor card, VLANs	VEM
	Cisco Nexus 1010	Same as Cisco Nexus 1000	
	Cisco Catalyst 6500 VSS	Supervisor card, line cards, and service module	interfaces, subinterfaces, VLANs
	Cisco Catalyst Firewall Service Module	Contexts	connection counts, translation counts (global and per context)
	Cisco ACE 20/30	Contexts	connection counts at global level and per context level
	Cisco ACE 4712	Contexts	

Table 7-3 Supported Data Center Devices and Technologies (continued)

Category	Device/Technology	Chassis Components	Card/Interface Components
	Cisco ASA 5500	Supervisor card, modules	VPNs
Compute - Physical Devices	Cisco UCS 6100	+hosts, VMs, cluster and per chassis	per VM, CPU, memory, disk, buffer, I/O, process
	Cisco UCS 5000	hosts and VM per chassis	
	Cisco UCS B Series	hosts and VM per chassis	
	Cisco UCS C Series	per chassis	
	Fabric InterConnect switches: • Cisco 6100, 6200 Series	per chassis	
	Other blade servers (IBM, HP, and othes)		
	Bare metal servers	per server	
Compute Logical/Virtual Devices	VMWare • vCenter • ESXi		host/VM CPU, memory, disk and network reports
	Hyper-V		
	KVM		
	Xen		
Storage	Cisco MDS 9000	Supervisor card, line cards, power supply, fans, VSANs, zoning	Storage ports, host ports, ISL ports, NPV ports, VSANs
	EMC	• Capacity and volumes • Storage pools • LUNs	
	NetApp	• Capacity: – Used – Available in aggregates – Spare disks • Uptime • CPU Utilization • I/O Throughput • Protocol Latency	• Volumes: used/available • Shares • Exports • LUNs • Quotas • Aggregates • Disks
Integration	Northbound interface		

In the Prime Performance Manager GUI, data center features are listed under Views and Reports.Under Views, a default Data Center view is provided. It includes:

- Network
  - VDC

  - VSS
  - Routers/Switches
- Compute
  - UCS Clusters (includes the hosts/VMs to blade server mapping)

Under Reports, the following data center report categories are provided:

- Data Network Services:
  - ACE
- Hypervisors
  - Hyper-V
  - KVM
  - VMWare (includes ESXi and vCenter
- Xen
- Security
  - FWSM
- Storage
  - EMC
  - NetApp
  - VSAN Zoning

UCS Clusters

  - UCS Chassis (includes UCS Blade)
  - UCS Fabric InterConnect
- Virtualization
  - VDC

Setting Up Bulk Statistics Reports

Prime Performance Manager retrieves report data for most devices using SNMP to poll the device MIBs containing the performance data. Some devices, such as the Cisco ASR 5000 and Cisco ASR 5500, provide less SNMP support and few MIBs, so few statistics can be gathered using SNMP. However, you can generate reports for these devices using bulk statistics. Bulk statistics are statistics collected in a groups, called schemas, at regular intervals. The device sends the schemas to a specified location as comma separated value (CSV) files. Prime Performance Manager picks up the files and generates the reports. Each schema contains many performance data variables called counters.

The Cisco ASR 5000 and ASR 5500 devices can be configured to collect bulk statistics and FTP them to a collection server (remote folder). To generate reports from the bulk statistics, you must configure the device to generate the bulk statistics in the specific format expected by Prime Performance Manager and set up Prime Performance Manager so it can read the CSV files generated by the device.

To set up Prime Performance Manager for bulk statistics:

Step 1 Following instructions in the device documentation, configure devices to FTP bulk statistics files to either the Prime Performance Manager unit server or a SAN directory.

Step 2 Complete the "Creating the Device Bulk Statistics Configuration" procedure on page 7-27 to generate the device configuration. The procedure generates the bulk statistics in the format Prime Performance Manager expects.

Step 3 Copy the generated configuration to all the required devices. Prime Performance Manager does not configure the devices automatically, so you must copy the configuration file manually.

Note You do not need to configure all the schema types generated by the command. However the reports will have data only for the schemas that are configured.

Note If the drop directory is a SAN directory, the Prime Performance Manager unit must have read and write permissions to it.

Step 4 Verify the bulk statistics samples are received at the drop directory.

The drop location for the files is configured in the device config using the CLI "remotefile" format. Verify the devices actually FTP the bulk statistics CSV file to this location. If files are not received at the drop directory, verify the directory has the proper permissions and the login user name and password provided in the device configuration is valid.

Tip Perform a save configuration from the device to the drop directory. If save configuration works successfully, the bulk statistics samples should FTP without issues.

Step 5 Open the bulk statistics samples and verify the counter names are complete.

The example schema definitions below show incomplete counters at the end.

```
PPM,system,systemSch55,1349867400,20121010,071000,1702713,0,,%d
PPM,system,systemSch56,1349867400,20121010,071000,1702713,,0,%disc-reason
PPM,system,systemSch6,1349867400,20121010,071000,1702713,,,,,0,606734,%sess-s
```

Tip Incomplete counters in the bulk statistics samples often occur when you copy too many configuration lines to the device at the same time. Devices have a buffer limit on the number characters that can be pasted to it at one time. If you experience incomplete counters, configure a smaller number of lines at a time.

Bulk statistics samples with complete counter names enclosed within % symbols are acceptable. These are counters that are obsolete and not supported in the current Star OS version. Prime Performance Manager ignores these counters and used the default data type value for processing. For example, %cpu3-cpuused-user% is an obsolete or unsupported counter in the following:

```
PPM,card,cardSch3,1346768700,20120904,142500,928325,1,0,0,0,%cpu3-cpuused-user%,0.00,0.00,
0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,
```

Step 6 Set the drop location on the unit server, by entering:

```
/opt/CSCOppm-gw/bin/ppm csvdrop [dir]
```

When you install the unit, the default drop directory location is /opt/CSCOppm-unit/csvdrop/. Use the ppm csvdrop command to point to the directory where bulk statistics samples are received from the Cisco ASR 5000 and Cisco ASR 5500 devices. The command updates the CSV_DROP_DIR property in BulkStats.properties located in /opt/CSCOppm-unit/properties. Restarting the unit is not necessary; the property changes takes effect automatically.

Use the same drop directory for all Cisco ASR 5000 and Cisco ASR 5500 devices in the network. The %host% variable in the filename helps to uniquely identify each device.

Step 7 Discover devices and check for alarms in the Alarms/Events window. For information about device discovery, see Chapter 5, "Discovering Network Devices." For information about the Prime Performance Manager alarms management, see Chapter 9, "Managing Network Alarms and Events."

Prime Performance Manager might raise bulk statistics alarms. See Bulk Statistics Alarms, page 7-29 for alarm descriptions and actions to resolve them. The unit console and message log files in /opt/CSCOppm-unit/logs/ are also be a good place to view possible errors.

Step 8 Verify the Prime Performance Manager CSV Bulk Stats status for each device:

a. From the Network menu, choose **Devices**.

b. Click the link for each device configured for bulk statistics.

c. On the device window, click **Data Collection**.

d. In the Collector Status area, the CSV Bulk Stats item displays one of the following statuses:

- Active—The device is configured for bulk statistics and the unit is receiving the files regularly.
- Not Active—The device is configured for bulk statistics but it might not be discovered or some files are skipped.
- Not Configured—The device is not configured properly or bulk statistics are not supported for the device type.

Prime Performance Manager processes new files in the drop directory when they arrive. If the file name format is valid, Prime Performance Manager processes the new files for enabled Star OS reports.

If parameters are missing in the file name or the headers and footers in the bulk statistics samples do not match the property file values, marker files are created in the drop directory. The files have zero size and have the same name as the file in error but are appended with an error extension.

If multiple sample files are collected in the drop directory, Prime Performance Manager processes from the oldest to latest sample. Prime Performance Manager processes about 50 files at a time until it catches up with the recent files. Daily statistics can be looked up for older time range if necessary.

Note To process more than 50 files, edit the BulkStats.properties file and change MAX_FILE_COUNT. Increasing the number may cause performance issues depending on the number of devices discovered on the unit.

Step 9 Verify the device reports by choosing **Reports** from the Performance menu and scrolling to the Mobile StarOS Statistics reports in the navigation tree. If the Star OS reports lack data, complete the following steps:

a. Verify that the report is enabled at the network and device level. To check the network level, from the Administration menu, choose **Report Status**. To check at the device level, select a device and click the **Report Status** tab.

b. Verify the particular schema is configured on the device. Prime Performance Manager server might also be processing a backlog of files in the drop directory, check for data for longer durations.

c. Verify the device StarOS[tm] software version. The StarOS version for Cisco ASR 5000 and ASR 5500 devices is taken from the bulk statistics files. You can view the version by displaying the device, then clicking the **Details** tab. If the version is Unknown, verify if you have the system schema 71 configured on the device. This is the schema line where version information is taken from. The schema systemSch71 format is:

```
PPM,system,systemSch71,%epochtime%,%localdate%,%localtime%,%uptime%,%disc-reason-490%,
%disc-reason-491%,%disc-reason-492%,%disc-reason-summary%,,,,,%swversion%,%peak-cpuusa
ge%,%peak-memusage%,,%system-capacity-usage%,%session-capacity%,%session-capacity-usag
e%,%npu-capacity%,%npu-capacity-usage%,%sess-max-lastreset-time%,,,,
PPM,system,systemSch71,1349964000,20121011,100000,3595,0,0,0,,,,,,14.0,15.61,11291412.
00,,0.06,10137600,6095,1207959552,608208,Never,,,,
```

Creating the Device Bulk Statistics Configuration

The ppm starbuild command builds the StarOS bulk statistics device configuration with the desired schemas and counters. Prime Performance Manager requires bulk statistics files to be in a very specific format. This command generates the device configuration in the format that Prime Performance Manager expects. The command generates the configuration that you must copy to the Cisco ASR 5000 and Cisco ASR 5500 devices. The command format is:

```
/opt/CSCOppm-gw/bin/ppm starbuild <schemafilename>
```

The input, *schemafilename*, is the CSV file with the bulk statistics schema and counters that need to be configured on the devices. Prime Performance Manager includes a full schema file for StarOS 14.0 that supports all the EPC counters. It is located in the install directory:

/opt/CSCOppm-gw/install/ASR5K_BulkStats_Schemas_Counters-staros14-epc.csv

Prime Performance Manager expects the filenames to be in the following format:

```
%host%_bulkstats_%localdate%_%localtime%_%localtz%_5_5.csv
```

%host%, %localdate%, %localtime%, %localtz% are common bulk statistics counter variables.

Prime Performance Manager uses the %host% variable to identify the device. This is usually the device sysName. The "_5_5" at the end of the file name is the sample and transfer interval set on the device.

To build the StarOS device configuration:

Step 1 log into the gateway as an administrator user.

Step 2 Enter the ppm starbuild command using the provided StarOS 14.0 schema file for the *schemafilename*:

```
/opt/CSCOppm-gw/bin/ppm starbuild
/opt/CSCOppm-gw/install/ASR5K_BulkStats_Schemas_Counters-staros14-epc.csv
```

Step 3 Enter the IP address of Prime Performance Manager unit where the Cisco ASR 5000 and Cisco ASR 5500 devices are discovered, or the SAN folder location IP address.:

```
Enter the IP Address of Prime Performance Manager unit To Send Files To:
```

Step 4 Enter the path to the file directory where you want the device to drop the CSV files. This is usually a folder mounted on SAN. The bulk statistics files are retained for 14 days by default in this directory. The full path to the folder is provided here.

Note Note: If you need to change the default 14 days bulk statistics age use ppm bulkstatsage command.

```
Enter File Directory On Prime Performance Manager unit To Drop Files To:
```

Step 5 Enter the output file name. This can be any valid filename. The output configuration file is created in /opt/CSCOppm-gw/bin/ folder by default.

```
Enter Output Filename To Write StarOS 14.0 Config To: staros14-bulkstats-config.txt
```

Note You can simply press Enter to the prompts and change the values by editing the generated output file later.

Removing Bulk Statistics Device Configurations

To remove bulk statistics configurations from a device on a per schema basis:

Step 1 log into the gateway as an administrator user.

Step 2 Enter the following command:

```
/opt/CSCOppm-gw/bin/ppm starbuild
/opt/CSCOppm-gw/install/ASR5K_BulkStats_Schemas_Counters-staros14-epc.csv -no
```

The output configuration file is created in /opt/CSCOppm-gw/bin/ folder by default. The file contains the delete CLIs for all the available schemas.

Adding New Bulk Statistics Schemas or Counters

If config needs to be generated for a smaller subset of schemas or if new schemas need to be added, modify the spreadsheet included in the install directory.

```
/opt/CSCOppm-gw/install/ASR5K_BulkStats_Schemas_Counters-staros14-epc.xlsx
```

After the changes are complete, update the CSV file in the install folder by saving the spreadsheet in comma separated format and execute the ppm starbuild command to generate the revised configuration.

Note If counters within a schema counters must be removed, mark the Export column as “no” in the spreadsheet. This generates the configuration with consecutive commas (,,,,) to maintain the counter position in the schema.

Updating the Prime Performance Manager Bulk Statistics Schema File

To add a new schema or counter to an existing Prime Performance Manager report or to a new report, you must update the gateway schema file. Prime Performance Manager looks up this schema file to identify the format in which the devices are configured.

Note You only need to generate the Prime Performance Manager schema file when new counters need to be used in reports.

To generate the schema file for Prime Performance Manager:

Step 1 log into the gateway as the administrator user.

Step 2 Enter the ppm starbuild with the -ppm option:

```
/opt/CSCOppm-gw/bin/ppm starbuild
/opt/CSCOppm-gw/install/ASR5K_BulkStats_Schemas_Counters-staros14-epc.csv -ppm
```

Step 3 Enter the output file name:

```
Enter Output Filename To Write PPM Schema:staros14-ppm-bulkstatsschema.csv
PPM Schema File Written To: staros14-ppm-bulkstatsschema.csv
```

The output schema file is created in /opt/CSCOppm-gw/bin/ folder by default.

Step 4 Copy the file to the etc gateway directory and save it as bulkstatsschema.csv:

```
/opt/CSCOppm-gw/etc/bulkstatsschema.csv
```

Step 5 Reload the new schema file:

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

Bulk Statistics Alarms

Bulk statistics alarms you might see are listed below. You can view BulkStats.properties in /opt/CSCOppm-unit/properties to see values shown in the alarm generation.

- BulkStatsInfo Alarm - Files available but node not discovered.

  This is an Informational alarm. Examples:

  ```
  Unit: ppm-ucs-vm13 - Bulk Statistics available for RTPZ5SVCGW01 but device not
  discovered.
  ```

- BulkStatsInfo Alarm - File name parameter is missing/invalid.

  This is an Informational alarm. If parameters are missing in the file name, Prime Performance Manager stops processing the file. New files with zero size are created in drop directory with same name as the original file appended with extension, skipped. Examples:

  ```
  Unit: ppm-ucs-vm13 - Missing parameters in filename:
  _bulkstats_20120419_152500_EDT_5_5.csv Missing Hostname.

  Unit: ppm-ucs-vm13 - Missing parameters in filename:
  Prime5k_bulkstats_20sds120419_155500_EDT_5_5.csv Unparseable date:
  "20sds120419155500EDT" format:yyyyMMddHHmmssz value: 20sds120419155500EDT.

  Unit: ppm-ucs-vm13 - Missing parameters in filename:
  Prime5k_bulkstats_20120419_160000_EDT.csv Mising Sample Interval.
  ```

  If necessary the following properties can be modified in BulkStats.properties

  FILENAME_SUBSTR = _bulkstats_

  FILENAME_DELIMITER = _

DATE_VARIABLE_FORMAT = yyyyMMdd

TIME_VARIABLE_FORMAT = HHmmss

- BulkStatsInfo Alarm - Files with no header or no footer information.

  The header is the first line in the bulk statistics samples. A missing header indicates the file is incomplete. Cisco ASR 5000 and 5500 devices maintain a buffer while collecting the samples until the time when it can transfer the CSV file to the drop directory. The header is the first information stored in the buffer. If the buffer allocated on the device is too small for the sample and transfer interval, the old data in the buffer is overwritten, so the header and some collected data might be removed.

  The footer is the last line in the bulk statistics samples. A missing footer also indicates the file is incomplete. The file might be in the transfer process or FTP transfer issues might exist. The header and footer are required for processing. If necessary, the following properties can be modified in BulkStats.properties.

  HEADER_LINE_PREFIX = Version

  FOOTER_LINE_PREFIX = EndOfFile

  If header and footer is missing in the filename, Prime Performance Manager stops processing the files. New files of zero size are created in drop directory with same name as the original file appended with extension, noheader or nofooter. Examples:

  ```
  Unit: ppm-ucs-vm13 - Bulk statistics skipped. File
  Prime5k_bulkstats_20120419_161500_EDT_5_5.csv received with no header information.
  Unit: ppm-ucs-vm13 - Bulk statistics skipped. File
  Prime5k_bulkstats_20120419_161500_EDT_5_5.csv received with no footer information.
  ```

  If a footer is unavailable, Prime Performance Manager waits for a specified interval to see if the transfer gets completed. If no footer exists after the specified interval, Prime Performance Manager creates the zero size file and raises the NoFooter alarm. If necessary the following property can be BulkStats.properties to control the wait duration:

  FOOTER_WAIT_TIME = 3

- BulkStatsError Alarm - Device is Discovered but there are no files available.

  This is a Major alarm. Check if the drop directory is correct in BulkStats.properties. Also check device configurations. Example:

  ```
  Device 172.18.53.231 has no bulk statistics.
  ```

- BulkStatsError Alarm - Device missing 1-5 files.

  This is a Minor alarm. Check if device is being reloaded. Example:

  ```
  Device 172.18.20.166 failed to receive 4 bulk statistics. Last received time is Apr
  19, 2012 5:12:00 PM.
  ```

- BulkStatsError Alarm - Device missing more than 5 files.

  This is a Major alarm. Examples:

  ```
  Device 172.18.20.166 failed to receive 17 bulk statistics. Last received time is Apr
  19, 2012 5:39:57 PM.
  ```

- BulkStatsError Alarm - When files are received after a period of failure.

  This is a Normal alarm. Examples:

  ```
  Device 172.18.53.231 receives bulk statistics as of Apr 19, 2012 5:12:00 PM.
  ```

- BulkStatsError Alarm - Several devices missing more than five files.

This is a Major alarm. Examples:

```
Unit ppm-ucs-vm13 - 2 devices failed to receive bulk statistics. Devices are:
Prime5k,RTPZ5SVCGW02,
```

If necessary, modify the following properties in BulkStats.properties to control when to raise alarms.

MINOR_ALARM_COUNT = 1

MAJOR_ALARM_COUNT = 5

NODES_FAIL_COUNT = 5

Managing 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 ICMP hourly packet rates, total errors, total echoes, and echo replies. The CPU/Memory dashboard presents the hourly CPU average and peak utilization as well as the top *nn* hourly memory pool average and peak utilization. Many dashboards are provided with the Prime Performance Manager package. High-level dashboard categories include:

- Application
- Availability
- IP Protocols
- IP QoS
- IPSLA
- Network Health
- Resource
- Response Time
- Server Health
- Transport
- VPDN Statistics
- Video Broadcast

Because dashboards are presented in graph output, only the top 10 report items are presented. You can change this number with the ppm topxxsize command. For information, see ppm topxxsize, page B-77.

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

Displaying Dashboards Status

Be default, all Prime Performance Manager dashboards are enabled. System-level dashboards depend upon the regular report to define what data to poll and monitor for the dashboard report. This is done by the regular report that the dashboard draws from. Disabling the report that actually defines the data for the dashboard will cause that data to stop being gathered, so the dashboard will only have data up to the time that the associated report was disabled. However, you can create a poller definition within the dashboard XML to enable the dashboard to draw the data independently from any reports.

You cannot enable or disable dashboards from that dashboard status page. The Dashboard Status page is a static list showing you which dashboards are on or off. The dashboard state is based on the status of its reports. If none of the reports used for the dashboard are enabled, the dashboard is disabled automatically.

To display dashboard status:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Performance menu, click **Dashboards**.

Step 3 In the Dashboard Status Table, enabled dashboards contain a check in the box next to the dashboard title.

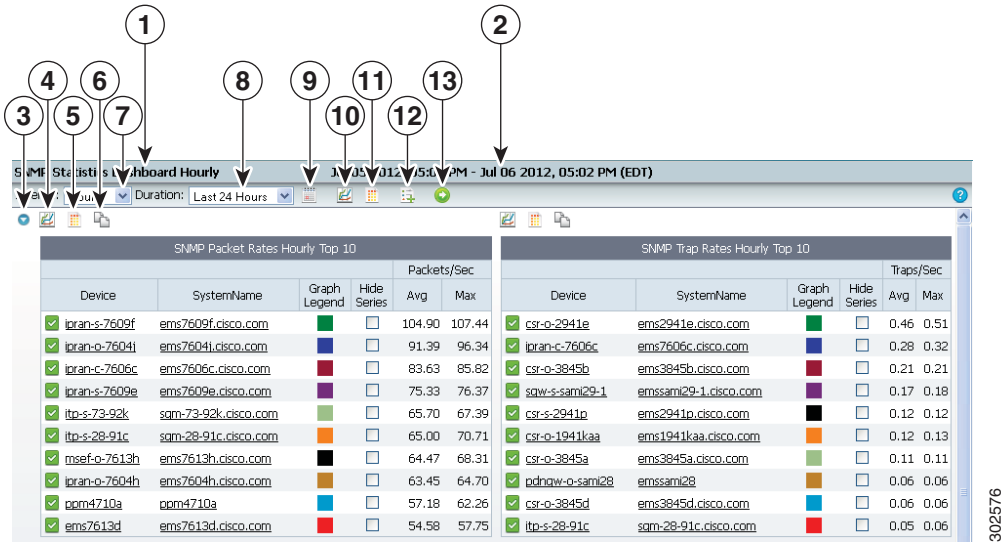
Editing Dashboard Display

You can change the dashboard information display using options in the Dashboard menu bar, shown in Figure 7-7. Menu bar items include:

- Interval—Dashboard intervals are: Hourly, Daily, Weekly, Monthly.
- Duration—Allows you to choose the dashboard report duration. The duration options depend on the dashboard report interval:
  - 5 Minute—Last 6 hours, 24 hours, 3 days, 7 days.
  - 15 Minute—Last 12 hours, 24 hours, 3 days, 7 days, 14 days.
  - Hourly reports—Last 12 hours, 24 hours, 3 days, 7 days. 14 days, 21 days, 30 days, current month, previous month.
  - Daily reports—Last 7 days, 14 days, 21 Days, 30 days, 6 months.
  - Weekly reports—Last 30 days, 60 days, 90 days, 6 months, 1 year.
  - Monthly reports—Last 90 days, 6 months, 1 year, 5 years.
- Customize Date and Time Range—Allows you to create a report with a customized date and time range. The maximum custom time periods are:
  - 5 Minute—Three days.
  - 15 Minute—Seven days.
  - Hourly reports—Seven days.
  - Daily reports—31 days.
  - Weekly reports—One year.
  - Monthly reports—Five years.
- Graph Mode—Displays all the dashboard parameters in chart format. For readability in this format, only the top *nn* items are displayed.
- Table Mode—Displays all the dashboard parameters in table format.
- Toggle Legends—For reports displayed in graph format, this tool allows you to turn the graphical legend on and off.
- Run Selected Report—Runs the report after you modify any report parameters in the menu bar.

- Help for Report—Displays a text file with the MIB variables that are polled for generating the selected report, including any calculations that are performed. This text file also has links to the associated report XML files.

Figure 7-7 Dashboard Menu Bar



1	Dashboard title	**8**	Duration
2	Dashboard time period	**9**	Customize the Date and Time
3	Display/hide graph row.	**10**	Graph Mode for all dashboard parameters
4	Graph Mode for the individual dashboard parameter.	**11**	Table Mode for all dashboard parameters
5	Table Mode for the individual dashboard parameter.	**12**	Toggle legends option
6	Interval	**13**	Run the Report option
7	Copy chart to clipboard		

To change a dashboard display:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Performance menu, choose **Dashboards**.

Step 3 In the Performance Reports navigation area, click **Dashboards**.

Step 4 In the Dashboard navigation tree, navigate to the dashboard category that you want to modify.

Step 5 As needed, perform any or all of the following modifications by choosing items on the dashboard menu bar (Figure 7-7):

- Click **Interval** and choose a different interval: Hourly, Daily, Weekly, or Monthly.
- Click **Duration** and choose a different time period for the dashboard: the last 12 (default) or 24 hours, or the last 3, 7, 14, 21, or 30 days. The list of available durations depend upon the interval that is selected.

- Click **Customize Date and Time** and choose a custom start and end date and time for the dashboard. Use this option if the default Duration time periods do not meet your needs. The maximum time period you can specify depends on the report interval selected.
- Click **Graph Mode** to display all the dashboard parameters in chart format.
- Click **Table Mode** to display all the dashboard parameters in table format.

Note The View Chart and View Report tools appear above each dashboard parameter so you can change the display of individual dashboard parameters.

- For graph format, click **Toggle Legends** to turn the graph legend on and off.

Step 6 When finished, click **Run the Selected Report** (green arrow) to run the report with the modified parameters.

Step 7 Within each individual dashboard report, you can do the following:

- Click the **Graph Mode** and **Table Mode** tools to switch between graphical chart and report table displays.
- In report table display, check **Hide Series** for any report items you do not want displayed in the graph, then click **Graph Mode** to view chart with the selected items hidden.
- Click **Hide this row of graphs** to hide or display individual graph rows.
- Click **Copy to clipboard** to copy a graph to the Prime Performance Manager clipboard where it can be pasted into a custom report view. (See Creating and Managing Custom Report Views, page 7-34.)

Creating and Managing Custom Report Views

Prime Performance Manager allows you to create custom report views, for example, to monitor a particular function on selected devices or interfaces. You can attach devices to custom views and view all device information from menus within the view.

Creating and managing custom report views are described in the following topics:

- Creating a Custom Report View, page 7-34
- Copying and Pasting Views, page 7-36
- Modifying Custom Report Views, page 7-37
- Merging View Charts, page 7-40
- Editing Views, page 7-40

Creating a Custom Report View

You can create a custom report view to monitor specific performance data and functions across selected devices and interfaces. These charts and tables update automatically to show the most recent data from the server.

To create a custom report view:

Step 1 From the Performance menu, select **Views**.

Step 2 In the View Editor window toolbar, click the **Create a New View** tool.

Step 3 In the Add View Entry dialog box, enter the following information:

- **View Name**—Enter the custom view name.
- **Editable**—Check this box if you want other users to have the ability to modify the view.
- **Visible**—Check this box if you want the custom report view to be viewed by other users.
- **Device**—If you want to add a device to the view, enter the device hostname or IP address. Adding devices to the view allows you to view device information from within the view including device details, reports, alarms and events,

Step 4 Click **OK**.

The new custom report view appears in the View Editor window with the text, "No entries found."

Step 5 Display the the data that you want to add to the custom view:

a. From the Performance menu, choose **Reports**.

b. Navigate to the report containing the data you want to add. You can navigate to reports, dashboards, grouped reports, and other views that have graphs defined within them. You can also copy device or group level data and maintain whatever filter or series selections you apply to the report.

Step 6 If the report is not displayed in graph output, in the toolbar Output Mode, choose **Graph**.

Tip You can filter the report before you copy it and bring only the filtered report data to your custom view. For information about report filtering, see Filtering Report Information, page 7-13.

Step 7 Scroll to the graph that you want to add and click the **Copy to Clipboard** tool.

Step 8 From the navigation area, click the custom report view you just created.

Step 9 On the custom report view toolbar, click **Paste Charts from Clipboard**.

You can copy multiple graphs to the clipboard before you need to click the Paste Charts from Clipboard. so you do not need to go back and forth. For example, you can copy six charts from six individual reports, then paste them into the view at one time.

Step 10 Repeat Steps 5 through 9 until you have added report data.

Step 11 To modify custom report display, continue with the "Modifying Custom Report Views" procedure on page 7-37.

Alternately, you can copy a view that already exists by clicking **Copy this view**. This creates a copy of the view, except you are the new view owner (current user).

Adding Views to the Navigation Tree

Views navigation tree behavior differs from the Reports, Dashboards, and Groups navigation trees because of the following:

- Any user can manually create multiple views.
- Prime Performance Manager includes a Data Center view. This is a special view built and maintained by Prime Performance Manager. (For information about the Data Center view, see Displaying Data Center Reports, page 7-22.)

- Users with the edit view privilege (network operator user and above) can copy the Data Center view and make changes to the copy.
- Views can contain many subviews and many reports and devices.
- Views have a visibility attribute that allows you to hide views from other users.

You generally will only open one view because that view represents the way you want to see the devices and reports are laid out hierarchically. When you select Views in navigation tree, a list of views you are allowed to see is presented in the content area. To display the views in the navigation tree, click **Views**, then click the folder icon of the view you want to add. Prime Performance Manager adds the view to the navigation tree.

If user access is enabled, you only need to perform this step once per user. If user access is not enabled, the user is the hostname of the device communicating with Prime Performance Manager. Whenever you switch hostnames, for example, if you go from wired to Wi-Fi, or from office to home, Prime Performance Manager will consider you a different user and you will need to repeat the step.

Copying and Pasting Views

An alternate method for creating new views is to copy an existing view and paste it into another one. This is often easier if an existing view will meet your needs with some modifications.

To copy and paste a view:

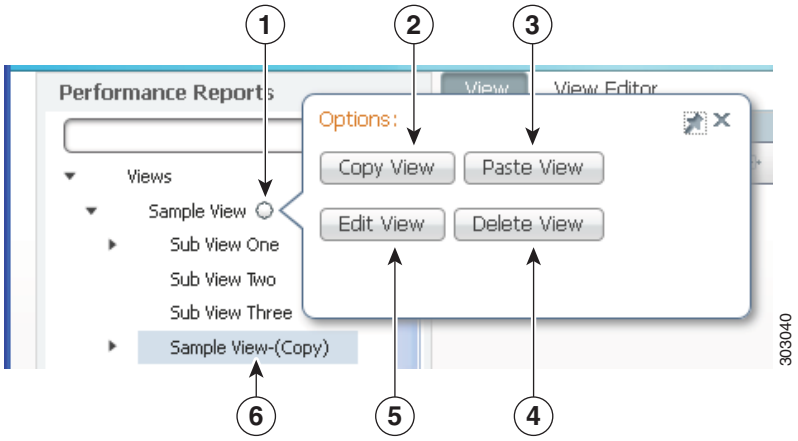
Step 1 Highlight the view or subview you want to copy and click the options icon. The options icon is a circle located to right of the view title.

Step 2 From the Options menu, click **Copy View**.

Step 3 Navigate to the view where you want to paste the view, click the options icon next to it and choose **Paste View**.

The view appears in the new location with the name [*view name*}-Copy, as shown in Figure 7-8.

Figure 7-8 Copying and Pasting Views



1	Copy and Paste View options icon	**3**	Edit View
2	Copy View	**4**	Delete view
3	Paste View	**5**	Pasted view

To modify the copied view, see Modifying Custom Report Views, page 7-37 and Editing Views, page 7-40.

Modifying Custom Report Views

After you create a custom report view, you can modify the data display and change the custom report configuration from the View and View Editor tabs.

To modify a custom report view:

Step 1 From the Performance menu, select **Views**.

Step 2 In the navigation area, choose the custom report view or subview that you want to modify.

Step 3 From the View tab toolbar, shown in Figure 7-9, perform any of the following changes to the reports contained in the view:

- Click **Home** to make the view your home view. After you click it, "(Home View)" appears in the view title, and this view appears when you click the main menu Home icon. (See Figure 3-2 on page 3-4.)
- Click **Paste Charts from Clipboard** to paste report charts copied from other reports.
- Click **Columns** to change the graph width, from 1 to 3 columns. 2 is the default.
- Click **Show/Hide Chart Legends** to display or hide legends from the report graphs.
- Click **Enable Compact Mode** to reduce the graph size and see more graphs within the same screen area. Enabling compact mode can be useful when trying to see patterns among multiple charts.
- Click **Merge Selected Charts** to merge two or more selected charts. See Merging View Charts, page 7-40.
- Click **Lock this Page** to prevent the report from being updated; click **Unlock this Page** to allow updates. This function is provided when continual, automatic updates are not needed.
- Click **Refresh** to manually update all the graphs and tables in the page.

Step 4 From each report chart toolbar you can perform any of the following changes:

- **Drag to Reorder Items**—Click and drag the chart to a new location within the view.
- **Fullscreen Graph**—Displays the chart in full screen.
- **Delete**—Deletes the report item from the report.
- **Graph Mode**—Displays the report item in chart view.
- **Table Mode**—Displays the report item in table view.
- **Comparative View**—Displays a full-screen comparative view of the report, for example a 15-minute and hourly comparison.

