Cisco Prime Performance Manager 1.7 User Guide

Released: August 31, 2015

Revised: November 30, 2017

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Cisco Prime Performance Manager 1.7 User Guide

CONTENTS

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:

New and Revised Information

Table 1-1 lists new and revised information since the Prime Performance Manager 1.7 release.

Table 1-1 New and Revised Information

Date	Change	Location
8/31/15	Initial release	
11/10/15	Added a note about integrating Prime Performance Manager to Prime Network gateways configured for high availability.	Updating the Prime Network Device Inventory, page 4-8
10/13/15	Changed 3G Access Points to 3G and 4G Access Points.	• Small Cell Discovery Requirements, page 5-16 • Setting Up Small Cell Reports, page 8-33

Table 1-1 New and Revised Information

Date	Change	Location
03/31/17	• Added a procedure to ensure version compatibility between StarOS devices and Prime Performance Manager. • Local High Availability support on RHEL 6.x	• Upgrading StarOS devices and Prime Performance Manager to ensure Version Compatibility, page 8-26 • Configuring the RHCS Conga Web Interface, page 14-6
05/31/17	• Revised procedure for assigning correct serial number to unknown devices. • Support for RHEL 6.7 • Supported Mobility StarOS Releases	• Table 9-2 • Managing Local High Availability, page 14-1 • Table 8-2
07/31/17	Enhancements for Threshold and KPI Values	• Threshold Values, page 11-6 • KPI Values, page 11-7

Features and Functions

Prime Performance Manager acquires devices by importing Cisco Prime Network devices or by running device discovery (see Chapter 5, "Discovering Devices With Prime Performance Manager"). 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 device credentials for many other protocols including:

- Telnet
- SSHv1
- SSHv2
- WSMA_SSH
- collectd_SSH
- HTTP
- HTTPS
- HTTP_BULK
- WMI_HTTP
- WMI_HTTPS
- SMI_HTTPS
- ULS_HTTP
- vCenter_HTTPS
- ESXi_HTTP

- ESXi_HTTPS
- XEN_TLS
- KVM_TLS
- HyperV_HTTP
- HyperV_HTTPS
- JMX
- PNSC_HTTPS
- GMOND_SOCKET
- AVI_HTTPS

For information about device credentials outside of SNMP supported by Prime Performance Manager, see Adding Device Credentials for Other Protocols, page 5-6.

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 collection 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 8-1.

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 7300 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. In addition, you can create custom web reports using the Prime Performance Manager Web Report Editor.

Tip For a list of all Prime Performance Manager reports, 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.
- The ability to create custom web reports.
- 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.
- Synchronized device inventory and credentials from Prime Network and/or Prime Central.
- Automatic device discovery and data collection based on device IP address ranges.
- Geographical HA and disaster recovery.
- Support for NetFlow data collection.
- Support for JMX data collection.
- Support for monitoring virtualized environments running VMware, Zen, KVM, and Hyper-V.
- 95th percentile reporting.
- Trending and forecasting.
- Automatic emailing of scheduled reports.
- Graphical report writing.
- Data collection support for:
  - Standard protocols
  - SNMP V1, V2, and V3
  - CLI-based and CSV-based (bulk statistics)
  - NETCONF
  - NetFlow
- Support for Cisco Small Cell Solutions devices and technologies.
- 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 7200 reports. With a few exceptions, all reports support table and graph outputs. Top-level report categories include:

- Application Traffic
- Applications
- Availability
- Compute
- IP Protocols
- IP QoS
- IP SLA
- JMX Applications
- Layer 2 Protocols
- Mobile IOS Statistics
- Mobile StarOS All Counters
- Mobile StarOS CDMA KPI
- Mobile StarOS CDMA Statistics
- Mobile StarOS KPI
- Mobile StarOS Statistics
- NetFlow
- NetFlow AVC
- Network
- Network Services
- OpenStack
- Orchestration
- PPM System
- Resources
- Security
- Small Cell Statistics
- Storage
- Transport Statistics
- Video Broadcast

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 1.7 Integration Developer Guide*.

Tip To display an alphabetical list of every report provided by Prime Performance Manager, from the Help menu, choose **Reports > Reports List Readme**.

Dashboards

Prime Performance Manager dashboards present data from different sources on a single page. For example, the Internet Control Message Protocol (ICMP) 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. Dashboard categories provided with Prime Performance Manager include:

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

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.

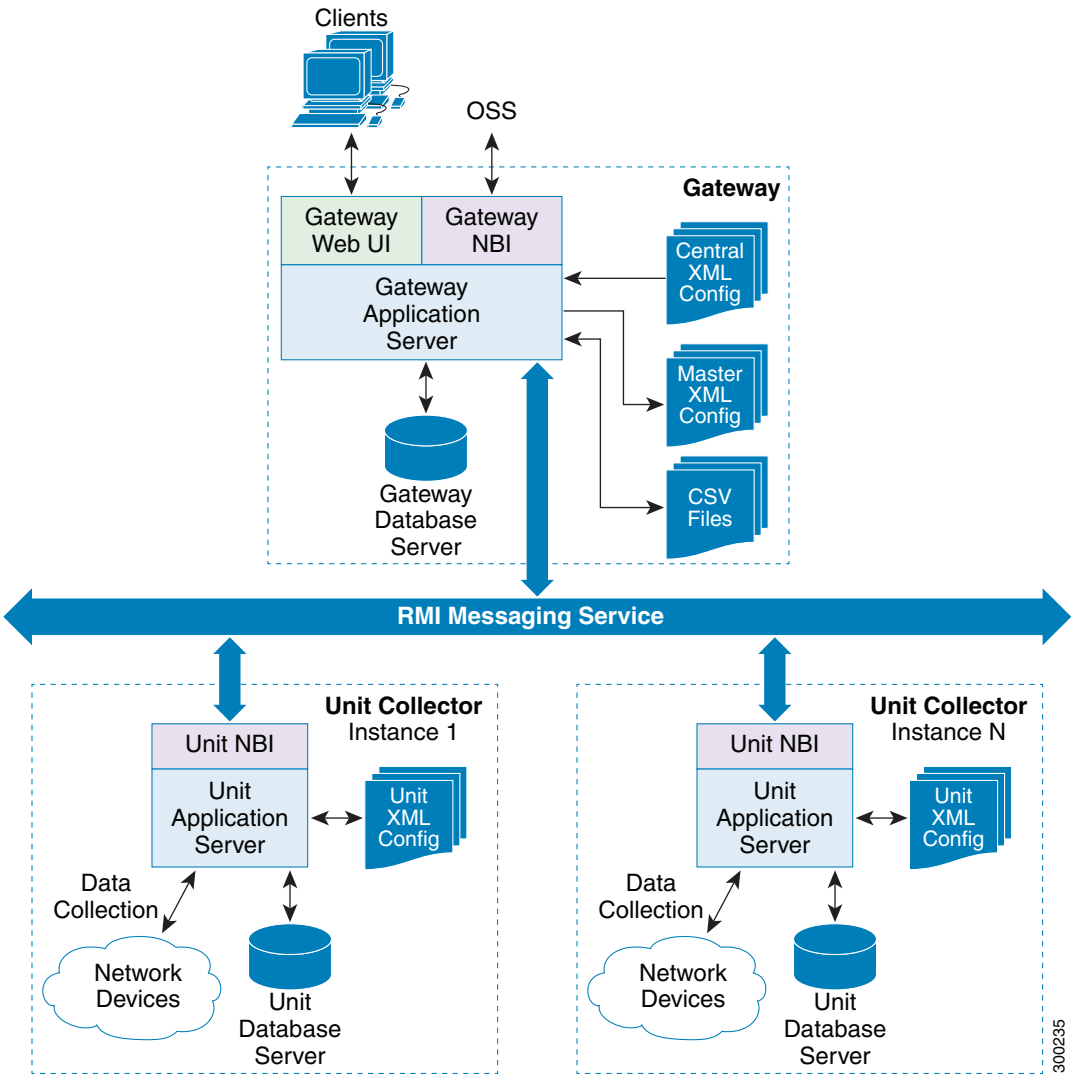
Units poll network devices and compute and store the data received from the devices. A unit can be installed with a gateway on the same physical server, or a unit can be installed on a separate physical server. The monitored devices are distributed across a single or multiple units, as directed by the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



The Prime Performance Manager database is based on Apache Derby and LevelDB. Apache Derby is an open source relational database based on Java, LevelDB is a fast key-value storage library written at Google that provides an ordered mapping from string keys to string values. LevelDB is used primarily for report data.

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, Cisco Prime Central, or Cisco Prime Network Service Controller.
- 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 Devices With Prime Performance Manager."

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."

Managing Gateways and Units Using the CLI

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

Logging In as the Root User

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

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
```

For information about the ppm superuser command, see ppm superuser, page B-108.

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.

Running Prime Performance Manager as a Non-Root User

You can use the ppm superuser command to create a user that can run Prime Performance Manager as a non-root user. The command will update the number of soft and hard processing sessions (nproc) in /etc/security/limits.conf to 63536. Before starting your first non-root user session, verify that the number of soft and hard nprocs are greater than 16000.

To find the nproc values look for entries marked with the super user id in the first column. For example, if the user ID is superuser the entries might look like the following in /etc/security/limits.conf:

```
superuser    soft    nproc           63536
superuser     hard    nproc           63536
```

If no user specific entries are found, look for default nproc entries, for example:

```
*    soft    nproc           63536
*     hard    nproc           63536
```

The number in the fourth column is the number of processes allowed. If there are no entries or the number of processes allowed is too low, add or update the following lines in /etc/security/limits.conf:

```
superuser    soft    nproc           16000 > 63536
superuser     hard    nproc           16000 > 63536
```

Gateway and Unit Command Summary

You can use the following CLI commands with parameters to start and stop the Prime Performance Manager gateway and units:

ppm start gw—Starts all processes on the gateway.

ppm restart gw—Restarts all processes on the gateway.

ppm start unit—Starts all processes on the unit.

ppm restart unit—Restarts all processes on the unit.

ppm start both—Starts all processes on the gateway and unit.

ppm restart both—Restarts all processes on the gateway and unit.

ppm stop gw—Stops all process on the unit.

ppm stop unit—Stops all process on the unit.

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, or other protocol used to connect to devices, is enabled. For information about other device protocols supported by Prime Performance Manager, see Adding Device Credentials for Other Protocols, page 5-6.

- 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 StarOS Bulk Statistics Reports, page 8-21.

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 installation, 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 or user enabled with ppm superuser. See Logging In as the Root User, page 2-1.

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

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

The gateway components are started:

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

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

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

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

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

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

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

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

Step 2 To start the unit, enter:

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

The unit components are started:

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

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

Stopping 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 or user enabled with ppm superuser. See Logging In as the Root User, page 2-1.

Step 2 To stop the gateway, enter:

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

The gateway components are stopped:

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

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

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

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

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

Note The ppm stop command stops the gateway and automatically stops the unit if it is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-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 into the unit as the root user. See Logging In as the Root User, page 2-1.

Step 2 To stop the unit, enter:

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

The unit components are stopped:

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

Restarting Gateways and Units

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

Step 1 Log in as the root user or user enabled with ppm superuser. See Logging In as the Root User, page 2-1.

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

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

First, the gateway components are stopped:

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

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

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

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

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

Next, the gateway components are started:

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

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

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

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

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

Note The ppm restart command restarts the gateway and automatically restarts the unit if it is installed on the same machine. This occurs regardless of whether you initiate the command from the gateway install directory (/opt/CSCOppm-gw/bin/) or the unit install directory /opt/CSCOppm-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 Logging In as the Root User, page 2-1.

Step 2 To restart the unit, enter:

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

The unit components are stopped:

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

Then the unit components are started:

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

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 user enabled with ppm superuser. See Logging In as the Root User, page 2-1.

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

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

The gateway status is displayed, for example:

```
================================================================================
Prime Performance Manager Gateway Version      : 1.7.0.000
Prime Performance Manager Gateway Build        : Tue Jul 28 16:02 EST 2015
Prime Performance Manager Gateway Install      : Tue Jul 28 16:25 EST 2015
Prime Performance Manager Gateway Hostname     : ems-lnx408
Prime Performance Manager Gateway SSL Support  : Installed [Disabled]
================================================================================
   sgmMsgLogServer:    1.7.0.000   Tue Jul 28 15:59 EST 2015
   sgmDataServer:      1.7.0.000   Tue Jul 28 15:59 EST 2015
================================================================================
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/Web        Server  IS  Running.
Maximum Memory Used: 1387562/2097152
Event model queue size is 0. Queue is not congested!
Last Restart:
   Tue Jul 28 16:26:29 EST 2015
Linux Uptime:
 14:50:07 up 87 days, 14:28,  2 users,  load average: 0.39, 0.42, 0.44
Current Time: 2015/12/12 14:50:07 EST
================================================================================
Prime Performance Manager Unit Version      : 1.7.0.000
Prime Performance Manager Unit Build        : Tue Jul 28 16:02 EST 2015
Prime Performance Manager Unit Install      : Tue Jul 28 16:25 EST 2015
Prime Performance Manager Unit Hostname     : ems-lnx408
Prime Performance Manager Unit SSL Support  : Installed [Disabled]
Prime Performance Manager Unit Gateway Name : ems-lnx408
```

```
================================================================================
   sgmMsgLogServer:    1.7.0.000   Tue Jul 28 15:59 EST 2015
   sgmDataServer:      1.7.0.000   Tue Jul 28 15:59 EST 2015
================================================================================
```

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

```
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.
Maximum Memory Used: 2133650/3145728
Event model queue size is 0. Queue is not congested!
Last Restart:
   Tue Jul 28 17:51:18 EST 2015
Linux Uptime:
 14:50:15 up 87 days, 14:28,  2 users,  load average: 0.65, 0.47, 0.46
Current Time: 2015/12/12 14:50:15 EST
```

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

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

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

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

The unit status is displayed, for example:

```
================================================================================
Prime Performance Manager Unit Version:      1.7.0.000
Prime Performance Manager Unit Build        : Tue Jul 28 16:02 EST 2015
Prime Performance Manager Unit Install      : Tue Jul 28 16:25 EST 2015
Prime Performance Manager Unit Hostname     : ems-lnx408
Prime Performance Manager Unit SSL Support  : Installed [Disabled]
Prime Performance Manager Unit Gateway Name : ems-lnx408
================================================================================
   sgmMsgLogServer:    1.7.0.000   Tue Jul 28 15:59 EST 2015
   sgmDataServer:      1.7.0.000   Tue Jul 28 15:59 EST 2015
================================================================================
Current Time: 2015/12/12 14:50:15 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 Logging In as the Root User, page 2-1.

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

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

The gateway version details are displayed, for example:

The gateway status is displayed, for example:

```
================================================================================
Prime Performance Manager Unit Version      : 1.7.0.000
Prime Performance Manager Unit Build        : Tue Jul 28 16:02 EST 2015
Prime Performance Manager Unit Install      : Tue Jul 28 16:25 EST 2015
Prime Performance Manager Unit Hostname     : ems-lnx408
Prime Performance Manager Unit SSL Support  : Installed [Disabled]
Prime Performance Manager Unit Gateway Name : ems-lnx408
================================================================================
   sgmMsgLogServer:    1.7.0.000   Tue Jul 28 15:59 EST 2015
   sgmDataServer:      1.7.0.000   Tue Jul 28 15:59 EST 2015
================================================================================
Current Time: 2015/12/12 14:50:15 EST
```

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

```
================================================================================
Prime Performance Manager Unit Version:      1.7.0.000
Prime Performance Manager Unit Build        : Tue Jul 28 16:02 EST 2015
Prime Performance Manager Unit Install      : Tue Jul 28 16:25 EST 2015
Prime Performance Manager Unit Hostname     : ems-lnx408
Prime Performance Manager Unit SSL Support  : Installed [Disabled]
Prime Performance Manager Unit Gateway Name : ems-lnx408
================================================================================
   sgmMsgLogServer:    1.7.0.000   Tue Jul 28 15:59 EST 2015
   sgmDataServer:      1.7.0.000   Tue Jul 28 15:59 EST 2015
================================================================================
Current Time: 2015/12/12 14:50:15 EST
```

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

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

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

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

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

```
================================================================================
Prime Performance Manager Unit Version:      1.7.0.000
Prime Performance Manager Unit Build        : Tue Jul 28 16:02 EST 2015
Prime Performance Manager Unit Install      : Tue Jul 28 16:25 EST 2015
Prime Performance Manager Unit Hostname     : ems-lnx408
Prime Performance Manager Unit SSL Support  : Installed [Disabled]
Prime Performance Manager Unit Gateway Name : ems-lnx408
================================================================================
   sgmMsgLogServer:    1.7.0.000   Tue Jul 28 15:59 EST 2015
   sgmDataServer:      1.7.0.000   Tue Jul 28 15:59 EST 2015
================================================================================
```

```
Current Time: 2015/12/12 14:50:15 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-48.

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 2-5.

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

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

- Microsoft Internet Explorer 9.0, 10.0, and 11.0 (Windows).

Note Microsoft Internet Explorer 8.0 is not supported. Later IE versions have not been formally tested, but should work in most cases.

- Mozilla Firefox 24 or later up to Firefox 32 (Linux and Windows).
- Mozilla Firefox 24 Extended Support Release (ESR) or later up to Firefox 28 (Linux and Windows).

Note Later Firefox versions have not been formally tested, but should work in most cases.

- Safari and Chrome—Not formally tested but widely used.

Other requirements:

- The minimum screen resolution should be set to 1280 x 1024.

- The hostname configured on Prime Performance Manager gateway must be resolvable to an IP address on the client machine using DNS or local hosts file.

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 SSL is enabled, use https instead of http. For information, see Enabling SSL on Gateways and Units, page 6-2 and ppm ssl, page B-99.

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. 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 Creating Messages of the Day, page 6-25.

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 3-1). 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 7-39.

The GUI window is comprised of the following elements:

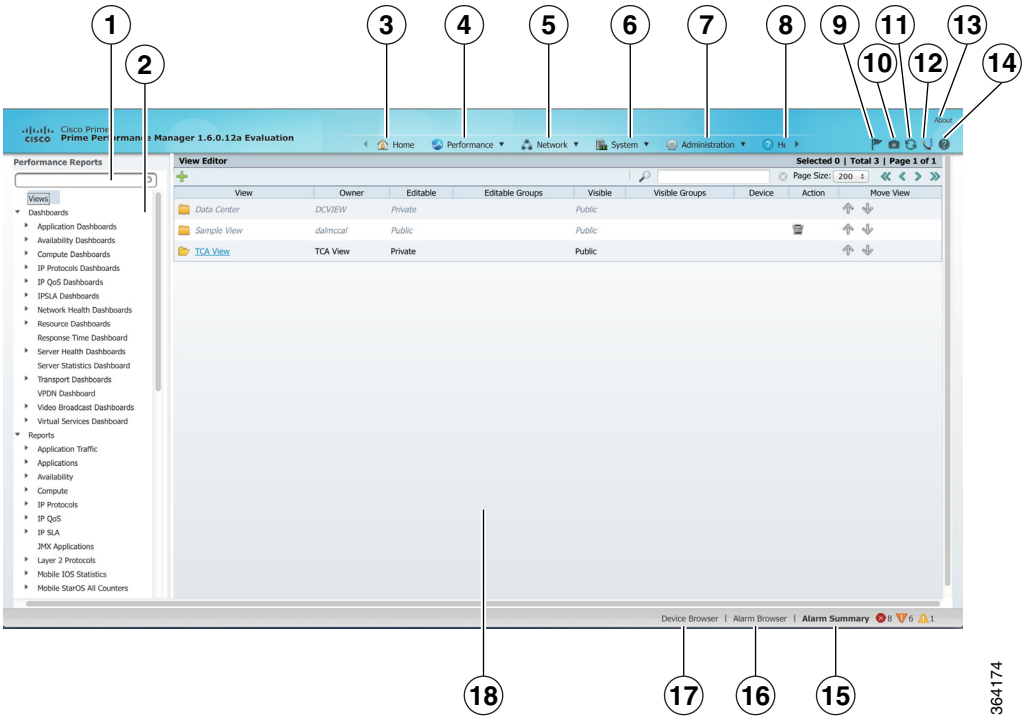
- Main menus—Prime Performance Manager provides six main menus that appear in all windows: Home, Performance, Network, System, Administration, and Help. Submenus displayed from each main menu are described in Table 3-1.

  Note The System and Administration menus are only displayed for Administrator users.

- Toolbar options—Standard toolbar options include:
  - Getting Started—Displayed for Administrator users, the popup window provides links to administration, network, and reports areas. The Quick Start appears at startup, but can be turned off by checking **Do not show this on startup**. Getting Started can be displayed at any time by clicking the flag tool.
  - User Preferences—Allows users to customize Prime Performance Manager display. For information, see Customizing the GUI and Information Display, page 3-8.
  - Refresh—Refreshes the currently-displayed window.
  - Send Announcement—Allows you to send messsages to online users. For information, see Sending Announcements to Online Users, page 6-25.
  - Page Help—Displays the online help topic for the currently-displayed window.
- Navigation area—The navigation area is displayed in some, but not all, Prime Performance Manager windows. 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 Device Properties at the Network Level, page 9-3.
  - 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 10-7.
  - 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 Customizing the GUI and Information Display, page 3-8.

  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 Customizing the GUI and Information Display, page 3-8.

Figure 3-1 Prime Performance Manager Window



1	Performance Reports search field	**10**	User Preferences
2	Performance Reports navigation area	**11**	Refresh tool
3	Home	**12**	Send announcements
4	Performance menu	**13**	Information about Prime Performance Manager
5	Network menu	**14**	Context help tool
6	System menu	**15**	Alarm Summary
7	Administration menu	**16**	Alarm Browser
8	Help menu	**17**	Device Browser
9	Getting Started	**18**	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 7-44
Performance	Views	Creating and Managing Custom Report Views, page 7-39
	Dashboards	Managing Dashboards, page 7-36
	Reports	Displaying Reports, page 7-1

Table 3-1 Navigation Menus (continued)

Menu	Submenu	For information, see...
Network	*Network Overview*	
	Devices	Chapter 9, "Managing Devices"
	Tenants	Importing Tenants into Prime Performance Manager, page 8-5
	Alarms/Events	Chapter 10, "Managing Network Alarms and Events"
	Network Administration	
	SNMP Editor	Adding SNMP Device Credentials, page 5-3
	Polling Group Editor	Creating and Editing Device Polling Groups, page 9-35
	Credentials Editor	Adding Device Credentials for Other Protocols, page 5-6
	Threshold Editor	Managing Thresholds, page 11-12
	Report Mail Editor	Emailing Reports, page 7-20
	Discovery	Chapter 5, "Discovering Devices With Prime Performance Manager"
	Web Report Editor	Creating Web Reports, page 7-57
	Probe Editor	Creating Probes, page 9-37
System	*System Information*	
	Gateway/Units	Chapter 13, "Managing Gateways and Units"
	Status	System Properties, Statuses, Logs, and Messages Overview, page 12-1
	Logs	Displaying System Logs, page 12-4
	Messages	Displaying System Information Messages, page 12-13
	Security Messages	
	User Actions	Displaying User Actions, page 12-14
Administration	*System Administration*	
	Prime Central Integration	Chapter 4, "Importing Devices From Other Cisco Prime Applications"
	Prime Network Integration	Importing Devices From Prime Network, page 4-6
	Prime Network Services Controller Integration	Prime Network Services Controller Integration Overview, page 4-9
	OpenStack Tenant Integration	Importing Tenants into Prime Performance Manager, page 8-5
	Users/Tenants/Security	Chapter 6, "Managing Users and Security"
	Unit Editor	Managing Device-to-Unit Assignments, page 13-5
	Alarms/Events Editor	Configuring Upstream Alarm Hosts and Tuning Event and Alarm Parameters, page 10-14
	Group Editor	Managing Report Groups, page 7-55
	System Settings	Displaying System Properties and Settings, page 12-8

Table 3-1 Navigation Menus (continued)

Menu	Submenu	For information, see...
	Reports Administration	
	Report Settings	Displaying Reports Settings, page 12-11
	Report Status	Customizing Individual Report Settings, page 7-27
	Report Custom Aging	Customizing Individual Report Aging Settings, page 7-30
	Report Policies	Creating Report Policies, page 7-33
	NB Push Editor	Pushing Prime Performance Manager Data to Other Applications, page 17-1

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:

- Prime Performance Manager Help—Displays the Prime Performance Manager online help. The online help is based on the *Cisco 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 1.7 release.
  - Devices Info—Displays a list of devices that have been used with Prime Performance Manager by customers and in labs.
  - Collectors Info—Provides a list of supported data collectors.
  - 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:
  - Reports XML Definitions—Provides the XML, properties, and notes for Prime Performance Manager reports.
  - 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.

  - 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.
  - Threshold API Parameters—Threshold API parameters for REST report users who want to create TCAs based on REST report data. Each report (including dashboard reports) includes the reportKey and kpiReport threshold parameters. The following metadata is added for each column: dataType plus the threshold parameters, columnName and kpiName. (The last two are empty for non-thresholdable columns.) You can also run a script on specific files and folders to generate a list of API parameters and thresholdable columns. For information, see the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*,
  - REST API Documentation—Displays REST API methods that can be used to retrieve Prime Performance Manager reports.
- 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 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.

Screen Information

- 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.

System Information

Includes Dojo and XWT Version. This internal data is used by Cisco TAC for customer support.

Customizing the GUI and Information Display

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. These options help you tailor the GUI to your individual needs and preferences.

User preferences apply only to the individual user. However, user preferences can be saved to the Prime Performance Manager gateway and made available for use by any user. How user preferences 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 customize the Prime Performance Manager GUI and information display:

Step 1 On the right side of the main menu bar, click **User 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, user preferences are accessed through the Device Display, General Display, Graph Color, Report, Utilization Color, and Graph tabs described in the following sections:

- Device Display Preferences, page 3-8
- General Display Preferences, page 3-9
- Graph Color Preferences, page 3-11
- Report Preferences, page 3-11
- Utilization Color Preferences, page 3-13
- Graph Preferences, page 3-14
- Load/Save Preferences, page 3-15

Device Display Preferences

Indicates how devices are identified in the Prime Performance Manager GUI:

- 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 synchronization name.
- Show Business Tag—For devices imported from Prime Network, identifies devices by their 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.
- Show Device Domain Names—If checked, displays the device domain names. 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, Time Zone, and Location, page 9-16),
  - 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.
- 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.
- Device History Limit—Sets the number of devices displayed in the Network Devices window (Network > Devices > Device Summary). The default is 20. The range is 5 to 100.
- Details Displayed on Device Links—Sets the information that appears when you move your mouse over device links.
  - **None** turns off this feature.
  - **Mouse Hover Details Popup** displays device information as a popup when you move your cursor over the device link.
  - **Mouse Click 360 Device View** displays the 360 Network Device View window. This window includes detailed device information including alarms, events, availability, collector status, and polling information. For information on the 360 Network Device View window, see Displaying the 360 Device Details View, page 9-23.

General Display Preferences

- Optimize GUI for Slow Connections—If you are using a low-speed connection, for example, a dial-up modem or long-distance VPN connection, this option enhances performance by turning off the row index count 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.

- 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 Global Toolbar—If checked (default) displays the global toolbar.
- Show Icons With Labels—If checked, shows icons with labels.
- Color Highlight TCAs—If checked (default), color highlights TCAs in reports.
- Compact Graph Mode as Default—If checked, sets Compact (Graph) Mode as the default for all reports. When Output is set to Graph, toggles the display of the Zoom, Aggregate Lines, Graph Styles, and Export Graphs tools displayed inside graphs. Additionally, the graph border is hidden and graph title reduced in size. This option reduces the overall size of the graph and is useful when screen real estate is needed. This option is not enabled by default. Users can enable it for individual reports using the Toggle Compact Mode option on the report toolbar. If this preference is enabled, all reports are displayed in compact mode; users can disable it for individual reports.
- Default Number of Views Per View Level—Sets the default number of views per view level. 10 is the default.
- Status Page Refresh Interval (secs)—Specifies how frequently Prime Performance Manager status pages are refreshed. Status pages include tabs displayed from the Network menu > Devices, Tenants, and Alarms/Events items, as the System menu > Gateways/Units. It does not affect the reports, views, and dashboards display. 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.
- Maximum Number of Views Per View Level—Sets the maximum number of views per view level. For information about the default and maximum view entries, see Managing Large Numbers of Views, page 7-51.
- Date Format—Allows you to customize the date format displayed in the Prime Performance Manager GUI. The following is accepted:
  - Month: m, M, mm, MM, mmm, MMM, mmmm, MMMM (for example 6, 06, Jun, June)
  - Day: d or dd (for example, 5 or 05)
  - Year: yy or yyyy (for example, 14 or 2014)
  - Upper and lower case are accepted. You can use a slash (/), dot (.), dash (-), or space as separators.
- View Autoplay Interval (secs)—Sets the autoplay view delay in seconds. (20 seconds is the default.) This parameter is used for the view autoplay feature, which scrolls through custom views automatically. For information, see Modifying Custom Report Views, page 7-44.
- View Autoplay Style—Sets the autoplay style for views, either Inline or Full Screen.
- User Work Shift—Sets the work shift start and end times. Work shift is a report, dashboard, and view interval option that allows you to see report data for a work shift time period. If the work shift is 9:00 AM to 5:00 PM and the time you run the report is within the work shift, for example, 10:30 AM, the time since the beginning of the work shift is used (9:00 –10:30AM today). If the current time is outside the work shift (say 8:00 AM or 6:07 PM), yesterday's work shift is used (9:00 – 5:00 yesterday).
- Tenant Setting—If Prime Performance Manager is integrated with OpenStack tenants sets the tenant scope:
- Tenant Scope—Sets the report tenant scope:
  - All—Displays all reports, not just tenant reports.
  - All Tenants—Displays all tenant reports.

  - SELECTED—Allows you to select and display reports for individual tenants.
- Tenant Display—Sets the tenant identifier when displayed in reports:
  - Name (internal tenant name)
  - Display Name

  For information about managing multi-tenancy in Prime Performance Manager, see Chapter 16, "Managing Multi-Tenant Services."

Graph Color Preferences

Allows you to edit the colors used in report and group graphs, as well as:

- Graph data
- Plot area
- Background color
- Border color
- Legend color
- Title color
- Date text color

Fifty colors are available. To edit a color, you can edit the color hex # directly in the color sample, or click the Color Picker to the right 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 any of the three 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**.

- Use Bold Fonts in Graph Text—Displays all graph text in bold. This is enabled by default. Uncheck this box if you do not want chart text displayed in bold.

Report Preferences

- Show Values in Graphs and Summary Tables—Provides options to display, or not display, report values in graphs and summary tables. Values include:
  - Min—The report minimum value,
  - Min Date—The date the report minimum value was reached,
  - Avg—The average report value,

Note If the Avg value is enabled, an Average [*data value*] As% is displayed for certain reports, for example NetFlow reports. Average As% is the percentage of the total of all data averages for all data series. In other words, add all the averages for all data series and then divide the average for this specific data series by the sum of all averages for all data series. For example, if the report shows the input for multiple interfaces, this value shows how the average of one interface compares to the average of the others.

- Max—The report maximum value,
- Max Date—The date the report maximum value was reached,
- Total—The total of all data points for that line item. For example, in an hourly report with 5-minute polling, Total represents the sum of 12 data points.

Note Total is only meaningful if the data series is a numeric.

- Std Dev—Is the standard deviation for that data series, that is, a measurement of how spread out the data series values are. A low value indicates that the data points tend to be very close to the mean; a high value indicates that the data points are spread out over a large range of values. Standard deviation is the square root of the variance.
- Variance— Is the data series variance, that is, the mean of the squares of individual differences from the mean of the data series.
- Current—The current report value.

Min Date, Avg, Max, and Max Date are enabled by default.

- Show TCAs in Graphs—Options to show or hide critical, major, minor, or normal TCAs in report graphs. All alarm levels are checked by default.
- 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 Customizing Individual Report Settings.
- Hide Empty Reports—If checked, reports that do not provide any data are not displayed.
- 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.
- Always Display All Report Data Intervals—If enabled, displays all intervals in the device-level report Duration menu even if the intervals are disabled at the network or device levels. This allows you to see report data for intervals that might exist in the past but are currently disabled, or to see TCA data for a time period that is disabled at the device or network levels. Device-level report durations include: 5 minute, 15 minute, hourly, daily, weekly, monthly.
- 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.

- 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.
- 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.
- Maximize Graph Data (Hide Inputs)—Hides the display of the Zoom, Aggregate Lines, Graph Styles, and Export Graphs tools displayed inside charts. Additionally, the chart border is hidden and chart title reduced in size. Enabling this option reduces the overall chart size and increases screen real estate. You can toggle chart decorations and styling at the individual chart level.
- Export All CSV Data With Report Export—Exports all CSV data with report exports.
- Show Intervals On Report Menus—If selected, report intervals are displayed in the report navigation tree. By default, intervals are selected separately on the report menu bar and not displayed on the report navigation tree.
- CSV File Name Date Format—Sets the date format used in CSV file names, either yyyy-MM-dd-HH-mm-ss (year-month-day-hour-minute-second) or MM-dd-yyyy-HH-mm-ss (month-day-year-hour-minute-second).
- Show Live Mode Report Data For—Allows you to change the amount of data available for Go Live reports: Last Hour (default), Last 12 Hours, Last Day, Last 3 Days. Go Live reports display data every 15 seconds. For more information, see Displaying Network and Device Reports, page 7-10.
- 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 1.7 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 3-17.
- Set Top Number For NetFlow Reports—Specifies the top number of NetFlow reports displayed. This number cannot be higher than the number specified in the Maximum Entries for Top XX Output in NetFlow Reports specified on the System Configuration tab. The default is 10. For information about system configuration parameters, see Changing System Configuration Settings, page 3-17.
- Bytes in Megabyte—Sets the bytes multiplier used to calculate megabytes: 1000 or 1024. If set to 1024 (default), volume is represented with two-letter acronyms: MB, GB, TB. If set to 1000, volume is represented with one letter: M, G, T. For example, if set to 1024, 42.75 megabytes is shown as 42.75MB. If set to 1000, 42.75MB becomes 44.82M.

Utilization Color Preferences

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/Utilization Metrics
  - Green—00.00 > 50.00
  - Gold—50.01 > 70.00

  - Orange—70.01 > 90.99
  - Red—91.00 > 100.00
- Descending/Utilization Metrics
  - Green—100.00 > 99.91
  - Gold—99.90 > 99.51
  - Orange—99.50 > 99.01
  - Red—99.00 > 00.00
- Enabled Colors—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.

Graph Preferences

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 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 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.
- Max Graphs Per Report (One Graph/Series Mode)—Allows you to set the maximum number of graphs that will appear in a report.

- Margins—Allows you to set the width of the graph margin: No Margins, Narrow Margins, or Wide Margins.

Load/Save Preferences

Allows you to save user preferences to the Prime Performance Manager gateway where they can be loaded by other users. See Saving and Loading User Preferences, page 3-15.

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

Step 4 To view the new preferences, 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.

Saving and Loading User Preferences

After modifying user preferences, you can save them to the Prime Performance Manager gateway where they can be loaded by other Prime Performance Manager users.

To save your modified 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, click **Load/Save**.

Step 3 In the Load/Save Preferences window, click **Save Current Preferences to Gateway**.

Step 4 In the Save User Preferences to Gateway dialog box, choose the preference groups you want to save:

- Device Display
- General Display
- Graph Color
- Reports
- Utilization Color
- Graph

Step 5 Enter a file name. File names can be any alphanumeric character including spaces, underscores, and hyphens. Special characters are not allowed.

Step 6 Click **OK**.

The file is displayed in Load/Save Preferences table.

Note Saved user preferences cannot be edited or deleted.

To load a saved user preferences file:

Step 1 On the right side of the main menu bar, click **Preferences**.

Step 2 In the User Preferences window, click **Load/Save**.

Step 3 In the list of preferences, select the preference file you want to load, then click **Load Selected Preferences**.

The new preferences are loaded and will take effect immediately.

Customizing GUI Page Sizes

Information in the Prime Performance Manager GUI is generally presented in tables, including summary tables, report tables, and editors. You can customize the number of table entries using the Page Size field. This field is located in the toolbar of every page allowing customization.

Prime Performance Manager retains your entry for each table. For example, you can set the page size for the Devices window to 400 if you prefer to see all device data at one time, and set the page size for SNMP Editor to 25, if you want that screen to load quickly instead of seeing a large volume of data at once.

Page size values are maintained across user sessions.

Table 3-2 shows the Prime Performance Manager windows where you can adjust the page size.

Note The Page Size field maximum is controlled by the Maximum Rows for Table Pages in the Administration Configuration Settings window. For information, see Changing System Configuration Settings, page 3-17.

Table 3-2 Windows Affected by the Page Size Preference

Area or Menu	Submenu or Window	Page
Views	Subview	—
	Event History	—
	Active Alarms	—
Dashboards	—	—
Reports (Table output mode)	—	—
Grouped Reports (Table output mode)	—	—

Table 3-2 Windows Affected by the Page Size Preference (continued)

Area or Menu	Submenu or Window	Page
Network	Devices	Devices
		Types
		Alarms By Device
		Alarms By Device Type
		Unreachable
		NetFlow
		Polling
		Ping
		Uptime
		Data Collection
		Software
		Contact/Location
		Vendor
		Prime
	Tenants	—
	Alarms/Events	Alarms
		Events
		Daily Archives
		Alarms By Device
		Alarms By Device Type
	SNMP Editor	—
	Polling Group Editor	—
	Credential Editor	—
	Threshold Editor	—
System	Gateway/Units	—
Administration	Groups Editor	—

Changing System Configuration Settings

In addition to user preferences (see Customizing the GUI and Information Display, page 3-8), 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, HTML page and table sizes, as well as database backup preferences. 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 configuration settings, as needed:

System Configuration Settings

- Display Device Location in Google Maps—If enabled, converts the provisioned device location into a Google Maps hyperlink. The hyperlink is displayed in the device Location property. When selected, Google Maps displays the device location in a separate browser session. This property is disabled by default.

  Note Prime Performance Manager displays the location that is provisioned on the device unless you edit the location in Prime Performance Manager. (For information, see Editing a Device Name, Web Port, Time Zone, and Location, page 9-16.) If you enable this feature, verify that enough location information is entered for the device to display its location accurately in Google Maps. Location abbreviations or notations might not display the device location accurately.

- Default Map Zoom Level—Sets the default Google Maps zoom level, 0 (global view) to 21+ (street level view). The default zoom value is 13.
- TCA Warning Severity—If enabled, TCA alarms are generated when the warning threshold is reached.
- TCA Informational Severity—If enabled, TCA alarms are generated when the information threshold is reached.
- 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 (Shut Down) 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-32.

- 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-62.
- 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 tomcatver, page B-114.

  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 Customizing the GUI and Information Display, page 3-8.

- Maximum Entries for Top XX Output Specifically for NetFlow—Sets the maximum number of entries in NetFlow Top XX reports. 10 is the default. The range is 5-20. You can also set the maximum using the ppm topxxsizenetflow command. For information, see ppm topxxsizenetflow, page B-115.
- Maximum Rows for Table Pages—Sets the maximum browser page size for Prime Performance Manager tables. Effectively, this sets the maximum users can select from the Page Size field. The default value 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-56. For more infomation, see Customizing GUI Page Sizes, page 3-16.
- 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-56.
- Interface Name Format—Defines the format for displaying interface names in the Prime Performance Manager GUI:
  - Description—The interface description is displayed.
  - Alias—The interface alias is displayed.
  - Both—(default) 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-45.
- SMTP Mail Server—Sets the SMTP mail server for report emails.
- Global Email From Address—Sets an email address to populate the Email From Address fields for emailed reports, alarms, and thresholds. For information, see Emailing Reports, page 7-20.

System Polling Threads

Displays the number of slow and fast polling threads, and the interval between the slow and fast threads. Polling threads prevent slow polling devices from blocking the processing of fast polling devices. The fast interval determines the thread a device is assigned to based on how long it took to poll all report data for the device. If polling time is less time than the fast interval, the device is assigned to the fast polling thread. If not, it is assigned to the slow polling thread.

The fast interval might need tuning if the average poll time for the majority of devices is greater than the 15-second default. The number of threads assigned to each pool might need tuning if it takes longer to process all devices than the lowest enabled report interval. Polling threads and intervals can be modified using the following commands:

- ppm numfastthreads, page B-65
- ppm numslowthreads, page B-66
- ppm fastinterval, page B-39

Note Polling thread and interval modification should only occur at the direction of Cisco support.

System Backup Settings

- Database Backups—Enables or disables database backups. This preference is enabled by default.
- Reports Backups—Enables of disables report backups. This preference is disabled by default.
- Backup Logs—Enables of disables log backups. This preference is disabled by default.

- Zip Old Backups—If enabled, zips old backups instead of deleting them. This preference is disabled by default.
- Number of Days to Save Backup Files—Configures the number of days to save old backups. The default is 1. The range is 1 to 365 days.
- Minimum Free Disk Space to Attempt Backups—Sets the amount of disk space, in megabytes, that must be free before a backup is attempted. The default is 300 megabytes. The range is 1 to 1000 megabytes.
- Backup Directory—Allows you to specify the directory into which backups will be placed. The default is /opt/.
- Backup/Restore Script—Allows you to run a script before and after a backup or restore is completed. Enter the path and script file name.
- Backup/Restore Email ID list—Allows you to enter a list of email addresses to which emails are sent after a backup or restore occurs. The email includes the backup or restore statistics.

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.

Adding and Removing Properties from Property Views

Prime Performance Manager displays many properties and attributes in tables, including Devices, Alarms by Device, Unreachable Alarms, and many 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.

Note Changes to displayed table properties will persist from user session to user session.

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 Customizing the GUI and Information Display, page 3-8.

Displaying Prime Performance Manager Information

To display information about Prime Performance Manager, click **About** at the top right corner of the Prime Performance Manager window. Displayed information includes:

- License Type—The Prime Performance Manager license type. For Evaluation licenses, the number of days remaining is shown.
- Build Date—The Prime Performance Manager build date.
- Build Version, Patch Level—The build version and patch level. For example, 1.7.0.6, 0 indicates a 1.7 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.
- Open Source Information—Displays the Open Source Used in Prime Performance Manager 1.7.0 document describing open source products used in the release.

Changing the Prime Performance Manager Corporate Branding

Prime Performance Manager allows you to replace the Cisco corporate branding presented in the GUI, with your corporate branding including your company name, logo, and background. Your users will see this brand in the header page of all Prime Performance Manager GUI pages as well as in any email reports.

Changing the corporate branding requires:

- Root access to the Prime Performance Manager gateway.
- A gateway restart.

To customize the Prime Performance Manager corporate branding:

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

Step 2 Navigate to the gateway properties directory:

```
cd /opt/CSCOppm-gw/properties
```

Step 3 Open Branding.properties with a text editor and modify the following entries using the format, [*propertyname=propertyvalue*]:

- enabled—Set to true to turn on the custom branding; set to false (default) to return to the default Cisco branding.
- productFamily—Defines the first header line in the Prime Performance Manager GUI.
- applicationTitle—Defines the second header line, Prime Performance Manager displays its title, version, and indicates whether you have an evaluation license.
- productLogoClickUrl—Defines the website that is displayed when a user clicks on the company logo.
- productLogo—Defines the image file used for your company logo. Copy the image entered here to the images directory where you installed Prime Performance Manager. By default this is located at
- /opt/CSCOppm-gw/images
- backgroundImage—Defines the background image shown in the top title area. Copy the image entered here to the images directory where you installed Prime Performance Manager.
- *productHelp*—Allows you to optionally provide help documentation to your users. Copy the help file to the help subdirectory where you installed Prime Performance Manager. By default this is located at:

  ```
  /opt/CSCOppm-gw/apache/share/htdocs/help
  ```

- retainCiscoHelp—Indicates whether or not Cisco online help links are retained after you define custom online help. The default is false. Only the custom help link is displayed. If you set to true, both the Cisco online help links and your custom help links are displayed,

Step 4 After you modify and save the Branding.properties file and copy any custom image files to the gateway images directory, restart the gateway. (See Restarting Gateways and Units, page 2-5.)

Your custom branding will appear at the first login.

Importing Devices From Other Cisco Prime Applications

You can import devices into Prime Performance Manager by integrating it with other Cisco Prime products including Cisco Prime Central (Prime Central), Cisco Prime Network (Prime Network), and Cisco Prime Network Services Controller (Prime Network Services Controller). Integration and device import procedures are provided in the following topics:

Prime Central Integration Overview

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
- Dynamic inventory updates: when Prime Central receives physical device change notifications from domain managers, it sends notifications to all subscribing domain managers, including Prime Performance Manager, so the Prime Performance Manager device inventory is kept synchronized with the Prime Central inventory.

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

- Running the Prime Central integration (required)
- Creating users (required)

- Importing trap destinations (optional)

Procedures are provided in the following topics:

- Integrating Prime Performance Manager with Prime Central, page 4-2
- 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.

After you integrate Prime Performance Manager with Prime Central, the following Prime Performance Manager changes occur:

- Users and user logins—Prime Performance Manager users are removed. All logins and user management operations are performed in 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 1.4 User Guide*. Should you decide to remove Prime Performance Manager integration with Prime Central, SSL and user access are disabled. To enable users, see Setting Up User Access and Security, page 6-1.
- Alarm management—The following alarm actions are available and synchronized between Prime Performance Manager and Prime Central:
  - Acknowledge/Unacknowledge
  - Clear
  - Delete
  - Clear/Delete
  - Change Severity

  Assign Owner is not available, however.

Note You can only integrate one Prime Performance Manager gateway with Prime Central.

Step 1 Log in as the root user or user enabled with ppm superuser. (See Logging In as the Root User, page 2-1.)

Step 2 Start Prime Performance Manager. (See Starting Gateways and Units, page 2-2.)

Step 3 Launch the Prime Central integration from one of the following:

- GUI—From the Administration menu, choose **Prime Central Integration**.
- CLI—Enter the following command:

```
ppm primecentralintegration
```

Step 4 In the Prime Central Integration window, or at the command prompts, enter the Prime Central server information:

- Database Host—Enter the Prime Central database hostname or IP address.
- Database Port—Enter the Prime Central database port number. The default port, 1521, is recommended.
- Database User—(HA only) Enter the Prime Central database username, which is primedba by default.
- Database Password—(HA only) Enter the Prime Central database user password.
- Database SID—Enter the Prime Central database service name, which is primedb by default.
- Enable Default Reports—Check (or enter **y**) if you want the default reports enabled following the integration.

Step 5 Perform one of the following:

- GUI—Click the **Submit Prime Central Integration** 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.
- CLI—Press **Enter**.

Step 6 Restart the Prime Performance Manager gateway and unit(s). For information, see Restarting Gateways and Units, page 2-5.

Step 7 Log into the Prime Central server and stop the Prime Central Integration Layer:

```
itgctl stop
```

Step 8 Wait two minutes, then start the Prime Central integration layer:

```
itgctl start
```

Step 9 If you want to run Prime Performance Manager as a non-root user:

```
ppm superuser nonRootUser
```

Step 10 Verify the integration,

a. Log into Prime Central. (For Prime Central login procedures, see the *Cisco Prime Central 1.4 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 11 If remote units are connected to the gateway, complete the "Enabling SSL on Remote Units" procedure on page 6-4 to enable SSL on the remote units.

Step 12 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 1.4 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 6-15.

In the Administration Prime Central Integration window, the Submit Prime Central Integration tool changes to Import inventory after Prime Performance Manager is integrated with Prime Central. The inventory is imported about fifteen minutes after you complete the integration and restart Prime Performance Manager. You can update the inventory after the Prime Central Integration Layer is restarted.

Note If you try to import the inventory while the Prime Central Integration Layer is down, the import will fail.

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 Logging In as the Root User, 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 **Remove**. 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 4-2, 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 2-5.
	2. Check the Prime Performance Manager operational status. See the "Displaying Gateway and Unit Status" procedure on page 2-7.
	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 1.4 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 2-7. All services should be running. 2. If not, restart the gateway. See the "Displaying Gateway and Unit Status" procedure on page 2-7. 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 1.4 User Guide* for login and user management procedures, as well as general information about using Prime Performance Manager in the Cisco Prime Carrier Management 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, from selected devices and interfaces in the Prime Central inventory view, and from selected alarms in the Fault Management window.

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

Table 4-2 Post Integration Commands and Procedures

Task	Command or Procedure
Remove Prime Performance Manager from the Prime Central Suite Monitoring table and return it to standalone domain manager.	ppm primecentralintegration remove **Note** The command switches Prime Performance Manager from suite to standalone mode. You must remove Prime Performance Manager from the Prime Central Suite Monitoring table manually using the Prime Central GUI.
Change Prime Performance Manager trap destination from Prime Fault Management to Prime Network.	ppm setpctrapdestination See ppm setpctrapdestination, page B-88, for command options.
Update the device inventory from Prime Central. The inventory is automatically imported several minutes after integration, if the Integration Layer is running.	Using the GUI: 1. From the Administration menu, choose **Prime Central Integration**. 2. From the Prime Central Integration toolbar, choose **Import Inventory**. **Note** The Prime Central Integration Layer must be running. If not, the import will fail. Using the CLI: ppm inventoryimport command. See ppm inventoryimport, page B-47, for command options.
Adds cross-launch capability to Cisco Prime Network. Cross launches are automatically installed in each Prime Network instance registered with Prime Central.	ppm crosslaunch See ppm crosslaunch, page B-25, for command options.

Importing Devices From Prime Network

To integrate Prime Performance Manager with Prime Network you generally integrate with Cisco Prime Central, the Cisco Carrier Management parent application. However, you can integrate Prime Performance Manager with Cisco Prime Network separately. To import a Prime Network device inventory, Prime Performance Manager connects to the Prime Network gateway and retrieves the Prime Network device IP addresses and the following device credentials:

- SNMP
- Telnet
- SSHv1
- SSHv2
- HTTP

- HTTPs
- VCENTER_HTTPs

If the Prime Network device has multiple credentials, for example, SNMP credentials and Telnet and HTTP credentials, those credentials are downloaded. Prime Network devices are retrieved except devices whose Prime Network VNEs:

- Are in Maintenance investigation state.
- Are ICMP or cloud VNEs.
- Have a down admin status.

Note Prime Performance Manager can integrate with Prime Network 4.1, 4.0, 3.11, and 3.10.

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 credential 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.

Device Integration Notes

If you are importing Cisco Carrier Packet Transport (CPT) devices, Prime Performance Manager considers every CPT Packet Transport Fabric (PTF) card as a separate device. Prime Performance Manager synchronizes the device status of the CPT and PTF devices according to the CPT device status changes received from Prime Network.

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. (For information on importing Prime Network devices using the CLI, see ppm inventoryimport, page B-47.) This procedure requires a Level 5 (administrator) user level.

Note If the Prime Network gateway to which you are integrating Prime Performance Manager is in a high availability (HA) configuration, complete the following steps whenever a Prime Network gateway HA switchover occurs. Prime Performance Manager does not automatically switch to the new active Prime Network gateway.

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 (Admin User Level)—Enter the Prime Network gateway administrator or configurator username. This user must have an assigned scope of All Managed Elements.
- 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.
- Automatically Remove Devices From PPM When Removed From Prime Network—If checked, Prime Network devices are automatically removed from Prime Performance Manager when they are removed from Prime Network. If not checked, devices removed from Prime Network are retained in Prime Performance Manager but changed to an unmanaged state.

Step 4 From the Prime Network Integration toolbar, click the **Prime Network Integration Setup** 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 Device Properties at the Network Level, page 9-3.**

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.

Updating the Prime Network Device Inventory

Complete the following steps to update the Prime Network device inventory after you complete the Importing Devices From Prime Network, page 4-6.

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 Administration Prime Network Integration window, choose **Import Inventory** on the toolbar.

The device inventory is updated.

Note Should Prime Network VNE IP addresses change from the first discovery to the next, Prime Performance Manager will update the device IP address with no loss of report information.

Prime Network Services Controller Integration Overview

Prime Network Services Controller is the management application for Cisco Nexus 1000V (Nexus 1000V) switches and services that can enable transparent, scalable, and automation-centric network management for virtual data center and hybrid cloud environments. Nexus 1000V switches and services deliver a highly secure multitenant environment by adding virtual intelligence to the data center network. The virtual switches are built to scale for cloud networks. Virtual Extensible LAN (VXLAN) support enables scalable LAN segmentation and virtual machine (VM) mobility.

Prime Network Services Controller allows administrators to manage Cisco virtual services through its GUI or XML API. Its model-centric architecture provides a flexible mechanism for provisioning and securing virtual infrastructure using Cisco Virtual Security Gateway (Cisco VSG) and Cisco Adaptive Security Appliance 1000V (ASA 1000V) Cloud Firewall virtual security services.

General integration flow:

- Initiation—Prime Performance Manager initiates integration with Prime Network Services Controller. It sends the Prime Performance Manager information (IP address) to Prime Network Services Controller through the Prime Network Services Controller API.
- One-to-one integration—One Prime Performance Manager gateway is connected to one Prime Network Services Controller gateway.
- Integration removal—To remove the Prime Network Services Controller integration, you must remove from both the Prime Performance Manager and Prime Network Services Controller GUIs.

Integrating Prime Performance Manager with Prime Network Services Controller provides the following capabilities:

- System level cross launch—Prime Performance Manager can be launched from Prime Network Services Controller. This capability is largely for administrators to access Prime Performance Manager to manage devices and users, and to set up performance reporting configurations such as thresholds. The cross-launch process steps include:
  - Prime Performance Manager initiates integration with Prime Network Services Controller. It sends the Prime Performance Manager information (IP address) to Prime Network Services Controller through the Prime Network Services Controller API.
  - A Prime Performance Manager cross launch menu item is added to the Prime Network Services Controller dashboard.
  - One-to-one integration—One Prime Performance Manager gateway is connected to one Prime Network Services Controller gateway.
  - Integration removal—To remove the Prime Network Services Controller integration, you must remove from both the Prime Performance Manager and Prime Network Services Controller GUIs.
- Device level cross launch—Prime Network Services Controller users can launch Prime Performance Manager reports from Prime Network Services Controller devices. Prime Performance Manager supports vDevices managed by Prime Network Services Controller in the private cloud. It gets

device IP addresses or hostnames from Prime Network Services Controller through its North Bound API (NBAPI in XML). Prime Performance Manager uses the default account for device cross launch. No user information is needed for a device cross launch. Prime Performance Manager is launched as a separate application.

- Device import—Prime Network Services Controller devices are imported into Prime Performance Manager in an unmanaged state. You must add the Prime Network Services Controller credentials to Prime Performance Manager, then change the device state to managed. Additional notes:
  - Prime Performance Manager needs an IP or hostname and login credentials to access devices.
  - Prime Network Services Controller only has IP or hostname information.
- User management—Prime Network Services Controller and Prime Performance Manager have their own authentication and credential management. Users must log into Prime Performance Manager for administrator cross launch. Report cross launch to Prime Performance Manager does not require user log in. Separate user accounts must be independently created and maintained in both Prime Performance Manager and Prime Network Services Controller.
- TCA alarm integration—Prime Performance Manager passes TCA events (performance thresholds, etc) to Prime Network Services Controller, which displays the alarms and events in the device alarm table. Prime Performance Manager sends the alarm ID, message text, device name, and severity. Prime Network Services Controller adds a time stamp based on the local system time. Alarms deleted in Prime Performance Manager are cleared in Prime Network Services Controller.
- Prime Network Services Controller host—The Prime Network Services Controller host is displayed in the Prime Performance Manager Administration Alarms/Events Editor Upstream OSS Hosts table. Table fields and the Delete button are disabled. Filter and Resend are enabled.
- The Prime Network Services Controller host is removed from the Prime Performance Manager Upstream OSS Hosts table when Prime Network Services Controller integration is removed on the Prime Network Services Controller Integration page.

Integrating Prime Performance Manager With Prime Network Services Controller

To integrate Prime Performance Manager with Prime Network Services Controller:

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

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

Step 3 In the Administration Prime Network Services Controller Integration window, enter the following:

Prime Network Services Controller Integration Setup

- Host—Enter the Prime Network Services Controller hostname or IP address.
- Admin User Name—Enter the Prime Network Services Controller administrator user name.
- Admin User Password—Enter the Prime Network Services Controller Integration administrator user password.

Prime Performance Manager User Setup

- Admin User Name (New)—Allows you to enter a new Prime Performance Manager new administrator username.

Note If user security is enabled, you can use an existing Prime Performance Manager user. If user security is not enabled, the user and password will be added as a new user expressly for Prime Network Services Controller access.

- Admin User Password(New)—If you entered a new Prime Performance Manager administrator user, enter the new administrator user password.

Step 4 On the toolbar, click **Submit Prime Network Services Controller Integration**.

Wait a few minutes for the integration to complete.

Step 5 From the Network menu, choose **Devices**.

Step 6 In the Network Devices window, verify the Prime Network Services Controller devices are added. These include:

- Cisco Virtual Security Gateway
- Cisco Adaptive Security Appliance 1000V Cloud Firewall
- Cisco Cloud Services Router 1000V Series
- Citrix NetScaler VPX load balancers Application Delivery Controller

Because device credentials have not been added, Prime Network Services Controller devices have an unmanaged status.

Step 7 Complete the "Adding SNMP Device Credentials" procedure on page 5-3 to add the Prime Network Services Controller SNMP credentials.

Step 8 Complete the "Adding Device Credentials for Other Protocols" procedure on page 5-6 to add the Prime Network Services Controller Telnet and SSH credentials.

Step 9 From the Administration menu, choose **Prime Network Services Controller Integration**.

Step 10 If you want Prime Performance Manager to manage only Prime Network Services Controller devices, check the Strict Sync checkbox. If not, continue with the next step.

Note If strict sync is not enabled, devices removed from Prime Network Services Controller are deleted from Prime Performance Manager. Prime Performance Manager listens for inventory notifications from Prime Network Services Controller so devices added or deleted in Prime Network Services Controller are reflected immediately in Prime Performance Manager.

Note A Prime Performance Manager cron job runs a full synchronization four times a day.

Step 11 On the Administration Prime Network Services Controller Integration window, click **Import Inventory**.

Step 12 From the Network menu, choose **Devices**.

Step 13 In the Network Devices window, verify the Prime Network Services Controller devices are added and their status is Active.

Step 14 Open Prime Network Services Controller.

Step 15 Verify that you can open Prime Performance Manager with the user and password entered in Step 3.

Note You can also perform Prime Network Services Controller integration using the ppm pnscintegration command. For information, see ppm pnscintegration, page B-68.

Removing Prime Network Services Controller Integration

To remove Prime Network Services Controller integration with Prime Performance Manager:

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

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

Step 3 On the Administration Prime Network Services Controller Integration window, click the Remove Integration tool.

Step 4 To complete the removal, log into Prime Network Services Controller and remove Prime Performance Manager through the Prime Network Services Controller GUI.

Discovering Devices With Prime Performance Manager

To generate reports, Prime Performance Manager must discover your network devices. Devices are commonly added to Prime Performance Manager by integrating it with other applications, then importing the application devices. Procedures for importing devices from other applications are provided in Chapter 4, "Importing Devices From Other Cisco Prime Applications."

You can also run device discovery from Prime Performance Manager. Use this discovery method when you have not imported devices from other applications, or want to add devices that aren't available in the other application. Before this can occur, you must create the credentials to allow Prime Performance Manager to connect to devices.

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

Device Discovery Requirements

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

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-performance-manager/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, from the Help menu choose **READMES and CLI Commands > Devices Info**.

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 credentials.

To discover a device, you must have the following information:

- The device identifier, such as IP address, DNS hostname, or other identifier.
- The credentials authorizing Prime Performance Manager to access the device.

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

In addition to these general requirements, some devices require special provisioning and setup. These requirements are described in the following topics:

- Data Center Discovery Requirements, page 5-13
- Small Cell Discovery Requirements, page 5-16
- Cisco CPT and ONS Discovery Requirements, page 5-18
- OpenStack Ceilometer Discovery Requirements, page 5-19
- Discovering Devices With Multiple Collectors, page 5-19
- Ceph Discovery Requirements, page 5-21
- KVM Discovery Requirements, page 5-21
- Cisco ME 4600 GPONs Discovery Requirements, page 5-23
- Cisco NAM Blade and Appliance Discovery Requirements, page 5-23

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 Device Credentials, page 5-3.
- Run discovery from Prime Performance Manager to acquire the gateways and units. See Running Device Discovery, page 5-11.

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.

Managing Device Credentials

You can run device discovery from Prime Performance Manager if you are not importing devices from another application or wish to add devices that are not in the imported application device inventory. Before you can run device discovery from Prime Performance Manager, 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 most Prime Performance Manager reports. However, many other protocols are supported to communicate with the many devices that Prime Performance Manager supports. Adding and managing device credentials are covered in the following topics:

Adding SNMP Device Credentials

Complete the following steps to add the SNMP credentials to communicate with network devices discovered by Prime Performance Manager. Complete this procedure if you run device discovery from Prime Performance Manager. You do not need to complete it if you imported devices from another application and do not wish to add devices not in the application imported device inventory.

Note You can enter an SNMP v2 community string and an SNMP v3 username and authentication password. If you specify both for the same device, Prime Performance Manager will try the SNMP v3 username and authentication password first. If this fails, Prime Performance Manager will try the SNMP v2 community string. Subsequent polls will try the SNMP v3 credentials and if it fails, try the SNMP v2. This provides a retry mechanism for failed SNMP v3 credentials.

Note To add SNMP credentials using the CLI, see ppm addsnmpcomm, page B-9.

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 New 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.
- SNMP Version—Enter the SNMP version used to poll the device: 1, 2c, or 3. Version 1 and 2c require a Read Community string. Version 3 requires a username, at a minimum.

- Read Community—Enter the SNMP community name that the device uses for read access to the information maintained by the SNMP agent on the device.
- Max Table Varbind—SNMP requests (Get, GetNext, GetBulk) can get multiple variables (varbinds) in a single request. All devices do not support the same number of varbinds per request; some devices behave abnormally if too many varbinds are included in a single request.

  Use this parameter only at the direction of Cisco support to manually reduce the number of SNMP varbinds that Prime Performance Manager polls in one request. For performance, Prime Performance Manager normally polls for multiple varbinds per request. Because of a combination of factors including platform, IOS version, device config, and others, some devices do not support the number of variables that can be contained in a single request, so Max Table Varbind can be used to manually reduce the number of variables in one request. It should only be specified when a problem occurs with a given device. Problems are normally determined by reviewing packet captures, interpreting the request and responses for adherence to protocol standards.
- Port—Allows you to specify an alternate device port for SNMP polling. By default, Prime Performance Manager uses Port 161, unless another port is entered here. For example, 4000 is the Cisco Network Service Orchestrator default SNMP port. (To get the NSO SNMP port, log into NSO using **ncs_cli -u admin** and run the **show configuration snmp** command. The agent udp-port will point to the supported SNMP port number, which you must use for NSO device discovery.

  Note The alternate device port is not supported if Prime Performance Manager is integrated with Prime Network.

- User Name (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 Device 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 Device Credentials, page 5-3, for parameter descriptions.

- IP Address Range or Hostname
- Read Community
- Max Table Varbind
- Port
- 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 Device 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 Device Credentials for Other Protocols

In addition to SNMP, Prime Performance Manager supports over twenty other device connection protocols including Telnet, SSH, HTTP, Data Center VMs, and many others. These credentials are added through the Network > Credentials Editor window.

In cases were multiple credentials are required, you complete the following procedure multiple times. For example, the Cisco Nexus 7000 BGP VRF Messages and BGP Neighbor Messages reports require Netconf, while the MPLS Traffic Engineering Tunnel report requires Telnet. To enable these reports, you would add an SSHv2 credential for Netconf and then add the Telnet credential, both on the same device.

To add device credentials for other connection protocols:

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

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

Step 3 In the Device Credentials Editor toolbar, click the **Add New Credentials Entry** tool.

Step 4 In the Add Credentials Entry dialog box, enter the following:

- Device—Enter the device hostname or IP address.
- Connection Protocol—Choose the 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.
  - collectd_SSH—A daemon that collects, transfers, and stores performance data.
  - HTTP—HyperText Transfer Protocol.
  - HTTPS—Secure HTTP.
  - HTTP_BULK—Bulk statistics through HTTP.
  - WMI_HTTP—Windows Management Instrumentation over HTTP.
  - WMI_HTTPS—Windows Management Instrumentation HTTPS.
  - SMI_HTTPS—Storage Management Initiative over HTTPS.
  - ULS_HTTP—Allows Prime Performance Manager to perform Small Cell upload server HTTP credential verification including subsystem, username, password, and credential parameters. Beyond that, ULS_HTTP is identical to HTTP protocol.
  - vCenter_HTTPS—VMware vCenter server over HTTPS.
  - ESXi_HTTP—VMware ESXi embedded bare metal hypervisor over HTTP.
  - ESXi_HTTPS—VMware ESXi embedded bare metal hypervisor over HTTPS

Note When you define the credential for vCenter and ESXi devices, make sure the user account you use has the session privilege. For information, see Hypervisor Discovery Requirements, page 5-15.

  - XEN_TLS—Xen hypervisor over Transport Layer Security (TLS) protocol.
  - KVM_TLS—Linux Kernal-based Virtual Machine (KVM) over TLS.

    Note Xen_TLS and KVM_TLS have discovery requirements. See Xen and KVM TLS Discovery Requirements, page 5-16

  - HyperV_HTTP—Microsoft HyperV server over HTTP.
  - HyperV_HTTPS—Microsoft HyperV server over HTTPS.
  - JMX—Java Management Extensions. Collects statistics from Java processes running on various servers.

    Note JMX reports are not enabled by default. After adding the JMX credential, you will need to enable the reports. For information, see Customizing Individual Report Settings, page 7-27.

  - PNSC_HTTPS—Cisco Prime Network Services Controller secure HTTP connection.
  - GMOND_SOCKET—Ganglia Monitoring Daemon (gmond) socket.
  - AVI_HTTPS—AVI Networks load balancing device secure HTTP connection.
- 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”.

  Note To poll the Cisco Nexus 7000 through its XML management interface using Network Configuration Protocol (NETCONF), enter **netconf** in the Sub System field. Using the XML interface allows you to generate Border Gateway Protocol (BGP) reports.

- User Name—Enter the device login username.

  Note For vCenter and ESXi devices that are members of an Active Domain, you can enter the domain and username in the format *domain/username*.

  Note For KVM_TLS, if SASL is enabled on the KVM device, add Simple Authentication Security Layer (SASL) credentials to the entry. SASL usernames typically have the SASL realm appended to it, such as user@hostname. If SASL is not enabled on the KVM device, you can leave the User Name and Password fields blank.

- Password—Enter the password for the login user.
- Secondary Login Type—Indicates how the secondary user and password should be processed:
  - Enable—Executes the Cisco IOS enable command, which provides Prime Performance Manager privileged EXEC level (Level 15) access to the device.

– Second Login—Executes the login command to log into the device using the secondary username and password. If you choose this option, the secondary user must have privileged EXEC access to the device,

Note Secondary Login Type is only available for Telnet or SSH connections.

- Secondary User Name—Enter the secondary username.
- Secondary User Password—Enter the secondary user password.

Note For NSO, use the secondary username and password for the NSO NETCONF username and password.

Step 5 Click **OK**.

The new credential is added to the credential table.

Step 6 If you entered an SSHv2 or HTTPS credential and want to use the SSHv2 key authentication, complete the following steps. Otherwise, continue with Step 7. By default, Prime Performance Manager authenticates itself to the device using the User Name and Password entries. To change to the SSHv2 authentication keys:

a. In the Credentials Editor window Client Authentication Type field, and choose **Public Key**.

b. Click the Client Private Key field.

c. In the SSH Credentials for [hostname] dialog box, enter the private key file name and click **Import**.

d. Enter the public key file name and click **Import**.

e. Click **Generate Public Key**.

Step 7 In the new credential table row Actions column, click the **Test the Credential** tool.

A Testing Credentials for [*device name*] dialog box appears. If Prime Performance Manager succeeded in connecting to the device with the credentials you entered, the following is displayed:

```
****Starting Credentials Test****
Connection test successfully!
****Test Completed****
```

If Prime Performance Manager could not connect to the device, an error is displayed, for example:

```
****Starting Credentials Test****
Exception while connecting to device!
****Test Completed****
```

Step 8 In the Test Credentials for [*device name*] dialog box, click **Close**.

Step 9 If the credentials test succeeded, on the Credentials Editor toolbar, click the **Save Credentials Entries** 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 click the **Clear the Row** tool in the Action column to clear the row contents or click the **Delete** tool to delete the entire credential.

Note For Telnet/SSH credentials, verify the 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 device credentials for other protocols, you might want to run device discovery. See Chapter 5, "Discovering Devices With Prime Performance Manager," for procedures. You should also enable the reports for the devices whose credentials you added. see Chapter 7, "Managing Reports, Dashboards, and Views."

Credential Notes for Other Protocols

After you add credentials for other protocols, run device discovery, and enable the appropriate reports, review the following information:

- Default Credential—Prime Performance Manager includes a default *.*.*.* Telnet credential. The default values are from the XMP_PAL.properties file. You can edit XMP_PAL.properties to set new default credentials. If you change the default credentials in the GUI and save them, the edited credentials are saved to a credential file, not XMP_PAL.properties. Thereafter, the default credentials come from the credential file and not XMP_PAL.properties.
- Device Discovery—During device discovery, non-SNMP credentials of discovered devices are displayed in a table beneath the SNMP credentials. The device discovery search algorithm seeks an exact match first. If no exact match is found, the default entry is used for device access credential.
- Events—If a credential issue arises, a Credential Problem state event is displayed in the device summary indicating an issue accessing the device by its credential exists.
- 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.

Adding Credentials for Cisco CPT 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 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; only one 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, page 5-11), 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.

Configuring vCenter and ESXi for Active Directory Authentication

To enhance VM troubleshooting, for example vCenter, ESXi, or other hosts with high CPU or memory utilization, you can configure vCenter and ESXi for Active Directory. For devices, such as vCenter, which have Windows authentication based on Active Directory, Prime Performance Manager provides an HTTP or HTTPS credential check through its domain and username, not simply the username.

Deleting Device Credentials for Other Protocols

Complete the following steps to delete other connection protocol device 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 **Credentials Editor**.

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

Step 4 On the Credential Editor toolbar, click **Delete Selected Credential Entry**.

Step 5 When finished, on the Credential Editor toolbar, click **Save Credentials Entries**.

Running Device Discovery

Before you run device discovery from Prime Performance Manager, you must add the credentials for all the devices you want to discover. Procedures are provided in Managing Device Credentials, page 5-3. Before you begin device discovery, you will need one of the following:

- A list of IP addresses, address ranges, subnets, Classless Inter-Domain Routing (CIDR) blocks, or DNS hostnames that you want Prime Performance Manager to use for discovery, or
- 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 Network Discovery window displays the following areas:

- Discovery Seeds—Displays the seed files, if they exist, containing the address information you want Prime Performance Manager to use for device discovery. It also displays the unit to which the discovered addresses will be assigned.
- SNMP Parameters—The SNMP credentials that will be used to connect to devices. See Adding SNMP Device Credentials, page 5-3.
- Other Credentials—Device credentials for other protocols are displayed. See Adding Device Credentials for Other Protocols, page 5-6, for a list of all supported protocols.

Step 3 If you want to run device discovery from a saved seed file, continue with Step 4. If you have no saved seed files, or want to run device discovery with a new one, complete the following steps:

a. In the IP Address, Address Range, Subnet, CIDR, or DNS hostname field, enter an IP address or address range, subnet, CIDR block, or DNS host name. Examples:

- 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. By default, Prime Performance Manager assigns units to discovered devices automatically. If you want to specify the unit, assign it in the Unit field.

Note You generally should allow Prime Performance Manager to allocate discovered devices to the units. Never use this field to reassign a device. To change a device-to-unit assignment, see Changing a Device-to-Unit Assignment, page 13-8.

c. Click **Add**. The device address or range is added as a seed entry.

d. Repeat Steps a through c until all information covering the devices you want to discover are added. (Should you wish to remove the address or range, select it and click **Delete**.

e. To save the individual seed entries as a seed file, on the toolbar click **Save Seeds**.

f. In the Save As dialog box, enter the following:

- Filename—Enter the file name. Spaces are not permitted.

- New Folder—(optional) If you want to place the seed file in a new folder, click **New Folder** and enter the new folder name.
- Make this my preferred Startup—(optional) Check if you want this seed file to appear by default whenever you run device discovery.

g. Click **OK**.

Prime Performance Manager saves the seed entries, closes the dialog box, and returns to the Network Discovery window. Device address information from the seed file is displayed in the Seed Devices File pane. SNMP and other protocol credentials for each seed device are shown in the SNMP Parameters and Other Credentials areas.

h. Continue with Step 5.

Step 4 To load a device from a saved seed file:

a. From the Network Discovery 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.

c. If needed, you can make the selected seed file you preferred startup file by clicking **Make This My Preferred Startup**

d. Click **OK**.

Step 5 When you are ready to start device discovery, on the Network Discovery toolbar, 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 9-2 on page 9-3.) 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 6 To view the devices that Prime Performance Manager discovered, from the Navigation menu, choose **Devices**. (See Displaying Device Information at the Network Level, page 9-2 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 or other communications required protocol 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 7 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 Discovery Requirements

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

- Cisco ASA 1000v
- Cisco ASA 5500
- Cisco Nexus 9000 Series
- Cisco Nexus 7000 Series
- Cisco Nexus 6000 Series
- Cisco Nexus 5000 Series
- Cisco Nexus 3000 Series
- Cisco Nexus 2000 Series
- Cisco ACE20/30
- Cisco ACE 4710
- 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
- Cisco MDS 9500
- Cisco ME 1200 and 4600 Series
- Cisco Catalyst 6000, 6500 and 7600 Series Firewall Service Module
- VMware vCenter Server
- ESXi hypervisor
- Kernal-Based Virtual Machine (KVM)
- Xen
- Hyper-V
- Cisco ASA 5500 cluster
- Cisco Nexus 9000 Series
- Cisco ASR cluster and 9Kv

- Citrix NetScaler VPX and SDX Virtual Appliance Family
- Cisco Virtual Security Gateway
- Cisco CSR 1Kv
- Cisco vNAM
- Ceph
- NetApp Storage
- AVI Load Balancer
- Cisco IOS XRv Router
- Cisco Web Security Appliance (WSA)
- Cisco Next Generation Intrusion Prevention System (NGIPS)
- Cisco Email Security Appliance (ESAV)
- Cisco Open Virtual Switch (OVS)
- Cisco Network Service Orchestrator
- Cisco Integrated Services Routers (ISR)

Prime Performance Manager also supports the following Windows OSs as data center hypervisor VM hosts:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

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 5-14
- Hypervisor Discovery Requirements, page 5-15
- Xen and KVM TLS Discovery Requirements, page 5-16

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 physical switch framework. The VDC runs as a separate logical entity within the switch. It maintains its own unique set of running software processes, has its own configuration, and is managed by a separate administrator. A Nexus can be configured with four VDCs, each appearing as a separate device.

Prime Performance Manager polls each VDC separately. This means you must add all VDC management IP addresses and credentials to 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 is 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 virtualized hypervisor devices including Hyper-V, Xen, KVM and ESXi. For VMware hypervisors, Prime Performance Manager uses the virtualization API, libvirt. This API requires a user with a session privilege.

Following procedures in the vSphere documentation (https://www.vmware.com/support/pubs/), complete the following steps:

Step 1 Log into VMware vSphere ESXi or vCenter.

Step 2 Create a new user role cloned from the vSphere default read-only role.

Step 3 Assign the new role the Sessions privileges.

Step 4 Add permission to vSphere ESXi or vCenter with an individual or group of vSphere recognized users and assign them the newly created role.

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 the libvirt website. For Prime Performance Manager servers, install the cyrus-sasl-md5 library to support SASL authentication.

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

cyrus-sasl-md5 is also required to support SASL authentication (if you sign your certificates using md5, which is the default). You can create TLS certificates using an older hashing algorithm, but installing the md5 package on Prime Performance Manager is easier.

UCS Server Discovery Requirements

Prime Performance Manager uses the Cisco Unified Computing System (UCS) Manager XML API for UCS discovery. The UCS XML is a programmatic interface to the Cisco UCS. The API accepts XML documents through HTTP or HTTPS. Therefore, to discover UCS servers, add its credentials using HTTP or HTTPS to Prime Performance Manager. See the "Adding Device Credentials for Other Protocols" procedure on page 5-6. To test the UCS credentials, you must configure the SNMP read community.

If you import UCS servers through Cisco Prime Network or other application, Prime Performance Manager automatically configures the SNMP and HTTP or HTTPS credentials for the servers.

Note For UCS C-Series with CIMC 1.6 or later, you must configure the SNMP Community with the HTTP/HTTPS credential on the CIMC port.

Small Cell Discovery Requirements

Prime Performance Manager supports the following small cell devices:

- RMS Central Node
- RMS Serving Node
- RMS Upload Server
- 3G and 4G Access Points (APs)

To prepare Prime Performance Manager for small cell support:

Step 1 Verify that Network Time Protocol (NTP) is synchronized between the Prime Performance Manager unit and the small cell devices.

Step 2 Verify the Radio Access Network (RAN) Management System (RMS) upload server find utility is 4.4.2 or higher. If not, upgrade it.

Step 3 Enable the SNMP service on the RMS Central Node, Serving Nodes, and Upload Servers.

- Configure the SNMP community; grant read access to the Prime Performance Manager unit.
- If you need to monitor system resources such as CPU, MEM, IO, or DISK, configure the SNMP agent to enable the related management information bases (MIBs).

Step 4 Before discovering the RMS Central Nodes and Serving Nodes and upload servers, add and test the following credentials to verify the credential connectivity. See Adding SNMP Device Credentials, page 5-3.

- SNMP—SNMP credentials must be configured for each PMG and upload server.
- SSH—SSH credentials must be configured for each PMG and upload server.

Step 5 For PMG performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway in etc/csvPull/system/pmg-perf.properties.

Step 6 For upload server performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway in etc/csvPull/system/uls-perf.properties.

Step 7 For BAC RDU and DPE reports, verify the parameters are correctly configured on the Prime Performance Manager gateway:

etc/bacStats/system/bac-rdu-perf.properties

etc/bacStats/system/bac-dpe-perf.properties

etc/csvPull/system/rdu-kpi.properties

etc/csvPull/systemdpe-kpi.properties

Step 8 For Device Command and Control (DCC) UI reports, verify that the settings in the gateway etc/csvPull/system/dccui-stats.properties file are consistent with the DCC UI configuration. The gateway synchronizes the file to all units. If settings are inconsistent, make the appropriate changes. For information, see Setting Up DCC UI Reports, page 8-43.

Note Before you begin collecting AP data, review and modify, if needed, the APSTATS_BACK_PERIOD setting in /properties/APStats.properties. This setting controls how far back Prime Performance Manager should retrieve data files. The default is 259200 seconds, or three days. If a large backlog has accrued before the first report polling cycle, you can change this setting to retrieve more backlog data. For more information, see Setting Up AP Reports, page 8-40

Step 9 Add the ULS to a ULS redundancy group, for example:

```
/opt/CSCOppm-gw/bin/ppmManageULSRedundancy.sh set SampleRedundancyGroup 10.74.125.205
```

Step 10 For Cisco Prime Network Registrar (PNR) Caching/Recursive Domain Name System (CDNS) performance log reports, verify that the settings in the gateway etc/bacStats/system/PNR-CDNS.properties file are consistent with the CDNS configuration. The gateway synchronizes the file to all units. If settings are inconsistent, make the appropriate changes. For information, see Setting Up DCC UI Reports, page 8-43.

Step 11 Restart Prime Performance Manager. See Restarting Gateways and Units, page 2-5.

Step 12 Enable the small cell reports, located in the Small Cell Statistics report category. For information on enabling reports, see Customizing Individual Report Settings, page 7-27.

Note The TR-069 Session Utilization report assumes the default SSL port is in use on the RMS serving device BAC-DPE component. If the default SSL port is changed on the BAC-DPE serving device, the TR-069 Session Utilization report will not display accurate information.

Cisco CPT and ONS Discovery Requirements

Cisco Carrier Packet Transport (CPT) devices are ordinarily added through Cisco Prime Network. If you add them through Prime Performance Manager device discovery, the requirements depend on the CPT release:

- Releases before Release 9.7—Define two devices, one for each CPT card, for example, 1.1.1.1@4 and 1.1.1.1@5.
- Release 9.7—Define one device. The CPT will route the SNMP request to the active card, for example, 1.1.1.1@2.

Ports 2000 and 2004 are for Telnet access to CPT cards. Prime Performance Manager does not support dynamic Telnet routing. It accesses the cards through Port 2000 plus the slot number.

Prime Performance Manager supports Optical Networking Service (ONS) and CPT devices through HTTP bulk statistics residing on the device side. Prime Performance Manager can access the devices through HTTP(s) using PAL or HTTPClient.

Prime Performance Manager supports the following performance management (PM) parameters:

- Optical Transport Network (OTN) /G.709 PM statistics for a client or Dense Wavelength Division Management (DWDM) line (ONS and CPT)
- FEC PM (ONS and CPT)
- Ethernet statistics for PT systems (CPT only)

Supported gateway network element (GNE) and end network element (ENE) SNMP credentials include:

- SNMP Community: the SNMP Community is specified in the SNMP editor.
- Add GNE device IP with a public community entry.
- Add ENE device IP with the community, <GNE IP>@public.

Table 5-1 lists the Telnet and SSH credentials for ONS and CPT devices.

Table 5-1 Telnet and SSH Credentials for ONS and CPT Devices

Parameters	GNE	ENE
IP Address	GNE device IP	ENE device IP
Port	80	80
Username	GNE user name	ENE user name
Password	GNE user password	ENE user password

Table 5-1 Telnet and SSH Credentials for ONS and CPT Devices (continued)

Parameters	GNE	ENE
Subsystem	n/a	<GNE IP>@1080
Protocol	HTTP_BULK	HTTP_BULK

To discover ONS and CPT devices, enter the following:

- GNEs—Enter the GNE device IP address.
- ENEs—Enter <ENE device IP>@<GNE device IP>.

OpenStack Ceilometer Discovery Requirements

OpenStack Ceilometers provide points of contact for billing systems to acquire the measurements needed for customer billing across OpenStack core components.

To discover Ceilometers, complete the "Adding Device Credentials for Other Protocols" procedure on page 5-6 and enter the following information:

- Device—Enter the OpenStack identity administration URL.
- Connection Protocol—Choose **HTTP** or **HTTPS**.
- Port—The default port is 35357.
- Subsystem—Enter **identity**.
- User Name—The username format is TenantName\Username

After entering the Ceilometer credentials, you can complete discovery following normal device discovery procedures. For information, see Managing Device Credentials, page 5-3 procedure.

Discovering Devices With Multiple Collectors

Prime Performance Manager uses SNMP as the primary protocol to discover a device and assign the device type based on the base sysObjectID value. However, some devices might have multiple collectors including SNMP, Ceilometers, Cisco UCS Manager (UCSM), Storage Management Initiative (SMI), Windows Management Instrumentation (WMI), hypervisors ESIx, Xen, Hyper-V, and KVM, and the gmond and collectd daemons, For devices containing multiple collectors, you can control the collector Prime Performance Manager uses to access the device. For example, if you are discovering a server that provides data through collectd, you might not want to enable SNMP collectors for the device.

To specify the collector Prime Performance Manager uses to discover a device with multiple collectors:

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

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

Step 3 With a text editor, open Server.properties and set the MULTI_COLLECTOR_ENABLED flag to true.

Step 4 Save your change.

Step 5 Reboot the gateway. See Restarting Gateways and Units, page 2-5.

Step 6 Repeat Steps 2 through 5 on each unit connected to the gateway.

Step 7 After the gateway and unit reboots are complete, log into the Prime Performance Manager gateway GUI.

Step 8 Verify credentials are added for all collectors contained on the device you want to manage. For information, see the following topics:

- Adding SNMP Device Credentials, page 5-3
- Adding Device Credentials for Other Protocols, page 5-6

Step 9 From the Network menu, choose **Discovery**.

Step 10 In the Network Discovery window IP Address, Address Range, Subnet, CIDR, or DNS Hostname field, enter the IP address of the device containing multiple collectors that you want to manage.

Step 11 Click **Add**.

Step 12 In the Collector Parameters area, select each discovery type that reside on the device and click **Add**. Available types include:

- SNMP
- Ceilometer
- collectd
- WMI
- UCSM
- SMI
- Hypervisor (includes ESXi, KVM, Hyper-V, Xen, and vCenter)
- gmond
- AVI
- UCS-CIMC
- Openstack

Step 13 Under Selected Discovery Types, choose the type you want Prime Performance Manager to use for device discovery and click **Raise** until it is at the top. For example, if you choose Ceilometer + SNMP, the device will be discovered as Ceilometer device. If you choose SNMP + Ceilometer, the device will be discovered as a Linux device.

Step 14 On the Network Discovery toolbar, click **Discover Network**.

Step 15 Wait a few minutes for the discovery to complete and data collected, then, from the Network menu, choose **Devices**.

Step 16 Verify the device is displayed on the Network Devices list.

Step 17 Should you wish to change or remove the primary collector:

a. Select the device.

b. From the Actions menu, choose **Edit Discovery Type**.

c. In the Edit Discovery Type dialog box, add or remove the discovery types making sure the discovery type you want Prime Performance Manager to use as the primary discovery type is at the top of Selected Discovery Types list.

d. Click **Save**.

Ceph Discovery Requirements

Ceph is a distributed object store and file system designed to provide performance, reliability and scalability. Ceph runs on commodity hardware in the Linux kernel. To discover Ceph devices, add the Ceph device credentials for which you want to gather performance statistics. A Ceph cluster consists of one or more Monitors, one or more Object Storage Daemons (OSDs) and, optionally, a Metadata Server (MDS).

Monitors provide basic availability statistics for the cluster: number of Monitors, OSDs, MDSs, their availabilities and statuses. OSDs are the main performance statistics provider. They provide I/O, latency, disk utilization, and other performance statistics.

Note Prime Performance Manager does not gather statistics from MDS devices.

To gather performance statistics from Ceph clusters install the Ceph plugin, which you can get from https://github.com/collectd/collectd. The plugin provided on this site is the only one that is supported.

Because Prime Performance Manager gathers collectd data through RRD files, install collectd with the RRDTool plugin enabled. The collectd.conf file must have an RRDTool entry that specifies the data directory (DataDir) where the RRD files are stored.

Prime Performance Manager defines the COLLECTD_BASE_DIR. It assumes collectd stores RRD files as /var/lib/collectd. As long as the collectd.conf file DataDir definition matches this directory, Prime Performance Manager will collect data from collectd. If the Ceph device does not have COLLECTD_BASE_DIR, the Ceph device status displayed in the Prime Performance Manager Network Devices window will be “Collectd base directory does not exist.”

Define Ceph device credentials in the Credentials Editor using collectd_SSH as the connection protocol and the Ceph device IP, username, password. See Adding Device Credentials for Other Protocols, page 5-6. Device discovery is the same as any other device. Enter the Ceph device IP address entered in the Credentials Editor. See Running Device Discovery, page 5-11.

KVM Discovery Requirements

Kernel-based Virtual Machine (KVM) is a virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, kvm-intel.ko or kvm-amd.ko.

KVM allows you to run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc. The KVM kernel component is included in mainline Linux, as of 2.6.20.

To monitor KVM devices with Prime Performance Manager, you can use the kvmTLSConfigScript located in /opt/CSCOppm-gw/samples/kvmTLSConfiguration, to configure the Transport Layer Security (TLS) and optionally, Simple Authentication and Security Layer (SASL) on libvirt for KVM devices. Ubuntu is the only supported Linux distribution for this script. Puppet files are included to make multiple KVM device configurations easier. Puppet installs all required packages. However, if you run the script manually, the following packages are required to configure TLS authentication:

- libvirt-bin
- gnutls-bin
- policycoreutils

To configure SASL authentication, the following packages are required:

- cyrus-sasl-md5
- sasl2-bin
- expect

Sample execution of the script looks like the following:

```
.../kvmTLSConfigScript off false false
```

or:

```
.../kvmTLSConfigScript on false true user password novaUser novaPassword
```

kvmTLSConfigScript takes the following parameters:

- sasl (on|off, default=off)—Configure SASL for libvirt
- overwrite_certs (true|false, default=false)—If TLS certs already exist, overwrite?
- sasl_nova_compute (true|false, default=false)—If Openstack Nova-compute is installed on this device, whether to create a nova user if SASL is enabled. Nova-compute won't be able to authenticate without a special authentication file for the nova SASL user.
- sasl_user—User to create for SASL authentication.
- sasl_pw—Password for the sasl_user
- nova_user (default=nova@$HOST—(only valid if sasl_nova_compute=true) User to create as the Openstack Nova-compute user for SASL
- nova_pw (default=nova—(only valid if sasl_nova_compute=true)—Password for nova_user.

If you are using puppet, specify these parameters and the IP addresses/hostnames of the KVM devices in the site.pp file. A sample site.pp file is included in this directory. Your site.pp file should be placed in /etc/puppet/manifests/site.pp on the puppet master node. The necessary puppet class files are provided here in the classes directory. Place these in /etc/puppet/manifests/classes/ on the puppet master node. Finally, place the script itself at: /etc/puppet/modules/kvmTLSConfig/files/kvmTLSConfigScript.

Avi Networks Discovery Requirements

Avi Networks Load Balancer provides the health and availability reports for Controller, Service Engine, Virtual Services, Pool, Members and Throughput and connection-related statistics.

To discover AVI devices, complete the "Adding Device Credentials for Other Protocols" procedure on page 5-6 and enter the following information:

- Device—Enter the AVI identity administration URL.
- Connection Protocol—Choose **AVI_HTTPS**.
- Port—The default port is 443.

After entering the AVI credentials, complete the "Running Device Discovery" procedure on page 5-11 and select **AVI** from the available discovery types. For information about device credentials, see Managing Device Credentials, page 5-3.

Cisco ME 4600 GPONs Discovery Requirements

If you are discovering Cisco ME 4600 Series devices Gigabit Passive Optional Networks (GPONs), disable the following reports before you discover the ME 4600 Optical Line Terminal (OLT) devices. Reports that you must disable include:

- IP Protocols > ICMP v4/v6
- Resources > IP Address
- Transport Statistics > PE-CE Interface >
  - PE-CE IPv4 Interface
  - PPE-CE IPv6 Interface

See gponPtin.notes for additional ME 4600 device implementation notes.

Cisco NAM Blade and Appliance Discovery Requirements

Prime Performance Manager supports the collection of data from the following Cisco Network Analysis Module (NAM) blades and appliances:

- Cisco Network Analysis Module Blades
  - Cisco Nexus 7000 Series Network Analysis Module (NAM-NX1)
  - Cisco Catalyst 6500 Series Network Analysis Module (NAM-3)
  - Cisco Catalyst 6500 Series Network Analysis Module (NAM-1/NAM-2)
- Cisco Prime Network Analysis Module Appliances
  - Cisco NAM 2000 Series Appliances
- Cisco Prime Network Analysis Module Virtual Blades
  - Cisco Prime Network Analysis Module for ISR G2 SRE
  - Cisco Prime Network Analysis Module for Nexus 1100 Series
  - Cisco Prime Network Analysis Module for WAAS Virtual Blade (VB)
- Cisco Prime Network Analysis Module Virtual Appliances
  - Cisco Prime Virtual Network Analysis Module (vNAM)

NAM support requires the following:

- Timing must be synchronized between the Prime Performance Manager gateway and the device where the Cisco NAM blade or appliance is installed.
- SNMP must be enabled on the device hosting the Cisco NAM blade or appliance.

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:

Tip If you have a collocated single server and only want to enable user access, you can use the ppm uaenable command. This command does everything for you except create the first admin level user. The command will set up everything else including configuring the SSL keys, and swapping the keys between the gateway and unit, and prompting you to enter the first admin level user. For more information, see ppm uaenable, page B-117.

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, “Importing Devices From Other Cisco Prime Applications.”

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 6-8
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.	Adding New Users, page 6-15
User and Security Management Tasks	
Edit user information.	Displaying User Information, page 6-16
Define the reports users can access.	Filtering Reports Assigned to Individual Users, page 6-20
Change user passwords.	Changing User Passwords, page 6-20
Edit user security settings.	Editing User Security Settings, page 6-21
Manually disable users and passwords.	Manually Disabling Users and Passwords, page 6-22
Enable user accounts and passwords.	Enabling User Accounts and Passwords Using the CLI, page 6-24
List currently defined users.	Listing Currently Defined Users, page 6-27
Display the system security log.	Displaying the System Security Log, page 6-27

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.

Note If you are purchasing an SSL certificate from a third-party Certificate Authority vendor, complete the Enabling Third Party CA Certificates for Cisco Prime Performance Manager, page 6-6, before you enable SSL on the gateway and unit.

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

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

Enabling SSL on a Gateway or Collocated Gateway and Unit

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

Step 1 Log into the gateway as the root user.

Step 2 Enter the ssl enable command:

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

Prime Performance Manager:

- Stops the gateway.
- Stops the collocated unit.
- Generates RSA private key.
- 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 "Enabling 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**

Enabling 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 Enable SSL on gateway:

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

Step 5 Execute the autoExchangeSSL.sh script to exchange SSL certificates between the gateway and remote unit:

```
/opt/CSCOppm-gw/bin/autoExchangeSSL.sh
```

Step 6 Enter the path to the gateway certificate:

```
Please Enter Gateway( ppm64-v6.cisco.com) Node Certificate Path:
[/opt/<gateway>/etc/ssl/server.crt]
```

Step 7 Enter the remote unit IP address:

```
Please Enter Remote Node IP: nnn.nnn.nnn.nnn
```

Step 8 Enter the remote unit username and password:

```
Please Enter SSH username for Remote Node(10.74.125.192):  [root]
Please Enter SSH Password for Remote Node(10.74.125.192):
SSH Connection Test successful!
```

Step 9 Enter the path to the unit certificate:

```
Please Enter Certificate Path for Remote Node(10.74.125.192)
[/opt/<unit>/etc/ssl/server.crt]
```

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:

```
#################Remote Node(nnn.nnn.nnn.nnn) import Gateway (gatewayIP)
Certificate...#################
```

```
Remote Node (unitIP) import Gateway (gateway) Certificate was added to keystore
successful!
################ Gateway(gateway) import Remote Node(unitIP)
Certificate...#################
localsever(gateway) import Remote Node(unitIP) Certificate was added to keystore
successful !
```

Step 10 Restart the gateway:

/opt/CSCOppm-gw/bin/ppm restart

Step 11 Restart the remote unit:

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

Related Topics:

Exporting SSL Certificates, page 6-5

Displaying SSL Status, page 6-5

Disabling SSL, page 6-6

Exporting SSL Certificates

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

To export a SSL certificate, enter the following command:

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

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

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

Displaying 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`

Printing 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
```

Displaying the 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
  ```

Disabling 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
```

Enabling Third Party CA Certificates for Cisco Prime Performance Manager

To enable third-party Certificate Authority (CA) SSL certificates for your website, you must purchase certificates issued by a third-party CA vendor such as Symantec (previously VeriSign), DigiCert, GoDaddy or other third party vendor. When you order the certificate, the vendors might ask you to enter

the number of servers that will be secured with the certificate. This is the number of licenses you want to purchase for the certificate, or the number of web servers on which you're going to install the certificate.

To generate a self-signed key and certificate for Prime Performance Manager:

Step 1 From the Prime Performance Manager gateway, enter the following command:

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

The command generates the following files:

```
-rw-r--r--. 1  root root 1647 Jun 12 15:42 server.crt
-rw-r--r--. 1  root root 1054 Jun 12 15:42 server.csr
-rw-------. 1 root root 1675 Jun 12 15:37 server.key
-rw-r--r--. 1  root root 2973 Jun 12 15:42 sgmSslCerts
-rw-------. 1 root root 2896 Jun 12 15:42 sgmSslKey
```

where server.csr is the certificate signing request file (CSR).

Step 2 Purchase the third-party CA certificate:

a. Log into the third-party CA website and register an account to purchase your SSL certificate.

b. During the order, open the server.csr file listed above in a text editor and copy the entire content including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines.

c. Paste the content in the form that asks you to enter the CSR on the third-party CA website.

d. Enter any additional required information, then submit the purchase order.

Note When you enable SSL in Prime Performance Manager, the ppm ssl enable command also generates the above key/certificate files. However, the default CSR file is generated with a few items left empty such as: Country Name, State or Province Name, Locality Name, Organization Name. and other fields. If you request a third-party CA signed certificate, do not use the default CSR file during the purchase because it will not pass the CA validation and an SSL certificate will not be issued.

Step 3 Download the signed, third-party CA certificate:

After your SSL certificate purchase request is validated, the CA company issues you a signed SSL certificate. Depending on the vendor, you can have the signed SSL certificate sent to you by email or you can download the certificate from the vendor's website. Usually the signed SSL certificate is named <your-domain-name>.crt. (The certificate file can also have the extension DER, PEM, or CER). Save the signed SSL certificate file locally for later import into Prime Performance Manager.

Note Some CA vendors might also send you an intermediate certificate file. If so, download it and save locally.

Step 4 In Prime Performance Manager, enter the following command to import the signed third-party CA certificate:

```
/opt/CSCOppm-gw/bin/ppm keytool import_cert <cert_filename>
```

where the <cert_filename> is the signed CA certificate from the CA vendor.

Note If you received an intermediate certificate file from the CA vendor, import it before you import the above signed certificate. Contact the CA vendor for any technical support and service.

After the import, the old self-signed certificate is replaced with the imported one.

Step 5 Complete the Enabling SSL on a Gateway or Collocated Gateway and Unit, page 6-3 to configure SSL for the gateway.

The web interface is now be secured by the signed CA certificate.

Note Gateway and unit communication uses Java RMI. After SSL is enabled, the gateway and unit also uses SSL to secure the communication. However, because the unit is not open to end users, a signed CA SSL certificate is not required for gateway and unit communication. Therefore, you can still use the default Prime Performance Manager self-signed certificate for the unit servers. For details, see Enabling SSL on Remote Units, page 6-4.

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.
- 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 can use authentication through Pluggable Authentication Modules (PAM) for Remote Authentication Dial in User Service (RADIUS), Terminal Access Controller Access-Control System (TACACS+), Lightweight Directory Access Protocol (LDAP), and Microsoft Active Directory 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.
- INSTALL.pam_msactivedir.txt

These files are located in the Prime Performance Manager gateway installation directory (/opt/CSCOppm-gw/install by default). Cisco provides the configuration information only as general guidance. Any specific PAM deployment issues are beyond the scope of Cisco support.

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/Tenants/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 127.
- Password maximum length must be *n* characters.

  The default is 80. You can set a value ranging from 0 through 127.

- 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 two consecutive times in the password.
- Password must contain at least one character from the three character classes:
  - upper case
  - lower case
  - digits and 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 five 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, you can use the **ppm adduser** command, as described in User Authentication, page 6-8, or **ppm updateuser** or **ppm newlevel** commands, as described in Enabling User Accounts and Passwords Using the CLI, page 6-24.

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.
View Administrator	• 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. • Create and edit views.
Network Operator	• Access all basic user actions. • View alarms and events. • Access only the Normal Poll and Edit Properties options in the device Actions menu.
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, “Importing Devices From Other Cisco Prime Applications.”

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 Logging In as the Root User, 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 Logging In as the Root User, page 2-1.

Step 2 Change to the */bin* directory:

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

Step 3 Disable user-based access:

```
./ppm useraccess disable
```

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

Configuring Microsoft Active Directory Authentication

You can configure Prime Performance Manager to use Microsoft Active Directory for authenticating users using PAM and LDAP.

To configure Prime Performance Manager to use Microsoft Active Directory for authenticating users:

Step 1 Log into the Active Directory server.

Step 2 Launch Active Directory and display the New Users and Computers window.

Step 3 Create a PPM Bind bind user directly under the domain, ppm.local.

Note This procedure uses ppm.local as an example domain. The domain can have any name of your choosing. The user should not belong to any groups.

Step 4 In the New Object - User wizard, enter the following:

- First name—PPM
- Last name—Bind
- Full name—PPM Bind
- User logon name—PPMBind @ppm.local
- User logon name (pre-Windows 2000)—PPMBind.

Step 5 Click **Next**.

Step 6 In the next wizard panel, enter the following:

- Password—Enter Cisco123.
- Confirm password—Enter Cisco123.
- Check the following options:
  - User cannot change password
  - Password never expires

  Do not check the other options.
- User logon name—PPMBind @ppm.local
- User logon name (pre-Windows 2000)—PPMBind.

Step 7 At the command prompt, enter **dsquery** to verify the user is configured properly. The following response should appear:

```
C:\Documents and Settings\Administrator.LDAP-MBARUCH>dsquery user -namne PPM*"CN=PPM
Bind,DC=ppm,DC=local"
C:\Documents and Settings\Administrator.LDAP-MBARUCH>
```

Note The dsquery command was executed on Window 2003. You might need to install users separately on other Windows versions, and the command format or syntax might differ. See the Microsoft Windows documentation for details.

Step 8 Complete the following steps to edit the ldap.conf:

```
vi /etc/ldap.conf
```

a. Add the hostname:

```
# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
host LDAP-Server.cisco.com
```

b. Add the search base:

```
# The distinguished name of the search base.
base DC=ppm,DC=local
```

c. Add the bind user details. This must match the dsquery results.

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn CN=PPM Bind,DC=ppm,DC=local
```

d. Add the bind password:

```
# The credentials to bind with.
# Optional: default is no credential.
bindpw Cisco123
```

e. Update the PAM details in the # RFC 2307 (AD) mappings section:

```
pam_login_attribute sAMAccountName
pam_password ad
```

f. Verify that /etc/ldap.conf has the following:

```
# cat /etc/ldap.conf | grep -v '^[#]' | grep -v '^$'
host LDAP-Server.cisco.com
base DC=t4,DC=local
CN=PPM Bind,DC=t4,DC=local
bindpw Cisco123
timelimit 120
bind_timelimit 120
idle_timelimit 3600
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm
pam_login_attribute sAMAccountName
pam_password ad
```

Step 9 Edit the ppm-jpam file based on your OS type:

```
vi /etc/pam.d/ppm-jpam
# Change pam_unix_auth.so to pam_ldap.so
# Change pam_unix_acct.so to pam_ldap.so
# The following is for Linux 64
    auth        required  /lib64/security/pam_ldap.so
    account     required  /lib64/security/pam_ldap.so
# The following is for Linux 32
    auth        required  /lib/security/pam_ldap.so
    account     required   /lib/security/pam_ldap.so
```

Step 10 If Prime Performance Manager user access is not enabled, enable it:

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

Choose the auth mode as Linux

When you create the default user, enter **y** for the following confirmation:

```
Can't match key TestLinux in map passwd.byname. Reason: No such key in map
Could not find user in /etc/passwd or NIS.
Should User User1 be added anyway? [n] y
```

Step 11 Add the Prime Performance Manager users:

#/opt/CSCOppm-gw/bin/ppm adduser

When you create the default user, enter **y** for the following confirmation:

```
Can't match key TestLinux in map passwd.byname. Reason: No such key in map
Could not find user in /etc/passwd or NIS.
Should User User1 be added anyway? [n] y
```

Users created on the MS AD server but not added to Prime Performance Manager can still log into Prime Performance Manager but only with the basic access level.

Step 12 Verify the user login

a. Connect to https://servername:4440.

b. Test the user login using any username/password configured on the MS-AD server.

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:

Adding 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/Tenants/Security**.

Step 3 In the Users window, click the **Add User** 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 6-8.)

- User Name—Enter the new username.
- First Name—Enter the user first name.
- Last Name—Enter the user's last name.

Note A star "*" character is not permitted in the user names.

- Role—Enter the user authentication role for the user. The valid values are:
  - Basic User
  - Network Operator
  - System Administrator
  - View Administrator
  - Custom Level 1
  - Custom Level 2

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

- User Group—Allows you to assign a user to a user group. To do this, you must create a user group. See Creating User Groups, page 6-18.
- Home View—Allows you to assign a home view to the user. Views created in the Prime Performance Manager gateway appear in the Home View drop down list. The view you assign is the one the user sees when he or she logs into Prime Performance Manager,
- 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 e-mail 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.
- Tenant Name—If multi-tenancy is implemented, allows you to associated the user to a tenant account.
- 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 **Save**.

Displaying User Information

After you add users, you can display the user information at any later point:

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

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

Note A star "*" character is not permitted in the user names.

- User Group—The user group assigned to the user, if any.
- Home View—The home view assigned to the user, if assigned,
- Report Filter—Allows you filter reports by user. See Filtering Reports Assigned to Individual Users, page 6-20.
- 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
  - View Administrator
  - Custom Level 1
  - Custom Level 2

  See Table 6-2 on page 6-11, 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 Disabling Users and Passwords" section on page 6-22 for more information.
  - Prime Performance Manager disabled the account because of too many failed attempts to log in. See the "Editing User Security Settings" section on page 6-21 for more information.
  - Prime Performance Manager disabled the account because it was inactive for too many days. See the "Editing User Security Settings" section on page 6-21 for more information.
  - Expired Password—Indicates the user's password has expired.
  - Temporary Password—Indicates the user has a temporary password.
- Tenants—If tenants are assigned to the user, there are displayed.
- 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

Editing User Information

To edit user information:

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

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

Step 3 In the Users window, check the box next to user whose information you want to edit.

Step 4 Click **Edit** on the Users toolbar.

Step 5 In the Edit User Information dialog box, revise any of the following information:

- First Name
- Last Name
- Email address
- Phone
- Customer Name
- Account Number
- Role
- User Group
- Home View
- Password Aging
- Tenant Name

Step 6 Click **Save**.

Creating User Groups

You can create user groups and assign users to them. You can then customize the reports that are available to the user group. For example, if you have an external customer with many individuals who want to look at the same reports, you can assign those individuals to a user group and customize the reports available to the user group.

Note Users can only be assigned to one user group.

To create a user group:

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

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

Step 3 On the Users window, click **User Groups**.

Step 4 In the User Groups window, click **Add**.

Step 5 In the Add User Group dialog box, enter the use group name. The name cannot have spaces or special characters, except hyphens and underscores.

Step 6 Enter a description in the User Group Description field.

Step 7 Click **Save**.

The new group appears in the User Groups list.

Step 8 To assign users to user groups, complete one of the following procedures:

- Adding New Users, page 6-15
- Editing User Information, page 6-18

Filtering Reports Assigned to User Groups

To assign specific reports to user groups:

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

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

Step 3 On the Users window, click **User Groups**.

Step 4 In the User Groups window, choose the user groups for which you want to filter reports.

Step 5 On the User Groups toolbar, click **Filter Reports**.

Step 6 In the Filter User Reports dialog box, expand the report trees and deselect the reports you do not want the user to access.

Step 7 If you want to provide additional report 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, choose one of the following:

– Filter Using a Group—If you choose this option, choose the group name in the Group Name list. (Processing Name is always set to default.)

– Filter Using a Report Column—If you choose this option, complete 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**.

Filtering Reports Assigned to Individual Users

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/Tenants/Security**.

Step 3 In the Users window, choose the users for which you want to filter reports.

Step 4 On the Users toolbar, click **Filter Reports**.

Step 5 In the Edit User Reports dialog box, expand the report trees and deselect the reports you do not want the user to access.

Step 6 If you want to provide additional report 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, choose one of the following:

- Filter Using a Group—If you choose this option, choose the group name in the Group Name list. (Processing Name is always set to default.)
- Filter Using a Report Column—If you choose this option, complete 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**.

Note If you are member of a group and that group has reports filtered, your individual report filtering settings take priority over the group settings.

Tip To quickly clear all user report filters, click **Reset to Default**.

Changing 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/Tenants/Security**.

Step 3 In the Users window, 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 **Save**.

Note You can also change user passwords using the ppm userpass command. See ppm userpass, page B-120.

Editing 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/Tenants/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-18.)
- 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-19.)

Note Prime Performance Manager restricts users who attempt to log in from different IP addresses within ten-minute period. A threshold is calculated based upon the number of IP addresses that made unsuccessful login attempts. Prime Performance Manager calculates the maximum number of login attempt number for a given user from those IP Addresses.

- 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-46.)
- 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-67.)
- 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-23.)
- 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.
- 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.

Step 5 Click **Save** to save your security settings.

Note For information about creating login messages, see Creating Messages of the Day, page 6-25.

Manually Disabling Users and Passwords

As described in the Editing User Security Settings, page 6-21, 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 6-15 for more details.

To disable Prime Performance Manager users and passwords:

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

Step 2 Enter:

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

Step 3 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.

Step 5 To disable a user 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.

Step 6 To re-enable the user account:

- Using the same password—Enter the **ppm enableuser** command.
- Using a new password—Enter the **ppm userpass** command.

Enabling 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 Logging In as the Root User, 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.

Creating 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/Tenants/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-60 and ppm premotd, page B-71.

Sending Announcements to Online Users

Administrator users can send announcement messages to all online Prime Performance Manager users. Announcements are displayed in a message window and require users to acknowledge to close the window.

To send an announcement to online users:

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

Step 2 From the menu bar at the top right window corner, choose **Send Announcement**, shown in Figure 6-1.

Note The Send Announcement tool is only displayed to Administrator users.

Figure 6-1 Send Announcement Tool

Step 3 In the Send an Announcement to All Online Users window, type the message you want to send.

Note If user access is enabled, the message window contains a From field populated with your username.

Step 4 When finished, click **Send Announcement**.

The announcement appears in a popup window on the screens of all online users, Users must click **OK** to dismiss the message.

Displaying 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/Tenants/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:

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

Listing 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 6-15 for more details.

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

Step 2 Change to the */bin* directory:

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

Step 3 List all users:

```
./ppm listusers
```

Prime Performance Manager displays the following information for each user:

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

Displaying the System Security Log

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

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

Step 2 Change to the */bin* directory:

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

Step 3 Display the security log contents:

```
./ppm seclog
```

The following security events are recorded in the log:

- All changes to system security, including adding users
- Login attempts, whether successful or unsuccessful, and logoffs

- Attempts to switch to another user's account, whether successful or unsuccessful
- Attempts to access files or resources of higher account level
- Access to all privileged files and processes
- Operating system configuration changes and program changes
- 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.

You can also view the system security log on Prime Performance Manager System Security Log web page. For more information, see Displaying the Security Audit Log, page 12-6.

Managing Reports, Dashboards, and Views

Prime Performance Manager provides over 7200 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

After Prime Performance Manager device discovery is completed (see Chapter 5, “Discovering Devices With Prime Performance Manager”), 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 an alphabetical list of all provided reports, from the Help menu, choose **Reports > Reports List Readme**.

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

- Application Traffic
- Applications
- Availability
- Compute
- IP Protocols
- IP QoS
- IP SLA
- JMX Applications
- Layer 2 Protocols
- Mobile IOS Statistics
- Mobile StarOS All Counters
- Mobile StarOS CDMA KPI
- Mobile StarOS CDMA Statistics
- Mobile StarOS KPI
- Mobile StarOS Statistics
- NetFlow
- NetFlow AVC
- Network
- Network Services
- OpenStack
- Orchestration
- PPM System
- Resources
- Security
- Small Cell Statistics
- Storage
- Transport Statistics
- Video Broadcast

By default, all reports are disabled except for the following:

- Application Traffic
  - SNMP
  - UDP
  - TCP
- Availability
  - ICMP Ping
  - ICMP Ping Aggregate
  - SNMP/Hypervisor Ping

  - SNMP/Hypervisor Ping Aggregate
  - Interface Status
  - Interface Status Aggregate
  - Interfaces
- IP Protocols
  - ICMP
- PPM System
  - Data Metrics
  - Data Metrics Aggregate
  - Device State
  - Poller Metrics
  - Server Metrics
- Resources
  - CPU
  - Memory
  - Disk
- Transport Statistics
  - Interface

To enable reports, see Customizing Individual Report Settings, page 7-27.

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.
- Device OS changes, such as upgrades, temporarily stop the report data flow to Prime Performance Manager, particularly for video monitoring. After a device OS change, set the device to its original policy group and do a manual poll.

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

- The time zone entered in the device Time Zone field. See Editing a Device Name, Web Port, Time Zone, and Location, page 9-16.
- The device time zone when the device was imported from other applications.
- The time zone retrieved from the device.
- 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-1.6.0,172.18.20.168,20120912-153526,20120912-113526,EDT,-0400,120912-11:35, private

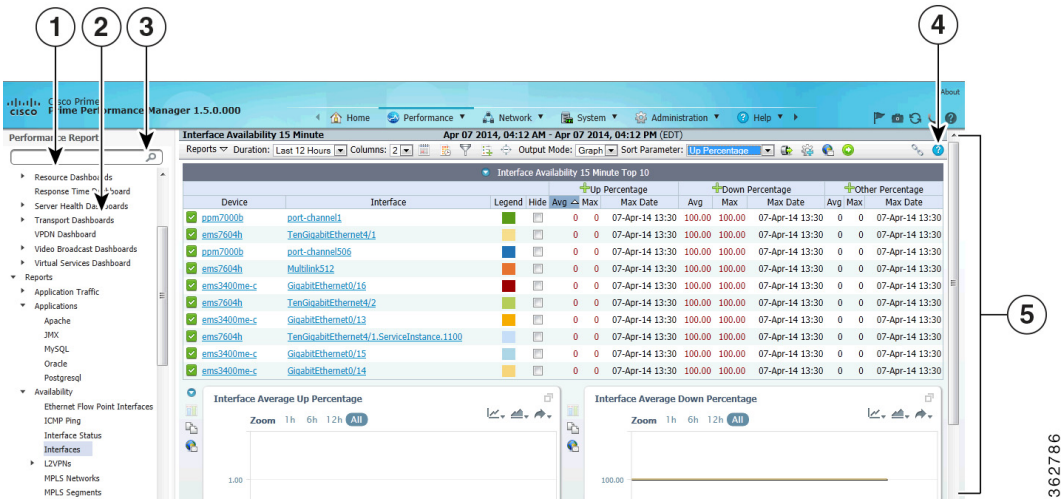
Figure 7-1 shows the Prime Performance Manager reports window with the Interface Availability report displayed in graph output format. Window elements include:

- Navigation tree—Allows you to select high-level report categories and subcategories.
- 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



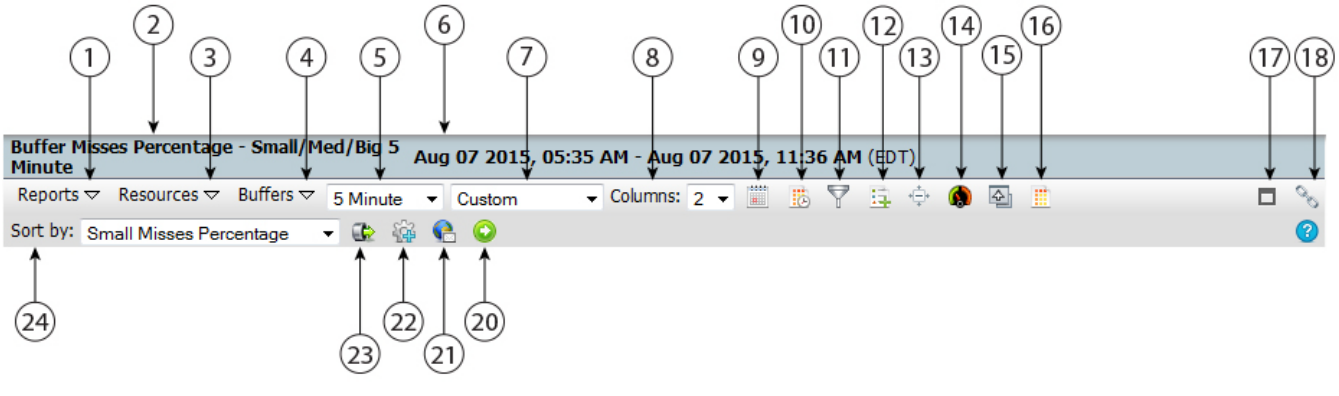
1	Navigation tree display tools	**4**	Menu bar
2	Navigation tree	**5**	Content area (graph view)
3	Search field		

Reports Menu Bar

The Prime Performance Manager 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 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 Customizing the GUI and Information Display, page 3-8.

The tools and options displayed on the reports menu bar depend on whether the output mode. scope, and other factors. Figure 7-2 shows the report toolbar at the device level when output is set to Graph.

Figure 7-2 Reports Menu Bar in Graph Mode



1	Reports selection menu	**13**	Toggle Compact Mode
2	Report title	**14**	Go Live
3	Report subcategory menu (Resources in this example)	**15**	Disable Leaf Graph
4	Report subcategory menu (Buffers in this example)	**16**	Graph/Table View
5	Duration (5 minute in this example)	**17**	Open Report in New Tab
6	Duration	**18**	Report links
7	Report Date and Time	**19**	Report Help
8	Columns	**20**	Run Report
9	Customize Date and Time	**21**	Email Report
10	Daily Comparative Analysis	**22**	Graph Series Editor
11	Filter	**23**	Export report as CSV File
12	Toggle Legends	**24**	Sort parameter

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.

Note Report subcategories displayed on the report toolbar reflect the subcategories for the displayed report. For example, if you display an hourly temperature report for a device you will see Reports, Resources, and Environment on the toolbar menu because the device temperature is located in the Resources > Environment subcategories. If multiple subcategories exist between Reports and the subcategory containing the report, you will see the first Reports subcategory and the subcategory containing the report.

- Interval and Duration fields—Two unnamed drop-down lists allow you to choose the report interval and duration. The interval and duration options depend on the report intervals that are enabled. Table 7-1 shows the possible intervals and durations. In the duration field, the terms, past and previous, have distinct meanings:
  - Past—Is the specified time unit up to the report query date and time. For example, if Last Hour is specified for a report run at 8:34 AM, the report period would be 7:34 AM to 8:34 AM.
  - Previous—Is the last complete time period before the report query date and time. In this example, the Previous Hour report period would be 7:00 AM to 8:00 AM.

Table 7-1 Report Interval and Duration Options

Interval	Duration
1 Minute	Custom, last minute, last hour, previous hour, last 6 hours, work shift, today, last 24 hours, yesterday **Note** Custom uses the time period defined using the Customize Date and Time Range tool. Work shift uses the time period defined in system settings. See Changing System Configuration Settings, page 3-17.
5 Minute	Custom, last 5 minutes, last hour, previous hour, last 6 hours, work shift, today, last 24 hours, yesterday, last 3 days
15 Minute	Custom, last 15 minutes, last hour, last 6 hours, work shift, last 12 hours, today, last 24 hours, yesterday, last 3 days, last 7 days
Hourly	Custom, last hour, work shift, last 12 hours, today, last 24 hours, yesterday, last 3 days, this week, last 7 days, previous week
Daily	Custom, yesterday, this week, last 7 days, previous week, last 14 days, last 21 Days, this month, last 30 days, previous month, last 60 days, last 90 days
Weekly	Custom, previous week, last 4 weeks, last 8 weeks, last 12 weeks, 6 months, this year, last 1 year, previous year
Monthly	Custom, previous month, last 3 months, last 6 months, this year, last 1 year, previous year

Note Intervals greater than the reporting aging intervals will not be displayed. For information, see Customizing General Report Settings, page 7-25.

- 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. For reports one hour or less in duration, two options are available:
  - Specific Days—Allows you to choose a start and end date and time.
  - Daily Repeat—Allows you to set up queries starting and ending at specific times of day. The queries run every day without a start and end calendar date.

  The maximum time span you can specify depends on the report interval:
  - One minute reports—Two days
  - Five minute reports—Four days
  - Fifteen minute reports—Seven days
  - Hourly reports—Seven days
  - Daily reports—94 days
  - Weekly reports—Two years
  - Monthly reports—Five years

  Increments also

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

- Daily Comparative Analysis—Allows you to create a report comparing data gathered on the same day(s) and times, for example, CPU usage at 5:00 PM every day. The option is available for daily report intervals or shorter. After you click Daily Comparative Analysis, choose the days of the week and time of day. then click **OK**. When the report reloads, it filters the report data on the days of week and time of day you selected. If you copy a filtered graph to a view, the filter is applied to the copied graph as well.

  After you set the daily comparative analysis filter, the tool is highlighted. To reset it, open the dialog and click **Reset**. When the report is displayed, the filter is not applied and the tool is not highlighted.
- Filter—Allows you to filter report information based on different criteria. See Filtering Report Information, page 7-17 for information.
- Toggle Legends—When Output is set to Graph, turns the graph legend on and off. If turned on, the graph legend appears under each graph displaying the color-coded report items. and the average and maximum data values for each item.

- Toggle Compact Mode—When Output is set to Graph, toggles the display of the Zoom, Aggregate Lines, Graph Styles, and Export Graphs tools displayed inside graphs. Additionally, the graph border is hidden and graph title reduced in size. Using this option reduces the overall size of the graph and is useful when screen real estate is needed.
- One Graph Per Series—When Output is set to Graph and the report is device level, allows you to display all data series as separate graphs. The option is a toggle.
- Go Live—Initiates 15-second, 30-second, or 1-minute polling for device-level reports. For information, see Creating Live Mode Reports, page 7-16.
- Disable Leaf Graph—Appears when you drill down to the report leaf graph level and the leaf graph has multiple data series. For example, you can drill down an Interface Availability report to the interface level and see three outputs: Up Percentage, Down Percentage, and Average Other Percentage. By default, these are displayed on the same leaf graph. To see the data on separate graphs, click Disable Leaf Graph. To display the leaf graph, click Enable Leaf Graph again.
- Change to Table/Graph View—Allows you to display your report in two different ways:
  - Graph—(Default) Displays the report in summary table and graph formats. The summary table summarizes each data series by report entity, for example, device, device interface, or other entity. Summary values includes minimum, maximum, average, and current values, the times the minimum and maximum values occurred, and total, standard deviation, and variance values. Not all values are displayed by default. You can display or hide values by enabling or disabling them in User Preferences. See Customizing the GUI and Information Display, page 3-8. The summary table legend allows you match a table row to the graph element. The graph presents report data visually and includes individual data points. By default, ten report items are displayed. (You can change the number of items displayed in User Preferences. You can also customize the graph display. For information, see Customizing Report Display, page 7-13.)
  - Table—Displays all report data in table format. Page controls, shown in 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. Figure 7-3 shows the report toolbar in table output mode.

  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.
- Export Report Page as CSV File.—Exports the report to a comma separated values (CSV) file, See Exporting Report Data to CSV Files, page 7-20.
- Graph Series Editor—Opens the Graph Series Editor where you can add, remove, or change the report data series display name in the report graph. 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.)
  - To change a report data series name, clear the current name in the Display Name field, then type the new name. To remove the custom name and redisplay the system name, click the "**Clear the custom name**" arrow.
  - To delete a series, click the **X** next to the series item.
  - To add a series, enter the first few letters of the series name in the Add Series field. A list of available items matching the letters you entered is displayed. Click the one you want to add; it is automatically added to the bottom of the data series.

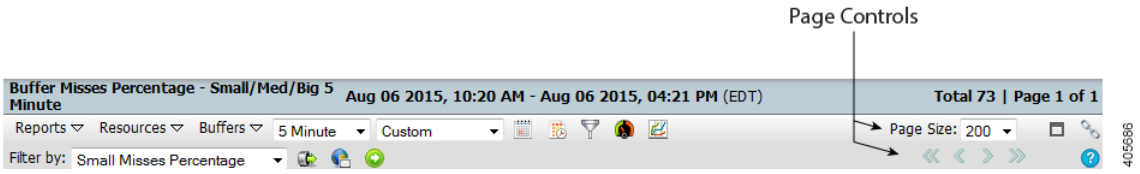
  When finished, click **Run & Close** to update the graph with your changes. Other actions:
  - Close—Closes the Graph Series Editor and does not save any changes,
  - Clear—Removes all content from the Graph Series Editor.

  - Reset—Returns the Graph Series Editor to the default data series.

- Email Report—Allows you to email the report to individuals of your choosing. For information, see Emailing Reports, page 7-20.
- Run Report—Runs the report after you modify any report parameters in the menu bar.
- Page Link—Retrieves the URL used to launch the selected report from an integrated Cisco Prime application (such as Prime Central), from a Prime Performance Manager Representational State Transfer (REST) client, or on its own in a browser. See Sharing Report and Dashboard URLs, page 7-35 for more information.
- 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.
- Sort Parameter—Allows you to sort the report by different parameters.
- Play View—Scrolls through views automatically. The option appears when you display the highest level of your created view. You can change the view interval (20 seconds is the default) and display type (inline or full screen) in User Preferences. For information, see Customizing the GUI and Information Display, page 3-8. For information about views, see Creating and Managing Custom Report Views, page 7-39.

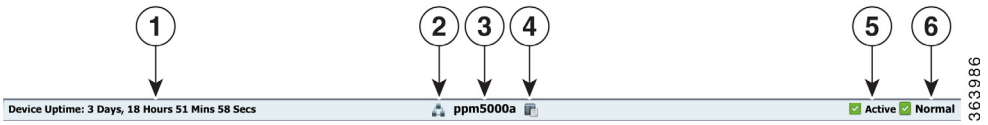
Figure 7-3 shows the reports toolbar when Output is Table. All items pertaining to graphs are removed, and the report length, specified in pages, is shown at the top right. The Page Size option allows you to set the number of table rows displayed in one individual page.

Figure 7-3 Reports Menu Bar in Table Mode



When you drill to a device-level report, a device status bar, shown in Figure 7-4, appears above the report. It shows the device name (center), uptime (left), and the device status and highest alarm on the far right. Two tools are provided allowing you to return to network level view or to display a detailed view of the device.

Figure 7-4 Device Status Bar



1	Device uptime	**4**	Explore Device tool
2	Return to Network Level Report tool	**5**	Device status
3	Device name	**6**	Device alarm status

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 assigned to the report. The sort weight is a numeric that indicates the report's importance relative to other reports in the category. Not all reports are assigned sort weights, however, in which case, reports are arranged alphabetically.

Reports are displayed in graph format by default. For practicality, only ten devices are displayed in graph views by default. If more are available, the report includes Top 10 in the 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.

To change the number of devices displayed in network device graph view:

- Individual users can change the Maximum Number of Data Series Per Report setting in the User Preferences. (See Customizing the GUI and Information Display, page 3-8.)
- Administrators can set system-wide maximums for all users by changing the Maximum Entries for Top XX Output in the Administration > System Settings window (see Changing System Configuration Settings, page 3-17), or by using the ppm topxxsize command (see ppm tomcatver, page B-114).

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 Customizing the GUI and Information Display, page 3-8.

Note If you drill down to a report, you can refresh it by double-clicking the report category in the navigation tree. For example, if you display Resources > CPU reports, and drill down to the CPU 1 Min Utilization - Device Average Hourly report, to refresh the report, you would double click CPU.

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 the interval and duration fields **to** choose a different report interval and duration. The duration options depend on the report interval. See Table 7-1 for a list of possible intervals and durations.
- 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 Filter** to filter report information. For information, see Filtering Report Information, page 7-17.
- 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 graph legend on and off. If turned on, the graph legend appears under each graph 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 7-13.)

- 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 data for the selected report in table format.

Note To export the current report page in comma separated values format, click **Export report page as CSV file**. In table output mode, the entire table is exported to a CSV file. In graph mode, the summary table is exported to a CSV file.

- 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.

Tip Icons located on each side of the report title allow you to return to network view or explore the device on which the report is based.

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 the unnamed interval and duration fields **to** choose a different report interval and duration. The duration options depend on the report interval. See Table 7-1 for a list of possible intervals and durations.
- 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 Filter** to filter report information. See Filtering Report Information, page 7-17.
- 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 graph, 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 is displayed in full screen mode,

  For additional information about live mode behavior and requirements, see Creating Live Mode Reports, page 7-16.
- Click **Output Mode** and choose a different report output:
  - Graph (default)—Displays the top ten data series for the selected report in graphical format.

    Note Graph output provides many other customization options. For information, see Customizing Report Display, page 7-13.)
  - Table—Displays all the data series for the selected report in table format.

- Click **Sort Parameter** and choose a different report parameter to sort the report information. The parameters are based on the report.
- Click the V**iew Network Level Report** tool to the left of the report title to return to the network level report.

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

Tip Device reports provide **View Network Level Report** and **Explore Device** tools next to the report title to allow you to return to the device-level report or to display the device details page at any time.

Related Topic

Customizing General Report Settings, page 7-25

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 graph. In addition to Hide Series, clicking the 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 graph 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 11-1.

Note To display threshold on graphs, the threshold must be created in Graph mode.

- Click different report time intervals on the **Zoom** tool
- Click **Copy to Clipboard**—Copies the graph to a clipboard that is unique for each user on the server. You can copy multiple graphs 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 7-41.

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 graph to the Star Graphs tab. See Creating Custom Device Star Graphs, page 7-17 for information.

  Inside the graphs are tools you can select to modify the graph display:

- **Display Data Lines**—Allows you to display or not display lines in the graph for the following:
  - Average—Displays the average of all data series in the graph.
  - Total—Displays the total of all data series in the graph.
  - 95 Percentile—Displays the 95th percentile of all data series in the graph.
  - Forecast Values—Displays a dotted line showing projected data values based upon the date entered in the Configure Forecast Data field. The projected data is based on the graph intervals. If the graph is hourly, the projected data will be hourly. If the graph interval is daily, the projected data will be daily. This feature can be used to predict (based on past trends) when an interface or other network object will reach 100% utilization, for example, or other network data trends. Like the other aggregate lines, click once to display the Forecast Values line, click again to hide it.

    Note Average, Total, 95th Percentile, and Forecast Values are not displayed by default. If you click the option, it changes to blue indicating the line is displayed in the chart.

  - Configure Forecast Values—Allows you to configure a date or duration to which you want the Forecast Values data line projected. Clicking this option displays the Forecasting Menu dialog box. It shows the number of sample points currently in the graph, and the number of points that you can project. To enter a forecast, the graph must have a minimum of three data points. You can enter a date or duration three times the number of sample points. For example, if an hourly graph has eight sample points, you cannot enter a date or duration beyond three hours from the last graph date and time. If the interval is days with eight sample points, you cannot enter a date or duration 24 days beyond the last date in the graph.
  - Configure Y-Axis Values—Displayed when you drill down to a leaf graph, this option allows you to display a second Y axis and assign a data series to it. You can also customize the primary and secondary Y axis ranges. For example, if a KPI is generally between 99.1 and 100. you can change the primary Y axis to 99-101 to provide greater graph display variance over the default 0-100 range. Enabling the secondary Y axis allows you to view a KPI and its raw counters in separate scales. For example, you can display raw counters individually, compare them against the KPI graph, and isolate the counter causing the KPI to be lower than an expected SLA.

    Note The first data series in the leaf graph definition, which is often the KPI itself, always aligns to the left axis. The raw counters align to the right axis.

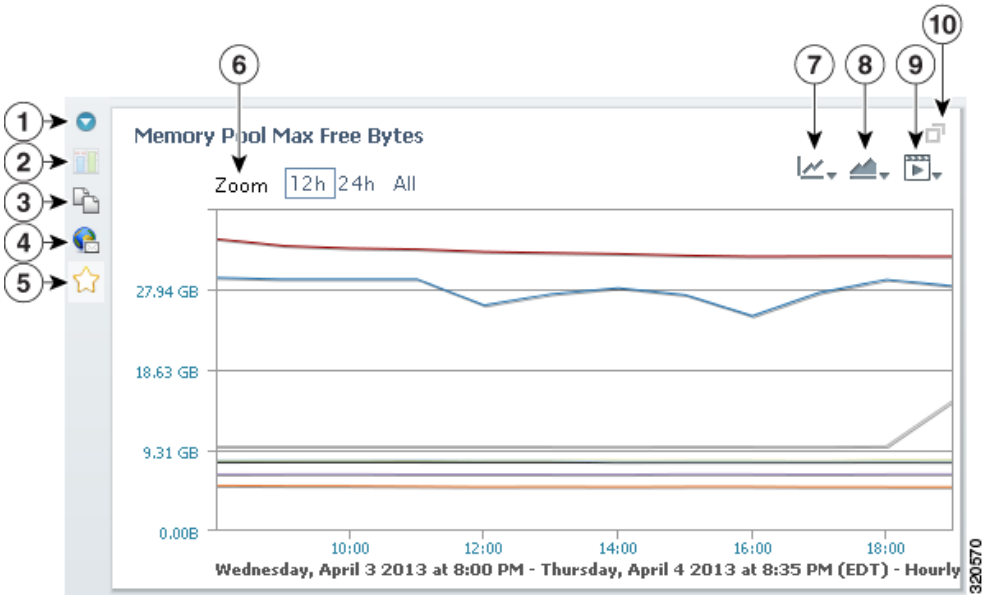
- **Change Graph Display**—Allows you to change how data is presented in the graph:
  - Line—Displays data in lines.
  - Selected Area—Highlights one series.
  - Stacked Area—Shades and stacks all series.
  - Basic Area—Displays a basic area graph.
  - Percentage Area—Displays the percentage contribution of each series as a graph area.
  - Utilization Area—Displays utilization values of each series as a graph area.
  - Toggle Time Bar—Allows you to display a time bar within the graph.
  - Toggle Vertical Graph Grid—Displays or hides a vertical grid.

- Toggle Multiple Axes—In merged graphs, allows you to switch between the axis of each chart. (The option does not appear in single graphs.) For information about merging charts, see Merging Graphs in Views, page 7-48.
- Pie—Displays a pie graph with the average value of each series.
- Percentage Column—Similar to the Percentage Area option, but displayed in columns.
- Column—For leaf graphs, that is, for the lowest report level, displays basic bar columns. Not available for other level graphs.
- Stacked Column—Works same as StackedPercentageColumn in report XML but sets chart type to Stacked Column type.
- Bar—Displays the average value of each series. The vertical axis is the series list, and the horizontal axis displays the average values of those series for the specified interval.
- Utilization Column—Displays the utilization of each series as bar sequence.
- Toggle Logarithmic Axis—Moves the axis to logarithmic scale, that is, displays a quantity value using intervals corresponding to orders of magnitude rather than a standard linear scale.
- ToggleVertical Graph Grid—Displays vertical grid within the graph.

Tip Clicking an individual data point in a graph displays the data series summary table view.

- **Export Chart**—Downloads the graph to your computer in one of the following formats: PNG, JPG, PDF.

Figure 7-5 Graph Display Options



1	Hide Row	**6**	Zoom
2	Toggle Related Threshold	**7**	Aggregate lines

3	Copy to Clipboard	**8**	Graph style options
4	Email report	**9**	Export chart options
5	Add to Star Graph	**10**	Show Graph in Fullscreen

You can control the display of report data values through settings in the User Preferences window. For example, you can choose whether you want the minimum, maximum, average, total, current, standard deviation, and variance 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, current, standard deviation, and variance values can be displayed. 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. For information about changing user preferences, see Customizing the GUI and Information Display, page 3-8.

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

The time span bar is another option you can use to reduce the time span within a graph so you can view intervals of interest in greater detail. By default, the time span bar is displayed in all full screen graphs. However, it can be enabled so that it appears on all report graphs.

To display the time span bar, click **Change Graph Display** in the upper right corner of the graph and click **Toggle Time Bar** to display or hide the time bar. You can also enable it by default by selecting Enable Graph Time Span Bar in User Preferences. These and many other options are provisioned in the User Preferences window. For information, see Customizing the GUI and Information Display, page 3-8.

Creating Live Mode Reports

Prime Performance Manager live mode reports have 15-second, 30-second, or one-minute polling. To start a live mode report, navigate to the device level report and click the **Go Live** tool on the report toolbar. Live mode reports share presentation and tools with other Prime Performance Manager reports, but have certain unique requirements and behaviors.

First, you can only run live mode for device-level reports. You cannot run it for network, group, and tenant reports, or for reports using CSVPoll, flowPoll, DCMPoll, sysDataMetrics.xml, sysPollerMetrics.xml, and ping.xml. In addition, some reports, such as ICMP Ping, do not support 15-second polling. If live mode polling is not available for a report, the Go Live tool is not displayed in the report toolbar.

When you start live mode polling, an End Live Mode tool appears at the top of the report window. Use this tool to stop live mode polling. Next to End Live Mode is a field that allows you to change the report polling frequency from 15 seconds to 30 seconds or one minute.

Tip Should data not appear to be correct, or if a time out appears in the report, increase the frequency. Time outs occur when the device response time is greater than the selected polling frequency.

You can display live mode reports in table or graph format. However, to change the report format, you must return to the network level report, change the format, then click **Go Live** to start live mode in the new report format.

Live mode data is saved for three days. Report export (CSV, JPG, PNG, PDF) and display options available for longer-period reports are available for live mode reports. For information, see Customizing Report Display, page 7-13.

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, for example if you click the View Network Level Report or Explore Device tools next to the report title, live mode stops. To start it, return to the device report and click the **Go Live** tool.

Some devices take longer than 15 seconds to poll. If so, Prime Performance Manager sends messages indicating the device is not responding. If the device remains unresponsive, Prime Performance Manager increases the polling interval until it finds an interval that is successful. It attempts each interval two times. If data is not recovered at 1-minute polling, live mode exits.

Creating Custom Device Star Graphs

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

To create a custom device star graph:

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 Reports menu, display the report containing the data you want to add to the custom view. You can also choose a dashboard by clicking **Dashboards** and selecting a dashboard.

The report (or dashboard) is displayed in graph output format by default.

Step 4 Navigate to the graph 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.

Step 5 Repeat Step 4 until you have added the graphs that you want to the Star Graphs tab. You can navigate to different reports (or dashboards) and select graphs 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 graphs in normal report view. View menu bar (see Figure 7-2 on page 7-5) actions are available.

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 graph you want to delete. You can also remove a star graph report by unchecking the star of the report on the page where it was first starred.

Filtering Report Information

Prime Performance Manager provides many methods for displaying report information in different ways. Many (but not all) reports display one of the following options:

- Sort by—Provides a second report sorting layer in addition to sorting available through the report data columns. You can effectively sort the report by the data series first, then sort by individual parameters within the data series.
- Filter by/Sort by—Filter by (table reports) and Sort by (graph reports) appear in reports that have many data items, such as small cell reports. The option is a convenience to make sorting the report easier. Choosing a Filter by option sorts the report in descending order by the selected data item.
- Group by—Appears in small cell group reports. It allows you to filter the report by small cell inventory group. Prime Performance Manager creates the groups dynamically based on inventory data retrieved from RMS servers. Selecting **None** displays all small cell inventory groups,

In addition to sorting and filtering data by report menu bar selections, you can filter report information to display data within specific parameters, for example, to display devices containing certain letters in the device names, or a down percentage KPI higher than a specific number. You can filter reports based on report columns or by groups if groups are defined,

To filter a report, display the report and click the **Filter** tool on reports toolbar. The Report Filter dialog box, shown in Figure 7-6, allows you to filter reports in one of several ways.

- Enter one or more filter rules then click **Filter Report** to quickly filter a report.
- Save a filter for future use by entering a filter name in the Filter Name field and clicking **Save**.
- Load a previously-saved filter by clicking **Load Filter**. Prime Performance Manager always runs the filter rules currently displayed in the dialog box. You only click Load Filter when:
  - No filters are displayed and you want to load a previously-saved filter,
  - A filter is displayed and you want to switch to another saved filter.

Creating Filter Rules

Filter rules are added by clicking the **Add a New Filter Rule** tool. In the Report Filter, shown in Figure 7-6, you can add multiple rules to a filter using the following drop-down fields:

- First drop-down—Lists all filterable report columns plus Device Type and Group Definition items. If you choose a report column, the report is filtered by that column. If you choose Device Type, you can filter the report by device types. If you choose Group Definition, you can filter the report by a defined group. (For more information about groups, see Creating and Managing Report Groups, page 7-52.)
- Second drop-down—Displays the operations permitted for the report column selected in the first drop-down. The available operations depend on the data type of the column selected in the first drop-down:
  - Device and Device Type—Equals, Does Not Equals, Begins With, Ends With, Contains, Does Not Contain.
  - Group, String, InetAddress—Equals, Does Not Equals, Begins With, Does Not Begin With, Ends With, Does Not End With, Contains, Does Not Contain.
  - Float, Timestamp, Double, Integer, Long, Short, Util—Equals, Does Not Equals, Greater Than, Greater Than or Equal To, Less Than, Less Than or Equal To.
  - Group Definition—Equals
- The third drop-down is where you enter the value to be used with the report column and operator to filter the report. For example, if you want to display only GigabitEthernet interfaces, you would enter the following values:
  - First drop-down: **Interface**
  - Second drop-down: **Contains**

  - Third drop-down: **GigE**

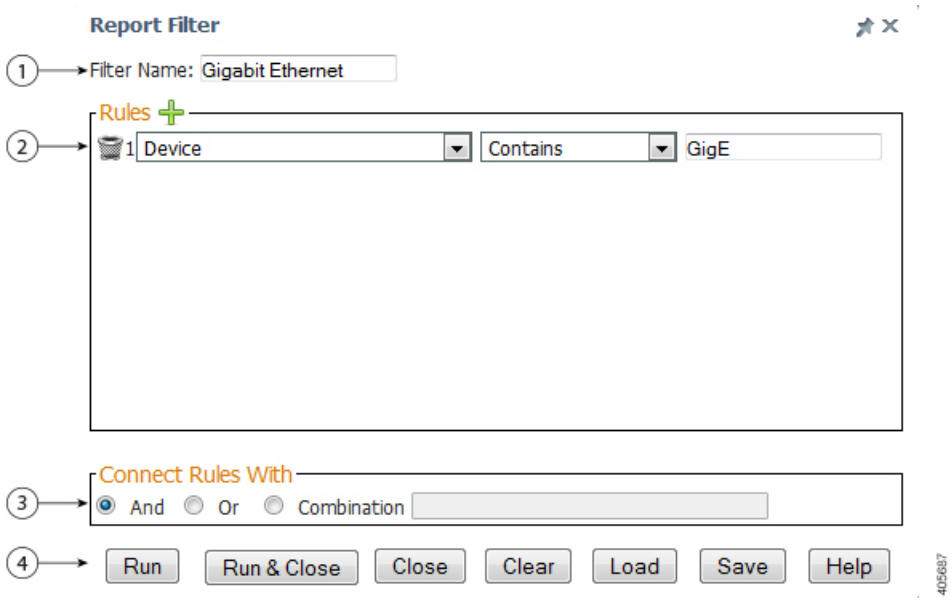
  If you choose Group Definition, it displays a list of defined groups. If you choose a group with more than one process item, a fourth drop-down is displayed allowing you to pick the process item to use with the group.

- Connect Rules With—After creating the filter rules, you can set the relationships between them:
  - And—If selected, every rule must apply before results are returned.
  - Or—If selected, only one rule needs to apply before results are returned.
  - Combination—Allows you to set the rule relationships using a combination of connectors: and, or, not. Examples: 1 and (2 or 3); 1 and not (2 or 3).

Report Filter actions:

- Run—Runs the filter against the report but leaves the Report Filter displayed.
- Run & Close—Runs the filter against the report and closes the Report Filter
- Close—Closes the Graph Series Editor and does not save any changes,
- Clear—Removes all content from the Graph Series Editor.
- Load—Loads a previously saved filter.
- Save—Saves the current filter

Figure 7-6 Report Filter Dialog Box



1	Filter name	**3**	Filter join options
2	Filter rules	**4**	Filter actions

Exporting Report Data to CSV Files

You can export Prime Performance Manager report data to CSV files, which you can display in a spreadsheet or database management application for further review and analysis. The data exported depends on the output mode. In Graph mode, the summary table is exported. In Table mode, the detailed data table page is exported.

To export a report to a CSV file:

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

Step 2 Navigate to the report you want to export to CSV.

Step 3 On the report toolbar, click **Export Report Page as CSV.**

Note Report Page only applies to Table view. Only the table page currently displayed is exported. If you want to export all the Table view data, set the page size to the maximum, export each page, then merge the files in your spreadsheet or database application.

Step 4 In the Export Report Columns to CSV dialog box you can do any of the following:

- By default, all report columns are selected for export. To remove a column, select it and click **Remove**. The column moves to Available Columns. To add the column, select it and click **Add**
- To change the order in which columns appear in the CSV file, select the column and click Move Up or Move Down. Columns at the top appear first in the CSV; columns at the bottom appear last.
- To save the customized columns for future exports, click **Save**.
- To load a previously-saved column filter, click **Load**.
- To remove all non-key data fields, click **Remove All Data Fields**.

Note Columns in bold are the table keys.

Step 5 When finished, click **Export** to export the data and leave the dialog displayed, or **Export and Close** to export the data and close the dialog.

Emailing Reports

You can set up schedules to have Prime Performance Manager automatically email report, view, or dashboard graph image to individuals. The emails can be sent at regular intervals on an ongoing basis, or they can be sent for a set number of times. You can also end the mail one time immediately instead of on a schedule.

To email reports, complete the following procedures:

- Creating a Mail Report, page 7-21
- Managing Mail Reports, page 7-24

Creating a Mail Report

You can create report emails for report graphs or tables in the views, dashboards, network or device reports, or star graphs. Creating a report email creates a schedule for sending a report, view, or dashboard graph to individuals by email. Graphs can be included as attachments or embedded in the email in PNG, JPG, GIF, or PDF format.

To create a report email:

Step 1 Verify the SMTP server is configured for Prime Performance Manager:

a. From the Administration menu, choose **System Settings**.

b. In the System Configuration Settings, verify an SMTP server is entered in the SMTP Mail Server field. If not, provision the mail server that Prime Performance Manager should use for outgoing emails. This can be the mail server IP address or host name. In many cases, you can enter **localhost.** If needed, consult your network administrator.

Step 2 From the Performance menu, choose **Reports, Views**, or **Dashboards**.

Step 3 Navigate to the report containing the graph(s) for which you want to create an email report.

Step 4 Perform one of the following, depending on what you want to email:

- Entire report—Click **Email Report** on report toolbar.
- An individual report graph—Click **Email Report** on the vertical toolbar to the left of the graph.

Step 5 In the Email Report dialog box, complete the report fields.

Email Configuration—Provides the email address and subject:

- Email From Address—Enter the email address that you want used as the report sender. This is the address to which replies are sent. You can enter any legitimate email address. However, the intent is for the user creating the report email to enter their email address or an alias to which replies can be sent, for example, ppmreports@mycompany.com.

  Note If a global email from address is configured, that address automatically populates the Email From Address field. You can remove or edit the global address, however. The global email from address is configured in Administration > System Settings > System Configuration.

- Email To Addresses—Enter the email address(es) of the individual(s) to whom you want to send the report. The addresses must be legitimate. If you enter multiple addresses, separate the addresses with semicolons and no spaces. You can enter an email alias or list as long as it is recognized by the email server.
- Email Subject—Is the subject line in the email that is sent. It is required. You can enter variables that will list the report and server names in the email subject:
  - $name—The ReportMail name.
  - $server—The gateway server name.

  For example, if your gateway server is gateway_123, your ReportMail is named SampleReport, and you type $name from $server in the Subject field, the email subject will be SampleReport from gateway_123.

Note $name only applies to scheduled report emails. If you click **Send Now**, $name is replaced with "current_state" indicating the report email current state is the time you clicked Send Now.

Output Configuration—Defines the report output and email delivery.

- Output Format—Enter the format in which you want the graph to be sent. Options include PNG (default), JPG, and GIF graphic formats, as well as PDF and CSV. File sizes vary, In one sample report, file sizes were:
  - PNG: 202.5 KB
  - JPG: 209.1 KB
  - GIF: 91.1 KB
  - PDF: 45.6 KB
  - CSV: 42.2 KB

  PNG produces the best overall results, depending on the graph complexity, so is the format you should generally use. PDF is not recommended for complex reports or views with multiple graphs, GIF image quality is lower overall.
- Embed Image—If checked, the image is embedded in the email. If not checked, it will be attached to the email.
- Width—If you want to change the width, enter it in this field. The default is 1280 pixels.
- Height—If you want to change the width, enter it in this field. The default is 1024 pixels.

Note Embed Image, Width, and Height apply only to PNG, GIF, and JPG output formats.

Note The width and height do not guarantee the image size will match exactly. However, the resulting image will generally be close to the width provided and the height will vary depending on the image itself.

Schedule Configuration—Allows you to define a report email schedule:

- Scheduled—If selected, displays fields that allow you to schedule the timeframe and frequency to email the report. If you do not want to schedule the report, you can click **Send Now** to send the report immediately.
- Name—Allows you to add additional information to distinguish the report when viewed in the Report Mail Editor. Spaces and special characters are not allowed, with the exception of underscores and hyphens, which are allowed.
- Enabled—If checked, enables the email report. If not checked, the email will not be sent. This parameter allows you to create the report and enable it at a later time. You can also disable the report email temporarily at a later point.
- Repeat—Enter the interval at which you want the email report to run:
  - Hourly
  - Daily
  - Weekly

  - Monthly
  - Yearly

- Frequency—Sets the number of times the report should run for the selected Recurs Type. For example, if you select a recurs type of hourly and enter a frequency of 4, an email will be sent every four hours. The Start Date and End Date are optional fields that further refine the time that emails are sent. If you enter a start date, no emails are sent prior to that date. Similarly, if you enter an end date, no emails are sent after that date. If you do not enter dates, no date restrictions are applied.
- Start Date—Enter the report start date by clicking the field and choosing the start date from the calendar.

  Beneath the Start Date, choose the days you want the report run. The days selected are another way to restrict when emails are sent. If the day is selected, emails are sent. If the day is not selected, no emails are sent.

  In other words, all selected criteria must be met for an email to be sent. The day must be selected, the date has to be in range (if dates are specified), the time of day has to be between the times specified (if they are not set to the same time).
- End Date—If you entered a start date, enter the end date by clicking the field and choosing the end date from the calendar.
- Begin Time—Enter the report start time: hour (24-hour clock):minute
- End Time—Enter the report end time: hour:minute

Note If both times are set to 0:00, no time of day restriction is applied.

Note If the report mail runs near the top of the hour, which is the default, the Prime Performance Manager will not have time to process all the last time interval statistics. If recipients receive an email at, for example, 10:04. The report will include hourly data up to 9:00 but not 10:00 because data collecting and processing takes time. Adding an offset to the start and end times can produce better results. If the report email is scheduled for ten minutes after the hour, time is allocated for the data to be processed. For example, if you set the Start Time and End Time to 12:10, the report mail will run at 10 minutes after the hour, every hour and have sufficient time to collect statistics for the 10:00-11:00 interval.

Step 6 Perform one of the following:

- If you are not scheduling the email, click **Send Now**.
- If you scheduled the email, click **Save**.

  The report is added to the Network Report Mail Editor screen. To view it, from the Network menu, choose **Report Mail Editor**.

Related Topic

Managing Mail Reports, page 7-24

Managing Mail Reports

You can manage mail reports from the Network Report Mail Editor. The editor displays all the mail reports that have been created in Prime Performance Manager and allows you to view, edit, enable, disable, and delete individual reports.

To manage email reports:

Step 1 From the Network menu, choose **Report Mail Editor**.

Step 2 The Network Report Mail Editor displays the following information for each mail report:

- Name
- From
- Mail To
- Output (format and dimensions)
- Recurs Type/Frequency
- Applicable Days
- Start and End Dates
- Start and End Times
- Report URL

The Report URL provides a link you can click to view the report. For other parameter descriptions, see Creating a Mail Report, page 7-21.

Tip Hovering over a row with your mouse displays a tool tip that shows the text entered in the Subject field when you created the scheduled the email.

Step 3 To enable, disable, or delete one or more email reports:

a. Choose the email report(s) that you want to enable, disable, or delete. (To choose multiple thresholds, press the **Shift** key to select contiguous thresholds, or **Ctrl** to choose noncontiguous thresholds.

b. From the Actions menu, choose **Enable Selected Report Mails**, **Disable Selected Report Mails**, or **Delete Selected Report Mails**.

Prime Performance Manager will update the email report information.

Step 4 To perform other email report actions, from the Action column, perform any of the following:

- Click **Duplicate Report Mail** to create a new mail report based on an existing one.

  The Duplicate Report Mail dialog appears. All entries are identical to the original report, but "_duplicate" is appended to the report name. Edit any parameter, including the provided default name, which must be should be unique, then click OK to create the new report. For parameter descriptions, see Creating a Mail Report, page 7-21.

- Click **Edit Report Mail** to display and edit the mail report parameters. Only the report name cannot be edited.
- Click **View Report Mail** to display a read-only view of the report parameters.

Customizing General 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 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 7-2 for general setting descriptions.

Note The Aging Settings area sets the global report aging values. For information about setting report aging, see Customizing Report Aging Settings, page 7-28.

Step 3 When finished, return to the previous Prime Performance Manager window.

Step 4 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 7-2 General Report Settings

Field	Description
Reports Directory	Directory where Prime Performance Manager stores exported reports. The default is /opt/CSCOppm-gw/reports. You cannot edit this field. This is the directory of where we store exported reports. To change the reports directory, use the ppm repdir command. See ppm repdir, page B-82.
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 Customizing Individual Report Settings, page 7-27.) 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-17.
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.

Customizing Individual Report Settings

While you can apply report settings to all Prime Performance Manager reports (see Customizing General Report Settings, page 7-25), 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 device polling interval required for these report 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/Group Status**.

The Administration Reports Status table 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 Report setting changes are implemented immediately. If you change the settings while users are active, notifying them of the changes will avoid surprises. To communicate system information to online users, see Sending Announcements to Online Users, page 6-25.

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 7-3 lists the report data options.

Table 7-3 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.

Note You can use the ppm statreps command to modify the report statusD. For information, see ppm statreps, page B-105.

Customizing Report Aging Settings

Prime Performance Manager reports are retained for a specified number of days, after which they are discarded to ensure disk space is available for new reports. You can modify the aging value at the global and individual report level, as described in the following procedures:

- Customizing Global Report Aging Settings, page 7-29
- Customizing Individual Report Aging Settings, page 7-30

Customizing Global Report Aging Settings

Modifying report aging at the global level sets aging values for all reports and CSV entries at the specified report intervals: 1 minute, 5 minute, 15 minute, hourly, daily, weekly, monthly. These values apply to all reports unless you modify aging at the individual report level.

To modify report aging settings at the global level:

Step 1 From the Administration menu, click **Report Custom Aging**.

Step 2 In the Report Custom Aging window, click a field and edit the aging value for the report, as needed. See Table 7-4 for aging setting descriptions.

Step 3 When finished, from the toolbar click **Save Custom Report Aging Settings**.

Step 4 Return to the previous Prime Performance Manager window.

Step 5 To display the report setting changes, 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 7-4 Global Report Aging Settings

Field	Description	Default (Days)
Reports	Displays a list of all reports in the report table.	n/a
1 Minute	Database aging value for 1-minute statistics.	2
5 Minute	Database aging value for 5-minute statistics.	4
15 Minute	Database aging value for 15-minute statistics.	7
Hourly	Database aging value for hourly statistics.	14
Daily	Database aging value for daily statistics.	94
Weekly	Database aging value for week statistics.	730
Monthly	Database aging value for monthly statistics.	1825

Customizing Individual Report Aging Settings

Modifying report aging at the individual report level sets aging values by report table and report interval. Each report table can contain one or more individual reports. Each value saved through Prime Performance Manager GUI saves two entries in the properties file: one used to age the database data associated with the table and one to age the CSV data.

Aging values that you save in the Report Custom Aging window will be the same for both web reports and CSV entries. However, if you want them to be different, you must manually change the CSV_ entry for the table and interval in the ReportAges.properties file.

For report table data, any value saved on the Report Custom Aging window overrides the global value set for the same interval on the Report/Group Settings tab. The custom value is used regardless of whether the aging value is greater than or less than the global value.

However, for CSV data, the lowest value wins. If the global setting is two days, and the custom report aging setting is three, the data will still be deleted after two days. In other words, the custom value only takes effect if it is less than the global value.

To customize individual report aging settings:

Step 1 Get the report ID for the report you want to modify:

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

b. Display the report whose aging you want to change.

c. Click the **Report Help** tool at the far right of the report toolbar.

The report definition file is displayed.

d. Scroll through the report definition file until you come to the Web Report ID.

e. Record the report ID, then close the definition file.

Step 2 From the Administration menu, choose **Report Custom Aging**.

Step 3 In the Search field of the Report Custom Aging window, enter the report ID whose aging you want to modify, then click **Search**.

The report is displayed.

Step 4 Click the tool under **Reports** to verify the report is the one you want to modify.

The WebReports for Base Table [Report ID] window lists the reports and report category that are associated with the report ID. Report tables can contain multiple reports. They can also contain the associated CSV processor.

Step 5 As needed, modify the aging values for any or all of the following report intervals: 1 Minute, 5 Minute, 15 Minute, Hourly, Daily, Weekly, and Monthly.

By default, report aging values are set to the values assigned in the Report Settings window. (See Customizing Global Report Aging Settings, page 7-29.) These values are displayed in light grey text. Customized aging values are displayed in black text. All aging values represent days.

Step 6 From the toolbar, click **Save Custom Report Aging Settings**.

The new report aging values are saved.

Step 7 Repeat Steps 1 through 6, as needed, to modify additional reports.

Tip Alternatively, you can go directly to the Report Custom Aging tab and use the Search field to find the reports you want to modify. For example, you can enter a technology acronym, such as DWDN, CGN, or ICMP to get a list of report tables containing that technology, then use the Child Reports look up to narrow the list down to the reports whose aging you want to modify.

Customizing CSV Export Settings

You can export reports that have CSV enabled (see Customizing General Report Settings, page 7-25) by displaying the report and clicking the **Export Report Page as CSV File** tool on the report toolbar. (For a description of the report toolbar, see Displaying Reports, page 7-1.)

You can change some attributes of the exported CSV file by changing settings in the User Preferences window, or by modifying properties the report.properties file. Properties that you can change in User Preferences include:

- Export All CSV Data With Report Export—Exports all CSV data with report exports.
- CSV File Name Date Format—Sets the date format used in CSV file names, either yyyy-MM-dd-HH-mm-ss (year-month-day-hour-minute-second) or MM-dd-yyyy-HH-mm-ss (month-day-year-hour-minute-second).

For more information about user preferences, see Customizing the GUI and Information Display, page 3-8.

You can also modify the following parameters by editing report.properties file located in /opt/CSCOppm-unit/properties:

- RPT_CSV_NAME_FORMAT—Defines the timestamp string format in report titles. For example, if you enter yyyy-MM-dd-HH-mm, the exported 15-minute report title will be something like VPN_CONNECTIONS.2013-11-18-06-45.csv and an hourly report title will be something like vCenterNodeTotalCPU.2013-11-18-07.csv. The title timestamp string has the same format as the parameter with different precisions based on the report interval. To avoid file naming errors, special characters are not allowed in the title except for dash ("-"). For example, if you enter HH:mm yyyy/MM/dd, special characters are automatically replaced by a dash. The actual format will be HH-mm-yyyy-MM-dd. Furthermore, the value you enter must be able to be parsed as a Java SimpleDateFormat. If Java cannot recognize the format, it uses the default yyyy-MM-dd-HH-mm format.
- RPT_NAME_COL_TITLE—Defines the timestamp string format under the Timestamp column in the report. The entry must be able to be parsed as a SimpleDateFormat in Java. If not, an error occurs and the report export will fail.
- RPT_NAME_COL_NAME—Defines the Node column name. Many exported reports have a Node column. If you want to use a different name, enter it here. For example, if RPT_NAME_COL_NAME = VNE, the column name will be VNE instead of Node.
- RPT_DELIM—Defines the exported report delimiter. If you open any export report, you can see the contents in one row, for example:

  11-18-2013 07:00,ems3845a.cisco.com,Voltage 3,normal,normal,2525,2525,2250,2525,2750

A comma, the default, is the delimiter used to separate contents in the different cells. However, you can specify other values, for example, if RPT_DELIM=!, the file contents would be separated by !, for example:

11-18-2013 07:00!ems3845a.cisco.com!Voltage 3!normal!normal!2525!2525!2250!2525!2750

Device Report Capability Polling

Prime Performance Manager polls devices to see what MIBs they support, then identifies the reports that can be generated from each device. 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 only occurs for device reports that are enabled at the master or individual device report levels. When you display individual device reports, only reports enabled at the master or individual device report levels are displayed.

For performance, keep capability polling optimization enabled. However, in certain scenarios, for example, in labs or testing environments where device configurations and capabilities change frequently, you can disable capability polling optimization with the ppm optimizecapabilitypoll command. This allows you to see what reports could be enabled for a device as well as the reports that are enabled. For information, see ppm optimizecapabilitypoll, page B-66.

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 Logging In as the Root User, 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

- Assigning Devices to Report Policies, page 7-34
- Editing Report Policies, page 7-33
- Assigning Devices to Report Policies, page 7-34

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 Complete the “Editing Report Policies” procedure on page 7-33 to edit the reports and report intervals that you want for the new report policy.

Editing Report Policies

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**.

The Administration Report Policies tab displays the existing report policies.

- Policy Type—Displays the policy type:
  - Blank—The policy was created by Prime Performance Manager and cannot be deleted.
  - User Created Policy— The policy was created by users and can be deleted.
  - Policy in Use—The policy has devices associated with it and cannot be deleted.
- Report Policy Name—The report policy name. Clicking the policy link takes you to the edit policy window.

Step 3 Scroll to the device type group you want to modify and click the report policy link.

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
  - DB

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.

Tip To return the report policy to its default settings, click **Reset Report Settings to the System Default** on the Edit Report Policy toolbar.

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

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 Prime Performance Manager 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 only appears after you modify reports for a specific device. The 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. This option only appears after you modify reports for a specific device.
- Default—Assigns the device(s) to the default Prime Performance Manager report policy.
- Custom groups—If you created report policies, they are displayed.

Step 6 Click **OK**.

Displaying Report Definitions

Prime Performance Manager covers 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 1.7 Integration Developer Guide*.

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

Sharing Report and Dashboard URLs

Clicking **Page Links** from either the Reports or Dashboard menu bar, allows you to retrieve URLs for a particular report or dashboard that you can share with applications integrated with Prime Performance Manager or with other users. The following options are available:

- **REST API**—Lists the base URL used by a Prime Performance Manager Representational State Transfer (REST) client to launch the selected report or dashboard. By default, this is the URL that is first displayed after you click either **Get Cross Launch Information** or **Get Page Links**. For more information about the REST API and customizing this URL, please view the Prime Performance Manager 1.7 REST API Guide.

- **Crosslaunch API**—Lists the URL used by an integrated Cisco Prime application (such as Prime Central) to launch the selected report from that application. Note that this option is not available for Prime Performance Manager dashboards.
- **Permalink**—Lists the URL that launches only the selected report or dashboard, without the main Prime Performance Manager menu and navigation area. Use this option to easily share particular information with another user.

Note that the displayed link (regardless of the option you select) is automatically selected, so you can quickly copy and paste the link as needed.

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
- Compute
- IP Protocols
- IP QoS
- IPSLA
- Network Health
- Resource
- Response Time
- Server Health
- Server Statistics
- Transport
- VPDN
- Video Broadcast
- Virtual Services

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 tomcatver, page B-114.

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 area, enabled dashboards are indicated with a green circle next to the title. Disabled dashboards display a red circle next to the title.

Editing Dashboard Display

You can change the dashboard information display using options in the Dashboard menu bar. The following menu bar items are displayed in individual dashboards:

- Interval—Dashboard intervals are: 1 Minute, 5 Minutes, 15 Minutes, Hourly, Daily, Weekly, Monthly.
- Duration—Next to the Interval field, the Duration field allows you to choose the dashboard report duration. The duration options depend on the dashboard report interval:
  - 1 Minute—Custom, last hour, previous hour, last 6 hours, work shift, today, last 24 hours, yesterday, last 3 days.
  - 5 Minute—Custom, last hour, previous hour, last 6 hours, work shift, today, last 12 hours, yesterday, last 24 hours, last 3 days, last 7 days.
  - 15 Minute—Custom, last hour, previous hour, last 6 hours, work shift, last 12 hours, today, last 24 hours, 3 days, 7 days.
  - Hourly reports—Custom, work shift, last 12 hours, today, last 24 hours, yesterday, last 3 days, this week, last 7 days, previous week.
  - Daily reports—Custom, this week, last 7 days, previous week, last 14 days, last 21 days, this month, last 30 days, previous month, last 60 days, last 90 days,
  - Weekly reports—Custom, last 4 weeks, last 8 weeks, last 12 weeks, lst 6 months, this year, last 1 year, previous year.
  - Monthly reports—Custom, last 3 months, last 6 months, this year, last 1 year, previous year.
- Columns—Change the number of dashboards columns that are displayed, from one to three.
- 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 graph format. For readability in this format, only the top *nn* items are displayed.
- Table Mode—Displays all the dashboard parameters in table format.
- Show Graph Legends—For reports displayed in graph format, turns the graph legend on and off.
- Toggle Compact Mode—Toggles the display of the Zoom, Aggregate Lines, Graph Styles, and Export Graphs tools displayed inside graphs. Additionally, the graph border is hidden and graph title reduced in size. Using this option reduces the overall size of the graph and is useful when screen real estate is needed.
- Merge Selected Graphs—Allows you to merge two or more selected graphs.
- Disable Automatic Updates—Prevents the dashboard from being updated; click **Enable Automatic Updates** to allow updates. This function is provided when continual, automatic updates are not needed.
- Email Report—Emails the report to selected users. For information, see Emailing Reports, page 7-20.
- Process Dashboard—Updates the dashboard after you modify any parameters in the menu bar.
- Open Dashboard in New Tab—Opens the dashboard in a new tab.
- Get Page Links—Retrieves the URL used to launch the selected dashboard from a Prime Performance Manager REST client or on its own in a browser. See Sharing Report and Dashboard URLs, page 7-35 for more information.
- 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.

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:

- Click **Interval** and choose a different interval: 1 Minute, 5 Minutes, 15 Minutes, Hourly, Daily, Weekly, Monthly.
- Click **Duration** and choose a different time period for the dashboard: 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 graph format.
- Click **Table Mode** to display all the dashboard parameters in table format.

Note The View Graph 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.
- Toggle Compact Mode—Toggles the display of the Zoom, Aggregate Lines, Graph Styles, and Export Graphs tools displayed inside graphs. Additionally, the graph border is hidden and graph title reduced in size. Using this option reduces the overall size of the graph and is useful when screen real estate is needed.
- Email Report—Sends the dashboard report in an email. See Emailing Reports, page 7-20.

Step 6 When finished, click **Process Dashboard** (green arrow) to refresh the dashboard 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 graph 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 graph 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 7-39.)

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:

View Permissions

Views allow individuals to create their own perspective on the network. Whether other users can view or edit an individual's view depends on multiple factors, including user permissions, roles, and abilities.

Permissions

Views have two permissions:

- Edit.Other.Views—Can edit any view in any way, and can view all views regardless of visibility settings. This permissions is effectively root privilege for views.
- Edit.Views—Can create private and group views. If it is private, then only that user can view or edit it. If it is a user group, then only members of the user group can view or edit it.

Roles

User roles affect view permissions:

- System Administrator—Has the Edit.Other.Views permission.
- Views Administrator—Has the Edit.Views permission. Can create new private and group views. Cannot see other groups or private views owned by other users. This user role can be assigned to a customer to allow them to create, and edit views without providing access to other Prime Performance Manager features.
- Basic User/Network Operator—Can only view the views for which they are given permission. They cannot create or edit views.

Abilities

Users can have view and/or edit abilities on a particular view. They can also have the ability to create views, and can own views:

- View—The view appears on the main view screen for a user, and they can open it. No controls to paste, delete, or reorganize the view are available.
- Edit—The user can add and delete subviews, paste graphs into the view, change the view name, and create merged graphs. They cannot change the ownership settings, or the editable/visibility settings.
- Owner—The user has edit privileges on any views they own. They can also change the visibility and editable settings. (If the user is a view administrator, they can only choose private or group views.)
- Create—The users can create new views with themselves as the owner.

View Actions

View actions are divided into three areas:

- Public—View available to all users.
- Private—View available only to the view creator.
- Group—View available only to members of a user group

View actions include:

- Create Root View—Can only be performed by the system administrator.

The system administrator, view owner, and group members can perform the following actions to public and group views:

- Edit Root View
- Delete Root View

- Move Root View
- Open Root View
- Create Subview
- Edit Subview
- Delete Subview
- Move Subview

Note If the view edit privilege is set to Group, any group member can delete any subview or view, even if they are not the view owner. For example, if User A and User B are in the same group with edit privileges, User A can create a view and User B can delete it.

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 graphs 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 **Create a New View**.

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

- View Name—Enter the custom view name.
- Editable—Choose one of the following options to set the users who can edit the view.
  - Private—Editable only by the view creator or System Administrator users.
  - Public—Editable by any user.
  - Group—If the user creating the view is a System Administrator, the view will be editable only by users who are members of the user group(s) selected under Groups. If the user creating the view is a Views Administrator, the view will be editable to whatever group the Views Administrator is currently in.
- Visible—Choose one of the following options to set the visibility of the view to other users:
  - Private—Viewable only by creator or System Administrator users.
  - Public—Viewable by any user
  - Group—If the user creating the view is a System Administrator, the view will be viewable only by users who are members of the user group(s) selected under Groups. If the user creating the view is a Views Administrator, the view will be visible to whatever group the Views Administrator is currently in.

Note The Editable and Visible parameters are set at the top view level. If you create a new subview, it will inherit the Editable and Visible settings from the parent view.

- Device—If you want to associate a device to the view, enter the device hostname or IP address. Associate a device with a view that allows you to see device information from within the view including device details, reports, alarms and events.

Tip As you enter text, the field alphabetically matches existing device names in your network If you know the first letters of the device name, you can choose from devices presented in the list. You can also enter any substring of the device name or IP address. to match. For example, if all devices were named SOME_BUILDING-boston, you could enter "boston" and get a list of devices with boston somewhere in its name.

- Go to New View—Check this box if you want to go straight to the new view after it is created. That is, you want to create the view and begin editing it.

Step 4 Click **OK**.

If you checked Go to New View, the new custom report view appears in the View Editor window with the text, "No entries found." If you did not check this option, the window displays the last-displayed view.

Step 5 To add data 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 7-17.

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 Graphs from Clipboard**.

You can copy multiple graphs to the clipboard before you need to click the Paste Graphs from Clipboard. so you do not need to go back and forth. For example, you can copy six graphs 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 7-44.

Adding Views to the Navigation Tree

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

- Users with the correct permissions can manually create multiple views.
- Prime Performance Manager includes:

  - A special Data Center view that is built and maintained by Prime Performance Manager. (For information about the Data Center view, see Displaying Data Center Reports, page 8-1.)
  - A TCA view that is automatically generated. Prime Performance Manager periodically grabs all the active TCAs and creates a view hierarchy of the graphs associated with the top TCAs across the network.
- Users with the edit view privilege (System Administrator and Views Administrator) 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.

Views represent the way you want to see the devices and reports are laid out hierarchically. When you select Views in the navigation tree, a list of views you are allowed to see appears 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 must only perform this step once. 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 considers 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 pencil located to right of the view title.

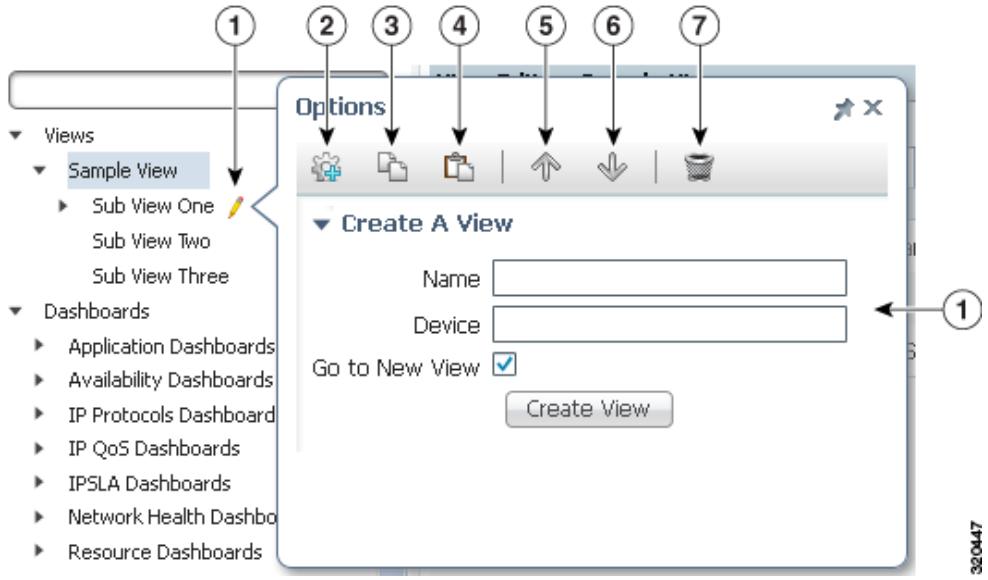
Step 2 From the Options menu (Figure 7-7), click **Copy View**.

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 under the view you selected.

Note The options icon allows you to perform other view actions including edit, delete, and moving views.

Figure 7-7 Copying and Pasting Views



1	Options icon	**5**	Move View Up
2	Edit View	**6**	Move View Down
3	Copy View	**7**	Delete view
4	Paste View		

To modify the copied view, see Modifying Custom Report Views, page 7-44 and Editing Views, page 7-49.

Modifying Custom Report Views

Your ability to modify custom views depends upon the permissions you were assigned. By default, System Administrator users can view and edit any custom view. If you are not a system administrator, you can modify custom views only when you are a Views Administrator and the view permissions allow you to edit the view.

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 main View tab toolbar (Figure 7-8) perform any of the following changes to report views.

These actions affect all graphs contained in the view. Not all toolbar tools will be available, depending on the read and write permissions for the view.

- **Home**—Makes 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 3-1 on page 3-4.)

- **Paste Graphs from Clipboard**—Pastes report graphs copied from other reports.
- **Columns**—Changes the graph width, from 1 to 3 columns. 2 is the default.
- **Graph Mode**—Displays all view reports in graphs.
- **Table Mode**—Displays all view reports in tables.

Note In table mode, an Export to CSV tool is added to the toolbar.

- **Show/Hide Graph Legends**—Displays or hide legends from the report graphs.
- **Enable Compact Mode**—Reduces 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 graphs.
- **Merge Selected Graphs**—Merges two or more selected graphs. See Merging Graphs in Views, page 7-48.
- **Disable Automatic Updates**—Prevents the report from being updated; click **Enable Automatic Updates** to allow updates. This function is provided when continual, automatic updates are not needed.
- **Email Report**—Emails the report. See Emailing Reports, page 7-20, for information about setting up schedules for emailing graphs as graphic files or PDFs to other users by email.
- **Refresh**—Manually updates all the graphs and tables in the page.

Note Refresh will not refresh the page if the page is locked.

- **Play View**—Scrolls through the views automatically. This option appears only when you display the highest level of your created view. You can change the view interval (20 seconds is the default) and display type (inline or full screen) in User Preferences. See Customizing the GUI and Information Display, page 3-8.

Figure 7-8 Main View Toolbar

1	Home View	**7**	Compact Mode
2	Paste from Clipboard	**8**	Merge Selected Graphs
3	Columns	**9**	Lock Page
4	Graph Mode	**10**	Email Report
5	Table Mode	**11**	Refresh
6	Show Graph Legends		

Step 4 From each report graph toolbar you can perform any of the following changes.

Note These actions affect only the individual graph. Not all toolbar tools will be available, depending on the read and write permissions for the views.

- **Hide Row/Display Row**—Hides or displays the view row.
- **Drag to Reorder Items**—Click and drag the graph to a new location within the view.
- **Delete**—Deletes the report item from the report.
- **Graph Mode**—Displays the report item in graph 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 graph name, add or edit a subtitle, and modify the columns displayed in the graph summary table:

  Use Default Columns—Enables the default columns listed below. If not selected, you can choose any of the following columns:

  – Minimum (default)
  – Average (default)
  – Maximum (default)
  – Std Dev (standard deviation; default)
  – Variance (default)
  – Total
  – Current (default)

  Additionally, under Customize Reference Line you can add or modify a graph reference line:

  – Name—The reference line name.
  – Value—The value where you want the reference line to appear. This should be within the range displayed on the chart X axis.
  – Color—Sets the reference line color.
  – Opacity—Sets the reference line opacity. You can use the slider or enter a numeric value. The range is .05 to 1 (default).
  – Display Data Series Lines in Red/Green for Values Above/Below Reference Line—If enabled, the reference line is hidden. Data series lines above the reference line value appear in red, and data series lines below the reference line value appear in green.

    If you create multiple reference lines, you can only apply the red/green optionI to one of them. f you enable the red/green option and decide you do not want it enabled, delete the reference line and create a new one.

  Click **Save** after you complete the view graph property edits.
- **Copy to Clipboard**—Copies the report to the Prime Performance Manager clipboard to allow you to paste it into other views.
- **Email Report**—Emails the graph to selected recipients.
- **Select this Graph**—Selects the graph. The function allows you to select multiple graphs and merge them into one graph using the Merge Selected Graphs tool.

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

Inside each view graph, the following options are available:

- Show in Fullscreen Mode
- Show Aggregate Lines
- Change Graph Display
- Export This Chart

These are the same options that are available for report graphs. See Customizing Report Display, page 7-13, for descriptions of these options.

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

- Reports
- Dashboards
- Details
- Events
- Alarms
- Report Status
- Availability
- Star Graphs

For descriptions of the device menus, see Displaying Device Information at the Device Level, page 9-25.

Editing Graphs in Custom Views

To edit graphs in your custom view:

Step 1 Display the view containing the graphs you want to edit.

Step 2 On the graph toolbar, click **Edit**.

Step 3 In the Edit Report Properties dialog box, enter the following:

- Custom Report Name—Edit the report name.
- Custom Subtitle—(optional) Edit (or add) a subtitle.
- Use Default Columns—If selected, the default columns are used in the chart. If not selected, you can choose one or more of the following columns:
  - Minimum (default)
  - Average (default)
  - Maximum (default)
  - Std Dev (standard deviation; default)
  - Variance (default)

  - Total
  - Current (default)

Step 4 Edit the graph reference line or add a chart reference line by clicking **Add Reference Line**:

- Name—The reference line name.
- Value—The value where you want the reference line to appear. This should be within the range displayed on the chart X axis.
- Color—Sets the reference line color.
- Opacity—Sets the reference line opacity.

Step 5 Click **Save**.

Merging Graphs in Views

Merging graphs in views can be useful to create a composite view of similar data within similar times. For example, graphs for TE tunnels between two provider edge (PE) devices could be merged into one graph 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

Note To maximize the effectiveness of merged graphs, merged graphs should have similar data and time frames.

Note Although you can merge any number of graphs at one time, you can only define two labeled axes.

To merge graphs:

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

Step 2 Click **Select This Graph** (the bottom tool on the left side of the graph) for each graph you want to merge.

Step 3 On the Views toolbar, click **Merge Selected Graphs**.

Step 4 In the Edit Merged Graph Properties dialog box, enter the following:

- Custom Report Name—Enter the report name. The default name is Merged Chart.
- Custom Subtitle—(optional) Enter a subtitle, if needed.

Step 5 In the Edit Report Properties dialog box, enter the following:

- Custom Report Name—Edit the report name.
- Custom Subtitle—(optional) Edit (or add) a subtitle.
- Primary Axis—Edit the text of the primary axis, if needed. The primary axis is the name of the first chart you selected.

- Secondary Axis—Edit the text of the secondary axis, if needed. The secondary axis is the name of the second chart you selected.
- Use Default Columns—If selected, the default columns are used in the chart. If not selected, you can choose one or more of the following columns:
  - Minimum
  - Average (default)
  - Maximum (default)
  - Std Dev (standard deviation; default)
  - Variance (default)
  - Total
  - Current (default)

Step 6 Edit the chart reference line or add a chart reference line by clicking **Customize Reference Line**:

- Name—The reference line name.
- Value—The value where you want the reference line to appear. This should be within the range displayed on the chart X axis.
- Color—Sets the reference line color.
- Opacity—Sets the reference line opacity.

Step 7 Click **Save**.

The merged report appears beneath the other graphs.

Step 8 If you want to export the merged graphs as a CSV table, click **Export Table as CSV**.

An Opening [*merged file name*].csv dialog box allows you to open the CSV file in Excel or save it to a local drive,

Step 9 Click **OK**.

Tip You can use the Toggle Multiple Axes option in the Change Graph Display graph menu to toggle among the axes in merged charts.

Editing Views

You can edit any view to which you have edit permission and which have the Editable attribute turned on.

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—Displayed only at the highest view level. Options determine who can edit the view:
  - Private—Editable only by the view creator or System Administrator users.
  - Public—Editable by any user.
  - Group—If the user creating the view is a System Administrator, the view will be editable only by users who are members of the user group(s) selected under Groups. If the user creating the view is a Views Administrator, the view will be editable to whatever group the Views Administrator is currently in.
- Visible—Displayed only at the highest view level. Options set the visibility of the view to other users:
  - Private—Viewable only by creator or System Administrator users.
  - Public—Viewable by any user
  - Group—If the user creating the view is a System Administrator, the view will be viewable only by users who are members of the user group(s) selected under Groups. If the user creating the view is a Views Administrator, the view will be viewable to whatever group the Views Administrator is currently in.
- 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**.

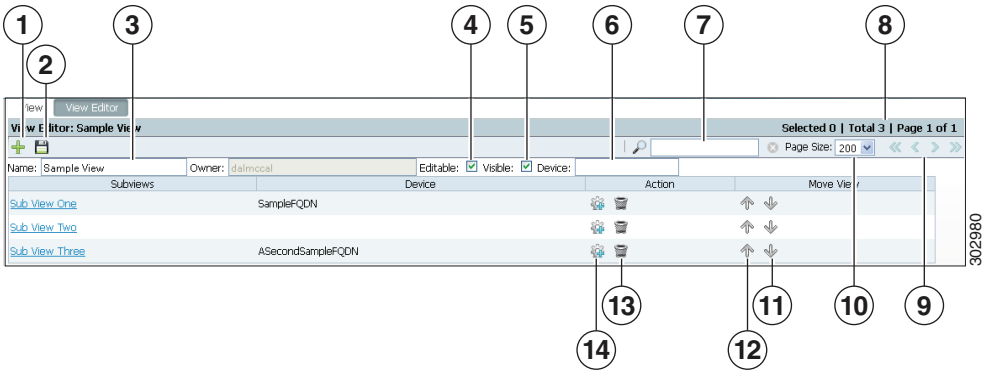
Step 6 To delete, edit, or display a view, from the View Editor Actions column, click the following:

- **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 7-7 on page 7-44.

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.

Figure 7-9 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

Managing Large Numbers of Views

Two user preferences (see Customizing the GUI and Information Display, page 3-8) help you manage large numbers of views:

- Default Number of Views Per View Level
- Maximum Number of Views Per View Level

These settings control the number of views displayed on a view tree. If the number of view tree items reaches the maximum, the top subview is rolled out and the new view item is added at the bottom. This allows you to scroll through many views while keeping your screen real estate manageable. Other view management elements include:

- Ellipsis—An ellipsis after a view indicates the number of subviews on the view tree has reached the default setting.
- Pencil icon—Depending on the user permissions, a pencil icon provides quick access to view operations including edit, copy, paste, move, delete, and create.
- View browse history—Prime Performance Manager retains a history of the views that you visit in a given session. You can go back and forth among views and view levels as you would with website pages.

To clean up views and return to the default order, that is, the top 10, you can:

- Restart the gateway. The view history for all users would be reset.

- Close a view to reset it for the current user

Working with Data Center Views

Prime Performance Manager delivers many Data Center views. When working with these views, keep the following in mind:

- If the Data Center feature is disabled, the views won't appear.
- Data center views can automatically build relationships between physical devices and logical devices such as UCS and ESXi, UCS and vCenter, and VSS and VDC devices.
- Data Center views cannot be edited, so some operation buttons are not available. However, you can copy Data Center views, then edit the copied views.

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 might require you to create new group reports. Information for creating group reports is provided in the *Cisco Prime Performance Manager 1.7 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. If the XML for a group is in the groups/system/ directory, it is not editable by any user from the GUI, If it is in the groups/user/ directory, it is editable by anyone with access to the group editor.
- 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:

- Provided Groups, page 7-53
- Creating a Report Group, page 7-54
- Managing Report Groups, page 7-55
- Displaying Group Reports, page 7-56

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 levels. 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 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 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 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 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 group:

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:

- Enabled—Check if you want the group enabled, that is, group report data will be collected and displayed.
- Section 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 “default.” 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/Tag—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.

Note You might see groups with a ppm_tenant type/tag. This tag is generated during the Prime Performance Manager OpenStack integration, which imports tenant information from OpenStack and creates ppm_tenant groups. When Prime Performance Manager processes report data, it checks the appropriate group definitions by summary processor and applies tags to the tenant data as defined by the algorithm and object list defined in the group. The summary processor specifies what report data is to be tagged and the group name specifies the data tag name. Do not specify the ppm_tenant tag through the GUI unless you are directed to by Cisco support.

- 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.

Note A data source is not required. If you only want to create and use the group to filter on a report, you do not need to specify a data source, and the group does not need to be enabled. However, to do aggregation, the group must have a data source, or no results will appear when the group is enabled.

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 Managing Report Groups, page 7-55. 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.

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:

- Section Name
- Type/Tag
- 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.
- List of Objects

For field descriptions and entry examples, see Creating a Report Group, page 7-54.

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 7-13.

Creating Web Reports

Prime Performance Manager allows you to define a new report by using report metrics that are already in place for existing reports. This feature allows you to choose report metrics that are defined in current report ProcessDBSummary tables, but not from the report Poll sections. Fundamentally, you can create WebReport sections using the following report elements:

- Name—Ensures the report is kept unique.
- Category—Where the report appears in the report tree.
- Context—The report index structure.
- Filtering
- GraphView and graphsPerRow
  - GraphSummary + title + hide/show options
  - Graph + title—Util/Column/Bytes columns
  - LeafGraph + title—Util/Column/Bytes columns
- TableView
  - HeaderRow with Labels
  - Link Columns
  - Time Column
  - Column/Util/Bytes Columns

To create a web report:

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

Step 2 From the Network menu, choose **Web Report Editor.**

Step 3 On the Get Started With The Web Report Editor screen, choose **Create New Web Report Document** and click **Go**.

Note You can also use the Web Report Editor to open existing web reports. If the web report is a user report located in the user directory, you can edit it directly. If it is a system report located in the system directory, the Web Report Editor will save a copy in the user directory and and use this report as long as it exists.

Step 4 On the Basic Report Properties screen, enter the report basic properties:

- Data Source—Click the field and choose the data source for your report from the alphabetical list of available data sources.
  - To filter the data sources, enter the first several letters of the data source, for example, entering MPLS displays MPLS data sources.
  - As you scroll over the available data sources, the data source variables appear on the right. The data source keys are identified with a key icon.

  After you choose the data source the Report Preview is automatically updated with the report XML for the chosen data source.
- File Name—Enter a name for the report file. Only alphanumeric characters are permitted. Special characters, including spaces, are not allowed.

- Readable Name—Is automatically populated with the file name. Enter another name, if needed.
- Report Tree Location—Sets the location of the report in the Reports navigation tree:
  - Use Existing—Displays existing navigation tree top categories sequentially and allows you to place the report in an existing category.
  - Create New—Allows you to create a new navigation tree category and sublevels.
- Text Properties File Name—Is automatically populated with the [*file name*].properties. The field is not editable.
- Criteria—Click the field and choose the report criteria from the displayed list of network device capabilities.
- Go Live Disabled—Check if you do not want Go Live enabled for this report. The Go Live option allows users to initiate 15-second polling for device-level reports.
- Show Compact—Check if you want the report displayed in compact mode. In compact mode, when graph output is selected the Zoom, Aggregate Lines, Graph Styles, and Export Graphs tools displayed inside graphs are hidden. Additionally, the graph border is hidden and graph title reduced in size. This option reduces the overall size of the graph and is useful when screen real estate is needed.
- Column Keys—Check the boxes of the data source keys if you want to prefix the drill-down report columns with the name of the column. If not checked, the column values provide drill-down context to users.

Step 5 Click **Next**.

Step 6 Enter the graph view properties:

- Summary Table Title Tag—Enter the title of the report summary table.
- Readable Summary Table Title—Enter the summary table title displayed to users. You can enter alphanumeric characters. No special characters are allowed including spaces.
- Summary Table Minimized—Check this box if you want the summary table minimized when the report is first displayed.
- Show Legend by Default—Check this box if you want the graph legends displayed by default.
- Enable Leaf Graph—Check if you want to enable leaf graphs in the report. If checked, the following leaf graph fields appear:
  - Leaf Graph Readable Title—A readable leaf graph title.
  - Leaf Graph Title—The actual leaf graph title.
  - Default Graph Type—Allows you to choose the default graph type. Line is the default. Other choices include Bar, Stacked Column, Stacked Percentage Column, Utilization Area, and Utilization Column. For descriptions, see Customizing Report Display, page 7-13.

Note A leaf graph is a combined graph that appears when you drill down to the appropriate level. For example, if a report has graphs A, B, and C, and Enable Leaf Graph is checked, A, B, and C will display the top 10 series at the network level. However, if you click a device and drill to a lower level, a fourth graph is displayed that combines the A, B, and C series on one graph. Leaf graphs only appear when you drill to a sufficient level, depending on context.

- Number of Columns—Choose the number of columns you want for the report.

Step 7 Click **Next**.

Step 8 In the Graph Properties window, complete the following graph fields:

- Graph Title Tag—Enter the graph title in alphanumeric characters. No special characters, including spaces are permitted.

  After you enter the graph title, the Readable Graph Title, Column Name Tag, and Readable Column Name are automatically populated with the graph title.
- Readable Graph Title—The graph title displayed to users.
- Show Values In Graph—Allows you to choose which of the following values to display in the graph:
  - Min—Minimum value.
  - Avg—Average value (checked by default).
  - Max—Maximum value (checked by default).
  - Total—Total value.
  - Current—Current value.
- Column Name Tag—The name of the column.
- Readable Column Name—The readable column name.
- Variable—The variable associated with the graph. All variables associated with the data source are available except for key columns and the TenantId column. If you choose Custom Formula, a Custom Formula/KPI field appears where you can enter a custom formula.
- Show as Rate—Causes the data to be displayed as a rate. For example, if your variable is InPkts, checking the box will create the XML, InPkts / IntervalDuration(), which will cause the data to display as a rate.
- Variable Type—Sets the variable type:
  - Column (default)
  - Bits
  - Bytes
  - Util
  - ipAddr

    If you choose ipAddr, a checkbox appears allowing you to indicate whether it is a key.
- Default Value—The default value.
- No Data Value—The value displayed when no data is present.
- Decimal Precision—The decimal precision, entered as zeros.
- Sortable—If checked (default), indicates the graph is sortable.
- Descending—If checked (default), indicates the data is displayed in descending values.
- Thresholdable—If checked (default), indicates thresholds can be provisioned on the data.
- Filterable—If checked (default), indicates the graph is filterable.
- Default Sort Column—If checked, indicates the column is the default sort column
- TCA Rising—If checked (default), indicates the threshold crossing alert, if provisioned, is rising. (This value is ignored if Thresholdable is not enabled.)
- No Color—Indicates no colors are displayed on the graph.
- Down Colors—Indicates down colors are displayed on the graph.

- Show Percentage Column—Adds a column in the graph view summary table that shows the value as a percent. For example, if the column is InPkts and you check this box, the summary table will have an Avg column but will also have a Avg as % column. If the average value is 10, and that represents 14.3% of the top ten (all the rows in the summary table), 14.3 will appear in the Avg as % column.
- Hide Series—Hides this series in the leaf graph by default. If a user views the leaf graph, it is as if they clicked on the series in the legend to hide it. They can still select it in the legend to display the series. If a report has graphs A-D, and A and B have Hide Series checked, the leaf graph will only show series C and D. A and B will be grayed out in the legend.

Step 9 Click **Continue**.

The graph is added to the report. The Graph View Properties window displays the key properties.

Step 10 If you want to add another graph to the report, click Add under Graph View on the left and repeat Steps 6 through 9. If not, click **Next**.

Step 11 If you want to a add filter, under Filters click **Add**, then enter the following filter properties:

- Variable—Choose the variable you want to associate with the filter.
- Enter the filter value; check **Not** if you want the filter not equal.

Step 12 Click **Continue**.

Step 13 If you want to add another graph to the report, click **Add** under Graph View on the left and repeat Steps 6 through 12. If not, click **Next**.

Step 14 On the Final Preview window, preview the web report XML under Report Preview. If needed, you can make manual adjustments by editing the report XML.

Step 15 Click **Next**.

Step 16 On the Confirmation dialog, click **OK**.

The new report is added to Prime Performance Manager.

Deleting Web Reports

To delete a user-created web report:

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

Step 2 From the Network menu, choose **Web Report Editor.**

Step 3 On the Get Started With The Web Report Editor screen, choose **View/Edit/Delete Existing Web Report Document**, then click **Go**.

Step 4 In the Search Web Reports dialog box, enter the title of the web report you want to delete, or scroll to the report in the web report list.

Step 5 Click **Delete Web Report**.

Note If the Delete Web Report is not active, the report is a system report and cannot be deleted. You can only delete user reports.

Step 6 On the confirmation, click **OK**.

The report is deleted.

Setting Up Reports for Specialized Technologies

The following topics tells you how to set up Prime Performance Manager reports for specialized devices and technologies including Data Center, NetFlow, Star OS Bulk Statistics, Generic CSV Bulk Statistics, OpenStack Ceilometer, Ganglia Reports, Managing Dashboards, Ceph Reports, Custom Report Views, Report Groups and Web Reports:

Displaying Data Center Reports

Prime Performance Manager supports many data center networking, computing, storage, virtualization, and management devices and technologies. Data center report display is covered in the following topics:

Supported Data Center 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 8-1 lists the data center devices and technologies that Prime Performance Manager supports.

Table 8-1 Supported Data Center Devices and Technologies

Area	Device/Technology	Notes
Network	Citrix NetScaler VPX and SDX	Specifies global and context level LB data; Resources, High Availability (state transitions, failed trans, conf sync failures, heartbeats Tx/Rx).
	Nexus 7000	Specifies new features and performance of Freetown, SUP2E
	GRE	Specifies GRE Tunneling Protocol.
	VM-FEX	
	Cisco ASA 5585	Specifies firewall feature, and four-node clusters
	Cisco ASA 1000v	Specifies FW for tenant edge control.
	Cisco CSR 1000v	Specifies resource, interfaces, MPLS L3VPNs, BGP, IPSEC VPN statistics, LISP, ISIS, FW connections and rate, NAT stats, QoS, NBAR.
	Fabricpath	Specifies L2 multi-path F-tag tree
	OTV	
	LISP	Specifies MR, MS, DB, cache statistics and other details.
	ISIS	Specifies statistics for original ISIS and different variances (for example in OTV).
	vWAAS	
	vNAM	
	IPv6 and Security	
	eBGP	Specifies Cisco CSR XE < eBGP > Cisco ASR 9000
	Cisco ASA 5500	Specifies physical FW and RA VPN termination
	VSM on Nexus 1kv	
	Bare metal UCS servers + Virtual appliances	
	Cisco UCS C without UCSM	
	Cisco ASR 9000-nV	Specifies Cisco ASR 9000 cluster
	Nexus 6000	Specifies Cisco Nexus 6000 series
	Nexus 1100	
	Nexus 9000	Specifies Nexus 9300 and 9500/ACI
	SourceFire	Supports NGIPS first and NGFW next
	Avi Load Balancer	Avi Networks Cloud Application Delivery Platform provides the health and availability reports for Controller, Service Engine, Virtual Services, Pool, Members and Throughput and connection related statistics.

Table 8-1 Supported Data Center Devices and Technologies (continued)

Area	Device/Technology	Notes
Compute Logical/Virtual Devices	VMware	Specifies: • vMotion statistics: vMotion counts, Storage vMotion counts, utilization, top five VMs, allocated space and performances, both host and VM level: IOPS and latency • Capacity planning, utilization trend and history, ESXi and VM KPIs: ESXi start time, VM system uptime, VM power usage, VM details, hosts and VM resource report, vCenter clusters and multiple vCenters, statistics at virtual data center and cluster level
	Hypervisor	Specifies host credentials
Storage	Storage Area Network (SAN)	Specifies FC and SAN statistics from Cisco MDS 9000 and Nexus 5000
	EMC Storage	Specifies VNX and VMAX devices
	Ceph	Specifies Ceph device details
System	Tenant	Specifies interfaces with Prime Network Service Controller, IAC, and OpenStack
	Support for MSDC and Vinci	
	Dashboard for PC reports	
Application	Monitoring	Specifies CPU, memory, and processes
Integration	Adjust TCA and XL for Prime Network integration	
	Integration with OpenStack	Specifies the Ceilometer services like Nova, Glance, and Swift.
	Integration with IAC/PSC	
	Integration with UCS Director	Specifies integration with Cisco UCS-D, and support storage (NetApp ONTAP 8.2; VMAX and VNX)
Others	Nexus Switches	Collects and pushes data to Prime servers
	DCM	
	OnePK	Uses Java API to collect data and configuration
	REST API scale and performance	Specifies many REST calls from Prime Central.
	VM free space	

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 Devices
  - VSS
  - Routers
- Compute
  - vCenter
  - ESXi

  - HyperV
  - KVM
  - Xen
  - UCS Clusters (includes the hosts/VMs to blade server mapping)
  - UCS Standalone
- Tenants

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

- Compute
  - ESXi
  - Ganglia
  - Hyper-V
  - KVM
  - OpenStack
  - UCS/Hypervisor Relationships
  - UCS Clusters
  - UCS Standalone
  - Xen
  - vCenter
- Storage
  - Ceph
  - EMC
  - Fabric Configuration Server
  - Fibre Channel
  - NetApp
  - SMI-S
  - VSAN Zoning

Some Data Center technologies require special setup procedures, described in the following topics:

- Displaying ESXi and vCenter Reports, page 8-4
- Displaying Data Center Tenant Reports, page 8-5
- Setting Up collectd Performance Monitoring For a Single Device, page 8-8

Displaying ESXi and vCenter Reports

ESXi and vCenter reports have two qualifications:

- Prime Performance Manager supports domain and username to access vCenter and ESXi that are members of an Active Directory domain. For information on adding Telnet and SSH credentials for vCenter and ESXi, see Adding Device Credentials for Other Protocols, page 5-6.

- To display ESXi and vCenter Datastore IOPS, Total Latency and Normalized Latency reports, you must manually enable the Storage I/O Controller option in VMware [*datastore*] Properties dialog box. (This option is only available in VMware Enterprise Plus.) Enabling Storage I/O Controller allows Prime Performance Manager to poll data from ESXi and vCenter. If the Storage I/O Controller is not enabled, Prime Performance Manager displays 0 in these reports.

Displaying Data Center Tenant Reports

Prime Performance Manager supports multitenant software architectures and technologies including Cisco Network Segmentation Manager (NSM) and OpenStack. NSM integrates VMware vCloud Director 1.6 with the Cisco Nexus 1000V for networking management. OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a data center.

To display tenant reports, perform the following tasks:

- Import data center devices, such as hypervisors, routers, and switches containing the tenant data. You can import the devices from Cisco Prime Network or Cisco Prime Central, or you can discover the devices from Prime Performance Manager. See Chapter 5, "Discovering Devices With Prime Performance Manager."
- Enable the data center personality in Prime Performance Manager. See ppm maxhtmlrows, page B-55.
- Import the tenants into Prime Performance Manager. See Importing Tenants into Prime Performance Manager, page 8-5.
- Display the tenant reports. See Displaying Tenant Details and Reports, page 8-5.

Importing Tenants into Prime Performance Manager

To import tenants into Prime Performance Manager and display the tenant reports:

Step 1 Verify the data center personality is enabled:

```
ppm manage datacenter status
```

If the status is inactive, complete the following steps:

a. Enable the data center personality:

```
ppm manage datacenter enable
```

b. Restart Prime Performance Manager. See Restarting Gateways and Units, page 2-5

Step 2 Complete the tenant integration. See Adding Tenants Through OpenStack Integration, page 16-4.

Displaying Tenant Details and Reports

If OpenStack tenant integration is enabled, hypervisor and OpenStack Ceilometer report data are filtered automatically.

Note For OpenStack tenant integration, Prime Performance Manager must import Ceilometer as the monitored device for data filtering. Hypervisors are optional.

For tenants added to Prime Performance Manager directly, filtering is set up at the time you create the tenant. See Creating Tenants in Prime Performance Manager, page 16-2

To display report data by tenant:

Step 1 Verify that the tenants were imported into Prime Performance Manager. See Importing Tenants into Prime Performance Manager, page 8-5.

Step 2 Log into the Prime Performance Manager GUI as the administrator user.

Step 3 On the Prime Performance Manager toolbar, click **User Preferences**.

Step 4 In the User Preferences window, click **General Display**.

Step 5 In the right column, modify the following tenant report properties:

- Tenant Scope—Sets the report tenant scope:
  - All—Displays all reports, not just tenant reports.
  - All Tenants—Displays all tenant reports.
  - SELECTED—Allows you to select and display reports for individual tenants.
- Tenant Display—Sets the tenant identifier when displayed in reports, either Name (internal tenant name), or Display Name.

For example, if you set Tenant Scope to All Tenants and Tenant Display to Display Name, then navigate to Reports > Compute > OpenStack > [Ceilometer], you will notice a new Tenant column is displayed with the data for all Tenants.

Step 6 From the Network menu, choose **Tenants**.

The System Tenants window displays the tenants that are integrated with Prime Performance Manager.

Step 7 Click a tenant in the navigation tree.

The tenant name, status, description, source, last successful import, and ongoing synchroniation data are displayed on the Tenant Details tab.

Step 8 You can also display tenant reports by choosing **Reports** from the Performance menu, then choosing:

- **Views > Data Center > Tenants**

  Provides a unified structure for each tenant even if tenants were imported from different cloud systems.Tenant performance data is divided into Network and Compute categories. Essentially, Views > Tenants provides a visual map for tenants management.

- **Reports > Network > Tenants**

  Lists all Prime Performance Manager tenant reports. In this release, ESXi, VLAN, VRFs reports are available. Reports list the Top 10 (by default) tenants data.

Note For NSM, only performance data associated with networks, such as VLANs and VRFs are collected. For OpenStack, only performance data associated to VMs is collected.

Displaying Data Center Resource Allocation and Trend Analysis

The data center group report allows you to see a profile of your network data center VMware vCenter servers and perform trend analysis to predict future capacities, availabilities, and other resource allocations. vCenter allocations that you can track and analyze future trends for include:

- Top N hosts by CPU availability (CPU total available, provisioned, consumed).
- Top N hosts by memory availability.
- Top N hosts by storage disk availability (datastores by space available).
- Top VMs with the most alarms (per downtime) availability, including:
  - VM name
  - Severity
  - Alarm count
- Top N hosts with the least resource availability, including:
  - VM name
  - CPU used
  - Memory used
  - Disk usage

To display data center resource allocation:

Step 1 Verify that VMware vCenter devices were added to Prime Performance Manager:

a. From the Network menu, choose **Credentials Editor**.

b. In the device list, vCenter devices are listed with vCenter_HTTPS connection protocol.

c. If no vCenter servers are listed, you must add them. See Managing Device Credentials, page 5-3. For the device credential, use vCenter_HTTPS.

Step 2 From the Administration menu, choose **Group Editor**,

Step 3 Verify that the following group reports are enabled:

- DatacenterCPU
- DatacenterDatastore
- DatacenterMemory
- VMwareClusterCPU
- VMwareClusterDatastore
- VMwareClusterMemory

These reports are enabled by default. If they are not enabled, check the Enabled checkbox then choose **Enable Selected Groups** from the Actions menu.

Step 4 To view vCenter resource allocation reports, in the navigation tree, choose: **Grouped Reports > Compute > vCenter > Hosts and Clusters > VMware Clusters**.

Step 5 To perform Data Center resource trend analysis:

a. In the navigation tree, choose **Trend Analysis > Data Center** located at the bottom of the Performance Reports navigation tree.

Wait until enough data is aggregated in the group reports. A minimum of 12 data points are needed in these reports.

b. Experiment with the Trend Analysis to see how the analysis works. Configure different parameters for example. set Interval as Day or Hour, and change the Sample Period (time period on which the analysis is based) and the Forecast Period.

c. After specifying parameters, click **Calculate** to recalculate the trend of resource utilization.

Setting Up collectd Performance Monitoring For a Single Device

collectd is a computer background process that collects system performance statistics. These statistics can be used for performance analysis and capacity planning.

To monitor collectd statistics in Prime Performance Manager for a single device:

Step 1 Verify that the following are installed on the computer where you want to gather collectd statistics:

- Net-SNMP
- RRDTool
- Collectd

Step 2 Add the rrdtool binary directory into the environment variable PATH. For example, if the default device shell is BASH, add the following line into ~/.bash_profile:

```
PATH=$PATH: /opt/rrdtool-1.6.7/bin
```

Step 3 Enable the following section in the collectd configuration file.

```
LoadPlugin rrdtool
<Plugin rrdtool>
        DataDir "/var/lib/collectd"
        CacheTimeout 120
        CacheFlush   900
        RRARows      1
        RRATimespan  3600
</Plugin>
```

The DataDir parameter must be configured with /var/lib/collectd by default. If you want to change the default rrdtool data output directory, change DataDir here and then modify the XMP_PAL.properties under $PPM_INSTALLATION/properties/. You must modify this file both on gateway and unit, then restart them.

```
# collectd base directory to store the rrd files
COLLECTD_BASE_DIR = /var/lib/collectd/
```

Step 4 If you are monitoring an application, configure the appropriate collectd plugin. See the following topics for configuration examples:

- Apache Plugin Example, page 8-9
- MySQL Plugin Example, page 8-9
- GenericJMX Plugin Example, page 8-9
- Oracle Plugin Example, page 8-11
- PostgreSQL Plugin Example, page 8-13

- Ceph Plugin Example, page 8-13

Step 5 Add the SNMP community configured on Net-SNMP in Prime Performance Manager. For information see Adding SNMP Device Credentials, page 5-3.

Step 6 Add collectd_SSH in the Credentials Editor, The credential is the operating system SSH username and password. For information see Adding Device Credentials for Other Protocols, page 5-6.

Step 7 Run device discovery. For information, see Managing Device Credentials, page 5-3

Apache Plugin Example

The following shows a sample Apache plugin configuration:

```
LoadPlugin apache
<Plugin apache>
  <Instance "local">
    URL "http://localhost/server-status?auto"
  </Instance>
</Plugin>
```

MySQL Plugin Example

The following shows a sample MySQL plugin configuration:

```
LoadPlugin mysql
<Plugin mysql>
<Database example>
        Host "localhost"
        Socket "/var/lib/mysql/mysql.sock"
        User "root"
        Password ""
        Database "example"
</Database>
</Plugin>
```

GenericJMX Plugin Example

The GenericJMX collectd plugin reads Managed Beans (MBeans) from an MBeanServer using JMX. The plugin is written in Java and requires the Java plugin.

```
<Plugin "java">
  JVMARG
"-Djava.class.path=/usr/share/collectd/java/collectd-api.jar:/usr/share/collectd/java/gene
ric-jmx.jar"
  LoadPlugin "org.collectd.java.GenericJMX"

  <Plugin "GenericJMX">
    <MBean>
     ...
    </MBean>

   <Connection>
      Host "crdc-c210-3-6"
      InstancePrefix "ppm_unit-"
      ServiceURL "service:jmx:rmi:///jndi/rmi://10.74.125.84:9011/jmxrmi"
      Collect "memory_pool"
      Collect "classes"
      Collect "compilation"
```

```
      Collect "memory"
      Collect "garbage_collector"
     </Connection>
<Connection>
    ...
     </Connection>

  </Plugin>  </Plugin>
</Plugin>
```

Run your applications with something similar to the following arguments on the computer monitored by GenericJMX. In this example, 10.74.125.84 is used:

```
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.port=17264
-Dcom.sun.management.jmxremote.ssl=false
```

The MBean configuration includes the following:

- Memory pools

  Memory usage by memory pool:

  ```
  <MBean "memory_pool">
    ObjectName "java.lang:type=MemoryPool,*"
    InstancePrefix "memory_pool-"
    InstanceFrom "name"
    <Value>
          Type "memory"
          #InstancePrefix ""
          #InstanceFrom ""
          Table true
          Attribute "Usage"
    </Value>
  </MBean>
  ```

- Memory

  Generic heap and nonheap memory usage:

  ```
  <MBean "memory">
      ObjectName "java.lang:type=Memory"
      #InstanceFrom ""
      InstancePrefix "memory"
      # Creates four values: committed, init, max, used
      <Value>
          Type "memory"
          #InstancePrefix ""
          #InstanceFrom ""
          Table true
          Attribute "HeapMemoryUsage"
          InstancePrefix "heap-"
      </Value>
          # Creates four values: committed, init, max, used
      <Value>
          Type "memory"
          #InstancePrefix ""
          #InstanceFrom ""
          Table  true
          Attribute "NonHeapMemoryUsage"
          InstancePrefix "nonheap-"
      </Value>
  </MBean>
  ```

- Classes

  Number of classes loaded by the JVM:

```
<MBean "classes">
  ObjectName "java.lang:type=ClassLoading"
  InstancePrefix "classes"
  #InstanceFrom ""
  <Value>
    Type "gauge"
    InstancePrefix "loaded_classes"
    #InstanceFrom ""
    Table false
    Attribute "LoadedClassCount"
  </Value>
</MBean>
```

- Compilation

  Time spent by the JVM compiling or optimizing:

```
<MBean "compilation">
  ObjectName "java.lang:type=Compilation"
  InstancePrefix "compilation"
  #InstanceFrom ""
  <Value>
    Type "total_time_in_ms"
    InstancePrefix "compilation_time"
    #InstanceFrom ""
    Table false
    Attribute "TotalCompilationTime"
  </Value>
</MBean>
```

- Garbage Collector

  The garbage collector account and time is shown below:

```
<MBean "garbage_collector">
  ObjectName "java.lang:type=GarbageCollector,*"
  InstancePrefix "gc-"
  InstanceFrom "name"

  <Value>
    Type "invocations"
    #InstancePrefix ""
    #InstanceFrom ""
    Table false
    Attribute "CollectionCount"
  </Value>

  <Value>
    Type "total_time_in_ms"
    InstancePrefix "collection_time"
    #InstanceFrom ""
    Table false
    Attribute "CollectionTime"
  </Value>

</MBean>
```

Oracle Plugin Example

A generic Oracle plugin configuration is shown below:

```
loadPlugin  oracle
<Plugin oracle>
   <Query "db_efficiency">
    Statement "SELECT round(sum(decode(METRIC_NAME, 'Database Wait Time Ratio',
value)),2) AS DATABASE_WAIT_TIME_RATIO,
       round(sum(decode(METRIC_NAME, 'Database CPU Time Ratio', value)),2) AS
DATABASE_CPU_TIME_RATIO,
       'DB_EFFICIENCY' AS DB_EFFICIENCY
        FROM SYS.V_$SYSMETRIC
        WHERE METRIC_NAME IN ('Database CPU Time Ratio', 'Database Wait Time Ratio')
              AND INTSIZE_CSEC = (SELECT max(INTSIZE_CSEC) FROM SYS.V_$SYSMETRIC)"
      <Result>
           Type "efficiency"
           InstancesFrom "DB_EFFICIENCY"
           ValuesFrom "DATABASE_WAIT_TIME_RATIO" "DATABASE_CPU_TIME_RATIO"
      </Result>
  </Query>

  <Query "io_per_tablespace">
  Statement "SELECT sum(vf.PHYBLKRD)*8192 AS PHY_BLK_R,
                    sum(vf.PHYBLKWRT)*8192 AS PHY_BLK_W,
                    'tablespace' AS i_prefix,
                    dt.tablespace_name
                FROM ((dba_data_files dd JOIN v$filestat vf ON dd.file_id = vf.file#
)
                      JOIN dba_tablespaces dt ON dd.tablespace_name =
dt.tablespace_name)
                GROUP BY dt.tablespace_name"
  <Result>
    Type "io_octets"
    InstancesFrom "i_prefix" "TABLESPACE_NAME"
    ValuesFrom "PHY_BLK_R" "PHY_BLK_W"
  </Result>
</Query>

  <Database "cisco">
    ConnectID "cisco"
    Host "10.74.125.76"
    Username "cisco"
    Password "cisco"
    Query "db_efficiency"
    Query "io_per_tablespace"
  </Database>
</Plugin>
```

If remote mode is enabled add the following dataset specification to $COLLECTD_HOME/share/collectd/types.db at both the remote collectd server and the client:

```
efficiency wait:GAUGE:0:100.1, cpu:GAUGE:0:100.1
```

Database blocks define database connections and the queries that should be sent to the database:

- ConnectID—Defines the database alias or service name to connect to. Usually, these names are defined in the file named $ORACLE_HOME/network/admin/tnsnames.ora.
- Host—Hostname to use when dispatching values for this database. Defaults to using the global hostname of the collectd instance.
- Username—Username used for authentication.
- Password—Password used for authentication.

- Query—Associates the query named QueryName with this database connection. The query needs to be defined before this statement, that is, all query blocks you want to refer to must be placed above the database block you want to refer to them from.

PostgreSQL Plugin Example

Query blocks are not used in the PostgreSQL plugin, The plugin uses the default statistics collected from the PostgreSQL statistics collector, which you must enable. The collector is usually enabled by default.

```
loadPlugin postgresql
<Plugin postgresql>
     Database test>
                Host "localhost"
                Port "5432"
                User "postgres"
                Password "postgres"
    </Database>
    <Database foo>
    ...
    <Database>
  </Plugin>
```

Ceph Plugin Example

You can base your Ceph plugin configuration on the following example:

```
<LoadPlugin ceph>
  <Daemon "osd.0">
        SocketPath "/var/run/ceph/ceph-osd.0.asok"
  </Daemon>
  <Daemon "mon.a">
        SocketPath "/var/run/ceph/ceph-mon.ceph1.asok"
  </Daemon>
  <Daemon "mds.a">
        SocketPath "/var/run/ceph/ceph-mds.ceph1.asok"
  </Daemon>
</Plugin>
```

Notes:

- The name must start with osd if the SocketPath points to an osd socket file. mon and mds can be done in the same manner.
- The Ceph plugin does not support remote mode, so you cannot use network plugin to do centralized deployment.

Setting Up collectd Performance Monitoring For Multiple Devices

If you're collecting performance data for multiple devices, data should be in one central location and not across multiple servers. The recommended approach is to designate one server and multiple clients that send their data to the server. For information about collectd, visit the collectd website:

https://collectd.org/wiki/index.php/Networking_introduction

Managing Hypervisors on Windows Servers

You can use Prime Performance Manager to display reports on Xen, KVM, and Hyper-V hypervisors for the following Windows operating systems:

- Windows Server 2012 R2
- Windows Server 2012 ST
- Windows Server 2008 R2
- Windows Server 2008 ST

The following topics provide instructions for each hypervisor:

- Managing Windows Server VMs in KVM, page 8-14
- Managing Windows Server VMs in Xen, page 8-15
- Managing Windows Server VMs in Hyper-V, page 8-16
- Manage Windows Server VMs Using SNMP Credentials, page 8-16

Managing Windows Server VMs in KVM

You can manage Windows Server VMs in KVM through KVM_TLS or SNMP credentials.

To manage Windows Server VMs in KVM using KVM_TLS credentials:

Step 1 Log into Prime Performance Manager as the system administrator user. For login procedures, see Launching the Web Interface, page 3-1.

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

Step 3 On the Credentials Editor toolbar, click **Add New Credentials Entry**.

Step 4 In the Add Credentials Entry dialog box, enter the following:

- Device—Enter the KVM device IP address.
- Connection Protocol—Enter **KVM_TLS**.
- Sub System—Enter **TBD**.
- User Name—If necessary, enter the KVM device username.
- Password—If necessary, enter the username password.

Note Secondary Login Type, Secondary Username, and Secondary Password are not applicable

Step 5 Click **OK**.

Step 6 From the Network menu, choose **Discovery**,

Step 7 In the IP Address, Address Range, Subnet, CIDR, or DNS Hostname field, enter the KVM device IP address.

Step 8 Click **Add**.

Step 9 From the Network Discovery toolbar, click **Discover Network**.

Step 10 From the Network menu, choose **Device**,

Step 11 Verify the KVM device is added to the device list with Device type QEMU/KVM 1.5.0.

Step 12 Click the KVM device.

Step 13 Under the device reports, navigate to **Compute > KVM** to view KVM Host and KVM VM reports.

Note You can also view KVM Host and Windows VM reports by choosing **View > Data Center > Compute > KVM.**

Managing Windows Server VMs in Xen

You can manage Windows Server VMs in Xen through XEN_TLS or SNMP credentials.

To manage Windows Server VMs in Xen using XEN_TLS credentials and check host and VM reports:

Step 1 Log into Prime Performance Manager as the system administrator user. For login , see Launching the Web Interface, page 3-1.

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

Step 3 On the Credentials Editor toolbar, click **Add New Credentials Entry**.

Step 4 In the Add Credentials Entry dialog box, enter the following:

- Device—Enter the Xen device IP address.
- Connection Protocol—Enter **XEN_TLS**.
- Sub System—Enter **TBD**
- User Name—If necessary, enter the Xen device username.
- Password—If necessary, enter the username password.

Note Secondary Login Type, Secondary Username, and Secondary Password are not applicable

Step 5 Click **OK**.

Step 6 From the Network menu, choose **Discovery**,

Step 7 In the IP Address, Address Range, Subnet, CIDR, or DNS Hostname field, enter the Xen device IP address.

Step 8 Click **Add**.

Step 9 From the Network Discovery toolbar, click **Discover Network**.

Step 10 From the Network menu, choose **Devices**,

Step 11 Verify the Xen device is added to the device list with Device type Xen 3.1.

Step 12 Click the Xen device.

Step 13 Under the device reports, navigate to **Compute > XEN** to view Xen Host and Xen VM reports.

Note You can also view Xen host and Windows VM reports by choosing **View > Data Center > Compute > XEN.**

Managing Windows Server VMs in Hyper-V

You can manage Windows Server VMs in Hyper-V through XEN_TLS or SNMP credentials.

To manage Windows Server VMs in Hyper-V using XEN_TLS credentials and check host and VM reports:

Step 1 Log into Prime Performance Manager as the system administrator user. For login, see Launching the Web Interface, page 3-1.

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

Step 3 On the Credentials Editor toolbar, click **Add New Credentials Entry**.

Step 4 In the Add Credentials Entry dialog box, enter the following:

- Device—Enter the Hyper-V device IP address.
- Connection Protocol—Enter **XEN_TLS**.
- Sub System—Enter the Hyper-V subsystem.
- User Name—If necessary, enter the Hyper-V device username.
- Password—If necessary, enter the username password.

Note Secondary Login Type, Secondary Username, and Secondary Password are not applicable

Step 5 Click **OK**.

Step 6 From the Network menu, choose **Discovery**,

Step 7 In the IP Address, Address Range, Subnet, CIDR, or DNS Hostname field, enter the Hyper-V device IP address.

Step 8 Click **Add**.

Step 9 From the Network Discovery toolbar, click **Discover Network**.

Step 10 From the Network menu, choose **Device**,

Step 11 Verify the Hyper-V device is added to the device list with Device type HyperV6.2.0.

Step 12 Click the Hyper-V device.

Step 13 Under the device reports, navigate to **Compute > Hyper-V** to view Hyper-V Host and Hyper-V VM reports.

Note You can also view Hyper-V Host and Windows VM reports by choosing **View > Data Center > Compute > HyperV.**

Manage Windows Server VMs Using SNMP Credentials

To manage Windows Server VMs using SNMP credentials:

Step 1 Enable SNMP Service on the Windows VM Servers.

Step 2 Log into Prime Performance Manager as the system administrator user. For information, see Launching the Web Interface, page 3-1.

Step 3 From the Network menu, choose **SNMP Editor**.

Step 4 On the Network SNMP Editor toolbar, click **Add New SNMP Entry**.

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

- IP Address Range or Hostname—Enter the Windows VM server IP address.
- SNMP Version
- Read Community
- Max Table Varbind
- Port
- User Name
- Authentication Protocol
- Authentication Password
- Privacy Protocol
- Privacy Password

Step 6 Click **OK**.

Step 7 From the Network menu, choose **Discovery**,

Step 8 In the IP Address, Address Range, Subnet, CIDR, or DNS Hostname field, enter the Windows server IP address.

Step 9 Click **Add**.

Step 10 From the Network Discovery toolbar, click **Discover Network**.

Step 11 From the Network menu, choose **Device**,

Step 12 Verify the Windows VM is added to the list with the device type, WindowsNT Server.

Step 13 Click the device and view the Windows VM reports.

Setting Up NetFlow Reports

Prime Performance Manager can generate NetFlow data reports. NetFlow is a Cisco network protocol that collects IP traffic information. Devices are configured to export IP packets to the NetFlow collector on the Prime Performance Manager unit. The unit processes the packets and generates report data. Prime Performance Manager supports:

- NetFlow v5 and v9
- Flexible NetFlow IP Flow Information Export (IPFIX)
- NetFlow records exported using User Datagram Protocol (UDP).

If you plan to use Prime Performance Manager for NetFlow reports, use the ppm tune command to optimize Prime Performance Manager for NetFlow.

- ppm tune netflow—Tunes all parameters including jvmsize.
- ppm tune netflow nojvmsize—Tunes all parameters listed above except jvmsize.

- /sbin/sysctl -p—Applies Linux kernel changes immediately without requiring a reboot.

Monitor the unit logs/messageLog.txt to ensure no socket receive buffer error strings are displayed. For information about the ppm tune command, see ppm tune, page B-116.

When configuring NetFlow for reports, keep the following in mind:

- To support UDP, configure the NetFlow collector IP address and the UDP destination port on the sending router. The NetFlow collector IP address is the unit server IP Address. The destination UDP port needs an available unit port. All configured devices must send NetFlow packets to the same unit UDP port.
- To change the default UDP port on the unit, use the ppm netflowport command. See ppm netflowport, page B-63.
- To accurately calculate statistics, set the device active cache timeout to one minute: **ip flow-cache timeout active 1**.

NBAR2 Support

Network-Based Application Recognition 2 (NBAR2), or Next Generation NBAR, is a revised Cisco NBAR architecture. NBAR is a method through which Cisco routers and switches identify data flows to determine the flow traffic category.

Prime Performance Manager provides the following NBAR2 application reports:

NetFlow > NetFlow Applications:

- Conversations
- Destinations
- Interfaces
- Source Destinations
- Sources
- ToS

An Application column is added to the table view of existing NetFlow All Flows reports. When defining the flow record on the managed device, verify the application name matches as one flow record key, for example:

```
cisco_281(config-flow-record)#match application name
```

This statement allows NBAR data to be included in the NetFlow records.

Flow Start and End Times

Prime Performance Manager uses the time values sent in the packet header and in the flow to calculate the exact flow start and end times. The flow start and end times help Prime Performance Manager place the flow in the right reporting interval.

For NetFlow Version 1-9, the flow sysUpTime and UTC seconds headers and flowStartSysUpTime and flowEndSysUpTime are used for calculation.

For IPFIX Version 10, several field combinations can be sent in the flow. Prime Performance Manager uses these fields and the UTC seconds header to calculate the flow start and end times.

Valid IPFIX combinations include:

- systemInitTimeMilliseconds, flowStartSysUpTime, flowEndSysUpTime

Note If start and end uptime fields are sent in the flow, the systemInitTimeMilliseconds field is also required to calculate the reporting interval.

- flowStartSeconds, flowEndSeconds
- flowStartMilliseconds, flowEndMilliseconds
- flowStartMicroseconds, flowEndMicroseconds
- flowStartNanoseconds, flowEndNanoseconds
- flowStartDeltaMicroseconds, flowEndDeltaMicroseconds

Example of NetFlow IPFIX record collecting on absolute timestamps:

```
flow record netflow
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match interface output
match application name
collect datalink mac source address input
collect datalink mac destination address input
collect routing destination as
collect routing next-hop address ipv4
collect ipv4 dscp
collect ipv4 id
collect ipv4 source prefix
collect ipv4 source mask
collect ipv4 destination mask
collect transport tcp source-port
collect transport tcp destination-port
collect transport tcp flags
collect transport udp source-port
collect transport udp destination-port
collect flow direction
collect flow sampler
collect counter bytes
collect counter packets
collect timestamp absolute first
collect timestamp absolute last
```

Missed Flow Sequence Numbers Report (MFSNs)

The NetFlow Metrics Missed Flow Sequence Numbers (MFSNs) report captures the NetFlow header Sequence Number fields in the NetFlow Header. The Sequence Number value has a different meaning, depending on the NetFlow version:

- Version 5—The total flows sent by the device. For example, if the number of flows is 20, the sequence increments by 20 with every packet sent from the device. Reports for this version help identify flows sent by the device but not received by the collector.
- Version 9—A running sequence of all export packet sent by the device, starting with 1 and incrementing by 1 when each packet is sent from the device. Reports for this version help identify missing packets sent by the device but not received by the collector.

- Version 10—The total flows sent by the device. For example, if the number of flows is 20, the sequence increments by 20 with every packet sent from the device. Reports for this version help identify total flows sent by the device.

To set up Prime Performance Manager for NetFlow reports:

Step 1 Log into the Prime Performance Manager GUI. See Launching the Web Interface, page 3-1.

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

Step 3 Click the link of the first device configured for NetFlow.

Step 4 On the device window, click **Data Collection**.

Step 5 In the Collector Status area, the NetFlow item displays one of the following statuses:

- Active—The device is configured to export NetFlow and the collector is receiving the flows regularly.
- Not Active—The device is configured for NetFlow but it might not be receiving flows recently.
- Not Configured—The device is not configured for NetFlow export.

Step 6 Repeat Steps 2 through 5 to identify all the NetFlow devices.

Step 7 Enable the NetFlow reports:

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

b. Click **Report/Group Status**.

c. Navigate to the NetFlow reports and enable the ones you want to see.

Note Some NetFlow reports display detailed NetFlow stream information. These reports are available only for the lowest enabled interval and are not aggregated to higher intervals. These reports can be viewed only from the device level, for example, the NetFlow All Flows reports.

Setting Up NetFlow Reports For IP Addresses

You can create NetFlow reports for specified IP addresses or address ranges assigned to logical entities that you want to monitor, for example, a customer, building, department, or other logical entity for which you want to monitor data.

To set up NetFlow reports for IP addresses:

Step 1 Log into Prime Performance Manager using the CLI.

Step 2 Navigate to the IP group definition file:

```
/opt/CSCOppm-gw/etc/IPGroupSchema
```

Step 3 Open **IPGroupSchema** with a text editor.

Step 4 Add the IP address(es) and/or IP address range(s):

- You can list addresses separately or as IP ranges.
- Each line represents one unique IP group definition. If two lines are entered for the same group, the second definition overrides the first definition.

- Use commas to separate IP addresses (or IP ranges).
- List IPv6 addresses individually and not in a range format. IPv4 addresses can be listed in a range format.
- IPv4 group definition examples:
  - groupA = 10.10.10.10,192.168.0.3,10.10.11-13.5
  - groupB = 20.20.20.10-20, 20.20.21.*
- IPv6 group definition examples:
  - groupV6A = 2001::cafe:1,2001::cafe:2,2001::cafe:3
  - groupV6B = 2012:20bf:30cf:40df:50ef:60ff:beef:1,2013:0:0:0:32e4:dbff:fe32:f4c0

Step 5 Configure NetFlow on the device and verify that NetFlow records are exported successfully.

Step 6 To view IP address reports:

a. Log into the Prime Performance Manager GUI.

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

c. In the report navigation tree, click **Reports > NetFlow > NetFlow IP Group**.

The IP group reports are divided by source and destination.

Setting Up NetFlow Reports For Top XX Entries

By default, Prime Performance Manager displays the top 10 report items for any report. This number can be changed at the system and individual user level. For example, the system setting could be 25, which allows individual users to change their Top XX setting to any number below 25.

To implement this feature for NetFlow reports, add a seriesLimit tag with the value MAX_CHART_SERIES_NETFLOW into the GraphSummary section of the NetFlow webreport.

```
<GraphView>
            <GraphSummary title="gstNetFlowSrcASAggStats"
seriesLimit="MAX_CHART_SERIES_NETFLOW"/>
            <Graph title="gtNetFlowSrcASAggBytes" showTotal="true">
                <Column name="bytes" showPercentageColumn="true">inBytes</Column>
            </Graph>
```

For information about editing Prime Performance Manager reports, see Creating Web Reports, page 7-57 or the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*.

Setting Up StarOS 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 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 retrieves 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 StarOS Device Bulk Statistics Configuration" procedure on page 8-24 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 uses 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-unit/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 Devices With Prime Performance Manager." For information about the Prime Performance Manager alarms management, see Chapter 10, "Managing Network Alarms and Events."

Prime Performance Manager might raise bulk statistics alarms. See Bulk Statistics Alarms, page 8-28 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 StarOS 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 not configured for bulk statistics or Prime Performance Manager is not receiving files from this device.

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 might 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 containing the version information. 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 StarOS 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 StarOS schema file. It is located in the install directory:

/opt/CSCOppm-gw/install/ASR5K_BulkStats_Schemas_Counters.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 schema file for the *schemafilename*:

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

For information, see ppm starbuild, page B-101.

Step 3 Enter the IP address of the 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.

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

Note If you need to change the default 14 days bulk statistics age use the ppm bulkstatsage command. For information, see ppm bulkstatsage, page B-20.

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 Config To: staros-bulkstats-config.txt
```

Note You can press **Enter** to each prompt and change the values by editing the generated output file later.

Note The config file generates with limit 1000. Change this value to one based on the bulkstats file size expected in your deployed network. For information about the StarOS limit command, see the Command Line Interface Reference, StarOS.

Removing StarOS 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.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 StarOS Bulk Statistics Schemas or Counters

If you must generate a configuration for a subset of schemas or add new schemas, modify the spreadsheet included in the install directory.

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

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

Note If you must remove counters within a schema, 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 StarOS Bulk Statistics Schema File

To add a new schema or counter to an existing Prime Performance Manager report or to a new report, 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 must 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 command with the -ppm option:

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

Step 3 Enter the output file name:

```
Enter Output Filename To Write PPM Schema: /opt/CSCOppm-gw/etc/bulkstatsschema.csv
PPM Schema File Written To: /opt/CSCOppm-gw/etc/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
```

Upgrading StarOS devices and Prime Performance Manager to ensure Version Compatibility

StarOS device versions must be compatible with the Prime Performance Manager release versions as described in the Version Compatibility Matrix Table as shown in Table 8-2.

Table 8-2 Version Compatibility Matrix Table

PPM Releases	New StarOS Versions Supported
1.7.0.1711	21.4
1.7.0.1709	21.3
1.7.0.1705	21.2, 20.3
1.7.0.1703	21.1
1.7.0.1701	21.1 EFT2, 19.6
1.7.0.1611	21.0, 19.5
1.7.0.1609	20.2
1.7.0.1607	20.1, 19.4
1.7.0.5	20.0, 18.6
1.7.0.4	19.3, 18.5
1.7.0.3	19.2
1.7.0.2	19.1, 18.4, 17.6, 17.5
1.7.0.1	19.0
1.6.0.4	18.3, 17.4
1.6.0.3	18.2, 17.3, 16.5
1.6.0.2	18.1, 18.0, 17.2, 15.6
1.6.0.1	17.1
1.5.1.3	16.4, 16.3, 15.5
1.6	17.0

Each Prime Performance Manager version supports the corresponding StarOS versions mentioned in Table 8-2 and the earlier StarOS versions. For example, 1703 manages StarOS 21.0 and earlier versions.

To upgrade StarOS devices and Prime Performance Manager, follow the steps:

Step 1 Upgrade the StarOS device.

For more information, see Upgrading the Operating System Software.

Step 2 Upgrade Prime Performance Manager.

For more information, see Upgrading Prime Performance Manager.

Step 3 Complete the Creating the StarOS Device Bulk Statistics Configuration, page 8-24 to generate the device configuration.

Step 4 Copy the generated configuration to the Cisco ASR 5000 or Cisco ASR 5500 devices.

APN Reports

In the Prime Performance Manager 1.7 1609 and later releases, QCI and ARP keys are added for the StarOS APN reports.

You need to update the bulkstats configuration in the ASR 5000 device with the latest bulkstats configuration if the Prime Performance Manager Release is earlier to 1.7 1705. If the bulkstats config is not updated, the Prime Performance Manager shows “Data Unavailable for report” for StarOS APN reports.

HNBGW RTP Statistics Reports

You need to configure the service name of HNBGW and GTPU services to the same value so that the HNBGW RTP statistics reports are generated successfully.

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 are 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—The file name parameter is missing or 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 the drop directory with the 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 Missing Sample Interval.
  ```

  If necessary, you can modify the following properties in BulkStats.properties

  FILENAME_SUBSTR = _bulkstats_

  FILENAME_DELIMITER = _

  DATE_VARIABLE_FORMAT = yyyyMMdd

  TIME_VARIABLE_FORMAT = HHmmss

- BulkStatsInfo Alarm—Indicates files have no header or 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 they can transfer the CSV files 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, you can modify the following properties 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, you can edit the following property in BulkStats.properties to control the wait duration:

FOOTER_WAIT_TIME = 3

- BulkStatsError Alarm—The device is discovered but no files are 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—The device is 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—The device is 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—Indicates 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 are 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

Setting Up StarOS Quantum Virtual Packet Core Reports

Prime Performance Manager supports the following virtual cloud architectures:

- Quantum Virtual Packet Core - Single Instance (QvPC-SI)—QvPC-SI is essentially StarOS running within a virtual machine (VM). The Single Instance architecture is best suited for low capacity scenarios. Each QvPC-SI VM takes on the roles of an entire StarOS system. The only interfaces exposed outside the VM are those for external management and service traffic. Each QvPC-SI is managed independently.
- Quantum Virtual Packet Core - Distributed Instance (QvPC-DI)—QvPC-DI addresses the scaling and redundancy limitations of QvPC-SI by extending the StarOS boundaries beyond a single VM. QvPC-DI allows multiple VMs to act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management.

  QvPC-DI operates as a fully distributed network of multiple VMs grouped to form a StarOS instance with following major components:

  – QvPC-DI Control Function CF VMs —Two CF VMs act as an active:standby (1:1) redundant pair. The active CF is responsible for controller tasks, local context MGMT, system boot image, out of band management.

  – QvPC-DI Service Function SF VMs—SF VMs provide service context (user I/O ports) and handle protocol signaling and session processing tasks. A QvPC- DI instance can contain up to 46 SF VMs. A minimum configuration for a QvPC-DI instance requires four SFs - two active and two in standby mode.

  – QvPC-DI Network—In order for the VMs within a QvPC-DI instance to communicate with each other, each QvPC-DI instance must have a private L2 network that interconnects the VMs. The QvPC-DI network must be for the exclusive use of a single QvPC-DI instance. No other devices might be connected to this network.
- Quantum Virtual Packet Core - Virtualized Services Module (VSM) (QvPC-VSM) on Cisco® Aggregation Services Router (ASR) 9000 Series—QvPC-VSM consists of a single StarOS instance running in a VM on a Cisco ASR 9000 VSM. The VM is represented as a virtual card with a single CPU subsystem.

Install StarOS in the virtualized environment using the StarOS product documentation. After you install StarOS, complete the following configuration steps specific for Prime Performance Manager:

Step 1 Configure the SNMP read community string on the device.

Step 2 Configure the system host name to a unique value across the network. This value must match the %host% bulk statistics counter value.

Step 3 Verify the required number of cards are active using the "show card table" CLI on the device. For SI and VSM, one virtual card should be up with an operation state as Active. For DI, a minimum of six virtual cards must be up: one active CF, one standby CF, two active SFs ,and two standby SFs.

Step 4 Verify the clock is set correctly on the device. (You can use the **show clock** command.)

Step 5 Configure the bulk statistics receivers and Prime Performance Manager bulk statistics. Verify the bulk statistics files drop to the Prime Performance Manager drop directories.

After you complete these steps, you can discover QvPC devices. For information, see Chapter 5, “Discovering Devices With Prime Performance Manager.”

Step 6 Enable the QvPC report following steps in the “Customizing Report Display” procedure on page 7-13. The report is located in Reports > Availability > QvPC - DI - VM. It shows all the VMs that are grouped together to form a StarOS DI instance along with the specific slot number, UUID for each distributed VM, the VM type SF/CF and the Operation State of each VM.

Converting StarOS Bulk Statistics CSV Input Files to 3GPP XML Exports

Prime Performance Manager supports the direct conversion of StarOS bulk statistics CSV input files to 3rd Generation Partnership Project (3GPP) XML exports. You have the option to export 3GPP XML files with delta calculations for counter type bulk statistics variables.

After you enable the export, each input StarOS bulk statistics CSV file has a corresponding converted export file. These files are created after the input CSV is parsed and placed in the user-specified drop directory accessible from the unit server. The directory can be mounted on SAN storage. The files collected in the export drop directory are automatically cleaned using the Bulk Stats Export Age value set in Administration menu > System Settings > Report Settings.

The converted files can also be created in CSV in the same format and filename as the input bulk statistics CSV, but with delta calculations for counter type bulk statistics variables. The converted files can be zipped in the end if you set the ZIP_EXPORT_FILES property in /opt/CSCOppm-unit/properties/BulkStats.properties to true.

The export is not enabled by default. To enable it, use the following commands:

- ppm starexp (See ppm starexp, page B-103.)
- ppm starexpdropdir {dir} (See ppm starexpdropdir, page B-103.)
- ppm starexprules (See ppm starexprules, page B-104.)
- ppm starexpxmlformat (See ppm starexpxmlformat, page B-104.)
- ppm statreps bulkstatsexpage (See ppm statreps bulkstatsexpage, page B-104.)

Setting Up Generic CSV Bulk Statistics Reports

The generic CSV bulk statistics collection framework allows you to customize and define the CSV file format used to parse the CSV bulk statistics files. End users write the report extensible markup language (XMLs) to retrieve the counter metrics from the CSV bulk statistics files using the GenericCsvPoll macro definition.

For sample template definition files and report XML usage of the GenericCsvPoll macro, see examples in /opt/CSCOppm-gw/samples/csvstats. The properties files are the template definitions that need to be copied to /opt/CSCOppm-gw/etc/csvstats/user/ after you customize them. The XML files are report poller definitions that you must copy to /opt/CSCOppm-gw/etc/pollers/user/ after customizations are completed.

To set up generic CSV bulk statistics reports, complete the following procedures:

- Defining a Generic CSV Bulk Statistics Template, page 8-31
- Setting Up Devices to Drop Files in the Drop Directory, page 8-33
- Writing Report XML Definitions to Retrieve Metrics, page 8-33

Defining a Generic CSV Bulk Statistics Template

A template property file has properties that help Prime Performance Manager read and parse the CSV bulk statistics file. One template file is written for each generic CSV collection type. The template is saved in /opt/CSCOppm-gw/etc/csvstats/system or the user folder with properties filename extension.

The filename or the template name must be unique in both the csvstats/system and csvstats/user folders. The templates in /opt/CSCOppm-gw/etc/csvstats automatically synchronizes to all the connected units. Key properties include:

- header—Comma-separated fields occurring in the CSV in the same order as expected in the CSVs.

  Note All statistical data row in the CSV file must match with the fields defined in header property.

- checkHeader—If set to true, Prime Performance Manager validates the first CSV line starting with the first token in the header property. Prime Performance Manager raises alarm if checkHeader is true and the first CSV file line does not match the header property. The file is skipped. If checkHeader is false and CSV has a header line matching the header property, the line is skipped.
- footer—Defines the text for the last CSV file line. Enable this property only when CSV files have a specific footers.
- checkFooter—Operates the same as checkHeader but but checks the footer.
- dropDir—The folder path where CSV files are dropped from the devices. The same folder is used for all the devices using the same collection type. Folder can be mounted on a storage area network (SAN) or local disk. Prime Performance Manager must have read and write access to the folder used for collection.

  Note Only one drop can exist for one specific CSV file format. If a different CSV format must be monitored and processed, then you must define a new template with its own drop directory location.

- skipLines—Indicates other CSV non-data lines that might be skipped during CSV file parsing. The lines can occur anywhere in the CSV, not necessarily at the beginning or end.

  The format of the CSV filenames is always nodeid_constant_datetime.extension.

  The filename starts with Node or Device Identifier. This can be sysname, displayname, customname, syncname or primaryIP. The middle of the filename is a constant that can be made up of one or more strings. Date and Time follow the constant and indicate whether a file is ready to age, sort files to process oldest file first, and so on. The date and time format must include year, month, day, hour, minutes, seconds and, timezone information. The following properties further define the filename. Extensions can be csv, gz or zip.

  – filenameNodeID—Identifies the attribute Prime Performance Manager uses to identify the device. Valid values are sysname, displayname, customname, syncname or primaryIP. For example, if you choose sysname, Prime Performance Manager uses the device system name to look up the device and associate the CSV file to that device.

  Note Each CSV file has statistics for only one device. The device must be identified by one of the filenameNodeID attributes.

  – filenameDelimiter—Delimits the various filename sections.

  – filenameConstant—Identifies the text used in the constant part of the filename. This can be one or more strings separated by the filenameDelimiter.

  – filenameExtension—The filenameExtension is csv, gz, or zip.

Each CSV statistics row must contain a date and time field that helps calculate the start and end reporting interval for that row. The following fields help calculate the reporting interval and the format used to parse the field. The index is the field position in the header property starting with zero for the first field.

- startTimeIndex—The field index number used for reporting the interval start time.
- startTimeFormat—The measurement or format used to parse the start time field. The values can be epochsecs, epochmillisecs, epochmins, or custom date and time format.
- endTimeIndex and endTimeFormat—If the start time cannot be specified, you can use the endTimeIndex and endTimeFormat properties to indicate the end time of the reporting interval.
- durationIndex—Helps calculate the start or end times when only one of them can be indicated in the CSV file. The applicable durationFormat are secs, millisecs, or minutes. If duration cannot be specified, the sampleInterval property is specified.

Note See the property files defined in /opt/CSCOppm-gw/etc/csvstats/system for complete list of applicable property definitions and usage.

Setting Up Devices to Drop Files in the Drop Directory

Setting up devices to drop files in the drop directory is similar to other bulk statistics device setups that send CSV files to the Prime Performance Manager unit where the device is discovered. The mechanism that sends files is implementation-specific and left to you to choose. Multiple templates are available, so be sure to send files to the correct drop directories indicated in the template file.

Prime Performance Manager monitors all drop directories based on the templates in the /opt/CSCOppm-gw/etc/csvstats/system or user folder. After new files arrive, Prime Performance Manager starts processing the CSV bulk stats files specific to the collector type.

Prime Performance Manager can raise bulk statistics alarms when files are skipped or when filename attributes are missing or incorrect. See Bulk Statistics Alarms, page 8-28 for more information on bulk statistics alarms.

Writing Report XML Definitions to Retrieve Metrics

To collect metrics from the generic bulk statistics framework you must write your report in extensible markup language (XMLs) using the GenericCsvPoll macro. The template file name without the properties extension is passed as the first argument of the GenericCsvPoll followed by the fields to pull from CSV files.

Note See the **GenericCsvPoll** macro description in the *Cisco Prime Performance Manager 1.7 Integration Developer Guide* for more details.

Setting Up Small Cell Reports

If you are using Prime Performance Manager to monitor small cell devices, you must first complete the following steps:

Step 1 Run one of the following command to tune other small cell parameters:

ppm tune smallcell

For information, see ppm tune, page B-116.

You must also add the small cell devices to Prime Performance Manager and perform a number of configurations and configure the following small cell devices:

- RAN Management System (RMS) Central node—Device Command and Control (DCC) UI.
- RMS Serving node—Broadband Access Center (BAC) Device Provisioning Engine (DPE), Prime Network Registrar (PNR), and Prime Access Registrar (PAR) components.
- RMS Upload Server
- 3G and 4G Access Points (APs)

Note Prime Performance Manager supports the following R.MS components with redundant mode (reports based on properties in /opt/CSCOppm-gw/etc/csvPull/system/): PMG, ULS, BAC, DCCUI, CDNS. The procedure to add redundant RMS components into Prime Performance Manager. is the same with those in standalone mode.

Concepts and procedures for discovering and configuring small cell devices are provided in the following topics:

- Adding Central RMS Nodes to Prime Performance Manager, page 8-34
- Adding Upload Servers to Prime Performance Manager, page 8-36
- Setting Up Broadband Access Center Reports, page 8-39
- Running AP Reports, page 8-40
- Collecting Small Cell Access Point Inventory Data, page 8-46

Adding Central RMS Nodes to Prime Performance Manager

The RMS central node PMG component provides its performance statistics in CSV files. Currently Prime Performance Manager only supports the pmg-perf-periodic.csv file, which is located in /rms/log/pmg/ by default.

pmg-perf-periodic.csv is archived regularly as gzip files. After each archive the pmg-perf-periodic.csv contains only the lines added after the last archive. Prime Performance Manager unit regularly pulls the pmg-perf-periodic.csv file from PMG by SCP over SSH, then finds the lines of statistics added after the last pull. Prime Performance Manager processes the new lines and stores the statistics in the database.

PMG might archive the pmg-perf-periodic.csv file between two continuous pulls by Prime Performance Manager. When this occurs, Prime Performance Manager goes to the latest archived .csv.gz file to find the last line it processed.

```
[rms-aio-central] /rms/log/pmg $ ls -l pmg-perf-periodic.csv
pmg-perf-periodic.csv

[rms-aio-central] /rms/log/pmg $ ls -l pmg-perf-periodic-*.csv.gz
-rw-r--r--. 1 ciscorms ciscorms 125 Nov  9 00:03 pmg-perf-periodic-11-08-2014.0.csv.gz
-rw-r--r--. 1 ciscorms ciscorms 125 Nov 10 00:03 pmg-perf-periodic-11-09-2014.0.csv.gz
-rw-r--r--. 1 ciscorms ciscorms 125 Nov 11 00:03 pmg-perf-periodic-11-10-2014.0.csv.gz

[rms-aio-central] /rms/log/pmg $ more pmg-perf-periodic.csv
```

```
Server restarted.
period end,summary period sec,msg name,avg response time ms,max response time ms,min
response time ms,num msgs,num errors
2013-05-24T00:00:00.519Z,1913,GetAllFRMPools,69,87,53,16,0
2013-05-24T00:00:00.520Z,1913,SetFRMPools,115,130,100,2,0
2013-05-24T00:00:00.520Z,1913,GetFRMGroupType,78,84,73,5,0
2013-05-24T00:00:00.520Z,1913,GetAllFRMGroupTypes,88,124,69,23,0
2013-05-24T00:00:00.521Z,1913,GetAllFRMPoolTypes,87,377,54,34,0
2013-05-24T00:00:00.521Z,1913,GetFRMPools,53,53,53,2,0
2013-05-24T00:00:00.522Z,1913,GetAllFRMGroups,122,205,86,28,0
2013-05-24T01:00:00.517Z,3599,SetFRMGroups,88,108,69,13,0
2013-05-24T01:00:00.518Z,3599,GetFRMGroupType,66,90,39,21,0
2013-05-24T01:00:00.518Z,3599,SetFRMPoolType,90,160,57,6,0
2013-05-24T01:00:00.518Z,3599,Register,92,184,70,11,0
2013-05-24T01:00:00.519Z,3599,SetFRMGroupType,129,186,85,5,0
2013-05-24T01:00:00.519Z,3599,GetFRMPoolType,56,59,52,6,0
2013-05-24T01:00:00.519Z,3599,GetFRMGroups,80,126,53,26,0
2013-05-24T01:00:00.520Z,3599,GetAllFRMPoolTypes,69,93,46,37,0
2013-05-24T01:00:00.520Z,3599,GetAllFRMGroups,82,147,47,47,0
2013-05-24T01:00:00.520Z,3599,GetAllFRMGroupTypes,74,96,54,23,0
2013-05-24T01:00:00.521Z,3599,GetAllFRMPools,69,86,55,30,0

Server restarted.
```

To add the Central RMS node to Prime Performance Manager:

Step 1 Verify that Network Time Protocol (NTP) is synchronized between Prime Performance Manager unit and the small cell devices.

Step 2 Configure the RMS node SNMP credential. See Adding SNMP Device Credentials, page 5-3.

Step 3 Configure the RMS node SSH credential. See Adding Device Credentials for Other Protocols, page 5-6.

Step 4 Complete the RMS node discovery. See Managing Device Credentials, page 5-3.

Step 5 Verify the etc/csvPull/system/pmg-perf.properties file settings on the gateway are consistent with the PMG configuration. The gateway synchronizes the file to all units. If settings are inconsistent, make the appropriate changes:

a. Verify the activeFileDir and activeFileName so Prime Performance Manager knows the pmg-perf-periodic.csv absolute file path.

b. Verify the rollOverFileDir and rollOverFilePattern so Prime Performance Manager knows where the archived csv files are located in PMG.

c. Verify the headerPrefix matches the pmg-perf-periodic.csv header line. This setting tells Prime Performance Manager which line is the CSV file header. Configure the fixed part that the header line starts with, such as period end. Do not configure the whole header line because the header line might change across different versions.

d. Verify the skipLines. PMG creates a line Server Restarted in the CSV file when it is started or restarted. Prime Performance Manager ignores this line by configuring it in the skipLines field.

e. Verify the endTimeFormat. This is the date and time format for the first field period end in the CSV file.

Sample pmg-perf.properties:

```
[root@crdc-c240-176 CSCOppm-unit]# more etc/csvPull/system/pmg-perf.properties
# Copyright (c) 2014 by Cisco Systems, Inc.
#
# The active file directory: absolute path
```

```
activeFileDir = /rms/log/pmg/
# The active file name
activeFileName = pmg-perf-periodic.csv
# Archived file directory: absolute path
rollOverFileDir = /rms/log/pmg/

# Archived file name pattern
rollOverFilePattern = pmg-perf-periodic-.*.csv.gz

# File content delimiter
contentDelimiter = ,

# The fixed part that the header line starts with, used by Prime Performance Manager to
identify the header line.
# Don't configure the whole header line here because the header line may be different
across versions.
headerPrefix = period end

# Specify non-data lines to be skipped in CSV file.
# Separate multiple lines with comma, for each line just specify the intial part the line
starts with.
# PMG creates a line "Server restarted." in its CSV file when it's started/restarted.
skipLines = Server restarted.

# Format of the "period end" field in the CSV file.
endTimeFormat = yyyy-MM-dd'T'HH:mm:ss.SSS
```

Note You only need to configure the etc/csvPull/system/properties/pmg-perf.properties file. The etc/csvstats/system/pmg-perf.properties file, which used to configure how Prime Performance Manager pulls CSV and generate intermediate CSV files, is removed in this release.

Adding Upload Servers to Prime Performance Manager

Upload Servers provide their performance statistics (non-AP statistics) in CSV files. Currently Prime Performance Manager only supports the upload-perf-periodic.csv file located under /opt/CSCOuls/logs/ by default. upload-perf-periodic.csv is archived regularly as gzip files. After each archive, upload-perf-periodic.csv contains only the lines added after the last archive.

Prime Performance Manager units regularly pull the upload-perf-periodic.csv file from the Upload Server using SCP over SSH and finds the statistics lines added after the last pull. The new lines are processed and the statistics are stored in the database.

The Upload Server might archive the upload-perf-periodic.csv file between two continuous pulls by Prime Performance Manager. If this occurs, Prime Performance Manager goes to the last archived .gz file to find the last line it processed.

```
[admin1@rms-aio-upload logs]$ ls /opt/CSCOuls/logs/upload-perf-periodic.csv
/opt/CSCOuls/logs/upload-perf-periodic.csv[admin1@rms-aio-upload ~]$ more
/opt/CSCOuls/logs/upload-perf-periodic.csvperiod end,period duration (sec),uptime ms,
SB uploads completed,SB uploads failed,SB status sent,SB status failure,SB bytes rcvd,
SB bytes sent,SB session timeout,NB downloads completed,NB downloads failed,NB bytes
rcvd,NB bytes sent,NB session timeout,Bytes before compression,Bytes after
compression,Bytes deleted,Bytes archived,Number of files listed,Number of files
deleted,Number of files archived,Total time compressing,Total time archiving,Total time
deleting,Total time listing,Number of archives,Total stat files,Total stat bytes,
Total demand files,Total demand bytes,Total unknown files,Total unknown bytes,max
concurrent uploads,max concurrent downloads
```

```
2014-11-12T00:00:00.000,3599,1705636932,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,7,2,0,0,0,0,0,0,0,0,0
2014-11-12T01:00:00.000,3599,1709236932,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,8,1,0,0,0,0,0,0,0,0,0
2014-11-12T02:00:00.000,3600,1712836932,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,6,1,0,0,0,0,0,0,0,0,0
2014-11-12T03:00:00.000,3600,1716436932,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,7,1,0,0,0,0,0,0,0,0,0
2014-11-12T04:00:00.001,3600,1720036933,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,8,2,0,0,0,0,0,0,0,0,0
2014-11-12T05:00:00.001,3600,1723636933,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,7,2,0,0,0,0,0,0,0,0,0
2014-11-12T06:00:00.000,3599,1727236932,0,0,0,0,0,0,0,160,0,169872,77520,0,0,0,0,0,80,0,0,
0,0,7,1,0,0,0,0,0,0,0,0,0

 [admin1@rms-aio-upload ~]$ ls -l /opt/CSCOuls/server-perf-archives/daily_archives/
-rw-r--r--. 1 ciscorms ciscorms  572 Nov  9 00:00 upload-perf-periodic-2014-11-08.0.gz
-rw-r--r--. 1 ciscorms ciscorms  549 Nov 10 00:00 upload-perf-periodic-2014-11-09.0.gz
-rw-r--r--. 1 ciscorms ciscorms  562 Nov 11 00:00 upload-perf-periodic-2014-11-10.0.gz
```

To add Upload Servers to Prime Performance Manager:

Step 1 Verify that Network Time Protocol (NTP) is synchronized between Prime Performance Manager unit and the small cell devices.

Step 2 Verify the Linux find utility on the Upload Server is 4.4.2 or later. If not, upgrade it following procedures in the Linux documentation. (This is required for AP reports.)

Step 3 Configure the Upload Server SNMP credential. See Adding SNMP Device Credentials, page 5-3.

Step 4 Configure the Upload Server SSH credentials. See Adding Device Credentials for Other Protocols, page 5-6.

Step 5 Discover the Upload Servers. See Managing Device Credentials, page 5-3.

Step 6 Verify the etc/csvPull/system/uls-perf.properties file settings are consistent with the Upload Server configuration. The gateway synchronizes this file to all units. If settings are inconsistent, make the appropriate changes:

a. Verify the activeFileDir and activeFileName so Prime Performance Manager knows the upload-perf-periodic.csv absolute file path.

b. Verify the rollOverFileDir and rollOverFilePattern so Prime Performance Manager knows the archived CSV file location on the Upload Server.

c. Verify the headerPrefix to match the header line of upload-perf-periodic.csv. This setting tells Prime Performance Manager the CSV file header line. Configure the fixed part that begins the header line, such as “period end”, Do not configure the whole header line because the header line might differ across different versions.

d. Verify the skipLines. The Upload Server might add server restarted lines in the CSV file when it is started or restarted. Prime Performance Manager ignores these lines by adding them to the skipLines field.

e. Verify the endTimeFormat. This is the date and time format for the first field "period end" in the CSV file.

f. For multiple Upload Servers, if CSV files are located in different directories or the CSV file name or pattern varies, configure the following per-device settings:

– activeFileDir.<node_primary_IP>

– activeFileName. <node_primary_IP>

– rollOverFileDir. <node_primary_IP>

– rollOverFilePattern. <node_primary_IP>

For example:

```
activeFileDir.192.168.0.100 = /aa/bb/cc
activeFileName.192.168.0.100 = upload-perf-periodic.csv
rollOverFileDir.192.168.0.100 = /dd/ee/ff
rollOverFilePattern. 192.168.0.100 = upload-perf-periodic-.*.gz
```

Per-device settings override the default ones if both exists.

Sample upload-perf-periodic.csv:

```
[root@crdc-c240-176 CSCOppm-gw]# more etc/csvPull/system/uls-perf.properties
# Copyright (c) 2014 by Cisco Systems, Inc.
#
# The active file directory: absolute path
activeFileDir = /opt/CSCOuls/logs/

# The active file name
activeFileName = upload-perf-periodic.csv

# Archived file directory: absolute path
rollOverFileDir = /opt/CSCOuls/server-perf-archives/daily_archives/

# Archived file name pattern
rollOverFilePattern = upload-perf-periodic-.*.gz

# File content delimiter
contentDelimiter = ,

# The fixed part that the header line starts with, used by Prime Performance Manager to
identify the header line.
# Don't configure the whole header line here because the header line might be different
across versions.
headerPrefix = period end

# Specify non-data lines to be skipped in CSV file.
# Separate multiple lines with comma, for each line just specify the intial part the line
starts with.
# Upload Server might create a line "Server restarted." in its CSV file when the Upload
Server is started or restarted.
skipLines = Server restarted.

# Format of the "period end" field in the CSV file.
endTimeFormat = yyyy-MM-dd'T'HH:mm:ss.SSS
```

Note You only need to configure the etc/csvPull/system/properties/uls-perf.properties file. The etc/csvstats/system/uls-perf.properties file, which used to configure how Prime Performance Manager pulls CSV and generates intermediate CSV files, was removed in this release.

Step 7 If you have two or more ULSs in HA mode, which means APs upload files to one of the ULS randomly, complete the following steps to add ULSs:

a. You can leave all the ULSs on one unit, or assign ULSs to multiple units. See Changing a Device-to-Unit Assignment, page 13-8.

b. Create a ULS redundancy group:

```
opt/CSCOppm-gw/bin/ppm manageulsredundancy set [RedundancyGroup] [ULS_1] [ULS_2]...[ULS_N]
```

c. Restart Prime Performance Manager.

Setting Up Broadband Access Center Reports

Cisco Broadband Access Center performance reports are supported. BAC consists of a BAC RDU component running on an RMS Central Node, and a BAC DPE component running on RMS serving nodes.

The BAC RDU and DPE provide performance counters log files in CSV format. Prime Performance Manager retrieves the log files by SCP over SSH and parses them to generate reports that can be viewed in the Prime Performance Manager GUI. Currently Prime Performance Manager only supports the perfstat.log file. By default:

- BAC RDU perfstat.log is located in /rms/data/CSCObac/rdu/logs/statistics.
- BAC DPE perfstat.log is located in /rms/data/CSCObac/dpe/logs/statistics.

BAC log file properties: perfstat.log [root@ppmgateway1 ~]# cd /opt/CSCOppm-gw /etc/bacStats/system/bac-dpe-perf.properties bac-rdu-perf.properties PNR-CDNS.properties

BAC csv KPI file propeertiess: dpeDPERMSKPI.csv, rduRDURMSKPI.csv[root@ppmgateway1 system]# cd /opt/CSCOppm-gw/etc/csvPull/system/

perfstat.log file is archived daily by renaming the current perfstat.log file to perfstat.1.log, and renaming the old perfstat.1.log (if it exists) to perfstat.2.log, and so on. The last 30 days of perfstat.log files are retained. perfstat.1.log is always the last day before the current day. This is a fixed file name pattern handled automatically by Prime Performance Manager; you do not need to configure the file name pattern in the Prime Performance Manager properties file.

The BAC RDU and DPE might archive the active perfstat.log file between two continuous pulls by Prime Performance Manager. If this occurs, Prime Performance Manager goes to the archived perfstat.xx.log files to find the last line it processed.

```
[rms-aio-central] ~ $ ls -lt /rms/data/CSCObac/rdu/logs/statistics
total 18388
-rw-rw-r--. 1 root root 223180 Nov 12 08:02 perfstat.log
-rw-rw-r--. 1 root root 662640 Nov 11 23:56 perfstat.1.log
-rw-rw-r--. 1 root root 662640 Nov 10 23:56 perfstat.2.log
-rw-rw-r--. 1 root root 660340 Nov  9 23:55 perfstat.3.log
-rw-rw-r--. 1 root root 662640 Nov  8 23:59 perfstat.4.log
-rw-rw-r--. 1 root root 662640 Nov  7 23:58 perfstat.5.log
-rw-rw-r--. 1 root root 662640 Nov  6 23:57 perfstat.6.log
-rw-rw-r--. 1 root root 662640 Nov  5 23:57 perfstat.7.log
-rw-rw-r--. 1 root root 662640 Nov  4 23:56 perfstat.8.log
-rw-rw-r--. 1 root root 660340 Nov  3 23:55 perfstat.9.log
-rw-rw-r--. 1 root root 662640 Nov  2 23:59 perfstat.10.log
-rw-rw-r--. 1 root root 662640 Nov  1 23:58 perfstat.11.log
-rw-rw-r--. 1 root root 662640 Oct 31 23:57 perfstat.12.log
-rw-rw-r--. 1 root root 662640 Oct 30 23:57 perfstat.13.log
-rw-rw-r--. 1 root root 662640 Oct 29 23:56 perfstat.14.log
-rw-rw-r--. 1 root root 660340 Oct 28 23:55 perfstat.15.log
-rw-rw-r--. 1 root root 662640 Oct 27 23:59 perfstat.16.log
-rw-rw-r--. 1 root root 662640 Oct 26 23:58 perfstat.17.log
-rw-rw-r--. 1 root root 662640 Oct 25 23:57 perfstat.18.log
-rw-rw-r--. 1 root root 662641 Oct 24 23:57 perfstat.19.log
-rw-rw-r--. 1 root root 662640 Oct 23 23:55 perfstat.20.log
-rw-rw-r--. 1 root root 662641 Oct 22 23:55 perfstat.21.log
-rw-rw-r--. 1 root root 662640 Oct 21 23:55 perfstat.22.log
-rw-rw-r--. 1 root root 662643 Oct 20 23:55 perfstat.23.log
```

```
-rw-rw-r--. 1 root root 662641 Oct 19 23:55 perfstat.24.log
-rw-rw-r--. 1 root root 296837 Oct 18 23:55 perfstat.25.log
-rw-rw-r--. 1 root root 241786 Oct 17 08:36 perfstat.26.log
-rw-rw-r--. 1 root root 667228 Oct 16 23:55 perfstat.27.log
-rw-rw-r--. 1 root root 669552 Oct 15 23:59 perfstat.28.log
-rw-rw-r--. 1 root root 669554 Oct 14 23:59 perfstat.29.log
```

You must enable the performance log (perfstat.log) for BAC RDU and DPE. See Setting Up Cisco Broadband Access Center Reports, page 8-50 to complete this and remaining report setup steps.

Running AP Reports

Access Points (APs) send performance files regularly to the Upload Server in 3GPP XML format. Upload Servers are added to Prime Performance Manager as devices, and Prime Performance Manager pulls the AP performance files from the Upload Server local disk to generate reports.

Prime Performance Manager units regularly scan the Upload Server AP file directory through SSH to find the files uploaded to it since last scan. The file names are inserted to the Prime Performance Manager AP file list queue. Prime Performance Manager periodically scans for new files and streams them back to the units.

AP reports are viewed only at the network level require ULS servers be placed in redundancy groups, In addition, you can modify the APSTATS_BACK_PERIOD parameter if you want to collect backlog data prior to the first data polling. These and other AP setup tasks are covered in the following topics:

- Setting Up AP Reports, page 8-40
- Adding Upload Servers to Prime Performance Manager, page 8-41
- Verifying AP Report Data, page 8-43

Setting Up AP Reports

To set up Prime Performance Manager for AP reports:

Step 1 On the gateway and all units, run the following command.

```
/opt/CSCOppm-gw/bin/ppm tune smallcell
```

Step 2 Configure the following settings in etc/apStats/system/RMS-ULS.properties and verify they match the Upload Server configuration:

- deviceCapability is an internal Prime Performance Manager property, do not modify it.
- Enter the top AP fileDirectory absolute path so Prime Performance Manager knows the Upload Server AP performance files location. Multiple Upload Servers might have different AP file directories. To configure per Upload Server settings, enter: **fileDirectory.<node_primary_IP>**. For example:

  ```
  fileDirectory.192.168.0.100 = /opt111/CSCOuls/files/uploads/stat
  ```

  The per-device setting overrides the default setting if both exist.

- Configure the endTimeFormat to match the endTime attribute of the <granPeriod> in the AP performance file.

  ```
  # endTime format used by the 3GPP XML file
  #   <granPeriod duration="PT900S" endTime="1970-01-01T01:15:00+01:00"/>
  endTimeFormat = yyyy-MM-dd'T'HH:mm:ssXXX
  ```

- maxFileSize controls the file size that the Prime Performance Manager unit pulls from the Upload Server. This is for performance tuning with assistant by Cisco TAC.

```
[root@crdc-c240-176 CSCOppm-gw]# more etc/apStats/system/RMS-ULS.properties
# Copyright (c) 2014 by Cisco Systems, Inc.
#
# What capability a device should have to enable this template
deviceCapability = RMS_ULS_AP

# The 3GPP XML file directory (top directory)
fileDirectory = /opt/CSCOuls/files/uploads/stat

# endTime format used by the 3GPP XML file
#   <granPeriod duration="PT900S" endTime="1970-01-01T01:15:00+01:00"/>
endTimeFormat = yyyy-MM-dd'T'HH:mm:ssXXX

# Pull and parse this amount of file size from device each time, unit: KB
maxFileSize = 81920
```

- The APSTATS_BACK_PERIOD is the amount of time, in seconds, that Prime Performance Manager looks back in time for files to pull down from the upload server. The default is 259200 seconds (three days). This setting is useful for processing the backlog after the first upload server discovery. If you have an upload server with many days of old files that they want to collect, you can modify this property for the amount of time in the past you want Prime Performance Manager to collect.

  You must set this property before Prime Performance Manager begins collecting files from an upload server. After Prime Performance Manager retrieves the first file, it will not look back before that file timestamp, regardless of the APSTATS_BACK_PERIOD setting.

The gateway automatically synchronizes RMS-ULS.properties with the units.

Adding Upload Servers to Prime Performance Manager

To add Upload Servers to Prime Performance Manager for AP reports:

Step 1 Verify that Network Time Protocol (NTP) is synchronized between Prime Performance Manager unit and the small cell devices.

Step 2 Verify the Linux find utility on the RMS server is 4.4.2 or later. If not, upgrade it following procedures in the Linux documentation.

Step 3 Configure the Upload Server SNMP credential in Prime Performance Manager. See Adding SNMP Device Credentials, page 5-3.

Step 4 Configure the Upload Server SSH credential in Prime Performance Manager. See Adding Device Credentials for Other Protocols, page 5-6.

Step 5 For Cisco RAN Management System 4.1 or later, verify the archives/stat directory is configured in RMS-ULS.properties:

```
#############################################################################
# The 3GPP XML file directory: the absolute and top AP file directory.
#
# RMS Upload Server provides compressed XML AP files in its archives/stat
# directory since RMS 4.1.
# The compressed files are in gzip format with .xml.gz file extension.
# PPM identifies the format automatically by the file extension .xml.gz,
# no need to configure this format.
```

```
#########################################################################
fileDirectory = /opt/CSCOuls/files/archives/stat
```

Note The RAN Management System 4.1 Upload Server archives/stat directory contains compressed XML AP files in gzip format with an .xml.gz file extension. Prime Performance Manager identifies the format automatically so you do not need to configure this format.

Step 6 Restart the gateway. See Restarting Gateways and Units, page 2-5.

Step 7 Discover the Upload Servers. See Managing Device Credentials, page 5-3.

Step 8 After all upload servers are discovered and all units are online, run the ppm manageulsredundancy command on the gateway for each set of ULSs that are run together in redundancy (either active-active or active-redundant):

opt/CSCOppm-gw/bin/ppm manageulsredundancy set [*RedundancyGroup*] [*ULS_1*] [*ULS_2*]...[*ULS_N*]

Where:

- *RedundancyGroup* is the name of the redundancy group. All AP data for ULSs within this redundancy group will appear under this name in Prime Performance Manager.
- *ULS_N* is the hostname or IP address of the upload server you want included in the redundancy group.

For example, you have five ULSs. ULS1 and ULS2 receive files from the same AP; ULS3 and ULS4 where ULS3 is active and ULS4 is standby, and ULS5 that is standalone. In this case, you would run the following commands:

opt/CSCOppm-gw/bin/ppm manageulsredundancy set FirstRedundancyGroup ULS1 ULS2

Creates a redundancy group called FirstRedundancyGroup composed of ULS1 and ULS2.

opt/CSCOppm-gw/bin/ppm manageulsredundancy set SecondRedundancyGroup ULS3 ULS4

Creates a second redundancy group called SecondRedundancyGroup composed of ULS3 and ULS4.

opt/CSCOppm-gw/bin/ppm manageulsredundancy set ThirdRedundancyGroup ULS5

Creates a third redundancy group, ThirdRedundancyGroup, composed solely of ULS5.

After creating the redundancy groups, you can enter the following to list the groups and see the ULSs they manage:

opt/CSCOppm-gw/bin/ppm manageulsredundancy list

Should you want to add a ULS to the third redundancy group that has only ULS5 in it, you would enter:

opt/CSCOppm-gw/bin/ppm manageulsredundancy set ThirdRedundancyGroup ULS5 ULS6

This resets the ThirdRedundancyGroup and includes ULS6 in it.

If a want to delete a redundancy group, enter:

opt/CSCOppm-gw/bin/ppm manageulsredundancy delete [*RedundancyGroup*]

Deleting a redundancy group does not delete the data collected for it; only prevents new data from being collected.

For scalability, multiple units can now collect, process, and store data from a single ULS redundancy group. Each time you add or permanently remove a unit, you must run a repartitioning command on the primary gateway:

```
opt/CSCOppm-gw/bin/ppm manageulsredundancy partitioner repartition
```

The command balances the workload across all active units. Do not run the command for short-term unit failures. When the failed unit is back up, it will catch up to the other units that did not fail.

To see the current partitioning scheme, you can run:

```
opt/CSCOppm-gw/bin/ppm manageulsredundancy partitioner print
```

This prints the current partitioning strategy. Each active unit should have an equal number of partitions of work to operate on. The partition From value is the timestamp of the most recent file collected by that unit. All units should have reasonably similar From times. If one unit is significantly behind the others, that unit may be falling behind in its processing.

Verifying AP Report Data

You can use the RMS > 3G AP Single DB Table report to verify report data for a small number of APs. Because of the report's performance impact, never enable the 3G AP Single DB Table report in production environment. Enable it only for testing and troubleshooting environment when with a small number of APs are enabled.

To verify AP report data:

Step 1 Enable the RMS 3G AP counters:

```
ppm statreps show rms3GApAllCounters
```

Step 2 From the Administration menu in the Prime Performance Manager GUI, choose **Report Status**.

Step 3 On the Administration Report Status window, expand the Small Cell Statistics category, then check the box next to RMS: 3G AP Single DB Table.

Step 4 To view report data, from the Performance menu, choose Reports, then scroll to **Small Cell Statistics > RMS** and choose 3**G AP Single DB Table**.

Step 5 When finished, disable the RMS 3G AP counters:

```
ppm statreps hide rms3GApAllCounters
```

Setting Up DCC UI Reports

The Device Command and Control (DCC) application is the RMS user interface that provides 3G access point operation, administration and management. It is a collection of tools and contains both a graphic user interface (UI) and a command line interface (CLI). The DCC enables the following functions:

- Device data export
- Upgrade monitoring
- Device group management
- Single device management for troubleshooting
- Mass connection request and reboot
- SAI pool management

Prime Performance Manager DCC UI reports include the DCC UI All Counters and DCC UI KPI reports, which provide information about DCC UI performance and data.

To enable the DCC UI reports:

Step 1 If the RMS node has not been added to Prime Performance Manager, complete the following procedures:

- Small Cell Discovery Requirements, page 5-16
- Running Device Discovery, page 5-11

If the RMS has been discovered, continue with the next step.

Step 2 Verify the settings in the gateway etc/csvPull/system/dccui-stats.properties file are consistent with the DCC UI configuration. The gateway synchronizes the file to all units. If settings are inconsistent, complete the following steps and make changes where needed:

a. Verify the activeFileDir and activeFileName so Prime Performance Manager knows the dccui-stats-periodic.csv absolute file path.

b. Verify the rollOverFileDir and rollOverFilePattern so Prime Performance Manager knows the DCC UI archived CSV files lcation.

c. Verify the headerPrefix matches the dccui-stats-periodic header line.

This setting tells Prime Performance Manager which line is the CSV file header. Configure the fixed part that starts the header line, such as period end. Do not configure the whole header line because the header line might change across different versions.

d. Verify the skipLines. The DCC UI creates a Server Restarted line in the CSV file when it is started or restarted. Prime Performance Manager ignores this line by configuring it in the skipLines field.

e. Verify the endTimeFormat. This is the date and time format for the first field period end in the CSV file.

Sample dccui-stats.properties is provided below:

```
# Copyright (c) 2015 by Cisco Systems, Inc.
#
# The active file directory: absolute path
activeFileDir = /rms/log/dcc_ui/

# The active file name
activeFileName = dccui-stats-periodic.csv

# Archived file directory: absolute path
rollOverFileDir = /rms/log/dcc_ui/

# Archived file name pattern
rollOverFilePattern = dccui-stats-periodic-.*.csv.gz

# File content delimiter
contentDelimiter = ,

# The fixed part that the header line starts with, used by PPM to identify the header
line.
# Don't configure the whole header line here because the header line may be different
across versions.
headerPrefix = Time

# Specify non-data lines to be skipped in CSV file.
# Separate multiple lines with comma, for each line just specify the intial part the line
starts with.
# DCC_UI creates a line "Server restarted." in its CSV file when it's started/restarted.
skipLines = Server restarted.
```

```
# Format of the "period end" field in the CSV file.
endTimeFormat = yyyy-MM-dd'T'HH:mm:ss.SSS
```

Setting Up Prime Network Registrar CDNS Reports

Cisco Prime Network Registrar is a DHCP product used to allocate IPSec addresses for SeGW through DHCP. The lease database can then be queried to discover the current AP IP address. Prime Performance Manager PNR reports include the PNR Caching/Recursive Domain Name System (CDNS) All Counters and DHCP KPI reports.

To enable the PNR CDNS reports:

Step 1 If the RMS node has not been added to Prime Performance Manager, complete the following procedures:

- Small Cell Discovery Requirements, page 5-16
- Running Device Discovery, page 5-11

If the RMS has been discovered, continue with the next step.

Step 2 Verify that the settings in the gateway/opt/cscoppm-gw/etc/bacStats/system/PNR-CDNS.properties file are consistent with the CDNS configuration. The gateway synchronizes the file to all units.If settings are inconsistent, complete the following steps, changes where needed:

a. Verify the activeFileDir and activeFileName so Prime Performance Manager knows the cdns_log absolute file path.

b. Verify the activeFileName so Prime Performance Manager knows the CDNS archived cdns_log files location.

c. Verify the headerPrefix matches the cdns_log header line.

This setting tells Prime Performance Manager which line is the CSV file header. Configure the fixed part that starts the header line, such as period end. Do not configure the whole header line because the header line might change across different versions.

Sample PNR-CDNS.properties is provided below:

```
# Copyright (c) 2014 by Cisco Systems, Inc.
#
# The active file directory: absolute path
activeFileDir = /var/nwreg2/local/logs/