- **Edit**—Displays the Edit Report Properties dialog box where you can modify the chart name and add or edit a subtitle.
- **Copy to Clipboard**—Copies the report to the Prime Performance Manager clipboard to allow you to paste it into other views.
- **Select this Graph**—Selects the graph. The function allows you to select multiple charts and merge them into one graph using the Merge Selected Charts tool.

Note If Compact Mode is enabled, the chart toolbar is not displayed.

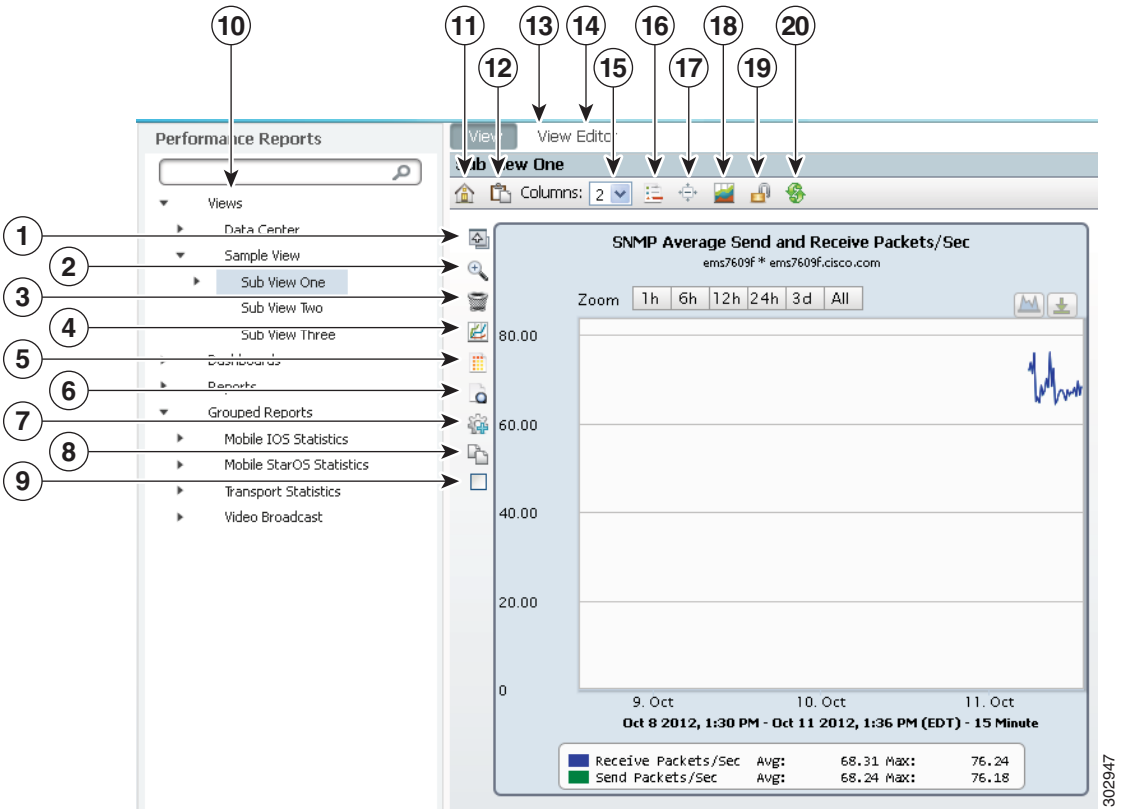
Step 5 If devices are attached to the view, the following device menus are displayed:

- Reports
- Dashboards
- Details
- Event History
- Active Alarms
- Report Status
- Availability
- Star Graphs

For descriptions of the device menus, see Displaying Individual Device Information, page 8-17.

Figure 7-9 shows the custom report options in the View tab.

Figure 7-9 View Tab



1	Reorder tool	**11**	View tab
2	Show full screen tool	**12**	View Editor tab
3	Delete tool	**13**	Home view tool
4	Chart mode tool	**14**	Paste charts tool
5	Table mode tool	**15**	Column editor
6	Comparative view tool	**16**	Chart legend display tool
7	Edit tool	**17**	Compact Mode
8	Copy to clipboard tool	**18**	Merge charts
9	Select chart	**19**	Page lock
10	View menus	**20**	Refresh

Merging View Charts

Merging charts in views can be useful to create a composite view of similar data within similar times. For example, charts for TE tunnels between two provider edge (PE) devices could be merged into one chart to give a composite view of traffic between the two PEs, for example:

ifInOctects TE_Tunnel_1000_PE_A__PE_B

ifOutOctects TE_Tunnel_1000_PE_A__PE_B

ifInOctects TE_Tunnel_1001_PE_B__PE_A

ifOutOctects TE_Tunnel_1001_PE_B__PE_A

To merge charts:

Step 1 Display the view containing the charts you want to merge.

Step 2 Click Select This Graph for each chart you want to merge.

Step 3 On the Views toolbar, click Merge Selected Charts.

Step 4 In the Edit Report Properties dialog box, enter the report name and, if desired, a subtitle, then click **Save**.

The merged report appears beneath the other charts.

When creating merged charts, keep the following points in mind:

- To maximize effectiveness, merged charts should be created from charts with similar data and time frames.
- Merged charts cannot be viewed in table mode.

Editing Views

By default, the Prime Performance Manager View Editor lists every available custom view, including views you created and views other users created with the Visible attribute turned on. Views that you created are open, and views other users created are closed.

To hide or display views, and perform other view management tasks:

Step 1 From the Performance menu, select **Views**.

Step 2 In the navigation area, choose the custom report view or subview that you want to modify.

Tip Alternatively, you can search for views from any View Editor tab by entering text strings. Views or subviews with text in their titles that match the search text titles will be displayed.

Step 3 Click the **View Editor** tab.

Step 4 As needed, modify the following:

- Name—Enter report name edits, if any.
- Editable—If checked, allows other users to modify the view.
- Visible—If checked, allows the custom report view to be viewed by other users.

- Device—To include a device, enter the device hostname or IP address. (Only one device can be attached to a view or subview.)

Step 5 To add a subview:

a. From the View Editor toolbar, click **Add Subview**.

b. In the Add Subview dialog box, enter the subview name and, if you want to attach a device, the device hostname or IP address.

c. Click **OK**.

Step 6 To delete, edit, or display a view, from the View Editor Actions column, click the following:

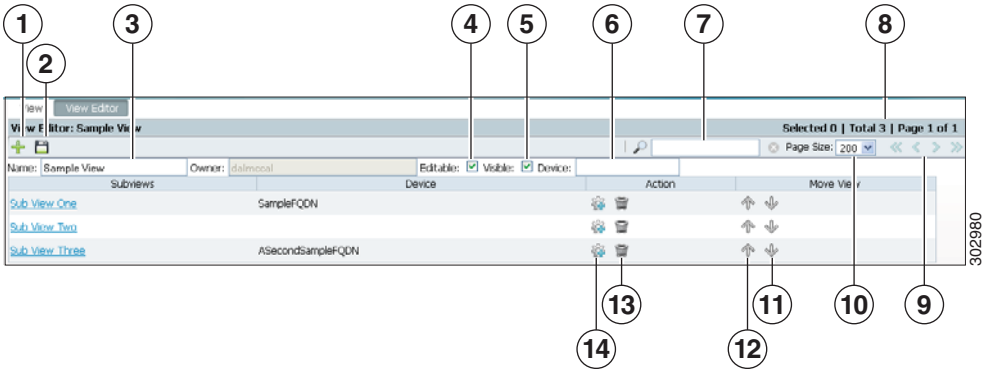
- **Delete This View** to delete the view or subview.
- **Edit This View** to display the selected view or subview in the View Editor.

Note Alternatively, you can choose Edit View or Delete View from the view context menu, shown in Figure 7-8 on page 7-36.

Step 7 To change the position of a view or subview, select the view then click the up or down arrow under the Move View column.

Step 8 When finished, click **Update View Information** on the view toolbar.

Figure 7-10 View Editor



1	Add view or subview	**8**	View page summary
2	Update view or subview information	**9**	View page scroll buttons
3	View name	**10**	Page size
4	Editable option	**11**	Move view/subview up
5	Visible option	**12**	Move view/subview down
6	Device attachment field	**13**	Delete view
7	Search	**14**	Edit view

Creating and Managing Report Groups

Prime Performance Manager allows you to generate reports based on groups of network objects, for example, devices, interfaces, CPUs, or a combination of devices and device elements. You create the group by providing a list of network objects that you want included, or by providing an algorithm that is used to search the network and return objects that meet the provided criteria.

Creating new groups requires you to create new group reports. Information for creating group reports is provided in the *Cisco Prime Performance Manager 1.3 Integration Developer Guide*. Prime Performance Manager includes example groups in four categories: Mobile IOS Statistics, Mobile StarOS Statistics, Transport Statistics, and Video Broadcast.

Group elements that you work with in the Prime Performance Manager GUI include:

- Group ID—Is assigned by Prime Performance Manager when a group is created. It uniquely identifies the group.
- Editable (true or false)—Indicates whether the group can be edited by other users. If true, users with the appropriate permissions can edit the group.
- Enabled (true or false)—Enables or disables the group. If true, the group processes the input data and returns the appropriate return values. If false, the group does not return any data.
- Name—Is assigned by the group creator. This is the group name displayed in the GUI.
- Algorithm—Defines the criteria Prime Performance Manager uses to search the network for objects. The algorithm is built from macros joined by standard operators, for example, +, =, >=, and others. The algorithm final output is true (the object meets the criteria and is included) or false (the object does not meet the criteria and is not included). For example, the following algorithm return devices with “To_Rome” or “To_Venice” in the interface descriptions:

  ```
  If(Contains(ifDescr,"To_Rome") || Contains(ifDescr,"To_Venice"),true,false)
  ```

- Objects—Is a list of objects by their Fully Qualified Domain Names (FQDNs) that map to objects within the Prime Performance Manager network. The object format is:

  Node=<host or IP>,<other keys as defined in the corresponding report XML file>

  Examples:

  ```
  Node=em1941kbf.cisco.com
  Node=10.74.125.210
  Node=em1941kbf.cisco.com,ifDescr=FastEthernet0/0
  Node=10.74.125.210,CPUSlot=0,CPUNum=0,processorIndex=1
  ```

  The objects contained in this list are included in the group processing. Objects are returned if they meet the criteria specified in the algorithm or items in the Objects list.

- Type—Is used to identify the report domain to users. For example, a group that filters data at the network level may specify a Network type, while a group that filters data for a particular region may specify a Regional type. Specifying the domain is useful when reviewing grouped report information.

The following topics describe how to create, manage, and display group reports:

- Creating a Report Group, page 7-44
- Creating Algorithms Using the Algorithm Editor, page 7-45
- Managing Report Groups, page 7-47
- Displaying Group Reports, page 7-48

Provided Groups

Prime Performance Manager includes sample groups that are shipped in the disabled state. You can use these as standalone groups to generate network-level statistics or you can copy them and add algorithms to aggregate similar objects at different level. For example,you might want to aggregate statistics to the network level as well as regional, group, or device levels.

Provided groups include:

- apn.xml—Aggregates the statistics for an APN (AccessPointName) to a network level on GGSN devices. An APN can be defined on multiple routers. This group aggregates APN statistics for all routers. It is defined on into a single statistic. This aggregation type reports, for example, the sum of the up stream traffic volume for the APN in the network. It requires the device to implement the MIB, CISCO-GPRS-ACC-PT-MIB.my.
- pdngwApn.xml—Aggregates the statistics for an APN to the network level on PDNGW devices. An APN can be defined on multiple routers. This group aggregates the APN statistics for all routers. It is defined into a single statistic. This type of aggregation reports, for example, the sum of active PDPs for the APN in the network. It requires the device to implement the MIB, CISCO-GPRS-ACC-PT-MIB.my.
- sgwApn.xml—Aggregates the statistics for an APN to a network level on SGW devices. An APN can be defined on multiple routers and this group will aggregate the statistics for an APN for all routers. It is defined on into a single statistic. This type of aggregation reports, for example, the sum of active PDP's for the APN in the network. It requires the device to implement the MIB, CISCO-GPRS-ACC-PT-MIB.my.
- spgwApn.xml—Aggregates the statistics for an APN to a network level on SPGW devices. An APN can be defined on multiple routers and this group will aggregate the statistics for an APN for all routers. It is defined on into a single statistic. This type of aggregation reports, for example, the sum of active PDP's for the APN in the network. It requires the device to implement the MIB, CISCO-GPRS-ACC-PT-MIB.my.
- cableDownModem.xml—Aggregates the number of online downstream cable modems in the network.
- cableModem.xml—Summarizes the per-state count of all cable modems in network.
- cableUpModem.xml—Aggregates the number of online upstream cable modem in the network.
- dbdsApplicationProcessState.xml—Aggregates the application processes by state for Scientific America controllers.
- dbdsControllerProcess.xml—Aggregates the general purpose processes by state for Scientific America controllers.

The following groups aggregate data for the StarOS running on Cisco ASR 5000 platforms. The aggregated statistics are the similar to those collected through the apn, pdngwApn, sgwApn, and spgwApn groups listed above.

- starOsApnBearers.xml
- starOsApnPdp.xml
- starOsApnQos.xml
- starOsApnSess.xml
- starOsApnTraffic.xml
- starOsApn.xml

Creating a Report Group

To display grouped reports within the Prime Performance Manager GUI:

- From the Performance menu, choose **Reports** then scroll to **Grouped Reports** in the navigation tree.

To create a new grouped report:

Step 1 Log into the Prime Performance Manager GUI as the system administrator user.

Step 2 From the Administration menu, choose **Group Editor**.

Step 3 In the navigation area, click **Groups Summary**.

The default system groups are displayed:

Step 4 In the System Groups window, click the **Create New Group** tool.

Step 5 In the Create Group dialog box, enter the group name. Valid characters are letters, numbers, underscores, hyphens, and periods. Spaces are not permitted. The group name must be unique.

Step 6 Click **OK**.

The Group Details window is displayed.

Step 7 In the Group Details window, enter the parameters for the new group:

- Name—Allows you to create multiple processing sets for the same group. For example, you might want to create a group of objects defined by multiple algorithms or objects lists. Each processing set is identified with a unique name. The default processing set is “records.” It cannot be deleted.

  To create a new processing set, click **+**, then enter the new processing set name in the dialog that appears and click **OK**. Conversely, to delete a processing set, click -.

- Type—Enter the group type. The group type is a tag for the group processing section. It is used by other Prime Performance Manager functions to qualify the data. For example, in an aggregate report that uses this processing group the data is tagged with the type entered here. The type is included in each data row.

- Enabled—Check if you want the group enabled, that is, group report data will be collected and displayed.

- Data Source—Click **Change** and choose the data source you want included in the group by selecting the data source under Available Usages and clicking **Add** to move it to the Assigned Usages group. The data source identifies the report processors that use this group processing section when the group is enabled. Report processors are defined in the individual report XML files. Provided data sources include:

Step 8 Enter the object selection criteria using one or both of the following:

- Algorithm—Enter the algorithm that you want to use to define the objects added to the group. You can enter the algorithm by typing it into the Matching Algorithm box, or click **Launch Algorithm Editor** to create the algorithm using an editor. For information about using the algorithm editor, see Creating Algorithms Using the Algorithm Editor, page 7-45. If you enter the algorithm directly, click **Validate Algorithm** to validate it.

- List of Objects—Enter a list of objects using the object FQDNs, using the format:

  Node=<host or IP>,<other keys as defined in the corresponding report XML file>

  Examples:

  ```
  Node=em1941kbf.cisco.com
  Node=10.74.125.210
  ```

```
Node=em1941kbf.cisco.com,ifDescr=FastEthernet0/0
Node=10.74.125.210,CPUSlot=0,CPUNum=0,processorIndex=1
```

To validate the algorithm, click **Validate**.

Step 9 Click **Save**.

The new group is added to the Prime Performance Manager grouped reports list.

Creating Algorithms Using the Algorithm Editor

You can create group algorithms by typing it into the Matching Algorithm box, or by using the Algorithm Editor. The Algorithm editor provides a list of all possible macros and operators and allows you to create the algorithm by dragging and dropping them into a work area. To create a group algorithm using the Algorithm Editor, complete the following steps from Step 8 in "Creating a Report Group" procedure on page 7-44, or Step 5 in "Managing Report Groups" procedure on page 7-47:

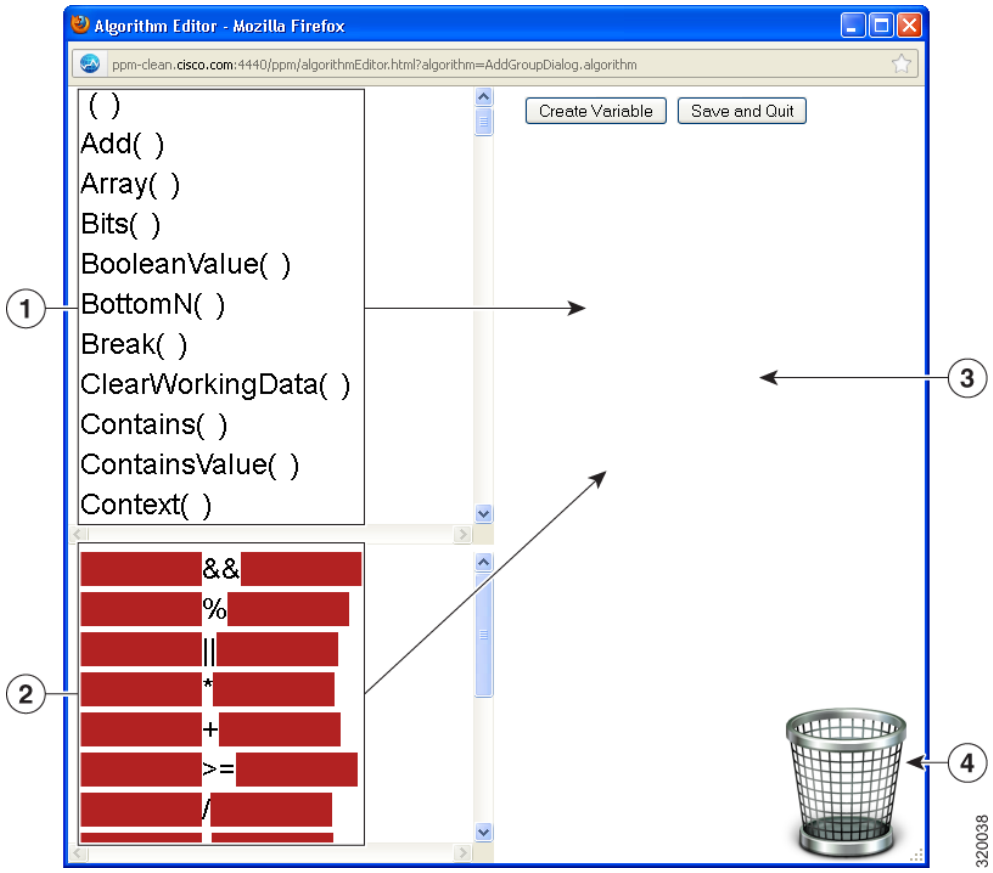
Step 1 In the Group Details tab, click **Launch Algorithm Editor**.

The Algorithm Editor (Figure 7-11) displays the following elements.

- Macros—Macros perform a discrete mathematical or programmatic routine. For a list of macro definitions, see the *Cisco Prime Performance Manager 1.3 Integration Developer Guide*.
- Operators—Define the mathematical or analytical operation to be performed between two macros.

Operator	Description	Operator	Description
&&	And	-	Subtract
%	Modulo operator	= =	Equality check
||	Or	<=	Less than or equal to
*	Multiplied by	!=	Not equal to
+	Add	>	Greater than
>=	Greater than or equal to	=	Assignment operator
/	Divided by	<	Less than

Figure 7-11 Algorithm Editor



1	Macros	**3**	Algorithm build area
2	Operators	**4**	Delete

Step 2 Drag a macro from the macro list to the work area.

Step 3 Drag an operator from the operator list to the work area and assemble the algorithm.

Dragging a macro or operation to the work area creates a copy that you can manipulate by dragging variables, operations, or other macros into it. If you drop an item into a macro, Prime Performance Manager inserts the item wherever you release your mouse button. For example, if you drop an item on the space between two parameters inside a macro, the item is placed inside that macro between the two parameters. However, if you drop the item on top of a parameter within a macro, Prime Performance Manager assumes you are trying to drop the item into the parameter, not the containing macro. For example:

```
        (1)         (2)
                          v    v
Array( SomeMacro(),     SomeOtherMacro() )
```

If you try to drop on (1), Prime Performance Manager assumes you want to drop into SomeMacro(), not Array(). However, if you drop on (2), Prime Performance Manager assumes you want to insert the item between SomeMacro() and SomeOtherMacro().

An operation allows two items to be dropped into it on either side into red boxes, one for the left operand and one for the right operand. Operands can be macros, other operations, or variables. You can only place one item into each operand target (). You can drop items into whatever is placed as an operand for an operator, however. So, if you placed a macro onto the left hand side of an operator, you can still drop parameters into that macro, you just can't add another item to the left hand side of that operator.

- Create Variable—Allows you to create a variable for use in algorithms. Click **Create Variable**, enter the variable text, then click **OK**. The new variable is placed on the page. You can drag and drop the variable into macros and operators. (You can not drop anything into a variable.)
- Delete—To delete a macro, operator, or variable item, drag it to the trash can at the bottom of the Algorithm Editor.

Step 4 When your algorithm is completed, click **Save and Quit**.

The editor validates the algorithm. If it has errors, a popup tells you errors so you can fix it, then try saving it again. You cannot save an algorithm until it passes the validation. If you want to cancel the algorithm creation attempt, close the editor. If all the algorithms pass the validation, the editor closes and the new algorithm appears in the Matching Algorithm box in the Group Details page.

Managing Report Groups

After you create report groups, you can edit, enable, disable, duplicate, and delete them at any later time.

To edit, enable, disable, duplicate, or delete a grouped report:

Step 1 Log into the Prime Performance Manager GUI as the system administrator user.

Step 2 From the Administration menu, choose **Group Editor**.

Step 3 In the navigation area, click **Groups Summary**.

Step 4 To edit a group, click the group link under the Name column.

Step 5 In the Group Details tab, edit any of the following:

- Name
- Type
- Enabled
- Data Source
- Matching Algorithm

  To edit algorithms, you can:

  – Edit the algorithm directly in the Matching Algorithm text box, then click **Validate Algorithm** to validate your edits, or,

  – Click **Launch Algorithm Editor** and edit the algorithm in the algorithm editor. See Creating Algorithms Using the Algorithm Editor, page 7-45 for information.
- List of Objects

For field descriptions and entry examples, see Creating a Report Group, page 7-44.

Step 6 To enable, disable, duplicate, or delete groups:

a. Click Groups Summary

b. Highlight the groups you want to enable, disable, or delete. Press **Shift** to choose more than one group.

c. From the Actions menu, choose the action you want to perform:

- **Enable Selected Groups**
- **Disable Selected Groups**
- **Duplicate Selected Groups**
- **Delete Selected Groups**

d. On the confirmation, click **OK**.

Displaying Group Reports

Group reports are displayed following steps similar to the display of non-group reports. To display a group report:

Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Performance menu, choose **Reports**.

Step 3 Click **Grouped Reports**, then navigate to the report you want to see.

The group report appears on the content area. For information on managing the report display, see Customizing Report Display, page 7-9.

CHAPTER 8

Managing Devices

After Prime Performance Manager discovers your network devices, you can view detailed information, perform management actions, and create individualized polling for discovered network devices.

Device views, the properties you can display, and the actions you can perform are described in the following topics:

- Displaying Network-Level Device Information, page 8-1
- Managing Devices in the Network-Level View, page 8-11
- Displaying Individual Device Information, page 8-17
- Managing an Individual Device, page 8-21
- Creating and Editing Device Polling Groups, page 8-22

Displaying Network-Level Device Information

The Prime Performance Manager network device view provides the broadest overview of your network devices. From this view you can drill down to different device details, as well as to individual devices for details about one device. (See Displaying Individual Device Information, page 8-17.)

To display the network-level device view, from the Network menu, choose **Devices**. The Network Devices window displays the last updated time in the window title bar. If the gateway and client reside in the same time zone, one time is presented. If the gateway and client are in different time zones, both times are presented.

Device information areas, accessed from Network Devices window tabs, are displayed in Table 8-1.

Table 8-1 Network-Level Device Information

Details	Description	For information, see
Devices	Lists all network devices and device properties.	Displaying Network-Level Device Properties, page 8-2
Types	Displays a device distribution by device type.	Displaying Device Type Distributions, page 8-4
Alarms by Device	Displays alarms by device.	Displaying Alarms by Device, page 8-5
Alarms by Device Type	Displays alarms by device type.	Displaying Alarms by Device Type, page 8-6

Table 8-1 Network-Level Device Information (continued)

Details	Description	For information, see
SNMP Timeouts	Displays SNMP timeout alarms.	Displaying Device SNMP Time Out Alarms, page 8-7
Poll Response	Displays poll response data.	Displaying Device Poll Responses, page 8-7
Ping Response	Displays ICMP ping response data.	Displaying Device ICMP Ping Responses and Availability, page 8-8
Uptime	Displays device up time.	Displaying Device Up Time, page 8-8
Software	Displays device software information.	Creating and Editing Device Polling Groups, page 8-22
Contact/Location	Displays device contacts and locations.	Displaying Device Contacts and Locations, page 8-9
Vendor	Displays the device manufacturer.	
Prime Style	Displays device properties in Cisco Prime format.	Displaying Device Details in Cisco Prime Format, page 8-10

Displaying Network-Level Device Properties

Prime Performance Manager displays properties for all network devices in one view. To display them:

- From the Network menu, choose **Devices**.

All discovered network devices are displayed. Table 8-2 lists the available device properties. In addition, the following items can be changed in User Preferences.

- Moving your cursor over device links displays the device details described in Table 8-2 on page 8-2, and in Table 8-10 on page 8-18. The popup is useful in other windows that list devices, for example, the Network Active Alarms window, or when drilling down to the interface report level. However, you can disable this feature in the User Preferences window.
- Devices include an alarm severity icon indicating the highest level alarm on the device. You can disable this feature in the User Preferences window.
- Deleted devices, without hyperlinks, can be displayed by enabling this option on the User Preferences window.

For information about changing user preferences, see Changing User Preferences, page 3-7

Table 8-2 Devices Properties

Property	Description
Internal ID[1]	Device internal ID. Prime Performance Manager assigns this ID to the device for internal use.
Unit[2]	Name of the unit to which the device is assigned.
Display Name	Device display name.
Sync Name	Device sync name.
Custom Name[1]	Device custom name, if available.

Table 8-2 Devices Properties (continued)

Property	Description
IP Address or DNS Hostname[1]	Device IP address or DNS name as Prime Performance Manager discovered it.
System Name[1]	Device system name.
Management IP Address	IP address used to poll the device.
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Vendor	Device manufacturer.
Software Version[1]	Device software version.
Software Description	Device software description, if available.
Last Full Poll Time	The time of the last Prime Performance Manager poll.
Last SNMP Poll Response (secs)	The time for the device to respond to the last SNMP poll requests.
Avg. SNMP Poll Response (secs)[1]	Average time for the device to respond to Prime Performance Manager SNMP poll requests.
Last CLI/XMP Poll Response (secs)	The time for the device to respond to the last CLI/XMP (for example, Telnet, SSH) poll requests.
Avg. CLI/XMP Poll Response (secs)[1]	Average time for the device to respond to Prime Performance Manager CLI/XMP poll requests.
Uptime[1]	Time the device has been up in days, hours, minutes, and seconds.
Reboot Reason[1]	Reason for the last device reboot.
Discovery Source	Indicates how Prime Performance Manager discovered the device: PPM (Prime Performance Manager) or Prime Network. See Chapter 5, "Discovering Network Devices."
Sending Alarms	Indicates whether or not the device is sending alarms. Users with authentication level Network Operator (level 3) and higher can edit this field. See Creating and Editing Device Polling Groups, page 8-22.
Report Polling	Indicates whether report polling is enabled for this device.
Severity	If alarms are raised for the device, the highest severity: Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal.
Last Status Change[1]	Date and time that the device status last changed.

Table 8-2 Devices Properties (continued)

Property	Description
Status[3]	Current device status: • Active—The device is active. • Discovering—Prime Performance Manager is in the process of discovering the device; not all device details are known. • Polling—Prime Performance Manager is polling the device. • Unknown—Prime Performance Manager does not have the device details, possibly because connectivity is lost or other reasons. • Unmanaged—Indicates a Prime Network device that is not managed by Prime Network. • Waiting—Prime Performance Manager has sent a polling request and is waiting for a response. • Warning—The device is in a warning status.
Status Reason	Reason for the current device status. (If you cannot see all of the status reason text, place the cursor over the cell to see the full text in a tooltip.) A list of possible reasons is provided in the stateReasons.html, located at: /opt/CSCOppm-gw/apache/share/htdocs/eventHelp.
Contact[1]	The device contact name, if added.
Location[2]	The device location, if added.
Polling Group[1]	The polling group to which the device is assigned. See Creating and Editing Device Polling Groups, page 8-22
Report Policy[1]	The report policy to which the device is assigned. See Creating Report Policies, page 7-20.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.
2. Not displayed by default for device alarms; displayed for SNMP timeout alarms.
3. Not displayed by default for SNMP timeout alarms.

Displaying Device Type Distributions

The Device Distributions page presents your device type distributions in table and pie chart format (Figure 8-1). Information includes the device type, the total number of devices, and the device type percentage within the network. To display device distributions:

- From the Network menu, choose **Devices**, then click **Types**.

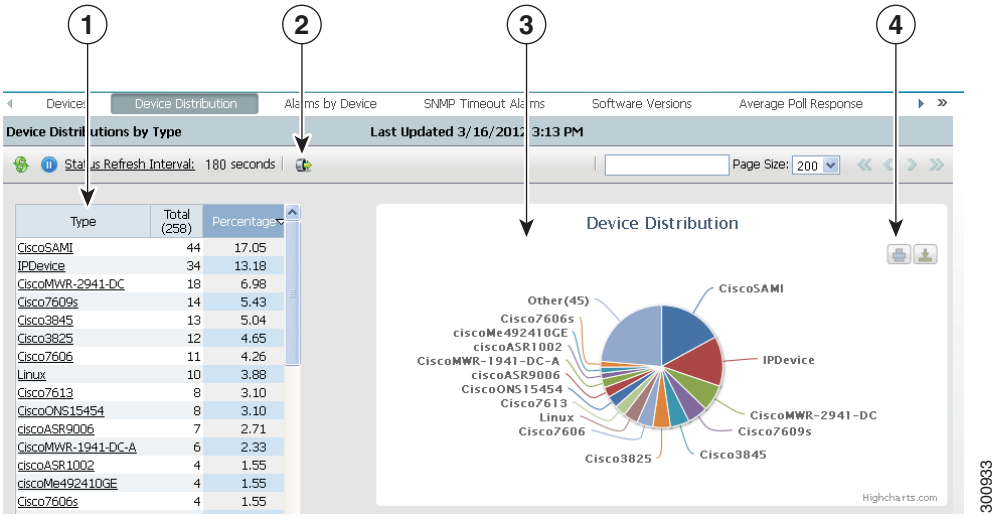
Device Distribution fields include:

- Type—The name of the device platform, for example, Cisco1706, ONS15454.
- Total (*total number of devices*)—The total number of devices of a particular type.
- Percentage—The percentage of devices of this type out of all the discovered devices.

From the Device Distributions window, you can:

- Click a device type link to display all the devices of that type. From there you can drill down into individual devices to view reports, alarms, events, and other information described in Displaying Network-Level Device Properties, page 8-2.
- Export the data to a CSV file.
- Send the distributions pie chart to a printer or graphic image.

Figure 8-1 Device Distributions



1	Device distributions in table format	**3**	Device distributions in pie chart.
2	Export to CSV file.	**4**	Send to printer and graphic image.

Displaying Alarms by Device

The Network Alarms by Device area displays a count of alarms by device and severity. You can display alarms by device from either the Devices or Alarms/Events windows:

- From the Network menu, choose either **Devices** or **Alarms/Events**, then click **Alarms by Device**.

Table 8-3 lists the Alarms by Device properties.

Table 8-3 Network Alarms by Device Properties

Column	Tool	Description
Internal ID[1]	—	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
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.