# The active file name
activeFileName = cdns_log

#property name for HEADER_PREFIX */
headerPrefix = 11/02/2014 19:53:16 cdns Info Stats 0 22173 [
```

Collecting Small Cell Access Point Inventory Data

Small cell access point (AP) inventory data is static, and not performance KPIs for which you can create threshold crossing alerts in Prime Performance Manager. Collecting AP inventory data can be used to group AP performance reports. For example, you might want to group AP performance reports by a particular AP site or Home Node B Gateway (HNBGW).

To collect AP inventory data, you must provide information to the ApInv.properties file located in the /opt/CSCOppm-gw/etc/apInventory/template/ directory. ApInv.properties collects AP inventory from:

- Get Device Data Tool (GDDT). This script is included in the Provisioning Management Gateway (PMG) component of the RAN Management System (RMS).
- DNPrefix. DNPrefix is contained in normal AP performance file polled by other collectors.

Note Prime Performance Manager merges inventory data from DNPrefix and GDDT. When merging for a specific AP node, the inventory data coming from GDDT has a higher priority and overrides the DNPrefix data.

Information you will provide includes:

- The field name that represents the unique AP ID.
- The fields to extract from the exported GDDT CSV file.
- The path of the file exported by the GDDT script.
- The default GDDT output file extension is .csv.
- The local directory where the exported GDDT file will be copied.
- Interval in (hours) at which Prime Performance Manager retrieves the GDDT exported file from PMG. The default is 24 hours.
- The length of the time, in days, that Prime Performance Manager should keep copied CSV files. The default is three days. Files are archived and deleted after this time period.
- Indicator telling Prime Performance Manager how to treat the field, Role, in inventory data. If this property is set to false, Prime Performance Manager assigns Role with the value contained in the GDDT output identified by the field, Enterprise, or DNPrefix, identified by the field, Enterprise. Otherwise, Prime Performance Manager treats Role as a binary value, namely Enterprise or Residential.
- The name of the DNPrefix output field to reference for the Role value. The default is Enterprise.
- The name of the GDDT output field to reference for the Role value. The default is Enterprise,
- The number of attempts allowed to retrieve the GDDT output file before considering it a failure. The default is 3.
- The interval, in minutes, between each adjacent attempt to retrieve the GDDT output file, The default is 3 minutes.

Prime Performance Manager uses a minimum set of fixed field names, shown in Table 8-3. To generate small cell reports, the constructed AP inventory data must have corresponding fields names. The preferred method is to configure RMS to have field names that match the names used by Prime Performance Manager for each inventory item, whether it is from GDDT output or DNPrefix. For example, when configuring the inventory item, site, (for DNPrefix or GDDT output), the name, SITEID, should be used to match the site name used by Prime Performance Manager. If you cannot name inventory items on the RMS side, you must do additional field name mapping on the Prime Performance Manager side so Prime Performance Manager knows what field to look for a certain inventory items. The

field mapping can be configured in /opt/CSCOppm-gw/etc/apInventory/template/FieldName.properties. After you modify FieldName.properties, restart the gateway and units. See Restarting Gateways and Units, page 2-5.

Table 8-3 AP Inventory Field Names

Field Name Used by Prime Performance Manager	Description
HNB-GW	Unique ID for the Cisco ASR 5000 chassis at discretion of the SP. This tag is only provided for HNB.
HNB-GW-SRV	HNB-GW service name within a chassis. Same value as in ASR 5000 CLI. This tag is only provided for HNB.
HeNB-GW	Unique ID for Cisco ASR 5000 chassis at discretion of SP. This tag is only provided for HeNB.
HeNB-GW-SRV	HeNB-GW service name within a chassis. Same value as in Cisco ASR 5000 CLI. This tag is only provided for HeNB.
SeGW	Unique ID for SeGW chassis at discretion of SP. In case of Cisco ASR 5000 SeGW, the value is the same as for HNB-GW tag.
SeGW-SRV	Unique ID for SeGW service within the chassis. In case of Cisco ASR 5000 SeGW, the value is the same as for HNB-GW-SRV tag.
Area	Geographical area of Small Cell. Optional in some deployments - empty value or no tag.
Enterprise	Numeric enterprise ID for Small Cell. Empty value or no tag for Resi APs.
Site	Numeric enterprise Site ID for Small Cell. Empty value or no tag for Resi APs.
DeviceID	The device ID.
Chassis ID	The ID of the chassis of the multi-stack AP. Empty value or no tag for single-stack AP.
RNC ID	The HNB ID or HeNB ID.
SecondaryID	The optional secondary ID for the AP, at SP discretion. Tag can be missing or have empty value.
SW Version	Software version.
HW Version	Hardware version.
RAT Type	3G or LTE.
Manufacturer	Manufacturer.
Live HW Model	Live HW Model.
Role	Role.
RF Profile	RF Profile.

After you modify ApInv.properties, it is automatically sent to all connected units. You must restart the units. A sample ApInv.properties file is shown below:

```
# What capability a device should have to enable this template.
deviceCapability = RMS_PMG_PERF

# Name of the field representing the unique id of Access Point node.
```

```
apNodeIdField = EID

# A list of fields users want to extract from GDDT exported csv file. Empty
# value or non-explicitly specified value means users want to extract all fields
# included in the csv file.
header =

# Full path of the file exported by GDDT script.
gddtExportFile = /rms/ops/GetDeviceData-reports/latest/device-data.csv

# File extension of the GDDT output file, will use '.csv' as default
# if not explicitly specified.
fileExtension = .csv

# Local directory which the GDDT exported file will be copied to.
dropDir = /tmp/apinv/

# Interval(hours) in which PPM regularly pull GDDT exported file from RMS-PMG.
updateInterval = 24

# Length of the time(days) PPM will keep those copied csv files. Those pulled
# files will be archived and deleted after this period of time.
ageOutInterval = 3

# Toggle telling PPM how to treat the field 'Role' in inventory data. If this
# property is explicitly specified with 'false' value, PPM will assign 'Role'
# with the value contained in GDDT output(identified by field 'ENTID') or
# DNPrefix(identified by field 'EnterPriseID'). Otherwise, PPM will treat 'Role'
# as a binary value, namely Enterprise or Residential.
roleAttrBinary = true

# Name of the field in DNPrefix which we refer to for the value of 'Role',
# default with 'Enterprise'
entidInDnprefix = Enterprise

# Name of the field in GDDT output which we refer to for the value of 'Role',
# default with 'Enterprise'
entidInGddt = Enterprise

# Number of attempts allowed to retrieve GDDT output file before considered failure.
retryCount = 3

# Interval between each adjacent attempt to retrieve GDDT output file, in minutes.
retryInterval = 3
```

GDDT and DNPrefix field names must match the field names used by Prime Performance Manager listed in Table 8-3. If the field names do not match, configure the mapping in the FieldName.properties to map from GDDT to Prime Performance Manager or from DNPrefix to Prime Performance Manager.

Setting Up Ganglia Reports

The Ganglia Monitoring System is a scalable distributed monitoring system for high-performance computing systems such as clusters and grids. The Ganglia hierarchical organization is designed for cluster federations. It uses XML for data representation, External Data Representation (XDR) for portable data transport, and the Round Robin Databast (RRD) tool for data storage and visualization. For additional information, visit the Ganglia website: http://ganglia.info.

To generate Ganglia performance reports:

Step 1 Complete the "Adding SNMP Device Credentials" procedure on page 5-3 to add the SNMP credentials for the server hosting Ganglia.

Step 2 Complete the "Adding Device Credentials for Other Protocols" procedure on page 5-6 to add the Ganglia information. In the Add Credentials Entry dialog box,

- Device Name—Enter the device name.
- Connection Protocol—Choose **GMOND_SOCKET**.
- Port—Port 8649 is the default.
- Sub System—Leave blank.
- User Name—Leave blank.
- Password—Leave blank.

Step 3 Click **OK**.

Step 4 On the dialog asking if you want to save without a username or password, click **OK**.

Step 5 Complete the "Running Device Discovery" procedure on page 5-11 to add the server that hosts Ganglia.

Step 6 To view performance data for remote Gmond hosts:

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

b. In the report navigation tree choose **Compute > Ganglia > Gmond.**

The report lists all remote hosts collected by the gmond server including the local host.

Step 7 To view performance data for the local gmond host:

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

b. Choose a subcategory, for example Buffers, CPU, or Disk.

The report displays the gmond node performance data. It does not include remote hosts.

Setting Up Cisco Network Service Orchestrator Device Reports

To support reports from Cisco Network Service Orchestrator (NSO):

Step 1 Enable SNMP on the NSO server. By default, NSO runs SNMP on Port 4000.

Step 2 Add the NSO SNMP connection to Prime Performance Manager following steps in Adding SNMP Device Credentials, page 5-3, or the ppm addsnmpcomm command, for example:

```
/opt/CSCOppm-gw/bin/ppm addsnmpcomm -i NSO_IP -c public -P 4000
```

Step 3 Add the NSO SSH NETCONF credential to Prime Performance Manager following steps in Adding Device Credentials for Other Protocols, page 5-6, or the ppm addcreds command, for example:

```
/opt/CSCOppm-gw/bin/ppm addcreds -i NSO_IP -r SSH_V2 -u user_admin -p password -n
NSO_netconf_username -e NSO_netconf_password
```

Note To poll NSO through its XML management interface using NETCONF, enter the NETCONF user name and password in the Secondary Username and Secondary Password in the Prime Performance Manager Credential Editor accessed through the Network menu.

To monitor NSO devices, the NETCONF Console command is executed from the paths shown below. If you need to update the path, update the NETCONF port, console path, and query path in the Device Capability file. The defaults are:

```
<entry name="CLI_NSO_NETCONF_PORT">2022</entry>
<entry name="CLI_NSO_NETCONF_PATH">/home/arundeb/ncs-3.4.2/bin/netconf-console</entry>
<entry name="CLI_NSO_NETCONF_QUERY">/cloudvpn-data/oper-data</entry>
```

Prime Performance Manager currently supports data metric collection for the following set of NSO NETCONF queries:

oper-data/oper-state

oper-data/nodes/node/oper-state

oper-data/onnet_traffic

oper-data/internet_traffic

oper-data/connected_users

oper-data/S2S

oper-data/RA

Note To execute the CLI-based NSO reports in Prime Performance Manager, set the NSO source file path in the bash profile.

Step 4 Run device discovery to add the NSO server to Prime Performance Manager following the steps in Running Device Discovery, page 5-11 or the following command:

```
/opt/CSCOppm-gw/bin/ppm discover NSO_IP
```

Setting Up Cisco Broadband Access Center Reports

Cisco Broadband Access Center (BAC) provides information about the traffic between customer premises equipment (CPE) and the BAC device provisioning engine (DPE). This data provides visibility into traffic flows that might be causing network issues. This traffic profiling provides statistics on the following:

- The number of handled CPE WAN Management Protocol (CWMP) sessions.
- The number of rejected devices.
- The number of handled HTTP file requests.
- The Home Provisioning Group redirection status.
- Identification of traffic caused by chatty clients.

The periodic statistics provides details, including the name of each Remote Procedure Call (RPC) and the specific information message types. The following RPC methods are monitored and reported:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes

- GetParameterAttributes
- AddObject
- DeleteObject
- Download
- Reboot
- Inform
- TransferComplete
- AutonomousTransferComplete
- GetQueuedTransfers
- ScheduleInform
- SetVouchers
- GetOptions
- Upload
- FactoryReset
- GetAllQueuedTransfers
- Kicked
- RequestDownload

The BAC DPE and RDU provide performance counters log files in CSV format. Prime Performance Manager retrieves and parses the log files for reports that can be viewed in the Prime Performance Manager GUI.

To enable reports based on BAC performance logs:

Step 1 Log into the BAC RDU.

Step 2 From the user interface, choose **Configuration > Defaults > System Defaults**.

Step 3 For Performance Statistics Collection, click **Enabled**.

Step 4 To enable traffic statistics on the DPE, from the DPE CLI in the enabled mode, enter **debug dpe statistics**.

Step 5 Verify that Network Time Protocol (NTP) is synchronized between the Prime Performance Manager unit and the small cell devices.

Step 6 Enable the SNMP and SSH on the BAC system by configuring the SNMP and SSH credentials.

Note For additional information about Steps 1 through 6, see the *Cisco Broadband Access Center Administration Guide 3.8*.

Step 7 For BAC statistics performance reports, verify the parameters are correctly configured on the Prime Performance Manager gateway:

- For RDU performance statistics, see the etc/bacStats/system/bac-rdu-perf.properties file.
- For DPE performance statistics, see the etc/bacStats/system/bac-dpe-perf.properties file.

The properties files contains the log file path. It supports configuring different fileDirectory for source log files in the properties file by activeFileDir.<node_primary_IP>. It shows the default directory. If per-device configuration exists, the new directory overrides the default.

For example:

```
activeFileDir.192.168.0.100 = /aa/bb/cc
activeFileName.192.168.0.100 = perfstat.log
```

Per-device setting overrides the default one if both exists.

```
 [root@crdc-c240-176 CSCOppm-gw]# more etc/bacStats/system/bac-rdu-perf.properties
# Copyright (c) 2014 by Cisco Systems, Inc.
#
# The active file directory: absolute path
activeFileDir = /rms/data/CSCObac/rdu/logs/statistics

# The active file name
activeFileName = perfstat.log
[root@crdc-c240-176 CSCOppm-gw]# more etc/bacStats/system/bac-dpe-perf.properties
# Copyright (c) 2014 by Cisco Systems, Inc.
# The active file directory: absolute path
activeFileDir = /rms/data/CSCObac/rdu/logs/statistics

# The active file name
activeFileName = perfstat.log

[root@crdc-c240-176 CSCOppm-gw]# more etc/bacStats/system/bac-dpe-perf.properties
# Copyright (c) 2014 by Cisco Systems, Inc.
#
# The active file directory: absolute path
activeFileDir = /rms/data/CSCObac/dpe/logs/statistics

# The active file name
activeFileName = perfstat.log
```

Step 8 Enable the relevant BAC performance statistics reports (Small Cell Statistics > RMS > RMS System). For information, see Customizing Individual Report Settings, page 7-27.

Setting Up Cisco Prime Network Registrar Reports

To set up Cisco Prime Network Registrar reports, you must set up the Prime Network Registrar SNMP agent as a subagent through proxy support of the NETSNMP daemon.You can integrate the Prime Network Registrar SNMP server into the SNMP server for the system it runs on. The integration can be done in a way where the system will respond to queries for the Prime Network Registrar MIB entries. On systems using NET-SNMP (and compatible servers) this is done by adding the following entries to the /etc/snmp/snmpd.conf configuration file

view systemview included .1.3.6.1.4.1.9.9

view systemview included .1.3.6.1.4.1.9.10

proxy -v 2c -c public 127.0.0.1:4444 .1.3.6.1.4.1.9.9

proxy -v 2c -c public 127.0.0.1:4444 .1.3.6.1.4.1.9.10

The community string public and the port number 4444 might need to be replaced if the Prime Network Registrar SNMP server is configured with different values for those settings.

NET-SNMP is commonly available on Linux and other Unix-like systems. On other systems, similar mechanisms might also be available.

Ceph and KVM VM Report Notes

Ceph is a distributed object store and file system designed to provide performance, reliability and scalability. If you enabled Ceph reports (see Ceph Discovery Requirements, page 5-21), they appear under the Storage report category.

Note If no Ceph data is collected, verify that the Ceph device time is synchronized with the Prime Performance Manager server. If necessary, add an NTP server to the Ceph device.

Hypervisor-level disk space monitors the capacity and used space from a layer above the OpenStack instance where it is deployed. For local storage, this means disk space usage as viewed by the KVM hypervisor. For certain block device formats, the KVM hypervisor can allocate the entire disk capacity, even though disk capacity might not actually be used one level lower (guest level).

Prime Performance Manager provides two KVM VM disk space reports, one for the hypervisor-level storage, and one for the lower guest-level storage:

- KVM VM Hypervisor-Level Disk Space (formerly KVM VM Disk Bytes)—Supports only local storage.
- KVM VM Guest-Level Disk Space—Gathers data for both local and network (Ceph) storage back ends.

Guest-level disk space monitors the capacity and used space as it appears inside the OpenStack instance. This is the usable space in the OpenStack instance. Guest-level disk space is calculated using the libguestfs library. To monitor guest-level disk space in KVM, you must add a new device credential. Previously, only a KVM_TLS user credential was required to get hypervisor-level disk space statistics. For guest-level storage disks, a SSH_V2 user credential for the KVM device is required. The libguestfs (specifically the virt-df command) version installed on the KVM device must be 1.26.0 or later.

To get Ceph Storage and KVM VM Guest-Level Disk Space report data, the device user credential must have access to the Ceph configuration file. The default configuration file location is /etc/ceph/$clusterName.conf, where $clusterName is the name of the cluster. The default is ceph. If the user credential added to Prime Performance Manager is a non-root user, the user must have read permission in the Ceph configuration file. (If the device is not getting Ceph Storage and KVM VM Guest-Level Disk Space report data, this might be the problem.) For KVM VM Guest-Level Disk Space reports, if you follow the documentation for integrating Ceph with OpenStack, the Ceph configuration file should have the required permission. If it does not, you can set it using the chmod +r /etc/ceph/$clusterName.conf command.

ONS and CPT Device Report Notes

Prime Performance Manager provides reports at 15-minute and 1-day intervals for Cisco Optical Network Service (ONS) and Carrier Packet Transport (CPT) devices. You can access these reports in Reports > Transport Statistics > CPT/ONS. CPT and ONS device report data include:

- Ethernet interfaces—Bytes, Unicast Packets, Multicast Packets, Total Packets, Interface Discards, Interface Errors.
- G.709 Section—Errored Seconds, Severely Errored Seconds, Unavailable Seconds, Background Block Errors, Failure Counts, Errored Seconds Ratio, Severely Errored Seconds Ratio, Background Block Errors Ratio.

- G.709 Path—Errored Seconds, Severely Errored Seconds, Unavailable Seconds, Background Block Errors, Failure Counts, Errored Seconds Ratio, Severely Errored Seconds Ratio, Background Block Errors Ratio

Additionally, Prime Performance Manager supports HTTP DT FEC and DWDM client statistics.

Setting Timing Tolerance for collectd, Ceilometer, vCenter, and ESXi

Ceilometer, collectd, vCenter, and ESXi require close timing synchronization between the Prime Performance Manager unit clock and the clocks where Ceilometer, collectd, vCenter, and ESXi reside. By default, timing tolerance is set to 15 minutes (900 seconds). Prime Performance Manager monitors this timing regularly and issues alarms should timing synchronization exceed 15 minutes. You can change the tolerance using the ppm clocktolerance command. For information, see ppm clocktolerance, page B-23.

Note Synchronizing the Prime Performance Manager unit and Ceilometer, collectd, vCenter, and ESXi device clocks must be performed by your network administrator. The ppm clocktolerance command simply sets the tolerance at which alarms are raised.

Setting Up OpenStack Ceilometer Reports

OpenStack ceilometers provide a point of contact for billing systems to acquire measurements for customer billing across all current OpenStack core components. Ceilometer reports are located in the Compute > OpenStack report category.

By default, ceilometer collects metrics every 10 minutes. Prime Performance Manager allows you to configure other intervals. If the interval is lower than the ceilometer interval, Prime Performance Manager fills the data automatically by using most recent data. Therefore, the polling interval must always be larger then the ceilometer interval.

When configuring Prime Performance Manager to monitor OpenStack, review the default OpenStack Ceilometer poll interval. By default this is 10 minutes. Disable OpenStack reports that are less than the Ceilometer poll interval, otherwise Prime Performance Manager will poll OpenStack more frequently than OpenStack is updated. For example, if the OpenStack Ceilometer poll interval is the 10-minute default, disable OpenStack 1 and 5 minute reports. See Customizing Individual Report Settings, page 7-27.

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:

Options for Displaying Device Information

Prime Performance Manager provides many ways for you to see device information. Some are intended as a quick display of the highest priority device details; others are intended for detailed exploration of every single device parameter. Device information display options include:

- Network view—Displayed by choosing **Devices** from the Network menu. This view displays all network devices and allows you to see device information for all devices at one time. For information about parameters and editing options available in the network view, see Displaying Device Information at the Network Level, page 9-2.
- Device view—Displayed when you click a device hyperlink. Device hyperlinks appear in many locations including the device, alarms, and events windows. Information displayed at the individual device level is much the same as that displayed in network view, with some variations. For information about parameters and editing options available in the network view, see Displaying Device Information at the Device Level, page 9-25.
- Device Hyperlinks—You can view device details from device hyperlinks in one of two ways:
  - Mouse hover popup—A quick view of device details can be displayed when you move your cursor over a device hyperlink. The benefit of this option is speed.

  - 360 Device View—Clicking the icon next to a device hyperlink displays the 360 Network Device Details window. This window provides access to most device details including alarms and events. For information about this view, see Displaying the 360 Device Details View, page 9-23.

- Device Browser—You can display device details by clicking **Device Browser** at the bottom of the Prime Performance Manager window. The browser window displays key device details including polling data, uptime, alarms, and status. Options available in the network or device-level windows are available in the device browser.

Displaying Device Information at the Network Level

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 Device Information at the Device Level, page 9-25.)

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 9-1.

Table 9-1 Network-Level Device Information

Details	Description	For information, see
Devices	Lists all network devices and device properties.	Displaying Device Properties at the Network Level, page 9-3
Types	Displays a device distribution by device type.	Displaying Device Type Distributions at the Network Level, page 9-6
Alarms by Device	Displays alarms by device.	Displaying Alarms by Device at the Network Level, page 9-6
Alarms by Device Type	Displays alarms by device type.	Displaying Alarms by Device Type at the Network Level, page 9-7
Unreachable	Displays devices that have NodeUnreachable alarms.	Displaying Devices Time Out Alarms at the Network Level, page 9-7
NetFlow	Displays devices with NetFlow provisioned. The table displays the same device parameters as the Devices table. See Table 9-2 on page 9-3. If no network devices have NetFlow provisioned, the NetFlow tab is not displayed.	Displaying NetFlow Devices at the Network Level, page 9-7
Polling	Displays poll response data.	Displaying Device Polling Responses at the Network Level, page 9-8

Table 9-1 Network-Level Device Information (continued)

Details	Description	For information, see
Ping	Displays ICMP ping response data.	Displaying Device ICMP Ping Responses at the Network Level, page 9-9
Uptime	Displays device up time.	Displaying Device Up Time at the Network Level, page 9-9
Data Collection	Displays device data collection status.	Displaying Device Data Collection Status at the Network Level, page 9-10
Software	Displays device software information.	Displaying Device Software at the Network Level, page 9-11
Contact/Location	Displays device contacts and locations.	Displaying Device Contacts and Locations at the Network Level, page 9-11
Vendor	Displays the device manufacturer.	Displaying Device Vendors at the Network Level, page 9-12
Prime	Displays device properties in Cisco Prime format.	Displaying Device Details in Cisco Prime Format, page 9-13

Displaying Device Properties at the Network Level

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 9-2 lists the available device properties. In addition, you can change the following items in User Preferences.

- Device details displayed from device hyperlinks—You can display device details from hyperlinks either as a popup that automatically appears when you move your mouse over the link, or in the 360 Network Device View window, which is displayed when you click an icon next to the hyperlink.

  The device details displayed in the popup or 360 Network Device View are described in Table 9-2, and Table 9-11 on page 9-26. The details display option is useful in other windows that list device links, for example, the Network Alarms window, or when drilling down to the interface report level. However, you can disable this feature in User Preferences.
- Alarm severity icons—Devices include an alarm severity icon indicating the highest level alarm on the device. You can disable this feature in User Preferences.
- Deleted devices—Deleted devices, without hyperlinks, can be displayed by enabling this option in User Preferences.

For information about changing user preferences, see Customizing the GUI and Information Display, page 3-8

Table 9-2 Devices Properties at the Network Level

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.

Table 9-2 Devices Properties at the Network Level (continued)

Property	Description
Custom Name[1]	Device custom name, if available.
Sync Name[1]	Device sync name.
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.
Annotation	Displays any annotation that was written about the device. See Annotating a Device, page 9-23.
Feature[1]	A short descriptive term for the device, if known. Otherwise, Generic.
Software Version[1]	Device software version.
Serial Number[1]	Device serial number. The serial numbers that are displayed as unknown, can be customized using the following steps: • Open the */opt/CSCOppm-gw/properties/Device.properties* file on the Prime Performance Manager Gateway. • Append the DEVICE_SERIALNUM_INDEX property with the device type OID and the serial number index separated by a colon. **Note** Append the correct index to its appropriate device type OID. Example: For cisco340024TSA, the device OID is 1.3.6.1.4.1.9.1.736, the serial number index is 1001, the entry added needs to be as follows: 1.3.6.1.4.1.9.1.736:1001 To configure multiple devices, use a comma separated string without any spaces. Example: DEVICE_SERIALNUM_INDEX=1.3.6.1.4.1.9.1.574:1001,1.3.6.1.4.1.9.1.1252:100
Last Full Poll Time[1]	The time of the last Prime Performance Manager poll.
Last Poll Response (secs)[1]	The time for the device to respond to the last poll request.
Avg. Poll Response (secs)[1]	Average time for the device to respond to Prime Performance Manager 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.

Table 9-2 Devices Properties at the Network Level (continued)

Property	Description
Discovery Source[1]	Indicates how Prime Performance Manager discovered the device: PPM (Prime Performance Manager) or Prime Network. See Chapter 5, "Discovering Devices With Prime Performance Manager."
Report Polling	Indicates whether report polling is enabled for this device.
Sending Alarms	Indicates whether 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 9-35.
Severity	If alarms are raised for the device, the highest severity: Critical, Major, Minor, Warning, Informational, Unmanaged, or Normal.
Last Status Change[1]	Date and time that the device status last changed.
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.) The stateReasons.html provides a list of possible reasons,located at: /opt/CSCOppm-gw/apache/share/htdocs/eventHelp.
Contact[1]	The device contact name, if added.
Location[2]	The device location, if added. If GPS locations are enabled, the location is displayed as a hyperlink that, when launched, displays the device location in a separate Google Maps browser session.
Polling Group[1]	The polling group to which the device is assigned. See Creating and Editing Device Polling Groups, page 9-35
Report Policy[1]	The report policy to which the device is assigned. See Creating Report Policies, page 7-33.
Vendor[1]	Device manufacturer.
Software Description[1]	Device software description, if available.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-20.
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 at the Network Level

The Network - Device Distribution by Type window presents your device type distributions in table and pie chart format. 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**.

Network - Device Distribution by Type 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 Device Properties at the Network Level, page 9-3.
- Export the data to a CSV file.
- Send the distributions pie chart to a printer or graphic image.

Displaying Alarms by Device at the Network Level

The Network - Alarms by Device window 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 9-3 lists the Network - Alarms by Device properties.

Table 9-3 Network Alarms by Device Properties at the Network Level

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.
Sending Alarms	—	Indicates whether 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 9-35.
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.

Table 9-3 Network Alarms by Device Properties at the Network Level (continued)

Column	Tool	Description
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.
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 3-20.

Displaying Alarms by Device Type at the Network Level

The Network - Alarms by Device Type window 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
  - Normal

Displaying Devices Time Out Alarms at the Network Level

The Network - Unreachable window displays devices for which a NodeUnreachable alarm is present. To display devices with unreachable alarms:

- From the Network menu, choose **Devices**, then click **Unreachable**. The table displays the same device parameters as the Devices table. See Table 9-2 on page 9-3.

Displaying NetFlow Devices at the Network Level

The Network - NetFlow window displays devices that have NetFlow provisioned. To display NetFlow devices:

- From the Network menu, choose **Devices**, then click **NetFlow**. The Network - NetFlow Enabled Devices table displays the same device parameters as the Devices table. See Table 9-2 on page 9-3.

Note If no network devices have NetFlow provisioned, the NetFlow tab is not displayed.

Displaying Device Polling Responses at the Network Level

The Network - Polling window 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 **Polling**.

Table 9-4 lists the Network - Polling information.

Table 9-4 Device Polling Responses at the Network Level

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.
Management IP Address	Device 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.
Location	The device location.
Report Polling	Indicates whether report polling is enabled for this device.
Report Policy	The report policy, if any, assigned to the device.
Polling Group	The polling group, if any, assigned to the device.
Last Full Poll Time (*device time zone*)	The date and time Prime Performance Manager last polled the device.
Last Poll Response (secs)	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.
Uptime	The amount of the time the device has been up.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-20.

Displaying Device ICMP Ping Responses at the Network Level

The Network - Ping window 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.

Note The ICMP Ping reports must be enabled in order for data to appear in the Network Ping table. The ICMP Ping reports are located in the Availability report group.

To display ICMP ping results and device availability:

- From the Network menu, choose **Devices**, then click **Ping**.

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 at the Network Level

The Network - Uptime window displays the uptime for managed devices. To display device up times:

- From the Network menu, choose **Devices**, then click **Uptime**.

Table 9-5 lists the device up time properties.

Table 9-5 Device Up Time at the Network Level

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, Unmanaged, or Normal.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-20.

Displaying Device Data Collection Status at the Network Level

The Network - Data Collection table allows you to quickly see the data collection status of devices across the network. To display the device data collection status:

- From the Network menu, choose **Devices**, then click **Data Collection**.

Table 9-6 lists the data collection status parameters.

Table 9-6 Device Data Collection at the Network Level

Column	Description
SNMP	Indicates whether the device SNMP data collector is active, inactive, or not configured for polling.
Hypervisor	Indicates whether the device Hypervisor data collector is active, inactive, or not configured for polling.
SMICollector	Indicates whether the device storage management initiative (SMI) collector is active, inactive, or not configured for polling. It is used to collect performance statistics from storage devices and network.
CLI	Indicates whether the device CLI data collector is active, inactive, or not configured for polling.
NetFlow	Indicates whether the device NetFlow data collector is active, inactive, or not configured for polling.
JMX	Indicates whether the device Java Management Extensions data collector is active, inactive, or not configured for polling.
Data Collection Manager	Indicates whether the Cisco Data Collection Manager (DCM) bulk statistics collector is active, inactive, or not configured for polling. DCM is a data collection agent that is embedded in managed devices, such as routers and switches. DCM works on a push model, which is based on a subscribe-and-notify data pattern, as opposed to the pull model, which is based on a request-and-response data pattern, in traditional SNMP-based network management.
Collectd Stats	Indicates whether the collectd statistics data collector is active, inactive, or not configured for polling. collectd is a daemon which collects system performance statistics periodically and provides mechanisms to store the values in a variety of ways.
Star OS Bulk Stats	Indicates whether the Cisco Star OS bulk statistics data collector is active, inactive, or not configured for polling. It is used to process performance statistics pushed from Cisco ASR 5000 devices.
RMS_LOGCollector	Displays Radio Access Network (RAN) Management System (RMS) upload servers log collector data.
ICMP	Indicates whether the device IP data collector is active, inactive, or not configured for polling.

Table 9-6 Device Data Collection at the Network Level (continued)

Column	Description
Small Cell	Indicates whether the Cisco Small Cell Solution bulk statistics data collector is active, inactive, or not configured for polling. It is used to collect performance statistics from small cell AP devices on a upload server in wireless access network.
Generic CSV	Indicates whether the generic CSV bulk statistics data collector is active, inactive, or not configured for polling.
GMOND	Indicates whether the Ganglia Monitoring Daemon (GMOND) data collector is active, inactive, or not configured for polling.
Internal	Internal device ID. Prime Performance Manager assigns this ID to the device for internal use.
Optical Bulk Stats	Indicates whether the optical bulk statistics data collector is active, inactive, or not configured for polling.

Displaying Device Software at the Network Level

The Network - Software window 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 9-7 lists the Network - Software parameters.

Table 9-7 Device Software at the Network Level

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.
Vendor	The device manufacturer or technology.
Software Version	Software version used by the device.
Software Description	Full software version information.

Displaying Device Contacts and Locations at the Network Level

The Network - Contacts/Locations window 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 9-8 lists the Network - Contact/Location properties.

Table 9-8 Device Contacts and Locations at the Network Level

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.
Contact	The device contact name.
Location	The device location.
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.

1. Not displayed by default. To display hidden properties, see Adding and Removing Properties from Property Views, page 3-20.

Displaying Device Vendors at the Network Level

The Network Vendors window displays the device types, manufacturers, and status. To display the device vendor information:

- From the Network menu, choose **Devices**, then click **Vendor**.

Table 9-9 displays the device vendor information.

Table 9-9 Device Vendor Information at the Network Level

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 3-20.

Displaying Device Details in Cisco Prime Format

If Prime Performance Manager is integrated with Cisco Prime Central (see "Importing Devices From Other Cisco Prime Applications"), you can display the device details in a format that matches Prime Central. Because fewer properties are displayed than the Devices tab, Prime 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**.

Table 9-8 lists the device properties displayed in the Network - Prime window.

Table 9-10 Device Details Displayed in Network - Prime

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.
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	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 3-20.

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

- Types
- Alarms by Device
- Alarms by Device Type
- Unreachable
- NetFlow
- Polling
- Ping
- Uptime
- Data Collection
- Software
- Contact/Locations
- Vendor
- Prime

See Displaying Device Information at the Network Level, page 9-2 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, Time Zone, and Location, page 9-16.
- Edit Device Credentials—Allows you to edit the device connection credentials used to poll the device. See Editing the Device Credentials, page 9-17.
- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 9-20
- Edit Polling Policy—Allows you to change the polling policy assigned to the device. See Creating and Editing Device Polling Groups, page 9-35 and Editing the Polling Group Assigned to a Device, page 9-20.
- Edit Management IP Addresses—Allows you to edit a device management IP addresses. See Editing the Device Management IP Addresses, page 9-21.
- Change Interface Polling—Allows you to remove device interfaces from polling. See Removing Device Interfaces From Polling, page 9-22.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 9-22.
- Disable Alarms and TCAs—Displays the Customize Date and Time Range dialog box in which you can configure a date and time span during which alarms and TCAs will be suppressed on the selected device(s). You can specify a specific start and end date using the calendar, or you can specify the start date and time, then click any of the time presets (1 Day, 2 Days, 1 Week, and so on).
- Enable Alarms and TCA—If you disabled alarms and TCAs, this option enables them, even if the duration specified in the Customize Date and Time Range dialog box has not been reached.
- Unmanage Device—Changes managed devices to unmanaged.
- Manage Device—Changes unmanaged devices to managed.

- Enable Maintenance Mode—Allows you to place the device in maintenance mode (polling is stopped) for a specified time period entered in the Enable Maintenance Mode dialog box.
- Annotation—Allows you to enter the notes for the selected device. See Annotating a Device, page 9-23.
- 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-68 and ppm traceroute, page B-115.

Editing a Device Name, Web Port, Time Zone, and Location

Within the device network view, you can change the device name, web port, time zone and location. To edit these device properties:

Step 1 Navigate to one of the following device views: Devices, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

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, type the first two or more letters of the time zone. The field will populate with time zones matching the letters you entered. (Time zones are expressed using the tzdata, or IANA Time Zone Database formats.)
- Location—The device location, which is displayed in the device Location property. If GPS Locations is enabled (see Changing System Configuration Settings, page 3-17), the location you enter is used to display the device location in Google Maps. If GPS is enabled, be sure to enter sufficient location information to enable Google Maps to display the device location accurately.

Step 5 Click **Save**.

Editing the Device Credentials

To edit the device connection credentials:

Step 1 Navigate to one of the following device views: Devices, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

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

- SNMP Version—Indicate the SNMP version, either 1, 2c, or 3.
- Max Table Varbind—Sets the maximum table variable binding.
- Port—Sets the SNMP port number.

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
- 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.

Other Credentials

- ID—An internal identifier.
- 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.
  - collectd_SSH—A daemon that collects, transfers, and stores performance data.
  - HTTP—HyperText Transfer Protocol.
  - HTTPS—Secure HTTP.
  - HTTP_BULK—Bulk statistics through HTTP.
  - WMI_HTTP—Windows Management Instrumentation over HTTP.
  - WMI_HTTPS—Windows Management Instrumentation HTTPS.
  - vCenter_HTTPS—VMware vCenter server over HTTPS.
  - ESXi_HTTP—VMware ESXi embedded bare metal hypervisor over HTTP.
  - ESXi_HTTPS—VMware ESXi embedded bare metal hypervisor over HTTP.S

Note When you define the credential for vCenter and ESXi devices, make sure the user account you use has the session privilege. For information, see .

  - XEN_TLS—Xen hypervisor over Transport Layer Security (TLS) protocol.
  - KVM_TLS—Linux Kernal-based Virtual Machine (KVM) over TLS.

Note Xen_TLS and KVM_TLS have discovery requirements. See Xen and KVM TLS Discovery Requirements, page 5-16

  - HyperV_HTTP—Microsoft HyperV server over HTTP.
  - HyperV_HTTPS—Microsoft HyperV server over HTTPS.
  - JMX—Java Management Extensions. Collects statistics from Java processes running on various servers.

Note JMX reports are not enabled by default. After adding the JMX credential, you will need to enable the reports. For information, see Customizing Individual Report Settings, page 7-27.

  - PNSC_HTTPS—Cisco Prime Network Services Controller secure HTTP connection.
  - GMOND_SOCKET—Ganglia Monitoring Daemon (gmond) socket.
  - SMI_HTTPS—Storage Management Initiative over HTTPS.
  - ULS_HTTP—Allows Prime Performance Manager to perform Small Cell upload server HTTP credential verification including subsystem, username, password, and credential parameters. Beyond that, ULS_HTTP is identical to HTTP protocol.
  - AVI_HTTPS—A secure connection with AVI Networks load leveling device.

- User Name—The device login username.
- Password—The password for the login user.

- Secondary Login Type—Enables
- Enable User Name—The privileged username.
- Enable Password—The privileged user password.
- 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".

Note To poll the Cisco Nexus 7000 through its XML management interface using Network Configuration Protocol (NETCONF), enter **netconf** in the Sub System field. Using the XML interface allows you to generate Border Gateway Protocol (BGP) reports.

- User Name—Enter the device login username.

Note For vCenter and ESXi devices that are members of an Active Domain, you can enter the domain and username in the format *domain/username*.

Note For KVM_TLS, if SASL is enabled on the KVM device, add Simple Authentication Security Layer (SASL) credentials to the entry. SASL usernames typically have the SASL realm appended to it, such as user@hostname. If SASL is not enabled on the KVM device, you can leave the User Name and Password fields blank.

- Password—Enter the password for the login user.
- Secondary Login Type—Indicates how the secondary user and password should be processed:
  - Enable—Executes the Cisco IOS enable command, which provides Prime Performance Manager privileged EXEC level (Level 15) access to the device.
  - Second Login—Executes the login command to log into the device using the secondary username and password. If you choose this option, the secondary user must have privileged EXEC access to the device,

Note Secondary Login Type is only available for Telnet or SSH connections.

- Secondary User Name—Enter the secondary username.
- Secondary User Password—Enter the secondary user password.

Step 5 If you entered an SSHv2 or HTTPS credential and want to use the SSHv2 key authentication, complete the following steps. Otherwise, continue with Step 6. By default, Prime Performance Manager authenticates itself to the device using the User Name and Password entries. To change to the SSHv2 authentication keys:

a. In the Client Authentication Type field, and choose **Public Key**.

b. Click the Client Private Key field.

c. In the SSH Credentials for [hostname] dialog box, enter the private key file name and click **Import**.

d. Enter the public key file name and click **Import**.

e. Click **Generate Public Key**.

Step 6 Click the **Test Credential**.

A Testing Credentials for [*device name*] dialog box 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 Test Credentials for [*device name*] dialog box, click **Close**.

Step 8 If the credentials test succeeded, 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, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

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, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

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 Group—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 9-35

- 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 Management 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, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

Step 2 In the device list, select the device whose management IP addresses you want to edit.

Step 3 From the Actions menu, choose **Edit Management IP Addresses**.

The Edit Management IP Address dialog box displays the following:

- Available IP Addresses—Lists all IP addresses not associated polling.
- IP Addresses for Management—Lists the IP addresses associated with the device, including the primary SNMP address and all backup IP addresses.

Step 4 Click any of the following:

- **Add**—Adds the IP Addresses from the Available IP Address box to the IP Addresses for Management 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 Management 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 Management box.
- **Raise**—Moves the selected IP address up one level in the IP Addresses for Management box. This option is disabled if there is only one IP address in the IP Addresses for Management box.
- **Lower**—Moves the selected IP address down one level in the IP Addresses for Management box. This option is disabled if there is only one IP address in the IP Addresses for Management box.

Note If only one IP address is available, the Raise and Lower buttons are not available.

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

Removing Device Interfaces From Polling

By default, all device interfaces are polled. At certain times you might want to remove one or more device interfaces from polling. For example in a network that aggregates very large numbers of low speed links pointing to the customer edge of the network, you might not want to retrieve data for every customer link, most of which are fixed bandwidths. In this case, you can use the Change Interface Polling action to remove the interfaces from polling.

Note If you remove interfaces from polling, reports requiring information from the removed interfaces, for example, QOS, MPLS, VPN, might show incomplete data points.

To remove a device interface from polling:

Step 1 Navigate to one of the following device views: Devices, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

Step 2 Select the device containing the interfaces you want to remove.

The device must have an Active status and not have alarms. If the device is not active or has alarms, the Change Interface Polling action is not available.

Step 3 From the Action menu, choose **Change Interface Polling**.

Step 4 In the Change Interface Polling dialog box, select the interfaces you want polled and click **Add** to move from the Available Interfaces to the Selected For Polling group.

Tip Press **Shift** to choose more than one interface.

Step 5 Click **Save**.

Only interfaces in the Selected For Polling group will be polled.

Relocating Devices to Units

To relocate a device to a different unit:

Step 1 Navigate to one of the following device views: Devices, Alarms by Device, Unreachable, NetFlow, Polling, Ping, Uptime, Data Collection, Software, Contact/Location, Prime. (For information on displaying these views, see Displaying Device Information at the Network Level, page 9-2.)

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**.

Annotating a Device

You can add annotative notes to devices to communicate details to network personnel that aren't included in the device information picked up by Prime Performance Manager.

To annotate a device in the network.

Step 1 Login to the Prime Performance Manager GUI.

Step 2 From the **Network** menu, choose **Devices.** The Device summary page displays.

Step 3 Highlight the device you want to annotate.

Step 4 From the **Actions** menu, click **Annotation**.

The Annotation screen displays and allows you to enter text for the selected device.

Step 5 Click **Save** to save the text.

Step 6 Click on the **Edit Note icon** to edit the existing text.

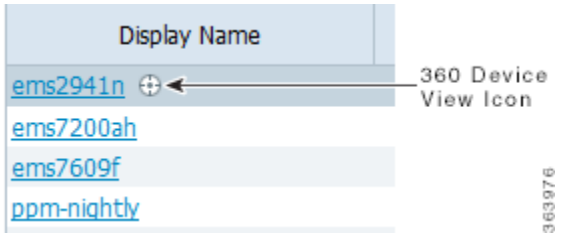
Step 7 Click on the **Cancel Editing Note icon** if you do not want to save the edited text.

Step 8 Click on the device link on which you have annotated the text. The selected device page displays the Annotate tab.

Displaying the 360 Device Details View

Every device, device element, or device technology hyperlink displayed in Prime Performance Manager includes an icon, shown in Figure 9-1, that, when clicked, displays a 360 detailed device view, shown in Figure 9-2. This window provides detailed information about the device, element, technology from various Prime Performance Manager GUI locations including devices, alarms, reports, and views.

Figure 9-1 360 Device View Icon



To display the 360 device details view:

Step 1 Navigate to a device hyperlink in one of the following windows:

- Network menu >
  - Devices > Devices tab
  - Alarms/Events > Alarms tab
- Performance menu >
  - Reports > Any report

– Views > Any view

– Dashboards > Any dashboard

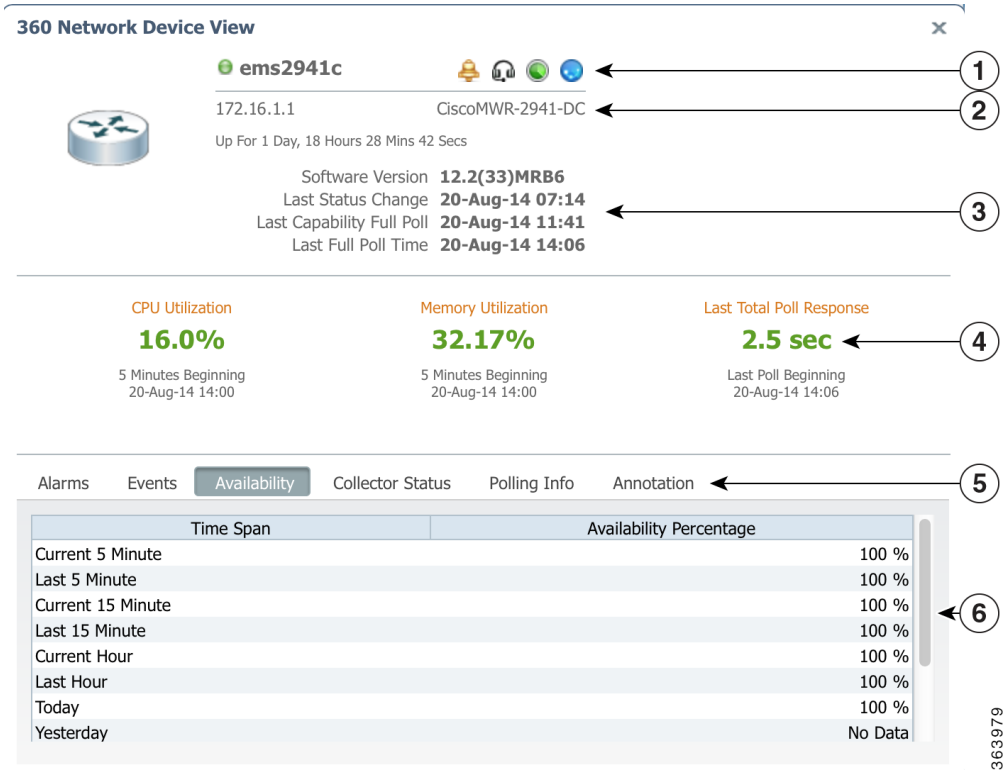
Step 2 Move your cursor over a device link and click the display icon to the right of the link.

The 360 Network Device Details window (Figure 9-2) appears. Information displayed in the window includes:

- Device name and IP address.
- Software and polling information
- CPU and memory utilization, and the last total poll response, CPU and memory utilization is the average for the specified time period, The timestamp is the beginning of the interval.
- Device alarms, events, availability, collector status, polling information, and annotation.
- Tools that display device alarms in the Alarms window, display the Cisco support website, and run ping and traceroute commands on the device.

Note The data and tabs displayed depend on the particular device and information that is available for it. Data Center devices and device elements, such as hypervisors, UCS server blades, VM, and other Data Center elements will display information specific to the Data Center element, and not necessarily information that appears for standard network devices.

Figure 9-2 360 Network Device Details



1	Alarms, support, ping, and traceroute tools.	**4**	CPU and memory utilization, last poll response.
2	Device name and IP address	**5**	Alarms, Events, Availability, Collector Status, Polling Information, and Annotation tabs.
3	Software, status, and polling information.	**6**	Device information display.

Note Not all information is displayed for Basic users.

Step 3 To close the window, click the **Close** icon at the top right. The window also closes automatically when you navigate to other windows.

Displaying Device Information at the Device Level

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, 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 Customizing the GUI and Information Display, page 3-8.

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 7-39.)

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 7-39.

- 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 dashboards, see Managing Dashboards, page 7-36.
- Details—Displays the detailed device information listed in Table 9-11.

Table 9-11 Device Details at the Device Level

Section	Field	Description
Toolbar	Actions menu	Allows you to modify devices by choosing a device in the table, then selecting an option. For a description of actions you can perform, see Managing Individual Devices, page 9-34.
	Ping	Pings the selected device.
	Traceroute	Runs a traceroute to the selected.
	Launch	Launches the device home page.
	Pause	Pauses the refreshing of data displayed in the GUI.
	Refresh Interval	Sets the time the GUI page will be refreshed. The range is 30 to 900 seconds. The default is 180 seconds.

Table 9-11 Device Details at the Device Level (continued)

Section	Field	Description
Naming Information	Display Name	The device display name.
	Custom Name	The custom device name, if one is defined. If not, this field displays Unknown.
	Sync Name	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.
	Report Policy	If the device has a report policy, the policy is displayed here. Clicking its link takes you to the policy on the Report Policy tab. Other entries you might see: • Default—The device is pulling the system default report policy. • This Device Only—A custom report policy was set for only that device by going into the Report Status tab and customizing it for the device. For information about report policies, see Creating Report Policies, page 7-33.
	Polling Group	The polling group to which the device is assigned. For information about polling groups, see Creating and Editing Device Polling Groups, page 9-35.

Table 9-11 Device Details at the Device Level (continued)

Section	Field	Description
Status Information	Sending Alarms	Indicates whether the device is sending alarms, Yes or No.
	Alarm Severity	Indicates the alarm severity of the object.
	Maintenance Mode	Indicates whether maintenance mode is enabled for the device. If maintenance mode is enabled, alarms and report polling are disabled. The Status Information area displays the dates the alarms are disabled, and the dates maintenance mode is enabled in red text.
	Device 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.
	Last Poll IP Address	The IP address that was last polled

Table 9-11 Device Details at the Device Level (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 Customizing the GUI and Information Display, page 3-8.
	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.
	Vendor	The device manufacturer or network technology.
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.
Unique Device Identifier (UDI)	Name	The device name.
	Description	The device description.
	Product ID	The device product ID number.
	Version ID	The device version number.
	Serial Number	The device serial number.

- Data Collection—Displays the device data collection information shown in Table 9-12.

Table 9-12 Device Data Collection at the Device Level

Section	Field	Description
Toolbar	Actions menu	Allows you to modify devices by choosing a device in the table, then selecting an option. For a description of actions you can perform, see Managing Individual Devices, page 9-34.
	Ping	Pings the selected device.
	Traceroute	Runs a traceroute to the selected.
	Launch	Launches the device home page.
	Pause	Pauses the refreshing of data displayed in the GUI.
	Refresh Interval	Sets the time the GUI page will be refreshed. The range is 30 to 900 seconds. The default is 180 seconds.
Polling Information	Status	Indicates the device status. See Table 9-2 on page 9-3 for a list of device statuses.
	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.
	Uptime	The device uptime, that is, the time since the last startup or reboot.
	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 Poll Response (secs)	The time, in seconds, taken by this device to respond to the last poll request.
	Avg Poll Response (secs)	The average time, in seconds, taken by this device to respond to poll requests.
	Polling Group	The polling group to which the device is assigned. For information about polling groups, see Creating and Editing Device Polling Groups, page 9-35.
	Report Policy	If the device has a report policy, the policy is displayed here. Clicking its link takes you to the policy on the Report Policy tab. Other entries you might see: • Default—The device is pulling the system default report policy. • This Device Only—A custom report policy was set for only that device by going into the Report Status tab and customizing it for the device. For information about report policies, see Creating Report Policies, page 7-33.

Table 9-12 Device Data Collection at the Device Level (continued)

Section	Field	Description
Collector Status	SNMP	Indicates whether data has been retrieved through SNMP. Will be Active unless data has never been retrieved using SNMP.
	SMI	Indicates whether Storage Management Institute statistics were collected.
	Hypervisor	Indicates whether a hypervisor is active. This will normally be active for VM devices.
	CLI	Indicates whether an XML poll was performed: • Active—A successful XML poll has occurred. • Not Active—An XML poll failed because of credentials.
	NetFlow	Indicates whether NetFlow data was collected. • Active—The device is configured to export NetFlow and the collector is receiving the flows regularly. • Not Active—The device is configured for NetFlow but it might not be receiving flows recently.
	JMX	Indicates whether Java Management Extensions data was collected.
	Data Collection Manager	Indicates whether Data Collection Manager bulk statistics were collected.
	Collectd Stats	Indicates whether collectd statistics were collected.
	StarOS Bulk Stats	Indicates whether StarOS bulk statistics were collected.
	RMS Log	Indicates whether the RAN Management System log is active.
	ICMP	Indicates whether Internet Control Message Protocol (ICMP) statistics were collected.
	Small Cell	Indicates whether small cell bulk statistics were collected.
	Generic CSV	Indicates whether generic CSV statistics were collected.
	GMOND	Indicates whether ganglia monitoring daemon (gmond) statistics were collected.
	Internal	Indicates whether internal statistics were collected.
	Optical Bulk Stats	Indicates whether optical bulk statistics were collected.
IP Addresses for Management	IP Address	IP address(es) associated with this device, including the primary address and all backup IP addresses.
	Last Full 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.
	Manageable	Indicates whether the IP address is used for polling, Yes or No.

- Events—Displays events that have occurred on the device. For a list of event parameters, see Table 10-1 on page 10-2.
- Alarms—Displays alarms that have been raised on the device. For a list of event parameters, see Table 10-1 on page 10-2.
- Thresholds—Displays thresholds that apply to the device. For information, see Displaying Thresholds by Device, page 11-13.
- Report Status—Displays the reports available for the device.
- Availability—Displays device availability information in table and bar chart format. Availability increments include current and last 15 minutes, hour, day, week and month.
- 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 7-17.
- Device Status—Displays information from the Details, Data Collection, Events, Alarms, and Availability tabs in a snapshot device status view.
- Probes—Displays any probes that are defined for the devices. Actions and fields include:
  - Add Probe—Adds a probe to the device. For information, see the Creating Probes, page 9-37.
  - Probe Name—The probe name.
  - Probe Type—The probe type: HTTP, TCP, NTP, DNS, or DHCP.
  - Enable/Disable—Enables or disables the probe.
  - Edit—Displays the Edit [probe type] Probe dialog box where you can edit the probe parameters. For information, see one of the following topics for the probe type:

    Creating a DHCP Probe, page 9-38

    Creating a DNS Probe, page 9-39

    Creating an HTTP Probe, page 9-40

    Creating a TCP Probe, page 9-42

    Creating an NTP Probe, page 9-43
- Annotation—Allows you to add annotation to the device. See Annotating a Device, page 9-23.

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.

Viewing Information in the Device Header

The following device-level tabs, Reports, Dashboards, Details, Data Collection, Events, Alarms, Thresholds, Report Status, Availability, Star Graphs, Device Status, Probes, and Annotation, display summary information about the device. Information includes:

- Device uptime—The Reports and Dashboard headers display time the device has been active since the last startup or reboot.

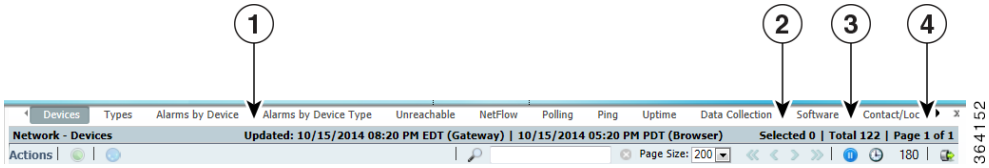
- Last update—The date and time of the last GUI update displayed. If the gateway and browser are in separate time zones, both times are displayed.
- Device IP or hostname—The device IP address or hostname is displayed in the center of the header. For the reports and dashboards, device components, for example, VMs, blades, are appended to the device IP address or host name with an asterisk, for example,