Table 8-3 Network Alarms by Device Properties (continued)

Column	Tool	Description
Sending Alarms	—	Indicates whether or not the device is sending alarms. Users with authentication level Network Operator (level 3) and higher can edit this field. See Creating and Editing Device Polling Groups, page 8-22.
Last Status Change[1]	—	Date and time that the status of the device alarms last changed.
Total	—	Total number of alarms for the device.
Critical (*alarm count*) (*alarm percentage*)		Total number of critical alarms for the device.
Major (*alarm count*) (*alarm percentage*)		Total number of major alarms for the device.
Minor (*alarm count*) (*alarm percentage*)		Total number of minor alarms for the device.
Warning (*alarm count*) (*alarm percentage*)		Total number of warning alarms for the device.
Informational (a*larm count*) (*alarm percentage*)		Total number of informational alarms for the device.
Indeterminate (*alarm count*) (*alarm percentage*)		Total number of indeterminate alarms for the device.
Normal (*alarm count*) (*alarm percentage*)		Total number of normal alarms for the device.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

Displaying Alarms by Device Type

The Network Alarms by Device Type area displays device alarm information organized by device types. You can display alarms by device type from either the Devices or Alarms/Events windows:

- From the Network menu, choose either **Devices** or **Alarms/Events**, then click **Alarms by Device Type**.

Network Alarms by Device Type displays the following information:

- Device Type—The device type, for example, Cisco7606 for Cisco 7606 Routers, CiscoONS15454 for Cisco ONS 15454 Multiservice Transport Platform, and so on.
- Total—The total number of alarms for the device type.
- Alarms—The following alarm totals are provided along with the total alarm count and alarm percentage:
  - Critical
  - Major
  - Minor
  - Warning
  - Information

- Indeterminate
- Normal

Displaying Device SNMP Time Out Alarms

The SNMP Timeout Alarms link displays the devices for which a Node Unreachable alarm is present. To display SNMP timeout alarms:

- From the Network menu, choose **Devices**, then click **SNMP Timeout**. The table displays the same device parameters as the Devices table. See Table 8-2 on page 8-2.

Displaying Device Poll Responses

The Poll Response table displays the number of seconds devices take to respond to the Prime Performance Manager poll requests. To display the device poll responses:

- From the Network menu, choose **Devices**, then click **Poll Response**.

Table 8-4 lists the Poll Response information.

Table 8-4 Device Average Poll Responses

Column	Description
Internal ID[1]	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
Unit[1]	Name of the unit to which the device is assigned.
Display Name	Name of the device.
Primary SNMP Address	IP address of the device, which SNMP uses to poll the device.
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Location	The device location.
Report Polling	Indicates whether or not report polling is enabled for this device.
Last Full Poll Time	The date and time Prime Performance Manager last polled the device.
Last Poll Response	The time, in seconds, it took for the device to respond to the poll.
Avg. Poll Response (secs)	Average response time for the device to respond to poll from the Prime Performance Manager server.
Severity	The highest severity alarm currently raised on the device.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

Displaying Device ICMP Ping Responses and Availability

The ICMP Ping Response and Device Availability table displays the number of seconds devices take to respond to the Prime Performance Manager Internet Control Message Protocol (ICMP) pings, and the resulting device availability percentages. To display ICMP ping results and device availability:

- From the Network menu, choose **Devices**, then click **Ping Response**.

The following information is displayed:

- Last ICMP Response—The time required for the device to respond to the last ICMP ping.
- Availability—Based upon the ping responses, the device availability is provided for the previous and current time periods for the following intervals:
  - 15 Minutes
  - Hourly
  - Daily
  - Weekly
  - Monthly

Displaying Device Up Time

The Uptime link displays the uptime for managed devices. To display device uptimes:

- From the Network menu, choose **Devices**, then click **Uptime**.

Table 8-5 lists the device up time properties.

Table 8-5 Device Up Time

Column	Description
Internal ID[1]	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
Unit[1]	Name of the unit to which the device is assigned.
Display Name	The device display name.
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Uptime	Time the device has been up, in days, hours, minutes, and seconds.
Reboot Reason	Reason for the last reboot of the device.
Severity	Indicates the highest alarm severity for the chosen device: Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

Displaying Device Software

The Network Software table lists the software versions and descriptions for each device in the Prime Performance Manager network. To display the device software information,

- From the Network menu, choose **Devices**, then click **Software**.

Table 8-6 lists the Software parameters.

Table 8-6 Software

Column	Description
Display Name	Name of the device.
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Software Version	Software version used by the device.
Software Description	Full software version information.

Displaying Device Contacts and Locations

The Contacts/Locations link displays the device contacts and locations if that information was entered for the device. To display the device contacts and locations:

- From the Network menu, choose **Devices**, then click **Contacts/Locations**.

Table 8-7 lists the Contact and Location properties.

Table 8-7 Device Contacts and Locations

Column	Description
Internal ID[1]	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
Display Name	The device display name.
IP Address or DNS Hostname[1]	IP address or DNS name of the device, as the Prime Performance Manager discovered it.
SysName[1]	System name of the device.
Primary SNMP Address[1]	The IP address that SNMP uses to poll the device.
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Contact	The device contact name.
Location	The device location.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

Displaying Device Vendors

The Vendors link displays the device types, manufacturers, and status. To display the device vendor information:

- From the Network menu, choose **Devices**, then click **Vendor**.

Table 8-8 displays the device vendor information.

Table 8-8 Device Vendor Information

Column	Description
Internal ID[1]	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
Display Name	The device display name.
IP Address or DNS Hostname[1]	IP address or DNS name of the device, as the Prime Performance Manager discovered it.
System Name[1]	System name of the device.
Management IP Address[1]	The IP address that SNMP uses to poll the device.
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Vendor	The device manufacturer.
Status	The device status, for example, Active.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

Displaying Device Details in Cisco Prime Format

If Prime Performance Manager is integrated with Cisco Prime Central (see "Prime Central Integration"), you can display the device details in a format that matches Prime Central. Because fewer properties are displayed than the Devices tab, Prime Style can provide a quick look at the Prime Performance Manager devices in an organization that aligns with their display in Prime Central.

To display Prime Performance Manager device details in Prime Central format:

- From the Network menu, choose **Devices**, then click **Prime Style**.

Table 8-7 lists the device properties displayed in the Prime Style tab.

Table 8-9 Device Details in Prime Style

Column	Description
Internal ID[1]	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
Unit[1]	The unit to which the device is assigned.
Device Name	IP address or DNS name of the device, as the Prime Performance Manager discovered it.

Table 8-9 Device Details in Prime Style (continued)

Column	Description
Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
Status	Current device status: • Active—The device is active. • Discovering—Prime Performance Manager is in the process of discovering the device; not all device details are known. • Polling—Prime Performance Manager is polling the device. • Unknown—Prime Performance Manager does not have the device details, possibly because connectivity is lost or other reasons. • Unmanaged—Indicates a Prime Network device that is not managed by Prime Network. • Waiting—Prime Performance Manager has sent a polling request and is waiting for a response. • Warning-—The device is in a warning status.
Management IP Address	IP address used to poll the device.
Software Version	The software version installed on the device.
System Name	The device system name.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

Managing Devices in the Network-Level View

At the network-level device view, operator or higher users can perform some device modifications. To manage network devices:

Step 1 From the Network menu, choose Devices.

Step 2 Navigate to one of the following device view tabs:

- Devices
- Alarms by Device
- SNMP Timeouts
- Poll Response
- Ping Response
- Uptime
- Software
- Contact/Locations
- Vendor

- Prime Style

See Displaying Network-Level Device Information, page 8-1 for information on displaying these views.

Step 3 Select a device. Press **Shift** to select multiple contiguous devices, or **Ctrl** to select devices that are not contiguous.

Step 4 From the Actions menu (located just above the device table), choose any of the following actions.

- Poll Device—Polls the devices selected in the device list.
- Edit Properties—Allows you to edit the device display name and default web port. See Editing a Device Name, Web Port, and Time Zone, page 8-13.
- Edit Device Credentials—Allows you to edit the device SNMP or Telnet/SSH credentials used to poll the device. See Editing the Device Credentials, page 8-13.
- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 8-15
- Edit Polling Policy—Allows you to change the polling policy assigned to the device. See Creating and Editing Device Polling Groups, page 8-22 and Editing the Polling Group Assigned to a Device, page 8-15.
- Edit SNMP IP Addresses—Allows you to edit a device SNMP IP addresses. See Editing the Device SNMP IP Addresses, page 8-16.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 8-16.
- Disable Sending Alarms—Disables sending alarms from the selected device.
- Enable Sending Alarms—Enables sending alarms from the selected device.
- Unmanage Device—Changes managed devices to unmanaged.
- Manage Device—Changes unmanaged devices to managed.
- Delete—Deletes the selected device(s).

Note If multiple devices are selected, not all actions are available.

Step 5 To check device connectivity, from the device toolbar, click one or both of the following:

- Ping—Pings the device and displays the results in a Ping Device: [*device name*] window.
- Traceroute—Runs the traceroute command to detail the route from the gateway to the device and displays the results in a Traceroute Device: [*device name*] window.

Note You can also use the ppm ping and ppm traceroute commands to check device connectivity. See ppm ping, page B-47 and ppm traceroute, page B-77.

Editing a Device Name, Web Port, and Time Zone

Within the device network view, you can change the device name, web port, or time zone. To edit these device properties:

Step 1 Navigate to one of the following device views: Devices, Device Distribution, SNMP Timeout Alarms, Software, Average Poll Response, Uptime, Contact/Locations. (For information on displaying these views, see Displaying Network-Level Device Information, page 8-1.)

Step 2 In the device list, select the device whose name you want to edit.

Step 3 From the Actions menu, choose **Edit Properties**

Step 4 In the Edit Properties dialog box, edit the following properties:

- 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—Should you wish to change the default device web port, enter the web port number.
- Time Zone—Should you wish to change the device time zone, enter the time zone by typing the first letters. The field will populate with time zones matching the letters you entered.

Note For device alarms and events to be displayed in the device time zone,

Step 5 Click **Save**.

Editing the Device Credentials

To edit the device SNMP or Telnet/SSH credentials:

Step 1 Navigate to one of the following device views: Devices, Device Distribution, SNMP Timeout Alarms, Software, Average Poll Response, Uptime, Contact/Locations. (For information on displaying these views, see Displaying Network-Level Device Information, page 8-1.)

Step 2 In the device list, select the device whose credentials you want to edit.

Step 3 From the Actions menu, choose **Edit Device Credentials**.

Step 4 In the Edit Device Credentials dialog box, edit any of the following:

SNMP v1, v2

- Read Community—The SNMP community name used by the device for read access to the information maintained by the SNMP agent on the device.

SNMP v3

- User Name—The user name.
- Authentication Protocol—The authentication protocol:

- md5—Uses the Hash-based Message Authentication Code (HMAC) MD5 algorithm for authentication
- sha—Uses the HMAC SHA algorithm for authentication
- Authentication Password—The authentication password (SNMP v3),
- Privacy Protocol—The privacy protocol:
- 3des—Uses Data Encryption Standard (DES).
- des—Uses the Data Encryption Standard (DES).
- aes128—Uses Advanced Encryption Standard (AES) 128-bit encryption.
- Privacy Password—The privacy password.

Telnet/SSH

- 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—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.
  - vCenter_HTTPs
  - vCenter_HTTP
  - ESXi_HTTPs
  - ESXi_HTTP
  - XEN_TLS
  - KVM_TLS
  - HyperV_HTTPs
  - HyperV_HTTP
- 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 5 Click **Save**.

The edited credentials are saved for the device.

Editing the Report Policy Assigned to a Device

To edit the report policy assigned to a device:

Step 1 Navigate to one of the following device views: Devices, Device Distribution, SNMP Timeout Alarms, Software, Average Poll Response, Uptime, Contact/Locations. (For information on displaying these views, see Displaying Network-Level Device Information, page 8-1.)

Step 2 In the device list, select the device whose report policy you want to edit.

Step 3 From the Actions menu, choose **Edit Report Policy**.

Step 4 In the Edit Report Policy dialog box, choose the report policy that you want assigned to the device from the Report Policy policy list.

Step 5 Click **Save**.

Editing the Polling Group Assigned to a Device

To edit the polling group assigned to a device:

Step 1 Navigate to one of the following device views: Devices, Device Distribution, SNMP Timeout Alarms, Software, Average Poll Response, Uptime, Contact/Locations. (For information on displaying these views, see Displaying Network-Level Device Information, page 8-1.)

Step 2 In the device list, select the device whose polling group you want to edit.

Step 3 From the Actions menu, choose **Edit Polling Group**.

Step 4 In the Polling Group Details dialog box, edit the following properties:

- Polling Policy—Allows you to assign a different polling policy to the device. For information about creating and editing polling policies, see Creating and Editing Device Polling Groups, page 8-22
- 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.

Step 5 Click **Save**.

Editing the Device SNMP IP Addresses

To edit the polling group assigned to a device:

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

Step 1 Navigate to one of the following device views: Devices, Device Distribution, SNMP Timeout Alarms, Software, Average Poll Response, Uptime, Contact/Locations. (For information on displaying these views, see Displaying Network-Level Device Information, page 8-1.)

Step 2 In the device list, select the device whose SNMP addresses you want to edit.

Step 3 From the Actions menu, choose **Edit SNMP Addresses**.

The Edit SNMP IP Address dialog box displays the following:

- Available IP Addresses—Lists 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.

Step 4 Click any of the following:

- **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.

Step 5 When finished, click **Save**.

Relocating Devices to Units

To relocate a device to a different unit:

Step 1 Navigate to one of the following device views: Devices, Device Distribution, SNMP Timeout Alarms, Software, Average Poll Response, Uptime, Contact/Locations. (For information on displaying these views, see Displaying Network-Level Device Information, page 8-1.)

Step 2 In the device list, select the device that you want to relocate.

Step 3 From the Actions menu, choose **Relocate Device**.

Step 4 In the Relocate Device dialog box, choose the unit to which you want to assign the device from the Units list.

Step 5 Click **Save**.

Displaying Individual Device Information

Prime Performance Manager allows you to drill down to individual devices and review additional parameters and details not displayed at the network level. including device-level reports, dashboards, properties, event history, active alarms, status, and availability.

Device time stamps can be displayed in the device time zone by enabling the Display Device Level Data in Device Time Zone option in User Preferences. Time stamps affected by this option include the time stamp displayed in report titles, calendar popup selections, summary table maximum date strings, graph date strings, tooltip hover information,.the Timestamp column in report table format, and the Timestamp values in exported CSV files. For information about changing user preferences, see Changing User Preferences, page 3-7.

To display individual device information:

Step 1 Navigate to one of the following:

- Performance menu > Reports > Choose a report. > Click a device link in the report.
- Network menu > Devices
- Network menu > Alarms/Events
- System menu > Gateways/Units
- If you attached devices to custom report views, display the view or subview. (For information about custom report views, see Creating and Managing Custom Report Views, page 7-34.)

Step 2 Click a device link or, if you are displaying a custom view, display the view or subview containing the device.

At the individual device view, the following is displayed:

Note In addition to the menus listed below, custom report views and subviews with attached devices will display a View and View Editor menus. For information, see Creating and Managing Custom Report Views, page 7-34.

- Reports—Allows you display any report that is generated for the device. The reports that are available depend upon the device hardware and network provisioning. In many cases, you can drill down to detailed device component reports, for example, interfaces and ports. For additional information about the Prime Performance Manager reports, see Chapter 7, “Managing Reports, Dashboards, and Views.”
- Dashboards—Allows you display any dashboard that can be generated for the device based upon the hardware and technologies that are provisioned for it. Like reports, you can often drill down to view device component dashboards. For additional information about the Prime Performance Manager reports, see Managing Dashboards, page 7-31.
- Details—Displays the detailed device information listed in Table 8-10.

Table 8-10 Device Details

Section	Field	Description
Toolbar	Actions menu	Allows you to modify device parameters. See Managing an Individual Device, page 8-21
	Ping	Pings the selected device.
	Traceroute	Runs a traceroute to the selected.
	Launch	Launches the device home page.
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	If devices were imported from Prime Network, the device name (or business tag, if defined) as it appears in Prime Network.
	IP Address or Host Name	The device IP address or DNS name, as discovered by Prime Performance Manager.
	System Name	The name set on the router and returned, using the SNMP variable sysName.
	Unit	The name of the unit to which the device belongs.
	Homepage	Provides a link to the device home page.
Status Information	Sending Alarms	Indicates whether the device is sending alarms, Yes or No.
	Alarm Severity	Indicates the alarm severity of the object.
	Status	Current device status: • Active—The device is active. • Discovering—Prime Performance Manager is in the process of discovering the device; not all device details are known. • Polling—Prime Performance Manager is polling the device. • Unknown—Prime Performance Manager does not have the device details, possibly because connectivity is lost or other reasons. • Unmanaged—Indicates a Prime Network device that is not managed by Prime Network. • Waiting—Prime Performance Manager has sent a polling request and is waiting for a response. • Warning—The device is in a warning status.
	Last Status Change	Date and time when the device status was last changed.
	Status Reason	Reason for the current device status. (If you cannot see all of the status reason text, place the cursor over the cell to see the full text in a tooltip.) A list of possible reasons is provided in the stateReasons.html, located at: /opt/CSCOppm-gw/apache/share/htdocs/eventHelp.

Table 8-10 Device Details (continued)

Section	Field	Description
Device Performance	Memory Utilization	Displays the memory utilization at the time of the poll. If the device has multiple memory pools, the utilization is the average of the pools. Text color is based on the Enabled Colors user preference: • Off—Text is not color coded. • On—Text follows the ascending metric. • Red/Orange/Gold Only—follows the ascending metric, with the exception of green. For information about user preferences, see Changing User Preferences, page 3-7.
	CPU Utilization	Displays the memory utilization at the time of the poll. If the device has multiple CPUs, the utilization is the average of the CPUs. Text color is also based on the Enabled Colors user preference.
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.
	Device Type	The device type, which is usually based on the device family, for example, Cisco1706 for Cisco 1706 Series Routers. If the device family type is not known, IP Device is displayed. Prime Performance Manager gateway and unit servers are listed as ciscoGatewayServer and ciscoUnitServer.
	Location	The device physical location. If the device location details are not available, this field displays Unknown.
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.

- Data Collection—Displays the data collection information for the device shown in Table 8-11.

Table 8-11 Data Collection

Section	Field	Description
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 Capability Full Poll Time	The last time the device capabilities were assessed. This query is performed once every 24 hours at a minimum. It also occurs when Prime Performance Manager detects a device configuration or entity change, or when the SystemCapabilities or UserCapabilities file changes.
	Last Full Poll Time	The date and time of the last full poll of the device for device-related MIBs.
	Last SNMP Poll Response (secs)	The time, in seconds, taken by this device to respond to the last SNMP poll request.
	Avg SNMP Poll Response (secs)	The average time, in seconds, taken by this device to respond to SNMP poll requests.
	Last CLI/XML Poll Response (secs)	The time, in seconds, taken by this device to respond to the last CLI (for example, Telnet) or XML (for example, HTTP) poll request.
	Avg CLI/XML Poll Response (secs)	The average time, in seconds, taken by this device to respond to a CLI or XML poll request.
	Polling Group	The polling group to which the device is assigned. For information about polling groups, see Creating and Editing Device Polling Groups, page 8-22.
	Report Policy	The report policy assigned to the device. If no report policy is assigned, the field will display “This device only.” For information about report policies, see Creating Report Policies, page 7-20.
Collector Status	IP	Indicates whether IP connectivity is achieved. This will be Active unless the device was never successfully pinged.
	SNMP	Indicates whether data has been retrieved through SNMP. Will be Active unless data has never been retrieved using SNMP.
	CLI	Indicates whether an XML poll was performed: • Active—A successful XML poll has occurred. • Not Configured—An XML poll was never performed. • Not Active—An XML poll failed because of credentials.

Table 8-11 Data Collection (continued)

Section	Field	Description
	CSV Bulk Stats	Indicates whether CSV bulk stats were collected. This will be Not Configured for any device other than the Cisco ASR 5000. For the Cisco ASR 5000, the field will display: • Not Configured—If no CSV poll was conducted. • Active—If a successful CSV poll occurred and bulk stats results were available. • Not Active—If a successful CSV poll occurred but no bulk stats were available.
IP Addresses for SNMP	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, Yes or No.

- Event History—Displays events that have occurred on the device. For a list of event parameters, see Table 9-1 on page 9-2.
- Active Alarms—Displays alarms that have been raised on the device. For a list of event parameters, see Table 9-1 on page 9-2.
- Report Status—Displays the reports available for the device.
- Availability—Displays device availability data in table and bar chart format. Availability increments include current and last 15-minute, hourly, daily, weekly, and monthly time periods.
- Star Graphs—Allows you to add selected charts from multiple device reports and effectively create a custom report view for a specific device. For information, see Creating Custom Device Star Graphs, page 7-12.
- Device Status—Displays information from the Details, Data Collection, Event History, Active Alarms, and Availability tabs in a snapshot device status view.

Note When you select an individual device, it is added to the Devices navigation list so you can go back to it at any later point during the session. For example, if you select five devices, Device 1, Device 2, Device, 3, Device 4, and Device 5, these devices will appear in the navigation area so you can display them at any point.

Managing an Individual Device

When you drill down to an individual device, you can perform the management actions that you can perform from the device summary window.

To manage an individual device:

Step 1 Navigate to one of the following:

- Performance menu > Reports > Choose a report. > Click a device link in the report.
- Network menu > Devices
- Network menu > Alarms/Events
- System menu > Gateways/Units
- If you attached devices to custom report views, display the view or subview. (For information about custom report views, see Creating and Managing Custom Report Views, page 7-34.)

Step 2 Click a device link or, if you are displaying a custom view, display the view or subview containing the device.

Step 3 Click the **Details** tab.

Step 4 From the Actions menu, choose any of the following options:

- Poll Device—Polls the devices selected in the device list.
- Edit Properties—Allows you to edit the device display name and default web port. See Editing a Device Name, Web Port, and Time Zone, page 8-13.
- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 8-15
- Edit Polling Policy—Allows you to change the polling policy assigned to the device. See Creating and Editing Device Polling Groups, page 8-22 and Editing the Polling Group Assigned to a Device, page 8-15.
- Edit SNMP IP Addresses—Allows you to edit a device SNMP IP addresses. See Editing the Device SNMP IP Addresses, page 8-16.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 8-16.
- Disable/Enable Sending Alarms—Disables or enables sending alarms from the selected device. The menu item displayed is based on the current device state.
- Manage/Unmanage Device—Changes managed devices to unmanaged, and unmanaged devices to managed. The menu item displayed is based on the current device state.
- Delete—Deletes the selected device(s).

Creating and Editing 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 5, “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 8-12. 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 8-12 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 administrator user.

Step 2 From the Network menu, choose **Polling Groups**.

Step 3 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 8-12 on page 8-23, for polling group parameter descriptions and default values.

Note You cannot edit the polling group name.

Step 4 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 administrator user.

Step 2 From the Network menu, choose **Polling Groups**.

Step 3 On the Polling Group Editor toolbar, click the **Add Polling Group** tool.

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 8-12 on page 8-23, for polling group parameter descriptions and default values.

Note You cannot edit the polling group name.

Step 5 On the Polling Group Editor 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 administrator user.

Step 2 From the Network menu, choose **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 9

Managing Network Alarms and Events

Prime Performance Manager allows you to view alarms and events that occur in your network. The following topics provide information about displaying network alarms and events:

- Displaying Active Alarms and Event History, page 9-1
- Managing Alarms and Events, page 9-3
- Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters, page 9-11

Displaying Active Alarms and Event History

You can view active network alarms and historical events and manage them in multiple ways. Each alarm and event includes parameters to help you understand the alarm, its cause, and its history. Alarms and events are displayed from the Prime Performance Manager Performance menu:

- From the Network menu, choose **Alarms/Events > Active Alarms** to display all network alarms organized by occurrence date and time.
- From the Network menu, choose **Alarms/Events > Event History** to display historical events organized by occurrence date and time.
- Move cursor over **Alarm Browser** at the bottom of the Prime Performance Manager window to display all network alarms organized by occurrence date and time in a popup window.
- Move cursor over **Alarm Summary** at the bottom of the Prime Performance Manager window to display the number of alarms organized by device in a popup window.

Note The popup Alarm Browser and Alarm Summary can be turned off. For information, see Changing User Preferences, page 3-7.

- Display a device and choose **Active Alarms** to display alarms for that device.

Table 9-1 shows the alarm and event parameters. Not all parameters are displayed by default. To display them, see Adding and Removing Properties from Property Views, page 3-13.

Table 9-1 Active Alarms and Event History

Column	Description
Internal ID[1]	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 used when the Cisco Technical Assistance Center must debug problems.
Ack	Indicates whether the alarm or event is acknowledged.
Name	The alarm or event name.
Alarm Nature[1]	The alarm nature, which is determined when the alarm is created. Valid values: • ADAC—Automatically detected and automatically cleared • ADMC—Automatically detected and manually cleared • Undefined—Undefined
Alarm Type[1]	The alarm type. Alarm types include: • Communications • Processing Error • Environmental • QOS • Equipment • Undefined
Probable Cause[1]	The alarm or event probable cause.
Element Name[1]	The network element name associated with the event.
Category[1]	The event category. Categories include: • Network—Events pertaining to managed elements. • System—Events pertaining to Prime Performance Manager. • TCA—Threshold crossing alarm.
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[1]	The original severity of the event.
Count	The number of events in the event sequence for an alarm.
Note[1]	Indicates whether a note is associated with the event.
Create Time (*gateway time zone*)[2]	The time when this event was received in the gateway time zone. This column is displayed by default in the Event History window and the Events tab.
Create Time (Device Time Zone)[13]	The time when the event was created in the device time zone.
Change Time (*gateway time zone*)[2]	The time when this event was last updated in the gateway time zone.
Change Time (Device Time Zone)[2]	The time when the event was last updated in the device time zone.

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

Column	Description
Ack By[1]	The user who last acknowledged the alarm or event, or, user-based access is not implemented, the device name that last acknowledged the event. If not acknowledged, this field is blank.
Ack Time (*gateway time zone*)[2]	The time when the event was acknowledged in the gateway time zone.
Ack Time (Device Time Zone)[1]	The time when the event was acknowledged in the device time zone.
Device	Name of the device associated with the alarm or event. If no device is associated, None is displayed.
Device type[1]	The device type.
Clear By[1]	The user who cleared the event. If cleared automatically, the device name or IP address that cleared the alarm.
Clear Time (*gateway time zone*)[12]	The time when the event was cleared in the gateway time zone.
Clear Time (*device time zone*)[13]	The time when the event was cleared in the device time zone.
Message	Message associated with the alarm or event.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.
2. Format: mm-dd-yy hh:mm (XXX), where XXX is the gateway server time zone.
3. Format: mm-dd-yy hh:mm GMT-hh:mm.

Managing Alarms and Events

Prime Performance Manager provides many functions to filter and change the alarms and events display. Most functions are performed from the Network Active Alarms tab (Network > Alarms/Events > Active Alarms) or the Network Event History tab (Network > Alarms/Events > Event History). Actions that you can perform are described in the following topics:

- Filtering Alarms and Events, page 9-4
- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9
- Displaying Device Details for an Alarm, page 9-9
- Displaying Alarms by Device From the Alarms Window, page 9-11
- Filtering Alarms and Events, page 9-4

Displaying an Alarm Summary

You can display a snap shot of your network health including the devices with the highest number of alarms, the device types with the highest alarm counts, alarm severity percentages, and alarm counts by device. These charts are displayed in one window so you get a quick overview of your network health at any given time.

To view the alarm summary, from the Network menu, choose **Alarms/Events**, then click **Alarms Overview**.

The following alarm charts are displayed:

- Top 10 Devices by Alarm Count—Displays the top 10 devices in the network with the highest alarm counts, starting with the highest alarm count.
- Top 10 Device Types by Alarm Count—Displays the top 10 device types in the network with the highest alarm counts, starting with the highest alarm count.
- Percentage of Alarm Severities—Displays the percentages of active alarms on the network, starting with the highest percentage.
- Number of Devices by Highest Severity—Presents a chart of devices and the device highest severity alarm.

Filtering Alarms and Events

You can filter alarms and events to show only alarms and events with particular interest, for example, you might want to display only critical alarms, or display only alarms and events for a particular device. These settings are applied to all alarms or events displayed in the current view.

To filter alarms or events:

Step 1 From the Network menu, choose **Alarms/Events**, then click **Active Alarms** or **Event History**.

Step 2 In the Active Alarms or Event History tab, click the **Modify event filter** tool.

In the Alarm and Event Filter dialog box, set the categories, severities, and other filter options that you want to use to filter the alarms and events.

- Categories options specify the alarm or event categories you want displayed:
  - System—Prime Performance Manager alarms and events.
  - Network—Managed element alarms and events.
  - TCA—Threshold crossing alerts.

  All categories are checked by default.
- Severities options specify the alarm and event severities you want displayed:
  - Informational
  - Normal
  - Indeterminate
  - Warning
  - Critical
  - Minor

  - Major

- Other options, listed in Table 9-2, further define the alarms and events you want filtered.

Table 9-2 Alarm and Event Filter Dialog Box Other Pane

Field	Description
Acknowledged	Indicates whether only acknowledged alarms/events appear in the Active Alarms or Event History window. This check box is checked by default.
Unacknowledged	Indicates whether only unacknowledged alarms/events appear in the Active Alarms or Event History window. This check box is checked by default.
Time Before	Indicates whether only alarms/events that Prime Performance Manager logs before a specified date and time, appear in the Active Alarms or 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 or 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 or 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 or Event History window. This field is dimmed unless the Time After check box is checked.
Name or Message Matches	Indicates whether only alarms/events that contain the specified message text appear in the Active Alarms or 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.
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 or 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 or 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.

Table 9-2 Alarm and Event Filter Dialog Box Other Pane (continued)

Field	Description
Match Regex	Indicates 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 or 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 or 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 or Event History table does not contain any rows.
Acknowledged By	Filters alarms or events by the individual who acknowledged the alarm. The username text you enter must match the Prime Performance Manager username or, if Prime Performance Manager is integrated with Prime Central, the Prime Central username.
Cleared By	Filters alarms or events by the individual who cleared the alarm. The username text you enter must match the Prime Performance Manager username or, if Prime Performance Manager is integrated with Prime Central, the Prime Central username.
Device Type	Filters alarms or events by device type. Check **Device Type**, then choose a network device from the drop-down list.
Suppress for unmanaged devices	Suppresses 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.

Step 3 When finished, click **OK**.

Prime Performance Manager filters the alarms and events by the filter options you entered. To turn off the filter, click **Remove Filter**. Alternatively, to apply the filter, click **Apply Filter**. (The tool name alternates depending on whether the filter is applied.)

Displaying Alarm and Event Properties

Not all alarm or event properties are displayed in the Active Alarms or Event History windows. While you can choose to display the properties not displayed by default in the Active Alarms and Event History window, you can quickly view all parameters for individual alarms and events.

To view the properties for an individual alarm or event:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Do one of the following:

- In Active Alarms window, check the alarm whose properties you want to view or,
- Click **Event History** and check the event whose properties you want to view.

Step 3 From the Active Alarms or Event History window toolbar, click **Properties**.

The Prime Performance Manager Alarm and Event Properties window Properties tab displays the all properties listed in Table 9-1.

Related Topics

- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Adding Notes to Alarms or Events

Prime Performance Manager allows you to add notes to alarms and events, for example, you might want to add information about an alarm for others to know or as reminders, for example, the alarm or event's associated object, what triggered the alarm or event, how often it has occurred, and so on.

To add a note to an alarm or event:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Do one of the following:

- In Active Alarms window, click the alarm to which you want to add a note or,
- Click **Event History** and click the event to which you want to add a note.

Step 3 From the Active Alarms or Event History window toolbar, click **Edit Notes**.

The Prime Performance Manager Alarm and Event Properties window Notes tab is displayed. Any previously added notes are displayed. The date and time the notes were last updated is displayed in the Last Updated field. (If no notes have been added, the Last Updated field displays Not Set.)

Step 4 To add a new note, type the text in the note page, then click **Save Note** on the Notes toolbar.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Alarm or Event Details

Prime Performance Manager includes additional details for some alarms and events that are not included in the alarm or event message text or properties. For example, the SchedulerQueueSize alarm might display the following message:

```
Unit: unitname - The PPM scheduler queue size is over threshold which indicates a possible
performance problem.
```

The Alarm and Event Properties window Details tab might display additional details, such as:

```
QSize    110
QMax    155
QMin    0
QThreshold    100
QAvg    105
isAlarm    True
UnitEventId    468002
```

To display alarm or event details:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Do one of the following:

- In Active Alarms window, check the alarm whose details you want to view or,
- Click **Event History** and check the event whose details you want to view.

Step 3 From the Active Alarms or Event History window toolbar, click **Event Properties**, then click the **Details** tab.

Additional alarm or event details, if present, will be displayed.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm Events, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Alarm Events

To assist you in analyzing any individual alarm, you can view the events that comprise it. The events can be displayed chronologically, or sorted by other criteria such as device, severity, or message text. The collection of events provide a more detailed profile of any give alarm.

To display alarm events:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 In Active Alarms window, check the alarm whose events you want to view.

Step 3 From the Active Alarms window toolbar, click **Events for Alarm**.

The alarm events are displayed.

Step 4 From the Events for Alarm tab you can perform any event function described in Table 9-1 on page 9-2.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Daily Alarm and Event Archives

Prime Performance Manager archives alarms and events every night. The archive process gathers all the events and alarms for that day and places them in a file-based archive. The daily archives can be stored back as far as several months, if needed. Eventually, you can move the daily archives out of your database and into compressed-file-based archives for long term storage.

To display the daily archive:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 From the Active Alarms window, click **Daily Archives**.

The message archive is displayed. The daily archive is named Status+Alarms.*archivedate*.

Step 3 To display the archive, click the archive link.

Step 4 In the archive you can do any of the following to change the archive display:

- Limit the number of events displayed per page by clicking **10/Page** (10 events per page), **20/Page**, **50/Page**, **100/Page**, **200/Page**, **300/Page**, **400/Page**, or **500/Page**. In addition, you can:
  - Click **Max/Page** to display all archive events on one page.
  - Click **DefPrefs** to return to the default archive display.
  - Click **Reload** to reload the archive.
- Display only alarms and events with a particular severity level by clicking **Critical**, **Major**, **Minor**, **Warning**, **Informational**, **Admin**, **Error**, **Normal**, **Indeterminate**, **AlarmsOnly**, **AllEvents**.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Alarm Events, page 9-8

Displaying Device Details for an Alarm

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 In the Active Alarms window, click the alarm whose details you want to view.

Step 3 From the Active Alarms window toolbar, click **Properties**.

Step 4 In the Alarm and Event Properties window, click **Device Details**.

The following device details are displayed.

- Naming Information
- Status Information
- Polling Information
- Descriptive Information
- Uptime Information
- IP Addresses for SNMP

For information about the properties displayed, see Table 8-10 on page 8-18.

Step 5 From the Device Details tab, you can perform the following device actions.

- Poll Device—Polls the devices selected in the device list.
- Edit Properties—Allows you to edit the device display name and default web port. See Editing a Device Name, Web Port, and Time Zone, page 8-13.
- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 8-15
- Edit Polling Policy—Allows you to change the polling policy assigned to the device. See Creating and Editing Device Polling Groups, page 8-22 and Editing the Polling Group Assigned to a Device, page 8-15.
- Edit SNMP IP Addresses—Allows you to edit a device SNMP IP addresses. See Editing the Device SNMP IP Addresses, page 8-16.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 8-16.
- Disable/Enable Sending Alarms—Disables or enables sending alarms from the selected device. The menu item displayed is based on the current device state.
- Manage/Unmanage Device—Changes managed devices to unmanaged, and unmanaged devices to managed. The menu item displayed is based on the current device state.
- Delete—Deletes the selected device(s).
- Ping—Pings the device to check connectity.
- Trace—Invokes traceroute to map the network route to the device.
- Launch—Launches the device home page.

Related Topics

- Displaying Alarm and Event Properties, page 9-6
- Adding Notes to Alarms or Events, page 9-7
- Displaying Alarm or Event Details, page 9-8
- Displaying Daily Alarm and Event Archives, page 9-9

Displaying Alarms by Device From the Alarms Window

You can display alarms by device from the Prime Performance Manager Alarms window or the Devices window. To display alarms by device from the Alarms window, choose **Alarms/Events** from the Network menu, then click **Alarms by Device**. For a description of alarms by device parameters, see Table 8-3 on page 8-5.

Displaying Alarms by Device Type From the Alarms Window

You can display alarms by device type from the Prime Performance Manager Alarms window or the Devices window. To display alarms by device from the Alarms window, choose **Alarms/Events** from the Network menu, then click **Alarms by Device**. For a description of alarms by device parameters, see Table 8-3 on page 8-5.

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. They also tell you how to tune Prime Performance Manager alarms and events:

- Adding Upstream OSS Hosts, page 9-11
- Editing Upstream OSS Hosts, page 9-12
- Tuning Event and Alarm Parameters, page 9-15
- Prime Performance Manager SNMP Traps, page 9-16

Adding Upstream OSS Hosts

Prime Performance Manager allows you to send alarms and events to OSS hosts. To add an OSS host for Prime Performance Manager SNMP traps:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 On the Alarms/Events Editor toolbar, click the **Add a New Host** tool.

Step 4 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. See CISCO-PRIME Notification Attributes, page 9-16
  - CISCO-SYSLOG—The Cisco Syslog trap type.
  - CISCO-EPM-2—The Cisco EPM 2 trap type. See CISCO-EPM-2 Trap Notification Attributes, page 13-6

Step 5 Click **OK**.

Step 6 On the Alarms/Events Editor toolbar, click **Save Configuration**.

The new host is added to the Upstream OSS Hosts table.

Editing Upstream OSS Hosts

After you add an OSS host, you can edit the SNMP community, version, and trap type at a later point. You can filter alarms and events based upon alarm category or severity, device type, days of the week and hours within the day.

To edit OSS host SNMP details and/or filter events sent to the host:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 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 9-11.

- Host
- Port

Note Host and Port are not editable. If you need to change the host or host port, delete the host entry by clicking the Delete tool, then complete Adding Upstream OSS Hosts, page 9-11.

- Community
- SNMP Version
- Trap Type:
  - CISCO-PRIME
  - CISCO-SYSLOG
  - CISCO-EPM-2

Step 4 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Step 5 To filter the alarms and events sent to OSS hosts, complete the "Configuring Alarms Sent to OSS Hosts" procedure on page 9-13.

Configuring Alarms Sent to OSS Hosts

You can configure the alarms and events that you want sent to OSS hosts based upon alarm category or severity, device type, days of the week and hours within the day.

To edit OSS host SNMP details and/or filter events sent to the host:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 In the Upstream OSS Hosts list, click the OSS host whose alarms you want to configure and click the **Set Filter** tool.

Step 4 In the OSS Filter dialog box, uncheck the alarm and event categories and severities that you do not want to send to the OSS host. (By default, all categories and severities are enabled.)

- Categories—System, Network, and TCA.
- Severities—Critical, Major, Minor, Warning, Informational, Indeterminate, Normal.
- Device Types—Include all the device types that have been added to Prime Performance Manager.
- Applicable—Specifies the days of the week and time of day when you want alarms sent to the OSS host.

Step 5 If you want an automation script executed when alarms and events are sent to the host, enter the path/script name in the Run Script field. The script can reside anywhere on your file system as long as you specify the full path, and the root user has the appropriate file and directory permissions to execute the script.

Step 6 Click **OK**.

Step 7 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Configuring Alarms Sent to E-mail Addresses

You can configure alarms and events to be sent to e-mail addresses based upon alarm category or severity, device type, days of the week and hours within the day. You can configure multiple e-mail groups and define

To configure e-mail addresses:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 If a mail server is not configured, that is, the Mail Server field under Properties is blank, complete the following steps:

a. Under Properties, enter the mail server in the Mail Server field.

b. On the Alarms/Events Editor toolbar, click **Save Configuration**.

Note By default, Prime Performance Manager uses SMTP port 25. Should you need to change it to a different port, use the ppm smtpport command. See ppm smtpport, page B-75.

Step 4 On the Alarms/Events Editor toolbar, click **Add email address**.

Step 5 Enter the address(es) in the Add Email Address dialog box. If you are adding multiple addresses, use a semicolon to separate them.

Step 6 Click **OK**. The address(es) are added to the first row of the Email Addresses group at the bottom

Step 7 To configure the alarms and events you want sent to the addresses, in the address row click the **Set Filter** tool.

Step 8 In the Email Filter dialog box, uncheck the alarm and event categories and severities that you do not want to send to the OSS host. (By default, all categories and severities are enabled.)

- Categories—System, Network, and TCA.
- Severities—Critical, Major, Minor, Warning, Informational, Indeterminate, Normal.
- Device Types—Include all the device types that have been added to Prime Performance Manager.
- Applicable—Specifies the days of the week and time of day when you want alarms sent to the OSS host.

Step 9 Click **OK**.

Step 10 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Step 11 You can perform the following actions at any future point:

- Repeat Steps 4 through 10 to add another address row. This allows you to send different alarms and events to different e-mail addresses.
- Add a new address or delete an existing from an address row.
- Click **Resend events and/or alarms** to send the alarms and events to the addresses in an address row.
- Click **Delete this entry** to delete the address row.

Forwarding Traps Directly to Hosts

In certain circumstances, you might want to forward SNMP traps directly to other alarm-processing servers without any Prime Performance Manager interaction. To forward SNMP traps to other hosts and bypass Prime Performance Manager alarm processing:

- Add the host information to TrapForwarder.properties, then,
- Use ppm traprelay command to enable trap forwarding.

By default, TrapForwarder.properties resides in /opt/CSCOppm-gw/properties. Enter host information using the format:

```
SERVERxx=dest-address[,portno]
```

where:

- •xx—Is the user-defined server number.
- •dest-address—Is the hostname, or the IP address in IPv4 or IPv6 format.
- •portno—Is the optional port number. The default port number is 162.

For example:

```
SERVER01=64.102.86.104
SERVER02=64.102.86.104,162
SERVER03=2011::2:c671:feff:feb0:e1ee
SERVER04=2011::2:c671:feff:feb0:e1ee,162
```

After you make changes to TrapForwarder.properties file:

- Restart the gateway using the ppm restart command (see ppm restart, page B-56).
- Enable trap forwarding using the ppm traprelay command (see ppm traprelay, page B-76).

Tuning Event and Alarm Parameters

To modify Prime Performance Manager event and alarm parameters:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Alarms/Events Editor**.

Step 3 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 events.
- Maximum Alarms—Edit the maximum number of alarms that Prime Performance Manager should retain in the alarms database. The default is 25,000 alarms.
- Maximum Database Size—Edit the maximum database size that Prime Performance Manager should allow the database to reach. The default is 200,000 table rows.
- 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.
- Send Deletes—Indicates whether traps are sent to the OSS upstream host for deletes, True (default) or False.

Note Send Events, Send Alarms, Send Updates, and Send Deletes control the traps sent to the OSS host. For example, if Send Updates is false, Prime Performance Manager only sends traps when the alarm is raised, and not when it is updated.

- OSS 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 0 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, which means no trap is sent.
- Node Display Name—Sets the device display name in the Prime Performance Manager Alarms and Events window:
  - DNS or User Defined—Uses the device DNS or user-defined name (default).
  - IP Address—Uses the device IP address.
  - System Name—Uses the device system name.
  - Sync Name—Uses the device sync name.
  - Business Tag—Uses the device business tag.
  - Business Tag - DNS Name—Uses the device DNS name business tag.
  - Business Tag - System Name—Uses the device system name business tag.
  - Business Tag - Sync Name—Uses the device sync name business tag.
- Database Maintenance Interval—Sets the interval, in minutes, when the events database is updated based on the properties entered here. The default is 15 minutes.
- Automation Timeout—Sets the amount of time to wait, in seconds, before an OSS host automation script times out because it cannot execute, for whatever reason. (See Editing Upstream OSS Hosts, page 9-12 for information about adding automation scripts.) The default is 300 seconds.
- Event Automation: Disable Override—Specifies the event script priority if event automation scripts are entered for the OSS host and for thresholds.
  - True (default)—The OSS automation script and threshold script are executed.
  - False—Scripts entered for thresholds are executed when the trap is sent northbound not the script entered in for the OSS host.
- Mail Server—Enter the e-mail server to be used for e-mail addresses entered for TCAs (see Creating Thresholds, page 10-1) and OSS traps.

Step 4 When finished, on the Alarms/Events Editor toolbar, click **Save Configuration**.

Prime Performance Manager SNMP Traps

The following sections describe the OSS host traps used by Prime Performance Manager.

- CISCO-PRIME Notification Attributes, page 13-4
- CISCO-EPM-2 Trap Notification Attributes, page 13-5

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 9-3 describes the CISCO-PRIME notification attributes.

Table 9-3 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	Unused Varbind.
cenAlarmUpdatedTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.4	Unused Varbind.
cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	The unique alarm instance ID.
cenAlarmStatus (Integer32)	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Possible values: • 0—New • 1—Update • 2—Delete
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	Alarm nature: • ADAC(1)—Auto detected; auto cleared • ADMC(2)—Auto detected; manually cleared
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 the event category. Default Categories: <0,System> <1,Network> <2,TCA>
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, and 2 for IPv6 management.
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager gateway IP address. Set the server address to any address (0.0.0.0) if it is a SNMP v1 trap with an IPv6 address.
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	For service 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 Internet address type where the managed object is reachable. This value is set to 1 for IPV4 management, and 2 for IPv6 management.

Table 9-3 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
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.
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 (Integer32)	1.3.6.1.4.1.9.9.311.1.1.2.1.19	Unused varbind.
cenEventIDList (OCTET STRING)	1.3.6.1.4.1.9.9.311.1.1.2.1.20	Examples: Format: key=value; includes X.733 alarm type and probable cause. AlarmType=Communications ProbableCause=ThresholdCrossed NodeCreateTime=Alarm create time in device time zone NodeChangeTime=Alarm change time in device time zone NodeClearTime=Alarm clear time in device time zone NodeAckTime=Alarm acknowledgement time in device time zone VNEName=Prime Network VNE name, if applicable Other values can be set for different alarms and events.
cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	User input message.

Table 9-3 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	User input message. Value is “PPM”.
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 (Unsigned32)	1.3.6.1.4.1.9.9.311.1.1.2.1.25	Unused varbind.
cenPartitionName (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.26	Acknowledged by username/time.
cenCustomerIdentification (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.27	Cleared by username/time.
cenCustomerRevision (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.28	Create Time.
cenAlertID (SnmpAdminString)	1.3.6.1.4.1.9.9.311.1.1.2.1.29	Update Time.

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.

Table 9-4 describes the CISCO-EPM-2 notification attributes.

Table 9-4 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	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)
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 updated time indicates the last time a field changed and this alarm updated.
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

Table 9-4 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
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 event category. Default categories: <0,System> <1,Network> <2,TCA>
cenAlarmServerAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.11	The alarm server address type. This is set to 1 for IPV4 management and 2 for IPv6 management.
cenAlarmServerAddress	1.3.6.1.4.1.9.9.311.1.1.2.1.12	Prime Performance Manager gateway IP address. Set the server address to any address (0.0.0.0) if it is a SNMP v1 trap with an IPv6 address.
cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	For network and TCA alarms that pertain to a managed element, the value is Node. For alarms that pertain to Prime Performance Manager, the value is an empty string.
cenAlarmManagedObjectAddressType	1.3.6.1.4.1.9.9.311.1.1.2.1.14	The Internet address type where the managed object is reachable. This value is set to 1 for IPV4 management, and 2 for IPv6 management.
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 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 9-4 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 event severity. 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,-220 2 NodeClearTime=2010-06-17,23:31:41.516,-2202 NodeAckTime=2010-06-17,23:28:38.337,-2202 AlarmType=Communications; TCAValue=; TCAObject=; TCARelation=; TCAEvaluation=; TCAPeriod=;
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	The alarm mode. Values are either Alarm(2) Event(3)

Table 9-4 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
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	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"

CHAPTER 10

Configuring Thresholds

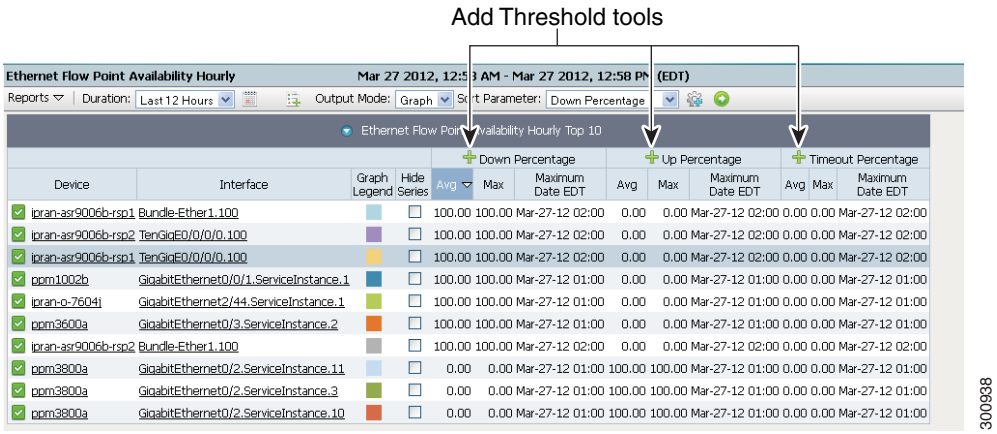
You can create thresholds for any key performance indicators (KPIs) displayed in Prime Performance Manager reports. Prime Performance Manager provides latitude in defining the alarm severities and onset and remission points. The following topics provide information about configuring thresholds in Prime Performance Manager:

- Creating Thresholds, page 10-1
- Managing Thresholds, page 10-5

Creating Thresholds

Prime Performance Manager allows you to create thresholds to generate alarms when a given report key performance indicator 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



You can create thresholds on device objects, such as CPUs, and memory pools. For example, if you navigate to the Resources CPU, click a slot or CPU. Thresholds can be created on the CPU utilization.

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 includes predefined thresholds that you can use as is or duplicate and modify to meet your needs. For a list of predefined thresholds, see Appendix C, "Predefined Thresholds."
- Prime Performance Manager validates your threshold entries based on the KPI type, either rising or falling. For a rising threshold, for example interface availability down 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:

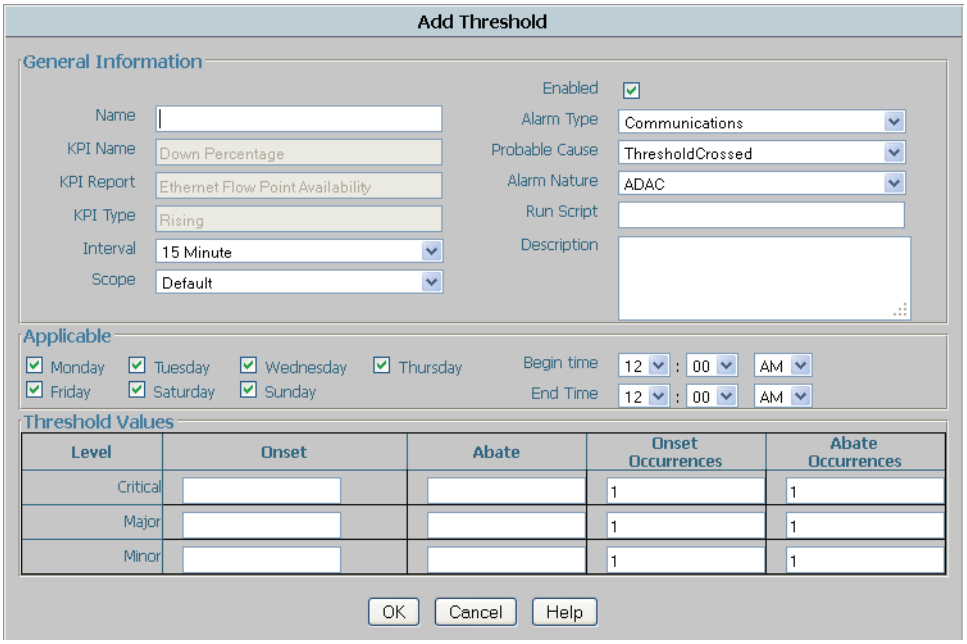
Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

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



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 when you want Prime Performance Manager to 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, "Managing Reports, Dashboards, and Views."

- 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.

Note If you create a threshold on a device element, for example, a CPU, the element will be displayed in the Scope, for example, "...CPUNum=123".

- 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 10-5**.
- Alarm Type—Indicate the alarm type you want raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Threshold Crossed is the default probably cause. If you want to assign a different probably cause, choose one from the displayed list.
- Alarm Nature—Choose the alarm nature ADAC (automatically detected and automatically cleared), or ADMC (automatically detected and manually cleared). ADAC is the default.

Note If you set Alarm Nature to ADMC, abate values are not allowed. If you change a threshold from ACAC to ADMC, any existing abate values are cleared.

- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. The script can reside anywhere on your file system as long as you specify the full path, and the root user has the appropriate file and directory permissions to execute the script. If you enter an OSS host automation script, you can specify whether the threshold script has priority. See Editing Upstream OSS Hosts, page 9-12 and Tuning Event and Alarm Parameters, page 9-15 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here. If you enter an e-mail address, an e-mail server must be entered in the Event Editor Mail Server field. (To display the Event Editor, from the Administration menu, choose **Event Editor**. For more information, see Tuning Event and Alarm Parameters, page 9-15.)

Note If you enter an e-mail address in the Mail To field here, it overrides e-mail addresses entered in the Event Editor Mail To field.

- Description—Add any notes, as needed, to help describe the threshold. The field accepts any alphanumeric text.
- Applicable—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. After selecting the days, enter the beginning and ending time in the Begin Time and End Time fields (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, from the Network menu, choose **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 Thresholds Editor, shown in Figure 10-3. The editor displays thresholds added from the Prime Performance Manager reports GUI (see Creating Thresholds, page 10-1), and ones created using an XML editor and added directly to the gateway. Threshold management is covered in the following topics:

Editing Thresholds from the Threshold Editor, page 10-5

Enabling and Disabling Thresholds, page 10-8

Deleting Thresholds, page 10-9

Editing Thresholds from the Alarms Window, page 10-6

Viewing Threshold Events, page 10-9

Editing Thresholds from the Threshold Editor

You can edit thresholds either by displaying the Threshold Editor, selecting a threshold, and entering your edits, or by selecting a threshold alarm in the Active Alarms window and editing the threshold there.

To edit a threshold using the Threshold Editor:

Step 1 Log into Prime Performance Manager GUI as a Network Operator or higher user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to edit, click **Edit This [*Rising/Falling*] Threshold**.

Step 4 In the Edit Thresholds dialog box, edit any of the following values.

Note Only brief parameter descriptions are provided here. For detailed descriptions, see Creating Thresholds, page 10-1.

- Name—The threshold name (not editable).
- KPI Name—The key performance indicator name (not editable).
- KPI Report—The report containing the KPI (not editable).
- KPI Type—The KPI type, either rising or falling (not editable).
- Enabled—Enables and disables the threshold.
- Alarm Type—Indicate the alarm type you that is raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Indicates the TCA probable cause.
- Alarm Nature—Indicates the alarm nature, either ADAC or ADMC.
- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. See Editing Upstream OSS Hosts, page 9-12 and Tuning Event and Alarm Parameters, page 9-15 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here.
- Description—Edit or add any threshold notes.

- Applicable—Edit the days for which you want the threshold applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical

Step 5 When finished, click **OK**.

The edits are displayed in the Thresholds Editor.

Editing Thresholds from the Alarms Window

From the Prime Performance Manager Alarms window can perform the following perform the following actions from a threshold crossing alarm:

- Display 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 display the threshold parameters from the Alarms window:

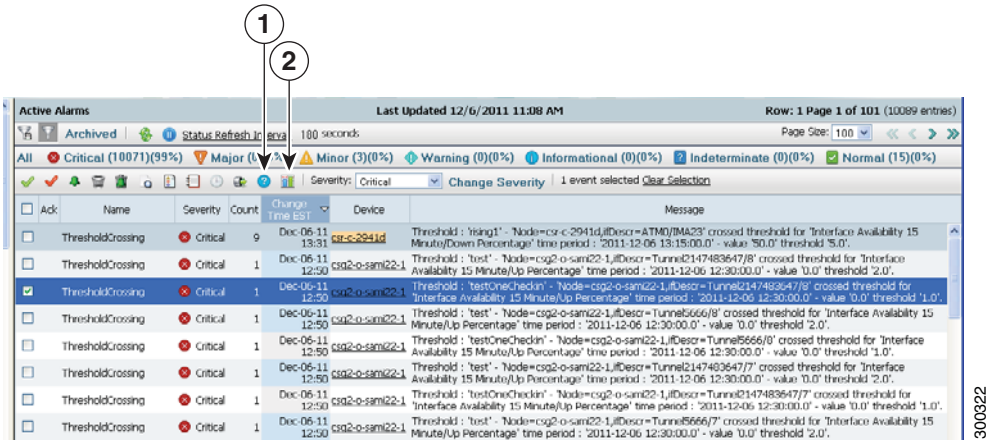
Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Network menu, choose **Alarms/Events**.

Step 3 In the Active Alarms window (Figure 10-3), choose a Threshold Crossing alarm.

Step 4 From the Active Alarms window toolbar, click **Help for Event**.

Figure 10-3 Displaying Threshold Parameters from the Alarms Window



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.

Note Only brief parameter descriptions are provided here. For detailed descriptions, see Creating Thresholds, page 10-1.

- Name—The threshold name (not editable).
- KPI Name—The key performance indicator name (not editable).
- KPI Report—The report containing the KPI (not editable).
- KPI Type—The KPI type, either rising or falling (not editable).
- Interval—The the frequency at which Prime Performance Manager checks the data point value identified by the threshold.
- Scope—Set the threshold scope (not editable).
- Enabled—Enables and disables the threshold.
- Alarm Type—Indicates the alarm type that is raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Indicates the TCA probable cause.
- Alarm Nature—Indicates the alarm nature, either ADAC or ADMC.
- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. See Editing Upstream OSS Hosts, page 9-12 and Tuning Event and Alarm Parameters, page 9-15 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here.
- Description—Edit or add any threshold notes.
- Applicable—Edit the days for which you want the threshold applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical

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**. A threshold report is displayed. The report is in graph format by default. For information about

The threshold crossing report window appears.

Step 8 When finished, click **OK**.

Duplicating Thresholds

You might occasionally want to create a new threshold with only one or two changes from an existing threshold. If so, you can duplicate the existing threshold, modify the parameters and save the new threshold.

To duplicate a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to edit, click **Duplicate This Threshold**.

Step 4 In the Duplicate Threshold dialog box, edit any of the following values.

Note Only brief parameter descriptions are provided here. For detailed descriptions, see Creating Thresholds, page 10-1.

- Name—The original threshold name is displayed with "duplicate" appended at the end. You can edit the threshold name. The name must be unique.
- KPI Name—The key performance indicator name (not editable).
- KPI Report—The report containing the KPI (not editable).
- KPI Type—The KPI type, either rising or falling (not editable).
- Interval—The the frequency at which Prime Performance Manager checks the data point value identified by the threshold.
- Scope—Set the threshold scope (not editable).
- Enabled—Enables and disables the threshold.
- Alarm Type—Indicate the alarm type you that is raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Indicates the TCA probable cause.
- Alarm Nature—Indicates the alarm nature, either ADAC or ADMC.
- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. See Editing Upstream OSS Hosts, page 9-12 and Tuning Event and Alarm Parameters, page 9-15 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here.
- Description—Edit or add any threshold notes.
- Applicable—Edit the days for which you want the threshold applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical

Step 5 Click **OK**.

Enabling and Disabling Thresholds

To enable or disable a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Threshold Editor**.

Step 3 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 from the Alarms Window" procedure on page 10-6.

Deleting Thresholds

To delete a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Administration menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to delete, click the **Delete This Threshold** tool.

Step 4 On the confirmation, click **OK**.

Prime Performance Manager will remove the threshold from the table.

Viewing Threshold Events

To view threshold events, from the Navigation menu, choose **Alarms/Events**, then click **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

Displaying System Properties, Statuses, Messages, and Logs

You can display system properties, settings, statuses, messages, and logs to monitor and manage ongoing Prime Performance Manager performance. Properties, settings, statuses, messages, and logs are all accessed through the Prime Performance Manager System menu. The following topics describe how to display this information:

- System Properties, Statuses, Logs, and Messages Overview, page 11-1
- Displaying Connected Clients and System Status, page 11-2
- Displaying System Logs, page 11-4
- Managing Log Files, page 11-7
- Displaying System Properties and Settings, page 11-8
- Displaying System Messages, page 11-11

Note If Prime Performance Manager user-based access is enabled (see Setting Up User Access and Security, page 6-1), only Administrator users can view all administration options. Administrative menu options are not visible to Operator and lower users.

System Properties, Statuses, Logs, and Messages Overview

The Prime Performance Manager System menu allows you to display Prime Performance Manager statuses, properties, settings, logs, and messages. Table 11-1 provides an overview to the logs, messages, and information displayed from the System menu.

Table 11-1 System Menu Logs and Messages

Menu > Path	Source	For information, see:
System > Status > • Connected Clients • Status • System Versions • System Check • Install Locations • IP Access List	Displays the output of these commands: • ppm who • ppm status • ppm version • ppm checksystem • ppm ipaccess	Displaying Connected Clients and System Status, page 11-2.
System > Logs > • Install Log • Patch Log • Console Log • Backup Log • CLI Command Log • Event Automation Log • Security Log • Application Audit Log • Console Log Archives	Displays the contents of these system logs: • cisco_primepm_gw_install.log • sgmConsoleLog.txt • ppmBackupLog.txt • Command Log • eventAutomationLog.txt • sgmSecurityLog.txt • Application Audit Logs	Displaying System Logs, page 11-4.
System > Messages	Displays tabular information on system messages, including errors, information, trace, debug, dump, SNMP, and archived messages.	Displaying System Messages, page 11-11.
Administration > System Settings • System Settings • Poller Settings • Web Settings • Report Settings	Displays the contents of these system property files: • System.properties • Server.properties • WebConfig.properties • Reports.properties	Displaying System Settings, page 11-8.

Displaying Connected Clients and System Status

Prime Performance Manager allows you to display connected clients and system status. It also allows you to run a system check. You can also display an updated system status. To display this information, from the System menu, choose **System Status**, then choose one of the following:

- **Connected Clients**—Lists all Prime Performance Manager clients that are currently connected to the Prime Performance Manager gateway. These include:
  - PPM Clients—The Prime Performance Manager registered message observers, for example TrapGeneratorMsgHandler, EventPollerProcessor, and others.

  - Registered Units—The Prime Performance Manager registered unit(s) connected to the gateway.
  - Registered Web Clients—Users who are logged into the server. If user access is enabled (see Setting Up User Access and Security, page 6-1), the username is displayed. Otherwise, only the user hostname and IP address is provided.
  - Linux—Linux users that are logged into the Prime Performance Manager server.
  - Solaris—Solaris users that are logged into the Prime Performance Manager server.

Note You can also use the ppm who command to display connected clients.

- **System Status—**Displays the status of the Prime Performance Manager gateway and units, including version, install date, and hostname, as well as the status of gateway and unit processes, for example:

```
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.
```

Note You can also use the ppm status to display the system status.

- **System Version**—Lists the Prime Performance Manager software versions installed on the gateway and units, plus additional information including installation date, gateway and unit hostname, and SSL status.

Note You can also use the ppm version command to display the Prime Performance Manager software versions.

- **System Check**—Checks the gateway or unit server installation including:
  - Server RAM, CPU, and SWAP
  - TCP/IP address and port usage
  - Disk space usage

Note You can also use the ppm checksystem command to check the system.

- **Install Locations**—Displays the gateway and unit installation location. Output is:

```
SRG=/opt/CSCOppm-gw;export SRG SRU=/opt/CSCOppm-unit;export SRU
```

  SRG is the source root gateway directory and SRU is the source root unit directory.

Note You can also use the ppm rootvars command to display the gateway and unit installation location.

- **IP Access List**—Displays the IP addresses that can access the gateway. By default, all IP addresses can access the gateway. You can restrict access to specific IP addresses using the ppm ipaccess command.

Displaying System Logs

Prime Performance Manager provides the following system logs where you can view information about Prime Performance Manager processes and errors. These logs are described in the following topics:

- Displaying the Install Log, page 11-4
- Displaying the Patch Log, page 11-4
- Displaying the Console Log, page 11-5
- Displaying the System Check Log, page 11-5
- Displaying the Backup Log, page 11-5
- Displaying the CLI Command Log, page 11-5
- Displaying the Event Automation Log, page 11-6
- Displaying the Security Log, page 11-6
- Displaying the Application Audit Logs, page 11-7
- Displaying the Console Log Archived Messages, page 11-7

Displaying the Install Log

The install log displays the contents of Prime Performance Manager installation log file for the server to which you are connected that is running Prime Performance Manager. Information includes the date and time of the installation, results of the system requirements check, and the installation sequence.

To display the Install Log, you can:

- Choose **System Logs > Install Log** from the System menu, or
- Run the **ppm installlog** command.

Displaying the Patch Log

The patch log displays the Prime Performance Manager patches that have been installed. To display the Patch Log, you can:

- Choose **System Logs > Patch Log** from the System menu, or
- Run the **ppm patchlog** command.

Note If no patches are installed, a “File does not exist” message is displayed.

Displaying 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 that is currently running Prime Performance Manager. The console log file contains Prime Performance Manager server error and warning messages, 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.

To display the console log, you can:

- Choose **Logs > Console Log** from the System menu, or
- Run the **ppm console** command.