  ```
  192.11.11.11 * openstackvm.
  ```

- Query interval—The Dashboard header displays the report time period.
- Device and alarm statuses— Icons on the right of the header indicate the device status and highest alarm.
- Report policy—Displayed on the Report Status tab.
- Item count—Displayed on the Events and Alarms tabs.
- Page identifiers—Displayed on the Events, Alarms, Thresholds, and Probes tabs.

Figure 9-3 shows the device header at the network level. Because the browser is in a different time zone than the gateway, two updated dates and times are shown. Other header options include the number of devices selected, the total number of devices, and the page number.

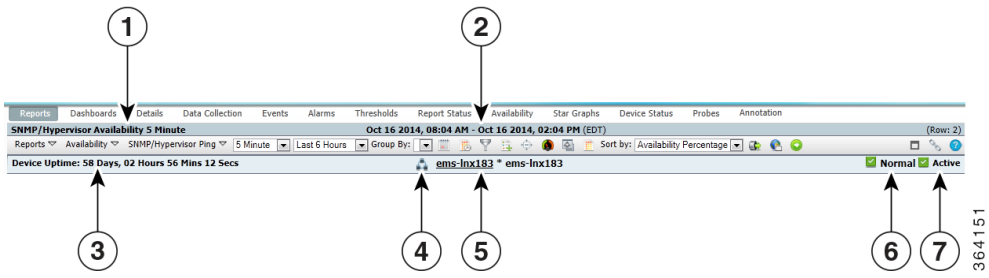
Figure 9-3 Device Header in Network View



1	Last screen update	**3**	Total items in Device window
2	Items selected	**4**	Page number

Figure 9-4 shows the device header at the device level for the Reports tab. The report header displays the report name and report period. The device header displays the device uptime, the device name and, because the report is for a device hypervisor, the hypervisor name. The device highest alarm and status icons are also shown.

Figure 9-4 Device Header in Device View



1	Report title	**5**	Device and hypervisor names
2	Report period	**6**	Highest alarm
3	Device uptime	**7**	Device status
4	Network view tool		

Managing Individual Devices

When you drill down to an individual device, you can perform the management actions that you are allowed to 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 7-39.)

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** or the **Data Collection** 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, Time Zone, and Location, page 9-16.
- Edit Device Credentials—Allows you to edit the device connection credentials. See Editing the Device Credentials, page 9-17.
- Edit Report Policy—Allows you to change the report policy assigned to the device or, alternatively, set the report to its default. See Editing the Report Policy Assigned to a Device, page 9-20.
- Edit Polling Policy—Displays the Report Policy dialog box where you can change the polling policy assigned to the device or return the report policy to its default settings. See Creating and Editing Device Polling Groups, page 9-35 and Editing the Polling Group Assigned to a Device, page 9-20.
- Edit Management IP Addresses—Allows you to edit a device Management IP addresses. See Editing the Device Management IP Addresses, page 9-21.
- Change Interface Polling—Allows you to remove device interfaces from polling, See Removing Device Interfaces From Polling, page 9-22.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 9-22.

- Disable/Enable Sending Alarms and TCA—Disables or enables sending alarms, including threshold crossing alerts, from the selected device. Disable Alarms displays a calendar dialog where you can set the duration the alarms and TCAs will be disabled. The menu item displayed depends on whether the alarms and TCAs are already disabled.
- Acknowledge Alarms—Acknowledges all open alarms on the device.
- Clear Alarms—Clears all open alarms on the device.
- Manage/Unmanage Device—Changes managed devices to unmanaged, and unmanaged devices to managed. The menu item displayed is based on the current device state.
- Enable/Disable Maintenance Mode—Enables or disables maintenance mode. If you place a device into maintenance mode, alarms and reports are disabled for the device. Enable Maintenance Mode displays a calendar dialog where you can set the maintenance mode duration. The menu item displayed depends on the maintenance mode status.
- Annotation—Allows you to add text descriptions and notes to the device. See Annotating a Device, page 9-23.
- 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 Devices With Prime Performance Manager"), 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 9-13. 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 9-13 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 Group Editor**.

Step 3 Scroll to the polling group you want to modify and edit the values in the following table cells:

- Time Out
- Retries

See Table 9-13 on page 9-35, 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.

Tip To see what devices belong to a polling group, under Device List column, click **Devices in Polling Group**. The devices in the group are displayed in the Device Browser. For information about the Device Browser attributes, see Table 9-2 on page 9-3. To return the Device Browser to the default list of network devices, navigate to a different window and refresh the browser page.

Creating a New Polling Group

Complete the following steps to create a new polling group:

Step 1 Login to the Prime Performance Manager GUI as the administrator user.

Step 2 From the Network menu, choose **Polling Group Editor**.

Step 3 On the Polling Group Editor toolbar, click the **Add Polling Group** tool.

Step 4 Complete the following:

- Polling Group—Enter the polling group name.
- Time Out
- Retries

See Table 9-13 on page 9-35, for polling group parameter descriptions and default values.

Step 5 Click **OK**.

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 Login to 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**.

Creating Probes

A probe is a program or other device inserted at a key network point to monitor and/or collect data about network activity. Probes:

- Show you which protocols are being used on your network, which hosts are sending and receiving data, where the traffic is coming from, and when this occurs.
- Provide an overview of the network throughput and the number of hosts, conversations, and protocols seen on the network.
- Provide an overview of the most active protocols, talkers, listeners, hosts, and conversations on your network.

Prime Performance Manager allows you to create the following probe types:

- Transmission Control Protocol (TCP)
- HyperText Transmission Protocol (HTTP)
- Network Timing Protocol (NTP)
- Dynamic Naming Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)

Probe creation procedures are provided in the following topics:

- Creating a DHCP Probe, page 9-38
- Creating a DNS Probe, page 9-39

- Creating an HTTP Probe, page 9-40
- Creating a TCP Probe, page 9-42
- Creating an NTP Probe, page 9-43

Creating a DHCP Probe

The DHCP probe helps to discover DHCP servers on the network. The probe broadcasts multiple DHCP request packets from a physical interface. Different request packet types are sent but a DHCP server may respond only to some requests depending on the server configuration.

After sending a request packet, DHCP probe listens for responses. Unknown server responses are captured in logs. As DHCP server broadcasts do not cross IP routers, it locates only servers that are attached to the same physical network as the specified interface.

Although DHCP probe supports monitoring only on a single physical interface, you can install a probe on each physical interface; each monitors a different physical network. When running multiple copies of DHCP probe, be sure to specify the appropriate file for each instance.

Note Before running DHCP probe on any network other than one for which you are responsible, contact that network's administrator to take permission for you to run this software on the specified network.

To create a DHCP probe:

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

Step 2 Display the Probe Editor using one of the following:

- From the Network menu, choose **Probe Editor**, or
- Navigate to the device where you want to add the probe and click the **Probes** tab.

The Network Probe Editor window appears.

Step 3 On the Probe Editor toolbar, click the **Create Probe** tool.

Step 4 In the Add Probe dialog box Probe Type field, choose:

- **DHCP Probe** for a DHCP probe with IPv4 addresses, or
- **DHCPv6 Probe** for a DHCP probe with IPv6 addresses.

Step 5 If templates exist and you want to apply one, choose the template from the **Apply Template** list. Otherwise, continue with Step 6.

Step 6 If you want to create a template based on entries, click **Create Template**. Otherwise, continue with Step 7.

Step 7 Enter the DHCP probe parameters.

- Device—The device associated with the probe that Prime Performance Manager polls for probe data. You can click the field to display a list of valid devices, or type the device name.
- Name—An arbitrary name assigned to the probe. The name should be unique within Prime Performance Manager when prepended with the device name, that is, Node=abc,Probe=xyz.
- Description—An optional description you can add to help identify the probe.
- Enabled—If checked (default), enables the probe.
- Interval (seconds)— The probe interval. Valid values are 1-300 seconds.

- Response Timeout—The amount of time to wait for a response from the probe before a timeout is issued. Valid values are 1-60 seconds.
- DHCP Server IP Address—(DHCP Probe only) Enter the DHCP server IP address associated with this probe.
- Port—Port on which the name server is listening. Port 67 is the default for DHCP probes and port 547 for DHCPv6 probes.

Step 8 Click **Save.**

The new DHCP probe is created and displayed in the Probe Editor.

Creating a DNS Probe

The DNS probe allows you to query DNS servers. A common check is whether your domain name (www.company.com) still points to your web server IP address. The DNS probe allows you to verify your web site domain names, mail server domain name mappings, DNS zone details, and other DNS information contained in text records. The DNS probe allows local servers to automatically fail or recover based on probe results. Probes are constantly sent to the DNS servers to determine their status. If a DNS server fails to respond to a certain number of probes, it is marked as failed. As soon as the DNS server starts to respond to DNS probes, it is returned to the in-service state. The configuration status helps you to find the load balance other ports on the same servers while you are probing DNS.

To create a DNS probe:

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

Step 2 Display the Probe Editor using one of the following:

- From the Network menu, choose **Probe Editor**, or
- Navigate to the device where you want to add the probe and click the **Probes** tab.

The Probe Editor window displays.

Step 3 On the Probe Editor toolbar, click the **Create Probe** tool.

Step 4 In the Add Probe dialog box Probe Type field, choose **DNS**.

Step 5 If templates exist and you want to apply one, choose the template from the **Apply Template** list. Otherwise, continue with Step 6.

Step 6 If you want to create a template based on entries, click **Create Template.** Otherwise, continue with Step 7.

Step 7 Enter the DNS probe parameters.

- Device—The device associated with the probe that Prime Performance Manager polls for probe data. If you chose the Probe Editor from the Network menu, you can click the field to display a list of valid devices, or type the device name. If you chose the Probe Editor from the device Probes tab, the device is automatically populated and cannot be changed.
- Name—An arbitrary name assigned to the probe. The name should be unique within Prime Performance Manager when prepended with the device name, that is, Node=abc,Probe=xyz.
- Description—An optional description you can add to help identify the probe.
- Enabled—If checked (default), enables the probe.
- Interval (seconds)— The probe interval. Valid values are 1-300 seconds.

- Response Timeout—The amount of time to wait for a response from the probe before a timeout is issued. Valid values are 1-60 seconds.
- DNS Server IP Address—Enter the DNS server IP address associated with this probe.
- Port—Port on which the name server is listening. This is normally port 53.
- Target Domain—Enter the target web domain address.
- Authoritative Name Server—If the server is a DNS authoritative name server, that is, it is responsible for their supported domains and can delegate authority over subdomains to other name servers, check this box,
- Expected IP Address Table—(optional) The IP addresses you expect to result from the DNS query. Type each entry on a new line.

Step 8 Click **Save.**

The new DNS probe is created in the Probe Editor.

Creating an HTTP Probe

An HTTP probe establishes a TCP connection and issues an HTTP request to the server for an expected string and status code. Prime Performance Manager compares the received response with the configured codes, looking for a configured string in the received HTTP page, or verifying the hash tag for the HTTP page. If any of these checks fail, the server is marked as failed. Probe credentials are the username and password used for authentication on the server.

You can use the HTTP probe to verify connectivity and monitor the real servers being load balanced. Probes determine the status of each real server in the server farm. For example, if you configure an expected string and status code and the Prime Performance Manager finds them both in the server response, the server is marked as passed. However, if the Prime Performance Manager does not receive either the server response string or the expected status code, it marks the server as failed

To create a HTTP probe:

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

Step 2 Display the Probe Editor using one of the following:

- From the Network menu, choose **Probe Editor**, or
- Navigate to the device where you want to add the probe and click the **Probes** tab.

The Probe Editor window displays.

Step 3 On the Probe Editor toolbar, click the **Create Probe** tool.

Step 4 In the Add Probe dialog box Probe Type field, choose **HTTP**.

Step 5 If templates exist and you want to apply one, choose the template from the **Apply Template** list. Otherwise, continue with Step 6.

Step 6 If you want to create a template based on entries, click **Create Template.** Otherwise, continue with Step 7.

Step 7 Enter the HTTP probe parameters:

- Device—The device associated with the probe that Prime Performance Manager polls for probe data. If you chose the Probe Editor from the Network menu, you can click the field to display a list of valid devices, or type the device name. If you chose the Probe Editor from the device Probes tab, the device is automatically populated and cannot be changed.
- Name—An arbitrary name assigned to the probe. The name should be unique within Prime Performance Manager when prepended with the device name, that is, Node=abc,Probe=xyz.
- Description—An optional description you can add to help identify the probe.
- Enabled—If checked (default), enables the probe.
- Interval (seconds)— The probe interval. Valid values are 1-300 seconds.
- Open Timeout—The timeout in seconds for opening a connection to the probe, that is, the time the probe waits to open and establish the connection with the server.
- Response Timeout—The amount of time to wait for a response from the probe before a timeout is issued. Valid values are 1-60 seconds.
- IP Address—Enter the HTTP server IP address associated with this probe.
- Port—The TCP port to probe. The range is 0 to 65536.
- Username—(optional) Enter the username associated with the HTTP probe. The maximum length is 64 byte with valid characters.
- Password—(optional) Enter the password for the HTTP probe. The maximum length is 64 byte with valid characters.
- HTTP Header Fields—Click **Add Row** to add an optional HTTP name and value.
  - Name—The HTTP header name. Any name can be assigned.
  - Value—The HTTP header value. You can enter any of the following.

    Accept

    Accept Charset

    Accept Encoding

    Accept Language

    Authorization

    Cache Control

    Connection

    Content MD5

    Expect

    From

    Host

    If Match

    Pragma

    Referer

    Transfer Encoding

    User Agent

    For information about HTTP headers, see the W3C RFC 2616 document: http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

- HTTP Request Methods—The HTTP request method. Valid values include:
  - DELETE
  - GET
  - HEAD
  - OPTIONS
  - POST
  - PUT
  - TRACE

Note If you type in the method, type in a method exactly as it appears in the drop-down list.

- HTTP Version—The HTTP version, either 1.1 or 1.0.

Note If you type in the version, type in a version exactly as it appears in the drop-down list.

- HTTP Status Code Ranges—(optional) Click **Add Row** to add expected HTTP status code ranges.
  - Begin—The bottom range of acceptable HTTP Status codes.
  - End— The top range of acceptable HTTP Status codes.
- HTTP Protocol—The HTTP protocol, either HTTP or HTTPS.

Note If you type in the protocol, you can enter HTTP, HTTPS, http, or https.

- Application—(optional) Enter the web application to test the given IP address.
- Regex—(optional) Enter the regular expression to inspect the returned data from the HTTP port. This field can be edited for valid regular expression syntax.

Step 8 Click **Save.**

The new HTTP probe is created in the Probe Editor.

Creating a TCP Probe

TCP probes record TCP connection responses to incoming packets. TCP probes connect to the specified device and port, and then execute a script that sends and receives data from the device.

To create a TCP probe:

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

Step 2 Display the Probe Editor using one of the following:

- From the Network menu, choose **Probe Editor**, or
- Navigate to the device where you want to add the probe and click the **Probes** tab.

The Probe Editor window displays.

Step 3 On the Probe Editor toolbar, click the **Create Probe** tool.

Step 4 In the Add Probe dialog box Probe Type field, choose **TCP**.

Step 5 If templates exist and you want to apply one, choose the template from the **Apply Template** list. Otherwise, continue with Step 6.

Step 6 If you want to create a template based on entries, click **Create Template**. Otherwise, continue with Step 7.

Step 7 Enter the TCP probe parameters.

- Device—The device associated with the probe that Prime Performance Manager polls for probe data. If you chose the Probe Editor from the Network menu, you can click the field to display a list of valid devices, or type the device name. If you chose the Probe Editor from the device Probes tab, the device is automatically populated and cannot be changed.
- Name—An arbitrary name assigned to the probe. The name should be unique within Prime Performance Manager when prepended with the device name, that is, Node=abc,Probe=xyz.
- Description—An optional description you can add to help identify the probe.
- Enabled—If checked (default), enables the probe.
- Interval (seconds)— The probe interval. Valid values are 1-300 seconds.
- Open Timeout—The timeout in seconds for opening a connection to the probe, that is, the time the probe waits to open and establish the connection with the server.
- Response Timeout—The amount of time to wait for a response from the probe before a timeout is issued. Valid values are 1-60 seconds.
- IP Address—Enter the TCP server IP address associated with this probe.
- Port—The TCP port to probe. The range is 0 to 65536.
- Over SSL/TLS—Check this box if the TCP connection employs the Secure Sockets Layer (SSL) or Secure Transport Layer cryptographic protocol.
- Send Data—(optional) Data to send on the TCP port. You can enter up to 255 alphanumeric characters.
- Regex—(optional) A regular expression used to inspect the returned TCP port data.

Step 8 Click **Save.**

The new TCP probe is created in the Probe Editor.

Creating an NTP Probe

NTP synchronizes computer clocks over a network with a dedicated time server. NTP is required between the source and the target device to provide accurate one-way delay (latency) measurements. Using Prime Performance Manager you can configure NTP probes on the source and target devices.

To create an NTP probe:

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

Step 2 Display the Probe Editor using one of the following:

- From the Network menu, choose **Probe Editor**, or

- Navigate to the device where you want to add the probe and click the **Probes** tab.

The Probe Editor window displays.

Step 3 On the Probe Editor toolbar, click the **Create Probe** tool.

Step 4 In the Add Probe dialog box Probe Type field, choose **NTP**.

Step 5 If templates exist and you want to apply one, choose the template from the **Apply Template** list. Otherwise, continue with Step 6.

Step 6 If you want to create a template based on entries, click **Create Template**. Otherwise, continue with Step 7.

Step 7 Enter the NTP probe parameters.

- Device—The device associated with the probe that Prime Performance Manager polls for probe data. If you chose the Probe Editor from the Network menu, you can click the field to display a list of valid devices, or type the device name. If you chose the Probe Editor from the device Probes tab, the device is automatically populated and cannot be changed.
- Name—An arbitrary name assigned to the probe. The name should be unique within Prime Performance Manager when prepended with the device name, that is, Node=abc,Probe=xyz.
- Description—An optional description you can add to help identify the probe.
- Enabled—If checked (default), enables the probe.
- Interval (seconds)— The probe interval. Valid values are 1-300 seconds.
- Response Timeout—The amount of time to wait for a response from the probe before a timeout is issued. Valid values are 1-60 seconds.
- NTP Server IP Address—The target IP Address for the probe. This can be one of the IP addresses associated with the device or it may be arbitrary IP address.
- Port—The NTP port to probe. The range is 0 to 65536.

Step 8 Click **Save.**

The new NTP probe is created in the Probe Editor.

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 Alarms and Events

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 one of the following:

- From the Network menu, choose **Alarms/Events > Alarms** to display all network alarms organized by occurrence date and time. The alarms are organized by the time they are last changed.
- From the Network menu, choose **Alarms/Events > Events** to display historical events organized by occurrence date and time. The events are organized by the time they occurred.
- 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 Customizing the GUI and Information Display, page 3-8.

- Display a device and choose **Alarms** to display alarms for that device.

Table 10-1 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 3-20.

Table 10-1 Alarms and Events

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.
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.
Condition	The alarm or event condition.
TCA Name[1]	For threshold crossing alerts (TCA), the TCA name. The name is assigned by the user who created the threshold.
TCA Metric	For TCAs, the TCA metric, for example, if the threshold is a percentage, the percent at which the threshold was crossed.
TCA Type	For TCAs, the TCA type.
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.

Table 10-1 Alarms and Events (continued)

Column	Description
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 Events 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.
Tenant	The tenant affected by, or connected to, the alarm.
Owner	The user assigned to the alarm, if user-access is enabled. To assign users to alarms, see Assigning Users to Alarms or Events, page 10-8.
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.
Clear By[1]	The user who cleared the event. If cleared automatically, the device name or IP address that cleared the alarm.
Clear Time	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 3-20.
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 Alarms tab (Network menu > Alarms/Events > Alarms) or the Network Events tab (Network menu > Alarms/Events > Events). Actions that you can perform are described in the following topics:

Responding to Alarms and Events

You can respond to alarms or events in the Alarms or Events window, for example, acknowledge, clear, or delete an alarm or an event. You can also add notes to alarms and change the alarm severity. You can also acknowledge and clear alarms from the device level.

Note If Prime Performance Manager is integrates with Prime Central, alarm responses and other actions are not available. All alarm responses must be performed in Prime Central.

To respond to alarms or events from the Alarms or Events window:

Step 1 From the Network menu, choose **Alarms/Events**, then click **Alarms** or **Events**.

Step 2 In the Alarms or Events tab, select the alarm or event, then choose any of the following responses on Alarms or Events toolbar:

- Ack (Acknowledge)—Acknowledges the alarm or event.
- Unack (Unacknowledge)—Unacknowledges the alarm or event.
- Clear—Clears the alarm or event.
- Annotate—Allows you to add notes to the alarm. (see Adding Notes to Alarms or Events, page 10-9)
- Assign—Assign this alarm to another user through e-mail. (Only visible when user access is enabled.)
- Delete—Deletes the alarm.
- Clear/Delete—Clears and deletes the alarm.
- Properties—Displays the alarm properties. See Displaying Alarm and Event Properties, page 10-7.
- Time Diff—Compares the time difference between two alarms. To compare alarms, click the first alarm, press **Ctrl** and choose the second, then click **Time Diff**.
- Events—Displays events associated with the alarm. See Displaying Alarm and Event Properties, page 10-7.
- Report—For alarms based on threshold crossing alerts (TCAs), displays the report containing the threshold on which the TCA was created.
- Change severity—Changes the alarm severity.

In addition, you can ping or start a trace route for any device with an alarm by selecting an alarm clicking the **Ping** or **Traceroute** tools on the alarm totals bar above the Network Alarms toolbar.

To acknowledge or clear alarms by device:

Step 1 From the Network menu, choose **Devices**, then click **Alarms by Device**.

Step 2 Select the device whose alarms you want to acknowledge or clear, then from the Actions menu choose:

- Acknowledge Alarm—Acknowledges the alarm or event for the selected device.
- Clear Alarms—Clears the alarm or event for the selected device.

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 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 **Alarms** or **Events**.

Step 2 In the Alarms or Events tab, click the **Modify 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
  - Warning
  - Critical
  - Minor
  - Major

- Other options, listed in Table 10-2, further define the alarms and events you want filtered.

Table 10-2 Alarm and Event Filter Dialog Box Other Pane

Field	Description
Acknowledged	Indicates whether only acknowledged alarms/events appear in the Alarms or Events window. This check box is checked by default.
Unacknowledged	Indicates whether only unacknowledged alarms/events appear in the Alarms or Events window. This check box is checked by default.
Time Before	(Checkbox and date entrance fields) Indicates whether only alarms/events that Prime Performance Manager logs before a specified date and time, appear in the Alarms or Events window. This check box is unchecked by default. This field is dimmed unless the **Time Before** checkbox is checked
Time After	(Checkbox and date entrance fields) Indicates whether only alarms/events that Prime Performance Manager logs after a specified date and time, appear in the Alarms or Events window. This check box is unchecked by default.This field is dimmed unless the **Time After** checkbox is checked.
Name or Message Matches	Indicates whether only alarms/events that contain the specified message text appear in the Alarms or Events 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 Alarms or Events 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 Alarms or Events 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 10-2 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 Alarms or Events 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 Alarms or Events 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 Alarms or Events 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.
Owner	Filters alarms or events by the alarm or event owner. After you check this option, choose a user from the list of Prime Performance Manager users that appear in the drop-down list. See Assigning Users to Alarms or Events, page 10-8 for more information.
Device Type	Filters alarms or events by device type. Check **Device Type**, then choose a network device or tenant 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 Alarms or Events windows. While you can choose to display the properties not displayed by default in the Alarms and Events 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 Alarms window, check the alarm whose properties you want to view or,
- Click **Events** and check the event whose properties you want to view.

Step 3 From the Alarms or Events window toolbar, click **Properties**.

The Prime Performance Manager Alarm and Event Properties window Properties tab displays the all properties listed in Table 10-1.

Related Topics

- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Alarm Events, page 10-10
- Displaying Daily Alarm and Event Archives, page 10-10

Assigning Users to Alarms or Events

Prime Performance Manager allows administrators to assign users to alarms and events when:

- Prime Performance Manager is not integrated with Prime Central. For information, see Integrating Prime Performance Manager with Prime Central, page 4-2.
- User access is enabled. For information, see Setting Up User Access and Security, page 6-1.
- The user you want to access is added to Prime Performance Manager. For information, see Adding New Users, page 6-15.

To assign a user to an alarm:

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 In Alarms window, click the alarm that you want to assign.

Step 3 From the Alarms window toolbar, click **Assign**.

Step 4 In the Alarm Owner dialog box, choose the user you want to assign from the Owner list.

Step 5 Click **Send Email** if you want to send the user you assign an e-mail about the alarm or event assignment. (This option is only available if an email address was added to the user profile. For information, see Adding New Users, page 6-15.

Step 6 Click **OK**.

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 Alarms window, click the alarm to which you want to add a note or,
- Click **Events** and click the event to which you want to add a note.

Step 3 From the Alarms or Events window toolbar, click **Annotate**.

The Details for Selected Alarm or Details for Selected Event 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 Type the note text, then click **Save Note** on the Notes toolbar.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Displaying Alarm or Event Details, page 10-9
- Displaying Alarm Events, page 10-10
- Displaying Daily Alarm and Event Archives, page 10-10

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 Alarms window, check the alarm whose details you want to view or,
- Click **Events** and check the event whose details you want to view.

Step 3 From the Alarms or Events window toolbar, click **Properties**, then click the **Details** tab.

Additional alarm or event details, if present, will be displayed.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm Events, page 10-10
- Displaying Daily Alarm and Event Archives, page 10-10

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 Alarms window, check the alarm whose events you want to view.

Step 3 From the Alarms window toolbar, click **Events**.

The alarm events are displayed.

Step 4 From the Events for Alarm tab you can perform any event function described in Table 10-1 on page 10-2.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Daily Alarm and Event Archives, page 10-10

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 Alarms window, click the **Daily Archives** tab.

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 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Alarm Events, page 10-10

Displaying Device Details for an Alarm

Step 1 From the Network menu, choose **Alarms/Events**.

Step 2 Click the Alarms tab and select the alarm whose details you want to view.

Step 3 From the 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
- Device Performance
- Descriptive Information
- Uptime Information
- Device Performance
- Unique Device Identifier

For information about the properties displayed, see Table 9-11 on page 9-26.

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, Time Zone, and Location, page 9-16.

- Edit Report Policy—Allows you to change the report policy assigned to the device. See Editing the Report Policy Assigned to a Device, page 9-20
- Edit Polling Group—Allows you to change the polling group assigned to the device. See Creating and Editing Device Polling Groups, page 9-35 and Editing the Polling Group Assigned to a Device, page 9-20.
- Edit Management IP Addresses—Allows you to edit a device management IP addresses. See Editing the Device Management IP Addresses, page 9-21.
- Change Interface Polling—Allows you to change interface polling. For information, seeRemoving Device Interfaces From Polling, page 9-22.
- Relocate Device—Allows you to relocate a device from one unit to another. See Relocating Devices to Units, page 9-22.
- Disable Alarms and TCAs—Disables sending alarms and TCAs from the selected device for the time period entered the date and time range dialog that is displayed.
- 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 connectivity.
- Trace—Invokes traceroute to map the network route to the device.

Note You can also ping or invoke a traceroute for a device from the Network Alarms window.

- Pause—Pauses the device polling.
- Refresh Interval—Changes the device refresh interval.

Related Topics

- Displaying Alarm and Event Properties, page 10-7
- Adding Notes to Alarms or Events, page 10-9
- Displaying Alarm or Event Details, page 10-9
- Displaying Daily Alarm and Event Archives, page 10-10

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 9-3 on page 9-6.

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 Type**. For a description of alarms by device parameters,

see Table 9-3 on page 9-6.

Monitoring System Health

Prime Performance Manager predefined alarms help you monitor your system health. Alarms reflecting your system health are listed in Table 10-3.

Note System health is affected by many network factors. Use the predefined alarms as a starting point.

Table 10-3 System Health Alarms

Alarm	Severity
DiskUtilization	• Critical—Exceeds minimum disk space requirement. • Warning—Approaching minimum disk space requirement.
ServerStateChanged	• Major—The gateway or unit changed state.
BulkStatsInfo	• Informational—Bulk statistics file processing information messages include: – DeviceNotDiscovered – NoHeader – NoFooter – MissingFilenameParams
BulkStatsError	Bulk statistics file processing error conditions: • Major - MultiDeviceFailure—Multiple devices failed to receive bulk statistics files. • Major - NoFiles—A single device is not seeing any bulk statistics files. • Minor - MinorSkip—A single device did not receive one bulk statistics file. • Minor - MajorSkip—A single device did not receive multiple bulk statistics files
ServerConnectionStatus	• Critical—A gateway or unit lost connection to each other unexpectedly. • Warning—A gateway or unit lost connection to each other through an operator shutdown.
ServerClockStatus	• Major—The unit server clock is out of sync with the gateway.
InventorySyncStatus	• Major—Inventory sync with Prime Network, Prime Central, or Prime Network Services Controller failed.
AlarmSyncStatus	• Major—Alarm sync with an upstream OSS failed.
UnitFailOver	• Major—Unit failed over to redundant unit unexpectedly. • Minor—Unit failed over to redundant unit via operator command.

Table 10-3 System Health Alarms (continued)

Alarm	Severity
GatewayFailOver	• Major—The gateway failed over to the secondary gateway unexpectedly or dual primary gateways are detected. • Informational—The gateway failed over to secondary gateway through operator command.
CSVFileError	• Major—An error occurred writing an exported CSV file.
DBProcessorError	• Major—An error occurred writing data to the database.
SchedulerQueueSize	• Major—The scheduler queue size is over threshold, indicating a possible performance problem.
PollerTaskOutOfMemeory	• Major—A congested scheduler queue indicates too many tasks are scheduled and waiting to be run on the queue. A performance issue could be preventing the system from running all the scheduled tasks.
SyncMsgOutOfMemory	• Major—Out of memory while trying to sync messages between gateway and unit.

You can also create TCAs on underlying server or OS metrics. Common ones include:

- CPU Utilization
- Memory Utilization
- Disk Utilization
- Swap Utilization

For information about setting thresholds, see Creating and Managing Thresholds, page 11-1.

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

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 OSS 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 supported for upstream OSS hosts.

- Trap Type—Enter the SNMP trap type:
  - CISCO-PRIME—The Cisco Prime trap type. See CISCO-PRIME Notification Attributes, page 10-21
  - CISCO-SYSLOG—The Cisco Syslog trap type.
  - CISCO-EPM-2—The Cisco EPM 2 trap type. See CISCO-EPM-2 Trap Notification Attributes, page 10-24

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 10-15.

- 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 10-15.

- 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 10-16.

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, Normal.
- Device Types—Include all the device types that have been added to Prime Performance Manager.
- Tenants—If tenants are created, they appear under Tenants and can be selected.
- Groups—If report groups are created, they appear under Groups and can be selected. For information, see Creating a Report Group, page 7-54. (If no groups are available, this item is not displayed.)
- Report Policies—If report policies are created, they appear under Report Policies and can be selected. For information, see Assigning Devices to Report Policies, page 7-34. (If no report policies are available, this item is not displayed.)
- 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 Send 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 **System Settings**.

Step 3 If a mail server is not entered in the SMTP Mail Server field, enter your mail server IP address or hostname now. The mail server must be configured before you can send alarms and event e-mails.

Step 4 From the Administration menu, choose **Alarms/Events Editor**.

Step 5 On the Alarms/Events Editor toolbar, click **Add Email Address**.

Step 6 In the From Email Address box, enter the email address that you want displayed to recipients. That is, while the email is generated by the gateway, the From Email Address is the one recipients will see and, should they respond to the email, the address to which responses are sent.

Step 7 In the Email To Addresses box, enter the address(es) to which you want the alarm email sent. To add multiple addresses, separate the addresses with semicolons and no spaces.

Step 8 Click **OK**. The address(es) are added to the first row of the Email Addresses group at the bottom

Step 9 To configure the alarms and events you want sent to the addresses, in the address row click the **Set Filter** tool.

Step 10 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, 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.
- Tenants—If tenants are created, they appear under Tenants and can be selected.
- Groups—If report groups are created, they appear under Groups and can be selected. For information, see Creating a Report Group, page 7-54. (If no groups are available, this item is not displayed.)

Step 11 Click **OK**.

Step 12 On the Alarms/Events Editor toolbar, click **Save Configuration**.

Step 13 You can perform the following actions at any future point:

- Repeat Steps 5 through 12 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-83).
- Enable trap forwarding using the ppm traprelay command (see ppm traprelay, page B-109).

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 Event Engine Parameters, edit the following:

- 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 Alarms—Indicate whether 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 10-15 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.

Step 4 When finished, on the Alarms/Events Editor toolbar, click **Save Configuration**.

Creating an Advanced Message Queuing Protocol Connection

Advanced Message Queuing Protocol (AMQP) is added to Prime Performance Manager alarms and events.

To add an AMQP connection:

Step 1 From the Administration menu, choose **Alarms/Events Editor**.

Step 2 On the Administration Alarms/Events Editor toolbar, click **Add AMQP Connection**.

Step 3 Enter the AMQP server and queue details:

- Description
- Host
- Port
- Virtual Host
- Exchange
- Exchange Type
- Queue
- Routing Key
- Username
- Password
- Message Type

For information about AMQP parameters, see the AMQP user documentation, which can be found at: http://www.amqp.org.

Step 4 Click **OK**.

A row representing the AMQP connection is added to the AMQP Connections table of the Alarms/Events Configuration window. Use the table to see the status of the connection, either Active or Down. You can edit the connection details, or delete the connection at any time.

If the AMQP connection message type is Alarm, a row representing the AMQP connection is also added to the Upstream OSS Hosts table of the Alarms/Events Configuration window. Use this table to filter and resend alarms.

Prime Performance Manager SNMP Traps

The following sections describe the OSS host traps used by Prime Performance Manager.

- CISCO-PRIME Notification Attributes, page 10-21
- CISCO-EPM-2 Trap Notification Attributes, page 10-24

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 10-4 describes the CISCO-PRIME notification attributes.

Table 10-4 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	1.3.6.1.4.1.9.9.311.1.1.2.1.6	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.

Table 10-4 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
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.
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 • 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.

Table 10-4 CISCO-PRIME Notification Attributes (continued)

Attribute Name	OID	Value
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. Contains additional key/value pairs described in cenEventIDList.
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. **Note** The custom event message text is found in this varbind.
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.

The following shows the CISCO-PRIME trap when tenants are defined. The tenant information is provided in the cenUserMessage1 varbind. The tenant information is also visible as part of the device FQDN in the cenAlarmManagedObjectClass and cenAlarmDescription varbinds. This tenant information is only present when the tenant feature is enabled and the TCA is defined for the tenant.

```
[ Tue Sep 02 14:39:42 EDT 2014]  TrapPDU [version = 2C community = public enterpriseOid =
.1.3.6.1.4.1.9.9.311.0.2 enterpriseName = ciscoEpmNotificationRev1 agentIpAddr =
10.81.82.99 genericId = 6 specificId = 2 sysUpTime = 4 days 23:22:42
```

```
OID: cenAlarmVersion              VALUE: 3
OID: cenAlarmTimestamp            VALUE: 0:0:0
OID: cenAlarmUpdatedTimestamp     VALUE: 0:0:0
OID: cenAlarmInstanceId           VALUE: 94760001
OID: cenAlarmStatus               VALUE: 0
OID: cenAlarmStatusDefinition     VALUE: ThresholdCrossing
OID: cenAlarmType                 VALUE: 1
OID: cenAlarmCategory             VALUE: 2
OID: cenAlarmCategoryDefinition   VALUE: 2,TCA
OID: cenAlarmServerAddressType    VALUE: 1
OID: cenAlarmServerAddress        VALUE: 10.81.82.99
OID: cenAlarmManagedObjectClass   VALUE:
Tenant=153ffb475fa0405bb94fc52696aa32c9,Node=172.18.116.190,UUID=9ef4f7a3-965d-4b0d-99c2-8
75e00ad02ca,name=instance-00000037
OID: cenAlarmManagedObjectAddressType VALUE: 1
OID: cenAlarmManagedObjectAddress VALUE: 172.18.116.190
OID: cenAlarmDescription          VALUE: Threshold : 'CPU_UTIL_1' -
'Tenant=153ffb475fa0405bb94fc52696aa32c9,Node=172.18.116.190,UUID=9ef4f7a3-965d-4b0d-99c2-
875e00ad02ca,name=instance-00000037' crossed threshold for 'Nova VM CPU Utilization 5
Minute/CPU Utilization' - value '7' threshold '2'. Severity: Critical
OID: cenAlarmSeverity             VALUE: 6
OID: cenAlarmSeverityDefinition   VALUE: 6,Critical
OID: cenAlarmTriageValue          VALUE: 0
OID: cenEventIdList               VALUE:
AlarmType=Communications;ProbableCause=ThresholdCrossed;NodeCreateTime=2014-08-28,15:51:56
.891,-0400;NodeChangeTime=2014-08-28,15:51:56.891,-0400;NodeClearTime=;NodeAckTime=;VNENam
e=;
OID: cenUserMessage1              VALUE:
Owner=;TCAName=CPU_UTIL_1;Tenant=153ffb475fa0405bb94fc52696aa32c9;
OID: cenUserMessage2              VALUE: PPM
OID: cenUserMessage3              VALUE: Threshold : 'CPU_UTIL_1' -
'Tenant=153ffb475fa0405bb94fc52696aa32c9,Node=172.18.116.190,UUID=9ef4f7a3-965d-4b0d-99c2-
875e00ad02ca,name=instance-00000037' crossed threshold for 'Nova VM CPU Utilization 5
Minute/CPU Utilization' - value '7' threshold '2'. Severity: Critical
OID: cenAlarmMode                 VALUE: 2
OID: cenPartitionNumber           VALUE: 0
OID: cenPartitionName             VALUE:
OID: cenCustomerIdentification    VALUE:
OID: cenCustomerRevision          VALUE: 2014-08-28,15:51:56.891,-0400
OID: cenAlertID                   VALUE: 2014-08-28,15:51:56.891,-0400
```

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 10-5 describes the CISCO-EPM-2 notification attributes.

Table 10-5 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	1.3.6.1.4.1.9.9.311.1.1.2.1.6	Unique event ID.
cenAlarmStatus	1.3.6.1.4.1.9.9.311.1.1.2.1.6	The alarm status: 0,New 1,Update 2,Delete
cenAlarmStatusDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.7	The alarm status definition: 0,New 1,Update 2,Delete
cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	AlarmNature (Undefined(0), ADAC(1), ADMC(2))
cenAlarmCategory	1.3.6.1.4.1.9.9.311.1.1.2.1.9	Integer corresponding to user-defined event category.
cenAlarmCategoryDefinition	1.3.6.1.4.1.9.9.311.1.1.2.1.10	String representation of 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.

Table 10-5 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
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.
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=2010-06-17,23:31:41.617,-2202 NodeClearTime=2010-06-17,23:31:41.616,-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.

Table 10-5 CISCO-EPM-2 Notification Attributes (continued)

Attribute Name	OID	Value
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)
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"

Creating and Managing Thresholds

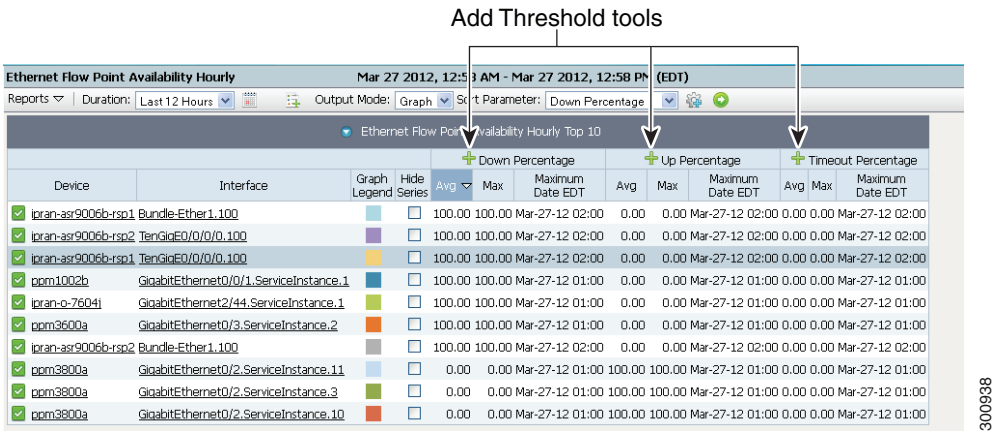
You can create thresholds for any key performance indicators (KPIs) displayed in Prime Performance Manager reports, views, or dashboards. Thresholds help you monitor network performance by sending notifications when a KPI exceeds or falls below a desired tolerance or performance target. In addition, you can have Prime Performance Manager define a baseline performance range for a KPI and notify you when performance changes significantly from the baseline range. Creating baselines alerts you to network problems before they cross the prescribed thresholds.

Prime Performance Manager gives you considerable flexibility in defining threshold ranges and the threshold crossing alerts that are issued when threshold ranges are exceeded. The following topics provide information about configuring thresholds in Prime Performance Manager:

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 11-1 shows an example.

Figure 11-1 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.

In addition, you can create and apply report policies that modify report intervals when thresholds are crossed. For example, if a CPU nears 100% utilization, you can create and apply a report policy that reduces the polling frequency until it returns to normal. Conversely, you can create and apply report policies that increase polling frequencies when KPIs pass critical thresholds. For information about creating report policies, see Creating Report Policies, page 7-33.

Note By default, only numeric KPIs are enabled for thresholds. However, Prime Performance Manager does provide the capability to create thresholds for string KPIs. For information, see Entering Thresholds for String KPIs, page 11-8.

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 the 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, test thresholds on a small group of devices before you roll them out to the full network.
- 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, view, or dashboard data that cannot have thresholds created, such as name and description.
- The TCA is generated if the beginning of the data period falls within the active TCA range. For example, if data crosses a threshold between 1:15-1:30 and the TCA active period is defined as 1:00-5:00, the TCA is generated. If the TCA active period is 12:00-1:00, the TCA is not generated.

To create a Prime Performance Manager threshold:

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

Step 2 Display the report, view, or dashboard containing the KPI for which you want to create a threshold.

Step 3 Click the Add Threshold tool (green + icon) in the KPI column header.

Step 4 In the Add Threshold window, enter the threshold parameters. Threshold parameters are grouped into Threshold Configuration and Threshold Values tabs described in the following sections:

- Threshold Configuration, page 11-3
- Threshold Values, page 11-6

Threshold Configuration

- Name—Enter a unique name for the threshold. The name cannot be the same as any existing threshold name. The field accepts any alphanumeric text. Spaces are not permitted.
- Enabled—The threshold is enabled by default. If you want to create the threshold but do not want it enabled, uncheck this box. You can enable the threshold later on the Threshold Editor window. For example, you might want to create all thresholds first, review them in the Thresholds Editor window, then enable them at one time. For information, see **Managing Thresholds, page 11-12.**
- Report Data Interval—Choose the time interval when you want Prime Performance Manager to check the data point value identified by the threshold. Threshold intervals include:
  - 1 Minute
  - 5 Minute
  - 15 Minute (default)
  - Hourly
  - Daily
  - Weekly
  - Monthly

Note Verify that the report has these intervals enabled. Prime Performance Manager enables the 15-minute, hourly, daily, weekly, and monthly intervals by default. To run a threshold every 5 minutes, you must enable 5-minute report interval. For information, see Chapter 7, "Managing Reports, Dashboards, and Views."

If you implemented multi-tenancy in Prime Performance Manager, complete the following tenancy fields. If not, continue with the Description field.

- Tenancy—Indicates the tenants that should be included in the threshold:
  - ALL—(default) Choose this option if you do not want to assign tenants to the threshold.
  - ALL_TENANTS—Includes all tenants in the threshold.

  - SELECTED—Allows you to choose the tenants added to the threshold
- Selected Tenants—If you chose SELECTED in the Tenancy field, displays the tenants that added.

  To add tenants, click **Change** then chose the tenants you want in the Select Tenants dialog box using the **Add**, **Add All**, **Remove**, **Remove All** buttons.
- Description—As needed, add any notes to describe the threshold. The field accepts any alphanumeric text.
- Alarm Type—Indicates the alarm type you want raised. Select the Alarm type with these options: Communications, Processing Error, Environmental, QoS, or Equipment
- Probable Cause—Threshold Crossed is the default probably cause. If you want to assign a different one, choose it from the displayed list.
- Alarm Nature—Choose the method for clearing the alarm, either 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, existing abate values are cleared.
- Continuous Alarm—If enabled, alarms are sent every polling cycle until the threshold falls below the abate value. If not enabled, the alarm is only sent once.
- Run Script—If you want to execute a script 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 it. If you enter an OSS host automation script, you can specify whether the threshold script has priority. See Editing Upstream OSS Hosts, page 10-15 and Tuning Event and Alarm Parameters, page 10-18 for more information. In addition, you can use the ppm extrarunpathcommand to define the script directory in the PATH variable. For information, see ppm extrarunpath, page B-39.

  You can also pass variables to scripts as $params, for example:

  - $abateValue—The threshold abate value.
  - $AckBy—The user who acknowledged the alarm.
  - $Action—The action performed on the alarm or event, for example: NEW("New", "0, New")/ UPDATE("Update", "1, Update")/ DELETE("Delete", "2, Delete").
  - $AlarmNature—The alarm nature, ADAC or ADMC.
  - $AlarmType—The alarm or event type.
  - $AlarmID—The alarm ID (alarm ID is the event ID).
  - $Category—The alarm or event category.
  - $ClearBy—The user who cleared the alarm or event.
  - $currentValue—The current threshold value.
  - $DeviceType—The device type
  - $Element—The unique network element to which the alarm or event pertains.
  - $ID—A unique ID assigned to all alarm or event objects.
  - $Name—The alarm or event name.
  - $onsetValue—The threshold onset value.

  - $OriginalSeverity—The original alarm or event severity.
  - $Owner—The alarm or event owner.
  - $ProbableCause—The alarm or event probable cause.
  - $relation—The TCA value
  - $Severity—The alarm or event severity.
  - $Tenant—The tenant name.
  - $TenantDisplayName—The tenant display name.
  - $TcaName—The TCA name.
  - $TcaMetric—The TCA metric.
  - $thresDetail—Threshold details.
  - $TimePeriod—The alarm or event time period.

  In addition, context-dependent variables are available that allow you to add any non-key column from any KPI in the form ${kpi<index>.<column header name>}. For simple thresholds these are all kpi0. More complicated thresholds could have any number of KPIs.

- Email From Address—If you want to send an email when the threshold is crossed, enter from email address here.

  Note If a global email from address is configured, that address automatically populates the Email From Address field. You can remove or edit the global address, however. The global email from address is configured in Administration > System Settings > System Configuration.

- Email To Addresses—If you want emails sent when the threshold is crossed, enter the recipient address(es). Separate multiple addresses with semicolons and no spaces.
- Email Subject—Allows you to customize the email subject to make the email more readable and helpful. You can use any parameter in the email subject that can be sent to scripts (see Run Script above), except AlarmID. AlarmID is not supported in messages.
- Message Text—Allows you to customize the message displayed when the TCA occurs. For example,

  TCA: $Severity: $TcaName: $TcaMetric: $relation

  Displays a message like the following when the alarm is raised:

  TCA: Critical: CPU_AverageUtilization_duplicate: CPU 5 Min Utilization 5 Minute/Average Utilization: value '23' threshold '20'

  Click **Insert Variable** to insert variables in the message text. These are the same variables that can be sent to scripts except AlarmID (see Run Script above).

- Occurrence—In the Occurrence area, 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

The Threshold Values tab is where you provision the threshold parameters for minor, major, and critical alarms. Warning and informational thresholds are not enabled by default. To enable them, choose **Administration > System Settings**. In System Configuration Settings, enable **TCA Warning Severity** and/or **TCA Informational Severity**.

- Onset Occurrences—The number of onset threshold crossings that must occur before the alarm is raised.

  The alarm is triggered when the incoming data exceeds the configured Onset value repeatedly.

  For example, if the onset value is 90 and if the onset occurrence is 3, then the following alarm conditions might occur:

  – Critical Alarm is triggered when the incoming data is 90, 95, 92.

  – Critical alarm is trigged at 90 when the incoming data is 90,85,92, 95, and 90.

  – Critical alarm is not trigged when the incoming data is 90, 85, 92, and 95.

- Abate Occurrences—The number of abate occurrences that must occur before the alarm is cleared.
- Report Policy Override—If you created a report policy for the specific alarm threshold, select the report policy here. Only user-created report policies are displayed. You can apply report policies to take effect when thresholds are crossed. For example, if a resource crosses a maximum usage value, you might decrease the report interval to reduce usage on the resource. Conversely, you might increase report intervals for other types of TCAs to get more timely data.

  If you create report policies for each threshold level, the minor report policy is applied when the threshold crosses the minor level, the major report policy is applied when the threshold cross the major threshold, and the critical report policy is applied when it crosses the critical threshold level. If a threshold level does not have an associated report policy, the default report policy is applied.

Note If you define a report policy for one severity level, you must define a report policy for all severity levels.

Individual TCA definitions and their associated report policy overrides are based on the KPI interval. If you apply a report policy to the threshold that excludes the TCA interval, the threshold will never clear. For example, suppose you create a default interface usage report policy that includes the 5-minute, 15-minute, hourly, and daily intervals. You then create a custom interface usage report policy X that includes the 15-minute, hourly, and daily report intervals, but not the 5-minute interval. Suppose you create an interface usage TCA for the 5-minute interval and assign report policy X to the Critical level report policy Override. When this threshold is exceeded, report policy X is applied but the TCA will never clear because the underlying KPI is not generated by the report policy (X).

The intent is to reduce the polling load on the device. This can be accomplished by reducing the number of reports polled at each interval or eliminating reports for a particular interval. If you add an override report policy, be sure not to remove the report or interval on which the TCA is based.

Note Report Policy Override does not apply to devices that have collectd provisioned because Prime Performance Manager polls the device on a prescribed minimum interval that supersedes report policy intervals.

KPI Values

- KPI—Select the KPI from the drop down list. Normally only one KPI is shown. Multiple KPIs are shown when you create compound thresholds. For more information, see Creating Compound Thresholds, page 11-8.
- Baseline—If you want the threshold to be based on a calculated value based on a collection of KPI values over a period of time and not an individual KPI value, check this box. To create a baseline threshold, you must specify the baseline method, window size, and onset and abate factors. For more information, see Creating Baseline Thresholds, page 11-10.
- Baseline Method—If you enabled baseline thresholds, choose the baseline method:
  - Average—The average of KPI values collected within the specified threshold window.
  - Exponential Average—Applies a calculation to the KPI values gathered in the specified window that places greater weight on recent values over older ones.
- Window Size (in intervals)—The number of intervals to include in the baseline. Intervals are defined by the Report Data Intervals field.
- Name—A read-only field displaying the name generated automatically from the report, view, or dashboard attribute name.
- Report—A read-only field displaying the report name.
- Type—Choose the KPI type, either rising or falling. 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.
- Scope—Set the threshold scope. 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".

- 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 higher than the onset value. For a falling KPI type, the abate value must be higher than the onset.

  Note A small number of KPIs allow you to define thresholds using strings. For details, see Entering Thresholds for String KPIs, page 11-8.

  If you do not define threshold values for all alarm levels, Prime Performance Manager skips them and goes to the next defined threshold level. For example, if you only define critical alarms, the threshold will go to normal after the critical alarm reaches the abate level.

Note If you selected Baseline, Onset and Abate change to Onset Factor and Abate Factor to indicate the number you enter is a factor multiplied by the baseline calculation to determine whether an alarm should be raised or cleared. For more information, see Creating Baseline Thresholds, page 11-10.

Step 5 Click **OK**.

The TCA is added to the gateway. To edit or perform other threshold actions, see Managing Thresholds, page 11-12. To create compound or baseline thresholds, see:

- Creating Compound Thresholds, page 11-8
- Creating Baseline Thresholds, page 11-10

Entering Thresholds for String KPIs

By default only numeric KPIs are enabled for thresholds. However, a small number of string KPIs are enabled so that you can enter thresholds for them, for example, operationalState Up, Degraded, or Down. If you choose an enabled string KPI, boxes appear below the Onset and Abate fields allowing you to define the point when TCAs are raised. To define thresholds for string KPIs:

- You can use any of the following operators: Equals, Does Not Equal, Contains, Does Not Contain, Begins With, Ends With.
- Test values can contain any printable characters except quotes.
- All matches are case-sensitive.
- For multiple test values:
  - If the operator is positive (Equals, Contains, Begins With, Ends With), the condition is true when the value matches any test value.
  - If the operator is negative (Does Not Equal, Does Not Contain), the condition is true when the value does not match any test value.
- You generally should not specify abates for string thresholds. If no abate is specified, the abate condition is true as soon as the onset condition is false.
- String thresholds always test severities from Critical to Normal (which always matches), and take the first value that matches.

Note You can enable additional string KPIs by setting thresholdable=true in the report XML. For information, see the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*.)

Creating Compound Thresholds

You can create thresholds for multiple KPIs and have alarms generated when the specified conditions exist for one or all of the KPIs. For example, you can define thresholds for CPU routing processors and specify the alarm to be raised when one or more processors exceed or fall below a specified value.

Compound thresholds can only be created for a single device object residing within the same device. For example, if you create a threshold for a CPU utilization KPI, you must do it for a single CPU. If you base it on multiple CPUs, the last CPU value polled will be the one used for the TCA calculation.

Compound threshold requirements are enforced by the Prime Performance Manager GUI. You can create compound thresholds based on objects across multiple devices by creating XML files and using Prime Performance Manager macros. For information, see the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*.

To create a compound threshold:

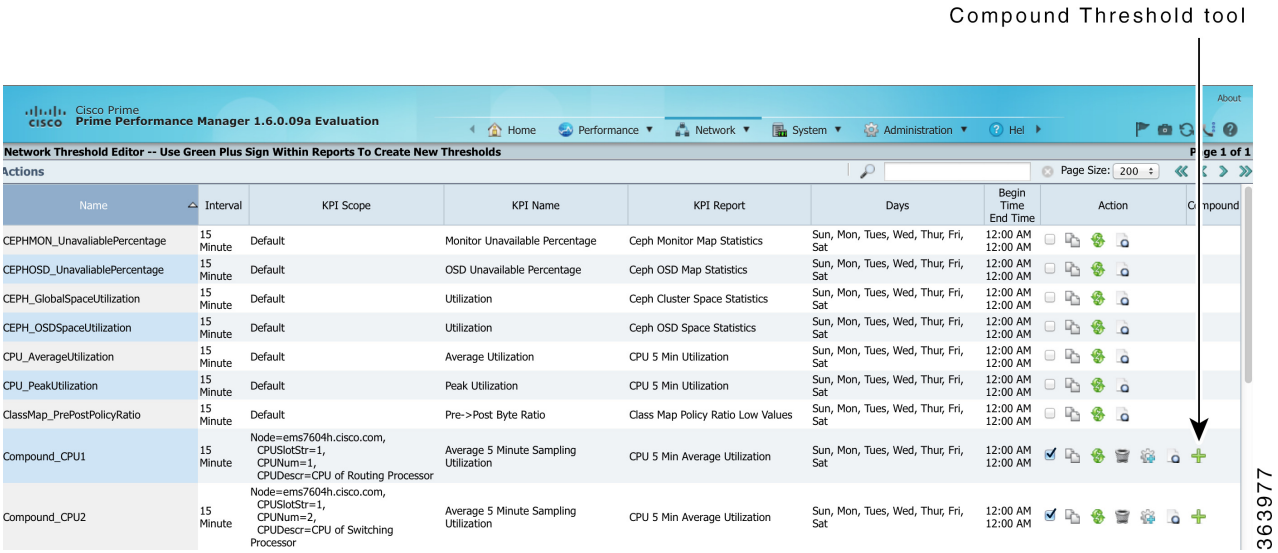
Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 If the thresholds that you want to compound are not created, create them using the "Creating Thresholds" procedure on page 11-1.

Step 3 From the Network menu, choose **Threshold Editor**.

Thresholds that can be joined into a compound threshold display the Compound Threshold tool under the Action column, as shown in Figure 11-2. Thresholds that do not display the tool cannot be compounded either because they were created for objects that don't reside within the same device or if on the same device, a single device object.

Figure 11-2 Compound Threshold Tool



Step 4 Select one of the thresholds you want to compound and click the **Compound Threshold** tool. The threshold you choose to start the compound will have the following impact on the compound threshold:

- The threshold days will be used for the compound threshold.
- For AND compound operations, the alarm level of the starting threshold will be displayed for the compound one.

The Create Compound Threshold dialog box displays a list of thresholds that you can compound with the selected threshold.

Step 5 Choose a threshold and click **OK**.

The Add Compound Threshold window appears. It is identical to the Create Threshold window with the following exceptions:

- The Compound Operation field is added so you can choose the compound type.
- The Select KPI field allows you to switch between or among the compounded KPIs. As you switch KPIs, the KPI values are displayed.

For information about other Add Compound Threshold fields, see the following topics:

- Threshold Configuration, page 11-3
- Threshold Values, page 11-6

Step 6 If desired, modify the compounded threshold name in the Name field. By default, the compounded threshold name is the name of the KPI from which you started the compound with "-compounded" appended to it.

Step 7 In the Compound Operation field, choose the compound operation:

- AND—An alarm is not displayed until conditions in all compounded thresholds meet their respective onset requirement.
- OR—An alarm is raised when any compounded KPI meets its onset requirement.

Step 8 Click **OK**.

The Threshold Editor displays the new compounded threshold. The values of all compounded thresholds are displayed. In addition, the Compound Threshold too is available under the Action column to add more thresholds to the compounded one, should you so choose.

Creating Baseline Thresholds

While you can create thresholds for individual KPI values, you can also create thresholds that create alerts when deviations to average values occur. For example, device object utilization might run 30% most of the time. You might want to know whenever a spike to that average occurs, in which case, you would create a baseline threshold. In a baseline threshold, a calculation is made on a specified number of KPI values over a specified time period. The value is multiplied by a specified factor to determine whether an alarm should be raised.

To create a baseline threshold complete the "Creating Thresholds" procedure on page 11-1 and complete the following baseline threshold fields:

- Baseline—Must be checked.
- Baseline method—Sets the method used to calculate the baseline value. Prime Performance Manager supports the average and exponential average methods, described in the following topics:
  - Average Baseline Method Overview, page 11-11
  - Exponential Baseline Method Overview, page 11-12
- Window size—The time period used to calculate the baseline. Window size is expressed as a number of report data intervals, which are specified in the Create Threshold window Report Data Interval field. For example, if you set the report data interval to 15 minutes and enter a window size of 4, the baseline window is one hour.

Note Prime Performance Manager begins calculating baselines with the first received KPI value and proceeds forward until all intervals specified in the window size are collected. If you set a large window size, you do not need to wait until all window values are accumulated before a baseline calculation is performed.

- Onset Factor and Abate Factor—The number that is multiplied by the calculated KPI values from the baseline method and window size to determine whether or an alarm should be raised or cleared. For example, if you want an alarm raised when the KPI rises 10% above the average, you would enter 1.1 as the onset factor. Similarly, if you want an alarm raised if the KPI falls 10% below the average, you would enter .9 as the onset factor.

Average Baseline Method Overview

For average baseline calculations, Prime Performance Manager averages the data points specified by the window size. For example, if the window size is four and the report data interval is 15 minutes, Prime Performance Manager collects the KPI values for the last four 15-minute periods and divides the total by four. This value is multiplied by the onset and abate factors to determine whether an alarm should be generated or cleared.

The following examples show the average baseline calculation method in actual practice. The examples are based on the following window size and onset and abate factors:

- Window Size = 10
- Onset Factor = 1.05
- Abate Factor = 1.01

Example 1

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 200, 200, 200
- Calculated average = 200
- Calculated onset = 210
- Calculated abate = 202

Example 2

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 200, 200, 205
- Calculated average = 200.50
- Calculated onset = 210.525
- Calculated abate = 202.505

Example 3

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 200, 205, 205
- Calculated average = 201
- Calculated onset = 211.05
- Calculated abate = 203.01

Example 4

In this example, the last baseline value, 220, is higher than the calculated onset, 213.05, so an alarm is raised. The next baseline value is 205, which is lower than the calculated abate value, so the alarm is cleared.

- Baseline values: 200, 200, 200, 200, 200, 200, 200, 205, 205, 220 (alarm raised)
- Calculated average = 203
- Calculated onset = 213.05

- Calculated abate = 205.03
- Baseline values: 200, 200, 200, 200, 200, 200, 200, 205, 205, 205 (alarm cleared)

Averaging is based on the last set of collected data values based on the window size and report interval, and therefore can change over time.

Exponential Baseline Method Overview

The exponential moving average (EMA) of KPI values collected in the selected threshold window. An EMA is a moving average for time-series data which places greater weight on more recent data. Using the exponential average baseline method provides a smoother running-average curve. It also requires less computing memory because fewer window size values must be stored. For large window sizes or scenarios where memory is restricted, exponential average might be a better choice over the average baseline calculation method.

Managing Thresholds

Prime Performance Manager thresholds can be viewed, edited, disabled, enabled, and deleted from the Thresholds Editor, shown in Figure 11-2. The editor displays thresholds added from the Prime Performance Manager reports GUI (see Creating Thresholds, page 11-1), 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 11-12

Enabling and Disabling Thresholds, page 11-14

Deleting Thresholds, page 11-16

Editing Thresholds from the Alarms Window, page 11-13

Displaying Threshold Events, page 11-16

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 threshold parameters described in the following topics:

- Threshold Configuration, page 11-3

Note You cannot edit the threshold name.

- Threshold Values, page 11-6

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, choose a Threshold Crossing alarm.

Step 4 From the Active Alarms window toolbar, click **Help for Event**.

Step 5 The View Thresholds dialog box or the Edit Threshold dialog box (administrator users) displays the following threshold parameters described in the following topics:

- Threshold Configuration, page 11-3

Note You cannot edit the threshold name.

- Threshold Values, page 11-6

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

Step 7 To view a report for the threshold crossing, in the Alarms window toolbar, click **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**.

Displaying Thresholds by Device

You can display thresholds that apply only to a specific device, either thresholds for physical device elements, such as CPU, ports, and interfaces, or thresholds applied to networking technologies provisioned on the device.

To display thresholds by device:

Step 1 Log into the Prime Performance Manager GUI.

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

Step 3 In the Network Devices window, click the device link for the device whose thresholds you want to view.

Step 4 In the individual device window, click the **Thresholds** tab.

Thresholds that apply to the device, including the polling or device group to which the device belongs, with the report enabled are displayed.

For information about the displayed threshold parameters, or to edit the threshold, see Creating Thresholds, page 11-1.

Actions you can perform from the device thresholds window are described in the following topics:

- Duplicating Thresholds, page 11-14
- Enabling and Disabling Thresholds, page 11-14
- Rearming Thresholds, page 11-15

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 Network 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 threshold parameters described in the following topics:

- Threshold Configuration, page 11-3
- Threshold Values, page 11-6

Step 5 Click **OK**.

Enabling and Disabling Thresholds

To enable or disable one or more thresholds:

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

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

Step 3 Choose the threshold(s) that you want to enable or disable. (To choose multiple thresholds, press the **Shift** key to select contiguous thresholds, or **Ctrl** to choose noncontiguous thresholds.

Step 4 From the Actions menu, choose **Enable Selected Thresholds** or **Disable Selected Thresholds**.

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 11-13.

Filtering Thresholds

To filter the displayed thresholds:

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

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

Step 3 In the Search field, enter the text that you want to use to filter the thresholds. For example, to filter the thresholds by response time, enter Responsetime.

Step 4 Press **Enter**.

Prime Performance Manager filters the thresholds by the text you entered.

Step 5 To display all thresholds, delete the text from the Search field and press **Enter**.

Rearming Thresholds

Rearming thresholds means you have reset the threshold so it can be raised again. In a normal threshold sequence, the TCA alarm is raised when a value crosses the onset value. The threshold is not reset until the parameter value crosses the abate value entered for the threshold at the next polling cycle.

For example, suppose you have a critical threshold defined with onset value of 95 and abate of 80. You have three devices: DevA, DevB, and DevC.

- Poll 1: DevA=98, DevB=97, DevC=98

  Three alarms will appear on the Alarms page, one for each device. You select and clear the alarms for DevB and DevC. You now have one alarm for DevA.

  Note Clearing an alarm rearms the TCA only for DevA and DevB. Rearming the threshold on the Threshold Editor clears all alarms and rearms the threshold for all devices.

- Poll 2: DevA=75, DevB=87, DevC=98

  You now have one alarm. The alarm for DevA is cleared now because the value is below the abate setting. DevB is not above onset. DevC has an alarm because the value is above onset.

- Poll 3: DevA=96, DevB=89, DevC=98

  You have two alarms. DevA is above onset value and DevC is still above abate. You go to Threshold Editor and click Rearm Threshold. Both of the above alarms are cleared. No alarms for this threshold appear on the alarms page.

- Poll 4: DevA=96, DevB=88, DevC=98

  Two alarms will be displayed again.

To rearm a threshold:

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

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

Step 3 In the Network Threshold Editor window, find the threshold you want to rearm then under the Action column (located on the far right of the threshold parameters), choose **Rearm Threshold**.

The threshold is reset and any existing threshold alarms are cleared.

Deleting Thresholds

You cannot delete thresholds provided the Prime Performance Manager installation, but you can delete user-created thresholds.

To delete one or more thresholds:

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

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

Step 3 Choose the threshold(s) that you want to delete. (To choose multiple thresholds, press the **Shift** key to select contiguous thresholds, or **Ctrl** to choose noncontiguous thresholds.)

Step 4 From the Actions menu, choose **Delete Selected Thresholds**.

Step 5 On the confirmation, click **OK**.

Prime Performance Manager will remove the threshold from the table.

Displaying 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.
```

Displaying Recent TCAs

You can view current TCAs in the TCA View. As TCAs occur, TCA View automatically displays the following subviews:

- TCA View—Displays one graph for each threshold with active TCAs. Each graph displays the top ten series for the TCA metric.
- Threshold View—Displays one graph for each defined threshold severity with active TCAs: Critical, Major, Minor. Each graph displays the severity top 10 series.
- Severity View—Displays one graph for each severity. Each graph displays the threshold top 10 series. No data is displayed if the severity level has no TCAs.

As you use TCA View, keep the following in mind:

- Each TCA graph displays the full TCA time range beginning with the first TCA (or the earliest time for which Prime Performance Manager has data) minus one 5-minute interval.
- TCA View is dynamic. Any TCA graph changes that you make are removed when you reload the page.
- TCA View is updated once every five minutes. If a TCA occurs right after an update, it could take up to five minutes to appear in TCA View.

Note For more information about Prime Performance Manager views, see Creating and Managing Custom Report Views, page 7-39.

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:

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

Prime Performance Manager System menu allows you to display Prime Performance Manager statuses, properties, settings, logs, and messages. Table 12-1 provides an overview to the logs, messages, and information displayed from the System menu.

Table 12-1 System Menu Logs and Messages

Menu > Path	Source	For information, see:
System > Status > • Connected Clients • System Status • Geo HA Gateway Status • System Versions • System Check • Install Locations • IP Access List • System Backup Statistics	Displays the output of these commands: • ppm who • ppm status • ppm primeha [status] • ppm version • ppm checksystem • ppm rootvars • ppm ipaccess • ppm systembackup	Displaying Connected Clients and System Status, page 12-2.
System > Logs > • Install Log • Patch Log • Console Log • System Check 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 • ppmPatchLog.txt • sgmConsoleLog.txt • sgmCheckSystemLog.txt • ppmBackupLog.txt • sgmCommandLog.txt • eventAutomationLog.txt • sgmSecurityLog.txt • Tomcat/logs • sgmConsoleLog-archives	Displaying System Logs, page 12-4.
System > Messages	Displays tabular information on system messages, including errors, information, trace, debug, dump, SNMP, and archived messages.	Displaying System Messages, page 12-12.
Administration > System Settings • System Configuration Settings • System Polling Settings • System Backup Settings	Displays the contents of these system property files: • Multiple files • Server.properties • ppmBackupLog.txt	Displaying System Settings, page 12-8.

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:

Step 1 From the System menu, choose **Status**.

Step 2 Choose any of the following tabs:

- **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.

- **Geo HA Gateway Status**—For Prime Performance Manager gateways configured in geographical high availability, displays the HA status: active, standby, or not configured. For more information about Prime Performance Manager HA, see Managing Timing Among Gateways, Units, and Clients, page 13-14.
- **System Versions**—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.
- You can also use the ppm version command to display the Prime Performance Manager software versions.
- **System Check**—Checks the gateway or unit server 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.
- **System Backup Statistics**—Displays statistics on recent Prime Performance Manager backups.

Note You can also use the ppm backupstats command to display backup statistics. For information about backing up Prime Performance Manager data, see Chapter 18, "Backing Up and Restoring Prime Performance Manager."

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

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 menu > Logs > Install Log**, 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 menu > Logs > Patch Log**, 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 **System menu > Logs > Console Log**, 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 **System menu > Logs > System Check Log**, 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 **System menu > Logs > Backup Log**, 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 **System menu > Logs >** CLI **Command Log**, 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 **System menu > Logs > Event Automation Log**, or
- Run the **ppm eventautolog** command.

Related Topics

Displaying the Security Audit Log, page 12-6

Displaying the Application Audit Logs, page 12-7

Displaying the Security Audit Log

The security audit 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. The system security log lists:

- All security events that have occurred for the Prime Performance Manager server. These include adding and removing users, and many other security events.
- 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 **System menu > Logs > Security Audit Log**, 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 **System menu > Logs > Application Audit Logs**, or
- Run the **ppm who** command.

Displaying the Console Log Archives

The system console archives displays all archived system console messages. To display the console log through the Prime Performance Manager GUI:

- **System menu > Logs > 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-62.

- **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-53.
- **ppm logtimemode**—Sets the log file time mode for dates. For more information, see ppm logtimemode, page B-54.
- **ppm 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-62.

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 12-8
- Displaying Poller Settings, page 12-9
- Displaying Web Settings, page 12-9
- Displaying Reports Settings, page 12-11

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:

- **Administration menu > System Settings**

System settings are displayed on the following tabs:

- System Settings—Displays the configured system settings.
- System Configuration—Displays configurable system settings. For information about changing system settings in the GUI, see Changing System Configuration Settings, page 3-17. You can also change system settings using the CLI. Table 12-2 shows commands that you can use to change system properties.

Table 12-2 Commands to Change System Properties

System Property	Command
BACKUP_RMIPORT	ppm backup, page B-13
BACKUP_SERVER	
BACKUP_WEBPORT	
BADLOGIN_TRIES_ALARM	ppm badloginalarm, page B-18
BADLOGIN_TRIES_DISABLE	ppm badlogindisable, page B-19
CHART_MAX_WINDOW	
CONSOLE_ARCHIVE_DIR_MAX_SIZE	ppm msglogage, page B-62
CONSOLE_LOG_MAX_SIZE	ppm consolelogsize, page B-24

Table 12-2 Commands to Change System Properties (continued)

System Property	Command
CSV_STRING_DELIMITER	
CW2K_SERVER	ppm datadir, page B-26
CW2K_WEB_PORT	
CW2K_SECURE_WEB_PORT	
FAST_INTERVAL	ppm fastinterval, page B-39
JSP_PORT	ppm javaver, page B-49
LOGAGE	ppm msglogage, page B-62
LOGDIR	ppm msglogdir, page B-62
LOGSIZE	ppm logsize, page B-53
LOGTIMEMODE	ppm logtimemode, page B-54
LOG_TROUBLESHOOTING	ppm maxrepqueries, page B-56
PERSISTENCEDIR	ppm datadir, page B-26
PROMPT_CREDS	ppm setpctrapdestination, page B-88
RP_NUM_FAST_POOL_THREADS	ppm numfastthreads, page B-65
RP_NUM_SLOW_POOL_THREADS	ppm numslowthreads, page B-66
SBACKUPDIR	ppm backupdir, page B-16
SERVER_NAME	ppm servername, page B-87
SNMPCONFFILE	ppm snmpconf, page B-91
SSL_ENABLE	ppm ssl, page B-99
TRAP_LIST_ENABLE	ppm uninstall, page B-117

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, choose:

- **Administration menu > System Settings > Poller Settings**

You can change the SNMP_MAX_ROWS property using the ppm snmpmaxrows command. (See ppm snmpmaxrows, page B-94.) To change other poller settings in the Server.properties file.

Displaying Web Settings

The web settings file contains properties that control the configuration of Prime Performance Manager web interface. For example:

```
# Copyright (c) 2005, 2012-2014 by Cisco Systems, Inc.
#
```

```
# Controls maximum number of rows to display when displaying raw log text
# Controlled by the maxasciirows CLI
MAX_ASCII_ROWS = 6000

# This is the default page size that is selected
# if a cookie has not been set or the maxPageSize parameter
# is not found in the request parameters.
# Controlled by the ppm maxhtmlrows CLI
# No longer used by anything but cgi-bin message log (CSCue09344)
MAX_HTML_ROWS = 200

# Max value in the list of available page sizes
# Trumps all page size system/user prefs (CSCue09344)
# Controlled by the ppm maxpagesize CLI
MAX_SELECTABLE_PAGE_SIZE = 800

# Controls how often the page autoupdates in SystemAdmin log file viewing
# There is no CLI to control this option
LOG_UPDATE_INTERVAL = 300
# Controls the total maximum number of event rows return to event archive
# web client
# There is no CLI to control this option
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, choose:

- **Administration menu > System Settings > Web Settings**

Table 12-3 describes the web settings.

Table 12-3 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 maxhtmlrows, page B-55.**
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 200 rows. To modify this setting, see **ppm maxhtmlrows, page B-55.**
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.

Table 12-3 Web Settings (continued)

Web Setting	Description
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-56.**
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:

```
# Copyright (c) 2011-2014 by Cisco Systems, Inc.
#
STATS_REPORTS = enable

# Partial days are supported for 3 sec, 5 sec, 15 sec only

RPT_3SEC_AGE = .125
RPT_5SEC_AGE = .25
RPT_15SEC_AGE = .5
RPT_1MIN_AGE = 2
RPT_DAILY_AGE = 94
RPT_WEEKLY_AGE = 730
RPT_MONTHLY_AGE = 1825

RPT_1MIN_CSV_AGE = 2
RPT_5MIN_CSV_AGE = 3
RPT_HOURLY_CSV_AGE = 14
RPT_DAILY_CSV_AGE = 94
RPT_WEEKLY_CSV_AGE = 730
RPT_MONTHLY_CSV_AGE = 1825

RPT_BULKSTATS_AGE = 14
RPT_BULKSTATS_EXP_AGE = 14

RPT_TIMEMODE = 24
NODE_NAME_TYPE = dnsname

RPT_1MIN_ENABLED = false
RPT_15MIN_ENABLED = true
RPT_HOURLY_ENABLED = true
RPT_DAILY_ENABLED = true
RPT_WEEKLY_ENABLED = true
```

```
RPT_MONTHLY_ENABLED = true

TEST_MODE = disabled

IFNAME_FORMAT = both

RPT_CSVNAMES = ppm
RPT_CSVTYPE = allnodes
RPT_CSV_NAME_FORMAT = yyyy-MM-dd-HH-mm
RPT_CSV_CONTENT_FORMAT = MM-dd-yyyy HH:mm
RPT_NAME_COL_TITLE = Node
RPT_DELIM = ,

EXP_REPORTS = export
RPT_5MIN_ENABLED = true
RPT_5MIN_AGE = 4
RPT_15MIN_AGE = 7
RPT_HOURLY_AGE = 7
RPT_15MIN_CSV_AGE = 2
```

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

- **Administration menu > System Settings > Report Settings**

Displaying Gateway Backup Times

You can display Prime Performance Manager gateway and collocated unit (if installed) backup information by choosing:

- **Administration menu > System Settings > Backup Times**.

Alternatively, you can display the backup information using the ppm getbackuptimes commend. (See ppm getbackuptimes, page B-41.) Displayed backup information includes:

- Last Backup Start—The date and time the gateway backup was started.
- Last Backup Stop—The date and time the gateway backup was completed.
- Next Backup Start—The date and time the next gateway backup will begin.

For information about the Prime Performance Manager backup and restore process, see Chapter 18, "Backing Up and Restoring Prime Performance Manager."

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 Archived Messages, page 12-15

Displaying System Information Messages

System information 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 system information messages through the Prime Performance Manager GUI, choose:

- **System menu > Messages**

Table 12-4 describes the System Info Messages table columns.

Table 12-4 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.
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.

Configuring Message Logs

By default, Prime Performance Manager collects action, error, and information messages. To monitor different message types:

Step 1 From the Administration menu, choose **System Settings**.

Step 2 On the Administration Configuration Settings window, click **Logging Configuration**.

Step 3 In the Message Level field, choose one of the following message types:

- **Normal**—Logs all action, error, and information messages.
- **All**—Logs all messages regardless of message type.
- **None**—Turns off message logging.
- **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 information messages.
- **SNMP**—Logs all SNMP messages.
- **Trace**—Logs all trace messages.
- **Traps In**—Logs all incoming trap messages.
- **Traps Out**—Logs all outgoing trap messages.
- **NBAPI-SOAP**—Logs all northbound SOAP messages.

Step 4 In the Maximum Number of Log Files, set the maximum number of log files you want to keep. The default is 35.

Note Increasing the number of log files can affect Prime Performance Manager performance.

Note Modifying the message log settings should be perform **only** under guidance from the Cisco Technical Assistance Center (TAC).

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:

- **System > User Actions**

Table 12-5 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 12-5 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.
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, choose:

- System menu. choose **Messages**, then click **Archives**. (The Archive link is located in the top right above the Message column.)

Table 12-6 describes the archive message information.

Table 12-6 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.

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

Prime Performance Manager allows you to view information about provisioned gateways and units including details about 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 To display gateway and unit statistics, you must add the gateway and unit 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 13-1.

Table 13-1 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. **Note** To change a gateway or unit IP address or host name, use the ppm servername command. For information, see ppm servername, page B-87.
Management IP Address	The IP address used to manage the gateway or unit.
Redundancy Group[1]	If the unit belongs to a redundancy group, the redundancy group name. See Managing Unit Redundancy Groups, page 13-8.
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.
Annotation	Any annotation added to describe the gateway or unit.
Connection Time	Connection time with the server to a unit or gateway.
Severity	Specifies the severity status of the unit or gateway. Possible values are: • Critical • Major • Minor • Normal
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

Table 13-1 Gateway and Unit Properties (continued)

Column	Description
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[1]	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 3-20.

To display detailed gateway or unit information, select the gateway or unit in the navigation area. Table 13-2 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 13-2 Detailed Gateway and Unit Properties

Tab	Description
Server Reports	Displays the unit or gateway CPU utilization.
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 13-4
Events	Displays the gateway or unit events. For a description of the event properties, see Displaying Alarms and Events, page 10-1.
Alarms	Displays the gateway or unit alarms. For a description of the alarm properties, see Displaying Alarms and Events, page 10-1.
Thresholds	Displays the gateway or unit device thresholds.
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.
Annotation	Displays any annotation that has been added to describe the gateway or unit. For more information, see Annotating a Device, page 9-23
Devices for Unit (Units only)	Displays the devices assigned to the selected unit. For a description of device properties, see Displaying Device Properties at the Network Level, page 9-3.
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 at the Network Level, page 9-6.
Device Poll Response (Units only)	Displays the poll responses for devices assigned to the selected unit. For a description of poll response properties, see Displaying Device Polling Responses at the Network Level, page 9-8.

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 reason for 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 Customizing the GUI and Information Display, page 3-8.

- 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 Customizing the GUI and Information Display, page 3-8.

– 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 7-10.

– 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 not 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, for example:

  ```
  /opt/CSCOppm-unit/bin/ppm servername = 111.222.333.444
  ```

- On the gateway add an entry to the /etc/hosts file for the unit.
- Add a DNS entry for the unit.

Note If you change the gateway server clock, restart Prime Performance Manager, or you might lose connectivity between the gateway and units.

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 13-6
- Creating Device-to-Unit Maps, page 13-6
- Editing Device-to-Unit Maps, page 13-7
- Deleting Device-to-Unit Maps, page 13-7
- Changing a Device-to-Unit Assignment, page 13-8

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 Device Information at the Network Level, page 9-2
- Creating and Editing Device Polling Groups, page 9-35

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** (the plus icon).

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 Devices With Prime Performance Manager.”

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 that you want to delete then under Action, click **Delete**.

Step 4 When 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 13-7.) 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 grayed 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.

Managing Unit Redundancy 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:

- 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.
- RMS upload servers are not moved to redundant units when a primary unit fails. To repartition the processing for an RMS upload server, use the ppm manageulsredundancy partitioner repartition command. For information, see ppm manageulsredundancy, page B-55.

Note Unit redundancy is not recommended for small cell implementations.

The following topics tell you how to create, edit, failover, failback or delete, unit redundancy groups:

- Creating New Unit Redundancy Groups, page 13-9
- Editing Redundancy Groups, page 13-10
- Performing Manual Redundant Unit Failovers, page 13-11
- Switching Redundant Units Back to Standby, page 13-11
- Unit Redundancy Group Failover Scenarios, page 13-12
- Replacing a Failed Unit, page 13-13

Creating New Unit Redundancy Groups

Creating new redundancy groups assigns a Prime Performance Manager redundancy unit to serve as the backup unit for one or multiple units.

To create a new unit redundancy group:

Step 1 From the System menu, choose **Gateways/Units**.

Step 2 In the left navigation pane, click **Redundancy Editor**.

The Redundancy Editor displays information about current redundancy groups.

Step 3 From the Actions menu, choose **New Group**.

Step 4 In the Redundancy Group Editor, complete the following:

- Name—Enter the name of the new group.
- Switchover Delay—Enter the switchover delay. This is the amount of time Prime Performance Manager waits before switching to a redundant unit after a primary unit problem occurs, The default is 300 seconds.
- Enabled—The redundancy group is enabled by default. If you do not want it enabled, uncheck this box.
- Redundant Unit—Under Available Units, choose the unit that you want to be the redundant unit, then click the arrow to move it into the Redundant Unit box.

Note Do not select the unit with the lowest internal ID because Prime Performance Manager uses it as the default unit. To display the internal ID in the System Gateway/Units window, right-click the table header and select **Internal ID**. (Internal ID is not displayed by default.)

- Units In Group—Under Available Units, choose the unit(s) that you want included in the redundant unit group, that is, the units that will be backed up by the redundant unit.

Step 5 Click **Save**. The Redundancy Editor window is refreshed and the new group is displayed.

Editing Redundancy Groups

To edit an existing unit redundancy group:

Step 1 From the **System** menu, choose **Gateways/Units**.

Step 2 In the left navigation pane, click **Redundancy Editor**.

The Redundancy Editor page displays information about current redundancy groups.

Step 3 Under Redundancy Groups, choose the group you want to edit, then from the Actions menu, choose **Edit Group**.

Step 4 In the Redundancy Group Editor, edit any of the following:

- Name—The redundant group name.
- Switchover Delay—The amount of time Prime Performance Manager waits before switching to a redundant unit after a primary unit problem occurs,
- Available Units—The units that are available for the redundant unit and units in the group.
- Enabled—Enables (checked) is disables (unchecked) the redundancy group.
- Redundant Unit—Use the arrows to change the redundant unit.
- Units In Group—Use the arrows to change the units in the redundancy group.

Step 5 Click **Save**. The Redundancy Editor window is refreshed and the edited group information is displayed.

Performing Manual Redundant Unit Failovers

Failovers normally occur automatically when system changes occur on the deployed gateway local HA clusters. (For information about automatic failovers, see Unit Redundancy Group Failover Scenarios, page 13-12 .) If a single service failure occurs, the service is restarted. If the restart fails, the service is relocated to the second gateway server. You normally perform manual failovers to revert the cluster to its original configuration.

To perform a manual failover:

Step 1 From the System menu, choose **Gateways/Units**.

Step 2 In the left navigation pane, click **Redundancy Editor**.

The Redundancy Editor page displays information about current redundancy groups.

Step 3 Under Redundancy Groups, choose the unit redundancy group you want to manually fail over.

Step 4 Under Group Members, choose the primary unit that you want to replace with the redundant unit.

Step 5 From the Actions menu, choose **Failover**.

The Redundancy Editor window is refreshed. Under Group Members, the redundant unit has an Active status; the primary unit has a Standby status with severity Minor.

Step 6 To switch the redundant unit back to Standby status, complete the Switching Redundant Units Back to Standby, page 13-11.

Switching Redundant Units Back to Standby

After the conditions that caused the failover to occur are fixed, you need to perform a manual switch back to return the redundant unit to Standby status.

To switch a unit back to Standby:

Step 1 From the System menu, choose **Gateways/Units**.

Step 2 In the left navigation pane, click **Redundancy Editor**.

Step 3 Under Redundancy Groups, choose the unit redundancy group containing the unit you want switch back.

Step 4 Under Group Members, choose the primary unit that is in Standby status.

Step 5 From the Actions menu, choose **Failback**.

The Redundancy Editor window is refreshed. Under Group Members, the redundant unit now has a Standby status; the primary unit has an Active status.

Displaying Redundancy Group Unit Status

After redundancy groups are created, you can view the status of units in the group by choosing **Gateways/Units f**rom the System menu, then in the navigation pane of the Redundancy Editor window, choose **Redundancy Editor**.

The Redundancy Editor displays the following information:

- Redundancy Groups—Displays the following details for created redundancy groups:
  - Group Name—Lists all created redundancy groups. You can click the column header to sort the groups in ascending or descending alphabetical order.
  - Is Enabled—Indicates whether the redundancy group is enabled.
  - Switchover Delay—Displays the redundancy group switchover delay time.
- Group Members—Displays the following details about redundancy group members.
  - Display Name—The redundancy group name.
  - Management IP Address—The group member IP address. This can be either gateway or unit IP address.
  - Primary/Redundant—The redundancy group role, either primary or redundant.
  - In Service—Indicates whether the group is in service.
  - Severity—If a failover occurs, the severity of the failover.
  - Status—The member unit status, either active or standby.
  - Status Reason—The member unit status description in detail.

You can also display redundancy group status on the Gateway/Units Summary window. This is displayed by default when you can choose from the Gateway/Units from the System menu.

Note To display the unit redundancy status, add the Redundancy Group and Primary/Redundant columns to the window. For information, see Adding and Removing Properties from Property Views, page 3-20. .

Unit Redundancy Group Failover Scenarios

Table 13-3 describes the unit redundancy group and failover behavior after common network circumstances occur.

Table 13-3 Unit Redundancy 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.

Replacing a Failed Unit

On occasion you might need to replace a unit in a unit redundancy group that failed and is no longer operable. To replace a unit with minimal data loss:

- The failed unit must be in a unit redundancy group.
- The active unit must be backed up regularly and the backup file must be available. By default, backup files are located under /opt:*unit*-backup.tar by default. Placing the /opt directory on share storage is recommended using the following command:

  ```
  /opt/CSCOppm-unit/bin/ppm backupdir /NewBackupDirLocation
  ```

  For more information about Prime Performance Manager backups, see Chapter 18, "Backing Up and Restoring Prime Performance Manager."

You can use the following unit replacement procedure for any gateway HA configuration including no HA, local HA only, geographical HA only, or both local and geographical HA.

Note This procedure is intended for a unit that has failed and will not be brought back into the network. If you bring a failed unit back into the network after you complete this procedure data corruption will occur.

To replace a failed unit:

Step 1 Install a new unit (Unit3) on a server connected to the gateway with the same parameters as the failed unit (Unit1) including SSL, gateway association, and other parameters. For installation procedures, see the *Cisco Prime Performance Manager 1.7 Quick Start Guide*.

Step 2 Copy the Unit1 backup file to Unit3:

#scp *failedactiveunit* backup.tar root@*newunit*:/opt/

Step 3 Verify the Unit1 backup file of is available to Unit3:

`scp /opt/ failedactiveunit-backup.tar root@newunit:/opt/`

Step 4 If Unit3 has the same hostname as Unit1, continue with the next step. If the units have different hostnames, rename the Unit1 backup file to the hostname of Unit3:

#mv *failedactiveunit*-backup.tar *newunit*-backup.tar

Note The name of the backup file is relative to the SERVER_NAME in the System.properties file. Failure to properly rename the backup file will cause problems during the restore process.

Step 5 Restore Unit3 with the backup file copied from Unit1:

```
# /opt/CSCOppm-unit/bin/ppm restore
```

Step 6 If SSL was enabled on Unit1, clear SSL on Unit3:

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

Step 7 Complete the "Enabling SSL on Remote Units" procedure on page 6-4 on Unit3.

Step 8 After the gateway and Unit3 reboot, if you want to switch the active and standby roles of Unit3 and Unit2 (the former unit redundancy group standby unit), complete the "Switching Redundant Units Back to Standby" procedure on page 13-11.

Note After Unit3 is online, do not start Prime Performance Manager on Unit1 again. Starting Prime Performance Manager on Unit1 will cause catastrophic database corruption.

Managing Timing Among Gateways, Units, and Clients

In general, set all Prime Performance Manager gateways, units, and clients to a common Network Timing Protocol server. If you do not provision them to an NTP server, timing can become unsynchronized. A message appears when timing is not synchronized between any of the following:

- Gateway and units.
- GUI clients and the current gateway.
- Primary and secondary gateways in a geographical redundant deployment.

If this occurs, update the date and time on the systems reporting the error. For the gateway and units, log into the server and set the time using the Linux date command. For clients, update the time using the client OS date time utilities.

Managing 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

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), Red Hat Enterprise Linux 5.9 (RHEL 5.9), Red Hat Enterprise Linux 5.10 (RHEL 5.10), Red Hat Enterprise Linux 5.11 (RHEL 5.11), Red Hat Enterprise Linux 6.5 (RHEL 6.5), Red Hat Enterprise Linux 6.7 (RHEL 6.7), and Red Hat Enterprise Linux 6.8 (RHEL 6.8) Advanced Program.

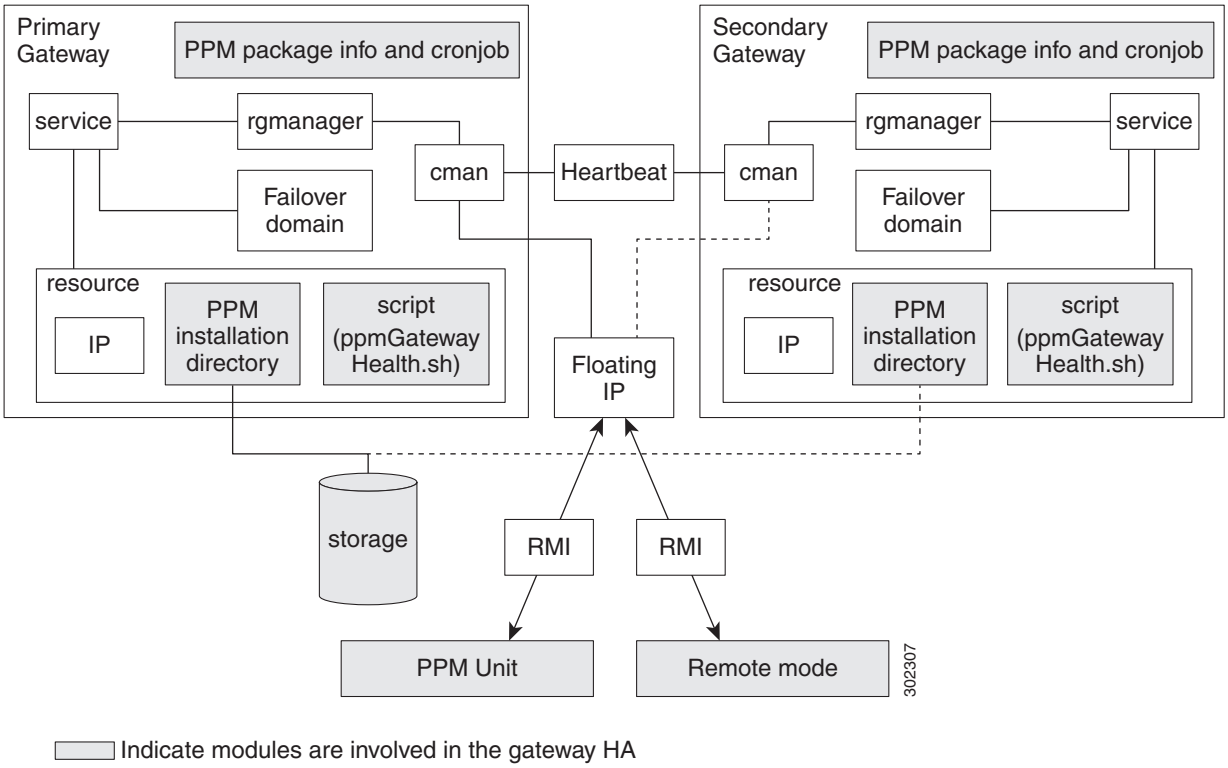
The RHCS cluster infrastructure provides the basic functions that allow the Prime Performance Manager gateways to work together as a cluster. RHCS components include:

- 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, follow 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 14-1 shows the local HA architecture.

Figure 14-1 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 operations, you must:
  1. Freeze the RHCS HA service following the "Freezing and Unfreezing RHCS" procedure on page 14-4.
  2. Complete the Prime Performance Manager operation.
  3. Unfreeze the RHCS service following the "Freezing and Unfreezing RHCS" procedure on page 14-4.

  If you do not freeze RHCS, RHCS will consider 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 service is 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 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 you unfreeze the RHCS cluster service, the service returns to normal operations and checks the Prime Performance Manager HA 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 14-4.

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 *fence_ipmilan* or *fence_vmware_soap* type, choose the **Manual fencing** option during the Prime Performance Manager installation. You can then configure RHCS manually using RHCS CLI or Conga GUI. Refer the Red Hat fencing configuration documentation using Conga.

Refer the following RHEL documentation:

For RHEL 5:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/Configuration_Example_-_Fence_Devices/index.html

For RHEL 6:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Fence_Configuration_Guide/index.html

Note

- The following procedure provides the general configuration of luci interface in RHEL 5. Refer the Red Hat *Conga User Manual* for complete procedure.
- To start and configure RHCS using luci in RHEL 6, refer https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/ch-config-conga-CA.html

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

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 14-1 shows the primary gateway running status.

Table 14-1 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.

Table 14-1 Primary Gateway Running Status

Item	Description
Messages need ack	Count of messages sent to the secondary gateway for which acknowledgment 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 14-2 shows the secondary gateway running status.

Table 14-2 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.
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 connects 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 14-8 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 Importing Devices From Prime Network, page 4-6.
- No BQL update messages are sent to the old primary gateway.
- Users can edit the server from web access.

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 gateway databases are out of synchronization, as indicated by the primary gateway Out of Sync parameter (see Displaying Geographical HA Status, page 14-8), complete the following steps to synchronize them:

Step 1 Log into the primary geographical HA gateway as a root user.

Step 2 Stop the secondary gateway.

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

For information, see Stopping Gateways and Units, page 2-4.

Step 3 Create a new directory on the primary gateway, for example:

```
mkdir /opt/backupdbdir
```

Step 4 Back up the database:

```
ppm primeha backupdb {path}
```

Example:

```
ppm primeha backupdb /opt/backupdbdir
```

Step 5 Remote copy the backupdb folder from the primary to the secondary gateway, for example:

```
scp -r /opt/backupdbdir 192.0.2.10:/opt/
```

Step 6 Log into the secondary gateway and restore its database from the copied remote folder containing the primary database backup files, Prime Performance Manager starts after restoredb completes.