Displaying the System Check Log

The system check log displays the results of the last check of the server where Prime Performance Manager is installed, including RAM CPU, swap space, DNS, TCP/IP port usage, and other properties. To display the console log, you can:

- Choose **Logs > System Check Log** from the System menu, or
- Run the **ppm checksystem** command.

Displaying the Backup Log

The backup log displays the contents of Prime Performance Manager backup log file for the server to which you are connected that 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 display the Backup log, you can:

- Choose **Logs > Backup Log** from the System menu, or
- Run the **ppm backuplog** command.

Displaying the CLI 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 that is currently running on the Prime Performance Manager server. The 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 display the command log, you can:

- Choose **Logs** > CLI **Command Log** from the System menu, or
- Run the **ppm cmdlog** command.

The Prime Performance Manager command log table is displayed. Command log table columns include Timestamp, User Name, and Command. To sort the table, click the column header, for example, to sort by username, click the **User Name** column.

Displaying 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 that 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 display the event automation log, you can:

- Choose **Logs > Event Automation Log** from the System menu, or
- Run the **ppm eventautolog** command.

Related Topics

Displaying the Security Log, page 11-6

Displaying the Application Audit Logs, page 11-7

Displaying 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 that 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 display the security log, you can:

- Choose **Logs > Security Log** from the System menu, or
- Run the **ppm seclog** command.

Note You must be an System Administrator to access security log.

The Prime Performance Manager security log table is displayed. Columns include Timestamp, User Name, Message, and Command. To sort the table, click the column header, for example, to sort by user, click the **User Name** column.

Displaying the Application Audit Logs

The application audit logs page displays daily audit files listing all applications that have accessed Prime Performance Manager server. The application audit log lists all access messages that are logged for the Prime Performance Manager server and provides 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 application audit log file is /opt/CSCOppm-gw/tomcat/logs/localhost_access_log.*date*.txt. If you installed Prime Performance Manager in a directory other than /opt, then the application audit log file is in that directory.

To display the application audit log, you can:

- Choose **Logs > Application Audit Logs** from the System menu, or
- Run the **ppm who** command.

Displaying the Console Log Archived Messages

The system console archives displays all archived system console messages. To display the console log through the Prime Performance Manager GUI:

- From the System menu, choose Logs, then choose **Console Log Archives**.

Console log 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 that is currently running Prime Performance Manager. If you restart the server, Prime Performance Manager creates a new file.

To view archived messages, click a timestamp. The Console Archive: Last *number* All Messages page displays all console messages that were in the system log at the time specified by the timestamp.

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-44.
- **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-37.
- **ppm logtimemode**—Sets the log file time mode for dates. For more information, see ppm logtimemode, page B-38.
- **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-43.

Displaying System Properties and Settings

Prime Performance Manager system, server, web, and report properties and settings are stored in the /opt/CSCOppm-gw/properties directory. These properties and settings are described in the following topics:

- Displaying System Settings, page 11-8
- Displaying Poller Settings, page 11-9
- Displaying Web Settings, page 11-9
- Displaying Reports Settings, page 11-10

Displaying System Settings

The Prime Performance Manager system properties file displays server and client properties that control various Prime Performance Manager configuration parameters. System properties are stored in:

```
/opt/CSCOppm-gw/properties/System.properties
```

To access the system properties through the Prime Performance Manager GUI, choose **System Settings** from the Administration menu.

Table 11-2 shows commands that you can use to change system properties.

Table 11-2 Commands to Change System Properties

System Property	Command
BACKUP_RMIPORT	ppm backup, page B-8
BACKUP_SERVER	
BACKUP_WEBPORT	
BADLOGIN_TRIES_ALARM	ppm badloginalarm, page B-12
BADLOGIN_TRIES_DISABLE	ppm badlogindisable, page B-12
CHART_MAX_WINDOW	
CONSOLE_ARCHIVE_DIR_MAX_SIZE	ppm msglogage, page B-43
CONSOLE_LOG_MAX_SIZE	ppm consolelogsize, page B-16
CSV_STRING_DELIMITER	
CW2K_SERVER	ppm datadir, page B-17
CW2K_WEB_PORT	
CW2K_SECURE_WEB_PORT	
JSP_PORT	ppm jspport, page B-34
LOGAGE	ppm msglogage, page B-43
LOGDIR	ppm msglogdir, page B-44
LOGSIZE	ppm logsize, page B-37
LOGTIMEMODE	ppm logtimemode, page B-38
LOG_TROUBLESHOOTING	ppm maxrepqueries, page B-40
PERSISTENCEDIR	ppm datadir, page B-17

Table 11-2 Commands to Change System Properties (continued)

System Property	Command
PROMPT_CREDS	ppm setpctrapdestination, page B-61
SBACKUPDIR	ppm backupdir, page B-10
SERVER_NAME	ppm servername, page B-59
SNMPCONFFILE	ppm snmpconf, page B-63
SSL_ENABLE	ppm ssl, page B-71
TRAP_LIST_ENABLE	ppm uninstall, page B-78

Displaying Poller Settings

The poller settings file contains various properties that control Prime Performance Manager polling, such as the delete aging timeout, status polling interval drift percentage, and many other settings. Poller settings are stored in:

```
/opt/CSCOppm-gw/properties/Server.properties
```

To access the poller settings through the Prime Performance Manager GUI, from the Administration menu, choose **System Settings**, then choose **Poller Settings**.

You can change the SNMP_MAX_ROWS property using the ppm snmpmaxrows command. (See ppm snmpmaxrows, page B-66.) To change other poller settings in the Server.properties file, see the "Changing the GUI Polling Refresh Setting" section on page 3-13.

Displaying Web Settings

The web settings file contains properties that control the configuration of Prime Performance Manager web interface. For example:

```
MAX_ASCII_ROWS      = 6000

# This is the default page size that is selected
# if a cookie has not been set or the maxPageSize parameeter
# is not found in the request parameters.
MAX_HTML_ROWS       = 200

# 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
```

Web settings are stored in:

```
/opt/CSCOppm-gw/properties/WebConfig.properties
```

To access the web settings through the Prime Performance Manager GUI, from the Administration menu, choose **System Settings**, then choose **Web Settings**. Table 11-3 describes the web settings.

Table 11-3 Web Settings

Web Setting	Description
MAX_ASCII_ROWS	Controls the size of the rows shown the message log archives debug log where contents are placed into one large page without any table rows. The default value is 6000 rows. To modify this setting, see **ppm maxasciirows, page B-39.**
MAX_HTML_ROWS	Sets 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. The command allows you to set the page size (if you have not explicitly chosen a page size). After you select a page size, Prime Performance Manager remembers your preference until you delete your browser cookies. The default value is 100 rows. To modify this setting, see **ppm maxhtmlrows, page B-39.**
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. To modify this setting, see **ppm maxpagesize, page B-40.**
LOG_UPDATE_INTERVAL	The valid range is 1 second to an unlimited number of seconds. The default value is 300 seconds (5 minutes).
MAX_EV_HIST	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 search results to the web browser, where the results are further limited by settings specified by the ppm maxhtmlrows command. The valid range is one row to an unlimited number of rows. The default value is 15,000 rows.

Each of the web configuration commands requires you to be logged in as the root user.

Displaying Reports Settings

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
```

Prime Performance Manager displays the reports settings contents in:

```
/opt/CSCOppm-gw/properties/Reports.properties
```

To access the report settings through the Prime Performance Manager GUI, choose **Report Settings** from the Administration menu.

Displaying System Messages

Prime Performance Manager provides a variety of messages to help you monitor errors, user actions, and other information. The following topics describe the available messages.

Note These messages are related to Prime Performance Manager system itself, not to your network.

- Displaying Information and Error Messages, page 11-11
- Displaying User Actions, page 11-12
- Displaying Archived Messages, page 11-13

Displaying Information and Error Messages

Information and error messages recorded in the Prime Performance Manager system log provide information about Prime Performance Manager operations to help you monitor and diagnose problems.

To access the information and error messages through the Prime Performance Manager GUI, choose **Messages** from the System menu.

Table 11-4 describes the information and error message table columns.

Table 11-4 Information and Error Message Information

Column	Description
Period (in heading)	Table collection period, such as *Since Server Restart*.
Timestamp (in heading)	Date and time that Prime Performance Manager last updated the message information.
Row	Unique number identifying each entry in the table.

Table 11-4 Information and Error Message Information (continued)

Column	Description
Time	Date and time the message was logged.
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 useful 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.

You can filter information and error message displays to a single information or error message type. To filter the messages to a single type, click one of the following message types located just above the table header:

- **Error**
- **Info**
- **Trace**
- **Debug**
- **Dump**
- **SNMP**
- **All**
- **Archive**

Additionally, you can reduce the number of messages displayed by clicking **10/Page**, to limit the messages to 10 per page, up to 500 per page. Max/Page displays the maximum number of messages per page. DefPrefs restores the default preferences, and Reload reloads the messages.

Displaying User Actions

User actions recorded in the Prime Performance Manager system log provide information about Prime Performance Manager user activities. To access user actions through the Prime Performance Manager GUI, choose **User Actions** from the System menu.

Table 11-5 describes the user actions table columns. To sort the table, click a column header, for example, to sort by time, click the **Time** column.

Table 11-5 User Actions

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.

Table 11-5 User Actions (continued)

Column	Description
Time	Date and time the message was logged.
Class	The type of user action: • **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. • **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. • **LogInOut**—Login event. A user has logged into Prime Performance Manager.
Message	Message text.

You can filter the actions to display only a single user action type. To filter the messages, click an action type located just above the table header: **Create**, **Delete**, **Discover**, **Edit**, **Ignore**, **OverWrite**, **Poll**, **Purge**, **LogInOut**.

Additionally, you can reduce the number of messages displayed by clicking **10/Page**, to limit the messages to 10 per page, up to 500 per page. Max/Page displays the maximum number of messages per page. DefPrefs restores the default preferences, and Reload reloads the messages.

Displaying Archived Messages

Prime Performance Manager archives the following messages in system logs: error, informational, trace, debug, dump, user actions, SNMP.

Each archived file contains all Prime Performance Manager system messages for a single session for the server to which you are connected that is currently running on the Prime Performance Manager. If you restart the server, Prime Performance Manager creates a new file.

Messages are archived by timestamp. To view archived messages, click a timestamp. All messages that were in the system log at the time specified in the timestamp are displayed. You might 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.

To access the archived messages through the Prime Performance Manager GUI, from the System menu. choose **Messages**, then click **Archives**. Table 11-6 describes the archive message information.

Table 11-6 Archived Messages

Description	Information
Index	Message number Prime Performance Manager assigns to the message.
Time	Date and time the message was logged.
Type	Message type: • Action • Debug • Dump • Error • Info • SNMP • Trace
Source	Message source in 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 helpful when two or more clients connected to the same Prime Performance Manager gateway are running on the same device.
Task	Task, or thread, that logged the message.
Message	Text of the message.

CHAPTER 12

Managing Gateways and Units

Prime Performance Manager gateway and unit management includes:

- Displaying gateway and unit information.
- Managing device-to-unit assignments.
- Creating and managing unit protection groups.
- Creating and managing local and geographical gateway high availability.

The following topics describe gateway and unit management:

- Displaying Gateway and Unit Information, page 12-1
- Managing Device-to-Unit Assignments, page 12-5
- Creating Unit Protection Groups, page 12-8
- Unit Protection Group Failover Scenarios, page 12-11
- Managing Gateway High Availability, page 12-11

Displaying Gateway and Unit Information

Prime Performance Manager allows you to view information about the gateways and units that are provisioned including details about the gateway and unit servers, alarms, events, and device-to-unit distributions. In addition, you can view more detailed server information including CPU, memory, and disk space utilization, user statistics, and other detailed information.

To display gateway and unit server statistics, from the Performance menu, choose **Dashboards**, then choose **Server Health Dashboards**. The following dashboards are displayed:

- Server CPU/Memory/Disk—Displays CPU, memory, and disk and swap space utilization.
- Server CPU/Memory/DiskIO—Displays CPU and memory utilization and disk read and write bytes.
- Server CPU/Memory/Interface—Displays CPU, memory, and interface utilization, and interface error and discard percentages.
- Server CPU/Memory/Temperature—Displays CPU and memory utilization and CPU temperatures.
- Server Disk—Displays disk and swap space utilization and disk read and write bytes.
- Server Processes/Users—Displays server process and user statistics.

Note Gateway and unit statistics appear require the gateway and unit to added as a Prime Performance Manager device. For information, see Discovering Gateways and Units, page 5-2.

To display general gateway and unit information, from the System menu, choose **Gateway/Units**. The System Gateway/Units window displays the gateway and unit properties listed in Table 12-1.

Table 12-1 Gateway and Unit Properties

Column	Description
Internal ID[1]	Gateway or unit internal ID. Prime Performance Manager assigns the ID for its internal use.
Display Name	Gateway or unit or display name.
Custom Name	Gateway or unit or display name custom name, if created.
IP Address or DNS Hostname	Gateway or unit IP address or DNS name.
Primary SNMP Address	Gateway or unit SNMP IP address.
Redundancy Group[1]	If the unit belongs to a redundancy group, the redundancy group name. See Creating Unit Protection Groups, page 12-8.
Primary/Redundant[1]	If the unit belongs to a redundancy group, the unit role in the group, either Primary or Redundant.
Type	Description of the device type, either gateway or unit.
Connection Time	Connection time with the server to a unit or gateway.
In Service	Total time the gateway or unit is in service.
Last Status Change[1]	Date and time that the status of the gateway or unit last changed.
Status	Current status of the unit or gateway. Possible values are: • Active • Standby • Discovering • Polling • Unknown • Unmanaged • Waiting • Warning
Status Reason	Reason for the current status. For a full list of possible reasons, see the *stateReasons.html* file, located in the following directory: `/opt/CSCOppm-gw/apache/share/htdocs/eventHelp` If you cannot see all of the status reason, place the cursor over the cell to see the full text in a tooltip.
Out of Sync	If the gateway is installed in a geographical HA configuration, indicates whether the primary gateway database is out of sync to the secondary one.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-13.

To display detailed gateway or unit information, select the gateway or unit in the navigation area. Table 12-2 lists the information that is displayed.

Note The Reports, Dashboards, and Report Status tabs require the gateway and unit to added as a Prime Performance Manager device. For information, see Discovering Gateways and Units, page 5-2.

Table 12-2 Detailed Gateway and Unit Properties

Tab	Description
Reports	Displays gateway or unit reports. These are the same reports you see when choosing **Devices** from the Network menu, selecting the gateway or unit from the device list and clicking the **Reports** tab. For more information, see Managing Reports, Dashboards, and Views, page 7-1.
Dashboards	Displays gateway or unit dashboards. These are the same dashboards you see when choosing **Devices** from the Network menu, selecting the gateway or unit from the device list and clicking the **Dashboards** tab. For more information, see Managing Reports, Dashboards, and Views, page 7-1.
Details	Provides detailed gateway or unit information. For a description of the detailed gateway and unit information, see Displaying Detailed Gateway and Unit Information and Performance, page 12-3
Event History	Displays the gateway or unit event history. For a description of the event properties, see Displaying Active Alarms and Event History, page 9-1.
Active Alarms	Displays the gateway or unit active alarms. For a description of the alarm properties, see Displaying Active Alarms and Event History, page 9-1.
Report Status	Displays the status of reports generated from the gateway or unit and allows you to enable or disable them. For more information, see Managing Reports, Dashboards, and Views, page 7-1.
Devices for Unit (Units only)	Displays the devices assigned to the selected unit. For a description of device properties, see Displaying Network-Level Device Properties, page 8-2.
Device Distributions for Unit (Units only)	Displays the device distributions for the selected unit. For a description of device properties, see Displaying Device Type Distributions, page 8-4.

Displaying Detailed Gateway and Unit Information and Performance

To display detailed Prime Performance Manager gateway and unit naming, status, and performance information:

Step 1 From the System menu, choose **Gateways/Units**.

Step 2 In the System Gateway/Units window, click the link of the gateway or unit whose detailed information and status you want to view.

Step 3 In the gateway or unit window, click **Details**.

The following gateway or unit information is displayed:

- Naming Information
  - Display Name—The gateway or unit display name.
  - Custom Name—The gateway or unit custom name.
  - DNS Name—The gateway or unit DNS name.
  - IP Address—The gateway or unit IP address.
  - Type—The type, either gateway or unit.
  - In Service—Indicates whether the gateway or unit is in service.
  - Connection Time—Provides the gateway or unit connection time.
- Status Information
  - Alarm Severity—The severity of the highest alarm on the gateway or unit.
  - Status—The gateway or unit status, either Active or Inactive.
  - Last Status Change—The date and time of the last status change.
  - Status Reason—The date and time of the last status change.
- Server Hardware Performance
  - Average CPU Utilization (Last 15 Min)—CPU utilization within the last 15 minutes.
  - Average CPU Utilization (Last 60 Min)—CPU utilization within the last 60 minutes.
  - Avg Server Memory Utilization (Last 15 Min)—Server memory utilization within the last 15 minutes.
  - Avg Server Memory Utilization (Last 60 Min)—Server memory utilization within the last 60 minutes.

Note Utilization data text color is based on the Utilization Color Settings defined in User Preferences. For information, see Changing User Preferences, page 3-7.

- Gateway (or Unit) Performance
  - Max JVM Memory Utilization (Last 15 Min)—Maximum Java Virtual Machine (JVM) utilization within the last 15 minutes.
  - Max JVM Memory Utilization (Last 60 Min)—Maximum JVM memory utilization within the last 60 minutes.
  - Avg JVM Memory Utilization (Last 15 Min)—Average JVM memory utilization within the last 15 minutes.
  - Avg JVM Memory Utilization (Last 60 Min)—Average JVM memory utilization within the last 60 minutes.

Note Utilization data text color is based on the Utilization Color Settings defined in User Preferences. For information, see Changing User Preferences, page 3-7.

- Average Scheduler Queue Size—Average scheduler queue size. This indicates the number of polling requests that are waiting in queue. 0 indicates polling requests are being processed normally. An increasing number indicates a backlog exists that might result in polling delays. To investigate, check the number of active Go Live sessions and reports with 1-minute polling enabled. For additional information, see Displaying Network and Device Reports, page 7-6.
- Persistence Directory Disk Usage—The usage data for the Prime Performance Manager directory where Prime Performance Manager data files are stored (/opt/CSCOppm-gw/data/ or /opt/CSCOppm-unit/data) MB or GB used and MB or GB available.
- Log Directory Disk Usage—The usage data for the Prime Performance Manager log directory (/opt/CSCOppm-gw/logs/ or /opt/CSCOppm-unit/logs) MB or GB used and MB or GB available.
- Report Directory Disk Usage—The usage data for the Prime Performance Manager reports directory (/opt/CSCOppm-gw/reports/ or /opt/CSCOppm-unit/reports) MB or GB used and MB or GB available.
- Backup Directory Disk Usage—The usage data for the Prime Performance Manager backup directory (/opt/) MB or GB used and MB or GB available.

Managing Gateway and Unit Connectivity

Gateway to unit connectivity requires that the unit hostname be resolvable on the gateway. To ensure gateway-to-unit connectivity is lost due to an unresolved unit hostname, you can perform any of the following actions:

- On the unit, use the unit IP address as its server name not its hostname:

```
/opt/CSCOppm-unit/bin/ppm servername = 1.2.3.4
```

- On the gateway add an entry to the /etc/hosts file for the unit.
- Add a DNS entry for the unit.

Managing Device-to-Unit Assignments

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:

- Displaying Device-to-Unit Assignments, page 12-6
- Creating Device-to-Unit Maps, page 12-6
- Editing Device-to-Unit Maps, page 12-7
- Deleting Device-to-Unit Maps, page 12-7
- Changing a Device-to-Unit Assignment, page 12-8

Displaying Device-to-Unit Assignments

If your Prime Performance Manager implementation has only one unit, all devices in your network are assigned to it. If you have allocated devices to multiple units, an easy way to view the device-to-unit assignments is to add the Unit parameter to the Devices table. To do this:

Step 1 From the Network menu, choose **Devices**.

Step 2 Right-click the table header and add the Unit parameter.

Step 3 Click **Apply**. (The Apply button is located at the bottom of the parameter list.)

For additional information, see:

- Displaying Network-Level Device Information, page 8-1
- Creating and Editing Device Polling Groups, page 8-22

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 a System Administrator user.

Step 2 From the Administration menu, choose **Unit Editor**.

Step 3 On the Unit Editor toolbar, click **Add a Device to Unit Map**.

Step 4 In the Add Device to Unit Map dialog box, enter the following:

- IP Address Range or Hostname—Enter the device IP ad dress, device IP address range, or hostname 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 5 Click **OK**.

The map is added to the Unit Editor table.

Step 6 Repeat Steps 3 through 5 until you have completed the device maps that you want.

Step 7 In the Unit Editor toolbar, click **Save all Unit Entries**.

Step 8 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 5, "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 a System Administrator user.

Step 2 From the Administration menu, choose **Unit Editor**.

Step 3 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 hostname.
- 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 4 When you are finished, in the Unit Editor toolbar, click **Save all Unit Entries**.

Step 5 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 a System Administrator user.

Step 2 From the Administration menu, choose **Unit Editor**.

Step 3 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 4 When you are finished, in the Unit Editor toolbar, click **Save all Unit Entries**.

Step 5 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-to-Unit Assignment

If your network has multiple Prime Performance Manager units, you can change the device unit assignment by editing the device-to-unit map. (See Editing Device-to-Unit Maps, page 12-7.) You can also change the device unit assignment by individual device in the Devices window.

To change a device assignment:

Step 1 Log into the Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **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**.

Note This option is greyed if only one unit is available.

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.

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.

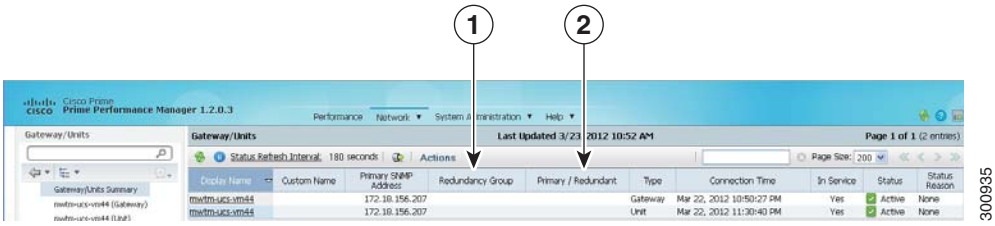
- **delete** [*group name*]—Deletes a redundancy group. The unit redundancy mode is not checked.

- **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 12-1. 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.

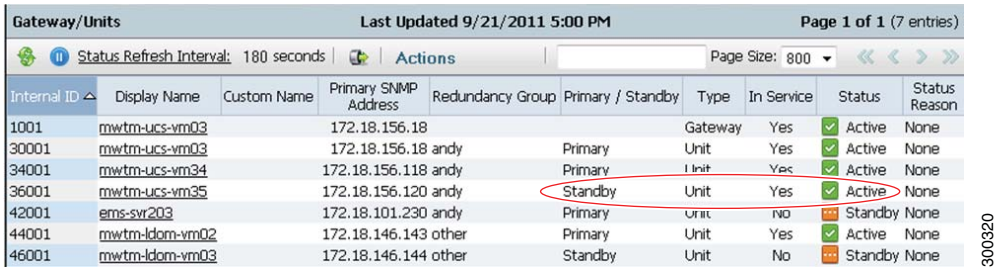
Figure 12-1 Protection Groups



1	Redundancy Group column.	**3**	Status column.
2	Primary/Redundant column.		

Figure 12-2 shows a redundant unit that has been switched to active status.

Figure 12-2 Redundant Units in Active Status



Unit Protection Group Failover Scenarios

Table 12-3 describes the unit protection group and failover behavior after common network circumstances occur.

Table 12-3 Unit Protection Group Failover Scenarios

Circumstance	Response
Unit is shut down or fails.	The gateway waits for the delay time configured for the protection group. After the gateway determines the unit is down, it forces a failover of its devices to the redundant unit. The redundant unit begins collecting statistics for the devices; it 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.
Connectivity between a gateway and unit is lost.	The redundant unit picks up for the “failed” unit and takes ownership of its 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, because it cannot connect 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, so 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.
The gateway is brought down or fails.	The unit continues to process devices and queue data for the gateway. After the gateway is restored, the unit forwards the queued data to it. Because the gateway contains the unit protection group configuration information, a gateway failure causes the unit redundancy to be lost. 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.

Managing Gateway High Availability

Prime Performance Manager provides both local and geographical high availability. HA installations include:

- Local HA only
- Geographical HA only
- Local and geographical HA

Prime Performance Manager HA management procedures are provided in the following topics:

- Managing Local High Availability, page 12-12
- Managing Geographical High Availability, page 12-18
- Managing Geographical and Local High Availability, page 12-25

Managing Local High Availability

For local HA, Prime Performance Manager uses the Red Hat Cluster Suite (RHCS) provided with the Red Hat Enterprise Linux 5.5 (RHEL 5.5), Red Hat Enterprise Linux 5.7 (RHEL 5.7), Red Hat Enterprise Linux 5.8 (RHEL 5.8) Advanced Program.

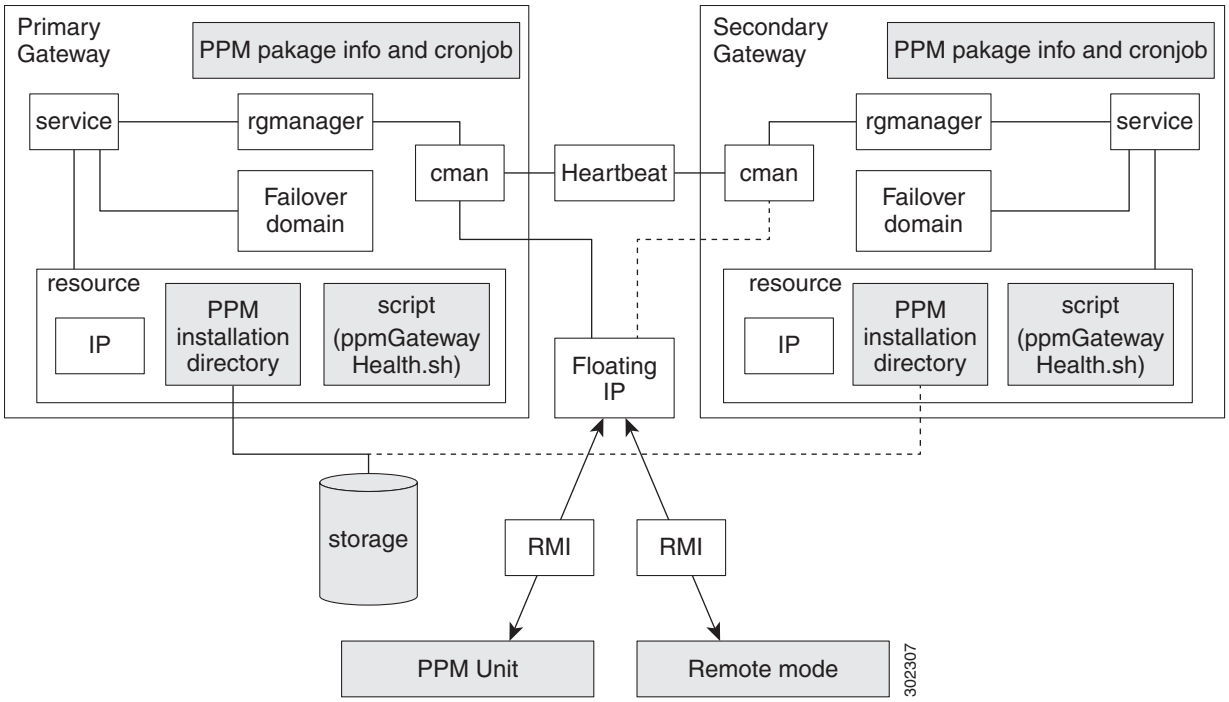
The RHCS cluster infrastructure provides the basic functions that allow the Prime Performance Manager gateways to work together as a cluster. RHCS components include:

- **Cluster infrastructure**—Provides fundamental functions for nodes to work together as a cluster: configuration-file management, membership management, lock management, and fencing.
- **High Availability Service Management**—Provides failover of services from one cluster node to another when a node becomes inoperative.
- **Cluster administration tools**—Provides configuration and management tools for setting up, configuring, and managing a Red Hat cluster including the cluster infrastructure components, the high availability and service management components, and storage.

Note Before performing any RHCS configuration changes, following the guidelines provided in Gateway HA Operations Notes.

The Prime Performance Manager local HA utilizes a fencing hardware unit to cut off a gateway server from the shared storage. Fencing ensures data integrity and prevents a split brain scenario, where the gateway servers are disconnected from each other and each assumes the other has failed. If a failure occurs, the cut off can be accomplished by powering off the node with a remote power switch, disabling a switch channel, or revoking a host's SCSI 3 reservations. Figure 12-3 shows the local HA architecture.

Figure 12-3 Local High Availability Architecture



Note Because of RHCS limitations, IPv6 is not supported on gateways configured for local HA.

Additional RHCS information can be found at the Red Hat website: http://www.redhat.com/.

Local HA Operations Notes

Before you perform any Prime Performance Manager local HA operation, review the following notes:

- To avoid data loss, never manually mount or unmount a gateway storage device while Prime Performance Manager local HA is running. Always stop the Prime Performance Manager local HA service first.
- Always mount a storage device to one HA gateway server; never mount the storage device to both local HA gateway servers.
- Never access the storage device directories while RHCS configuration is in progress. If RHCS configuration starts and a user accesses a storage mount directory, a mount/unmount failure will occur.
- If the local HA service is running and you want to stop, restart, or upgrade, Prime Performance Manager, or perform any similar action affecting Prime Performance Manager operability, you must:
  1. Freeze the RHCS HA service following the "Freezing and Unfreezing RHCS" procedure on page 12-14.
  2. Complete the Prime Performance Manager operation.

3. Unfreeze the RHCS service following the "Freezing and Unfreezing RHCS" procedure on page 12-14.

If you do not freeze RHCS, RHCS will detect the Prime Performance Manager action as a failure and begin the recovery process. This can include restarting and relocating Prime Performance Manager, or disabling the service, which will cause Prime Performance Manager stop working temporally.

Local HA Failovers and Switchovers

After the Prime Performance Manager gateway local HA cluster is deployed, failovers are automatic. If a single service failure occurs, RHCS attempts to restart the service. If the restart fails, the service is relocated and started on the second gateway server.

Human intervention is required only in exceptional cases, such as database corruption or a component failure, and the component is not configured for HA. Manual switchovers are performed using the RHCS web GUI or the CLI clusvcadm utility. After a failed node is repaired, you must perform a manual switchover to revert the cluster to its original configuration.

Note For complete redundancy, a configuration with no single point of failure is recommended. See the RHCS documentation for recommended configurations.

Two general conditions can trigger Prime Performance Manager local HA failovers:

- The Linux server containing the RHCS that manages the local HA is not functioning properly, for example, network connectivity is down. If this occurs, the RHCS service is automatically relocated to the another RHCS server.
- The Prime Performance Manager gateway is not functioning properly, for example, it cannot access the database. If this occurs, RHCS initiates recovery based upon the user-configured recovery policy:
  - Restart (recommended)—RHCS restarts the gateway on the server where it is installed. If the restart does not succeed, RHCS initiates the Relocate policy.
  - Relocate—RHCS switches to the backup gateway server immediately.
  - Disable—Do nothing; RHCS places the gateway service in disabled state.

During failovers, the gateway does not respond to its attached units, so units cache their requests. After the gateway service is back up, either by restarting the primary gateway successfully or by switching to the secondary gateway, the unit resends cached requests, so no data is lost.

To change the recovery policy after RHCS configuration, use the Red Hat Conga application following procedures in the RHCS documentation. Conga runs on a standalone RHCS server; it is not part of the Prime Performance Manager local HA cluster.

Freezing and Unfreezing RHCS

If you must stop Prime Performance Manager for any reason, you must freeze RHCS so that it stops checking the Prime Performance Manager status. Freezing RHCS places it in maintenance mode. If you stop Prime Performance without freezing RHCS, the cluster will detect that the services are down and attempt to restart it.

To freeze or unfreeze the RHCS cluster service:

Step 1 Log into the primary local HA gateway as a root user.

Step 2 Change to the HA lib bin directory, for example:

```
/var/CSCOppm-ha/ppm-ha-bin
```

Step 3 To freeze the RHCS service, enter the following command:

```
./ppmGatewayHA.sh freeze
```

Step 4 To unfreeze the RHCS service, enter the following command:

```
./ppmGatewayHA.sh unfreeze
```

After unfreeze the service, the RHCS will back to the normal, and begin to check the ppm status periodically.

Switching the RHCS Cluster Server

On occasion, you might need to switch over the RHCS cluster server. To switch the server:

Step 1 Log into the primary local HA gateway as a root user.

Step 2 Change to the HA lib bin directory, for example:

```
/var/CSCOppm-ha/ppm-ha-bin
```

Step 3 Enter the following command:

```
./ppmGatewayHA.sh switchover
```

The RHCS service switches from the active to the standby gateway.

Note All mount devices should only be accessed by Prime Performance Manager and not by other applications. For example, if you have another terminal accessing the mount device directories, use cd command to leave that directory.

Note Do not perform a manual mount when the RHCS local HA service is running.

Changing the Floating IP Address

Use the following steps if, for any reason, you need to change the floating IP address for the primary and secondary local HA servers:

Step 1 Freeze RHCS following the "Freezing and Unfreezing RHCS" procedure on page 12-14.

Step 2 Stop the Prime Performance Manager gateway:

```
ppm stop
```

Step 3 Change the RHCS cluster service floating IP address using the Red Hat Conga GUI. (Conga runs on a standalone node and is not part of the cluster.)

Step 4 Verify that the new floating IP and its hostname mapping relationship are added in both the primary and the secondary gateways.

Step 5 On Prime Performance Manager gateway, enter the following command to change the gateway to the new floating IP address:

```
ppm servername servername
```

Step 6 On Prime Performance Manager unit, enter the following command to change the unit to the new floating IP address:

```
ppm gatewayname servername
```

Step 7 Start Prime Performance Manager gateway and unit and make sure Prime Performance Manager gateway and unit status is OK.

Step 8 Use Conga or CLI to unfreeze the cluster service for Prime Performance Manager.

RHCS Log Messages

The RHCS log messages provide information about cluster-related issues, such as service failure. Every thirty seconds, RHCS issues status commands to check the Prime Performance Manager, internal database, and other processors. These messages are logged to /var/log/messages and can be viewed by the root user, or from the RHCS web GUI. Sample RHCS log messages are provided below:

```
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd[7629]: <notice> Starting stopped service
service:PPM_GW_HA
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info> mounting /dev/sde1 on /ha
Jun  4 07:54:49 crdc-ucs-109 kernel: kjournald starting.  Commit interval 5 seconds
Jun  4 07:54:49 crdc-ucs-109 kernel: EXT3FS on sde1, internal journal
Jun  4 07:54:49 crdc-ucs-109 kernel: EXT3-fs: mounted filesystem with ordered data mode.
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info>quotaopts =
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info> mounting /dev/sdf1 on /ha_array1
Jun  4 07:54:49 crdc-ucs-109 kernel: kjournald starting.  Commit interval 5 seconds
Jun  4 07:54:49 crdc-ucs-109 kernel: EXT3FS on sdf1, internal journal
Jun  4 07:54:49 crdc-ucs-109 kernel: EXT3-fs: mounted filesystem with ordered data mode.
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info>quotaopts =
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info> mounting /dev/sdg1 on /ha_array2
Jun  4 07:54:49 crdc-ucs-109 kernel: kjournald starting.  Commit interval 5 seconds
Jun  4 07:54:49 crdc-ucs-109 kernel: EXT3FS on sdg1, internal journal
Jun  4 07:54:49 crdc-ucs-109 kernel: EXT3-fs: mounted filesystem with ordered data mode.
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info>quotaopts =
Jun  4 07:54:49 crdc-ucs-109 clurgmgrd: [7629]: <info> Adding IPv4 address
10.74.125.114/25 to eth0
Jun  4 07:54:51 crdc-ucs-109 avahi-daemon[7490]: Registering new address record for
10.74.125.114 on eth0.
Jun  4 07:54:52 crdc-ucs-109 clurgmgrd: [7629]: <info> Executing
/ha/CSCOppm-gw/bin/ppmGatewayHealth.sh start
Jun  4 07:54:52 crdc-ucs-109 logger: start /ha/CSCOppm-gw/bin/sgmServer.sh ....
Jun  4 07:54:52 crdc-ucs-109 logger: ppm is not running.
Jun  4 07:54:52 crdc-ucs-109 logger: call /ha/CSCOppm-gw/bin/sgmServer.sh start silent 3.
Jun  4 07:55:25 crdc-ucs-109 logger: ppm health: everything is OK, return 0
Jun  4 07:55:25 crdc-ucs-109 logger: ppm start OK!!!.
Jun  4 07:55:25 crdc-ucs-109 clurgmgrd[7629]: <notice> Service service:PPM_GW_HA started
```

```
Jun  4 07:56:02 crdc-ucs-109 clurgmgrd: [7629]: <info> Executing
/ha/CSCOppm-gw/bin/ppmGatewayHealth.sh status
Jun  4 07:56:06 crdc-ucs-109 logger: ppm health: everything is OK, return 0
```

Configuring the RHCS Conga Web Interface

The RHCS web interface is configured during installation. Use the information provided in this section only if you decide to change the web interface configuration after installation or if the web interface was not configured during installation.

Installing the RHCS web interface module on a standalone server instead of the dual primary or secondary gateway servers is recommended.

The RHCS luci web interface allows you to configure and manage storage and cluster behavior on remote systems. You will use it to manage the Cisco Prime Performance local HA. Before you begin this procedure, you should have the Red Hat Conga User Manual. It can be obtained at:

http://sources.redhat.com/cluster/conga/doc/user_manual.html

If your fencing device is supported by RHCS but not ipmilan type, that is, you chose the Manual fencing option during the installation; manually configure the device using the Red Hat fencing configuration documentation. This can be obtained at;

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/pdf/Configuration_Example_-_Fence_Devices/Red_Hat_Enterprise_Linux-5-Configuration_Example_-_Fence_Devices-en-US.pdf

Note The following procedure provides the general steps to configure the luci interface. See the Red Hat *Conga User Manual* for details on performing steps in this procedure.

Note The RHCS web interface must be configured for both servers in the local redundant dual-node cluster.

Step 1 As root user, run the following command and enter the needed details:

```
luci_admininit
```

Step 2 Edit **/etc/sysconfig/luci** to change the default port to an available port. (The default 8084 port is used by Prime Performance Manager.) For example:

```
# defaults for luci,
# web UI fronted for remote cluster and storage management
LUCI_HTTPS_PORT=8084
```

Step 3 As root the root user, enter:

```
serviceluci restart
```

Step 4 Enter the web interface using the following link:

```
https://<node hostname>:<port>
```

Step 5 In the luci web interface, add the cluster that was configured by the Prime Performance Manager installation. See the Red Hat *Conga User Manual* for details on performing the following:

- Add a system.
- Add an existing cluster.
- Add a user.

Step 6 If your fencing device is supported by RHCS but not by Prime Performance Manager, use the Red Hat fencing configuration guide to configure the device.

Note If you provision a new fencing device, provision it as the primary fencing method. Keep the manual fencing agent as the backup fencing method.

Step 7 To use the web interface, connect to:

```
https://<cluster node hostname>:<port>
```

From the RHCS web interface you can stop, start, and relocate the services managed by the cluster.

Managing Geographical High Availability

The Prime Performance Manager geographical HA is installed in two different geographical locations, each configured with unique IP addresses. The two gateways work active-active on each site at the same time. The secondary gateway can take over immediately without administrative intervention if the primary site is not available.

This solution supports two kinds of deployment:

- Both sides are installed on single gateway.
- The primary gateway is deployed as a dual-end by the local HA and the secondary gateway is single.

Note Do not install units within the primary or secondary geographical HA gateways.

The Prime Performance Manager geographical redundancy gateway HA is based on database and file synchronization:

- Database synchronization—All database changes are synchronized from the primary to the secondary gateway. If the secondary gateway is not available when database changes occur, the primary gateway caches the changes. After secondary is up, the full synchronization will run the database synchronization first.
- File synchronization—If changes occur to dynamic and static files, they are synchronized to the secondary gateway.

Geographical HA management procedures are provided in the following topics:

- Displaying Geographical HA Status, page 12-19
- Switch the Primary and Secondary Geographical HA Gateways, page 12-20
- Configure Geographical HA, page 12-21
- Synchronizing the Geographical HA Gateways, page 12-21
- Freezing and Unfreezing Geographical HA Gateways, page 12-22
- Backing Up and Restoring Geographical HA Gateway Data, page 12-22
- Accessing Geographical HA Gateways Using the GUI, page 12-22
- Managing Devices in Geographical HA Gateways, page 12-23
- Managing Users in Geographical HA Gateways, page 12-23

- Managing Reports, Views, and Groups in Geographical HA Gateways, page 12-23
- Managing Alarms and Events in Geographical HA Gateways, page 12-23
- Managing Thresholds in and Upstream Alarm Hosts in Geographical HA Gateways, page 12-24
- Configuring SSL on Geographical HA Gateways and Remote Units, page 12-24
- Unit Redundancy Groups and Geographical HA, page 12-25

Displaying Geographical HA Status

To display the geographical HA status:

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Enter the following command:

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

Prime Performance Manager provides static configuration and running status information for the primary and secondary gateway. Table 12-4 shows the primary gateway running status.

Table 12-4 Primary Gateway Running Status

Item	Description
Service Role	Indicates the HA role, in this case, Primary.
Freezed	If True, the gateway is frozen.
Message Queue	Displays all sync messages that primary gateway need to handle.
DB Stored Messages	The cached messages for database changes.
Messages count to	Current count of received messages that have not been handled.
Messages need ack	Count of messages sent to the secondary gateway for which acknowledgement is not received. **Note** If this is not zero, do not switch over.
CSV files need sync	CSV files to be synced when it is enabled **Note** If this is none zero, do not switch over
Out Of Sync: false	Up to DB cache limit or age out. **Note** If true, run the ppm primeha backupdb to remove the label.

Table 12-5 shows the secondary gateway running status.

Table 12-5 Secondary Gateway Running Status

Item	Description
Service Role	Indicates the HA role, in this case, Secondary
Freezed	If True, the gateway is frozen.
Last Down Time	The time that primary gateway is detected down.
Primary Accumulate Down Times	If this value reaches the configured value, the service role manager takes over.

Table 12-5 Secondary Gateway Running Status (continued)

Item	Description
Acks to send back	Messages received from primary gateway that need acknowledgement.
Primary Gateway Alive	True means that current primary gateway is alive.
Initial Full Sync Done	When the secondary gateway connect to the primary gateway, database and files synchronizations occur. **Note** If the initial full sync is not complete, do not restart server or run switch in primary gateway side.
Health Check Working	Indicates whether the health check is working. The primary side ppm primeha freeze/unfreeze will stop/start health check of secondary gateway.

Switch the Primary and Secondary Geographical HA Gateways

On occasion, you might need to manually switch the primary and secondary geographical HA gateways, for example, to perform server maintenance or upgrades, or for other reasons. To manually switch geographical HA gateways:

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Complete the "Displaying Geographical HA Status" procedure on page 12-19 to verify the gateway status. The following statuses are required:

- Both primary and secondary gateways are active.
- The following status indicators have "0" counts:
  - Message Queue
  - DB Stored Messages
  - Messages count to
  - Messages need ack
  - CSV files need sync
- Connectivity exists between the primary and secondary gateway.
- All the units connect to the current primary gateway.

Step 3 Enter the following command:

```
/opt/CSCOppm-gw/bin/ppm primeha switch
```

After the switchover, the following occurs:

- Prime Network cross-launch capability, if installed on the primary gateway, is uninstalled and installed in the new one. For information about Prime Network cross launching, see Enabling Prime Network Cross-Launching, page 5-4.
- No BQL update messages are sent to the old primary gateway.
- Users can edit the server from web access.
- Users can view the reports data.
- Users can view the Views results.
- The old primary gateway is view only.

- Switch over events are raised for the new primary gateway.

Configure Geographical HA

You can configure a parameters that affect geographical HA processes. To configure geographical HA:

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Enter the following command and configuration option:

```
/opt/CSCOppm-gw/bin/ppm primeha (peergatewayname | peergatewayrmiport |
healthcheckinterval | maxfailnum | synccsv |)
```

Command options include:

- peergatewayname—Configures the IP address or hostname of peer gateway. If you are logged into the primary gateway, this would be the secondary gateway IP address or hostname. If you are logged into the secondary gateway, this would be the primary gateway IP address or hostname.
- peergatewayrmiport—Configures the RMI port of peer gateway. The RMI port is the port used for HA communications If you are logged into the primary gateway, this would be the secondary gateway RMI port.
- healthcheckinterval—Configures the frequency at which the primary and secondary gateways check their health status, in seconds.
- maxfailnum—Configures the maximum number of continuous tolerated connectivity failures before a failover is initiated.
- synccsv—Manually synchronizes the primary and secondary CSV files.
- ageout—Configures the primary database age out, in hours.
- cachelimit—The database differences cache records limitation.

Synchronizing the Geographical HA Gateways

If the primary and secondary gateways are out of synchronization, as indicated by the primary gateway Out of Sync parameter (see Displaying Geographical HA Status, page 12-19), complete the following steps to synchronize them:

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Enter the following command:

```
ppm primeha backupdb {path}
```

Step 3 Remote copy the backup files to the secondary gateway.

Step 4 log into the secondary gateway and restore its database from the backed up primary database:

```
ppm start restoredb {dbpath}
```

Step 5 Restart the secondary gateway:

```
ppm restart
```

Freezing and Unfreezing Geographical HA Gateways

If you must stop the primary Prime Performance Manager gateway for any reason, you must freeze the geographical HA gateways to stop the primary and secondary gateway health checking. To freeze the geographical HA gateway;

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Verify the secondary gateway is running. If not, you do not need to complete this procedure.

Step 3 Enter the following command:

```
/opt/CSCOppm-gw/bin/ppm primeha freeze
```

Health checking will stop on the secondary gateway.

Step 4 After you restart the primary gateway, unfreeze it to restart the secondary gateway health checking:

```
/opt/CSCOppm-gw/bin/ppm primeha unfreeze
```

Backing Up and Restoring Geographical HA Gateway Data

If the geographical gateways get out of synchronization, you will need to back up the primary gateway, copy the files to the secondary gateway and restore the data to it.

To back up and restore geographical HA data:

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Enter the following command to backup the gateway data:

```
/opt/CSCOppm-gw/bin/ppm primeha backup
```

Step 3 Enter the following command to restore the gateway data:

```
/opt/CSCOppm-gw/bin/ppm primeha restore {filename}
```

The gateway system files are restored with specified backup file.

Accessing Geographical HA Gateways Using the GUI

You can view the primary and secondary gateways by choosing **Gateways/Units** from the System menu. Two gateways are displayed. One has an Active status and one has a Standby status. Any gateway edits can only be applied to the primary (Active) gateway. Changes to the user preference are automatically synchronized to secondary gateway.

Managing Devices in Geographical HA Gateways

Devices can only be imported from Prime Network into the primary HA gateway. Additionally, device discovery can only be run from the primary HA gateway. Device credentials added to the primary gateway are synchronized to secondary gateway. If a switchover or failover occurs, the new primary gateway automatically imports the primary gateway devices.

If Prime Network cross launch capability is implemented, Prime Network cross launches go to the primary HA gateway. After a switchover or failover, the new primary gateway reinstall the cross launch capability.

Any changes to devices credentials are synchronized from the primary to secondary gateway. Device discovery seed files are also synchronized from the primary to secondary gateway.

For information about device discovery, see Chapter 5, "Discovering Network Devices."

Note You cannot update device information in the secondary HA gateway.

Managing Users in Geographical HA Gateways

In a geographical HA environment, users are handled in the following manner:

- Primary gateway—User information is automatically synchronized from the primary to the secondary gateway when the secondary gateway starts and connects to the primary gateway.
- Secondary gateway—For the secondary gateway, choose the same use authentication type that is used on the primary gateway and agree to use the existing user database when enabling user access.

For more information, see Chapter 6, "Managing Users and Security."

Managing Reports, Views, and Groups in Geographical HA Gateways

Changes to report settings in the primary gateway are synchronized to the secondary gateway. Report settings cannot be modified in the secondary gateway. Similarly, changes to the primary gateway views are synchronized to the secondary gateway. View modifications can only be performed on the primary gateway. The same principles apply to groups. Group settings cannot be changed on the secondary gateway. However, changes to the primary gateway groups are synchronized to the secondary gateway

Managing Alarms and Events in Geographical HA Gateways

The two HA gateways will display the same alarms and events. Any change to the event, such addition of notes, is synchronized to the secondary gateway. During switchover and failovers, the following events appear:

- Gateway $FailedGateway switched over to $SecondaryGateway.
- Gateway $FailedGateway failed over to $SecondaryGateway.

If two primary gateways detected, there will also one alarm issued.

If Prime Performance Manager discovers dual primary gateways, the following event is displayed: $LocalPrimaryGateway, $PeerPrimaryGateway.

Managing Thresholds in and Upstream Alarm Hosts in Geographical HA Gateways

Thresholds created on the primary gateway (see "Configuring Thresholds") are synchronized to the secondary gateway. Thresholds cannot changed on the secondary gateway. However, thresholds will operate after a switchover or failover to the secondary gateway. Threshold alarms raised on the primary gateway can be viewed on the secondary gateway.

If the OSS is enabled on the primary gateway (see Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters, page 9-11), you can view the configuration results on the secondary gateway. The secondary gateway does not send any traps to its northbound interface unless a switchover or failover occurs.

Configuring SSL on Geographical HA Gateways and Remote Units

The following procedures cover the enabling of SSL on geographical HA gateways and remote units. For additional information, see Enable SSL on a Gateway or Collocated Gateway and Unit, page 6-3.

To enable SSL on the primary gateway:

Step 1 Log into the primary gateway as the root user.

Step 2 If the secondary gateway is up, complete the "Freezing and Unfreezing Geographical HA Gateways" procedure on page 12-22 to freeze the primary gateway and stop the secondary gateway health checking.

Step 3 Enable SSL:

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

Step 4 Enter **y** if you want to restart the gateway now, or **n** if you want to restart it later.

Step 5 If you froze the primary gateway in Step 2, complete the "Freezing and Unfreezing Geographical HA Gateways" procedure on page 12-22 to unfreeze it.

To enable SSL on the secondary gateway:

Step 1 Log into the secondary gateway as the root user.

Step 2 Enable SSL on the secondary gateway.

Step 3 Import the secondary certificate into the primary gateway:

Step 4 Import the secondary certificate to all remote units.

Step 5 Import the primary gateway certificate to the secondary gateway.

Step 6 Import all the unit certificates to the secondary gateway.

Step 7 If secondary gateway is still up, complete the "Freezing and Unfreezing Geographical HA Gateways" procedure on page 12-22 to freeze the primary gateway.

Step 8 Restart primary gateway.

Step 9 Restart secondary gateway.

Step 10 Restart all units.

Step 11 Run the ppm primeha status command in the primary gateway to see if it is frozen. If yes, complete the "Freezing and Unfreezing Geographical HA Gateways" procedure on page 12-22 to unfreeze the primary gateway.

Enable SSL on remote units:

Step 1 Log into the remote unit.

Step 2 Enable SSL on the unit.

Step 3 Import the unit certificate to the primary gateway

Step 4 Import the unit certificate to the secondary gateway.

Step 5 Import the primary gateway certificate to the unit.

Step 6 Import the secondary gateway certificate to the unit.

Step 7 If secondary gateway is still up. complete the "Freezing and Unfreezing Geographical HA Gateways" procedure on page 12-22 to freeze the primary gateway.

Step 8 Restart the primary gateway.

Step 9 Restart the secondary gateway.

Step 10 Restart the remote unit.

Unit Redundancy Groups and Geographical HA

Any changes to the unit redundancy groups, for example create, add, or delete, are synchronized to the secondary gateway. If a failover occurs in the unit redundancy group or the gateway HA, complete the following steps to stop the servers:

Step 1 Disable unit redundancy groups. See Creating Unit Protection Groups, page 12-8.

Step 2 Stop the protection unit. See Stopping Gateways and Units, page 2-3.

Step 3 Stop the work units.

Wait until all units are completely shut down.

Step 4 Stop the secondary gateway.

Step 5 Stop primary gateway.

Managing Geographical and Local High Availability

If Prime Performance Manager gateway HA is installed with a local HA, the two local gateways are combined as the one active gateway for geographical HA, and the remote geographical HA gateway is the standby. To manage the local HA gateways, follow the procedures in Managing Local High Availability, page 12-12. To manage geographical HA, follow procedures in Managing Geographical High Availability, page 12-18.

Manual Disaster Recovery

If a disaster occurs and primary gateway become inoperable, the secondary gateway becomes active and Prime Performance Manager continues to function, with the following exceptions:

- Only administrator users can login to secondary gateway.
- All primary gateway configurations will appear on the secondary gateway with no changes.
- All web client sessions to the primary gateway and secondary gateway at the time of disaster will be invalidated. All client users will need to log into the secondary gateway.
- If the secondary gateway is not connected to units, no reports will be available.

After the primary gateway is restored, complete the following steps to bring it back online:

Step 1 Log into the secondary gateway as the root user.

Step 2 Complete the "Backing Up and Restoring Geographical HA Gateway Data" procedure on page 12-22 to create a backup file of the secondary gateway. Place the file in the directory specified by the value of SBACKUPDIR inSystem.properties.

Step 3 Complete the "Backing Up and Restoring Geographical HA Gateway Data" procedure on page 12-22 to restore the primary gateway with the secondary gateway backup file.

CHAPTER 13

Configuring Prime Performance Manager for Firewalls

The following topics tell you how to configure Prime Performance Manager for firewalls:

- Gateway-to-Unit Connectivity, page 13-1
- Configuring Gateways and Units for Firewalls, page 13-2

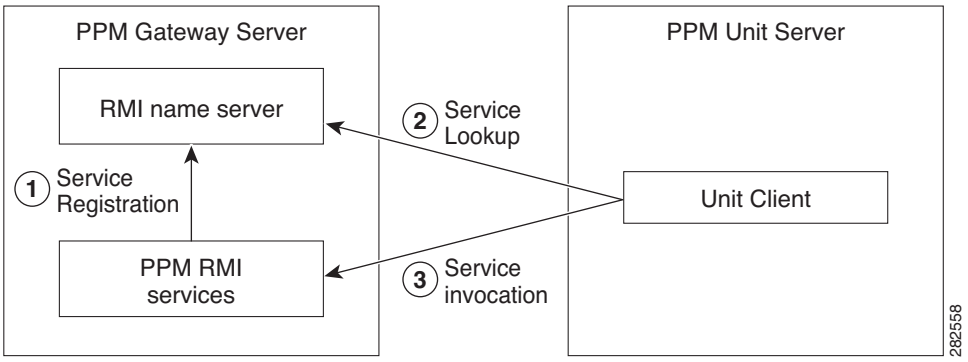
Gateway-to-Unit Connectivity

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 13-1 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 13-1 Prime Performance Manager Communication



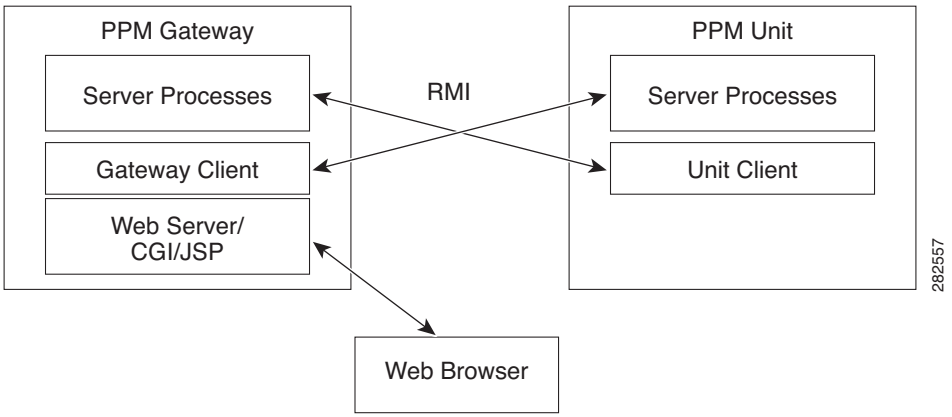
1	Service registration	**3**	Service invocation
2	Service lookup		

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 13-2 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 13-3
- Configuring Gateway and Unit Communication, page 13-3
- Configuring Unit and Device Communication, page 13-6

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. To change it to a different port, you can use the ppm jspport command. See ppm jspport, page B-34, 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 13-1 lists the Prime Performance Manager ports and firewall requirements.

Table 13-1 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 it to a different port, you can use the ppm webport command. See ppm jspport, page B-34, for more information.

Table 13-1 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 13-1.

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 13-1 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 Administration. 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 14

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, page 14-1
- Backing Up Prime Performance Manager Data Files, page 14-2
- Changing the Backup Directory, page 14-3
- Setting the Number of Backup Days, page 14-3
- Restoring Prime Performance Manager Data Files, page 14-3

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. Restore the gateway first. Backup is restored to the gateway.
3. Restore the unit. Backup is restored to the unit.
4. Start the gateway.
5. Start the unit.

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 3:30 AM.
2. Restore the gateway first. Backup is restored to the gateway.
3. Restore each unit. These can be done in parallel.

4. Start the gateway.
5. Start each unit, 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 14-2
- Changing the Backup Directory, page 14-3
- Setting the Number of Backup Days, page 14-3
- Restoring Prime Performance Manager Data Files, page 14-3

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 14-3), 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, page A-1
- Adding SNMP and Telnet/SSH Credentials, page A-1
- Unit Configuration, page A-2
- Device Discovery, page A-2
- Reports, page A-2
- Device Management Actions, page A-2
- Alarms and Events, page A-2
- Clients, page A-2
- Trap Forwarding, page A-3
- Prime Network Integration, page A-3
- Command Line Interface, page A-3

IPv6 Support in Prime Performance Manager

You can use Prime Performance Manager to set up gateways and units with IPv6 addresses:

- Install a gateway and unit with IPv6 addresses.
- Support web access gateway with IPv6 address or hostname
- Support device discovery with IPv6 addresses.
- Install units with connectivity to an IPv6 address and hostname.
- Integrate with Cisco Prime Network using IPv6 addresses, including cross launch and device inventory imports.
- Set up an OSS with IPv6 as the source and (or) destination server.

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 cannot 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 do not 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 device actions, see Creating and Editing Device Polling Groups, page 8-22.

Alarms and Events

Similar as IPv4 device, the alarms or events generated for IPv6 device are also available in Alarm and Event GUI.

Clients

You can use both IPv4 and IPv6 addresses and hostname to access the Prime Performance Manager gateway using a web browser. If you connect to the gateway using a literal IPv6 address. enclose the address with "[" and "]" in the URL.

For example,

```
http://[2011::2:21b:78ff:febd:9e16]:4440
```

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 IPv6 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 IPv6 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.

IPv6 Troubleshooting

The DNS server is usually enabled. You can view the install log to get the configurations, for example:

```
==================- TCP/IP Address Check -==================
…
INFO: Local address resolution -> Primary:files, Secondary:dns
```

- Linux and Solaris—Verify that the following line is present in your /etc/nsswitch.conf file:

  ```
  hosts: files dns
  ```

- Solaris only
  - Verify that your /etc/hosts file is a soft link file link to /etc/inet/hosts. If the soft link is broken, add the link to /etc/inet/hosts using **ln** command.
  - Verify that your /etc/nsswitch.conf file has the following line:

    ```
    ipnodes:   files dns
    ```

APPENDIX B

Prime Performance Manager Commands

Prime Performance Manager provides commands that allow you to perform functions from the command line interface. Many command functions can also be performed in the Prime Performance Manager GUI, but many others, particularly administrative or root user functions, can only be performed in the CLI. Commands can be run on Solaris and Linux. Some commands can be performed on both the gateway and unit, others on only the gateway or only the unit. You run commands from:

install_directory/bin

where *install_directory* is the directory where Prime Performance Manager is installed (by default, /opt/CSCOppm-gw or /opt/CSCOppm-unit)

Alternatively, if *install_directory*/bin is in your path, you can run commands from your path.

A quick reference of commands organized in functional groups is available from the Prime Performance Manager GUI. To view them, from the Help menu choose **Readmes and CLI Commands > PPM Commands**.

Prime Performance Manager commands in alphabetical order are described in the following topics:

- Prime Performance Manager, page B-5
- ppm addcreds, page B-5
- ppm addsnmpcomm, page B-6
- ppm addunitconf, page B-6
- ppm adduser, page B-7
- ppm authtype, page B-7
- ppm backup, page B-8
- ppm backupdata, page B-9
- ppm backupdata, page B-9
- ppm backupdir, page B-10
- ppm backuplog, page B-11
- ppm backuprep, page B-11
- ppm backupstats, page B-11
- ppm badloginalarm, page B-12
- ppm badlogindisable, page B-12
- ppm bulkstatsage, page B-13
- ppm bulkstatsage, page B-13

- ppm changes, page B-14
- ppm checksystem, page B-14
- ppm clitimeout, page B-14
- ppm cmdlog, page B-15
- ppm compilemibs, page B-15
- ppm console, page B-16
- ppm consolelogsize, page B-16
- ppm countnodes, page B-16
- ppm datadir, page B-17
- ppm dbbackupdir, page B-18
- ppm deletecreds, page B-19
- ppm deletesnmpcomm, page B-19
- ppm deleteunitconf, page B-19
- ppm deluser, page B-20
- ppm devcachedir, page B-20
- ppm devcachedir, page B-20
- ppm disablepwdage, page B-21
- ppm discover, page B-22
- ppm diskcheck, page B-22
- ppm diskmonitor, page B-22
- ppm enablepwdage, page B-24
- ppm enablepwdage, page B-24
- ppm eventautolog, page B-24
- ppm eventconfig, page B-25
- ppm eventlimitsconfig, page B-25
- ppm eventsnmpserversconfig, page B-26
- ppm eventlimitsconfig, page B-25
- ppm evilstop, page B-28
- ppm export, page B-28
- ppm exportcustnames, page B-28
- ppm exportusers, page B-28
- ppm gatewayname, page B-29
- ppm help, page B-29
- ppm ifnameformat, page B-30
- ppm ifnameformat, page B-30
- ppm importcw, page B-30
- ppm inactiveuserdays, page B-31
- ppm installlog, page B-32

- ppm inventoryimport, page B-32
- ppm iosreport, page B-32
- ppm ipaccess, page B-33
- ppm ipslaftpfilesize, page B-33
- ppm ipslaftpfilesize, page B-33
- ppm keytool, page B-34
- ppm listusers, page B-35
- ppm localhabackupflag, page B-35
- ppm localhacommands, page B-36
- ppm localhappmtimeout, page B-36
- ppm logdir, page B-36
- ppm logdir, page B-36
- ppm logsize, page B-37
- ppm logtimemode, page B-38
- ppm maxasciirows, page B-39
- ppm maxhtmlrows, page B-39
- ppm maxpagesize, page B-40
- ppm maxrepqueries, page B-40
- ppm maxrepqueries, page B-40
- ppm modifysnmpcomm, page B-41
- ppm modifyunitconf, page B-42
- ppm motd, page B-42
- ppm movenode, page B-43
- ppm movenode, page B-43
- ppm msglogage, page B-43
- ppm msglogdir, page B-44
- ppm netlog, page B-44
- ppm netlogger, page B-45
- ppm newlevel, page B-45
- ppm optimizecapabilitypoll, page B-45
- ppm osinfo, page B-46
- ppm passwordage, page B-46
- ppm patchlog, page B-47
- ppm ping, page B-47
- ppm poll, page B-47
- ppm premotd, page B-48
- ppm primecentralintegration, page B-48
- ppm primeha, page B-49

- ppm printreportstatus, page B-50
- ppm printreportstatus, page B-50
- ppm purgedb, page B-51
- ppm pwdchangeinterval, page B-51
- ppm pwdchangelimit, page B-52
- ppm pwdchangerestrict, page B-52
- ppm readme, page B-53
- ppm reboot, page B-53
- ppm redundancygroups, page B-54
- ppm redistributenodes, page B-53
- ppm reloadbulkstats, page B-55
- ppm repdir, page B-56
- ppm rephelp, page B-56
- ppm restart, page B-56
- ppm restore, page B-57
- ppm restore all, page B-57
- ppm restoreprops, page B-58
- ppm rootvars, page B-58
- ppm sechelp, page B-58
- ppm seclog, page B-59
- ppm servername, page B-59
- ppm setpath, page B-60
- ppm setpctrapdestination, page B-61
- ppm showcreds, page B-61
- ppm showsnmpcomm, page B-61
- ppm showunitconf, page B-62
- ppm singlesess, page B-62
- ppm snmpcomm, page B-63
- ppm snmpconf, page B-63
- ppm snmpget, page B-63
- ppm snmphelp, page B-66
- ppm snmpmaxrows, page B-66
- ppm snmpnext, page B-66
- ppm snmpsetup, page B-68
- ppm snmpwalk, page B-69
- ppm ssl, page B-71
- ppm sslstatus, page B-72
- ppm starbuild, page B-72

- ppm start, page B-73
- ppm statreps, page B-73
- ppm status, page B-75
- ppm status, page B-75
- ppm smtpport, page B-75
- ppm syncunits, page B-76
- ppm tac, page B-77
- ppm topxxsize, page B-77
- ppm traceroute, page B-77
- ppm uninstall, page B-78
- ppm unknownage, page B-78
- ppm updateuser, page B-78
- ppm useraccess, page B-79
- ppm userpass, page B-79
- ppm version, page B-80
- ppm who, page B-80
- ppm who, page B-80
- ppm xmlpoll, page B-81

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.

Available in GUI

No

Related Topic

Chapter 3, “Managing the 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 hostname.

- **-i** *ipaddress*—The device IP address or hostname.
- **-u** *username*—The username to log into the device.
- **-n** *enable_username*—Enables the privileged username.
- **-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

Available in GUI

Yes

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.

Available in GUI

Yes

Related Topic

- ppm deletesnmpcomm, page B-19
- ppm modifysnmpcomm, page B-41
- ppm showsnmpcomm, page B-61
- ppm snmpsetup, page B-68

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.

Available in GUI

Yes

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 Modifying the Password Policy, page 6-9.
- 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 User Authentication, page 6-7).

Available in GUI

Yes

Related Topic

- Setting Up User Access and Security, page 6-1
- User Authentication, page 6-7

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 Users and User Security, page 6-12 to ensure secure passwords between Prime Performance Manager client and server.)

You must log in as the root user to use this command.

Available in GUI

No

Related Topic

- Setting Up User Access and Security, page 6-1
- User Authentication, page 6-7

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).

Available in GUI

No

Related Topics

- Backing Up Prime Performance Manager Data Files, page 14-2
- ppm restore, page B-57

ppm backupdata

Syntax

/opt/CSCOppm-gw/bin/ppm backupdata [**enable** | **disable** | **status**]

Command Description

This command enables and disables the backup of the Prime Performance Manager database. You must log in as the root user to use this command.

Available in GUI

No

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-10). 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-57.

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-10).

Available in GUI

No

Related Topic

- Backing Up Prime Performance Manager Data Files, page 14-2
- ppm restore, page B-57

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.

Available in GUI

No

Related Topic

- Backing Up Prime Performance Manager Data Files, page 14-2
- ppm restore, page B-57

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.

Available in GUI

Yes

ppm backuprep

Syntax

/opt/CSCOppm-gw/bin/ppm backuprep [**enable** | **disable** | **status**]

Command Description

This command enables and disables the backup of the Prime Performance Manager reports. You must log in as the root user to use this command.

Available in GUI

No

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.

Available in GUI

No

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 Display the System Security Log, page 6-21).

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.

Available in GUI

Yes

Related Topic

Edit User Security Settings, page 6-16

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.

Available in GUI

Yes

Related Topic

Edit User Security Settings, page 6-16

ppm bulkstatsage

Syntax

/opt/CSCOppm-gw/bin/ppm bulkstatsage [*days*]

Command Description

Specifies the number of days bulk statistic files are retained. The default is 14 days. You do not need to restart Prime Performance Manager server. (This command is supported only on the gateway.)

Available in GUI

Yes

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 **ppm keytool** command (see ppm keytool, page B-34) 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.

Available in GUI

No

Related Topic

- Display SSL Key and Certificate, page 6-6
- Export SSL Certificates, page 6-5

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.

Available in GUI

Yes

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.

Available in GUI

Yes

ppm clitimeout

Syntax

/opt/CSCOppm-gw/bin/ppm clitimeout [*mins* | *clear*]

Command Description

Specifies how long, in minutes, a 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 zero (clears the command) 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.

Available in GUI

Yes

Related Topic

Edit User Security Settings, page 6-16

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.

Available in GUI

Yes

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 variables 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.

Available in GUI

No

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.

Available in GUI

Yes

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**.

Available in GUI

Yes

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.

Available in GUI

Yes

ppm crosslaunch

Syntax

/opt/CSCOppm-gw/bin/ppmcrosslaunch [**install** | **uninstall**]

Command Description

Installs or uninstalls cross launch on Prime Network so that Prime Performance Manager can be launched from Prime Network.

Available in GUI

Yes

ppm csvdrop

Syntax

/opt/CSCOppm-gw/bin/ppmcsvdrop [*dir*]

Command Description

Changes the Bulk Statistics Drop directory and updates the CSV_DROP_DIR property in /opt/CSCOppm-unit/properties/BulkStats.properties. The default directory location is /opt/CSCOppm-unit/csvdrop. This command sets a new directory location.

You do not need to restart Prime Performance Manager server.

The command is only supported on units.

Available in GUI

No

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 where Prime Performance Manager data files are stored. 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.

The default data storage directory is in the Prime Performance Manager installation directory. If you installed Prime Performance Manager in /opt, the default directory is /opt/CSCOppm-gw/data. If you installed Prime Performance Manager in a different directory, the default directory is in that directory.

The server must be restarted for the directory changes to take effect. This normally occurs after running the command. Enter the **nostart** option if you want to restart server at a later time.

You must log in as the root user to use this command.

Available in GUI

No

ppm dbbackupdir

Syntax

/opt/CSCOppm-gw/bin/ppmdbbackupdir [*directory*] [**nostart**]

Command Description

Sets the directory used for database backup staging. The server must be restarted for the directory changes to take effect. This normally occurs after running the command. Enter the **nostart** option if you want to restart server at a later time.

Available in GUI

No

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.

Available in GUI

Yes

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 hostname.

-a—Deletes all Telnet and SSH device credentials on the gateway.

Available in GUI

Yes

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.

Available in GUI

Yes

Related Topic

- ppm addsnmpcomm, page B-6
- ppm modifysnmpcomm, page B-41
- ppm showsnmpcomm, page B-61
- ppm snmpsetup, page B-68

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.

Available in GUI

Yes

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.

Available in GUI

Yes

Related Topic

Manually Disable Users and Passwords, page 6-17

ppm devcachedir

Syntax

/opt/CSCOppm-gw/bin/ppmdevcachedir [*directory*] [**nostart**]

Command Description

Sets the directory used for device cache files. The server must be restarted for the directory changes to take effect. This normally occurs after running the command. Enter the **nostart** option if you want to restart server at a later time.

Available in GUI

No

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**.

Available in GUI

Yes

Related Topic

Manually Disable Users and Passwords, page 6-17

ppm disablepwdage

Syntax

/opt/CSCOppm-gw/bin/ppm enablepwdage [*username*]

Command Description

Disables password aging for the specified user.

You must log in as the root user to use this command.

Available in GUI

Yes

Related Topic

ppm enablepwdage, page B-24

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.

Available in GUI

Yes

Related Topic

Manually Disable Users and Passwords, page 6-17

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.

Available in GUI

Yes

Related Topic

Running Device Discovery from Prime Performance Manager, page 5-10

ppm diskcheck

Syntax

/opt/CSCOppm-gw/bin/ppm diskcheck

Command Description

Manually runs the disk space usage check.

Related Topic

ppm diskmonitor, page B-22

ppm diskmonitor

Syntax

/opt/CSCOppm-gw/bin/ppm diskmonitor [**enable** | **disable** | **status**] | **warning** {*MBs*} | **critical** {*MBs*} | **warnscript** {*path* | *clear*} | **critscript** {*path* | *clear*}

Command Description

Monitors the Prime Performance Manager installed directories disk space usage. When enabled, the diskWatcher.sh script runs every ten minutes to check two thresholds:

- Warning—When the disk space usage passes the threshold defined with the warning option, a disk space warning alarm is created and logged in the sgmConsoleLog.txt file. For example:

```
WARNING: The following partition is getting low on free disk space:
                          /opt
                          Space left = 905 MB
```

The script identified with the warnscript option is executed to begin disk cleanup.

- Critical—When the disk space usage passes the threshold defined with the critical option, a disk space critical alarm is created and logged in the sgmConsoleLog.txt file. For example:

```
WARNING: The following partition is getting low on free disk space:
                          /opt
                          Space left = 100 MB
```

The script identified with the critscript option is executed to begin disk cleanup.

The ppm diskmonitor parameters include:

- **enable**—Enables the Prime Performance Manager installed directories disk space usage check.
- **disable**—Disables the Prime Performance Manager installed directories disk space usage check.
- **status**—Displays the disk monitor status, either enabled or disabled.
- **warning** {*MBs*}—Sets the warning threshold. The default is 1000 MB.
- **critical** {*MBs*}—Sets the critical threshold. The default is 100 MB.
- **warnscript** {*path* | *clear*}—Provides the path to the script to call when the warning threshold is crossed. The script should initiate disk cleanup. The clear option clears the diskmonitor warning alarm.
- **critscript** {*path* | *clear*}—Provides the path to the script to call when the critical threshold is crossed. The script should initiate disk cleanup. The clear option clears the diskmonitor critical alarm.

You must log in as the root user to use this command.

Available in GUI

- enable, disable, status: Yes
- warnscript, critscript: No

Related Topic

ppm diskcheck, page B-22

ppm dumpdb

Syntax

/opt/CSCOppm-gw/bin/ppm dumpdb [*directory*]

Command Description

Dumps the current database, incremental, if it exists, to the provided directory. Allows an external process to trigger a database dump to a staging area that could be used by another backup, restore, or archival system.

Available in GUI

No

ppm enablepwdage

Syntax

/opt/CSCOppm-gw/bin/ppm enablepwdage [*username*]

Command Description

Enables password aging for the specified user.

You must log in as the root user to use this command.

Available in GUI

Yes

Related Topic

- ppm discover, page B-22
- Managing Users and User Security, page 6-12

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.

Available in GUI

Yes

Related Topic

Enable User Accounts and Passwords Using the CLI, page 6-18

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.

Available in GUI

Yes

ppm eventconfig

Syntax

/opt/CSCOppm-gw/bin/ppm eventconfig [**view** | **edit** | **restore** | **master**]

Command Description

Manages the event configuration. Options:

- **view**—Displays the event configuration file.
- **edit**—Allows you to edit the event configuration file in your environment with a text editor. (The default text editor is 'vi'.)
- **restore**—Restore the event configuration file to the last active copy.
- **master**—Stores the event configuration file to the master copy (the default copy shipped with Prime Performance Manager).

You must log in as the root user to use this command.

Available in GUI

Yes

ppm eventlimitsconfig

Syntax

/opt/CSCOppm-gw/bin/ppm eventlimitsconfig [**view** | **edit** | **restore** | **master**]

Command Description

Manages the event limits configuration. Options:

- **view**—Displays the event limits configuration file.
- **edit**—Allows you to edit the event limits configuration file in your environment with a text editor. (The default text editor is 'vi'.)
- **restore**—Restore the event limits configuration file to the last active copy.
- **master**—Stores the event limits configuration file to the master copy (the default copy shipped with Prime Performance Manager).

You must log in as the root user to use this command.

Available in GUI

Yes

ppm eventsnmpserversconfig

Syntax

/opt/CSCOppm-gw/bin/ppm eventsnmpserverssconfig [**view** | **edit** | **restore** | **master**]

Command Description

Manages the SNMP servers configuration. Options:

- **view**—Displays the SNMP servers configuration file.
- **edit**—Allows you to edit the SNMP servers configuration file in your environment with a text editor. (The default text editor is 'vi'.)
- **restore**—Restore the SNMP servers configuration file to the last active copy.
- **master**—Stores the SNMP servers configuration file to the master copy (the default copy shipped with Prime Performance Manager).

You must log in as the root user to use this command.

Available in GUI

Yes

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**

Option	Action Names	Required Parameters
	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.

Available in GUI

No

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.

Available in GUI

No

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.

Available in GUI

Yes

ppm exportcustnames

Syntax

/opt/CSCOppm-gw/bin/ppm exportcustnames

Command Description

Allows to export custom names for import to another server.

Available in GUI

Yes

ppm exportusers

Syntax

/opt/CSCOppm-gw/bin/ppm exportusers

Command Description

Allows to export users for import to another server.

Available in GUI

No

ppm gatewayname

Syntax

/opt/CSCOppm-gw/bin/ppm gatewayname [*gatewayname*] [nostopstart]

Command Description

Command resets Prime Performance Manager remote unit's connected gateway name, where *gatewayname* is the connected gateway's hostname or IP address.

- Verify that the new *gatewayname* is connectable. If not, you might not be able to connect to the remote gateway.
- Verify that the unit-side IP protocol is consistent with *gatewayname* used in the gateway side. See ppm servername, page B-59.
- You must log in as root user to run this command.
- nostopstart - The server is not stopped and started automatically while running this command.

Available in GUI

No

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.

Available in GUI

No

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, "Managing the Web Interface"

ppm ifnameformat

Syntax

/opt/CSCOppm-gw/bin/ppm ifnameformat [**desc** | **alias** | **both**|]

Command Description

Defines the format for displaying interface names in the Prime Performance Manager GUI:

- desc—Only the interface description is displayed.
- alias—Only the interface alias is displayed.
- both—Both the interface description and alias is displayed.

Available in GUI

- Yes

ppm importcustnames

Syntax

/opt/CSCOppm-gw/bin/ppm importcustnames [*inputfile*]

Command Description

Allows to import custom names from another server.

Available in GUI

No

ppm importcw

Syntax

/opt/CSCOppm-gw/bin/ppm importcw [***cwfile***] [**force** | **telnet**]

Command Description

Imports device hostname and read-community strings from the CiscoWorks v3 server to Prime Performance Manager. SSH is the default import protocol.

cwfile—File name of the CiscoWorks export file. The file must be in CSV format.

The following parameters are not required if Prime Performance Managerdoes not have any communities or credentials.

force—Overrides any preexisting SNMP communities. Instead of adding new communities, the existing communities are modified automatically. This parameter applies to all imported communities.

telnet—Sets the connection protocol to Telnet and the port to 23. SSH v2 is the default import protocol and 22 the default port. This parameter applies to all imported communities.

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.

Available in GUI

No

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 zero (clears the command) 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.

Available in GUI

Yes

Related Topics

- Chapter 6, "Managing Users and Security"
- Edit User Security Settings, page 6-16

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.

Available in GUI

Yes

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.

Available in GUI

Yes

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

To run this command, you must log in as the root user.

Available in GUI

Yes

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 User Authentication, page 6-7 for more information about using this command.

You must log in as the root user to use this command.

Available in GUI

Yes

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.

Available in GUI

No

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 port number. Only numeric entries can be entered. Prime Performance Manager verifies that the new port number is not already used.

This command can be used to change the port number after you install Prime Performance Manager and, for example, find that another application needs the port.

You must log in as the root user to use this command.

Note If you enabled Cisco Prime Central cross launching, you must reenable it after you change the JSP server port number. For information, see Enabling Prime Network Cross-Launching, page 5-4.

Available in GUI

No

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.

Available in GUI

No

Related Topic

Managing Users and User Security, page 6-12

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.

Available in GUI

Yes

Related Topic

List Currently Defined Users, page 6-20

ppm localhabackupflag

Syntax

/opt/CSCOppm-gw/bin/ppm localhabackupflag [enable | disable | status]

Command Description

This command is used when a Prime Performance Manager gateway is installed in the local directory and want to upgrade it to a gateway HA environment. (The SAN storage must be installed.) For information about upgrading a non-HA gateway to an HA environment, see the *Cisco Prime Performance Manager 1.2 Quick Start Guide*.

You must log in as the root user to use this command.

Available in GUI

No

ppm localhacommands

Syntax

/opt/CSCOppm-gw/bin/ppm localhacommands

Command Description

Prints Prime Performance Manager gateway local HA commands usage information such as how to do switchover, freeze, or unfreeze a gateway in an HA environment. Example:

```
[root@crdc-ucs-109 ~]# /ha/CSCOppm-gw/bin/ppm hacommands
Usage:
   ppmGatewayHA.sh switchover  - Switch the service to another cluster node.
   ppmGatewayHA.sh freeze      - Freeze the service in RHCS.
   ppmGatewayHA.sh unfreeze    - Unfreeze the service in RHCS.
   ppmGatewayHA.sh status      - Show the service status in RHCS.

***** Do NOT run these commands in ppm install directory. *****
***** Please go to /var/CSCOppm-ha/ppm-ha-bin directory to run these commands. *****
```

You must log in as the root user to use this command.

Available in GUI

No

ppm localhappmtimeout

Syntax

/opt/CSCOppm-gw/bin/ppm localhappmtimeout [**start | stop | info**] [*minutes*]

Specify or show ppm start/stop timeout minutes.

Command Description

Specifies or shows the Prime Performance Manager start and stop timeout in minutes for Prime Performance Manager gateways in an HA environment.

The default start timeout value is 3 minutes. The default stop timeout value is 2 minutes. You can use these commands to adjust the timeout values.

You must log in as the root user to use this command.

ppm logdir

Syntax

/opt/CSCOppm-gw/bin/ppm logdir [*directory*] [**nostart**]

Command Description

Sets the directory used for log files. The server must be restarted for the directory changes to take effect. This normally occurs after running the command. Enter the **nostart** option if you want to restart server at a later time.

Available in GUI

No

ppm logger

Command Description

Displays the system messages *messageLog.txt* file with tail -f.

To stop the display, press **Ctrl-C**.

Available in GUI

Yes

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**).

Available in GUI

No

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.

Available in GUI

No

ppm maxasciirows

Syntax

/opt/CSCOppm-gw/bin/ppm maxasciirows [*number-of-rows*]

Command Description

Sets the maximum browser rows for ASCII web log output.

Available in GUI

No

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 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.

Available in GUI

Yes

Related Topic

Chapter 3, “Managing the Web Interface”

ppm maxpagesize

Syntax

/opt/CSCOppm-gw/bin/ppm maxpagesize [*number-of-rows*]

Command Description

Sets the maximum browser page size for table reports. 800 rows is the default.

Available in GUI

No

ppm maxrepqueries

Syntax

/opt/CSCOppm-gw/bin/ppm maxrepqueries [*number*]

Command Description

Sets the maximum number of report sessions that can be open at one time.

Available in GUI

No

Note After changing this setting, you must restart the Prime Performance Manager server. See ppm restart, page B-56.

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.

Available in GUI

No

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.

Available in GUI

Yes

Related Topic

- ppm addsnmpcomm, page B-6
- ppm deletesnmpcomm, page B-19
- ppm showsnmpcomm, page B-61
- ppm snmpsetup, page B-68

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.

Available in GUI

Yes

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 before launching.

If you enable the Message of the Day, it appears whenever a user attempts to launch an Prime Performance Manager 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.

Available in GUI

No

Related Topic

ppm premotd, page B-48

Launching the Web Interface, page 3-1

ppm movenode

Syntax

/opt/CSCOppm-gw/bin/ppm movenode [*node1 unit1*] [*node2 unit2...*]

Command Description

Moves devices from one unit to another.

Available in GUI

Yes.

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.

Available in GUI

Yes

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.

Available in GUI

Yes

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.

Available in GUI

No

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.

Available in GUI

Yes

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**.

Available in GUI

Yes

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.

Available in GUI

Yes

Related Topic

Enable User Accounts and Passwords Using the CLI, page 6-18

ppm optimizecapabilitypoll

Syntax

/opt/CSCOppm-gw/bin/ppm optimizecapabilitypoll {**enable** | **disable** | **status**}

Command Description

Enables or disables capability poll optimization. If enabled, Prime Performance Manager capability polling polls devices for capabilities based on network-level or device-level enabled reports. If disabled, Prime Performance Manager polls devices for all the device capabilities regardless of whether reports are enabled at the network or device levels. Use these keywords and arguments with this command:

- **enable**—Enables capability poll optimization.
- **disable**—Disables capability poll optimization.

- **status**—Displays the capability poll optimization status.

Available in GUI

No

Related Topic

Capability Polling, page 7-18

ppm osinfo

Syntax

/opt/CSCOppm-gw/bin/ppm osinfo

Command Description

Depending on the networks that you have set, displays the operating system versions of software that Prime Performance Manager supports.

Available in GUI

Yes

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-43.

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.

Available in GUI

Yes

Related Topic

Edit User Security Settings, page 6-16

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.

Available in GUI

Yes

ppm ping

Syntax

/opt/CSCOppm-gw/bin/ppm ping [*hostname*]

Command Description

You use this command to ping a device from the command line.

You must log in as the root user to use this command.

Available in GUI

Yes

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.

Available in GUI

Yes

ppm premotd

Syntax

/opt/CSCOppm-gw/bin/ppm premotd [**cat** | **disable** | **edit** | **enable**]

Command Description

Manages the message that appears at the bottom of the Prime Performance Manager login window (see Figure 3-1 on page 3-2.

Use these keywords with this command:

- **enable**—Enables the message at the bottom of the login window.
- **edit**—Edits the message at the bottom of the login window.
- **cat**—Displays the message at the bottom of the login window.
- **disable**—Disables the login window message.

You must log in as the root user to use this command.

Available in GUI

No

Related Topics

ppm motd, page B-42

Launching the Web Interface, page 3-1

ppm primecentralintegration

Syntax

/opt/CSCOppm-gw/bin/ppm primecentralintegration

Command Description

Use this command to integration Prime Performance Manager with Cisco Prime Central. After you enter the command, you will be prompted for the following information:

- Enter Prime Central Server—Enter the Prime Central database server IP address or hostname.
- Enter SID [primedb]—Enter the Prime Central database service name, which is primedb by default.
- Enter DB User [primedba]—Enter the Prime Central database username, which is primedba by default.

- Enter DB Password [*****]—Enter the Prime Central database user password; for example, Test456!
- Enter DB Port [1521]—Enter the Prime Central database port number, which is 1521 by default.
- Restart Prime Central Integration Layer [Yes]—Enter **Y** to restart the integration layer server.

You must log in as the root user to use this command. For additional information, see Chapter 4, "Prime Central Integration."

Available in GUI

Yes

ppm primeha

Syntax

/opt/CSCOppm-gw/bin/ppm primeha [**status | switch | configure {peergatewayname | peergatewayrmiport | healthcheckinterval | maxfailnum | synccsv | ageout | cachelimit**} **| backupdb** (***path***)**| freeze | unfreeze | backup | restore** (***file name***)]

Command Description

Manages Prime Performance Manager geographical HA implementation.

Use these keywords with this command:

- **status**—Shows the geographical HA status.
- **switch**—Immediately moves from the primary HA gateway to secondary gateway.
- **configure**—Configures the following geographical HA parameters
  - **peergatewayname**—The peer gateway IP address or host name.
  - **peergatewayrmiport**—The peer gateway RMI port.
  - **healthcheckinterval**—The health check interval, in seconds.
  - **maxfailnum**—The maximum number of health check failures before a failover is initiated.
  - **synccsv**—Synchronizes the CSV files.
  - **ageout**—Sets the age time out.
  - **cachelimit**—Sets the cache limit.
- **backupdb** {*path*}—Backs up the primary gateway database. If the primary gateway is out of sync, sets it to in sync.
- **freeze**—Stop the health check of remote Secondary Gateway. Prevent failover during the Primary Gateway restart.
- **unfreeze**—Start the health check of remote Secondary Gateway.
- **backup**—Backs up data files to a backup location.
- **restore** {*filename*}—Restores gateway system files with specified backup file.

You must log in as the root user to use this command.

Available in GUI

No

Related Topics

Managing Geographical High Availability, page 12-18

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.

Available in GUI

No

ppm printreportstatus

Syntax

/opt/CSCOppm-gw/bin/ppm printreportstatus {**enable** | **disable**}

Command Description

Enables or disables report status printing in the Prime Performance Manager GUI.

Available in GUI

Yes

ppm props

Syntax

/opt/CSCOppm-gw/bin/ppm props

Command Description

Displays the contents of the *System.properties* files for both Prime Performance Manager server and client installations.

You must log in as the root user to use this command.

Available in GUI

Yes

ppm purgedb

Syntax

/opt/CSCOppm-gw/bin/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 are 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.

This command immediately removes logically deleted data from the 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. Some configuration changes might not be detected, and the viewable data displayed in the client application is incorrect.

Note This command does not cause the loss of any collected statistical data.

You must log in as the root user to use this command.

Available in GUI

No

ppm pwdchangeinterval

Syntax

/opt/CSCOppm-gw/bin/ppm pwdchangeinterval [*hours*]

Command Description

If password change restriction is enabled, specifies the length of time within which users cannot change their password more than the number of times specified in ppm pwdchangelimit applies in hours. The default is 48 hours. The allowable range is 1 through 745 hours.

Available in GUI

Yes

Related Topic

- ppm pwdchangerestrict, page B-52
- ppm pwdchangelimit, page B-52
- Edit User Security Settings, page 6-16

ppm pwdchangelimit

Syntax

/opt/CSCOppm-gw/bin/ppm pwdchangelimit [*limit*]

Command Description

If password change restriction is enabled, specifies the number of times users can change their passwords within length of time specified in ppm pwdchangeinterval. The default is 2. The allowable range is 1 through 10.

Available in GUI

Yes

Related Topic

- ppm pwdchangerestrict, page B-52
- ppm pwdchangeinterval, page B-51
- Edit User Security Settings, page 6-16

ppm pwdchangerestrict

Syntax

/opt/CSCOppm-gw/bin/ppm pwdchangerestrict {**enable** | **disable**}

Command Description

Enables or disables the password change restriction. If enabled, users cannot change their passwords more frequently than the number specified in ppm pwdchangelimit with the time interval specified in ppm pwdchangeinterval.

Available in GUI

Yes

Related Topic

- ppm pwdchangeinterval, page B-51
- ppm pwdchangelimit, page B-52
- Edit User Security Settings, page 6-16

ppm readme

Syntax

/opt/CSCOppm-gw/bin/ppm readme

Command Description

Displays the Prime Performance Manager README file contents.

Available in GUI

Yes

Related Topic

Chapter 3, “Managing the Web Interface”

ppm reboot

Syntax

/opt/CSCOppm-gw/bin/ppm reboot

Command Description

Reboots the Solaris Prime Performance Manager system.

You must log in as the root user to use this command.

Available in GUI

No

ppm redistributenodes

Syntax

/opt/CSCOppm-gw/bin/ppm redistributenodes

Command Description

Redistributes discovered network devices based upon the current unit configuration.

Available in GUI

Yes

ppm redundancygroups

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 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 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.

- **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.

Available in GUI

No

Related Topic

Creating Unit Protection Groups, page 12-8

ppm reloadbulkstats

Syntax

/opt/CSCOppm-gw/bin/ppm reloadbulkstats

Command Description

Reloads the bulkstatsschema.csv schema file. The bulkstatsschema.csv, located in the /opt/CSCOppm-gw/etc/, gathers bulk statistics from the Cisco ASR 5000 and 5500 Series devices. The bulk statistics include counters that Prime Performance Manager uses for reports. The counters are grouped into schemas, and schemas are grouped into types. For example, card is a type, so card schema 1 might have 20 card counters, card schema 2 might have another 20 card counters, and so on.

To generate reports from ASR 5000 and 5500, the devices must be configured with the schemas and counters, and the schema file must be generated in CSV format and exported at regular intervals to Prime Performance Manager.

Only counter values are exported. The bulkstatsschema.csv file provides the corresponding counter names used by Prime Performance Manager to read the CSV files (bulk statistics) generated from the ASR 5000/5500. If the ASR 5000/5500 devices are configured with a new schema or type or the counter sequence changed, the bulkstatsschema.csv file must be updated. This command updates the Prime Performance Manager in-memory schema counters list with the new counter information from /opt/CSCOppm-gw/etc/bulkstatsschema.csv.

You do not need to restart Prime Performance Manager.

The command supported only on the gateway.

Available in GUI

No

ppm reloadmibs

Syntax

/opt/CSCOppm-gw/bin/ppm reloadmibs

Command Description

Reloads the snmpinfo.dat file.

Available in GUI

Yes

ppm repdir

Syntax

/opt/CSCOppm-gw/bin/ppm repdir [*directory*] [**nostart**]

Command Description

Command to set directory used for reports. The server must be restarted for the directory changes to take effect. This normally occurs after running the command. Enter the **nostart** option if you want to restart server at a later time.

You must log in as the root user to use this command.

Available in GUI

No

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.

Available in GUI

Yes

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.

Available in GUI

No

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.

Available in GUI

No

Related Topic

- Backing Up Prime Performance Manager Data Files, page 14-2
- ppm backupdata, page B-9
- ppm backupdir, page B-10

ppm restore all

Syntax

/opt/CSCOppm-gw/bin/ppm restore all [**nostart**]

Command Description

Restores all system files. The server must be restarted for the directory changes to take effect. This normally occurs after running the command. Enter the **nostart** option if you want to restart server at a later time.

You must log in as the root user to use this command.

Available in GUI

No

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.

Available in GUI

No

ppm rootvars

Command Description

Displays the Prime Performance Manager gateway and unit root installation location, which is stored in the */etc/CSCOppm.sh* file.

Available in GUI

Yes

ppm sechelp

Syntax

/opt/CSCOppm-gw/bin/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.

Available in GUI

No

Related Topic

Chapter 6, “Managing Users and Security”

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 log offs.
- 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.

Available in GUI

Yes

Related Topic

Display the System Security Log, page 6-21

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.

- Verify that the new default hostname is valid and defined in your /etc/hosts file. If not, you might not be able to start the Prime Performance Manager server.
- Verify that the IP address of the resolved server name is the same to connect the gateway name.
- You must log in as root user to run this command.

- nostopstart - The server is not stopped and started automatically while running this command.

Note If you enabled Cisco Prime Central cross launching, you must reenable it after you change the server hostname. For information, see Enabling Prime Network Cross-Launching, page 5-4.

Available in GUI

No

Related Topic

- Chapter 2, "Managing Gateways and Units Using the CLI"

ppm setpath

Syntax

/opt/CSCOppm-gw/bin/ppm setpath [*username*]

Command Description

Appends binary (*bin*) directories to the user path so users can append 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.

Available in GUI

No

ppm setpctrapdestination

Syntax

/opt/CSCOppm-gw/bin/ppm setpctrapdestination

Command Description

After you integrate Prime Performance Manager with Prime Central, this command allows you to change the default trap destination. After integration, traps are sent to the Prime Central Fault Management. This command allows you to change the trap destination to Prime Network. When you run the command, output similar to the following is displayed:

```
Trap destinations registered with Prime Central:
1. Prime Fault Management (hostname)
2. Prime Network (hostname)
Enter trap destination: [1, 2] 2
Prime Performance is sending traps to: Prime Network
```

Available in GUI

No

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 hostname of the device (required)

Available in GUI

Yes

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.

Available in GUI

Yes

Related Topic

- ppm addsnmpcomm, page B-6
- ppm deletesnmpcomm, page B-19
- ppm modifysnmpcomm, page B-41
- ppm snmpsetup, page B-68

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.

Available in GUI

Yes

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 | block | status]

Command Description

Defines whether a user can log into multiple web interface sessions.

- **enable**—Only a single session is allowed per user. If a user logs into a second web interface session, the first session is ended.
- **disable**—Disables the single session per user restriction. The user can log in as the same user from multiple web interfaces.
- **block**—Only a single session is allowed per user. If a user attempts to log into a second web interface session, they are blocked until they close the first session.
- **status**—Shows the status of the single session per user.

You must log in as the root user to use this command.

Available in GUI

Yes

ppm snmpcomm

Syntax

/opt/CSCOppm-gw/bin/ppm snmpcomm [*name*]

Command Description

Sets 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.

Available in GUI

Yes

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.

Available in GUI

No

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.

Available in GUI

No

ppm snmphelp

Syntax

/opt/CSCOppm-gw/bin/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.

Available in GUI

No

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.

Available in GUI

No

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.

Available in GUI

No

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.

Available in GUI

Yes

Related Topics

- ppm addsnmpcomm, page B-6
- ppm deletesnmpcomm, page B-19
- ppm modifysnmpcomm, page B-41
- ppm showsnmpcomm, page B-61

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.

Available in GUI

No

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.

Available in GUI

no

Related Topics

Managing Users and User Security, page 6-12

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.

Available in GUI

Yes

Related Topic

Managing Users and User Security, page 6-12

ppm starbuild

Syntax

/opt/CSCOppm-gw/bin/ppm starbuild [**ppm** | **no** | **zero**]

Command Description

Sets up bulk statistics reporting configurations for Cisco ASR 5000 and Cisco ASR 5500 devices.

- **ppm**—Creates the configuration file to enable the Cisco ASR 5000 and Cisco ASR 5500 device to generates bulk statistics in the format expected by Prime Performance Manager.
- **no**—Removes the device configuration.
- **zero**—Sets the configuration to zero.

You must log in as the root user to use this command.

Related Topic

Setting Up Bulk Statistics Reports, page 7-24

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.

Available in GUI

No

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 CLI, page 2-1

ppm statreps

Full Syntax

/opt/CSCOppm-gw/bin/ppm statreps [**none**] [**default**] [**all**] [*enable* | *disable*] [*noexport* | *export*] [*nogenerate* | *generate*] **status,** [**status** [*node*]] **status config**, **status reps**, **config**, **reps**, [**setstatus**[*category*] [*enable* | *disable*]], [**setstatus**[*category*] [*enable* | *disable*] [*node*]], [**5min** [*enable*|*disable*|*enableall*]], [**15min** [*enable*|*disable*|*enableall*]], [**hourly** [*enable*|*disable*|*enableall*]], [**hourly** [*enable*|*disable*|*enableall*]], [**daily** [*enable* |*disable*|*enableall*]], [**weekly** [*enable* |*disable*|*enableall*]], [**monthly** [*enable* |*disable*|*enableall*]], [**5mincsvage** [*days*]], [**15mincsvage** [*days*]], [**hourlycsvage** [*days*]], [**dailycsvage** [*days*]], [**weeklycsvage** [*days*]], [**monthlycsvage** [*days*]][**5minage** [*days*]], [**15minage** [*days*]], [**hourlyage** [*days*]], [**dailyage** [*days*]], **weeklyage** [*days*]], **monthlyage** [*days*]],[*nodiskcheck* | *diskcheck*], [**timemode** [*12* | *24*]], [**csvnames** [*ppm* | *3gpp*]], [**expformat** [*xml*]], [**nametype**[*dnsname*] [*customname* | *sysname*]], [**csvtype** [*allnodes* | *pernodeuniq*]], [**zipcsvdelay** [*mins*]] [**zipcsvfiles** [*internal* | *script*]] [**zipcsvnotifscript** [*path* | *disable*]]

This command defines the master report settings. 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 with the IP address specified in *ip address.*

```
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 or disable the master report.

[*all*] - Enable all report types.

[*default*] - Enable all default report types.

[*none*] - Disable all report types.

[*noexport* | *export*] - Enable or disable all csv files.

[*nogenerate* | *generate*} - Generate database reports

status - Display network report settings.

status [*node*] - Display node report settings.

status config - Display master report configuration settings.

status reps - Display individual report enable status.

config - Display master report configuration settings.

reps - Display individual report enable status.

setstatus [[*category*] [*enable* | *disable*]] - Enable or disable network report settings.

setstatus [[*category*] [enable | disable] [node]] - Enable or disable node report settings.

1min [*enable* | *disable* | *enableall*] - Enable, disable, or enable all 1 minute master report.

5min [*enable* | *disable* | *enableall*] - Enable, disable, or enable all 5 minute master report.

15min [*enable* | *disable*] | *enableall* - Enable, disable, or enable all 15 minute master report.

hourly [*enable* | *disable* | *enableall*] - Enable, disable, or enable all hourly master report.

daily [*enable* | *disable*] | *enableall* - Enable, disable, or enable all daily master report.

weekly [*enable* | *disable*] | *enableall* - Enable, disable, or enable all weekly master report.

monthly [*enable* | *disable*] | *enableall* - Enable, disable, or enable all monthly 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.

weeklycsvage [*days*] - Specifies the days to keep weekly csv files.

monthlycsvage [*days*] - Specifies the days to keep monthly csv files.

ppm statreps bulkstatsage [*days*] - Specifies the days to keep bulk statistics import 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.

weeklyage [*days*] - Specifies the days to keep weekly data.

monthlyage [*days*] - Specifies the days to keep monthly data.

ppm statreps [*nodiskcheck* | *diskcheck*] - Enables or disables disk space monitoring.

timemode [*12* | *24*] - Display in 12 or 24 hour time.

csvnames [*ppm* | *3gpp*] - Specifies the format for csv file names, either ppm (CSV) or 3rd Generation Partnership Program (3GPP).

expformat [*xml*] - Specifies the export format as XML.

nametype [*dnsname* | *customname* | *sysname*] - Specifies the device name 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.

Available in GUI

- nodiskcheck, diskcheck, and timemode options: Yes
- All other options: No

Related Topic

Changing the Master Report Settings, page 7-14

ppm status

Syntax

/opt/CSCOppm-gw/bin/ppm status

Command Description

Displays the status of all Prime Performance Manager servers on the local host.

Available in GUI

Yes

Related Topic

Chapter 3, “Managing the Web Interface”

ppm status

Syntax

/opt/CSCOppm-gw/bin/ppm status

Command Description

Displays the status of all Prime Performance Manager servers on the local host.

Available in GUI

Yes

Related Topic

Chapter 3, “Managing the Web Interface”

ppm smtpport

Syntax

/opt/CSCOppm-gw/bin/ppm stmpport [*port #*)

Command Description

Changes the STMP mail server port for sending alarm e-mails. The default is 25.

You must log in as the root user to use this command.

Available in GUI

No

Related Topic

Configuring Alarms Sent to E-mail Addresses, page 9-13

ppm syncunits

Syntax

/opt/CSCOppm-gw/bin/ppm syncunits [enable | disable | status | now | force**]**

Command Description

Manages the synchronizations of configuration files between the gateway and units. The gateway is the master of configuration files. A change to the gateway report poller or other configuration file is replicated to the units by default.

Command options:

- enable—Enables file synchronization. It is enabled by default.
- disable—Disables file synchronization.
- status—Displays current status of file synchronization.
- now—Starts synchronization of changed or deleted files.
- force—Starts syncrhonization of all files.

Note Running the ppm syncunits force option can affect system performance. Use this option only for troubleshooting known problems.

Available in GUI

No

ppm traprelay

Syntax

/opt/CSCOppm-gw/bin/ppm traprelay [enable | disable | status**]**

Command Description

Enables or disables trap relays directly to hosts bypassing the Prime Performance Manager alarm processing. Before you enable the trap relay, you must add the host information to TrapForwarder.properties. See Forwarding Traps Directly to Hosts, page 9-14.

Available in GUI

No

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.

Available in GUI

No

ppm topxxsize

Syntax

/opt/CSCOppm-gw/bin/ppm topxxsize [*number*]

Command Description

Sets the number of entries displayed in the Top *nn* reports. By default, Prime Performance Manager displays the top 10 entries. This command can be used to change the default.

Available in GUI

Yes

ppm traceroute

Syntax

/opt/CSCOppm-gw/bin/ppm traceroute [*hostname*]

Command Description

You use this command to run the trace the route from a gateway to a device.

You must log in as the root user to use this command.

Available in GUI

Yes

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.

Available in GUI

No

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.

Available in GUI

No

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 Modifying the Password Policy, page 6-9.

See Enable User Accounts and Passwords Using the CLI, page 6-18 for more information on authentication levels and the use of this command.

You must log in as the root user to use this command.

Available in GUI

Yes

Note If you have enabled Solaris authentication, you must log in as the root user, to use this command (see Setting Up User Access and Security, 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 Up User Access and Security, page 6-1).

The **ppm useraccess** command goes through the following commands:

- **ppm useraccess**—Enabled or disabled.
- **ppm authtype**—If you have not set Prime Performance Manager authentication type, you must do so now.
- **ppm adduser**—If you have created 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.

Available in GUI

No

Related Topic

Setting Up User Access and Security, 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.

Available in GUI

Yes

Related Topic

Enable User Accounts and Passwords Using the CLI, page 6-18

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.

Available in GUI

Yes

ppm who

Syntax

/opt/CSCOppm-gw/bin/ppm who

Command Description

Displays a list of all client usernames and processes connected to the server.

Available in GUI

Yes

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 hostname of the device (required)
- **-p**—Package
- **-a**—Action
- **-d**—Parameters

Available in GUI

No

DRAFT - Cisco Confidential

APPENDIX C

Predefined Thresholds

You can create thresholds for any Prime Performance Manager report key performance indicator. For information about creating and managing thresholds, see Chapter 10, "Configuring Thresholds." Prime Performance Manager is delivered with predefined thresholds that cover common scenarios. These are listed in the following sections.

Utilization

- CPU Utilization
- Memory Utilization

Availability

- Disk Space Used Percentage
- ICMP Ping Response Time
- ICMP Ping Availability
- SNMP Ping Availability

IPSLA

- IPSLA DHCP Response Time
- IPSLA DNS Response Time
- IPSLA Ethernet OAM Response Time
- IPSLA HTTP Response Time
- IPSLA ICMP Jitter Response Time
- IPSLA MPLS Probe Response Time
- IPSLA RTT Response Time
- IPSLA TCP Connection Response Time
- IPSLA UDP Jitter Response Time
- IPSLA VoIP Delay Response Time
- IPSLA VoIP RTP Response Time
- IPSLA UDP Jitter Millisecs
- IPSLA UDP Jitter Packet Loss

DRAFT - Cisco Confidential

- IPSLA UDP Jitter Reachability
- IPSLA DHCP Reachability
- IPSLA DNS Reachability
- IPSLA Ethernet OAM Reachability
- IPSLA FTP Reachability
- IPSLA HTTP Reachability
- IPSLA ICMP Jitter Reachability
- IPSLA MPLS Probe Reachability
- IPSLA RTT Reachability
- IPSLA TCP Connection Reachability
- IPSLA Video Reachability
- IPSLA VoIP Delay Reachability
- IPSLA VoIP RTP Reachability
- IPSLA Y1731 Reachability
- IPSLA Y1731 Delay Two Way
- IPSLA ICMP Jitter Millisecs

IP

- IP Protocols -> OSPF
- IP QoS -> Class Map

Transport Statistics

- Interface Utilization
- Interface Error Percentage
- Interface Discard Percentage
- MPLS Interface
- Interface Availability

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.

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 hostnames, 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 "User Authentication" section on page 7.

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.

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 Up User Access and Security" section in Chapter 6, "Managing Users and Security."

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

A

accessing
  geographical HA gateways using the GUI 12-22
active alarms and event history
  displaying 9-1
active alarms and event history 9-2
active sessions
  displaying 6-20
adding
  upstream OSS hosts 9-11
  views to the Navigation Tree 7-35
adding and removing, properties 3-13
alarm and event properties
  displaying 9-6
alarm events
  displaying 9-8
alarm or event details
  displaying 9-8
alarms
  active alarms and event history 9-2
  and event filter dialog box other pane 9-5
  and events A-2
  bulk statistics 7-29
  by device properties 8-5
  displaying by device from the alarms window 9-11
  sent to e-mail addresses, configuring 9-13
  sent to OSS hosts, configuring 9-13
alarms and events, filtering 9-4
alarms and events, managing 9-3
alarms and events in geographical HA gateways, managing 12-23
alarms by device
  displaying 8-6
algorithms
  creating 7-45
algorithms, editor 7-46
and editing device polling groups
  creating 8-22
and removing properties from property views
  adding 3-13
a new polling group
  creating 8-23
application audit logs, displaying 11-7
architecture
  local HA 12-13
  Prime Performance Manager 1-4
archived, messages 11-14
archived messages, displaying 11-13
assigning devices, polling group 8-24
attributes
  notification 9-17
authentication
  local 6-9
  PAM, TACACS+, and LDAP 6-7
  Solaris and Linux 6-9
auto expand, report summary tables 3-10

B

backup directory
  changing 14-3
backup directory, changing 14-3
backup logs, displaying 11-5
bulk statistics
  alarms 7-29

bulk statistics device configurations, removing 7-28
bulk statistics reports, setting up 7-24

C

capability polling 7-18
changing
    report settings 7-14
changing, poller settings 3-13
chart legends, editing color 3-8
CISCO-EPM-2 trap, notification attributes 9-19
CISCO-PRIME trap
    notivation attributes 9-16
CISCO-PRIME trap, notification attributes 9-16
CLI command log, displaying 11-5
client access, limiting access to servers 2-9
color
    setting chart legend colors 3-8
command line interface A-3
command reference B-1
commands
    changing system properties 11-8
    hacommands B-36
    ppm B-5
    ppm addunitconf B-6
    ppm adduser B-7
    ppm backup B-8
    ppm backupdir B-10
    ppm badloginalarm B-12
    ppm badlogindisable B-12, B-13
    ppm certtool B-13
    ppm changes B-14
    ppm checksystem B-14
    ppm clitimeout B-14
    ppm cmdlog B-15
    ppm console B-16
    ppm consolelogsize B-16
    ppm countnodes B-16
    ppm datadir B-17
    ppm delete B-18
    ppm deletesnmpcomm B-19
    ppm deleteunitconf B-19
    ppm deluser B-20
    ppm disablepass B-20
    ppm disableuser B-21
    ppm discover B-22
    ppm diskcheck B-22
    ppm diskmonitor B-22
    ppm enablepwdage B-24
    ppm enableuser B-21, B-24
    ppm eventautolog B-24
    ppm eventconfig B-25
    ppm eventlimitsconfig B-25
    ppm eventsnmpserversconfig B-26
    ppm eventtool B-26
    ppm evilstop B-28
    ppm export B-28
    ppm exportcustnames B-28
    ppm exportusers B-28
    ppm gatewayname B-29
    ppm habackupflag B-35
    ppm happmtimeout B-36
    ppm help B-29
    ppm ifnameformat B-30
    ppm inactiveuserdays B-31
    ppm installlog B-32
    ppm inventoryimport B-32
    ppm iosreport B-32
    ppm ipaccess B-33
    ppm ipslaftpfilesize B-33
    ppm jspport B-34
    ppm keytool B-34
    ppm listusers B-35
    ppm logger B-37
    ppm logsize B-37
    ppm logtimemode B-38
    ppm maxasciirows B-39
    ppm maxhtmlrows B-39

ppm maxpagesize B-40
ppm maxrepqueries B-40
ppm mldebug B-40
ppm modifyunitconf B-42
ppm motd B-42
ppm msglog B-43
ppm msglogage B-43
ppm msglogdir B-44
ppm netlog B-44
ppm netlogger B-45
ppm newlevel B-45
ppm optimizecapabilitypoll B-45
ppm osinfo B-46
ppm passwordage B-46
ppm patchlog B-47
ppm ping B-47
ppm poll B-47
ppm premotd B-48
ppm primecentralintegration B-48
ppm primeha B-49
ppm print B-50
ppm printreportstatus B-50
ppm props B-50
ppm purgedb B-51
ppm pwdchangeinterval B-51
ppm pwdchangelimit B-52
ppm pwdchangerestrict B-52
ppm readme B-53
ppm reboot B-53
ppm redistributenodes B-53
ppm redundancygroups B-54
ppm reloadbulkstats B-55
ppm repdir B-56
ppm rephelp B-56
ppm restart B-56
ppm restore B-57
ppm restoreprops B-58
ppm rootvars B-58
ppm sechelp B-58
ppm seclog B-59
ppm servername B-59
ppm setpath B-60
ppm setpctrapdestination B-61
ppm showcreds B-61
ppm showsnmpcomm B-61
ppm showunitconf B-62
ppm singlesess B-62
ppm smtpport B-75
ppm snmpcomm B-63
ppm snmpconf B-63
ppm snmpget B-63
ppm snmphelp B-66
ppm snmpmaxrows B-66
ppm snmpnext B-66
ppm snmpwalk B-69
ppm ssl B-71
ppm sslstatus B-72
ppm starbuild B-72
ppm start B-73
ppm statreps B-73
ppm status B-75
ppm syncunits B-76
ppm tac B-77
ppm topxxsize B-77
ppm traceroute B-77
ppm uninstall B-78
ppm unknownage B-78
ppm updateuser B-78
ppm useraccess B-79
ppm userpass B-79
ppm version B-80
ppm who B-80
ppm xmlpoll B-81
configuring
gateway and unit communication 13-3
gateways and units for firewalls 13-2
unit and device communication 13-6
web client and gateway communication 13-3

connected clients and system status, displaying 11-2
console log, displaying 11-5
console log archived messages, displaying 11-7
creating
  custom device star graphs 7-12
  custom report views 7-34
  device bulk statistics configuration 7-27
  device polling groups 8-22
  device-to-unit maps 12-6
  report groups 7-42
  report policies 7-20
  star graphs 7-12
  unit protection groups 12-8
creating, a new polling group 8-23
creating, thresholds 10-1
credentials for Cisco Carrier Packet Transport devices
  adding 5-10
cross launch, enabling from Prime Network 5-4
CSV
  exporting 7-5
custom device star graphs, creating 7-12
customizing
  date and time 7-7
  report display 7-9
custom report view
  creating 7-34
custom report views, creating 7-34

D

daily alarm and event archives, displaying 9-9
dashboards
  editing the display 7-32
  enabling and disabling 7-31
  managing 7-31
  menu bar 7-33
dashboards, managing 7-31
data
  accessing, from the web 10-1
  collection 8-20
data center
  device support 5-12
  supported devices and technologies 7-22
deleting
  device-to-unit maps 12-7
  SNMP credentials 5-6
  Telnet/SSH credentials 5-9
deleting, thresholds 10-9
device
  average poll responses 8-7
  changing history limit 3-8
  contacts and locations 8-9
  details 8-18
  details in prime style 8-10
  details when cursor is placed over a link 3-8
  discovery A-2
  discovery overview 1-6
  discovery requirements 5-1
  distributions 8-5
  management actions A-2
  name settings, changing 3-8
  properties 8-2
  show domain name 3-8
  up time 8-8
  vendor information 8-10
device bulk statistics configuration
  creating 7-27
device contacts and locations, displaying 8-9
device credentials, managing 5-5
device discovery
  from Prime Performance Manager 5-10
device name and web port, editing 8-13
device polling groups, creating 8-22
device poll responses, displaying 8-7, 8-8
devices
  assigning to polling groups 8-24
  assigningto report policies 7-21
  discovering 5-4

importing from Prime Network 5-2
devices in geographical HA gateways, managing 12-23
devices in the network-level view, managing 8-11
device snmp ip addresses, editing 8-16
device SNMP time out alarms, displaying 8-7
device software versions, displaying 8-9
devices to units, relocating 8-16
device-to-unit assignment
changing 12-8
device-to-unit assignments, changing 12-8
device-to-unit assignments, managing 12-5
device-to-unit assignments, viewing 12-6
device-to-unit maps
creating 12-6
device-to-unit maps, creating 12-6
device-to-unit maps, deleting 12-7
device-to-unit maps, editing 12-7
device type distributions, displaying 8-4
device up time, displaying 8-8
disabling 7-16
passwords 6-17
users 6-17
disaster recovery, manual 12-26
discovering
network devices from Prime Network 5-2
discovery
from Prime Performance Manager 5-10
XEN and KVM TLS requirements 5-14
discovery, overview 5-1
discovery requirements
hypervisor 5-14
displaying
active alarms and event history 9-1
alarm and event properties 9-6
alarm events 9-8
alarm or event details 9-8
alarms by device 8-5
alarms by device from the alarms window 9-11
alarms by device type 8-6
alarms by device type from the alarms window 9-11
an alarm summary 9-4
application audit logs 11-7
archived messages 11-13
backup log 11-5
cli command log 11-5
connected clients and system status 11-2
console log 11-5
console log archived messages 11-7
daily alarm and event archives 9-9
dashboards status 7-31
data center reports 7-22
detailed gateway and unit information and performance 12-3
device contacts and locations 8-9
device details for an alarm 9-9
device details in cisco prime format 8-10
device icmp ping responses and availability 8-8
device poll responses 8-7
device snmp TIME out alarms 8-7
device software 8-9
device-to-unit assignments 12-6
device type distributions 8-4
device up time 8-8
device vendors 8-10
event automation log 11-6
gateway and unit information 12-1
gateway and unit software versions 2-8
gateway and unit status 2-6
geographical HA status 12-19
group reports 7-48
individual device information 8-17
information and error messages 11-11
install log 11-4
network and device reports 7-6
network-level device information 8-1
patch log 11-4
poller settings 11-9
Prime Performance Manager information 3-14

Prime Performance Manager version 2-8
report definitions 7-22
reports 7-1
reports settings 11-10
security log 11-6
system check log 11-5
system logs 11-4
system messages 11-11
system properties and settings 11-8
system security log 6-21
system settings 11-8
threshold parameters from the alarms window 10-6
user actions 11-12
web configuration properties 11-9
web settings 11-9
display settings, changing 3-9
duplicating, thresholds 10-7

E

editing
dashboard display 7-32
device credentials 8-13
device name, web port, and time zone 8-13
device SNMP IP addresses 8-16
device-to-unit maps 12-7
polling group assigned to a device 8-15
polling group parameters 8-23
report policy assigned to a device 8-15
report policy parameters 7-20
snmp credentials 5-6
thresholds from the alarms window 10-6
thresholds from the threshold editor 10-5
upstream OSS hosts 9-12
views 7-40
editing polling group parameters, polling 8-23
enabling
Prime Network cross-launch 5-4
reports and report intervals 7-18
secure user access 6-11
SSL on a gateway or collocated gateway and unit 6-3
SSL on gateways and units 6-2
SSL on remote units 6-4
user accounts and passwords using the CLI 6-18
enabling and disabling
reports 7-16
thresholds 10-8
error messages, information 11-11
event automation log, displaying 11-6

F

failovers and switchovers
local HA 12-14
features
security 1-6
filtering
alarms and events 9-4
report information 7-13
floating IP address
changing 12-15
floating IP address, changing 12-15
forwarding
traps to hosts 9-14

G

gateway
HA operations notes 12-13
high availability architecture 12-13
gateway and unit, properties 12-2
gateway and unit connectivity, managing 12-5
gateway and unit information, displaying 12-1
gateway and unit status, displaying 2-6
gateway high availability, managing 12-11
gateways, restarting 2-4
gateways, starting 2-2

gateways, stopping 2-3
gateways and units
properties 12-3
starting using the CLI 2-1
gateways and units, discovering 5-2
gateways and units, version 2-8
gateway-to-unit connectivity 13-1
geographical and local high availability, managing 12-25
geographical HA
configuring 12-21
geographical HA gateway data
backing up and restoring 12-22
geographical HA gateways, freezing and unfreezing 12-22
geographical HA gateways, synchronizing 12-21
geographical high availability, managing 12-18
graph, time span bar 7-12
graph bar and data display options 7-11
groups
protection 12-10
provided 7-43
GUI, optimize for slow connections 3-9
GUI polling refresh setting, changing 3-13

H

HA, failovers and switchovers 12-14
hypervisor, discovery requirements 5-14

I

individual device information, displaying 8-17
individual devices, managing 8-21
information
error messages 11-11
from the Help Menu 3-5
information and error messages, displaying 11-11
install log, displaying 11-4
integrating
Prime Performance Manager with Prime Central 4-1
IPv6
Prime Performance Manager support A-1
troubleshooting A-3

J

JVM, checking versions 6-8

L

last login date and time, changing 3-9
launching,web interface 3-1
LDAP 6-7
local HA
architecture 12-13
failovers and switchovers 12-14
operations notes 12-13
local high availability, managing 12-12
log files, managing 11-7
logging in
as the Root user 2-1
login window 3-2
log messages, RHCS 12-16

M

managing
alarms and events 9-3
alarms and events in geographical HA gateways 12-23
dashboards 7-31
device credentials 5-5
devices in geographical HA gateways 12-23
devices in the network-level view 8-11
device-to-unit assignments 12-5
gateway and unit connectivity 12-5
gateway high availability 12-11
geographical and local high availability 12-25

geographical high availability 12-18
individual devices 8-21
local high availability 12-12
log files 11-7
report groups 7-47
reports 7-1
reports, views, and groups in geographical HA gateways 12-23
thresholds 10-5
thresholds and upstream alarm hosts in geographical HA Gateways 12-24
user access and security 6-1
users and user security 6-12
users in geographical HA gateways 12-23
manual, disaster recovery 12-26
master report settings, changing 7-14
menus, navigation 3-4
merging
view charts 7-40
message of the day, configuring 6-19
messages
display, changing 11-7
messages of the day 6-19
creating 6-19
modifying
custom report views 7-37
password policy 6-9

N

navigation
menus 3-4
network alarms by device properties 8-5
network-level device information 8-1
network-level device information, displaying 8-1
network-level device properties, displaying 8-2
new bulk statistics schemas or counters
adding 7-28
new polling group
creating 8-23
new report policy
creating 7-21
new users
adding 6-12
Nexus switches in VDC mode, discovering 5-13
notes to alarms or events
adding 9-7
notification, attributes 9-17
notification attributes
CISCO-EPM-2 trap 9-19
number of backup days, setting 14-3

O

operations notes
local HA 12-13
options, data 7-11
options, graph bar 7-11

P

page size 7-5
parameters
polling group 8-23
passwords, changing user 6-15
patch log, displaying 11-4
Pluggable Authentication Modules (PAM) 6-7
poller
settings, changing 3-13
poller settings, displaying 11-9
polling
creating a new polling group 8-23
editing polling group parameters 8-23
polling group parameters 8-23
polling, capability 7-18
polling group
assigning devices to 8-24

parameters 8-23
polling group assigned to a device, editing 8-15
polling group parameters, editing 8-23
polling group parameters, polling 8-23
ports
used by Prime Performance Manager 13-3
post integration,commands and procedures 4-6
primary and secondary geographical HA gateways, switching 12-20
primary gateway, running status 12-19
Prime Central
integrating Prime Performance Manager 4-1
Prime Central integration
considerations and next steps 4-5
post integration commands and procedures 4-6
troubleshooting 4-4
Prime Network, importing devices 5-2
Prime Network cross-launch, enabling 5-4
Prime Performance Manager
about 3-xv
architecture 1-4
backing up data files 14-2
back up and restore process 14-1
client and server communication
VPN 13-2
commands B-1
communication 13-1
dashboards overview 1-3
database 1-5
device discovery 5-4
discovering devices 5-10
displaying information about 3-14
features and functions 1-1
integrating with Prime Central 4-1
IPv6 A-1
login window 3-2
ports 13-3
ports 13-3
reports overview 1-3
restarting gateways and units 2-4
server 5-1
SNMP traps 9-16
starting gateways and units 2-1
stopping gateways and units 2-3
supported browsers 3-1
user levels 6-10
user levels 6-10
web interface
archived messages 11-13
logs
command 11-5
console 11-5
event automation 11-6
security 11-6
Prime Performance Manager, architecture 1-4
Prime Performance Manager bulk statistics schema file, updating 7-28
Prime Performance Manager client, limiting access 2-9
Prime Performance Manager data files
backing up 14-2
Prime Performance Manager data files, restoring 14-3
Prime Performance Manager server, starting 5-1
Prime Performance Manager Window 3-4
Prime Performance Manager with Prime Central, integrating 4-1
properties
tables, sorting 3-14
properties, adding and removing 3-13
properties, detailed gateway and unit 12-3
properties, gateway
and unit 12-2
protection, groups 12-10
provided, groups 7-43

R

redundant units, in active status 12-10
reference, commands B-1
relocating

devices to units 8-16
removing
bulk statistics device configurations 7-28
report chart, adding to clipboard tool 7-9
report graphs
add to star charts tool 7-10
export to image tool 7-10
report group
creating 7-44
report groups, creating 7-42
report groups, managing 7-47
report policies
assigning devices to 7-21
creating 7-20
creating new 7-21
editing 7-20
report policies, creating 7-20
report policy assigned to a device, editing 8-15
reports
changing settings 7-14
creating policies 7-20
custom views 7-34
data options 7-17
definitions, displaying 7-22
displaying 7-1
enabling and disabling 7-16
filtering information 7-13
historical statistics settings 7-15
managing 7-1
menu bar 7-3
settings, changing 3-10
viewing 7-6
reports, searching 7-3
reports, views, and groups in geographical HA gateways, managing 12-23
reports, window 3-4
reports and report intervals, enabling 7-18
reports graphs
show chart in full screen tool 7-9
toggle area charts tool 7-10
reports in 3GPP XML format, exporting 7-19
reports settings, displaying 11-10
reports table view
hide series tool 7-9
restarting
gateways 2-4
units 2-5
restoring
Prime Performance Manager data files 14-3
RHCS, freezing and unfreezing 12-14
RHCS, log messages 12-16
RHCS cluster server, switching 12-15
RHCS Conga web interface
configuring 12-17
RHCS conga web interface, configuring 12-17
RMI
how it works 13-2
RMI components 13-2
root user
becoming 5-1
login 2-1
Root user, logging in 2-1
RSA, generation 6-3

S

searching
reports 7-3
secondary HA gateway, running status 12-19
secure user access
disabling 6-12
secure user access, enabling 6-11
security
client access, limiting 2-9
days before forcing password change 6-16
editing user security 6-16
logs, system 6-21
message of the day 6-19

number of active client sessions 6-16
overview 1-6
passwords, creating 6-9
passwords, disabling manually 6-17
passwords, re-enabling 6-18
user-based access
disabling 6-12
implementing 6-7
user levels 6-10
basic user 6-10
network operator 6-10
system administrator 6-11
users
changing 6-18
listing current 6-20
security log, displaying 11-6
server
Prime Performance Manager 5-1
server properties
displaying 11-9
setting
number of backup days 14-3
settings
historical reports 7-15
setting up
bulk statistics reports 7-24
slow connections, optimize 3-9
SNMP and Telnet/SSH credentials
adding A-1
SNMP credentials
adding 5-5
deleting 5-6
editing 5-6
SNMP credentials, deleting 5-6
software versions 8-9
Sorting, tables 3-14
SSH
adding credentials 5-7
SSL
configuring on geographical HA gateways and remote units 12-24
disabling 6-6
enabling 6-2
enabling on gateway or collocated gateway and unit 6-3
enabling on remote units 6-4
key and certificate, displaying 6-6
status, displaying 6-5
status and printing certificates 6-5
viewing and exporting certificates 6-5
SSL certificates, exporting 6-5
SSL certificates, printing 6-5
SSL on a gateway or collocated gateway and unit, enabling 6-3
SSL on gateways and units, enabling 6-2
SSL on remote units, enabling 6-4
star graphs, creating 7-12
starting
gateways 2-2
Prime Performance Manager server 5-1
units 2-3
status, gateway and unit 2-6
stopping
gateways 2-3
units 2-4
strict synchronization 5-3
switching
primary and secondary geographical HA gateways 12-20
RHCS cluster server 12-15
synchronizing, geographical HA gateways 12-21
system
menu logs and messages 11-2
system configuration settings, changing 3-11
system logs, displaying 11-4
system messages, displaying 11-11
system properties
statuses, logs, and messages overview 11-1
systemproperties

viewing 11-8
system properties and settings, displaying 11-8
system settings, displaying 11-8

T

tables, sorting 3-14
TACACS+ 6-7
Telnet
adding credentials 5-7
Telnet/SSH credentials, deleting 5-9
Telnet and SSH, credential notes 5-9
Telnet and SSH credentials
adding 5-7
threshold dialog box
adding 10-2
threshold events, viewing 10-9
threshold parameters from the alarms window, displaying 10-6
thresholds
creating 10-1
deleting 10-9
editing 10-5, 10-7
enabling and disabling 10-8
managing 10-5
predefined C-1
viewing from Alarms window 10-6
thresholds, deleting 10-9
thresholds, duplicating 10-7
thresholds, managing 10-5
thresholds, predefined C-1
thresholds and upstream alarm hosts in geographical HA Gateways, managing 12-24
thresholds from the alarms window, editing 10-6
thresholds from the threshold editor, editing 10-5
threshold tools
adding 10-1
time span bar, graph 7-12
trap forwarding A-3
traps to hosts, forwarding 9-14
tuning
event and alarm parameters 9-11, 9-15

U

unit protection groups
creating 12-8
units
configuration A-2
protection group failover scenarios 12-11
redundancy groups and geographical HA 12-25
units, restarting 2-5
units, starting 2-3
units, stopping 2-4
updating
Prime Performance Manager bulk statistics schema file 7-28
upstream alarm hosts
configuring 9-11
upstream OSS hosts, adding 9-11
upstream OSS hosts, editing 9-12
user
access,disabling 6-12
access, enabling 6-11
actions 11-12
authentication 6-7
passwords, configuring 6-9
security levels 6-10
user, editing information 6-13
user access and security, managing 6-1
user accounts and passwords using the CLI, enabling 6-18
user actions, displaying 11-12
user passwords
changing 6-15
configuring 6-9
user preferences
changing 3-7
user preferences, changing 3-7

user reports, editing 6-14
users
  changing passwords 6-15
  changing preferences 3-7
  editing information 6-13
  managing through GUI 6-12
  setting up access and security 6-1
  setting up and managing 6-1
users, list currently defined 6-20
users and passwords
  manually disable 6-17
users and user security, managing 6-12
user security settings, editing 6-16
users in geographical HA gateways, managing 12-23

V

view
  editor 7-41
  graph 7-3
  list 7-3
  tab 7-39
  table 7-3
  tree 7-3
view charts, merging 7-40
viewing
  device-to-unit assignments 12-6
  reports 7-6
  system properties 11-8
  threshold events 10-9
views
  copying and pasting 7-36
  creating custom 7-34
  managing 7-40
  modifying custom 7-37
views to the Navigation Tree, adding 7-35

W

web
  checking browser settings 3-7
  configuration properties, displaying 11-9
  settings 11-10
web browser
  checking 3-7
web browsers,supported 3-1
web interface, launching 3-1
web settings, displaying 11-9

X

XEN and KVM TLS, discovery requirements 5-14