```
ppm start restoredb {path}
```

Example:

```
ppm start restoredb /opt/backupdbdir
```

Prime Performance Manager starts after restoredb is completed.

Step 7 Restart the secondary gateway:

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

For information, see Restarting Gateways and Units, page 2-5.

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

Geographical HA backup and restore follows two general scenarios. You can restore the primary gateway HA data from the primary or peer gateway backup file:

- Primary gateway backup file—You reinstall the gateway OS or Prime Performance Manager. In these cases, the primary gateway backup file is available.
- Peer gateway backup file—The primary gateway suddenly is not available. After it is brought back online, you must restore it using the peer gateway backup file.

Backing Up the Geographical HA Gateway

To back up the geographical HA gateway:

Step 1 Locate the gateway backup file. For automatic gateway backups, the backup file is placed in the Prime Performance Manager install folder, which is /opt, by default. For example:

```
/opt/ppm17-Gateway-crdc-c210-143-backup.tar
```

Step 2 If the gateway is not backed up automatically, back up the gateway manually:

```
/opt/CSCOppm-gw/bin/ppm primeha backup
```

Example:

```
[root@crdc-c210-143 opt]# /opt/CSCOppm-gw/bin/ppm primeha backup
2014/03/06 12:52:09: Prime Performance Manager Gateway backup started.
2014/03/06 12:52:16: Checking size of database started...
2014/03/06 12:52:16: Checking size of reports/logs/etc started....
2014/03/06 12:52:16: Database backup/copy started...
2014/03/06 12:52:19: Pausing for 5 seconds...
2014/03/06 12:52:24: Creating component tars started...
2014/03/06 12:52:24: Pausing for 5 seconds...
touch: cannot touch `cache/device': No such file or directory
2014/03/06 12:52:32: Creating main backup tar started...
FinalServerBackup    =
/opt/ppm17-Gateway-crdc-c210-143-backup.tar
Press Enter to display BackupStats for Gateway:
..
```

Restore the Geographical HA Data From the Gateway Backup File

Step 1 Restore the geographical gateway using the gateway backup file:

```
/opt/CSCOppm-gw/bin/ppm primeha restore {filename}
```

Example:

```
[root@crdc-c210-143 opt]# /opt/CSCOppm-gw/bin/ppm primeha restore
ppm17-Gateway-crdc-c210-143-backup.tar
2014/03/06 14:07:53: Prime Performance Manager Gateway restore
ppm17-Gateway-crdc-c210-143-backup.tar started.
The Gateway must be stopped to perform this operation.
Would you like to stop the Gateway?  [y]
Server files restored from:
/opt/ppm17-Gateway-crdc-c210-143-backup.tar
Follow below procedures for restore:
ppm restore gw
ppm restore unit
ppm start gw
ppm start unit
2014/03/06 14:05:51: Prime Performance Manager Gateway restore
ppm17-Gateway-crdc-c210-143-backup.tar complete.
```

Step 2 Start the gateway. See Starting Gateways and Units, page 2-2.

Restore the Geographical HA Data From the Peer Gateway Backup File

In the following procedure the HA gateways are PPM-1 and PPM-2. The down gateway is PPM-2. Its backup file is not available, so you restore PPM-2 using the PPM-1 backup file.

To restore the gateway using a peer gateway backup file:

Step 1 Back up PPM-1:

```
/opt/CSCOppm-gw/bin/ppm primeha backup
```

Step 2 Copy the backup file from PPM-1 to PPM-2.

```
scp -r ppm17-Gateway-crdc-c210-143-backup.tar root@192.0.2.10:/opt/
```

Step 3 Restore PPM-2 using the PPM-1 backup file:

```
/opt/CSCOppm-gw/bin/ppm primeha restore {filename}
```

Example:

```
/opt/CSCOppm-gw/bin/ppm primeha restore ppm17-Gateway-crdc-c210-143-backup.tar
```

After the restore, PPM-2 has the same configuration as PPM-1 including the HA configuration.

Step 4 Change the PPM-2 peergateway to PPM-1:

```
/opt/CSCOppm-gw/bin/ppm primeha configure peergatewayname PPM-1 IP address
```

Example:

```
/opt/CSCOppm-gw/bin/ppm primeha configure peergatewayname 192.0.2.143
```

Step 5 Start PPM-2. See Starting Gateways and Units, page 2-2.

Recovering From an HA Brain Split

An HA brain split occurs when both HA servers run as the primary gateway. Complete the following steps to recover from an HA brain split. In the procedure, PPM-1 and PPM-2 are used to refer to the two HA gateways.

Step 1 Verify that an HA brain split has occurred by checking the status of each HA gateway:

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

Verify that no errors exist for PPM-1 and PPM-2 status and the HA configuration including peergatewayname, service name, and other attributes. For example, the PPM-2 peergateway should be PPM-1, and the PPM-1 peergateway should be PPM-2. If this is not the case, continue with the next step.

Step 2 Run the following command to see which gateway manages the unit servers:

```
[root@crdc-b200-193 logs]# cat /opt/CSCOppm-unit/properties/System.properties | grep
GATEWAY_NAME
GATEWAY_NAME     = 172.11.11.11
```

Step 3 Stop the gateway that is not managing the units. For example, assuming the current unit servers' GATEWAY_NAME is PPM-1, you would stop PPM-2:

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

Step 4 Complete the "Synchronizing the Geographical HA Gateways" procedure on page 14-11 to synchronize the PPM-1 and PPM-2 databases,

Step 5 Restart PPM-2. It will function as the secondary gateway.

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

Step 6 Monitor the PPM-2 sgmConsoleLog.txt for database synchronization progress. The databases are synchronized when a Sync from Primary Gateway done message appears, for example:

```
[root@crdc-c210-144 bin]# tail -f /opt/CSCOppm-gw/logs/sgmConsoleLog.txt
2014/09/05 10:00:24: NetFlowConfiguration started
2014/09/05 10:00:24: Intializing Server Report Task
2014/09/05 10:00:24: sgmDataServer started: (all services running)
2014/09/05 10:00:24: Starting sgmJMXProxy...
2014/09/05 10:00:24: sgmJMXProxy started.
2014/09/05 10:00:24: Starting sgmTomcat...
2014/09/05 10:00:35: Using Server Version: Apache Tomcat/7.0.55
2014/09/05 10:00:35: sgmTomcat started
2014/09/05 10:00:35: JBoss (MX MicroKernel) [4.2.2.GA (build: SVNTag=JBoss_4_2_2_GA
date=200710221139)] Started in 47s:185ms
2014/09/05 10:00:43: Starting sync from Primary Gateway...
2014/09/05 10:02:27: Sync from Primary Gateway done.
```

Step 7 Verify the primary and then the secondary HA gateway status:

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

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

You can only import Prime Network devices into the primary HA gateway. Additionally, you can only initiate Prime Performance Manager device discovery from the primary HA gateway. Device credentials added to the primary gateway are synchronized to the secondary gateway. If a switchover or failover occurs, the new primary gateway automatically imports the primary gateway devices.

If the 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 reinstalls 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 Devices With Prime Performance Manager.”

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 user 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 as 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 be one alarm issued.

If Prime Performance Manager discovers dual primary gateways, the following event is displayed: $LocalPrimaryGateway, $PeerPrimaryGateway.

Managing Thresholds and Upstream Alarm Hosts in Geographical HA Gateways

Thresholds created on the primary gateway (see "Creating and Managing Thresholds") are synchronized to the secondary gateway. You cannot change thresholds 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 10-14), 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

Use the following procedures to enable SSL on geographical HA gateways and remote units. For additional information, see Enabling 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. (For login steps, see Logging In as the Root User, page 2-1.)

Step 2 If the secondary gateway is up, complete the "Freezing and Unfreezing Geographical HA Gateways" procedure on page 14-11 to freeze the primary gateway and stop the secondary gateway health checking.

Step 3 Enable SSL:

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

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 14-11 to unfreeze it.

To enable SSL on the secondary gateway:

Step 1 Log into the secondary gateway as the root user. (For login steps, see Logging In as the Root User, page 2-1.)

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 Restart primary gateway. (For restart steps, see Restarting Gateways and Units, page 2-5

Step 8 Restart secondary gateway.

Step 9 Restart all units.

Step 10 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 14-11 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 14-11 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

Changes to 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 Managing Unit Redundancy Groups, page 13-8.

Step 2 Stop the protection unit. See Stopping Gateways and Units, page 2-4.

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.

Deploying Prime Performance Manager in an Integrated Geographical HA Configuration with Prime Central

Complete the following procedure to deploy Prime Performance Manager in a geographical HA configuration when integrated with Cisco Prime Central when Prime Central is also configured for geographical HA.

Note Cisco Prime Network must be integrated with Prime Central before you integrate Prime Performance Manager with Prime Central.

Step 1 Use procedures in the *Cisco Prime Performance Manager 1.7 Quick Start Guide* to install Prime Performance Manager gateways on two servers, referred to as PPM-1 and PPM-2.

- Choose installation option 3) **Install Prime Performance Manager Gateway Only**.
- When asked if you want to enable SSL, choose **Yes**.

Step 2 On both gateways, add the following lines to /opt/CSCOppm-gw/properties/System.properties:

```
SYNC_IIU = false
SYNC_EVENT_SNMP_CONFIG = false
```

Step 3 Use procedures in the *Cisco Prime Performance Manager 1.7 Quick Start Guide* to install Prime Performance Manager units on two servers. Choose installation option 4) **Install Prime Performance Manager Unit Only**. These units will be referred to as Unit-1 and Unit-2. When asked to enter a gateway IP address or hostname, enter the IP address or hostname of PPM-1.

Step 4 Integrate PPM-1 with the primary Prime Central server using the "Integrating Prime Performance Manager with Prime Central" procedure on page 4-2.

Step 5 Integrate PPM-2 with the secondary Prime Central server using the "Integrating Prime Performance Manager with Prime Central" procedure on page 4-2.

Step 6 Use the "Exporting SSL Certificates" procedure on page 6-5 to exchange SSL certificates between the following:

- PPM-1 and PPM-2, Unit-1, and Unit-2
- PPM-2 and Unit-1 and Unit-2

Step 7 Use the "Restarting Gateways and Units" procedure on page 2-5 to restart PPM-1, PPM-2, Unit-1, and Unit-2.

Step 8 Log into the primary Prime Central server and restart the integration layer:

```
$PRIMEHOME/bin/itgctl start
```

Step 9 On PPM-1, run the geographical HA script, ppmGeoHA.sh, to configure the geographical HA parameters. Set the Service Role as Primary Gateway, and configure PPM-2 as its peer gateway name.

```
/opt/CSCOppm-1/bin/ppmGeoHA.sh
```

Sample configuration:

```
Configure Geographical HA Gateway Properties...
========================- Service Role -=====================
1 - Primary Gateway
2 - Secondary Gateway
Enter Predefined Service Role : [1]
==================- Peer Gateway Configuration -===============
Enter IP Address or Hostname Of Peer Gateway : 10.74.125.7
Enter RMI Port of Peer Gateway : [45742]
==================- Health Check Configuration -===============
Enter Health Check Interval (Seconds) : [10]
Enter Maximum Continuous Tolerated Fail Numbers : [6]
===========- Gateways Synchronization Configuration -==========
Enable CSV file Synchronization? [n]
Enter Primary Database Age Out (Hours): [24]
```

Step 10 On PPM-1, create a backup directory, ppmgwbackup:

```
mkdir /ppmgwbackup/
```

Step 11 Back up PPM-1 to the new backup directory:

```
/opt/CSCOppm-1/bin/ppm primeha backupdb /ppmgwbackup/
```

Step 12 Copy the PPM-1 ppmgwbackup directory to the PPM-2 /opt/ directory,

Step 13 Stop PPM-2. See Stopping Gateways and Units, page 2-4.

Step 14 On PPM-2, run the geographical HA script, ppmGeoHA.sh, to configure the geographical HA parameters. Set the service role as Secondary Gateway, and configure PPM-1 as its peer gateway name.

```
/opt/CSCOppm-2/bin/ppmGeoHA.sh
```

Sample configuration:

```
Configure Geographical HA Gateway Properties...
========================- Service Role -=====================
1 - Primary Gateway
2 - Secondary Gateway
Enter Predefined Service Role : [2]
==================- Peer Gateway Configuration -===============
Enter IP Address or Hostname Of Peer Gateway : 10.74.125.6
Enter RMI Port of Peer Gateway : [45742]
==================- Health Check Configuration -===============
Enter Health Check Interval (Seconds) : [10]
Enter Maximum Continuous Tolerated Fail Numbers : [6]
===========- Gateways Synchronization Configuration -==========
Enable CSV file Synchronization? [n]
Enter Primary Database Age Out (Hours): [24]
Step 5   After you configure the geographical HA parameters, restart the gateway. It will
operate as the secondary gateway.
```

Step 15 Restore PPM-2 from the ppmgwbackup directory:

```
cd /opt/CSCOppm-2/bin/
./ppmGeoHA.sh
./ppm start restoredb /opt/ppmgwbackup/,
```

Step 16 Verify the PPM-1 geographical HA status:

```
/opt/CSCOppm-1/bin/ppm primeha status
```

Step 17 Verify the PPM-2 geographical HA status.

```
/opt/CSCOppm-2/bin/ppm primeha status
```

Step 18 Freeze PPM-1

```
/opt/CSCOppm-1/bin/ppm primeha freeze
```

Step 19 Use the "Creating New Unit Redundancy Groups" procedure on page 13-9 or the command, ppm redundancygroups, page B-79, to set up a redundancy group for Unit-1 and Unit-2. Make Unit-1 the active unit, and Unit-2 the standby unit.

Performing Disaster Recovery When the Primary Prime Central Server is Not Available

Use the following procedure to test manual disaster recovery in the event the primary Prime Central server is not available. The initial PPM-1 and PPM-2 service roles, statuses, and HA freeze states are shown in Table 14-3.

Table 14-3 Initial PPM-1, PPM-2 Service Roles, Statuses, and HA Freeze States

Gateway	HA Service Role	HA Running Status	Prime Performance Manager Status	HA Freeze
PPM-1	Primary	Primary	Stopped or unreachable	Yes
PPM-2	Secondary	Secondary	Started	Yes

Note In an actual disaster, skip the Step 1 and verify PPM-2 has connectivity to the PPM-1 daily backup file through the SAN.

To test the manual disaster recovery:

Step 1 If PPM-1 is still reachable, that is, you can establish an SSH session with it, set the PPM-1 HA service role to Secondary, then stop Prime Performance Manager:

```
/opt/CSCOppm-1/bin/ppm setservicerole secondary
/opt/CSCOppm-1/bin/ppm stop
```

Step 2 Restart PPM-2:

```
/opt/CSCOppm-2/bin/ppm restart
```

After the restart, PPM-2 will be the primary gateway.

Step 3 Log into the primary Prime Central server and restart the integration layer if this is the first time the switch occurred:

```
$PRIMEHOME/bin/itgctl start
```

Step 4 Check the PPM-2 and Unit-2 connection. If the unit has an Unknown status, provision the unit gateway as PPM-2:

```
/opt/CSCOppm-unit2/bin/ppm gatewayname ppm-2 IP address
```

The switched PPM-1 and PPM-2 service roles, statuses, and HA freeze states are shown in Table 14-4.

Table 14-4 Switched PPM-1, PPM-2 Service Roles, Statuses, and HA Freeze States

Gateway	HA Service Role	HA Running Status	Prime Performance Manager Status	HA Freeze
PPM-1	Primary	Primary	Stopped	Yes
PPM-2	Primary	Primary	Started	Yes

Switching Back to the Primary Gateway Following Disaster Recovery

After Prime Central and the primary Prime Performance Manager gateway return to normal service, complete the following steps to switch from the secondary gateway back to the primary gateway. The steps assume you performed the disaster recovery steps in Performing Disaster Recovery When the Primary Prime Central Server is Not Available, page 14-20, and the status of the primary (PPM-1) and secondary (PPM-2) gateways is shown in Table 14-4.

To switch back to the primary gateway (PPM-1):

Step 1 If PPM-1 status is Secondary/Stopped, continue with Step 2. If not, complete the following commands:

```
/opt/CSCOppm-1/bin/ppm setservicerole secondary
/opt/CSCOppm-1/bin/ppm stop
```

Step 2 Back up PPM-2 to the PPM-1 /opt/ directory:

```
/opt/CSCOppm-2/bin/ppm primeha backupdb
scp tar file ppmxxxxx-backup.tar ppm-1/opt/
```

Step 3 Set the PPM-2 service role to secondary:

```
/opt/CSCOppm-gw/bin/ppm setservicerole [secondary]
```

Step 4 On PPM-1, verify the PPM-2 backup tar file exists on the PPM-1 /opt/ directory. If not, repeat Step 2.

Step 5 Restore PPM-1 from the PPM-2 backup file:

```
/opt/CSCOppm-gw/bin/ppm primeha restore ppmxxxxx-backup.tar
```

Step 6 Set the PPM-1 service role to primary:

```
/opt/CSCOppm-1/bin/ppm setservicerole [primary]
```

Step 7 Set the PPM-1 peer gateway as PPM-2:

```
/opt/CSCOppm-1/bin/ppm primeha peergatewayname [ppm-2 IP address or hostname]
```

Step 8 Start PPM-2:

```
/opt/CSCOppm-2/bin/ppm start
```

Step 9 Verify the PPM-1 geographical HA status:

```
/opt/CSCOppm-1/bin/ppm primeha status
```

Step 10 Verify the PPM-2 geographical HA status:

```
/opt/CSCOppm-2/bin/ppm primeha status
```

The PPM-1 and PPM-2 service roles, statuses, and HA freeze states should match Table 14-4. If not, repeat Steps 2 through 10.

Table 14-5 PPM-1, PPM-2 Service Roles, Statuses, and HA Freeze States Following Switch Back

Gateway	HA Service Role	HA Running Status	Prime Performance Manager Status	HA Freeze
PPM-1	Primary	Primary	Started	Yes
PPM-2	Secondary	Secondary	Started	Yes

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 14-1. To manage geographical HA, follow procedures in Managing Geographical High Availability, page 14-7.

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 the secondary gateway.
- All primary gateway configurations appear on the secondary gateway with no changes.
- All web client sessions to the primary gateway and secondary gateway at the time of disaster are invalidated. All client users must log into the secondary gateway.
- If the secondary gateway is not connected to units, no reports are 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 Enable SSL and user access. See Setting Up User Access and Security, page 6-1.

Step 3 Complete Backing Up and Restoring Geographical HA Gateway Data, page 14-12 to create a backup file of the secondary gateway. Place the file in the directory specified by the value of SBACKUPDIR in System.properties.

Step 4 Complete Backing Up and Restoring Geographical HA Gateway Data, page 14-12 to restore the primary gateway with the secondary gateway backup file.

Configuring Prime Performance Manager for Firewalls

The following topics tell you how to configure Prime Performance Manager for firewalls:

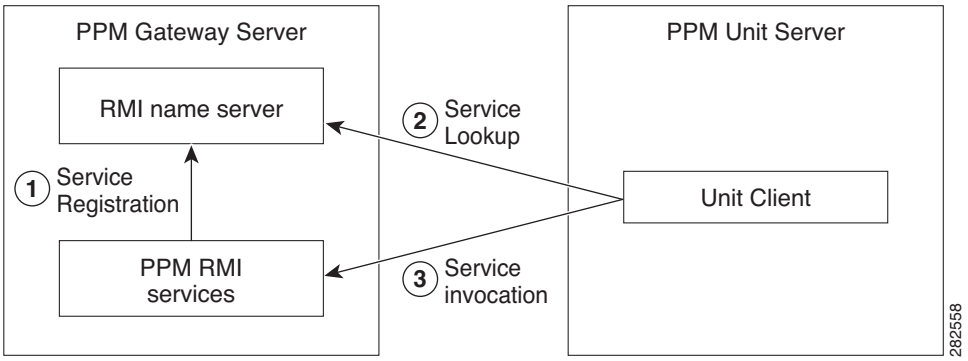
Gateway-to-Unit Connectivity

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 15-1 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 15-1 Prime Performance Manager Communication



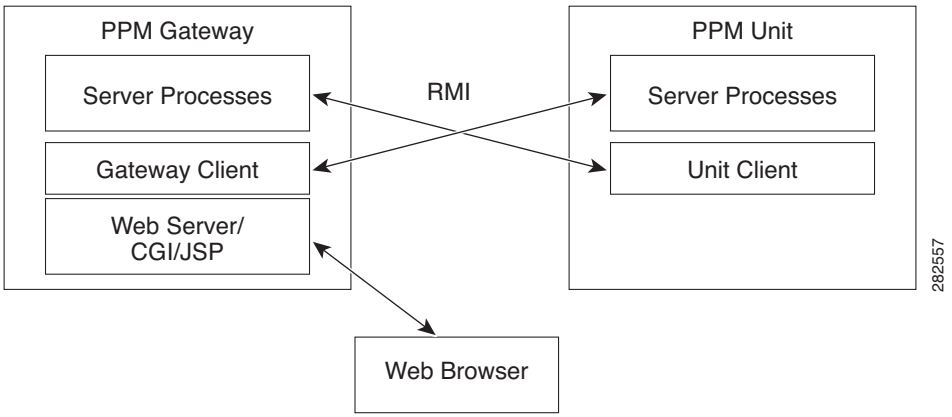
1	Service registration	**3**	Service invocation
2	Service lookup		

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 15-2 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 15-3
- Configuring Gateway and Unit Communication, page 15-3
- Configuring Unit and Device Communication, page 15-6

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 javaver, page B-49, 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 15-1 lists the Prime Performance Manager ports and firewall requirements.

Table 15-1 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 javaver, page B-49, for more information.

Table 15-1 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 15-1.

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 modify the DATASERVER_PORT, LOGINSERVER_PORT, and CLIENT_PORT gateway and unit ports as indicated below. See Table 15-1 for port descriptions and values.

Default gateway:

```
RMIREGISTRY_PORT = 45742
DATASERVER_PORT = 0
LOGINSERVER_PORT = 0
CLIENT_PORT = 0
WEB_PORT = 4440
JSP_PORT = 4440
```

Gateway modified for firewall:

```
RMIREGISTRY_PORT = 45742
DATASERVER_PORT = 45751
```

```
LOGINSERVER_PORT = 45752
CLIENT_PORT = 33459-33479
WEB_PORT = 4440
JSP_PORT = 4440
```

Default unit:

```
RMIREGISTRY_PORT = 55742
DATASERVER_PORT = 0
LOGINSERVER_PORT = 0
CLIENT_PORT = 0
```

Unit modified for firewall:

```
RMIREGISTRY_PORT = 55742
DATASERVER_PORT = 55751
LOGINSERVER_PORT = 55752
CLIENT_PORT = 33459
```

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, ports used by the connection protocol used to connect to the device must be open. Table 15-2 lists the default ports. However, other ports might be assigned when you configure the credential. For information about adding device credentials, see Managing Device Credentials, page 5-3.

Table 15-2 Default Connection Protocol Ports

Protocol	Default Port
SNMP	160
Telnet	23
SSHv1 SSHv2 WSMA_SSH collectd_SSH	22
HTTP HTTP_BULK ESXi_HTTP	80
HTTPS vCenter_HTTPS ESXi_HTTPS PNSC_HTTPS	443
WMI_HTTP WMI_HTTPS	5985
XEN_TLS KVM_TLS	16514
HyperV_HTTP	5985
HyperV_HTTPS	5986
JMX	9001
GMOND_SOCKET	8649
SMI_HTTPS	5989
ULS_HTTP	8082

Managing Multi-Tenant Services

Multi-tenancy is a principle of software architecture where a single instance of the software runs on a server serving multiple client organizations, or tenants. Tenants are logically isolated, but physically integrated.

In Prime Performance Manager you can create tenants directly or import tenants by integrating with OpenStack servers. You can then filter reports, alarms, and thresholds by one or more tenants. Procedures for managing tenants in Prime Performance Manager data are provided in the following topics:

Overview to Multi-Tenancy in Prime Performance Manager

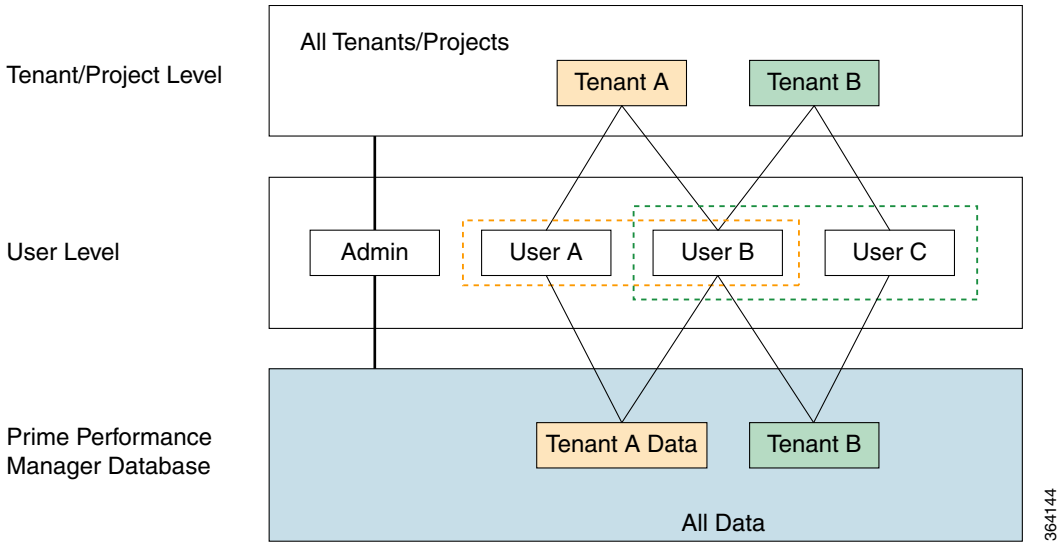
Multi-tenant actions you can perform in Prime Performance Manager include:

- Adding tenants directly.
- Creating tenant groups.
- Importing and synchronizing tenants through integration with an OpenStack server.
- Filtering reports, thresholds, and alarms by tenant scope.
- Displaying alarms filtered by tenant scope.
- Associating Prime Performance Manager users to tenants.

Figure 16-1 provides an overview to the Prime Performance Manager tenant and user data access:

- User A is a member of Tenant A, User A can only access data defined for Tenant A.
- User B is a member of both Tenant A and Tenant B, User B can access data defined for both Tenant A and Tenant B.
- User C is a member of Tenant B, User C can only access data defined for Tenant B.
- The Admin user is the administrator, and can access all Prime Performance Manager data.

Figure 16-1 Multi-Tenancy Support in Prime Performance Manager



Creating Tenants in Prime Performance Manager

You can create tenants in Prime Performance Manager using one of the following methods:

- Create tenants through the Tenant window, then create the report filtering for the tenant.
- Create a tenant group then assign the data source and algorithms to filter the data objects and reports for the tenant group.

In general, creating tenants through the Tenants window is quicker and simpler, but does not provide the filtering capabilities tenant groups provide.

Following tenant creation, you must modify the definition file.

Instructions are provided in the following topics:

- Adding Tenants to Prime Performance Manager From the Tenants Window, page 16-2
- Adding Tenants to Prime Performance Manager Through Tenant Groups, page 16-3
- Adding Tenants Through OpenStack Integration, page 16-4

Adding Tenants to Prime Performance Manager From the Tenants Window

To add tenants Prime Performance Manager through the Tenants window:

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

Step 2 If user access is not enabled, enable it following the "Enabling Secure User Access" procedure on page 6-11.

Step 3 From the Administration menu, choose **Users/Tenants/Security**.

Step 4 On the Users window, click the **Tenants** tab.

Step 5 On the Tenants window, click **Add**.

Step 6 In the Add Tenant dialog box, enter:

- Tenant Name—The tenant name.
- Display Name—The tenant display name.
- Tenant Status—Choose Enabled to enable the tenant (default), or Disabled to not enable it.

Step 7 Click **Save**.

Step 8 On the Tenants window, choose the tenant you created and on the toolbar click **Filter Reports**.

Step 9 On the Tenant Reports window, check or uncheck the reports you want available to the tenant.

Step 10 To display or hide report data columns:

a. Navigate to the report and click the **Tenant Report Condition** icon next to the report title.

The Tenant Filter Condition: [*report category:report title*] dialog box is displayed.

b. In the Column Name field choose the report column for which you want to set conditions.

The column display name and data type are displayed in the Display Name and Column Type fields.

c. In the Filter Value field, enter the value that you want the report data column to equal before it is displayed to tenant members. (Equal is the only available operator.)

d. Click **Add**.

e. If you want to add or append additional conditions, repeat Step c and click **Add** to add a new condition, or click **Append** to append the condition to the existing one.

f. When finished, click **OK**.

Step 11 On the Tenant Reports window, click **Save** to save the tenant filter.

Adding Tenants to Prime Performance Manager Through Tenant Groups

To add tenants to Prime Performance Manager by creating tenant groups:

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

Step 2 If user access is not enabled, enable it following the "Enabling Secure User Access" procedure on page 6-11.

Step 3 From the Administration menu, choose **Group Editor**.

Step 4 Click the **Create New Group** tool.

Step 5 In the Create Group dialog box, enter the group name.

Step 6 Click **OK**.

The new group is added to the System Groups table.

Step 7 Click the new group link.

Step 8 In the Group Details tab Type/Tag field, enter **ppm_tenant**.

This tag identifies the group as a tenant and will cause it to appear on the Tenants window.

Step 9 In the Data Source area, click **Change**.

Step 10 In the Edit Group Data Source dialog box, choose the data sources you want for the tenant and click Add to move them to the Assigned Data Sources group.

Step 11 When finished, click **Save**.

Step 12 To create an algorithm to run against the selected data source(s), click **Launch Algorithm Editor (Beta)**.

Step 13 Create the algorithm by dragging blank operator equations to the area on the right, then dragging the variables on the top to fill in the blank elements of the operator equation.

Step 14 When finished, click **Save and Quit**.

Step 15 On the Group Details tab, click **Validate** to validate the data source and algorithm.

Step 16 Click **Save**.

Adding Tenants Through OpenStack Integration

OpenStack is an open-source cloud computing platform generally deployed in infrastructure as a service (IaaS) solutions. OpenStack controls data center processing pools, storage, networking resources, and many other IaaS functions.

Tenants are primary organizational elements within the OpenStack Compute service. (The OpenStack Compute service provides virtual servers upon demand.) OpenStack tenants include a separate VLAN, volumes, instances, images, keys, and users.

You can import OpenStack tenant data into Prime Performance Manager by connecting to the OpenStack server and running the tenant integration function. After the OpenStack tenants are added, you can set up report filtering to restrict report data to that which is appropriate for the tenant.

To add OpenStack tenant data to Prime Performance Manager:

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

Step 2 From the Administration menu, choose **OpenStack Tenant Integration.**

The Administration Tenants window displays.

Step 3 Click the **Tenants** tab.

Step 4 On the OpenStack Tenants toolbar, click **Add New Tenant**.

In the Add Tenant Integration dialog, enter the integration parameter:

- Host Name or IP Address—Enter the OpenStack server host name or IP address. For multi-node OpenStack deployments, this is the server where the OpenStack Keystone API service is installed.
- Protocol—Choose the protocol used to access the server, either HTTP or HTTPs.
- Port—Enter the OpenStack Identify service administrative endpoint. The default is 35357.
- Tenant Name\User Name (Admin Role)—Enter the OpenStack project name and user in the format: [*ProjectName*]\[*UserName*]. For example, if the username is admin and the project name to which the admin user belongs is openstack, you would enter openstack\admin.
- Password—Enter the user password.
- Version—The Keystone Web API version. Currently only Version 2.0 is supported.
- Sync Interval—Choose the tenant data synchronization interval: 30 minutes, 1 hour, or 6 hours.

Note The synchronization interval must be longer than the life of the OpenStack authenticate token.

Step 5 Click **Save & Import**.

Note Save & Import will not activate if fields are blank or have invalid entries.

The tenant import After successful integration, the tenant is added to the Administration Tenant Integration table with the parameters entered in the previous step as well as the following:

- Ongoing Tenant Synchronization—Indicates whether the tenant data is automatically updated.
- Last Import of Tenant—The date the tenant data was last updated.

Step 6 At any later time, you can:

- Edit any tenant parameter in the table except the host name or IP address. After editing, click **Save All Tenants** on the toolbar to update the edited entries.
- Select a tenant and perform the following actions in the Action column:
  - **Synchronize Tenant Data**—Synchronizes the tenant data and updates the last import date and time.
  - **Disable Tenant Data Synchronization**—Stops ongoing tenant data synchronization.
  - **Enable Tenant Data Synchronization**—Starts ongoing tenant data synchronization.
  - **Delete Tenant**—Removes the tenant entry and all associated tenant data.

Adding OpenStack Tenant Message Brokers

After you create an OpenStack tenant and import its data to Prime Performance Manager, you can set up message brokers that listen for OpenStack tenant changes and update the Prime Performance Manager tenant data when they occur. The message brokers supplement the ongoing tenant data synchronization set up at 30-minute, one-hour, or six-hour intervals when you add the tenant entry to Prime Performance Manager. Message brokers have two requirements:

- OpenStack must use the RabbitMq message broker. Qpid and ZeroMQ are not supported.
- At least one OpenStack tenant must be added to Prime Performance Manager. See Adding Tenants Through OpenStack Integration, page 16-4.

To add an OpenStack tenant message broker:

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

Step 2 From the Administration menu, choose **OpenStack Tenant Integration.**

Step 3 Click the **Message Broker** tab.

Step 4 On the OpenStack Message Broker Configuration toolbar, click **Add New Message Broker Entry**.

Step 5 In the Add New Message Broker Entry dialog box, enter the following properties:

- Name—Enter unique name for the message broker entry.

- Broker IP Address—Enter the IP address of the RabbitMq message broker.
- Broker Listener Port—Enter the port used by the message broker to listen for messages. The default port is 5672.
- Broker Virtual Host—Enter the virtual host configured on message broker. The default is /.
- User Name—Enter the username needed to connect to the message broker.
- Password—Enter the username password.
- Enabled—Check if you want to enable the message broker after it is created.
- IP Address of OpenStack—Choose the OpenStack IP address from the list, which is populated from the OpenStack tenants that appear in the OpenStack tab.

Step 6 Click **OK**.

The message broker entry is added to the Message Broker table.

Step 7 At any later time, you can:

- Edit any message broker parameter in the table except the name or OpenStack IP address. After editing, click **Save Message Broker Entries** on the toolbar to update the edited entries.
- Select a tenant and perform the following actions in the Action column:
  - **Enable/Disable Message**—Check the box to enable the message broker; uncheck the box to disable it.
  - **Delete**—Removes the message broker entry.

Note If the tenant that the message broker is monitoring is disabled, the status changes to Unknown. Some brokers should not be added.

Adding Users to Tenants

After you create or add tenants to Prime Performance Manager, you can add users to them. User creation and editing procedures are provided in the following topics:

- Adding New Users, page 6-15
- Editing User Information, page 6-18

When you create or edit a user, in the Tenant Name field check the tenants to which you add the user. After you save the user or user information updates, you can display the tenants to which the user belongs by clicking the **Tenants** box.

Setting Up OpenStack Ceilometer Reports

OpenStack ceilometers provide a point of contact for billing systems to acquire measurements for customer billing across all current OpenStack core components. Ceilometer reports are located in the Compute > OpenStack report category.

By default, ceilometer collects metrics every 10 minutes. Prime Performance Manager allows you to configure other intervals. If the interval is lower than the ceilometer interval, Prime Performance Manager fills the data automatically by using most recent data. Therefore, the polling interval must always be larger then the ceilometer interval.

When configuring Prime Performance Manager to monitor OpenStack, review the default OpenStack Ceilometer poll interval. By default this is 10 minutes. Disable OpenStack reports that are less than the Ceilometer poll interval, otherwise Prime Performance Manager will poll OpenStack more frequently than OpenStack is updated. For example, if the OpenStack Ceilometer poll interval is the 10-minute default, disable OpenStack 1 and 5 minute reports. See Customizing Individual Report Settings, page 7-27.

Displaying Tenant Reports

If OpenStack tenant integration is enabled, hypervisor and OpenStack Ceilometer report data are filtered automatically.

Note For OpenStack tenant integration, Prime Performance Manager must import Ceilometer as the monitored device for data filtering. Hypervisors are optional.

For tenants added to Prime Performance Manager directly, filtering is set up at the time you create the tenant. See the following topics:

- Adding Tenants to Prime Performance Manager From the Tenants Window, page 16-2,
- Adding Tenants to Prime Performance Manager Through Tenant Groups, page 16-3

To display report data by tenant:

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

Step 2 On the Prime Performance Manager toolbar, click **User Preferences**.

Step 3 In the User Preferences window, click **General Display Settings**.

Step 4 In the right column, modify the following tenant report properties:

- Tenant Scope—Sets the report tenant scope:
  - All—Displays all reports, not just tenant reports.
  - All Tenants—Displays all tenant reports.
  - SELECTED—Allows you to select and display reports for individual tenants.
- Tenant Display—Sets the tenant identifier when displayed in reports, either Name (internal tenant name), or Display Name.

For example, if you set Tenant Scope to All Tenants and Tenant Display to Display Name, then navigate to Reports > Compute > OpenStack > [Ceilometer], you will notice a new Tenant column is displayed with the data for all Tenants.

Displaying Alarms and Events by Tenant

Alarms and events have a Tenant attribute that you can use to sort alarms and events by tenant. The Tenant attribute is not displayed by default. To display it, see Adding and Removing Properties from Property Views, page 3-20.

Adding Tenants to Thresholds

Prime Performance Manager thresholds allow you define performance criteria for displaying threshold crossing alert alarms and events. For complete information about Prime Performance Manager thresholds, see Chapter 11, "Creating and Managing Thresholds." When you create thresholds, you can apply one, multiple, or all tenants to it.

To add tenants to threshold crossing alerts:

Step 1 Complete the "Creating Thresholds" procedure on page 11-1.

Step 2 Complete the following tenancy fields:

- Tenancy—Indicates the tenants that should be included in the threshold:
  - ALL—(default) Choose this option if you do not want to assign tenants to the threshold.
  - ALL_TENANTS—Includes all tenants in the threshold.
  - SELECTED—Allows you to choose the tenants added to the threshold
- Selected Tenants—If you chose SELECTED in the Tenancy field, displays the tenants that added.

  To add tenants, click **Change** then chose the tenants you want in the Select Tenants dialog box using the **Add**, **Add All**, **Remove**, **Remove All** buttons.

Tenant Views

After you integrate Prime Performance Manager with OpenStack tenants, you view information about them in the Data Center > Tenants view. Each tenant view includes the following subviews retrieved from the OpenStack server:

- Network—Displays information about the tenant VLAN.
- Compute—Displays the tenant virtual machines. In OpenStack Horizon, these are called instances.
- Storage—Displays information about tenant storage volumes.

To display tenant details, click the tenant in the View tree. The following tenant details are displayed:

- Name—The tenant name.
- Status—The tenant status, either enabled or disabled.
- Description—A description of the tenant, if added.
- Tenant Source—The source of the tenant. Currently, this will be OpenStack.
- Ongoing Tenant Synchronization—Indicates whether regular synchronization occurs between Prime Performance Manager and the OpenStack server, either Yes or No.

- Last import of tenant—Indicates the data and time of the last tenant information synchronization.

Pushing Prime Performance Manager Data to Other Applications

Although Prime Performance Manager is designed to get data from devices and display that data in a variety of ways, you can push Prime Performance Manager data to certain applications including Graphite, Apache Kafka, and OpenStack ceilometers. Procedures for pushing data to these applications are provided in the following topics:

Pushing Data to Graphite

Graphite is an open-source tool that monitors and graphs computer performance. It stores numeric time-series data and displays data graphs on demand. To display Prime Performance Manager data in Graphite, you push the data to Carbon, twisted daemon Graphite component that listens for time-series data. For information about configuring Carbon, see the Graphite user documentation at: http://graphite.readthedocs.org/en/latest/.

Note Prime Performance Manager only pushes numeric data to Graphite. Non-numeric data, such as string value report data, is ignored.

To push Prime Performance Manager data to Carbon:

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

Step 2 Verify that devices are imported into Prime Performance Manager and reports are being generated successfully.

Step 3 From the Administration menu, choose **NB Push Editor**.

Step 4 In the NB Push Editor window, click the **Add a New North Bound Destination** tool.

Step 5 In the Destination Server area, enter the following:

- Name—Enter a unique name for the northbound destination entry.
- Enabled—If checked, data is pushed to Carbon after the entry is created.

- Queue Size—The maximum number of messages in the push queue. The default is 10000.
- Reconnect Interval—After a disconnect, the time to wait before attempting a reconnect. The default is 60000 milliseconds.
- Type—Choose **CARBON**.
- Server Name or IP Address—Enter the Graphite server name or IP address.
- Port—Enter the Graphite port to be used to push data to Carbon.
- Maximum Datapoints Per Message—Sets the maximum number of datapoints per message. In Graphite, a datapoint is a value stored at a timestamp bucket.
- Base Folder—Enter the folder Prime Performance Manager should use to push data to Carbon. In Graphite calls this a naming hierarchy, which is a path with components delimited by dots, for example, [*DeviceName*].[*TableName*].[*KeyNames*].[*KPIName*].[*Interval*].

Step 6 On the Destination Server toolbar, click **Save Destination Server**.

The new northbound server entry is added to the NB Push Editor navigation tree with two items:

- Web Reports—Allows you to define the push data using the report categories displayed in Performance > Reports.
- DB Summary—Allows you to define the data to push using the actual Prime Performance Manager database tables, not the virtual tables Prime Performance Manager creates for report data. For more information, see Overview to Database Summary Tables, page 17-8.

Step 7 In the NB Push Editor tree, choose either **Web Reports** or **DB Summary**.

Step 8 Complete the following parameters:

- Enabled—Check if you want to enable the data options chosen for Web Reports or DB Summary. The option allows you to turn the Web Reports or DB Summary options on and off separately.
- Enable All Reports—Enables all report or database summary data items down to the lowest level.
- Tenant—Sets the type of tenant data to push:
  - Raw—Push non-tenant data only.
  - Tenant—Push tenant data only.
  - Both—Push both tenant and non-tenant data.
- Available Intervals—Choose one or more report intervals:
  - 1 Minute
  - 5 Minute
  - 15 Minute
  - Hourly
  - Daily
  - Weekly
  - Monthly

Note Only enabled intervals are shown. If an interval you want to use is not shown, from the Performance menu choose **Reports** > **Report/Group Settings** and enable it.

Step 9 Complete one of the following:

- If you selected Web Reports, choose the categories containing the reports you want to push, or click Select All if you want all categories selected.
- If you selected Database Summary Tables, choose the tables containing the data you want to push.

Tip You can also click **Selection Dialog** and choose report categories or database tables in the dialog.

Step 10 After making your selections, click either **Save Web Report Settings** or **Save DB Summary Settings** to save your entries.

The saved entry items appear in the NB Push Editor navigation tree. Entries with lower level report or database entries will have an small arrow on the left that you can click to display lower-level entries.

Step 11 On the navigation tree, expand the new entry and select an item under it. New report or data categories or items appear in the display area.

Step 12 In the display area, choose the categories or data items you want included in the push data.

Step 13 Click either **Save Web Report Settings** or **Save DB Summary Settings** to save your entries.

Step 14 Repeat Steps 11 through 13 until you reach the end of the report or summary table tree.

If needed, you can select items up and down the navigation tree to refine your category or data choices.

Note Always click **Save Web Report Settings** or **Save DB Summary Settings** before you move to a new navigation tree item.

Step 15 After you finish your data selections, if you enabled Prime Performance Manager to push the data, you can perform one or both of the following to verify Carbon is receiving it:

- You can go to the Graphite Carbon console to watch the data.
- You can go to the Prime Performance Manager console and watch for messages such as:

```
15631 | 2015/06/04 21:40:37 | Info | sgmProcessManager.crdc-b200-vm152.14dbec69e6b |
Thread-48 | None | Push to Carbon Status: Time: 2015/06/04 21:35:00; TotRec: 286000;
AvgLen: 1216; TotKPI: 10115.0; KPIThr: 266184.2105263158; QSize: 1989 | 1433425237 |
null | null
```

Where,

  - TotRec is the total number of records pushed.
  - AvgLen is the average record length.
  - TotKPI is the total number of KPIs pushed since last time.
  - KPIThr is the KPI throughput.
  - QSize is current number of records in the Prime Performance Manager queue

By default, this message is printed every five minutes.

Pushing Data to Apache Kafka

Apache Kafka is a distributed, partitioned, replicated, publish-subscribe commit log service. It provides the functionality of a messaging system, but with a unique design. A single Kafka broker can handle hundreds of megabytes of reads and writes per second from thousands of clients. For information about configuring Kafka, see the Apache Kafka user documentation at: http://kafka.apache.org/.

To display Prime Performance Manager data in Kafka:

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

Step 2 Verify that devices are imported into Prime Performance Manager and reports are being generated successfully.

Step 3 From the Administration menu, choose **NB Push Editor**.

Step 4 In the NB Push Editor window, click the **Add a New North Bound Destination** tool.

Step 5 In the Destination Server area, enter the following:

- Name—Enter a unique name for the northbound destination entry.
- Enabled—Check if you want the report data pushed to Kafka after it is created.
- Queue Size—The maximum number of messages in the push queue. The default is 10000.
- Reconnect Interval—If a disconnect occurs, the interval that a reconnect attempt is made. The default is 60000 milliseconds.
- Type—Choose **KAFKA**.
- Compression—Choose the data compression method:
  - None—No data compression is used.
  - GZIP—GNU zip (gzip) compression is used.
  - SNAPPY—Snappy compression is used.
- Metadata Push Frequency—The metadata push frequency:
  - NONE—Metadata is not pushed.
  - ONCE—Metadata is pushed once.
  - ALWAYS—Metadata is always pushed.
- Serializer Class—(serializer.class) The serializer class used at the Kafka producer Prime Performance Manager configuration.
- Event ID—Is used only by the Cisco Cloud Service and is the Kafka producer ID. In this case, it is the Prime Performance Manager ID, which is 1001.
- Batch Size—(batch.size) The number of messages batched at the Kafka producer before being displatched to the event.handlere. The default is 200.
- Topic—The Kafka topic to which Prime Performance Manager data is pushed.
- ZooKeeper Connections—(zookeeper.connect) Is not used in this release.

Step 6 On the Destination Server toolbar, click **Save Destination Server**.

The new northbound server entry is added to the DB Push Editor navigation tree with two items:

- Web Reports—Allows you to define the push data using the report categories displayed in Performance > Reports.

- DB Summary—Allows you to define the data to push using the actual Prime Performance Manager database tables, not the virtual tables Prime Performance Manager creates for report data. For more information, see Overview to Database Summary Tables, page 17-8.

Step 7 In the NB Push Editor tree, choose either **Web Reports** or **DB Summary**.

Step 8 Complete the following parameters:

- Enabled—Check if you want to enable the data options chosen for Web Reports or DB Summary. The option allows you to turn the Web Reports or DB Summary options on and off separately.
- Enable All Reports—Enables all report or database summary data items down to the lowest level.
- Tenant—Sets the type of tenant data to push:
  - Raw—Push non-tenant data only.
  - Tenant—Push tenant data only.
  - Both—Push both tenant and non-tenant data.
- Available Intervals—Choose one or more report intervals:
  - 1 Minute
  - 5 Minute
  - 15 Minute
  - Hourly
  - Daily
  - Weekly
  - Monthly

Note Only enabled intervals are shown. If an interval you want to use is not shown, from the Performance menu choose **Reports > Report/Group Settings** and enable it.

Step 9 Complete one of the following:

- If you selected Web Reports, choose the categories containing the reports you want to push, or click Select All if you want all categories selected.
- If you selected Database Summary Tables, choose the tables containing the data you want to push.

Tip You can also click **Selection Dialog** and choose report categories or database tables in the dialog.

Step 10 After making your selections, click either **Save Web Report Settings** or **Save DB Summary Settings** to save your entries.

The saved entry items appear in the NB Push Editor navigation tree. Entries with lower level report or database entries will have an small arrow on the left that you can click to display lower-level entries.

Step 11 On the navigation tree, expand the new entry and select an item under it. New report or data categories or items appear in the display area.

Step 12 In the display area, choose the categories or data items you want included in the push data.

Step 13 Click either **Save Web Report Settings** or **Save DB Summary Settings** to save your entries.

Step 14 Repeat Steps 11 through 13 until you reach the end of the report or summary table tree.

If needed, you can select items up and down the navigation tree to refine your category or data choices.

Note Always click **Save Web Report Settings** or **Save DB Summary Settings** before you move to a new navigation tree item.

Step 15 After you finish your data selections, if you enabled Prime Performance Manager to push the data, you can perform one or both of the following to verify Carbon is receiving it:

- You can go to the Kafka console to watch the data.
- You can go to the Prime Performance Manager console and watch for messages such as:

```
15631 | 2015/06/04 21:40:37 | Info | sgmProcessManager.crdc-b200-vm152.14dbec69e6b |
Thread-48 | None | Push to Kafka Status: Time: 2015/06/04 21:35:00; TotRec: 286000;
AvgLen: 1216; TotKPI: 10115.0; KPIThr: 266184.2105263158; QSize: 1989 | 1433425237 |
null | null
```

  Where,

  – TotRec is the total number of records pushed.

  – AvgLen is the average record length.

  – TotKPI is the total number of KPIs pushed since last time.

  – KPIThr is the KPI throughput.

  – QSize is current number of records in the Prime Performance Manager queue

  By default, this message is printed every five minutes.

Pushing Data to OpenStack Ceilometers

Prime Performance Manager can monitor OpenStack virtual machines (VMs) through different paths and therefore retrieve some VM data not available in OpenStack Ceilometers. For example, Prime Performance Manager can get the availability percentage of each OpenStack VM. By pushing this data to the OpenStack Ceilometers, OpenStack users will see the new meter created and supported by Prime Performance Manager in the Ceilometer. For information about configuring OpenStack Ceilometers, see the OpenStack developer documentation at: http://docs.openstack.org/developer/ceilometer/.

To display Prime Performance Manager data in OpenStack Ceilometers:

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

Step 2 Verify that devices are imported into Prime Performance Manager and reports are being generated successfully.

Step 3 From the Administration menu, choose **NB Push Editor**.

Step 4 In the NB Push Editor window, click the **Add a New North Bound Destination** tool.

Step 5 In the Destination Server area, enter the following:

- Name—Enter a unique name for the northbound destination entry.
- Enabled—Check if you want the report data pushed to the Ceilometer after it is created.
- Queue Size—The maximum number of messages in the push queue. The default is 10000.
- Reconnect Interval—If a disconnect occurs, the interval that a reconnect attempt is made. The default is 60000 milliseconds.

- Type—Choose **CEILOMETER**.
- Server Name or IP Address—Enter the Ceilometer server name or IP address.
- Port—Enter the Ceilomeeter port.
- Protocol—Choose the Ceilometer protocol.

Step 6 On the Destination Server toolbar, click **Save Destination Server**.

The new northbound server entry is added to the DB Push Editor navigation tree with two items:

- Web Reports—Allows you to define the push data using the report categories displayed in Performance > Reports.
- DB Summary—Allows you to define the data to push using the actual Prime Performance Manager database tables, not the virtual tables Prime Performance Manager creates for report data. For more information, see Overview to Database Summary Tables, page 17-8.

Step 7 In the NB Push Editor tree, choose either **Web Reports** or **DB Summary**.

Step 8 Complete the following parameters:

- Enabled—Check if you want to enable the data options chosen for Web Reports or DB Summary. The option allows you to turn the Web Reports or DB Summary options on and off separately.
- Enable All Reports—Enables all report or database summary data items down to the lowest level.
- Tenant—Sets the type of tenant data to push:
  - Raw—Push non-tenant data only.
  - Tenant—Push tenant data only.
  - Both—Push both tenant and non-tenant data.
- Available Intervals—Choose one or more report intervals:
  - 5 Minute
  - 15 Minute
  - Hourly
  - Daily
  - Weekly
  - Monthly

Step 9 Complete one of the following:

- If you selected Web Reports, choose the categories containing the reports you want to push, or click Select All if you want all categories selected.
- If you selected Database Summary Tables, choose the tables containing the data you want to push.

Tip You can also click **Selection Dialog** and choose report categories or database tables in the dialog.

Step 10 After making your selections, click either **Save Web Report Settings** or **Save DB Summary Settings** to save your entries.

The saved entry items appear in the NB Push Editor navigation tree. Entries with lower level report or database entries will have an small arrow on the left that you can click to display lower-level entries.

Step 11 On the navigation tree, expand the new entry and select an item under it. New report or data categories or items appear in the display area.

Step 12 In the display area, choose the categories or data items you want included in the push data.

Step 13 Click either **Save Web Report Settings** or **Save DB Summary Settings** to save your entries.

Step 14 Repeat Steps 11 through 13 until you reach the end of the report or summary table tree.

If needed, you can select items up and down the navigation tree to refine your category or data choices.

Note Always click **Save Web Report Settings** or **Save DB Summary Settings** before you move to a new navigation tree item.

Step 15 After you finish your data selections, if you enabled Prime Performance Manager to push the data, you can perform one or both of the following to verify Carbon is receiving it:

- You can go to the OpenStack Ceilometer console to watch the data.
- You can go to the Prime Performance Manager console and watch for messages such as:

```
15631 | 2015/06/04 21:40:37 | Info | sgmProcessManager.crdc-b200-vm152.14dbec69e6b |
Thread-48 | None | Push to OpenStack Ceilometer Status: Time: 2015/06/04 21:35:00;
TotRec: 286000; AvgLen: 1216; TotKPI: 10115.0; KPIThr: 266184.2105263158; QSize: 1989
| 1433425237 | null | null
```

Where,

  - TotRec is the total number of records pushed.
  - AvgLen is the average record length.
  - TotKPI is the total number of KPIs pushed since last time.
  - KPIThr is the KPI throughput.
  - QSize is current number of records in the Prime Performance Manager queue

By default, this message is printed every five minutes.

Overview to Database Summary Tables

You can push Prime Performance Manager data to northbound applications using two options: Web Reports and DB Summary. Web reports displays data in the report categories displayed when you choose Reports from the Performance menu. The DB Summary option refers to the processdbsummary report parameter and defines the Prime Performance Manager raw to push northbound. Use of this option requires an understanding of the Prime Performance Manager architecture described in the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*.

DB Summary folder parameters define the next level of parameters and identify the processdbsummary defnition (database table). The folder hierarchy for a processdbsummary is single level and is used only to identify the database table of interest. The data is raw Prime Performance Manager data after processing by the polldefinition and processpollresults functions and not the data as collected directly from devices/objects.

The Prime Performance Manager report XML files provide some database summary details and definitions, for example, here is the report XML file for (/opt/CSCOppm-gw/etc/pollers/system/hypervisorESXi.xml):

```
<PollDefinition>
      ESXiVMAvailabilityTable = hypervisorPoll("ListVMAvailability",
                                               "",
```

```
                                                "",
                                                false);
 </PollDefinition>

<ProcessPollResult>
   vmAvailabilityPer            = numOfActiveDomains / totalOfDomains;
</ProcessPollResult>

<ProcessDBSummary name="ESXiVMAvailability"
                  baseTableName="ESXiVMAvailability"
                  maxEntriesPerId="1000000" maxEntriesPerInterval="1000000">

  <Var name="NumOfActiveDomains"  type="Integer">numOfActiveDomains</Var>
  <Var name="NumOfInActiveDomains"  type="Integer">numOfInActiveDomains</Var>
  <Var name="TotalOfDomains"  type="Integer">totalOfDomains</Var>
  <Var name="VMAvailabilityPer"  type="Float">vmAvailabilityPer</Var>
</ProcessDBSummary>
```

For more information, see the *Cisco Prime Performance Manager 1.7 Integration Developer Guide*

CHAPTER 18

Backing Up and Restoring Prime Performance Manager

The following topics tell you how to back up and restore Prime Performance Manager:

Prime Performance Manager Back Up and Restore Process

The Prime Performance Manager backup and restore function allows you to retrieve user accounts, logs, reports, and security-related parts of Prime Performance Manager data files from the previous night's backup. You should perform backup and restore in sets at the same clock time. Sets consists of a gateway and its units.

Note If backups are not performed in sets, data might become unsynchronized between the gateway and its units.

The backup and restore steps on a gateway and collocated unit include:

1. Backup is normally performed on the unit at 2:30 AM and gateway at 3:30 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 or user enabled with ppm superuser and change the *root crontab* file:

- **crontab -l** lists cron jobs.
- **crontab -e** opens up an editor so you can make changes and save them.

Related Topics:

- Backing Up Prime Performance Manager Data Files, page 18-2
- Changing the Backup Directory, page 18-3
- Setting the Number of Backup Days, page 18-3
- Restoring Prime Performance Manager Data Files, page 18-3

Backing Up Prime Performance Manager Data Files

To manually back up Prime Performance Manager data files at any time on a Solaris or Linux server:

Step 1 Log in as the root user or user enabled with ppm superuser.

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 or user enabled with ppm superuser.

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 or user enabled with ppm superuser.

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 or user enabled with ppm superuser.

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 accidentally edited the report definition files.

Step 4 To view statistics on the backup process, enter:

```
./ppm backupstats
```

Note If the number of backup days has been set to more than one day (see Setting the Number of Backup Days, page 18-3), Prime Performance Manager will prompt you for a server backup file restore from as there is no client backups.

Warning **Do not interrupt this command. Doing so can corrupt your Prime Performance Manager data files.**

Additional Backup Commands

Additional backup commands include:

- ppm backupstats—Displays backup process statistics. For information, see ppm backupstats, page B-18.
- ppm backupdata {enable|disable|status} [gw|unit|both]—Specifies whether the database is included in backups. For information, see ppm backupdata, page B-13.
- ppm backuprep {enable|disable|status]—Specifles whether to Include CSV reports in backups. For information, see ppm backuprep, page B-17.

Prime Performance Manager and IPv6

The following topics describe Prime Performance Manager IPv6 behavior and configuration practices:

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 Device 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 other protocol 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 9-35.

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
    ```

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.

By default, all Prime Performance Manager commands require Superuser privilege with the exception of commands requiring root user privilege listed in Table B-1. The root user can run any Prime Performance Manager command. If you use the ppm superuser command to set Prime Performance Manager to run under a user ID other than root, all commands other than ones requiring root user privilege, can be run under that user ID.

Table B-1 Root User and All User Commands

Commands Requiring Root User Privilege		Commands Available to all Users
• ppm authtype • ppm backup • ppm backupdir • ppm checksystem • ppm certtool • ppm datadir • ppm devcachedir • ppm dbbackupdir • ppm evilstop • ppm genkey • ppm jspport • ppm keytool • ppm logdir • ppm msglogdir (ppm logdir and ppm msglogdir perform the same action.) • ppm netflowport • ppm ramdisksize • ppm reboot • ppm reportdir • ppm repdir • ppm restore • ppm rpm • ppm restoreprops • ppm superuser	• ppm threshcachedir • ppm reportdir (same as ppm repair) • ppm shutdown • ppm setpath (when setting path for another user) • ppm ssl • ppm syncusers • ppm tac • ppm uaenable • ppm uadisable • ppm uninstall • ppm webport	• ppm help • ppm sechelp • ppm rephelp • ppm status • ppm version • ppm readme • ppm quickstart • ppm relnotes • ppm osinfo • ppm changes • ppm localhacommands • ppm msglog • ppm netlog • ppm rootvars • ppm rephelp • ppm backupstats • ppm setpath • ppm starbuild • ppm sslver • ppm javaver • ppm logger • ppm pmess • ppm statreps • ppm csvstats • ppm setpath (when setting path for user running CLI)

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

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, WSMA over SSHv2, AVI_HTTPS.
- [**-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* **-c** *read community* **| -u** *snmpv3 username* [**-a** *authentication protocol* **| -A** *authentication password*] [**-x** *privacy protocol* **| -X** *privacy password*] [**-v 1 |2c | 3**]

Command Description

Adds an SNMP configuration to Prime Performance Manager server.

- **-i** *ipaddress*—The IP address of the device (required)
- **-c** *read community*—The SNMP read community. Read community is required for SNMP v1 and 2c.
- **-u** *snmpv3 username*—The SNMP username. The username is required for SNMP v3.
- **-a** *authentication protocol*—The authentication protocol.
- **-A** *authentication password*—The authentication password.
- **-x** *privacy protocol*—The privacy protocol.
- **-X** *privacy password*—The privacy password.
- **-v** *version*—The SNMP version, 1, 2c, or 3. The default is 2c.
- **-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-28
- ppm modifysnmpcomm, page B-59
- ppm showsnmpcomm, page B-89

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 [-n *username* [1 | 3 | 5 | 11 | 12] [-f *filename*]

Command Description

If you enable Prime Performance Manager User-Based Access, adds the specified user(s) to the authentication list.

Options

- -n*username*—Adds the specified user with the default password, ppm124A@ and the specified authentication level:
  - **1**—Basic User
  - **3**—Network Operator
  - **5**—System Administrator
  - **11**—Custom Level 1
  - **12**—Custom Level 2
- -f *filename*—Adds a group of users with the default password, ppm124A@. Format: userID]:[acessLevel

Default password for users created using this command is ppm124A@. You can change thisin "/opt/CSCOppm-gw/properties/System.properties.

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 6-8).

Available in GUI

Yes

Related Topics

- Setting Up User Access and Security, page 6-1
- User Authentication, page 6-8

ppm alarmwarning

Syntax

/opt/CSCOppm-gw/bin/ppm alarmwarning {enable | disable}

Command Description

Allows you to define warning and informational threshold alarms.

Available in GUI

Yes

Related Topic

- Creating Thresholds, page 11-1

ppm allowgiantnames

Syntax

/opt/CSCOppm-gw/bin/ppm allowgiantnames {enable | disable | status}

Command Description

Allows custom names for nodes or devices to be up to 255 characters. By default, the limit is 100 characters.

- enable—Enables giant names and allows custom names for devices to be up to 255 characters.
- disable—Disables giant names and reduces the length for custom names to 100 characters.
- status—Displays the status of the giant names option, either enabled or disabled.

Available in GUI

No

ppm apdiff

Syntax

/opt/CSCOppm-gw/bin/ppm apdiff [*oldcsv*] [*newcsv*]

Command Description

Finds the differences between an older AP CSV file and a new AP CSV file. Both files must be in the Prime Performance Manager installation directory.

Available in GUI

No

ppm apgenxml

Syntax

/opt/CSCOppm-gw/bin/ppm apdiff

Command Description

Generates an AP XML file.

Available in GUI

No

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 6-15 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 Topics

- Setting Up User Access and Security, page 6-1
- User Authentication, page 6-8

ppm backup

Syntax

/opt/CSCOppm-gw/bin/ppm backup [gw | unit | both]

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 2:30 AM for the unit and 3:30 AM for the gateway. 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)* 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.*

If you installed Prime Performance Manager in a different directory, the backup files reside in that directory.

Command options allow you to choose whether to back up the gateway, unit, or both:

- gw—Backs up the gateway.
- unit—Backs up the unit.
- both—Backs up the gateway and unit.

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 18-2
- ppm restore, page B-84

ppm backupdata

Syntax

/opt/CSCOppm-gw/bin/ppm backupdata [**enable | disable | status**] **[gw | unit | both]**

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. Command options allow you to choose whether to back up the gateway, unit, or both:

- gw—Backs up the gateway.
- unit—Backs up the unit.
- both—Backs up the gateway and unit.

Available in GUI

Yes

ppm backupdays

Syntax

/opt/CSCOppm-gw/bin/ppm backupdays [*days*] **[gw | unit | both]**

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.

Command options allow you to choose whether to back up the gateway, unit, or both:

- gw—Backs up the gateway.
- unit—Backs up the unit.
- both—Backs up the gateway and unit.

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-16). 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-84.

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-16).

Available in GUI

Yes

Related Topics

- Backing Up Prime Performance Manager Data Files, page 18-2
- ppm restore, page B-84

ppm backupuncheckeddata

Syntax

/opt/CSCOppm-gw/bin/ppm backupuncheckeddata [**enable | disable | status**] **[gw | unit | both]**

Command Description

Enables or disables the inclusion of unverified data in the Prime Performance Manager database backup tar files. Prime Performance Manager daily backups maintain a snapshot directory of the database with data integrity under the backup directory. The snapshot directory is updated each day using incremental data backups. The directory is then included in the main backup tar file as long as the backupdata function (see ppm backupdata, page B-13) is enabled. (If the backupdata option is disabled the backupuncheckeddata option has no impact.)

In the event the snapshot directory of the database cannot be written to during backup, backupuncheckeddata controls whether the backup should include the main database files directly from their source directory. If backups occur while the server is running, inconsistent data could be included in the backup, which could lead to issues during a restore from this backup.

If you do not wish to include data from the main database files while running backups during this condition, disable this option. If the Prime Performance Manager backup directory never becomes full or experiences other access issues, enabling backupuncheckeddata will have no impact.

Command options:

- enable—Enables the backup of unchecked Prime Performance Manager data.
- disable—Disables the backup of unchecked Prime Performance Manager data.
- gw—Enables or disables the unchecked data backups for the gateway.
- unit—Enables or disables the unchecked data backups for the unit.
- both—Enables or disables the unchecked data backups for the gateway and unit.

Note The backupuncheckeddata option requires the backupdata option to be enabled. For information, see ppm backupdata, page B-13.

You must log in as the root user to use this command.

Available in GUI

No

ppm backupminfree

Syntax

/opt/CSCOppm-gw/bin/ppm backupminfree [**gw | unit | both**] *MB*

Command Description

Sets the minimum available space, in megabytes that must be available before a backup is started. Options include:

- gw—Sets the minumum space for the gateway.
- unit—Sets the minumum space for the unit.
- both—Sets the minumum space for the gateway and unit.

Available in GUI

Yes

ppm backupdir

Syntax

/opt/CSCOppm-gw/bin/ppm backupdir [*directory*] **[gw | unit | both]**

Command Description

Note You must stop Prime Performance Manager server before performing this command. You are prompted whether you want to continue.

Command options allow you to choose whether to back up the gateway, unit, or both:

- gw—Backs up the gateway.
- unit—Backs up the unit.
- both—Backs up the gateway and unit.

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 Topics

- Backing Up Prime Performance Manager Data Files, page 18-2
- ppm restore, page B-84

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 backuplogs

Syntax

/opt/CSCOppm-gw/bin/ ppm backuplogs [enable|disable|status] [gw | unit | both]

Command Description

Determines whether to include logs in backups or not.

Command options allow you to choose whether to back up the gateway, unit, or both:

- gw—Backs up the gateway.
- unit—Backs up the unit.
- both—Backs up the gateway and unit.

If this command is enabled, logs are included in backups. If this command is not enabled, then log files backup are not included. The status option tells whether this command is enabled or not and the gw/unit/both options indicate whether this applies only to gateway backups, unit backups, or both.

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

Yes

ppm backuprestorescript

Syntax

/opt/CSCOppm-gw/bin/ppm backuprestorescript [*path* | **clear**]

Command Description

This command calls a script before and after a backup or restore occurs. You must log in as the root user to use this command.

Available in GUI

Yes

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 Displaying the System Security Log, page 6-27).

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

Editing User Security Settings, page 6-21

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

Editing User Security Settings, page 6-21

ppm buildstarconfig

Syntax

/opt/CSCOppm-gw/bin/ppm buildstarconfig [{**schemafilename** | **default**} **ppm** | **no** | **zero**]

Command Description

Sets up bulk statistics reporting configurations for Cisco ASR 5000 and Cisco ASR 5500 devices.

- **schemafilename**—The schema file name containing the bulk statistics schema you want to use
- **default**—Generates a configuration for all counters and all schemas supported by Prime Performance Manager. The default file is:

```
/opt/CSCOppm-gw/install/ASR5K_BulkStats_StarOS_Schema_Counters.csv
```

- **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.

Available in GUI

No

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 bulkstatver

Syntax

/opt/CSCOppm-gw/bin/ppm bulkstatver

Command Description

Prints the StarOS BulkStat version.

Available in GUI

No

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-50) 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 Topics

- Displaying the SSL Key and Certificate, page 6-6
- Exporting 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 cleancache

Syntax

/opt/CSCOppm-gw/bin/ppm cleancache [gw |unit | both]

Command Description

- Remove device and TCA cache files:
- gw—Removes device and TCA files from the gateway.
- unit—Removes device and TCA files from the unit.
- both—Removes device and TCA files from the gateway and unit.

Available in GUI

No

ppm clientclocktolerance

Syntax

/opt/CSCOppm-gw/bin/ppm clientclocktolerance [*secs*]

Command Description

Sets the number of seconds timing between Prime Performance Manager and a client can be out of synchronization before an alarm is raised. The default is 900 seconds.

Available in GUI

No

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

Editing User Security Settings, page 6-21

ppm clocktolerance

Syntax

/opt/CSCOppm-gw/bin/ppm clocktolerance [**client** | [**device** | **server**] [*secs*]

Command Description

Sets the number of seconds timing between Prime Performance Manager and a client, device, or server can be out of synchronization before an alarm is raised. The default is 900 seconds.

Available in GUI

No

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 dependent 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 criticalalarm

Syntax

/opt/CSCOppm-gw/bin/ppm criticalalarm [*Critical Alarm*]

Command Description

Generates a critical Prime Performance Manager alarm. This alarm is generated on the Prime Performance Manager gateway and will also be forwarded northbound if configured.

Available in GUI

No

ppm crosslaunch

Syntax

/opt/CSCOppm-gw/bin/ppmcrosslaunch [**install** | [**hideLegend** | **hideNavigator** | **hideDateString** | **hideButtons** | **hideTitle**] **uninstall**]

Command Description

Installs (or uninstalls) the ability to cross launch Prime Performance Manager from Prime Network. Installation options allow you to hide Prime Performance Manager chart elements when reports are launched from Prime Network:

- hideLegend—Hides the chart legend. Users can normally turn legends on or off using the Toggle Legend tool. This option turns the legend off when launched from Prime Network.
- hideNavigator—Hides the bar that appears at the bottom of charts in full screen or leaf graph mode that lets you scroll to or select a specific area of the chart.
- hideDateString—Hides the report date string that appears at the bottom of charts.
- hideButtons—Hides the Zoom, Graph Style, and Export options that appear within an individual chart.
- hideTitle—Hides the report title and/or subtitle that normally appears inside a chart.

Available in GUI

Yes

ppm csvdropdir

Syntax

/opt/CSCOppm-unit/bin/ppmcsvdropdir [*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 Topics

- ppm addsnmpcomm, page B-9
- ppm modifysnmpcomm, page B-59
- ppm showsnmpcomm, page B-89

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*|*filename*]

Command Description

Deletes a user or a list of users. 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 the **ppm adduser** command. (See ppm adduser, page B-10.

You must log in as the root user to use this command.

Available in GUI

Yes

Related Topic

Manually Disabling Users and Passwords, page 6-22

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 deviceclocktolerance

Syntax

/opt/CSCOppm-gw/bin/ppm deviceclocktolerance [*secs*]

Command Description

Sets the number of seconds timing between Prime Performance Manager and a device can be out of synchronization before an alarm is raised. The default is 900 seconds.

Available in GUI

No

ppm disablepass

Syntax

/opt/CSCOppm-gw/bin/ppm disablepass [*username*|*filename*]

Command Description

Disable password for a user or a list of users**.** If you enable Prime Performance Manager User-Based Access, and set **ppm authtype** to **local**, it 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 Disabling Users and Passwords, page 6-22

ppm disablepwdage

Syntax

/opt/CSCOppm-gw/bin/ppm enablepwdage [*username*|*filename*]

Command Description

Disables password aging for the specified user or a list of users.

You must log in as the root user to use this command.

Available in GUI

Yes

Related Topic

ppm enablepwdage, page B-34

ppm disableuser

Syntax

/opt/CSCOppm-gw/bin/ppm disableuser [*username*|*filename*]

Command Description

Disable a user or a list of users. 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 Disabling Users and Passwords, page 6-22

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, page 5-11

ppm discovertype

Syntax

/opt/CSCOppm-gw/bin/ppm discovertype {*seed1*}. [*seed2*], ... [*seedN*] -p {*collect1*], [*collect2*], [*collectN*]

Normally you use the ppm discover {*seed1*} [*seed2*] [*seedN*] [-p [*collect1*... [*collectN*] command to discover a seed set using *collector1* > *collectorN* in a multi-collector context. This process has two steps:

- Configure the polling policy for the seed set so that Prime Performance Manager uses the specified collector to collect data from the devices.
- Discover the specified seed sets and begin regular polling.

However, in some scenarios the modified policy file does not synchronize to the unit in time. As a result, the first poll of the specified seed set fails because the unit does not have the updated polling policy. In this case you can use ppm discovertype to update the polling policy including unit synchronization. You can then run ppm discover to discover the specified seed set based on the latest polling policy.

ppm discoveryrange

Syntax

/opt/CSCOppm-gw/bin/ppm discoveryrange *[true|false]*

Command Description

You use this command to discover the devices IP address is within the network range.

If this command is true, then devices within address range that are not reachable are deleted from Prime Performance Manager. If this command is false, then the devices that are not reachable during discovery are retained in Prime Performance Manager in an unmanaged state.

You must log in as the root user to use this command.

Available in GUI

Yes

ppm diskcheck

Syntax

/opt/CSCOppm-gw/bin/ppm diskcheck

Command Description

Manually runs the disk space usage check.

You must log in as the root user to use this command.

Related Topic

ppm diskmonitor, page B-32

ppm diskmonitor

Syntax

/opt/CSCOppm-gw/bin/ppm diskmonitor [**enable** | **disable** | **status**] | **warning** {*MBs*} | **critical** {*MBs*} | **warnscript** {*path* | *clear*} | **critscript** {*path* | *clear*} [**gw** | **unit** | **both**]

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 use passes the threshold defined with the warning option, a disk space major 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 use 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.

Options:

- 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.
- gw—Applies the command actions to the gateway.
- unit—Applies the command actions to the unit.
- both—Applies the command action to both the gateway and unit.

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-32

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*|*filename*]

Command Description

Enables password aging for the specified user or a list of users.

You must log in as the root user to use this command.

Available in GUI

Yes

Related Topics

- ppm discover, page B-31
- Managing Users and User Security, page 6-15

ppm enableuser

Syntax

/opt/CSCOppm-gw/bin/ppm enableuser [*username*|*filename*]

Command Description

Enable a user or a list of users. 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

Enabling User Accounts and Passwords Using the CLI, page 6-24

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
	deleteEvents	**-l** or **-L** -u -n
	getAllEventsAsTraps	-t
	getAllOpenAlarmsAsTraps	-t -H -p -S -h
	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.

Parameter	Description (continued)
-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 extrarunpath

Syntax

/opt/CSCOppm-gw/bin/ppm extrarunpath [*path***]**

Command Description

Appends {*path*} to the run path for alarm scripts. This can be useful when running scripts when TCAs occur. To add multiple directories, separate each directory with a colon, for example:

path1:path2

Available in GUI

No

ppm fastinterval

Syntax

/opt/CSCOppm-gw/bin/ppm fastinterval

Command Description

Displays the interval between slow and fast SNMP polling threads.

Available in GUI

Yes

Related Topics

- ppm numfastthreads, page B-65
- ppm numslowthreads, page B-66

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 connectible. 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-87.
- 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 getbackuptimes

Syntax

/opt/CSCOppm-gw/bin/ppm getbackuptimes

Command Description

Displays the following Prime Performance Manager and collocated unit (if installed) backup information:

- Last Backup Start—The date and time the gateway backup was started.
- Last Backup Start—The date and time the gateway backup was completed.
- Next Backup Start—The date and time the next gateway backup will begin.

Available in GUI

Yes

ppm grouptool

Syntax

/opt/CSCOppm-gw/bin/ppm grouptool

Command Description

Displays the contents of the add group, delete group, update group and get group information probe details.

- **-a**—Specifies the type of operation to be performed.
- **-l**—Specifies a file name for the group.
- **-k**—Specifies the name for the group.
- **-H**—Specifies a hostname to connect to. If not specified, default value is obtained from the gateway System.properties file, SERVER_NAME property.
- **-p**—Specifies a port to connect to. If not specified, default value is obtained from the gateway System.properties file, WEB_PORT property.
- **-S**—Specifies whether to use SSL (https) for NBAPI access, default is no SSL.
- **-h**—Print help information.

You must log in as the root user to use this command.

ppm grouptool -a addGroup

-l <XML file>

[-H <hostname>]

[-p <port number>]

[-S <y|n>]

[-h <help>]

ppm grouptool -a updateGroup

-l <XML file>

-n <note>

[-H <hostname>]

[-p <port number>]

[-S <y|n>]

[-h <help>]

ppm grouptool -a deleteGroup

-k <groupName>

[-H <hostname>]

[-p <port number>]

[-S <y|n>]

[-h <help>]

ppm grouptool -a getGroupInfo

-k <groupName>

[-H <hostname>]

[-p <port number>]

[-S <y|n>]

[-h <help>]

Available in GUI

Yes

Example of Prime Performance Manager Group File

```
<ns:Group xmlns:ns="http://cisco.com/ppm">
      <name>Test-group</name>
    <enabled>false</enabled>
    <processingSectionList>
          <GroupProcessingSection>
              <name>default</name>
            <type>Network</type>
            <matchingAlgorithm>If(Contains(cmStatusName, "online"), true,
false)</matchingAlgorithm>
            <matchingObjectList/>
            <dataSourceList>
                  <dateSource>AGG_CMTS_CM_UP_STATE</dateSource>
            </dataSourceList>
        </GroupProcessingSection>
    </processingSectionList>
</ns:Group>
```

Example Probe.xml file for Command Line Interface

```
probe.xml
---------

<ns2:Probe xmlns:ns2="http://cisco.com/ppm">
               <PropertyList>
                  <Property name="Type">
                     <Value>HTTPProbe</Value>
                  </Property>
                  <Property name="Device">
```

```
   <Value>ppm-lnx-vm012.cisco.com</Value>
</Property>
<Property name="Name">
   <Value>HTTP-Probe-2</Value>
</Property>
<Property name="Description">
   <Value>HTTP Probe 1</Value>
</Property>
<Property name="Enabled">
   <Value>true</Value>
</Property>
<Property name="Interval">
   <Value>15</Value>
</Property>
<Property name="OpenTimeout">
   <Value>60</Value>
</Property>
<Property name="ResponseTimeout">
   <Value>60</Value>
</Property>
<Property name="IPAddress">
   <Value>google.com</Value>
</Property>
<Property name="Port">
   <Value>80</Value>
</Property>
<Property name="Username">
   <Value>username1</Value>
</Property>
<Property name="Password">
   <Value>password2</Value>
</Property>
<Property name="HttpHeaderFieldTable">
   <ValueList/>
</Property>
<Property name="HttpRequestMethod">
   <Value>GET</Value>
</Property>
<Property name="HttpStatusCodeTable">
   <ValueList>
      <Property name="HttpStatusCodeRow">
         <ValueList>
            <Property name="HttpStatusCode">
               <ValueList>
                  <Property name="HttpStatusCodeRangeBegin">
                     <Value>200</Value>
                  </Property>
                  <Property name="HttpStatusCodeRangeEnd">
                     <Value>200</Value>
                  </Property>
               </ValueList>
            </Property>
         </ValueList>
      </Property>
   </ValueList>
</Property>
<Property name="Protocol">
   <Value>HTTPS</Value>
</Property>
<Property name="Application">
   <Value>mail</Value>
</Property>
<Property name="UrlPath">
   <Value>HTTPS://google.com:80/mail</Value>
```

```
                    </Property>
                  </PropertyList>
</ns2:Probe>
```

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 hypervisor checklibrary

Syntax

/opt/CSCOppm-gw/bin/ppm hypervisor checklibrary

Command Description

Checks the Linux OS library to ensure it contains all RPMs required for Prime Performance Manager to successfully connect to hypervisors. The command will indicate whether the library is complete. If the library is incomplete, a list of needed RPMs is provided.

Available in GUI

No

ppm hypervisor connect

Syntax

/opt/CSCOppm-gw/bin/ppm hypervisor connect *[hypervisor URL]*

Command Description

Checks the connection between the Prime Performance Manager gateway and the hypervisor. Hypervisor URLs are entered in the following format:

- ESXi

  ```
  ./ppm hypervisor connect esx://nnn.nnn.nnn.nnn/?no_verify=1
  ```

- HyperV

  ```
  ./ppm hypervisor connect hyperv://nnn.nnn.nnn.nnn/?no_verify=1
  ```

- VPX

  ```
  ./ppm hypervisor connect vpx://nnn.nnn.nnn.nnn/?no_verify=1
  ```

- Xen

  ```
  ./ppm hypervisor connect
  xen://nnn.nnn.nnn.nnn/?no_verify=1\&pkipath=/opt/CSCOppm-gw/hypervisor/libvirt/etc/pki
  /CA
  ```

- QEMU

  ```
  ./ppm hypervisor connect
  qemu://nnn.nnn.nnn.nnn/system?no_verify=1\&pkipath=/opt/CSCOppm-gw/hypervisor/libvirt/
  etc/pki/CA
  ```

Available in GUI

No

ppm ifnameformat

Syntax

/opt/CSCOppm-gw/bin/ppm ifnameformat [desc | alias | both | ifindex]

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 are displayed.
- ifindex—Displays the interface by its Interface Index value, a unique identifying number associated with a physical and logical interfaces.

You can run this command on the gateway, and it will update all units.

Note After you change the interface name format, restart the gateway and all units. See ppm restart, page B-83.

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"
- Editing User Security Settings, page 6-21

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 6-8 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 javaver

Syntax

/opt/CSCOppm-gw/bin/ppm javaver

Command Description

Displays the version of Java that is used.

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.

Available in GUI

No

ppm jvmsize

Syntax

/opt/CSCOppm-gw/bin/ppm jvmsize {megs} {gw|unit} {list}

Command Description

Sets the gateway or unit Java Virtual Machine (JVM) size in MBs.

You must log in as a Prime Performance Manager Superuser to use this command.

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 6-15

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

Listing Currently Defined Users, page 6-27

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 lognum

Syntax

/opt/CSCOppm-gw/bin/ppm lognum [*num*]

Command Description

Sets the maximum number of logs to retain, after which, logs will be archived.

Available in GUI

No

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

Variable	Meaning	Example
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 majoralarm

Syntax

/opt/CSCOppm-gw/bin/ppm majoralarm[*Major Alarm*]

Command Description

Generates a major Prime Performance Manager alarm. This alarm is generated on the Prime Performance Manager gateway and will also be forwarded northbound if configured.

Available in GUI

No

ppm manageulsredundancy

Syntax

/opt/CSCOppm-gw/bin/ppm manageulsredundancy [**list** | **set** | **delete** | **partitioner**]

Command Description

Manages small cell upload server (ULS) redundancy.

Options:

- list—Lists all ULS redundancy groups.
- set [*redundancygroup device1 device2 device3*...]—Creates a ULS redundancy group. Requires the redundancy group name and the devices you want in the group.
- delete [*redundancygroup*]—Deletes the ULS redundancy group.
- partitioner—Manages the ULS partitions:
  - print—Prints the current file fetching partitions.
  - repartition—Repartitions the set of APs each active unit is responsible for.
  - delete—Deletes the current partitions.

    Caution: After you invoke the delete option, a new set of partitions are created and files are retrieved from the Max Back Time onward.

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-83.

ppm maxquerycachecolumns

Syntax

/opt/CSCOppm-gw/bin/ppm maxquerycachecolumns [*number*]

Command Description

Sets the maximum number of columns that will be kept in the query cache for a report. 50 columns is the default.

Available in GUI

No

ppm messagequeuetool

Syntax

/opt/CSCOppm-gw/bin/ppm messagequeuetool [**-a | -i | -b | -T | -v | -u | -w | -E | -o**]

Command Description

Sets the set up message brokers that listen for OpenStack tenant changes and update the Prime Performance Manager tenant data when they occur. The message brokers supplement the ongoing tenant data synchronization set up at 30-minute, one-hour, or six-hour intervals when you add the tenant entry to Prime Performance Manager. Message brokers have two requirements:

- OpenStack must use the RabbitMq message broker. Qpid and ZeroMQ are not supported.
- At least one OpenStack tenant must be added to Prime Performance Manager.

Options:

- -a—The primary message broker action:
  - addOpenstackMessageQ—Adds a new message broker.
  - updateOpenstackMessageQ—Update an existing message broker.
  - deleteOpenstackMessageQ—Deletes an existing messasge broker.
  - listOpenstackMessageQ—Displays a list of created messasge broker entries. When an entry status is active, that means Prime Performance Manager is listening to the OpenStack tenant it is set up to monitor.
  - -i uniqueName -b msgBroker -T port -v vHost -u user -w password -E enabled -o openstack to add an configuration entry, where
- -i *Name*—is the unique name for the message broker entry.
- -b—*MessageBrokerIP*—The IP address of the RabbitMq message broker
- -T *ListenerPort*—The message broker port used to listen for updates.
- -v *VirtualHost*—The virtual host configured on the message broker. The default is '/'.
- -u *username*—The user name used to connect to the message broker.
- -w *password*—The username password.
- -E—Indicates whether the message broker is enabled, true (default) or false.

- -o *openstack, ip*—The OpenStack IP address containing the tenant that the message broker will monitor. The OpenStack IP must be added to Prime Performance Manager through the OpenStack tenant integration process.

Available in GUI

Yes

Related Topics

- Adding Tenants Through OpenStack Integration, page 16-4
- Adding OpenStack Tenant Message Brokers, page 16-5

ppm mibcap

Syntax

/opt/CSCOppm-gw/bin/ppm mibcap [*device_name*]

Command Description

Displays device MIB capabilities.

Available in GUI

No

ppm mibver

Syntax

/opt/CSCOppm-gw/bin/ppm mibver

Command Description

Displays all SNMP MIB versions.

Available in GUI

No

ppm minoralarm

Syntax

/opt/CSCOppm-gw/bin/ppm minoralarm[*Minor Alarm*]

Command Description

Generates a minor Prime Performance Manager alarm. This alarm is generated on the Prime Performance Manager gateway and will also be forwarded northbound if configured.

Available in GUI

No

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 addsnmpcomm -i *ipaddress* **-c** *read community* **| -u** *snmpv3 username* [**-a** *authentication protocol* **| -A** *authentication password*] [**-p** *privacy protocol* **| -P** *privacy password*] [**-v 1 |2c | 3**]

Command Description

Modifies an SNMP configuration on a Prime Performance Manager server.

- **-i** *ipaddress*—The IP address of the device (required)
- **-c** *read community*—The SNMP read community. Read community is required for SNMP v1 and 2c.

- **-u** *snmpv3 username*—The SNMP username. The username is required for SNMP v3.
- **-a** *authentication protocol*—The authentication protocol.
- **-A** *authentication password*—The authentication password.
- **-p** *privacy protocol*—The privacy protocol.
- **-P** *privacy password*—The privacy password.
- **-v** *version*—The SNMP version, 1, 2c, or 3. The default is 2c.
- **-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 Topics

- ppm addsnmpcomm, page B-9
- ppm deletesnmpcomm, page B-28
- ppm showsnmpcomm, page B-89

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 Topics

ppm premotd, page B-71

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 netflow

Syntax

/opt/CSCOppm-unit/bin/ppm netflow [**enable** | **disable** | **status**]

Command Description

Enables, disables or checks the status of the NetFlow collection on the unit server. If enabled, the NetFlow collector listens for and processes NetFlow packets on the unit. The NetFlow collector must be enabled to generate NetFlow reports. The command changes the NETFLOW_ACTIVE property in /opt/CSCOppm-unit/properties/NetFlow.properties. The default value is enabled. However, if you are not generating NetFlow reports, disabling NetFlow is recommended to free up memory.

The command is available only on the unit. Enabling or disabling NetFlow requires a unit restart. The restart is performed by the ppm restart command (see ppm restart, page B-83).

Available in GUI

No

ppm netflowport

Syntax

/opt/CSCOppm-unit/bin/ppm netflowport [*port*]

Command Description

Changes the NetFlow collector port where the collector listens for NetFlow packets from devices. The command changes the UDP_PORT property in /opt/CSCOppm-unit/properties/NetFlow.properties. The default value is 9991 port. The command is available only on the unit. Changing the NetFlow port requires a unit restart. The restart is performed by the command.

Available in GUI

No

ppm netflowservfile

Syntax

/opt/CSCOppm-unit/bin/ppm netflowservfile [*file*]

Command Description

Changes the NetFlow services files used by GetServByPort macro. The macro looks up service names for NetFlow ports and protocol. By default, the file is /opt/CSCOppm-gw/etc/services and /opt/CSCOppm-unit/etc/services. (The file is available on both gateway and unit.) You can add or modify the services file entries on the gateway and the changes are automatically sent to all the units.

If you have your own lookup file that you want to use instead of the default services file, use this command to specify the alternate file. The new file must be in the same syntax as the default services file.

This command changes the NETFLOW_PORTSERVICES_FILE property in System.properties. You must execute the command on both the gateway and unit servers for the changes to take effect.

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

Enabling User Accounts and Passwords Using the CLI, page 6-24

ppm nontoerrcount

Syntax

/opt/CSCOppm-gw/bin/ppm nontoerrcount [*number*]

Command Description

Sets the number of non-timeout errors allowed in a report sequence. This command and the ppm toerrcount command control the number of polling errors to get from a device in a polling sequence before giving up on that entire polling sequence.The default is 1.

Available in GUI

No

Related Topic

- ppmtoerrcount, page B-114

ppm numfastthreads

Syntax

/opt/CSCOppm-gw/bin/ppm numfastthreads

Command Description

Displays the number of fast SNMP polling threads.

Available in GUI

Yes

Related Topics

- ppm fastinterval, page B-39
- ppm numslowthreads, page B-66

ppm numslowthreads

Syntax

/opt/CSCOppm-gw/bin/ppm numslowthreads

Command Description

Displays the number of slow SNMP polling threads.

Available in GUI

Yes

Related Topics

- ppm fastinterval, page B-39
- ppm numfastthreads, page B-65

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

Device Report Capability Polling, page 7-32

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-62.

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

Editing User Security Settings, page 6-21

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 pingpolldelay

Syntax

/opt/CSCOppm-gw/bin/ppm pingpolldelay [*minutes*]

Command Description

You use this command to set the polling delay, in minutes.

You must log in as the root user to use this command.

Available in GUI

No

ppm pnscintegration

Syntax

/opt/CSCOppm-gw/bin/ppm pncsintegration [**remove**]

Command Description

Integrates Prime Performance Manager with Cisco Prime Network Services Controller. Running ppm pnscintegration displays the following prompts:

- PNSC Host—The Prime Network Service Controller host name.
- PNSC Admin Username—The Prime Network Service Controller username.
- PNSC Admin Password—The Prime Network Service Controller user password.

- PPM Admin Username (New)—If user security is not enabled on Prime Performance Manager, the new administrator user that will be used to log into Prime Performance Manager from Prime Network Services Controller. (If user security is enabled, this prompt is not displayed._
- PPM Admin Password (New) The new administrator user password.

Command options:

- Remove—Removes the integration.

You must log in as the root user to use this command.

Available in GUI

Yes

Related Topics

- Prime Network Services Controller Integration Overview, page 4-9
- Integrating Prime Performance Manager With Prime Network Services Controller, page 4-10

ppm policytool

Syntax

/opt/CSCOppm-gw/bin/ppm policytool [-a actionName] [parameters]

Command Description

Invokes report policy API operations.

Actions and parameters:

- assignReportPolicies
  - -A <deviceName>,<policyName>
  - -H <hostname>
  - -p <port number>
  - -S <y|n>
  - -h <help>
- deleteReportPolicies
  - -n <policyName>
  - -H <hostname>
  - -p <port number>
  - -S <y|n>
  - -h <help>
- getReportPolicies
  - -w <deviceName>
  - -P <policyName>
  - -R <categoryName>
  - -r <reportName>

  - -o <outputType>
  - -H <hostname>
  - -p <port number>
  - -S <y|n>
  - -h <help>
- updateReportPolicies
  - -u <policyFile>
  - -H <hostname>]
  - -p <port number>
  - -S <y|n>
  - -h <help>

  The updateReportPolicies file should contain an xml ReportPolicyList produced by the getReportPolicies action. The ordering of categories, reports, flags, and numbers is not significant. The command will always generate output in the same order but can handle any input order as long as the types are in the correct order.

  For each update flag set, you can specify that all intervals are enabled or disabled, or you can specify individual interval settings. You cannot do both. Trying to do both will cause a validation failure.

  The updateReportPolicies action does not change unspecified settings; you do not need to specify any settings that you do not want to change.

Parameters:

- -a—Specifies the operation type to perform.
- -A—Specifies a comma-separated assignment <deviceName>,<policyName>. Repeat for multiple assignments.
- -n—Specifies a policy name to delete. Repeat for multiple deletions.
- -u—Specifies a file name for the policies with the same format as the getReportPolicies xml output.
- -w—Specifies the device name (blank for all).
- -P—Specifies the policy name (blank for all, 'Default' for default).
- -R—Specifies the category name (blank for all, 'master' for global).
- -r—Specifies the report name (blank for all)
- -o—Specifies the output type (xml [default] or json)
- -H—Specifies a hostname to connect to. If not specified, the default value is obtained from the gateway System.properties file, SERVER_NAME property.
- -p—Specifies a port to connect to. If not specified, the default value is obtained from the gateway System.properties file, WEB_PORT property.
- -S—Specifies whether to use SSL (https) for NBAPI access, default is no SSL.
- -h—Print help information.

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 pollstarschemas

Syntax

/opt/CSCOppm-gw/bin/ppm pollstarschemas [*schemaName*] [*schemaName2*][*schemaNameN*]...

Command Description

Poll for all or selected StarOS schemas for the discovered device.

Available in GUI

No

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.

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-60

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, "Importing Devices From Other Cisco Prime Applications."

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.

  You must log in as the root user to use this command option.
- **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.

  You must log in as the root user to use this command option.
- **restore** {*filename*}—Restores gateway system files with specified backup file.

  You must log in as the root user to use this command option.

You must log in as the root user to use this command.

Available in GUI

No

Related Topic

Managing Geographical High Availability, page 14-7

ppm primenetworkintegration

Syntax

/opt/CSCOppm-gw/bin/ppm primenetworkintegration [remove]

Command Description

Use this command to integrate Prime Performance Manager with Cisco Prime Network. After you enter the command, you will be prompted for the following information:

- Enter Prime Network Host Name or IP Address—Enter the Prime Network hostname or IP address.
- Enter the Prime Network port—Enter the Prime Network port.
- Secured?—Enter **y** if the port is secured; **n** if it is not.
- Enter Prime Network User Name—Enter the Prime Network username.
- Enter Prime Network User Password [*****]—Enter the Prime Network user password; for example, Test456!
- Enable Strict Synchronization?—Enter **y** if the port is secured if you want to enable strict synchronization; **n** if you do not. If strict synchronization is enabled, Prime Performance Manager can only generate reports from devices imported from Prime Network

You must log in as the root user to use this command. For additional information, see Chapter 4, “Importing Devices From Other Cisco Prime Applications.”

Available in GUI

Yes

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 probetool

Syntax
/opt/CSCOppm-gw/bin/ppm probetool -a {addProbe | updateProbe | deleteProbe | getProbeInfo}

Command Description
This command adds and manages probes in Prime Performance Manager.

Options
- addProbe—Adds a probe to Prime Performance Manager. Options:
  - -u <XML file>
  - [-H <hostname>]
  - [-p <port number>]
  - [-S <y|n>]
  - [-h <help>]

- updateProbe—Updates a probe. Options:
  - -u <XML file>
  - [-H <hostname>]
  - [-p <port number>]
  - [-S <y|n>]
  - [-h <help>]

- deleteProbe—Deletes a probe. Options:
  - -w <deviceName>
  - -v <probeName>
  - [-H <hostname>]
  - [-p <port number>]
  - [-S <y|n>]
  - [-h <help>]

- getProbeInfo—Gets probe information. Options:
  - -w <deviceName>
  - -v <probeName>
  - [-H <hostname>]
  - [-p <port number>]

– [-S <y|n>]

– [-h <help>]

Parameters:

- -a—Specifies the type of operation to be performed.
- -u—Specifies a file name for the probe.
- -v—Specifies the name for the probe.
- -w—Specifies the name for the device
- -H—Specifies a hostname to connect to. If not specified, default value is obtained from the gateway System.properties file, SERVER_NAME property.
- -p—Specifies a port to connect to. If not specified, default value is obtained from the gateway System.properties file, WEB_PORT property.
- -S—Specifies whether to use SSL (https) for NBAPI access, default is no SSL.
- -h—Print help information.

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. The command also starts the report aging task so any report data that has reached the aging time for any report and time interval is removed.

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 Topics

- ppm pwdchangerestrict, page B-77
- ppm pwdchangelimit, page B-77
- Editing User Security Settings, page 6-21

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 Topics

- ppm pwdchangerestrict, page B-77
- ppm pwdchangeinterval, page B-77
- Editing User Security Settings, page 6-21

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 Topics

- ppm pwdchangeinterval, page B-77
- ppm pwdchangelimit, page B-77
- Editing User Security Settings, page 6-21

ppm ramdisksize

Syntax

/opt/CSCOppm-gw/bin/ppm ramdisksize {[*MB*] **gw** | **unit**}

Command Description

Sets the gateway or unit RAM disk size. You can run the command in two ways. You can enter the command with the specified MB value, or you can enter the command and enter responses to command prompts.

Options:

- ppm ramdisksize—Displays the current value and prompts you to enter a new value for both the gateway and collocated unit (if present). If you change the RAM value, a message is shown to restart the gateway and unit.
- ppm ramdisksize *nnn*—Changes the RAM disk size immediately for both the gateway and collocated unit (if present) for the new *nnn* RAM value, then shows the restart gateway and restart unit messages.
- ppm ramdisksize *nnn* gw—Changes the gateway RAM disk size immediately to the *nnn value* and displays the restart gateway message.
- ppm ramdisksize *nnn* unit—Changes the unit RAM disk size immediately to the *nnn value* and displays the restart unit message.

Note Before running this command, check for the available memory.

Note You must restart the gateway or unit after you change its RAM disk size.

Available in GUI

No.

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

Managing Unit Redundancy Groups, page 13-8

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 current or master snmpinfo.dat file.

Available in GUI

Yes

ppm rename

Syntax

/opt/CSCOppm-gw/bin/ppm rename *dnsname customname*

Command Description

Renames a device DNS name to a custom name:

- dnsname—The DNS name you want to change.
- customname—The new custom name.

Available in GUI

No

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 reportdir

Syntax

/opt/CSCOppm-gw/bin/ppm reportdir

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

Syntax

/opt/CSCOppm-gw/bin/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 resolvehostnames

Syntax

/opt/CSCOppm-gw/bin/ppm resolvehostnames [*object*] [**arg {***argument***}]**

Command Description

Returns the host name in a string format. The hostname is resolved using the naming resolution defined in the optional arg parameter. If the arg parameter is not provided, the macro uses the naming resolution defined in RESOLVE_HOST_NAMES in the Reports.properties file. If RESOLVE_HOST_NAMES is not found in Reports.properties, the macro uses DNS to resolve the IP to a hostname. Regardless of the naming resolution strategy, if the command cannot resolve the IP address, it returns the IP address as the hostname.

- object—Is an IP address.
- arg—An optional parameter that defines the naming resolution, either DNS name or Prime Performance Manager device name:
  - dns—Resolves the IP address using the DNS. If the IP is not resolved to a name, it returns the IP address.
  - ppm—Resolves the IP address using the Prime Performance Manager device name based on the definition specified in the ppm statreps nametype command.
  - ppm,dns—Resolves the IP address using the Prime Performance Manager device name. If the device cannot be found for that IP address, it resolves the IP using the DNS.
  - dns,ppm—Resolves the IP address using the DNS. If the IP cannot be resolved to a name because the IP is not registered in the DNS, it uses the Prime Performance Manager device name.

You must log in as the root user to use this command.

Available in GUI

No

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 Topics

- Backing Up Prime Performance Manager Data Files, page 18-2
- ppm backupdata, page B-13
- ppm backupdir, page B-16

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 rpm

Syntax

/opt/CSCOppm-gw/bin/ppm rpm

Command Description

Displays Prime Performance Manager RPMs instlalled.

You must log in as the root user to use this command.

Available in GUI

No

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

Displaying the System Security Log, page 6-27

ppm serverclocktolerance

Syntax

/opt/CSCOppm-gw/bin/ppm serverclocktolerance [*secs*]

Command Description

Sets the number of seconds timing between Prime Performance Manager and a server can be out of synchronization before an alarm is raised. The default is 900 seconds.

Available in GUI

No

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.

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 setservicerole

Syntax

/opt/CSCOppm-gw/bin/ppm setservicerole [primary | secondary]

Command Description

In an High Availability (HA) configuration, sets the primary and secondary servers.

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 Topics

- ppm addsnmpcomm, page B-9
- ppm deletesnmpcomm, page B-28
- ppm modifysnmpcomm, page B-59

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 shutdown

Syntax

/opt/CSCOppm-gw/bin/ppm shutdown

Command Description

This command will completely shutdown the hardware system.

You must log in as the root user to use this command.

Available in GUI

No

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 smallcellver

Syntax

/opt/CSCOppm-gw/bin/ppm smallcellver

Command Description

Prints versions for small cell counter compliance.

Available in GUI

No

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*] [**-u** *snmpv3_username*] [**-a** *authentication protocol* | **-A** *authentication password*] [**-p** *privacy protocol* | **-P** *privacy password*] [**--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**] [**--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**, **2c**, or **3**. The default version is **2c**.
- **-c** *community_string*—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-u** *snmpv3_username*—The SNMP username. The username is required for SNMP v3.
- **-a** *authentication_protocol*—The authentication protocol.
- **-A** *authentication_password*—The authentication password.
- **-p** *privacy_protocol*—The privacy protocol.
- **-P** *privacy_password*—The privacy password.
- **-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.
- **--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*] [**-u** *snmpv3_username*] [**-a** *authentication protocol* | **-A** *authentication password*] [**-p** *privacy protocol* | **-P** *privacy password*] [**--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**] [**--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**, **2c**, or **3**. The default version is **2c**.
- **-c** *community_string*—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-u** *snmpv3_username*—The SNMP username. The username is required for SNMP v3.
- **-a** *authentication_protocol*—The authentication protocol.
- **-A** *authentication_password*—The authentication password.
- **-p** *privacy_protocol*—The privacy protocol.
- **-P** *privacy_password*—The privacy password.
- **-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.
- **--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, *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 by using Prime Performance Manager client.

You must log in as the root user to use this command.

Available in GUI

No

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*] [**-u** *snmpv3_username*] [**-a** *authentication protocol* **| -A** *authentication password*] [**-p** *privacy protocol* **| -P** *privacy password*] [**--tabular**|**--no-tabular**] [**--getbulk**|**--no-getbulk**] [**--header**|**--no-header**] [**--raw-octets**|**--no-raw-octets**] [**--str-octets**|**--no-str-octets**] [**--raw-timeticks**|**--no-raw-timeticks**] [--**date-timeticks**|**--no-date-timeticks**] [--**date-format date_format**] [**--resolve-integer**|**--no-resolve-integer**] [**--resolve-bits**|**--no-resolve-bits**] [**--get-sysuptime**|**--no-get-sysuptime**] [**--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**, **2c**, or **3**. The default version is **2c**.
- **-c** *community_string*—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-u** *snmpv3_username*—The SNMP username. The username is required for SNMP v3.
- **-a** *authentication_protocol*—The authentication protocol.
- **-A** *authentication_password*—The authentication password.
- **-p** *privacy_protocol*—The privacy protocol.
- **-P** *privacy_password*—The privacy password.
- **-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.
- -date-timeticks|-no-date-timeticks - Specifies format timetick data in date format. Use:
  - -date-timeticks to format timetick data in date format, such as 2015-09-16 00:03:45
  - -no-date-timeticks to use default timeticks format, such as 6 Hours 26 Mins 12 Secs. This is the default setting.

    Note: -raw-timeticks overrides -date-timeticks.
- -date-format date_format - Specifies date format to use when -date-timeticks is specified. Use:
  - -date-format "yyyy-MM-dd HH:mm:ss" to specify format to use. The example in quotes will render "2015-09-16 00:03:45" format which is the default.

    Note: Any Java SimpleDateFormat format strings are acceptable for the double quoted format.
- **--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 Topic

Managing Users and User Security, page 6-15

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 6-15

ppm sslver

Syntax

/opt/CSCOppm-gw/bin/ppm sslver

Command Description

Displays the version of openSSL that is used.

Available in GUI

No

ppm starbuild

Syntax

/opt/CSCOppm-gw/bin/ppm starbuild [{**schemafilename** | **default**} **ppm** | **no** | **zero**]

Command Description

Sets up bulk statistics reporting configurations for Cisco ASR 5000 and Cisco ASR 5500 devices.

- **schemafilename**—The schema file name containing the bulk statistics schema you want to use
- **default**—Generates a configuration for all counters and all schemas supported by Prime Performance Manager. The default file is:

  `/opt/CSCOppm-gw/install/ASR5K_BulkStats_StarOS_Schema_Counters.csv`

- **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.

A sample command sequence using the default option is shown below:

```
ppm17-demo> ppm starbuild default
Enter IP Address of PPM Unit To  Send Files To: 1.2.3.4
Enter File Directory On PPM Unit To Drop Files To: /opt/csvdrop
Enter Output Filename To Write StarOS Config To: staros-config
StarOS Config File Written To: staros-config
```

You must log in as the root user to use this command.

Related Topic

Setting Up StarOS Bulk Statistics Reports, page 8-21

ppm stardiffs

Syntax

/opt/CSCOppm-gw/bin/ppm stardiffs [*ipaddress*]

Command Description

Finds differences between the StarOS install CSV and the polled CSV. Polls StarOS version if IP is provided.

Available in GUI

No

ppm stargenall

Syntax

/opt/CSCOppm-gw/bin/ppm stargenall

Command Description

Polls, diffs, and generates the StarOS schema file and regenerates all counter pollers with new counter information.

Available in GUI

No

ppm stargenschema

Syntax

/opt/CSCOppm-gw/bin/ppm stargenschema <ipaddress/hostname> [all]

Command Description

This command updates bulkstatsschema.csv schema with new bulkstats variable information in a StarOS release. It runs the command, show bulkstats variables, on the device entered as the argument, compares the device output with bulkstats variables information in /opt/CSCOppm-gw/install/ASR5K_BulkStats_StarOS_Schema_Counters.csv, and identifies the differences, for example, new schemas, new bulkstats variables, and other changes. The differences are updated in the /opt/CSCOppm-gw/install/ASR5K_BulkStats_StarOS_Schema_Counters.csv, and a bulkstatsschema.csv file is generated with the new bulkstats variables.

- **ipaddress/hostname**—The IP address or hostname of the Cisco ASR 5000, Cisco ASR 5500, or Cisco Quantum Virtualized Packet Core (QvPC) device in Prime Performance Manager. The StarOS release must be loaded on the device. Also, the device must have an Active status and valid Telnet/SSH credentials so show commands can run on it.
- **[all]**—(optional) Identifies the data type gauge/counter, obsolete counter, and removed bulkstats variable differences found in the StarOS release and updates the /opt/CSCOppm-gw/install/ASR5K_BulkStats_StarOS_Schema_Counters.csv. Use this option only if required because the option could change the way the Prime Performance Manager reads the StarOS bulkstats files.

As an intermediate step the command generates the Prime Performance Manager StarOS config file with the new bulkstats variables, which you can use to configure the new schemas or bulkstats variables on the device.

After the command finishes, you can copy the generated bulkstatsschema.csv schema file to /opt/CSCOppm-gw/etc/. This updates the Prime Performance Manager in-memory schema counters list with the new counter information from /opt/CSCOppm-gw/etc/bulkstatsschema.csv. Make a copy of the file before loading a new version.

Note This command has potential risks for StarOS report processing. Verify the device you provide has a valid StarOS release image as the contents of bulkstatsschema.csv. If not, the /opt/CSCOppm-gw/install/ASR5K_BulkStats_StarOS_Schema_Counters.csv could receive invalid information and jeopardize its ability to parse StarOS bulkstats files correctly.

The command supported only on the gateway.

Available in GUI

No

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 starexp

Syntax

/opt/CSCOppm-unit/bin/ppm starexp [enable | disable | status]

Command Description

Enables, disables or checks the status of the StarOS Direct Conversion Export on the unit server. If enabled, the StarOS input Bulk Statistics CSV files are converted to 3GPP XML files or CSV files with deltas calculations. The command changes the EXPORT_ENABLED property in /opt/CSCOppm-unit/properties/BulkStats.properties. The default value is disabled.

You do not need to restart Prime Performance Manager server. The command is only supported on units.

Available in GUI

No

ppm starexpdropdir

Syntax

/opt/CSCOppm-unit/bin/ppm starexpdropdir [dir]

Command Description

Sets the StarOS export drop directory for collecting the converted bulk statistics files and updates the EXPORT_DROP_DIR property in /opt/CSCOppm-unit/properties/BulkStats.properties. You do not need to restart Prime Performance Manager server. The command is only supported on units.

Available in GUI

No

Related Topics

- Converting StarOS Bulk Statistics CSV Input Files to 3GPP XML Exports, page 8-31

ppm starexprules

Syntax

/opt/CSCOppm-unit/bin/ppm starexprules {3gppxml|3gppxmldeltas|csvdeltas}

Command Description

Sets the StarOS direct conversion export rules for converting the input CSV Bulk Statistics files. Valid options are 3GPP XML files with or without delta calculations or CSV files with Delta calculations. It updates the EXPORT_RULE property in /opt/CSCOppm-unit/properties/BulkStats.properties. Default option is 3GPP XML with delta calculations. You do not need to restart Prime Performance Manager server. The command is only supported on units.

Available in GUI

No

Related Topics

- Converting StarOS Bulk Statistics CSV Input Files to 3GPP XML Exports, page 8-31

ppm starexpxmlformat

Syntax

/opt/CSCOppm-unit/bin/ppm starexpxmlformat {allinone|oneperfile}

Command Description

Sets the StarOS direct conversion export formats for converting the input CSV Bulk Statistics files. This option is specific for 3GPP XML rule and controls if all StarOS Bulk Statistics schema is saved in the same XML file or if a new XML file is created for each schema. It updates the EXPORT_3GPP_XML_FORMAT property in /opt/CSCOppm-unit/properties/BulkStats.properties. Default option is All Schemas in one XML file. You do not need to restart Prime Performance Manager server. The command is only supported on units.

Available in GUI

No

Related Topics

- Converting StarOS Bulk Statistics CSV Input Files to 3GPP XML Exports, page 8-31

ppm statreps bulkstatsexpage

Syntax

/opt/CSCOppm-gw/bin/ppm statreps bulkstatsexpage [days]

Command Description

Specifies the number of days StarOS direct conversion export files are retained in Prime Performance Manager server. 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

Related Topics

- Converting StarOS Bulk Statistics CSV Input Files to 3GPP XML Exports, page 8-31

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* | *all*] [*enable* | *disable*] [*interval*], [**setstatus** [*categoryy* | *all*] [*enable* | *disable*] [*node* | *interval*]], [**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*]], [**csvdevtypes** [*enable* | *disable*]], [**expformat** [*xml*]], [**nametype**[*dnsname*] [*customname* | *sysname*]], [**csvtype** [*allnodes* | *pernodeuniq*]], [**zipcsvdelay** [*mins*]] [**zipcsvfiles** [*internal* | *script*]] [**zipcsvnotifscript** [*path* | *disable*]] **[*show* | *hide* [*xmlfilename*]]**

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* | *all*] [*enable* | *disable*] [*interval*]—Enable or disable network report settings, where interval = *1min, 5min, 15min, hourly, daily, weekly, monthly, db, csv.*

setstatus [[*category* | *all*] [*enable* | *disable*] [*node* | *interval*]]—Enable or disable device report settings, where interval = *1min, 5min, 15min, hourly, daily, weekly, monthly, db, csv.*

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).

csvdevtypes [*enable* | *disable*]—If enabled, the device type is included as the third column in all CSV exported files.

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.

zipcsvfiles [*internal* | *script]*—Zips CSV files using the Prime Performance Manager internal process or a script.

zipcsvnotifscript [*path* | *disable*]—Allows you to call another script after the CSV file is zipped, for example, for auditing.

show | hide [*xml file name*]—Enables the RMS 4G AP All Counters (rms4GApAllCounters.xml) or RMS All Counters report (rmsApPerfAllCounters.xml) small cell reports. The reports store over 450 columns for 3G and over 1500 columns for 4G in one table. They are purposefully disabled because their size and system resource requirements make display in the Prime Performance Manager GUI impractical. However, these commands, which are intended for lab and testing environments, allow you to enable the reports so you can export the data from these reports to CSV files.

Available in GUI

- nodiskcheck, diskcheck, and timemode options: Yes
- All other options: No

Related Topic

Customizing General Report Settings, page 7-25

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 Send to E-mail Addresses, page 10-17

ppm superuser

Syntax

/opt/CSCOppm-gw/bin/ppm superuser [*username*]

Command Description

Displays all the commands that superuser can perform on the gateway and units files. The command also changes the Linux user account used to perform Superuser functions which by default are required to perform the root user account. This user account must exist in the local /etc/passwd file. It is not possible to assign these functions to a user defined in a remote authentication service such as NIS. After the Superuser functions are assigned to another user account this user account can perform all functions such as starting and stopping the server, viewing and changing server configurations, and managing security features. The unit is stopped to perform this operation.

You must log in as the root user to execute this command.

Available in GUI

No

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 1

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 10-18.

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 thresholdtool

Syntax

/opt/CSCOppm-gw/bin/ppm thresholdtool {**-a** actionName} {parameters}

Command Description

Invokes Prime Performance Manager threshold API operations. The action names (and any corresponding required parameters) can be specified with the -a option described in Table B-2.

Table B-2 ppm thresholdtool Operations

Option	Action Name	Available Parameters
-a	addThreshold	-n <userThresholdName> -r <reportKey> -c <columnName> [-s <scope>] [-i <interval>] [-b <baselineEnabled>] [-d <day>] [-e <enabled>] [-g <msgText>] [-h <help>] [-f <mailFrom>] [-m <mailTo>] [-j <mailSubject>] [-p <port number>] [-t <time>] [-B <baselineParameters>] [-C <critical>] [-M <major>] [-N <minor>] [-W <warning>] [-I <informational>] [-A <alarmNature>] [-D <description>] [-E <continuousAlarmEnabled>] [-H <hostname>] [-L <alarmScript>] [-P <probableCause>] [-R <rising>] [-S <y|n>] [-T <alarmType>] [-x <tenant_list>]
	addThresholdInfoList	-u <thresholdFileName> [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]

Table B-2 ppm thresholdtool Operations (continued)

Option	Action Name	Available Parameters
	editThreshold	-n <userThresholdName> -s <scope> -i <interval> [-b <baselineEnabled>] [-d <day>] [-e <enabled>] [-g <msgText>] [-h <help>] [-f <mailFrom>] [-m <mailTo>] [-j <mailSubject>] [-p <port number>] [-t <time>] [-B <baselineParameters>] [-C <critical>] [-M <major>] [-N <minor>] [-W <warning>] [-U <updatedScope>] [-I <informational>] [-A <alarmNature>] [-D <description>] [-E <continuousAlarmEnabled>] [-H <hostname>] [-L <alarmScript>] [-P <probableCause>] [-R <rising>] [-S <y|n>] [-T <alarmType>] [-x <tenant_list>]
	editThresholdInfoList	-u <thresholdFileName> [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]
	enableThreshold	-n <userThresholdName> -i <interval> -s <scope> [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]
	disableThreshold	-n <userThresholdName> -i <interval> -s <scope> [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]
	rearmThreshold	-n <userThresholdName> -i <interval> -s <scope> [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]

Table B-2 ppm thresholdtool Operations (continued)

Option	Action Name	Available Parameters
	deleteThreshold	-n <userThresholdNme> -i <interval> -s <scope> [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]
	getThresholdInfo	-n <userThresholdName> -i <interval> -s <scope> [-o <outputType>] [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]
	getAllThresholdInfo	[-o <outputType>] [-H <hostname>] [-p <port number>] [-S <y|n>] [-h <help>]
	getFilteredThresholdInfo	[-b <baselineEnabled>] [-n <userThresholdName>] [-r <reportKey>] [-c <columnName>] [-s <scope>] [-i <interval>] [-e <enabled>] [-g <msgText>] [-h <help>] [-f <mailFrom>] [-m <mailTo>] [-j <mailSubject>] [-p <port number>] [-A <alarmNature>] [-B <baselineParameters>] [-D <description>] [-E <continuousAlarmEnabled>] [-H <hostname>] [-L <alarmScript>] [-P <probableCause>] [-R <rising>] [-S <y|n>] [-T <alarmType>] [-o <outputType>]

Table B-3 lists the parameters that can be used.

Table B-3 ppm thresholdtool Parameters

Parameter	Description
-a	The action to perform.
-b	Enables or disables the baseline. The default is false. See Creating Baseline Thresholds, page 11-10.

Table B-3 ppm thresholdtool Parameters (continued)

Parameter	Description
-c	The KPI name.
-d	The threshold applicable days, indicated with true or false separated by “,” Monday through Sunday. The default is true, true, true, true, true, true, true, which means the threshold applies to all days of the week.
-e	Enables or disables the threshold. The default is true, enabled.
-f	The from email address. To set to null, enter "".
-g	The message to send. To set to null, enter "".
-h	Prints help information.
-i	The threshold interval. The default is 15MIN.
-j	The email subject. To set to null, enter "".
-m	The email address to receive the message. To set to null, enter "".
-n	The threshold name.
-o	The output type: xml or json. (Blank is legacy, xml.)
-p	Specifies a port to connect to. If unspecified, the default value is obtained from the WEB_PORT property in the gateway server System.properties file.
-r	The KPI report.
-s	The threshold scope. The default is default, that is, all applicable devices.
-t	The threshold begin and end time, separated by “,”. The format is hh:mm,aa,hh:mm,The default is 12:00,AM,12:00,AM which means the threshold applies to the entire day.
-x	Specifies the tenant list, which is a list of tenant names separated by commas with no spaces. Examples: • ALL • ALL_TENANTS • MyCustomer1,MyCustomer2
-A	The threshold alarm nature. Default is “ADAC”.
-B	Sets the baseline method and window size. Format, Operation,WindowSize. Examples: • average,10 • exponential\ average,12 • exponential\ average,12
-C	The critical alarm threshold values separated by “,”. Format: Onset,Onset Occurrences, Abate,Abate Occurences, [Policy Override]. Example: 95,1, 90, 1.
-D	The threshold description.
-E	Indicates if the continuous alarm is enabled. Default is “false” (disabled).
-H	Specifies a hostname to connect to. If unspecified, the default value is obtained from the SERVER_NAME property in the gateway server System.properties file.
-I	The informational alarm threshold values separated by “,”. Format: Onset, Onset Occurrences, Abate,Abate Occurences, [Policy Override]. Example: 55,1, 50, 1.

Table B-3 ppm thresholdtool Parameters (continued)

Parameter	Description
-L	The threshold alarm script.
-M	The major alarm threshold values separated by “,”. Format: Onset,Onset Occurrences, Abate,Abate Occurences, [Policy Override]. Example: 85,1, 80, 1.
-N	The minor alarm threshold values separated by “,”. Format: Onset,Onset Occurrences, Abate,Abate Occurences, [Policy Override]. Example: 5,1, 70, 1.
-P	The threshold probable cause. The default is ThresholdCrossed.
-R	The threshold type: “true” for rising and “false” for falling. Default is “true”.
-S	Specifies whether to use SSL (https) for NBAPI access. The default is no SSL.
-T	The threshold alarm type. The default is Communications.
-W	The warning alarm threshold values separated by “,”. Format: Onset,Onset Occurrences, Abate,Abate Occurences, [Policy Override]. Example: 65,1, 60, 1.

You must log in as the root user to use this command.

Available in GUI

Yes

ppmtoerrcount

Syntax

/opt/CSCOppm-gw/bin/ppm toerrcount [*number*]

Command Description

Sets the number of timeouts allowed in a report sequence. This command and the ppm nontoerrcount command control the number of polling errors to get from a device in a polling sequence before giving up on that entire polling sequence.The default is 0.

Available in GUI

No

Related Topic

- ppm nontoerrcount, page B-65

ppm tomcatver

Syntax

/opt/CSCOppm-gw/bin/ppm tomcatver

Command Description

Displays the version of Tomcat that is used.

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 topxxsizenetflow

Syntax

/opt/CSCOppm-gw/bin/ppm topxxsizenetflow [*number*]

Command Description

Sets the number of entries displayed in the Top *nn* NetFlow reports. By default, Prime Performance Manager displays the top 10 entries. This command can be used to change the default.

Note Before the Top XX feature can be implemented, you must modify the NetFlow report. See Setting Up NetFlow Reports, page 8-17.

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 tune

Syntax

/opt/CSCOppm-gw/bin/ppm tune [small | med | large | verylarge | verylargedist | extreme | extreme5min | max | medepc | epcsingle | epcdist | smallcell | netflow | collectd | esxi | dcm | kvm | ceph | largegeo]

Command Description

You use this command to tune Prime Performance Manager for different size networks and technologies. Most command options are described in the "Installation Requirements" in the *Cisco Prime Performance Manager 1.7 Quick Start Guide.*

Command options:

- small—Proof of concept single-server installation.
- med—Medium network single-server installation.
- large—Large network single-server installation.
- verylarge—Very large network single-server installation.
- verylargedist—Very large network distributed server installation.
- extreme—Extremely large network distributed server installation.
- extreme5min—Extremely large network distributed server installation with 5-minute reports enabled.
- max—Maximum supported network distributed server installation.
- medepc—Mediume Evolved Packet Core (StarOS) installation.
- epcsingle—Single-server Evolved Packet Core installation.
- epcdists—Distributed server Evolved Packet Core installation.
- smallcell—Small cell support.
- netflow—NetFlow support.
- collectd—collectd support
- esxi—ESXi hypervisor support.
- dcm—Data Collection Manager support.
- kvm—KVM hypervisor support.
- ceph—Ceph support.
- largegeo—Large geographical HA support.

You must log in as the root user to use this command.

Available in GUI

No

ppm uadisable

Syntax

/opt/CSCOppm-gw/bin/ppm disenable

Command Description

Disables user access and SSL on a collocated server.

You must log in as the root user to use this command.

Available in GUI

No

ppm uaenable

Syntax

/opt/CSCOppm-gw/bin/ppm uaenable

Command Description

Enables user access and SSL on a collocated server (gateway and unit installed on the same server). The command performs all the SSL functions including key generation and swapping between gateway and unit, and prompting for creation of the first admin user.

You must log in as the root user to use this command.

Available in GUI

No

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 Enabling User Accounts and Passwords Using the CLI, page 6-24 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 upgradelog

Syntax

/opt/CSCOppm-gw/bin/ppm upgradelog

Command Description

Displays the latest upgrade log.

You must log in as the root user to use this command.

Available in GUI

No

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

Enabling User Accounts and Passwords Using the CLI, page 6-24

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 webport

Syntax

/opt/CSCOppm-gw/bin/ppm webport

Command Description

Displays port number and allows to change the JSP/Web Server port number.

You must log in as the root user to use this command.

Available in GUI

No

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** [*package*] **-a** [*Action*] **-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

ppm zipoldbackups

Syntax

/opt/CSCOppm-gw/bin/ppm zipoldbackups [**disable | enable | status**] [**gw | unit | both**]

Command Description

If enabled, zips Prime Performance Manager backups older than the number of days specified by ppm backupdays. If disabled, backups older than the number of specified backup days are deleted.

- **enabled**—(default) Backups older than the specified backup days are automatically zipped.
- **disabled**—Backups older than the specified backup days are deleted.
- **status**—Displays the ppm zipppmbackups status.
- **gw**—Backs up the gateway.
- **unit**—Backs up the unit.
- **both**—Backs up the gateway and unit.

Available in GUI

Yes

Related Topic

- ppm backupdays, page B-14

Predefined Thresholds

You can create thresholds for any Prime Performance Manager report key performance indicator. For information about creating and managing thresholds, see Chapter 11, "Creating and Managing Thresholds." Prime Performance Manager is delivered with predefined thresholds that cover common scenarios. These are listed in the following sections.

Utilization

- CEPH Global Space Utilization
- CEPH OSD Space Utilization
- CPU Utilization
- Memory Utilization

Availability

- CEPH OSD Unavailable Percentage
- CEPH Monitor Unavailable Percentage
- 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
- 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

Compliance

The following topics provide Prime Performance Manager compliance information:

StarOS BulkStats

You can display the StartOS BulkStats version using ppm status and ppm bulkstatsver commands, for example:

```
/opt/CSCOppm-gw/bin/ppm status
Prime Performance Manager Gateway Version: 1.7.0.000
Prime Performance Manager Gateway Build: Wed Apr 29 04:06 EDT 2015
Prime Performance Manager Gateway Install: Wed Apr 29 04:34 EDT 2015
Prime Performance Manager Gateway Hostname: mwtm-ucs-vm44
Prime Performance Manager Gateway SSL Support: Installed [Disabled]
Prime Performance Manager Gateway StarOS BulkStats: Version-18.1
```

Or,

```
/opt/CSCOppm-gw/bin/ppm bulkstatsver
StarOS BulkStats Version: Version-18.1
```

MIBs

Prime Performance Manager provides a list of device MIBs including release and compliance levels on a per-object basis.

You can use the ppm mibver command to display a list of all MIBs and MIB versions that ship with Prime Performance Manager:

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

Prime Performance Manager does not poll the Starent MIBs. It retrieves only the following SNMP-based reports:

- MemoryPool using the CISCO-ENHANCED-MEMPOOL-MIB
- Interface using IETF standard IF-MIB.

To show the version of the Starent IF-MIB, and CISCO-ENHANCED-MEMPOOL-MIB, enter the ppm mibver staros command:

```
/opt/CSCOppm-gw/bin/ppm mibver staros
```

StarOS

Prime Performance Manager provides metrics on StarOS schemas, counters, and ALL_COUNTERS tables. To view, from the Help menu, choose **Reports > Reports List Readme**. Scroll to the StarOS section near the end of the file to view:

- BulkStats version
- List of supported schemas
- Number of counters in each schema
- List of ALL_COUNTERS database tables and web report names

Other StarOS counter information is provided at the end of the Reports List Readme. Prime Performance Manager supports all schema counters for each supported StarOS version. It also supports all counters in any schema for that specific BulkStats version in the AllCounters reports.

DB, CSV, and WebReport are all automatically supported.

Cisco ASR 5000 StarOS Key Performance Indicators

Prime Performance Manager is compliant with the Cisco ASR 5000 Series Key Performance Indicator Guide 7.0 Global Mobility Practice.

SNMP, SOAP, HTTP, JSON and 3GPP Versions and Standards

Prime Performance Manager is compliant with the following SNMP, SOAP, HTTP, JSON, and 3GPP standards and versions:

- SNMPv1, SNMPv2, SNMPv3
- SOAPv1.1
- HTTPv1.1
- JSON—IETF RFC 7159
- 3GPP
  - TS 32.432 Release 9: Performance Measurement File Format Definition
  - TS 32.435 Release 9: Performance measurement eXtensible Markup Language (XML) File Format Definition

Small Cell KPIs

Prime Performance Manager includes KPI documents in Microsoft Word and Excel for each Small Cell report. To view the documents, displaying the report in GUI, then on the report toolbar click the blue help icon to display the Report Help. Links to the KPI documents are provided at the top of the report information, for example:

```
================================================
Definition File:
     rmsApPerf.xml  (Product Viewer)
     rmsApPerf.xml  (Browser Viewer - Use View Page Source Menu For Color Coded View)

   rmsApPerf.properties  (Product Viewer)

Custom Help

SmallCell KPI Reference (DOC)
SmallCell KPI Reference (XLS)
SmallCellVersions.properties
================================================
rmsApPerf.xml
```

Small Cell Devices

To view supported Small Cell devices, from the Help menu, choose **Readmes and CLI Commands**, then click **Devices Info**. For example:

```
SmallCell
=========

   RMS 4.1, RMS 4.1 Hotfix4
   RMS 5.0, RMS 5.1
   AP USC 3.4, 3.5, 3.5.8.10, 3.5.X MR, 3.5.10, 3.5.11
   ULS 9.2
   PMG 4.1.0
   PAR 6.0.1-5
   BAC 3.8.1, 3.8.1.1
   BAC 3.9.0
   PNR 8.1.3-2
```

You can also use the ppm smallcellver command to display the latest version of software supported for each device:

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